The choice of optical system is critical for the security of double random phase encryption systems

Inbarasan Muniraj[1], Changliang Guo[1], Ra'ed Malallah[1, 2], Liang Zhao[1,3] Derek Cassidy[1], James P Ryle[1], John J Healy[1†], John T Sheridan[1]*
[1]School of Electrical and Electronic Engineering, IOE[2] Lab, University College Dublin, Ireland.
[2]Physics Department, Faculty of Science, University of Basrah, Garmat Ali, Basrah, Iraq.
[3]The Insight Centre for Data Analytics, University College Dublin, Belfield, Dublin 4, Ireland.
Corresponding Authors: *john.sheridan@ucd.ie, †john.healy@ucd.ie.

ABSTRACT

The linear canonical transform (LCT) is used in modeling a coherent light field propagation through first-order optical systems. Recently, a generic optical system, known as the Quadratic Phase Encoding System (QPES), for encrypting a two-dimensional (2D) image has been reported. In such systems, two random phase keys and the individual LCT parameters (α, β, γ) serve as secret keys of the cryptosystem. It is important that such encryption systems also satisfies some dynamic security properties. In this work, we therefore examine such systems using two cryptographic evaluation methods, the *avalanche effect* and *bit independence criterion*, which indicate the degree of security of the cryptographic algorithms using QPES. We compared 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 compared to the conventional Fourier and Fresnel based encryption systems.

Keywords: Quadratic Phase Encoding system, linear canonical transform, Double Random Phase Encryption, Avalanche effect and bit independence criterion.

1. INTRODUCTION

The ubiquitous use of multimedia communication systems, the risk of attacks thereon and the resulting theft of private data from secured systems have led to the demand for ever improving information security techniques [1-3]. 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 [4-6]. Often both processes, i.e., hiding and encryption, are simultaneously employed. Among them, a technique proposed by Refregier *et al* [7], known as Double Random Phase Encryption (DRPE), using the 4*f* optical processor has received particular attention. Principally, this algorithm

turns an intensity image into an unreadable format by using two randomly distributed 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 [7]. In addition to this conventional technique, some of its extensions have also been examined in the fractional Fourier domain [8], the Fresnel transform domain [9], the Hartley transform [10], and the Arnold transform based encoding systems [11]. Furthermore, optical encryption techniques can also be implemented as a cryptographic algorithm (i.e., numerical approximations) and such implementations were shown to be vulnerable to some organized attacks [12-15].

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 [16]. Among its special cases are the Fourier transform (FT), the Fractional Fourier transform (FRT), the Fresnel transform (FST), and the Gyrator transform (GT) [17]. Since the conventional encryption technique has shown to be vulnerable for phase retrieval based attacks [18, 19] such as Chosen Ciphertext Attack (CCA), Ciphertext Only Attacks (COA) and Known Plaintext-Ciphertext Attack (KPCA), Unnikrishnan *et al* have proposed a generalized cryptosystem using Quadratic Phase Encoding System [20]. 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 [20].

In principle, the cryptographic algorithms should satisfy some dynamic properties such as the Avalanche Effect (AE), and Bit Independence Criterion (BIC) which tell us the relationship between the plaintext and ciphertext [21-23]. Recently, Moon *et al* have demonstrated Avalanche and bit independence characteristics of DRPE in the classical Fourier and Fresnel domains. As noted, the generalized LCT constitute a parameterized continuum of the classical transforms that includes the Laplace, the Fourier transform (FT), the fractional Fourier transform (FRT), the Fresnel transform (FST), in this paper, we present an analysis of AE and BIC for the generalized LCT based DRPE. Furthermore, a comparison is made with the existing systems that are based on the classical Fourier, Fresnel transforms based DRPE systems. Result shows that the LCT based DRPE system augments the key space and thus enhances the data security.

This paper is structured as follows: In Section 2, we briefly review the Fourier, the Fresnel and the LCT based DRPE systems, respectively. The concepts of the avalanche effect and bit independence are discussed in Section 3. In Section 4, we show our computer simulation results. Finally, we conclude our discussions in Section 5.

2. DOUBLE RANDOM PHASE ENCODING (DRPE)

The rapid development of communication systems indicates the need for both higher levels of data security and intellectual property protection. Data protection techniques, include steganography, watermarking, copy-move forgery detection, encryption are in increasing demand [24-31]. The simplicity and elegance of the classical Fourier based Double Random Phase Encryption system (DRPE), has led to proposals for numerous techniques over the past two decades [4]. The reason for plenty of optically inspired encryption system proposed in the literature was that it can offer the possibility of high-speed parallel processing of data. In addition to this, the ability to conceal information using multiple degrees of freedom such as the amplitude, phase, wavelength, polarization, fractional orders, and propagation distances available when using linear lossless paraxial optical systems makes DRPE in the limelight [4-6]. It is known that in optical encryption system, diffracted light from the object passes through one another and thus can additionally be combined in novel passive multiplexing schemes. Typically, such optical security systems require the modulation and capture of the full complex encrypted field information, i.e., both the intensity and the phase, involving for example digital holographic (DH) and interferometric techniques [32-35]. In following, we briefly review the fundamental optical encryption methods.

2.1. The classical Fourier transform based DRPE

The classical encryption system, proposed by Refregier *et al*., uses the 4*f* optical system to encode the information [7]. Figure 1 shows the schematic setup of classical amplitude encoding DRPE system in the Fourier domain. As it can be seen, it involves multiplication of the diffracted input light field by random phase masks or keys (RPMs) placed both in the input (space) and the Fourier (spatial frequency) domains. We note that RPMs can be implemented using, for example, ground glass, optical diffusers or suitable modulated spatial light modulator (SLM) [35].

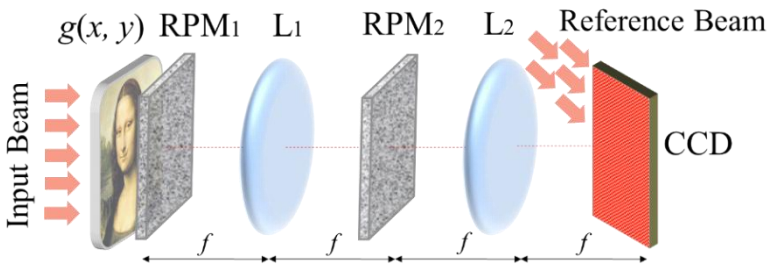

Fig. 1. A possible optical implementation of DRPE in the Fourier domain. L_1, L_2 refers the Fourier lens and the primary optical axis is shown in Red color dotted line.

Let, $g(x,y)$, represent the spatial coordinates of a two dimensional (2D) signal or an image. 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, are used to encrypt the 2D image. Here, the phase keys $n_1(x,y), n_2(x',y')$ are statistically independent and uniformly distributed in $[-0.5, 0.5]$. First, the input image is multiplied 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 is defined as follows,

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

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. The decryption process is said to be an inverse procedure of encryption process, thus the original intensity image can be retrieved by using the secret phase keys [5].

2.2. The Fresnel transform based DRPE

In this section, we briefly analyze the concept of a lens-less optical DRPE encryption system proposed by Situ *et al* [9]. It is reported that this system is more flexible and the simplest way of encryption, in which the illuminated light wavelength can also be regarded as a secret key. The encryption system shown in Fig. 2, is illuminated by a plane wave with the operational wavelength λ.

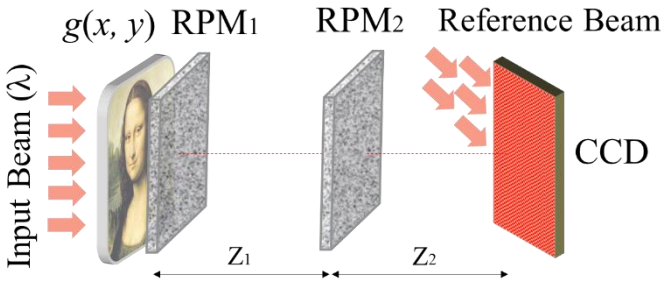

Fig. 2. Optical schematic setup for DRPE in the Fresnel domain: λ operational wavelength, z_1, z_2 are the propagation distances.

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 [36], 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 the propagation distances z_1 and z_2. As it can be seen in Eq. (2) that the security of an encrypted image $E(x'',y'')$ in Fresnel based system 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)[9].

2.3. The Linear Canonical Transform based DRPE

Owing to the inherent capabilities of optical signal processing, various extensions to the classical DRPE have been proposed and implemented. For instance, FT-based DRPE is replaced by the fractional Fourier Transform (FRT) [8], Fresnel Transform (FST) [9], or Hartley Transform (GT) [10], to mention a few. Since the FT, FRT, FST are the special cases (or the subsets) of the linear canonical transform (LCT), the use of the LCT has also been proposed for optical encryption using quadratic phase systems [20]. In this case, the three independent QPS transformation parameters provide further extra keys for the encryption system and thus augments the security. The LCT is a three-parameter class of linear integral transform and 2D separable LCT is defined as [16]:

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

Where α,β,γ represents the real canonical transform parameters. We briefly describe the LCT-based DRPE system [19, 20]. At first, the primary amplitude image, $g(x,y)$, is modulated by 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 [19]:

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

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 $exp\{i\pi\gamma_1(x'^2+y'^2)\}$ [19]. Thus, Eq. (4) can be rewritten as,

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

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

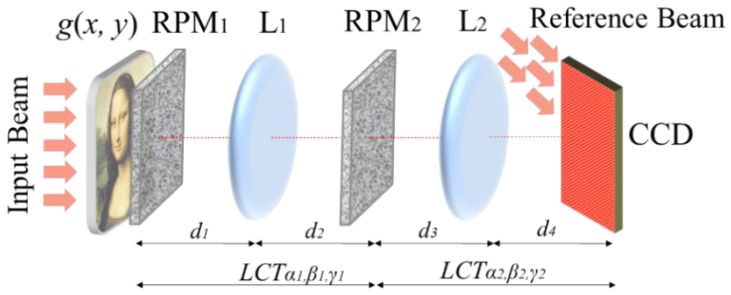

Fig. 3. Optical schematic setup for DRPE in the linear Canonical domain.

The encrypted image is complex-valued and resembles a noisy signal. The decryption process involved, when using this LCT based DRPE system, is given by [19]:

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

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 [16, 19]:

$$\begin{aligned} \alpha_1 &= \frac{d_1 - f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]}, \\ \beta_1 &= \frac{f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]}, \\ \gamma_1 &= \frac{d_2 - f_1}{\lambda[f_1(d_1 + d_2) - d_1 d_2]}. \end{aligned} \quad (7)$$

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 [16].

3. SECURITY ANALYSIS

3.1. Avalanche Criterion (AVAC)

H. Feistel *et al.*, first defined the Avalanche Criterion (AVAC) as a desirable property for the Substitution and Permutation Networks (SPNs) [37]. AVAC is considered an important cryptographic property, which says that even a

tiny amount of changes in the plaintext (or key) leads to an "unpredictable avalanche" of 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 [37-39]. 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 effect (AE)) can be measured using (two different strings of equal length) Hamming distance (H), which gives the number of changed bits. Let us consider an example of 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: $H(C, C') = H(110011001100, 0011110101) = 4$. Similarly, in order to measure AVAC that occurs in the encrypted image and when the input image bits are inverted, we use the following equation [23]:

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

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 it is a satisfactory avalanche effect.

3.2. Bit Independence Criterion (BIC)

A. F. Webster *et al* defined the Bit Independence Criterion (BIC) for S-boxes [40]. Briefly, a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ said to be satisfying to BIC, when 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's 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 ciphertexts 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 [40]:

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

where $C(b_i)$ and $C\left(b_j\right)$ represent 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 $BI\left[C(b_i), C(b_j)\right]$ is close to 1

i.e., 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:

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

Where $i \neq j$ and we note that when $BIC[E(X,K)]$ is much 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 52×52 pixels image (see Fig. 4(a)) in order to measure the avalanche effect and the bit independence criterion. In order to analyze the proposed encryption methods (i.e., FT, FST, LCT-based DRPE) in bit units, each pixel intensity value in the input plaintext and the phase keys 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 [41]. This uses 64 bits (i.e., 1 sign bit, 11 bits for exponent width, and 52 bits for significant digits) as shown in Fig. 4 (b). 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.

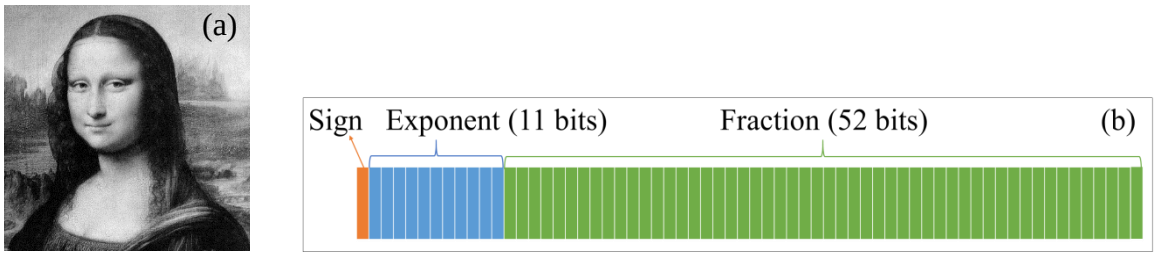

Fig. 4: (a) Grayscale test image used in our simulations and (b) IEEE 754 double-precision binary floating-point format.

We note that except the classical Fourier transform (single transform) based encryption, all the other transform-based encryption systems (considered in this work) uses additional security keys. Therefore, in our simulations, for the Fresnel z_1 = 24 mm, z_2 = 32 mm and λ = 0.632 μm, and the LCT has six additional parameters α_1 = 613.51, β_1 = 1932.49, γ_1 =927.27, α_2 = 496.43, β_2 = 0.44, γ_2 =835.49 are considered. Figure 5 shows the measured avalanche effect, using Eq. (8), plotted against the varying number of flipped bits (i.e., both the bit, pixel units) in the plaintext of the DRPE system in the FT, FST, and LCT domains, respectively. 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, on average, achieves lower AE values.

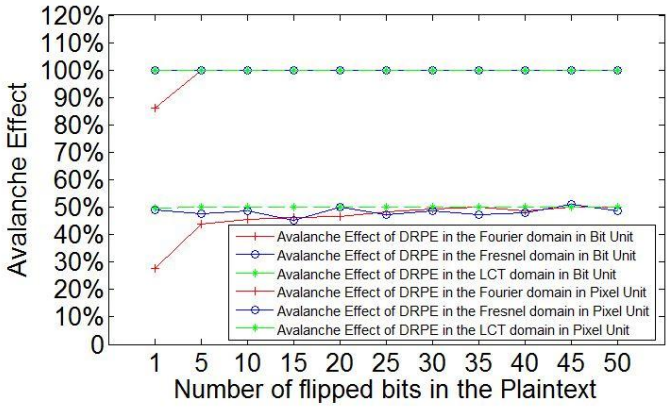

Fig. 5. AVAC with varying number of perturbed bits in the plaintext. Bit unit refers that the encrypted image is compared in binary units, the Pixel unit represents the encrypted image is compared in pixel values.

We interpret these results as the fact that when just 1 bit is inverted in the plaintext, almost all of the ciphertext values will be changed in the LCT, and FST (note that 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 the chirp function [17]. In the FST based DRPE, we use 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 [13]. Whereas, the chirp function becomes unity in the Fourier domain. As a consequence, the conventional FT based DRPE system did not achieve a satisfactory avalanche effect for the lower bit perturbation.

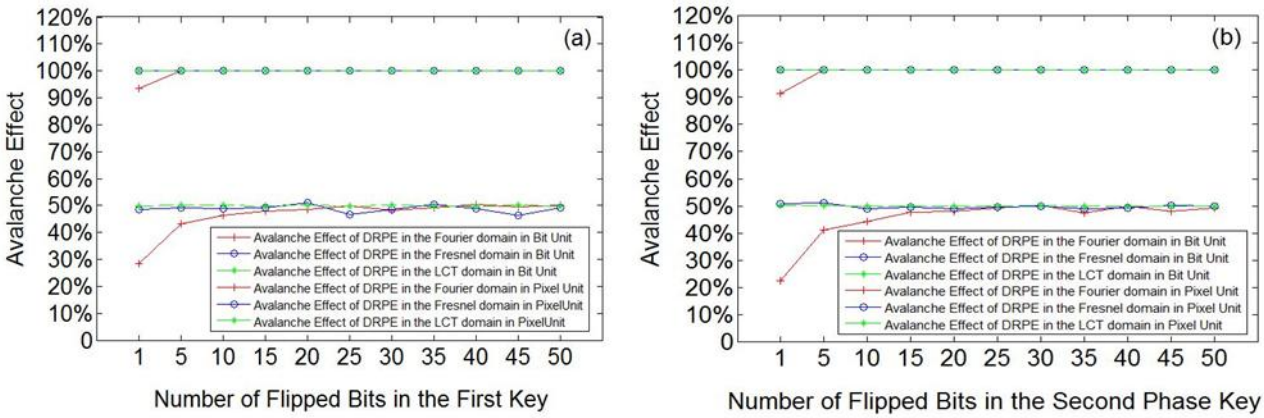

Fig. 6. Simulated results for the Avalanche effect with varying number of bits in the perturbed phase keys. (a) Avalanche effect with bits changed in the first phase key (RPM_1) (b) Avalanche effect with bits changed in the second phase key (RPM_2).

Figure 6 shows the calculated AVAC values plotted against the varying number of flipped bits in the first and second phase keys (RPMs) of the DRPE system in the FT, FST, and LCT domains, respectively. As it can be seen, when only one bit was flipped either of the input phase keys (i.e., first or second phase key) we get similar 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 keys were flipped. Similarly, in the pixel values, DRPE in LCT, FST domains stay at 100% while that in the FT based system increases to be 100% after about five bits in the phase keys are changed.

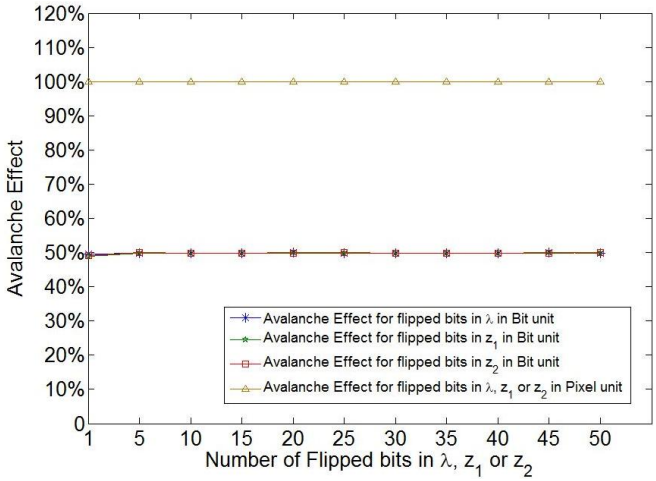

Fig. 7. Avalanche effect with some bits in the wavelength (λ) and two distance values (z_1, z_2) are perturbed.

In contrast to the DRPE in the Fourier domain, the DRPE in the Fresnel domain considers the wavelength and the two propagation distance values as additional security keys. Thus, the avalanche effects for these additional keys were also examined. The corresponding results are depicted in Fig. 7. The results demonstrate that the avalanche effect for the

FST-based DRPE with bits flipped in λ, z_1, and z_2 are performing good since the values are close to 50%. Also, we note that, each of the pixel values are altered when a slight change is made to a bit in λ, z_1, or z_2. Similarly, as noted, LCT-based DRPE introduces at least 6 additional parameters (keys) to the encryption system. The results of avalanche effects for these additional keys are analyzed and shown in Fig. 8. As it can be seen, the avalanche effect for the DRPE in the LCT domain with perturbed bits in α_1, β_1, γ_1 and α_2, β_2, γ_2 are very sensitive as the values are 50%. From these simulation results, we may, therefore, conclude that the DRPE in the LCT domain has a better avalanche effect than the DRPE in the Fresnel and Fourier domains. This result validates the fact that each of the key parameters in an encryption system is a significant contributor to the security of DRPE in the LCT domain.

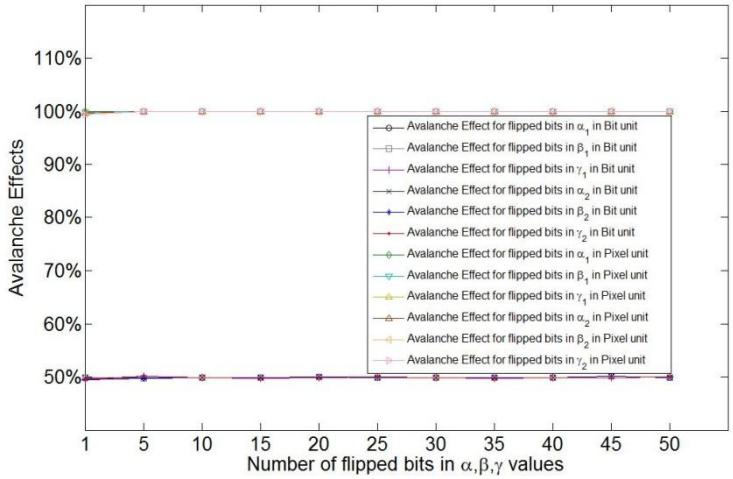

Fig. 8. Avalanche effect with some bits in α_1, β_1, γ_1 and α_2, β_2, γ_2 are flipped.

DRPE system	Perturbed texts in	Bit Independence Criterion
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

Table 1. Bit Independence Criterion (BIC) for the DRPE in the FT, the FST and the LCT based domains.

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. 10. Table 1 shows the bit independence results for the FT, FST, and LCT based DRPE system. As it can be seen from Table 1, the bit independence values for the DRPE systems, employed in this study, are far away from 1, in other words correlation lesser than 1, meaning that the DRPE possess a satisfactory bit independence property. Furthermore, these results also prove the fact that when an input image is encrypted using the amplitude-encoding DRPE system, knowledge of the first phase key, i.e., RPM_1 is not necessary (in other words not significant) during the decryption process [18]. We note that the computed avalanche effect and bit independence values are calculated by averaging 100 consecutive simulation results.

5. CONCLUSION

We presented a method for calculating the avalanche effect and the bit independence criterion (which are common metrics used in evaluating the block cipher algorithms) on optical 4*f* based double random phase encryption (DRPE) system in the Fourier (FT), the Fresnel (FST) and the linear canonical transformation (LCT) domains. Simulation results show that LCT based DRPE system achieves excellent performance in the sense of better avalanche effect and bit independence properties than that both of the Fourier and Fresnel transform based DRPE system. To be more precise, the avalanche effect values in the DRPE in the linear canonical and Fresnel domains achieve superior results than that in the DRPE in the Fourier domain. These results validate the fact that each of the keys in an encryption system is a significant contributor to the security of encryption system. Thus, a slight change either in the plaintext or the phase keys fail to realize a satisfactory avalanche effect or bit independence criterion.

ACKNOWLEDGEMENT

IM acknowledges the support of Irish Research Council (IRC). RM is supported by the Iraqi Ministry of Higher Education and Scientific Research. CG, LZ, DC, JPR, JJH and JTS thanks Science Foundation Ireland (SFI), and Enterprise Ireland (EI) under the National Development Plan (NDP).

REFERENCES

[1] Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," Appl. Opt. 39, 5295-5301 (2000).
[2] D. Abookasis, O. Montal, O. Abramson, and J. Rosen, "Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator," Appl. Opt. 44, 3019-3023 (2005).
[3] J. Glückstad and D. Z. Palima, [Generalized Phase Contrast: Applications in Optics and Photonics], Springer Series in Optical Sciences, (2009).
[4] A. Alfalou, and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon 1(3), 589-636 (2009).
[5] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt Laser Technol 57, 327-342 (2014).
[6] B. Javidi, [Optical and digital techniques for information security], Springer, New York, 241-269 (2005).
[7] P. Refregier, and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett 20(7), 767-769 (1995).
[8] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain," Opt. Lett 25(12), 887-889 (2000).
[9] G. Situ, and J. Zhang, "Double random phase encoding in the Fresnel domain," Opt. Lett 29(14), 1584-1586 (2004).
[10] I. Muniraj, C. Guo, B. G. Lee, and J. T. Sheridan, "Interferometry based multispectral photon-limited 2D and 3D integral image encryption employing the Hartley transform," Opt. Exp 23(12), 15907-15920 (2015).
[11] N. Rawat, R. Kumar, B. Kim, and B. G. Lee, "Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique," Optik 127 (12), 2282–2286 (2016).
[12] A. Carnicer, M. M. Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett 30(13), 1644-1646 (2005).
[13] G. Unnikrishnan. D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Exp 14(8), 3181-3186 (2006).
[14] W. Liu, G. Yang, and H. Xie, "A hybrid heuristic algorithm to improve known plaintext attack on Fourier plane encryption," Opt. Exp 17(16), 13928-13938 (2009).
[15] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett 31(8), 1044–1046 (2006).
[16] J. J. Healy, M. A. Kutay, H. M. Ozaktas, and J. T. Sheridan, [Linear Canonical Transforms], Springer, New York, (2016).
[17] L. Zhao, J. J. Healy, and J. T. Sheridan, "Two-dimensional nonseparable linear canonical transform: sampling theorem and unitary discretization," J. Opt. Soc. Am. A 31(12), 2631-2641 (2014).
[18] C. Guo, S. Liu, and J. T. Sheridan, "Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems," Appl. Opt 54(15), 4709-4719 (2015).
[19] C. Guo, I. Muniraj, and J. T. Sheridan, "Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," Appl. Opt 55(17), 4720-4728 (2016).
[20] G. Unnikrishnan, and K. Singh, "Optical encryption using quadratic phase systems," Opt. Commun. 193(1-6), 51-67 (2001).

[21] W. Stallings, [Cryptography and network security Principles and Practice], Prentice Hall, New York, Chapter 3, (2011).
[22] H. C. V. Tilborg, and S. Jajodia, [Encyclopedia of cryptography and security], Springer Science & Business Media, Netherlands, 598-602 (2005).
[23] I. Moon, F. Yi, Y. H. Lee, and B. Javidi, "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).
[24] Z. Fu, X. Wu, C. Guan, X. Sun and K. Ren, "Toward Efficient Multi-keyword Fuzzy Search over Encrypted Outsourced Data with Accuracy Improvement", IEEE Trans on Info Forensics and Security. 11 (12), 2706-2716 (2016).
[25] Z. Fu, F. Huang, X. Sun, A. V. Vasilakos, and C. N. Yang, "Enabling Semantic Search based on Conceptual Graphs over Encrypted Outsourced Data," IEEE Trans on Services Computing, PP (99) 1-1 (2016).
[26] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based Image Copy-move Forgery Detection Scheme," IEEE Trans on Info Forensics and Security. 10 (3), 507-518 (2015).
[27] C. Yuan, X. Sun, and L.V. Rui, "Fingerprint Liveness Detection Based on Multi-Scale LPQ and PCA," China Commun. 13(7), 60-65 (2016).
[28] J. Wang, T. Li, Y. Q. Shi, S. Lian, and J. Ye, "Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics", Multimedia Tools and Applications, Springer Science & Business Media (2016).
[29] Z. Xia, X. Wang, X. Sun, Q. Liu, and N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels," Multimedia Tools and Applications. 75(4), 1947-1962 (2016).
[30] Z. Zhou, C. N. Yang, B. Chen, X. Sun, Q. Liu, and Q. M. J. Wu, "Effective and Efficient Image Copy Detection with Resistance to Arbitrary Rotation," IEICE Transactions on information and systems. E99-D(6), 1531-1540 (2016).
[31] B. Chen, H. Shu, G. Coatrieux, G. Chen, X. Sun, and J. L. Coatrieux, "Color image analysis by quaternion-type moments," Journal of Mathematical Imaging and Vision. 51(1), 124-144 (2015).
[32] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. 39(35), 6595–6601 (2000).
[33] B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. 25(1), 28–30 (2000).
[34] O. Matoba and B. Javidi, "Secure Holographic Memory by Double Random Polarization Encryption," Appl. Opt. 43, 2915–2919, (2004).
[35] A. Vijayakumar, Y. Kashter, R. Kelner, and J. Rosen, "Coded aperture correlation holography–a new type of incoherent digital holograms," Opt. Express 24, 12430-12441 (2016).
[36] J. W. Goodman, [Introduction to Fourier Optics], the McGraw-Hill, Chapter 4 (1968).
[37] H. Feistel, [Cryptography and computer privacy], Sci. Am. 228, 15-23 (1973).
[38] I. Vergili, and M. D. Yücel, "Avalanche and bit independence properties for the ensembles of randomly chosen n×n S-boxes," Turk. J. Elec. Eng., 9(2), 137-146 (2001).
[39] G. Arumugam, V. L. Prabha, and S. Radhakrishnan, "Study of chaos functions for their suitability in generating Message Authentication Codes," Appl. S. Comp 7(3), 1064-1071 (2007).
[40] A. F. Webster, and S. E. Tavares, "On the design of S-boxes," Advance in Cryptology: Proc.Crypto'85, Springer-Verlag, Berlin 218, 523-534 (1986).
[41] IEEE, "IEEE standard Floating-Point Arithmetic," IEEE. Std 754™-2008, 1-58 (2008).