International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Image Encryption Using Structured Phase Mask in Fractional Fourier Domain

PoonamLata Yadav[1], Hukum Singh[2]

[1]*Department of Applied Sciences, Singhania University, Pacheri Beri, Raj., (India)*

[2]*Department of Applied Science, The NorthCap University, Gurgaon, (India)*

ABSTRACT

In order to enrich the security of the image cryptosystem and to defend it from the intruders, this paper recommends a new asymmetric cryptosystem based on Fractional Fourier Transform which adds non linearity by including cube and cube root operation in the image encryption and decryption paths separately. In this cryptosystem Structured Phase Mask (SPM) and Hybrid Mask (HM) are used as the encryption keys and the phase masks generated after the cube operation in the encryption scheme are earmarked as the decryption keys and we make use of cube root operation to decrypt image in the decryption process. The cube and the cube root operations used make the cryptosystem resilient against various attacks. Recommended scheme strengthens the safety of DRPE by growing the key space and the number of parameters for safety and robust against various attacks. The strength of the recommended cryptosystem has been calculated on the basis of various constraints by simulating on MATLAB 7.9.0 (R2008a). A set of simulated results shows the power of the proposed asymmetric cryptosystem.

***Key words*:Asymmetric Cryptosystem, DRPE, Fractional Fourier Transform, Hybrid Phase Mask,Structured Phase Mask..**

I. INTRODUCTION

Because of the fast development of Internet and computer technologies, the protection of digital and optical imaging has become very difficult.It is in great demand to maintain the discretion of these images so that no third party can have access for these images. One of the ways by which we can provide privacy in these fields is cryptographic methods .This can be done through optical image encryption methods [1-4] which is one of the best methods for encryption and safeguarding delicate information.The most successfully known practice for optical image encryption is double random phase encoding (DRPE), which was first proposed by Refregier and Javidi in 1995 [5].The DRPE is an optically symmetric key system which encrypts the input image and converts it into stationary white noise called cipher images by using two random phase masks (RPMs) using Fourier transforms [5, 6], one in input plane and another in Fourier plane. The two phase masks used are independent of each other. DRPE with Fourier transform suffers many attacks. In order to reinforce the security level DRPE was prolonged and applied with other transforms such as Fractional Fourier transform [7-15], Fresnel transform [16-20], gyrator transform [21-27], fractional Mellin transform [28-29], discrete fractional cosine transform[30], Hartley transform [31], Arnold transform [32] etc. But all these methods were used with symmetric key

encryption [33-35] which uses similar key for encoding and decoding purpose. Hence, this method brings much lethal damage to consistency as it is open to many attacks like chosen- cipher text attack [36], chosen plain image attack [37], and Known plane image attack [38-39] and grieved from various practical problems like management and key distribution.

Thus to strengthen the security system and overcome these circumstances asymmetric cryptosystem scheme [40-50] was introduced which uses two keys for encoding and decoding respectively.

In this paper a new nonlinear asymmetric cryptosystem has been recommended. The proposed scheme tries to overcome the vulnerabilities in symmetric scheme like the chosen- cipher text attack. This scheme uses cube operation while encoding image at the sender end and uses cube root operation while decoding images at the receiver end which makes it resilient against various attacks and gives very good performance. The use of cube and cube root adds lot of non-linearity in the path which makes it problematic for an attacker to find the genuine key. In the suggested scheme phase part are used as the decoding keys, for an attacker it becomes difficult to obtain the private keys and hence enhances the security. Here, we propose a combined system using SPM [51, 52] along with Hybrid Phase Mask (HM) [53]. The HM used is dissimilar from random masks used in DRPE scheme as it is caused from the angle of Fourier transform of the product of random phase masks with the secondary image.Experimental results are also provided for validation. The robustness of our proposed cryptosystem has been analyzed and verified on the basis of various factors on MATLAB 7.9.0 (R2008a) and investigational results are presented below to highlight the efficiency of the algorithm.

I.THEORETICAL ANALYSIS

In this system, a new concept of asymmetric key cryptosystem has been proposed which uses HM and SPM using FrFT.

1.1. Fractional Fourier transform

In our recommended scheme we have used DRPE in Fractional Fourier domain (FrFT) [7-15].

The FrFT of order α of an input function f(x) can be defined in terms of kernel function as follows:

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

Where the kernel function (x, u) is expressed as

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

(2)

Here, A=

Where, is the angle corresponding to the transform order α along the x- axis.

1.2. Asymmetric DRPE using phase truncation

Qin & Peng [40] proposed an asymmetric cryptosystem based on FrFT. In this cryptosystem P1 and P2 are used for encryption and the phase masks DK1 and DK2 are used for decryption.

The proposed scheme is created on FrFT using asymmetric keys. This transform is very flexible than the basic FT due to

usage of more parameters of transform order. Let I (x, y) is the input plain image which is to be encrypted. Let R1 is the

HM and R2 is the SPM which are used as the encryption keys. These mask used act as the secret key of DRPE. Let PT (.)

and AT (.) are operators for the Phase truncation and Amplitude truncation respectively. They are:

(3)

(4)

Just like DRPE the PTFT scheme also uses two independent phase masks SPM and HM as the encryption keys.

The Fig 1(a) depicts the encryption process and the stages of encryption of the original image used, it is expressed as:

$$G \quad (5)$$

$$E(x, y) : \quad (6)$$

Thus, the decryption keys developed in the encryption process are directly related to plaintext and encoding keys. Hence,

this system is much more secure since dissimilar period masks are taken for different plaintexts in each encryption technique.

The two decryption keys obtained are:

$$DK_2 = PR\,[FrFT\,(p, q)\,\{E(x, y) \times SPM\}] \quad (7)$$

$$DK_1 = PR\,[FrFT\,(-p, -q)\,\{G\,(u, v) \times HM\}] \quad (8)$$

For decryption purpose DK_1 and DK_2 serve as two private keys which are different from encoding keys SPM and HM. Fig.

1(b) depicts the decryption process, in which we can obtain input image by two steps:

$$= [\,FrFT\,(p, q)\,(E\,(x, y).\,DK_1)]^{1/3} \quad (9)$$

$$I(x, y) = [\,FrFT\,(-p, -q)\,(G\,(u, v).\,DK_2)]^{1/3} \quad (10)$$

From the processes described above it is clear that decryption is only possible because of usage of private keys DK_1 and

DK_2. Any attempt to decrypt the image without using these private keys even if we use encryption keys will fail. Our proposed

scheme is highly resistant to known plain text attacks and chosen- plain text attacks .Hence, it is a very secure method.

1.3. Hybrid Mask

The HM [53] is generated using random phase masks, R1 and the secondary image, S (x, y). R1 is first multiplied with S (x, y) and the resulting product is Fourier transformed (FT). The argument of the FT i.e. the phase part of the transformed output is the Hybrid phase Mask (HM). It is given by the equation:

(11)

Where, FT is Fourier transforms, Arg is the argument of the FT, and R1 is the conventional RPM. The Fig 2(f) – (g) represents the Hybrid Mask (HM).

1.4. Structured Phase Mask

The SPM [43, 51-52] used is very user friendly and also helps a lot in the security drive. It consists of Toroid zone plates (TZP) [54] and Radial Hilbert mask (RHM) [55-57]. The TZPs are the diffractive optical element (DOE) which cannot be replicated hence is able to maintain the secrecy of the input image information. The SPM [43] i.e, combined key is obtained from TZP and RHM. The usage of these keys will make the system much more secure and helps in increasing the key space and also makes an image edge-enhanced in comparison to original image. The complex amplitude produced by Toroid wave front is given by:

(12)

Where, k and f=400 mm, λ=632.8nm and pixel spacing =0.023.

The radial Hilbert phase function in log-polar coordinates (p,) can be written as:

(13)

Where P denotes the order of transformation. It is clear that contrary halves of any radial line of the mask have a

comparative phase difference of Pπ radian. The combined key (SPM) generated is given by:

$$V(r,p,\theta) = U(r)\ x\ H(p,\theta) = \exp\left(\frac{-iK(r)^2}{2f}\right)\ x\ \exp($$ (14)

The Toroid zone plate, Hilbert mask with Transformation order 5 and combined key(SPM) are depicted in Fig. 2(c) – (e)

respectively.

II. PROPOSED TECHNIQUE

3.1 Encoding**: I**t is an asymmetric method [40-50] which makes the scheme much more secure and confidential without any loss of information. The encoding process involves following steps:

3.1.1. In this step we first multiply the input image by the HM (R1) in the input domain and the product is cubed. The

cubing is done pixel-wise. The resultant obtained is a complex function.

3.1.2. The resultant found is then fractional Fourier transformed (FrFT). The phase truncated [44] portion gives the

intermediate function G(u, v) , given by:

$$G(u, v) = PT\{FrFT[CU[I(x, y) \times R11(x, y)]]\} \quad (15)$$

3.1.3. The G (u, v) is further multiplied with the SPM (V (u, v)) which is a combined key of TZP and RHM. And the product

is again cubed and again FrFT is applied.

$$E(x, y) = PT\{FrFT[CU[G(u, v) \times V(u, v)]]\} \quad (16)$$

Here, CU[.] represents pixel by pixel cubing, R11(x,y) and V (u,v) represents the encryption Keys. The decryption

keys DK_1 and DK_2 are given by:

$$DK_1 = PR\{FrFT[CU[I(x, y) \times R11(x, y)]]\} \quad (17)$$

$$DK_2 = PR\{FrFT[CU[G(\alpha, \beta) \times V(u, v)]]\} \quad (18)$$

Both the keys DK_1 and DK_2 are used for decryption.

3.2 Decoding:The decoding process involves following steps:

3.2.1. At first we multiply the cipher image E(x, y) with the First asymmetric key (Phase reversal part-DK_2).

3.2.2. Then we do the decryption of previous step using DRPE technique taking the FrFT.

3.2.3. The cube root of this function is done and we obtain the intermediate function G (u,v).

$$G(u, v) = PT\{FrFT[CURT[E(x, y) \times DK_2]]\} \quad (19)$$

Here, CURT [.] represents the pixel by pixel cube root operation.

3.2.4. The G (u, v) is further multiplied with the Second asymmetric key DK_1. And the cube root of this function is done and again FrFT is applied.

$$I(x, y) = PT\{FrFT[CURT[G(u, v) \times DK_1]]\} \quad (20)$$

The flowchart of cryptosystem for encryption and decryption is shown in Fig. 1(a) and 1(b).

IV. SIMULATION AND RESULTS

Numerical simulation has been performed to evaluate the effectiveness and security of the proposed cryptosystem. In our proposed simulation, an image of Barbara is used as the secondary image. In the encryption process, some parameters are set since a selected domain of cipher-text is transformed by FrFt. The Lena and Kids image, TZP, RHM, SPM, HM and the encoded images are shown in Fig. 2(a) – (h) respectively. The simulation results shown in Fig. 3(a)-(f) depicts the 3D view of original, encoded and the decoded images. Fig. 4(a) &(b) represents the decoded images with correct keys respectively. In order to check the quality of the decrypted image, proposed algorithm is checked against Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR). To evaluate the performance of the proposed algorithm, algorithm has also been analyzed against Relative Error (RE).

To prompt the quality of decoded image and to confirm the security and efficiency of the proposed scheme MSE is calculated. If $I_o(x, y)$ and $I_d(x, y)$ denotes original and the decrypted image, then MSE is calculated using

equation :

$$MSE = \frac{}{(} \quad (21)$$

The technique proposed is very secure because in order to correctly decrypt the image all the values of HM and SPM must be correctly chosen. If any of the value is wrongly chosen automatically there is error (MSE value is positive) hence, decrypted image is not obtained. The MSE obtained for the Lena and Kids image is: 1.79 x 10^{-23} and 1.14 x 10^{-23}. The MSE obtained for our algorithm is small which means it recovers high quality image and demonstrates robustness of our proposed algorithm. Fig. 5(a) & (b) depicts the curve between MSE and Fractional order for α value = 0.4 and 0.8.

Similarly, the degree of transparency of noise in the noised image is assessed by calculating the peak signal to noise ratio (PSNR) between input and noised image. PSNR measures the alteration between original image $I_o(x, y)$ and the decoded image $I_d(x, y)$ obtained using suggested algorithm. Equation (22) shows the mathematical expression of PSNR:

PSNR=10 x log { (22)

The PSNR obtained for our proposed algorithm for the Lena and Kids image is: 136.04 and 183.34 respectively. These values indicate high quality of decoded image.

4.1.1. Relative Error (RE)

It can be calculated between the original image $I_o(x, y)$ and the decoded image$I_d(x, y)$ using the proposed algorithm. Equation (23) shows the mathematical expression of the RE:

RE= (23)

If the value of RE is close about to zero it indicates the image is perfectly recovered. The value of RE for our algorithm for Lena and Kids image is: 0.0038 and 0.0042 respectively which is nearly zero. These values indicate that the images are perfectly recovered from our algorithm. Table 1 indicates comparative analysis of our proposed algorithm with the DRPE approach using FT.

4.1.2. Recovery Attack

It is a process of decryption of original image by using correct keys. Without the knowledge of receiver's private keys it is challenging task for the attack to retrieve the original image without any loss of information. Similar cases have been evaluated by the attackers where incorrect keys are used to decrypt the encrypt image. Decoded images are shown in the Fig. 4(a), (b). Various cases like interchanging the decryption keys, DK_1 uses as first decryption key and DK_2 used as second decryption key then the MSE obtained is 1.68 x 10^{+04} and 1.048 x 10^{+04} and the decrypted images are obtained in Fig. 4(c) - (d). In the next case if we use amplitude mask obtained as the decryption keys to obtain the original image, it gives 3.9574 x 10^{+04} and 5.8873 x 10^{+04} MSE and are shown in Fig. 4(e) – (f). Similarly, using the phase truncated part as the decrypted keys then the MSE obtained is 2.1172 x 10^{+04} and 3.2033 x 10^{+04} and are shown in Fig. 4(g) – (h). It is clear now that the scheme used here is very secure and it is not possible to retrieve any kind of meaningful information about the original image. Only correct keys can help in recovering the correct original image.

4.1.3. Occlusion attack

The robustness of the scheme is also verified with occlusion attacks on encrypted images. Here, some part of the encrypted image is blocked and the loss of encryption is simulated and analyzed. As a result of this the decrypted image is blurred depending on the part being blocked. Fig. 6(a) & (e) depicts the cipher text with 50% of the encrypted image occluded; the recovered image is shown in Fig. 6(b) & (f) and its MSE is 2.08 x 10^{+03}& 8.08 x 10^{+03}. Fig. 6(c) & (g) depicts the cipher text with 25% of the encrypted image occluded; the recovered image is shown in Fig. 6(d) & (h) and its MSE is 3.24 x 10^{+03}& 1.31 x 10^{+03}. Larger the value of MSE it means much bigger is the loss of information which in turn means larger the occluded area of encrypted image larger is the loss hence, we cannot retrieve the good quality of image.

4.1.4. Correlation Coefficient

In order to test the correlation coefficient (CC) of adjacent pixels, the 10,000 pairs of adjacent pixels are randomly selected in vertical, horizontal and diagonal directions from the plaintext images as well as encrypted. The CC of each pair is evaluated using equation (24):

, ,

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

c ,

(24)

With Here, , are the values of two adjacent pixels, N is the number of pairs (,), and ( ) are the mean values respectively. Table 2 gives the CC values of adjacent pixels in the horizontal, vertical and diagonal directions of original images and their corresponding encrypted versions. An illegal user cannot obtain any valid information from this statistical data. Fig 7(a) – (d) indicate the scatter plots of correlation distribution of original image and its encrypted image respectively.

4.2. Statistical Analysis

To evaluate the performance of the proposed algorithm, statistical analysis can be performed through histogram and by finding entropies of original $I_o(x, y)$ and the encrypted image E(x, y).

4.2.1. Histogram Analysis

Histogram is one very important feature in image verification. The encryption algorithm should be able to transform the input image into cipher images. The histograms of plain input images are different but if the histograms of the cipher (encrypted) images are similar then it is good encryption scheme and it is free from attacks since the attacker cannot gain useful information out of it.The histograms of the plain input image Lena and Kids and their encrypted (cipher) images are plotted in Fig. 8(a) – (d) respectively. Hence, a hacker cannot obtain useful information according to histograms properties.

4.2.2. Entropy Analysis

Entropy measures the haphazardness or uncertainty in the Cipher image. More the randomness in Cipher image, it becomes difficult for the attacker to recover the original image [I]. Mathematically entropy H can be given by equation:

(25)

Where represents the probability. The ideal value of entropy is 8. The entropies obtained for cipher image of Lena and Kids images using proposed algorithm are 5.59 and 6.2 respectively.All these values are near about the ideal value, then the loss is negligible and the proposed algorithm is strong against the entropy attack. This shows that the proposed algorithm is strong and has high randomness in cipher image.

4.2.3. Noise AttackTo check the strength of and effectiveness of the proposed algorithm, it has been analyzed against noise attack. It is certain that the noise impacts directly the quality of the decrypted image. We have taken Gaussian noise in the encrypted image. The noise interferes with the ciphered images by relation:

$$A^1 = A\,(1+kG) \qquad (26)$$

Where, A is the ciphered (encrypted) image which is without noise and A^1 is the noise affected encrypted image, k is the noise strength and G is a Gaussian noise with 0 and 1 standard deviation. By varying the noise strength the quality of the noise strength is examined. The Fig 9(a) – (d) shows the recovered images from the encrypted data distorted by Gaussian noise with standard deviations of 0.025 and 0.5 respectively. Fig. 10 illustrates the MSE curve against the noise factor (K). The quality of the recovered image declines with the increase of noise disturbances.

V.CONCLUSION

The proposed new asymmetric cryptosystem introduces non linearity by using Hybrid Mask along with SPM in the encryption and decryption paths respectively which enhances the security of the system. When an image is encoded using fractional Fourier Transform it enhances the safekeeping and discretion of the original image. The proposed method uses fractional Fourier using asymmetric keys since these keys are different for both encryption and decryption techniques. The authors have also used different masks to perform simple DRPE (HM &SPM) along with Hybrid mask which enhances the key space. The scheme is also verified against noise attack besides many other attacks.The simulation result confirms the compassion of the security parameters and the robustness of the schemes against noise and occlusion attacks and also validates the sustainability and competence of this cryptosystem.

REFERENCES

[1]O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan and B. Javidi, Optical techniques for information security, Proceedings of IEEE, 97 ,2009, pp. 1128-1148.

[2]A. Alfalou and C. Brosseau, Optical image compression and encryption methods, Adv. Opt. Photon. 1, 2009, pp. 536-589.

[3] W. Chen, B. Javidi and X. Chen, Advances in Optical security system, Adv. Opt. Photon. 6, 2014, pp. 120-155.

[4]B. Javidi,et al., Roadmap on optical security, Journals of Optics, 18 ,2016, pp. 1-39.

[5] P. Refregier and B.Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 ,1995, pp. 767-769.

[6] P. Kumar, J. Joseph and K. Singh, Double random phase encoding based optical encryptionsystems using some linear canonical transforms: Weaknesses and countermeasures, Springer series in Optical Sciences, 198, 2016, pp. 367-396.

[7]G.Unnikrishnan and K. Singh, Double random fractional Fourier domain encoding for optical security, Opt. Eng. 39(11),2000, pp. 2853-2859.

[8]G.Unnikrishnan, J.Joseph and K. Singh, Optical encryption by double random phase encoding in the fractional Fourier domain, Opt. Lett. 25,2000, pp. 887-889.

[9]N.K.Nishchal, J. Joseph and K.Singh, Fully phase encryption using Fractional Fourier transform,Opt. Eng. 42(6), 2003, pp. 1583-1588.

[10]B.M.Hennellyand J.T.Sheridan,Image encryption and fractional Fourier transform, Optik, 114, 2003, pp. 251-265.

[11]R. Tao, Y.Xin and Y.Wang, Double image encryption based on random phase encoding inthe fractional Fourier domain", Optics Express, 15-24, 2007, pp. 16067-16079.

[12] A. Sinhaand N. Singh, Optical image encryption using fractional Fourier transform and chaos,Opt. Lasers Eng. 46(2), 2008,pp. 117-123.

[13]S.K.Rajput and N.K.Nischal, Image encryption based on interference that uses fractional Fourier domain asymmetric keys, Applied Optics, 51(10), 2012, pp. 1446-1452.

[14]M. Dahiya, S. Sukhija,and H. Singh, Image encryption using Quad phase masks in fractional Fourier domain and Case study,IEEE, 2014, 978-1- 4799-2572-8.

[15]S.K.Rajput and N.K.Nischal, Optical double image security using random phase fractional Fourierdomain encoding and phase- retrieval algorithm, Optical Communication, 388,2016, pp. 38-46.

[16]O.Matoba and B.Javidi, Encrypted optical memory system using three dimensional keys in the Fresnel domain, Opt. Lett. 24 ,1999, pp. 762 -764.

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

[18]G.Situ&Zhang, Double random- phase encoding in the Fresnel domain, Opt. Lett. 29, 2004, pp. 1584-86.

[19]S.K. Rajput and N. K. Nischal, Fresnel domain nonlinear optical encryption scheme based on Gerchberg-Saxtonphase retreival algorithm", Appl. Opt. 53, 2014, pp. 418-425.

[20]H. Singh, A . K. Yadav,S. Vashisth and K. Singh, Optical image encryption using devil'svortex toroidal lens in the Fresnel transform domain, International J. of Opt., 2015, 926135:1 13.

[21]J.A.Rodrigo,T.Alieva and M.L.Calvo, Gyrator Transform: properties and applications, OpticsExpress ,15, 2007, pp. 2190-2203.

[22]N.Singh and A.Sinha,Gyrator Transform- based optical image encryption, using chaos, Opticsand Lasers in Engineering, 47(5), 2009, pp. 539-546.

[23]Z.Liu, L.Xu, C.Lin, J.Dai and S.Liu, Image encryption scheme by using iterative random phaseencoding in gyrator transform domains, Optics and Lasers in Engineering, 49(4), 2011, pp. 542-546.

[24]M.R.Abuturab, Color image security system using double random structured phase encoding in gyrator transform domain, Applied optics, 51, 2012, pp. 3006-3016.

[25]H. Singh, A.K. Yadav, S Vashisth and K. Singh, Fully- phase image encryption using doublerandom – structured phase masks in gyrator domain, Appl Opt, 2014, 53, pp. 6472-81.

[26]H. Singh, A.K. Yadav, S Vashisth and K. Singh, Double phase- image encryption using gyrator transforms, and structured phase mask in the frequency plane, Opt. Lasers Eng. 67, 2015, pp. 145-56.

[27]S. Vashisth, A . K. Yadav, H. Singh and K.Singh, Watermarking in Gyrator domain using asymmetric cryptosystem, Int. conference on Optics and Photonics, Proc. of SPIE , 96542E, 2015, 10.1117/12.2183394.

[28]N. R. Zhou, Y. Wang and L.Gong, Novel Optical image encryption scheme based on fractional Mellin transform, Opt. Commun. 284, 2011, pp. 3234-3242.

[29]S. Vashisth, H. Singh, A. K. Yadav and K. Singh, Devil's vortex phase structure as frequencyplane mask for image

encryption using the fractional Mellin transform, Int. Journal Opt., 728056, 2014, pp. 1-9.

[30]J. Wu, L. Zhang and N. Zhou,Image encryption based on the multiple order discrete fractional cosine transform, Opt. Commun. 283(9), 2010, pp. 1720-1725.

[31]L. Chen& D. Zhao,Optical image encryption with Hartley transforms, Optics Letters 31, 2006, pp. 3438-3440.

[32]M. R. Abutturab, Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain, Optics and Laser Technology 45, 2013, pp. 524-532.

[33]N. Zhou,T. Dong and J. Wu, Novel image encryption algorithm based on multiple- parameter discrete fractional random transform, Opt. Commun. 283(15), 2010, pp. 3037-3042.

[34]P. Kumar, J. Joseph and K. Singh,Double random phase encoding based optical cryptosystems using some linear canonical

transforms: Weakness and Countermeasures, Springer Series in Optical Sciences 198, 2016, pp. 367-396.

[35]H. Singh,Optical cryptosystems of color images using random phase masks in fractional wavelet transform domain, In AIP Conference Proceedings, Vol. 1728, 2016, pp. 020063-1/4.

[36] A. Carrnicer, M. Montes- Usategui, S. Arcos and I. Juvells,Vulnerability to chosen- ciphertext attacks of optical encryption schemes based on double random phase keys, Opt.Lett. 30, 2005,pp. 1644-1646.

[37]Y. Frauel, A. Castro, T.J. Naughton and B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express, 15(16), 2007, pp. 10253-10265.

[38] X. Peng, P. Zhang, H. Wei and B. Yu, Known plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 , 2006, pp. 1044-1046.

[39]S. K. Rajput&N. K. Nishchal, Known plaintext attack on encryption domain independent optical asymmetric cryptosystem, Opt. Commun. 309, 2013, pp. 231-235.

[40]W.Qin& X. Peng,Asymmetric cryptosystem based on phase truncated Fourier transforms,Opt. Lett. Vol. 35 , 2010, pp. 118-120.

[41]X. Wang & D. Zhao, Security enhancement of a phase truncation based image encryption algorithm, Applied Optics 50, 2011,pp. 6645-6651.

[42]X.Wang& D. Zhao, Double images encrypted method with resistance against the specific attack based on an asymmetric algoirthm, Optics Express 20, 2012, pp. 11994-12003.

[43]S. K. Rajput& N. Nishchal, Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask, Applied Optics, 51, 2012,pp. 5377-5786.

[44]X. Wang& D. Zhao, A special attack on the asymmetric cryptosystem based on phase truncated Fourier transform, Opt. Commun. 285(6), 2012, pp. 1078-1081.

[45]Q. Wang, Q. Guo and J. Zhaou, Color image hiding based on phase truncation and phase retrieval technique in fractional fourier domain, Optik 124, 2013, pp. 1224-1229.

[46]X. Wang, Y. Chen, C. Dai and D. Zhao, Discussion and a new attack of the asymmetric cryptosystem based on phase truncated Fourier transform, Appl Opt. 53(2), 2014, pp. 208-213.

[47] I. Mehra & N. K. Nischal, Image fusion using wavelet transform and its application toasymmetric cryptosystem and hiding, Optics Express 22, 2014, pp. 5474-5482.

[48] Anshula & H. Singh, Asymmetric image encryption scheme by using random phase masks in Fourier transform domain, The International Conference on Fibre and Photonic, 2016.

[49]A. Sinha, Non linear optical cryptosystem resistant to standard and hybrid attacks, Optics andLasers in Engineering 81, 2016, pp. 79-86.

[50]M. Khurana& H. Singh, An asymmetric image encryption based on Phase Truncated Hybrid Transform, 3D Res, 2017, 8:28.

[51] H. Singh, A.K. Yadav, S. Vashisth and K. Singh, 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.

[52]H. Singh,Cryptosystem for securing image encryption using structured phase masks in Fresnel Wavelet transform domain, 3 D Res,7-34, 2016, pp. 1-18 .

[53]R. Kumar & B. Bhaduri, Optical image encryption using Kronecker product and hybrid phase masks, Opitcs and Laser Technology, 95, 2017, pp. 51-55.

[54]J. F. Barrera,R. Henao and R. Torroba, Fault tolerances using toroidal zone plate ecryption, Opt. Comm., 2000, vol.256, pp. 489-494.

[55]J.A. Davis, D. E. McNamara and D. M. Cottrell, Image Processing with the radial Hilbert transform:theory and experiments, Opt. Lett. 25, 2000, pp. 0146-9592.

[56] M. Joshi, C. Shakher and K. Singh, Image encryption using radial Hilbert transform filter bank as an additional key in the modified double random fractional Fourier encoding architecture, Opt. Laser Eng. 48, 2010, pp. 605-615.

[57] M. Joshi, C. Shakher and K. Singh, Fractional fourier plane image encryption technique using radial Hilbert and Jigsaw transform, Opt. Laser Eng. 48, 2010, pp. 754-759.

FIGURES AND TABLES

Fig. 1(a) & (b) Flow chart for proposed Encryption and Decryption Scheme

Fig. 2 Experimental materials for simulation: (a) Lena image; (b) Kids image; (c) Toroid Zone Plate (TZP); (d) Radial

Hilbert Mask (RHM); (e) Combined Key (SPM); (f) Hybrid Mask; (g) - (h) Encoded image

Fig. 3 3D views of (a)-(b) Lena and Kids image; (c)-(d) Encoded image; (e)-(f) Decoded image

Fig. 4(a)-(b) Decoded images with correct parameters; (c)-(h) Decoded image with wrong parameters

Fig. 5(a) – (b) Plot of MSE against the fractional order for input images Lena and Kids with Fractional order 0.4 & 0.8

Fig. 6 Tolerance to an occlusion attack: (a) & (e) encoded images with 50% occlusion; (b) & (h) recovered image of (a) &

(e); (c) & (g) encoded image with 25% occlusion; (d) & (h) recovered image of (c) & (g)

Fig. 7(a) – (d) Correlation curves of input and encoded image of Lena and Kids

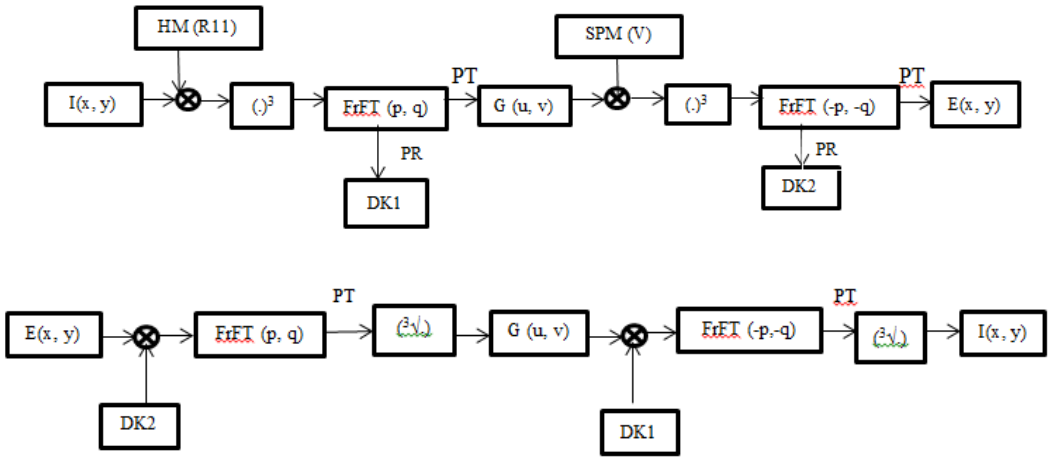
Fig. 8(a) – (d) Histograms of the Input image and encoded image

Fig. 9(a) –(d) Recovered image with Gaussian Noise 0.2 and 0.5

Fig. 10 MSE curve against the MSE and the Noise Factor (K)

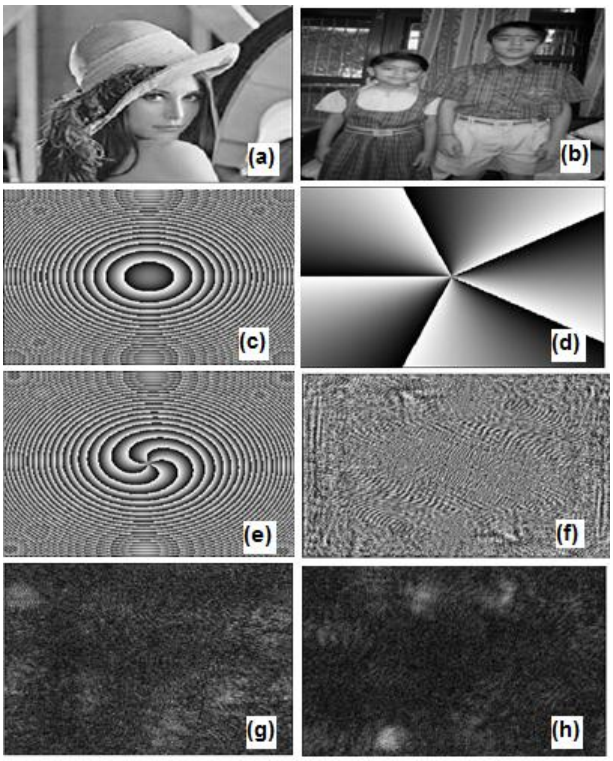
Table1: Analysis of Proposed algorithm on the basis of MSE, PSNR, RE and Entropy

Table2: Correlation coefficients of original, Encoded and decoded image using proposed algorithm



International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fig. 1(a) - (b)



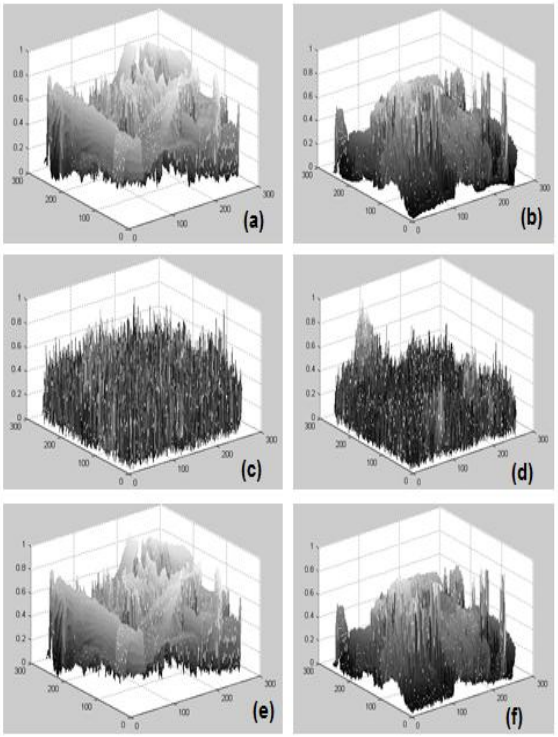
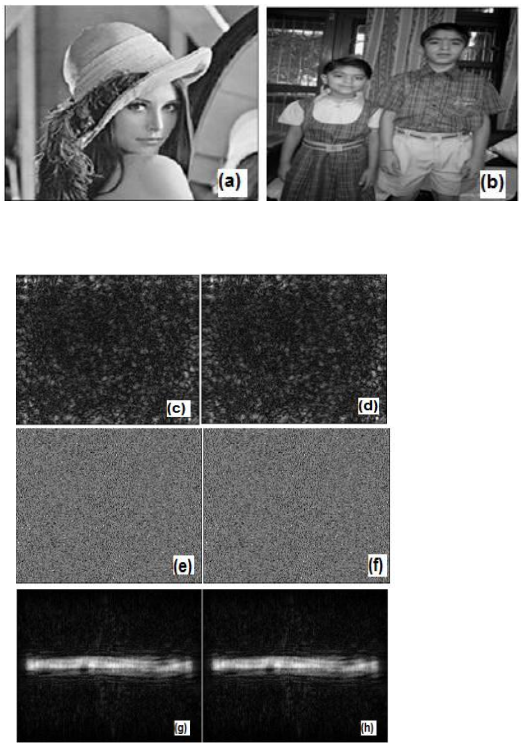
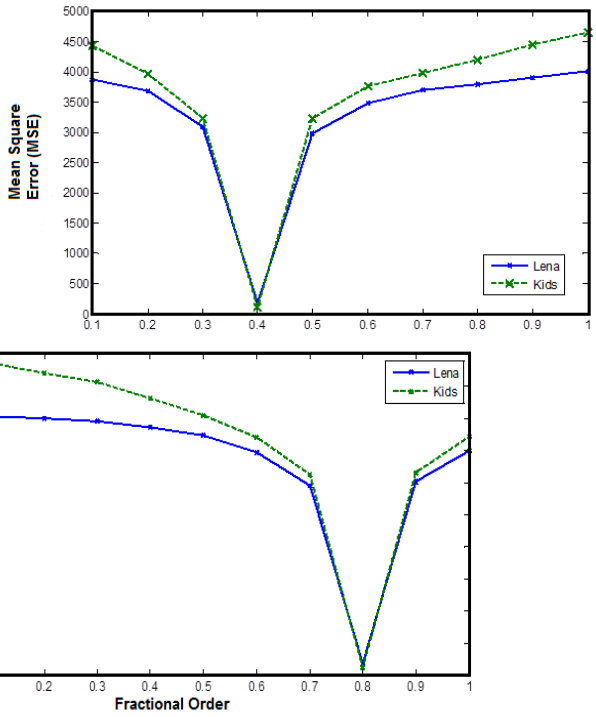


Fig. 2(a) – (h)

Fig. 3 (a) – (f)





International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fig 4 (a) – (h)

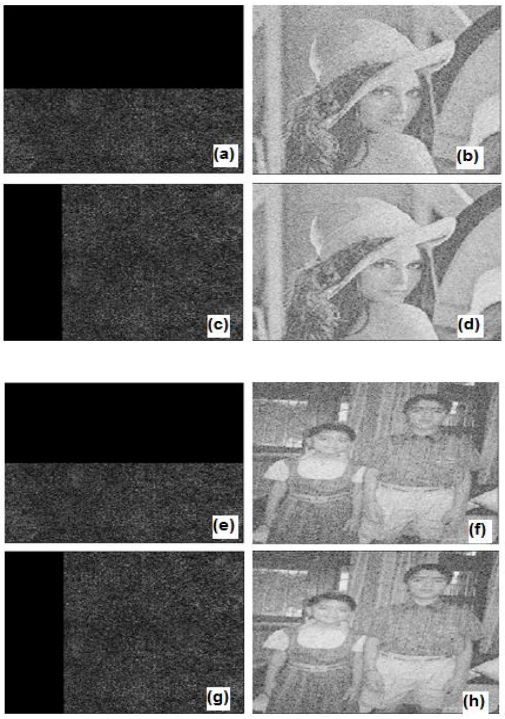


Fig. 5(a) – (b)

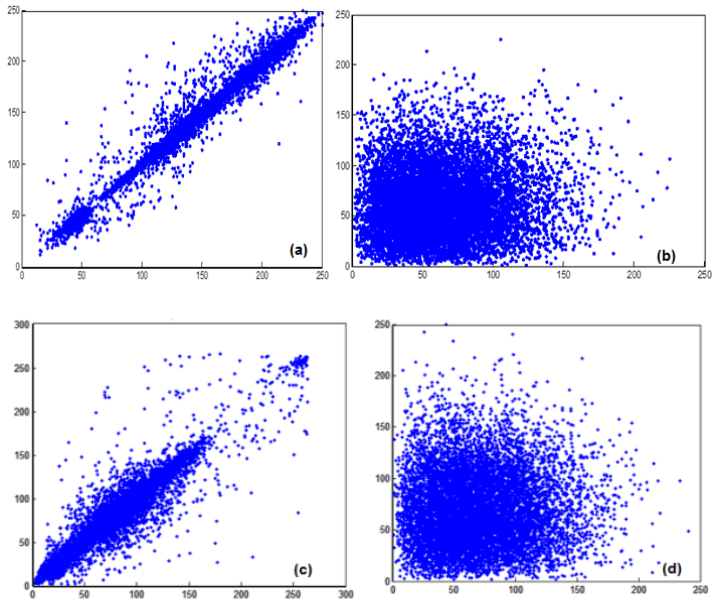


Fig. 6 (a) – (h)

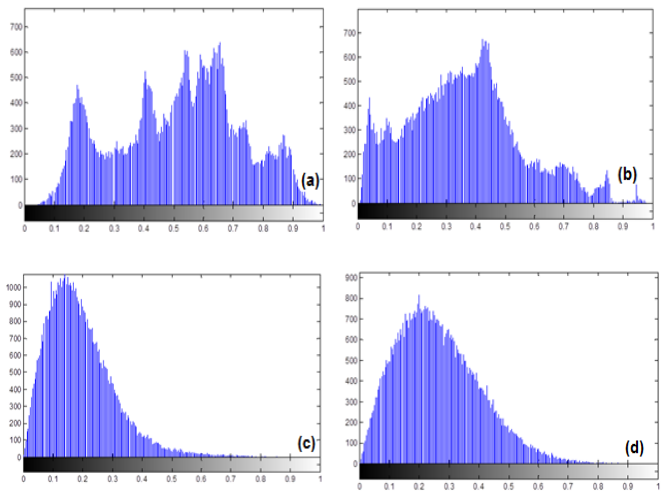


Fig. 7 (a) – (d)

Fig. 8 (a) – (d)

Fig. 9(a) – (d)

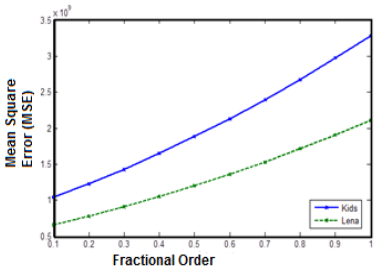


Fig. 10

Algorithm	Input Image	Parameters			
		MSE	PSNR	RE	Entropy
DRPE					
	Lena image	1.89×10^{-23}	123.94	0.0044	5.8
	Kids image	1.21×10^{-23}	168.83	0.0048	5.2
Proposed Algorithm	Lena image	1.79×10^{-23}	136.04	0.0038	5.59
	Kids image	1.14×10^{-23}	183.34	0.0042	6.2

Table 1

Algorithm	Correlation coefficients		Horizontal	Vertical	Diagonal
Proposed Algorithm	Lena Image	Original Image	0.9542	0.9836	0.9495
		Encrypted Image	0.0612	0.0251	0.0100
		Decrypted image	0.0147	0.0278	0.0044
	Kids Image	Original Image	0.9307	0.9487	0.8649
		Encrypted Image	0.0762	0.0200	0.0862
		Decrypted image	0.0169	0.0424	0.0088

Table 2