International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

An Asymmetric image encryption based on Fresnel Transform using Spiral Phase Mask and Hybrid Mask

Poonam Lata Yadav[1], Hukum Singh[2]

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

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

ABSTRACT

To enhance the security in optical image encryption scheme and to safeguard it from the invaders, this paper proposes new digital Spiral Phase Mask (SPM) based on Fresnel Transform. In this technique asymmetric cryptosystem is carried out in the Fresnel Transform (FrT) using SPM which is mixture of Fresnel Zone Plate (FZP) and Radial Hilbert Mask (RHM) along with Hybrid Mask (HM). In the proposed system we have also used a squaring and square root action in the encoding and decoding track respectively. These two operations would make the system resistant or unstable against standard attacks. Proposed scheme uses SPM which increases the key space also it increases the number of parameters for better safety and robust against various attacks. We have also used different keys for encoding and decoding purpose to make the system much more secure. The power of the proposed system has been analyzed by simulating on MATLAB 7.9.0 (R2008a).

Keywords: Fresnel Transform, Spiral Phase Mask, Hybrid Mask, Mean Square error, Peak Signal to Noise Ratio.

I.INTRODUCTION

With the increased use of internet and digital communication, here is a great need of safety for storing and passing of digital information. It is in high demand to maintain the secrecy of these images so that no third party can have access for these images. One of the ways by which we can provide security in these fields is cryptographic techniques. This can be completed through pictorial image encoding methods [1-2] which is one of the best methods for encoding and locking sensitive information. The most effective and successfully known practice for image encoding is double random phase encoding (DRPE), was first proposed by Refregier and Javidi in 1995[3]. In order to strengthen the security of data, DRPE was extended to many other transforms such as Fractional Fourier transform [4-7], Fresnel transform [8-11], gyrator transform [12-16], etc. But all these systems were used with symmetric key encryption which uses same key for encoding and decoding purpose. Hence, these systems bring much eternal damage to reliability as it is open to many attacks like chosen plain image attack, Known plane image attack [17-21]. Thus to reinforce the security system and overcome these problems asymmetric system was introduced by Qin and Peng [22]. Here, we propose a joint system using SPM [23-26] as one of the keys along with HM [27]. The SPM used is much more secure since we use more

fractional orders, for enlarging the key space we make use of fractional keys as a result of which the optical system is much more secure. The SPM is made from FZP [24] and RHM [25]. Here, a innovative hybrid asymmetric methods is suggested with an aim to overcome the weaknesses of the symmetric system. This system uses square operation while encoding image and uses square root operation while decoding images which makes it impervious to many conventional attacks [28]. This square and square root enhances non linearity hence makes it problematic for the attackers to find the real key.The power of our recommended cryptosystem has been examined and tested on the basis of various factors on MATLAB 7.9.0 (R2008a).

II.THEORETICAL ANALYSIS

2.1 Fresnel domain DRPE

In our proposed scheme we have used DRPE scheme in Fresnel domain. The FrT of an image I (x, y) at a propagation distance z, when it is illuminated by a plane wave of wavelength λ can be written as

$$F_z(u,v) = FrT_{\lambda,z}\{f(x,y)\} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} I(x,y)h_{\lambda,z}(u,v,x,y)dxdy \quad (1)$$

With $h_{\lambda,z}(u,v,x,y) = \frac{1}{\sqrt{i\lambda z}} exp\left(i\frac{2\pi z}{\lambda}\right) exp\left\{\frac{i\pi}{\lambda z}(u-x)^2 + (v-y)^2\right\}$,

Where (x,y) and (u,v) represent the coordinates of the input and output plane, the operator $FrT_{\lambda,z}$ denotes the FrT parameters λ and z, and $h_{\lambda,z}$ is kernel of the transform.

2.2 Hybrid Mask

The HM is generated using RPM, 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 HM. It is given by the equation,

HM= Arg {FT [S (x, y). R1]} (2)

Where, FT is Fourier transforms, Arg is the argument of the FT, and R1 is the predictable RPM.

2.3 Spiral Phase Mask

The joint mask SPM consist of FZP [24] and RHM [25] .The FZPs are the diffractive optical element (DOE) which cannot be replicated. The usage of these keys will make the scheme much safer and helps in increasing the key space and also makes an image edge-enhanced comparative to original image. The intricate amplitude produced by Fresnel wave front is given by

$$U(r) = \exp\left(\frac{-ik(r)^2}{2f}\right) \quad (3)$$

Where, $k = \frac{2\pi}{\lambda}$ and f=400 mm, λ=632.8nm and pixel spacing =0.023.

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

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

$$H(p,\theta) = \exp(iP\theta) \quad (4)$$

Where P denotes the order of transformation. It is clear that opposite halves of any radial line of the mask have a relative phase difference of Pπ radian. The combined key (SPM) created is given by

$$V(r,p,\theta) = U(r)xH(p,\theta) = \exp(\frac{-ik(r)^2}{2f})x\exp(iP\theta) = e^i(P\theta - \frac{k(r)^2}{2f}) \quad (5)$$

III.PROPOSED TECHNIQUE

Encoding: We make use of two keys since it is asymmetric method [27]. The steps for encryption are:

3.1.1 In this step we first multiply the original image by the HM (R11) in the input domain and the product is squared. The squaring is done pixel-wise.

3.1.2 The resultant obtained is then Fresnel transformed. The phase truncated [28] portion gives the intermediate function G (α, β) , given by

$$G(\alpha, \beta) = PT\ \{FrT\ [SQ\ [I(x, y)\ x\ R11(x, y)]]\} \quad (6)$$

3.1.3 The G (α, β) is further multiplied with the SPM (V (u, v)) which is a combined key of FZP and RHM. And the product is again squared and again FrT is applied.

$$E(x, y) = PT\ \{FrT\ [SQ\ [G(\alpha, \beta)\ x\ V(u, v)]]\} \quad (7)$$

Here, SQ [.] represents pixel by pixel squaring, R11(x, y) and V (u, v) represents the masks used for encoding and K_1 (u, v) and K_2 (x, y) are the keys used for decoding. These keys are:

$$K_1(u, v) = PR\ \{FrT\ [SQ\ [I(x, y)\ xR11(x, y)]]\} \quad (8)$$

And

$$K_2(x, y) = PT\ \{FrT\ [SQ\ [G(\alpha, \beta)\ x\ V(u, v)]]\} \quad (9)$$

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- K_2).

3.2.2. Then we do the decoding of previous step using DRPE technique taking the FrT

3.2.3. The square root of this function is done and we obtain the intermediate function G (α, β).

$$G(\alpha, \beta) = PT\ \{FrT\ [SQRT\ [E(x, y)\ x\ K_2(x, y)]]\} \quad (10)$$

Here, SQRT [.] represents the pixel by pixel square root operation.

3.2.4. The G (α, β) is multiplied with the Second asymmetric key K_1 (u, v). Then we apply FrT and take the square root of this function.

$$I(x, y) = PT\ \{FrT\ [SQRT\ [G(\alpha, \beta)\ x\ K_1(u, v)]]\} \quad (11)$$

The flowchart of cryptosystem for encoding and decoding is revealed in Fig. 1(a) and 1(b).

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

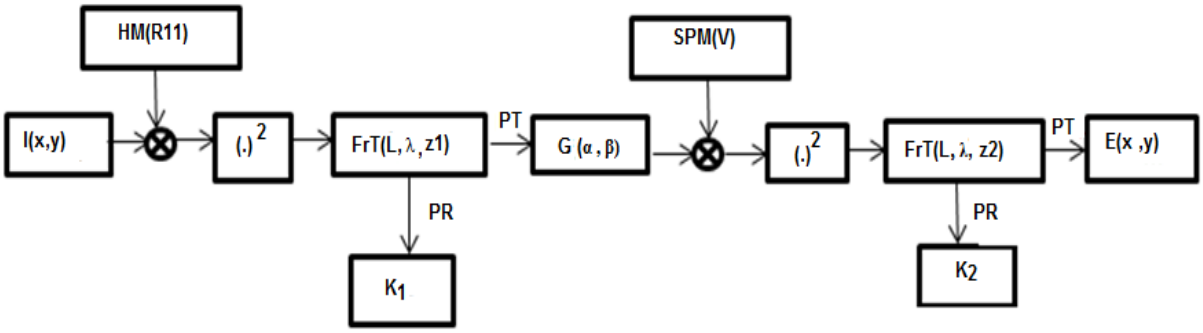

Fig. 1(a) Encoding scheme

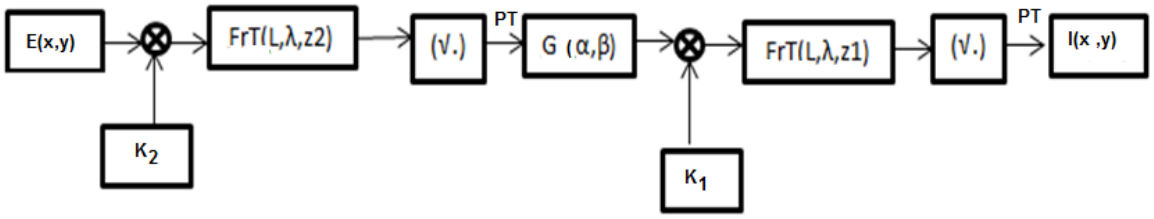

Fig. 1(b) Decoding scheme

IV.SIMULATION AND RESULTS

We have performed the numerical simulation of the proposed system using MATLAB 7.9.0 (R2008a). Two original images 256×256 pixels namely: Lena and Barbara are chosen. Fig. 2(a) and 2(b) shows the Lena and the Barbara images. For encoding purpose some parameters are set because a selected domain of cipher-text is transformed by FrT. For simplicity we use SPM proposed by Barrera etal.[23] Fig. 2(c), 2(d) and 2(e) shows the FZP ,RHM with p=5 and SPM respectively. Fig. 2(f) represents the HM used, Fig. 2(g) and 2(h) indicate the noise affected encoded images and Fig. 2(i) and 2(j) represents the encoded images. We have finally decoded the images using phase retrieval keys (K_1 & K_2) to check the correctness of the technique used. Fig. 2(k) and 2(l) shows the final decrypted image using the accurate keys. In order to check the excellence of the decoded image, proposed system is checked against Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR).

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

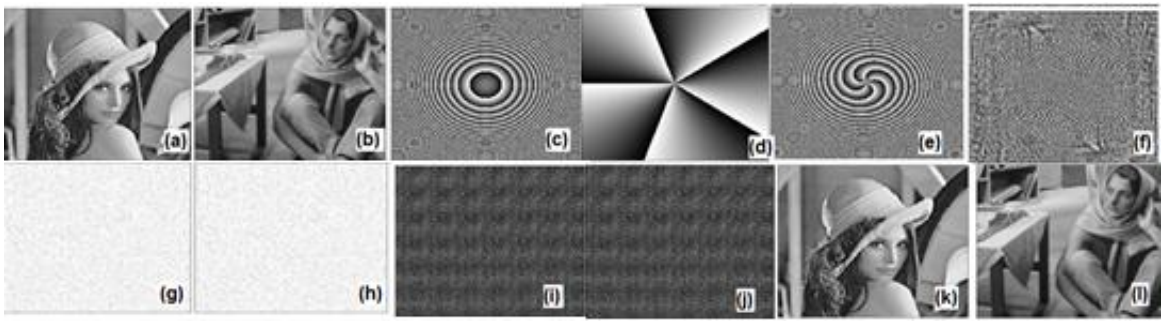

Fig. 2

MSE helps in calculating the safekeeping and efficacy of the proposed system. MSE verifies the quality of the final recovered image. If $I_o(x, y)$ and $I_d(x, y)$ denotes original and the decrypted image, then MSE is calculated using equation (12)

$$MSE = \frac{1}{(M \times N)} \sum_{x=1}^{M} \sum_{y=1}^{N} \left| I_o(x,y) - I_d(x,y) \right|^2 \quad (12)$$

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 thereis error (MSE value is positive) hence, decrypted image is not obtained. The MSE obtained for the two input image Lena and Barbara are: 3.85×10^{-25} and 6.10×10^{-25}. MSE is a normalized error function. These values are microscopic which means it recovered high eminence image and this signifies the strength of our proposed system. Fig. 3 depicts the curve between MSE and Fractional order of α value = 0.4.

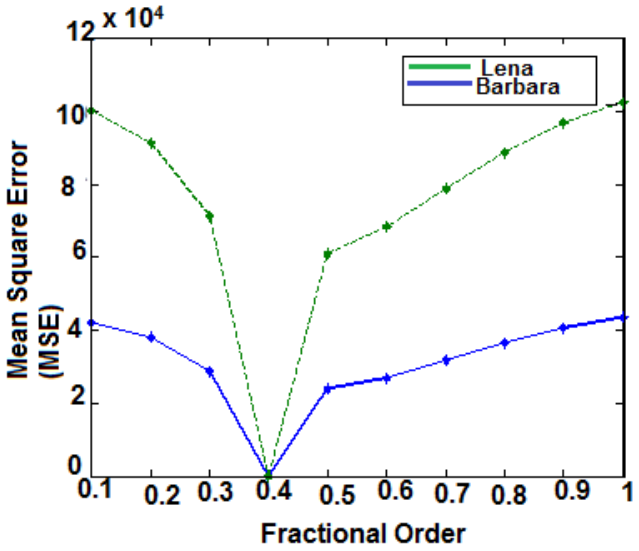

Fig. 3 Plot of MSE against Fractional order

Similarly, the degree of transparency of noise in the noised image is assessed by calculating the PSNR between input and noised image. PSNR measures the difference between original image $I_o(x, y)$ and the decoded image $I_d(x, y)$ obtained using suggested algorithm. Equation (13) shows the mathematical expression of PSNR,

$$PSNR = 10x\log\{\frac{(255)^2}{\frac{1}{(M\times N)}\sum_{x=1}^{M}\sum_{y=1}^{N}|\ I_o(x,y) - I_d(x,y)|^2}\} \quad (13)$$

The PSNR obtained for our suggested algorithm for both the images Lena and Barbara are292.42 and 257.34 respectively. These values indicate high eminence of decoded image.

4.1.1. NOISE ATTACK

To check the strength and efficacy of the suggested system, it has been investigated against noiseattack. It is certain that the noise impacts directly the quality of the decoded image. We have taken Gaussian noise in the encoded image. The noise hinders with the ciphered images by relation

$$A^1 = A(1+kG) \quad (14)$$

Where, A is the ciphered (encoded) image which is deprived of noise and A^1 is the noise affected encoded image, k is the noise power and G is a Gaussian noise with 0 and 1 standard deviation.

Fig. 4 indicates the plot of MSE against the noise factor (K).

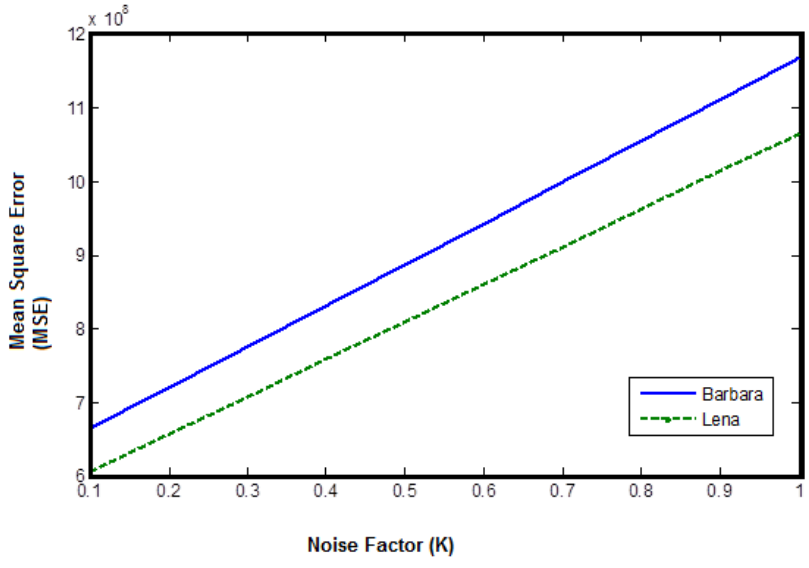

Fig. 4 Plot of MSE against Noise Factor (K)

4.1.2. HISTOGRAM ANALYSIS

The encoding system should be able to convert the original image into cipher images. The histogramsof original images are dissimilar but if the histograms of the cipher (encoded) image are similar then it is good encoding scheme and it is open from attacks since the invader cannot gain useful information out of it. The histograms curves of the original images and encoded images are shown in Fig. 5(a) and 5(b) and Fig. 6(a) and 6(b) respectively.

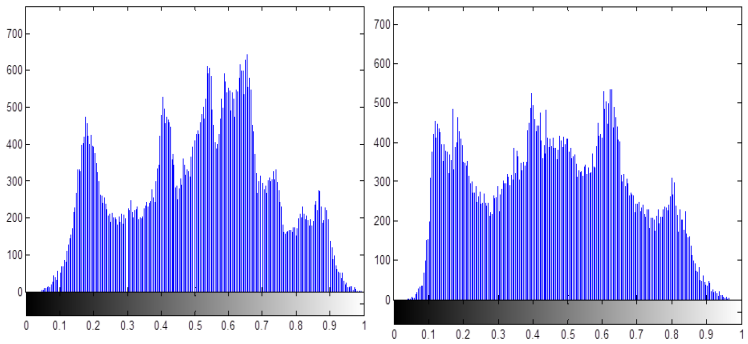

Fig. 5(a), 5(b) Histograms of the Lena and Barbara image

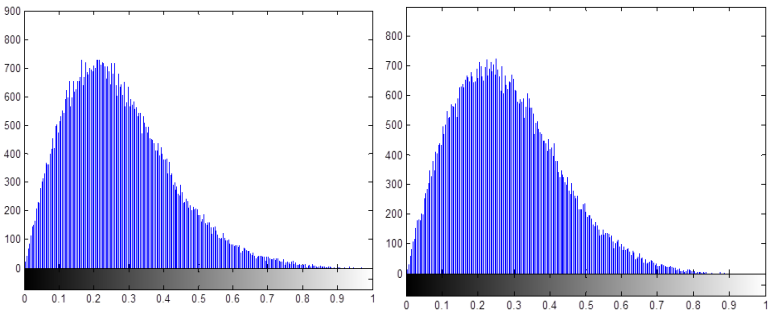

Fig. 6(a), 6(b) Histograms of the encoded images

4.1.3. ENTROPY ANALYSIS

Entropy measures the unpredictability or vagueness in the Cipher image. More the unpredictability in Cipher image, it becomes difficult for the attacker to improve the original image. Mathematically entropy H can be given by equation (15).

$$H = -\sum_{i=1}^{M} pi \; log2 \; pi \qquad (15)$$

Where p represents the probability. The perfect value of entropy is 8.The entropies obtained for cipher image of Lena and Barbara using anticipated system is 6.7272 and 7.55890 respectively, which is near about the idyllic value. This shows that the suggested system is strong and has high unpredictability in cipher image.

V.CONCLUSION

The suggested asymmetric cryptosystem presents non linearity by adding square and square root operation in the encoding and decoding tracks respectively which enhances the safety of the system. When an image is encoded using Fresnel Transform it enhances the safety and privacy of the original image. The suggested method uses Fresnel using asymmetric keys since these keys are different for both encoding and decoding schemes. The authors have also used different masks to perform simple DRPE (HM &SPM) which enhances the key space. The system is also proved against noise attack. The simulation outcome authenticates the sustainability and efficacy of this cryptosystem.

REFERENCES

[1] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan & B. Javidi , Optical techniques for information security,Proceedings of IEEE97 ,2009, 1128-1148.

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

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

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

[5] R.Tao, Y. Xin & Y. Wang , Double image encryption based on random phase encoding in the fractional Fourier domain, Optics Express, 15 (24), 2007, 16067-16079.

[6] S. K. Rajput & N. K. Nischal , Image encryption based on interference that uses fractional Fourier domain asymmetric keys, Applied Optics 51,2012, No.10.

[7] S. K. Rajput & N. K. Nischal , Optical double image security using random phase fractional Fourier domain encoding and phase- retrieval algorithm, Optical Communication ,2016.

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

[9] B. M. Hennelly & J. T. Sheridan , Random phase and jigsaw encryption in the Fresnel domain, Optics Letters 29 (14) ,2004, 1584-1586.

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

[11] H. Singh, A . K. Yadav, S. Vashisth & K. Singh , Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain, International J. of Opt. 926135, 2015, 1- 13.

[12] J. A. Rodrigo, T. Alieva & M. L. Calvo, Gyrator Transform: properties and applications, Optics Express 15, 2007, 2190-2203.

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

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

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

[16] H. Singh, A. K. Yadav, S. Vashisth & K. Singh , Fully- phase image encryption using double random – structured phase masks in gyrator domain, Appl Opt 53, 2014, 6472-81.

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

[18] S. Vashisth, A . K. Yadav, H. Singh & K. Singh ,Watermarking in Gyrator domain using asymmetric cryptosystem, Proc. of SPIE : 2015, 96542E.

[19] X. Wang & D. Zhao, Double images encryption method with resistant against the specific attack based on an asymmetric algorithm,Opt. Exp., 2012, 11994 -12300.

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

[21] A. Carnicer, M. Montes- Usategui, S. Arcos & I. Juvells, Vulnerability to chosen-ciphertext attacks of optical encryption schemesbased on double random phase keys, Opt. Lett. 30 ,2005, 1644-1646.

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

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

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

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

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

[27] A .Sinha , Nonlinear optical cryptosystem resistant to standard and hybrid attacks, Optics and Lasers in Engineering 81,2016, 79- 86.

[28] W. Qin, X. Peng, X. Meng & B. Gao ,Universal and special keys based on phase truncated Fourier Transform, Optical Engineering, 50 ,2011, 080501.