Analysis of Encryption and Decryption of Image using Canonical Transforms & Scrambling Technique

[1]Kamini Kanchan, [2]Brij Kishore, [3]Manish Sharma
[1]M.Tech Scholar, [2]Assistant Professor, [3]Assistant Professor
[1]Computer Science,
[1,2,3]Apex Institute of Engineering & Technology, Jaipur, India

Abstract : Data security is a prime objective of various researchers & organizations. Because we have to send the data from one end to another end so it is very much important for the sender that the information will reach to the authorized receiver & with minimum loss in the original data. Data security is required in various fields like banking, defence, medical etc. So our objective here is that how to secure the data. So for this purpose we have to use encryption schemes. Encryption is basically used to secure the data or information which we have to transmit or to store. Various methods for the encryption are provided by various researchers. Some of the methods are based on the random keys & some are based on the scrambling scheme. Chaotic map, logistic map, Fourier transform & Fractional Fourier transform etc. are widely used for the encryption process. Now day's image encryption method is very popular for the encryption scheme. The information is encrypted in the form of image. The encryption is done in a format so no one can read that image. Only the person who are authenticated or have authentication keys can only read that data or information. So this work is based on the same fundamental concept. Here we use Linear Canonical Transform for the encryption process. Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text. Encryption is used to guarantee the hidden information from anyone of concern not intended to, even those who can comprehend the encrypted data. The procedure of backsliding cipher text to its original plaintext is considered as decryption. Various parameters are calculated which shows various aspects. Like Change in the value of MSE with change in order of transform tells the quality of encrypted image. Correlation coefficient of encrypted and decrypted image also shows the difference between the encrypted and decrypted image. The original image is then reconstructed and histogram of all these images analyzed. Robustness and imperceptibility of images increases by the proposed method.

Index Terms **– Linear Canonical Transform (LCT); Mean Square Error (MSE); Image Scrambling, Image Encryption & Decryption.**

I. INTRODUCTION

If we talk about today's era we want to transfer the large amount of information with higher data rates. Another major concern related to the data transmission is the data security. As Cyber crime increases day by day so it is very much tedious work to secure the data or information. For that purpose various concepts are proposed by various researchers in the literature. The main conclusion of all the researchers is to hide the information so any unauthenticated system & person not able to steal the information. To overcome this problem a method is proposed in which the data encrypted in the form of image. The image is considered best solution for this problem because it can contain huge information & it has the huge correlation between its picture elements. Various image encryption processes which are given in the literature mentioned below.

- Chaotic Map.
- Logistic Map.
- Advance Encryption Standard (AES).
- Arnold map.
- Affine Transformation.
- Fourier Transform.
- Fractional Fourier Transform.

Some of the researchers proposed the encryption by using scrambling of the image pixels, other came which an idea to convert the space domain in which the image given to the frequency domain. Some researchers concluded that the masking with the Fourier transform or Fractional Fourier transform is the efficient method to do the encryption. But the problem is not highly resolved using these all methods. So an another efficient scheme known as LCT (Linear Canonical Transform) is one of the transform which is used widely in double picture encryption process due to its efficient outputs, Encryption process based on LCT, scrambling process & the mathematical approach which is used to design this transform.

A. Encryption Process For Image

Image encryption is the scheme by using which we can authenticate users with any mean so only they have the rights to access the data which can be an image, but the unauthenticated users or much precisely we can say hackers cannot access that data. First of all the data or image which is considered as an information converted in to the unreadable format by using encrypted algorithms so no one can read the data. Generally the process is done using the various specified "Keys" which are used to encode the image. Any person which is not authenticated cannot access the information which is hidden in an image. Only the authenticated person or system which has the decryption key can decode or decrypt the information and can access that.

B. Cryptographic services

Information confidentiality or we can say privacy is came in to the picture to unaffected the data or information from the outer environment. This outer environment can be considered as a system which creates error in the data. So for the confidentiality of data and to secure it from outer environment we have to do various arrangements. These arrangements are known as ciphering& inherit various random keys in the data which can only be accessible to the certain user or organization that have the authority.

Authentication is very big problem in the modern era. To resolve this problem various techniques are came in to the modern society. If you are transmitting a message then there must be the authentication is required in that process, you are trying to withdraw money from the ATM then you will be authenticate only when you provide the correct ATM pin. There are various other ways for the authentication process some of the methods are biometrics like thumb impression, eye retina scanner, face detection or voice detection etc all the methods for the authentication process of the user and the data.

This study is performed on MATLAB R2016b with standard database grey scale images like Barbara, Cameraman and Lenna or by using the personalize images in standard format. First of all, the images are scrambled and then the generation of a new complex image took place. Initially phase mask is applied on the complex image by using RPM 1, and then the complex image is encrypted by using LCT of first order. Again the phase mask RPM 2 is applied on the encrypted image followed by the LCT of second order to get the encrypted image finally. Reverse process is applied to get the original image. Additionally, histogram &correlativity coefficient analysis is executed for the analysis of the quality of encryption.

II. LITERATURE SURVEY

Abraham Panicker O et al. in paper, "Advanced Image Encryption and Decryption Using` Sandwich Phase Diffuser and False Image along with Cryptographically Enhancement", (2010), projected An algorithm for encoding & decoding of 2-D image. In this method, encoding is done by implementing as and that phase diffuser formed by 2 spot patterns, & put it in Fourier region of 2 phase encryption method [1]. Other image is combined with consequent image after phase diffusion & then crypto graphical enrich is completed that gives a secure system. This cryptographic method is came from AES cryptosystem in that a changed row surgery is executed. For decoding firstly reverse crypto is completed, and after that minus of combined image is completed. Then we will do next decoding process. MSE calculation in middle of the decoded and master image, reliableness of the technique is measured.

Li Xuemei et al. in paper, "A Novel Scheme on Reality Preserving Image Encryption", (2011), projected a fresh model on realness keeping image encryption. The Hilbert's transform & 2 phase encryption are used in this technique [2]. The encoded picture is genuine evaluation without information enlarging that profits image processing by using computing device in which velocity of calculation is crucial. In this image is worked in those planes which can relate as various FrF regions. Additionally, projected method fulfills the encoding& decryption in equivalent construction that becomes it easy to apply encoding in pragmatic app. For confirming validness of the fresh method, Simulations are available.

Yaqing Wang et al. in paper, "A Novel Image Encryption Algorithm Based on Fractional Fourier transform", (2011), projected encoding method which rely on the FrFT& chaos. First of all, scampering picture with chaos into time region, then fuse this & DFrFT in way of X. Second thing is, scampering the picture got in FrFT region with disorderly, then fuse this & DFrFT in way of Y. At last, make mapping the genuine and picture piece of the encoded image on red green blue, making a colored picture for transmitting [3]. Conclusion from experimental is this code have nice protection, this has importance in the data protection area.

Xianzhe Luo et al. in paper, "Single-channel Color Image Encryption Based on the multiple order Discrete Fractional Fourier Transform and Chaotic scrambling", (2012), projected a technique which uses MODFrFT and disorderly scamper for image encoding [4]. Image is modified from red green blue method into the YCbCr and complex number is original piece & an imaginary is featured to relieve the transmission load in this encryption method. Human sight have sensitivity to Y element compare to other 2 elements in YCbCr& for encrypting the image, this color format is implemented. To scramble the matrix in the FrFT region, Chaos is also introduced. Thus result is validness & efficiency of method & hardiness of the method against closure attack is tested.

Sudhir keshri et al. in the paper, "color image authentication scheme in linear canonical transform domain", (2012), created a technique to encode a image depends on the LCT through 2 Linear Canonical Transform encryption method [5]. This method has more security for malicious exploiters because it has bigger protection keys than Fractional Fourier transform, also proposed that this technique is more worthy for the image authentication purpose. The hardiness of system is displayed by statistical analysis of the algorithm.

Jun Shi et al. in paper, "Function Spaces Associated with the Linear Canonical Transform", (2011), We studied about the linear canonical transform (LCT) a very useful and powerful tool in signal processing, optics, etc and there are many results which are already known with sampling theory inclusion. Most LCT sampling theories consider the class of band limited signals [6]. However, in the real world scenario from the engineering application point of view, many analog are non-band limited. In this analogy, a sampling and reconstruction strategy for a class of function spaces related to the LCT is projected, which provides a suitable and realistic model for real applications. Firstly, definitions of semi- and fully-discrete convolutions of the LCT are introduced. Then necessary and sufficient conditions pertaining to the LCT are derived, where integer shifts of a chirp-modulated function generate a rises basis for the function spaces. In the results, a more comprehensive sampling theory for the LCT in the function spaces is presented and sampling theorem is also established which recovers the signal from its samples value in the function space. In addition of it, some special cases of sampling theorems for shift-invariant spaces and for band limited signals associated with the Fourier transform (FT), the fractional FT, or the LCT are also derived. Finally, we proposed some potential applications of the derived theory. Yupu Dong et al. in paper, "Image Encryption Algorithm Based on Chaotic Mapping", (2010), As the paper named, a image scrambling algorithm based on chaotic mapping is presented here [7]. To achieve the effect of image scrambling, each pair of pixel points is exchanged to all the possible pair combinations. This algorithm has some advantages like as simple design and high efficiency compare to other image encryption algorithm based on chaotic mapping. A position correlation based methodology is used to evaluate the image scrambling degree and the encryption effect, which is consistent with the results of subjective evaluation.

Xiao Feng et al. in paper "A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Magic Cube Rotation", (2011), Paper describes a new image encryption algorithm using discrete fractional Fourier transform (FFT) plus a better magic cube turning round scrambling method [8]. The method which is given here, using fractional FFT & position scrambling

approach is able to achieve double image encryption in the time-frequency domain and has better performance compared to other encrypted images and decrypted images.

Zhang Zhao et al. in paper, "Image encryption algorithm based on Logistic chaotic system and s- box scrambling", (2011) proposed a system which is used for the encryption process & derived using Logistic chaotic. Design status sliding block & line shift, efficiently confusing data& extension of salient features. Simulation results & theoretical study proved that the algorithm can effectively resist brute force attack, statistical analysis and differential attack, with a good of cryptography features [9].

Qiudong Sun et al. in paper, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", (2012), designed an algorithm based on the scrambling of image & bit planes related to image. In the proposed algorithm first of all a grey image is converted in to various bit-planes [10]. After this the bit planes are shuffled using this method of scrambling. When the shuffling is completed then the images are combined based on the levels of their bit planes & finally we got an image which is encrypted. The results which are given in this paper shown that this method not only effectively scrambled the image but can change the prepared histogram too. The given scheme is much more efficient than conventional scrambling method.

Elisabet Pérez- Cabre et al. in paper, "Photon-counting imaging based double-random phase encryption for information security and verification", (2011), in this photon calculation method is consolidated to encoding of optical that causes high data authentication security. This method requires thin encoded data to start division with some photons and gives enough reduction in bandwidth. This encoding limited by photons has enough data to decode, recollect signals. Now a day's many methods are analyzed to compact the data [11].

Karuna Kesavan K et al. in paper, "Optical color image encryption based on Hartley transform and double random phase encoding system", (2011), Proposed a technique for image encoding which has basic concept of Hartley transform & 2 phase encoding method. In this method a color image is decomposed in to its RGB components. RGB colors are encoded separately with help of2 phase encoding system and Hartley transform. Here the random phase masks and the Hartley transforms are the encryption parameters. During decoding process, if correct identities are applied then only decoded image meets with input picture. For checking robustness of this code, we calculate MSE in middle of decoded and master image. The technique can be realized by optical means and hence is useful for optical networks and holographic data storage systems for information security [12].

Zhi Zhong et al. in the paper, "Double image encryption using double pixel scrambling and random phase encoding", (2012), proposed an encoding technique which uses scampering of 2 pixels & FF domain encryption method [13]. In this, first image is scampered by 1st matrix and then modified as complex signal's phase, now second image is scampered by 2nd matrix and then modified as complex signal's amplitude. Now using 2 phase encoding in FF region, we encoded used complex signal in white disturbance. We can retrieve those 2 master images without disturbance in this method only by using correct identity with FF, phase cloak & scampering of pixels.

III. Basic Properties of Linear Canonical Transform

If we talk about LCT then it is transform by using which we can simplify various classical transforms. As it contains four parameters &one constraint so it is visualized as from a three dimensional family. It is visualized in the time- frequency domain. This transform is used to generalize the Fractional Fourier & Fourier transforms.

A. The Freedom of the LCT with the Fractional Fourier Trasform

The Fractional Fourier Transform

$$O_F^{\alpha}(f(t)) = X_{\alpha}(u) = \int_{-\infty}^{\infty} K(\alpha,t,u)x(t) \tag{1}$$

The Linear Canonical Transform when q ≠ 0

$$O_F^{(p,q,r,s)}(f(t)) = F_{(p,q,r,s)}(u) = \sqrt{\frac{1}{j2\Pi q}} e^{\frac{js}{2q}u^2} \int_{-\infty}^{\infty} e^{\frac{-j}{q}ut} e^{\frac{jp}{2q}t^2} f(t)dt \tag{2}$$

B. Additive Property of Linear Canonical Transform

The additive property is given below

$$O_F^{(p_2,q_2,r_2,s_2)}(O_F^{(p_1,q_1,r_1,s_1)}(f(t))) = O_F^{(k,l,m,n)}(f(t)) \tag{3}$$

Here (k, l, m, n) is

$$\begin{pmatrix} k & l \\ m & n \end{pmatrix} = \begin{pmatrix} p_2 & q_2 \\ r_2 & s_2 \end{pmatrix} \begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix} \tag{4}$$

C. Inverse Property of Linear Canonical Transform

As per previously described in the additive property, the inverse Linear Canonical Transform is given as:

$$O_F^{(s,-q,-r,p)}(O_F^{(p,q,r,s)}(f(t))) = (f(t)) \tag{5}$$

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} s & -q \\ -r & p \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (6)$$

Because $p\,s - q\,r = 1$ (7)

D. Random Phase Encoding System

Incoherence is evaluation measurement in which it defined the correlation among the sensing matrix element to the basis matrix elements. The encoding scheme which is based on double random phase encoding is the fundamental approach for virtual encryption scheme. The standard method is the way to get the random phase encoding scheme as given in the Fig.1. Put 2 dissimilar statistical random phase plate (RPM) on input plane & the Fourier frequency spectrum plane of optical system, & provides an arbitrary interruption to spatial information& spectral information of the actual image f(x, y)respectively, so as to average the spectral density distribution of the image to attain the function of encryption.

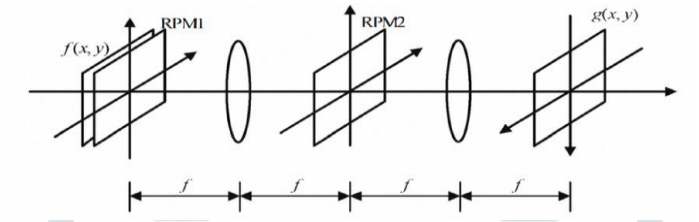

Figure.1 Double random phase encryption scheme [40]

In the compressive sensing we must be hold the Restricted Isometry Property for the recovery the original signal from the small number of samples as we use algorithm for reconstruction. Let a vector v which has a coefficient of A for representation of zero and nonzero elements in the subset of S with positive value of ε. If we talk about encryption process, then in that scheme actual image f(x, y) is modulated with the help of a phasor function exp [j2Πφ$_1$(x, y)](R. Tao et al.,2007) in to the spatial domain. After this the signal is filtered by using arbitrary phase function exp [j2Πφ$_2$ (μ, υ)] in the spatial frequency domain. These frequency domain sequences are considered as φ$_1$(x, y) & φ$_2$ (μ, υ) which are independently distributed white noise sequences. The encrypted value of the result is shown below:

$$g(x,y) = F^{-1}\{f'(\mu,\nu)\exp[j2\Pi\Phi_2(\mu,\nu)]\} \quad (8)$$

Here

$$f'(\mu,\nu) = F\{f(x,y)\exp[j2\Pi\Phi_1(x,y)]\} \quad (9)$$

For the convenience the above formula is written as

$$g(x,y) = L[f(x,y);\Phi_1,\Phi_2] \quad (10)$$

If we talk about the decryption process then this process places the data which is encrypted in nature g(x, y) in the plane which is based on 4-f optical system, followed by the Fourier Transform $f(x,y)\exp[j2\Pi\Phi_1(x,y)]$ which can be find out is using $\exp[j2\Pi\Phi_2(\mu,\nu)]'$ s which is a filtered response of the FT of g(x, y).

IV. Result & Analysis

Simulation is used to verify the method which is used for the encryption purpose for double images. Two images on which we perform the simulation are cameraman (Test Image 2) & another one is my image (Test Image 1) in grey scale. Both the images are considered with 256 x 256 pixels & 256 grey levels. Both the images are shown below in Figure 2(a) and 2(b). Here we consider the Test image 1 as the amplitude based image & Test Image 2 as a phase based image. Two random phase mask are generated with the specific values of the order of transform. Figure 2(c) and 2(d) are the images which we get after the scrambling of images. Figure 2(e) & Figure 2(f) shows the encrypted image. The encryption is done using the AWGN. Figure 2(g) and 2(h) shows the decrypted image with the correct order of transform.

.

Figure 2(a) Test Image 1

Figure 2(b) Test Image 2

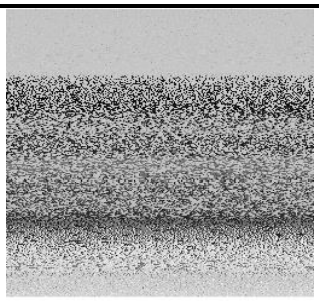

Figure 2(c) Scrambled Images 1

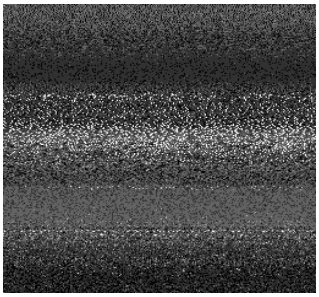

Figure 2(d) Scrambled Image 2

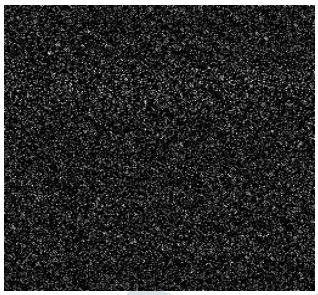

Figure 2(e) Encrypted Image 1

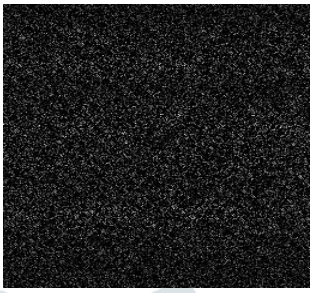

Figure 2(f) Encrypted Image 2

Figure 2(g) Decrypted Amplitude Image

Figure 2(h) Decrypted Phase Image

If we do deviation in the parameters of the order of transform then due to this deviation we get the following results.

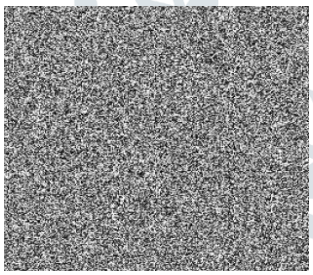

Figure 2.1(i) Amplitude based image using wrong order of transform

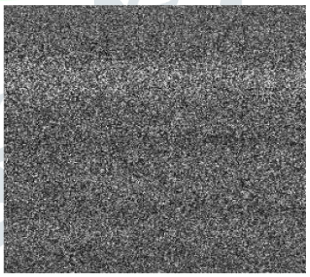

Figure 2.1(j) Phase based image using wrong order of transform

Now the images which are given below shows the variation in the MSE values with the change in the order of transform.

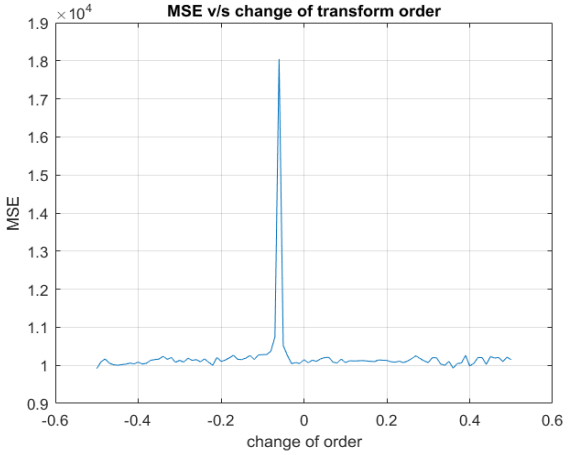

Figure 3 Variation of MSE of phase image with change in order of LCT (α_3) remaining all parameters constant

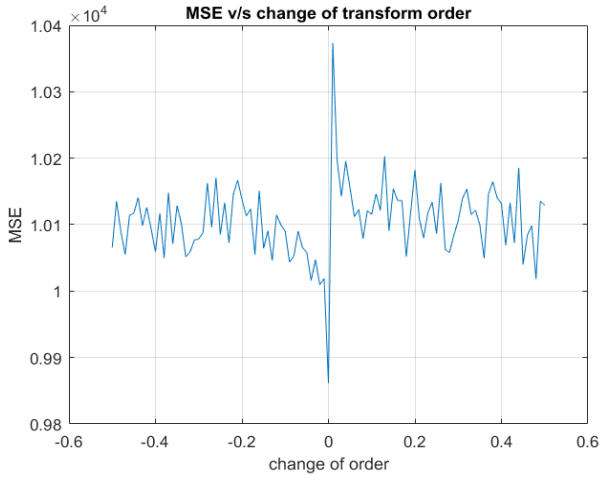

Figure 4 Variation of MSE of phase image with change in order of LCT (β_3) remaining all Parameters constant

Figure 5 Variation of MSE of phase image with change in order of LCT (γ_3) remaining all Parameters constant

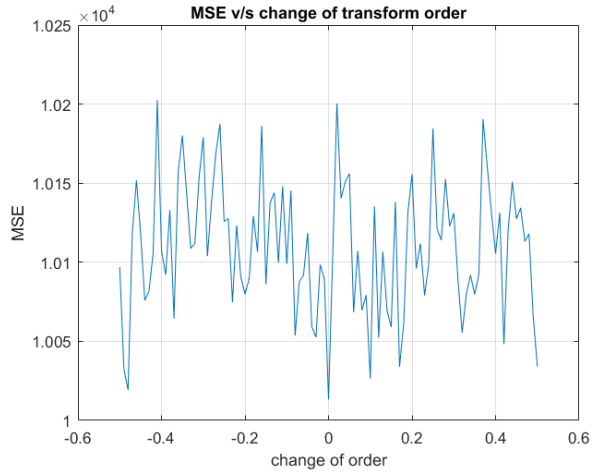

Figure 6 Variation of MSE of phase image with change in order of LCT (α_4) remaining all Parameters constant

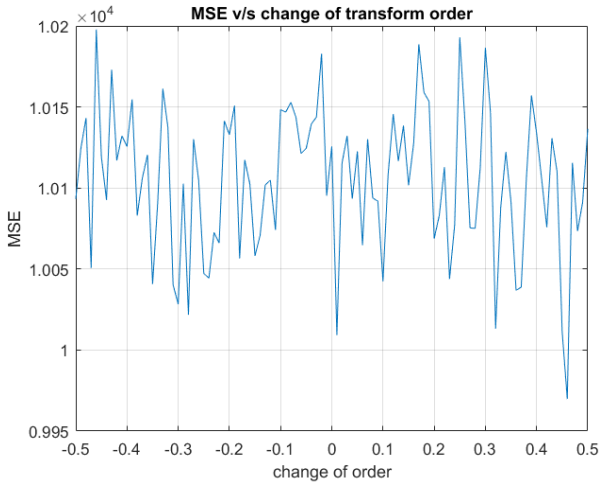

Figure 7 Variation of MSE of phase image with change in order of LCT (β_4) remaining all Parameters constant

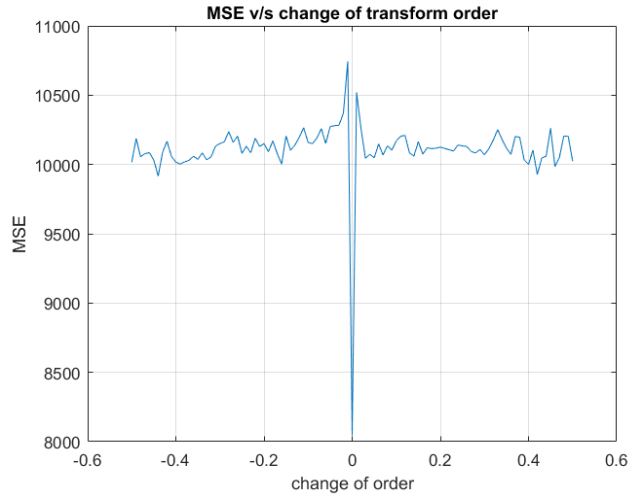

Figure 8 Variation of MSE of phase image with change in order of LCT (γ_4) remaining all Parameters constant

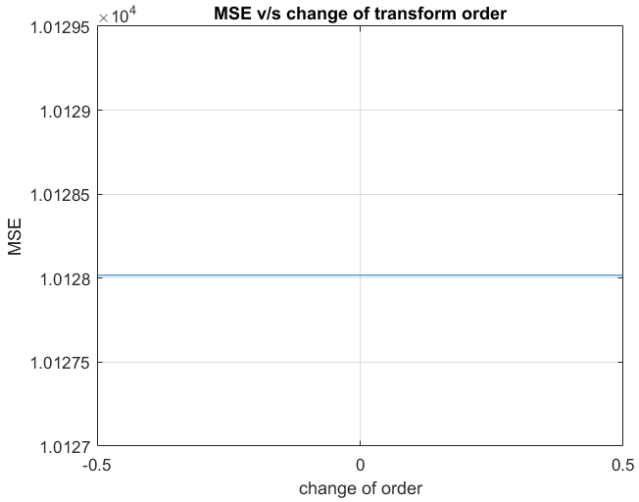

Figure 9 Variation of MSE of phase image with no change in order of LCT

The MSE curves of image decryption for different fractional order parameters are shown in figure. It can be seen from Figures, that the MSEs approximate to zero when fractional orders approach to correct key values. However, a deviation of ≥0.08 from any correct fractional order parameters will result in sufficiently high MSEs of ≥10059.89. The order of the transform is a crucial parameter as per the results depicted here. The MSE values which we get using this simulation has the stronger deviation from the previous work which is done using DFrFT. This shows that even the deviation is in the fraction but there will be precise & significant change in the values of MSE. When recovering the correct phase based image in this method. So for an unauthorized user, blind decryption is more difficult to perform. In addition, it is evident that the enhancement of the security is mainly because

of the more number of key elements in linear canonical transform. The deviation of the parameter α2 of inverse LCT Produces Zero MSE while recovering the amplitude based image.

V. Conclusion

In this paper our main motive is the Encryption & Decryption of image in a highly efficient manner. In the literature review section various algorithm proposed by various researchers for the encryption and decryption purpose. In this thesis we used the method which is based on Double pixel scrambling is used for the encryption purpose. Random phase Linear Canonical Transform is also used for the encoding purpose and the encryption of two images. The advantage of using Linear Canonical Transform is that it will provide a sufficient space between the keys & also provide a much higher security as compared to the other conventional Double image encryption schemes. The simulation result which is performed using the MATLAB indicates that a small variation in the order of transform will cause a large deviation in the MSE value. As there is a large variation in the value of MSE so we can conclude that when there is little deviation in the order of transform so we will never found the correct recovery of images. Means there is very much difference in the encrypted image and the decrypted image. The results also indicate that this scheme is much sensitive to the change in the value of keys. And this scheme provides a high robustness. As the scheme is much sensible to the change in the keys so this method is very much secure as our prime motive is the security of data or information. We can also enhance this security level by increasing the value of order for the Linear Canonical Transform.

VI. Future Scope

As per the concern about the future scope so we can also use some algorithms which can compress the data as the level of compression can also reduce the security breaching. So we can also use the compressive sensing approach which is highly popular now days related to the data compression.

References

[1] Panicker, O. Abraham, A. Jabeenaa, and Abdul Hassan Mujeebb. "Advanced image encryption and decryption using sandwich phase diffuser and false image along with cryptographical enhancement." In Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on, pp. 833-837. IEEE, 2010.

[2] Xuemei, Li, Tong Xinhai, and Dai Lin. "A Novel Scheme on Reality Preserving Image Encryption." In Measuring Technology and Mechatronics Automation (ICMTMA), 2011 Third International Conference on, vol. 1, pp. 218-221. IEEE, 2011.

[3] Wang, Yaqing, and Shangbo Zhou. "A novel image encryption algorithm based on fractional Fourier transform." In Computer Science and Service System (CSSS), 2011 International Conference on, pp. 72-75. IEEE, 2011.

[4] Luo, Xianzhe, Jinghui Fan, and Jianhua Wu. "Single-channel color image encryption based on the Multiple-order discrete fractional Fourier transform and chaotic scrambling." In Information Science and Technology (ICIST), 2012 International Conference on, pp. 780-784. IEEE, 2012.

[5] Keshari, Sudhir, Mahboob Alam, and Shri Gopal Modani. "Color image authentication scheme in Linear Canonical Transform domain." In Recent Advances in Information Technology (RAIT), 2012 1st International Conference on, pp. 38-42. IEEE, 2012.

[6] Shi, Jun, Xiaoping Liu, Xuejun Sha, and Naitong Zhang. "Sampling and reconstruction of signals in function spaces associated with the linear canonical transform." IEEE Transactions on Signal Processing 60, no. 11 (2012): 6041-6047.

[7] Dong, Yupu, Jiasheng Liu, Canyan Zhu, and Yiming Wang. "Image encryption algorithm based on chaotic mapping." In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 1, pp. 289-291. IEEE, 2010.

[8] Feng, Xiao, Xiaolin Tian, and Shaowei Xia. "A novel image encryption algorithm based on fractional fourier transform and magic cube rotation." In Image and Signal Processing (CISP), 2011 4th International Congress on, vol. 2, pp. 1008-1011. IEEE, 2011.

[9] Zhang, Zhao, and Shiliang Sun. "Image encryption algorithm based on logistic chaotic system and s-box scrambling." In Image and Signal Processing (CISP), 2011 4th International Congress on, vol. 1, pp. 177-181. IEEE, 2011.

[10] Sun, Qiudong, Wenying Yan, Jiangwei Huang, and Wenxin Ma. "Image encryption based on bit-plane decomposition and random scrambling." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 2630-2633. IEEE, 2012.

[11] Pérez-Cabré, Elisabet, Héctor C. Abril, María S. Millán, and Bahram Javidi. "Photon-counting imaging based double-random-phase encryption for information security and verification." In Information Optics (WIO), 2011 10th Euro-American Workshop on, pp. 1-3. IEEE, 2011.

[12] Kesavan, K. Karuna, and M. Ratheesh Kumar. "Optical color image encryption based on Hartley transform and double random phase encoding system." In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on, pp. 1-3. IEEE, 2011.

[13] Zhong, Zhi, Jie Chang, Mingguang Shan, and Bengong Hao. "Double image encryption using double pixel scrambling and random phase encoding." Optics Communications 285, no. 5 (2012): 584-588.