International Journal of Scientific & Engineering Research Volume 8, Issue 7, July-2017
ISSN 2229-5518

An Improved Image Encryption Scheme Based on Pixels Permutation and Fractional Wavelet Transform

Wessam M. Salama and Hassan Elkamchouchi
Electrical Engineering Department
Faculty of Engineering, Alexandria University
Alexandria, Egypt

Yasmine Abouelseoud
Engineering Mathematics Department
Faculty of Engineering, Alexandria University
Alexandria, Egypt
email address: yasmine.abouelseoud@gmail.com

Abstract— This paper presents an image encryption scheme based on pixels permutation and the discrete fractional wavelet transform. Random interleaving of pixels is employed to improve the security of the encryption scheme by extending the encryption key space. Additionally, four fractal images are used as a key component as fractals are traditionally known as efficient sources of randomness for key-stream generation. The use of the Fractional Wavelet Transform (FWT) aims to replace the pixel values of the original image, showing high correlation among adjacent pixels, by other values that conceal the features of this image from eavesdroppers. Moreover, bit shifts of pixel values are used to obtain a more uniform histogram for the encrypted image and to broaden the key space. The preliminary results show that the proposed algorithm achieves low correlation coefficients among adjacent pixels for the encrypted image, a uniform histogram, and ensures resistance to differential attacks.

Keywords— Correlation, Image Encryption, Entropy, Fractional Fourier transform, Pixels permutation.

1. Introduction

Security is a major concern in our information age. Security goals include achieving confidentiality of information, which means concealing the information content from unauthorized users. An image is worth thousands words and thus digital images is in many applications a suitable form for storing information such as medical and military applications as well as pay-per-view systems. Image encryption is one of the means of achieving secrecy, where a properly chosen key is used to convert the image to an unreadable form.

Images contain a lot of data that are strongly related to each others. An image is represented as a rectangular array of small blocks called pixels. Each pixel is assigned an intensity value that represents the color value of that part of the image. The challenge is to design a strong encryption system that is capable of breaking down the correlation inherent in image pixels and satisfying the needs of speed and ease of application for normal users.

An efficient image encryption technique must have certain properties such as small encryption time and complexity, a large key space to prohibit exhaustive search attacks, sensitivity to small changes in the plain image and in the key used and providing an encrypted image with a histogram that is significantly different from the plain image [1].

In order to protect digital images from unauthorized access and to prevent illegal reproduction and modifications to them, a variety of image encryption schemes have been proposed in literature. The existing image encryption techniques fall into three major categories: position permutation [2], value transformation (substitution) [3] and a combination of both approaches [4]. Position permutation based algorithms scramble the data positions within the image itself and usually have low security, yet they are computationally efficient. On the other hand, the value transformation algorithms substitute the data value of the original image by another one providing better security but usually they are more time-consuming compared to position permutation based algorithms. Finally, to combine the advantages of both, techniques involving both types of transformations have appeared in literature [5].

In 2010, Yoon and Kim developed a chaotic image cipher in which initially small matrices are generated using the logistic map [6]. A large permutation matrix is then generated from small matrices. The constructed permutation matrix is used to permute the plain image pixels. Another chaos-based image cipher is suggested by Ismail et al. in [7], where they use two chaotic logistic maps as well as an external secret key of 104-bits size. Control parameters for both chaotic logistic maps are generated from the external secret key [8]. Moreover, they employed a feedback mechanism in their image cipher to enhance its level of security. Chen and Chang also suggested an image encryption scheme based on two logistic maps and an 80-bit secret key. In 2011, Jolfaei and Mirghadri [9] suggested a chaotic image cipher based on pixel shuffling, using Baker's map, and a modified version of the simplified AES (S-AES), that was developed by Musa et al. in 2003[10]. Nayak et al. proposed a chaotic image cipher using the logistic map [11]. In their algorithm, permutation of image pixels is made on the basis of the index position generated by the chaotic map. Sathishkumar and Bagan [12] suggested an image cipher based on block permutation, pixel permutation and value transformation.

The finite field cosine transform (FFCT) was first defined as a finite field version of the discrete cosine transform (DCT) [13]. The FFCT interesting properties make it valuable for cryptographic purposes. In [14], a simple method for uniformizing histograms of grey scale digital images is introduced based on an 8-point FFCT without any encryption mechanism. Moreover, in [15], a method for histogram uniformization of grey scale images integrated with a full encryption mechanism is developed. Later, a FFCT-based image processing mechanism has been introduced in [16] for encrypting color images, where the three color channels of RGB images are concatenated and thus their pixels are treated as elements of $GF(2^{24})$. In [17], the fractional wavelet transform is suggested for use in image encryption. However, the authors in do not provide enough security analysis for their scheme and do not make clear suggestions for the choice of the random matrices comprising the key used for encryption.

In this paper, an improvement to the scheme in [17] is presented. The proposed scheme employs pixels permutation and bit-shifts, in addition to the fractional Fourier transform to achieve better security through widening the key space and improve the characteristics of the encrypted image, that is; an encrypted with a more uniform histogram, lower correlation coefficients and increased entropy.

The rest of the paper is organized as follows. Section 2 presents the background necessary to the understanding of the proposed scheme. In Section 3, the techniques for evaluating the quality of an image encryption scheme are reviewed. Section 4 introduces the proposed encryption scheme and Section 5 provides the results of implementing our algorithm on grayscale images. Finally, in Section 6, the paper is concluded.

2. Background

2.1 Fractional Fourier Transform

The idea of fractional powers of the Fourier transform operator appeared in the mathematical literature as early as 1929 [18,19]. However, it was not until the 1990's that it became popular due to its related interpretations and applications in optics [20]. Like for the Fourier transform, there exists a discrete version of the fractional Fourier transform.

The fractional Fourier transform (FrFT) is a generalization of the standard Fourier Transform (FT) by means of the continuous fractional order a, which covers densely the entire transition between image (or time) domain (a = 0) and the Fourier domain (a = 1). Mathematically, the a^{th} order fractional Fourier transform is the a^{th} power of the Fourier transform operator. The first order fractional transform is the standard Fourier transform. The fractional Fourier transform is, however, useful in noisy images.

The discrete fractional Fourier transform is based on an eigen-value decomposition of the discrete Fourier transform matrix. If $F = E \wedge E^{-1}$ is this decomposition, then $F^a = E \wedge^a E^{-1}$ is the corresponding discrete fractional Fourier transform matrix. The main point is to construct the Eigen-value decomposition of the discrete Fourier transform matrix F [21].

2.2. Bit Permutations and Pixels Permutations

An image can be seen as an array of pixels, each with eight bits for 256 gray levels. The bits in each pixel taken from the image are permuted according to a chosen key [22]. Bit permutations aim to generate images with a more uniform distribution of color intensities of their pixels. However, relying solely on bit permutations yields weak encryption schemes as there are only 8! possible permutations of the bits of a pixel value.

Pixel permutations provide a wider space to search through in exhaustive search attacks. Pixel permutations can be done based on chaotic maps [23,24] and/or pseudo-random number generators, such as Mersenne Twister algorithm [25].

2.4 Fractals

Fractals are self-similar objects, where self-similarity refers to the fact they are "the same from near as from far". Fractals may be exactly the same at every scale, or, they may be nearly the same at different scales [26]. Some examples of fractal images used in our work are shown in Figure 1.

Numerous fractals are readily available from the Internet, for instance, the set of fractals available from [27].

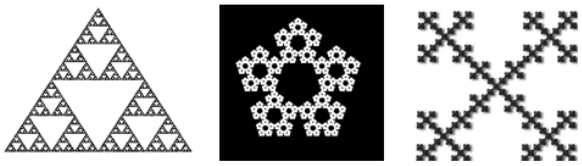


Figure 1 A sample of fractal images

2.5 Image Histogram

An image histogram is a graphical representation of the pixels intensities distribution in an image. Histograms are made up of bins, each bin representing a certain intensity value range. The histogram is computed by examining all pixels in the image and assigning each to a bin depending on the pixel intensity. The height of a bin represents the number of pixels assigned to it. The number of bins in which the whole intensity range is divided is usually in the order of the square root of the number of pixels [28].

3. Security Metrics for Image Encryption Schemes

A secure image encryption scheme should produce a cipher image showing the following desirable characteristics.

- One of the encryption targets is to make the correlation coefficients for horizontal, vertical and diagonal pixels very small [28]. This in contrast to the plain images, where adjacent pixel values show high correlation.

- For an encrypted image, the distribution of the pixel intensity values should be flat as no specific intensity should appear more than another. On the contrary, plain image usually have histograms with peaks and valleys.

- The cipher image should be much different from the plain image. One possible measure of this attribute is given by the mean absolute error (MAE) computed as

$$MAE = \frac{1}{W \text{ x } H} \sum_{i=1}^{H} \sum_{j=1}^{W} \left| P(i,j) - E(i,j) \right|$$

where P(i,j) and E(i,j) denote the color intensities of pixel (i,j) in the plain image and encrypted image, respectively. Moreover, W and H stand for the width and height of the image under consideration.

- The cipher image should be sensitive to small variations in the plain image and variations in the encryption key. Two possible measures are: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) [29]. NPCR is used to measure the percentage of pixels that are different between two encrypted images whose corresponding plain images are identical except for only one pixel and it is calculated as

$$NPCR = \frac{1}{W \text{ x } H} \sum_{i=1}^{H} \sum_{j=1}^{W} D(i,j) \text{ x } 100\% \ ,$$

where E_1 is the encrypted image from the original image and E_2 is the encrypted image from an image that has one pixel different from the original image.

Moreover, $D(i,j) = \begin{cases} 0, E_1(i,j) = E_2(i,j) \\ 1, E_1(i,j) \neq E_2(i,j) \end{cases}$.

Finally, UACI measures the average intensity of absolute differences between two encrypted images provided that their corresponding two original images are identical except for only one pixel difference and it is calculated according to the following equation:

$$UACI = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} \left| E_1(i,j) - E_2(i,j) \right| / 255 \ \times 100\% \ .$$

- The entropy value for a sequence is considered as a measure of the predictability of that sequence. In case of image encryption, the high correlation between image adjacent pixels makes it easy to predict a pixel value from neighboring pixels values and, therefore, image data have low entropy values. On the other hand, enciphered image data should appear as a random sequence to avoid any pixel predictability. This means that for a good cipher image the entropy value should be high. The entropy of a sequence with elements S_i and corresponding probability $p(S_i)$ is calculated as

$$Entropy = -\sum_{i=1}^{2^8} p(S_i) \log_2 p(S_i)$$

4. The Proposed Encryption Scheme

In this section, the proposed image encryption scheme for grayscale images is presented. The sender and the receiver should agree on the system key consisting of the following items:

- The key used in the bit shift step.
- The fractional orders (α_x , α_y) of the 2-D fractional Fourier transform.
- A seed for the interleaved pixel permutation pseudo-random number generator.
- A set of four fractal images.

4.1. Encryption algorithm steps

a. Load the plain image (I) of size N x N.

b. Apply pixels permutation based on Mersenne Twister algorithm according to the shared seed and the resulting image is denoted as (I_p).

c. Take the 2-D fractional Fourier [17] transform of I_p according to the following equation:

$$I_F = F^{\alpha x} I_s F^{\alpha y}$$

d. Load the fractal images (M_1, M_2, M_3, M_4).

e. Take the 2-D discrete wavelet transform and calculate

$\{CA, DH, DV, DD\} = DWT(I_F)$

$CAM = CA \times Mask_1$, $DHM = DH \times Mask_2$

$DVM = DV \times Mask_3$, $DDM = DD \times Mask_4$

$I_E = IDWT\{CAM, DHM, DVM, DDM\}$

where $Mask_i$ is generated from the fractal image (M_i) by applying the complex exponential function to each element of the fractal image.

f. Apply bit shift to each pixel value in I_E according to the key k. This step returns an image with pixel values shifted to the left by k bits, equivalent to multiplying by 2^k. Negative values of k correspond to shifting bits right or dividing by $2^{|k|}$. Denote the result of this step as I_s.

4.2. Decryption algorithm steps

Upon receiving the encrypted image (I_s), the following steps are carried out by the authorized recipient.

a. Apply the reverse bit shift operation to obtain I_E.

b. Compute

$\{CAM, DHM, DVM, DDM\} = DWT(I_E)$

$CA = CAM \times inv(Mask_1)$; $DH = DHM \times inv(Mask_2)$

$DV = DVM \times inv(Mask_3)$; $DD = DDM \times inv(Mask_4)$

$$I_p = F^{-\alpha x} \times IDWT(CA, DH, DV, DD) \times F^{-\alpha y}$$

where $inv(Mask_i)$ denotes the multiplicative inverse of the $Mask_i$ matrix.

c. Apply the inverse image pixels permutation to recover the original image.

5. Experimental Results

The proposed encryption scheme is implemented using MATLAB program. It is applied to a sample of 1024 × 1024 standard images available from [30], including Cameraman, Mandrill (4.2.03), Boat (4.2.05), and Peppers (4.2.07). The encryption quality is evaluated using different measures including both statistical means like correlation coefficients, and histogram analysis. Moreover, sensitivity tests like NPCR and one bit change in key have been investigated. It is clear from the results that the proposed scheme successfully meets various requirements for a strong image encryption scheme as detailed in the following points.

a. As apparent in Figures 2, 3, 4 and 5, the histogram of encrypted images is approximately uniform and clearly distinct from the original image histogram. Additionally, the proposed scheme is sensitive to small changes in the key, where one bit change in the key produces a visually corrupted decrypted image.

b. In Table1, the correlation among pixels is significantly reduced in the encrypted image and the correlation coefficients are approximately equal to zero.

c. Table 2, shows the processing time required for the encryption and decryption modules for sample test images. The timing analysis has been done on a personal computer with Intel i2duo 2.20 GHZ processor and 3GB RAM. The average encryption/decryption rate is 0.867 Mbps.

d. Table 3 shows the differential tests results and entropy. It is apparent from the obtained results that the proposed scheme is sensitive to small changes in the plain image. Moreover, the uncertainty increases after encryption as apparent from the values for entropy.

e. Table 4 shows a comparative study between the results obtained using the proposed scheme and other related schemes in literature. It provides comparable performance, while the key space is wider which rules out exhaustive search attacks.

6. Conclusions

In this paper, an improved image encryption scheme based on random interleaved pixel permutation, circular bit shifts and fractional Fourier transform is proposed. Unlike the scheme in [17], a clear choice for the random matrices employed in the encryption process is made based on fractals. Moreover, the use of bit shifts and pixels permutation broadens the key space and helps obtain encrypted images with more uniform histograms.

The experimental results show that the encrypted image has significantly low correlation coefficients among adjacent pixels in horizontal, vertical and diagonal directions. Moreover, the decryption using slightly different decryption key results in a totally different image compared to the original plain image. Furthermore, the encrypted image and the plain image are far from each as indicated by the relatively high values obtained for the MAE measure. Finally, the proposed encryption scheme results are sensitive to small changes in the plain image as indicated by the NPCR and UACI obtained in our tests.

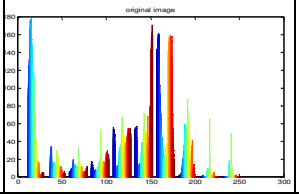
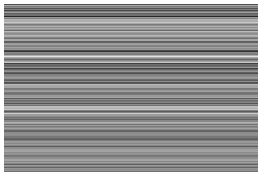
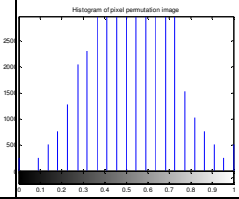
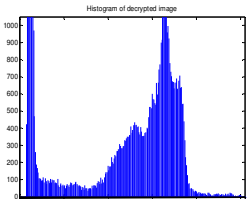
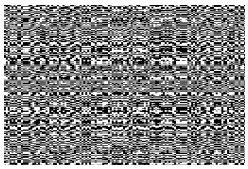
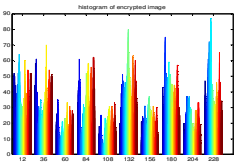
Original image	*Histogram of original image*	*Image after permutation*	*Histogram of image after permutation*	*Histogram of decrypted image*
Cameraman 				
Encrypted image	*Histogram of encrypted image*	*Decrypted image with the correct key*	*Decrypted image with the wrong key*	
				

Figure 2 Histogram analysis of Cameraman original and encrypted image.

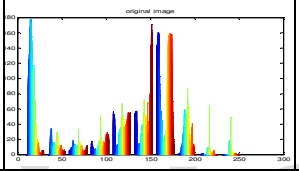
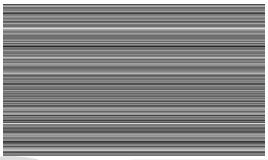
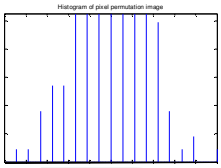
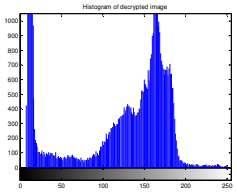
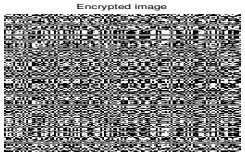
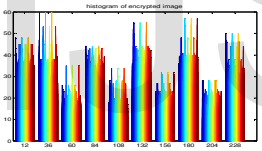
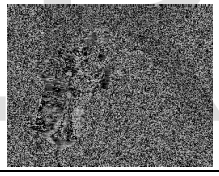
Original image	*Histogram of original image*	*Image after permutation*	*Histogram of image after permutation*	*Histogram of decrypted image*
Boat(4.2.05) 				
Encrypted image	*Histogram of encrypted image*	*Decrypted image with the correct key*	*Decrypted image with the wrong key*	
				

Figure 3 Histogram analysis of Boat original and encrypted image.

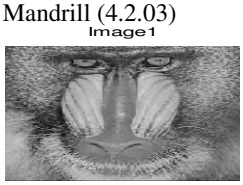
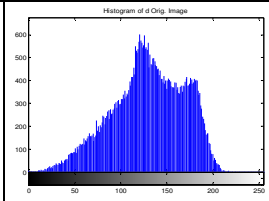
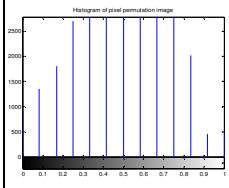
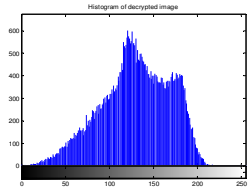
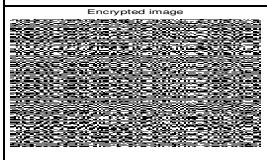
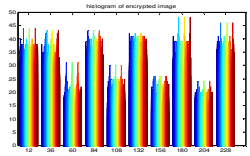
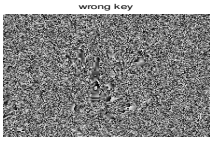
Original image	*Histogram of original image*	*Image after permutation*	*Histogram of image after permutation*	*Histogram of decrypted image*
Mandrill (4.2.03) 				
Encrypted image	*Histogram of encrypted image*	*Decrypted image with the correct key*	*Decrypted image with the wrong key*	
				

Figure 4 Histogram analysis of Mandrill original and encrypted image.

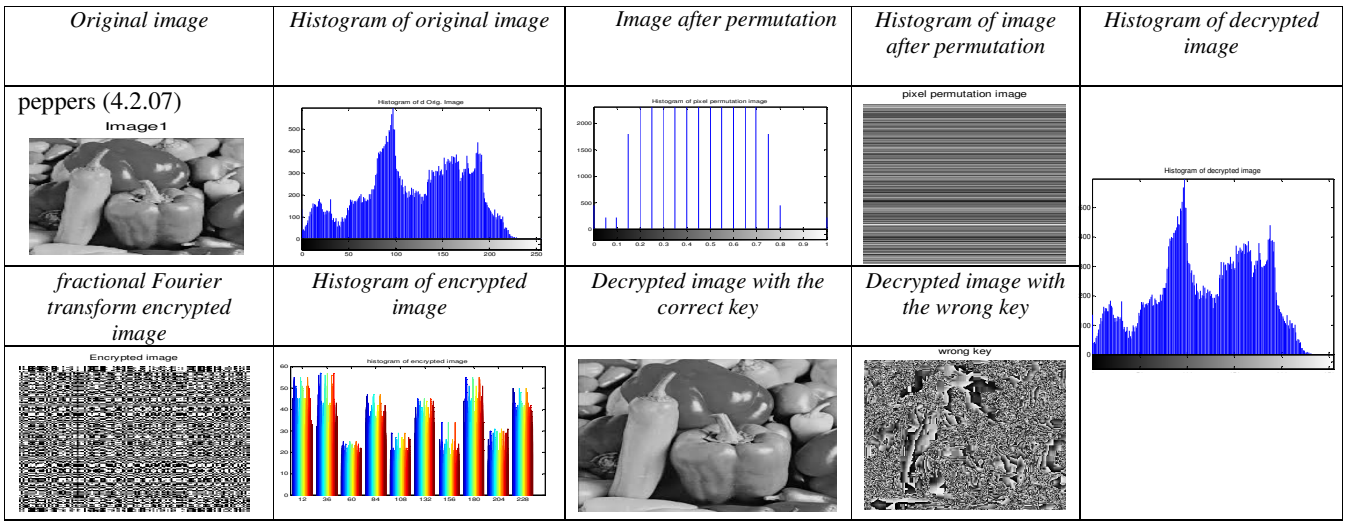


Figure 5 Histogram analysis of Peppers original and encrypted image

Table 1 Correlation coefficients values for some 1024 ×1024 original and encrypted test images.

Image	*Original image corr*			*Encrypted image corr*		
	Horz.	*Vert.*	*Diag.*	*Horz.*	*Vert.*	*Diag.*
Cameraman	0.9941	0.9901	0.9775	-0.0005	-0.0198	0.0024
Boat	0.9701	0.9655	0.9612	0.0072	0.0002	-0.0359
Pepper	0.9825	0.9815	0.9941	-0.0008	-0.0086	0.04277
Mandrill	0.9611	0.9509	0.9459	-0.0246	-0.0236	0.0145

Table 2 Time required for encryption and decryption for some sample images

Image	*Encryption time (sec)*	*Decryption time (sec)*
Cameraman (256 x 256)	0.07212	0.07222
Lena (512 x 512)	0.07322	0.07331
Boat (225 x 225)	0.07445	0.07541

Table 3 Differential tests results and entropy

Image	*MAE*	*NPCR%*	*UACI%*	*Entropy*	
				Orig.	*Enc.*
Cameraman	89.881	99.98	46.15	7.0097	7.8912
Boat	80.621	96.62	47.48	7.3124	7.8883
Pepper	88.22	99.51	43.01	7.0021	7.8882
Mandrill	57.498	98.62	33.44	7.7061	7.8884

Table 4 Comparison between the proposed scheme and other schemes in literature

Scheme	*Encrypted image corr*			*UACI%*	*Entropy*	*NPCR %*
	Horz.	*Vert.*	*Diag.*			
This work (cameraman)	-0.0005	-0.0198	0.0024	46.15	7.8912	99.98
[31]	0.0140	0.0092	0.0051	27.880	7.9982	99.670
[32]	–0.0049	0.0015	0.0021	33.4758	7.9993	99.6066
[33]	0.00089	0.00170	—	--	7.9899	--

REFERENCES

1. Wagh, Neha Balu. "Permutation based Digital Image Encryption and Decryption Methods." Digital Image Processing 8.10, 320-323, 2016.

2. Indrakanti, Sesha Pallavi, and P. S. Avadhani. "Permutation based image encryption technique." International Journal of Computer Applications (0975–8887) Volume, 2011.

3. Mahmood Al-Khassaweneh and Shefa Tawalbeh, "A value transformation and random permutation based colored image encryption technique", International Journal of Information and Computer Security, Vol.5, No-4, pp.290-300, 2013.

4. A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer engineering 1:2, 2006.

5. Li, C.-G., Han, Z.-Z., & Zhang, H.-R. Image encryption techniques: A survey. *Journal of Computer Research and Development, 39*(10), 1317–1324, 2002.

6. Yoon, J. W., & Kim, H. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 15(12), 3998-4006, 2010.

7. Ismail, I. A., Amin, M., & Diab, HA digital image encryption algorithm based a composition of two chaotic logistic maps. IJ Network Security, 11(1), 1-10, 2010.

8. N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.

9. A. Jolfaei and A. Mirghadri, "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1," Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10), Sanya, China, 2010.

10. N.K. Pareek, Vinod Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing , Vol. 24, pp. 926-934, 2006.

11. Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm", International Journal of Research and Review in Computer Science, Vol. 2, No. 2, pp. 275-279, 2011.

12. G.A. Sathishkumar and K. Bhoopathy Bagan, "A novel image encryption algorithm using pixel shuffling Base 64 encoding based chaotic block cipher", WSEAS Transactions on computers, Vol. 10, No. 6, pp. 169-178, 2011.

13. Rao, K. Ramamohan, and Ping Yip. Discrete cosine transform: algorithms, advantages, applications. Academic press, 2014.

14. Lima, Juliano B., E. A. O. Lima, and F. Madeiro. "Image encryption based on the finite field cosine transforms." Signal Processing: Image Communication28.10, 1537-1547, 2013.

15. J. B. Lima and R. M. C. de Souza, "Histogram uniformization for digital image encryption," in Proceedings of the 25th Conference on Graphics, Patterns and Images (SIBGRAPI '12 IEEE, Ouro Preto, Brazil,), pp. 55–62,August 2012.

16. J. B. Lima, E. S. da Silva, and R. M. de Souza, "A finite field cosine transform-based image processing scheme for color image encryption," in Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP '15), pp. 1071–1075, Orlando, Fla, USA, December 2015.

17. L. B. Almeida, "The fractional Fourier transform and time-frequency representations," IEEE Trans. Signal Process., vol. 42, no. 11, pp. 3084–3091, Nov. 1994.

18. Bultheel A, Martínez H. Computation of the Fractional Fourier Transform. Appl. And Comput. Harmonic Analysis. vol. 16, 182-202, 2004.

19. Ozaktas, Haldun M., and M. Alper Kutay. "The fractional Fourier transform." Control Conference (ECC), 2001 European. IEEE, 2001.

20. C. K. Huang, H. H. Nien, Multi chaotic systems based pixel shuffle for image encryption [J], Optics Communications, 282(11): 2123-2127, 2009.

21. Candan C, 1998, dFRT: The Discrete Fractional Fourier Transform, A Matlab Program, http://www.ee.bilkent.edu.tr/~haldun/dFRT.m

22. Sesha Pallavi Indrakanti and P.S.Avadhani, Permutation based Image Encryption Technique, International Journal

of Computer Applications (0975 – 8887) Volume 28 – No.8, August 2011.

23. G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solutions and Fractals, vol. 21, no. 3, pp. 749–761, 2004.

24. C. K. Huang, H. H. Nien. Multi-chaotic systems based pixel shuffle for image encryption [J], Optics Communications, 282(11): 2123-2127, 2009.

25. Matsumoto, Makoto, and Takuji Nishimura. "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator." ACM Transactions on Modeling and Computer Simulation (TOMACS) 8.1 3-30(1998).

26. Falconer, Kenneth. Fractal Geometry: Mathematical foundations and applications. John Wiley & Sons, 2004.

27. Chaotic Fractals Generator http://www.chaospro.de/

28. G. A. Sathishkumar, Srinivas Ramachandran and K. Bhoopathy Bagan.— Image Encryption Using Random Pixel Permutation by Chaotic Mapping, IEEE Symposium on Computers and Informatics, 2012.

29. Yue Wu, Joseph P. Noonan, and Sos Agaian. NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011.

30. The USC-SIPI Image Database, “University of Southern California, signal and image processing institute,” http://sipi.usc.edu/database/

31. Vinod Patidar, N.K. Pareek, G. Purohit and K.K. Sud, “A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption”, Optics Communications, Vol. 284, pp. 4331-4339, 2011.

32. Ozaktas, Haldun M., and M. Alper Kutay. "The fractional Fourier transforms." Control Conference (ECC), 2001 European. IEEE, 2001.

33. Xu, Shu-Jiang, et al. "An improved chaotic cryptosystem based on circular bit shift and XOR operations." Physics Letters A 376.10, 1003-1010, 2012.