Data Hiding in Encrypted Image Based on Multi-Chaotic Approach

Hazem Al-Najjar, Nadia Al-Rousan

Abstract—In this paper, we propose a new data hiding and image encryption algorithm based on chaos theory. Our Approach depends on converting the texts files to pixels value using a logistic map chaotic function then stores the result in the image's border. The image with the hidden data will be encrypted by dividing the image into blocks and create a linear independence between the blocks to change the pixels value using X-plane from the Rossler function. After that, the indices of the columns and rows will be used to increase the randomness in the cipher image. Finally, the image will be shuffled using Y-plane and Z-plane from the Rossler chaotic function. However, by analyzing our algorithm, we show that it's strong against different types of attacks and it's sensitive to the initial conditions.

Index Terms— Image Encryption, Data Hiding, Logistic map, Linear independence, Rossler, shuffling approach,pixel padding.

1 INTRODUCTION

Chaos theory was firstly used in the computer system by Edward Lorenz 1963. The deterministic behavior of the chaos system, initial sensitivity, parameter sensitivity and unpredictability are the main reasons that bring chaos on the information security. Information security is divided into: cryptography and stegnography. In cryptograph, new models and algorithms are used to make data unreadable in the cipher form such as: RSA, DES, IDEA. Where, in stegnography new models and algorithms are used to hide information, data or messages in an image without destroying the image. Moreover, many methods suggested in the literatures to encrypt the images in an efficient way (e.g: less computational time and large key size) by using a chaos systems. Therefore, in [1,8] they 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 image. The one time pads with the logistic map (as a chaotic function) are used in [4] to encrypt the image and increase the size of the encrypted keys. Where, in [7] an improved DES and the logistic map are used to encrypt the image. Others, like [5] proposed new modifications to the Advanced Encryption Standard (MAES) to increase the security level by using a chaotic system. Chaos-based data encryption algorithm for images and videos are proposed by using three chaotic systems to encrypt the image and to enhance the encryption properties [2]. However, security analysis, results and drawbacks of some chaotic cryptosystems are analyzed in [3,6].

Moreover, there are many problems in applying chaos on data hiding and image encryption, such as: the existing number of invalid and weak keys and the keys are not sensitive to the initial conditions. Because of this, we conduct to create a new model to hide the data within the encrypted image using a Rossler and logistic Map chaotic functions, so it's doubly protected from the attackers.

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

The rest of this paper is organized as follows. In section 2, the used chaotic functions are described in detail. The proposed algorithm is presented in section 3. Experimental results and security analysis are presented in section 4. Finally, our conclusions are drawn in section 5.

2 CHAOTIC FUNCTIONS

In the following two chaotic models are discussed in detail to study the features of each model.

2.1 Logistic Map

Logistic map is a chaotic function quantifies the sensitivity of the system to initial conditions. The sensitivity means that small changes in the initial parameters 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 $\lambda \in [3.57,4]$ as shown in Fig. .1. In our encryption algorithm, we used logistic map to convert the data to pixels value by generating the chaotic shifter; to increase the randomness in the hidden data.

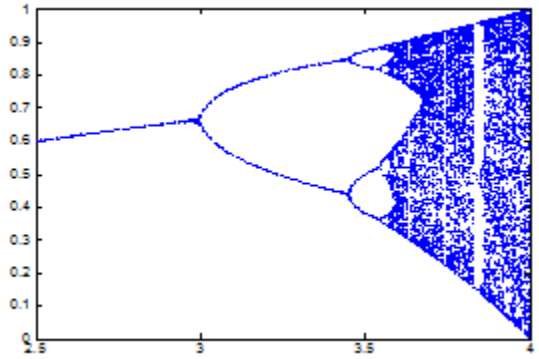

Fig. 1: Logistic map bifurcation

2.1. 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. Moreover, the ordinary differential equation can generate a chaotic behavior under certain conditions, 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 ∈ R, depending on the chaos theory 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: -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. The Rossler attractor with the three dimensional system is shown in Fig. 2. Furthermore, to enhance the Rossler output variables the preprocessing function is used as follow [3]:

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

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

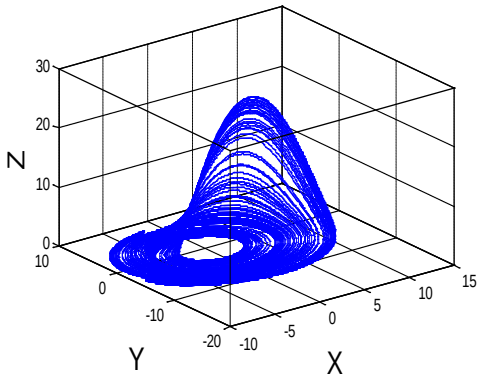

Fig. 2: Rossler attractor

3 Data Hiding in Encrypted Image

Our approach is divided into two phases in the first phase the data will be converted to pixels and in the second phase the image with the hidden data will be encrypted.

3.1 Data Hiding Model

Data hiding is a method to hide large amounts of information within image, audio, text files and videos by using different methods such as Least Significant Bit (LSB). That is defined as the process of replacing the least significant bit pixels of the carrier image with the data hiding bit, so the changing is not noticeable to the human vision.

In this section, we try to design data hiding technique within the encrypted image, so, the data is doubly protected from the attackers. In which, the data hiding algorithm will convert the text file characters to pixel values using the chaotic shifter that generated using a logistic map as shown in equation.4. Where, character is the decimal value of the character in the file, chaotic_shifter is the chaotic value generated using the logistic map and mod is the modulus operation to convert the value to 8-bit grey level.

$$Hpixel = mod\ (\ character + chaotic\_shifter\ ), 256) \quad (4)$$

After that, the converted pixels will be inserted in the container image as a border for the image as shown in Fig. 3. Then, the resulted image will use the proposed encryption method to encrypt the resulted image. However, the total number of data embedded in the image is depending on the image size. For example, if the image size is 256 x 256 then the total number of secret data that can be hidden is equal (2x258+2x256) = 1028 bits in the image only.

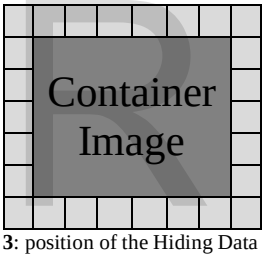

Fig. 3: position of the Hiding Data

3.2 Image Encryption

Image Encryption is divided into two approaches as follows: pixel replacement approach and pixel scrambling approach. In replacement approach, the pixels value is changed, where in the shuffling approach pixels' position is changed. Therefore, in this paper, two approaches are used to encrypt the image with the hidden information. So, as a first step, the image with the hidden data will be divided into number of blocks equal N x M blocks as shown in equation.5. Then, the linear independence relationship will be created between the blocks in the same row to increase the randomness in the image using equation. 6 & 7 with X-plane from the Rossler chaotic function.

$$Image = \bigcup_{i=0}^{i=MxN} Block_i \quad (5)$$

$$Block_1 = Block_1 \otimes Choatic\_block \quad (6)$$

$$Block_i = Block_i \otimes Block_{i-1} \quad , i \in \{2, \dots MxN\} \quad (7)$$

Moreover, the XORing operation between the row indices and column indices will be used to blur image by using equation.8. Where P_{i+1} and P_i are the new and old pixel values, respectively

and J and I is the column index value, row index value of the current pixel after converting them to 8 bits, respectively.

$$P_{i+1}(J) = P_i \otimes J \otimes I \quad (8)$$

Finally, the shuffling approach is applied in the resulted image by using Y-plane and Z-plane from the Rossler chaotic function. Our approach is described as follow:

1- Divide the image into blocks.
2- XOR the adjacent blocks in the same row using chaotic block (Key1(X-plane)).
3- Repeat 1-2 for all blocks in the image.
4- XOR each pixel with its column index value and row index value.
5- Shuffle the resulted image using key.2 and key.3, Y-plane and Z-plane, respectively.

3.3 Data Hiding in Encrypted Image Diagram

The data will be embedded in the image by using the approach in subsection.2.2, and then encrypted using the proposed algorithm in subsection.2.3. Our encryption 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 pixels value, the linear independence relationship between the blocks will be created by using X-plane, then the column and row indices will be used to change the pixels value. Moreover, in scrambling approach the Y-plane and Z-plane were used; to change the location of the pixels. However, the decryption process is done in the reverse order.

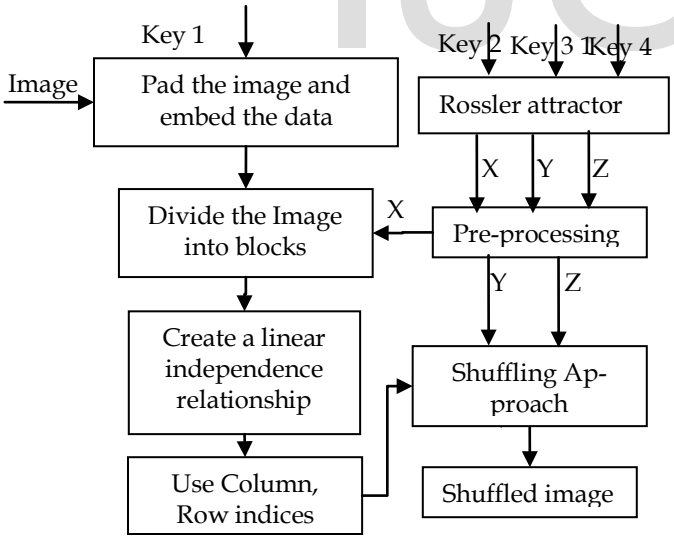

Fig. 4: Encryption algorithm diagram

4 EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

Due to the page limit, only Lena image and Peppers image with a size 256 x 256 are used in our experimental. In Fig.5 (a – b) shows the Lena image and cipher image respectively, where, Fig. 5 (c-d) shows the peppers image and cipher image respectively. With input keys Key2= 1.7814, Key3= 1.8932 ,key4=1.4685 for two images. Where for data hiding algorithm the key1=1x10^{-14}, It is clear that the cipher images are totally different from the plain-text images.

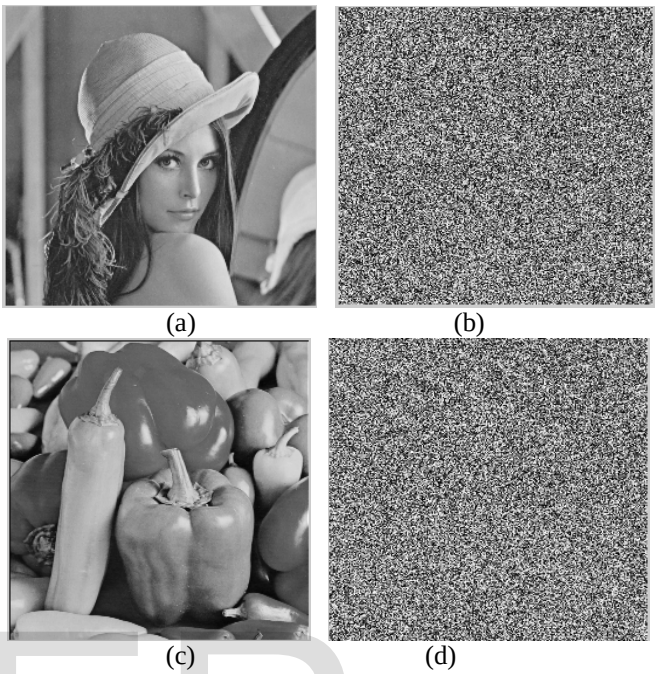

Fig. 5: Encryption for Lena and Peppers

4.1 Keys Space analysis

Key1 is used in data hiding algorithm and Key2, Key3 and Key4 are used in encryption algorithm, the key space of data hiding is equal to 10^{15},where for encryption keys is at least 10^{45}, so it's large enough to resist the brute force attacks.

4.2 Keys sensitivity analysis

A secure image encryption algorithm should be sensitive to the small changes in decryption keys, even a single bit change of keys. Fig.3 shows the decrypted image with different keys Key1=2x10^{-14}, Key2= 1.7815, Key3= 1.8933, Key4=1.4686.

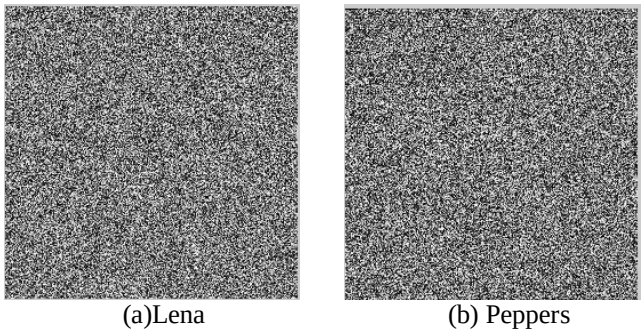

Fig. 6: Sensitivity tests of keys

4.3 Information Entropy Analysis

The entropy is a measure of the uncertainty of the random variables. In which, a true random variable should generate 28 symbols with equal probability and the entropy value equal 8.

Moreover, to check the randomness in our algorithm, we used a following formula as described in [5]:

$$H(s) = \sum_{s} P(S_i) log \frac{1}{P(S_i)} \quad (9)$$

Where P (Si) represents the probability of symbol Si, in our tests the average entropy of the Lena cipher image is equal to 7.9968 and for the Peppers cipher image is equal to 7.9958, which are very close to the optimal value then the entropy attack is not possible.

4.4 Histogram Analysis

It's known that some algorithms were broken by using histogram analysis. Because of this, we try to test our system by drawing a histogram. Where, Fig. 7 shows the histogram analysis for Lena and Peepers images and their cipher images. The histograms of ciphers images are fairly uniform distribution and do not give the user any information about the original images.

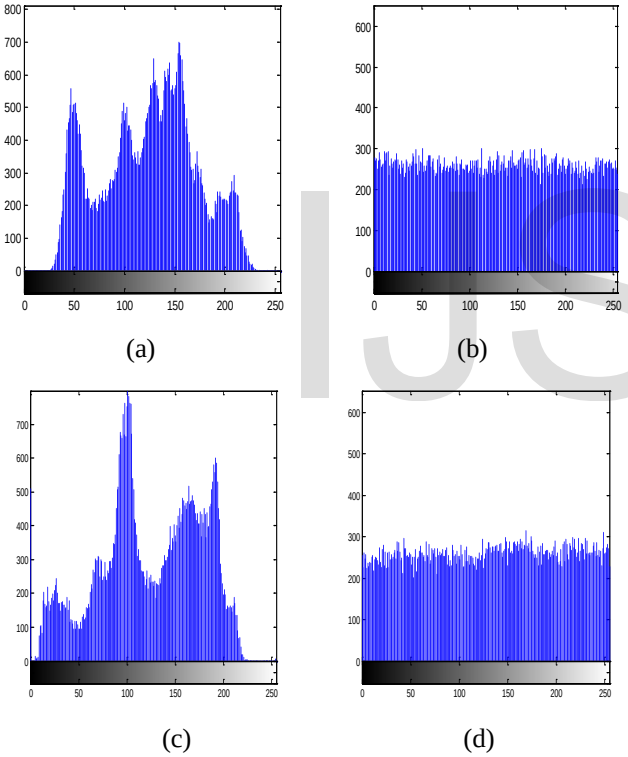

Fig. 7: Histogram of Lena and Peppers and cipher images, respectively.

4.4 Correlation Analysis

It's known that some algorithm was broken by using correlations between two adjacent pixels (in vertical, horizontal and diagonal). For this reason, we try to test our system by using a correlation analysis and by calculating the correlation coefficient.

Furthermore, the correlation coefficient is calculated by using the following formula [5]:

$$r = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (10)$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x}\ )^2 \quad (11)$$

$$Con(x,y) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x})(y - \bar{y}) \quad (12)$$

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		Peppers	
	Plain Image	Cipher Image	Plain Image	Cipher Image
Vertical	0.9603	0.0075	0.9567	-0.0059
Horizontal	0.9257	0.0189	0.9497	0.0068
Diagonal	0.9055	0.0038	0.9147	-0.0045

The results in table.1 show that the proposed method randomized the pixels in very good way.

4.6 Plain –text sensitivity Analysis

The last metric to study is the plain-text sensitively. In which, 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. To check the sensitivity of the plain-text attacks, 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 numbers between two cipher images and UACI defined as an average intensity of differences between two cipher images as defined in the following:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MxN} x100\% \quad (13)$$

$$UACI = \frac{1}{MxN}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} x100\% \quad (14)$$

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 follows:

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (15)$$

After calculations, we get the Average NPCR and UACI of Lena image are: NPCR = 99.6429 and UACI = 25.4318 and that of the Peppers are: NPCR = 99.6170 and UACI = 25.125. Then our algorithm has a good ability against known plain text attacks.

5 Conclusion

In this Paper, we used a chaos theory in order to hide the data within the encrypted image by converting the data to pixels and storing the result in the border of the image using key1 from the logistic map. Where, the encryption phase begins by creating a linear independence relationship between the blocks of the image using key2 from Rossler chaotic function then used a column and row index value to change the pixels value. After that, the image will be shuffled using key3 and key4 from the Rossler chaotic function. However, we show by experimental results that our algorithm is sensitive to initial conditions and strong against the brute force attacks. Finally, after some tests like entropy analysis, statistical analysis and plain-text sensitivity, we show that our algorithm has a high security against different types of attacks.

References

[1] Ying-yu C. and Chong Fu,"An image encryption scheme based on high dimension chaos system," Int. Cof. Intelligent computation technology and automation, pp. 104-108, 2008

[2] Ching-kun C., Chun-liang L. and Yen-Ming C. "Data Encryption using ECG Signals with chaotic Henon map," Int. Conf Information Science and Applications (ICISA), Seoul, pp. 1 – 5,April. 2010.

[3] Xiang D., L. X. and Wang P, "Analysis and improvement of a chaos image encryption algorithm," Chaos, Solution and Fractals, vol. 40, pp. 2191-2199, 2009.

[4] Ching J., 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.

[5] Min L. and Li T., "A chaos –based data encryption algorithm for image/video," Int. Conf. on Multimedia and information technology, pp 172-175, 2010.

[6] L. Shujun, L. Chengqping and C. Guangrong, G. Nikolas, L. Kwok-Tung. "A general quantitative cryptoanalysis of permutation-only multimedia ciphers against attacks," Signal Processing: Image Communication, no 23, pp. 212-223, 2003.

[7] Z. Yun-Png, Z. jun, L. Wei, N. Xuan C. Ping and D. di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES," Int. Conf. On System, Man and Cybernetics, San Antonio,TX, USA, pp.474-478, October. 2009.

[8] Hazem N. "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.

Biography

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.

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.