*Optica Applicata, Vol. XLVII, No. 4, 2017*
DOI: 10.5277/oa170406

# Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain

Hukum SINGH

Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurgaon-122 017, India;
e-mail: hukumsingh@ncuindia.edu, hukumsingh.dhs@gmail.com

This paper proposed an enhanced asymmetric cryptosystem scheme for optical image encryption in the fractional Hartley transform domain. Grayscale and binary images have been encrypted separately using double random phase encoding. Phase masks based on optical vortex and random phase masks have been jointly used in spatial as well as in the Fourier planes. The images to be encrypted are first multiplied by optical vortex and random phase mask and then transformed with direct and inverse fractional Hartley transform for obtaining the encrypted images. The images are recovered from their corresponding encrypted images by using the correct parameters of the fractional Hartley transform and optical vortex, whose digital implementation has been performed using MATLAB 7.6.0 (R2008a). The random phase masks, optical vortex and transform orders associated with the fractional Hartley transform are extra keys that cause difficulty to an unauthorized user. Thus, the proposed asymmetric scheme is more secure as compared to conventional techniques. The efficacy of the proposed asymmetric scheme is verified by computing the mean squared error between recovered and the original images. The sensitivity of the asymmetric scheme is also verified with encryption parameters, noise and occlusion attacks. Numerical simulation results demonstrate the effectiveness and security performance of the proposed system.

Keywords: fractional Hartley transform (FrHT), image encryption, mean squared error, noise attacks, entropy.

## 1. Introduction

An optical beam with a phase singularity is called an optical vortex that focuses to form a ring-like intensity/phase pattern. Recently, optical vortex arrays, which are regular nets of vortices, have generated an enormous interest among the many research groups [1–5]. Optical vortices represented by spiral waves that carry angular momentum are diffractive optical elements and have many applications in various fields, including quantum computing, cryptography, biophotonics and astronomy. An important component in the design of systems using optical vortices is the vortex lens or phase mask. An optical vortex is characterized by the azimuthal phase dependence of the type $\exp(il\Phi)$ where $l$ is the topological charge. The magnitude of topological charge represents the total phase accumulated by the helical wave in one complete revolution around the vortex point. These beams carry orbital angular momentum of $l\hbar$ per photon. A large number of papers are devoted to the generation of optical vortices [6–10].

In today's interconnected world, the security of information exchanged over a network is a critical issue. The safe storage and transmission of data continues to be a challenge because of increasing threats to the confidentiality and integrity of information. In the recent decades, optical processing techniques have provided effective solutions to some of these problems and therefore have become an active research field [11–17]. Optical security systems based on opto-electronics can perform highly accurate encryption and decryption in almost real time and at a high speed. The most popular technique, double random phase encoding (DRPE) was first introduced by Refregier and Javidi [11] for optical image encryption. DRPE is a widely known technique which is based on the 4-*f* optical correlator: optically symmetric-keys encrypt a given image using two random phase masks (RPMs), one in a spatial plane and the other in a frequency plane. It may be implemented optically and has a great number of applications especially in areas such as security verification systems, watermarking, information hiding, optical storage and multiple-image encryption. It is interesting to note that DRPE was further extended to several other transform domains such as the fractional Fourier [18, 19], Fresnel transform [20–22], gyrator transform [23–26], gyrator-wavelet transform [27], fractional Mellin transform [28–31] and Fresnel-wavelet transform [32] to strengthen security. Most of these encryption schemes mentioned above can be regarded as a symmetric cryptosystem, in which the decryption keys are identical to encryption keys.

In practice, however, one observes that the DRPE scheme lacks strength against specific attacks such as chosen-ciphertext attack (CCA), chosen-plaintext attack (CPA) and known-plaintext attack (KPA) due to inherent linearity. Among them, the cryptosystem based on phase-truncated Fourier transform (PTFT) plays an impressive role of eliminating the linearity in DRPE. In order to resolve this problem, Wan Qin and Xiang Peng proposed an asymmetric cryptosystem with high security by combining nonlinear PTFT, in which the decryption keys (private keys) differ from encryption keys (public keys) [33]. In this case one retains the amplitude of the Fourier while the other truncates the phase part of the spectrum. Similarly, in amplitude truncation, one retains the phase part of the spectrum, while the other truncates the amplitude part of the spectrum. Using PTFT approach, two decryption keys, namely universal keys and special keys, are generated [34]. Even for an attacker, who knows the encryption key and the corresponding ciphertext, it becomes extremely difficult to recover the input image. Some of the other asymmetric based work is noted down [35–40]. Furthermore, it is interesting to know that the use of fractional Hartley transform (FrHT) has advantages such as computational ease and convenience in its optical implementation. The proposed scheme provides enhanced security by increasing the key space, by making use of optical vortex-based structured phase mask (SPM).

The outline of this paper is as follows. Section 2 enumerates the principles of fractional Fourier transform (FrFT) and fractional Hartley transform (FrHT) and further explains process of generation of a phase mask based on optical vortex and encryption-decryption scheme. Numerical simulation results and various attacks are mentioned in Section 3. Finally, conclusions are presented in Section 4.

## 2. Principle

### 2.1. Fractional Fourier transform (FrFT)

The fractional Hartley transform (FrHT) can be defined using the fractional Fourier transform (FrFT). The FrFT at order $\alpha$, is a linear integral operator that maps a given function $f(x)$ onto a function $G^{\alpha}(u)$ by [18]

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

where

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

is the fractional Fourier kernel, sgn is signum function, and $\Phi = \pi\alpha/2$. The inverse FrFT corresponds to the FrFT at the fractional order $-\alpha$. The FrFT operator is additive with respect to the fractional order $\mathcal{F}^{\alpha}\mathcal{F}^{\beta} = \mathcal{F}^{\alpha+\beta}$. The FrFT has a periodicity of 4 with respect to the fractional order $\alpha$.

### 2.2. Fractional Hartley transform (FrHT)

The Hartley transform was proposed as an alternative to the Fourier transform by Hartley in 1942 [41]. It is an integral and Fourier-related transform which transforms real-valued functions to real-valued functions and is its own inverse. Two-dimensional Hartley transform (HT) of a real function $f(x, y)$ is defined as [42–52]

$$\begin{aligned} \mathrm{FrHT}(u, v) &= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x, y)\,\mathrm{cas}\left[2\pi(ux + vy)\right]\mathrm{d}x\mathrm{d}y \\ &= \frac{\exp(i\pi/4)}{\sqrt{2}}\left[\mathcal{F}(u, v) + \exp\left(\frac{-i\pi}{2}\right)\mathcal{F}(-u, -v)\right] \end{aligned} \tag{3}$$

and its inverse transform can be written as

$$f(x, y) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathrm{FrHT}(u, v)\,\mathrm{cas}\left[2\pi(ux + vy)\right]\mathrm{d}u\mathrm{d}v \tag{4}$$

where cas = cos + sin.

Two-dimensional FrHT of an input image $I(x, y)$ can be written as

$$\mathrm{FrHT}^{\alpha,\beta}(u, v) = \frac{\sqrt{\left[1 - i\cot(\varphi_1)\right]\left[1 - i\cot(\varphi_2)\right]}}{2\pi}$$

$$\times \exp\left\{ i\pi\left[\frac{u^2\cot(\varphi_1)}{\lambda f_{s1}} + \frac{v^2\cot(\varphi_2)}{\lambda f_{s2}}\right]\right\}$$

$$\times \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp\left[\frac{i\pi x^2\cot(\varphi_1)}{\lambda f_{s1}}\right]\exp\left[\frac{i\pi y^2\cot(\varphi_2)}{\lambda f_{s2}}\right]$$

$$\times \left\{ \frac{1 - i\exp\left[i(\Phi_1 + \Phi_2)/2\right]}{2}\operatorname{cas}\left[\frac{ux\csc(\varphi_1)}{\lambda f_{s1}} + \frac{vy\csc(\varphi_2)}{\lambda f_{s2}}\right]\right.$$

$$\left. + \frac{1 + i\exp\left[i(\Phi_1 + \Phi_2)/2\right]}{2}\operatorname{cas}\left[-\frac{ux\csc(\varphi_1)}{\lambda f_{s1}} - \frac{vy\csc(\varphi_2)}{\lambda f_{s2}}\right]\right\}$$

$$\times I(x, y)\,\mathrm{d}x\,\mathrm{d}y \tag{5}$$

where $\alpha$ and $\beta$ are the fractional orders of FrHT, $\Phi_1 = \alpha\pi/2$ and $\Phi_2 = \beta\pi/2$, $\lambda$ is the wavelength of the input light, $f_{s1}$ and $f_{s2}$ are the standard focal lengths of lenses in the $x$ and $y$ directions, respectively. The simplified expression (5) can be written as

$$\mathrm{FrHT}^{\alpha,\beta}(u, v) = \frac{1 + \exp\left[i(\Phi_1 + \Phi_2)/2\right]}{2}\mathcal{F}^{\alpha,\beta}(u, v)$$

$$+ \frac{1 - \exp\left[i(\Phi_1 + \Phi_2)/2\right]}{2}\mathcal{F}^{\alpha,\beta}(-u, -v) \tag{6}$$

Because FrHT can be defined in terms of the FrFT, one can say that the FrHT meets all properties of the FrFT. The FrHT has a periodicity of 2 with respect to fractional orders. Moreover, when $\alpha = \beta = 1$, the FrHT reduces to HT. It is reversible since it satisfies the additive properties. Thus, the inverse 2D FrHT of the order $(\alpha, \beta)$ is obtained from the order $(-\alpha, -\beta)$. From the given Eq. (6) it can be applied in the four channel way of FrFT. Two channels indicate $\mathcal{F}^{\alpha,\beta}(u, v)$ and $\exp[i(\Phi_1 + \Phi_2)/2]\mathcal{F}^{\alpha,\beta}(u, v)$, whereas

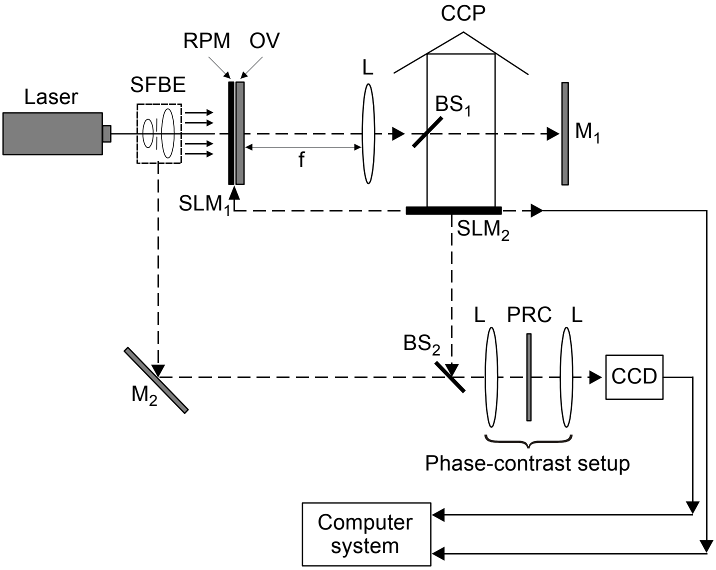

Fig. 1. Proposed opto-electronic experimental setup. SFBE – spatial filter beam expander assembly, SLM – spatial light modulator, RPM – random phase mask, OV – optical vortex, CCP – cube corner prism, BS$_1$, BS$_2$ – beam splitters, M$_1$, M$_2$ – mirrors, CCD – charged coupled device, PRC – photorefractive crystal, and L – lens.

the other two channels indicate $\mathcal{F}^{\alpha,\beta}(-u, -v)$ and $\exp[i(\Phi_1 + \Phi_2)/2]\mathcal{F}^{\alpha,\beta}(-u, -v)$. Here $\mathcal{F}^{\alpha,\beta}$ is a two-dimensional fractional Fourier order of $(\alpha, \beta)$.

The proposed optical implementation of the 2D FrHT is shown in Fig. 1. The collimated beam from a laser ($\lambda$ = 632.8 nm) is split by a spatial filter beam expander into two beams, one beam serves as an object beam, which illuminates the given image along with RPM, optical vortex on the first spatial light modulator (SLM$_1$) digitally. The $\mathcal{F}^{\alpha,\beta}(u, v)$ is well known whereas $\mathcal{F}^{\alpha,\beta}(-u, -v)$ is obtained by a cube corner prism that rotates the field of one arm through 180°. The sum of real and imaginary part of FrHT implemented by cube corner prism is displayed on the second spatial light modulator (SLM$_2$) and through a phase-contrast setup with photorefractive crystal (PRC) is recoded in CCD camera connected with the computer system.

## 2.3. Generation of optical vortex phase masks

Optical vortex, also called as optical phase singularity, is a point phase defect at which the phase is intermediate and amplitude is zero. The structured phase masks (SPMs) based on optical vortex have some advantages over the commonly used RPMs. Since phase optical vortex are phase diffractive optical elements, it is difficult to replicate them. Optical vortices also have the advantage of overcoming the problem of axis alignment in an optical setup and possess characteristics of various keys in a single mask that creates additional security parameters. Unlike the DRPE scheme, where RPMs are used in the encryption, in this paper SPM along with RPM is used for enhancing the system security by increasing the key space through additional phase mask keys.

The radial Hilbert transform mask is another SPM which can serve to make an image edge-enhanced relative to the input image in addition to increasing the key space. The radial Hilbert transform is expressed in terms of a vortex function as

$$V_l(\Phi) = \exp(il\Phi) \tag{7}$$

where $\Phi$ is the azimuth angle and $l$ is an integer denoting the order of transformation, also called as topological charge. It is apparent that the opposite halves of any radial line

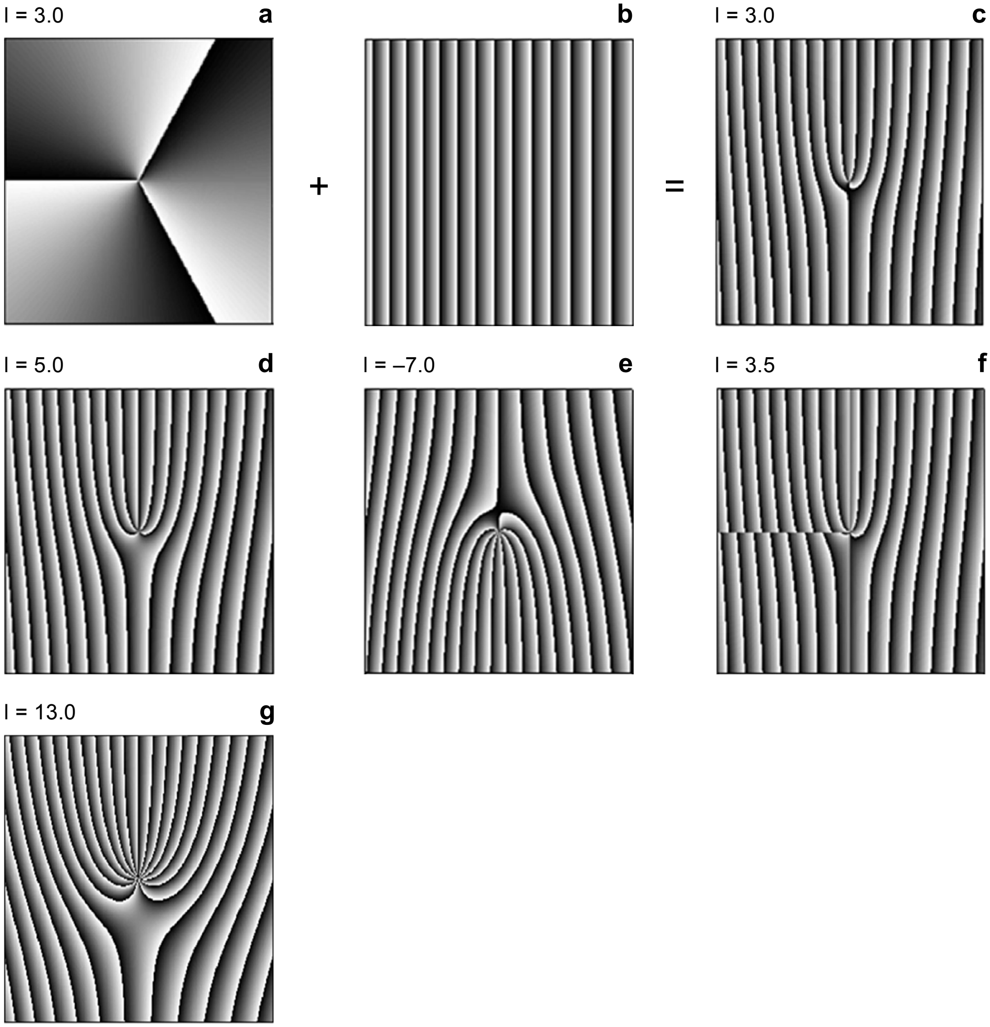

Fig. 2. Formation of optical vortex phase key at wavelength $\lambda$ = 632.8 nm, focal length $f$ = 50 cm, and pixel spacing = 0.00457. Radial Hilbert transform mask for $l$ = 3.0 (**a**). Plane of phase (**b**). Optical vortex for: $l$ = 3.0 (**c**), for $l$ = 5.0 (**d**), for $l$ = –7.0 (**e**), for $l$ = 3.5 (**f**), and for $l$ = 13.0 (**g**).

of the mask have a relative phase difference of $l\pi$ radian. Therefore, for each radial line we have the equivalent of a one-dimensional Hilbert transform of the order $l$. The radial Hilbert transform can be helpful in aligning the axis of the optical setup.

A Fresnel lens is based on quadratic phase change and is given by

$$L(x) = \exp\left(-\frac{i\pi x^2}{\lambda f}\right) \tag{8}$$

Now, an optical vortex phase mask is obtained by taking the product of the two functions $V_l(\Phi)$ and $L(x)$. A phase singularity in the wave field can be imprinted using a phase mask with transmittance of the form given by [2, 3, 7, 8]

$$t(\Phi, x) = \exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right] \tag{9}$$

where $l$ may be known topological charge (plus or minus sign), $f$ is the focal length, $\lambda$ is the illuminating wavelength and $x$ is the distance. Figure 2 represents phase patterns in a grayscale: radial Hilbert masks with topological charge $l = 3.0$ (Fig. 2**a**), plane of phase (Fig. 2**b**), and optical vortex for $l = 3.0, 5.0, -7.0, 3.5$ and $13.0$ (Figs. 2**c**–2**g**).

## 2.4. Asymmetric cryptosystem based on phase truncation

The original amplitude image $I_1(x, y)$ is bonded with a phase mask generated from optical vortices (9) and RPM$_1$, *i.e.* $\exp[2i\pi n_1(x, y)]$, and it is then fractional Hartley transformed with order $(\alpha, \beta)$. The obtained spectrum is an amplitude and the phase truncated to achieve one way encryption. The amplitude-truncated value helps generate first decryption key (DK$_1$) and the phase-truncated value bonded with another phase mask is generated from optical vortices, *i.e.* Eq. (9) and RPM$_2$, *i.e.* $\exp[2i\pi n_2(u, v)]$. Next it is fractional Hartley transformed with order $(-\alpha, -\beta)$ to give an encrypted image that is amplitude-truncated and generates second decryption key (DK$_2$). Here, $n_1(x, y)$ and $n_2(u, v)$ are statistically independent and randomly distributed in [0, 1].

The steps of encryption of an input image $I_1(x, y)$ can be expressed as (see Fig. 3**a**):

$$g(u, v) = \mathrm{PT}\left\{\mathrm{FrHT}^{\alpha, \beta}\left\{I_1(x, y)\exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right]\exp\left[2i\pi n_1(x, y)\right]\right\}\right\} \tag{10}$$

$$C(x, y) = \mathrm{PT}\left\{\mathrm{FrHT}^{-\alpha, -\beta}\left\{g(u, v)\exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right]\exp\left[2i\pi n_2(x, y)\right]\right\}\right\} \tag{11}$$

where PT$\{\cdot\}$ denotes a phase truncation operator, FrHT$^{\alpha, \beta}\{\cdot\}$ and FrHT$^{-\alpha, -\beta}\{\cdot\}$ represents fractional Hartley transform of order $(\alpha, \beta)$ and inverse fractional Hartley transform of order $(-\alpha, -\beta)$, respectively. In the PTFT-based asymmetric cryptosystem, the main objective is to break the linearity of conventional systems. The decryption keys generated in the encryption process are directly related to the plaintext and encryption keys. Thus, the cryptosystem is valuable only when different phase masks are taken for dif-

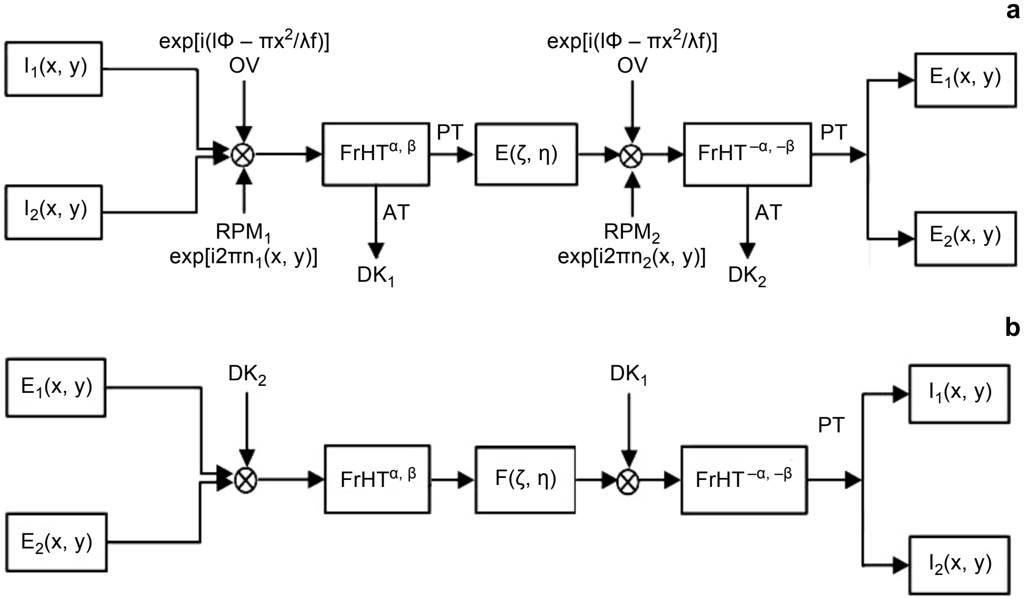

Fig. 3. Flow chart for the scheme encryption (**a**) and decryption (**b**) process; OV – optical vortex, RPM – random phase mask, AT – amplitude-truncated, PT – phase-truncated, DK – decryption key.

ferent plaintexts during each encryption. The decryption keys are obtained from the following expressions. In the proposed method, the two encryption keys are treated as public keys and are not employed in the decryption process. The two decryption keys employed are given as:

$$\mathrm{DK}_1(u, v) = \mathrm{AT}\left\{\mathrm{FrHT}^{\alpha,\beta}\left\{I_1(x, y)\exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right]\exp\left[2i\pi n_1(x, y)\right]\right\}\right\} \tag{12}$$

$$\begin{aligned}\mathrm{DK}_2(x, y) = {} & \mathrm{AT}\left\{\mathrm{FrHT}^{-\alpha,-\beta}\left\{\mathrm{FrHT}^{\alpha,\beta}\left\{I_1(x, y)\exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right]\exp\left[2i\pi n_1(x, y)\right]\right\}\right.\right. \\ & \left.\left.\times \exp\left[i\left(l\Phi - \frac{\pi x^2}{\lambda f}\right)\right]\exp\left[2i\pi n_2(x, y)\right]\right\}\right\}\end{aligned} \tag{13}$$

Here, AT$\{\cdot\}$ symbolizes the amplitude-truncation operator. It is seen that decryption keys $\mathrm{DK}_1(u, v)$ and $\mathrm{DK}_2(x, y)$ are different from encryption keys optical vortices, $\mathrm{RPM}_1$ and $\mathrm{RPM}_2$.

The decryption method shown in Fig. 3**b** is the same as the encryption in the inverse sense on the encrypted complex image $C(x, y)$ with the negative fractional orders of

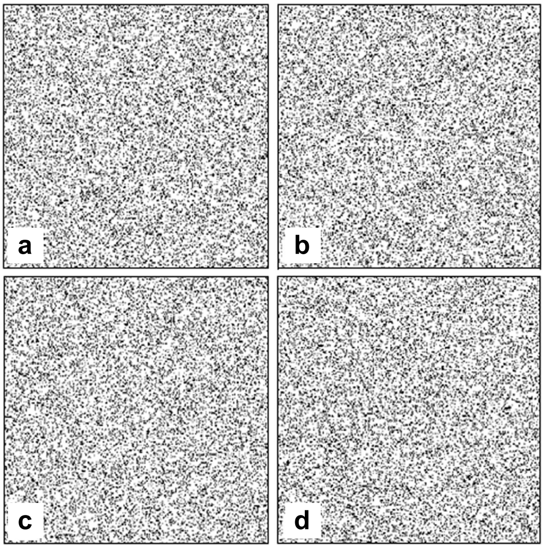

Fig. 4. Asymmetric keys generated during the encryption process: $\mathrm{DK}_1$ and $\mathrm{DK}_2$ for the binary image of *text* (**a**, **b**); $\mathrm{DK}_3$ and $\mathrm{DK}_4$ for the grayscale image of *Lena* (**c**, **d**).

the FrHTs. The encrypted images are first multiplied by $\mathrm{DK}_2$ and then subjected to the fractional Hartley transform $\mathrm{FrHT}^{\alpha,\,\beta}$. The resulting complex image is multiplied by another decrypting key $\mathrm{DK}_1$ and then the inverse fractional Hartley transform $\mathrm{FrHT}^{-\alpha,\,-\beta}$ is performed. Mathematical expression for decryption is given by

$$I_{\mathrm{d}}(x, y) = \mathrm{FrHT}^{-\alpha,\,-\beta}\left\{\mathrm{FrHT}^{\alpha,\,\beta}\{C(u, v)\}\mathrm{DK}_2\right\}\mathrm{DK}_1 \qquad (14)$$

where $I_{\mathrm{d}}(x, y)$ is the decrypted image same as the input one. Figures 4**a** and 4**b** are the two decryption keys generated during the encryption process of amplitude truncation for a binary image of *text* (optical image processing). Figures 4**c** and 4**d** are the two decryption keys generated corresponding to the grayscale image *Lena* in the encryption process.

## 3. Computational simulation results and discussion

The proposed scheme has been validated by performing the numerical simulation on a MATLAB 7.6.0 (R2008a). In this scheme, two images are considered, namely a grayscale of size 256 × 256 pixels (Fig. 5**a**) and binary of size 256 × 256 pixels (Fig. 5**b**). Figure 5**c** shows the optical vortex phase masks used together with RPMs in the spatial and Fourier plane as generated with values of wavelength $\lambda = 632.8$ nm, focal length $f = 50$ cm, $l = 13$, $r = 0.8273$ cm, $r_0 = 4.5$ cm, and $x = y = 0.5850$ cm. Figures 5**d**

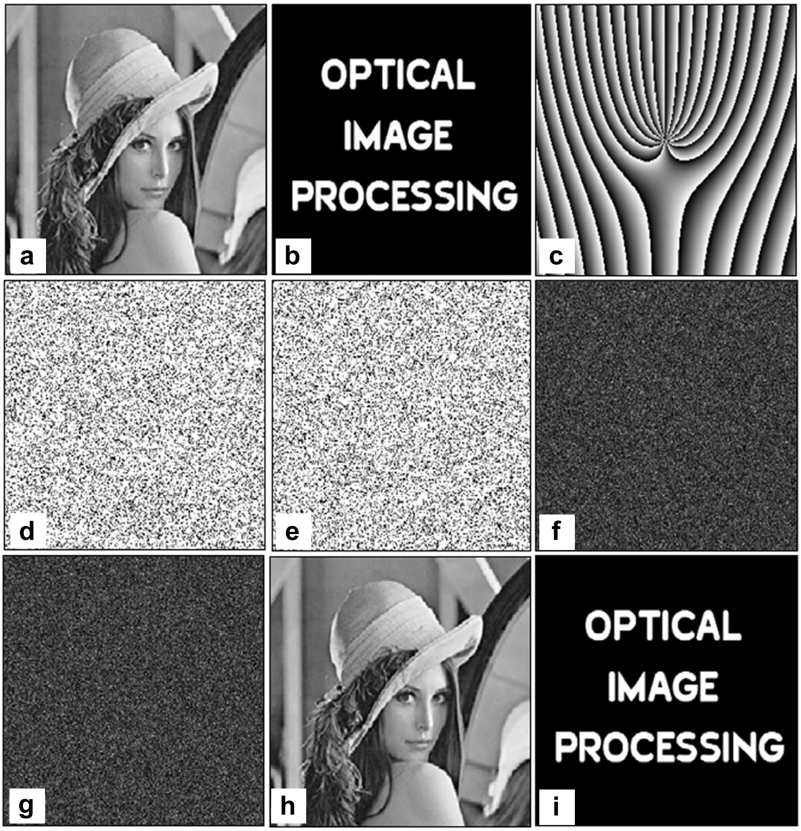

Fig. 5. Results for validation of the proposed scheme for grayscale (*Lena*) and binary (*text*) images: input images of 256 × 256 pixels (**a**, **b**); optical vortex phase key at wavelength $\lambda = 632.8$ nm, focal length $f = 50$ cm, pixel spacing = 0.00457, and $l = 13.0$ (**c**); RPMs (**d**, **e**); encrypted images (**f**, **g**); decrypted images (**h**, **i**).

and 5**e** are the two RPMs generated randomly. Using the encryption scheme, correct FrHT orders ($\alpha$, $\beta$), optical vortices parameters, and the encrypted images are shown in Figs. 5**f** and 5**g**. The FrHT orders are used for the present scheme $\alpha = 0.7$ and $\beta = 0.8$. These values have been taken arbitrarily and considered unequal for simplicity. Using all correct parameters in the scheme, the input images are obtained in Figs. 5**h** and 5**i**, respectively. To express the quality of the decrypted image and to verify the reliability of the encryption algorithm, a common mean squared error (MSE) is introduced between the decrypted image and the original image as

$$\mathrm{MSE} = \sum_{x=0}^{255} \sum_{y=0}^{255} \frac{\left| I_\mathrm{o}(x,y) - I_\mathrm{d}(x,y) \right|^2}{256 \times 256} \tag{15}$$

where $I_\mathrm{o}(x, y)$ and $I_\mathrm{d}(x, y)$ denote the pixel values of the original input image and the decrypted image, respectively. The computed values of MSE between the input and the recovered images of the image *Lena* is $1.8456 \times 10^{-26}$ and for the binary image of *text* is $9.2268 \times 10^{-27}$.

### 3.1. Image entropy analysis

Entropy is a statistical measure that demonstrates the randomness and the unpredictability of an information source. A secure encryption should provide a situation in which the encrypted image does not provide any information about the original image. Image information entropy measures the distribution of image values. The more uniform the pixel value distribution is, the bigger the information entropy gets.

Table 1. Entropy analysis for input,encrypted and decrypted images of *Lena* and *text*.

| Image | Type/size | Entropy | | |
|---|---|---|---|---|
| | | Input image | Encrypted image | Decrypted image |
| *Lena* | PNG/256 × 256 | 6.7272 | 7.4833 | 6.7272 |
| *Text* | JPEG/256 × 256 | 0 | 7.1853 | 0 |

The entropy $H(m)$ of a message source can be calculated as [53–55]

$$H(m) = -\sum_{i=0}^{L} P(m_i)\log_2\Big[P(m_i)\Big] \tag{16}$$

where $m_i$ is the $i$-th image value for $L$ level. Here $P(m_i)$ represents the probability of symbol $m_i$, and $\sum_{i=0}^{L} P(m_i) = 1$. The ideal value for the cipher information entropy is 8. The information entropy of the cipher image of *Lena* and *text* is computed by the proposed algorithm shown in Table 1. One can observe from here that the entropy is very close to 8.

### 3.2. Sensitivity analysis

A highly key sensitive encryption algorithm protects the encrypted data against various cryptanalytic attacks. While developing a cryptosystem, it is assumed that the intruder knows various encryption parameters. In accordance with Kerckhoffs's principle, secrecy of only the used keys is required. Even a very strong or well-designed cryptosystem can be attacked easily if the key used in encryption is poorly selected or if the key size is too small.

The role of encryption keys used in the scheme has been tested keeping in mind their sensitivity. So, the scheme's sensitivity has been verified to its parameters $\alpha$, $\beta$, $\lambda$, $f$, $l$, and pixel spacing. A number of simulations have been tested with incorrect values. The correct values being: wavelength $\lambda = 632.8$ nm, focal length $f = 50$ cm, $l = 13$ and pixel spacing = 0.00457 as optical vortex parameters, $\alpha = 0.7$ and $\beta = 0.8$ are the FrHT orders. The scheme's sensitivity has also been examined to the individual parameters. The recovered images for wrong values are shown respectively in Fig. 6 for various parameters of the mask used in FrHT domain. Figure 6**a** is the decrypted gray-

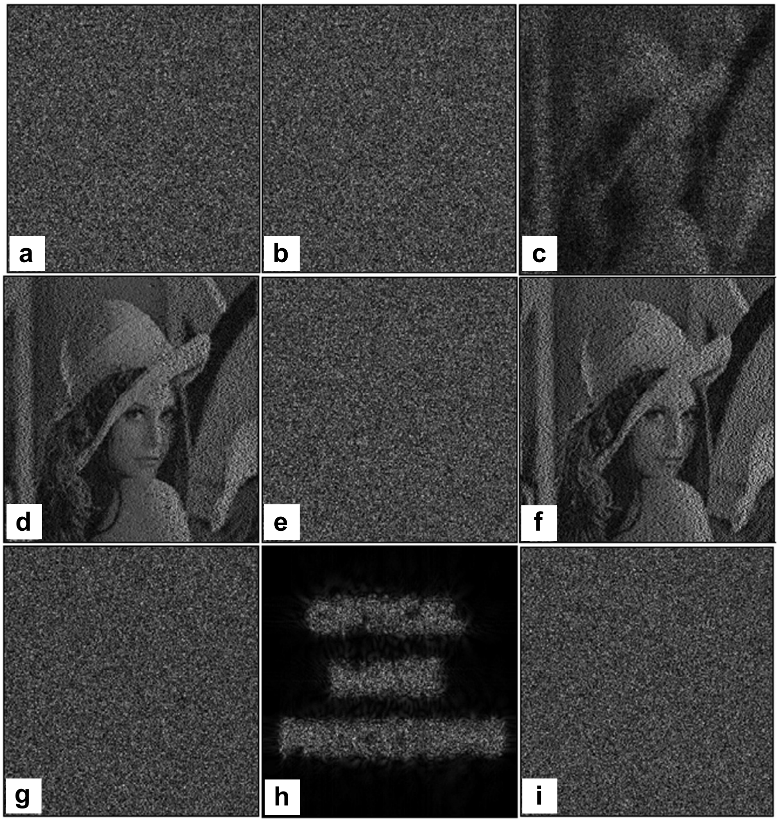

Fig. 6. Results with incorrect parameters. For *Lena* first incorrect FrHT order α = 0.6 (**a**), second incorrect FrHT order $\beta$ = 0.9 (**b**), incorrect topological charge $l$ = 2 (**c**), decrypted images with incorrect focal length $f$ = 600 mm (**d**), decrypted images with incorrect RPM (**e**), decrypted image with incorrect $\lambda$ = 532.8 nm (**f**). For *text* decrypted images with incorrect RPM (**g**), incorrect topological charge $l$ =1 (**h**), and second incorrect FrHT order $\beta$ = 0.9 (**i**).

scale image of *Lena* with first incorrect FrHT order $\alpha$ = 0.6. Figure 6**b** corresponds to the decrypted image of *Lena* with second incorrect FrHT order $\beta$ = 0.9. Figure 6**c** corresponds to the decrypted image of *Lena* with incorrect topological charge $l$ = 2 used in FrHT domain. Figure 6**d** is the decrypted image with incorrect focal length $f$ = 600 mm. Figure 6**e** is the decrypted image with decrypted images with incorrect RPM. Figure 6**f** is the decrypted image with decrypted images with incorrect $\lambda$ = 532.8 nm. Similarly, the proposed scheme for a binary image of *text* has also been tested. Figure 6**g** corresponds to the decrypted images with incorrect RPM. Figures 6**h** and 6**i** are the decrypted images with incorrect topological charge $l$ = 1 and second incorrect FrHT order $\beta$ = 0.9.

MSE plots for a wider range of values of FrHT parameters are shown in Fig. 7**a** and optical vortex parameters in Figs. 7**b**–7**d**. Each plot shows the MSE curves relative to the deviation from the correct parameter value for the grayscale and the binary inputs. It is clearly visible from the plots that the proposed algorithm is highly sensitive

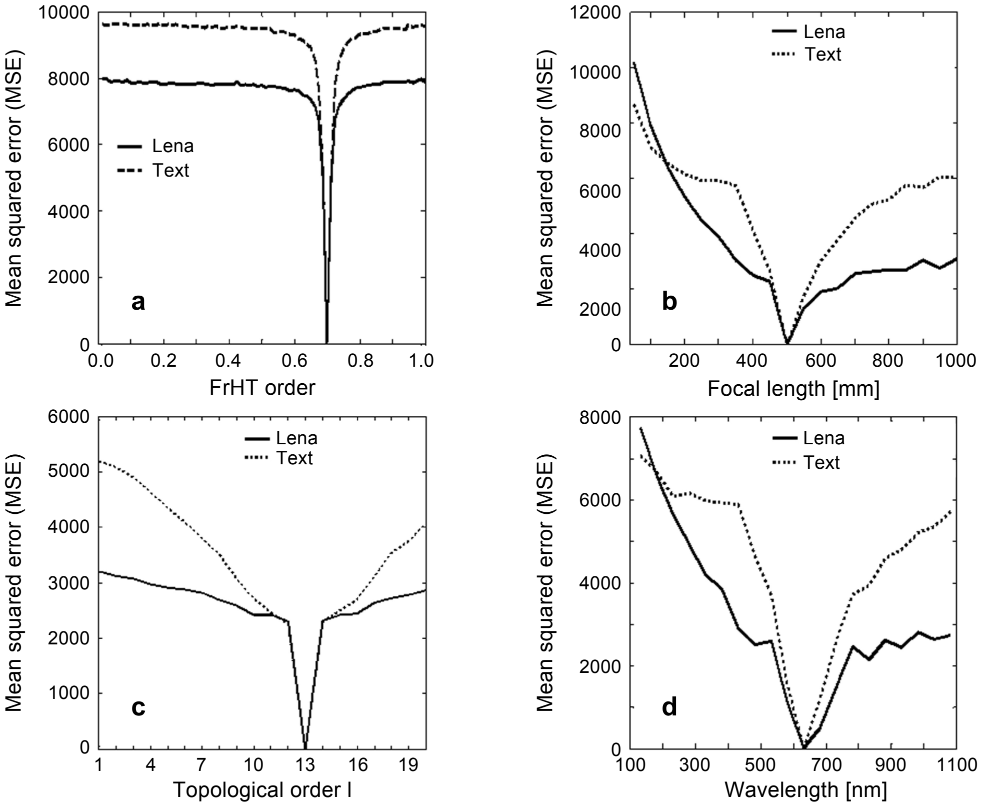

Fig. 7. Sensitivity plots of MSE as a function of deviation from the correct value of the parameter of FrHT: $\alpha = 0.7$ (**a**), $\lambda = 632.8$ nm (**b**), topological charge $l = 13$ (**c**), and focal length $f = 600$ mm (**d**).

to the propagation parameters of FrHT. Though the scheme is also sensitive to optical vortex parameters, the variation in MSE is less steep. In all these sub-figures, a comparison of the two curves indicates that the algorithm shows greater sensitivity for the binary, as compared to the grayscale image for each of the encryption parameters.

In order to test the correlation coefficient of adjacent pixels, the 10 000 pairs of adjacent pixels are randomly selected in vertical, horizontal and diagonal directions from the plaintext as well as encrypted images. The correlation coefficient (CC) of each pair is calculated by the following relations:

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{17}$$

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

Table 2. Values of correlation coefficients of original and cipher images along horizontal, diagonal and vertical.

| Image | Original image | | | Cipher image | | |
|---|---|---|---|---|---|---|
| | Horizontal | Diagonal | Vertical | Horizontal | Diagonal | Vertical |
| *Lena* | 0.9025 | 0.8622 | 0.9378 | 0.0214 | 0.0066 | 0.0176 |
| *Text* | 0.9499 | 0.9464 | 0.9839 | 0.0473 | 0.0082 | 0.0210 |

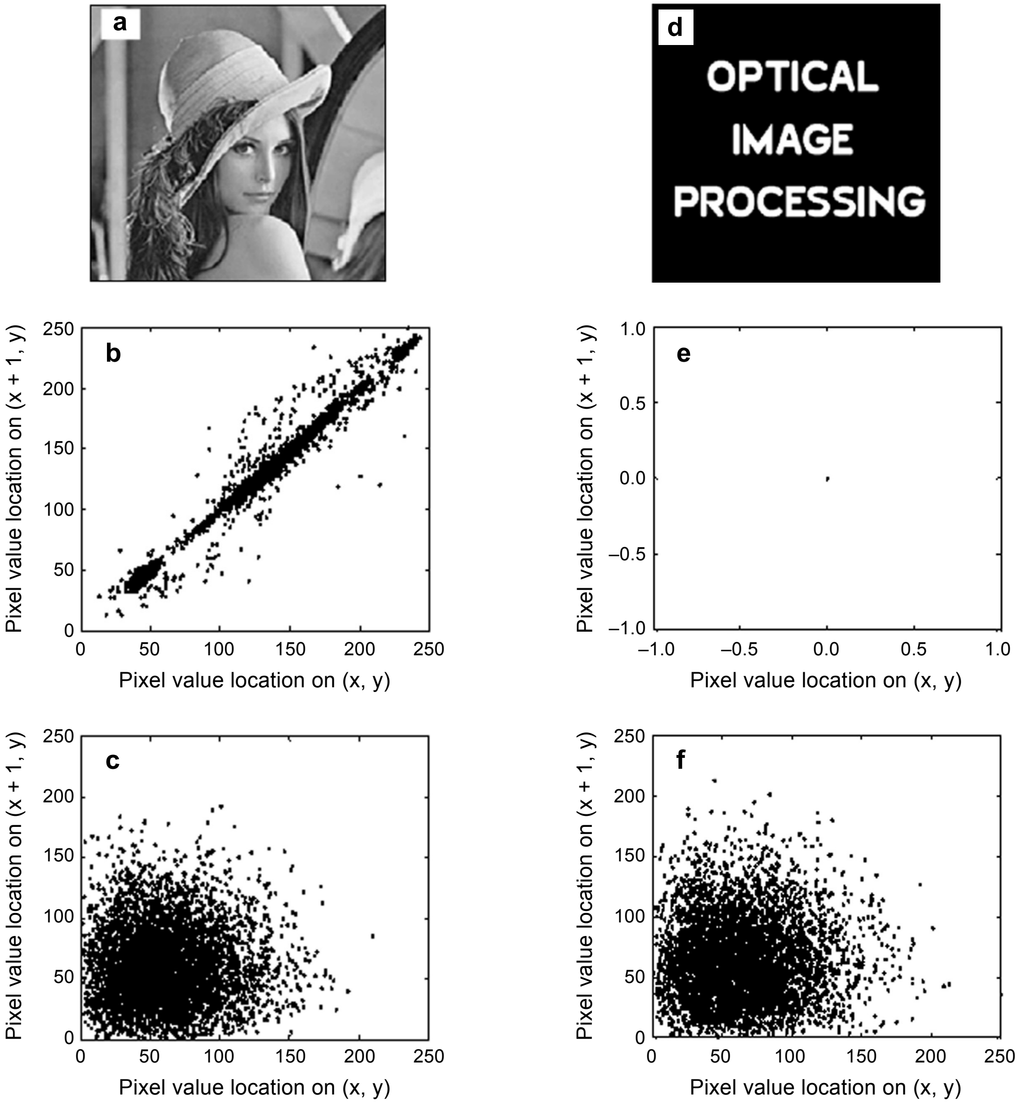

Fig. 8. Plots of correlation distribution for randomly chosen 10 000 pixel pairs. Input image of *Lena* (**a**), correlation distribution of input and encrypted image of *Lena* (**b**, **c**), input image of *text* (**d**), and correlation distribution of input and encrypted image of *text* (**e**, **f**).

The correlation coefficient values of adjacent pixels in the horizontal, vertical and diagonal directions of the original images for *Lena* and *text* are listed in Table 2. The arbitrarily chosen pixels of images are generally highly correlated in horizontal, vertical and diagonal directions. Furthermore, the correlation coefficient of the encrypted images is much weaker than that of the original images. Correlation coefficient values of the original images are very high as compared to those of the encrypted images. Thus the unauthorized user cannot obtain any valid information from this statistical data. Figure 8**a** shows the original image of *Lena*, whereas Figs. 8**b** and 8**c** show the scatter plot of correlation distribution of horizontally adjacent pixels in the original and the encrypted image, respectively. Similar information about the binary image of *text* is shown in Fig. 8**d**. Their corresponding scatter plot of correlation distribution of horizontally adjacent pixels in the original and the encrypted image is shown in Figs. 8**e** and 8**f**, respectively. It can be seen that the proposed algorithm is very effective.

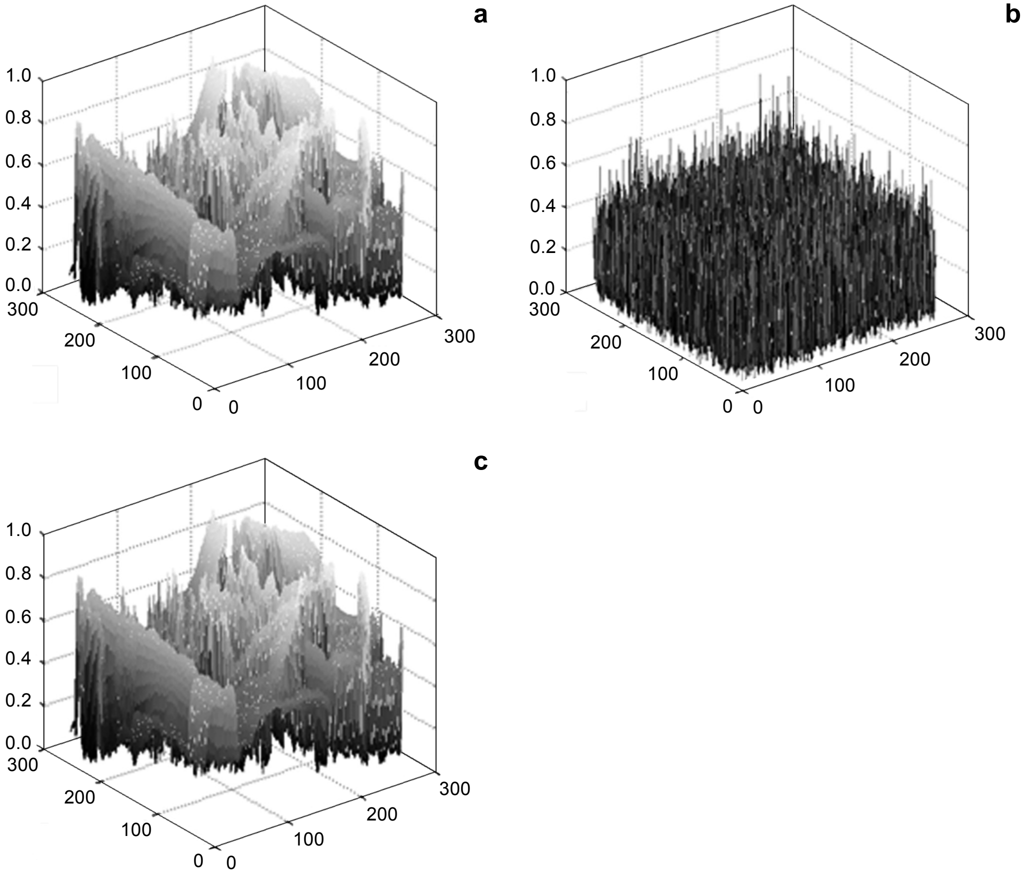

Fig. 9. Three-dimensional surface plots of input image of *Lena*, where the third dimension is the bar graph of intensity of each pixel (**a**), three-dimensional surface plots of encrypted image of *Lena* (**b**), and three -dimensional surface plots of the decrypted image (**c**).

Figure 9**a** is the three-dimensional surface plot of the input images of *Lena*, Fig. 9**b** shows the surface properties of the encrypted image of *Lena*, whereas Fig. 9**c** is the surface plot of decrypted images.

### 3.3. Occlusion attack analysis

The robustness of the proposed algorithm against occlusion attacks has also been examined on the encrypted image. The occluded images are shown in Figs. 10**a**–10**d** for 10%, 25%, 50% and 75% occlusion of the encrypted image of *Lena*. Figures 10**e**–10**h** show the corresponding decrypted images which are recovered fairly well even for occlusion up to 75%. Similar results were obtained when we tested the scheme's robustness for occlusion of the binary image of *text* (Figs. 10**i**–10**l**). Additionally, MSE and CC plots against varying degrees of occlusion of the encrypted images are shown in Figs. 11**a**–11**d**. The variation of MSE and CC curves clearly indicates the scheme's

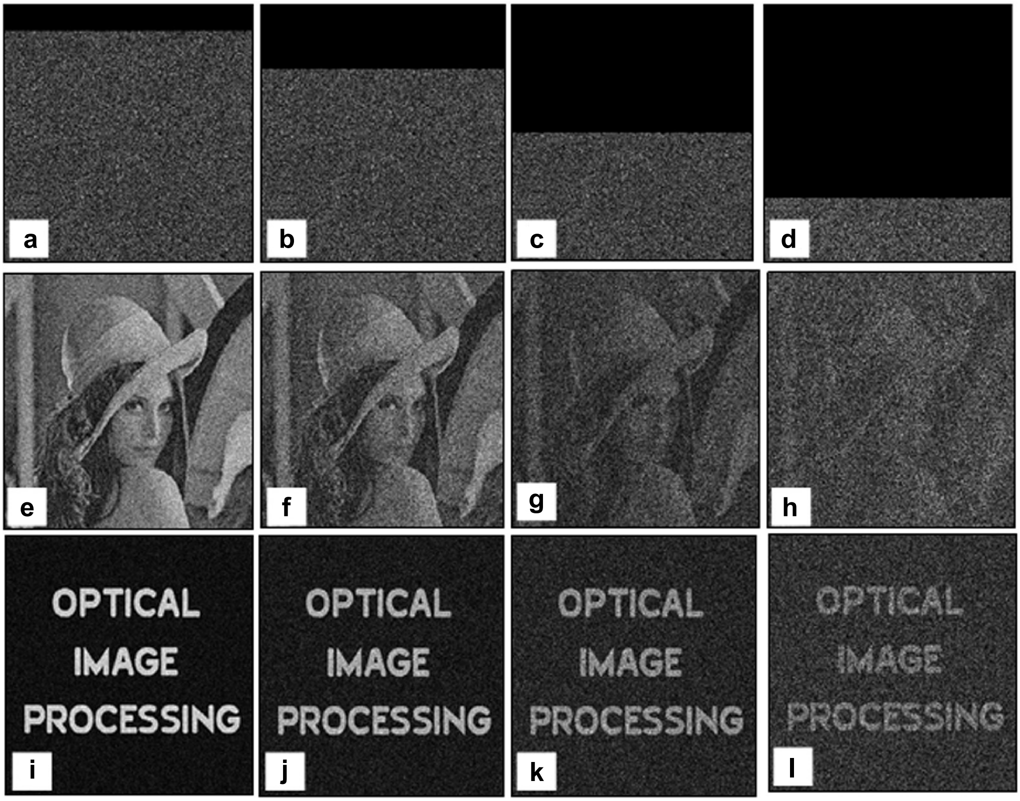

Fig. 10. Occlusion results for the grayscale and the binary image for varying degrees of occlusion: encrypted image with 10% occlusion (**a**), 25% occlusion (**b**), 50% occlusion (**c**), 75% occlusion (**d**), corresponding recovered grayscale images (**e**–**h**), corresponding recovered binary images (**i**–**l**).

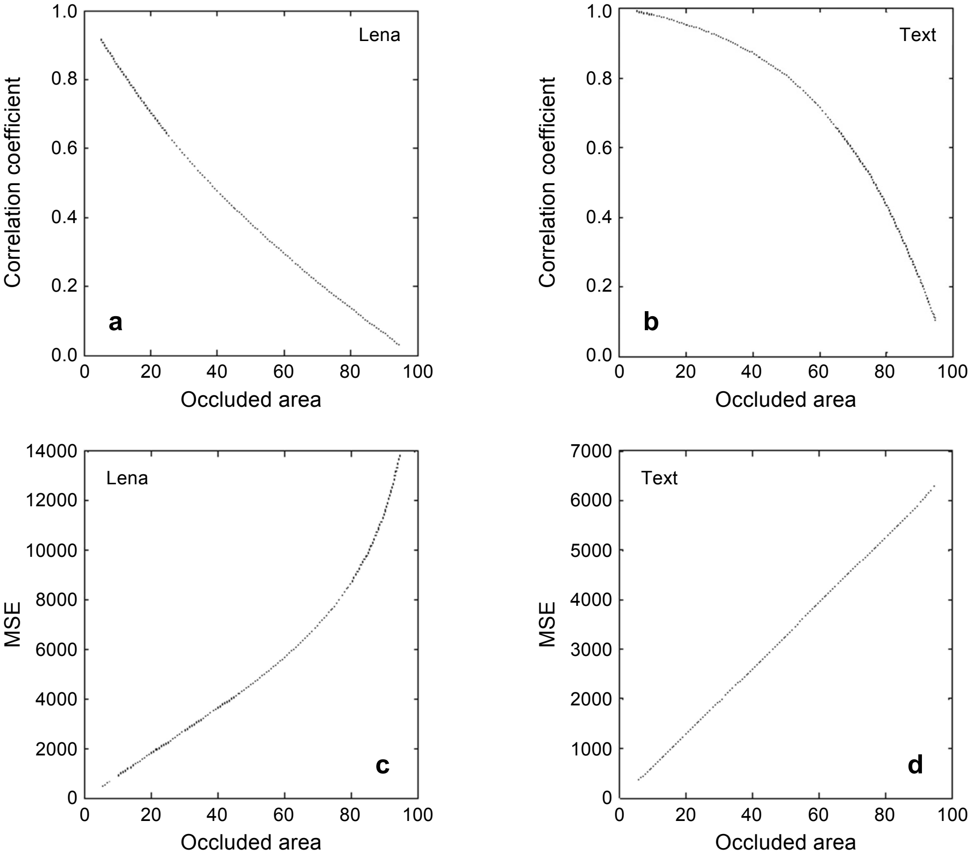

Fig. 11. Plots of correlation coefficient (**a**, **b**), and MSE (**c**, **d**) for grayscale (*Lena*) and binary (*text*) images with varying occluded area.

robustness to the occlusion attack. As expected, the binary image (*text*) shows higher robustness as compared to the grayscale image (*Lena*).

## 3.4. Noise attack analysis

It is inevitable for the noise to impact the quality of the decrypted images directly. The strength of the proposed scheme has also been tested against the noise attack by considering multiplicative Gaussian noise in the encrypted images. The multiplicative noise interferes with the encrypted images according to the following relation [53–55]

$$\xi' = \xi(1 + kG) \tag{18}$$

where $\xi$ and $\xi'$ are the encrypted and the noise-affected encrypted amplitude images, respectively, $k$ is a coefficient which represents the noise strength and $G$ is Gaussian

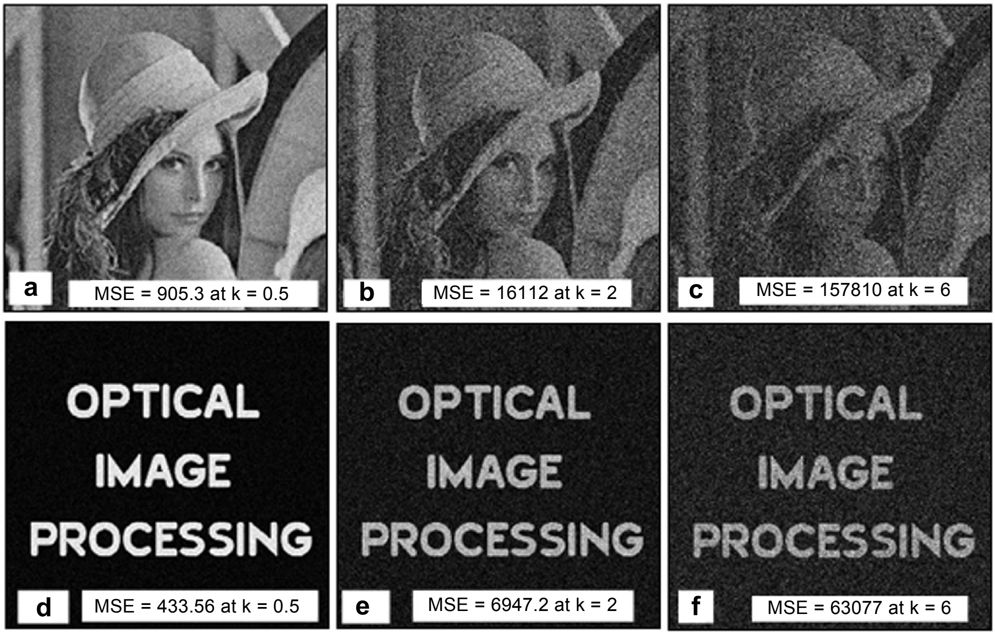

Fig. 12. Recovered images corresponding to Gaussian noise factor $k = 0.5$, 2 and 6, respectively.

random noise with zero-mean and unit standard deviation. Figures 12**a**–12**f** show the recovered images of *Lena* and *text* when $k$ is set to 0.5, 2 and 6 and MSE values are in an increasing order as 905.3, 16112, 157810 and 433.56, 6947.2, 63077. From the recovered images, it is observed that the scheme is robust to noise attacks with maximum resistance to Gaussian noise. The drop in quality of the recovered images is comparable to the cases of additive noise. Figure 13 shows the MSE plots against the noise factor $k$ of Gaussian for the image of *Lena* and *text*. One observes a monotonic increase in MSE

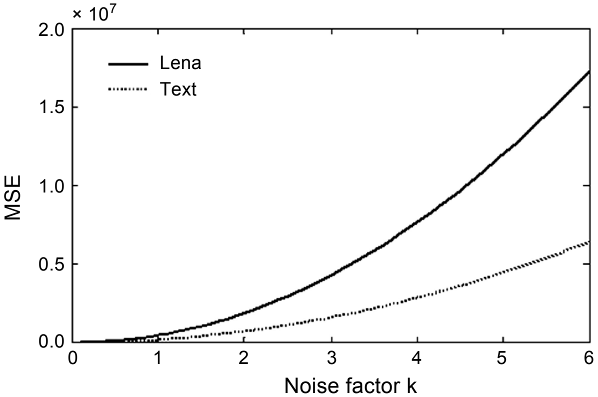

Fig. 13. Plot of MSE *vs*. Gaussian noise factor $k$.

curves of images with an increase in the noise factor. This establishes the robustness of the proposed algorithm against commonly reported noise attacks.

## 4. Conclusions

An asymmetric cryptosystem scheme for binary and grayscale images, using optical vortices, RPMs in the input and the corresponding frequency plane have been observed. This approach not only overcomes the problem of key space in an optical setup, but also makes the scheme more secure. The proposed scheme has been validated in the FrHT domain. The entropy values and three-dimensional plots show the validity of the proposed scheme. The efficacy of the proposed scheme is seen from the computed values of MSE. The sensitivity of the scheme has also been studied for various parameters of FrHT and optical vortices. The numerical simulation performed on MATLAB establishes the scheme's sensitivity to the encryption parameters. In the proposed method, security can be enhanced by increasing the number of keys. Numerical simulations verify the feasibility of the method and demonstrate the security of the scheme. In addition, the results also demonstrate the excellent robustness against noise and occlusion attacks.

*Acknowledgements* – The author wishes to thank the management of The NorthCap University for their encouragement and inspiration that lent support during the course of this work. The author is also thankful to the anonymous reviewers for critical reading and constructive comments.

### References

[1] Nye J.F., Berry M.V., *Dislocations in wave trains*, Proceedings of the Royal Society of London A **336**, 1974, pp. 165–190.

[2] Leach J., Yao E., Padgett M.J., *Observation of the vortex structure of a non-integer vortex beam*, New Journal of Physics **6**, 2004, article ID 71.

[3] Berry M.V., *Optical vortices evolving from helicoidal integer and fractional phase steps*, Journal of Optics A: Pure and Applied Optics **6**(2), 2004, pp. 259–268.

[4] Lee W.M., Yuan X.-C., Dholakia K., *Experimental observation of optical vortex evolution in a Gaussian beam with an embedded fractional phase step*, Optics Communications **239**(1–3), 2004, pp. 129–135.

[5] Flossmann F., Schwarz U.T., Maier M., *Propagation dynamics of optical vortices in Laguerre –Gaussian beams*, Optics Communications **250**(4–6), 2005, pp. 218–230.

[6] Swartzlander G.A. Jr., *The optical lens*, OPN, November, 2006, pp. 39–43.

[7] Vyas S., Singh R.K., Senthilkumaran P., *Fractional vortex lens*, Optics and Laser Technology **42**(6), 2010, pp. 878–882.

[8] Vyas S., Singh R.K., Devinder Pal Ghai, Senthilkumaran P., *Fresnel lens with embedded vortices*, International Journal of Optics, Vol. 2012, 2012, article ID 249695.

[9] Amaral A.M., Falcão-Filho E.L., De Araújo C.B., *Shaping optical beams with topological charge*, Optics Letters **38**(9), 2013, pp. 1579–1581.

[10] Preda L., *Generation of optical vortices by fractional derivative*, Optics and Lasers in Engineering **54**, 2014, pp. 42–48.

[11] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.

[12] 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.

[13] Alfalou A., Brosseau C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009, pp. 589–636.

[14] Millan M.S., Perez-Cabre E., *Optical data encryption*, [In] *Optical and Digital Image Processing: Fundamentals and Applications*, [Eds.] G. Cristobal, P. Schelkens, H. Thienpont, Wiley, 2011, pp. 739–767.

[15] Javidi B., Carnicer A., Yamaguchi M., Nomura T., Pérez-Cabré E., Millán M.S., Nishchal N.K., Torroba R., Barrera J.F., Wenqi He, Xiang Peng, Stern A., Rivenson Y., Alfalou A., Brosseau C., Changliang Guo, Sheridan J.T., Guohai Situ, Naruse M., Matsumoto T., Juvells I., Tajahuerce E., Lancis J., Wen Chen, Xudong Chen, Pinkse P.W.H., Mosk A.P., Markman A., *Roadmap on optical security*, Journal of Optics **18**(8), 2016, article ID 083001.

[16] 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 the First International Conference, IEM OPTRONIX 2014*, Springer Proceedings in Physics, Vol. 166, 2015, pp. 25–36.

[17] Kumar P., Joseph J., Singh K., *Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures*, [In] *Linear Canonical Transforms Theory and Applications*, [Eds.] J.J. Healy, M. Alper Kutay, H.M. Ozaktas, J.T. Sheridan, Springer Series in Optical Sciences, Vol. 198, 2016, pp. 367–396.

[18] Unnikrishnan G., Joseph J., Singh K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000, pp. 887–889.

[19] 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.

[20] Matoba O., Javidi B., *Encrypted optical memory system using three-dimensional keys in the Fresnel domain*, Optics Letters **24**(11), 1999, pp. 762–764.

[21] Guohai Situ, Jingjuan Zhang, *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586.

[22] 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 ID 926135.

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

[24] 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, pp. 6472–6481.

[25] Singh H., Yadav A.K., Vashisth S., Singh K., *Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane*, Optics and Lasers in Engineering **67**, 2015, pp. 145–156.

[26] Liansheng Sui, Minjie Xu, Ailing Tian, *Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain*, Optics and Lasers in Engineering **91**, 2017, pp. 106–114.

[27] 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, pp. 125–139.

[28] Nanrun Zhou, Yixian Wang, Lihua Gong, *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242.

[29] 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. 2014, 2014, article ID 728056.

[30] NANRUN ZHOU, HAOLIN LI, DI WANG, SHUMIN PAN, ZHIHONG ZHOU, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications **343**, 2015, pp. 10–21.

[31] VASHISTH S., SINGH H., YADAV A.K., SINGH K., *Image encryption using fractional Mellin transform, structured phase filters and phase retrieval*, Optik – International Journal for Light and Electron Optics **125**(18), 2014, pp. 5309–5315.

[32] SINGH H., *Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain*, 3D Research **7**(4), 2016, article ID 34.

[33] WAN QIN, XIANG PENG, *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010, pp. 118–120.

[34] WAN QIN, XIANG PENG, BRUCE GAO, XIANGFENG MENG, *Universal and special keys based on phase -truncated Fourier transform*, Optical Engineering **50**(8), 2011, pp. 080501.

[35] XIAOGANG WANG, DAOMU ZHAO, *Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval*, Optics Communications **284**(19), 2011, pp. 4441–4445.

[36] XIAOGANG WANG, DAOMU ZHAO, *Double images encryption method with resistance against the specific attack based on an asymmetric algorithm*, Optics Express **20**(11), 2012, pp. 11994–12003.

[37] 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.

[38] WEI LIU, ZHENGJUN LIU, JINGJING WU, SHUTIAN LIU, *Asymmetric cryptosystem by using modular arithmetic operation based on double random phase encoding*, Optics Communications **301–302**, 2013, pp. 56–60.

[39] QU WANG, QING GUO, JINYUN ZHOU, *Color image hiding based on phase-truncation and phase retrieval technique in fractional Fourier domain*, Optik – International Journal for Light and Electron Optics **124**(12), 2013, pp. 1224–1229.

[40] VASHISTH S., YADAV A.K., SINGH H., SINGH K., *Watermarking in gyrator domain using an asymmetric cryptosystem*, Proceedings of SPIE **9654**, 2015, article ID 96542E.

[41] HARTLEY R.V.L., *A more symmetrical Fourier analysis applied to transmission problems*, Proceedings of the IRE **30**(3), 1942, pp. 144–150.

[42] LINFEI CHEN, DAOMU ZHAO, *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006, pp. 3438–3440.

[43] DAOMU ZHAO, XINXIN LI, LINFEI CHEN, *Optical image encryption with redefined fractional Hartley transform*, Optics Communications **281**(21), 2008, pp. 5326–5329.

[44] SINGH N., SINHA A., *Optical image encryption using Hartley transform and logistic map*, Optics Communications **282**(6), 2009, pp. 1104–1109.

[45] ZHENGJUN LIU, AHMAD M.A., SHUTIAN LIU, *Image encryption based on double random amplitude coding in random Hartley transform domain*, Optik – International Journal for Light and Electron Optics **121**(11), 2010, pp. 959–964.

[46] XINXIN LI, DAOMU ZHAO, *Optical color image encryption with redefined fractional Hartley transform*, Optik – International Journal for Light and Electron Optics **121**(7), 2010, pp. 673–677.

[47] JIMENEZ C., TORRES C., MATTOS L., *Fractional Hartley transform applied to optical image encryption*, Journal of Physics: Conference Series **274**, 2011, article ID 012041.

[48] HONE-ENE HWANG, *An optical image cryptosystem based on Hartley transform in the Fresnel transform domain*, Optics Communications **284**(13), 2011, pp. 3243–3247.

[49] ABUTURAB M.R., *Color image security system on discrete Hartley transform in gyrator transform domain*, Optics and Lasers in Engineering **51**(3), 2013, pp. 317–324.

[50] VILARDY J.M., TORRES C.O., JIMENEZ C.J., *Double image encryption method using the Arnold transform in the fractional Hartley domain*, Proceedings of SPIE **8785**, 2013, article ID 87851R.

[51] 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.

[52] MUNIRAJ I., CHANGLIANG GUO, BYUNG-GEUN LEE, SHERIDAN J.T., *Interferometry based multispectral photon-limited 2D and 3D integral image encryption employing the Hartley transform*, Optics Express **23**(12), 2015, pp. 15907–15920.

[53] LIHUA GONG, XINGBIN LIU, FEN ZHENG, NANRUN ZHOU, *Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique*, Journal of Modern Optics **60**(13), 2013, pp. 1074–1082.

[54] 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*, Optics Communications **344**, 2015, pp. 172–180.

[55] SINGH H., *Optical cryptosystem of color images using random phase masks in the fractional wavelet transform domain*, AIP Conference Proceedings **1728**(1), 2016, article ID 020063.

*Received December 24, 2016*
*in revised form February 20, 2017*