Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 10, No. 01, pp. 81-91, March 2017

IMAGE ENCRYPTION BASED ON FRACTIONAL ORDER LORENZ SYSTEM AND WAVELET TRANSFORM

Abbas Salman Hameed
Lecturer, Electronic Engineering Department, College of Engineering, University of Diyala
E-mail: abbasfuture@yahoo.com

(Received: 24/3/2016; Accepted: 16/5/2016)

ABSTRACT: - To securely transmit data in open networks, encryption must be used. In this paper, cryptography technique of images is presented with chaos and Discrete Wavelet Transform (DWT). Fractional order Lorenz system that provides an expanded in key space is used to encrypt image. All properties of randomness and nonlinearity which are owned by this chaotic system are guarantee a highly secure and robustness for Encryption process. As well as DWT offers additional space and security by using wavelet domain to shuffled image pixels after passing in DWT filters and sampling. The combination between Lorenz system and DWT have been taken to make the image more secure and thus make very hard to get back the original image without having its correct key and procedure which were used to encrypt. The results show a large sensitivity to a small change in the secret key or DWT family type. Therefore, high complicated image security is offered using this system.

Keywords: *Cryptography, Fractional Order chaotic system, Lorenz flow.*

1- INTRODUCTION

To meet expanded desire for secure image transmission through wireless networks and over the Internet, Image encryption schemes have been increasingly studied. Cryptography hides the contents of a secret message from an unauthorized people by scramble the structure of a message in such a way as to make it meaningless and unintelligible manner [1,2,3].

DWT is suggestions here to convert image to wavelet domain then encrypted by randomness sequences to produce highly secure cryptography scheme. To perform this encryption process, nonlinear dynamic systems as chaos is used. It is characterized by extremely sensitive to initial conditions and control parameters and mathematically is defined as randomness governed by simple deterministic rules [4]. Lorenz with high dimensional chaotic system and fractional order will give a more system variables, more structure complexity, and parameters. Then large key space for cryptosystem will be get by use integer orders and very greatest by use fractional order, and the time sequence for system variables will be more stray and unpredictable than using the low dimensional chaotic system [5,3].

This paper demonstrates encryption of image using fractional order chaotic system to increase the security level of generated keys in Wavelet domain. The paper is organized as follows; section 2 describes main function of DWT and two-dimensional DWT components. In section 3, the Fraction Order Lorenz system, chaos permutation and the chaotic Mask Key generation will be illustrated. The proposed system model of the encrypted image is presented in section 4. In section 5, the simulation results that are computed by Matlab 2015a are shown. Finally, conclusions are clarified in section 6.

2. WAVELET TRANSFORM:

Variations in time-frequency resolutions will be provide by wavelet transform due to the variation in it basis function in terms of frequency and scale. The basis function of wavelet divides the data into different frequency components and chooses the component that relates to its scale. In the DWT, digital filtering techniques are used to obtain a space-scale depiction of the digital signal. The signal to be analyzed is passed through successive low pass and high pass filters with various cutoff frequencies at different scales. (1,6).

A two-dimensional DWT, can be accomplished by performing two separate one-dimensional DWT, is used here to decompose an image to wavelet domain. First, the image is filtered along the x-dimension using low pass (H) and high pass (G) analysis filters and decimated by 2. Then, it is followed by filtering the sub-image along the y-dimension and decimated by 2. Finally, the image has been split into four bands denoted by the approximate (ca), horizontal (cd_h), vertical (cd_v), and diagonal (cd_d), as in Fig.1.(7,8).

For Image reconstruction inverse method of the decomposition is followed by using Inverse Discrete Wavelet Transform (IDWT).

3. CHAOS SYSTEM:

One of the possible behaviors associated with evolution of a nonlinear physical system is chaos, and it's occurring for specific values of system parameters. chaotic systems have many substantial properties, such as the sensitivity to its parameters, no periodicity and topological transitivity, pseudorandom property, etc. Most chaos properties meet some requirements such as diffusion and mixing in the sense of cryptography (3).

3.1 FRACTION ORDER LORENZ FLOW:

The mathematical description of the fractional-order Lorenz system is expressed as (5):

$$\begin{cases} D^{\alpha 1}x = \sigma(y - x) \\ D^{\alpha 2}y = -xz + \rho x - y \\ D^{\alpha 3}z = xy - \beta z \end{cases} \tag{1}$$

where (σ, ρ, β) are system parameters ,($\alpha 1$, $\alpha 2$ and $\alpha 3$) are fractional orders of the equation and ($\alpha 1$, $\alpha 2$, $\alpha 3 > 0$) .

Fractional Backward Difference Methods (9) is used to solve fractional-order equations and its result can be shown as:

$$\begin{cases} x_m = h^{\alpha 1} * [\sigma * (y_{m-1} - x_{m-1})] - \sum_{k=1}^{m} w_k x(m - k_h) \\ y_m = h^{\alpha 2} * [-z_{m-1} * x_{m-1} + \rho * x_{m-1} - y_{m-1}] - \sum_{k=1}^{m} w_k y(m - k_h) \\ z_m = h^{\alpha 3} * [x_{m-1} * y_{m-1} - \beta * z_{m-1}] - \sum_{k=1}^{m} w_k z(m - k_h) \end{cases} \tag{2}$$

3.2 SHUFFLING USING CHAOTIC FLOW SEQUENCES:

After compute random sequences (x, y, and z) from fractional-order Lorenz system, as in Eq.2, the proposed shuffling method is done. This method assumes that there is a known chaotic flow with its initial condition and parameters negotiated between the encoder and the decoder. The design procedure to shuffling matrix elements that is provide a high dispersion and low correlation will be performed by using a chaotic sequence that is generated with length equal to N. For example, with *x* chaotic Lorenz sequence has eight elements (N=8) as shown in Fig.2, chaotic vector is sorting in descending order to generate new order indexes. So, the indexes are shuffling as results of sorting process, therefore new indexes are taken as chaotic permutation indexes.

3.3 MASK CODES USING CHAOTIC FLOW SEQUENCES:

After compute the sequences from fractional-order Lorenz system, magnification and modulo transformation will be perform on *x* and *z* chaotic sequences as in Eq. 3, as (10) :

$$M_L(n) = \mathrm{mod}(\mathrm{floor}(M_L(n) \times 10^{15}), 2^N) \tag{3}$$

where M_L is (x, z) sequences for Lorenz. N is maximum number of bits required to quantize M_L into an integer sequence.

As example, assume x and z are five element vectors. Each vector will be applied with Eq.3, the final process is performed by XORed z column by x row to generate the mask code chaotic matrix as shown in Fig. 3.

4. PROPOSED SYSTEM MODEL:

The proposed system is shown in Fig.4. First, four coefficient matrices; ca, cd_h, cd_v, and cd_d matrices, will be produced using single-level DWT on the original image. Each matrix is split to four sub-matrixes with equal size, then its reordered to generate a new size matrix goes to shuffle using fractional order Lorenz $\boldsymbol{x}$ and $\boldsymbol{y}$ sequences. After that, IDWT will be used and the produced matrix is XORed with mask code matrix generated using chaotic $\boldsymbol{x}$ and $\boldsymbol{z}$ sequences as a final step to produce encrypted image. Wavelet Transform used here to separate the image pixel to low and high frequency coefficient as primary shuffled and coded by the resolution / scale, which is produced by filtering operations, and up / down sampling operations. A high level of security for image encryption is produced by using combined of wavelet and chaotic sequences as a cryptography system.

In the following, the encryption of the images is illustrated:

Input: Target Image to be encrypted and the initial values and orders of Lorenz.

Output: Encrypted Image

Step1: Read the image with size (M×M) and generate chaotic sequences with length (M).

Step2: Perform a DWT on the image and generate four matrix ca , cd_h , cd_v and cd_d each with size ($\frac{M}{2}\times\frac{M}{2}$).

Step3: Split each matrix to four sub-matrix (taken ca as example in this procedure, (ca1, ca2, ca3, ca4) each sub-matrix with size ($\frac{M}{4}\times\frac{M}{4}$).

- Rearrange the split matrix as [ca1**,** ca2 **;** ca3**,** ca4] matrix with size ($\frac{M}{4}$ ×M).
- Shuffled each row of matrix depending on x chaotic sequence to generate new ca matrixes as [nca1**,** nca2 **;** nca3**,** nca4].
- Rearrange the shuffled matrix with size (M×$\frac{M}{4}$) as [nca1**;** nca2 **;** nca3**;** nca4].
- Now shuffled each column depending on y chaotic sequence.
- Return shuffled ca matrix back to first matrix size ($\frac{M}{2}\times\frac{M}{2}$).
- All other matrixes, cd_h , cd_v and cd_d, are shuffling as ca matrix.

Step 4: Rearrange all shuffled matrixes as one matrix with size (M×M).

Step 5: Perform IDWT on the matrix.

Step 6: Coded: XORed chaotic mask matrix with generated matrix from step 5 to produce the encrypted image.

To decrypt the image, all steps used in encryption will be performed with inverse order.

5. SIMULATION RESULTS:

The fraction-order Lorenz system used to generate chaotic permutation index and secure chaotic Mask have these qualifications:- Fraction order: $\alpha1=0.96$, $\alpha2=0.97$, $\alpha3=1.1$, initial conditions: $x(0)=0.11$, $y(0)= -0.12$, $z(0)=20$, control parameters: $\sigma=10$, $\beta=8/3$, $\rho=28$, and integer step-size: h=0.05.

Fig. 5 and Fig. 6 show original images of Peppers and Parrot with size (512×512) and the processing steps that are done as in section 4 to encrypted and decrypted image by using chaotic flow and DWT-Haar family.

To indicate the high quality for the proposed encryption method, correlation of adjacent pixels will be used by take 2000 pairs of random pixel organized in horizontal, vertical or diagonal directions. In each direction, correlation coefficient calculated as in [(10)]. Table 1 show correlation coefficients for original and cipher Peppers image. Outcomes of correlation coefficients computed in (10) and (11) references also mention here to illustrate the advantage of proposed method.

5.1 SENSITIVITY TO CHAOTIC PARAMETERS:

Effect of change one parameter of Lorenz system on the chaotic response will be tested by taken two identical chaotic systems A and B with the same parameters except a very small change in one of them, chosen to be nearly identical (10^{-10} is used). As example, Fig. 7-a depicts, the time series of sequence x_A and x_B for Lorenz with same parameters except small change in α2 by 10^{-10} used such as α2=0.97 for A system, α2=0.9700000001 for B system. Fig. 7-b shows, the time series of sequence x_A and x_B at small change in x(0) parameter by 10^{-10} as x(0) =0.11 for A system, and x(0) =0.1100000001 for B system.

Even though the two sequences started from identical parameters but they diverge from each other. So, the different time response which is produced from Lorenz system by tiny change in any parameter is lead to different chaotic shuffling and mask key.

Fig.8 and Fig.9 show the original and decrypted Peppers images with its histogram when used same chaos parameters and DWT family type in encryption and decryption process, and Fig.10 – Fig.12 show decrypted images produced from a tiny change in one of chaotic Lorenz parameters that was used in decryption side with respect to chaotic Lorenz parameters used in encryption side.

To illustrate similarity between decrypted image and original image corresponding to a tiny amount of 10^{-10} change in one parameter at a time for chaotic key or change DWT type at decryption side and keeping all other parameters unchanged, Normalized Correlation (NC) factor is computed according to Eq. 4 (12):

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\bar{C})(D(i,j)-\bar{D})}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\bar{C})^{2}\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(D(i,j)-D)^{2}\right)}} \qquad (4)$$

where M, N : No. of rows and columns of the images respectively, C(i,j): is the original image, D(i,j): is the decrypted image, $\bar{C}$:the mean of C(i,j) , $\bar{D}$:the mean of D(i,j).

Also, Peak signal to Noise Ratio (PSNR), the ratio between signal variance and reconstruction error variance, is presented here as another comparison parameter. PSNR is usually expressed in decibel scale as in Eq.5 (12):

$$PSNR = 10\log_{10}\frac{(L-1)^{2}}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(D(i,j)-C(i,j)\right)^{2}} \qquad (5)$$

where N and M are height and width of images respectively, L: is the number of the gray scale levels in the images, C(i,j): is the original image. D(i,j): is the decrypted image. In this work, PSNR=8.2636 dB for encrypted image.

Table 2, shows NC=1 for decryption image, same of original, with used same chaos parameters and DWT family type that are used in encryption process. Also, it shows the high sensitivity for a tiny change in any parameters of chaotic system or DWT family that is illustrating with low NC and small PSNR of decrypted image.

5.2 KEY SPACE AND SYSTEM SECURITY:

The total number of different keys that are used in the encryption is called Key space size. The chaotic key used in this paper is highly sensitive to fraction- order for Lorenz system (α1, α2, α3), Lorenz parameters (σ, ρ, β) and also to initial values of the system (x(0), y(0), z(0)). All parameters and initial conditions constitute the secret key of encryption system. Also, the DWT family type is providing an addition system security space. Hence, the space of the system, in general, will be a high dimensional space. To resist the exhaustive attack, large secret key parameters space is very important.

6. CONCLUSIONS

A high secure and efficient cryptography method of image using fraction order Lorenz flow and DWT is presented in this paper. Complicated chaotic shuffling and coded method with huge key space is very important to frustrate malicious attacks from unauthorized parties. With using of chaotic shuffling in wavelet domain and chaotic coding, the encrypted image has very low normalized correlation coefficients and PSNR = 8.2636 dB. These values is referring to an efficient encryption method and identify decrypted image when use same chaos system parameters and DWT family type. Also, weak PSNR and very low NC factor is getting at decryption side if a tiny change in chaos system parameters or change DWT family type.

REFERENCES

1. Nasrin M. Makbol, Bee Ee Khoo , Taha H. Rassem “Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics”, Proceedings on IET Journals & Magazines (Image Processing, IET), Vol. 10, No. 1 pp. 34–52, January 2016.
2. JiaYan Wang, Geng Chen, "Design of a chaos-based digitlal image encryption algorithm in time domain", Proceedings on IEEE, International Conference on Computational Intelligence and Communication Technology (CICT 2015), pp. 26–29, April 2015.
3. K. Sakthidasan, and B. V. Santhosh, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, vol. 1, No. 2, pp. 137 – 141, June 2011.
4. S. H. Strogatz, “Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering”, Westviewpress-Preseus Books Publishing, LLC, 2014.
5. R. Nicholas, “Introduction to Lorenz's System of Equations”, Math 6100, December 2003.
6. Satya P Singh, Shabana Urooj, " Wavelet Packets based Spectral Estimation of Textured images ", Proceedings on IEEE, International Conference on Computational Intelligence and Communication Technology (CICT 2015), pp. 651–654, 2015.
7. W. Shi, C. Zhu, Y. Tian, and J. Nichol, “Wavelet-based image fusion and quality assessment", International Journal of Applied Earth Observation and Geoinformation, vol. 6, pp. 241 - 251, 2005.
8. A. Cohen and J. Kovacevic, “Wavelets: the mathematical background” Proceedings of the IEEE, vol. 84, no. 4, pp. 514–522, 1996.
9. K. Sun, and X. Wang, "Bifurcations and Chaos in Fractional Order Simplified Lorenz System", International Journal of Bifurcation and chaos, vol. 20, No. 4, pp. 1209–1219, 2010.
10. M. Ahmad and O. Farooq, “A Multi-level Blocks Scrambling based Chaotic Image Cipher”, Springer, Third International Conference, IC3, vol. 94, pp. 171–182, August 2010.
11. O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, “A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity ", Springer- An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems, Volume 82, No.1, pp 107-117, May 2015.
12. V. Sreejith, K. Srijith, R. C. Roy, "Robust Blind Digital Watermarking in Contourlet Domain ", International Journal of Computer Applications, Volume 58, No.12, November 2012.

Table 1: correlation coefficients for Peppers image

Coefficient		horizontal	vertical	diagonal
Original image		0.9750	0.9813	0.9618
Cipher image	Proposed method	0.00067	0.000023	0.00059
	Method in (10)	0.00118	0.00191	0.00031
	Method in (11)	0.00078	0.00076	0.0048

Table 2: summarized NC and PSNR between of the original and decrypted image with change in one system parameter at decryption process

Parameter changed		NC	PSNR
changed by 10^{-10}	α1	-0.0027	8.2660
	α2	0.00098	8.2751
	α3	0.00081	8.2740
	x (0)	0.0020	8.2776
	y(0)	-0.000014	8.2713
	z(0)	0.00024	8.2779
	σ	0.00083	8.2728
	ρ	-0.0013	8.2617
	β	-0.0046	8.2457
DWT family	db4	-0.0191	8.8506
	db10	-0.0149	9.0260
	coif4	-0.0133	8.9628

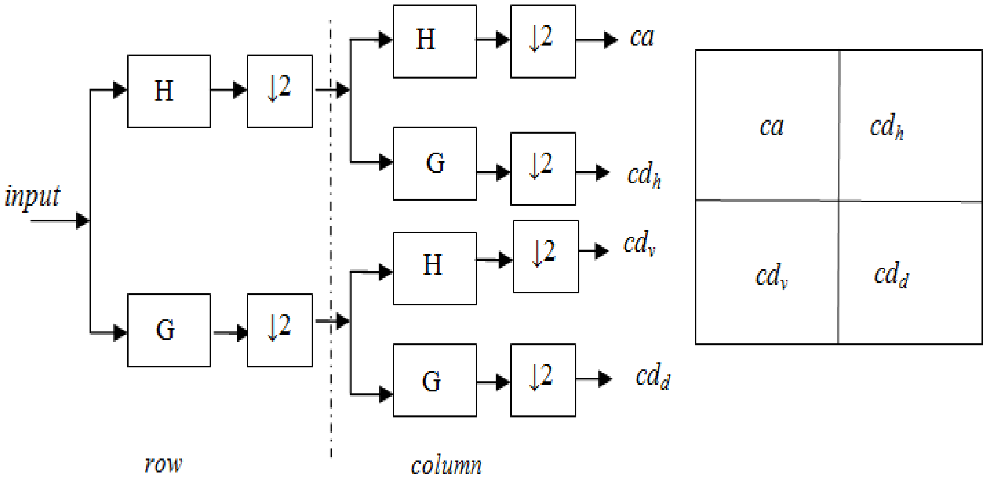
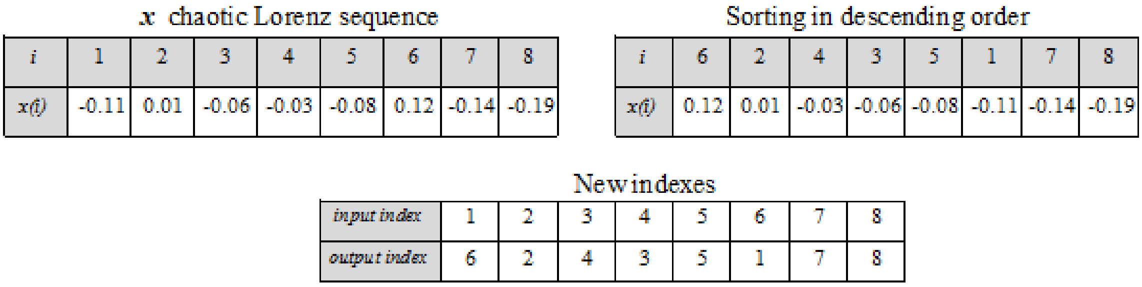


Fig.1: Two dimensional DWT decomposition.



x chaotic Lorenz sequence

i	1	2	3	4	5	6	7	8
x(i)	-0.11	0.01	-0.06	-0.03	-0.08	0.12	-0.14	-0.19

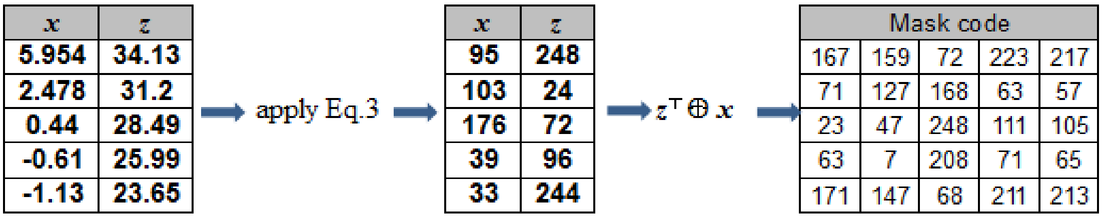
Sorting in descending order

i	6	2	4	3	5	1	7	8
x(i)	0.12	0.01	-0.03	-0.06	-0.08	-0.11	-0.14	-0.19

New indexes

input index	1	2	3	4	5	6	7	8
output index	6	2	4	3	5	1	7	8

Fig. 2: Proposed chaotic permutation pixels steps



x	z
5.954	34.13
2.478	31.2
0.44	28.49
-0.61	25.99
-1.13	23.65

apply Eq.3

x	z
95	248
103	24
176	72
39	96
33	244

$z^T \oplus x$

Mask code				
167	159	72	223	217
71	127	168	63	57
23	47	248	111	105
63	7	208	71	65
171	147	68	211	213

Fig. 3: Proposed mask code generation steps

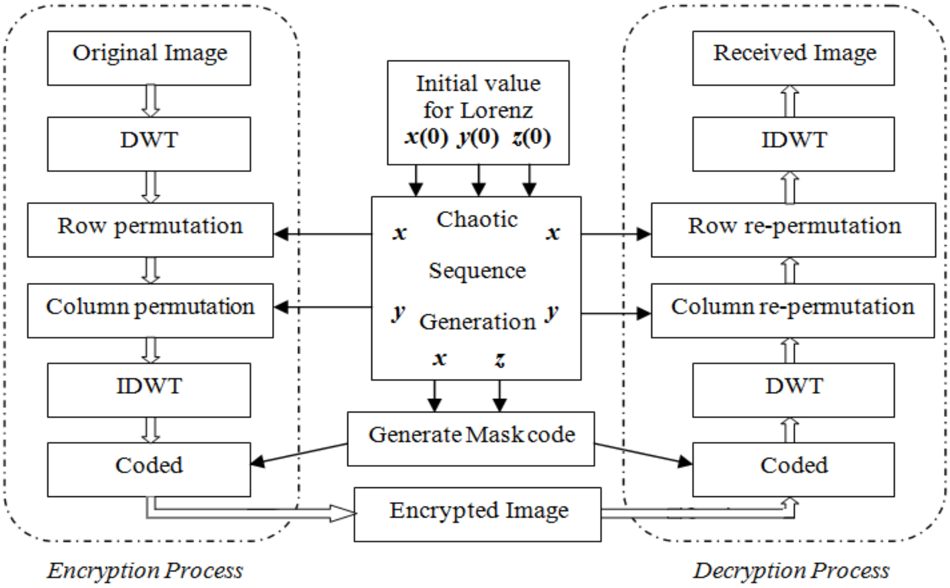
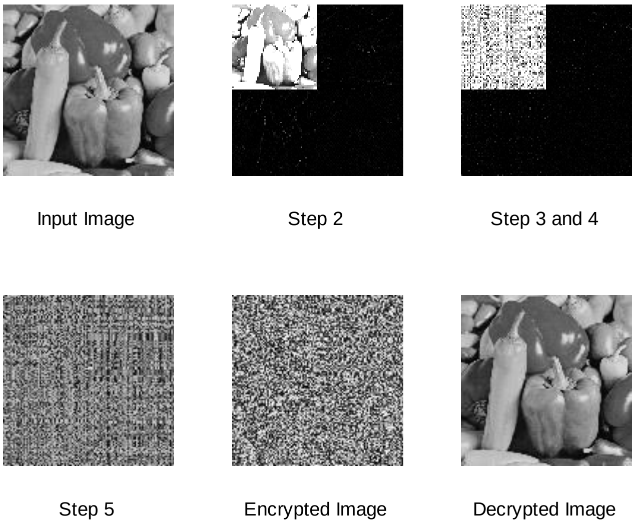


Fig. 4: Block diagram of proposed encryption and decryption image



Input Image

Step 2

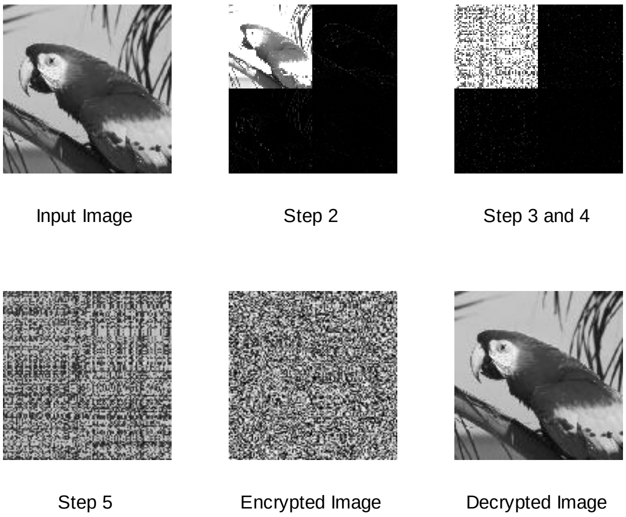
Step 3 and 4

Step 5

Encrypted Image

Decrypted Image

Fig. 5: Peppers image with its encrypted and decrypted steps



Input Image

Step 2

Step 3 and 4

Step 5

Encrypted Image

Decrypted Image

Fig. 6: Parrot image with its encrypted and decrypted steps

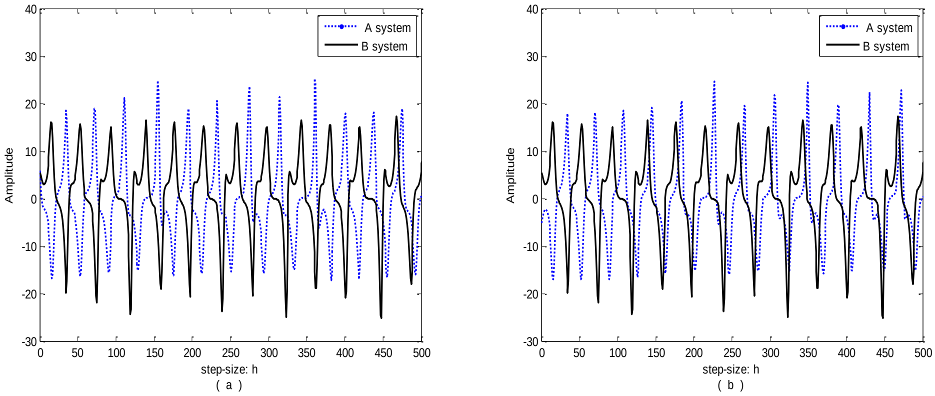
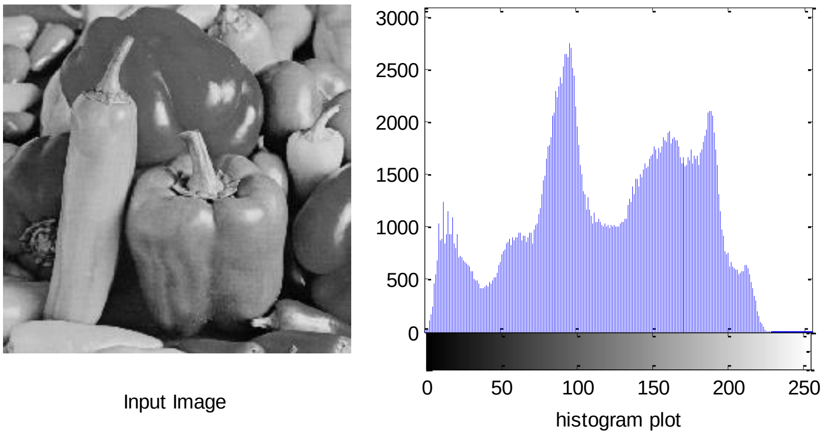


Fig. 7: Time series of variables *x* for Lorenz system, a) different in fraction order α2, b) different in initial condition x(0).



Input Image

histogram plot

Fig. 8: Input image with it histogram plot

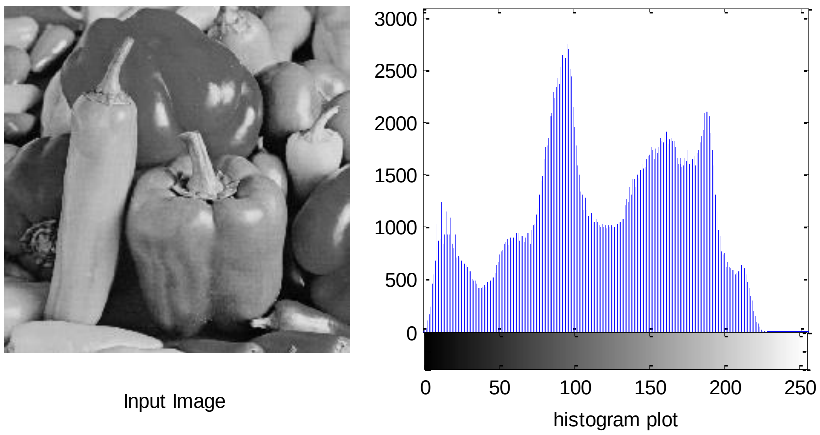


Fig. 9: Decrypted image with it histogram plot

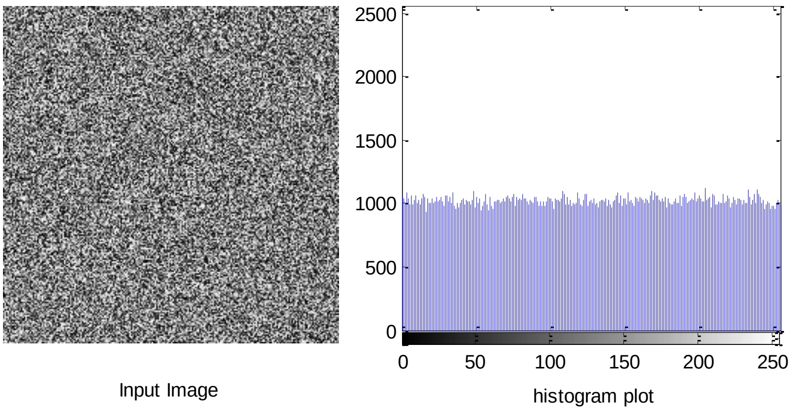


Fig. 10: Decrypted Image with histogram plot with 10^{-10} change in x(0)

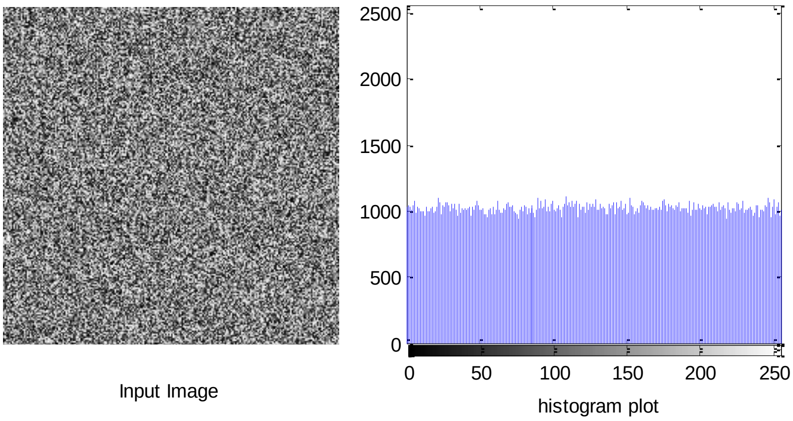


Fig. 11: Decrypted Image with histogram plot with 10^{-10} change in $\alpha 1$

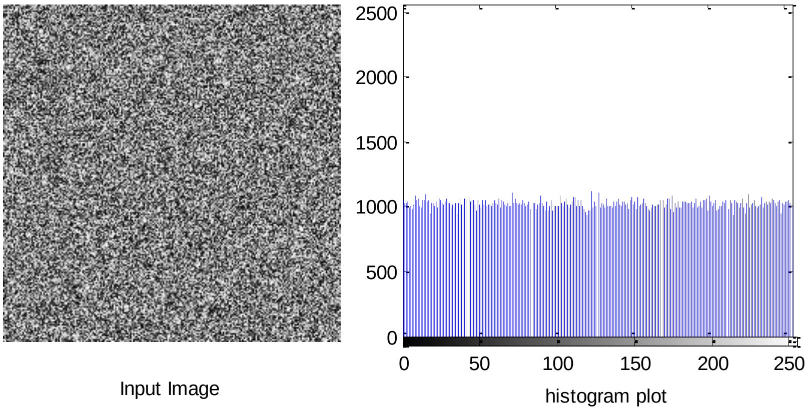


Fig. 12: Decrypted Image with histogram plot with 10^{-10} change in σ

تشفير الصورة المعتمد على نظام لورينز ذو الرتب الكسرية وتحويل المويجات

عباس سلمان حميد

جامعة ديالى / كلية الهندسة / ديالى، العراق

الخلاصة:

لنقل آمن للبيانات في الشبكات المفتوحة يتوجب وبشكل ضروري استخدام تقنية التشفير لذلك. في هذا البحث، يتم تقديم تقنية تشفير الصور مع النظام الفوضوي و تحويل المويجات (DWT). ويتم استخدام نظام لورينز الفوضوي ذو الرتب الكسرية والذي يوفر مساحة كبيرة جدا في الشفرة المستخدمة لتشفير الصورة. جميع الخصائص العشوائية و اللاخطية التي يملكها هذا النظام الفوضوي هي ضمان لأمن ومتانة عملية التشفير. وكذلك استخدام تحويل المويجات يوسع مساحة الشفرة ويزيد من امان عملية التشفير من خلال تحليل الصورة في نطاق الموجات والذي يقوم بتعديل قيم اجزاء الصورة بعد امرارها بالمرشحات المويجية واعادة تعينها.

ان الجمع بين نظام لورينز و تحويل المويجات جعل الصورة أكثر أمنا، حيث انه من الصعب جدا استرجاع الصورة الأصلية دون معرفة مفتاح التشفير الصحيح والإجراءات التي استخدمت لتشفير الصورة. اظهرت النتائج وجود حساسية كبيرة لتغيير طفيف في المفتاح أو نوع تحويل المويجات. وبذلك، تم تقديم نظام تشفير صور مؤمن وعالي التعقيد في هذا البحث.