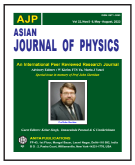


Asian Journal of Physics
Vol. 32, Nos 5-8 (2023) 385-397
Available on: www.asianjournalofphysics.com
ap

An asymmetric cryptosystem using deterministic phase masks, double random phase encoding, orthogonal encoding and decoding, and fractional Fourier transform

R Girija[1], H Singh[2], and Kehar Singh[3]

[1]*Department of Computer Science & Engineering,*
Manav Rachna International Institute of Research and Studies, Faridabad-121 004, India.

[2]*Department of Applied Sciences, The NorthCap University, Gurugram-122 017, India*

[3]*Optics and Photonics Center, Indian Institute of Technology Delhi, New Delhi-110 016, India*

Dedicated in memory of Prof John Sheridan

A Double Random Phase Encoding (DRPE) scheme has been proposed based on the use of deterministic phase masks, the fractional Fourier transform, and orthogonal encoding and decoding. In the proposed scheme, grey images are encrypted using an asymmetric cryptosystem. In order to convert the encrypted information to encoded information, Hadamard matrix with orthogonal property is used. In place of traditional masks, deterministic phase masks have been employed. Together with the use of orthogonal encoding, security of the proposed system is enhanced albeit at the cost of slight complication. The orthogonal encoding comprises only modest linear actions and is easy to implement. Numerous simulation results are provided in order to validate the proposed cryptosystem. Results have been provided for the mean-squared-error, peak signal-to-noise ratio, correlation-coefficient, histogram analysis, entropy, and sensitivity.

© Anita Publications. All rights reserved.

Keywords: Deterministic phase masks, Orthogonal encoding and decoding, Hadamard Matrix, Fractional Fourier transform.

1 Introduction

For the security of generated, transmitted, and stored sensitive information, encryption and decryption are essential to prevent unauthorized access to the information. Therefore, numerous encryption techniques have been developed by researchers for a long time. Algorithms for encryption of information using digital processing [1,2] has been commercially exploited in e-commerce, protection of copyrights and trademarks, banking, defence, fiber optic communication, internet-of things, earth resources survey using satellites, and medical applications etc. However, with the enormous volume of data that is becoming available in the present era, the processing speed and power consumed have been considered as bottlenecks for processing of images and videos. As a result, researches started investigating optical and hybrid encryption and decryption techniques. As is well-known, optical processing methods have several parameters (such as the amplitude, phase, wavelength, polarization, and orbital angular momentum) available to increase the key-space and therefore security of the cryptosystems.

Corresponding author
e mail: Girija.srikanth09@gmail.com (R Girija)

Double Random Phase Encoding (DRPE) in the Fourier domain has been a commonly used technique in optical cryptographic systems. Subsequently, the technique has been extended [3-20] to the Fresnel-, fractional Fourier-, gyrator, wavelet-, Hartley-, Mellin-, fractional Mellin-, and other domains to enhance the security and speed of the cryptosytems. There are many schemes based on use of joint-transform correlator, digital holography, computer holograms, speckles, full phase, watermarking and hiding, compression, and chaos etc. Several types of masks other than the random phase mask have also been used. Several books and review articles [3-20] are now available on the subject and can be referred to for details.

Despite all efforts to enhance the security of cryptosystems, information thefts and misuse are also on the increase. The attackers keep on designing newer algorithms and systems as attacking tools to break into the existing cryptosystems. Therefore, a desirable cryptosystem should withstand various types of attacks [8] such as the Brute force-, Differential-, Chosen-plaintext-, Known-plaintext, Chosen-cipher text-, and Specific attacks etc.

In the present paper, we propose the use of deterministic phase masks (DPMs), and orthogonal encoding in the fractional Fourier transform (FrFT) domain. The input image is multiplied with statistically-independent DPMs and FrFT of the product is obtained to get the encrypted image. To convert the encrypted image into an encoded image, orthogonal encoding plays an important role, by using the Hamdard matrix. Orthogonal encoding consists of linear actions and is easy to implement. The paper is organized as follows. Sec 1 is introductory in nature. Section 2 gives the necessary mathematical background, Sec 3 describes the proposed asymmetric scheme, and Sec 4 presents the numerical simulation results and their discussion. Performance analysis is discussed in Sec 5. Some conclusions and remarks are given in the last section.

2 Mathematical Background

2.1 Construction of the Deterministic Phase Masks (*DPMs*)[21,22]

In place of the traditional random phase masks (RPMs), two masks (DPM1,DPM2) [21,22] are used in the present asymmetric cryptosystem. The DPMs are statistically-independent of each other. The masks are characterized by the value of *m* (= 2, 3, and 4 in the present case), where *m*, an integer, is the order of encryption. The DPMs are made up of number of sub-masks and are used as keys. Each subkey has a linear phase with random orientation and spatial frequency. With respect to *m*, the NSKs (Number of Subkeys) are written as,

$$NSK = (2^m \times 2^m) \tag{1}$$

To construct the DMKs, the input image is fragmented as per the NSK size. Each NSK is equal to sub-block of size *d* as given by Eq (2),

$$d = dim/2^m \tag{2}$$

where *dim* is the input image size. DPMs are generated as per the following relation

$$\text{DPM1} = \textstyle\sum_{i=1}^{2^m} \sum_{j=1}^{2^m} M_{i,j}\,(d \times d) \tag{3}$$

where $M_{i,j}$ represents the number of sub-blocks and is given by,

$$M_{i,j}\,(x \times y) = \exp[i2\pi\,(u_k.\, x + \upsilon_k \,.\, y)] \tag{4}$$

Here *k* is defined in the interval $[1, 2^m]$, u_k and υ_k are randomly generated in the interval [1, *d*], and *x* and *y* are defined in the interval [1, *dim*]. Representation of the DPM is shown in Fig 1. The DPMs for *m* = 2,3, and 4 are shown in Fig 2. Remaining details of the mask generation can be found in Zamrani *et al* **[**21**].**

2.2 Fractional Fourier Transform (*FrFT*)

The FrFT [23-27], an integral transform, is a generalization of the normal Fourier transform, and has many applications, for example in diffraction theory, digital signal and image processing, image hiding, phase retrieval, optical signal processing. and holography.

The FrFT of order α of a one-dimensional input function $f(x)$ is defined as,

$$F^{\alpha}\{f(x)\}(u) = \int_{-\infty}^{\infty} K_{\alpha}(x, u)\, f(x)\, dx \tag{5}$$

where the kernel function $K_{\alpha}(x, u)$ is expressed as,

$$\begin{cases} A \exp[i\pi(x^2 \cot\varphi - 2xu \csc\varphi + u^2 \cot\varphi)], & \alpha \neq n\pi; \\ \delta(x-u), & \alpha = 2n\pi; \\ \delta(x+u), & \alpha = (2n+1)\pi; \end{cases} \tag{6}$$

$$A = \frac{\exp\left[-i\left(\pi \dfrac{sgn\ \sin\varphi}{4} - \dfrac{\varphi}{2}\right)\right]}{\sqrt{|\sin\varphi|}} \tag{7}$$

Here *sgn* is the *signum* function and $\varphi = \alpha\pi/2$, where α denotes the order of the FrFT. A generalization for a two-dimensional function is straightforward.

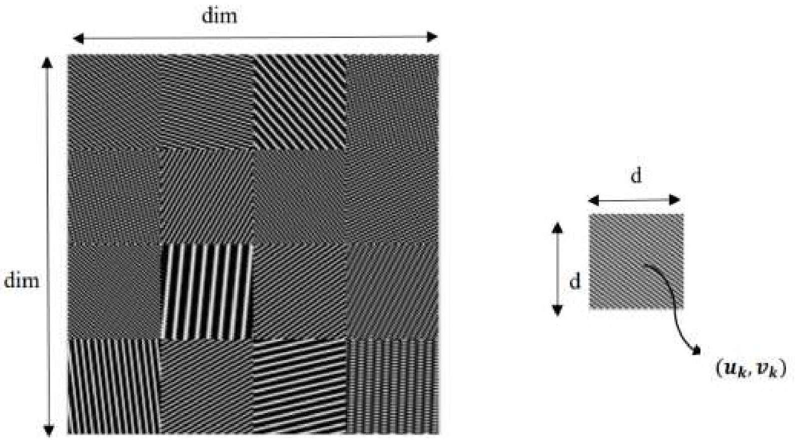


Fig 1. Construction of the Deterministic Phase Masks (DPMs)

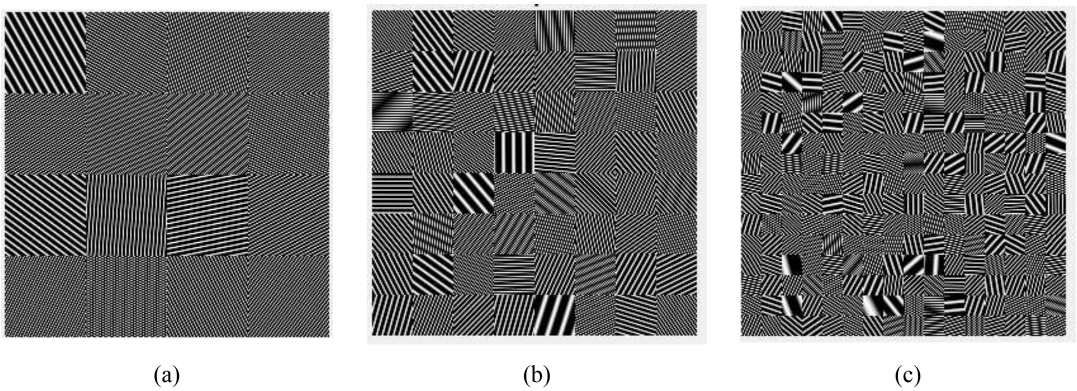


Fig 2. Deterministic phase masks (DPMs) for: (a) m=2, (b) m=3, and (c) m=4

3 Proposed asymmetric cryptosystem

3 1 Encryption and Encoding Process

The flow diagram of the encryption process (Fig 3) is explained in the following steps,

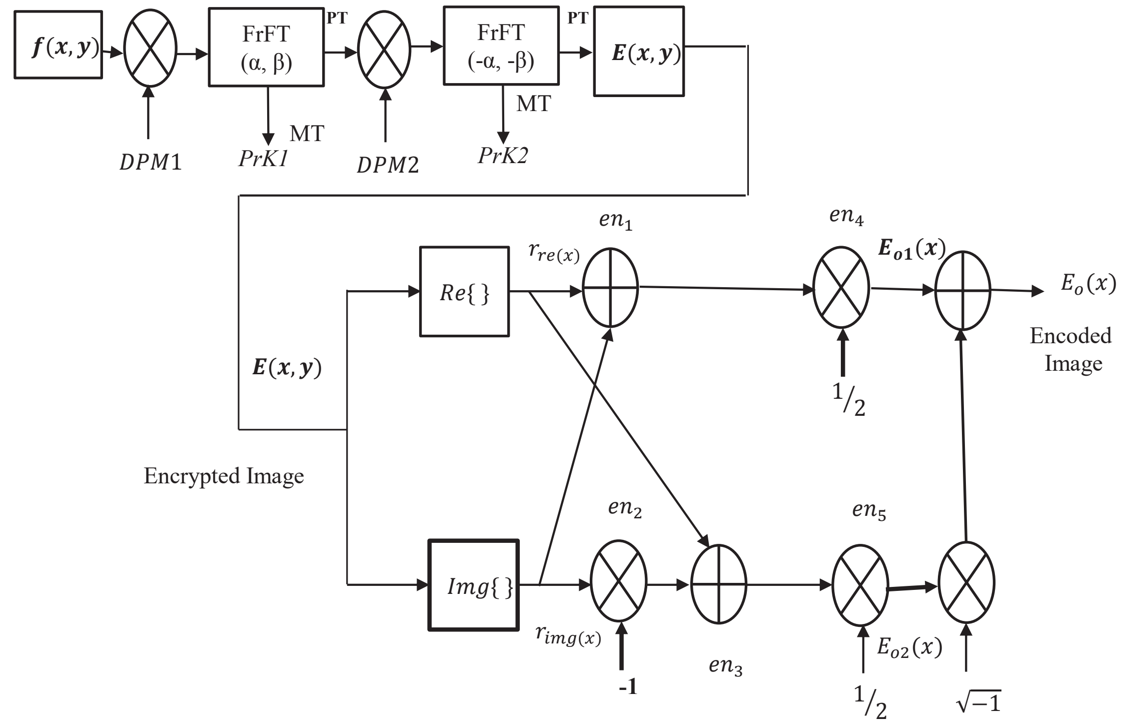


Fig 3. Flow diagram of the encryption process (upper part) and the encoding process (lower part): en_1, en_2, en_3, en_4, and en_5 are various stages of the encoding process; (Adapted from Lee and Cho Ref [28]).

Step 1. Let $f(x, y)$ be an input image which is multiplied by the first DPM1 and the product is transformed to the FrFT domain with orders (α, β).

Step 2: The transformed output is separated into two parts, as PT (Phase truncation) and MT (Magnitude truncation). The MT part serves as a private key (PrK1), whereas the PT part is multiplied with the second (DPM2) to obtain,

$$I(x, y) = [\{\mathrm{FrFT}(\alpha, \beta).\{f(x, y).\ \mathrm{DPM}_1(x, y)\}\}.\mathrm{DPM}_2\ (u, v)] \qquad (8)$$

Step 3: $I(x, y)$ is then transformed into the inverse FrFT domain and divided into two parts, MT and PT. Whereas the MT part serves as private key PrK2, the PT part is the encrypted image $E(x, y)$.

$$E(x, y) = \{\mathrm{FrFT}\ (-\alpha, -\beta).\ I(x, y)\} \qquad (9)$$

Step 4: To convert the encrypted image into an encoded image, $E(x, y)$ is put through an orthogonal encoder described by Lee and Cho [28]. For the orthogonal encoder, Hadamard matrix of order 2, represented by H_2, is given [29] by Eq (10),

$$H_2\, H_2^T = 2I_2 \qquad (10)$$

where $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, I_2 represents the 2×2 Identity matrix, and H^T is the transpose of H. From the encoded data, the real and imaginary parts of the encrypted data are encoded as

$$\begin{bmatrix} E_{01}(x) \\ E_{02}(x) \end{bmatrix} = \frac{1}{2} H_2 \begin{bmatrix} r_{re}(x) \\ r_{img}(x) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} r_{re}(x) \\ r_{img}(x) \end{bmatrix} = \begin{bmatrix} 1/2\ r_{re}(x) + r_{img}(x) \\ 1/2\ r_{re}(x) - r_{img}(x) \end{bmatrix} \tag{11}$$

where $r_{re}(x)$, $r_{img}(x)$ represent the real and imaginary parts of the encrypted data, $E_{01}(x)$, $E_{02}(x)$ denote the first and second encoded data, respectively, and 1/2 is multiplied for normalization.

Step 5: Then the complex-encoded data $E_0(x)$ is obtained from the real-valued encoded data $E_{01}(x)$ and $E_{02}(x)$.

$$E_0(x) = E_{01}(x) + E_{02}(x). \tag{12}$$

3.2 Decoding-, and Decryption Process

The procedure for decoding and decryption is given below in Fig 4.

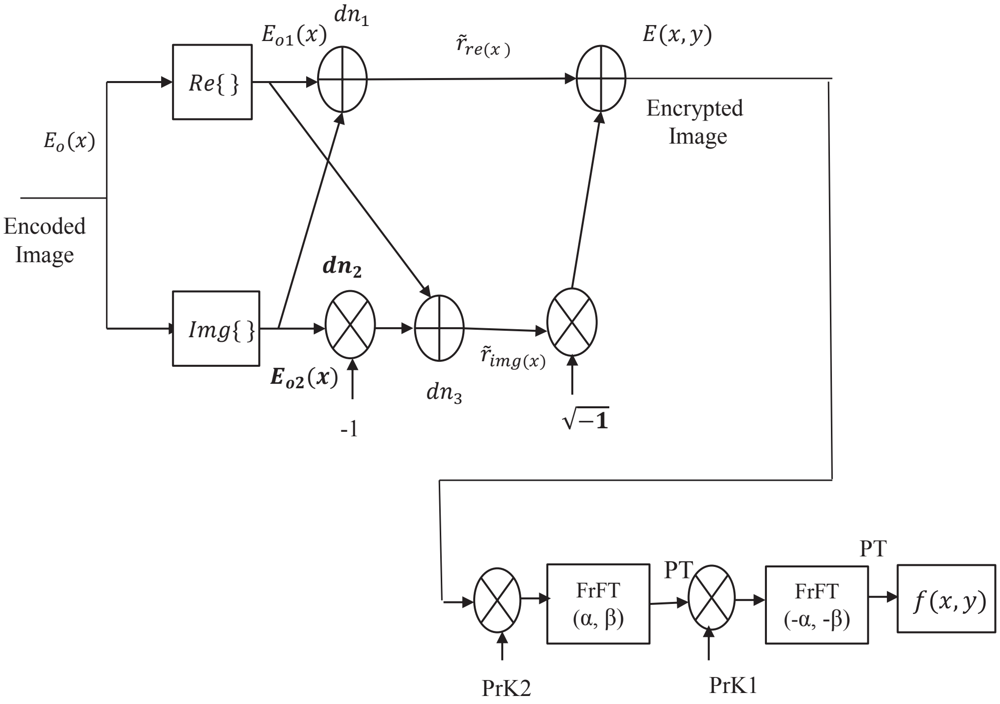


Fig 4. Flow diagram of the decoding (above left) and decryption (below right) processes; dn_1,dn_2, and dn_3 are the stages for the decoding process; (Adapted from Lee and Cho Ref [28]).

Step 1: In the decoder, the real and imaginary parts of $E_0(x)$, are decoded using the Hadamard matrix. The orthogonal decoding process is given below:

$$\begin{bmatrix} \tilde{r}_{re}(x) \\ \tilde{r}_{img}(x) \end{bmatrix} = H_2 \begin{bmatrix} E_{01}(x) \\ E_{02}(x) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} E_{01}(x) \\ E_{02}(x) \end{bmatrix} = \begin{bmatrix} E_{01}(x) + E_{02}(x) \\ E_{01}(x) - E_{02}(x) \end{bmatrix} \tag{13}$$

Step 2: After the decoding process as in upper portion of Fig 4, the decryption process starts with the cipher image which is multiplied by the secret key PrK2 and transformed into the FrFT domain with parameters (α, β). It is then multiplied by PrK1, as per Eq (14).

$$I(x,y) = [\mathrm{Fr\ FT}(\alpha,\beta)\{E(x,y) \times \mathrm{PrK2}\}] \times \mathrm{PrK1} \tag{14}$$

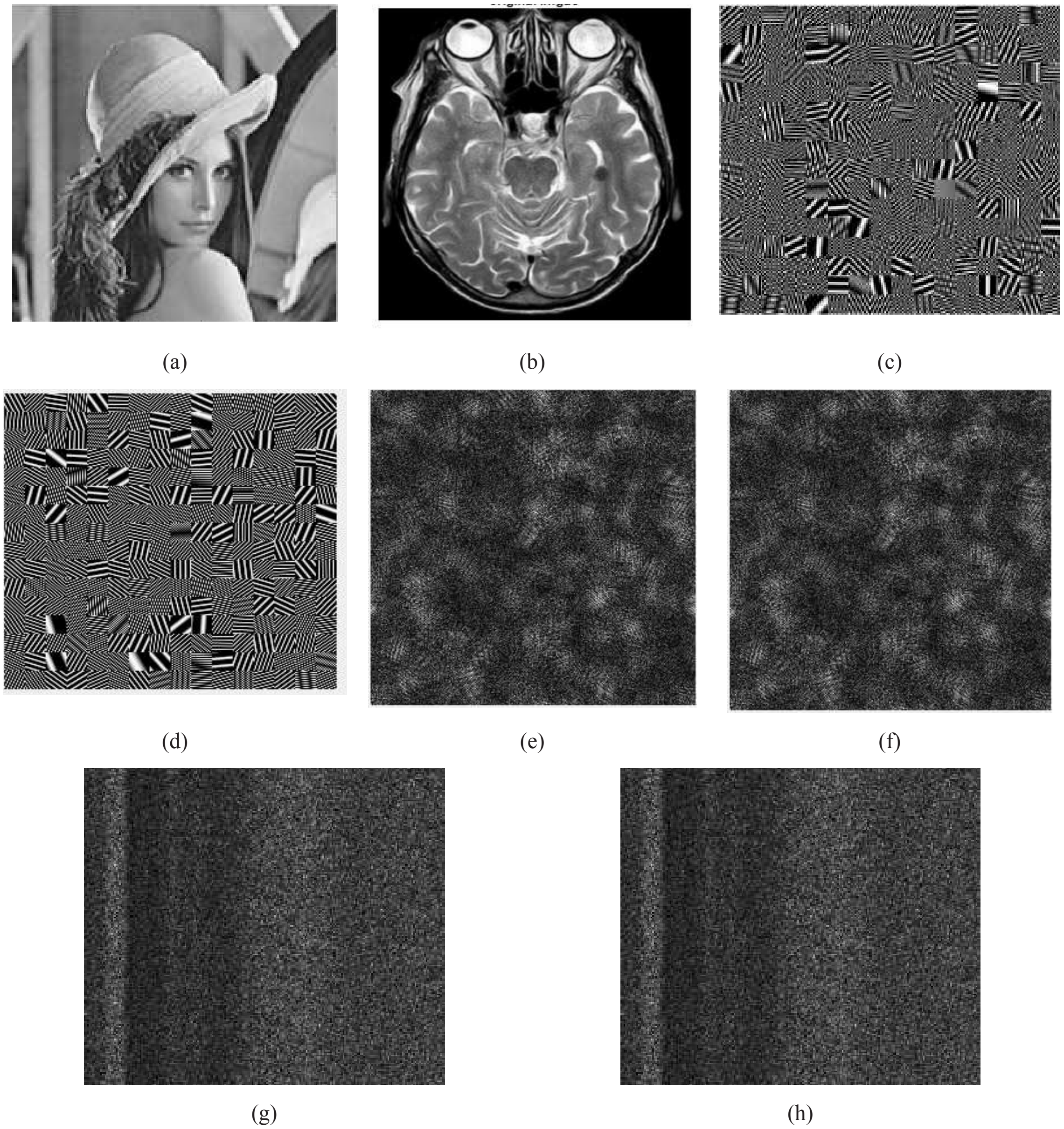
Step 3: The product received from step 2 of decryption process is transformed into inverse FrFT, to give.

$$f(x,y) = \{Fr\ FT(-\alpha, -\beta)\} \tag{15}$$

After Eq (15), the plain image is recovered back.

4 Simulation Results of the Cryptosystem

The proposed asymmetric cryptosystem with the use of orthogonal encoding and decoding, are tested by numerous simulations on the MATLAB R2014a. The encryption-, and decryption results are shown respectively in Figs 5 and 6. The input images (greyscale Lena image and MRI image of size 256×256) are the plain images as shown in Figs 5(a) and 5(b). The deterministic phase masks with encryption order of 4 are shown in Figs 5(c) and Figs 5(d). Encrypted images of Lena and MRI image are shown in Figs 5(e) and 5(f), respectively. The encoded images of Lena and MRI image are shown in Figs 5(g) and 5(h), respectively.



(a) (b) (c)

(d) (e) (f)

(g) (h)

Fig 5. Encryption process: (a) Plain image of Lena (256 × 256), (b) Plain image of MRI scan (256 × 256) (c) Deterministic masks m =4 (DPM1), (d) Deterministic masks m = 4 (DPM2), (e) Encrypted image of Lena, (f) Encrypted Image of MRI scan, (g) Encoded image of Lena input image, (h) Encoded image of MRI scan input image.

The proposed cryptosystem for the decryption process is represented in Fig (6). Figures 6(a) and 6(b) show the encoded images and Figs 6(c) and 6(d) show the encrypted images; Figs 6(e) and 6(f) show the recovered images of Lena and MRI scan image.

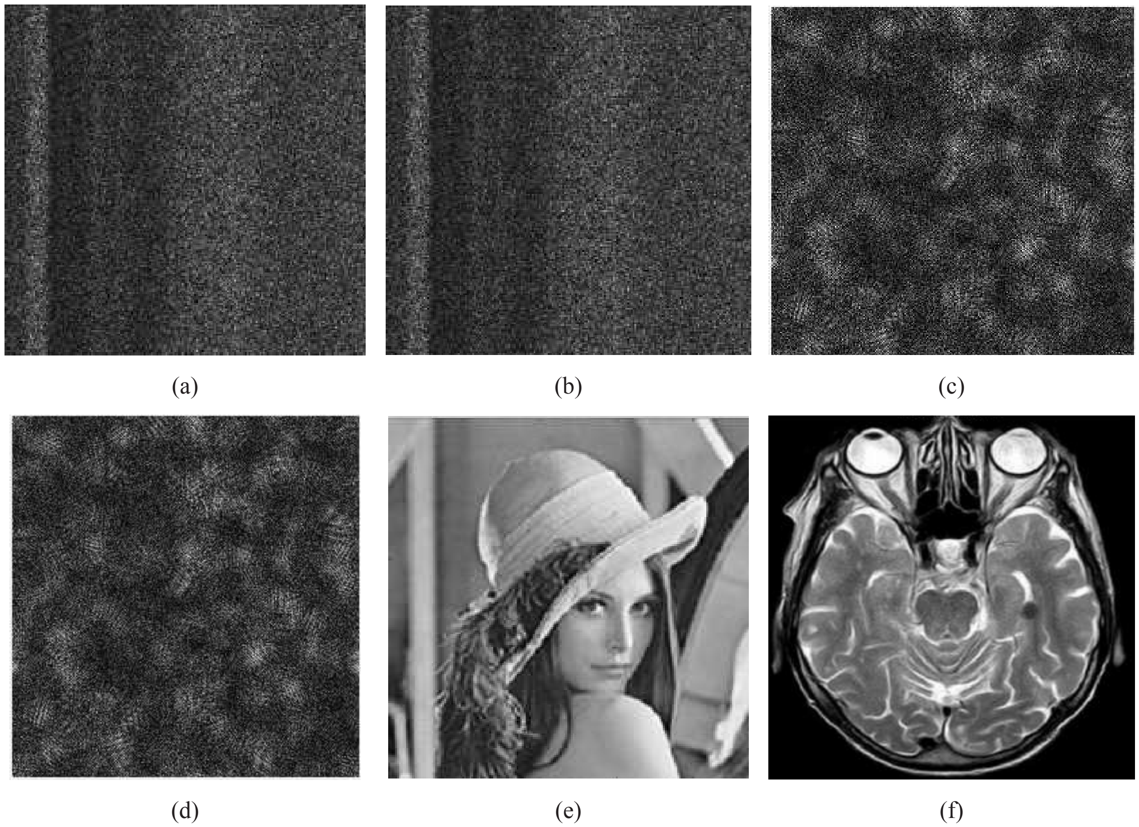


Fig 6. Decryption Process: (a) Encoded image of Lena, (b) Encoded image of MRI scan image, (c) Encrypted image of Lena, (d) Encrypted image of MRI scan, (e) Decrypted image of Lena, and (f) Decrypted image of MRI scan image.

5 Performance analysis

The quality of the decrypted image is checked by two parameters, (1) Mean-Square-Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE and PSNR are evaluated between the original-, and recovered images. The MSE is calculated by Eq (16) as given below,

$$MSE = \frac{1}{N \times M} \sum_{i=1}^{M} \sum_{i=1}^{N} | f(x, y) - f^{'}(x, y)|^2 \tag{16}$$

where $M \times N$ is the number of pixels of the original image. Smaller MSE value indicates the high similarities between the original and decrypted images. The MSE values are plotted for the correct fractional order ($\alpha = \beta = 0.5$) and other values in the interval (0.1 to 1.0) in Fig 7. The PSNR is calculated between the original-, and the decrypted images by Eq (17). Good quality of the image is characterized by a high PSNR value. Table 1 represents the MSE and PSNR values.

$$PSNR = 10\ log_{10}\left(\frac{255^2}{\sqrt{MSE}}\right) \tag{17}$$

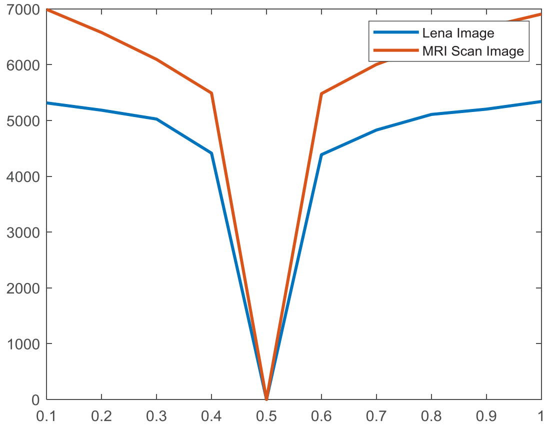
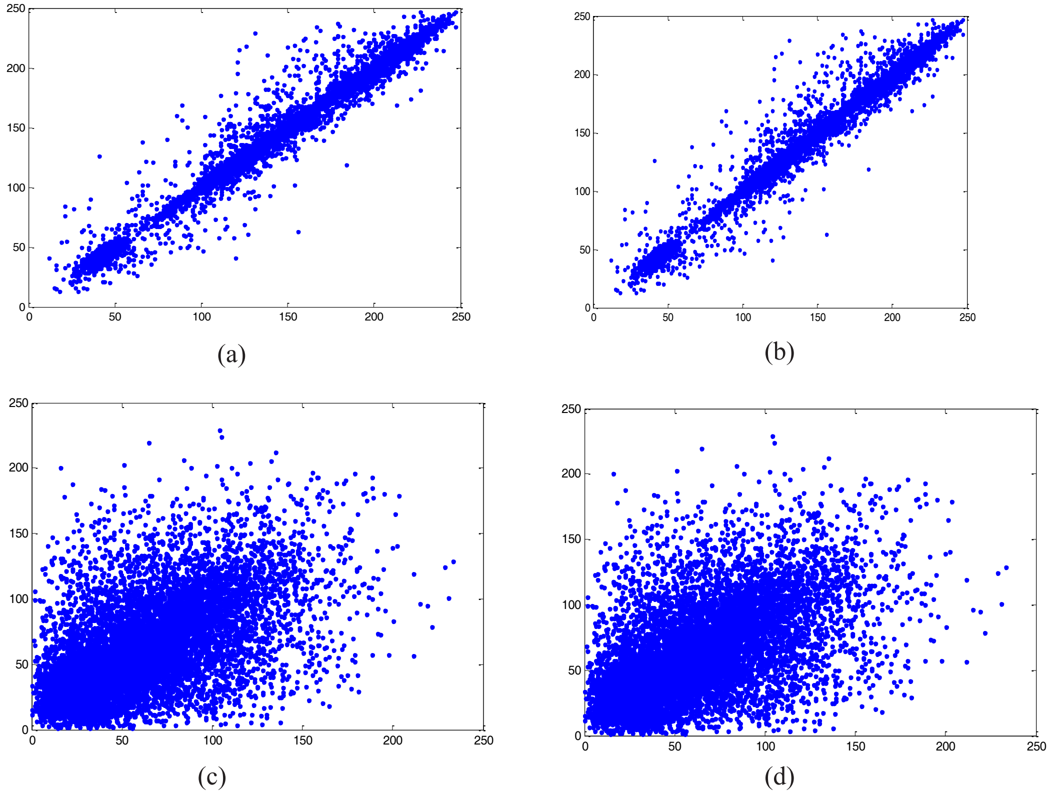


Fig 7. MSE plot of input images (Lena, MRI scan) with the fractional orders of the FrFT.

Table 1. MSE and PSNR values of the images

Parameters	Values (Plain Image Lena)	Values (Plain Image- MRI image)
Mean-Square-Error	1.983×10^{-29}	2.23×10^{-27}
Peak Signal-to-Noise Ratio	267.75 dB	234.23dB



(a)

(b)

(c)

(d)

Fig 8. Scatter plots (a, b) for the input image Lena and MRI scan image, respectively; CC analysis (c, d) for the input and encoded Lena image, input and encoded MRI scan image, respectively.

(ii) Correlation Coefficient (CC) analysis

The CC analysis is conducted by choosing hundred thousand pairs which are randomly picked horizontally, vertically, and diagonally neighbouring pixels between the input image and the encrypted images. The CC has been calculated by the following relation,

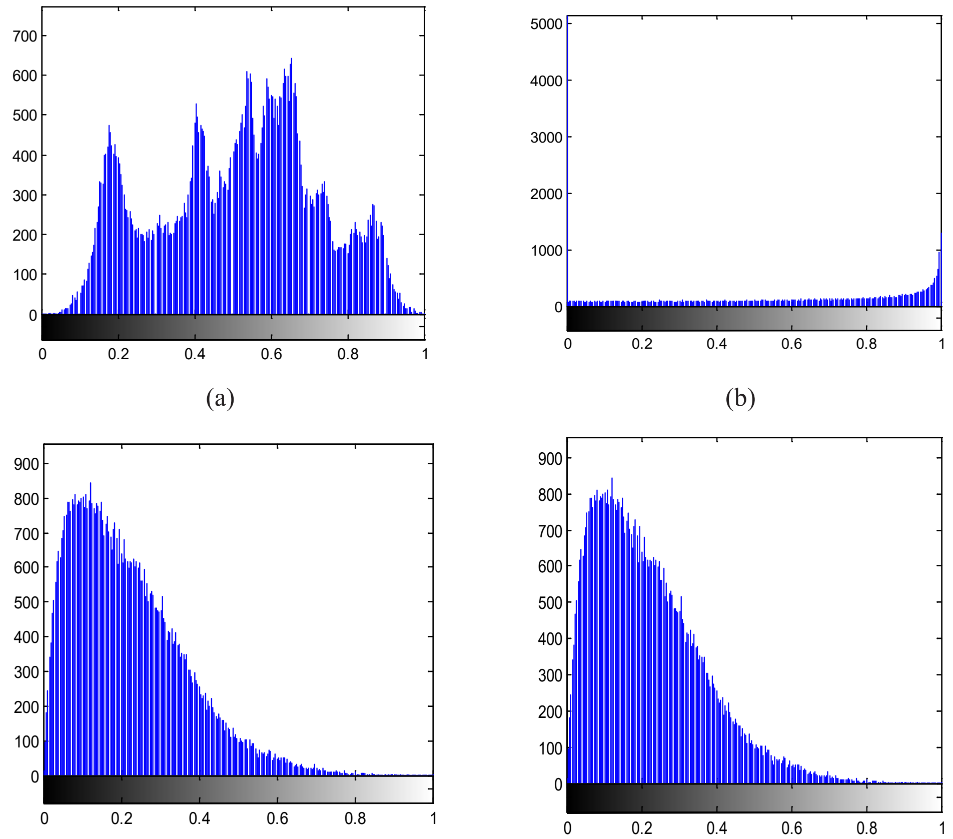
$$CC = \frac{\sum_{i=1}^{N}(x_i - \bar{x})\ (y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2}\ \sum_{i=1}^{N}(y_i - \bar{y})^2} \tag{18}$$

where $\bar{x} = \sum_{i=1}^{N} x_i$ and $\bar{y} = \sum_{i=1}^{N} y_i$ are the mean values of x_i and y_i.

From the CC analysis, it is very difficult to find the information. Scatter plots distribution for CC analysis are shown in Figs 8(a) and 8(b) for the input images of Lena and MRI scan. Figures 8 (c) and 8(d) are the results of CC analysis between the corresponding input-, and encoded images, respectively.

(iii) *Histogram Analysis*

A histogram is an illustration of spreading of the numerical data. This analysis is a noteworthy structure in image authorization. Histogram analysis has been carried out for the input image, deterministic masks, encrypted images, and encoded images. Figure 8 represents the results. Figures 9(a) and 9(b) show the histogram of plain image (Lena) and deterministic masks, respectively. Figures 9(c) and 9(d) show the encrypted-, and encoded images. Figure 9 (e) shows the decrypted image.

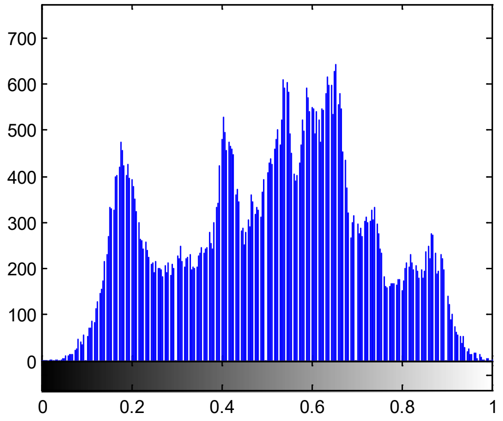


(a)

(b)

(c)

(d)

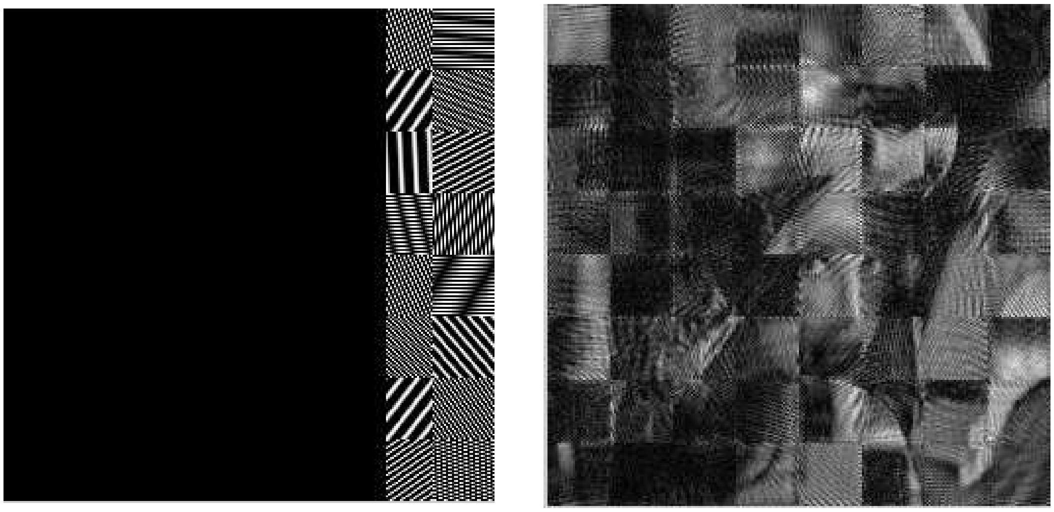


(e)

Fig 9. Histogram analysis of: (a) input image, (b) deterministic mask, (c) encrypted image, (d) encoded image, and (e) decrypted image.

a. Occlusion Analysis

In order to validate the robustness of the cryptosystem, occlusion analysis has been carried out for the mask. In this analysis, certain portions of the mask are hidden, and the corresponding result has been examined. It is seen that the decrypted image is not clear and is degraded considerably. Figure 10 shows the results of occlusion analysis. Figure 10(a) shows the 75% hidden portion in the mask, and the corresponding decrypted image is shown in Fig 10(b). It can be seen that a small trace of the input image can still be seen.



(a) (b)

Fig 10. Tolerance to occlusion attack (a) mask with 75% occlusion (b) Decrypted image of (a)

b Entropy Analysis

Entropy expresses the uncertainty of the information in the encrypted image. It is very difficult for an attacker to recover the original image if the value of entropy is very high. The entropy for a source *m* is calculated using the following equation:

$$H(m) = -\sum_{i=1}^{M} P(mi)\log_2 P(mi) \tag{19}$$

where $P(mi)$ represents the probability of source. The ideal value of the entropy for an encrypted image is 8. For the proposed asymmetric cryptosystem, the obtained entropy values are 7.06 for the Lena image, and 6.99 for the MRI scan image. The obtained values clearly indicate that they are very near to the ideal value. It proves that the proposed cryptosystem which uses orthogonal encoding produces better randomness.

c Sensitivity Analysis

The proposed cryptosystem based on the orthogonal encoding and decoding does not work for the incorrect fractional orders. If an attacker gets hold of any image, unless the fractional orders are known correctly, the input image may not be recovered. The correct fractional orders of the FrFT are $\alpha = 0.5$ and $\beta = 0.5$. From the analysis (Fig 7), it is clearly observed that our proposed system is highly sensitive to very small deviations from the correct fractional orders.

8 Conclusions and Some Remarks

This paper proposes the asymmetric cryptosystem with the use of deterministic masks (DMKs) in DRPE based upon orthogonal encoding and decoding using Fractional Fourier transform (FrFT). Orthogonal encoder uses very easy linear operations with small complications. All the simulation results shown in this paper prove that orthogonal encoding and decoding is an influential encryption effect. Hence, the proposed orthogonal encoding technique can be used as a low-complexity and effective encryption technique for images. Some more papers [30-36] on cryptography may also be noted.

We may add that the advances in the area of artificial intelligence also provide tools for the design of systems with enhanced security, but also suggest that the classical cryptographic methods are highly vulnerable to the tools of deep learning etc [37-42]. Another promising area of investigations that has emerged recently, is the marriage of metamaterial research and optical cryptography [43-46], providing avenues for designing and fabrication miniaturized optical cryptographic systems.

References

1. Schneir B, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed. John Wiley Hoboken, NJ USA, 1996)
2. Stallings W, Cryptography and Network Security: Principles and Practice, 2nd edn, (Prentice Hall, Hoboken NJ USA), 2000.
3. Singh K, Unnikrishnana G, Nishchal N K, Photorefractive Processing for Data Security, Proc SPIE Vol 4803, pp 205-219, in 'Photorefractive Fibers and Crystal Devices: Materials, Optical Properties, and Applications VII' (SPIE Press Bellingham WA, USA), 2002.
4. Javidi B (Ed), Optical and Digital Techniques for Information Security, (Springer Berlin), 2005.
5. Naughton T J, Sheridan J T, Optics in Information Systems, SPIE Int'l Techn Group Newsletter, 16(2005)1–12.
6. Singh K, John R, Joseph J, Encrypted holographic memories for information security, *Bull Laser Spectrosc Soc, India*, 15(2005-6)1–19.
7. Matoba O, Nomura T, Perez-Cabre E, Millan M S, Javidi B, Optical techniques for information security, *Proc IEEE*, 97(2009)1128–1148.
8. Al Falou A, Brosseau C, Optical image compression and encryption methods, *Adv Opt Photon*, 1(2009)589–636.
9. Kumar A, Singh M, Singh K, Speckle coding for optical and digital data security applications, In Advances in Speckle Metrology and Related Techniques, Chap 6, pp 239–299, (Ed) Kaufmann G, (Wiley-VCH Weinheim, Germany), 2011.
10. Liu S, Guo C, Sheridan J T. A review of optical image encryption techniques, *Opt Laser Technol*, 57(2014)327–342.
11. Chen W, Javidi B, Chen X, Advances in optical security systems, *Adv Opt Photon*, 6(2014)120–155.

12. Yadav A K, Vashisth S, Singh H, Singh K, Optical cryptography and watermarking using some fractional canonical transforms and structured masks, in Advances in Optical Science and Engineering, Lakshminarayanan V, Bhattacharya I, (Eds), Chap 5, pp 25–36, Springer Proceedings in Physics 166, (Springer India), 2015,
13. Al Falou A, Situ G, Peng X, He W, Rastogi P, 3DIM-DS 2015: Optical image processing in the context of 3D imaging, metrology, and data security, *Opt Lasers Eng*, 89(2015)1–202 (Special issue).
14. Kumar P, Joseph J, Singh K, Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures. In: Healy J, Kutay A, Ozaktas M, Sheridan J (eds), Linear Canonical Transforms. Springer Series in Optical Sciences, 198, (Springer New York), 2016, pp. 367–396.
15. Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M S, Nishchal N K, Torroba R, Barrera J F, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan J T, Situ G, Naruse M, Matsumoto T, Juvells I, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse Pepijn W H, Mosk A P, Markman A, Roadmap on optical security, *J Opt* (IOP), 18(2016)1–39.
16. Singh K, Photorefractive optical cryptography: a personal tour, In Advances in Optical Science and Engineering' Springer Proceedings in Physics194, (Eds) Bhattacharya I, Chakrabarti S, Reehal H S, Lakshminarayanan, (Springer Nature Singapore Pvt Ltd), 2017.
17. Al Falou A (Ed), Advanced Secure Optical Image Processing for Communications, (IOP Publ, Bristol, U K), 2018.
18. Singh P, Yadav A K, Vashisth S, Singh K, Review of optical image encryption schemes based on fractional Hartley transform, *Asian J Phys*, 28(2019)701–716.
19. Nishchal N K, Optical Cryptosystems, IOP Publishing, (Bristol, UK), 2019,
20. Muniraj I, Sheridan J T, Optical Encryption and Decryption, (SPIE Press Bellingham WA USA), 2019.
21. Zamrani W, Ahouzi E, Lizana A, Campos J, Yzuel M J: Optical image encryption technique based on deterministic phase masks, *Opt Eng*, 55(2016); doi.org/10.1117/1.OE.55.10.103108.
22. Girija R, Singh H, A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition, *Opt Quant Electron*, 50, 210 (2018); doi: 10.1007/s11082-018-1472-6.
23. Garcia J, Mas D, Dorsch R G, Fractional-Fourier-transform calculation through the fast-Fourier-transform algorithm, *Appl Opt*, 35(1996)7013–7018.
24. Ozaktas H M, Zalevsky Z, Kutay M A, The Fractional Fourier Transform with Applications in Optics and Signal Processing, (Wiley Chechester), 2001.
25. Unnikrishnan G, Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt Lett*, 25(2000)887–889.
26. Hennelly B M, Sheridan J T, Image encryption and the fractional Fourier transform, *Optik*, 114(2003)251–265.
27. Zhou N, Dong T, Wu J, Novel image encryption algorithm based on multiple-parameter discrete fractional random transform, *Opt Commun*, 283(2010)3037–3042.
28. Lee I, Cho M, Double random phase encryption based orthogonal encoding technique for color images, *J Opt Soc Korea*, 18(2014)129–133.
29. Sylvester J J, Thoughts on orthogonal matrices, simultaneous sign successions, and tessalated pavements in two or more colours, with applications to Newton's rule, ornamental tile work, and the theory of numbers, *Phil Mag*, 34(1867)461–475.
30. Girija R, Singh H, Triple-level cryptosystem using deterministic masks and modified Gerchberg-Saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition, *Optik*, 187(2019)238–257.
31. Girija R, Singh H, Abirami G, Cryptanalysis of DRPE using complex S-Box based on linear canonical transform, *Multimed Tools Appl*, 82(2023)12151–12166.
32. Girija R, Singh H, Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform, *3D Res*, 9(2018); doi.org/10.1007/s13319-018-0192-9.
33. Girija R, Singh H, An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain, *Multimed Tools Appl*, 79(2020)34717–34735.
34. Girija, R, Singh, H, Abirami, G. Optical medical image encryption based on digital hologram in various domains. *J Opt*, (2023), doi.org/10.1007/s12596-023-01186-x.

35. Mandapati V C, Vardhan H, Prabhakar S, Sakshi, Kumar R, Reddy S G, Singh R P, Singh K, Multi-user nonlinear optical cryptosystem based on polar decomposition and fractional vortex speckle patterns, *Photonics*, 10(2023) 561; doi.org/10.3390/photonics10050561.
36. Sachin, Singh P, Singh K, Nonlinear image authentication algorithm based on double fractional Mellin domain, *Nonlinear Dyn*, 111(2023)13579–13600.
37. Wu H, Li Q, Meng X, Yang X, Liu S, Yin Y, Cryptographic analysis on an optical random-phase-encoding cryptosystem for complex targets based on physics-informed learning, *Opt Express*, 29(2021)33558–33571.
38. Yi F, Jeong O, Moon I, Privacy-preserving image classification with deep learning and double random phase encoding, *IEEE Access*, 9(2021)136126–136134.
39. Panchikkil S, Manikandan S V M, Zhang Y, A convolutional neural network model based reversible data hiding scheme in encrypted images with block-wise Arnold transform, *Optik*, 250(2022)168137; doi.org/10.1016/j.ijleo.2021.168137.
40. Zhu A, Lin S, Wang X, Optical color ghost cryptography and steganography based on multi-discriminator generative adversarial network, *Opt Commun*, 512(2022)128032; doi.org/10.1016/j.optcom.2022.128032.
41. Ahmadi K, Carnicer A, Optical visual encryption using focused beams and convolutional neural networks, *Opt Lasers Eng*, 161(2023)107321; doi.org/10.1016/j.optlaseng.2022.107321.
42. Annadurai C, Nelson I, Nirmala Devi K, Manikandan R, Gandomi A H, Image watermarking-based data hiding by discrete wavelet transform quantization model with convolutional generative adversarial architectures, *Appl Sci*, 13(2023)804; doi.org/10.3390/app13020804.
43. Ouyang M, Yu H, Pan D, Wan L, Zhang C, Gao S, Feng T, Li Z, Optical encryption in spatial frequencies of light fields with metasurfaces, *Optica*, 9(2022)1022–1028.
44. Gao X, Li P, Zhong J, Wen D, Wei B, Liu S, Qi S, Zhao J, Stokes meta-hologram toward optical cryptography, *Nature Commun*, 13, Art ID:6687(2022); doi.org/10.1038/s41467-022-34542-9.
45. Ullah N, Zhao R, Huang L, Recent advancement in optical metasurface: Fundamental to application, *Micromachines*, 13(2022) Art ID:1025; doi.org/10.3390/mi13071025.
46. Zhang F, Guo Y, Pu M, Chen L, Xu M, Liao M, Li L, Li X, Ma X, Luo X, Meta-optics empowered vector visual cryptography for high security and rapid decryption, *Nature Commun*,14, 1946 (2023); doi.org/10.1038/s41467-023-37510-z.

[*Received*: 01.08.2023; *accepted*: 15.08.2023]

R Girija is an Associate Professor in Computer Science and Engineering in School of Engineering & Technology, Manav Rachna International Institute of Research & Studies, Faridabad (Haryana), India. She received Bachelor’s degree from Anna University, India and Master’s degree obtained her doctorate degree on the topic "Development of Optical image encryption techniques with the construction of different phase masks in canonical transforms” from The North Cap University, Gurugram, India. She got stipend from Information Security Education Awareness (ISEA), Ministry of DIT, India for carrying out her research work. She is member of OSA. Her research interests include medical image encryption and decryption systems, DRPE, Optical image processing. She has published a number of papers in high impact factor journals.

Dr Hukum Singh is currently Professor & Head Department of Applied Sciences, The NorthCap University, Gurugram, India. He obtained Ph D degree from Govind Ballabh Pant University of Agriculture and Technology, Pantnagar, India, in 2003. He has published 84 papers in reputed journals and as well presented 75 papers in national, international conferences and workshops. His name figure out in top 2% world's researcher by Standford University, Scopus data 2022.

Dr Singh has supervised 07 Ph D students and a number of students are working for their Ph D degree under his supervison. He is recipient of Prestigious Deokaran Award for "Glass"- 2018 by the Indian Ceramic Society, CSIR (CGCRI). Under best faculty award, Dr Singh was awarded best researcher award in the academic year 2021-22 by The NorthCap University, Gurugram, India. He is faculty adviser of The NorthCap University OPTICA student Chapter. He is Co-PI and Mentor of DRDO and DST research funded projects. He is senior member of The Optical Society (OPTICA), and The Optical Society of India (OSI). He is Associate Editor of IET Image Processing Journal and a Reviewer of Asian J Phys.