Optica Applicata, Vol. LII, No. 2, 2022
DOI: 10.37190/oa220204

Image encryption algorithm based on rear-mounted phase mask and random decomposition

SHIVANI YADAV*, HUKUM SINGH

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

*Corresponding author: shivani6400@gmail.com

To escalate the image encryption a new method has been devised which includes double random phase encoding (DRPE) using rear phase masking and random decomposition (RD) technique stranded on fractional Fourier transform. Here, asymmetric cryptographic system is developed in fractional Fourier transform (FrFT) mode using two random phase masks (RPM) and a rear mounted phase mask. In the projected scheme a colored image is decomposed into R, G and B channels. The amplitude of each channel is normalized, phase encoded and modulated using RPM. The modulated R, G and B channels of the colored image are individually transformed using FrFT to produce corresponding encrypted image. The proposed scheme is authorized on grayscale image also. The norm behind the development of the suggested scheme has been elaborated by carrying out cryptanalysis on system based on the RD. The method helps in escalations of the protection of double random phase encoding by cumulating the key length and the parameter amount, so that it vigorously can be used against various attacks. The forte of the suggested cryptographic system was verified using simulations with MATLAB 7.9.0 (R2008a). The efficiency of the suggested scheme includes the analysis using singular value decomposition (SVD), histogram and correlation coefficient.

Keywords: fractional Fourier transform, random decomposition, rear-mounted phase mask, SVD.

1. Introduction

In the epoch of the 21st century, rapid usage of internet has become the basis of information, communication, and data storage. The security of images remains a major issue while storing and transmitting these data. Data could be anything from someone's medical report, top secret military reports and government's confidential reports, personal bank account details, online banking operation details, student's official document of an institution, social media profile password, one-time password (OTP), biometric information, defense personals records and other susceptible information. The purpose of any encryption algorithm is to safeguard the information and to send it securely. Just like crypt analysis, image encryption is one of the methods to protect the information to be accessed by an illegal user. There are various popular digital image encoding methods like data encoding standard (DES), advanced encoding standard (AES) available for the data security. Still, their complex computation makes it tricky to be used by anyone. On the other hand, there are various optical encryption algorithms which have remarkable features like they have less computational complicity, parallel processing, multidimensional parameters like wavelength, focal distance, high speed, and time saving.

This can be done with optical image encryption techniques [1–3], which is one of the best methods of encryption and protection of confidential information. In the past few decades, several methods of encryption of images have been suggested. The most operative and well- rehearsed image encoding is double random phase encoding (DRPE), firstly studied by Refregier and Javidi in 1995 [4]. DRPE is an optically symmetric key encoding and decoding scheme which helps in encoding the primary image and converts the encoded image into stationary white noise, using two random phase masks (RPMs) in the Fourier transforms [4,5], one in input plane and another in Fourier plane. The RPM's used are independent of each other. To increase data security, the DRPE was extended to many other transforms, such as fractional Fourier transform (FrFT) [6–9], Fresnel transform [10–13], gyrator transform [14–16], fractional Mellin transform [17 –19], Daubechies quantum wavelet transform (DQWT) [20], discrete fractional Hartley transform [21], *etc*. These methods use symmetric encryption [22] in which we use similar keys at the time of encryption and decryption. In all these approaches, input images are well-lit by monochromatic light and improved images lose their color evidence, which is beneficial in image processing and practical applications. Use of symmetric keys conveys destructive destruction to constancy as it is unprotected from many attacks like chosen cipher text attack [23], chosen plain image attack [24], and known plane image attack [25,26]. To overcome from symmetric methods, Qin and Peng [27] proposed an asymmetric cryptosystem based on nonlinear phase truncated Fourier transforms (PTFTs). Asymmetric technique consists of different keys while encryption and decryption of an image and it helps in maintaining the strength of the system. Therefore, many nonlinear encryption methods [28–33] have been further suggested. The proposed work deals with enhancing the security of the original DRPE by introducing a rear phase mask operation using random decomposition which helps in adding more security by enhancing the key space. Considering random decomposition (RD), Wang *et al.* [34–37] proposed a cryptosystem which is an alternative to equal modulus decomposition scheme and two random masks are produced after decomposition. Both the masks are not equal in moduli which have limited available constraint to an interloper, likewise amplitude of the ciphertext. So, it does not transmit any information about the amplitude of the private key unlike in equal modulus decomposition. The rear-mounted phase mask [38] redefines the DRPE output, by converting ciphered image into a fractional Fourier domain without perfect information of the mask. Here, we recommend a collective system using two random phase masks (RPM) and one of the RPM is used as the key for rear mounted phase mask.

In the encryption, front singular value decomposition (SVD) [39–41] is deployed. In the decoding scheme, the original gray scale image is retrieved by utilizing the inverse singular value decomposition (ISVD). The use of Hybrid system during encoding and decoding process supports enhancement in robustness of DRPE scheme. SVD used in our recommended method delivers three components for encrypted image, which is another supplementary aspect that reinforces the security of DRPE scheme. Zhang and Karim first time reported DRPE system of single-channel color image encryption in Fourier domain [42]. Based on FrFT, the color image encoding using wavelength multiplexing [43] and enciphering of color and gray-scale image using single-channel DRPE have been proposed [44]. A color image is first decomposed into three components (R, G, B) [45] and in our paper blue component is encoded using FrFT and random decomposition (RD). The outcomes of the experiments are tested and are verified so as to check the validation of the suggested scheme. The reliability of the suggested encryption scheme is analyzed and tested based on several factors on MATLAB 7.9.0 (R2008a).

Based on RD in fractional Fourier transform, an asymmetric cryptosystem is recommended in the paper. With different set of private and public keys, the proposed scheme is executed both digitally as well as through an optoelectronic setup in Fig. 1 and is strong against noise attacks. The collimated ray from laser ($\lambda = 632.8$ nm) passes through a SFBE (spatial filter beam expander). Digitally on the first SLM (spatial light modulator), the ray helps as an object beam, which illumines the given image along with first random phase mask (R1). During the process, the image firstly passes through fractional Fourier transform with order p, q then on the second SLM, the ray again helps as an object ray, which illuminates the image along with second random phase mask (R2). The produced object is again passing through inverse fractional Fourier transforms with order $-p$, $-q$ and on the third SLM, the ray helps object beam which illuminates the image with rear-mounted phase mask. After that, it passes through RD (random

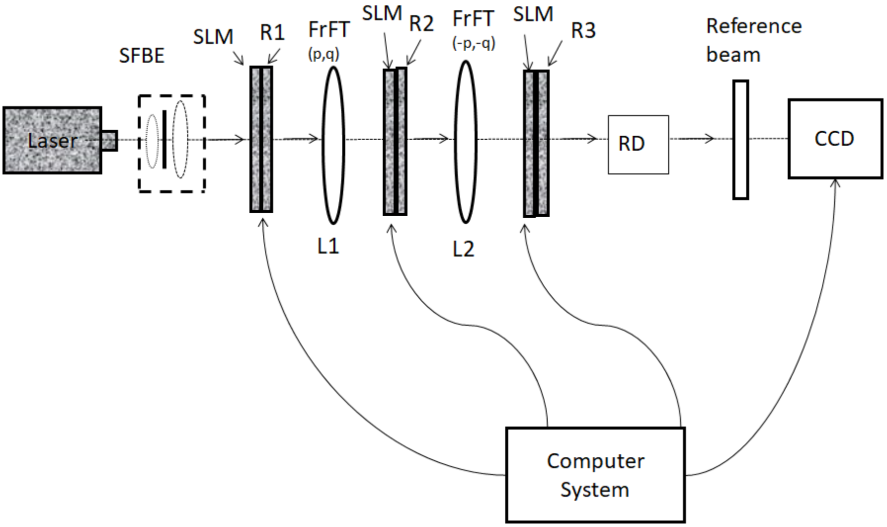

Fig. 1. Optical setup for the proposed work.

decomposition) and finally from reference beam and the derived image is demonstrated on the CCD device.

Section 2, of the paper, depicts the theoretical analysis of the principle used. The suggested procedure is explained in Section 3 of the paper. The outcomes of the experiments are tested and verified to check the validation of the suggested scheme. The reliability of the suggested encryption scheme is analyzed and tested based on several factors on MATLAB 7.9.0 (R2008a). Sections 4 and 5 show the results attained by MATLAB simulations to confirm the efficacy of the scheme.

2. Theoretical analysis

2.1. Fractional Fourier transform

In our proposed scheme we have used DRPE scheme in Fractional Fourier domain. The FrFT of order α of an input function $f(x)$ can be defined in terms of kernel function as follows:

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

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

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

Here, $A = \dfrac{1}{|\sin\varphi|^{1/2}} \exp\left[-i\left(\dfrac{\pi \operatorname{sgn}\varphi}{4} - \dfrac{\varphi}{2}\right)\right]$. Where, $\varphi = \alpha\pi/2$ is the angle corresponding to the transform order α along the x-axis.

2.2. Random decomposition (RD)

To an alternative to equal modulus decomposition [33], WANG *et al.* in 2007 proposed random decomposition which is an asymmetric optical cryptosystem entirely based on coherent superposition. The original image is bound with a random phase mask, $R(x, y) = \exp\{2\pi i m(x, y)\}$ and then Fourier transformed. After that, using random decomposition two complex-valued masks $K_1(u, v)$ *i.e.* a private key and $K_2(u, v)$, the other mask is obtained. Applying inverse Fourier transform, and using random decomposition results in one more private key (K_4) and ciphertext $K_3(x, y)$. Encryption and decryption process of random decomposition is shown in Fig. 2 with the help of flowchart. If $G'(x, y)$is the original image, then $G_1(u, v)$ is obtained by using the following equation:

$$G_1(u, v) = \mathrm{FT}\{G'(x, y) \times R(x, y)\} \tag{3}$$

where FT denotes Fourier transform.

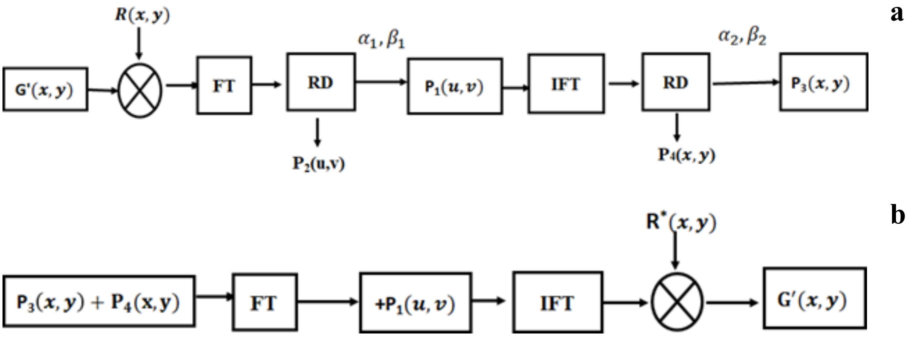

Fig. 2. The random decomposition flowcharts for (**a**) encryption and (**b**) decryption procedures.

Using random decomposition procedure, $G_1(u, v)$ is divided into $P_1(u, v)$ and $P_2(u, v)$ which is achieved as follows:

$$P_1(u, v) = \frac{N_1(u, v)\sin(\beta_1(u, v))}{\sin\left[\alpha_1(u, v) + \beta_1(u, v)\right]} e - i\left[\alpha_1(u, v) - \varphi_1(u, v)\right] \tag{4}$$

$$P_2(u, v) = \frac{N_1(u, v)\sin(\alpha_1(u, v))}{\sin\left[\alpha_1(u, v) + \beta_1(u, v)\right]} e - i\left[\varphi_1(u, v) + \beta_1(u, v)\right] \tag{5}$$

where, $\alpha_1(u, v) = 2\pi\text{rand}(u, v)$, $\beta_1(u, v) = 2\pi\text{rand}(u, v)$, $N_1(u, v) = |G_1(u, v)|$ and $\varphi_1(u, v) = \arg\{G_1(u, v)\}$.

Perform an inverse Fourier transform on $P_1(u, v)$, *i.e.*

$$G_2(x, y) = \text{IFT}(P_1(u, v)) \tag{6}$$

Using, $\alpha_2(x, y) = 2\pi\text{rand}(x, y)$ and $\beta_2(x, y) = 2\pi\text{rand}(x, y)$ as encryption keys, $G_2(x, y)$ is again random decomposed to give another private key (P_4) and cipher text $P_3(x, y)$ as follows:

$$P_4(x, y) = \frac{N_2(x, y)\sin(\beta_2(x, y))}{\sin\left[\alpha_2(x, y) + \beta_2(x, y)\right]} e - i\left[\alpha_2(x, y) - \varphi_2(x, y)\right] \tag{7}$$

$$P_3(x, y) = \frac{N_2(x, y)\sin(\alpha_2(x, y))}{\sin\left[\alpha_2(x, y) + \beta_2(x, y)\right]} e - i\left[\varphi_2(x, y) + \beta_2(x, y)\right] \tag{8}$$

where $N_2(x, y) = |G_2(x, y)|$ and $\varphi_2(x, y) = \arg\{G_2(x, y)\}$.

Two private keys developed by random decomposition, *i.e.* P_2 and P_4, are used to decrypt the original image. According to the principle of random decomposition

$$P_4(x, y) + P_3(x, y) = G_2(x, y) \tag{9}$$

$$P_1(u, v) + P_2(u, v) = G_2(u, v) \tag{10}$$

Combining Eqns. (5), (6), (9) and (10), we recovered input image as,

$$G'(x, y) = \mathrm{conj}(R(x, y))\{\mathrm{IFT}\{\mathrm{FT}[G_2(x, y)] + P_1(u, v)\}\} \tag{11}$$

2.3. Singular value decomposition (SVD)

Singular value decomposition (SVD) [19, 38–40] is an important matrix decomposition technique used in linear algebra. It is slightly similar to the symmetry matrix. For $m \times n$ matrix A there are U and V matrices, which contain $m \times m$ and $n \times n$ elements, respectively. It is defined as follows:

$$A = USV \tag{12}$$

where, $S = \mathrm{diag}(\sigma_1, \sigma_2, ..., \sigma_r)$, $\sigma_i > 0$ $(i = 1, 2, ..., r)$, $r = \mathrm{rank}(A)$.

The SVD process is used to encrypt digital images. We can divide the input images into three parts and protect them in different ways. The original image can only be returned if the three participants meet and are multiplied in the correct order. Figure 3

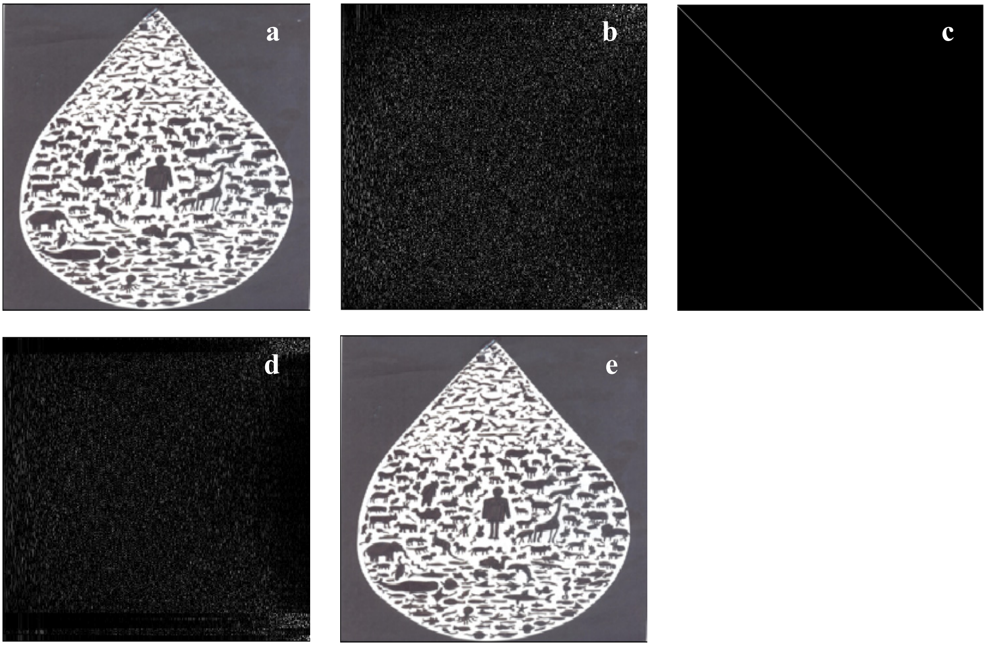

Fig. 3. SVD results for (**a**) original image, (**b**, **c**, **d**) the U, S and V components, respectively, and (**e**) the decomposed image.

shows the results of the SVD. The original image is displayed by Fig. 3**a** and the results of the SVD are shown in Figs. 3**b**–3**d**. Figure 3**b** is the U part, Fig. 3**c** is the diagonal part of S and Fig. 3**d** is the V part. Finally, Fig. 3**e** is the decomposed image.

2.4. Rear-mounted phase mask

The properties of DRPE are escalated with the assistance of rear-mounted phase mask operation [37]. To modulate the phase of the encrypted data, an extra phase mask R_3 is used at the output plane. The encoding and decoding steps involved in this enhanced suggested cryptosystem are elucidated in Figs. 4**a** and 4**b** separately. In the flowchart, R_3 is used as the RPM (*i.e.* rear-mounted phase mask) which is arbitrarily scattered in [0, 2π]. This serves as the additional secret key.

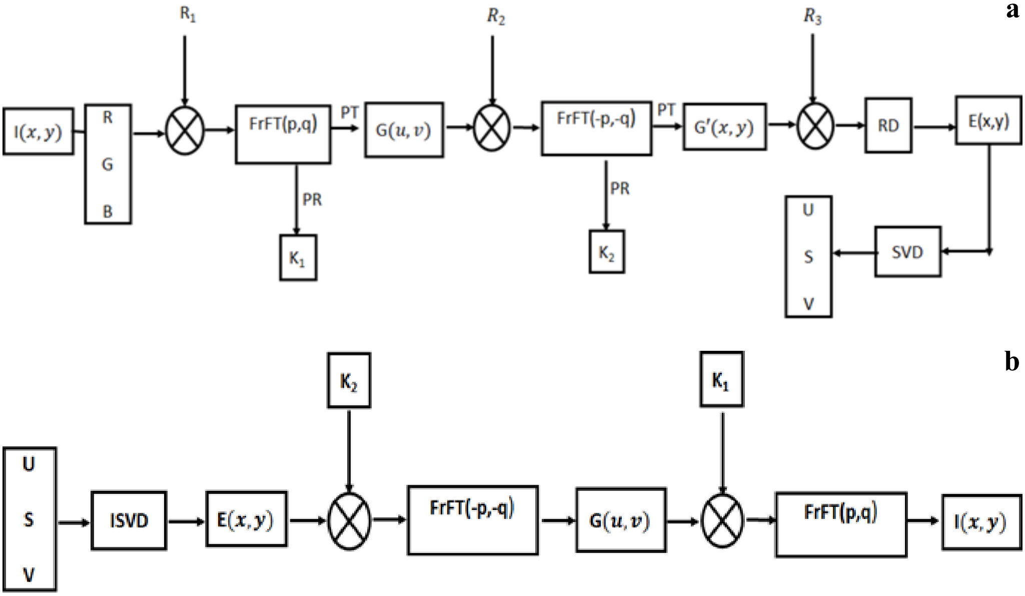

Fig. 4. Flowchart of (**a**) encryption and (**b**) decryption schemes.

3. Proposed technique

3.1. Ciphering

While encrypting, we are defining two keys in encryption process since it is an asymmetric method which makes the scheme much more secure and confidential without any loss of originality. The steps of the encryption process are:

1) In the input domain, first take the input gray scale image $I(x, y)$ and decompose into R, G and B channels denoted as $I_R(x, y)$, $I_G(x, y)$ and $I_B(x, y)$, respectively. For conciseness, only blue channel is illustrated.

2) Then take the blue channel and convolute with the first RPM (R_1) used.

3) Next perform FrFT with fractional orders (p, q) and define the first asymmetric key K_1, from here we get an intermediate image $G(u, v)$.

$$G(u, v) = K_1[\mathrm{FrFT}(p, q)\{I_\mathrm{B}(x, y) \times R_1\}] \tag{13}$$

4) To attained intermediate image $G'(x, y)$, convolute $G(u, v)$ with the second RPM (R_2) and perform inverse FrFT with orders $(-p, -q)$ and define the second asymmetric key K_2.

$$G'^{(x, y)} = K_2\{\mathrm{FrFT}(-p, -q)[G(u, v) \times R_2]\} \tag{14}$$

5) After that multiply the phase reversal key along with the rear-mounted phase mask R_3.

6) Now, performing random decomposition on $G'(x, y)$ given by Eq. (11) enhances the security to high level and from there we get encrypted image $E(x, y)$,

$$E(x, y) = \mathrm{RD}[R_3 \times \{G'(x, y)\}] \tag{15}$$

7) Finally, SVD is performed and three components are attained, *i.e.* U, S and V.

3.2. Deciphering

Two private keys developed by encryption procedure are used to decrypt the cipher image which included all the three-color components.

1) First retrieve the U, S and V components by taking inverse singular value decomposition (ISVD).

2) Then, convolute the encrypted image $E(x, y)$ with the second phase reserve key K_2 and taking inverse fractional Fourier transform gives intermediate image $G(u, v)$.

$$G(u, v) = \mathrm{FrFT}(-p, -q)[E(x, y) \times K_2] \tag{16}$$

3) So, multiply this intermediate image with the first phase reserve key K_1 and applying fractional Fourier transform on it, we can attain the original image $I(x, y)$.

$$I(x, y) = \mathrm{FrFT}(p, q)[G(u, v) \times K_1] \tag{17}$$

Hence, the use of two different keys K_1 and K_2 helps in increasing key space and security of the system. If both the keys are used correctly, then only the original image is recovered.

4. Outcomes

To assess the effectiveness and security of the suggested cryptographic system, digital simulations were carried out. A gray-scale image namely: the drop image used as the input image, RGB channels of the input image, rear-mounted phase mask, the two pri-

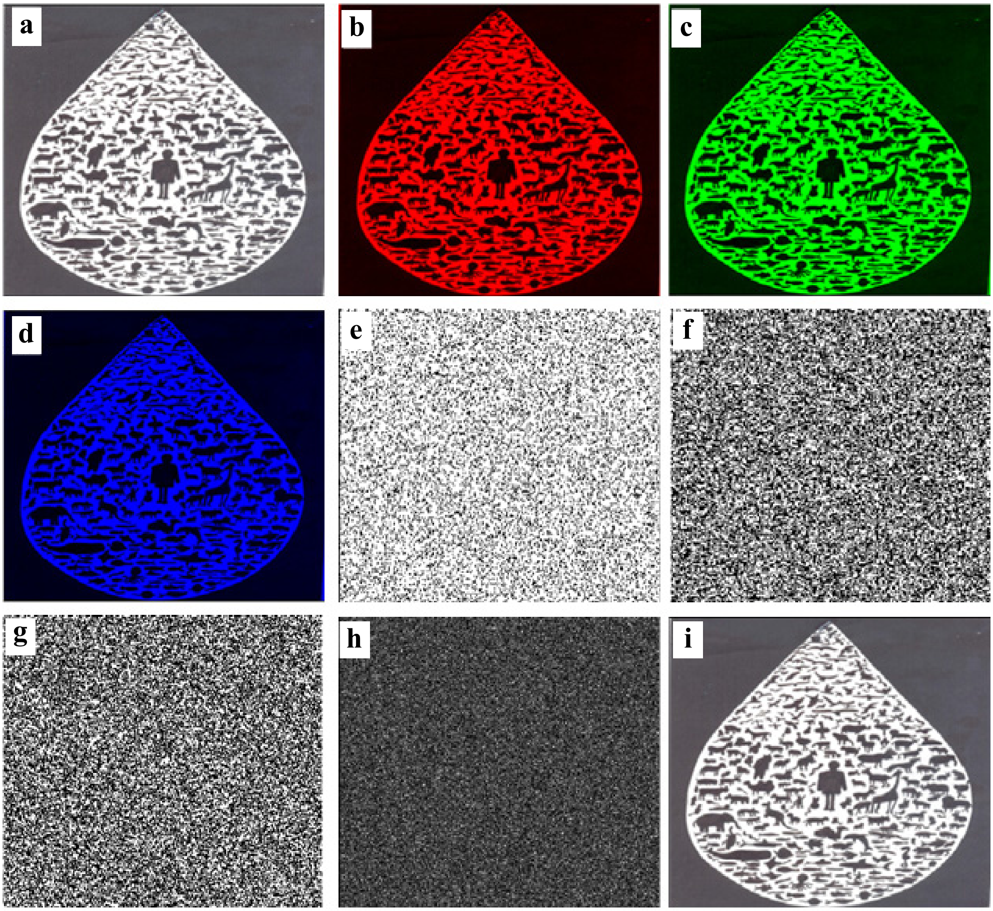

Fig. 5. (**a**) Drop image, (**b**, **c**, **d**) the red, green and blue images, (**e**) the rear mounted mask, (**f**, **g**) the two private keys K_1 and K_2, and (**h**, **i**) the encrypted and decrypted images, respectively.

vate keys obtained by random decomposition to have transformed a selected area of cryptographic text and the encoded, decoded image are depicted in Fig. 5. The outcome shown in Fig. 6 demonstrates the 3D view of input, ciphered and deciphered drop images.

To evaluate the excellence of the deciphered image, the recommended algorithm is verified by calculating mean square error (MSE) and peak signal noise ratio (PSNR).

Mean square error: MSE was calculated to express the quality of the decoded image by verifying the safety and performance of the recommended system. If $I_\mathrm{o}(x, y)$ and $I_\mathrm{d}(x, y)$ symbolize the plain and decoded image, MSE is evaluated with the following equation:

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left| I_\mathrm{o}(x, y) - I_\mathrm{d}(x, y) \right|^2 \tag{18}$$

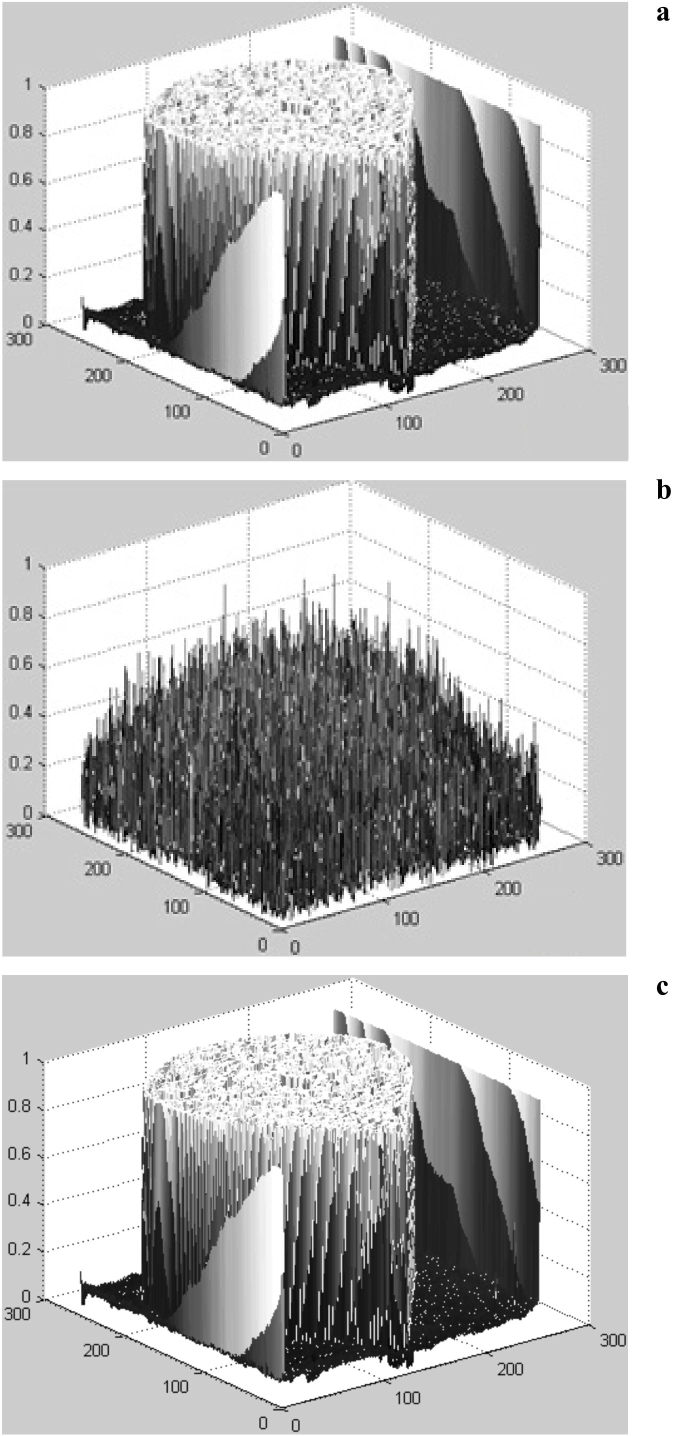

Fig. 6. 3D views of drop (**a**) original image, (**b**) encoded image, and (**c**) decoded image.

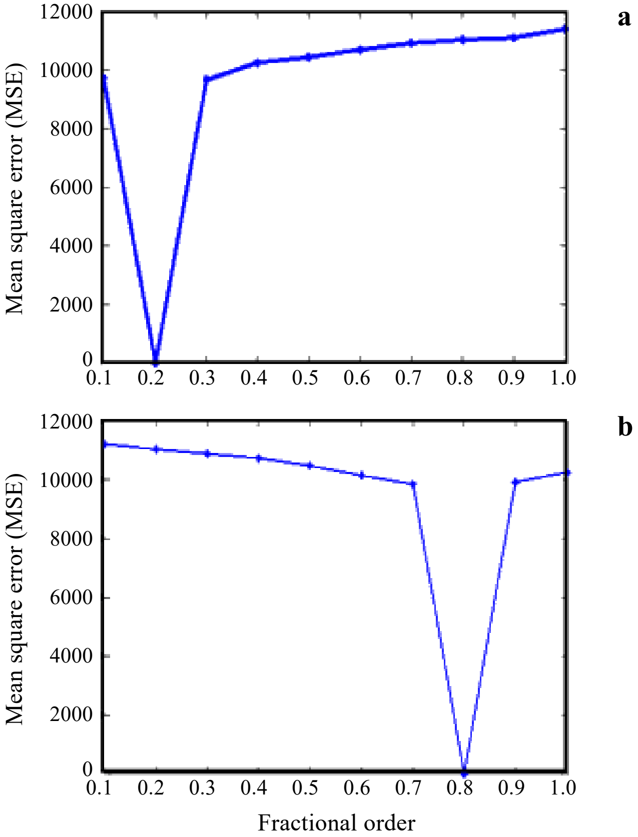

Fig. 7. The plot of MSE with fractional orders (p, q) at (**a**) 0.2 and (**b**) 0.8.

The MSE value attained for the suggested algorithm is 3.371×10^{-27} for drop image. The MSE value attained is insignificant, so it ensures high excellence of image and proves the reliability of the suggested scheme. MSE is a standard error function with very low values, which means that it has recovered high class image which represents the sturdiness of suggested procedure. The plot between MSE and Fractional orders for different values at 0.2 and 0.8 are shown in Figs. 7**a** and 7**b**, respectively.

Peak signal-to-noise ratio: The effectiveness of noise in any noise effected deciphered image is measured by the peak-to-noise ratio (PSNR). It processes the difference among the input and decoded images, *i.e.* $I_o(x, y)$and $I_d(x, y)$, respectively by using a mathematical expression which is illustrated by equation:

$$\mathrm{PSNR} = 10\log\left\{\frac{255^2}{\frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left|I_o(x, y) - I_d(x, y)\right|^2}\right\} \tag{19}$$

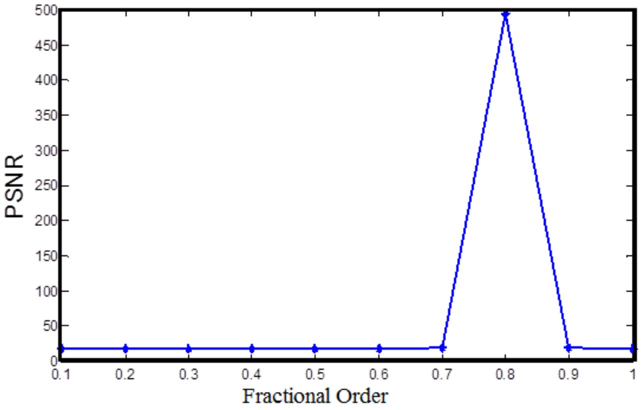

Fig. 8. Curve between PSNR and fractional orders at 0.8.

Table 1. Evaluation of the system based on mean square error and peak signal-to-noise ratio.

Algorithm	Input image	MSE	PSNR [dB]
Ref. [4]	Grayscale image	1.65×10^{-26}	704.54
Ref. [36]	Grayscale image	104.2	>50
Proposed asymmetric cryptosystem	Grayscale image	3.371×10^{-27}	671.59

The PSNR value of image drop is 498.89. High value designates the high quality of deciphered image. PSNR is measured as a degree of image excellence and its values are figured employing original image and its equivalent deciphered image. Figure 8 depicts the curve of PSNR versus fractional order at 0.8.

Table 1 presents a proportional analysis of the recommended procedure with the original DRPE method and with the Ref. [36]. The attained values of MSE, PSNR of our recommended procedure ensure high quality image in comparison with the DRPE approach and Ref. [36].

5. Statistical evaluation

To evaluate efficiency of the recommended method, statistical analysis is carried out using correlation coefficients and histogram of plain and ciphered image.

5.1. Correlation factor

To verify the correlation coefficient (CC), the analysis is carried out by randomly selected 10000 couples of adjacent pixels (in horizontal, vertical and diagonal direction) from plain and ciphered image. The CC factor is estimated by the following equation:

$$\mathrm{CC} = \frac{\mathrm{cov}(x, y)}{\sigma(x)\sigma(y)} \tag{20}$$

where

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \tag{21}$$

$$\sigma(x) = \left[\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})\right]^{1/2} \tag{22}$$

$$\sigma(y) = \left[\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})\right]^{1/2} \tag{23}$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{24}$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{25}$$

Here $\sigma(x) \neq 0$, $\sigma(y) \neq 0$ and $x(i), y(i)$ are the values of two adjacent pixels, N is the number of pairs (x_i, y_i), and $(\bar{x}, \bar{y})$ are the mean values, respectively. Table 2 elucidates the CC values of adjacent pixels of input images and their corresponding ciphered versions. The CC of encrypted images is much weaker than that of the input images.

Table 2. Correlation coefficients of grayscale drop image for original, encrypted and decrypted images in horizontal, vertical and diagonal directions.

Algorithm	Metrics	Correlation coefficients		
		Horizontal	Vertical	Diagonal
Proposed asymmetric cryptosystem	Original drop image	0.8897	0.8617	0.8036
	Encrypted drop image	0.1041	0.2101	0.0351
	Decrypted drop image	0.8827	0.8619	0.8045

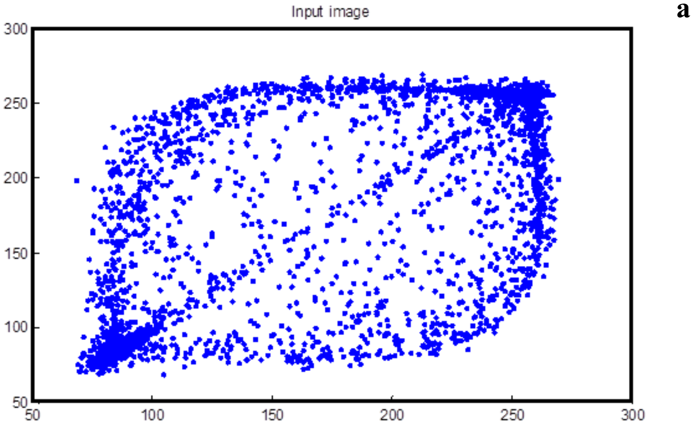

Fig. 9. CC curve for grayscale drop image: (**a**) input image and (**b**) encrypted image.

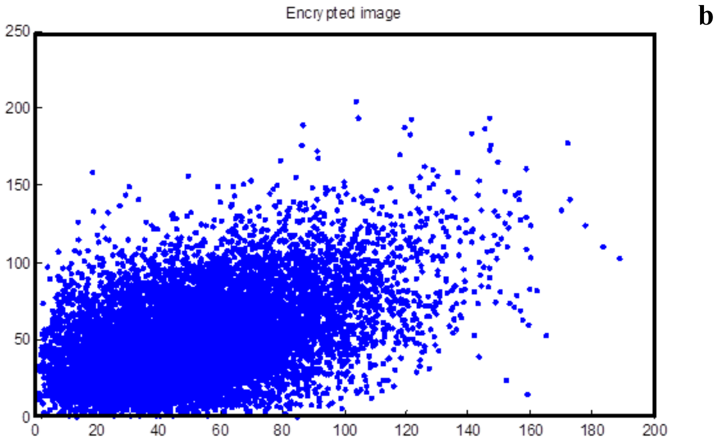

Fig. 9. Continued.

As a result, an attacker cannot obtain reliable information from these statistical data. Correlation distribution of input image and its ciphered image is shown in Figures 9**a** and 9**b**, respectively. The dense portion of scattering of pixels in the encrypted part of graph depicts a good algorithm.

5.2. Histogram study

Histogram is one of the most significant topographies of image authentication. It has been done on provided image encoding system. The encrypted scheme ought to be capable to convert the plain image into ciphered image and the histograms of plain images are dissimilar for both original and ciphered. Different histograms of encoded images yield a good, ciphered process and are attackproof because the attacker cannot attain valuable data from them. Figure 10 illustrates histograms of the original, ciphered, and

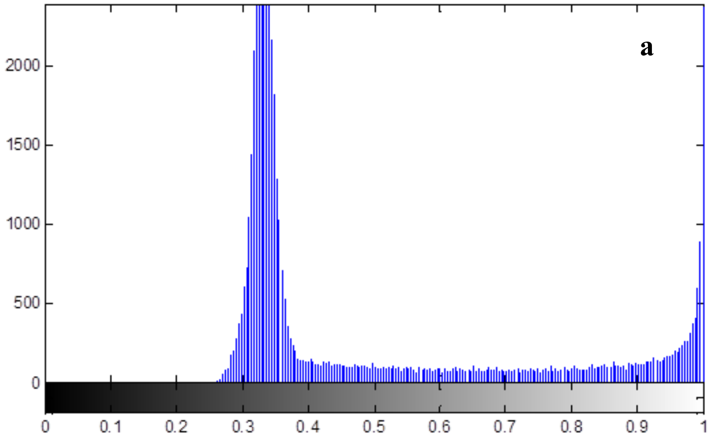

Fig. 10. Histogram of (**a**) original image, (**b**) encoded image and (**c**) decoded image.

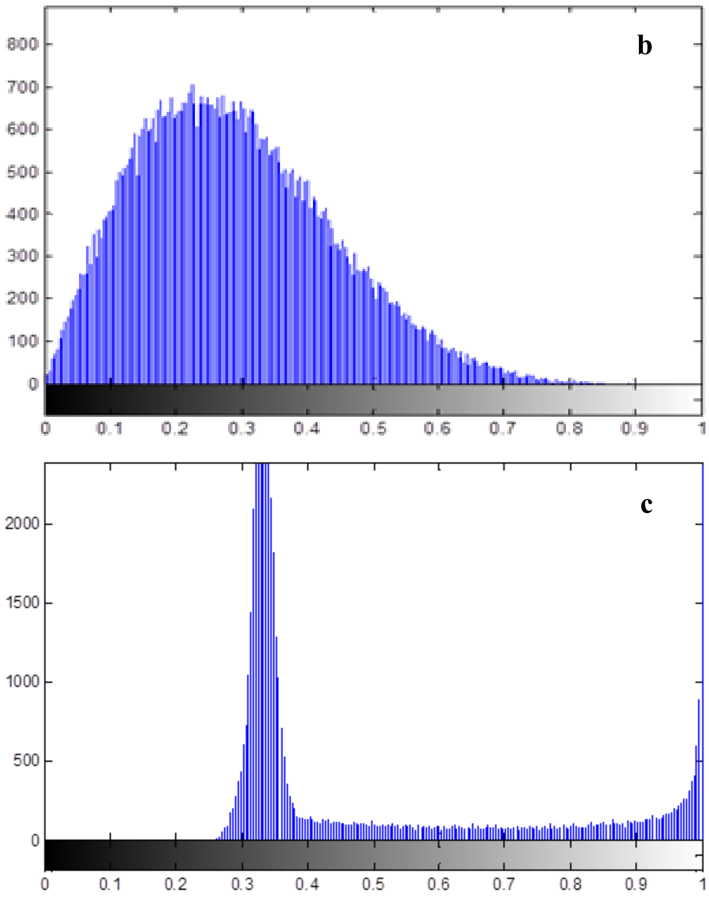

Fig. 10. Continued.

deciphered image of drop. The input image does not show any resemblance to the cipher image, hence the input image has been successfully encrypted and the similarity between input and the decrypted image clearly indicates the correct use of algorithm. Therefore, it is very difficult for a hacker to retrieve useful information from the properties of histograms.

6. Conclusion

The proposed novel asymmetric cryptographic system familiarizes non-linearity by using rear-mounted phase mask in the ciphered and deciphered path which upsurges the security of the scheme. If the image is ciphered with a fractional Fourier transform, then this increases safety and discretion of original image. Random decomposition helps in increasing the key space and security since it helps in developing two different masks P_2 and P_4, respectively. In the proposed work, a color image is decomposed into three components, *i.e.* red, green and blue. Further to avoid confusion, we have used the blue channel to procced with the algorithm. Fractional Fourier transform with asymmetric keys is used in the recommended method since these keys are unrelated to each other, *i.e.* for both encoding and decoding techniques. To achieve modest DRPE, random keys and a rear- mounted phase mask dissimilar masks are used so that it augments the key length. Simulation outcomes approves compassion of security constraints and substantiates stability for this cryptographic scheme.

Acknowledgement
The author wishes to thank the organization of The NorthCap University for their faith and inspiration that lent support throughout this effort.

References

[1] Javidi B., *Optical and Digital Techniques for Information Security*, Springer Sci. Business Media, 2005.

[2] Matoba O., Nomura T., Perez-Cabre E., Millan M.S., Javidi B., *Optical techniques for information security*, Proceedings of the IEEE **97**(6), 2009, pp. 1128–1148, DOI: 10.1109/JPROC.2009.2018367.

[3] Gong L., Qiu K., Deng C., Zhou N., *An optical image compression and encryption scheme based on compressive sensing and RSA algorithm*, Optics and Lasers in Engineering **121**, 2019, pp. 169–180, DOI: 10.1016/j.optlaseng.2019.03.006.

[4] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[5] Goodman J.W., *Introduction to Fourier Optics*, 2nd Ed., McGraw-Hill, New York, 1996.

[6] Unnikrishnan G., Singh K., *Double random fractional Fourier domain encoding for optical security*, Optical Engineering **39**(11), 2000, pp. 2853–2859, DOI: 10.1117/1.1313498.

[7] Rajput S.K., Nishchal N.K., *Image encryption based on interference that uses fractional Fourier domain asymmetric keys*, Applied Optics **51**(10), 2012, pp. 1446–1452, DOI: 10.1364/AO.51.001446.

[8] Dahiya M., Sukhija S., Singh H., *Image encryption using quad phase masks in fractional Fourier domain and case study*, IEEE International Advance Computing Conference (IACC), 2014, pp. 1048 –1053, DOI: 10.1109/IAdCC.2014.6779470.

[9] Maan P., Singh H., *Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain*, 3D Research **9**, 2018, article 53, DOI: 10.1007/s13319-018-0205-8.

[10] Hennelly B.M., Sheridan J.T., *Random phase and jigsaw encryption in the Fresnel domain*, Optical Engineering **43**(10), 2004, DOI: 10.1117/1.1790502.

[11] Situ G., Zhang J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586, DOI: 10.1364/OL.29.001584.

[12] Rajput S.K., Nishchal N.K., *Fresnel domain nonlinear optical encryption scheme based on Gerchberg-Saxton phase-retreival algorithm*, Applied Optics **53**(3), 2014, pp. 418–425, DOI: 10.1364/AO.53.000418.

[13] Singh H., Yadav A.K., Vashisth S., Singh K., *Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain*, International Journal of Optics, Vol. 2015, 2015, article 926135, DOI: 10.1155/2015/926135.

[14] Rodrigo J.A., Alieva T., Calvo M.L., *Gyrator transform: properties and applications*, Optics Express **15**(5), 2007, pp. 2190–2203, DOI: 10.1364/OE.15.002190.

[15] Rodrigo J.A., Alieva T., Calvo M.L., *Applications of gyrator transform for image processing*, Optics Communications **278**(2), 2007, pp. 279–284, DOI: 10.1016/j.optcom.2007.06.023.

[16] Pei S.C., Ding J.J., *Properties, digital implementation, applications and self image phenomena of the gyrator transform*, Proceedings 17th European Signal Processing Conference (EURASIP), 2009, pp. 441–445.

[17] Zhou N.R., Wang Y., Gong L., *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242, DOI: 10.1016/j.optcom.2011.02.065.

[18] Vashisth S., Singh H., Yadav A.K., Singh K., *Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform*, International Journal of Optics, Vol. 2017, 2014, article 728056, DOI: 10.1155/2014/728056.

[19] Singh H., *Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain*, IET Image Processing **12**(11), 2018, pp. 1994–2001, DOI: 10.1049/iet-ipr.2018.5399.

[20] Zhou N.R., Huang L.X., Gong L.H., Zeng Q.W., *Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map*, Quantum Information Processing **19**, 2020, article 284, DOI: 10.1007/s11128-020-02794-3.

[21] Ye H.S., Zhou N.R., Gong L.H., *Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion*, Signal Processing **175**, 2020, article 107652, DOI: 10.1016/j.sigpro.2020.107652.

[22] Hartley R.V.L., *A more symmetrical fourier analysis applied to transmission problems*, Proceedings of the IRE **30**(3), 1942, pp. 144–150, DOI: 10.1109/JRPROC.1942.234333.

[23] Carnicer A., Montes-Usategui M., Arcos S., Juvells I., *Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005, pp. 1644–1646, DOI: 10.1364/OL.30.001644.

[24] Frauel Y., Castro A., Naughton T.J., Javidi B., *Resistance of the double random phase encryption against various attacks*, Optics Express **15**(16), 2007, pp. 10253–10265, DOI: 10.1364/OE.15.010253.

[25] 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, pp. 1044–1046, DOI: 10.1364/OL.31.001044.

[26] Rajput S.K., Nishchal N.K., *Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem*, Optics Communications **309**, 2013, pp. 231–235, DOI: 10.1016/j.optcom.2013.06.036.

[27] Qin W., Peng X., *Asymmetric cryptosystem based on phase truncated Fourier transforms*, Optics Letters **35**(2), 2010, pp. 118–120, DOI: 10.1364/OL.35.000118.

[28] Huang Z. J., Cheng S., Gong L.H., Zhou N.R., *Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform*, Optics and Lasers in Engineering **124**, 2020, article 105821, DOI: 10.1016/j.optlaseng.2019.105821.

[29] Singh H., *Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase -truncated in gyrator wavelet transform domain*, Optics and Lasers in Engineering **81**, 2016, pp. 125 –139, DOI: 10.1016/j.optlaseng.2016.01.014.

[30] Rajput S.K., Nishchal N.K., *Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask*, Applied Optics **51**(22), 2012, pp. 5377–5786, DOI: 10.1364/AO.51.005377.

[31] Khurana M., Singh H., *An asymmetric image encryption based on phase truncated hybrid transform*, 3D Research **8**, 2017, article 28, DOI: 10.1007/s13319-017-0137-8.

[32] Girija R., Singh H., *Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform*, 3D Research **9**, 2018, article 42, DOI: 10.1007/s13319-018-0192-9.

[33] Yadav P.L., Singh H., *Optical asymmetric cryptosystem centered on fractional Fourier domain using Hilbert phase mask*, International Conference on Computing and Communication Technologies for Smart Nation (IC3TCN), IEEE, 2017, pp. 173–178, DOI: 10.1109/IC3TSN.2017.8284471.

[34] 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, pp. 679–686, DOI: 10.1364/AO.55.000679.

[35] Xu H., Xu W., Wang S., Wu S., *Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain*, Optics Communications **402**, 2017, pp. 302–310, DOI: 10.1016/j.optcom.2017.05.035.

[36] 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, pp. 1245–1252, DOI: 10.1080/09500340.2018.1431314.

[37] 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, article 163289, DOI: 10.1016/j.ijleo.2019.163289.

[38] Chen J., Zhang Y., Li J., Zhang L.B., *Security enhancement of double random phase encoding using rear-mounted phase masking*, Optics and Lasers in Engineering **101**, 2018, pp. 51–59, DOI: 10.1016/j.optlaseng.2017.09.019.

[39] Chen L., Zhao D., Ge F., *Image encryption based on singular value decomposition and Arnold transform in fractional domain*, Optics Communications **291**, 2013, pp. 98–103, DOI: 10.1016/j.optcom.2012.10.080.

[40] Girija R., Singh H., *A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition*, Optical and Quantum Electronics **50**, 2018, article 210, DOI: 10.1007/s11082-018-1472-6.

[41] Singh P., Yadav A.K., Singh K., *Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition*, Optics and Lasers in Engineering **91**, 2017, pp. 187–195, DOI: 10.1016/j.optlaseng.2016.11.022.

[42] Zhang S.Q., Karim M.A., *Color image encryption using double random phase encoding*, Microwave and Optical Technology Letters **21**(5), 1999, pp. 318–323, DOI: 10.1002/(SICI)1098-2760(19990605)21:5<318::AID-MOP4>3.0.CO;2-A.

[43] Joshi M., Chandrashakher, Singh K., *Color image encryption and decryption using fractional Fourier transform*, Optics Communications **279**(1), 2007, pp. 35–42, DOI: 10.1016/j.optcom.2007.07.012.

[44] Joshi M., Singh K., *Simultaneous encryption of a color and a gray-scale image using byte-level encoding based on single-channel double random-phase encoding architecture in fractional Fourier domain*, Optical Engineering **50**(4), 2011, article 047007, DOI: 10.1117/1.3569688.

[45] Singh H., *Optical cryptosystems of color images using random phase masks in fractional wavelet transform domain*, AIP Conference Proceedings **1728**, 2016, article 020063, DOI: 10.1063/1.4946114.

Received January 27, 2021
in revised form May 15, 2021