Digital Image Encryption Algorithm Based on Chaotic Block and Pixel Mapping Table

Nadia Al-Rousan, Hazem Al-Najjar

Abstract—In this paper, we propose a new image encryption algorithm that depends on changing the pixels value and on the shuffling approach of the image. Our algorithm used two chaotic functions to encrypt the image. First, the Rossler chaotic function to create a linear independence between random chaotic blocks and to shuffle the image, where the second chaotic function is a logistic map to create PMT to change the pixels value after creating the liner independence relationship between the blocks to increase the randomness of the cipher image. However, by analyzing our algorithm, we show that it's strong against different types of attacks.

Index Terms— Image Encryption, Data Hiding, Logistic map, Pixel replacement, Rossler, shuffling approach.

1 INTRODUCTION

Chaos theory Data security has become a critical issue in the internet. In which, the transition between the user's needs to be protected, so no one can know its contents. Because of this, the data encryption becomes very popular field nowadays. Therefore, many researchers suggest encrypting the image by using different methods. All of the suggested methods in this field, divided into two Approaches: 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.

On another hand, Chaos system was used in the computer technology by Edward Lorenz in 1963. Furthermore, because of chaos characteristics such as sensitivity to the initial conditions and unpredictability to the chaos sequences, chaos had been used in the encryption system. Many papers try to design encryption systems by using chaos, like [1-5] they used chaotic functions to encrypt the image using a replacement and shuffling approaches. Where, in [13] they used Chebyshev chaotic sequences for row and column scrambling for each pixel in the original image. In [11] a regressive function for color and grey level images was used to encrypt the image by using a cat map. Moreover, in [10] they used Rossler chaotic system to encrypt the image by applying changes in the pixels value and their positions; to increase the uncertainty in the cipher images. The one time pads with the logistic map (as a chaotic function) are used in [7] to encrypt the image and to increase the size of the encrypted keys in the cipher. Ikeda map was used to encrypt the color and grayscale images [8]. However, statistical analysis, results and drawbacks of the chaotic systems are analyzed in [6, 12]. In this paper, we conduct to use a Rossler and logistic map chaotic functions to encrypt the image and to increase the keys length by creating a linear independence relation between the block's image and by using a Pixel Mapping Table (PMT); to increase the randomness in the cipher image.

The rest of this paper is organized as follows. In section 2, our proposed approach is described in detail. Experimental results and security analysis are presented in section 3. Finally, our conclusions are shown in section 4.

2 PROPOSED ALGORITHM

2.1 Logistic Map

Logistic map is a chaotic function quantifies the sensitivity of the system to the initial conditions. So, small changes in the initial conditions will get extremely different behavior than the first one. For this reason, the chaotic function is widely used in the cryptography. The logistic map can be described as follow:

$$X_{n+1}=\lambda X_n(1-X_n) \quad (1)$$

$\lambda \in [0,4]$, $X \in (0,1)$, where the chaotic behavior is achieved when $\lambda \in [3.57,4]$. In our encryption algorithm, we used logistic map to shuffle the PMT to increase the uncertainty in the result.

2.2 Rossler Chaotic function

The Rossler chaotic function is a three dimensional ordinary differential equation, with one non-linear term (sometimes called Rossler attractor). The Rossler attractor was proposed in 1976 as an enhanced model of the Lorenz chaotic attractor that contains two nonlinear terms, which is defined in the following equations:

$$\begin{cases} \frac{dx}{dt} = -(y+z) \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + z(x-c) \end{cases} \quad (2)$$

x, y, z, t, a, b and c $\in R$, depending on the chaos theory

- *Nadia Al-Rousan is currently a lecturer in computer engineering Taibah university, KSA E-mail: nadia.rousan@yahoo.com*
- *Hazem Al-Najjaar is currently a lecturer in Computer engineering in Taibah university, KSA E-mail:hazem_najjar@yahoo.com*

some ordinary differential equations may have a chaotic behavior under certain conditions. In the Rossler function to generate the chaotic behavior the space variables should be in the following ranges (Fig. 1): -15<x<17, -16<y< 13 and 0<z<36 where the classic chaotic attractor that studied by Rossler defined a, b, and c as 0.15, 0.20 and 5.7, respectively.

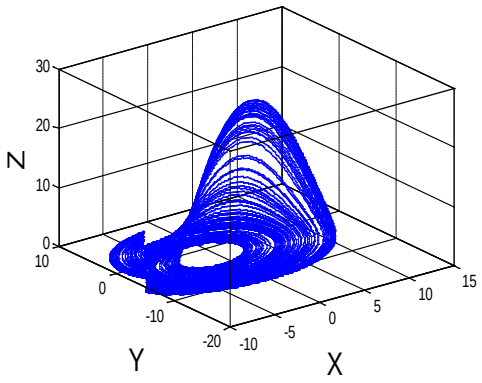


Fig. 2: Rossler attractor

Where, the pre-processing function, to enhance the output of the chaotic model can be described in the following equation [3]:

$$V(i) = 10^n V_n(i) - \text{round}(10^n V_n(i)) \quad (3)$$

In which, n is the right shift the number V(i) n digits and V is the plane to enhance x, y or z.

2.3 Pixel Mapping Table (PMT)

PMT is defined as a table that contains the value of the gray level pixels from 0-255 in the shuffled order. The PMT will be shuffled depending on the values in the logistic map generator. Therefore, any crypto-analysis of the ciphered images will not get any useful information about the PMT design. Since, linear independence between the random blocks in the image and shuffling images after replacement approach will hide the PMT design. Shuffled and unstuffed PMT are shown in Fig.2:

1	2	3	……	255
125	20	50	……	10

Fig. 2: Unstuffed and shuffled PMT, respectively.

2.4 Encryption Algorithm

In this paper, pixel replacement approach and pixel scrambling approach are used to encrypt the image. So, as a first step, the image will be divided into number of blocks equal N x M blocks as shown in equation.4. Then, the linear independence relationship will be created between the random chaotic blocks to increase the randomness in the image using equation. 5. Where i is the block number from the image and j is the chaotic block from the same image that chosen in the random way to enhance the encryption characteristics by using X-plane from the Rossler chaotic function.

$$Image = \bigcup_{i=0}^{i=MxN} Block_i \quad (4)$$

$$Block_i = Block_i \otimes Block_j, i \in \{1, \dots M\}, j \in \{1, \dots N\} \quad (5)$$

After creating the linear independence relationship between the blocks, the PMT will be used to increase the randomness and the uncertainty in each row. So, to enhance the cipher image the PMT will XOR each row in the cipher image using equation. 6. Where, ROW is the result of the row after applying the XOR operation between the Row and PMT.

$$ROW(J) = Row\ (i) \otimes PMT \quad (6)$$

Finally, the shuffling approach is applied in the resulted image by using Y-plane and Z-plane from the Rossler chaotic function as shown in equation.7. Where, each pixel in the image will be changed depending on the Y-plane and Z-plane from the Rossler function.

$$Pixel(Y,Z) = Pixel(i,j), i \in \{1, \dots M\}, j \in \{1, \dots N\} \quad (7)$$

However, to encrypt the image by using our algorithm the following steps were used:

1- Create a PMT using a logistic map function (Key.1).
2- Divide the image into blocks.
3- XOR each block in the image with another block from the same image that chosen chaotically using the Rossler chaotic function. (Key2(X-plane)).
4- Repeat 1-2 for all blocks in the image.
5- XOR each row with PMT.
6- Shuffle the resulted image using key.3 and key.4, Y-plane and Z-plane, respectively.

2.6 Decryption Algorithm

The decryption steps are the reverse order of the encryption steps as follow:

1- un-shuffle the image using the equation 8.

$$Pixel(Y,Z) = Pixel(i,j), i \in \{N, \dots 1\}, j \in \{N, \dots 1\} \quad (8)$$

2- Xor each Row using equation.6.
3- Solve the linear independence relationship between the blocks using the reverse order, using equation 9.

$$Block_i = Block_i \otimes Block_j, i \in \{M, \dots 1\}, j \in \{N, \dots 1\} \quad (9)$$

2.7 Encryption scheme diagram

Our algorithm is divided into two parts: pixel value replacement by using a PMT, and the Xor operation between the blocks in the image; to change the pixels value, and the shuffling approach; to change the position of the pixel in the image; to increase the uncertainty of the cipher image. Moreover, to shuffle the PMT the logistic map is used, where to chose the chaotic block in the image X-plane from Rossler

function is used, and finally to shuffle the image Y-plane and Z-plane from the Rossler function are used. However, the decryption process is done in the reverse order.

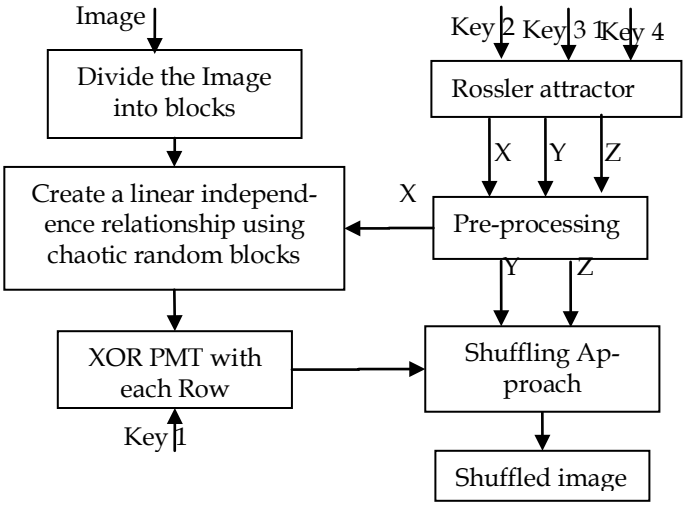


Fig.3: Encryption algorithm diagram

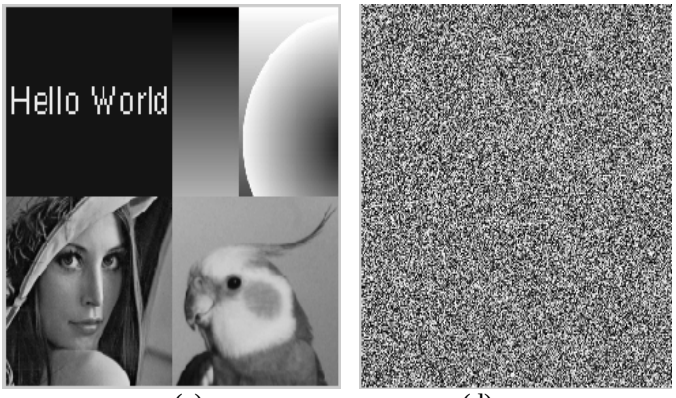
3 EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In our experiment, we used Lena and Montage as tested images with the size 256x256. The original images and the cipher images of the Lena and house are shown in Fig. 4. With input keys Key1= 6x10-14 Key2=1.7829, Key3=1.8963, Key4=1.4624, for two images.

3.1 Keys Space analysis

The key space of our algorithm is depending on logistic map and the Rossler chaotic function space keys. In our algorithm, the key space is calculated as follow: we have four keys key1, key2 and key3,key4 the key space of each one is equal to 10^{15} then the key length of the algorithm is at least 10^{60}.

(a) (b)

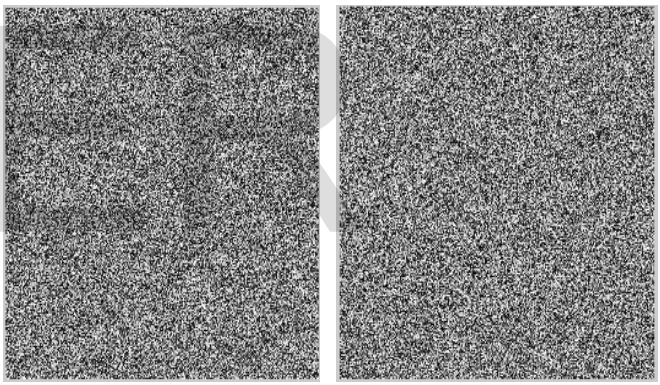


(c) (d)

Fig.4: Encryption for lena and montage images

3.2 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 between the encryption and decryption keys. Our sensitive tests keys are Key1= $7x10^{-14}$ Key2=1.7830, Key3=1.8964, Key4=1.4625, for two images. In which, Fig. 5 shows the decrypted image for the lena and montage tested images by using a wrong decryption keys.



(a) (b)

Fig. 5: Sensitivity tests, decrypted Lena and montage images by using a wrong keys, respectively.

3.3 Information Entropy Analysis

In this part, we test the randomness of our algorithm, where, the true random variable should generate 2^8 symbols with equal probability and the entropy value equal 8. To check, the entropy value of the cipher images, we used a following equation [9]:

$$H(s) = \sum_{s} P(S_i) log \frac{1}{P(S_i)} \qquad (10)$$

Where P (S_i) represents the probability of symbol S_i, in our tests the average entropy of the lena cipher image is 7.9967 and for the montage cipher image is equal to 7.9931, which are very close to the optimal value, then the entropy attack is not possible.

3.4 Histogram Analysis

The cryptanalyst can get very useful information from the image histogram by analyzing it. 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. 6 shows the histogram analysis of lena and house test images and there cipher images, respectively.

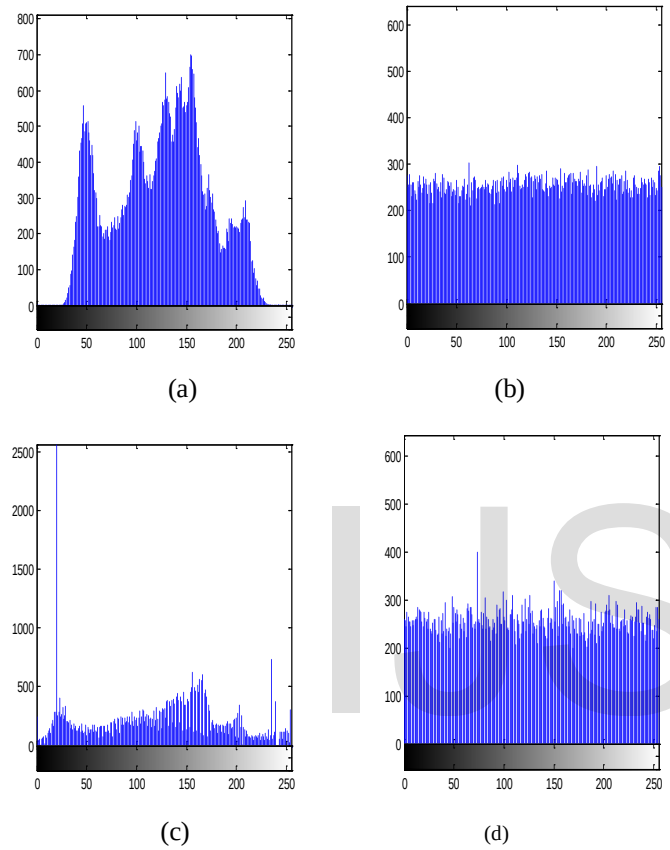


Fig. 6: Histogram of lena and montage and their cipher images, respectively.

3.5 Correlation Analysis

It's known that some algorithm was broken by using correlations analysis between the adjacent pixels. So, we try to study the relations between the adjacent pixels by calculating the correlation coefficient for all possible cases.

The correlation coefficient is calculated by using the following formula [1]:

$$r = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (11)$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x}\ )^2 \quad (12)$$

$$Con(x,y) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x})(y - \bar{y}) \quad (13)$$

Where, M is the total number of randomized pairs, x and y are the two vectors that contains x values and y values of the pair in the tested image, respectively.

Table.1: Correlation coefficients of adjacent pixels

Image / Coefficients	Lena		Montage	
	Plain image	Cipher image	Plain image	Cipher image
Vertical	0.9603	-0.0029	0.9737	-0.0013
Horizontal	0.9257	0.0157	0.9363	0.0026
Diagonal	0.9055	-0.0020	0.9069	-0.0125

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.

3.6 Plain –text sensitivity Analysis

If the cipher image is not sensitive in the changing of the plaintext then the cryptanalyst can get useful information from the encrypted image. Because of this, we have two criteria to study this type of analysis, 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:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MxN} x100\% \quad (14)$$

$$UACI = \frac{1}{MxN}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} x100\% \quad (15)$$

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:

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (16)$$

After calculations, we get the Average NPCR and UACI of lena image are: NPCR = 99.6033 and UACI = 25.0702and that of the house are: NPCR = 99.6109 and UACI = 25.0992. Then our algorithm has a good ability against known plain text attack.

4 Conclusion

In this paper, a new approach to encrypt the image by using a Logistic map and Rossler chaotic functions are proposed. In which, the algorithm used a replacement method and shuffling method together to encrypt the image. Hence; this will increase the reliability of the cipher image. Furthermore, the Logistic map is used; to create a PMT, where, X –plane is used

to create a chaotic linear independence relationship between the image's blocks, where Y and Z planes are used to shuffle the image. Our experimental results show 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. However, we found that UACI for two cipher images are small since the linear independence between the blocks will decrease the differences between the pixels value in different ciphers, therefore, in our future work we try to enhance the UACI for the cipher images.

REFERENCES

[1] H. al-Najjar "Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map" International Arab Conference on Information Technology (ACIT 2011).

[2] H. AL-Najjar "Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location" International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012.

[3] H. AL-Najjar and A. Al-Najjar "Multi-Chaotic Image Encryption Algorithm Based On One Time Pads Scheme" International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012.

[4] H. AL-Najjar and A. Al-Najjar "Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table" International Arab Conference on Information Technology (ACIT 2011).

[5] B. Acharya, S. Patra, and G. Panda," Image Encryption by Novel Cryptosystem Using Matrix Transformation," Int. Conf. on Emerging Trends in Engineering and Technology,pp.77-81,2008.

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

[7] 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, pp. 1 – 6, July, 2010.

[8] 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) pp. 1-5, Dec. 2009.

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

[10] 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) pp. 1-5, Dec. 2009.

[11] K. Rhee," Image Encryption Using Self Regressive Function," Int. Conf. on Networked Computing and Advanced Information Management, pp. 442-445,2008.

[12] R. Rhouma and B. Safya, "Cryptoanalysis of a new image encryption algorithm based on hyper-chaos," Phyiscal Letters A, Vol. 372, pp. 5973-5978, 2008.

[13] 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, pp.583-586, 2009.

Biography

Nadia AL-Rousan was born in Jordan in 1986. She 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 communication and software enginering from Balqa applied university, Irbid, Jordan, 2008. She worked as a teacher asisitance in compter engineering deprtment from 2009 to 2011. Since, February 2012, she has been with the Department of information and computer science, Taibah University, Madina, KSA. Her current research interest is in renewable enrgy with emphasis on sun solar system, network coding, wireless sensor networks, image and data encryption and mobile payment systems.

Hazem 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 information and computer science, Taibah University, Madina,KSA. His current research interest is in wireless networks with emphasis on wireless sensor networks, image and data encryption, grid computing, network coding and mobile payment systems.