Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location

Hazem Mohammad Al-Najjar

Abstract—**Any image encryption system divided mainly into two Methods: pixel replacement methods and pixel scrambling methods. In the pixel replacement method, each pixel in the image needs to change its value. Where, in the scrambling method the pixel needs to change its position. In this paper, we propose a new image encryption algorithm based on multi-dimensional chaotic function called a Rossler attractor; to enhance the encryption system, increase the complexity of the encryption keys and decrease the computational complexity of the cipher image. To do that, the Rossler attractor with the three dimensional planes as the encryption keys for the first level and the second level encryption are used, where, to decrease the execution time and computational complexity we used only one non-linear term function. Furthermore, our algorithm consists of two scrambling methods and two replacement methods. In which, each value in the image will be replaced by using a XORing operation with its location and change its location by using two shuffling approaches. Moreover, 3–planes chaotic function was used to scramble the pixels position as follows: in the first method we used X, Y planes of the Rossler attractor and in the second method we used X,Y and Z planes, so, the uncertainty of the adjacent pixels will be increased. However, by analyzing our algorithm, we show that the key space of our algorithm is equal to 10^{45}, where, the entropy tests shown that the average entropy for the tested images is not less than 7.9971.Furthermore, after analyzing the histogram and correlation between the adjacent pixels, we show that our algorithm is strong against different types of attacks and it's sensitive to the initial conditions.**

Index Terms—**Image encryption, rossler attractor, pixel replacement, position scrambling.**

I. Introduction

Information security is one of the important issues in the internet. Hence, every user needs to send the information in a secure way. Because of this, the data encryption becomes very important in the internet. Furthermore, many methods to encrypt the data had been proposed by the researchers such as: RSA, DES, IDEA, to send the information on a garbage way so the sniffing to these data is unreadable. On another hand, securing the data is not like securing the images since it needs special methods and special rules.

Chaos theory is one of the most important theories that used in the new image encryption systems. The chaos was used in the encryption system because of its characteristics, like sensitivity to the initial conditions and unpredictability to the chaos sequences. Furthermore, there are many suggested models to represent the chaos by using the mathematical models such as: logistic map, Lorenz attractor, Henon map and Rossler attractor. In Lorenz attractor, the system has two non-linear terms where in Rössler attractor there is only one non-linear term which makes the complexity of the Rolsser attractor is less than the Lorenz attractor. On hand side, many researchers try to design encryption systems by using chaos, like [1] divides the image into blocks and try to use a permutation on each block by using a logistic map to encrypt the image. Where, in [2] they used two one-dimensional discrete Chebyshev chaotic sequences for row and column scrambling for each pixel on the original image. In [3] they proposed an encryption method that used multi- chaotic systems to increase the key space and make system's breaking very difficult. In which [4] used Rossler chaotic system to encrypt the image by applying changes in the pixels value and their position; to increase the uncertainty in the cipher images. The one time pads with the logistic map (as a chaotic function) are used in [5] to encrypt the image and increase the size of the encrypted keys. Where, in [6] the CAT map was used to encrypt the discrete images by using the shuffling approach only, in which, the histogram after and before encryption will be the same. Others, like [7] used a knight's tour with slip encryption filter; to encrypt the image without using any chaotic functions. However, security analysis results, drawbacks and the strength of the chaotic systems are analyzed in [8], [9]. In this paper, we conduct to use a Rossler chaotic function to encrypt the image and increase the keys space. In which, two shuffling methods and two replacement methods in the pixels are used; to encrypt the image and increase its space.

The rest of this paper is organized as follows. In section 2, the pixel value replacement is described on detail. Section 3 describes the Rossler chaotic function and how to use it in the encryption system and on a pixel location scrambling. Experimental results and security analysis are presented in section 4. Finally, our conclusions are drawn in section 5.

II. Pixels-Value Replacement

A. First Replacement Method

To change the pixels value we need to replace the value of the current pixels. Moreover, there are many methods to do that such

as: multiplying the value with a constant then finds the modulus of this multiplication, or by applying a bit XORing with a specific value…etc. In this paper, we suggest to use rows indexes and the columns indexes to replace the value of the pixel in the image. So, each column index value will be used; to encrypt the pixels in that column as shown in the following equation:

$$P_{i+1}(J) = XOR(\, P_i \,, J + 1) \tag{1}$$

Manuscript received March 10, 2012; revised May 6, 2012.

H. N. is with the Department of Computer, Taibah University, Madina, KSA (e-mail: hazem_najjar@yahoo.com).

where P_{i+1} and P_i are the new and old pixel values, respectively and J is the column index value to that pixel. After that, we used a first shuffling approach to increase the randomness in the encrypted images (as discussed in section 3).

B. Second Replacement Method

After the first replacement method, we shuffle the image and change the pixels position. So, the input of the second replacement method is replaced-shuffled image. Moreover, in the second method, we replace the value of the pixels by XORing the Pixel's value with its row index value. So, the resulted image will be differed completely on the first image from the step one, the XORing is described in the following equation:

$$RSP_{i+1}(I) = XOR(\, RSP_i \,, I + 1) \tag{2}$$

where, RSP is the replaced-shuffled pixels, i, i+1 are the current pixel and the new pixel after the XORing, respectively and I is row index value of the current pixel.

III. Pixels- Location Scrambling

The Rossler chaotic function is one of the multi-dimensional chaotic function that represents the three dimensional ordinary differential equation with one non-linear term (some time called a Rosssler attractor). Furthermore, the ordinary differential equation can generate a chaotic behavior under certain initial values (x_0, y_0, z_0), which is defined as in the following equation, the Rossler attractor with the three dimensional system is shown in the following equation:

$$\begin{cases} \dot{x} \ = -(y + z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \tag{3}$$

x, y, z, t, a, b and $c \in R$, and $\dot{x}$ is the differential value for the variable x. In the Rossler function to generate the chaotic behavior, the space variables should be in the following ranges: $-15<x<17$, $-16<y< 13$ and $0<z<36$, where, the classic chaotic attractor is defined as follow a, b, and c as 0.15, 0.20 and 5.7 respectively.

Before using the chaotic sequence we need to modify the range of the chaotic output by pre-processing the X, Y, Z values as discussed in [3]:

$$V(i) = 10^n V_n(i) - round(10^n V_n(i)) \tag{4}$$

In which, n is the right shift the number $V(i)$ n digits and V is the plane to enhance x, y or z. After that, we modify the range to be between 0 and 255 to all planes values. Moreover, the pixel location scrambling is used to shuffle the pixels image to new position; to increase the randomness in the image and decrease the correlation coefficients between the adjacent pixels. To do that, we used a Rossler chaotic function that has three planes (X, Y, Z). In our algorithm two shuffling approaches are used as follows: first shuffling approach that used after the first value replacement method where the second method will be used after the second replacement approach, in which this will increase the uncertainty of the encrypted images. Our shuffling approach is divided as follow:

A. First Shuffling Approach

In the first shuffling approach we used X, Y Planes to change the position of the pixels. In which, each pixel will change his position to the new x, y position.

B. Second Shuffling Approach

In the second shuffling approach, the input image is modified by using two replacements method and one shuffling approach. After that, the image will be shuffled after the second replacement method by using X, Y and Z planes by using the following equation:

$$Pixel(mod(x, y) + 1, z) = Pixel(i, j) \tag{5}$$

where, Pixel represents the pixels values in the image and i, j is the location of the current pixel, x, y, z are the values from the sequence planes, X, Y and Z, respectively. After the second shuffling the uncertainty and the randomness of the values in the image will be grown and enhanced as will be shown in the experimental results.

C. Encryption Scheme Diagram

Our algorithm is divided into two parts: pixel value replacement; to change the pixels value. And, the scrambling approach; to change the pixels position. In which, to change the pixel value we used i, j indexes, where, the columns indexes used first then rows indexes. Moreover, in scrambling approach the X-plane and Y-plane were used; to change the location of the pixels, after the first replacement method. Then, the second scrambling approach that depends on Z, Y, X from the Rossler equation will be used after the second replacement method from the Rossler function (as shown in the Fig. 1). However, the decryption process is done in the reverse order.

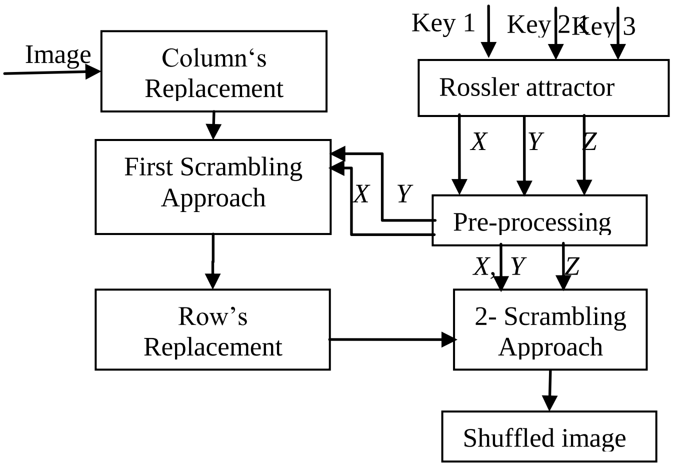


Fig. 1. Encryption algorithm diagram.

IV. Experimental Results and Security Analysis

The experiment evaluated the ability of the proposed method; to encrypt the images in the effective way. So, we used Lena and Cameraman as tested images with the size 256x256. The cipher and original images of the Lena and Cameraman are shown in Fig.2, respectively. With input keys Key1= 1.1045, Key2= 1.2831 and Key3 =1.3682 for two images.

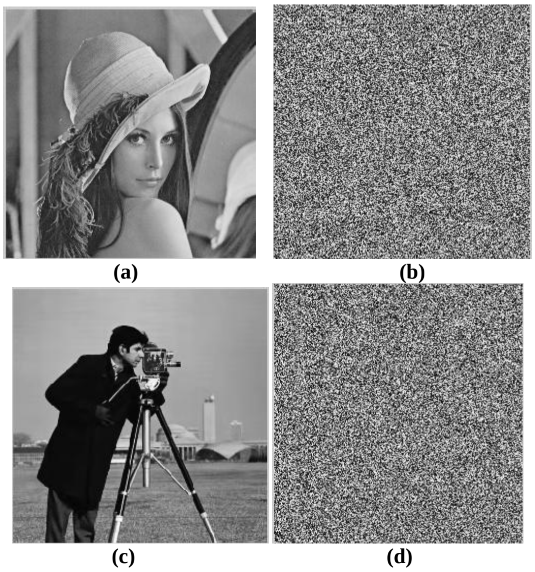


Fig. 2. Encryption for cameraman and Lena images

A. Keys Space Analysis

The key space of our algorithm is depending on the Rossler space keys. For our algorithm, the key space is calculated as follows: we have three keys key1, key2 and key3, the key space of each one is equal to 10^{15} then the key space of the algorithm is equal to 10^{45}.

B. Keys sensitivity Analysis

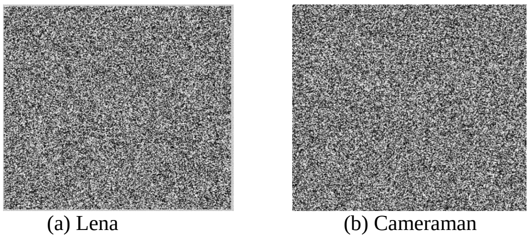
The encryption system should be sensitive to the small changes on the decrypted keys. And, generate a wrong decrypted image, if there is a small difference in the decryption keys. Only the same keys, should give the same image to the receiver side. Our sensitive tests keys are Key1= 1.1046, Key2= 1.2832 and Key3 =1.3683, in which, Fig.3 shows the decrypted image for the lena and cameraman tested images by using a wrong decryption keys.

C. Information Entropy Analysis

In this part we interested in the randomness of our system, where, the true random variable should generate 2^8 symbols with equal probability and the entropy value equal 8. To check, the randomness of our random cipher image, we used a following
equation [8]:

$$H(s) = \sum_{s} P(S_i) log \frac{1}{P(S_i)} \tag{5}$$

where P (S_i) represents the probability of symbol S_i, in our tests the average entropy of the lena cipher image is 7.9972 and for the cameraman cipher image is equal to 7.9971, which are very close to the optimal value, then the entropy attack is not possible.



(a) Lena (b) Cameraman

Fig. 3. Sensitivity tests of keys

D. Histogram Analysis

By analyzing the image histogram the cryptanalyst can get very useful information from the cipher image. In which, the good encryption algorithm should generate uniformly distribution of the histogram. In our tests, it's very difficult to get any information from the histogram; Fig. 4 shows the histogram analysis of cameraman and lena image and their cipher images, respectively.

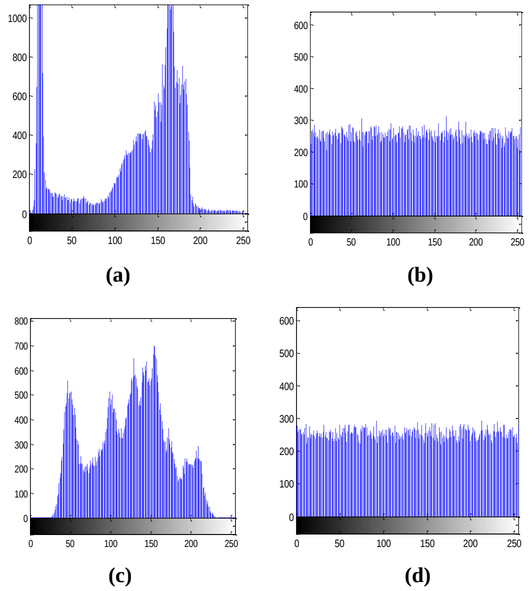


Fig. 4. Histogram of cameraman and Lena and cipher images, respectively.

E. Correlation Analysis

It's known that some algorithm was broken by using correlations between two adjacent pixels (in vertical, horizontal and diagonal adjacent). For this, we try to test our system by calculating the correlation coefficient for all possible cases. Where, the correlation coefficient is calculated by using the following formula [10]:

$$r = \frac{Cov(i,j)}{\sqrt{D(i)}\sqrt{D(j)}} \tag{6}$$

$$D(i) = \frac{1}{M}\sum_{i=1}^{M}(i - \bar{\imath}\ )^2 \tag{7}$$

$$Con(i,j) = \frac{1}{M}\sum_{i=1}^{M}(i - \bar{\imath})(j - \bar{\jmath}) \tag{8}$$

M is the total number of randomized pairs, *i* and *j* are the two vectors that contains *i* values and *j* values of the pair in the tested image, respectively.

Table.1 shows the correlation coefficients between two adjacent pixels in all possible cases (vertically, horizontally and diagonally) of the plain-text images and cipher images. The results revealed that the proposed method randomized the pixels in very good way.

TABLE I: CORRELATION COEFFICIENTS OF ADJACENT PIXELS

Image / Coefficient	Lena		cameraman	
	Plain image	**Cipher image**	**Plain image**	**Cipher image**
Vertical	0.9669	0.0199	0.9633	0.0121
Horizontal	0.9361	0.0173	0.9417	0.0201
Diagonal	0.9159	-0.0094	0.9183	0.0220

F. Plain –text sensitivity Analysis

The last metric, we need to test it in our system is a plain-text sensitivity. Since, if the cipher image is not sensitive in the changing of the plaintext then the cryptanalyst can get very useful information from the encrypted image. For this, we use two criteria, NPCR (Number of Pixel change Rate) and UACI (Unified Average Changing Intensity). Where, NPCR defined as a percentage of different pixels number between two cipher images and UACI defined as an average intensity of differences between two cipher images as defined in the following:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MxN} x100\% \qquad (9)$$

$$UACI = \frac{1}{MxN} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} x100\% \qquad (10)$$

where M x N is the size of the cipher images and $C1$ and $C2$ are two different cipher images encrypted by using a different keys, where $D(i\ ,j)$ is defined as follow:

$$D(i,j) = \begin{Bmatrix} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{Bmatrix} \qquad (11)$$

After calculations, we get the Average NPCR and UACI of lena image are: NPCR = 99.6597and UACI = 33.2669 and that of the cameraman image are: NPCR = 99.6185 and UACI = 33.5396. Then our algorithm has a good ability against known plain text attack.

V. Conclusion

In this Paper, a new approach to encrypt the image by using a Rossler chaotic function and the Row’s and column’s indexes are proposed. In which, the algorithm consists of two replacement methods and two scrambling methods; to change the value of the pixels and the location of the pixels, respectively. Where, the *X*, Y- planes of the Rossler equation are used in the first shuffling method and the *X*, *Y* and *Z* planes are used in the second shuffling method. Moreover, in the first replacement method we used a column index value and in the second replacement method we used a row index value. Therefore, the order to encrypt the image by using our algorithm is as follow: first replacement method, first shuffling method, second replacement method and finally second shuffling method. However, we shown by experimental results that our algorithm is sensitive to initial conditions and strong against the brute force attacks. Finally, we found that our algorithm has a high security against different types of attacks with the large space of the encryption keys.

References

[1] E. Xu, L. Shao, G. Cao, Y. Ren, and T. Qu. “A New Method of Information Encryption,” *Int. Colloquium on Computing, Communication, Control, and Management*, 2009, pp. 583-586.

[2] Z. Dinghui, G. Qiujie, P. Yonghua, and Z. Xinghua. “Discrete Chaotic Encryption and Decryption of Digital Images,” *Int. Conf. on Computer Science and Software Engineering*, 2009, pp. 849- 852.

[3] H. Nien, W. Huang, C. Hung, C. Huang, and Y. Hsu. “Hybrid image encryption using multi-chaos-system,” *Int. Conf. in Information, Communications and Signal Processing (ICICS)*, 2009, pp. 1-5.

[4] Y. Cao and C. Fu. “An image encryption scheme based on high dimension chaos system,” *Int. Cof. Intelligent computation technology and automation*, 2008, pp. 104-108.

[5] J. Jeyamala, S. GrpiGranesh, and S. Raman. “An image encryption scheme based on one time pads- a chaotic approach,” *Int. Conf. on computing, communication and networking technologies*, 2010, pp. 1 – 6.

[6] W. Zhu and Y. Shen. “Encryption Algorithms Using Chaos and CAT Methodology,” *Int. Conf. Anti-Counterfeiting Security and Identification in Communication (ASID)*, 2010, pp. 20 – 23.

[7] J. Delei, B. Sen, and D. Wenming. “An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter,” *Int. Conf. on Computer Science and Software Engineering*, 2008, pp. 251-255.

[8] R. Rhouma and B. Safya. “Cryptoanalysis of a new image encryption algorithm based on hyper-chaos,” *Phyiscal Letters A*, vol. 372, 2008, pp. 5973-5978.

[9] X. Di, L. Xiaofeng and W. Pengcheng, “Analysis and improvement of a chaos image encryption algorithm,” *Chaos, Solution and Fractals*, 2009, vol. 40, pp. 2191-2199.

[10] M. Long and L. Tan. “A chaos –based data encryption algorithm for image/video,” *Int. Conf. on Multimedia and information technology*, 2010, pp 172-175.

Hazem M. Al-Najjar was born in Jordan in 1986. He received the M. Sc. degree in computer engineering from Jordan University of Science and Technology (JUST), Irbid, Jordan, in 2011 and the B. Sc. degree in computer engineering from Yarmouk University, Irbid, Jordan, in 2008. Since February 2012, he has been with the Department of Computer, Taibah University, Madina, KSA. His current research interest is in wireless networks with emphasis on wireless sensor networks, grid computing, network coding, image and data encryption and Mobile payment systems.