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

Anshula¹ · Hukum Singh²

Received: 10 August 2020 / Accepted: 31 March 2021 / Published online: 10 April 2021 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
An asymmetric optical cryptosystem to encrypt images using devil’s vortex Fresnel lens (DVFLs) phase masks and lower upper decomposition with partial pivoting (LUDPP) is proposed in gyrator transform domain. The proposed cryptosystem utilizes DVFLs which are the complex phase masks designed using the combination of a phases of devil’s lens, vortex lens, and Fresnel lens. LUDPP is an operation used to decompose the matrix and is utilized to supersede the phase-truncation task in the traditional phase-truncated Fourier transform (PTFT). Hence, the proposed method is immune to the attacks to which the PTFT-based cryptosystems are vulnerable. The cryptosystem is asymmetric as both the encryption and decryption processes are different along with different keys. The private keys generated during the encryption process are utilised in the decryption process to retrieve the original image. The encryption and decryption process can be realised with both the digital and the modified optical architecture. In order to show the strength and robustness of the proposed encryption, a conspire numerical simulation was performed.

Keywords Gyrator transform · Devil’s vortex Fresnel lens phase masks · Lower upper decomposition with partial pivoting

1 Introduction

Optical methods utilized in data security framework show an undeniably significant job and have drawn substantially more consideration. In the previous year’s many encoding techniques have been developed (Refregier and Javidi 1995; Matoba et al. 2009; Alfalou and Brosseau 2009; Millan and Perez-Cabre 2011; Javidi 2016; Yadav et al. 2014). Double

* Hukum Singh
hukumsingh.dhs@gmail.com

¹ Department of Computer Science and Engineering, The NorthCap University, Sector 23-A, Gurugram 122 017, India
² Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurugram 122 017, India
random phase encoding (DRPE) method suggested by Refregier and Javidi (1995) is the most operational image encoding scheme. DRPE is an efficient scheme because the information is encrypted into an unrecognized format. In DRPE, original images are multiplying by random generated phase keys using in both input-, as well as Fourier domains, RPMs serve as security keys. The decryption is back tracing the optical path, using either conjugate of encrypted image or conjugate of the RPMs. Further, DRPE based encoding method is prolonged from Fourier transform (FT) to many other domains like fractional Fourier transform (FrFT) (Unnikrishnan et al. 2000; Dahiya et al. 2014; Singh 2016a, b; Maan and Singh 2018; Girija and Singh 2018), Fresnel transform (FrT) (Situ and Zhang 2004; Singh et al. 2015a), Fresnel wavelet transform (FWT) (Singh 2016b), fractional Mellin transform (FrMT) (Zhou et al. 2011; Vashisth et al. 2014a, b; Singh 2018a), gyrator transform (GT) (Rodrigo et al. 2007; Singh et al. 2014, 2015b; Singh 2018b; Khurana and Singh 2018, 2019), gyrator wavelet transform (GWT) (Singh 2016c; Mehra et al. 2017). In all these techniques indistinguishable RPMs act as keys in the decryption process. Also, the usage of symmetric schemes exposed to attacks for example chosen-cipher attack (CCA), chosen plain attack (CPA) and known plain attack (KPA) (Carnicer et al. 2005; Peng et al. 2006a, b) because of immanent stretch, it faces problem of precondition administering and conduct. To address aforesaid matter, some dissymmetric optical cryptosystem has been proposed. Qin and Peng (2010) proposed one of the pioneer work asymmetric phase reservation (PR) and amplitude truncation (AT) technique to get the better of the non-linearity of symmetric routine. Since the decryption keys are differs from encryption keys; the authors (Cai et al. 2015) claimed that EMD-based cryptosystem is nonlinear. Further, Chen et al. (2019) proposed an asymmetric encryption and compression method for a color image based on compressed sensing and equal modulus decomposition in the discrete random transform domain. In 2020, Abdelfattah et al. (2020) proposed a compact optical asymmetric encryption system for multicolor images without contours based on unequal modulus decomposition (UMD) in the GT domain. Asymmetric optical cryptosystem using lower upper (LU) decomposition is proposed in light of FrFT (Kumar et al. 2018), an asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain (Rakheja et al. 2020), a single-channel color information security system using LU decomposition in GT domain (Abuturab 2014). Further the cryptosystem is extended to use LUDPP (Xiong and Quan 2019). Ren et al. (2018) proposed an asymmetric image encryption scheme using a phase-truncated discrete multiple-parameter fractional Fourier transform (PTDMPFRFT). They used decryption keys in the system can generated during the encryption method, but differ from encryption keys. The decryption keys include the phase key, pixel-scrambling operation, and a set of PTDMPFRFT parameters. The security of the asymmetric cryptosystem can be enhanced using their scheme and also enlarge the key space. Chen et al. (2018) proposed an asymmetric multi-image encryption system based on compressed sensing and feature fusion. The method has advantages such as feature fusion, high frequency information, high quality of the decrypted images can be recovered. By using the PT and PR to encrypt the fused image, it is clearly realized that the asymmetric encryption algorithm makes us manage the keys safely. The main secret keys generated in the proposed encryption scheme are associated with the plain images, which can resist the various attacks. Wang et al. (2013) presented an asymmetric approach to hide multiple images in a host using nonlinear amplitude- and phase-truncation in FrFT domain. This method also offers multi-levels of security for multiple images. The decryption keys used in the system are generated during encryption process but different from the encryption keys. Mehra et al. (2013)
proposed a collision attack applied to an asymmetric cryptosystem. The scheme uses the amplitude and phase-truncation approach in a FrT and also uses diffractive optical elements as keys instead of the conventional RPMs. The modified G-S phase retrieval algorithm is used for generating the decryption keys. With the help of these keys, they are able to retrieve the collision image, instead of the original input image, and prove that asymmetric cryptosystem based on PTFT is not resistant to collision.

None of the aforementioned technique uses the novel DVFL masks in GT domain using LUDPP. The motivation behind this paper is LU decomposition with partial pivoting. The use of GT has advantages such as computational alleviate and convenience in their optical execution. The proposed scheme provides enhanced security by increasing the key space through the use of DVFL. Such phase masks are uncomplicated to location in the decoding and provide own centering masks. They have the properties of multiple keys in a single mask which provide extra security parameters. LUDPP technique is further used to achieve the private keys that are used in the decryption process. The public keys used are the two DVFLs that are designed using the combination of devils lens (DL), vortex mask (VM), and fresnel mask (FM). The designed asymmetric cryptosystem is capable of enduring basic attacks on PTFT and is much secure and robust. Numerical simulations have been done for this system to prove the level of security.

This article is composed as follows: Sect. 2 provides complete theoretical background for our proposed approach. Section 3 describes the proposed cryptosystem. Section 4 gives the simulation analysis to evaluate the security level through statistical analyses, attack analyses. Section 5 represents the comparison with other related work. Finally, conclusions are made in Sect. 6.

2 Theoretical background

2.1 The GT

The GT of a two-dimensional function \( f(x, y) \) is written (Rodrigo et al. 2007; Singh et al. 2014, 2015b; Singh 2018b; Khurana and Singh 2018, 2019) as,

\[
G(u, v) = G^a \{ f(x, y) \} (u, v) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x, y) K_a(x, y, u, v) \, dx \, dy
\]

(1)

where the kernel is defined as

\[
K_a(x, y, u, v) = \frac{1}{|\sin \alpha|} \exp \left[ 2i\pi \frac{(xy_i + uv) \cos \alpha - x_jv - y_ju}{\sin \alpha} \right]
\]

(2)

Here \( \alpha \) is the transform angle and \( G(u, v) \) is the output of the GT. When \( \alpha = 0 \), it corresponds to the identity transform. For \( \alpha = \pm \frac{\pi}{2} \), the GT reduces to a Fourier transform/ inverse Fourier transform with the rotation of the coordinates \( (u, v) \). The inverse transform of \( G^a \) is expressed as \( G^{-a} \) or \( G^{2\pi-a} \). The GT can be realized by an optimized flexible optical system having plano-convex cylindrical lenses with fixed distance between them. The angle \( \alpha \) is changed by proper rotation of these lenses.

The main properties of the GT, which will be used below in the following sections, are
where \( x_0, y_0, u_0 \) and \( v_0 \) are real constants.

### 2.2 DVFL-based phase mask

A phase mask based on devil’s lens can be described by one-dimensional cantor function (CF), a particular case of devil’s staircase. For some basic values of \( s \), the values of \( q_s, l \) and \( p_s, l + 1 \) are provided in references (Furlan et al. 2009, 2010; Calatayud et al. 2009, 2012; Barrera et al. 2012; Mitry et al. 2012; Calabuig et al. 2013; Yadav et al. 2015). A triadic cantor set in the interval \([0, 1]\) can be defined as

\[
F_s(x) = \begin{cases} 
\frac{1}{2} & \text{if } p_{s,j} \leq x < q_{s,j} \\
\frac{x-q_{s,j}}{p_{s,j+1}-q_{s,j}} + \frac{1}{2} & \text{if } q_{s,j} \leq x \leq p_{s,j+1}
\end{cases}
\]  

A DVFL-based phase mask is obtained by taking the product of the three functions \( D_s(\xi), V_m(\theta) \) and \( L_{s,f_0}(\xi) \) as follows:

\[
(DVFL)_{s,f_0} = e^{i\left(-2^{s+1}xF_s + m\theta - \frac{\sin^2 \theta}{f_0}\right)}
\]  

where a devil’s mask is a circularly symmetric pure phase diffractive optical element and is defined as

\[
D_{s}(\xi) = e^{(-2^{s+1}xF_s)}
\]  

where \( \xi = \left(\frac{\xi}{a}\right)^2 \) is the normalised quadratic radial coordinate and \( a \) is the lens radius.

The vortex mask (VM) is expressed in terms of a vortex function as

\[
V_m(\theta) = e^{(jm\theta)}
\]  

And Fresnel lens, the toroidal lens is based on quadratic phase change and is given by

\[
L_{s,f_0}(\xi) = e^{\left(-\frac{\sin^2 \theta}{f_0}\right)}
\]  

where \( f_0 \) is the focal length and \( \lambda \) is the wavelength of incident light.

A plot of DVFL, which is a combination of Devil’s lens (DL), a vortex lens (VL), and Fresnel lens (FL) is shown in Fig. 1.

### 2.3 Principle of LUDPP

In the proposed work, we can decompose a square matrix \( B \) which has dimension \( n \times n \) into lower, upper triangle matrices and a permutation matrix by using the process LUDPP given by
Fig. 1  a Fresnel mask,  b vortex mask for \( m = 15 \),  c DVFL for \( s = 2, m = 7 \),  d DVFL for \( s = 3, m = 7 \),  e DVFL for \( s = 2, m = -15 \),  f DVFL for \( s = 3, m = -15 \),  g DVFL for \( s = 2, m = 35 \),  h DVFL for \( s = 3, m = 35 \)
where $L$ is a lower triangle matrix having entries of elements below the diagonal whereas diagonal is consisting of ones, $U$ signifies an upper triangle matrix having entries of elements above the diagonal with diagonal elements of ones and $P$ is a permutation matrix. The size of the matrix is $256 \times 256$. The permutation matrix is consisting of 0’s and 1’s that is for each multiplying the matrix $B$ does the essential row exchange. $B$ is a matrix that must be decomposed. The 1st row is changed with another row if the first element of a matrix $B$ is equal to 0. In matrix $B$, the permutation matrix $P$ is an identity matrix if there is no exchange in the row. As we know from the group of permutation matrix that $P$ is a non-singular matrix and the corresponding inverse matrix exist. Algebraic features from an image are extract by using LUDPP. Hence, an image $I$ that has to decomposed can be expressed as (Xiong and Quan 2019):

$$I = P^{-1} \times L \times U$$

Here $P^{-1}$ indicates an inverse matrix of a permutation matrix i.e. $P$. The LUDPP procedure has benefited over LUD in two ways, the first one is that the problem of a matrix in which a diagonal coefficient of a matrix that is equal to 0 is reduced by the suggested lower upper decomposition with pivoting which will help in decomposing the intensity matrices of binary images as compared to conventional LUD which fail to work on it and the second one is that the LUDPP can be used as a decomposition factor for singular matrix and with the help of partial pivoting we can decrease rotating error and advance calculation correctness. A testing has been done to achieve LUDPP on the original image (baboon) as well as on the binary image (DH) and the outcomes are shown in Fig. 2. Figure 2a is the lower triangular matrix of original image baboon, Fig. 2b is upper triangular matrix of original baboon image. Similarly for binary text image (DH) Fig. 2c is partial pivoted matrices, Fig. 2d is the upper triangular matrix of binary image (DH).

### 3 Overview of encryption and decryption

Flow chart for encryption process of the proposed system is given in Fig. 3. $I_1(x, y)$ is the first input image that we are going to encrypt, $(x, y)$ represents the indices of the input plane and $(u, v)$ represents the indices of the transform plane. DVFL ($s = 2$) and DVFL($s = 3$) are the two DVFLs phase masks that are the main keys for the encryption process. The encryption is carried out as explained below:

**Step 1** Firstly, the input image $I_1(x, y)$ is multiplied with the first mask DVFL($s = 2$). A GT is performed on the $I_1(x, y) \times$ DVFL and then the transform spectrum is divided using LUDPP. This operation outputs the first private key Key 1 and generates the intermediate output $g_1(u, v)$ represented using the equations below:

$$[L_1, U_1, P_1] = \text{LUDPP} \{ \text{GT}^a[I_1(x, y) \times \text{DVFL}(s = 2)] \}$$

Private key Key 1 = $L_1U_1$

$$g_1(u, v) = P_1^{-1}(u, v)$$
Fig. 2 Decomposition of gray scale original baboon image a, b is the lower and upper triangular matrices of baboon, c is partial pivoted matrices, d is the upper triangular matrix of binary image (DH)

Fig. 3 Flowchart of encryption scheme
where \( LUDPP\{\cdot}\) express the lower upper decomposition with partial pivoting, \( L_1, U_1 \) and \( P_1 \) are the three products of first LUDPP operation, \( GT\{\cdot\} \) expresses the gyrator transform, \( \times \) represents the matrix multiplication operation, \( \{\cdot\}^{-1} \) denotes the inverse matrix operation.

**Step 2** The intermediate output \( g_1(u, v) \) is then multiplied by second mask \( DVFL(s = 3) \). The inverse gyrator transform \( GT(\beta) \) is applied on this resultant followed by second LUDPP which gives the output as second private key Key 2 and the final cipher image denoted by \( C(x, y) \). The equations are given below:

\[
\begin{align*}
[L_2, U_2, P_2] &= LUDPP \{GT^{-\beta}[g_1(u, v) \times DVFL(s = 3)]\} \\
\text{Private key Key 2} &= L_2 U_2 \\
C_1(x, y) &= P_2^{-1}(x, y)
\end{align*}
\]

where \( L_2, U_2 \) and \( P_2 \) are the three products of second LUDPP operation. The use of inverse matrix of the two permutation matrix in the proposed scheme.

**Step 3** For second binary input image \( I_2(x, y) \) is multiplied with the first mask \( DVFL(s = 2) \). A GT is performed on the \( I_2(x, y) \times DVFL \) and then the transform spectrum is divided using LUDPP. This operation outputs the third private key Key 3 and generates the intermediate output \( g_2(u, v) \) represented using the equations below:

\[
\begin{align*}
[L_3, U_3, P_3] &= LUDPP \{GT^{\alpha}[I_2(x, y) \times DVFL(s = 2)]\} \\
\text{Private key Key 3} &= L_3 U_3 \\
g_2(u, v) &= P_3^{-1}(u, v)
\end{align*}
\]

where \( LUDPP\{\cdot\} \) express the lower upper decomposition with partial pivoting, \( L_3, U_3 \) and \( P_3 \) are the three products of first LUDPP operation.

**Step 4** The intermediate output \( g_2(u, v) \) is then multiplied by second mask \( DVFL(s = 3) \). The inverse \( GT(-\beta) \) is applied on this resultant followed by second LUDPP which gives the output as fourth private key Key 4 and the final cipher image denoted by \( C_2(x, y) \). The equations are given below:

\[
\begin{align*}
[L_4, U_4, P_4] &= LUDPP \{GT^{-\beta}[g_2(u, v) \times DVFL(s = 3)]\} \\
\text{Private key Key 4} &= L_4 U_4 \\
C_2(x, y) &= P_4^{-1}(x, y)
\end{align*}
\]

where \( L_4, U_4 \) and \( P_4 \) are the three products of second LUDPP operation. The use of inverse matrix of the two permutation matrix in the proposed scheme.

This is the complete process of encryption which generates four private key namely, Private key Key 1, Private key Key 2, Private key Key 3 and Private key Key 4 which will be used in the decryption process.
The decryption algorithm is not similar to encryption one as the system we proposed is the asymmetric one. The process of decryption Fig. 4 is carried out as follows when we have the two private keys generated during the encryption step:

**Step 1**
The cipher image $C_1(x, y)$ that we get as final output of encryption process is taken as an input during the decryption process. Firstly, it is multiplied with the private key $Key_3$ and the resultant function is then subjected to GT ($\alpha$). The result of this transformation can be represented as $g(u, v)$ calling it an intermediate matrix given by:

$$g(u, v) = \text{abs}\{\text{GT}^\alpha[C_1(x, y) \text{ Private Key 3}]\} \quad (25)$$

where $\text{abs}\{\cdot\}$ defines the amplitude part extraction of a complex function.

**Step 2**
To obtain the final decrypted image, we multiplex the intermediate matrix $g(u, v)$ with the private key $Key_1$ and then subject it to the inverse gyrator transform. The decrypted image can be given by

$$I_1(x, y) = \text{abs}\{\text{GT}^{-\beta}[g(u, v) \text{ Private Key 1}]\} \quad (26)$$

**Step 3**
The cipher image $C_2(x, y)$ that we get as final output of encryption process is taken as an input during the decryption process. Firstly, it is multiplied with the private key $Key_4$ and the resultant function is then subjected to GT ($\alpha$). The result of this transformation can be represented as $g'(u, v)$ calling it an intermediate matrix given by:

$$g'(u, v) = \text{abs}\{\text{GT}^\alpha[C_2(x, y) \text{ Private Key 4}]\} \quad (27)$$

where $\text{abs}\{\cdot\}$ defines the amplitude part extraction of a complex function.

**Step 4**
To obtain the final decrypted image, we multiplex the intermediate matrix $g'(u, v)$ with the private key $Key_2$ and then subject it to the inverse GT. The decrypted image can be given by

$$I_2(x, y) = \text{abs}\{\text{GT}^{-\beta}[g'(u, v) \text{ Private Key 2}]\} \quad (28)$$

In the encryption process, the arrangement matrix $P^{-1}$ inverse is taken and reproduce as the midway result or the concluding cipher image, which has duplet of interest. Firstly, $P^{-1}$ is a sparse matrix which means its most of the elements are zero. This property makes the cipher text resistant to iterative attack based on amplitude phase retrieval technique despite

![Flowchart of decryption](image-url)
the fact that the attacker knows the original ciphertext. Thus, it will be a challenging task to recover the plaintext from the known ciphertext with no information of private keys. It makes the cryptosystem more secure and robust. Furthermore, $P^{-1}$ is a matrix having real values which make it easy to be directly recorded by charged coupled device (CCD). Thus, no hologram technique is needed to acquire the ciphertext. Hence, the proposed scheme is simple yet secure. As seen, the encryption keys (public keys) are different from the two recorded private keys (Key1 and Key 2) and the process of encryption and decryption are also different as shown in Figs. 3 and 4. Thus, it can be said that the above proposed cryptosystem is asymmetric in nature.

An optoelectronic experimental set-up of the proposed encryption scheme is appeared in Fig. 5a. In encryption, the image $f(x, y)$ and DVFL$(s = 2)$ are first displayed on phase only spatial light-modulator (PO-SLM) associated with the machine and lit up by a He–Ne laser source ($\lambda = 632.8$ nm). GT order ($\alpha$) is performed optically. Resulting spectrum and DVFL$(s = 3)$ are displayed on to second PO-SLM$_2$, which is additionally connected with computer and after that performing an inverse GT. The resultant spectrum is recorded by the CCD camera and stored in the computer system. The phase truncated part may be made by CCD. The amplitude truncated part may be done by phase-shifting interferometry. In decryption process Fig. 5b, the digitally acquired image $E(x, y)$ is multiplied with asymmetric private key Key 1 is displayed on PO-SLM$_1$ irradiated with a laser source, and then subjected Inverse GT through, then information is displayed on SLM$_2$ is associated with computer and intensity of decrypted image is recorded in the output plane. Thus, to regulate both the amplitude and phase information two SLMs, SLM$_1$ and SLM$_2$ are utilised. PC is the personal computer used to carry out the matrix multiplication, such as $c \times$ Key2 and $g \times$ Key1. The final decrypted image is acquired using a CCD.

4 Simulation and evaluation

The effectiveness and feasibility of the presented technique has been checked by carrying out various numerical simulations and analysis. The scheme has been tested against the speed by executing the scheme on personal computer with configuration Intel(R) Core (TM) i3-2328 CPU @ 2.20–2.71 GHz, 2 GB RAM running Windows 10 on MATLAB R2019a 5(9.6.0.0.1174912) 64-bit (win64), LM: 40664749. Two grayscale images baboon and DH shown in Fig. 6a, b having size $256 \times 256$ are taken as the input images to be encrypted using the proposed technique. Figure 6c, d shows the first set of private keys generated for both the input images employing the proposed algorithm and Fig. 6e, f shows the second set of private keys respectively for baboon and DH images. The final encrypted images are depicted in Fig. 6g, h when we apply the encryption process. When we correctly go through the decryption process with right set of decryption keys we get the decrypted images can be obtained which are similar to the original input images.

4.1 Statistical analyses

To figure out the authenticity and strength of the proposed technique, mean square error (MSE) and peak signal to noise ratio (PSNR) has been calculated for the decrypted image $I'(x, y)$ and the original image $I(x, y)$.
where \( N \times N \) represents the size of the image.

\[
\text{MSE}(I'(x, y), I(x, y)) = \sum_{x=1}^{N} \sum_{y=1}^{N} \frac{|I'(x, y) - I(x, y)|^2}{N \times N} \quad (29)
\]

\[
\text{PSNR} = 10 \times \log_{10} \left( \frac{(N - 1)^2}{\text{MSE}} \right) \quad (30)
\]
Fig. 6  a, b are two input images, c–f are four private keys, g, h are two encrypted images
where $N$ respresents the maximum number of pixels in the original and decrypted images. Here the value of $N$ is 256 as the size of images are $256 \times 256$.

Structural Similarity Index (SSIM) is used for measuring quality of an original input image with reference to the recovered image. SSIM value of one, defines recovery of high-quality image. The value of SSIM can vary between $-1$ to $1$. Greater the value more is the similarity and can be calculated using following formula

$$
SSIM (I, I') = \frac{(2\mu_I\mu_{I'} + c_1)(2\text{ covariance} + c_2)}{\left(\mu_I^2 + \mu_{I'}^2 + c_1\right)\left(\nu_I^2 + \nu_{I'}^2 + c_2\right)}
$$

where $c_1$ and $c_2$ are variable to stabilize the division, $\mu_i$ and $\mu_{i'}$, $\nu_i^2$ and $\nu_{i'}^2$ are the average and variance of $I$ and $I'$ respectively.

The calculate value of MSE for baboon image is $1.98 \times e^{-25}$ and for DH image is $5.56 \times e^{-24}$. PSNR value for Baboon image is 295.16 dB and for DH image is 280.68 dB. Lower the value of MSE and higher the value of PSNR represents the competency of the proposed method.

### 4.1.1 3-dimensional(3D) analysis

3D surface plot analysis of the proposed scheme is computed. Figure 7 illustrate that the 3D surface plots of input images (baboon, pepper and DH) are reflected in different in nature, but their encrypted plots are almost similar. So basis of encrypted plot it is very difficult to attacker to identify the images.

### 4.1.2 Entropy analysis

Entropy $H$ can be represented as (Girija and Singh 2019a, b)

$$
H = - \sum_{i=1}^{M} p_i \log_2 p_i
$$

where $p_i$ represents the probability. The ideal entropy is 8. The entropies obtained for cipher image of baboon and DH images using proposed algorithm are 7.150 and 7.352 respectively. Both these values are near about the ideal value, then the loss is insignificant, and the suggested algorithm is strong against the entropy attack.

### 4.1.3 Statistical analysis

In order to check the performance of the scheme the statistical terms CC, SSIM, MSE and PSNR have been computed for four images: baboon, pepper, DH and Lena. Table 1 shows the values of these parameters for between input and their encrypted images.

### 4.1.4 Compression ratio

For statistical evaluation the compression ratio is also computed by the relation
Compression ratio for the proposed scheme is

\[
\text{Compression ratio} = \frac{\text{Number of pixels/\text{bits per pixel}}_{\text{input}}}{\text{Number of pixels/\text{bits per pixel}}_{\text{compressed}}} \quad (33)
\]

Compression ratio for the proposed scheme is

![Fig. 7  a–c 3D plot of input images, d–f 3D plots of encrypted images](image)
Figure 8 manifest the compression ratio in opposition to distinct proportions of input images which also endorse the success of the compression term as with the image size compression ratio surpass. As seen from Fig. 8 for image of size 1024 × 1024 the compression ratio attain is 511.50 which is fairly exceptional.

4.2 security analysis

4.2.1 key sensitivity test

The image encryption technique desirable to sensitive towards the initial values of a secret key. To obtain the sensitivity analysis of an image encryption technique, take incorrect parameters. The correct parameters, \(\alpha = 0.7\pi, \beta = 0.9\pi\) as the rotation angles of GT. Four decrypting keys (Private key Key-1, Private key Key-2, Private key Key-3 and Private key Key-4) are generated during encryption process. The responsiveness of the architecture has also been substantiating against each individual parameter. The retrieved images for erroneous values are shown in Fig. 9a–c correspond to decrypted

\[
\text{Compression ratio} = \frac{65,536}{514} = 127.502
\]  

(34)

Table 1 CC, SSIM, MSE and PSNR between for input and encrypted image

| S. no | Image | CC     | SSIM   | MSE       | PSNR (dB) |
|-------|-------|--------|--------|-----------|-----------|
| 1     | Baboon| 0.0775 | 0.7996 | 3.82×10^6 | -17.70    |
| 2     | Pepper| 0.0707 | 0.7985 | 3.97×10^6 | -17.85    |
| 3     | DH    | 0.0814 | 0.7985 | 4.94×10^4 | 1.19      |
| 4     | Lena  | 0.0820 | 0.7985 | 4.35×10^6 | -18.26    |

Fig. 8 Input image size vs compression ratio plot
image of baboon with incorrect keys (Private key Key-1, Private key Key-2, Private key Key-3) while Private key Key-4 is correct key. Figure 9d–f are decrypted image baboon with using incorrect three decrypting keys (Private key Key-1, Private key Key-2, and Private key Key-4).
Figure 9g–i are decrypted image using another three wrong parameter of keys Private key Key-1, Private key Key-3 and Private key Key-4 Fig. 9j–l with wrong values of keys (Private key Key-2, Private key Key-3 and Private key Key-4. Figure 10a, b are MSE plot with first GT rotangle $\alpha = 0.7\pi$, combination of baboon, pepper and DH images, while Fig. 10c is another graph between PSNR with rotation angle for second GT. Figure 10d is another plot MSE with, GT rotation angle $\beta = 0.9\pi$ as a number of iterations. The graphs clearly reflects that the scheme is highly sensitive to the GT rotation angle.

4.3 Attack analysis

The attack analysis of the suggested scheme constitute of occusion attack and noise attacks analysis.

4.3.1 Occlusion attack analysis

Occlusion attack analysis has been done for the encrypted images. As we know, the greater parts of the occlusion examination are done uniquely for encrypted images in the past. The occlusion examination for encrypted images only proves the toughness of the cryptosystem while if it is done for the newly developed devil’s vortex Fresnel phase mask, it...

![MSE plots](image1.png)

![MSE plots](image2.png)

![PSNR plots](image3.png)

![MSE plots](image4.png)

**Fig. 10** a, b MSE plot with rotation angle $\alpha = 0.7\pi$ for baboon, pepper and DH images, c, d PSNR, MSE plots against the rotation angle and number of iterations
confirms the stability and robustness of the cryptosystem. Few portions of ciphered images are occluded in Fig. 11, and examinations are done on decrypted ones. 10% occluded ciphered images are shown in Fig. 11a for baboon and 25% occluded in Fig. 11b for peppers. Similarly, 50%, 75% occluded encrypted images for baboon and Peppers are shown in Fig. 11c, d. Figure 12a, b MSE and CC plots with varying occluded area of baboon and DH, c, d MSE and CC plots with varying occluded area of baboon and pepper respectively.
4.3.2 Noise attack analysis

The ciphered image at the stage of image processing and image transmission is susceptible to different kinds of noise. These noises have a great influence on the quality of the decryption images. In this work we have added Gaussian noise to the encoded image. The noise interferes with the ciphered images by relation (Singh 2017; Yadav and Singh 2018).

\[
\mu'(\rho, \sigma) = \mu(u, v) + kG
\]  

(35)

where \( \mu(u, v) \) is encrypted picture and \( \mu'(\rho, \sigma) \) is the noised image, \( k \) is a constant.

factor and \( G \) is a Gaussian noise with 0 and 1 standard deviation. The Fig. 13a, b shows the MSE plot with varying noise factor (k) data distorted by Gaussian noise with standard deviations of 0.02. It is entirely evident from the proposed scheme that it can be hold out against Gaussian noise to great extent the help of basic median filtering technique.

5 Performance comparison

The comparison of performance of the proposed algorithm with some of the widely known image encryption algorithms has been done based on various parameters. Table 2 shows the comparison and strengthens the fact that the performance of the proposed scheme.

![Mean square error plots](a) (b)

Fig. 13 a, b MSE plot against varying noise factor(k) effect of noise on baboon, DH and baboon, pepper images respectively
| Parameters                              | DRPE with Gyrator transform (Rodrigo et al. 2007) | LUD with fractional Fourier transform (Kumar et al. 2018) | LUD with partial pivoting and two random phase mask (Xiong and Quan 2019) | Proposed technique with PPLUD, DVFL using GT |
|----------------------------------------|---------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------|---------------------------------------------|
| Transform used                         | Gyrator transform                                 | Fractional Fourier transform                           | Fourier transform                                                      | Gyrator transform                           |
| Applied technique                      | Optical and digital                               | Optical and digital                                    | Optical and digital                                                    | Optical and digital                         |
| Number of diffusers                    | 2 RPM                                             | 2 RPM                                                  | 2 RPM                                                                  | 2 DVFLs                                     |
| Number of Security parameters          | 1 Rotational Angle                                | 2 fractional orders                                   | Nil                                                                    | 2 rotational angle of GT, \( f, r, \lambda, m \), 4 private keys |
| Execution time (s)                     | 0.2018                                            | 0.3139                                                 | 0.3710                                                                 | 0.3946                                      |
| Strength                               | Low complexity and fast                           | Low Complexity but addition of two security parameter by use of FRT | Several attack free cryptosystem, PT process is replaced by partial pivoting | Enhanced security potential by using DVFLs, additional parameters of rotation angle of gyrator transform, and robustness against attacks |
| Weakness                               | Easy to break, prone to attack                    | Susceptibility to various attacks                     | Small and simple key space                                            | A little bit more execution time            |
6 Conclusion

A DVFL mask along with lower upper decomposition with partial pivoting in gyrator transform domain has been utilised in the designing of the asymmetric cryptosystem. The main goal of the proposed scheme is to provide greater security to the LUDPP based encryption technique and to make it more confidential and robust. The proposed strategy has several features; firstly it is tough due to the introduction of a secure novel devils vortex Fresnel phase mask which is difficult to realise without accurate information of all the parameters used in its construction. Secondly, it is fast and the encryption operation can be realised digitally while decryption can be performed optically. Thirdly, it is an asymmetric cryptosystem where the two devils’s are considered as public keys and the particular decryption keys are caused by LUDPP during encryption process which generates unique plain text that helps in resisting known-plaintext attack. Lastly, the cipher text matrix generated by partial pivoting is a sparse matrix which resists iterative attack as it does not provide enough constraints to make it stable. The scheme has been verified on different factors, for example, MSE, PSNR, CC, entropy to check its adequacy and strength. It has been analysed that even under distortions caused by occlusion, one is able to recuperate the original image. The key space of the presented scheme is effectively large and the simulation results confirm the robustness and efficacy of the proposed cryptosystem.

References

Abdelfattah, M., Hegazy, S.F., Areed, N.F.F., Obayya, S.S.A.: Compact optical asymmetric cryptosystem based on unequal modulus decomposition of multiple color images. Opt. Lasers Eng. 129, 106063 (2020). https://doi.org/10.1016/j.optlaseng.2020.106063

Abuturab, M.R.: Single-channel color information security system using LU decomposition in gyrator transform domains. Opt. Commun. 323, 100–109 (2014)

Alfalou, A., Brosseau, C.: Optical image compression and encryption methods. Adv. Opt. Photon. 1, 589–536 (2009)

Barrera, J.F., Tebaldi, M., Ammaya, D., Furlan, W.D., Monsoriu, J.A., Bolognini, N., Torroba, R.: Multiplexing of encrypted data using fractal masks. Opt. Lett. 37, 2895–2897 (2012)

Cai, J., Shen, X., Lei, M., Lin, C., Dou, S.: Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition. Opt. Lett. 40(4), 475–478 (2015)

Calabuig, A., Sanchez-Ruiz, S., Martinez-Leon, L., Tajahuerce, E., Fernandez-Alonso, M., Furlan, W.D., Monsoriu, J.A., Pons-Marti, A.: Generation of programmable 3D optical vortex structures through devil’s vortex-lens arrays. Appl. Opt. 52, 5822–5829 (2013)

Calatayud, A., Monsoriu, J.A., Mendoza-Yero, O., Furlan, W.D.: Polyadic devil’s lenses. J. Opt. Soc. Am. A 26, 2532–2537 (2009)

Calatayud, A., Rodrigo, J.A., Tremon, L., Furlan, W.D., Cristobal, G., Monsoriu, J.A.: Experimental generation and characterization of Devil’s vortex-lenses. Appl. Phys. B 106, 915–919 (2012)

Carnicer, A., Montes-Usategui, M., Arcos, S., Juvels, I.: Vulnerability to chosen-cypher text attacks of optical encryption schemes based on double random phase keys. Opt. Lett. 30(13), 1644–1646 (2005)

Chen, X.-D., Liu, Q., Wang, J., Wang, Q.-H.: Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality images reconstruction. Opt. Laser Technol. 107, 302–312 (2018)

Chen, X.-D., Wang, Y., Wang, J., Wang, Q.-H.: Asymmetric color cryptosystem based on compressed sensing and equal modulus decomposition in discrete fractional random transform domain. Opt. Lasers Eng. 121, 143–149 (2019)

Dahiya, M., Sukhija, S., Singh, H.: Image encryption using quad masks in fractional fourier domain and case study. In: IEEE International Advance Computing Conference (IACC), pp. 1048–1053 (2014)

Furlan, W.D., Gimenez, F., Calatayud, A., Monsoriu, J.A.: Devil’s vortex-lenses. Opt. Express 17, 21891–21896 (2009)
Furlan, W.D., Gimenez, F., Calatayud, A., Remon, L., Monsoriu, J.A.: Volumetric multiple optical traps produced by Devil’s lenses. J. Eur. Opt. Soc. Rapid Publ. 5, 100375-1/5 (2010)

Girija, R., Singh, H.: A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. Opt. Quantum Electron. 50, 210 (2018)

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, 238–257 (2019a)

Girija, R., Singh, H.: An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain. Multim. Tools Appl. 78, 1–19 (2019b)

Javidi, B., et al.: Roadmap on optical security. J. Opt. 18, 1–39 (2016)

Khurana, M., Singh, H.: Asymmetric optical image triple masking encryption based on gyror and Fresnel transforms to remove silhouette problem. 3D Res. 9, 38 (2018)

Khurana, M., Singh, H.: A spiral-phase rear mounted triple masking for secure optical image encryption based on gyror transform. Recent Patents Comput. Sci. 12(2), 80–84 (2019)

Kumar, J., Singh, P., Yadav, A.K., Kumar, A.: Asymmetric cryptosystem for phase images in fractional fourier domain using LU-decomposition and Arnold transform. Procedia Comput. Sci. 132, 1570–1577 (2018)

Maa, P., Singh, H.: Non-Linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourrier transform domain. 3D Res. 9, 53 (2018)

Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M.S., Javidi, B.: Optical techniques for information security. Proc. IEEE 97, 1128–1148 (2009)

Mehra, I., Rajput, S.K., Nishchal, N.K.: Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification. Opt. Eng. 52(2), 028202–028206 (2013)

Mehra, I., Fatima, A., Nishchal, N.K.: Gyror wavelet transform. IET Image Proc. 12(3), 432–437 (2017)

Millan, M.S., Perez-Cabre, E.: Optical data encryption, optical and digital image processing: fundamentals and applications. In: Cristobal, G., Schelkens, P., Thienpont, H. (eds.) pp. 739–767. Wiley (2011)

Mitry, M., Doughty, D.C., Chaloupka, J.L., Anderson, M.E.: Experimental realization of the devil’s vortex Fresnel lens with a programmable spatial light modulator. Appl. Opt. 51, 4103–4108 (2012)

Peng, X., Zhang, P., Wei, H., Yu, B.: Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. 31(8), 1044–1046 (2006a)

Peng, X., Wei, H., Zhang, P.: Chosen-plaintext attack on lens-less double-random phase encoding in the Fresnel domain. Opt. Lett. 31(22), 3261–3263 (2006b)

Qin, W., Peng, X.: Asymmetric cryptosystem based on phase-truncated Fourier transform. Opt. Lett. 35, 118–120 (2010)

Rakheja, P., Singh, P., Vig, R.: An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain. Opt. Lasers Eng. 134, 106177 (2020)

Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 20, 767–769 (1995)

Ren, G., Han, J., Fu, J., Shan, M.: Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform. Opt. Rev. 25, 701–707 (2018)

Rodrigo, J.A., Alieva, T., Calvo, M.L.: Gyrator transform: properties and applications. In: Cristobal, G., Schelkens, P., Thienpont, H. (eds.) pp. 739–767. Wiley (2011)

Singh, H.: Optical cryptosystem of color images based on fractional-, wavelet transform domains using random phase masks. Ind. J. Sci. Technol. 95(1), 1–15 (2016a)

Singh, H.: Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain. 3D Res. 7, 34 (2016b)

Singh, H.: Devil’s vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncated in gyror wavelet transform. Opt. Lasers Eng. 81, 125–139 (2016c)

Singh, H.: Nonlinear optical double image encryption using random-vortex in fractional Hartley transform domain. Opt. Appl. 47(4), 557–578 (2017)

Singh, H.: Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain. IET Image Proc. 12(11), 1994–2001 (2018a)

Singh, H.: Hybrid structured phase mask in frequency plane for optical double image encryption in gyror transform domain. J. Mod. Opt. 65(18), 2065–2078 (2018b)

Singh, H., Yadav, A.K., Vashisth, S., Singh, K.: Fully-phase image encryption using double random-structured phase masks in gyror domain. Appl. Opt. 53, 6472–6481 (2014)

Singh, H., Yadav, A.K., Vashisth, S., Singh, K.: Optical image encryption using devil’s vortex toroidal lens in the Fresnel transform domain. Int. J. Opt. 2015, 1–13 (2015a)

Singh, H., Yadav, A.K., Vashisth, S., Singh, K.: Double phase-image encryption using gyror transforms, and structured phase mask in the frequency plane. Opt. Lasers Eng. 67, 145–156 (2015b)
Singh, H.: Optical cryptosystem of color images using random phase masks in the fractional wavelet transform domain. In: AIP Conference on Proceedings of 1728, pp. 020063–1/4 (2016)
Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett. 49, 1584–1586 (2004)
Unnikrishnan, G., Joseph, J., Singh, K.: Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett. 25, 887–889 (2000)

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. Int. J. Opt. 2014, 1–9 (2014a)
Vashisth, S., Singh, H., Yadav, A.K., Singh, K.: Image encryption using fractional Mellin transform, structured phase filters and phase retrieval. Optik 125, 5309–5315 (2014b)

Wang, Q., Guo, Q., Lei, L.: Asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation in fractional Fourier domain. Optik 124, 3898–3902 (2013)
Xiong, Y., Quan, C.: Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting. Opt. Laser Technol. 109, 456–464 (2019)

Yadav, P.L., Singh, H.: Optical double image hiding in the fractional Hartley transform using structured phase filter and Arnold transform. 3D Res. 9, 20 (2018)
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: Proceedings of IEM Optronix, pp. 25–36. Springer (2014)
Yadav, A.K., Vashisth, S., Singh, H., Singh, K.: A phase-image watermarking scheme in gyrator domain using devil’s vortex Fresnel lens as a phase mask. Opt. Commun. 344, 172–180 (2015)
Zhou, N.R., Wang, Y., Gong, L.: Novel optical image encryption scheme based on fractional Mellin transform. Opt. Commun. 284, 3234–3242 (2011)

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