International Journal Of Applied Research In Science And Engineering *ISSN (Online): 2456-124X*
International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - November 2016)

AN OPTICAL IMAGE ENCRYPTION USING CHAOTIC KICKED ROTATOR MAP WITH DOUBLE RANDOM PHASE ENCODING

R.Sivamalar[1], Dr.Swati Sharma[2]
[1]Lecturer, Department of Computer Science and Information System, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia.
[2]Department of Electrical Engineering, Jodhpur National University, Jodhpur, Rajasthan, India.

Abstract: The Optical images are subject to various attacks by the hackers while transmission. This problem can be solved by applying encryption of optical images. Optical encryption can provide a better and safer image communication. In order to receive and retrieve the original optical information at the receiver side, robust encryption scheme is needed. The Chaotic Baker Map & Double Random Phase Encoding (CBMDRPE) has been employed to encrypt the optical image. To test the strength of the proposed encryption algorithm, it is subjected to a known-plaintext attack in which the key estimation is done by Ant Colony Optimization (ACO). However, the CBMDRPE based encryption has certain drawbacks due to the usage of chaotic maps. The use of floating-point variables generates speed problem and causes issues in representing the numbers. Inorder to enhance the encryption performance, the Chaotic Kicked rotator map concept is introduced and it replaces the chaotic baker map to form Chaotic Kicked rotator map-DRPE (CKRMDRPE). This approach reduces the complexity in computations and increases the speed of mapping by employing bit-wise representation thus enhancing the encryption process. This approach is not affected by the known-plaintext attack ensuring its efficiency by providing better results interms of maximum deviation, correlation coefficient, mean square error and peak signal-to-noise ratio.

Keywords: Optical image Encryption, Chaotic Kicked Rotator Map(CKRM), Double Random Phase Algorithm (DRPE)

I. INTRODUCTION

IN recent years, there has been an increasing interest in the use of optical methods for data security applications. The characteristics of fast computing and parallelism of optics are very useful in real-time applications. Optics offers several dimensions in which information can be hidden such as - phase, polarization, wavelength etc. - which makes it possible to encode data more securely. It is believed that optical encryption techniques provide a more complex environment and are more resistant to attacks compared with digital electronic systems. Many optical image encryption systems have already been proposed due to their high parallel performance and ultra-fast processing speed with extensive applications. Some are done by Fourier transform (FT) [1, 2], Fresnel transform (FRT) [3], or fractional Fourier transform (FrFT), which is the generalization of traditional FT with its fractional order used as additional key in the image encryption. And some are done by fractional wavelet transform (FWT) or fractional Wavelet packet transform (FWPT) [4, 5]. Most of the above-mentioned encryption algorithms have relations with fractional Fourier transform, which was extensively used in the field of optical information processing. An early work of optical image encryption, chaotic Baker map and Double Random Phase Encoding (DRPE) is presented in [6]. This technique is implemented in two layers to enhance the security level of the classical DRPE. The first layer is a pre-processing layer, which is performed with the chaotic Baker map on the original image. In the second layer, the classical DRPE is utilized. However, the Chaotic Baker Map has low speed problem and number representation problems due to the utilization of floating point values over other number representations. Hence the Chaotic Baker Map is replaced by the efficient Chaotic Kicked rotator map which reduces the computation complexities and the speed problem by utilizing the bit-wise representation of the numbers. Thus the proposed CKRMDRPE enhances the security with efficient results. The strength of the CKRMDRPE and CBMDRPE are tested by a known plain test attack which uses ant colony optimization for key estimation it is observed that cipher text can be decrypted in CBMDRPE while cannot be decrypted while utilizing CKRMDRPE.

II. RELATED WORKS

Liu, S., et al [7] proposed an optical image encryption by using cascaded multiple fractional Fourier transforms along with random phase filtering. This method makes use of degrees of freedom provided by fractional orders as encryption keys together with random phase masks which are located at intermediate planes. This approach increases security of encryption without degradation of noise robustness. For cascaded fractional Fourier transforms scaling problem must be considered and random phase filtering is difficult. Zhang, Y., et al [8] proposed an optical encryption technique based on iterative fractional Fourier transform. This encryption technique encodes a primary image to white noise and also parameters of fractional Fourier transform provides additional keys for encryption to make code more difficult to break. This method is difficult for unauthorised person to access the right encrypted image. However, to reduce the complexity more number of iterations and fractional order are required. Hennelly, B. M., & Sheridan, J. T., [9] proposed an encryption method of 2-D information using optical systems based on the fractional

Fourier transform. For decrypting data random phase keys are required and must be stored and correctly aligned with encrypted data in receiver. To avoid phase keys new techniques such as random shifting or jigsaw algorithm is used. But time taken, complexity and susceptibility to noise are increased. Nishchal, N. K., et al [10] proposed a fully phase encrypted memory using cascaded extended fractional Fourier transform. Here fully phase image which is obtained from amplitude image is encrypted by fractional Fourier transformed three times and random phase masks are placed in two intermediate planes. Encrypted image is recorded in photorefractive crystal and decrypted by using phase contrast filter which uses lithium niobate crystal to reconstruct phase image. To make system more strong, more number of lenses is required. Zhao, J., et al [11] proposed en encryption method based on multistage fractional Fourier transforms (FRT) and pixel scrambling technique. This multistage fractional Fourier transform improves the security for encryption comparing with single FRT encryption. But increasing of encoding periodicities computational costs and complexity are also increased and selecting of proper encoding periodicities is also necessary. Vilardy, J. M., et al [12] proposed a phase encryption of digital images by using fractional Fourier transform. The digital image to be encrypted is placed as the phase of a complex exponential then transformed three times and multiplied in intermediate steps by two independent random phase masks. To decrypt applied inverse sense to the conjugated complex of the encrypted image then negative of phase of resulting function is taken. However encryption process is much complexity. Encryption is the most effective way to achieve data security. From the literature, it is found that the Fourier plane encryption algorithm and Double Random Phase Encoding can provide better encryption. However, these approaches are still affected by the known-plane text attack.

III. REVIEW OF OUR PREVIOUS STUDY

3.1 Chaotic Baker Map & Double Random Phase Encoding (CBMDRPE)

CBMDRPE is based on the concept of including a pre-processing chaotic baker map layer for the randomization of the optical image pixels before performing encryption. This layer can be performed numerically to avoid the complexity of the all-optical implementation. The second layer is the classical DRPE that twice Fourier transforms the image for efficient encryption.

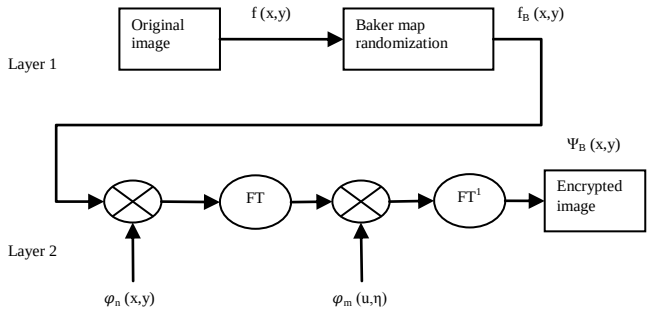

Figure 1. CBMDRPE Encryption process

The CBMDRPE approach enables better performances with the cracking or hacking the encrypted images becomes harder. When the hacker tries to crack the DRPE key, the target image cannot be obtained as the image is protected by the first auxiliary key of the chaotic baker map. Similarly when there are acts of hacking, the chaotic randomized pixels are affected so that the hacking process can be intercepted using the changes in map. This approach also facilitates the water-marketing technique for hiding secret information in the images. Double random phase encryption is a unique method of optically encoding an image. The primary input image f is encoded to stationary white noise by the use of two statistically independent random phase-keys and two Fourier transforms. One key is placed in the input domain and the other key is placed in the Fourier domain. An encryption technique's key-space is a set of possible keys that can be used to encode data using that technique. In Double random phase encryption system, there are typically several keys that will decrypt the encoded message with relatively low error. In this the key is regarded as phase-key R2. Therefore the number of keys in the key-space is completely determined by the phase-key R2 and depends on the key dimensions in pixels and the number of phase quantization levels used in the phase-key.

The encryption process of optical image f(x,y) is shown in Figure 1. It can be mathematically described as

$$\psi_B(x,y) = FT^{-1}[FT\big(f_B(x,y)\varphi_n(x,y)\big)\varphi_m(v,\eta)]$$

At the receiving end, the encrypted image is decrypted to retrieve the original image f(x,y). This process is shown in Figure 2. It can be described as

$$FT^{-1}[FT(\psi_B(x,y)\varphi_m^*(v,\eta)] = f_B(x,y)\varphi_n(x,y)$$

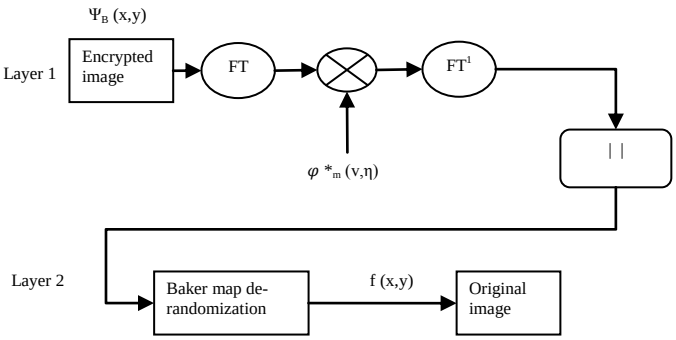

Figure 2. CBMDRPE Decryption process

Though this approach provides enhanced security of the optical images, the usage of floating points as number representations in Chaotic baker map causes performance degradation by reducing the speed of processing and increasing the computation complexity. Thus there arises a need for either modifying or replacing the chaotic baker layer. This is done by introducing Chaotic Kicked rotator map.

IV. PROPOSED RESOURCE SCHEDULING SCHEME

4.1 Chaotic Kicked Rotator Map & Double Random Phase Encoding (CKRMDRPE)

CKRMDRPE replaces the chaotic baker map with chaotic kicked rotator map. CKRM utilizes bit-wise representation of numbers so that the speed problems do not occur while the computation complexity is also reduced. CKRM can be described by employing the two-dimensional maps M. The variables p and q are considered which appear as canonical coordinate and momentum. The (p,q) plane and the phase space are mapped onto itself.

$$\bar{p} = f(p,q)$$
$$\bar{q} = g(p,q)$$

The mapping in M can be described as

$$(p,q) \overset{M}{\rightarrow} (\bar{p},\bar{q})$$

The mapping M is area preserving, the Jacobian determinant J that relates the phase space areas

$\Delta\bar{p}\Delta\bar{q} = J\Delta p\Delta q$is equal to unity

$$J = \left|\frac{\partial(\bar{p},\bar{q})}{\partial(p,q)}\right| = 1$$

Initializing at the point (p_0, q_0) and iterating the map, generates the sequence of points $(p_n, q_n), n = 0,1,2, \ldots$

The consideration of delta-kicked rotator with the Hamiltonian system can resolve the chaotic map.

$$H = \frac{p^2}{2m} + \delta_\tau(t)K\cos q$$

Where $\delta_\tau(t)$ is the τ-th periodic comb function, its value is non-zero only at a periodic sequence of delta-spikes.

$$\delta_\tau(t) = \sum_{n=-\infty}^{+\infty} \delta(\frac{t}{\tau} - n)$$

The chaotic kicked rotator system can be written as

$$H(p,q,t) = T(p) + \delta_\tau(t)V(q)$$

Where $V(q) = kq^2$ is the potential of the particle in map
Considering the angular momentum, the chaotic kicked rotator becomes

$$\bar{p} = p + K\sin q$$
$$\bar{q} = q + \bar{p}$$

The dimensionless parameter K is the measure of the kick strength and is proportional to the ratio of the potential energy of the field, dE, and the rotational energy for rotation in resonance with the period of kicks. It is given by

$$K = \tau^2 dE/I$$

Where I is the moment of inertia

When applying additional scaling, the chaotic kicked rotator becomes

$$\bar{p} = p + \frac{K}{2\pi}\sin 2\pi q$$
$$\bar{q} = q + \bar{p}$$

Where q is taken modulo one in the interval $0 \le q < 1$

Using this chaotic kicked rotator, the encryption process can be written as

$$\psi_B(x,y) = FT^{-1}[FT\big(f_B(x,y)\varphi_n(x,y)\big)\varphi_m(\bar{p},\bar{q})]$$

While the decryption process can be written as

$$FT^{-1}[FT(\psi_B(x,y)\varphi_m^*(\bar{p},\bar{q})] = f_B(x,y)\varphi_n(x,y)$$

4.2 Known-plaintext attack

Known-plaintext attack is one way to test the strength of an encryption algorithm. In known-plaintext cryptanalysis, the attacker has a priori knowledge of the encryption mechanism as well as a plaintext and cipher text pair. If the attacker is able to find the key used for a given plaintext-cipher text pair, then the security of all the past and future cipher texts, which used the same key, can be easily identified. Let us assume that the attacker tries to decrypt a cipher text encrypted using Fourier plane encoding by the blind decryption method. In this method, he tries to decrypt the cipher text by randomly picking a key from the key space, and compares the resulting 'decrypted' plain text to the original plaintext. The probability of finding the correct mask in t searches would be approximately tK−1 where K is the size of the key space. For an N ×N pixel encryption phase mask with m phase levels, the key space is as large as K = mN×N. If one considers that some fraction $r(\varepsilon) \in [0,1]$of the keys could give a decryption with some acceptable errorε, then the probability of finding one of these (estimated) keys increases to t $(r(\varepsilon)K)^{-1}$for a particularε. If the attacker finds anyone of these estimated keys he would decrypt the cipher text with some error. ACO algorithm to find a phase masks which would approximately decrypt the cipher text ψ (.) to give an estimated plaintext f̃. A system with a phase-key that has N * M pixels, each with Q quantization levels, has Q (N*M) keys. ACO algorithms have advantage over simulated annealing when the graph may change dynamically, the ant colony algorithms can be run continuously and adapt to changes in real time. Thus the most effective key is estimated using ACO. The cost value E is calculated as the NRMS error between the decrypted image and the original plaintext image. The normalized root mean squared (NRMS) error is equal to or less than some threshold ε. The NRMS error is calculated as

$$NRMS = \sqrt{\frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|I_d(i,j) - I(i,j)|^2}{\sum_{i=1}^{n}\sum_{j=1}^{n}|I(i,j)|^2}}$$

where $I_d(.) = |\tilde{f}|2$ and I (.) = |f|2

Depending on this attack, the strength of encryption is evaluated. The approach that is affected less by this attack is considered to provide better encryption.

V. EXPERIMENTAL RESULTS

The optical image encrypted using CBMDRPE and CKRMDRPE are shown below Figure 3 and 4

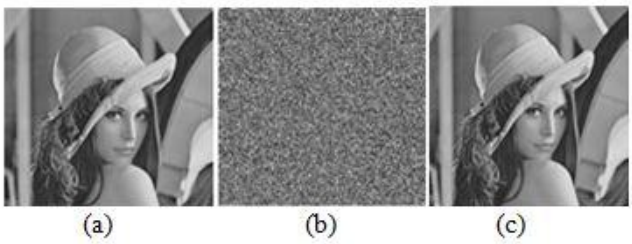

Figure 3.Encrypted Lena image (a) Original Image (b) CBMDRPE Encryped image (c) CBMDRPE Decrypted image

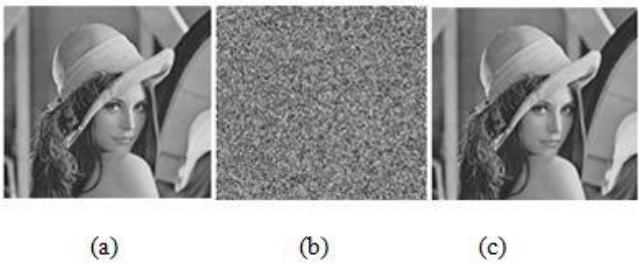

Figure 4.Encrypted Lena image (a) Original Image (b) CKRMDRPE Encryped image (c) CKRMDRPE Decrypted image

In performance evaluation, two optical images are taken as A and B. The images A and B are given as input to the encryption and image compression algorithms. On comparing the CBMDRPE and CKRMDRPE based on performance metrics such as maximum deviations, correlation coefficient, mean square error and peak signal-to-noise ratio

5.1 Maximum Deviation Analysis

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images. The steps of calculating this metric are:

1. Count the number of pixels for each gray-scale value in the range of 0 to 255 and present the results graphically for both the original and encrypted images (i.e. get their histogram distributions).
2. Compute the absolute difference or deviation between the two curves and represent it, graphically.
3. Estimate the area under the absolute difference curve, which is the sum of deviations.

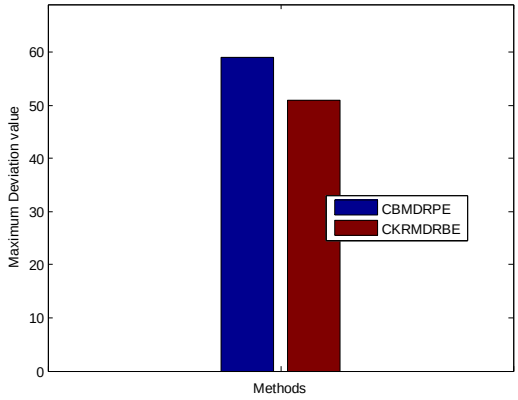

Figure 5.Maximum Deviation Value

Figure 5 shows the comparison of CBMDRPE and CKRMDRPE in terms of maximum deviation. CBMDRPE has 59 while CKRMDRPE 51 which means the CKRMDRPE provides better encryption with reduced deviation value.

5.2 Correlation Coefficient Analysis

The correlation coefficient between the original and the encrypted images has been used as a tool for encryption quality evaluation. The correlation coefficient is estimated as:

$$r = \frac{cov(f,\psi)}{\sqrt{D(f)}\sqrt{D(\psi)}}$$

and $D(f) = 1/L\sum_{l=1}^{L}(f_l - E(f))^2$

$$cov(f,\psi) = 1/L\sum_{l=1}^{L}(f_l - E(f)(\psi_t - E(\psi))$$

$$E(f) = 1/L\sum_{l=1}^{L} f_l$$

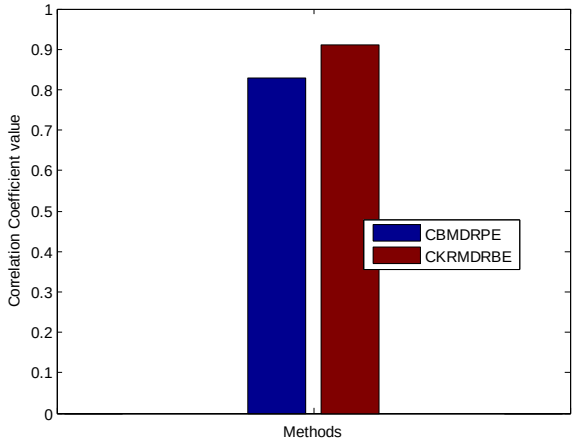

Figure 6 Correlation coefficient

Figure 6 shows the comparison of CBMDRPE and CKRMDRPE in terms of correlation coefficient. CBMDRPE has 0.83 while CKRMDRPE 0.91 which means the CKRMDRPE provides better encryption with increased value of correlation coefficient.

5.3 Mean Square Error (MSE)

Mean Square Error (MSE) between the decrypted and original images is calculated. It is defined as:

$$MSE = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}|f(x,y) - \tilde{f}(x,y)|^2$$

where X and Y are the image dimensions. $f(x,y)$ and $\tilde{f}(x,y)$ represent the original and the decrypted images, respectively.

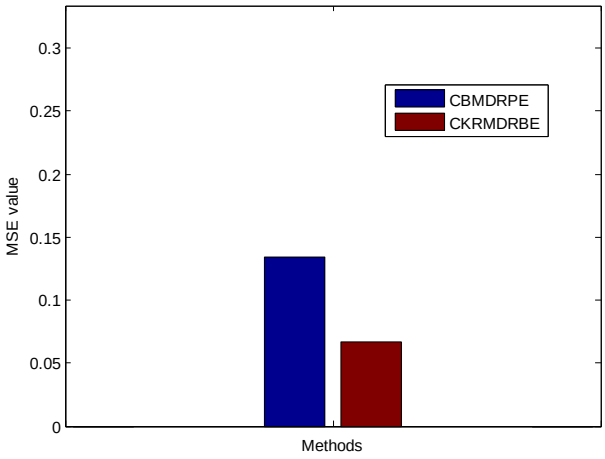

Figure 7. MSE comparison

Figure 7 shows the comparison of CBMDRPE and CKRMDRPE in terms of MSE values. CBMDRPE has 0.1337 while CKRMDRPE 0.0668 which means the CKRMDRPE provides better encryption with minimized MSE values.

5.4 Peak Signal-to-Noise Ratio

The Peak Signal-to-Noise Ratio is estimated from the MSE

$$10log_{10}\left(\frac{255^2}{MSE}\right)$$

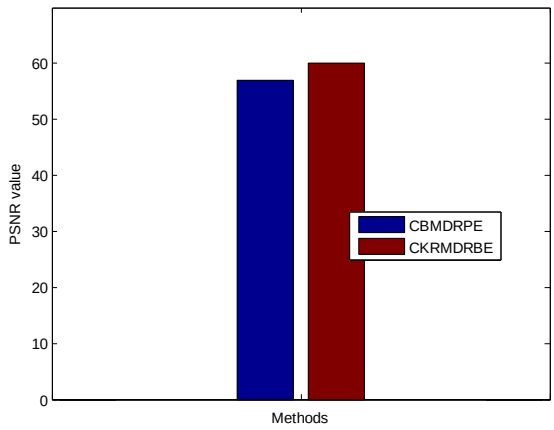

Figure 8. PSNR comparison

Figure 8 shows the comparison of CBMDRPE and CKRMDRPE in terms of PSNR values. CBMDRPE has 56.87 while CKRMDRPE 59.88 which means the CKRMDRPE provides better encryption with increased PSNR.

VI. CONCLUSION

In this paper, CKRMDRPE is proposed to enhance the security with efficient results. It replaces the chaotic baker map to form Chaotic Kicked rotator map-DRPE (CKRMDRPE). This approach reduces the complexity in computations and increases the speed of mapping by employing bit-wise representation thus enhancing the encryption process. This approach is not affected by the known-plaintext attack ensuring its efficiency by providing better results in terms of maximum deviation, correlation coefficient, mean square error and peak signal-to-noise ratio.

REFERENCES

[1] P. Refregier, and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, pp. 767–769, July 1995.

[2] T. Nomura, and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng., vol. 39, pp. 2031–2035, February 2000.

[3] G. H. Situ, and J. J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett., vol. 29, pp. 1584–1586, July 2004.

[4] L. F. Chen, and D. M. Zhao, "Optical image encryption based on fractional wavelet transform," Opt. Commun., vol. 254, pp. 361–367,May 2005.

[5] L. F. Chen, and D. M. Zhao, "Image encryption with fractional wavelet packet method," Optik, vol. 119, pp. 286–291, November 2008.

[6] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abd El-Samie, "Optical Image Encryption Based on Chaotic BakerMap and Double Random Phase Encoding", vol 31, August 2013

[7] Shutian Liu , Li Yu, Banghe Zhu, "Optical image encryption by cascaded fractional Fourier transforms with random phase filtering", Opt. Commun.,187, 2001

[8] Yan Zhang, Cheng-Han Zheng, "Optical encryption based on iterative fractional Fourier transform", Optics Communications 202 (2002) 277–285

[9] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains", optics letters, vol 28, February 2003

[10] Naveen Kumar Nishchal, Joby Joseph, and Kehar Singh, "Fully phase encrypted memory using cascaded extended fractional Fourier transform", 2016

[11] Jianlin Zhao, Hongqiang Lu, Xiaoshan Song, Jifeng Li, Yanghua Ma, "Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique", Optics Communications 249 (2005) 493–499

[12] Juan M. Vilardy, Jorge E. Calderon, Cesar O. Torres, Lorenzo. Mattos, "Digital Images Phase Encryption using Fractional Fourier Transform", IEEE, 2006.

R.Siva Malar received the MCA, M.Phil and M.Sc degrees from Bharathiar University, India in 2006, 2008 and 2009 respectively. She also received her M.E degree from Anna University, India in 2012. Since 2012 she has been working as lecturer in Computer Science department, Jazan University, Kingdom of Saudi Arabia. She is currently doing her Ph.D in Computer Science and Engineering at Jodhpur National University, India. Her research interests are in the areas of resource management and scheduling in the area of Cloud Computing and Image Processing.