Journal of Rajasthan Academy of Physical Sciences
ISSN: 0972-6306; URL: http://raops.org.in
International Conference on Mathematical and Statistical Computation (ICMSC-2022)
Swami Keshvanand Institute of Technology (SKIT), Jaipur, Rajasthan, (India) 3rd-5th March 2022
October, 2022, 107-118

PROFICIENT CRYPTOGRAPHY TECHNIQUES FOR IMAGES USING RAJAN TRANSFORM AND QUADRATIC EQUATION

B. Paulchamy,[1] S. Vairaprakash,[2] S. Chidambaram[3] and **K. Mahendrakar[4]**
[1]Professor and Head, Department of ECE, Hindustan Institute of Technology, India
[2]Associate Professor, Department of ECE, Ramco Institute of Technology, India
[3]Assistant Professor, Department of ECE, Christ University, India
[4]Associate Professor, Department of ECE, Hindustan Institute of Technology, India
Email: luckshanthpaul@gmail.com (Corresponding author)

Abstract: In the recent world, security is an important issue in transmitting information from end to end. Cryptography is a means of encrypting the original information into unreadable form to unauthorized individuals so that authorized recipients can decrypt and can be readily understood. As an alternative to other approaches, Rajan Transform (RT) is used as a tool for cryptography. RT exhibits invariance property in shifting and inverse. In these proposed methods, Rajan transforms changed the original pixels values. The Cumulative Point Index (CPI) is shifted and then the converted image is shuffled using Arnold Cat map and diffusion process is done by performing XOR operation between shuffled image and Transformation matrix obtained by using Henon map. The main purpose of using Rajan transform is that generation of keys in each stage and Inverse Rajan Transform (IRT) is done depending upon encryption keys. This shows that IRT is not reversible. Experimental results for statistical, differential attacks and the parameters Correlation Coefficient (CC), Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were done. The results demonstrated high resistance to attacks.

Keywords: Rajan Transform, Inverse Rajan transform, Cumulative Point Index, Image Encryption

1. Introduction

In recent world, Multimedia transmissions through communication networks have been created. For secure Image Transmission, Image encryption plays a vital role in transferring images through end to end. In cryptography there are so many algorithms such as AES, RSA, Diffehelmenkey etc. have been developed. For Image transmission and reception, Images with high security, good quality, Pixel correlation and speed attracts much attention.

A new transformation is introduced named Rajan in [1]. This transformation exhibits Invariance and duality. The transformed sequence contains CPI (first sequence in the transform) which contains maximum information and encrypted sequences. Rajan transform is a suitable tool for image watermarking, image encryption and for digital signatures.

Fractional transformations is applied to individual images in [4]. Individual image is transformed by using Fractional Wavelet, Dual tree complex wavelet. The transformed image is confused by using 2-D Arnold map with k-iterations. Then random matrix is created and it is XORed with confused image. Finally, all images are shared by using linear functions.

A new encryption method based on Henon map and matrix is proposed in [8]. Instead of generating random matrix for diffusion, Henon map is employed to create the transform matrix equal to image size and it is added with Image. Finally, it is XOR with Image. Here Decryption is irreversible. By using Arnold or Baker's map in confusion phase and PESH in diffusion various better results have been achieved.

In 3D chaotic Encryption proposed in [2], various attacks have been analysed, By increasing the number of Cipher rounds in chaotic system Number of Pixels Change Rate (NPCR) is increased and Unified Average Changing Intensity (UACI) has reduced. In [10], speed of the encryption is analysed

Efficient image security by means of Fractional Fourier Transform (FrFT) and Arnold cat map is presented [11]. In this technique, FrFT is applied to the image. The scrambling and diffusion process is done in the transformed image[7]. In the confusion phase, Arnold cat map is used to jumble up the image pixels by k iteration. Then the diffusion process is done by Henon maps. There is no correlation between encrypted images by the change of key values. Also, the change in pixel pair is entirely different. The major drawback is that the purpose of FrFT is not mentioned. For the process of confusion and diffusion, the use of transformed coefficients is missing. Also, the method is straightforward and unable to resist the attack.

Improved hyper-chaotic sequences are used to generate a key stream [12]. The final key stream is related to initial key values and also plain image. Two rounds of diffusion operations are carried out in the encryption algorithm. But it has broken with two known plain images. A chaotic image encryption scheme has a large key space with one round diffusion process, but it is unable to resist the differential attack because it has low key sensitivity [13]. The DWT is decomposed to generate matrices which are recombined to scramble [14]. The initial state and system parameters are sensitive with sizeable key space, and the algorithm has low computation complexity and it is highly robust against attacks. In the diffusion process, some image encryption schemes only accomplish XOR operation on the original or scramble images [15,16].

In this paper DRT is used as cryptographic tool for generation of encryption keys. Arnold Cat map is used for pixel shuffling. Transformation matrix using Henon map is used for matrix generation for diffusion phase. In diffusion phase shuffling pixels are XORed with matrix and previous ciphers to obtain Encrypting image.

2. Methodologies

2.1 Discrete Rajan Transform

Multi resolution transforms [4] performs decomposition where the order of fractional decomposition acts as key. Discrete Rajan Transform (DRT) [1] is one to one map transformation technique. This transformation is derived from Decimation in Frequency (DIF-FFT) but it is different. The elements used for transformations are arithmetic adder and subtractor. The peculiar characteristics of this algorithm is that it generates encryption sequence in each stage and finally encryption keys together with transformed sequences is appeared. For N sequence $N=2^m$ where m is the number of stages. For every N-point sequence, N transformed sequence and 3N encrypted sequences. Inverse Rajan Transform will be changed for every N-point transformed sequence depends upon the encryption keys.

Normally transformed image contains ac and dc coefficients. Here Cumulative Point Index (CPI) is a pixel which contains major information that are collected from individual pixels in each block. Hence it should be protected. Inverse Rajan Transform (IRT) consists of average, maximum and subtractor elements. Depending upon the encryption keys associated with transformed sequences, inverse algorithm differs. Hence IRT algorithm varies for each and every block. This proves that encryption using RT is highly secure.

In the initial stage, block (N=8) is divided into N/2 each containing four sequences. DRT is applied to corresponding sequences in the divided block. Again N/2 is separated into N/4 each containing two sequences. Finally, N/4 is separated into N/8 and DRT is applied in order to obtain N transformed sequence.

2.2 Arnold Cat map

The pixels in the image are shuffled by division and rotation as stated in [9]. Then Arnold cat map is used for scrambling. The pixels in the image are shuffled by using Arnold cat map. The mapping of pixels in new position is determined by 2D Arnold discretization map which is given by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

where a and b are positive integers which is equal to 1. (x', y') is the new location of the pixel by performing Arnold map one time. N denotes the breadth or height of the Image. Here modulus function is used to maintain the image size [5]. The period of cat map which varies [6] depends upon the size of the image

2.3 Diffusion Process

N.S. Raghava & Ashish Kumar [8] proposed image security using Henon map. The matrix will be generated using henon map and the obtained values are converted into 0 and 1 by using threshold. Then it is converted into binary and groups into 8-bits and XOR with image.

In diffusion phase, Henon map is used as initial vale for generating matrix equal to image size. The modified henon map given in [3] is as follows:

$$x(i+2) = 1 - a(x(i+1))^2 + b\,x(i) \quad (2)$$

The various and modified forms of Henon map as described in [11] are as follows:

Henon map 1: $$x\,(i+2) = 1 + a.x(i+1) - \frac{b}{x(i)} \quad (3)$$

Henon map 2: $$x(i+2) = a.x(i+1) + b.x(i+1) \quad (4)$$

Henon map 3: $$x(i+2) = a.x(i+1) + \frac{b}{1-x(i)} \quad (5)$$

Henon map 4: $$x(i+2) = a.x(i+1) + b.x(i) \quad (6)$$

where i ranges from 0 to quantity of pixels in the image. The factor a = 1.4 and b = 0.3 and initial values x (0) = 0.01 and x(1) = 0.02. For i = 0,1,2 matrix values are generated by the equation as stated in f(i) = x(i)*(x(i)+1) and Henon map 1 by substituting the initial values .For further values of i, Henon map 2,3,4 will generate matrix values and the process again repeats from Henon map1.

Hence the matrix M of size equal to image size I will be obtained. Two-dimensional matrix will be created by adding the image elements to double of M (I, j) matrix. The generated matrix elements W (i, j) will be XORed with image pixels I (i, j) together with previously obtained Ciphered pixel.

$$E(i, j) = I(i, j) \oplus W(i, j) \oplus E(i-1, j-1) \quad (7)$$

The result of the diffusion phase will be the encrypted Image. Here the parameters a, b and preliminary values used for matrix generation acts as secret keys.

3. Image Encryption Using DRT

Image encryption consists of transformation, shuffling and diffusion phase is shown in figure 2.

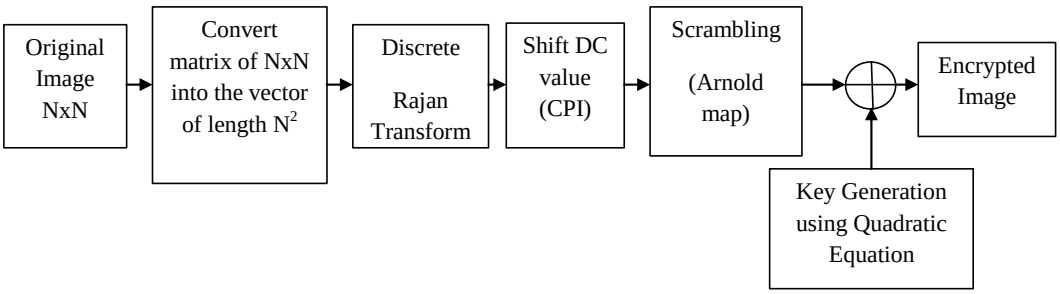

Fig 2: Process flow diagram of proposed Image Encryption

The steps to be followed in image encryption are as follows:

1. Consider a plain image of size NxN. Convert the image into size $1xN^2$
2. Scan the image into blocks each of length N=8.
3. Apply DRT to the scanned vectors N=8 to obtain eight transformed sequences together with 24 encrypted keys. Therefore, as a result of DRT, totally 32 sequences is generated.
4. Repeat the process for all blocks in the image to obtain N x N DRT sequences and 3xNxN encrypted keys (keys1). Shift the CPI of DRT sequence by N (2^4-1).
5. Shuffle the transformed pixels using Arnold cat map with K(key2) iterations [5].
6. *Diffusion process*. Based upon these initial values and Henon map, matrix elements 0,1,2 is obtained by substituting the initial values in the equation stated as

$$f(i) = x(i) * [x(i) + 1] \quad (8)$$

Thus, for each matrix element, each Henon map and the quadratic equation is used

7. Analyse various attacks to achieve high security.
8. In the receiver side, by knowing the secret keys in diffusion, shuffling and correct order of encryption keys in DRT, decrypted image is obtained.

The process flow diagram of proposed decryption is shown in Figure 3.

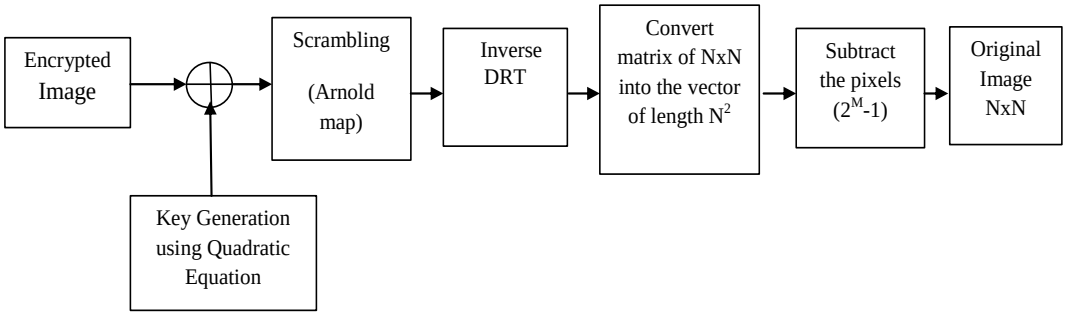

Figure 3 Proposed flow diagram of image decryption

4. Results and Discussion

Image encryption algorithm using Rajan Transform performance is demonstrated using MATLAB. Here encryption sequences of size (3xMxN) generated in RT, shuffling iterations, Initial values and parameters used in diffusion process are acted as keys in the encryption process. The original, encrypted and decrypted images of the suggested method are shown in Figure 3

Fig.3 a) Original image b) Encrypted Image c) Decrypted image

In the above, Fig 3.a) shows the original image, Fig 3.b) is the result of Arnold cat map shuffling with iteration five rounds. Fig 3.c) is the diffusion phase output image. Encryption scheme should be robust for all cryptanalytic attacks. Hence statistical, differential attacks analysis have been done to prove the security.

1. Statistical attack

The resistance to statistical attack has been demonstrating in the shuffling and diffusion phase. Correlation between pixels: The correlation coefficient measured between adjacent pixels is obtained by equation (10). The similarity between pixels is calculated by the formula and correlation coefficient will be 1 for highly correlated images.

$$\operatorname{cov}(x, y) = E[(x - E(x)) - (y - E(y)] \tag{9}$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{\sum_{i=1}^{N} (x - E(x))^2} \sqrt{\sum_{i=1}^{N} (y - E(y))^2}} \tag{10}$$

where x_i and Y_i are grey values of two adjacent pixels in image. E(x) & E(y) are mean of the pixels.

Arbitrarily choose 5000 pairs of two neighbouring pixels in horizontal, vertical and diagonal directions of an image and correlation coefficient is calculated. Similar calculations have been done for encrypted image. The correlation coefficients for horizontally adjacent pixels are 0.9675 and -0.0158 which is far apart. Table 1. Illustrates the pixel relationship for original and encrypted image in horizontal, vertical and diagonal directions.

Image	**Adjacent pixels in**	**Original Image**	**Proposed method**	**Mona FM Mursi *et al.* (2014)**
			Encrypted image	Encrypted image
Lena	Horizontal	0.9422	0.0001	0.0005
	Vertical	0.9641	-0.0157	0.0003
	Diagonal	0.9319	0.0025	0.0085
Boat	Horizontal	0.9347	0.0028	0.0118
	Vertical	0.9448	-0.0204	-0.0214
	Diagonal	0.9161	0.0014	0.0053
Cameraman	Horizontal	0.9587	-0.0112	0.0072
	Vertical	0.8936	0.0022	0.0052
	Diagonal	0.9047	0.0038	0.0052

	Vertical	0.9213	-0.0114	0.0024
	Diagonal	0.9225	0.0015	0.0053
Peppers	Horizontal	0.9547	-0.0022	-0.0082
	Vertical	0.9613	0.0034	0.0076
	Diagonal	0.9304	-0.0051	-0.0037
	Vertical	0.9556	0.0153	0.0353
	Diagonal	0.9516	-0.0156	0.0002
Plane	Horizontal	0.9247	0.0029	-0.0011
	Vertical	0.9427	0.0177	0.0326
	Diagonal	0.9172	0.0046	0.0138

Table 1. Correlation Coefficient analysis between adjacent pixels

The distributions of two adjacent pixels in the original and the encrypted images are shown from Figure 4 and Figure 5.

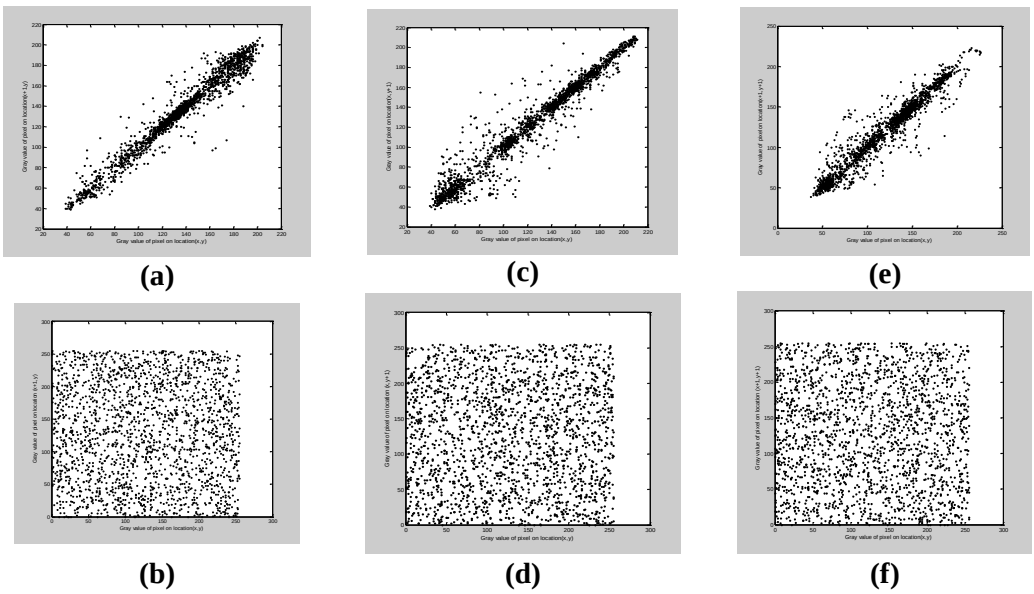

Figure 4 Correlation investigations between original Lena image and ciphered image: (a) and (b) Horizontal correlation of Lena image and ciphered image respectively. (c) and (d) Vertical correlation of Lena image and ciphered image respectively. (e) and (f) Diagonal correlation of Lena image and ciphered image respectively.

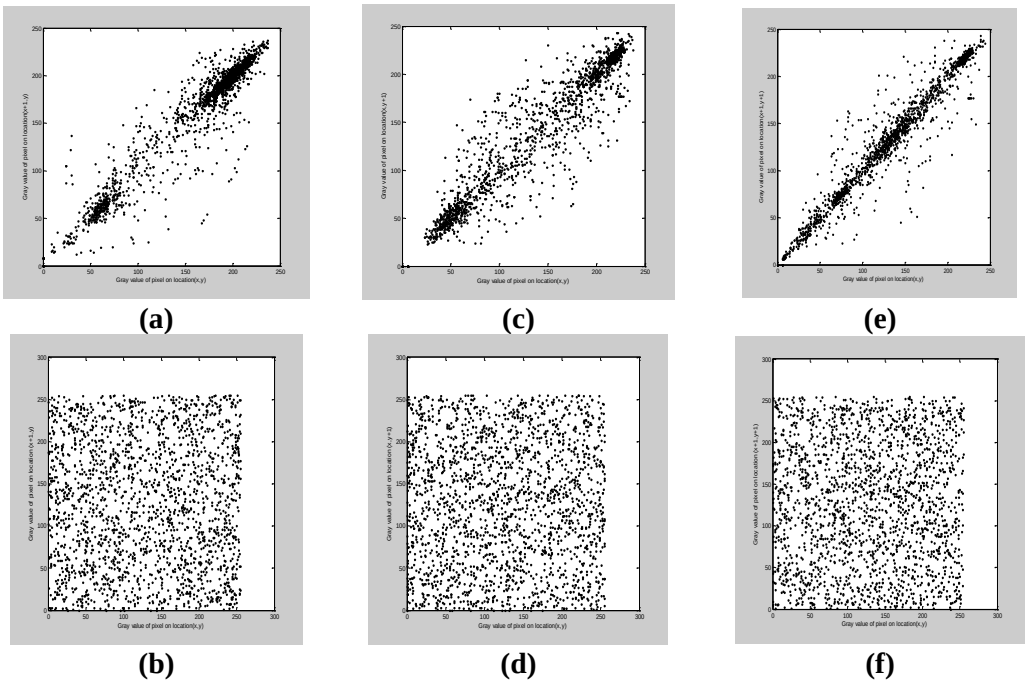

Figure 5 Correlation investigations between original Plane image and ciphered image: (a) and (b) Horizontal correlation of Plane image and ciphered image respectively. (c) and (d) Vertical correlation of Plane image and ciphered image respectively. (e) and (f) Diagonal correlation of Plane image and ciphered image respectively.

From the figures, it is observed that after the encryption, pixels correlation is broken and after the decryption, pixels are bound together with original correlation.

4.2 Differential Attack

Consider an original image with a change of one pixel. The influence of change of one pixel is measured in terms of two measures namely Number of Pixels Change Rate (NPCR) and Unified Average Changing intensity (UACI).

Let $E_1(i, j)$ and $E_2(i, j)$ be the encrypted images before and after one pixel change. Therefore NPCR is calculated by using equation (11)

$$NPCR = \frac{\sum_{i,j} D(i, j)}{M \, x \, N} x100 \tag{11}$$

where $D(i, j) = \begin{cases} 1 & if \;\; E_1(i, j) = E_2(i, j) \\ 0 & if \;\; E_1(i, j) \neq E_2(i, j) \end{cases}$; and M $\times$ N denotes size of the image.

The NPCR gives total number of pixels that are differed from $E_1(i, j)$ and $E_2(i, j)$. Higher the NPCR give high security.

UACI is defined as

$$UACI = \frac{1}{MxN}\sum_{i,j}\frac{\left|E_1(i,j)-E_2(i,j)\right|}{255}x100 \quad (12)$$

Average Intensity difference between two encrypted images should be low as possible.

Table 2. illustrates the NPCR and UACI between before and after one pixel change in the encrypted image

Image	**Proposed DRT and Quadratic equation**		**Mona FM Mursi *et al.* (2014)**	
	NPCR	UACI	NPCR	UACI
Lena	99.63	33.31	99.58	28.14
Boat	99.6	33.36	99.59	33.25
Cameraman	99.61	33.42	99.602	33.29
Peppers	99.63	33.43	99.6	33.36
Plane	99.66	33.52	99.56	33.39

Table 2 NPCR and UACI performance

From the table, it is observed that average NPCR is 99.62% and average UACI is 33.41%. This means that more than 99.62% of pixels in the encrypted image change their grey level when there is a change in one of the pixels.

5. Conclusion

In this paper, image security using Rajan Transform is proposed. Here Rajan transform is used as a cryptographic tool. In this work, RT changes the pixels and also generates encryption keys which are different for every eight pixels. The peculiar is that Inverse Rajan Transform used in decryption process will be varied for each block depending upon encryption keys. Hence the algorithm provides high security and robust. The experimental results were analysed in terms security. From the observations of NPCR and UACI analysis, encryption techniques are highly resisted to attacks and robust. Also, Correlation coefficient between neighbouring pixels in encrypted image is far away from that of original image. In the proposed work, encryption keys of size 3 times that of image size that is generated in RT, Initial values and factors used in diffusion a, b, x (0), x (1) are acted as secret keys. In future, compression technique will be implemented for handlings of Rajan transform keys.

Acknowledgement: The authors are thankful to the Referee for valuable comments and suggestions.

References

[1] Mandalapu Ekambaram Naidu, and E.G. Rajan (2006). Two-Dimensional Object Recognition using Rajan Transform, Engineering letters.

[2] Guanrong Chen, YaobinMao, Charles and K. Chui (2004). A symmetric Image Encryption scheme based on 3D chaotic at maps, Elsevier.

[3] Osama M. Abu Zaid, NawalA.El-Fishawy, E.M. Nigm and Osama S. Faragallah (2013). A proposed Encryption Scheme based on Henon chaotic system for image security, International Journal of Computer Applications.

[4] S. Arivaghagan, W. Sylvia Lilly Jebarani and M. Lakshmi (2015). Multiple Image Encryption using Fractional Multiresolution Transforms, International Journal of Applied Information Systems.

[5] Jianzhong Bao (2012). Period of the discrete Arnold cat map and general cat map, Springer.

[6] Pan Tian-gong and Li Da-yong (2013). A Novel Image Encryption Using Arnold Cat, International Journal of Security and Its Applications.

[7] Yadava, Ramesh Kumar, Dr. B. K. singh, S.K. Sinha, and K. Pandey (2016). A New Approach of Colour Image Encryption based on Henon like Chaotic Map, Journal of Information Engineering and Applications.

[8] Raghava, N. S. and Ashish Kumar (2013). Image Encryption Using Henon Chaotic Map with byte sequence, International Journal of Computer Science Engineering.

[9] Asia Mahdi Naser Alzubaidi (2014). Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System, International Journal of Engineering Research & Technology.

[10] Wanga, Y., Wanga, K.W., Liao, X. F. and Chen, G. R. (2011). A New Chaos-Based Fast Image Encryption Algorithm, Applied Soft Computing.

[11] Mona, FM Mursi, Hossam Eldin H Ahmed, Fathi, E, Abd El-same & Ayman H Abd El-Azeem (2014). Image encryption based on development of Henon chaotic maps using fractional Fourier transform, International Journal of Strategic Information Technology and Applications, 5(3), 62-77.

[12] Cong Zhu (2012). A novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications.

[13] Benyamin Norouz, Sattar Mirzakhani and Seyed Mohammad Seyedza (2014). A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimedia Tools and its Applications.

[14] Wei Wang, Haiyan Tan, Yu Pang, Zhangyong Li, Peng Ran and Jun Wu (2016). A novel encryption algorithm based on DWT and multichain mapping, Journal of Sensors.

[15] Jui-Cheng Yen and Jiun-In Guo (2000). New chaotic key-based design for image encryption and decryption, Proceedings of IEEE International Symposium on Circuits and Systems, Emerging Technologies for the 21st Century.

[16] Gao, TG and Chen, ZQ (2008). Image encryption based on a new total shuffling algorithm, Chaos Solitons Fractals.