International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 7
ISSN: 2454-4248
43 – 47

A Review on 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, 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.

Keywords*-data security; scrambling; encrytion; linear cononical transform.*

*****

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. 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 asLCT (Linear Canonical Transform) is one of the transform which is used widely in double picture encryption process due to its efficient outputs.

II. LITERATURE REVIEW

a. Encryption & Decryption

Qinglong Huang et al.in paper, "Secure Image Encryption Technique Based on Multiple Fresnel Diffraction Transforms", (2006) projected an algorithm which specified image encryption by a secure method using a transform which is called Multi Fresnel diffraction transform (MFST). This algorithm based on the distance of the diffraction, decryption will only take place when the keys have the exact values & one another advantage of this algorithm is that it is secure to the error caused by any mean. In the MFDTs, no "one-to-one" bond is present between the simple text & the text improved with ciphering. It is highly tedious to decode it using optical scanning. Encryption scheme which is used here have high ability to protection from outer malfunctions.[1]

Hone-Ene Hwang, et al. in the paper, "A Novel Wavelet Transform Algorithm for ImageEncryption", (2006) Projected A digital security system with high efficiency. This is based on the special type of wavelet transform (DCPWT) which is a chirp parent type wavelet transform [2].

Changjiang Zhang et al. in the paper, "Digital Image Watermarking Algorithm with DoubleEncryption by Arnold Transform and Logistic", (2008) projected an algorithm for insertion of a particular watermark & then detection process highly dependent on the wavelet transform which is stationary in nature [3].

Zheng Wei et al. in the paper, "Image Data Encryption and Hiding Based on Wavelet Packet Transform and Bit Planes

 ISSN: 2454-4248
43 – 47

decomposition", (2008) projected an efficient scheme to encoding & inherit grey scale images using bit planes decomposition & wavelet packet transform [4].

Hiroyuki Yoshimuraet al.in the paper, "New encryption method of 2D image by use of the fractional Fourier transforms", (2008) projected an algorithm for secure broadcast of image data [5].

Chun-jiang pang, in the paper, "An image encryption algorithm depends on discrete wavelet transform and two-dimension cat mapping" (2009) projected an algorithm for image encryption, by splitting the 2-dimensional mapping progression which is like a cat in nature, for origination of 2 value sequences, as per the dispersion of these 2 value sequence, launch elite comparable relationships between distinct wavelet translation coefficient matrix and the two-dimensional cat mapping chaos sequence [6].

Hui Zhaoet al. in the paper, "Image Encryption Based on Random Fractional Discrete Cosineand Sine Transforms", (2009) projected an algorithm for the image encryption by use of an approach which based of fractional transform of sine & cosine of different levels [7].

Cheng-Hung Chuang et al. in the paper, "Adaptive Steganography-based Optical ColorImage Cryptosystems",(2009), projected an image encryption and decryption algorithm with adaptive steganography based on an optical cryptosystem for colored image [8].

Nanrun Zhou et al.in paper, "Optical image encryption scheme based on multiple parameter random fractional Fourier transform", (2009) projected a way for encryption of image with multiple parameter random fractional Fourier transform (MPRFrFT) [9].

Lin Zhang et al. in the paper, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", (2009) projected an image encryption algorithm using DFrCT and chaos [10].

Jun LANG et al. in paper, "The Generalized Weighted Fractional Fourier Transform and Its Application to Image Encryption", (2009) projected a way for the image encryption using Shih's WFRFT have 2four dimensional vector parametric quantity (M,N) ∈Z4, that is referred as Generalized Weighted FrFT [11].

Shuo Zhang et al. in paper "An Image Encryption Algorithm Based on Multiple Chaos and Wavelet Transform" (2009), projected a technique in which 3 systems of 3d is merged with a logical disorderly map on the image to be encrypted [12].

WANG Juan in the paper, "Image Encryption Algorithm Based on 2-D Wavelet Transform and Chaos Sequences",(2009), projected a method for the image encryption based on the characteristics of disorderlyscheme [13].

Yuhong Zhang et al. in paper, "The algorithm of Fractional Fourier Transform and application in digital image encryption", (2009), projected a methodto encode an image which is helpful in transmission of internet information [14],

Ensherah A. Naeemet al. in paper, "Chaotic Image Encryption in Transform Domains", (2009) projected a encoding method depends on the disorderly Baker map, in dissimilar transform domains [15].

b. Linear Canonical Transform

Bryan M. Hennelly et al. paper, "Fast numerical algorithm for the linear canonical Transform", (2005) tells about the effect of any quadric phase system on an optical wave field using LCT calculation algorithm. There are many types of LCT such as fractional Fourier transform (FRT), the Fourier transform (FT), and the Fresnel transform (FST) which reports free-space propagation [16].

Adrian Stern et al. paper, "Why is the LCT so little known?",(2006),is about the LCT study. LCT is categorized as parameterized continuum named transforms with some specific cases, such as the Fourier transform, fractional Fourier transform(FRFT), Fresnel transform (FRST), time scaling, chirping which are commonly used linear transforms & operators in engineering & physics [17].

Aykut Koc et al. in paper, "Digital Computation of Linear Canonical Transforms", (2008) projected an exact and effective way to handle the problem of digital computation of the samples of the LCT of a function as compare to the samples of the original function [18].

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 [19].

c. Image Scrambling

Hai-yanzhang in paper, "A New Image Scrambling Algorithm Based on Queue Transformation", (2007), paper depicts the Image scrambling algorithm [20], which is based on improved queue transformation on previous approach by removing all the disadvantages presented in the previous approach.

HAI-YAN ZHANG in paper, "A New Image Scrambling Algorithm", (2008), paper presented a new image scrambling algorithm based on advanced transforms such as wavelet transformation and queue transformation [21].

LIU Xiang dong et al. in paper, "Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation", (2008), as the paper named it presented a novel image scrambling approach based on chaos theory and the sorting transformation [22].

Fan Jing et al. in paper, "FAN Transform in Image Scrambling Encryption Application", (2009), paper presented a image encryption method in the digital watermarking technology [23], often it uses Arnold transform scrambling watermark images, but Arnold transform is given only one open form, so reducing their security.

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 [24]. To achieve the effect of image scrambling, each pair of pixel points is exchanged to all the possible pair combinations.

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 abetter magic cube turning round scrambling method [25].

Zhang Zhao et al. in paper, "Image encryption algorithm based on Logistic chaotic system and s- box scrambling",

 ISSN: 2454-4248
43 – 47

(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 [26].

d. Double Random Phase Masking & Encoding

Juan M. Vilardyet al. in the paper "Digital Images Phase Encryption using Fractional Fourier Transform", (2006) used FFT and proposed a image encoding way to get phase encrypted images .In this method, image which we want to modify is kept according to phase , used fractional transform 3 times and then in medium step multiply by 2 stable phase masks. Thus for getting encoded image, the modification method is put in opposite to coupled complex of encoded image and after that from decoded method , take negative of phase from consequent image thus we received original image that had been encode and decoded [27].

Jinping Fan et al. in paper, "Color image encryption and decryption based on double randomphase encoding technique", (2009), proposed a latest method image encoding which is related to2 times phase encoding method. In this method we separated to be encoded image into red, green and blue colors [28].

WuPanet al. in paper "An Iterative Optical Image Encryption Based on Double RandomPhase", (2010), Proposed a latest encoding and decoding method depends on basic of virtually confined optical scheme. The unique characteristic of this method is in this method, the master image is separated into 2 equal parts.One part is encoded by 2 phase encryption method, and its cipher text is changed into 2 phase masks that will be identity of encoding of second part.This method has two steps [29].

Ratheeshkumar M et al. in paper, "Color Image Encryption and Decryption based onJigsawTransform Employed at the Input Plane of aDouble Random Phase Encoding System",(2010), proposed a method to encode and decodecolorful image. Initially, We use jigsaw transform and after that 2 phase encoding method to encode image. At stimulant plane, we use this jigsaw transform and at Fourier sheet we put RPM. Multiplication of FT with random phase mask1 is called Jigsaw Transformed image [30].

Jinhui Lai et al. in paper "A Novel Image Encryption Algorithm Based on Fractional FourierTransform and Chaotic System", (2010) proposed an encoding method rely on FFT & chaotic method. This process has2 steps: firstly the image to be modify is encoded by applying double phase FF after that using confusion matrix (created by chaotic method), resulted image is modified. Thus we got cipher picture. In this method, protection of codes relies on random phase mask. Theoretical experiment can get by FRFT and disorderly system. Thus this code is suitable for image encoding [31].

III. IMAGE ENCRYPTION SCHEME

Our objective in this work is to do encryption & decryption of image using double pixel scrambling & LCT. For this objective it is using the MATLAB simulation in this work. From that we will analyze the variation in the values of MSE corresponding to the change in transform order which we are using. The value of MSE (Mean square error) will provide us that how much change in the image after the decryption when we change the value of order.

Methodology

The proposed work formulates the use of scrambling & the linear canonical transform in encryption and decryption of double image.

This methodology is divided in to two parts.

Generation of combination image from two scrambled images and encryption of that image using LCT & double phase encoding which is random in nature.

Encryption

The scheme which is used for the encryption of the information or data is given below in Figure 1. Assume f(xi) and g(xi)are thetwo actual images which are normalized to the highest value which is 1 & encrypted with each other.

For image encryption the image scrambling operation is suggested in (Z. Zhao et al.,2011 [26])is applied to the original image f(xi) to obtain the scrambled imageJ1[f(xi)]and anotherpixel scrambling operation is applied to the original image g(xi) and the scrambled imageJ2[g(xi)] is then encoded into a full phase function exp{iπJ2[g(xi)]}. Next the two scrambled outputs are multiplied by each other to attain the synthesized input signal C (xi) which can beexpressed as:

$$C(x_i) = J1[f(x_i)].\exp\{i\Pi j_2[g(x_i)]\}$$

Here J1 & J2 are the parameters for image scrambling.

Let M1 (xi) = exp [iP1 (xi)] and M2 (xa) = exp [iP2 (xa)] denotes 2 phase masks which are random in nature.Where P1 (xi) &P2 (xa) are statically white uniformly distributed in [0,2π] then by usingdouble random phase encoding in linear canonical transform domain, finalDistributionψ(xb) which an encrypted image for the given input is calculated as given below:

$$\Psi(x_b) = L_{II}\{L_I\{C(x_i).M_1(x_i)\}.M_2(x_a)\}$$
$$= L_{II}\{L_I\{J1[f(x_i)].\exp\{i\Pi J_2[g(x_i)]\}.M_1(x_i)\}.M_2(x_a)\}$$

$\Psi(x_b)$ is considered as an encrypted output & the distribution of this encrypted output is stationary white distribution.

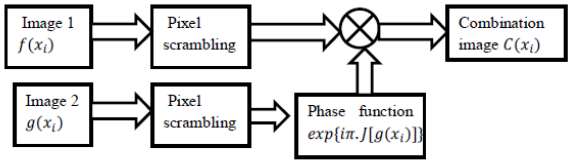

Figure 1: Creation of the composite image grouping after image scrambling

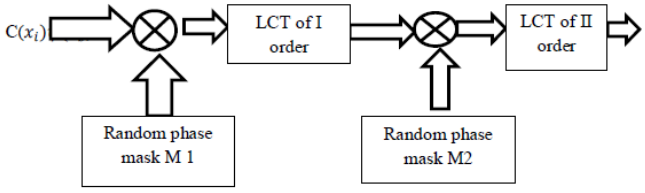

Figure 2: Encryption of the grouped image(S. Keshariet al., 2012)

Decryption

 ISSN: 2454-4248
43 – 47

The decryption process or much precisely we say the process which is used to get the original image is given in the diagrams.

Figure 3 and Figure 4 specifically shows the various processes which are conducted in the decryption process. First of all the decryption of grouped image which is composite or we can say complex in nature taken place. After the decryption our main aim is to separate the images which are grouped. This is done using the inverse pixel scrambling.

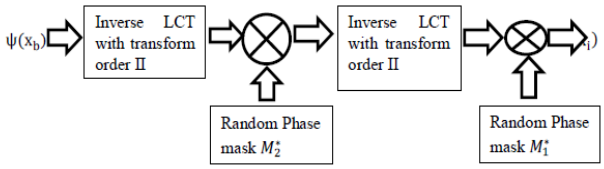

Figure 3 Decryption for encrypted composite grouped image

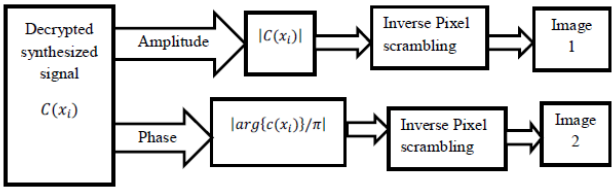

Figure 4 Disjointing of images from the Decrypted grouped image using inverse pixel Scrambling

The decrypted synthesized signal C(xi) can be obtained by application of inverse of thedouble random phase encoding in linear canonical transform domain. Mathematically it isgiven as follows:

$$C(x_i) = L_{-I}\{L_{-II}\{\Psi(x_b).M_2^*(x_a)\}.M_1^*(x_i)\}$$

Mathematical formulation for the decrypted images is given below in equations.

$$f(x_i) = J_1^{-1}(|C(x_i)|)$$

$$g(x_i) = J_2^{-1}\left\{\left|\frac{\arg(C(x_i))}{\Pi}\right|\right\}$$

Here J_1^{-1} & J_2^{-1} shows the inverse pixel scrambling operation

IV. Conclusion

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. In the literature review section various algorithm proposed by various researchers for the encryption and decryption purpose. Our objective in this work is to do encryption & decryption of image using double pixel scrambling & LCT. For this objective it is using the MATLAB simulation in this work.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

[18] 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.

[19] Shi, Jun, Xiaoping Liu, Xuejun Sha, and Naitong Zhang. "Sampling and reconstruction of signals in function spaces

 ISSN: 2454-4248
43 – 47

associated with the linear canonical transform." IEEE Transactions on Signal Processing 60, no. 11 (2012): 6041-6047.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.