Cryptanalysis of DRPE using complex S-Box based on linear canonical transform

R. Girija · H. Singh · G. Abirami

Received: 21 June 2021 / Revised: 2 April 2022 / Accepted: 31 August 2022
Published online: 20 September 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
During recent decades, double random phase encoding grasped more attention for researchers. To achieve nonlinearity, it had been done with random S-Box. We exhibit this involvement that DRPE system is much vulnerable in the above methodology. Concatenating anything with DRPE needs an imaginary value, wherein S-Box unsuccessful in it. Used S-Box has been reformed into various sizes. Due to this scenario, S-Box values are replicating. So, complex S-Box has been employed and proposed size of the S-Box is similar to an input image. Numerical simulations such as performance analysis, histogram analysis and 3D plot analysis have been performed out to validate the practicability and trustworthiness of traditional DRPE system with complex S-Box. Moreover, in order to check the cryptanalysis, much other analysis done such as occlusion attack, noise attack, chosen plaintext analysis and sensitivity analysis also accomplished.

Keywords Complex S-Box · Nonlinearity · DRPE · Chosen plaintext analysis

1 Introduction
In the past two to three decades, securing the data, images, audio files and video files from intruder plays a foremost task. Even though there are numerous algorithms are existing, it is very difficult to protect the information. A traditional image encryption algorithm delivers poor presentation for
small images. This can be easily accomplished by optical cryptography [29]. In the meantime, Refregier and Javidi [48] proposed DRPE and it has practised countless enhancements and enlargements by hosting few parameters such as wavelength, propagation distance, and polarization. Various transforms such as discrete cosine transform (DCT) [4, 5, 35, 56], Fresnel transform (FrT) [27, 39, 46, 54, 61, 62], Gyrorotor transform (GT) [49, 51, 52], Hartley transform (HT) [8, 19, 53], Fractional Fourier Transform (FrFT) [24, 33, 34, 37, 40, 45, 50, 58, 60, 67], Walsh-Hadamard Transform [13–15] and LCT [22, 23, 25, 26, 30, 43, 63, 64, 68, 69] are pooled with DRPE system. These transforms are prepared with symmetric cryptosystem. Symmetric cryptosystem is defenceless to CPA [44], CCA [7] and KPA [45]. In order to defeat these attacks, an asymmetric optical cryptosystem was designed by many researchers and proposed which uses two pair of keys. In order to improve the security concern in DRPE system, in the place of traditional phase masks, there are various other types of masks are used such as deterministic phase masks [16, 66], chaotic masks [6, 17, 32] etc. Enhancement of DRPE is not only shown on asymmetric cryptosystem, but also adding the nonlinearity factor which is done by random S-Box [18]. S-Box is the most important key factor in placing nonlinearity in DRPE system. Already mentioned Random S-Box is in the size of [16 16] and it has been regenerated to size of input image. Due to this values used in S-Box are replicating. Moreover, generated S-Box is not a complex S-Box. In other words, DRPE needs complex system to get merged with any input images. Moreover, deep learning neural network also plays a vital role in image encryption and decryption systems. That too in the medical field, for the classification of many diseases, deep neural network is hitting again and again [55]. A detailed survey also done regarding prediction of plant leaf disease based on the neural network [11]. In order to work with multiclass imbalanced datasets, a consolidated decision tree made in [41]. It’s been done for intrusion detection systems and also a performance assessment of supervised classifier for intrusion detection systems [42]. Cancer prediction model also done with outlier detection and oversampling methods done in [28]. In [9], some hybrid techniques for encryption and decryption calculated. Image encryption also mentioned with Ion-Acoustic waves in space plasma can be calculated using dynamical properties in [57]. Access control with trust calculation also done in [1–3].

In this, cryptanalyzing the random S-Box and proposing the solution for the DRPE system to add nonlinearity. Elucidation also produced for the random S-Box. The parameters for Complex S-Box has been checked and validated. Proposed system also holds Linear canonical transforms which also adds the more number of security parameters to our system.

2 Theoretical background

2.1 S-Box

S-Box shows a vibrant role in contemporary cryptosystems [10, 12, 36]. Without S-Box, no secured cryptosystem is possible to design in block cipher and stream cipher. Now-a-days, designing of S-Box are considered as an important component in image encryption and decryption. The foremost factor for DRPE is Nonlinearity, which is easily supported by S-Box. Even though nonlinearity is provided by S-Box, there is a huge ambiguity is available in constructed S-Box. Proposed S-Box is given below:

\[ S\text{-Box} = \text{rand}(r, c) \]  

(1)
Where \( \text{rand}, r \) and \( c \) are a random function, rows and columns respectively. \( M \) and \( N \) are the size of input images. While investigating the S-Box from eq. 1 and 2, its size is \( 16 \times 16 \), and then it had been resized into the size of the input image. Due to this, values are getting replicated. Moreover, DRPE system mainly deals with complex numbers. But the created S-Box, is not matching with complex numbers. Our proposed system overcomes the loopholes of the previous system and concentrated on enactment procedures for instance Non-linearity, Bit-Independence criterion (BIC), Strict Avalanche Criterion (SAC), Differential Probability (DP) and Linear Probability (LP). These parameters are shown in Table 1.

2.2 Linear canonical transform (LCT)

LCT is optically instigated by QPS (quadratic phase systems) [59]. LCT is considered as grander case of all the transforms such as Fourier Transform, Fractional Fourier Transform and Fresnel Transforms. The 2-dimensional LCT consists of three parameters. LCT is considered as based on linear integral transforms and it is completely defined as follows,

\[
f'(x,y) = LCT_{\alpha,\beta,\gamma}\{f(x_0,y_0)\} = \exp\left(-\frac{j\pi}{4}\right)\sqrt{|\beta|} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x_0,y_0) \exp\left\{\alpha(x^2 + y^2) - 2\beta(x_0x + y_0y) + \gamma(x^2 + y^2)\right\} d x_0 d y_0
\]

Where \( LCT_{\alpha,\beta,\gamma}\{\cdot\} \) represents the LCT transform through three real transform parameters \( \alpha, \beta \) and \( \gamma \). Two planes, one is called as input plane which is characterized as \((x_0, y_0)\) and the other is transform plane which is mentioned as \((x, y)\). The three transform factors \( \alpha, \beta \) and \( \gamma \) are associated through QPS renovation. Henceforward it is interconnected to the transmission distances \( d_1, d_2 \) and the focal length \( f \). Wavelength is denoted as \( \lambda \) and the real parameters are shown as (Fig. 1),

\[
\alpha = \frac{d_1-f}{\lambda[f(d_1 + d_2)-d_1d_2]};
\]

\[
\beta = \frac{f}{\lambda[f(d_1 + d_2)-d_1d_2]};
\]

\[
\gamma = \frac{d_2-f}{\lambda[f(d_1 + d_2)-d_1d_2]};
\]

Table 1  S-Box parameters

| Parameters                   | Values   |
|------------------------------|----------|
| Nonlinearity                 | 104.6    |
| Differential Probability     | 0.057    |
| Linear Probability           | 0.24     |
| Bit-Independence Criterion   | 104.67   |
| Strict Avalanche Criterion   | 0.606    |
Beginning from the Fig. 2, it is undoubtedly agreed, input and transform planes are placed as \( d_1 \) and \( d_2 \). The transform planes and output planes are positioned as \( d_3 \) and \( d_4 \). \( d_1, d_2, d_3 \) and \( d_4 \) are recognized as distance factors and deliberated as important to QPS. Random phase masks from DRPE system (RPM1 and RPM2) and six parameters of LCT \( (\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2) \). So, totally eight parameters are considered as the security space for LCT grounded DRPE system.

### 3 Proposed work

Figure 3 shows the encryption and decryption of proposed system. Let us consider \( f(x, y) \) as an input image. It is getting multiplied with first random phase mask \( RPM1(x, y) \). In order to overcome the loopholes in [60], complex random S-Box has been created with the size of input image using the following equation.

\[
S-box = \text{complex\_rand}\{M, N\} \tag{7}
\]

Where M, N are the size of the input images. In the place of traditional Fourier transform, Linear canonical transforms has been considered in the proposed model with three security parameters \( \alpha_1, \beta_1, \gamma_1 \).
Intermediate image $I(x, y)$ has been calculated with the following equations.

$$ I(x, y) = PT \left\{ \text{LCT} \left( \alpha_1, \beta_1, \gamma_1 \right) [f(x, y) \ast \text{RPM1}(x, y) \ast \text{Complex S-Box}] \right\} \quad (8) $$

$$ R3 = MT \left\{ \text{LCT} \left( \alpha_1, \beta_1, \gamma_1 \right) [f(x, y) \ast \text{RPM1}(x, y) \ast \text{Complex S-Box}] \right\} \quad (9) $$

Where PT and MT represents the phase truncation and magnetic truncation respectively. According to the above equations, input image is getting multiplied with first random phase mask and created complex S-Box. The resultant is transformed using linear canonical transforms with three security parameters. The absolution portion is called as $I(x, y)$. $R3$ is denoted as phase portion of eq. 9.

Encrypted image is obtained from an intermediate image with the following equations.

$$ E(x, y) = PT \left\{ \text{LCT} \left( \alpha_2, \beta_2, \gamma_2 \right) [I(x, y) \ast \text{RPM2}(x, y) \ast \text{Complex S-Box}] \right\} \quad (10) $$

$$ R4 = MT \left\{ \text{LCT} \left( \alpha_2, \beta_2, \gamma_2 \right) [I(x, y) \ast \text{RPM2}(x, y) \ast \text{Complex S-Box}] \right\} \quad (11) $$

Intermediate image is multiplied with another random phase mask and complex S-Box. The overall product is undergone for the linear canonical transforms with another set of three security parameters. The absolute portion is called as an encrypted image. $R4$ is denoted as phase portion of eq. 11. $R3$ and $R4$ are also called as decryption keys.

The flow chart for the decryption is given in Fig. 4. Cipher image from encryption portion is multiplied with one of the secret key and divide by randomly generated complex S-Box. The product undergoes for the Linear canonical transform using three security parameters $(\alpha_1, \beta_1, \gamma_1)$. After doing this process, $I(x, y)$ is obtained successfully.

$$ I(x, y) = \text{LCT} \left( \alpha_1, \beta_1, \gamma_1 \right) \{ (E(x, y) \ast R4) \ast \text{complex S-Box} \} \quad (12) $$

$$ f(x, y) = \text{LCT} \left( \alpha_2, \beta_2, \gamma_2 \right) \{ (I(x, y) \ast R3) \ast \text{complex S-Box} \} \quad (13) $$

To obtain the decrypted image back $I(x, y)$ is multiplied with another secret key $R3$ and divided with complex S-Box. The output undergoes for transformation with another set of three security parameters $(\alpha_2, \beta_2, \gamma_2)$.

Fig. 3 Proposed system-encryption process

Fig. 4 Proposed system-decryption process
4 Simulation results

4.1 Performance investigation

The suggested asymmetric cryptosystem has been surveyed by numerous methods such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC). MSE, PSNR and CC [20, 21, 38, 47, 65] have been computed using the given formulas. 

\[
MSE = \frac{\sum_{x=0}^{256} \sum_{y=0}^{256} |P(x,y) - P'(x,y)|^2}{256 \times 256}
\]  

\[
PSNR = 10 \times \log_{10} \left( \frac{255^2}{MSE} \right)
\]  

\[
CC = \frac{\text{cov}(P(x,y), P'(x,y))}{\sigma(P(x,y)) \sigma(P'(x,y))}
\]  

Where \(P(x, y)\) the plain is image and \(P'(x, y)\) is recovered image. \(\text{cov}, \sigma\) denotes the co-variance and standard deviation respectively. The computed MSE value from the above equation for 256 × 256 medical image is 9.06 × 10^{−26}. PSNR finds the variance between plain image and recovered image and it is represented in below equation. If the PSNR value is high, it gives the good quality of image. The result of PSNR  is 372.21 dB. From the result, it has been clearly observed the value is high, so, it gives the good quality of image. Since all the correct keys given in our system, the value of CC is equal to 1. Table 2 drafts the comparison results for all the analysis. It has been clearly understood from the Table 2; our proposed asymmetric cryptosystem provides better results.

4.2 Histogram analysis

Histogram is otherwise defined as evaluator for our proposed cryptosystem. To avoid the leakage of information [20, 21, 38, 47, 65], histogram of cipher image must be different from histogram of plain image. Figure 5 represents the histogram investigation of offered asymmetric cryptosystem. Figure 5 (a), (b) and (c) represents the plain image, cipher image and recovered image respectively. From the results, it is very clear that histogram of plain image and cipher image are totally different. Suppose, if any attacker attacks the histogram of encrypted image, it is not possible to get any information about plain image.

| Parameters | H. Singh Scheme [51] | Zamrani scheme [66] | P. Raheja Scheme [47] | Girija Scheme [16] | Girija scheme [3] | Proposed Model |
|------------|-----------------------|----------------------|-----------------------|--------------------|------------------|---------------|
| Transform Domain | Gyrator | Fourier | Hybrid multi-resolution Wavelet | Fractional Fourier | Fourier | Linear canonical |
| Applied Approach | Asymmetric | Symmetric | Asymmetric | Asymmetric | Asymmetric | Asymmetric |
| Masks | Random masks | Deterministic masks | Random masks | Deterministic masks | Random masks | Random masks |
| MSE | 4.6 × 10^{−28} | 7.31 × 10^{−32} | 3.10 × 10^{−32} | 1.74 × 10^{−24} | 7.0488 × 10^{−34} | 316.12 |
| PSNR (in db) | 310 | 359.13 | Infinite | 285.45 | 178.42 | 316.12 |
4.3 3D plot analysis

The efficiency of asymmetric system is checked by 3d plot analysis as indicated in Fig. 6. The 3D plot of plain image, encrypted image and recovered image are in Fig. 6 (a)( b)a n d (c) respectively.

5 DRPE S-Box cryptanalysis

In this segment, conflict of DRPE using S-Box has been checked against various attacks such as occlusion attack, noise attack and chosen plaintext attack in brief.

5.1 Occlusion attack analysis

Occlusion is defined as hiding some portions or overwriting throughout communication. To examine the robustness of an encrypted data, occlusion attack [20, 21, 38, 47, 65] has been preferred for this cryptosystem. Figure 7 demonstrates the occlusion analysis. Minimum portion that is 10% on encrypted images are hidden in Fig. 7 (a) and obtained recovered image is in Fig. 7 (b) 25% and 75% portion of encrypted images are occluded in (c) and (e) corresponding decrypted images are shown in fig. (d) and (f) respectively. As the data hiding is increasing, it is not possible to recover the image back.
5.2 Noise attack analysis

During transmitting and receiving the signals in channels, there is always a chance for noise distortion. In case, if the level of distortion is high, sometimes, it is not possible to clear picture the recovered image. Hence, it is mandatory to check our proposed system with respect to noise. In Fig. 8, it has been checked with salt and pepper noise. Figure 8 (a, b) represents the salt and pepper noise with density of 0.2 and 0.9 respectively. It has been observed from the Fig. 9, as the noise increases, MSE value decreases.

5.3 Chosen plaintext analysis

In CPA, attacker has the plain image and scheme. With respect to these, he will try the cipher image. Normally, DRPE is highly vulnerable to CPA. If an attacker chooses Dirac delta function [31] which is shown in the below equation,

$$\delta(x, y) = \begin{cases} 
1, & x = 0 \text{ and } y = 0 \\
0, & \text{otherwise}
\end{cases}$$

![Fig. 6 3D plot analysis (a) Plain image (b) cipher image (c) recovered image](image-url)
Fig. 7 Occlusion analysis (a) 10% are occluded (b) corresponding decrypted image (c) 25% are occluded (d) corresponding decrypted image (e) 75% are occluded (d) corresponding decrypted image
Dirac delta function is to be considering single nonzero pixel at the centre of the image and all the other values are zero. In order to perform Chosen plaintext analysis, created Dirac delta function is considered as plain image and cipher image calculation is given in the equation.

\[
DRPE_{cpa} = \frac{\text{ifft}(\text{fft}(\delta(x,y) \ast RPM1(x,y) \ast RPM2(x,y)))}{C_{16}}
\]

From the above equation, second secret key is easily obtained by \( drpe_{cpa} \). Figure 9 shows the CPA analysis of DRPE system (Fig. 10).

![Figure 8](image1.png)  
Fig. 8 Salt and pepper analysis (a) with the density of 0.2 (b) with the density of 0.9

![Figure 9](image2.png)  
Fig. 9 MSE Vs. Noise factor
5.4 Sensitivity analysis

The proposed system has been checked with sensitivity analysis [20, 21, 38, 47, 65]. It means, how much the system is sensitive even there is a small difference. Then only when attacker

![Fig. 10](a) Dirac delta function (b) 3D plot of Dirac delta function; (c) DRPE encrypted image with CPA; (d) decrypted image of DRPE with CPA (e) encrypted image based on complex S-Box (f) decrypted image of DRPE with CPA
tries with all possibilities, he should not be able to get back the image. Figure shows the clear picture about sensitivity analysis. LCT has three security parameters; until unless attacker gets all three parameters, he is not possible for cracking. So, analysis made w.r.t LCT. Figure 11. (a) represents the plot of medical image when all the security parameters are correct. Figure 11. (b) denotes the all wrong parameters Fig. 11 (c) Indicates one correct parameter and other two wrong parameters. Figure 11 (d) Represents only one wrong parameter. Hence, even attacker gets only one parameter, he is not capable to pull through the image. So, our proposed system is highly sensitive and provides best results.

6 Performance analysis

The proposed complex S-Box based asymmetric cryptosystem is instigated in MATLAB R2020b and the rapidity is tested on Intel(R) core(TM) i5–7200 CPU @ 2.5–2.71 GHz, 8 GB RAM successively Windows 10. The time duration for the proposed system execution is 0.534 seconds.

---

**Fig. 11** (a) All three are correct parameters (b) All three are wrong parameter (c) Two are wrong parameters (d) only one wrong parameter
7 Conclusion

Since, DRPE is in need of nonlinearity; the foremost important block to support nonlinearity is S-Box. Creation of random S-Box and embedded in DRPE is already done. The size of the random S-Box is small and it replicates the values in order to match with the plain image. Moreover, the created S-Box is not consisting of complex values. The cryptanalysis has been performed and a new approach has been specified and given as proposed asymmetric cryptosystem. Numerical analysis such as histogram, occlusion, noise attack and sensitivity analysis has been done for the proposed asymmetric cryptosystem. The transform used for proposed system is LCT with three security parameters. These three security parameters also play a vital role for the robustness of our system. Hence, the proposed asymmetric cryptosystem provides better results in comparison with other DRPE systems.

Declarations

Conflict of interest  The authors declare no conflict of interest.

References

1. Abirami G, Venkataraman R (2019, December) Performance analysis of abac and abac with trust (abac-t) in fine grained access control model. In: 2019 11th international conference on advanced computing (ICoAC). IEEE. pp. 372-375. https://doi.org/10.1109/ICoAC48765.2019.246870
2. Abirami G, Venkataraman R (2019) Attribute based access control with trust calculation (ABAC-T) for decision policies of health Care in Pervasive Environment. LIJITEE 8
3. Abirami G, Venkataraman R (2021) Performance analysis of the dynamic trust model algorithm using the fuzzy inference system for access control. Comput Electr Eng 92:107132. https://doi.org/10.1016/j.compeleceng.2021.107132
4. Abuturab MR (2012) Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding. Opt Lasers Eng 50(10):1383–1390
5. Abuturab MR (2012) Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. Opt Lasers Eng 50(9):1209–1216
6. Abuturab MR (2018) Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition. Opt Laser Technol 98:298–308. https://doi.org/10.1016/j.optlastec.2017.08.010
7. Carnicer A, Montes-Usategui M, Arcos S, Juvels I (2005) Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt Lett 30(13):1644–1646
8. Chen L, Zhao D (2006) Optical image encryption with Hartley transforms. Opt Lett 31(23):3438–3440
9. Chowdhary CL, Patel PV, Kathrotia KJ, Attique M, Perumal K, Ijaz MF (2020) Analytical study of hybrid techniques for image encryption and decryption. Sensors 20(18):5162. https://doi.org/10.3390/s20185162
10. Devanaj P, Kavitha C (2016) An image encryption scheme using dynamic S-boxes. Nonlinear Dyn 86(2):927–940. https://doi.org/10.1007/s11071-016-2934-7
11. Dhaka VS, Meena SV, Rani G, Sinwar D, Ijaz MF, Woźniak M (2021) A survey of deep convolutional neural networks applied for prediction of plant leaf diseases. Sensors 21(14):4749. https://doi.org/10.3390/s21144749
12. Farwa S, Muhammad N, Shah T, Ahmad S (2017) A novel image encryption based on algebraic S-box and Arnold transformation. 3D Res 8(3):1–14. https://doi.org/10.1007/s13319-017-0135-x
13. Girija R, Kumar P (2016, December) Walsh Hadamard transform and cryptographic properties in stream cipher. In: 2016 2nd international conference on contemporary computing and informatics (IC3I). IEEE. pp. 199-203
14. Girija R, Singh H (2017, October) A new substitution-permutation network cipher using Walsh Hadamard transform. In: 2017 international conference on computing and communication Technologies for Smart Nation (IC3TSN). IEEE. pp. 168-172
15. Girija R, Singh H (2018) Design of a novel pseudo random generator based on Walsh Hadamard transform and bi S-boxes. Procedia Comput Sci 132:795–804

16. Girija R, Singh H (2018) A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. Opt Quant Electron 50(5):1–24

17. Girija R, Singh H (2018) Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform. 3D Res 9(3):1–20. https://doi.org/10.1007/s13319-018-0192-9

18. Girija R, Singh H (2018) Enhancing security of double random phase encoding based on random S-box. 3D Res 9(2):1–20. https://doi.org/10.1007/s13319-018-0165-z

19. Girija R, Singh H (2019) Triple-level cryptosystem using deterministic masks and modified gerchberg-saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition. Optik 187:238–257

20. Girija R, Singh H (2019) An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain. Multimedia Tools Appl 79:34717–34735. https://doi.org/10.1007/s11042-019-7733-y

21. Girija R, Anshula, Singh H (2021) Security-enhanced optical nonlinear cryptosystem based on modified Gerchberg-Saxton iterative algorithm. Optik 244:167568. https://doi.org/10.1016/j.ijleo.2021.167568

22. Guo C, Muniraj I, Sheridan JT (2016) Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems. Appl Opt 55(17):4720–4728

23. Healy JJ (2017) Simulating first order optical systems—algorithms for and composition of discrete linear canonical transforms. J Opt 20(1):014008

24. Hennelly B, Sheridan JT (2003) Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 28(4):269–271

25. Hennelly BM, Sheridan JT (2005) Fast numerical algorithm for the linear canonical transform. J Opt Soc Am 22(5):928–937

26. Huang ZJ, Cheng S, Gong LH, Zhou NR (2020) Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Opt Lasers Eng 124:105821

27. Hwang HE, Han P (2006) Fast algorithm of phase masks for image encryption in the Fresnel domain. J Opt Soc Am 23(8):1870–1874

28. Ijaz MF, Attique M, Son Y (2020) Data-driven cervical cancer prediction model with outlier detection and over-sampling methods. Sensors 20(10):2809. https://doi.org/10.3390/s20102809

29. Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabrè E, Millán MS et al (2016) Roadmap on optical security. J Opt 18(8):083001

30. Kumar P, Joseph J, Singh K (2016) Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures. In: Linear canonical transforms. Springer, New York, pp 367–396

31. Kumari E, Singh P, Mukherjee S, Purohit GN (2020) Analysis of triple random phase encoding cryptosystem in Fresnel domain. Results Opt 1:100009. https://doi.org/10.1016/j.rjo.2020.100009

32. Liansheng S, Bei Z, Xiaojuan N, Ailing T (2016) Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. Opt Express 24(1):499–515

33. Liu S, Mi Q, Zhu B (2001) Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. Opt Lett 26(16):1242–1244

34. Liu S, Yu L, Zhu B (2001) Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. Opt Commun 187(1–3):57–63

35. Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, Liu S (2011) Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt Commun 284(1):123–128

36. Liu H, Kadir A, Gong P (2015) A fast color image encryption scheme using one-time S-boxes based on complex chaotic system and random noise. Opt Commun 338:340–347. https://doi.org/10.1016/j.optcom.2014.10.021

37. Lu D, Jin W (2011) Color image encryption based on joint fractional Fourier transform correlator. Opt Eng 50(6):068201

38. Maan P, Singh H (2018) Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain. 3D Res 9:53. https://doi.org/10.1007/s13319-018-0205-8

39. Matoba O, Javidi B (1999) Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt Lett 24(11):762–764

40. Nishchal NK, Joseph J, Singh K (2003) Fully phase encryption using fractional Fourier transform. Opt Eng 42(6):1583–1588
68. Zhao L, Healy JJ, Sheridan JT (2015) Constraints on additivity of the 1D discrete linear canonical transform. Appl Opt 54(33):9960–9965
69. Zhao L, Muniraj I, Healy JJ, Malallah RE, Cui XG, Ryle JP, Sheridan JT (2017, May) 2D non-separable linear canonical transform (2D-NS-LCT) based cryptography. In: Holography: advances and modern trends V. International Society for Optics and Photonics. Vol. 10233, p. 102331B

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.