

AJP

ISSN : 0971 - 3093

Vol 24, No 1 , January-March, 2015

ASIAN JOURNAL OF PHYSICS

An International Quarterly Research Journal



ANITA PUBLICATIONS

FF-43, 1st Floor, Mangal Bazar, Laxmi Nagar, Delhi-110 092, India
B O : 2, Pasha Court, Williamsville, New York-14221-1776, USA



Double phase-image encryption using gyrator-, and fractional Fourier transforms with structured phase mask in the frequency plane followed by a gyrator transform

Hukum Singh, A K Yadav, Sunanda Vashisth, and Kehar Singh

Department of Applied Sciences

ITM University, Sector 23-A, Gurgaon-122 017, India

Fully-phase image encryption is considered more secure as compared to an amplitude image encryption. In the present paper, an encryption scheme has been proposed for double phase-images. One of the phase-images is fractional Fourier transformed (FrFT) whereas the other one is gyrator transformed, after bonding them with random phase masks. The two resulting images are then added and subtracted to give intermediate images which are bonded with a structured phase mask (SPM) in the frequency plane. Thereafter, the images are once again transformed using a gyrator transform (GT) to give the corresponding encrypted images. The use of an SPM enhances the key space for encryption and also overcomes the problem of axis alignment associated with an optical set-up. The decryption process is the reverse of encryption. The validity of the proposed scheme has been established from the computer simulation results using MATLAB 7.1 platform. The performance of the scheme has been evaluated in terms of mean-squared-error (MSE) between the input-, and the decrypted image. In addition, the sensitivity to encryption keys such as SPM parameters, transform angles of GT and the FrFT orders has been investigated. The technique is likely to provide enhanced security in view of the increased number of encryption parameters. Robustness of the system for partial occlusion of the encrypted image has also been investigated. © Anita Publications. All rights reserved.

Keywords: phase-image, fractional Fourier transform, gyrator transform, structured phase mask, mean-squared-error

1 Introduction

Encryption techniques play a key role in information security. With the rapid development of modern techniques, information security for various applications is of great concern [1-7]. In the well-known double random phase encoding (DRPE) technique, two pairs of statistically independent random phase masks (RPMs) are used in the input-, and Fourier planes to encrypt a given image to a stationary white noise. Subsequently, the DRPE technique has been implemented in various canonical transform domains such as fractional Fourier, Fresnel-, discrete fractional random-, Hartley-, gyrator-, wavelet-, and fractional Mellin.

One of the canonical transforms, the gyrator transform [8] was introduced in the field of optics and image processing by Rodrigo *et al* [9-11]. Further discussion on applications and digital implementation is contained in the study by Pei and Ding [12]. Cryptosystems for securing the color images have also been proposed in GT domain [13-15]. Numerous other papers [16-22] dealing with different aspects of GT and its applications may also be noted.

It is known that the conventional DRPE technique suffers from the problem of optical axis alignment. Some studies have used structured phase mask, instead of random, to overcome the problem of axis alignment and to enlarge the key space for enhanced security [23, 24]. The structured phase mask is generally made from a Fresnel zone plate and a spiral phase plate. Certain recent studies on image encryption have used structured phase mask derived from Fresnel zone plate [13, 14, 25, 26]. In the proposed scheme, we have used random phase masks in the input plane, and a structured phase mask based on a Fresnel zone plate in the frequency plane.

Unlike the conventional approach of taking amplitude image as input in the encryption scheme, we have considered a fully-phase image which is more secure and has certain advantages reported in a few studies [27-34]. When the fully-phase image encryption is implemented optically, it is difficult to replicate the system. The scheme is also resistant to additive and multiplicative noise. Towghi *et al* [28] compared the performance of encryption methods based on the two approaches in a DRPE setup. It was shown that the

Corresponding author :

e-mail: hukumsingh@itmindia.edu (Hukum Singh); keharsiitd@gmail.com (Kehar Singh)

decrypted images from fully-phase encryption are more robust to additive noise than those from amplitude based encryption. In another study, Javidi *et al* [29] have reviewed the two encryption methods and have proposed a thresholding scheme that reduces the distortion in the decrypted information. In a study conducted using fractional Fourier transform, Nishchal *et al* [32] analyzed the performance of a fully phase-based encryption system. They chose a binary text and a grayscale image to study the tolerance to data loss, binarization of the encrypted image, and noise perturbation due to additive and multiplicative noise. The implementation of an optical phase encryption system has been done for a two-dimensional phase-image obtained from an amplitude image.

The present paper is organized as follows: in section 2, we present a brief mathematical description of FrFT, GT, and SPM, and the encryption scheme. In section 3, we present the results based on computer simulations for validation and evaluation of the scheme's performance. Finally, the conclusions of the study are summarized in section 4.

2 Principle

In this section, for the sake of continuity, we briefly reproduce essential mathematical formulation of two linear canonical transforms (FrFT and GT), and the SPM used in the present scheme.

2.1 The fractional Fourier transform

The fractional Fourier transform (FrFT) which is a linear canonical integral transform, is a generalization of the ordinary Fourier transform and is defined in terms of fractional order p . This transform has been widely used for many years. The generalization of the ordinary Fourier transform to the FrFT comes at no additional cost in digital computation or optical implementation. FrFT finds application in many fields such as quantum mechanics, optical signal processing, time-variant filtering, and multiplexing. Fractional order domain provides extra security against attacks since the fractional orders of transform provide additional encryption parameters. The ordinary Fourier transform is a special case of a continuum of fractional Fourier domains. Mathematical expression of the p -th order FrFT of $f(x)$ can be written as (for simplicity, one-dimensional function is considered) [35].

$$F^p\{f(x)\}(u) = \int_{-\infty}^{+\infty} K_p(x,u)f(x)dx \quad (1)$$

where the kernel function $K_p(x,u)$ is given by

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

and $A = \frac{\exp[-i(\pi \operatorname{sgn}(\Phi)/4 - \Phi/2)]}{\sqrt{|\sin\Phi|}}$, with $\Phi = p\pi/2$. Whenever p is an integral multiple of π , the kernel is

expressed in terms of Dirac delta function (δ). In the particular case of transform order $p=1$, FrFT reduces to the conventional full Fourier transform. When the fractional order p is zero, it leads to identity transform. The inverse transform of FrFT can be simply evaluated by taking negative of the fractional order. Optical implementation of the FrFT is done by using Lohmann's Type I and Type II setups [36, 37]. A simple extension of FrFT to two-dimensions can be written as

$$F^{p,q}\{f(x,y)\}(u,v) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} K_{p,q}(x,y;u,v)f(x,y)dx dy \quad (3)$$

where $K_{p,q}(x,y;u,v) = K_p(x,u)K_q(y,v)$ (4)

2.2 The gyrator transform

The gyrator transform is similar to the fractional Fourier transform (FrFT). It is also a linear canonical integral transform which produces the rotation in the twisted position-spatial frequency planes [8]. FrFT and

GT have some similarities but kernels used in them are different. FrFT uses a kernel which is the product of spherical and plane waves whereas GT uses kernel which is the product of hyperbolic and plane waves. The GT of a two-dimensional function $f(x,y)$ can be written [9] as,

$$G(u,v) = G^\alpha\{f(x,y)\}(u,v) = \iint f(x,y) K_\alpha(x,y;u,v) dx dy \quad (5)$$

The kernel of the GT is defined as

$$K_\alpha(x,y;u,v) = \frac{1}{|\sin\alpha|} \exp\left[2i\pi\frac{(xy+uv)\cos\alpha - xv - yu}{\sin\alpha}\right] \quad (6)$$

where α is the transform angle and $G(u,v)$ is the output of gyrator transform. 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^α is expressed as $G^{-\alpha}$ or $G^{2\pi-\alpha}$. The GT is periodic and additive with respect to rotation angle, $G^\alpha G^\beta = G^{\alpha+\beta}$.

2.3 Structured phase masks

The structured phase masks have some advantages over the commonly used random phase masks (RPM). Since phase Fresnel zone plates (FZPs) are phase diffractive optical elements, it is difficult to replicate them. FZPs 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 as additional security parameters [23].

Unlike the DRPE scheme, where RPMs are used in the encryption, in this paper we have used in the frequency plane, a structured phase mask based on FZP, aimed at enhancing the system security by increasing the key space through additional phase mask parameters. The transmittance function of an FZP can be written [23] as $T(r) = \exp\left\{\frac{-i\pi r^2}{\lambda f}\right\}$ where f is focal length, λ denotes the illuminating wavelength, and r is ring focus radius. The optical axis is assumed to coincide with the z -direction. The FZP has multiple storing key and its focusing ring can be aligned with the setup axis.

2.4 The Encryption scheme

The flowchart of the encryption process of the proposed scheme is shown in Fig 1. Here, the first amplitude image $I_1(x,y)$, to be encrypted, is phase-encoded as $\exp[i\pi I_1(x,y)]$ and is bonded with a random phase mask (RPM1), defined as $\exp[i2\pi n_1(x,y)]$, in the input plane. Simultaneously, the second amplitude image $I_2(x,y)$, converted to phase-encoded image $\exp[i\pi I_2(x,y)]$ is bonded with another random phase mask (RPM2) defined as $\exp[i2\pi n_2(x,y)]$. Here, $n_1(x,y)$ and $n_2(x,y)$ are statistically independent and are uniformly distributed in $[0,1]$. Then, the resulting first image is subjected to a gyrator transform GT_1 of rotation angle α , whereas the second image is subjected to an FrFT of order (p,q) . The images so obtained in the frequency domain are added and subtracted to give P1 and P2 which can be termed as intermediate encrypted images.

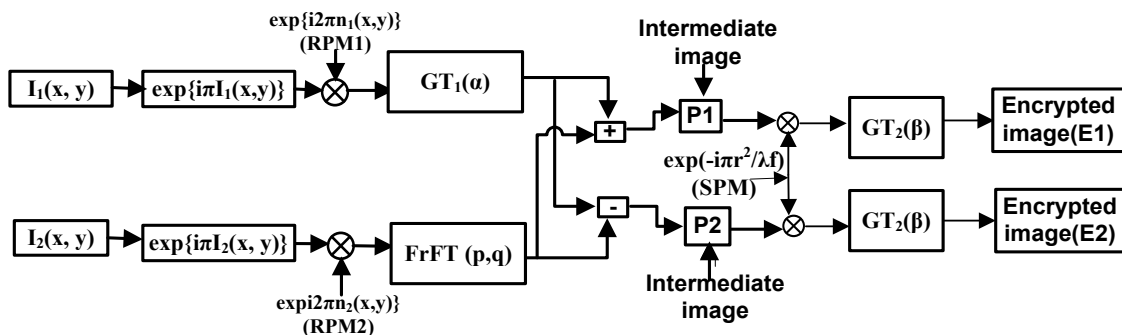


Fig.1 Flow chart for the encryption process of the proposed scheme

These are then bonded with a structured phase mask based on Fresnel zone plate, defined as $\exp\left\{\frac{-i\pi r^2}{\lambda f}\right\}$. Finally, we obtain two encrypted images E_1 and E_2 , respectively by performing another gyrator transform GT_2 of rotation angle β .

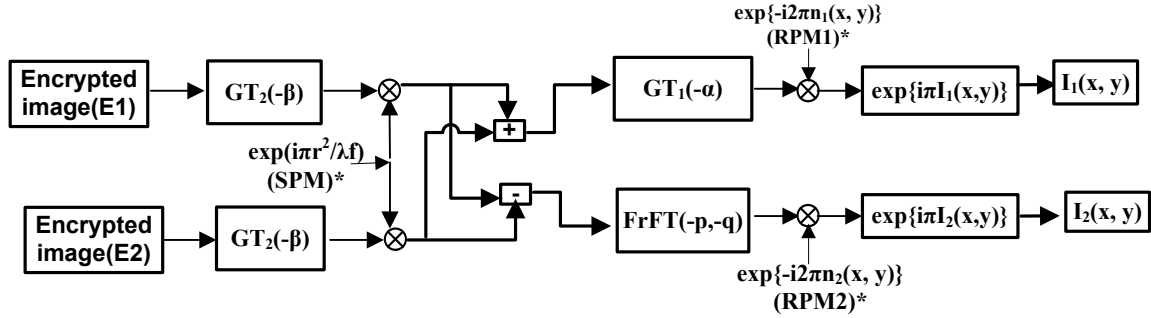


Fig 2. Flow chart for the decryption process of the proposed scheme

Decryption process is simply the reverse of encryption and follows the steps shown in Fig 2. The encrypted images E_1 and E_2 are inverse gyrator transformed with rotation angle β . The resulting complex images on multiplication by the conjugate of SPM, are added and subtracted. The added part is subjected to inverse GT of rotation angle α , followed by multiplication by the conjugate of RPM1, to recover the first phase-image. On the other hand, the subtracted part is subjected to an inverse FrFT and then multiplied by the conjugate of RPM2 to recover the second phase-image. Finally, the amplitude images $I_1(x, y)$ and $I_2(x, y)$ easily can be obtained from the recovered phase images by extracting the phase of $\exp[i\pi I_1(x, y)]$ and $\exp[i\pi I_2(x, y)]$ and dividing by π .

3 Results and discussion

In this section, the validity and robustness of the proposed scheme have been verified by performing numerical simulations on a MATLAB 7.1 platform. The scheme is simple and fast as the entire encryption-decryption process is accomplished in just a few seconds. We have also carried out sensitivity analysis of the scheme with respect to decryption parameters.

Two grayscale amplitude images, Barbara and baboon, each of size 256×256 pixels (Figs 3a and 3b), are converted to phase-encoded images before being used as input in the proposed scheme. The structured phase mask used in the frequency plane is generated with parameter values as wavelength $\lambda = 632.8$ nm, focal length $f = 125$ mm, and pixel spacing = 0.023. Figure 3(c) presents the FZP-based SPM used in the frequency plane of the encryption process, whereas Fig 3(d) displays the RPM used in the input plane. The encrypted images for phase-encoded Barbara and baboon obtained from the encryption process of Fig 1 are shown, respectively in Figs 3(e) and 3(f). One can easily see that the encrypted images are pure random stationary white noise. Based on the correct decryption parameters, the recovered images corresponding to the input images are shown in Figs 3(g) and 3(h). The results of the decrypted images clearly establish the validity of the proposed scheme. The fractional orders of FrFT used for the present scheme were $p = q = 0.3$. These have been taken arbitrarily and considered equal for simplicity. The transform angles are also taken arbitrarily as $\alpha = 0.4\pi$ and $\beta = 0.6\pi$ for the two gyrators transforms namely GT_1 and GT_2 used in the scheme.

In order to assess the efficacy of the proposed scheme, mean-squared-error (MSE) between the input image and the decrypted image has been computed. If $I_o(i, j)$ and $I_d(i, j)$ denote the pixel values of the original input image (size $M \times N$) and the decrypted image, a mathematical expression for MSE can be written as,

$$\text{MSE} = \frac{\sum_{i=1}^M \sum_{j=1}^N \{I_o(i, j) - I_d(i, j)\}^2}{M \times N} \quad (7)$$

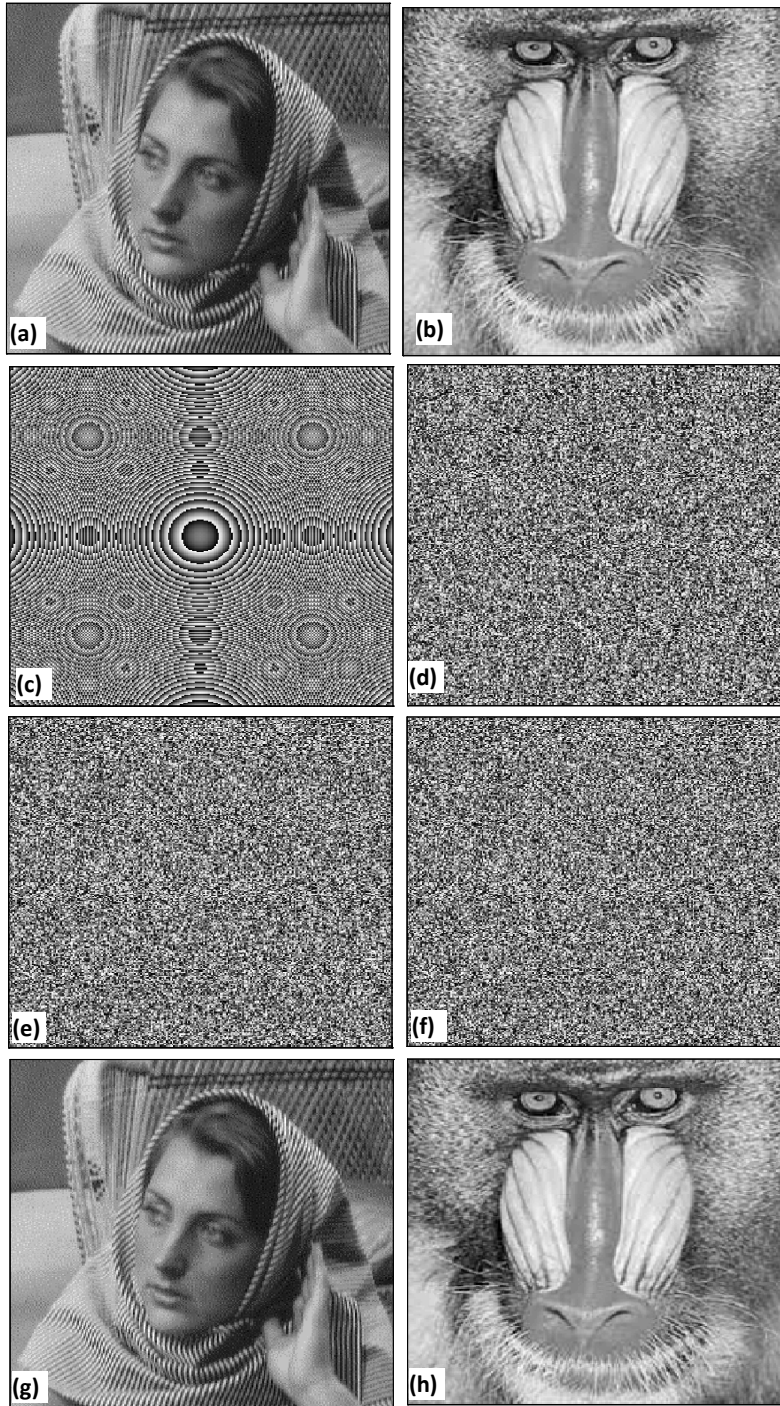


Fig 3 Results for validation of the proposed scheme: (a) input image Barbara, 256×256 pixels; (b) input image of baboon 256×256 pixels; (c) structured phase mask at pixel spacing = 0.023, $\lambda = 632.8\text{nm}$, $f = 125\text{mm}$; (d) random phase mask; (e) encrypted image of Barbara; (f) encrypted image of baboon; (g) decrypted image of Barbara; (h) decrypted image of baboon.

The computed value of MSE between the first input image (Barbara) and the recovered image using the proposed scheme is 1.8×10^{-32} . Similarly the MSE value between the second input image (baboon) and its recovered image is 2.4×10^{-28} . It may be noted that a smaller value of MSE means greater similarity between the input and decrypted images, further validating the proposed scheme.

3.1 Correlation Coefficient (CC)

Correlation coefficient is another criterion used in the literature [38, 39] to measure the similarity of two images quantitatively. It is obvious that arbitrarily chosen pixels of images are generally highly correlated in horizontal, vertical or diagonal directions. We know that CC of the encrypted images is much weaker than that of original images. However, a secure image encryption algorithm must produce an encrypted image having low CC between adjacent pixels. We have randomly selected 10,000 pairs of adjacent pixels (horizontal, vertical or diagonal) for computation of CC from the input and the encrypted images separately. Then, the CC of each pair is calculated by the following relations [38],

$$\rho(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad \rho(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (8)$$

$$\sigma(x) = \left[\frac{1}{N} \sum_{i=1}^N \{x_i - \rho(x)\}^2 \right]^{1/2} \quad (9)$$

$$\sigma(y) = \left[\frac{1}{N} \sum_{i=1}^N \{y_i - \rho(y)\}^2 \right]^{1/2} \quad (10)$$

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - \rho(x))(y_i - \rho(y)) \quad (11)$$

$$CC = \frac{\text{cov}(x,y)}{\sigma(x)\sigma(y)} \quad (12)$$

with $\sigma(x) \neq 0$, $\sigma(y) \neq 0$. Here x_i and y_i are the grayscale values of two adjacent pixels, N is the number of pairs (x_i, y_i) , and $\rho(x)$ and $\rho(y)$ are respectively, the mean values of x_i and y_i .

Table1 Correlation coefficients between adjacent pairs of pixels for original and encrypted images

| Correlation | | Horizontal | Vertical | Diagonal |
|-----------------|----------------|------------|----------|----------|
| Original image: | Barbara | 0.7904 | 0.8629 | 0.6612 |
| Encrypted image | | 0.0181 | 0.0174 | 0.0059 |
| Original image: | baboon | 0.8994 | 0.7897 | 0.7350 |
| Encrypted image | | 0.0142 | 0.0054 | 0.0061 |

Table 1 gives the CC values of adjacent pixels in the horizontal, vertical or diagonal directions of original images and their encrypted versions. It is clear that for the original images, the CC values are very high as compared to those of encrypted images. This clearly indicates that the adjacent pixels in the original images are strongly correlated. However, for the encrypted images, CC values are nearly zero, which means that the adjacent pixels in the horizontal, vertical or diagonal directions are weakly correlated. Figure 4(a) shows the original image of Barbara, whereas Fig 4(c) and 4(e) show the scatter plot of correlation distribution of horizontally adjacent pixels respectively in the original image and in the encrypted image. Similar information about the second image baboon is shown in Figs 4(b), 4(d) and 4(f).

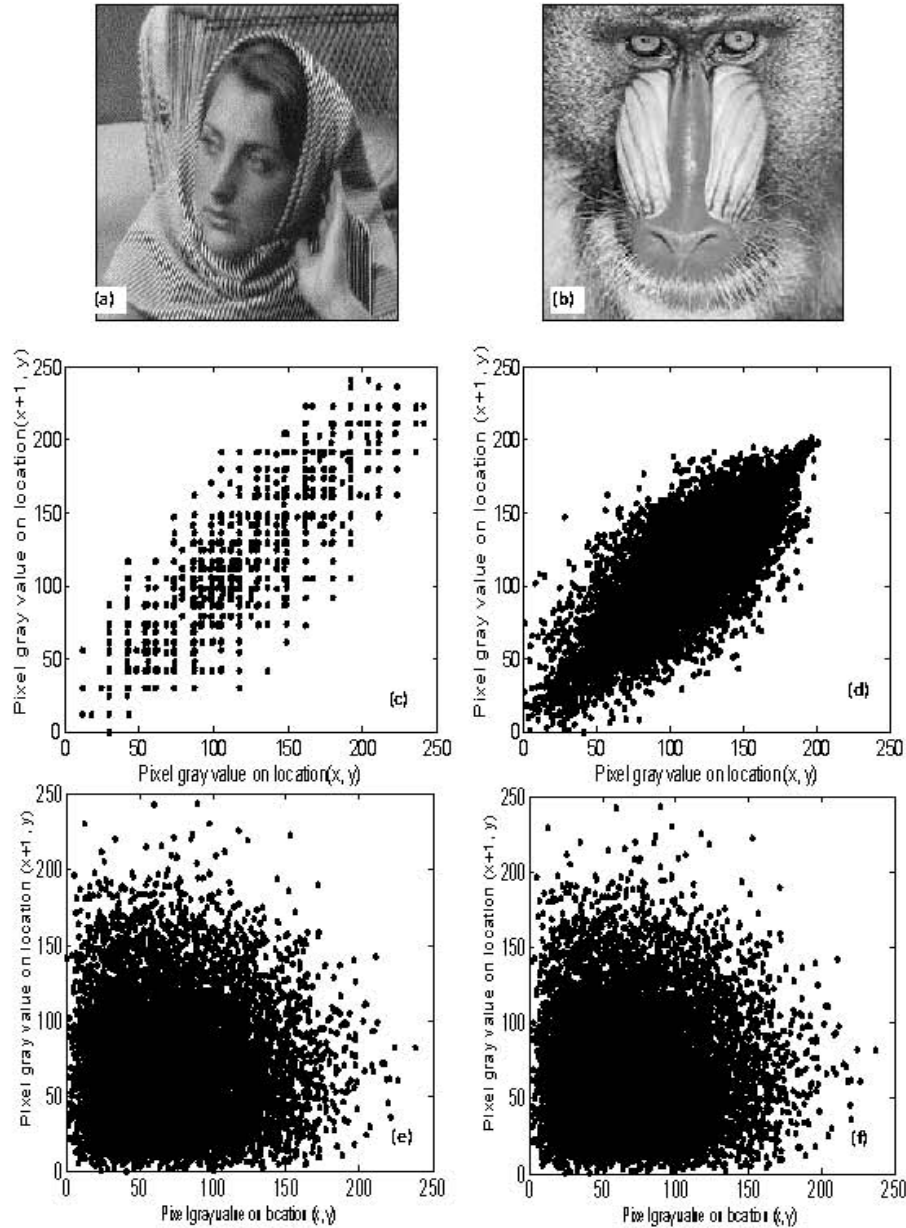


Fig 4 Simulation results: (a) input image Barbara; (b) input image of baboon; (c) correlation distribution of input image Barbara; (d) correlation distribution of input image baboon; (e) correlation distribution of Barbara encrypted image; (f) correlation distribution of baboon encrypted image.

3.2 Sensitivity analysis

We have investigated the scheme's sensitivity to various encryption parameters. The decryption in the proposed scheme depends on the SPM parameters such as focal length, wavelength, pixel spacing, and orders of the transforms, i.e., p , q of FrFT, and α and β of GT_1 and GT_2 . A series of numerical simulations have been performed with incorrect values of parameters, the correct values being $p = q = 0.3$ (FrFT orders), $\alpha = 0.4\pi$, $\beta = 0.6\pi$ (transform angles of GT_1 and GT_2), $f = 125\text{mm}$, $\lambda = 632.8\text{nm}$, and pixel spacing = 0.023 as

SPM parameters. We have considered only one wrong parameter for decryption at a time. Keeping all other parameters correct, we used $\lambda = 635.8\text{nm}$ and 637.8nm for the decryption of the first input image of Barbara (Fig 5a). The corresponding decrypted images (Figs 5b and 5c) indicate the scheme's sensitivity to a small variation of a few nanometers of wavelength. This is also confirmed by large values of the MSE (0.0916 and 0.1271). The scheme's sensitivity for the second input image of baboon is shown in Figs 5(d-f).

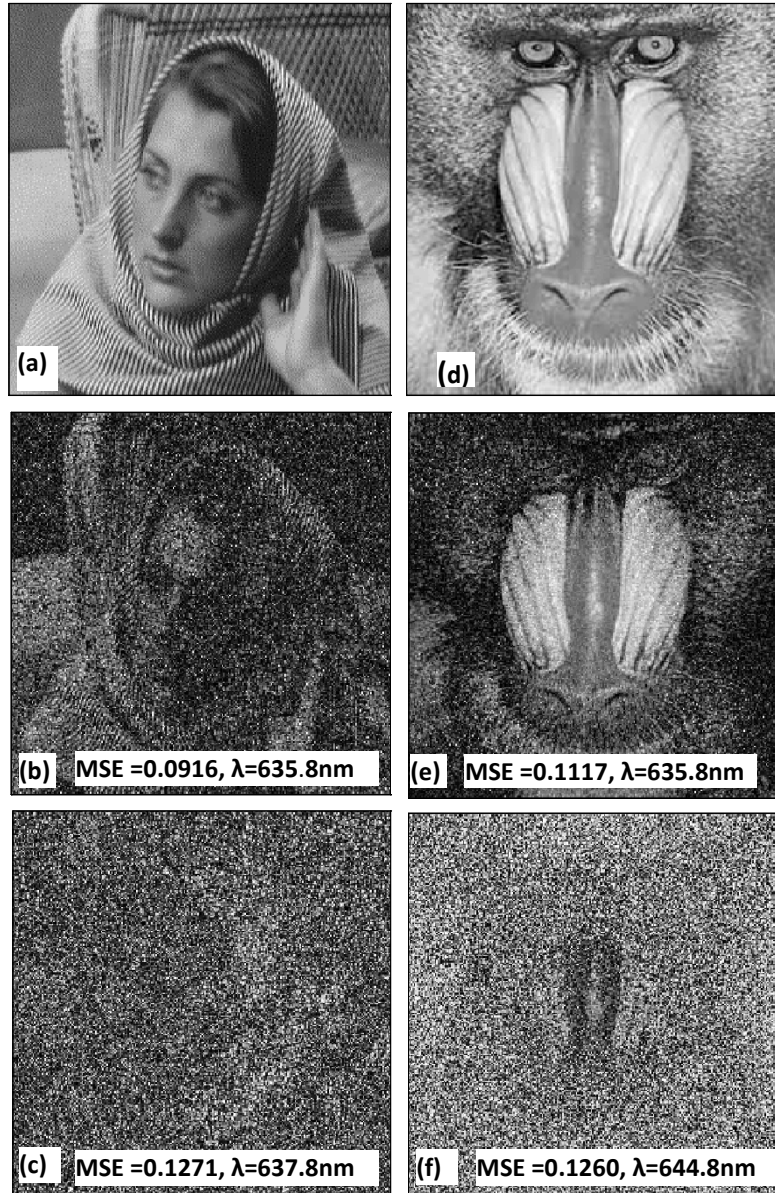


Fig 5 (a) Input image Barbara; (b-c) decrypted images with incorrect values of wavelength, (d) input image of baboon; (e-f) decrypted images with incorrect values of wavelength.(values used are shown in each figure, the correct value being 632.8nm).

We observe that there is a significant drop in quality of the decrypted image for $\lambda = 635.8\text{nm}$ (MSE = 0.1117) and the image almost disappears for $\lambda = 644.8\text{nm}$ (MSE = 0.1260). There is a progressive decline

in the quality of recovered images with increase in deviation from the correct wavelength $\lambda = 632.8\text{nm}$. We have also studied the scheme's sensitivity to the focal length (Fig 6). The decrypted images for Barbara with wrong focal lengths ($f = 126\text{mm}$ and 128mm) are shown in Figs 6(b) and 6(c). Though there appears to be slight traces/impression in Fig.6(b), the image completely disappears in Fig 6(c), thereby indicating strong sensitivity with respect to focal length. Similar results for baboon are shown in Fig 6(e) for $f = 126\text{mm}$ with $\text{MSE} = 0.1355$ where the image is just recognizable. Figure 6(f) shows the decrypted image of baboon for $f=129\text{mm}$ ($\text{MSE} = 0.1279$), where it nearly disappears.

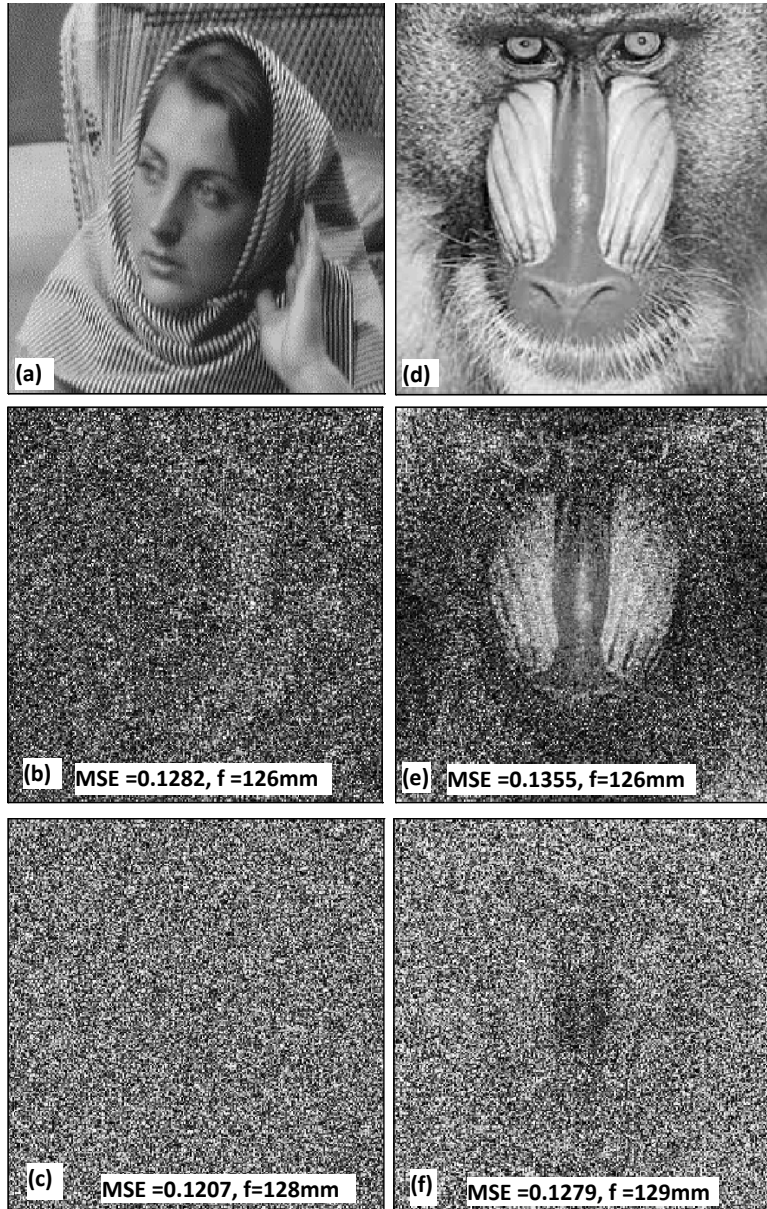


Fig 6 (a) Input image Barbara; (b-c) decrypted images with incorrect values of focal length, (d) input image of baboon; (e-f) decrypted images with incorrect values of focal length (values used are shown in each figure, the correct value being 125mm).

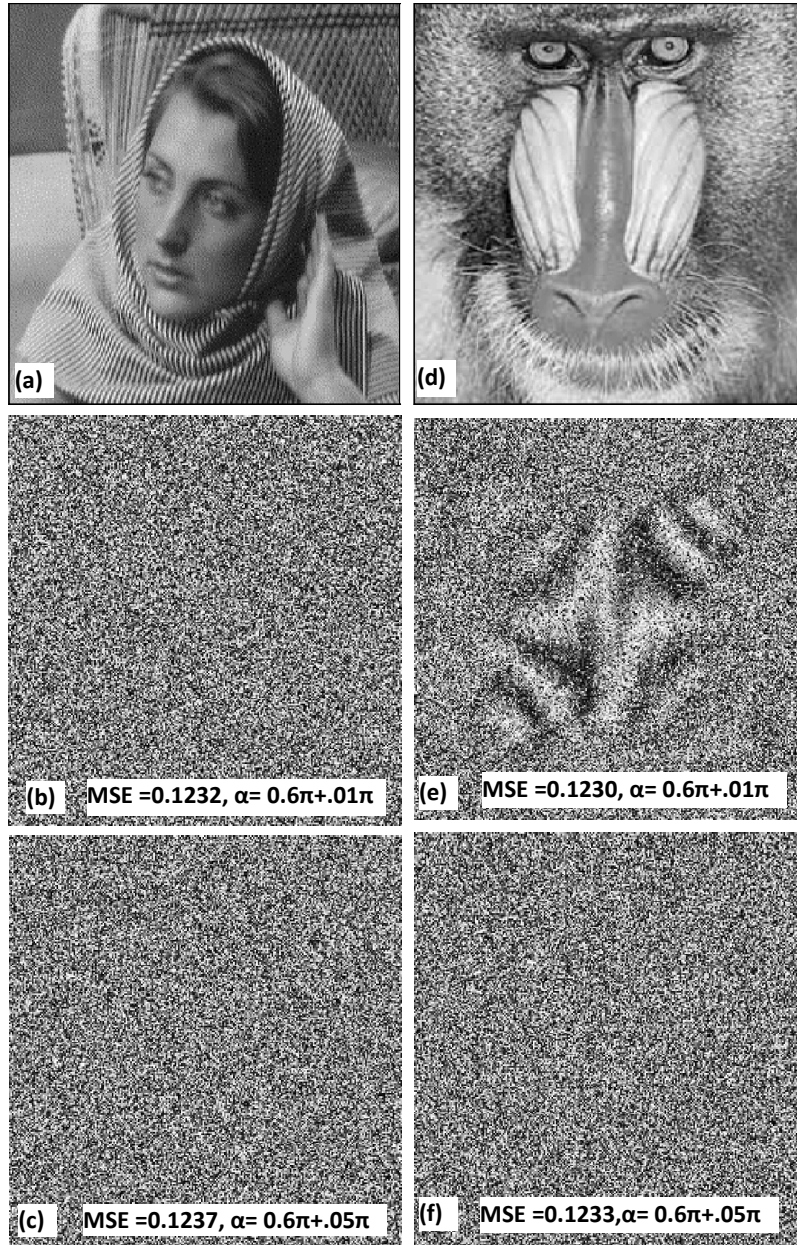


Fig 7 (a) Input image Barbara; (b-c) decrypted images of Barbara with wrong rotation angle α of gyrator transform with deviation 0.01π and 0.05π from the correct value 0.6π ; (d) Input image of baboon; (e-f) decrypted images of baboon with wrong rotation angle α of gyrator transform with deviation 0.01π and 0.05π from the correct value 0.6π .

We have verified the sensitivity with the GT rotation angle α . Figs (7b-c, 7e-f) show the decrypted images with wrong transform angles of GT, that is, $0.6\pi + 0.01\pi$ and $0.6\pi + 0.05\pi$ and the corresponding MSE values are equal to 0.1232, 0.1237 for Barbara, and 0.1230, 0.1233 for baboon respectively. The scheme is also sensitive to the orders of FrFT (Fig 8) but only for the second image, as the decryption of the first

image is independent of FrFT. Figures 8(b) and 8(c) show the respective decrypted images of baboon (Fig 8a) for deviation of 0.01 and 0.05 in the correct orders of FrFT. It is clear from the decrypted results and the MSE values that the scheme presented in the study is quite sensitive to the encryption parameters λ , f , and transform orders of FrFT and GT. We would like to point out that we have observed greater sensitivity for the first image, I_1 as compared to I_2 in all the cases. This is perhaps due to the fact that encryption of I_1 is based on addition in the frequency domain against subtraction for I_2 .

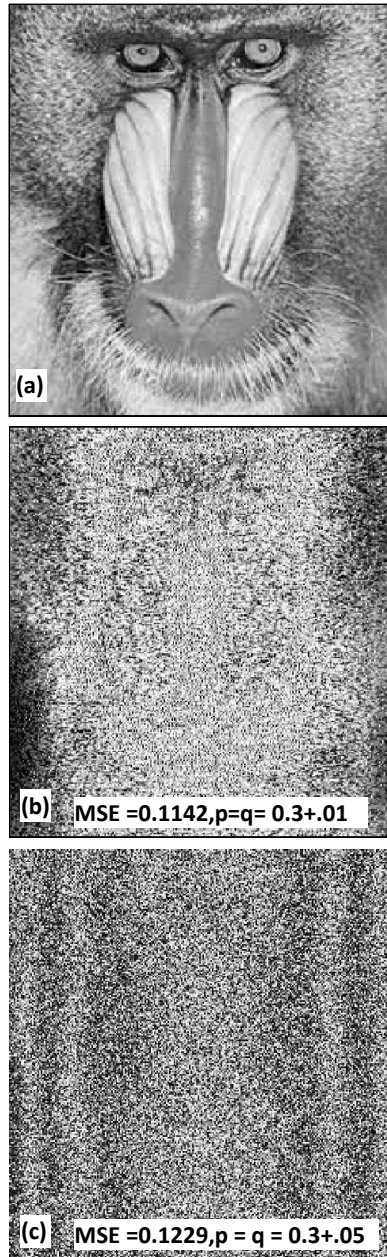


Fig 8 (a) Input image of baboon; (b-c) decrypted images of baboon with incorrect FrFT order (p, q) with deviation of 0.01 and 0.05 from the correct value 0.3.

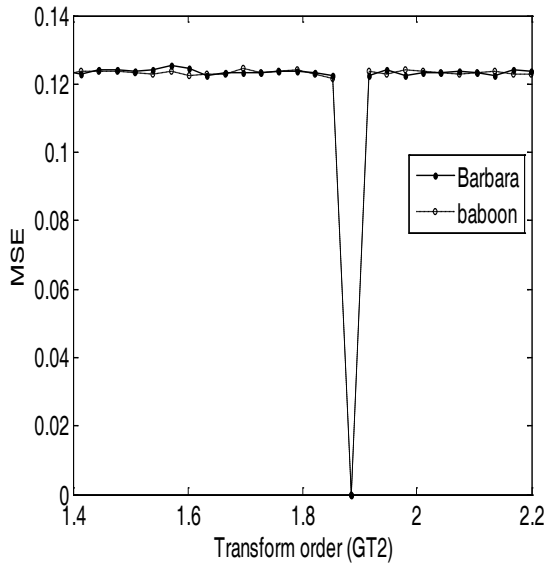


Fig. 9(a)

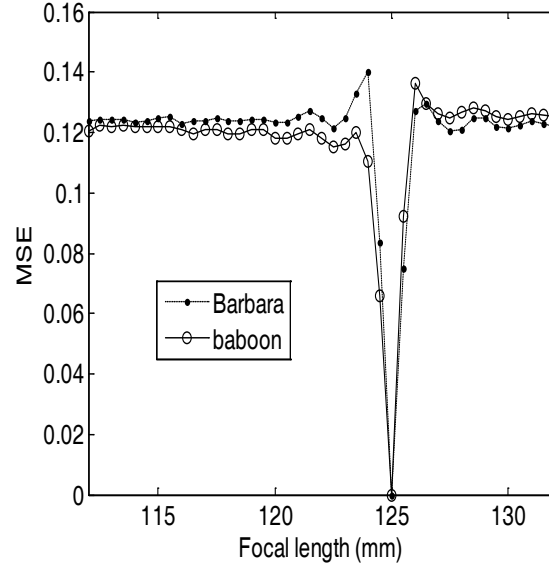


Fig. 9(c)

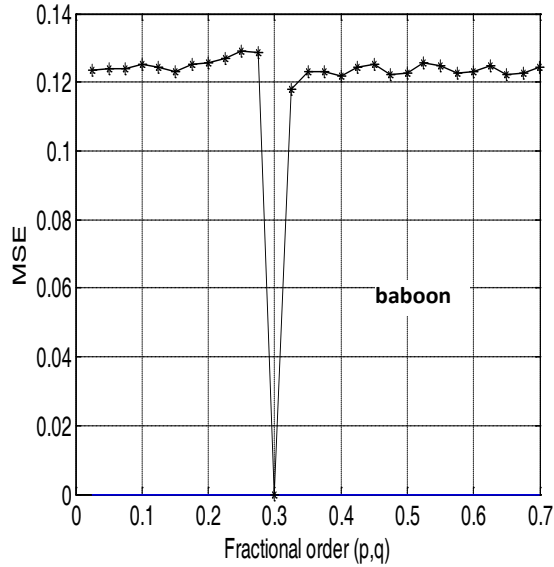


Fig. 9(b)

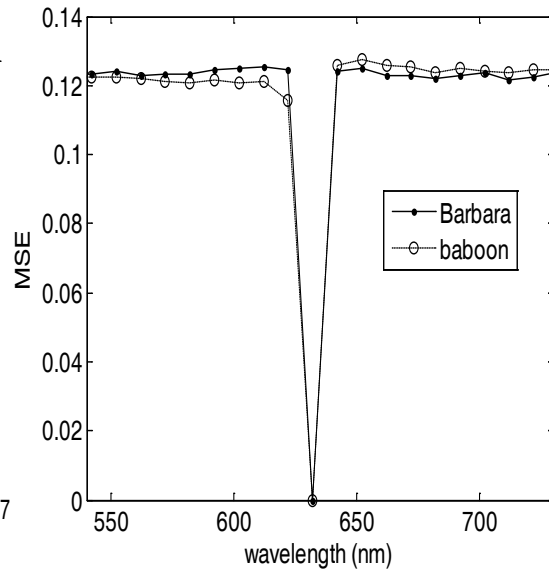


Fig. 9(d)

Fig 9 (a) Plot of MSE as a function of the transform orders of GT_2 ; (b) plot of MSE as a function of the FrFT orders; (c) MSE plot with various values of focal length; (d) MSE plot with various values of wavelength.

Further, in Fig 9, we have shown the plots of MSE against focal length, wavelength and transform orders. The curves of MSE between the input and their corresponding recovered images are plotted as a function of transform angle at an interval of $\alpha = 0.025\pi$ in Fig 9(a). In Fig 9(b), we have shown the MSE curve for the second image baboon as a function of FrFT orders. In both the plots (Figs 9a, 9b), MSE approaches zero when the images are decrypted with correct transform orders, whereas it increases sharply in case of even a slight departure from the correct orders. From the curves of MSE, it may be observed that the scheme is very sensitive to the variation in orders of GT and FrFT. The proposed scheme is examined

for its sensitivity to the parameters of SPM through MSE curves. We have presented the sensitivity plots of MSE with focal length and wavelength in Fig 9(c) and 9(d), respectively. It was found that the scheme is very sensitive to a small variation of $\pm 1\text{mm}$ in focal length (Fig. 9c). As observed from the MSE curves in Fig 9(d), the scheme is also sensitive to wavelength. A careful examination of the MSE curves reveals an asymmetric behavior on either side of the correct value of the parameter. Further, we observe fluctuations in the curves for higher values of MSE away from the correct parameter values. This behavior is attributed to the phase images as input. Such a behavior is not observed for amplitude images using the present scheme.

3.3 Occlusion attack analysis

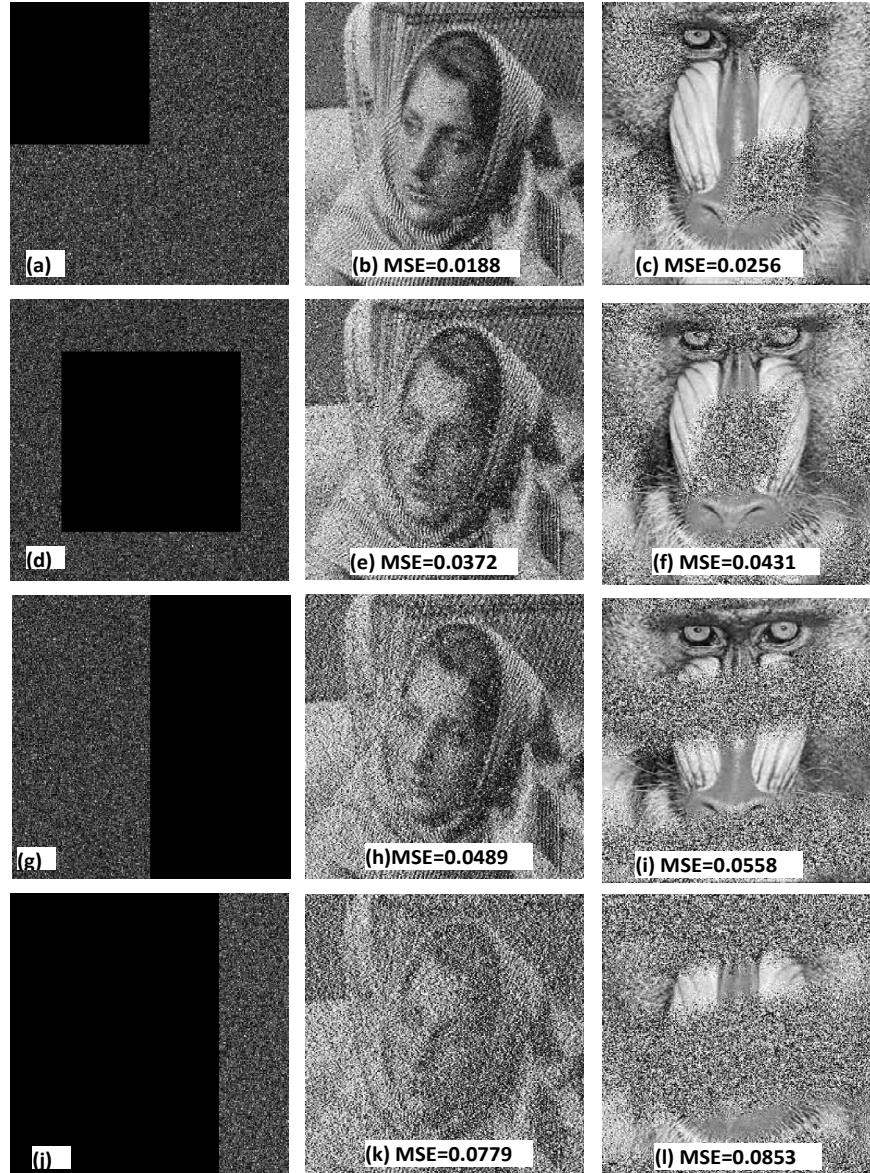


Fig 10 (a) Encrypted image with one-fourth part occluded in top-left corner, and (b-c) recovered images of Barbara and baboon respectively; (d) central half part occluded in the encrypted image, and (e-f) their recovered images respectively; (g) right-half part occluded in the encrypted image, and (h-i) their recovered images, respectively; (j) three-fourth left part occluded in encrypted image, and (k-l) their recovered images, respectively.

We examine the robustness of the proposed algorithm against occlusion attacks. When one-fourth of the encrypted image is occluded at the top-left corner (Fig 10a), the corresponding recovered images of Barbara (MSE = 0.0188) and baboon (MSE = 0.0256) are shown respectively in Figs 10(b) and 10(c). When half of the image is occluded in the center (Fig.10d), the corresponding recovered images of Barbara (MSE = 0.0372) and baboon (MSE = 0.0431) are shown respectively, in Figs 10(e) and 10(f). Similarly, when the right-half of the encrypted image is occluded (Fig. 10g), the effect of occlusion can be seen in Fig. 10(h) for Barbara (MSE = 0.0489) and in Fig. 10(i) for baboon (MSE = 0.0558). The last row of Fig 10 shows the effect of three-fourth left occlusion of the encrypted image (Fig. 10j) and the corresponding recovered images of Barbara (MSE = 0.0779) and baboon (MSE = 0.0853) in respectively, Figs 10(k) and 10(l). The quality of these decrypted images indicates the robustness of the proposed scheme against occlusion. It may be noted that even for 50% image loss, the information of the original image is clearly distinguishable. A plot of percentage of occlusion on encrypted images with MSE is shown in Fig 11, which indicates a steady increase in MSE with degree of occlusion.

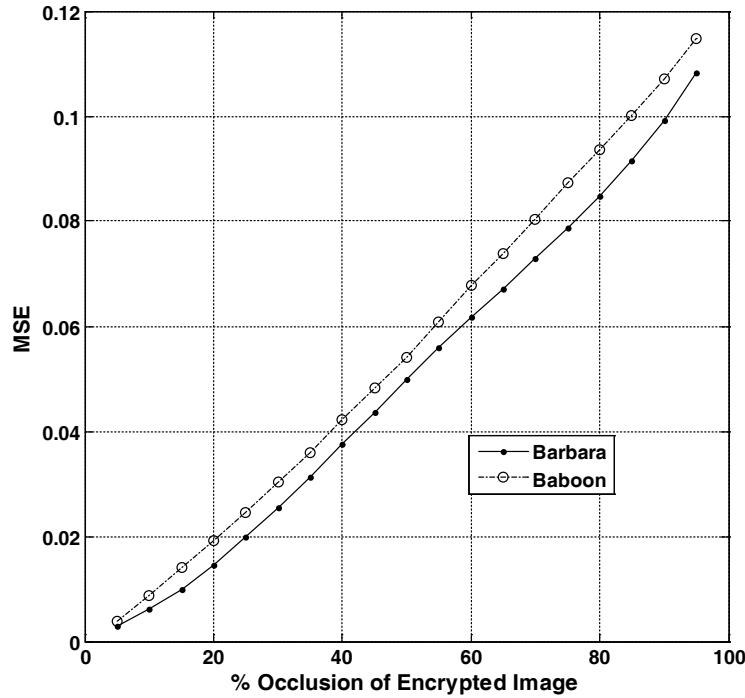


Fig 11 Plot of MSE with occluded area on encrypted image.

4 Conclusions

In the present paper, we have proposed an encryption scheme for double fully-phase grayscale images. The scheme uses random phase masks in the input plane and a common structured phase mask in the frequency plane. The structured phase mask is preferred over the random phase mask to introduce parameters that enlarge the keyspace. The use of SPM helps in overcoming the problem of axis alignment of the optical setup, and also enhances the system security. The proposed scheme uses FrFT in the input plane, for one of the double images, and GT for the other. However, in the frequency domain, GT is used for both the images. The scheme has been validated and its efficacy has been evaluated from the computed values of MSE between input and decrypted images. We have also examined the scheme's sensitivity for transform orders and parameters of SPM. The numerical simulations have been performed on MATLAB 7.1 and we have

found the scheme to be sensitive to the encryption parameters. We have also verified its robustness against occlusion attacks. Though the design of the scheme and presence of the additional parameters in encryption of double phase-images adds to the security of the system, with the rapid advancement of computational technology and emergence of new techniques, the system security may become vulnerable to attacks in future.

References

1. Javidi B (Ed), Optical and Digital Techniques for Information Security, Springer-Verlag; 2005.
2. Singh K, Unnikrishnan G, Nishchal N K, Photorefractive optical processing for data security, *Proc SPIE*, 4803(2002)205-219.
3. Singh K, John R, Joseph J, Encrypted holographic memories for information security, *Bull Laser Spectrosc Soc, India* No. 2005-06; 15:1-19.
4. Matoba O, Nomura T, Perez-Cabre E, Millan M S, Javidi B, Optical techniques for information security, *Proc IEEE*, 97(2009)1128-1148.
5. Kumar A, Singh M, Singh K, Speckle coding for optical and digital data security applications:, Chap. 6, pp.239-299, in "Advances in Speckle Metrology and Related Techniques", Ed G H Kaufmann, Wiley-VCH, 2011.
6. Liu Shi, Guo C-li, Sheridan J T, A review of optical encryption techniques, *Opt Lasers Engg*, 57(2014)327-342.
7. Chen W, Javidi B, Chen X-d, Advances in optical security system, *Adv Opt Photon*, 6(2014)120-155.
8. Wolf K B, Geometric optics on phase space, Springer-Verlag, Berlin; 2004.
9. Rodrigo J A, Alieva T, Calvo M L, Gyrator transform: properties and applications, *Opt Express*, 15(2007)2190-2203.
10. Rodrigo J A, Alieva T, Calvo M L, Applications of gyrator transform for image processing, *Opt Commun*, 278(2007)279-284.
11. Rodrigo J A, Alieva T, Calvo M L, Experimental implementation of the gyrator transform, *J Opt Soc Am A*, 24(2007)3135-3139.
12. Pei S-C, Ding J-J, Properties, digital implementation, applications, and self-image phenomena of the gyrator transform, 17thEurop. Signal Process. Confer. (EURASIP, 2009), Glasgow, Scotland, Aug. 24-28, 2009, pp 441-445.
13. Abuturab M R, Color image security system using double random-structured phase encoding in gyrator domain, *Appl Opt*, 51(2012)3006-3016.
14. Abuturab M R, Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain, *Opt Laser Technol*, 45(2013)525-532.
15. Abuturab M R, An asymmetric color image cryptosystem based on Schur decomposition in gyrator domain, *Opt Lasers Engg*, 58(2014)39-47.
16. Singh N, Sinha A, Digital image watermarking using gyrator transform and chaotic map, *Optik*, 121(2010)1427-1437.
17. Ma J-p, Liu Z-j, Guo Z-g, Double-image sharing encryption based on associated fractional Fourier transform and gyrator transform, *Chinese Opt Lett*, 3(2010)290-292.
18. Liu Z-j, Chen D, Ma J, Wei S, Zhang Y, Dai J-m, Liu S-t, Fast algorithm of discrete gyrator transform based on convolution operation, *Optik*, 122(2011)864-867.
19. Li J-z, An optimized watermarking scheme using an encrypted gyrator transform computer generated hologram based on particle swarm optimization, *Opt Express*, 22(2014)10002-10016.
20. Wang Q, Guo Q, Lei L, Multiple-image encryption system using cascaded phase mask encoding and a modified Gerchberg-Saxton algorithm in gyrator domain, *Opt Commun*, 320(2014)12-21.
21. Chen J-x, Zhu Z-l, Liu Z-j, Fu C, Zhang L-b, Yu H, A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domain, *Opt Express*, 22(2014)7349-7361.
22. Shao Z-h, Shu H-h, Wu J-s, Dong Z-f, Coatrieux G, Coatrieux J L, Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain, *Opt Express*, 22(2014)4932-4942.

23. Barrera J F, Henao R, Torroba R, Optical encryption method using toroidal zone plates, *Opt Commun*, 248(2005) 35-40.
24. Barrera J F, Henao R, Torroba R, Fault tolerances using toroidal zone plate encryption, *Opt Commun*, 256(2005) 489-494.
25. Rajput S K, Nishchal N K, Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask, *Appl Opt*, 51(2012)5377-5386.
26. Vashisth S, Singh H, Yadav A K, Singh K, Devil's vortex phase structure as frequency plane mask for encryption using the fractional Mellin transform, *Int J Opt*, 2014, Art ID 728056, 9 pages.
27. Javidi B, Sergent A, Fully phase encoded key and biometrics for security verification, *Opt Engg*, 36(1997)935-942.
28. Towghi N, Javidi B, Luo Z, Fully phase encrypted image processor, *J Opt Soc Am A*, 16(1999)1915-1927.
29. Javidi B, Towghi N, Maghzi N, Verrall S C, Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption, *Appl Opt*, 39(2000)4117-4130.
30. Tan X, Matoba O, Shimura T, Kuroda K, Javidi B, Secure optical storage that uses fully phase encryption, *Appl Opt*, 39(2000)6689-6694.
31. Nishchal N K, Joseph J, Singh K, Fully phase encryption using fractional Fourier transform, *Opt Engg*, 42(2003) 1583-1588.
32. Nishchal N K, Joseph J, Singh K, Fully phase-based encryption using fractional order Fourier domain random phase encoding: error analysis, *Opt Eng*, 43(2004)2266-2273.
33. Nishchal N K, Joseph J, Singh K, Fully phase-encrypted memory using cascaded extended fractional Fourier transform, *Opt Lasers Engg*, 42(2004)141-151.
34. Singh M, Kumar A, Singh K, Secure optical system that uses fully phase-based encryption and lithium niobate crystal as phase contrast filter for decryption, *Opt Laser Technol*, 40(2008)619-624.
35. Ozaktas H M, Zalevasky Z, Kutay M A, The Fractional Fourier Transform with Applications in Optics and Signal Processing, John Wiley and Sons, New York, 2001.
36. Mendlovic D, Ozaktas, H M, Fractional Fourier transforms and their optical implementation: I, *J Opt Soc Am*, A10(1993)1875-1881.
37. Ozaktas H M, Mendlovic D, Fractional Fourier transforms and their optical implementation: II, *J Opt Soc Am*, A10 (1993)2522-2531.
38. Loukhaoukha K, Chouinard J-Y, Berdai A, A secure image encryption algorithm based on rubik's cube principle, *J Elect Comput Eng*, Vol 2012, Art 173931, 1-9.
39. Zhou N-r, Zhang A, Zheng F, Gong L, Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, *Opt Lasers Technol*, 62(2014)152-160.

[Received: 1.5.2014; accepted: 15.5.2014]