opción

Revista de Antropología, Ciencias de la Comunicación y de la Información, Filosofía, Lingüística y Semiótica, Problemas del Desarrollo, la Ciencia y la Tecnología

Año 35, 2019, Especial N° 20
Revista de Ciencias Humanas y Sociales
ISSN 1012-1587/ ISSNe: 2477-9385
Depósito Legal pp 198402ZU45

Universidad del Zulia
Facultad Experimental de Ciencias
Departamento de Ciencias Humanas
Maracaibo - Venezuela

Opcion, Año 35, Especial Nº 20 (2019):*2899-2921*
ISSN 1012-1587/ISSNe: 2477-9385

Image Encryption Method Based on Image Dimension Transformation Using Chaotic Flow systems

Atheer J. Mansoor[1], Hikmat N. Abdullah[2] , Hadi T. Zeboon[3]

[1]Al-Turath University Collage, Baghdad , Iraq
dratheer.j.mansoor@turath.edu.iq
[2]Al-Nahrain University, College of Information Engineering, Baghdad, Iraq, dr.h.abdullah@ieee.org
[3]University of Technology, Baghdad, Iraq
Dr.hadi.zeboon@gmail.com

Abstract
Image encryption today is divided into changing image pixels' value or changing image pixels' coordinates. In this paper, an image encryption system based on changing both pixels' value and position using one chaotic flow systems is proposed. At first, image dimension is changed form an M*N matrix into a vector of 1*(M*N), then Implement the random number generated from chaos system to produce the final encrypted image. The system has been implemented on equal and non-equal dimension images and tested by using testing techniques:- correlation coefficient, DSF, ADC, PSNR, EQ ,ARE, MD, ID , measurement based on the value and position changing and entropy. Then the result is compared with the traditional scheme which uses ACM for scrambling then any chaotic system for changing pixel's value. The simulation results show that, keeping almost the same encryption results quality but with decreasing the required time for encryption and decryption.

Keywords: security, image encryption, image scrambling, chaotic sequences, pixels coordinate.

Método de cifrado de imagen basado en la transformación de la dimensión de imagen utilizando sistemas de flujo caótico

Resumen
El cifrado de imágenes hoy se divide en cambiar el valor de los píxeles de la imagen o cambiar las coordenadas de los píxeles de la imagen. En este artículo, se propone un sistema de encriptación de imágenes basado en cambiar el valor y la posición de ambos píxeles utilizando un sistema de flujo caótico. Al principio, la dimensión de la imagen cambia de una matriz M * N a un vector de 1 * (M * N), luego implemente el número aleatorio generado por el sistema de caos para producir la imagen cifrada final. El sistema se implementó en imágenes de dimensiones iguales y no iguales y se probó utilizando técnicas de prueba: - coeficiente de correlación, DSF, ADC, PSNR, EQ, ARE, MD, ID, medición basada en el valor y cambio de posición y entropía. Luego, el resultado se compara con el esquema tradicional que usa ACM para codificar y luego cualquier sistema caótico para cambiar el valor del píxel. Los resultados de la simulación muestran que, manteniendo casi la misma calidad de resultados de cifrado, pero disminuyendo el tiempo requerido para el cifrado y descifrado.

Palabras clave: seguridad, cifrado de imágenes, codificación de imágenes, secuencias caóticas, coordenadas de píxeles.

1 Introduction

Image encryption is a method for protecting the information in a digital image. There are two ways for image encryption: - the first one is changing image pixels' value and the other is changing image pixels' position (scrambling). The Highest degree of image encryption is by changing both the pixels' values and coordinates. The resulting image is an encrypted image that has the same size of the original image with different histogram and redistributed of pixels in the original image (Jing-yu, Efficient Color Image Encryption and Decryption Algorithm, 2013). Chaotic systems are used to produce the random numbers which are used for the encryption process because of its characteristics of random behavior and aperiodicity. (Mao, Cao, & Liu) (Gao & Chen, 2008)) (Prasad & Sudha, 2011).

Many algorithms are proposed for even changing pixels' value (Zhu

Liehuang, 2006) (Gao & Chen, 2008)) (H.H. Nien, 2005), or changing pixels position. Some proposed algorithms are proposed by using ACM for changing pixels' coordinate then using chaotic system (flow or map) to change the pixels' value. (Mao, Cao, & Liu) (Gao & Chen, 2008)) (Prasad & Sudha, 2011) (Zhu Liehuang, 2006).

In this paper, a new encryption algorithm for image encryption based on changing image pixels' value and position using chaotic flow sequences is proposed. At first, the proposed system is used to change the M*N image to a vector of 1*(M*N), the user to select one of five chaos flow systems which are: Lorenz, Rössler, Chua, Nien and CL for the encryption process. The main contributions of the proposed work are as follows: the use of the chaotic flows increases the immunity against the intruders as compared with the chaotic Maps because it is consists of three bands or higher. Also, the proposed system is applicable to equal and non-equal dimensional images. Changing pixels' value and position id done in one iteration and using one chaotic system for the whole process.

The rest of the paper is organized as follows: in section 2, the chaotic systems that are used in the proposed system are described in details. In section 3, the quality measurements of encryption that are used to evaluate the performance of the proposed system are reviewed. The proposed algorithm and the simulation results are presented section 4, while the conclusions drown throughout the work are given in section 5.

2. Description of Chaotic Systems

In this section, the mathematical models of the chaotic systems used are reviewed. First, the classical Arnold map used for image square images .Then, the chaotic flow sequences used in the proposed scheme are described.

A. Arnold cat map

"Arnold cat map" is a discrete system used in image processing for scrambling by changing the pixels positions. It is applied on images with size of N*N and given by (Willsey, Cuomoy, & Oppenheim, 2010)

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} mod(N)\,, \tag{1}$$

Where X_{n+1}, Y_{n+1} are pixel positions after scrambling, Xn, Ynare pixel positions before scrambling, a and b are positive integers. The determinant of

the matrix in equation (1) must be equal to 1. To achieve high scrambling complexity, the scrambling process must be repeated many times until the original pixels are displaced enough from their original positions.Table.1 shows the number of iterations (m) required to restore image of size N*N (Merah, Ali-Pacha, Said, & Mamat, 2013,)

Table 1. Number of iterations (m) required to restore Image of size N*N using Arnold cat map (Tang & Zhang, 2011)

N	60	100	120	128	256	480	512
m	60	150	60	96	192	240	384

B. Lorenz system

Lorenz system is considered the first chaotic system had been discovered by Edward N. Lorenz in 1963 for predicting weather, later it is used for many other applications one of them is encryption. Lorenz system is an example of a non-linear dynamic system which is a3-dimensional dynamical system. The equations of the Lorenz system are (H.H. Nien, 2005)

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= r * x - y - x * z \\ \dot{z} &= x * y - \beta * z , \end{aligned} \tag{2}$$

where σ, r and β are the parameters of the system (Gaspard, 2005).The values of σ, r and β must be greater than 0, σ > β+1, and

$$r > rc = \frac{\sigma(\sigma+\beta+3)}{\sigma-\beta-1} , \tag{3}$$

C. Rössler system

Otto Rössler presented 3-dimensional dynamical chaotic system with a series of prototype systems of ordinary differential equations in 1970. The equations of this system are (Jing-yu, Efficient Color Image Encryption and Decryption Algorithm, 2013):

$$\begin{aligned} \dot{x} &= -z-y \\ \dot{y} &= x+ay \\ \dot{z} &= b+z(x-c) , \end{aligned} \tag{4}$$

Where a, b and c are the parameters of the system.

D. Chua system

Another chaotic system is Chua system which had been developed from the Chua electrical circuit that had non-linear behavior. The equations of this system are (Mao, Cao, & Liu):

$$\dot{x} = \delta(y - x - h(x))$$
$$\dot{y} = x - y + z \quad (5)$$
$$z = -by - \gamma z ,$$

where δ, b *and* γ are the system parameters, and

$$h(x) = m1 + 0.5(m0 - m1)(|x + 1| - |x - 1|) , \quad (6)$$

E. Nien chaotic system

In 2007, H. Nien ... *et al.* proposed a novel chaotic system.This system is described by the following equations (H.H. Nien, 2005):

$$\dot{x} = -\delta(x + y + f(x))$$
$$\dot{y} = -\beta(x + y) - \gamma z \quad (7)$$
$$\dot{z} = y ,$$

Where δ, b *and* γ are the system parameters, and

$$f(x) = bx + 0.5(a - b)(|x + Io| - |x - Io|) , \quad (8)$$

where δ= 6.3; β=0.7; γ= 7; a=-1.143; b=-0.714; I_o=3

F. CL chaotic Systems

In 2007, Atheer J. Mansoor ... *et al.* proposed a novel chaotic system. This system is described by the following equations (Mansoor, Abdullah, & Zeboon, 2017) :-

$$\dot{x} = \delta(y - x - (m1 + 0.5(m0 - m1)(|x + 1| - |x - 1|))$$
$$\dot{y} = r * x - y - x * z \quad (2)$$
$$\dot{z} = x * y - \beta * z$$

Where, δ = 10, β = 8/3, r = 24, m0 = -1.27; m1 = -0.68

3. Encryption Quality Measurements

Many measurements are used to evaluate the strength of the scrambling algorithm quality. This section briefly discusses these measurements.

A. Distance scrambling factor (DSF)

This is the first theory for scrambling measurement. Here, the distance factor is calculated by comparing the pixels positions between the original image and the scrambled one. The calculation of distance scrambling factor degree could be described as follows:

For original image of pixels positions (i, j) and scrambled image of pixels positions (i',j'), the moving distance could be calculated as:

$$D(i,j)=\sqrt{(i - i')^2 + (j - j')^2} , \quad (10)$$

The average (mean) moving distance will be:

$$A(D) = D/(M * N) \quad (11)$$

Where M*N is the dimension of the image. The maximum distance could be calculated from:

$$A_{max}(D) = \sqrt{(M - 1)^2 + (N - 1)^2} , \quad (12)$$

So, the Distance scrambling factories

$$DSF = A(D)/A_{max}(D) , \quad (13)$$

The greater DSF means higher degree of scrambling (Arnold Transform Based Image Scrambling Method, 2013).

where (i', j') is the position of scrambled image pixel and (i,j) is the position of original image pixel. The average distance of the whole image could be calculated from the following equation:

$$ADC = \frac{1}{(M-2)*(N-2)} \sum_{i=1}^{M-2} \sum_{j=1}^{N-2} A\,DC(i,j) \quad , \qquad (16)$$

The average distance calculated from equation (16) must be greater than zero unless the scrambled image is the original image. Bigger ADC means higher scrambling (Mirghadri, 2010)

C. 2-D Correlation Coefficient

This method is used to obtain the degree of similarity between two images (matrices) by calculating the correlation coefficient between the two image with the same size M*N by the following equation:

$$r = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} ((X_{mn} - \overline{X})(Y_{mn} - \overline{Y}))}{\sqrt{(\sum_{m=1}^{M} \sum_{n=1}^{N} (X_{mn} - \bar{X})^2)(\sum_{m=1}^{M} \sum_{n=1}^{N} (Y_{mn} - \bar{Y})^2)}} \quad , \qquad (17)$$

where X and Y are two images (matrices), $\overline{X}$ and $\overline{Y}$ are the mean value of the elements of X and Y respectively. The range of the r values is between +1 and -1, where if r=+1 that's mean X and Y are identical, while if r=0 the two image are totally different, and if r=-1 that's mean that X and Y are identical but with phase shift of 180º (mirrored).

D. Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) can be used to evaluate the encryption scheme strength by indicating the pixel's value between the original image and the encrypted image. It can be calculated by using the following equation

$$PSNR = 10 * \log_{10} \left[\frac{M*N*255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (O(i,j) - E(i,j))^2} \right] \qquad \ldots (18)$$

Where O and E are the original and the encrypted image respectively, (i,j) is the coordinate of the pixel and M,N are the image size.
Lower PSNR means higher encryption effectively (Mirghadri, 2010)

E. Measurement Based on the Value Changing

This test depends on the comparison between the pixel's value before encryption with the pixel's value after encryption to obtain the changes whether regular or irregular.
The encryption quality could be obtained by measuring the deviation between the plain image and the cipher image as shown in the equation below:-

$$EQ = \frac{\sum_{i=0}^{255} |H_i(C) - H_i(P)|}{256} \quad \text{... (19)}$$

Where, $H_i(C)$ and $H_i(P)$ are the number of pixels at gray level i of the cipher and plain images respectively

There is another encryption quality measurement proposed by Luo et al., which could be evaluated by calculating the relative error of each pixel in the cipher image with its counterpart in the plain image, which is done by using the following equation

$$ARE = \frac{1}{M*N} \sum_{i=0}^{M-1} \sum_{j=0}^{W-1} \frac{|P(i,j) - C(i,j)|}{|P(i,j)|} \quad \text{...(20)}$$

Where P and C are the plain and cipher images of size M*N respectively (Mirghadri, 2010)

F. Maximum Deviation Analysis

Maximum Deviation analysis is a statistical analysis which is used to calculate the deviation between the original and the encrypted images. This analysis could be calculated according to the following equation

$$MD = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \quad \text{where } h=|H-H'| \quad \text{...(21)}$$

where H and H' are the histogram distribution of the original and the encrypted image. Higher MD means higher encryption degree and the encrypted image faraway (deviated) from the original one (Mirghadri, 2010)

G. Irregular Deviation Analysis

The irregular deviation is used to measure how the encryption process changes the values of the original image irregularly and randomizes it in uniform manner to make the statistical distribution of changing the pixels' values uniform

The irregular deviation analysis can be obtained from the following steps:-

Calculate the absolute difference between the original and the encrypted images:-

$$D=|O-E| \quad \text{... (22)}$$

where O and E represent the original and encrypted images respectively.

Obtain the histogram of the absolute difference

$$H=\text{histogram}(D) \quad \text{... (23)}$$

Calculate the average value of the histogram deviation

$$Av = \frac{1}{256} \sum_{i=0}^{255} H(i) \quad \text{... (24)}$$

Evaluate the absolute differences between the histogram deviation and the average deviation value

$$H_{D_i} = |h_i - Av| \quad \text{... (25)}$$

Compute the irregular deviation factor value

$$I_D = \sum_{i=0}^{255} H_{D_i} \quad \text{...(26)}$$

Smaller ID means higher encryption strength, where it is a pointer for the uniform distribution between the original and encrypted pixels' values (Mirghadri, 2010)

H. Measurement Based on the Value and Position Changing

This test depends on the comparison between the pixel's value before encryption with the pixel's value after encryption to obtain the changes whether regular or irregular.

The encryption quality could be obtained by measuring the deviation between the plain image and the cipher image as shown in the equation below:-

$$EQ = \frac{\sum_{i=0}^{255} |H_i(C) - H_i(P)|}{256} \quad \text{... (27)}$$

where, $H_i(C)$ and $H_i(P)$ are the number of pixels at gray level i of the cipher and plain images respectively

This measurement could be found by the flowing steps:-

Obtain the relationship between each pixel and its four neighbors as shown below

$$D1(i,j) = |[E(i-1,j) - E(i,j)]^2 - [O(i-1,j) - O(i,j)]^2|$$
$$D2(i,j) = |[E(i+1,j) - E(i,j)]^2 - [O(i+1,j) - O(i,j)]^2|$$
$$D3(i,j) = |[E(i,j-1) - E(i,j)]^2 - [O(i,j) - O(i,j-1)]^2|$$
$$D4(i,j) = |[E(i,j+1) - E(i,j)]^2 - [O(i,j+1) - O(i,j)]^2|$$
$$R(i,j) = D1(i,j) + D2(i,j) + D3(i,j) + D4(i,j) \quad \text{...(28)}$$

Calculate the scrambling degree S as below

$$S = \frac{\sum_{i=2}^{M-1} \sum_{j=2}^{N-1} R(i,j)}{255^2 \cdot (M-2) \cdot (N-2)} \quad \text{...(29)}$$

The value between 0 and 1, and greater S means better encryption results. (Mirghadri, 2010)

I. Entropy

The encryption quality could be measured by calculating the entropy of the plain image and the entropy of the cipher image, then comparing between them. The entropy if the image could be evaluated by the following equation:-

$$E = \sum_{i=0}^{2^n-1} [P(i) * \log_2 \left(\frac{1}{P(i)}\right)] \quad (30)$$

the maximum entropy equals 8, and it is referred to as an ideal case of randomness. In general, the entropy of practical image is less than the maximum entropy (Mirghadri, 2010)

4. The Proposed Encryption Algorithm:

The proposed scheme performs the image encryption by using chaotic systems. At first , the original image transformed form N*M into a vector of 1*D where D=M*N by taking row by row or column by column. Then creating three vectors with dimension of 1*D, where the vectors elements

are an indicator to pixel status (had been encrypted or not). The algorithm of the proposed scheme could be explained throughout the following flow chart:

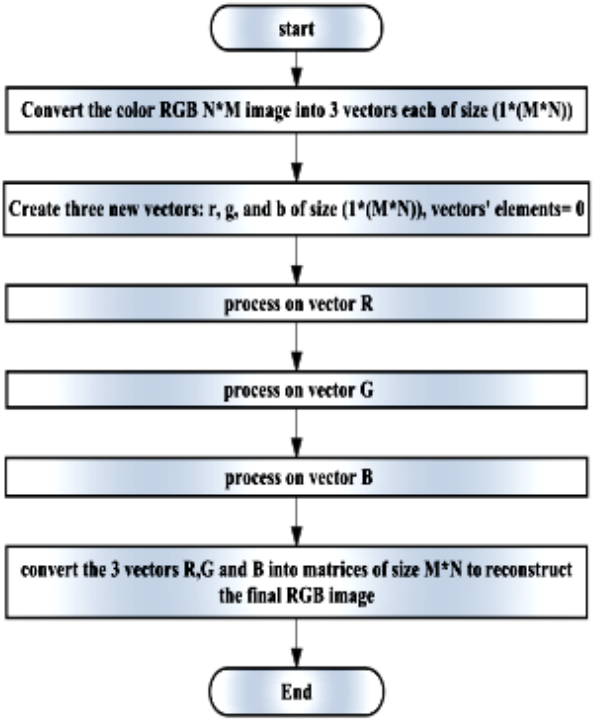


Fig.1. The Flowchart of the proposed algorithm

The decryption process is done by following the same steps of the encryption process with using the same chaotic system, same initial values and same parameters. Any difference in any parameter or initial value makes the decryption process incorrect. Figure 1 shows the flowchart of the proposed algorithm.

It is worth noted that the decryption processes for vectors R, G and B, shown in this figure as three successive blocks, are identical. Figure 2 shows the details of encryption process for vector R block as a flowchart.

The proposed system has been simulated via MATLAB. At first, the proposed algorithm applied on image of 256 * 256 and compared the result with the traditional systems when using ACM. Then the proposed system

Table 1. The parameters of chaotic flow systems used in simulations

Chaotic Flow System	Parameters
Lorenz	a=10, b=24, c=8/3
Rössler	a=0.2, b=0.2, c=5.7
Chua	δ =10, b=14.78, γ=0.0385, m_1=-1.27, m_0=-0.68
Nien	δ =6.3, β=0.7, γ=7, b=-0.714, a=-1.143, I_o=-3
CL	δ = 10, β = 8/3, r = 24, m0 = -1.27; m1 = -0.68

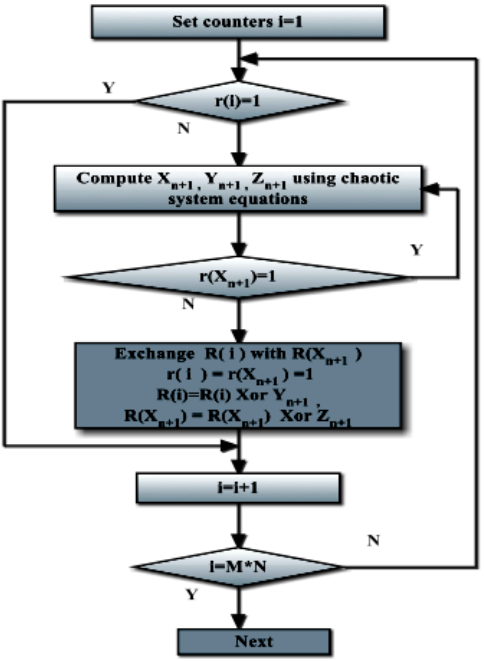


Fig.2. the flow chart of encryption process for vector R block of figure 1.

5. Simulation Results

For equal dimensions, the image sizes that are taken for the system implementation is (256*256),

Figure 3 shows the encrypted image for each chaotic system used in the proposed system with initial value X0=0.1, Y0=0.1 and Z0 =0.1 with parameters that are shown in Table 1

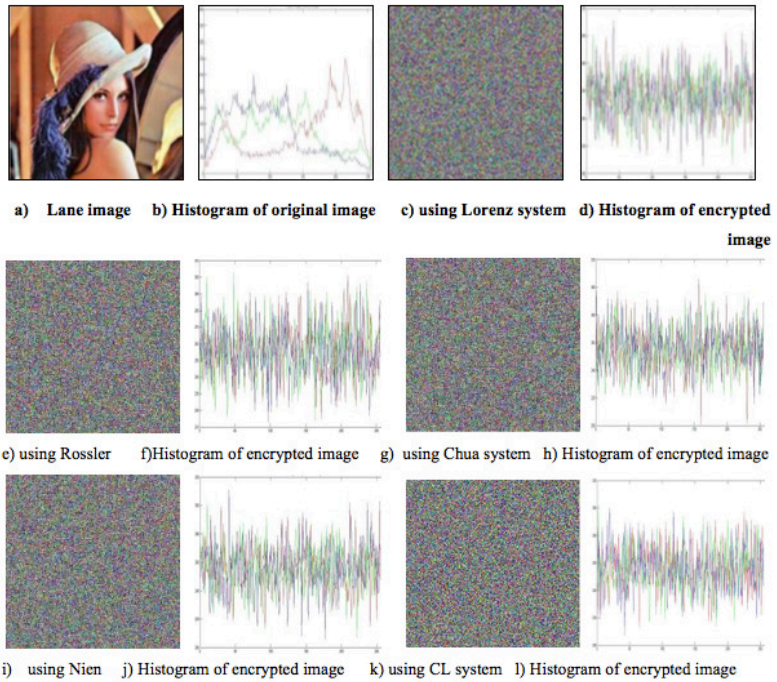


Fig.4. Results of the proposed algorithm for image of size 256*256 using chaotic flow sequences.

Table 2 shows the best result of the proposed algorithm compared with the best results of the traditional scheme (the best value of each case is taken for each iteration):-

Table 2. The statistical measurements of the encryption system result comparing with traditional method.

	system type	type / iteration	ARE	EQ	CORR.	ID	MD	PSNR	S	ENTROPY
Best ARE and ID	Nien propose	column	131.250	11.357	0.001	2649.417	2884.000	8.8582	0.6512	7.98327
	Arnold Chua	48	131.281	11.552	0.01148	2570.042	2932.833	8.870	0.652	7.984
Best EQ and MD	Rossler propose	column	131.242	11.586	-0.004	2278.708	2942.167	8.7960	0.6524	7.984
	Arnold Lorenz	23	131.252	11.948	-0.00532	3284.458	3036.333	8.728	0.654	7.98258
Best CORR.	Nien propose	column	131.250	11.357	0.00078	2649.417	2884.000	8.8582	0.6512	7.983
	Arnold Chua	60	131.270	11.354	0.000	2888.625	2888.000	8.845	0.653	7.98145
Best PSNR	CL proposed	column	131.228	11.523	-0.013	2639.042	2926.833	8.7817	0.6611	7.983
	Arnold CL	25	131.222	11.706	-0.03308	3007.917	2976.833	8.605	0.669	7.98163
Best S	Rossler propose	column	131.241	11.310	-0.005	2214.208	2877.333	8.8227	0.6618	7.98203
	Arnold Rossler	19	131.244	11.492	-0.00612	1867.417	2922.333	8.793	0.682	7.983
Best ENTROPY	Chua propose	column	131.235	11.409	-0.004	2764.625	2901.000	8.8404	0.655	7.98413
	Arnold Lorenz	3	131.230	11.589	-0.00979	2616.875	2945.333	8.752	0.6685	7.987

The colored cells are the best result of the tests, while green cells show the number of iterations in the traditional schemes to reach the best result. Figure 5shows the required time for encryption and decryption process of the proposed algorithm and the traditional scheme of each image size.

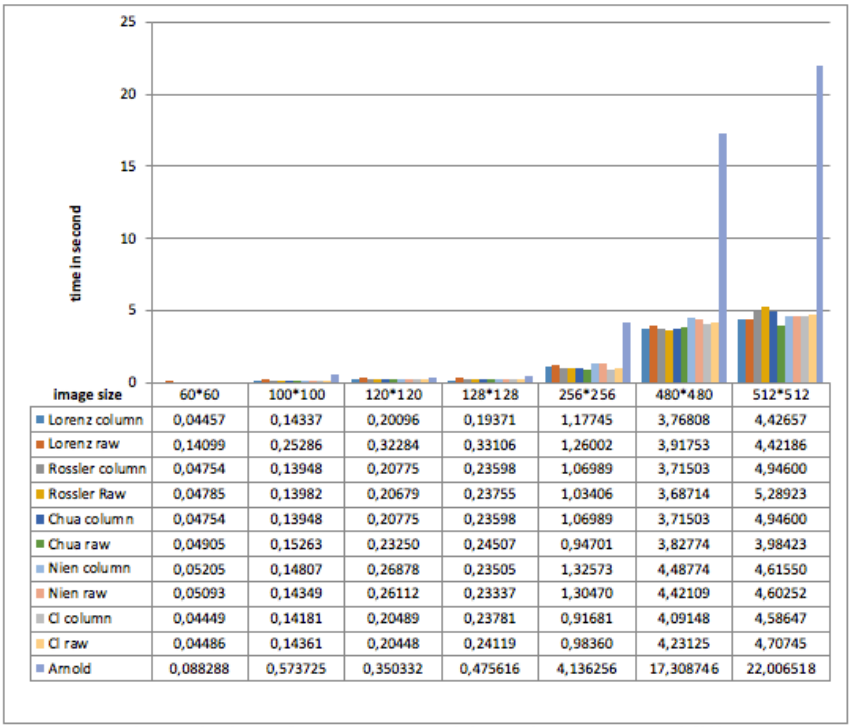


image size	60*60	100*100	120*120	128*128	256*256	480*480	512*512
Lorenz column	0,04457	0,14337	0,20096	0,19371	1,17745	3,76808	4,42657
Lorenz raw	0,14099	0,25286	0,32284	0,33106	1,26002	3,91753	4,42186
Rossler column	0,04754	0,13948	0,20775	0,23598	1,06989	3,71503	4,94600
Rossler Raw	0,04785	0,13982	0,20679	0,23755	1,03406	3,68714	5,28923
Chua column	0,04754	0,13948	0,20775	0,23598	1,06989	3,71503	4,94600
Chua raw	0,04905	0,15263	0,23250	0,24507	0,94701	3,82774	3,98423
Nlen column	0,05205	0,14807	0,26878	0,23505	1,32573	4,48774	4,61550
Nlen raw	0,05093	0,14349	0,26112	0,23337	1,30470	4,42109	4,60252
Cl column	0,04449	0,14181	0,20489	0,23781	0,91681	4,09148	4,58647
Cl raw	0,04486	0,14361	0,20448	0,24119	0,98360	4,23125	4,70745
Arnold	0,088288	0,573725	0,350332	0,475616	4,136256	17,308746	22,006518

Figure 5 The required time for (encryption and decryption processes) of different implemented systems

From figure 5 above, it is very clear that:

1) All the proposed algorithm systems are faster than the traditional one

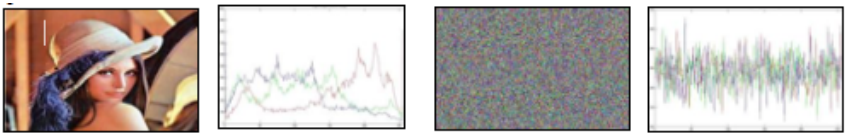
2) As the image size increases, the speed improvement of the propose scheme over the traditional one increases and this improvement increases as the image size increases. For example, image of size 60*60, 100*100, 120*120 and 128*128 the algorithm is faster two times.

3) For image size 256*256, the algorithm is faster four times.

4) For image sizes 480*480 and 512*512, the algorithm is faster about five times

For non-equal dimensions, the image size that is taken for the system

implementation is 473*846. Figure 6 shows the original image of size 473*846 with the resulting encrypted images after implementing the proposed algorithm. After one iteration only, the encrypted image is decrypted using any type of the chaotic flow sequences considered as shown.



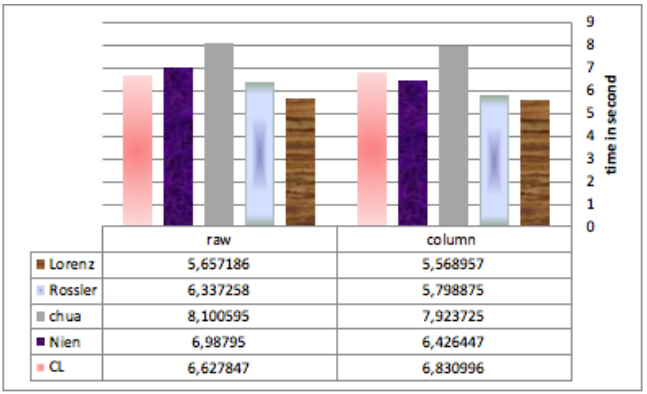
a) original image b) Histogram of the original c) Image after encryption with initial $x_0=y_0=z_0=0.1$ d) Histogram of the encrypted image

Figure 6 Lena original and the encrypted image using 4th propose algorithm (473*846)

Table 3 the testing techniques results of the proposed algorithm implementation on non-equal dimension images

system	type	ARE	EQ	CORR	ID	MD	PSNR	S
Lorenz	column	1385.708	93.302	0.00130	300905.255	353553.000	8.562	0.66939
	raw	1388.555	93.305	0.00084	297734.667	354278.833	8.557	0.66937
Rossler	column	1387.849	93.303	0.000	305964.667	354106.167	8.557	0.670
	raw	1387.617	93.302	-0.001	299280.432	354063.000	8.552	0.669
Chua	column	1385.073	93.307	0.00076	299108.432	353388.333	8.567	0.66809
	raw	1385.073	93.305	-0.00048	292406.313	353374.333	8.557	0.66745
Nien	column	1387.891	93.303	0.000	292806.589	354114.000	8.553	0.67030
	raw	1386.398	93.305	0.00184	298029.844	353704.000	8.565	0.66801
CL	column	1390.299	93.300	0.000	298424.901	354729.500	8.558	0.669
	raw	1386.753	93.304	-0.00007	301607.922	353819.833	8.559	0.669

The values of ADC and DSF are the same values that are listed in table 3 because these values depend only on the moved distance of the pixel from its original image. Figure 7 shows the required time for (encryption and decryption processes) of the proposed algorithm on Lena non-equal dimensions image.



	raw	column
Lorenz	5,657186	5,568957
Rossler	6,337258	5,798875
chua	8,100595	7,923725
Nlen	6,98795	6,426447
CL	6,627847	6,830996

Figure 7 The required time for encryption and decryption processes for non-equal image dimensions of different implemented systems

For the results that are shown in table 3 and figure 7, it could be noticed that the algorithm has relatively very high speed even with images with large size. According to the statistical analysis of the algorithm, it has an excellent performance with high encryption degree and a short time required for the implementation.
This result is obtained via MATLAB simulation using personal computer of type HP Elitebook2540p has CPU Intel core I5.

6. CONCLUSIONS

This paper proposes a new scheme for digital image encryption based on changing pixels' value and position using chaotic flow sequence. Firstly, the N*M color RGB image are converted into three 1*D vectors where D=N*M, then the positions of the pixels are changed according to the generated number from the chaotic system that had been used from the first band, which define the pixel position for each vector of the image. Then the value of two pixels that had been switched in positions changed by using the random number generated from the 2nd and 3rd band from the same chaptic flow system. The image then is reconstructed after changing all pixels' locations. The scheme performance is effectively evaluated by applying three types of tests which are Distance Scrambling Factor (DSF), Average Distance Change (ADC), 2-D correlation coefficient, Entropy required Time, Maximum Deviation , Peak Signal To Noise Ratio, Irregular Deviation and Measurement Based On The Value And Position Changing

(S) The experimental result shows that the proposed system has a higher degree of encryption from the first iteration comparing with the traditional encryption system such as Arnold Cat Map. Another advantage of the proposed system is the implementation on equal and non-equal dimension images. Future improvement of the proposed system can include using hybrid chaotic flows and maps, changing the value of the pixels in the same time when changing their position to obtain higher degree of security.

Bibliography

Gao, T., & Chen, Z. (2008)). A new image encryption algorithm based on hyper-chaos. Physics Letters, Elsevier, 394–400.

Tang , Z., & Zhang, X. (2011). Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies. JOURNAL OF MULTIMEDIA , 202-206.

Arnold Transform Based Image Scrambling Method. (2013). 3rd International Conference on Multimedia Technology (pp. 1309-1316). China: Atlantis Press.

Gaspard, P. (2005). R¨ossler systems. Encyclopedia of Nonlinear Science, 808-811.

Gupta, P., Singh, S., & Mangal, I. (2014). Image Encryption Based On Arnold Cat Map and S-Box. International Journal of Advanced Research in Computer Science and Software Engineering, 807-812.

H.H. Nien, C. H. (2005). Digital color image encoding and decoding using a novel chaotic random generator. Chaos, Solitons and Fractals, Elsevier, 1070–1080.

Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission. (March 2011). International Journal of Computer Sci ence and Technology IJCST, 132-135.

Jing-yu, P. (2013). Efficient Color Image Encryption and Decryption Algorithm. International Journal of Digital Content Technology and its Applications(JDCTA), 129-136.

Jing-yu, P. (2013). Efficient Color Image Encryption and Decryption Algorithm. International Journal of Digital Content Technology and its Applications(JDCTA), 7(6), 129-136.

Mansor, A. J., Abdullah, H. N., & Zeboon, H. T. (2017). Robust Encryption System Based on Novel Chaotic Sequence. Research Journal of Applied Sciences, Engineering and Technology, 14(1), 48-55.

Mao, Y., Cao, L., & Liu, W. (n.d.). Design and FPGA Implementation of a Pseudo-Random Bit Sequence Generator Using Spatiotemporal Chaos.

Merah, L., Ali-Pacha, A., Said, N. H., & Mamat, M. (2013,). Design and FPGA Implementation of Lorenz Chaotic System for Information Security Issues. Applied Mathematical Sciences, 237 - 246.
Mirghadri, A. J. (2010). A New Approach to Measure Quality of Image Encryption. (IJCNS) International Journal of Computer and Network Security, 38-43.
Peterson, G. (1997). Arnold's Cat Map.
Prasad, M., & Sudha, K. (2011). Chaos Image Encryption using Pixel shuffling. Computer Science & Information Technology (CS & IT), 169–179.
Willsey, M., Cuomoy, K., & Oppenheim, A. (2010). Selecting the Lorenz Parameters for Wideband Radar Waveform Generation. INTERNATIONAL JOURNAL OF BIFURCATION AND CHAOS, 1-12.
Zhu Liehuang, L. W. (2006). A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences. International Journal of Computer Science and Network Security (IJCSNS), 6(8B), 125-130.

UNIVERSIDAD
DEL ZULIA

opción
Revista de Ciencias Humanas y Sociales

Año 35, N° 20, (2019)

Esta revista fue editada en formato digital por el personal de la Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia.
Maracaibo - Venezuela

www.luz.edu.ve

www.serbi.luz.edu.ve

produccioncientifica.luz.edu.ve