Optica Applicata, Vol. LIII, No. 4, 2023
DOI: 10.37190/oa230407

Asymmetric cryptosystem with random decomposition using fractional Fourier and Fourier transforms

KAPIL SHANKAR GAUR*, HUKUM SINGH, SEEMA THAKRAN

Department of Applied Sciences, The NorthCap University, Gurugram, India

*Corresponding author: kapilshankar09@gmail.com

In this paper, an asymmetric cryptosystem based on random decomposition is proposed. The suggested scheme used three different decryption keys to get decrypted image, two of which are generated using phase truncation and one through random decomposition. The combination of these keys and fractional Fourier transform parameter increase the security of cryptosystem against various attacks. MATLAB simulations are used to validate the scheme's conclusions. The effectiveness of a scheme is validated by the key sensitivity performance of the cryptosystem. This research also includes a 3D plot for both grayscale and binary images. Correlation coefficient (CC) values between the original and recovered images is also calculated to validate the cryptosystem.

Keywords: fractional Fourier transform (FrFT), random phase mask (RPM), random decomposition (RD).

1. Introduction

With the arrival of the 21st century, the majority of human population require daily internet access. Due to this, security is a major concern for military reports, internet banking information, and personal passwords. For this reason, it is vital to develop a strong encryption algorithms which are fast and secure from unauthorized attacks. There are numerous encryption methods are available but due to the intricacy of these methods, optical encryption methods came into existence. Optoelectronic-based optical cryptosystems decrypt images with a high degree of accuracy and at a faster rate. Due to parallel processing and its high-speed encryption, the field of optical encryption is expanding at a rapid rate. REFREGIER and JAVIDI [1] present the double random phase encoding (DRPE) approach for encrypting images. DRPE is executed using the 4*f* system and two RPMs. RPM1 used in image encryption lies in the spatial domain, while the second RPM operates in the frequency domain. DRPE is applied both optically and digitally, and due to its wide range of applications in areas such as information concealment, watermarking, and encryption algorithms, it has been enhanced with additional transforms such as Fresnel transform [2,3], fractional Fourier transform [4], fractional Mellin transform [5], Hartley transform [6]. The aforementioned cryptosystems are based on symmetric key cryptosystems, in which encryption and decryption keys are identical. By knowing the vulnerability of symmetric DRPE to KPA [7], CPA [8] and CCA [9], QIN and PEN [10] presented the concept of asymmetric DRPE. In optical

cryptosystems based on asymmetric DRPE, the encryption and decryption keys are not identical. In asymmetric scheme with the knowledge of only encryption key, it is challenging to retrieve the image. Therefore, other asymmetric schemes [11-26] were also proposed. The issue of optical axis alignment affects the traditional DRPE method. In certain experiments, a structured phase mask [27-31] has been utilized in place of RPM to address the issue of axis alignment and to increase the key space for better security.

In optical cryptosystem, WANG *et al*. [32] proposed the cryptosytem based on random decomposition which has an edge over equal modulus decomposition (EMD) due to EMD's susceptibility to attacks. In RD-based cryptosystems, masks are not in equal modulus, which prevents the transmission of private key information. By understanding the significance of RD, afterwards numerous cryptosystems based on RD [33-35] are performed. In the presented work, we have proposed an asymmetric cryptosystem using random decomposition in Fourier and fractional Fourier transforms. The paper is divided into four subsections naming theoretical background, proposed cryptosystem, simulation results and conclusion.

2. Theoretical background

2.1. Fractional Fourier transform

Consider a function $f(x)$, then the fractional Fourier transform (FrFT) of $f(x)$ with respect to order α of the FrFT [4, 15] can be calculated as

$$G^{\alpha}(u) = F^{\alpha}\{f(x)\} = \int_{-\infty}^{+\infty} f(x) K_{\alpha}(x, u)\,\mathrm{d}x \tag{1}$$

$$K_{\alpha}(x, u) = \frac{\exp\left\{ i\left[\frac{\pi}{4}\operatorname{sgn}(\varphi) - \frac{\varphi}{2}\right]\right\}}{\sqrt{|\sin(\varphi)|}} \exp\left\{ i\pi\left[(u^2 + x^2)\cot(\varphi) - 2ux\csc(\varphi)\right]\right\} \tag{2}$$

where $K_{\alpha}(x, u)$ is the kernel of the FrFT, sgn represent signum function and $\varphi = \alpha\pi/2$ denote the angle corresponding to fractional Fourier order α. Simply replacing the negative fractional angle ($-\alpha$) with a positive one (α) allows us to calculate the inverse of FrFT.

2.2. Random decomposition

In RD [32-35] a complex valued function $f(\mu, \gamma)$ can be decomposed into two complex functions $f_1(\mu, \gamma)$ and $f_2(\mu, \gamma)$ such that

$$f_1(\mu, \gamma) = \frac{U_1(\mu, \gamma)\sin\left[b_1(\mu, \gamma)\right]}{\sin\left[a_1(\mu, \gamma) + b_1(\mu, \gamma)\right]} \exp\left\{-i\left[a_1(\mu, \gamma) - \varphi_1(\mu, \gamma)\right]\right\} \tag{3}$$

$$f_2(\mu,\gamma) = \frac{U_1(\mu,\gamma)\sin\left[a_1(\mu,\gamma)\right]}{\sin\left[a_1(\mu,\gamma)+b_1(\mu,\gamma)\right]}\exp\left\{-i\left[b_1(\mu,\gamma)-\varphi_1(\mu,\gamma)\right]\right\} \tag{4}$$

where, $a_1(\mu,\gamma) = 2\pi\,\mathrm{rand}(\mu,\gamma)$, $b_1(\mu,\gamma) = 2\pi\,\mathrm{rand}(\mu,\gamma)$, $U_1 = \mathrm{abs}(f(\mu,\gamma))$ and $\varphi_1 = \mathrm{angle}(f(\mu,\gamma))$.

In this cryptosystem, we used first complex function of RD as a private key.

3. Proposed cryptosystem

Flowchart for the enciphering of image for the proposed cryptosystem is presented in Fig. 1(a). In the presented scheme, the input image $I(x, y)$ is first bonded with RPM1 then FrFT of the order (p, q) is applied. Random decomposition operation is performed on resultant image which divides the image into two-parts P_1 and P_2. Obtained value of P_1 represents the first key of the cryptosystem say Key1. The phase-truncated (PT) part of P_2 provide the intermediate image $G(u, v)$ while amplitude-truncated (AT) preserves as Key2 of the cryptosystem.

$$P_2(u,v) = \mathrm{RD}\left[\mathrm{FrFT}(p,q)(I\times\mathrm{RPM1})\right] \tag{5}$$

$$G(u,v) = \mathrm{PT}\left[P_2(u,v)\right] \tag{6}$$

$$\mathrm{Key2} = \mathrm{AT}\left[P_2(u,v)\right] \tag{7}$$

The intermediate image is multiplied by RPM2 in the frequency domain. Then obtained complex image is subjected to FFT, and PT part of resultant image give the

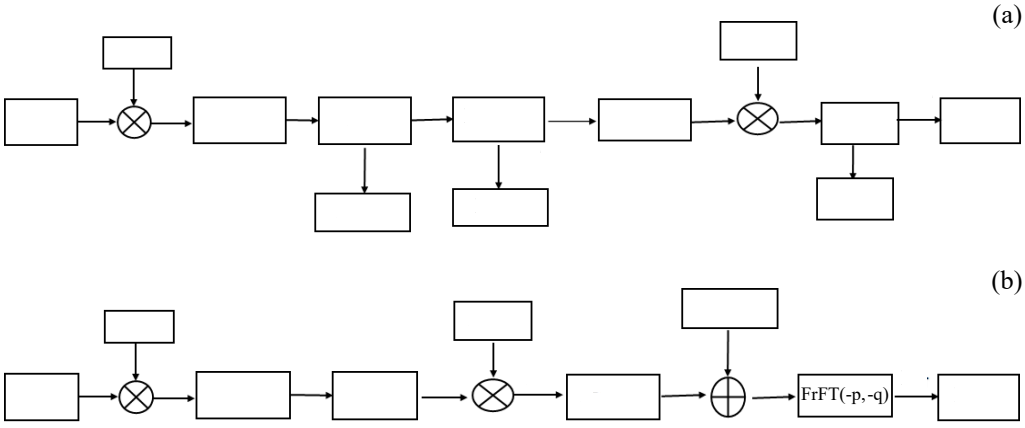

Fig. 1. Flow chart of (a) encryption process, and (b) decryption process.

encrypted result and AT part behaves as the third key of the scheme (Key3). Mathematically, the enciphering process can be represented as follows:

$$E(x, y) = \left\{ \mathrm{PT}\left[\mathrm{FFT}\left(G(u, v) \times \mathrm{RPM2} \right) \right] \right\} \tag{8}$$

$$\mathrm{Key3} = \left\{ \mathrm{AT}\left[\mathrm{FFT}\left(G(u, v) \times \mathrm{RPM2} \right) \right] \right\} \tag{9}$$

For the decryption of image, we follow the steps which are mentioned in the flow chart of Fig. 1(b). The encrypted image is first multiplied by Key3 and after that inverse Fourier transform (IFFT) is applied on it. By performing PT on obtained result, we get the intermediate image.

$$G(u, v) = \mathrm{PT}\left[\mathrm{IFFT}\left(E(x, y) \times \mathrm{Key3} \right) \right] \tag{10}$$

The intermediate image is first multiplied by Key2 followed by PT operation to obtain P_2 then Key1 is added to it. Finally, the decrypted image is obtained by performing FrFT with order $(-p, -q)$. The results for the above cryptosystem for the gray-scale and binary images are shown in Fig. 2.

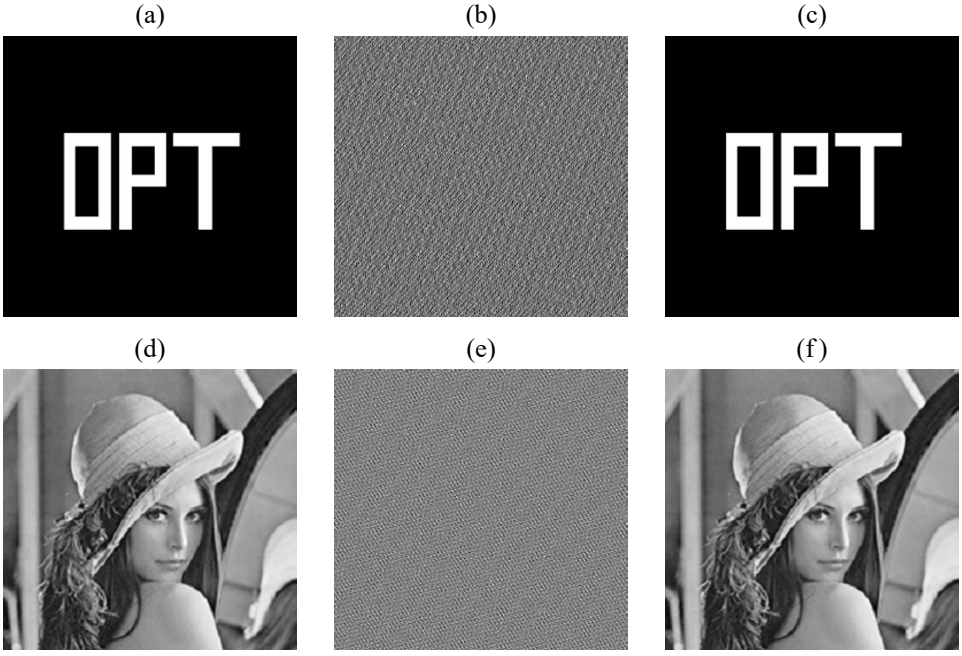

Fig. 2. (a) Binary original image; (b) binary encrypted image; (c) binary decrypted image; (d) *Lena* image; (e) *Lena* encrypted image; (f) *Lena* recovered image.

Mathematical expression for decryption is given by

$$P_2(u, v) = \mathrm{PT}\left[G(u, v) \times \mathrm{Key2}\right] \tag{11}$$

$$D(x, y) = \mathrm{PT}\left\{\mathrm{FrFT}(-p, -q)\left[P_2(u, v) + P_1(u, v)\right]\right\} \tag{12}$$

4. Simulation results

For validating our proposed scheme, we used binary and *Lena* image of size 256×256 pixel. The FrFT orders that are used in this scheme are $p = 0.35$ and $q = 0.6$. To check the reliability of proposed cryptosystem MSE and PSNR have been evaluated.

$$\mathrm{MSE} = \sum_{k=1}^{u} \sum_{k=1}^{v} \frac{\left|I_o(x, y) - I_d(x, y)\right|^2}{u \times v} \tag{13}$$

$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{14}$$

where $u \times v$ are the numbers of pixel of images while $I_o(x, y)$ and $I_d(x, y)$ represents the encrypted and decrypted image, respectively. For our scheme, the value of PSNR for *Lena* image is 216.12 dB and for binary is 228.79 dB which reflects the good quality of recover image, and calculated values of MSE between the original image and reconstructed image are 1.33×10^{-22} and 1.31×10^{-23}, respectively. The plot of MSE and CC with fractional order are depicted in Fig. 3.

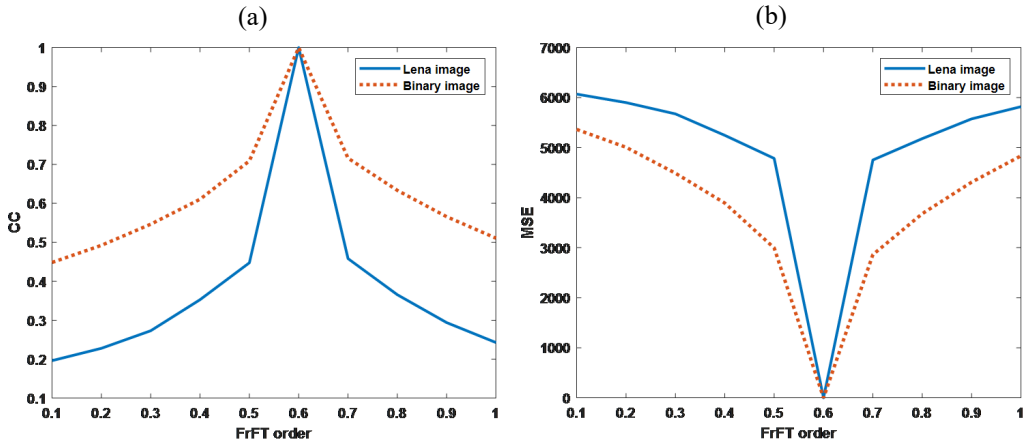

Fig. 3. (a) CC *vs*. fractional order plot; (b) MSE *vs*. fractional order plot.

Correlation coefficient (CC) between the input image and the deciphered image is evaluated using the following formula:

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{15}$$

where,

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

and N represents the number of pair of (x_i, y_i) and x_i, y_i are the values for the two adjacent pixels.

The ideal value of CC between encrypted and decrypted image is 1. In our proposed cryptosystem, the values of CC for both images are 1. For a strong cryptosystem, the CC between two adjacent pixel of cipher image pixel should be less than the plain text image.

The 16000 random pixels are used for the simulation results of CC in the horizontal, vertical, and diagonal directions.Their values are displayed in Table 1. The simulation results demonstrate that the CC value of the original image is greater than that of the encrypted image in every direction. Figure 4 shows the plots of the original and cipher images, which can be used to study the idea of CC graphically. From CC plot, it is clear that the CC of an encrypted image is correlated in all directions. This demonstrates that the proposed scheme is resistant to attacks.

4.1. Key sensitivity analysis

Key sensitivity analysis of the above mentioned cryptosystem is tested to validate its robustness. In this analysis it is found that the decryption of *Lena* image is only possible with the use of all keys. This means that if one skips any key in the scheme then it is impossible to get the information of the image. The results of decrypted image without Key1, without Key2, and without Key3 and using wrong FrFT order $q = 0.5$ are shown

T a b l e 1. Correlation coefficient (CC) results for both the images.

Algorithm	Image	Correlation coefficient value		
		Diagonal	Vertical	Horizontal
Proposed cryptosystem	Gray image (original)	0.9354	0.9779	0.9525
Proposed cryptosystem	Binary image (original)	0.8914	0.9197	0.9290
Proposed cryptosystem	Gray image (encrypted)	−0.3598	0.0020	−0.2338
Proposed cryptosystem	Binary image (encrypted)	−0.5912	−0.1784	−0.5469

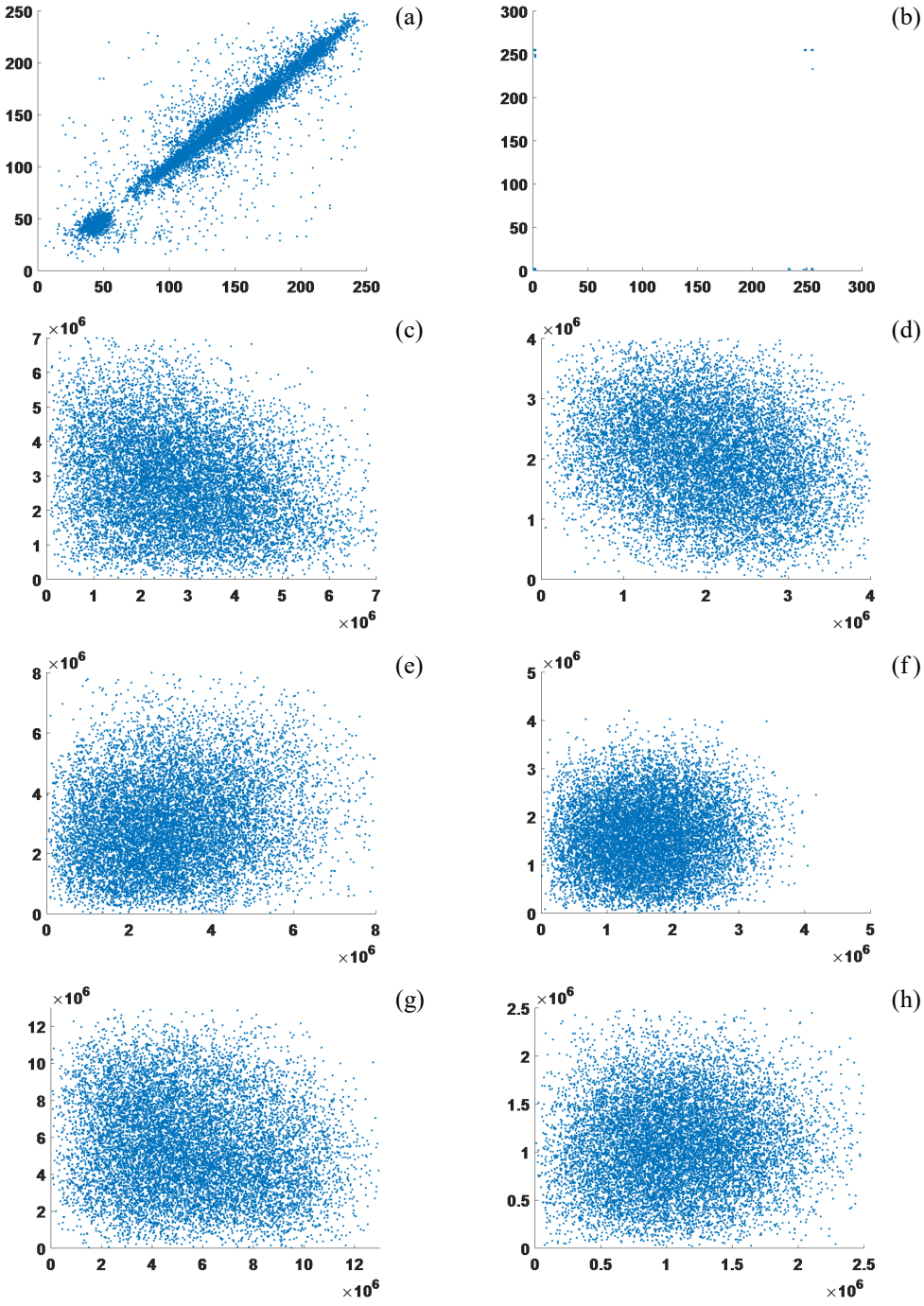

Fig. 4. CC plot (a, b) diagonal plot of original *Lena* and OPT image; (c, e, g) encrypted *Lena* image CC plot in diagonal, horizontal and in vertical directions; (d, f, h) binary ciphered image CC plot in diagonal, horizontal and in vertical directions.

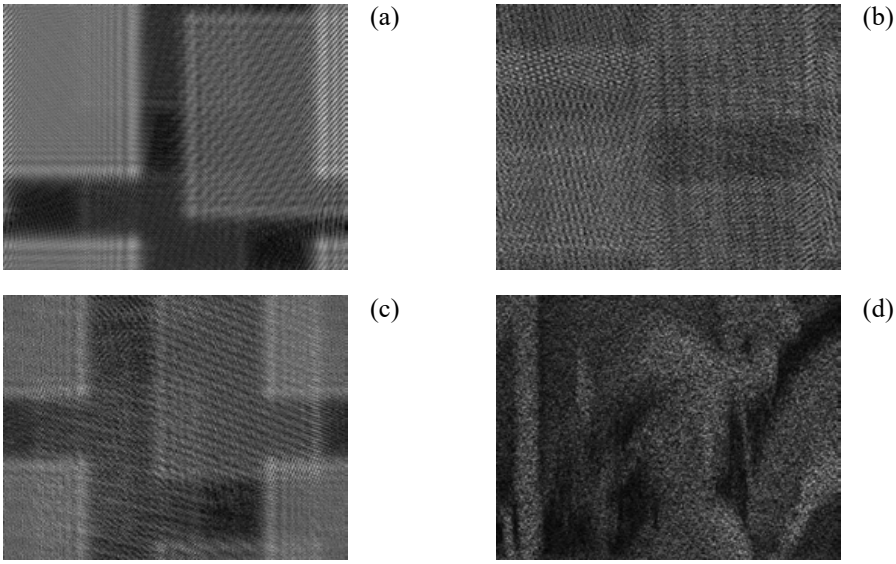

Fig. 5. Obtained image without (a) Key1; (b) Key2; (c) Key3; (d) wrong parameter of FrFT.

in Fig. 5. By visualising the decrypted result shown in the figure, it is evident that the scheme is extremely sensitive to the keys. Therefore, the scheme is more resilient.

4.2. 3D plot analysis

3D of an image represents the pixel spreading. For a good cryptosystem, the surface plot of the original and decrypted image must resemble with each other and for encrypted image pixels should be uniformly spread so that it is difficult for the attacker to get information from the cipher image. Figure 6 represents the 3D plot for the *Lena* and binary image.

4.3. Noise attack analysis

When noise is introduced in the transmission of images, it can easily degrade the quality of the encrypted image. Due to this, it affects the quality of decrypted image. Hence it is unavoidable to check the noise sensitivity for the cryptosystem. This following relation describes how noise affects encrypted images.

$$E = \tilde{E}(1 + kG) \tag{16}$$

where E is noise affected image while $\tilde{E}$ is encrypted image of the cryptosystem. In Eq. (16), G represents the Gaussian noise with mean value zero and having standard deviation equal to one. The noise strength k is set to different-different value to test the scheme against the noise attack. Figure 7(a) represents MSE plot with noise strength and Fig. 7(b,c) show the recovered binary images when we set the value of $k = 0.1$ and $k = 0.7$, respectively.

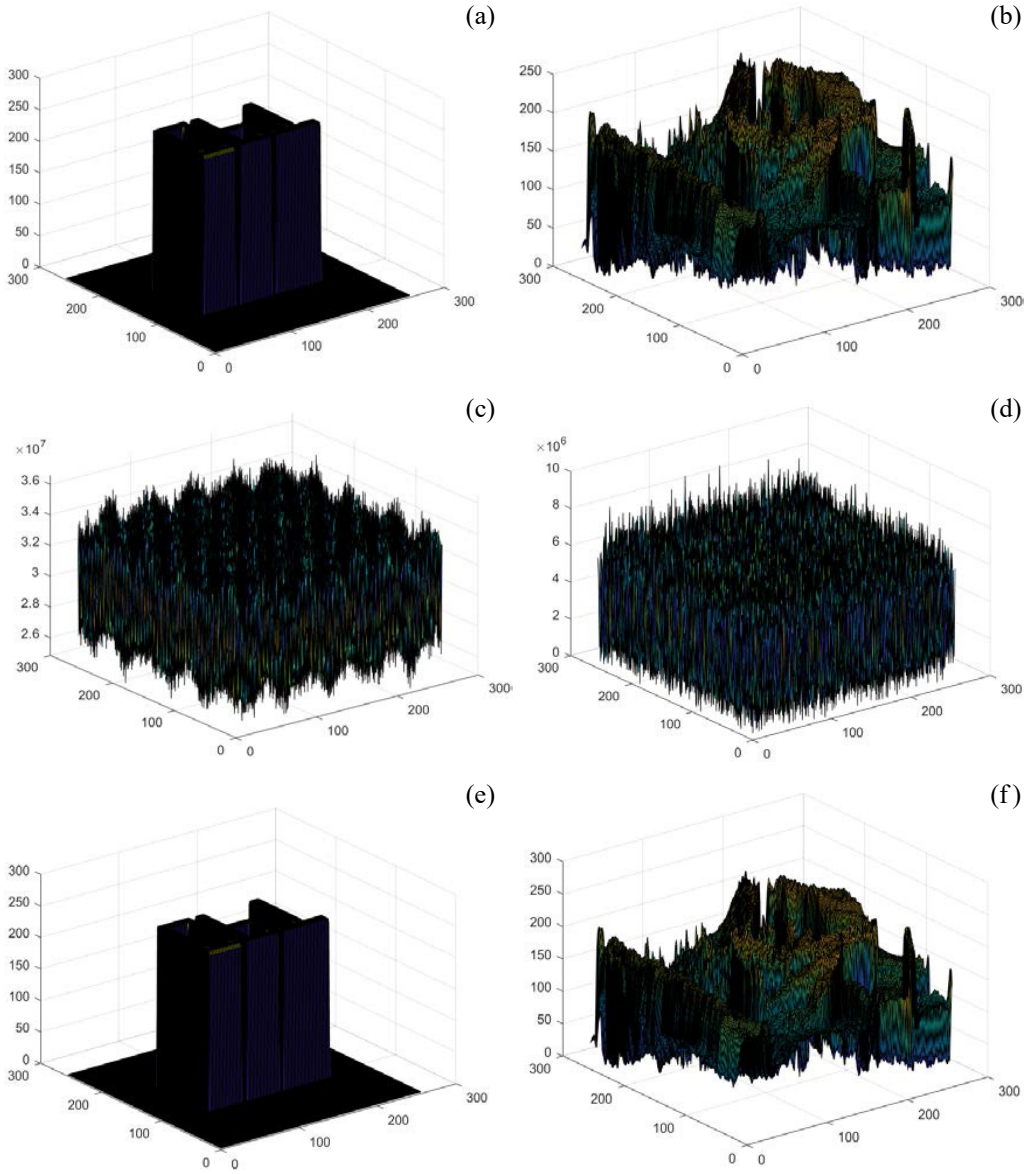

Fig. 6. 3D plot (a) binary image; (c) binary encrypted; (e) binary decrypted; (b) *Lena* image; (d) *Lena* encrypted image; (f) *Lena* decrypted image.

5. Conclusion

The asymmetric cryptosystem is implemented using FrFT as the fractional order of FrFT enhances the security of proposed scheme. RD is also utilized with phase truncation operation to enlarge the cryptosystem's key space. Also decryption keys of this asymmetric cryptosystem are different from public keys, they support the cryptosystem

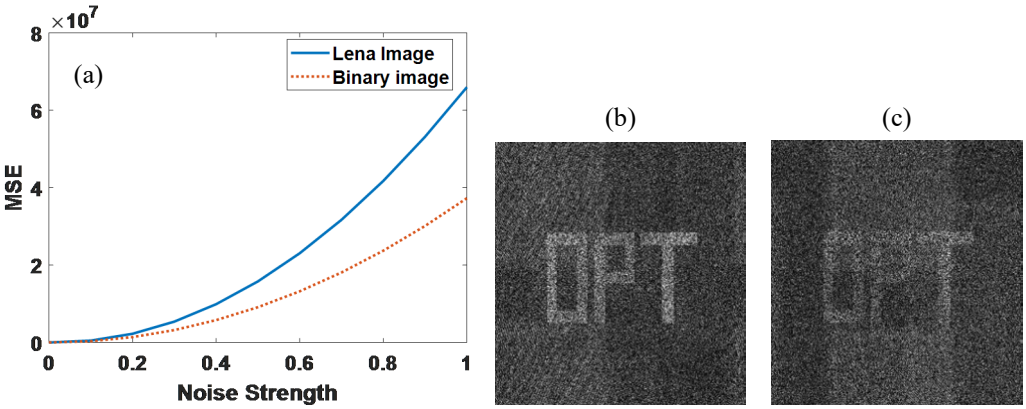

Fig. 7. Noise results (a) plot of noise strength with MSE; (b) binary recovered image with $k = 0.1$; (c) binary recovered image having noise strength $k = 0.07$.

T a b l e 2. Comparison analysis for different asymmetric cryptosystems.

Algorithm	Image	Comparision parameters	
		MSE	PSNR [dB]
Ref. [18]	Gray image	7.04×10^{-23}	178.4
Ref. [26]	Gray image	9.5×10^{-25}	240.1
Ref. [30]	Gray image	3.1×10^{-20}	201.23
Proposed cryptosystem	Gray image	1.33×10^{-22}	216.12

against various attacks. Grayscale and binary images are used to obtain the results. MSE and PSNR values indicated that the recovered image is of high quality. Using the key sensitivity analysis and results of correlation coefficient, we may conclude that this cryptosystem is resistant to attacks.

References

[1] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767

[2] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004: 1584-1586. https://doi.org/10.1364/OL.29.001584

[3] MATOBA O., JAVIDI B., *Encrypted optical memory system using three-dimensional keys in the Fresnel domain*, Optics Letters **24**(11), 1999: 762-764. https://doi.org/10.1364/OL.24.000762

[4] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000: 887-889. https://doi.org/10.1364/OL.25.000887

[5] ZHON N., WANG Y., GONG L., *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011: 3234-3242. https://doi.org/10.1016/j.optcom.2011.02.065

[6] CHEN L., ZHAO D., *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006: 3438-3440. https://doi.org/10.1364/OL.31.003438

[7] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006: 1044-1046. https://doi.org/10.1364/OL.31.001044

[8] Peng X., Wei H., Zhang P., *Chosen-plaintext atack on lensless double-random phase encoding in the Fresnel domain*, Optics Letters **31**(22), 2006: 3261-3263. https://doi.org/10.1364/OL.31.003261
[9] Carnicer A., Montes-Usategui M., Arcos S., Juvells I., *Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005: 1644-1646. https://doi.org/10.1364/OL.30.001644
[10] Qin W., Peng X., *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010: 118-120. https://doi.org/10.1364/OL.35.000118
[11] Liu W., Liu Z., Wu J., Liu S., *Asymmetric cryptosystem by using modular arithmetic operation based on double random phase encoding*, Optics Communications **301-302**, 2013: 56-60. https://doi.org/10.1016/j.optcom.2013.03.053
[12] Wang Q., Guo Q., Zhou J., *Color image hiding based on phase-truncation and phase retrieval technique in fractional Fourier domain*, Optik **124**(12), 2013: 1224-1229. https://doi.org/10.1016/j.ijleo.2012.03.004
[13] Mehra I., Nishchal N.K., *Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding*, Optics Express **22**(5), 2014: 5474-5482. https://doi.org/10.1364/OE.22.005474
[14] Liu W., Xie Z., Liu Z., Zhang Y., Liu S., *Multiple-image encryption based on optical asymmetric key cryptosystem*, Optics Communications **335**, 2015: 205-211. https://doi.org/10.1016/j.optcom.2014.09.046
[15] Singh H., *Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain*, Optica Applicata **47**(4), 2017: 557-578. https://doi.org/10.5277/oa170406
[16] Sachin S., Kumar R., Singh P., *Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain*, Optical and Quantum Electronics **53**, 2021: 254. https://doi.org/10.1007/s11082-021-02908-w
[17] Kumar R., Quan C., *Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform*, Optics and Laser in Engineering **120**, 2019: 118-126. https://doi.org/10.1016/j.optlaseng.2019.03.024
[18] Girija R., Singh H., *Enhancing security of double radom phase encoding based on radom S-box*, 3D Research **9**, 2018: 15. https://doi.org/10.1007/s13319-018-0165-z
[19] Girija R., Singh H., *An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain*, Multimedia Tools and Applications **79**, 2020: 34717-34735. https://doi.org/10.1007/s11042-019-7733-y
[20] Yadav A.K., Singh P., Saini I., Singh K., *Asymmetric encryption algorithm for colour images based on fractional Hartley transform*, Journal of Modern Optics **66**(6), 2019: 629-642. https://doi.org/10.1080/09500340.2018.1559951
[21] Khurana M., Singh H., *An asymmetric image encryption based on phase truncated hybrid transform*, 3D Research **8**, 2017: 28. https://doi.org/10.1007/s13319-017-0137-8
[22] Anshula, Singh H., *Security-enrichment of an asymmetric optical image encryption-based devil's vortex Fresnel lens phase mask and lower upper decomposition with partial pivoting in gyrator transform domain*, Optical Quantum Electronics **53**, 2021: 204. https://doi.org/10.1007/s11082-021-02854-7
[23] Sangwan A., Singh H., *A secure asymmetric optical image encryption based on phase truncation and singular value decomposition in linear canonical transform domain*, International Journal of Optics, Vol. 2021, 2021: 5510125. https://doi.org/10.1155/2021/5510125
[24] Cai J., Shen X., Lei M., Lin C., Dou S., *Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition*, Optics Letters **40**(4), 2015: 475-478. https://doi.org/10.1364/OL.40.000475
[25] Anjana S., Rakheja P., Yadav A., Singh P., Singh H., *Asymmetric double image encryption, compression and watermarking scheme based on orthogonal-triangular decomposition with column pivoting*, Optica Applicata **52**(2), 2022: 283-295. https://doi.org/10.37190/oa220210
[26] Gaur K.S., Singh H., Thakran S., *Asymmetric cryptosystem using QZ modulation with SPM in Fresnel domain*, Journal of Optics **52**, 2023: 1694-1703. https://doi.org/10.1007/s12596-022-00990-1

[27] BARRERA J.F., HENAO R., TORROBA R., *Fault tolerances using toroidal zone plate encryption*, Optics Communications **256**(4-6), 2005: 489-494. https://doi.org/10.1016/j.optcom.2005.06.077

[28] DAVIS J.A., MCNAMARA D.E., COTTRELL D.M., CAMPOS J., *Image processing with the radial Hilbert transform: Theory and experiments*, Optics Letters **25**(2), 2000: 99-101. https://doi.org/10.1364/OL.25.000099

[29] SINGH H., *Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain*, IET Image Processing **12**(11), 2018: 1994-2001. https://doi.org/10.1049/iet-ipr.2018.5399

[30] SINGH H., *Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase -truncation in gyrator wavelet transform domain*, Optics and Lasers in Engineering **81**, 2016: 125 -139. https://doi.org/10.1016/j.optlaseng.2016.01.014

[31] SINGH H., YADAV A.K., VASHISTH S., SINGH K., *Fully phase image encryption using double random -structured phase masks in gyrator domain*, Applied Optics **53**(28), 2014: 6472-6481. https://doi.org/10.1364/AO.53.006472

[32] WANG Y., QUAN C., TAY C.J., *New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition*, Applied Optics **55**(4), 2016: 679-686. https://doi.org/10.1364/AO.55.000679

[33] XU H., XU W., WANG S., WU S., *Phase-only asymmetric optical cryptosystem based on random modulus decomposition*, Journal of Modern Optics **65**(10), 2018: 1245-1252. https://doi.org/10.1080/09500340.2018.1431314

[34] RAKHEJA P., VIG R., SINGH P., *An asymmetric watermarking scheme based on random decomposition in hybrid multi-resolution wavelet domain using 3D Lorenz chaotic system*, Optik **198**, 2019: 163289. https://doi.org/10.1016/j.ijleo.2019.163289

[35] YADAV S., SINGH H., *Image encryption algorithm based on rear-mounted phase mask and random decomposition*, Optica Applicata **52**(2), 2022: 195-212. https://doi.org/10.37190/oa220204

Received January 21, 2023
in revised form April 23, 2023