International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 8
ISSN: 2454-4248
37 – 41

An Experimental Approach for Encryption and Decryption of Image using Canonical Transforms & Scrambling Technique

Jagdish Chandra Arya
M.tech Student,
Arya College of Engineering & IT, Jaipur (Raj.)

Dr. Rahul Shrivastava
Professor,
Dept. of ECE
Arya College of Engineering & IT, Jaipur (Raj.)

Dr.Chhavi Saxena
Professor,
Dept. of ECE
Arya College of Engineering & IT, Jaipur (Raj.)

Vivek Upadhyay
Associate Professor,
Arya College of engineering and IT(Jaipur)

***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, defense, medical etc. So our objective here is that how to secure the data. This study is performed on MATLAB R2016b with standard databasegrey 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.

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.

Keywords*-data security; personalize images;* LCT; histogram..

*****

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 rime 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.

1.1. **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.

1.2 Security Parameters:

Integrity, availability & the confidentiality are the fundamental security parameters which are mentioned below.

1.2.1. Confidentiality

It is a very crucial parameter related to the security of the data. The confidentiality of data is not only the concern when we have to store the data it is also mandatory to secure the data at the time of transmission. So the confidentiality arrangements are applied during the transmission process.

1.2.2. Integrity

In current era the information expires very quickly. So it is so much important to change the information with time constantly. The motive of integrity is that this change in the data or information is done by any authorized person or organization by the means of authorized method. Violation of integrity here may or may not be considered as a malicious act. If there is any interrupt in the system then it can also create error in data or information. Integrity violation is not necessarily the result of a malicious act, an interruption in the system may also create unwanted changes in the information.

1.2.3. Availability

The third parameter which is availability is very crucial parameter. The information which is created or stored at a particular location by any resource must be available for particular entities which are authorized. As in the previous section we discuss that the information must be change from time to time so it is also accessible to authorized entities.

 ISSN: 2454-4248
37 – 41

1.3. Cryptographic services

Some international authorities who provide some security related validations gave some guidelines related to the security of data. These guidelines are given below.

1.3.1. Privacy

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.

1.3.2. Data Integrity

The design of this methodology is done for the protection of the important information or data from the deletion, insertion or rather than the modification.Data integrity can secure a small part of a message or a full message. Integrity can be provided using the cryptographic techniques. The user can ensure that the data is not intact by anybody or by anything by using these services.

1.3.3. Authentication

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.

1.3.4 Access Control

It is the fundamental solution for the problem of unknown access of the data or meaningful information. For that purpose access control comes in to the picture.

.

II. PROPOSED MATHEMATICAL METHODOLOGY

a. Introduction about Linear Canonical Transform (LCT)

If it 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.

LCT is basically the simplification of the Fourier & FrFT. This transform consists of 3 factors which are widely used in the signal processing paradigm (Adrian Stern et al., 2006 [1]). Linear Canonical Transform for a signal which can be transform f (t) is stated given below:

$$Fp,q,r,s = \begin{cases} \sqrt{-j}\,\frac{js}{e^{2q}}u^2 \int_{-\infty}^{\infty} e^{-j\frac{2\Pi ute^{j\Pi\frac{p}{q}t^2}}{q}} f(t)dt \\ \sqrt{s}e^{\frac{j}{2}rs.u^2 f(t)du} \end{cases}$$

Here constants p, q, r, s are associated by determinant matrix N, N is a unit matrix in nature. This matrix has another name as unit modular matrix & shown below

$$N = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

Here ps- qr=1. The elements p, q, r, s deliver the same information as given by the three parameters α, β, & γ which represents the Linear canonical transform. The relationship for p, q, r, s is given below.

$$N = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} \frac{\gamma}{\beta} & \frac{1}{\beta} \\ -\beta + \frac{\alpha\gamma}{\beta} & \frac{\alpha}{\beta} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{\alpha}{\beta} & \frac{-1}{\beta} \\ \beta - \frac{\alpha\gamma}{\beta} & \frac{\gamma}{\beta} \end{pmatrix}$$

LCT converts in FRFT if the following equalities satisfied.

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

The calculation of linear canonical transform can be performed using two distinguishedways. In the first method the linear canonical transform is decomposed in the FrFt after that the scaling process taken place. For the modification purpose chirp multiplication performed.In second method first of all LT convert in to chirp multiplication & then scaling will be done preceded by Fourier transform. (A.Kocet al., 2008 [2])

Various properties of LCT

The fundamental properties of Linear Canonical Transform are as follows.

The Freedom of the LCT with the Fractional Fourier Trasform

The Fractional Fourier Transform

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

The Linear Canonical Transform when $q \neq 0$

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

	Fractional Fourier Transform	Linear Canonical Transform
Number of Variant	1	4
Freedom of Transform	1	3

Table 1 : Table for Number of variant & Freedom of Transform for Fractional Fourier Transform and LCT

b. Discrete Linear Canonical Transform

LCT is based on three parameters & it is an integral transform. The use of LCT is in the problems related to the wave propagation & optimal filters. Various other transforms like FT, FrFT, co-ordinate scaling, multiplicative transforms & convolutions are the modified cases of LCT.Here derivation between the LCT & discrete version of LCT provided (F. S. Oktem et al., 2009 [3]). This method can be used to find out the

 ISSN: 2454-4248
37 – 41

samples of continuous time LCT by replacing the integral parameters with the summation, & can easily design the relation between the continuous and discrete LCT parameters. This procedure is based on the theorem given by Papoulis. So as given in this paper the continuous time LCT can be approximated using the discrete time LCT & same can be done with Fourier transforms too.

c. Random Phase Encoding System

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. 4.1. Put 2dissimilar statistical random phase plate (RPM) on inputplane & the Fourier frequency spectrum plane of opticalsystem, & provides anarbitraryinterruption to spatial information& spectral information of the actual image f(x, y)respectively, so as to average the spectral density distributionof the image to attain the function of encryption.

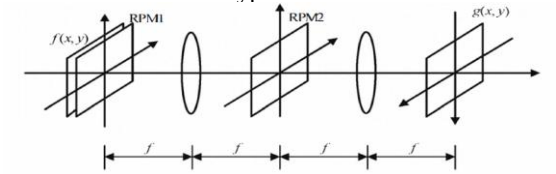

Figure 4.1 Double random phase encryption scheme [4]

d. Scrambling of Image

Scrambling is widely used in dataencryption. Another important application of the scrambling in the watermarking of image, after the scrambling the image is statistically imperceptible. This is the field in which there is so much research going on now-a-days. The purpose of the image scrambling is to convert the useful information in to useless information which is disordered in nature. This will make the information much more immune to the invalid attack or the security is enhanced (H. Zhang, 2007). Three types of image scrambling is used now-a-days one is the Frequency domain, another one is in the space domain and the last one is in the color or grey scale domain. There are various image scrambling algorithms are available in the literature but the scrambling algorithm based on the chaos provide high security. This algorithm is much more efficient that's why it is widely accepted by many researchers.

III. RESULT & ANALYSIS

a. Quality Parameters for Analysis

As we know that there are various parameters are used to check the quality of output image after the decryption. Some of the parameters are given below.

b. Mean Square Error (MSE)

Mean Square error is the parameter which is used to calculate the value of change in the original image & the decrypted image. It shows the quality of the image reconstruction. MSE must be as low as possible.

$$MSE = \frac{1}{QxR}\sum_{v=1}^{Q}\sum_{u=1}^{R}\left|I_d(u,v) - I_e(u,v)\right|^2$$

Here the value of Q=256, R=256 is calculated from the size of image, $I_d(u,v)$ & $I_e(u,v)$ shows the values of decrypted image & the actual image for the pixel (u, v) respectively.

c. Correlation Value for Adjacent Pixel Elements

It is a very crucial parameter which is used to check relationship between the adjacent pixels of images.If we talk about the correlation value for actual image then it is near to one but the value for the encrypted image is near about 0. Correlation coefficient is calculated using the below given formula.

$$Cov(A,B) = E\{[A - E(A)][B - E(B)]\}$$

$$\rho_{AB} = \frac{Cov(A,B)}{\sqrt{D(A)}\sqrt{D(B)}}$$

$$E(A) = \frac{1}{R}\sum_{u=1}^{R} A_u$$

$$D(A) = \frac{1}{R}\sum_{u=1}^{R}(a_u) - E(a))(b_u - E(b))$$

IV. SIMULATION RESULTS & DISCUSSION

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 5.1 (a) and (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 5.1 (c) and (d) are the images which we get after the scrambling of images. Figure 1 (e) & Figure 1 (f) shows the encrypted image. The encryption is done using the AWGN. Figure 1 (g) and (h) shows the decrypted image with the correct order of transform.

Figure 1(a) Test Image 1

Figure 1(b) Test Image 2

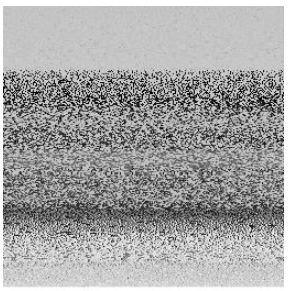

Figure 1(c) Scrambled Image 1

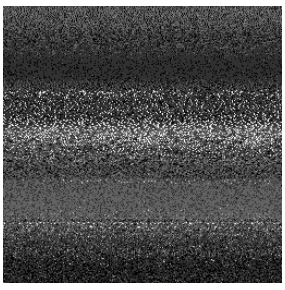

Figure 1(d) Scrambled Image 2

ISSN: 2454-4248
37 – 41

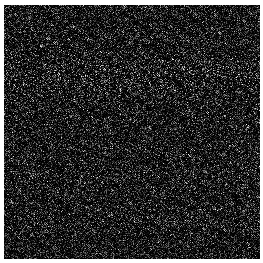

Figure 1(e) Encrypted Image 1

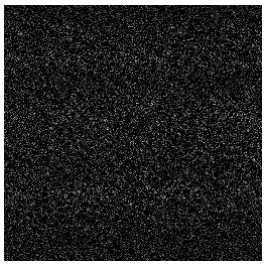

Figure 1(f) Encrypted Image 2

Figur 1(g) Decrypted Amplitude Image

Figure 1(h) Decrypted Phase Image

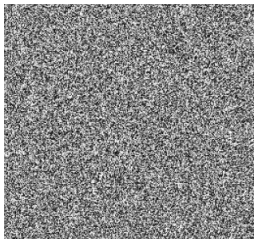

Figure 1(i) Amplitude based image using wrong order of transform

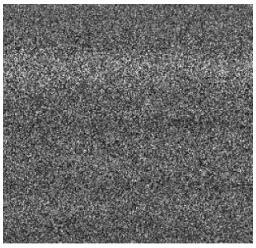

Figure 1(j) Phase based image using wrong order of transform

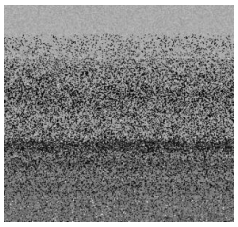

Figure 1(k) Amplitude based image using wrong scrambling of pixels

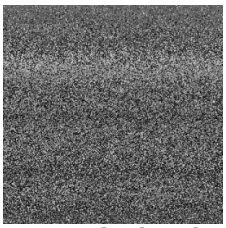

Figure 1(l) Phase based image using wrong scrambling of pixels

V. Histogram Analysis

Basically, Histogram analysis represents the frequency of change in the gray level pixel values of the image. Histogram of an image has some certain behavior and for the encrypted image it is in random nature. So from experiments the histogram of the original image of Test Image 1 and Test Image 2 is shown in Figure. 5.8(a), (b) and histogram after combining two images and after encrypting the combination image is shown in Figure. 2 (c), (d) respectively

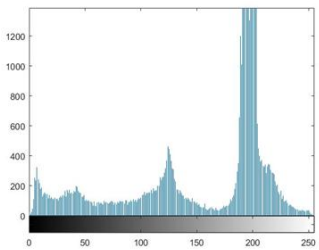

Figure2 (a) Histogram for Test Image 1

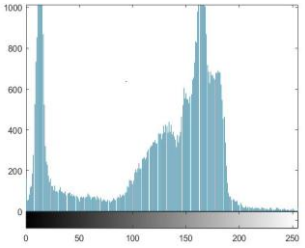

Figure 2 (b) Histogram for Test Image 2

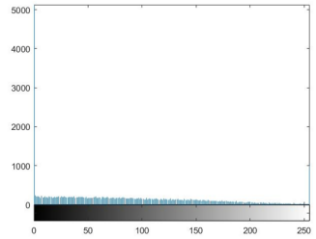

Figure 2 (c) Histogram for Combination of images

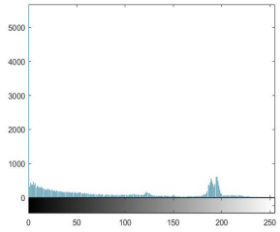

Figure 2 (d) Histogram for Encrypted Images

VI. Conclusion

In this research work main motive is the Encryption & Decryption of image in a highly efficient manner. 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.

References

[1] Stern, Adrian. "Why is the linear canonical transform so little known?." In AIP Conference Proceedings, vol. 860, no. 1, pp. 225-234. AIP, 2006.

[2] Koc, Aykut, Haldun M. Ozaktas, Cagatay Candan, and M. Alper Kutay. "Digital computation of linear canonical transforms." IEEE Transactions on Signal Processing 56, no. 6 (2008): 2383-2394.

[3] Oktem, Figen S., and Haldun M. Ozaktas. "Exact relation between continuous and discrete linear canonical transforms." IEEE signal processing letters 16, no. 8 (2009): 727-730.

[4] Pan, Wu, and Jing Qiao. "An iterative optical image encryption based on double random phase." In Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 14, pp. V14-80. IEEE, 2010.

[5] Huang, Qinglong, and Jianlan Liu. "Secure image encryption technique based on multiple Fresnel diffraction transforms." In Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on, pp. 1-4. IET, 2006.

[6] Hwang, Hone-Ene, and Pin Han. "A novel wavelet transform algorithm for image encryption." In Optical Fibre Technology/Australian Optical Society, 2006. ACOFT/AOS 2006. Australian Conference on, pp. 1-1. IEEE, 2006.

[7] Zhang, Changjiang, Jinshan Wang, and Xiaodong Wang. "Digital image watermarking algorithm with double encryption by Arnold transform and logistic." In Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on, vol. 1, pp. 329-334. IEEE, 2008.

[8] Zheng, Wei, Zhi-Gang Cheng, and Yue-li Cui. "Image data encryption and hiding based on wavelet packet transform and bit planes decomposition." In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on, pp. 1-4. IEEE, 2008.

[9] Yoshimura, Hiroyuki, and Reiko Iwai. "New encryption method of 2D image by use of the fractional Fourier transform." In Signal Processing, 2008. ICSP 2008. 9th International Conference on, pp. 2182-2184. IEEE, 2008.

[10] Pang, Chun-jiang. "An image encryption algorithm based on discrete wavelet transform and two dimension cat mapping." In Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on, vol. 2, pp. 711-714. IEEE, 2009.

[11] Zhao, Hui, Qiwen Ran, Guixia Ge, Jing Ma, and Liying Tan. "Image encryption based on random fractional discrete cosine and sine transforms." In Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on, vol. 1, pp. 804-808. IEEE, 2009.

[12] Chuang, Cheng-Hung, and Guo-Shiang Lin. "Adaptive steganography-based optical color image cryptosystems." In Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on, pp. 1669-1672. IEEE, 2009.

[13] Zhou, Nanrun, and Taiji Dong. "Optical image encryption scheme based on multiple-parameter random fractional Fourier transform." In 2009 Second International Symposium on Electronic Commerce and Security, pp. 48-51. IEEE, 2009.

[14] Zhang, Lin, Jianhua Wu, and Nanrun Zhou. "Image encryption with discrete fractional cosine transform and chaos." In Information Assurance and Security, 2009. IAS'09. Fifth International Conference on, vol. 2, pp. 61-64. IEEE, 2009.

[15] Lang, Jun, Ran Tao, and Yue Wang. "The Generalized Weighted Fractional Fourier Transform and Its Application to Image Encryption." In Image and Signal Processing, 2009. CISP'09. 2nd International Congress on, pp. 1-5. IEEE, 2009.

[16] Zhang, Shuo, Ruhua Cai, Yingchun Jiang, and Shiping Guo. "An image encryption algorithm based on multiple chaos and wavelet transform." In Image and Signal Processing, 2009. CISP'09. 2nd International Congress on, pp. 1-5. IEEE, 2009.

[17] Wang, Juan. "Image encryption algorithm based on 2-D wavelet transform and chaos sequences." In Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on, pp. 1-3. IEEE, 2009.

[18] Zhang, Yuhong, and Fenxia Zhao. "The algorithm of fractional Fourier transform and application in digital image encryption." In Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on, pp. 1-4. IEEE, 2009.

[19] Naeem, Ensherah A., Mustafa M. Abd Elnaby, and Mohiy M. Hadhoud. "Chaotic image encryption in transform domains." In Computer Engineering & Systems, 2009. ICCES 2009. International Conference on, pp. 71-76. IEEE, 2009.

[20] Hennelly, Bryan M., and John T. Sheridan. "Fast numerical algorithm for the linear canonical transform." JOSA A 22, no. 5 (2005): 928-937.

[21] Stern, Adrian. "Why is the linear canonical transform so little known?." In AIP Conference Proceedings, vol. 860, no. 1, pp. 225-234. AIP, 2006.

[22] Koc, Aykut, Haldun M. Ozaktas, Cagatay Candan, and M. Alper Kutay. "Digital computation of linear canonical transforms." IEEE Transactions on Signal Processing 56, no. 6 (2008): 2383-2394.

[23] 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.

[24] Zhang, Hai-Yan. "A new image scrambling algorithm based on queue transformation." In Machine Learning and Cybernetics, 2007 International Conference on, vol. 3, pp. 1526-1530. IEEE, 2007.

[25] Zhang, Hai-Yan. "A new image scrambling algorithm." In Machine Learning and Cybernetics, 2008 International Conference on, vol. 2, pp. 1088-1092. IEEE, 2008.

[26] Xiangdong, L. I. U., Zhang Junxing, Zhang Jinhai, and He Xiqin. "Image scrambling algorithm based on chaos theory and sorting transformation." IJCSNS International Journal of Computer Science and Network Security 8, no. 1 (2008): 64-68.

[27] Jing, Fan, and Huang Fei. "FAN transform in image scrambling encryption application." In Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference on, pp. 1-4. IEEE, 2009.

[28] 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.

[29] 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.

[30] 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.

[31] Vilardy, Juan M., Jorge E. Calderon, Cesar O. Torres, and Lorenzo Mattos. "Digital images phase encryption using fractional Fourier transform." In null, pp. 15-18. IEEE, 2006.

[32] Fan, Jinping, and Yonglin Zhang. "Color image encryption and decryption based on double random phase encoding technique." In Photonics and Optoelectronics, 2009. SOPO 2009. Symposium on, pp. 1-6. IEEE, 2009.

[33] Pan, Wu, and Jing Qiao. "An iterative optical image encryption based on double random phase." In Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 14, pp. V14-80. IEEE, 2010.

[34] Kumar, M. Ratheesh, C. L. Linslal, VP Mahadhevan Pillai, and Sudheer Sreedhara Krishna. "Color image encryption and decryption based on jigsaw transform employed at the input plane of a double random phase encoding system." In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on, pp. 860-862. IEEE, 2010.

[35] Lai, Jinhui, Song Liang, and Delong Cui. "A novel image encryption algorithm based on fractional Fourier transform and chaotic system." In Multimedia Communications (Mediacom), 2010 International Conference on, pp. 24-27. IEEE, 2010.