2D Non-separable Linear Canonical Transform (2D-NS-LCT) based cryptography

Liang Zhao[a,*], Inbarasan Muniraj[b], John J Healy[b], Ra'ed Malallah[b,c], Xiao-Guang Cui[d], James P Ryle[b], and John T. Sheridan[b].

[a]The Insight Centre for Data Analytics, University College Dublin, Belfield, Dublin 4, Ireland.

[b]School of Electrical and Electronic Engineering, IoE^2 Lab, SFI-Strategic Research Cluster in Solar Energy Conversion, University College Dublin, Dublin 4, Ireland.

[c]Physics Department, Faculty of Science, University of Basrah, Garmat Ali, Basrah, Iraq.

[d]Institute of Automation, Chinese Academy of Sciences, No. 95, East Zhong Guan Cun Road, Hai-Dian District, Beijing, 100190, P.R.China.

**Corresponding author:* liang.zhao@ucd.ie

ABSTRACT

The 2D non-separable linear canonical transform (2D-NS-LCT) can describe a variety of paraxial optical systems. Digital algorithms to numerically evaluate the 2D-NS-LCTs are not only important in modeling the light field propagations but also of interest in various signal processing based applications, for instance optical encryption. Therefore, in this paper, for the first time, a 2D-NS-LCT based optical Double-random-Phase-Encryption (DRPE) system is proposed which offers encrypting information in multiple degrees of freedom. Compared with the traditional systems, i.e. (i) Fourier transform (FT); (ii) Fresnel transform (FST); (iii) Fractional Fourier transform (FRT); and (iv) Linear Canonical transform (LCT), based DRPE systems, the proposed system is more secure and robust as it encrypts the data with more degrees of freedom with an augmented key-space.

Keywords: ABCD Transform, Optical security and encryption, Numerical approximation and analysis, Discrete optical signal processing.

1. INTRODUCTION

To meet the extensive demands in protecting personal information, more sophisticated security techniques have been highly sought. In the past few decades, a numerous optical as well as optically inspired digital techniques such as steganography, watermarking, and encryption in the interest of information security, have been proposed[1]. Among those techniques, Double Random Phase Encryption (DRPE) or 4*f* optical processor[1, 2], proposed by Refregier *et al*, has received a wide attention. It is known that DRPE turns an intensity image into stationary white noise using two statistically distributed random phase keys that are employed at spatial and the Fourier domains, respectively. As a consequent, the resulting encrypted data doesn't disclose any information for visual inspection. However, the decryption is said to be a reverse process of encryption and thus we can recover the original intensity image, by employing the correct keys [3, 4]. A substantial security of DRPE system in the Fourier domain gave an impetus to examine this approach in other transformation domains such as the fractional Fourier (FRT)[5,6] and the Fresnel transformation domains (FST)[7,8]. A digital counterpart of the conventional DRPE system is vulnerable to some organized attacks[9-12]. Thereafter, many studies for instance, pixel scrambling[13-16], random permutation technique[17] and photon-counting approaches[18-20] that associated with the classical encryption system, regarded as enhancing the information security. It however is widely accepted that the security of any encryption system depends on the keys used and therefore the larger the key-space the more the security will be[5]. In addition to these approaches, in this paper, for the first time, a novel 2D-NS-LCT[21-39] based optical DRPE system is proposed. This proposed system offers encrypting information in multiple (10) degrees of freedom (see Table 1). Therefore, compared with the traditional

- Fourier transform (FT),
- Fresnel transform (FST),
- Fractional Fourier transform (FRT),
- Linear Canonical transform (LCT),
- Gyrator transform,
- Arnold transform,

based DRPE systems, the proposed system is more secure and robust as it encrypts the data with more degrees of freedom and extends the key required.

Table 1. Transforms and their number of free parameters.

Transforms	No. of Free Parameters
Fourier transform (FT)	0
Fresnel transform (FST)	2
Fractional Fourier transform (FRT)	1
Linear Canonical transform (LCT)	3
Gyrator transform	1
2D-NS-LCT	10

This paper is organized as follows. In Section 2, we briefly introduce the classical DRPE system and the 2D-NS-LCT. The proposed 2D-NS-LCT based optical DRPE system is also described. In Section 3, simulation results of the proposed system is depicted and analyzed. Finally in Section 4 we conclude our discussion and future work is presented.

2. DOUBLE RANDOM PHASE ENCRYPTION (DRPE)

In this section, firstly the classical DRPE system, *the FT based DRPE system*, is introduced briefly. Following that the powerful 2D-NS-LCT as well as its numerical calculation is presented. Finally, the proposed 2D-NS-LCT based optical DRPE system is described.

2.1. The classical Fourier transform based encryption

As noted, DRPE is one of the widespread approaches for optical image encryption and hiding techniques[1]. The operation of *the FT based DRPE system* is illustrated in Fig. 1. The input image field, sequentially propagates through

(i) The 1st random phase key (D1),
(ii) One Fourier optical system,
(iii) The 2nd random phase key (D2),
(iv) One inverse Fourier optical system;

The resulting ciphertext (encrypted image) is a complex field and it does not disclose any of its content without the knowledge of two phase keys (i.e., secret keys). The decryption process is illustrated in Fig 1. (b), in which the input image can be retrieved. The optical implementation of *the FT based DRPE system* is shown in Fig. 2. We recall (see Table 1) that there is no free parameter in the FT, while there are 10 free parameters in the general 2D-NS-LCT. Therefore, the security of the DRPE system can be improved by means of introducing additional keys. In such a system, in order to retrieve the decrypted image, in addition to the two phase keys (i.e., D1, D2) all the ten free parameters are required. Subsection 2.3 discusses the proposed approach more in detail.

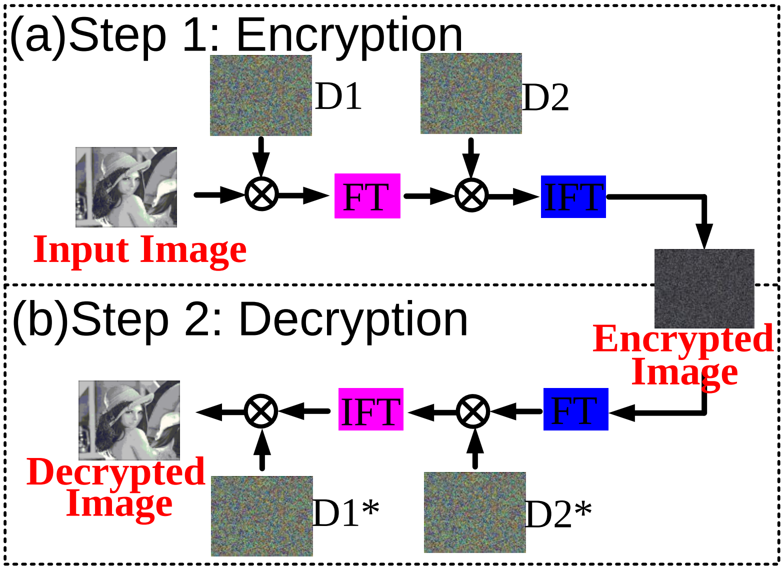

Fig. 1. The overview of FT based DRPE system: (a) DRPE encryption; (b) DRPE decryption. D1 and D2 represent two random phase keys, which are independent phase functions positioned in the space and Fourier domain (or spatial frequency domain) respectively. D1, in the space domain, makes the input field white. D2, in the Fourier domain, makes input field stationary and encoded. The symbol * refers to convolution operation.

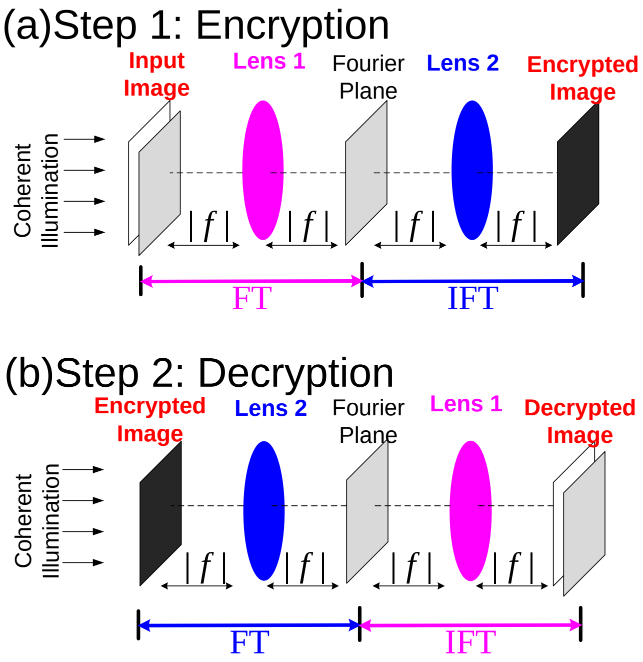

Fig. 2 Optical setup for the FT based DRPE system: (a) Optical setup for DRPE encryption, where |*f*| represents the absolute value of focal length of the lens; (b) Optical setup for DRPE decryption.

2.2. An overview of 2D-NS-LCT

The 2D-NS-LCT can represent a wide variety of non-orthogonal, non-axially symmetric and anamorphic systems[21-40]. Among its special cases are the FT, FRT, and FST, gyrator transform, chirp transform, homogeous coordinate/affine transform (including e.g. rotation transform, and shearing (interferometer) transform). The continuous 2D-NS-LCT of a signal $g(x,y)$ is defined as[22],

$$\mathrm{G}(x',y') = L_M\{g(x,y)\}(x',y') = \frac{1}{\sqrt{j\det(B)}}\iint_{-\infty}^{\infty} \exp\left[\frac{j\pi\left(k_1x'^2+k_2x'y'+k_3y'^2\right)}{\det(B)}\right]$$
$$\exp\left\{\frac{j2\pi[(-b_{22}x'+b_{12}y')x+(b_{21}x'-b_{11}y')y)]}{\det(B)}\right\}\exp\left[\frac{j\pi\left(p_1x^2+p_2xy+p_3y^2\right)}{\det(B)}\right]g(x,y)dxdy\ , \tag{1-1}$$

where,

$$k_1 = d_{11}b_{22} - d_{12}b_{21},\ k_2 = 2(-d_{11}b_{12} + d_{12}b_{11}), k_3 = -d_{21}b_{12} + d_{22}b_{11},$$
$$p_1 = a_{11}b_{22} - a_{21}b_{12},\ \ p_2 = 2(a_{12}b_{22} - a_{22}b_{12}),\ \ p_3 = -a_{12}b_{21} + a_{22}b_{11}. \tag{1-2}$$

A, *B*, *C*, and *D* are 2×2 submatrices defining the transformation matrix *M* of the system as follows,

$$M = \left(\begin{array}{cc:cc} a_{11} & a_{12} & b_{11} & b_{12} \\ a_{21} & a_{22} & b_{21} & b_{22} \\ \hdashline c_{11} & c_{12} & d_{11} & d_{12} \\ c_{21} & c_{22} & d_{21} & d_{22} \end{array}\right) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{1-3}$$

In these matrices, $\det(B) \neq 0$, where $\det(B)$ is the determinant of matrix *B*. The number of independent parameters in the matrix *M* is ten[22]. One of the most important properties of the continuous 2D-NS-LCT is the unitary property, i.e., they are always invertible as follows[40],

$$f(x) = L_{M^{-1}}\{L_M\{f(x)\}(y)\}(x). \tag{2}$$

Discrete transforms that approximate the continuous LCTs allow us to simulate a number of propagation problems. But such discretization can destroy the unitary property, i.e., in general the discrete 2D-NS-LCT is not unitary. In [38, 39], we recently proposed an unitary numerical implementation of the 2D-NS-LCT,

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & B^{T^{-1}} \end{pmatrix}\begin{pmatrix} I & 0 \\ B^TD & I \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} I & 0 \\ B^{-1}A & I \end{pmatrix}, \tag{3}$$

i.e., the 2D-NS-LCT can be numerically evaluated by taking a ① 2D Chirp; ② 2D FT; ③ another 2D chirp; and ④ an affine transform, see Eq. 3, from right side to left side. We have reported that a given 2D input image with rectangular shape/boundary, in general, after the 2D-NS-LCT the resulting output sampling grid is a parallelogram, i.e., the output samples may not located in a Cartesian coordinates, thus limiting the further calculations, e.g. inverse transform[38]. In [39], a fast unitary discrete algorithm for some 2D-NS-LCT is investigated for the iterative phase retrieval based applications. We also have demonstrated that unitarity can significantly improve the convergence of iterative phase retrieval algorithm[37, 39]. We note that such an unitary algorithm is not only important for phase retrieval techniques but also to extract information about an object given with some known illumination. It is therefore significant when solving inverse problems to decrypt information from an encrypted image, e.g. decryption.

Furthermore, in the encryption systems, if a non-unitary (or irreversible) numerical algorithm is used in optical transforms, its impossible to the decrypted image, even with known two phase keys. Since most discrete FTs are unitary, e.g. the *fft* command in MATLAB, the decryption process in Fig. 1, does not suffer such problem. However, in the proposed 2D-NS-LCT based DRPE system, it is mandatory to ensure the numerical algorithm used is unitary, which will be further analyzed later.

2.3. Proposed 2D-NS-LCT based DRPE system

As discussed above, since the digital implementations of DRPE systems are not secured enough, in this paper, for the first time, the 2D-NS-LCT transform (that has 10 free parameters) based DRPE system is introduced. We note that to decrypt the encoded information, this technique requires:

(I) Two phase keys: D1 and D2;

(II) Ten free parameters (of the 2D-NL-LCT);

(III) Unitary discrete 2D-NS-LCT (to generate the encrypted image and to help get the decrypted image when two phase keys are known).

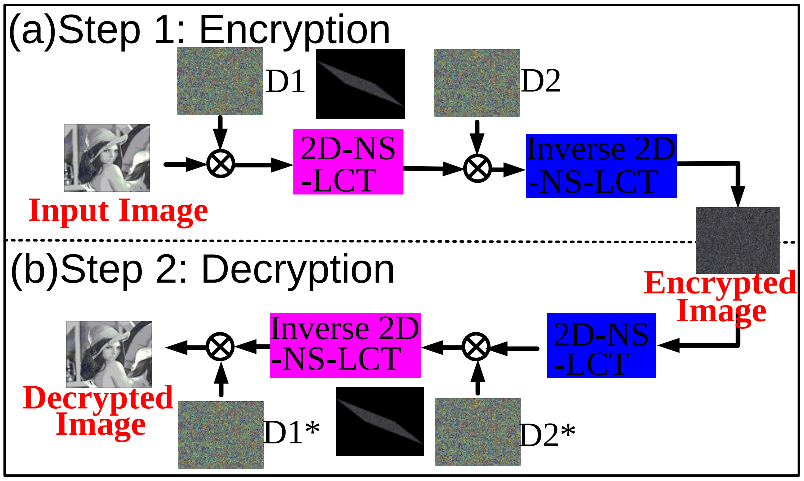

Fig. 3 Illumination of the 2D-NS-LCT based DRPE system: (a) DRPE encryption; (b) DRPE decryption.

3. PROPOSED METHOD ANALYSIS

A feasible optical setup to implement our proposed system is shown in Fig. 4. Here we used two colorful 3D cubes to represent the optical setup for the LCTs, pink and blue cubes represent the 2D-NS-LCT and its inverse transform respectively. The optical setup for the 2D-NS-LCT can be designed by matrix decomposition[29,38,41].

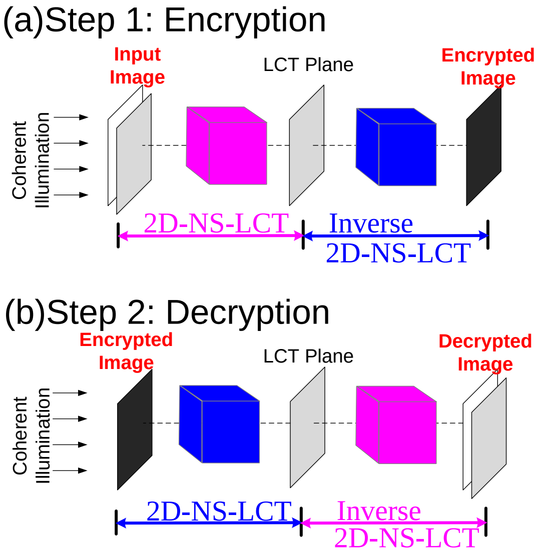

Fig.4 Optical setup for the 2D-NS-LCT based DRPE system: (a) Optical setup for DRPE encryption; (b) Optical setup for DRPE decryption.

We examine the proposed system by simulations. In our simulation, the number of input image samples are 256 by 256. The input sampling intervals along two dimensions are the same, both are set to be 0.1/256. Two following transform matrices of the 2D-NS-LCT are applied,

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & 0.5 \\ 0 & 0 & 0.5 & 0.5 \\ 0 & -58 & 0 & 0 \\ -26 & 164 & 0 & 0 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} 8 & 9 & 1 & 0.5 \\ 10 & -3 & 0.5 & 0.5 \\ 122 & -58 & 5 & 6 \\ -26 & 164 & 7 & 0 \end{pmatrix} \tag{4}$$

The decomposition given in Eq. (4) is applied to evaluate the continuous LCTs[39].

We start with a plaintext, a 2D gray Lenna image with 256 by 256 pixels, see Fig. 3(a). After applying the 1st phase key, it becomes a complex field. Then after further propagating through the 2D-NS-LCT, the resulting output image is located in a parallelogram, which has with 768 by 768 pixels, see the image with parallelogram boundary above the pink 2D-NS-LCT rectangle shown in Fig. 3(a). Finally after the inverse 2D-NS-LCT the encrypted image is located in a rectangular grid again with 256 by 256 pixels.
As long as the numerical algorithm to evaluate the LCTs is unitary, after the decryption process shown in Fig. 3(b), the decrypted image obtained will be the same as the original input image, i.e. plaintext. In our simulation, the mean squared error between the decrypted image and the input image is calculated by [42]

$$\mathrm{MSE} = \frac{\sum\sum(|\text{Decrypted image}|-|\text{Input image}|)^2}{\sum\sum|\text{Input image}|^2} \tag{5}$$

where $|\cdot|$ returns the absolute value. For transform M_1 and M_2, see Eq. (4), the MSE are 1.95×10^{-31} and 3.49×10^{-17} respectively.

4. CONCLUSION

The classical Fourier transform based DRPE shown to be vulnerable to organized attacks. To alleviate, in this paper, a novel 2D-NS-LCT based DRPE system is proposed. The proposed system improves the security of the encryption system by introducing more free parameters (secret keys).

REFERENCES

[1] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” Adv. Opt. Photon. **1**, 589 (2009).

[2] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767-769 (1995).

[3] B. Javadi, G. Zhang, and J. Li, “Experimental demonstration of the random phase encoding technique for image encryption and security verification,” Opt. Eng. **35**, 2506-2512 (1996).

[4] B. Javidi, A. Sergent, and E. Ahouzi, “Performance of double phase encoding encryption technique using binarized encrypted images,” Opt. Eng. **37**, 565-569 (1998).

[5] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” Opt. Lett. **25**, 887-889 (2000).

[6] X. Zhou, S. Yuan, S. W. Wang, and J. Xie, “Affine cryptosystem of double-random-phase encryption based on the fractional Fourier transform,” Appl. Opt. **45**, 8434-8439 (2006).

[7] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett. **24**, 762-764 (1999).

[8] G. Situ, and J. Zhang, “Double random phase encoding in the Fresnel domain,” Opt. Lett. **29**, 1584-1586 (2004).

[9] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett **30**, 1644-1646 (2005).

[10] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, “A known-plaintext heuristic attack on the Fourier plane encryption algorithm,” Opt. Express **14,** 3181-3186 (2006).

[11] X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett. **31**, 1044-1046 (2006).

[12] C. Guo, S. Liu, and J. T. Sheridan, “Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems,” Appl. Opt.**54**, 4709-4719 (2015).

[13] B. Hennelly, J.T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” Opt. Lett.**28**, 269–271 (2003).

[14] H. Lu, J. Zhao, Q. Fan, Y. Xu, and X. Wan, “Iterative double random phase encryption based on pixel scrambling technology,” Acta Photonica Sin. **34**, 1069-1073 (2005).

[15] J. Zhao, H. Lu, X. Song, J. Li and Y. Ma, “Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique,” Opt. Commun. **249**, 493-499 (2005).

[16] Z. Zhong, J. Chang, M. Shan, B. Hao, “Double image encryption using double pixel scrambling and random phase encoding,” Opt. Commun. **285**, 584-588 (2012).

[17] M. He, Q. Tan, L. Cao, Q. He and G. Jin “Security enhanced optical encryption system by random phase key and permutation key,” Opt. Express. **25**, 22462-22473 (2009).

[18] E. Pérez-Cabré, H. Abril, M. Millán, and B. Javidi, “Photon-counting double-random-phase encoding for secure image verification and retrieval,” J. Opt., **14**, 094001 (2012).

[19] A. Markman and B. Javidi, “Full-phase photon-counting double-random-phase encryption,” J. Opt. Soc. Am. A. **31**, 394-403 (2014).

[20] D. Maluenda, A. Carnicer, R. M. Herrero, I. Juvells, and B. Javidi, “Optical encryption using photon-counting polarimetric imaging,” Opt. Express **23**, 655-666 (2015).

[21] B. M. Hennelly, and J. T. Sheridan, “Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms,” J. Opt. Soc. Am. A **22**, 917-927 (2005).

[22] A. Koç, H. M. Ozaktas, and L. Hesselink, “Fast and accurate computation of two-dimensional non-separable quadratic-phase integrals,” J. Opt. Soc. Am. **27**, 1288-1302 (2010).

[23] K. Wolf and T. Alieva, “Rotation and gyration of finite two dimensional modes,” J. Opt. Soc. Am. A **25**, 365–370 (2008).

[24] S.-C. Pei and J.-J. Ding, “Properties, digital implementation, applications, and self-image phenomena of the gyrator transform,” 17th European Signal processing conference, 441-445 (2009).

[25] J. Shamir, “Cylindrical lens systems described by operator algebra,” Appl. Opt. **18**(24), 4195-4202 (1979).

[26] H. H. Arsenault, “A matrix representation for non-symmetrical optical systems,” J. Optics (Paris) **11**, 87-91 (1980).

[27] G. Nemes and A. E. Siegman, “Measurement of all ten second-order moments of an astigmatic beam by the use of rotating simple astigmatic (anamorphic) optics,” J. Opt. Soc. Am. A. **11**(8), 2257-2264 (1994).

[28] J. A. Rodrigo, T. Alieva, and M. L. Calvo, “Optical system design for orthosymplectic transformations in phase space,” J. Opt. Soc. Am. A. **23**(10), 2494-2500 (2006).

[29] A. Sahin, H. M. Ozaktas, and D. Mendlovic, “Optical Implementations of Two-Dimensional Fractional Fourier Transforms and Linear Canonical Transforms with Arbitrary Parameters,” Appl. Opt. **37**(11), 2130-2141 (1998).

[30] A. Sahin, M. A. Kutay, and H. M. Ozaktas, “Nonseparable Two-Dimensional Fractional Fourier Transform,” Appl. Opt. **37**(23), 5444-5453 (1998).

[31] S.-C. Pei, “Two-dimensional affine generalized fractional Fourier transform,” IEEE Trans. Signal Process. **49**, 878-897 (2001).

[32] P. Dong and N. P. Galatsanos, “Affine transformation resistant watermarking based on image normalization,” IEEEE ICIP, III 489-492 (2002).

[33] Z.-J. Liu, H. Chen, T. Liu, P.-F. Li, J.-M. Dai, X.-G. Sun, and S.-T. Liu, “Double-image encryption based on the affine transform and the gyrator transform,” J. Opt.**12**, 035407 (2010).

[34] J.-J. Ding and S.-C. Pei, “Eigenfunctions and self-imaging phenomena of the two-dimensional non-separable linear canonical transform,” J. Opt. Soc. Am. A **28**, 82-95 (2011).

[35] J.-J. Ding, S.-C. Pei and C.-L. Liu, “Improved implementation algorithms of the two-dimensional non-separable linear canonical transform,” J. Opt. Soc. Am. A **29**, 1615-1624 (2012).

[36] T. Alieva and M. J. Bastiaans, “Alternative representation of the linear canonical integral transform,” Opt. Lett. **30**, 3302-3304 (2005).

[37] L. Zhao, J. J. Healy, and J. T. Sheridan, “Unitary discrete linear canonical transform: Analysis and application,” Appl. Opt. **52** (7), C30-C36 (2013).

[38] L. Zhao, J. J. Healy, and J. T. Sheridan, “The 2D non-separable linear canonical transform: Sampling theorem and unitary discretization,” J. Opt. Soc. Am. A **31**(12), 2631–2641 (2014).

[39] L. Zhao, J. T. Sheridan, and J. J. Healy, “Unitary algorithm for non-separable linear canonical transforms applied to iterative phase retrieval,” accepted by IEEE Signal Proc. Lett. (2017).

[40] J. J. Healy, M. A. Kutay, H. M. Ozaktas, and J. T. Sheridan, *Linear Canonical Transforms*, Springer, New York (2016).

[41] J. A. Rodrigo, T. Alieva, and M. L. Calvo, “Experimental implementation of the gyrator transform,” J. Opt. Soc. Am. A **24**, 3135–3139 (2007).

[42] 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. Express **23**, 15907-15920 (2015).