Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

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

Inbarasan Muniraj
Changliang Guo
Ra'ed Malallah
Derek Cassidy
Liang Zhao
James P. Ryle
John J. Healy
John T. Sheridan

SPIE.

Inbarasan Muniraj, Changliang Guo, Ra'ed Malallah, Derek Cassidy, Liang Zhao, James P. Ryle, John J. Healy, John T. Sheridan, "Choice of optical system is critical for the security of double random phase encryption systems," *Opt. Eng.* **56**(6), 063103 (2017), doi: 10.1117/1.OE.56.6.063103.

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

Inbarasan Muniraj,[a] Changliang Guo,[a] Ra'ed Malallah,[a,b] Derek Cassidy,[a] Liang Zhao,[a,c] James P. Ryle,[a] John J. Healy,[a,*] and John T. Sheridan[a,*]
[a]University College Dublin, School of Electrical and Electronic Engineering, IOE[2] Lab, Dublin, Ireland
[b]University of Basrah, Physics Department, Faculty of Science, Garmat Ali, Basrah, Iraq
[c]University College Dublin, The Insight Centre for Data Analytics, Belfield, Dublin, Ireland

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 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 satisfy some dynamic security properties. 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 double random phase encryption (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. [DOI: 10.1117/1.OE.56.6.063103]

Keywords: quadratic phase encoding system; linear canonical transform; double random phase encryption; avalanche effect and bit independence criterion.

Paper 170482P received Mar. 30, 2017; accepted for publication May 26, 2017; published online Jun. 14, 2017.

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 are 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 and Javidi,[7] known as double random phase encryption (DRPE), using the $4f$ 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 are complex and 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 transform (FRT) domain ,[8] the Fresnel transform (FST) domain,[9] the Hartley transform (HT),[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 FRT, the 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, ciphertext only attacks, and known plaintext-ciphertext attack, Unnikrishnan and Singh[20] have proposed a generalized cryptosystem using a quadratic phase encoding system (QPS). It has been reported that the data are encrypted, in the canonical transformation domain, with the help of two random phase masks (RPMs), 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 (BI) characteristics of DRPE in the classical Fourier and Fresnel domains. As noted, the generalized LCT constitute a parameterized continuum of the classical transforms that include the Laplace, the FT, the FRT, and the FST, and 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, FSTs-based DRPE systems. The 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 Sec. 2, we briefly review the Fourier, the Fresnel, and the LCT-based DRPE systems, respectively. The concepts of the AE and BI are

*Address all correspondence to: John T. Sheridan, E-mail: john.sheridan@ucd.ie; John J. Healy, E-mail: john.healy@ucd.ie

0091-3286/2017/$25.00

discussed in Sec. 3. In Sec. 4, we show our computer simulation results. Finally, we conclude our discussions in Sec. 5.

2 Double Random Phase Encoding

The rapid development of communication systems indicates the need for both higher levels of data security and intellectual property protection. Data protection techniques, including steganography, watermarking, copy-move forgery detection, and encryption are in increasing demand.[24–33] The simplicity and elegance of the classical Fourier-based DRPE system has led to proposals for numerous techniques over the past two decades.[4] The reason for plenty of optically inspired encryption systems proposed in the literature was that they 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 systems, diffracted light from the object passes through one another and thus can additionally be combined in 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 and interferometric techniques.[34–37] In the following sections, we briefly review the fundamental optical encryption methods.

2.1 *Classical Fourier Transform-Based Double Random Phase Encryption*

The classical encryption system, proposed by Refregier and Javidi,[7] uses the $4f$ optical system to encode the information. Figure 1 shows the schematic setup of a classical amplitude encoding DRPE system in the Fourier domain. As it can be seen, it involves multiplication of the diffracted input light field by RPMs or keys 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 a suitable modulated spatial light modulator.[37]

Let $g(x,y)$ represent the spatial coordinates of a two-dimensional (2-D) signal or an image. The 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 2-D 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 FT ($\mathcal{F}$) is performed. Later, the resulting image is modulated by the second phase mask, RPM_2, in the frequency domain. Finally, by taking an inverse FT ($\mathcal{F}^{-1}$), we get the encrypted image $E(x'',y'')$. Mathematically, this process is defined as

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

The encrypted image $E(x'',y'')$ is complex and due to the statistical properties of the two RPMs, $D_1(x,y)$ and $D_2(x',y')$, it is unreadable. The decryption process is said to be an inverse procedure of the encryption process; thus, the original intensity image can be retrieved by using the secret phase keys.[5]

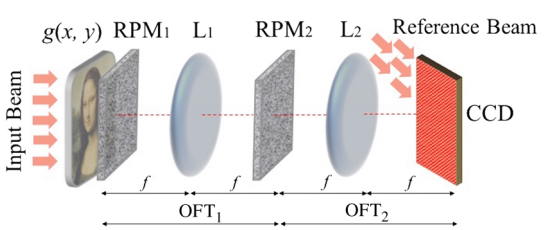

Fig. 1 A possible optical implementation of DRPE in the Fourier domain. L_1, L_2 refers to the Fourier lens and the primary optical axis is shown in red color dotted line.

2.2 *Fresnel Transform-Based Double Random Phase Encryption*

In this section, we briefly analyze the concept of a lens-less optical DRPE encryption system proposed by Situ and Zhang.[9] It is reported that this system is more flexible and the simplest method 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.

First, the primary amplitude image $g(x,y)$ is modulated with the 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 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,[38] the encrypted image is given as

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

where $u(x',y')=\Theta_\lambda\{g(x,y)\exp[in_1(x,y)];z_1\}$. The symbol Θ_λ stands for the FST 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 a Fresnel-based system depends not only on the RPMs (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 *Linear Canonical Transform-Based Double Random Phase Encryption*

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 FRT,[8] FST,[9] or HT,[10] to mention a few.

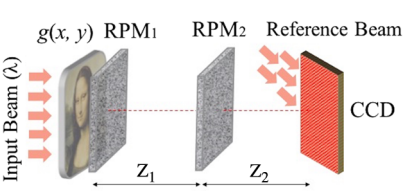

Fig. 2 Optical schematic setup for DRPE in the Fresnel domain: λ operational wavelength, z_1, z_2 are the propagation distances.

Since the FT, FRT, and FST are the special cases (or the subsets) of the 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 augment the security. The LCT is a three-parameter class of linear integral transform and 2-D separable LCT is defined as[16]

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

where $\alpha, \beta,$ and 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 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 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[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

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

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

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 Ref. 19

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

where $\mathcal{F}^{-1}$ represents an inverse FT. As it can be seen in Fig. 3, in the LCT-based DRPE system, together with the 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 Refs. 16 and 19

$$\alpha_1 = \frac{d_1 - f_1}{\lambda[f_1(d_1+d_2) - d_1d_2]},$$
$$\beta_1 = \frac{f_1}{\lambda[f_1(d_1+d_2) - d_1d_2]},$$
$$\gamma_1 = \frac{d_2 - f_1}{\lambda[f_1(d_1+d_2) - d_1d_2]}. \tag{7}$$

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 2-D separable case, the same parameter values (α,β,γ) are applied in both the horizontal (x) and vertical (y) directions.[16]

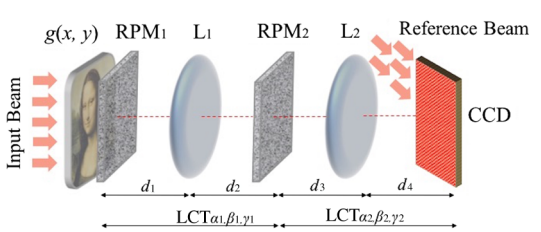

Fig. 3 Optical schematic setup for DRPE in the linear Canonical domain.

3 Security Analysis

3.1 *Avalanche Criterion*

Feistel et al. first defined the avalanche criterion (AVAC) as a desirable property for the substitution and permutation networks.[39] 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 $f:\{0,1\}^n \to \{0,1\}^n$ satisfies AVAC, when a flipped single input bit changes, on average, half of the output bits.[39–41] For instance, the conventional encryption method (E) can be described as $C = E(X,K)$, where C represents the ciphertext and X, K denotes the plaintext and the key, respectively. Suppose that, perturbation is made in the input texts such that $X \to x'$ or $K \to K'$, then the ciphertext will be changed (i.e., C') drastically. Then, the avalanche changes (also known as 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 AE is measured using Hamming distance between C, C' as: $H(C,C') = H(110011001100, 0011110101) = 4$. Similarly, to measure AVAC that occurs in the encrypted image and when the input image bits are inverted, we use[23]

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

where $\mathrm{Num}(C)$ 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 bits changed in either the plaintext or the keys) this usually means that it is a satisfactory AE.

3.2 *Bit Independence Criterion*

Webster and Tavares[42] defined the BIC for S-boxes. Briefly, a function $f:\{0,1\}^n \to \{0,1\}^n$ 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 us 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). Consequently, M ciphertexts can be obtained. Then, the BI between bit j and k in the ciphertext is defined using the absolute correlation coefficient value as[42]

$$\mathrm{BI}[C(b_i), C(b_j)] = |\mathrm{corr}[(b_i^1, \ldots, b_i^m, \ldots, b_i^N), (b_j^1, \ldots, b_j^m, \ldots, b_j^N)]|, \quad (9)$$

where $C(b_i)$ and $C(b_j)$ 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 $\mathrm{BI}[C(b_i), C(b_j)]$ is close to 1, i.e., the compared bits are strongly correlated (i.e., very similar), or else it is uncorrelated (i.e., independent). To measure the BIC on the encrypted image, we used

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

where $i \neq j$ and we note that when $\mathrm{BIC}[E(X,K)]$ is much less than 1 (i.e., BIC $\ll 1$), the encryption satisfies the BIC.

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)] to measure the AE and the BIC. In order to analyze the proposed encryption methods (i.e., FT, FST, and 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.[43] 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 the same for almost all amplitude values, and therefore, perturbation was considered only on the last 52 significant bits, without loss of generality.

We note that except the classical FT-(single transform) based encryption, all the other transform-based encryption systems (considered in this work) use additional security keys. Therefore, in our simulations, for the Fresnel $z_1 = 24$ mm, $z_2 = 32$ mm, and $\lambda = 0.632$ μm, and the LCT has six additional parameters $\alpha_1 = 613.51$, $\beta_1 = 1932.49$, $\gamma_1 = 927.27$, $\alpha_2 = 496.43$, $\beta_2 = 0.44$, $\gamma_2 = 835.49$ are considered. Figure 5 shows the measured AE, 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

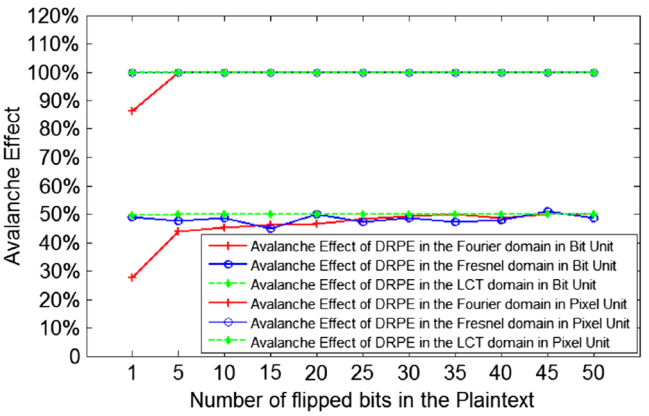

Fig. 5 AVAC with varying number of perturbed bits in the plaintext. Bit unit means that the encrypted image is compared in binary units, the pixel unit represents the encrypted image is compared in pixel values.

from Fig. 5 that the AE for the LCT-based DRPE is better than that in the Fourier and Fresnel domains. The AE value is 50% for DRPE in the LCT domain, while it is a 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.

We interpret these results as the fact that when just 1 bit is inverted in the plaintext, almost all 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, whereas in the LCT-based DRPE we use two chirp functions and that helps the LCT and FST domain to achieve a satisfactory AE,[13] while the chirp function becomes unity (value considered as 1) in the Fourier domain. Consequently, the conventional FT-based DRPE system did not achieve a satisfactory AE for the lower bit perturbation. We also note that a 100% AVAC value indicates that all the pixel values in the amplitude of the encrypted image are perturbed. It also states that in pixel unit it achieves a good AE, as it does not reveal any pixel values for the encrypted image based on the result from plaintext with some bits changed. Thus, the DRPE in the Fourier domain did not achieve a satisfactory AE.

As noted, the security of an encryption system relies on the durability of the phase keys. Therefore, in Fig. 6, we calculated AVAC values against the varying number of flipped bits in the first and second phase keys (RPMs) of the proposed DRPE systems in the FT, FST, and LCT

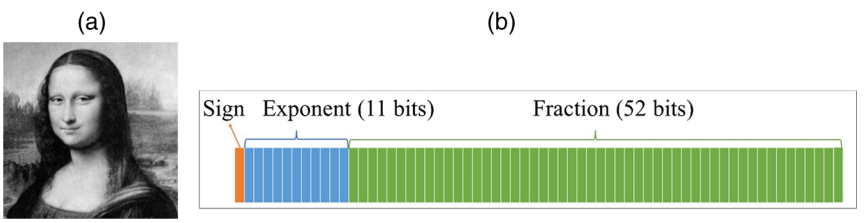

Fig. 4 Test images: (a) grayscale test image used in our simulations and (b) IEEE 754 double-precision binary floating-point format.

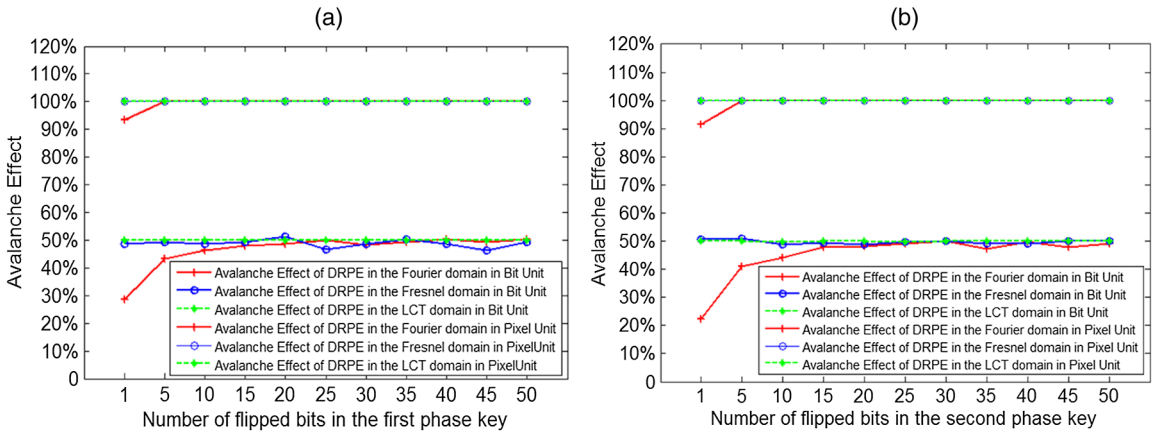

Fig. 6 Simulated results for the AE with varying number of bits in the perturbed phase keys: (a) AE with bits changed in the first phase key (RPM_1) and (b) AE with bits changed in the second phase key (RPM_2).

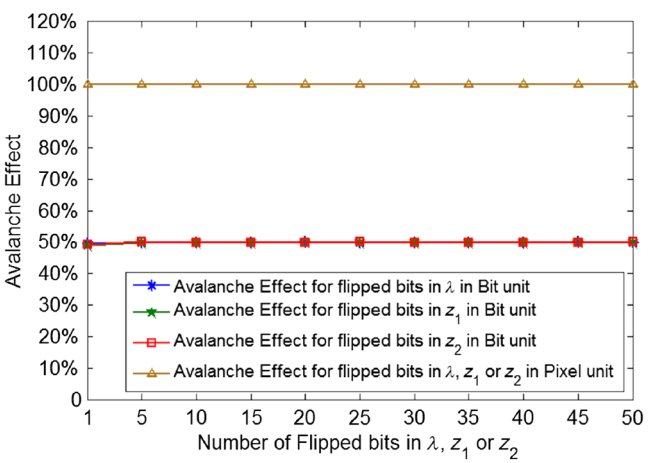

Fig. 7 AE with some bits in the wavelength (λ) and two distance values (z_1, z_2) are perturbed.

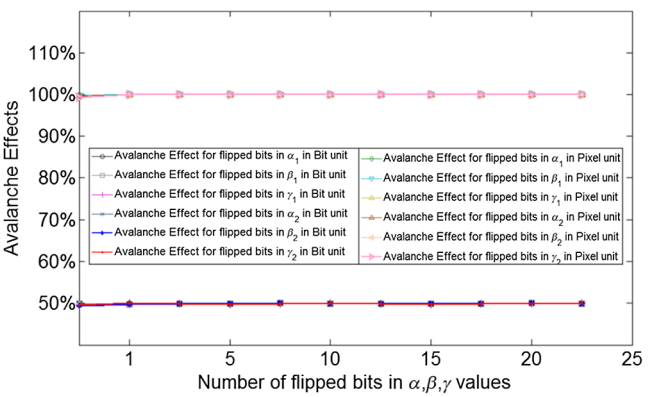

Fig. 8 AE with some bits in α_1, β_1, γ_1 and α_2, β_2, γ_2 are flipped.

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 AVAC 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 stays at 100% while that in the FT-based system increases to be 100% after about five bits if the phase keys are changed.

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 AEs for these additional keys were also examined. The corresponding results are depicted in Fig. 7. The results demonstrate that the AE 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 is 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 six additional parameters (keys) to the encryption system. The results of AEs for these additional keys are analyzed and shown in Fig. 8. As it can be seen, the AE for the DRPE in the LCT domain with perturbed bits in α_1, β_1, γ_1 and α_2, β_2, γ_2 is 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 AE 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.

For BI measurements, there are about $C^2_{52\times52\times52}$ bit pairs in a 52×52 encrypted image when considering only the 52 bits of significant digits. It is computationally difficult to compute results for these pairs, therefore in our simulations, 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 BI results for the FT-, FST-, and LCT-based DRPE system. As it can be seen from Table 1, the BI values for the DRPE systems, employed in this study, are far away from 1, in other words correlation less than 1, meaning that the DRPE possesses a satisfactory BI property. With these results, we can also conclude that DRPE achieves good BI property as the values are not large, meaning that there is no strong relationship for a pair of bits. 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 AE and BI values are calculated by averaging 100 consecutive simulation results.

Table 1 BIC for the DRPE in the FT, FST, and LCT-based domains.

DRPE system	Perturbed texts in	BIC
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 AE and the BIC (which are common metrics used in evaluating the block cipher algorithms) on an optical $4f$-based DRPE system in the FT, the FST, and the LCT domains. Simulation results show that the LCT-based DRPE system achieves excellent performance in the sense of better AE and BI properties than both of the FT- and FST-based DRPE systems. To be more precise, the AE values in the DRPE in the linear canonical and Fresnel domains achieve superior results over those 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 the encryption system. Thus, a slight change either in the plaintext or the phase keys fails to realize a satisfactory AE or BIC.

Acknowledgments

I.M. acknowledges the support of Irish Research Council (IRC). R.M. is supported by the Iraqi Ministry of Higher Education and Scientific Research. C.G., D.C., L.Z., J.P.R., J.J.H., and J.T.S. thank Science Foundation Ireland (SFI), and Enterprise Ireland (EI) under the National Development Plan (NDP). The authors sincerely thank Min Wan of Beijing University of Technology (BJUT) for her help with revising this manuscript.

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 et al., "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, Dordrecht (2009).
4. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photonics* **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*, pp. 241–269, Springer, New York (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 et al., "Interferometry based multispectral photon-limited 2D and 3D integral image encryption employing the Hartley transform," *Opt. Express* **23**(12), 15907 (2015).
11. N. Rawat et al., "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 et al., "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 et al., "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Express* **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. Express* **17**(16), 13928 (2009).
15. X. Peng et al., "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.* **31**(8), 1044–1046 (2006).
16. J. J. Healy et al., *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*, Chapter 3, Prentice Hall, New York (2011).
22. H. C. V. Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security*, pp. 598–602, Springer Science and Business Media, Netherlands (2005).
23. I. Moon et al., "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 et al., "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Trans. Inf. Forensics Secur.* **11**(12), 2706–2716 (2016).
25. Z. Fu et al., "Enabling semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Serv. Comput.* **PP**(99), 1–1 (2016).
26. J. Li et al., "Segmentation-based image copy-move forgery detection scheme," *IEEE Trans. Inf. Forensics Secur.* **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 et al., "Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics," *Multimedia Tools Appl.* **76**(270), 1–17 (2016).
29. Z. Xia et al., "Steganalysis of LSB matching using differences between nonadjacent pixels," *Multimedia Tools Appl.* **75**(4), 1947–1962 (2016).
30. Z. Zhou et al., "Effective and efficient image copy detection with resistance to arbitrary rotation," *IEICE Trans. Inf. Syst.* **E99.D**(6), 1531–1540 (2016).
31. B. Chen et al., "Color image analysis by quaternion-type moments," *J. Math. Imaging Vision* **51**(1), 124–144 (2015).
32. S. Liu, B. M. Hennelly, and J. T. Sheridan, "Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding," *Opt. Commun.* **300**, 162–177 (2013).
33. S. Liu et al., "Robustness of double random phase encoding spread-space spread-spectrum watermarking technique," *Sig. Process.* **109**, 345–361 (2015).
34. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* **39**(35), 6595–6601 (2000).
35. B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.* **25**(1), 28–30 (2000).
36. O. Matoba and B. Javidi, "Secure holographic memory by double random polarization encryption," *Appl. Opt.* **43**, 2915–2919 (2004).
37. A. Vijayakumar et al., "Coded aperture correlation holography-a new type of incoherent digital holograms," *Opt. Express* **24**, 12430 (2016).
38. J. W. Goodman, *Introduction to Fourier Optics*, Chapter 4, McGraw-Hill, New York (1968).
39. H. Feistel, "Cryptography and computer privacy," *Sci. Am.* **228**, 15–23 (1973).
40. I. Vergili and M. D. Yücel, "Avalanche and bit independence properties for the ensembles of randomly chosen n×n S-boxes," *Turk J. Electr. Eng.* **9**(2), 137–146 (2001).

41. G. Arumugam, V. L. Prabha, and S. Radhakrishnan, "Study of chaos functions for their suitability in generating message authentication codes," *Appl. Soft Comput.* **7**(3), 1064–1071 (2007).
42. A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advance in Cryptology: Proc. Crypto 1985*, pp. 218, 523–534, Springer-Verlag, Berlin (1986).
43. IEEE, "IEEE standard floating-point arithmetic," in *IEEE Std 754TM-2008*, pp. 1–58 (2008).

Inbarasan Muniraj received his BE degree from St. Peters Engineering College, India, in 2009, and his ME degree from Chosun University, South Korea, in 2013. He is a PhD student and research associate at the University College Dublin (UCD), Ireland. He is one of the successful award holders of the Irish Research Council (2014 to 2017). His research interests are three-dimensional integral imaging, photon-counted holography, ptychography, optical encryptions, and compressive sensing. He is a reviewer for many esteemed optics journals.

Changliang Guo received his PhD in optical engineering form UCD, Ireland. He is currently doing his postdoctoral research in Stony Brook University, New York, USA. His research focuses on optical image processing, optical encryption, phase retrieval, deconvolution, three-dimensional light-field microscopy imaging, PSF engineering, and super resolution imaging techniques.

Ra'ed Malallah received his BSc and MSc degrees from the University of Basrah, Iraq, in 1997 and 2006, respectively. Since 2007, he has been a member of the teaching staff at the Physics Department, College of Science, University of Basrah. He was awarded a fully funded scholarship by the Iraqi Ministry of Higher Education program to pursue his PhD at UCD. His interests are in holography storage and self-written waveguide formation.

Derek Cassidy received his MEng degrees in structural, mechanical, and forensic engineering and his MSc degree in optical engineering. He is a part-time student in UCD studying his PhD in optical engineering. He is also a chartered engineer and has worked for 23 years in the telecommunications industry. He is a chairman of IET Ireland, chairman of the Irish Communications Research Group, and is also a member of the IEEE and Engineers Ireland.

Liang Zhao received her PhD in electronic engineering from UCD in 2015. Since 2015, she has been a postdoctoral fellow for Insight UCD. Her research interests span digital holographic, image processing, and wearable sensor signal processing. She has published 13 reviewed journal papers and 15 conference papers. She is a section editor of Optik and a member of OSA and SPIE.

James P. Ryle worked as a postdoctoral research engineer developing a veterinary light therapy technology after completing his PhD. Following on from the incorporation of this university spin-out, he was awarded a competitive IRC postdoctoral fellowship to develop innovative digital holographic microscopic imaging systems. He was then employed as an assistant lecturer at UCD. He is currently a funded senior researcher in an industrial collaborative project to develop advanced imaging technologies.

John J. Healy received his BE and PhD degrees in electronic engineering from UCD in 2005 and 2010, respectively. Following postdoctoral work at Universidad Nacional Autónoma de México and at Maynooth University, he was appointed as an assistant professor in electrical and electronic engineering at UCD in 2015. His research interests include hybrid optonumeric imaging systems and signal processing. He is a member of IEEE, OSA, and SPIE.

John T. Sheridan received his BE degree from National University of Ireland, Galway, MScEE degree from Georgia Tech, DPhil degree from Oxford University. He held an Alexander von Humboldt fellowship in Erlangen-Nürnberg and was a visiting scientist at the European Commission Joint Research Centre, Italy. He is currently a professor of optical engineering at the School of Electrical and Electronic Engineering, UCD. He is the cofounder of Equilume Ltd., a fellow of both SPIE and OSA, and coeditor of linear canonical transforms in the Springer Series in Optical Sciences.