AJP

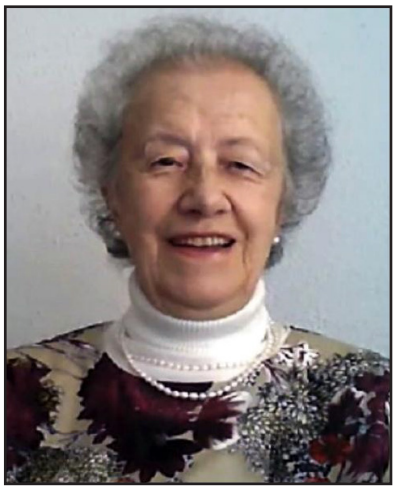
ISSN : 0971 - 3093

Vol 31, No 7, July 2022

ASIAN JOURNAL OF PHYSICS

An International Peer Reviewed Research Journal

Special issue in honour of Prof Maria J Yzuel



Prof Maria J Yzuel

Guest Editor : Eva Acosta

ap

ANITA PUBLICATIONS

FF-43, 1st Floor, Mangal Bazar, Laxmi Nagar, Delhi-110 092, India

B O : 2, Pasha Court, Williamsville, New York-14221-1776, USA

Asian Journal of Physics
Vol. 31, No 7 (2022) A1-A12
Available on: www.asianjournalofphysics.com

ap

An asymmetric optical cryptosystem based on Radon transform for phase image encryption

Ravi Kumar[1], Sakshi[2] and Kehar Singh[3]

[1]*Department of Physics, SRM University-AP, Andhra Pradesh-522 502, India,*
[2]*Ben-Gurion University of the Negev, P. O. Box 653, Beer-Sheva 8410501, Israel*
[3]*Optics and Photonics Center, Indian Institute of Technology Delhi, New Delhi-110 016, India*

Dedicated to Prof Maria J Yzuel

In this paper, we propose a fully-phase image encryption and decryption technique in the Radon transform (RT) domain, having multiuser capabilities. The RT of a two-dimensional (2D) digital image gives projections at arbitrarily given angles, providing additional layer of security in the system. Multiple private keys for decryption are obtained using polar decomposition (PD) in the encryption process, enabling the multiuser capability. For encryption, the input amplitude image is first converted to a phase image and modulated using a structured phase mask (SPM) having preset topological charge. Then the modulated complex image is Fresnel propagated to a certain distance at which the real and imaginary parts of the complex wavefront are separated making the scheme asymmetric. The imaginary part is stored as the private key and real part is further subjected to PD and RT to obtain a set of private keys and the final encrypted image. The proposed technique has large key space and is highly sensitive to the encryption parameters. The robustness of the proposed image encryption method is tested against various common attacks such as noise-, occlusion-, and brute force attacks. Numerical simulation results confirm the validity and effectiveness of the proposed cryptosystem.

Keywords: Phase image, Optical image encryption, Radon transform, Polar decomposition, Structured phase mask.
DOI: 10.54955/AJP.31.7.2022.A1-A12

1 Introduction

In the modern world, the ever-increasing digital dependency in every sphere of life such as the online governmental data, e-commerce, healthcare services, and remote sensing etc. has made information security an essential aspect. Therefore, the development of advanced security methods to avoid unauthorized access to information, is of paramount importance. In this regard, the optical encryption approach has been explored by many researchers to develop hybrid security-enhanced cryptosystems. Such an approach has several advantages [1] over digital counterparts, such as parallel processing, increased degrees of freedom (i.e. phase, coherence, wavelength, polarization, and orbital angular momentum of light), fast computing, and multidimensional capabilities. Double random phase encoding (DRPE) technique proposed by Refregier and Javidi [2] in 1995 opened pathway for optical image encryption. In DRPE, a 4-f optical setup is utilized to encode the image information into a random white noise. To achieve this, two statistically-independent random phase masks (RPMs) placed respectively in the object and the spatial frequency domains, serve as the security keys. Further, to enhance the security, the DRPE is explored in various other transform domains such as the Fresnel-, [3,4], fractional Fourier-, [5], gyrator-, [6], and Hartley transform [7] etc. However, the DRPE architecture is inherently linear and falls in the category of symmetric cryptosystems, i.e., the encryption and decryption keys are the same. Many cryptosystems are found to be vulnerable to various

Corresponding author
e mail: ry20724@gmail.com (*Ravi Kumar*)

type of attacks, such as chosen-plaintext attack (CPA) [8], chosen-ciphertext attack (CCA) [9], and known-plaintext attack (KPA) [10,11]. Kumar and Bhaduri [12] proposed an enhanced technique based on the DRPE architecture using Kronecker product and hybrid phase masks, which is robust against the KPA but still linear in nature.

To deal with the linearity issue, asymmetric optical cryptosystems were also reported [13,14]. As an example, the phase truncated Fourier transform (PTFT) was used for the asymmetric encryption. These methods are robust against some common attacks such as CPA and KPA, but a two-step iterative phase-retrieval algorithm-based special attack [15] has been reported to break the PTFT-based cryptosystems. Over a period, many attempts have been made and other optical techniques have been proposed to overcome these problems [16-25]. A number of techniques have been published based on diffractive imaging [16], computational ghost imaging [17], polarization [18], fully-phase encryption [19], interference [20-22], Kolmogorov phase screens [23], 2D non-separable linear canonical transform (2D NS-LCT) [24], and spiral phase function [25] etc. These techniques have been utilized to make the optical cryptosystems robust to various potential attacks and to significantly enhance the security.

Asymmetric optical cryptosystems based on different decompositions such as the equal modulus decomposition [26,27], random modulus decomposition [28], common vector decomposition [29], and singular value decomposition [30,31] were also introduced to increase the key space and enhance the system security. Recently, polar decomposition based optical cryptosystems having multiuser capabilities, have also been developed [32,33]. Lately, a few optical encryption techniques have been demonstrated experimentally also [34-40]. Mosso *et al* [34] experimentally validated an optical cryptosystem based on the single-lens imaging architecture and phase retrieval algorithm (PRA). Furthermore, the encryption techniques based on interference [35,36], joint Fresnel transform correlator with double optical wedges [37] and optical encryption of grayscale information [38] have also been verified experimentally. Despite the existence of many cryptosystems, the search continues for newer advanced methods which can provide higher security with less computational and practical complexity.

In this paper, we present a new optical cryptosystem for phase image encryption. The proposed method is asymmetric in nature and provide a large key space. The sensitivity of all the security keys is checked by calculating the cross-correlation (CC), peak-signal-to-noise ratio (PSNR), and mean-squared-error (MSE). The rest of the paper is organized as follows: theoretical details of the Radon transform, Fresnel propagation, and polar decomposition are given in Sec 2. In Sec 3, the proposed encryption and decryption processes are discussed in detail. Numerical simulation in support of the proposed method along with the key sensitivity and attack analysis, are discussed in Sec 4. Finally, some concluding remarks are given in Sec 5.

2 Theoretical background

In this section, the theoretical background of the Radon transform and polar decomposition is discussed with their mathematical equations.

2.1 Radon Transform

Radon transform is a linear integral transform proposed by the Austrian mathematician J Radon in 1917 to project 2D objects along parallel rays. The theory and applications of RT have been subjects of many review articles and books [41-46]. For a continuous 2D function $f(x, y)$ (i.e. 2D image in the current study), a one dimension (1D) projection can be formed by performing a line integration of the image intensity $f(x, y)$ along an arbitrary line in the xy-plane, a distance L from the origin and at angle θ to the x-axis in the range of 0 to 2π. Using this, the projection of a parallel-ray beam may be modeled by combining such lines, and an arbitrary point in the projection profile at coordinates (L, θ) can be obtained by sum along the line $x\cos\theta + y\sin\theta = L$. For a continuous 2D function (image), the ray sum will be a line integral and can be represented mathematically as [47-51],

$$RT(L, \theta) = \int\int_{-\infty}^{\infty} f(x, y)\, \delta(x\cos\theta + y\sin\theta - L)dxdy \quad (1)$$

where $f(x, y)$ denotes the gray level of a pixel in the input image and $\delta(\cdot)$ is the Dirac-Delta function. This collection $RT(L, \theta)$ at all angles θ, or the projection of $f(x, y)$ along an arbitrary line in the xy-plane is the Radon transform [49]. The original image can be reconstructed back by using the 1D projections at different angles. It has been shown that the Radon transform can also be implemented optically [49,51].

2.2. Polar Decomposition (*PD*)

In linear algebra, PD is used to factorize the matrices into a set of linearly independent components [32,52]. For a 2D matrix, $I(x, y)$ of size M × N, the PD can be given as:

$$PD(I) = [R\ U\ V]$$

where, U and V are symmetric, positive definite matrices and R is a rotational matrix. U, V, and R all have the same sizes as the input matrix. The original matrix I can be reconstructed back using the rotational matrix, R and one of the symmetric matrix, i.e. $I = R \times U$ or $I = V \times R$. This decomposition is very useful and generally used in continuum mechanics. If the matrix I is invertible, then U and V are positive definite matrices and R is unique. On the other hand, if $I \in P^{n \times n}$, then for the left or right PD, R is orthogonal, and U (or V) is symmetric matrix with non-negative eigenvalues.

3 Proposed optical cryptosystem

In this section, the step by step proposed encryption and decryption procedures are discussed in full details with the corresponding mathematical equations and flow charts. The encryption process involves of the following steps:

(i). First, the input image $I(x, y)$, is phase encoded and modulated with a *SPM*, to get $I'(x, y)$, as

$$I'(x, y) = exp[i2\pi I(x, y)] \times SPM \quad (3)$$

where, *SPM* is the structured phase mask obtained using the radial Hilbert phase function $exp(iq\theta)$, where q is the topological.

(ii). The modulated image $I'(x, y)$ is then Fresnel propagated with distance d and the real and imaginary parts of the complex output are separated as

$$I''(u, \upsilon) = FrT_{\lambda, d}\{I'(x, y)\} \quad (4)$$

$$I_1(u, \upsilon) = re\{I''(u, \upsilon)\} \quad (5)$$

$$I_2(u, \upsilon) = imag\{I''(u, \upsilon)\} \quad (6)$$

where, $re\{.\}$ and $imag\{.\}$ are the operators which give the real and imaginary parts of a complex function. The imaginary part $I_2(u, \upsilon)$ is stored as the private key.

(iii). The real part $I_1(u, \upsilon)$ is then polar decomposed to get two symmetric (U, V) and one rotational matrix (R). The rotational matrix image is then Radon transformed with projection angle θ to get $E(u, \upsilon)$.

$$PD\{I_1(u, \upsilon)\} = [R\ U\ V] \quad (7)$$

$$E(u, \upsilon) = RT_{\theta}\{R\} \quad (8)$$

(iv). Finally, the intermediate image $E(u, \upsilon)$ is modulated with the RPM to get the final encrypted image.

$$En(u, \upsilon) = E(u, \upsilon) \times RPM \quad (9)$$

where *RPM* is given by $exp\,(i2\pi R(x, y))$, $R(x, y)$ being the random matrix in the range of [0 1]. The schematic of the proposed cryptosystem is shown in Fig 1.

The original input image can be retrieved with high quality by using all the correct security keys and implementation as shown in Fig 1(b). The encrypted image is first multiplied with the complex conjugate of the *RPM* and then inverse Radon transform is calculated. The private key 2 (U or V) is then used as discussed

in section 2 to get the intermediate image. Then the first private key (i.e. imaginary part) is added to it to get the complex image. This complex image is then Fresnel propagated with distance d and modulated using complex conjugate of the SPM. Finally, the angle of this modulated image will give the decrypted image. Mathematically, the decryption process can be described by following equations:

$$D_1(u, \upsilon) = En(u, \upsilon) \times RPM^* \tag{10}$$

$$D_2(u, \upsilon) = IRT_\theta\{D_1(u, \upsilon)\} \times U \tag{11}$$

$$D_3(u, \upsilon) = FrT_{\lambda, d}\{D_2(u, \upsilon) + I_2(u, \upsilon)\} \tag{12}$$

$$D(x, y) = angle\{D_3 \times SPM^*\} \tag{13}$$

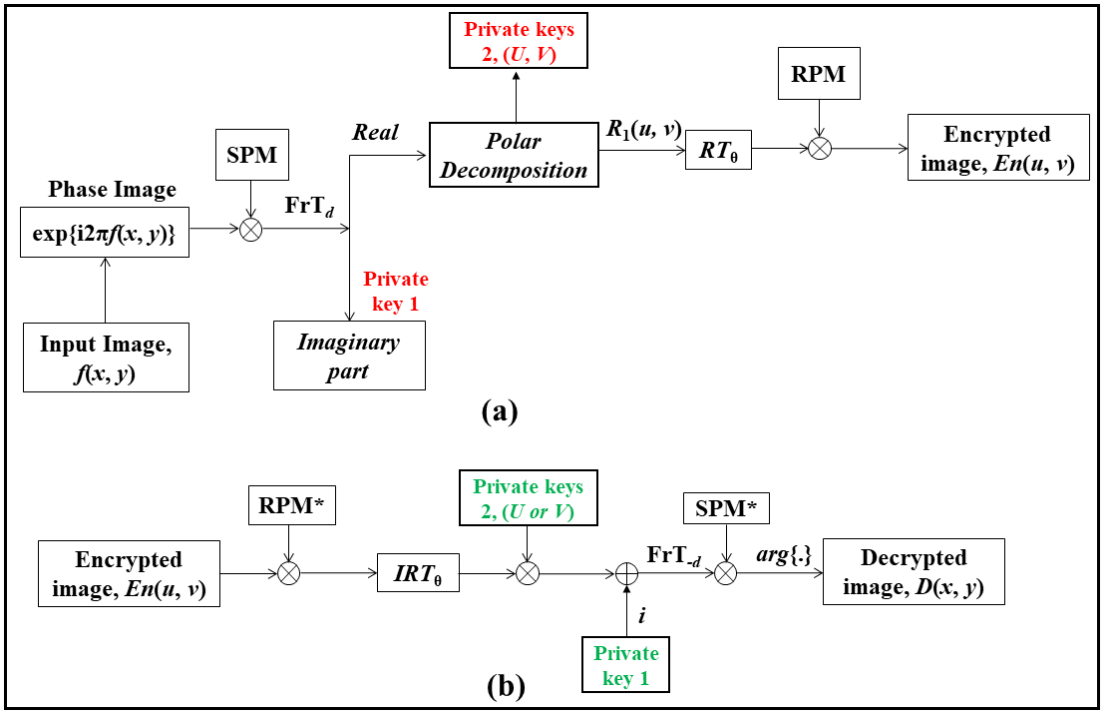


Fig 1. Schematic of the proposed scheme. (a) Encryption process, and (b) Decryption process.

4 Results and Discussions

The efficiency and validity of the proposed technique is verified through numerical simulations performed using MATLABTM (version R2020b) on a PC having an 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz processor and 8GB RAM.

4.1. Encryption and Decryption Results

To verify the proposed method, 'Lena' image (256×256 pixels) shown in Fig 2(a), is chosen as the input image. First, it is converted into a phase image as discussed in the previous section, which is further processed for encryption. Figure 2 (b) shows the *SPM* (q =10) used for encryption, whereas Figs 2(c) and 2 (d) show the two private keys obtained after the PD. The *RPM* is shown in Fig 2 (e) and the private key 1 is shown in Fig 2 (f). The final encrypted image for transmission is shown in Fig 2 (g); whereas the decrypted

image with all correct keys is shown in Fig 2 (h). The high CC value (~0.95) and good visible quality confirms the validity of the proposed scheme. For encryption, the Radon transform parameters used for encryption are as follows: 367 numbers of projections are taken for angles that are equally spaced at 0.49 degrees in the interval 0 to 179.49 degrees. For Fresnel propagation, a distance of 0.5 cm and wavelength of 632 nm is used.

We have also calculated the computation time (using our PC configuration) for the encryption and decryption processes. The time taken for encryption process was 0.1574 seconds, whereas the decryption process took 0.1575 seconds. This shows good computational efficiency of the proposed method.

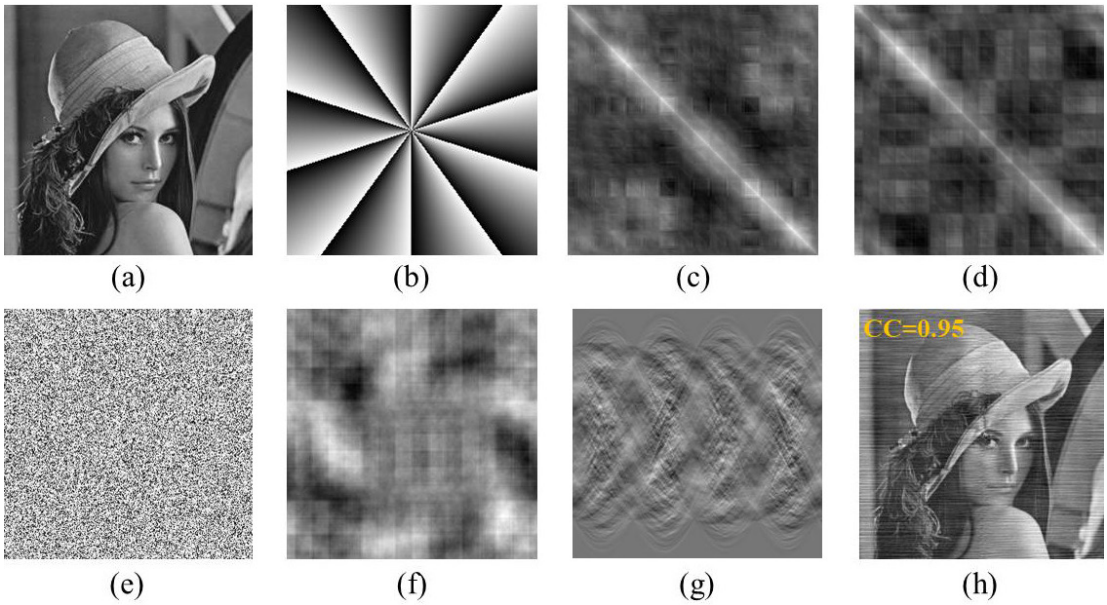


Fig 2. Encryption results: (a) Input image; (b) SPM with topological charge q =10; (c) and (d) two private security keys after PD, U and V, respectively; (e) RPM; (f) private key 1; (g) Final encrypted image; and (h) Correct decrypted image.

4.2. Key sensitivity analysis

We have checked the sensitivity of each security key by performing the decryption using wrong security keys and the results are shown in Fig 3. The decrypted images with wrong *SPM* (q = 5) are shown in Fig 3 (a). When wrong private key 1 is used, the decrypted image is shown in Fig 3 (b), whereas the decrypted image with wrong private key 2 is shown in Fig 3 (c). In both cases, the decrypted image does not reveal any information of the original image and the CC values are very low. The decrypted images with wrong Fresnel propagation parameters distance (change by 0.5 mm) and wavelength (change by 20 nm) are shown, respectively in Figs 3(d) and 3(e). Figure 3(f) shows the decrypted image with RPM. The results confirm that the original image can only be revealed when all the correct security keys are used for decryption. If any one of the keys is missing or when there is a slight deviation in the original values of the security keys parameters, no useful information of the original image can be revealed. This proves the effectiveness of the security keys.

The sensitivity to the topological charge q, and Fresnel propagation parameters (distance d and wavelength λ) are further analyzed by plotting the CC, PSNR, and MSE values with small deviation in the original values. The corresponding plots for each case are shown respectively in Figs 4 and 5. which clearly indicate that even a small variation in the original values will lead to sharp change in the CC, PSNR, and MSE values. This verifies the effectiveness of these parameters in enhancing the security of the cryptosystem.

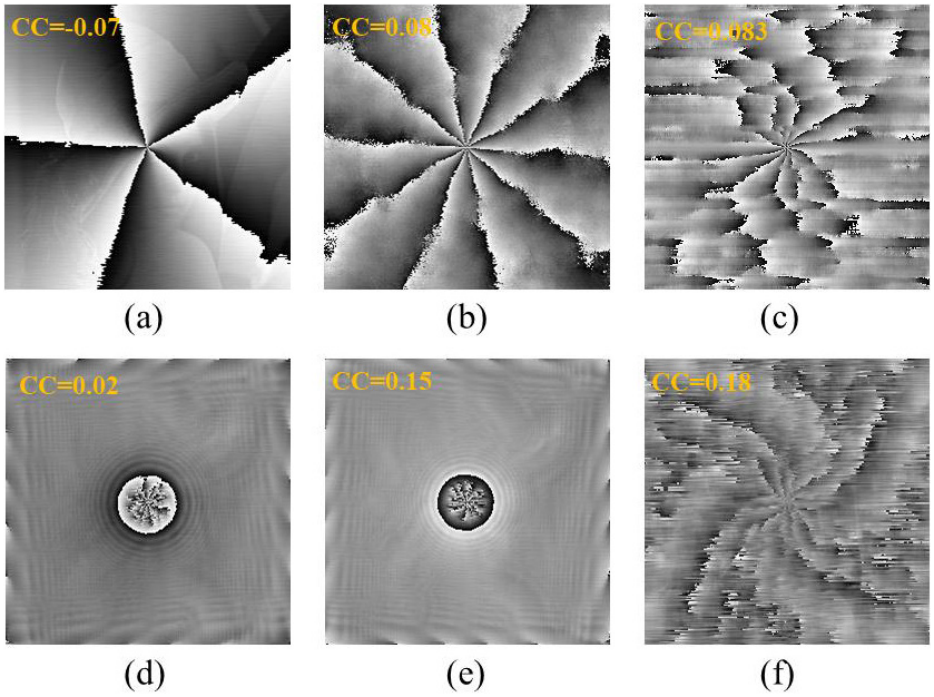


Fig 3. Decrypted images with wrong security keys: (a) Wrong topological charge; (b) Wrong private key 1; (c) Wrong private key 2; (d) and (e) Wrong Fresnel propagation parameters, distance (changed by 0.5 mm) and wrong wavelength (change by 20 nm) (f) Wrong RPM.

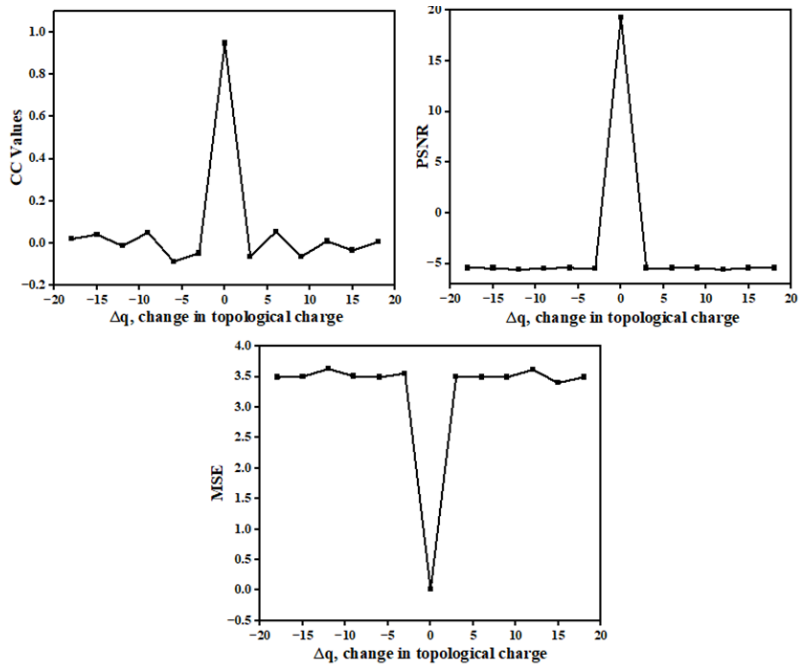


Fig 4. Plots for CC, PSNR and MSE values with small deviation in the original value of topological charge q used for the SPM.

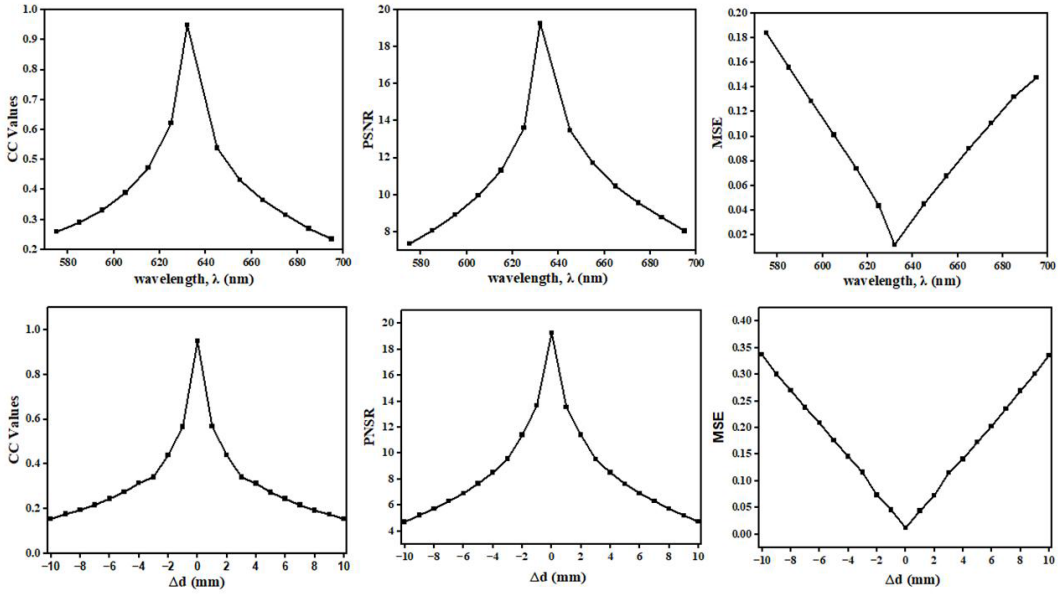


Fig 5. Plots for CC, PSNR and MSE values with small deviation in the original values of the Fresnel propagation parameters: distance d (first row) and wavelength λ (second row), respectively.

4.3. Robustness analysis

While designing new cryptosystem, it is important to check its robustness against various attacks. Thus, we have performed the attack analysis of the proposed technique against commonly existing attacks such as noise and occlusion contamination, and brute force attacks. The CC values were calculated between the original input image and the resulting decrypted image and examined.

4.3.1. Noise and occlusion attacks

There is always a risk of contamination by unwanted noise or loss of some information while transmitting sensitive encrypted information. Thus, the robustness of the proposed technique is checked under both possibilities. For noise contamination test, we have added the Gaussian noise in the encrypted image as follows:

$$E' = E(1+ k\,G), \tag{21}$$

where E and E' are respectively the encrypted and noise contaminated encrypted images. G is the added Gaussian random noise with zero mean and 0.05 variance, whereas k denotes the strength of the Gaussian noise. Decryption with all the correct keys is performed using the noise contaminated encrypted image. The results for noise attack analysis are shown in Fig 6. From the results, it can been seen that the proposed method is robust against noise contamination.

Similarly, for the occlusion (information loss) test, decryption is performed with some part of the encrypted image occluded, i.e., some pixels have been assigned zero values. For that, a square section in the central region of the encrypted images corresponding to 10% and 20% pixels are blocked (set to zero) as shown, respectively in Figs 7(a) and 7(c). The corresponding decrypted images from occluded encrypted images are shown, respectively in Figs 7(b) and 7(d). The retrieved images under noise and occlusion contamination reveal significant information about the original input image which confirms the robustness of the proposed method against such environment.

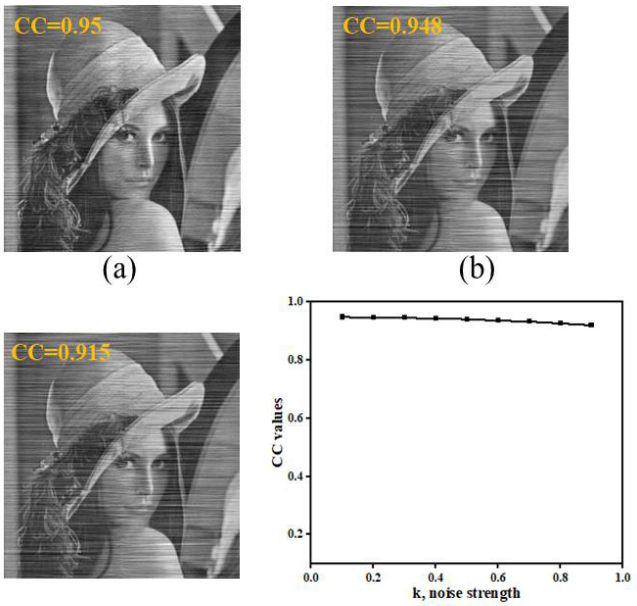


Fig 6. Noise attack results: Decrypted image with; (a) Without noise contamination; (b) With noise strength $k = 0.1$; (c) With noise strength $k = 0.9$; and (d) Variation of CC values with strength of noise.

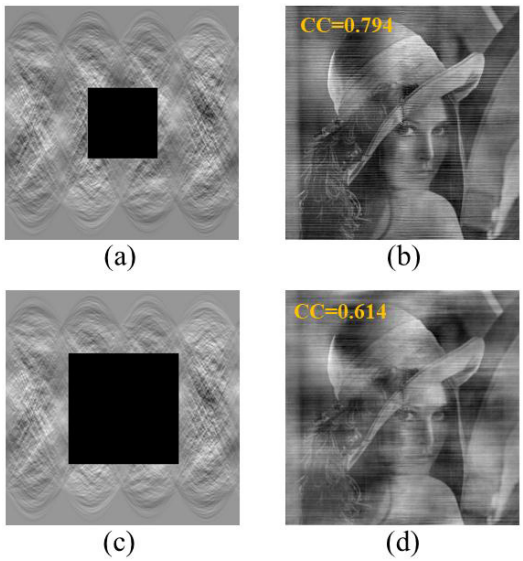


Fig 7. Occlusion attack results: (a) and (c) are 10% and 20% occluded encrypted images, respectively; (b) and (d) are corresponding decrypted images.

4.3.2. Brute force attack

In the brute force attack, the invader tries several random combinations for the security keys used in the encryption process. The total number of combinations for a given size of random phase key can be calculated based on the image size. For instance, for an input image of size 256 × 256 pixels, the total number

of combinations possible will be of the order of $L^{2(256\times256)}$. In the current study, the input image used has, L = 256 gray levels, resulting in 256^{131072} number of random keys to be tried. Consequently, for any practical value of L the number of random trials would be very large, and it increases exponentially with the size of the image. We have tried this attack for the first private security key. Figure 8 shows the plot of the calculated CC values between the original and decrypted images for 1000 random trials. From the results, it is clear that the proposed method is resistant to this type of attack, as the calculated CC values were very low.

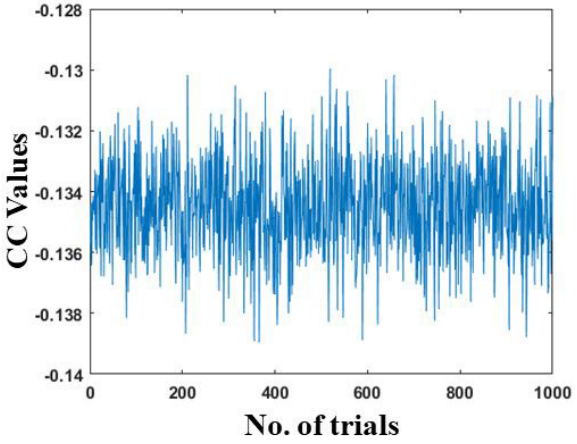


Fig 8. Plot for the calculated CC values between the original image and the decrypted image by testing 1000 possibilities for the first private security key.

5 Concluding remarks

In conclusion, a new multiuser asymmetric cryptosystem for phase image encryption is proposed in the Radon transform domain. Polar decomposition is used to generate multiple private security keys for decryption enabling the multiuser platform for the proposed method. The proposed scheme has a large number of security keys which includes the SPM, Fresnel propagation parameters, two private keys, RPM and Radon projection parameters. The robustness of the proposed method is checked against noise, occlusion, and brute force attacks. Moreover, the complex asymmetric nature of proposed techniques may make it immune to plaintext attacks such as KPA and CPA. The presented results validate the efficacy of the proposed method and sensitivity of the various security keys. However, the resistance against the KPA, CPA, and other attack remains to be analyzed. Also, the application of various tools of artificial intelligence (such as deep learning) [53-56] have proved the vulnerability of many cryptosystems hitherto considered safe. This aspect should also be addressed while checking the safety of the existing cryptosystems or that may be designed in future. This work is a subject of our ongoing research.

References

1. Chen W, Javidi B, Chen X, Advances in optical security systems, *Adv Opt Photon*, 6(2014)120–55.
2. Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding, *Opt Lett*, 20(1995)767–769.
3. Situ G, Zhang J. Double random-phase encoding in the Fresnel domain, *Opt Lett*, 29(2004)1584–1586.
4. Matoba O, Javidi B, Encrypted optical memory system using three-dimensional keys in the Fresnel domain, *Opt Lett*, 24(1999)762–764.
5. Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt Lett*, 25(2000)887–889.

6. Li H, Image encryption based on gyrator transform and two-step phase-shifting interferometry, *Opt Lasers Eng*, 47(2009)45–50.
7. Li X, Zhao D, Optical image encryption with simplified fractional Hartley transform, *Chin Phys Lett*, 25(2008) 2477–2480.
8. Peng X, Wei H, Zhang P. Chosen-plaintext attack on lens less double-random phase encoding in the Fresnel domain, *Opt Lett*, 31(2006)3261–3263.
9. Carnicer A, Montes-Usategui M, Arcos S, Juvells I. Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys, *Opt Lett*, 30(2005)1644–1646.
10. Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys, *Opt Lett*, 31(2006)1044–1046.
11. Tashima H, Takeda M, Suzuki H, Obi T, Yamaguchi M, Ohyama N. Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack, *Opt Express*, 18(2010)13772–13781.
12. Kumar R, Bhaduri B. Optical image encryption using Kronecker product and hybrid phase masks, *Opt Laser Technol*, 95(2017)51–55.
13. Qin W, Peng X, Asymmetric cryptosystem based on phase-truncated Fourier transforms, *Opt Lett*, 35(2010)118–120.
14. Chen W, Chen X, Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain, *Opt Commun*, 284(2011)3913–3917.
15. Wang X, Zhao D, A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms, *Opt Commun*, 285(2012)1078–1081.
16. Chen W, Chen X, Sheppard CJR, Optical image encryption based on diffractive imaging, *Opt Lett*, 35(2010)3817–3819.
17. Clemente P, Durán V, Torres-Company V, Tajahuerce E, and Lancis J, Optical encryption based on computational ghost imaging, *Opt Lett*, 35(2010)2391–2393.
18. Rajput S K, Nishchal N K, Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain, *Appl Opt*, 52(2013)4343–4352.
19. Nishchal N K, Joseph J, Singh K, Fully phase encryption using fractional Fourier transform, *Opt Eng*, 42(2003)1583–1588.
20. Zhang Y, Wang B, Optical image encryption based on interference, *Opt Lett*, 33(2008)2443–2445.
21. Wang Q. Optical image encryption with silhouette removal based on interference and phase blend processing, *Opt Commun*, 285(2012)4294–4301.
22. Niu C H, Wang XL, Lv N G, Zhou Z H, Li X Y. An encryption method with multiple encrypted keys based on interference principle, *Opt Express*, 18(2010)7827–7834.
23. Kumar R, Bhaduri B, Quan C, Asymmetric optical image encryption using Kolmogorov phase screens and equal modulus decomposition, *Opt Eng*, 56 (2017), Art.ID:113109; doi.org/10.1117/1.OE.56.11.113109.
24. Kumar R, Sheridan J T, Bhaduri B, Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm, *Opt Laser Technol*, 107(2018)353–360.
25. Kumar R, Bhaduri B. Optical image encryption in Fresnel domain using spiral phase transform. *J Opt*, 19(2017) Art.ID:095701; doi.10.1088/2040-8986/aa7cb1.
26. Deng X, Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: comment, *Opt Lett*, 40(2015)3913–3913.
27. Wu J, Liu W, Liu Z, Liu S. Cryptanalysis of an asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition, *Appl Opt*, 54(2015)8921–8924.
28. Abuturab M R. Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition, *Opt Laser Tech*, 98(2018)298–308.
29. Chen L, He B, Chen X, Gao X, Liu J. Optical image encryption based on multi-beam interference and common vector decomposition, *Opt Commun*, 361(2016)6–12.

30. Abuturab M R. Color information verification system based on singular value decomposition in gyrator transform domains, *Opt Lasers Eng*, 57(2014)13–19.
31. Kumar R, Bhaduri B, Nischal N K. Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition, *J Opt*, 2018; 20:015701; doi. 10.1088/2040-8986/aa9943.
32. Kumar R, Quan C, Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform, *Opt Lasers Eng*, 120(2019)118–126.
33. Sachin, Kumar R, Singh P, Multiuser optical image authentication platform based on sparse constraint and polar decomposition in Fresnel domain, *Phys Scripta*, 47(2022); Art.ID:115101; doi.org/10.2139/ssrn.4103716.
34. Mosso F, Bolognini N, Pérez D G. Experimental optical encryption system based on a single-lens imaging architecture combined with a phase retrieval algorithm, *J Opt*, 2015;17:065702; doi.10.1088/2040-8978/17/6/065702.
35. Weng D, Zhu N, Wang Y, Xie J, Liu J, Experimental verification of optical image encryption based on interference, *Opt Commun*, 284(2011)2485–2487.
36. Li J, Li J, Shen L, Pan Y, Li R, Optical image encryption and hiding based on a modified Mach-Zehnder interferometer, *Opt Express*, 22(2014)4849–4860.
37. Shen X, Dou S, Lei M, Chen Y, Optical image encryption based on a joint Fresnel transform correlator with double optical wedges, *Appl Opt*, 55(2016)8513–8522.
38. Zea A V, Barrera J F, Torroba R. Experimental optical encryption of grayscale information, Appl Opt, 56(2017) 5883–5889.
39. Li X, Zhao M, Xing Y, Zhang H, Li L, Kim S, Zhou X, Wang Q, Designing optical 3D images encryption and reconstruction using monospectral synthetic aperture integral imaging, *Opt Express*, 26(2018)11084–11099.
40. Rajput S K, Matoba O, Optical voice encryption based on digital holography, *Opt Lett*, 42(2017)4619–4622.
41. Barrett H H, Swindell W, Radiological Imaging: The Theory of Image Formation, Detection, and Processing, Vol 2, (Academic Press N.Y),1981.
42. Deans S R, The Radon Transform and Some of Its Applications, (Wiley, N.Y), 1983.
43. Barrette H H, III The Radon Transform and Its Applications, *Progr Opt*, 21(1984)217–286.
44. Herman G T, Fundamentals of Computerized Tomography: Image Reconstruction from Projections, 2nd edn. (Springer), 2010.
45. Feeman T G, The Radon transform, the mathematics of medical imaging; http://www.springer.com/978-0-387-92711-4.
46. Kuchment P K, The Radon Transform and Medical Imaging, (SIAM, 2014).
47. Ritika A, Xiong Y, Quan C. Optical image encryption using Radon transform, Progr Electromag Res Symp, Fall (PIERS - FALL), 2017:1235-1238. doi.10.1109/PIERS-FALL.2017.8293320.
48. Shi D-F, Huang J, Meng W-W, Yin K-X, Sun B-Q, Wang Y-J, Yuan K, Xie C-B, Liu D, Zhu W-Y, Radon single-pixel imaging with projective sampling, *Opt Express*, 27(2019)14594–14609.
49. Wu J-J, Li S-W, Optical multiple-image compression-encryption via single-pixel Radon transform, *Appl Opt*, 59(2020)9744–9754.
50. Leihong Z, Yang W, Dawei Z, Research on multiple-image encryption mechanism based on Radon transform and ghost imaging, *Opt Commun*, 504(2022); Art.ID:127494; doi.org/10.1016/j.optcom.2021.127494.
51. Ilovitsh T, Ilovitsh A, Sheridan J, Zalevsky Z, Optical realization of the Radon transform, *Opt Express*, 22(2014) 32301–32307.
52. Higham N J, Computing the polar decomposition with applications, *SIAM J Sci Stat Comp*, 7(1986)1160–1174.
53. Hai H, Pan S-X, Liao M H, Lu D J, He W-Q, Peng X, Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning, *Opt Express*, 27(2019)21204–21213.
54. Zhou L N, Xiao Y, Chen W, Learning-based attacks for detecting the vulnerability of computer-generated hologram based optical encryption, *Opt Express*, 28(2020)2499–2510.

55. Liao M H, Zheng S-S, Pan X-S, Lu D-J, He W-Q, Situ G-H. Peng X, Deep-learning based cipher text-only attack on optical double random phase encryption, *Optoelectron Adv*, 4 (2021) Art.ID:200016; doi.102906/oea.2021.20016.
56. He W-Q, Pan X-S, Liao M-H, Lu D-J, Xing Q, Peng X, A learning-based method of attack on optical asymmetric cryptosystems, *Opt Lasers Eng*, 138(2021) 106425; doi.org/10.1016/j.optlaseng.2020.106415

[*Received*: 30.08.2022]

Dr Ravi Kumar is an Assistant Professor at the Department of Physics, SRM University-AP, Andhra Pradesh, India. He received his Ph D degree in Physics from IIT (ISM) Dhanbad in June 2018. Before joining SRM-AP, he was a Postdoctoral Research Fellow at Electro-optics Laboratory, Ben-Gurion University of the Negev, Israel. The fellowship was sponsored by Planning and Budgeting Committee (PBC) of the Council for Higher Education, Israel. Prior to that, he was a postdoctoral research fellow at Smart Computational Imaging Laboratory, Nanjing University of Science and Technology, China, and National University of Singapore (NUS), Singapore. He has authored/coauthored a number of papers in high IF journals and presented several papers in international/national conferences. His research interests are in the field of optical information processing, digital holography, computational/optical imaging, quantitative phase imaging, optical metrology etc.