New Chaotic Information Security Algorithms

Hazem Al-Najjar, Nadia Al-Rousan
College of Bader, Department of Computer
Taibah University, Madina, KSA

ABSTRACT
In this paper, new information security algorithms using a Rossler chaotic function are suggested, which contain image encryption, data encryption and data hiding. In designing the image encryption algorithm, a chaotic block was used to change the pixels value using the target pixels in each block. The experiments show that the system performance is improved and the cipher image characteristics are enhanced. Where, in the data encryption algorithm N x N blocks were used to encrypt the text files, so each character in the file will represent one generated block. The experiments show that the system is efficient and fast in encrypting the large text files but the size of the encrypted file will be increased dramatically since the characters will be converted to nine bits. On another hand, the data hiding algorithm is designed using chaotic block which improves the PSNR of stego-images. However, the suggested algorithms show that using the chaotic functions and N x N blocks will enhance and improve the information security.
.

General Terms
Security, Algorithms, Image, Encryption, Chaos theory.

Keywords
Image encryption, Data encryption, Data hiding, Rossler Chaotic function

1. INTRODUCTION
Information security is divided into two types: cryptography and stegnography. In cryptograph, new models and algorithms are used to make the data unreadable in the cipher form, therefore many methods to encrypt the data had been proposed by the researchers such as: RSA, DES, IDEA, to send the data in the garbage form, so the sniffing to these data is unreadable. Where, in stegnography new models and algorithms are used to hide information, data or messages in an image without destroying the image and by faking the human vision.

Chaos theory is one of the most important theories that used in the new information security systems. Hence, the system's characteristics like sensitivity to the initial conditions and unpredictability to the chaotic sequences will improve the security systems. In addition, many researchers try to design information security systems by using chaos function such as: logistic map, Lorenz attractor, Henon map and Rossler attractor. Xu. et al. [1] divided the image into blocks and tried to use a permutation on each block by using a logistic map to encrypt the image. Electrocardiogram (EGC) signals of the persons are used to generate the encryption keys and to encrypt the data (like password) by extracting their features using Honen map as a chaotic system [2]. Where, in [3] they used two one-dimensional discrete Chebyshev chaotic sequences for row and column shuffling for each pixel on the original image. Nien et. al. [4] proposed an encryption method that used multi- chaotic systems to increase the key space and to make system's breaking very difficult. Zhu. et. al. [5] 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. Where, the one-time pads with the logistic map (as a chaotic function) are used in [6] to encrypt the image and to increase the size of the encrypted keys. 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].

Finally, our contribution in this paper is to use the chaotic function and N x N blocks to encrypt the image and data and to hide the data in the images; to increase the algorithm's strength and to enhance the encryption system.

1.1 Rossler Chaotic Function
Chaos theory was mainly presented to be used in a computer technology in 1963 by Lorenz. Lorenz defined the chaos as a relation between three differential equations with two nonlinear terms which increase the complexity and the execution time of the system. Because of this, Rossler modified the Lorenz equations and defined the chaos using one nonlinear term as shown in equation.1. The ordinary differential equation can generate a chaotic behavior under certain initial values (x_0, y_0, z_0) or called initial conditions.

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \quad (1)$$

x, y, z, t, a, b and c $\in R$, and $\dot{x}$ is the derivative 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. The classic chaotic attractor is defined (shown in Figure.1) as follow a, b, and c as 0.15, 0.20 and 5.7, respectively. But, before using the chaotic sequences, the ranges of the chaotic output should be modified by pre-processing the X, Y and Z values as discussed in [5]:

$$M(i) = 10^n M_n(i) - round\left(10^n M_n(i)\right) \quad (2)$$

In which, n is the right shift the number M(i) n digits and M is the plane to enhance x, y or z. After, using equation 2 for X, Y and Z, the range of the planes were modified. The modified values will be used to generate a chaotic grid and 3x3 blocks that used in the information security. So, to hide the data and to encrypt the image, the chaotic grid will be used. Where, to encrypt the data 3x3 blocks will be used.

1.2 Choatic Grid
The chaotic grid is a grid with NxN size and N targets, in each column there is one target that generated using Rossler chaotic function. Where, the chaotic block is a block which contains numbers from 1-8 that distributed in the block using a Rossler function. For example, in Figure.2 the chaotic grid with the size 3x3 and 3 targets are generated using a Rossler

chaotic function. Therefore, after defining the targets in the grid, the targets will be used to change the value in the pixels using equation.3.

$$Pixel_i = Pixel_i \otimes Pixel_{target} \quad (3)$$

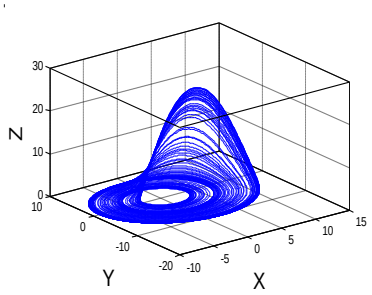

Figure.1: Rossler attractor

Where, i is the index in the same column. On another hand, the 3x3 blocks will be generated using the Rossler chaotic function. So, after generating the chaotic form the character's bits will be shuffled depending on the form.

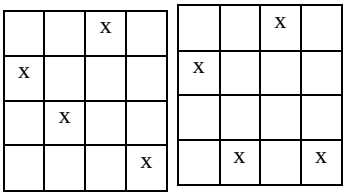

Figure.2: Chaotic grid two different solutions.

1	2	3
4	5	6
7	8	

a

4	2	3
8	1	5
6	7	

b

Figure.3: The 3x3 block, a: arrange form b: shuffled form.

The rest of the paper is organized as follows: In Section II, proposed information security models. The experimental results and security analysis are discussed in Section III. Finally, the conclusion is drawn in Section VI.

2. Proposed Information Security Models

2.1 Image Encryption

Image is type of data that visualize the information using small elements called pixels. Image encryption is a method to make the image unreadable in the garbage form so to encrypt the image the pixels need to be modified using pixel replacement approach or/and pixel scrambling approach. In pixel replacement approach, the pixels value is changed, where in pixel scrambling the position of the pixels is changed. In this section, the chaotic grid is used with the chaotic function to encrypt the image using a shuffling and replacement approaches. Furthermore, the encryption algorithm will divide the image into blocks with the size N x N. Each block contains N targets to create a linear independence relationship in each column. So, to generate a linear independence in each column within the block equation.4 is used, where to generate the relations between the blocks equations.5&6 are applied by using X-plane from the Rossler chaotic function and finally the resulted image will be shuffled using the Y-plane and Z-plane from the Rossler chaotic function.

$$Pixel(i,j) = Pixel(i,j) \otimes Pixel(Target) \quad (4)$$

$$Block(I,J) = Block(I,J) \otimes Chaotic\_Block(I,J) \quad (5)$$

$$Chaotic\_Block(I,J) = Block(I,J) \quad (6)$$

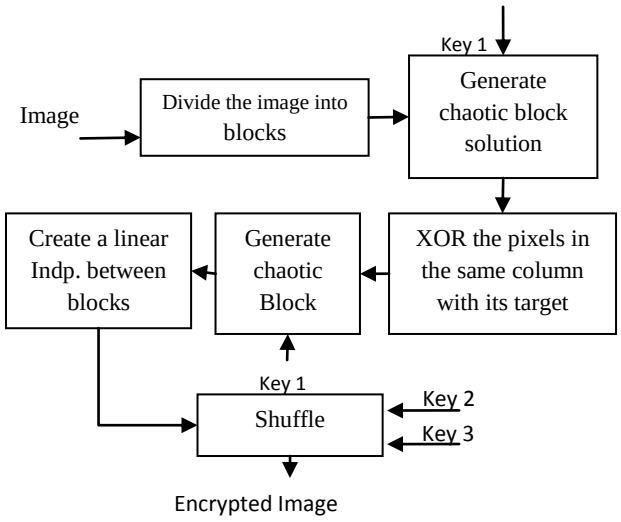

Figure.4: Proposed encryption algorithm

The proposed image encryption algorithm used replacement and shuffling approaches as shown in figure.4. The image will be divided into blocks with the size equal N x N. In each block, the generated chaotic block will create a linear independence relationship between the target intensity pixel and the other pixels in the same column. After that, another chaotic block is generated and Xored with the first block to create a linear independence relationship between blocks, so no block can be decoded without the previous one. Finally, the image will be shuffled to randomize the image and to increase the uncertainty in the encrypted image using Y and Z planes from the Rossler chaotic function.

2.2 Data encryption

In this subsection, the 3x3 blocks that contain numbers from 1-8 (Figure.3) generated by using the Rossler chaotic to design a new data encryption algorithm for the text files. Moreover, to encrypt the text files the following steps are used as discussed in Figure.5.In the first step, the files will be divided into equally blocks that have the same number of characters and then shuffle the

Table.1: Data encryption example

Data / Operation	h		e	l	l	o
Convert to Binary	1001000		1100101	1101100	1101100	1101111
Shuffle the characters (3x3 box)	001001110		001011111	100101111	110111010	101111111
Combine 8 bits together	4	226	252	127	117	127
Create a Linear indep. using X= 210	185⊗ 4 189	91 ⊗226 185	167 ⊗252 91	216 ⊗127 167	173 ⊗117 216	127 ⊗210 173
Y chaotic values	111	68	34	127	47	20
Y XOR Linear_ Independence	210	253	121	216	247	185
Shuffle	185	247	210	121	253	210
Character representation	¹	÷	Ò	Y	ý	Ò
Encrypted file	¹÷ÒyýÒ					

character's bits in each block using a 3x3 generated block (key 1). The resulted data will be used in the next step to create a linear independence relationship between the characters in the same block (key 2) by using equations 7&8. After that, the key3 is used to Xor each character in the block with the corresponding one. Finally, the file data will be shuffled by using key2 to generate the encrypted file. To simplify the idea example.1 is discussed.

Character1 = character 1 ⊗chaotic_value (7)

Characteri+1 = characteri ⊗characteri+1 where i>1 (8)

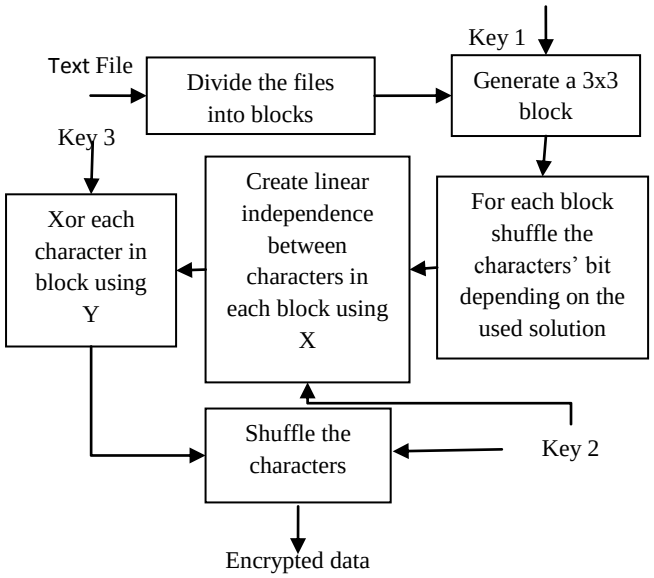

Figure.5: Data encryption algorithm

Example.1: assume the file which contains the word "hello", the block size is one and the unused bits are 8 and 9. For simplicity, we try to create a linear independence between the blocks only. The example is fully shown in Table.1.
In the first step, the characters will be converted to the binary data and the Z-plane from the Rossler function will be used to generate 3x3 shuffled blocks to shuffle and to convert the characters into 9 bits. Then the binary data will be grouped to 8 bits each and by using the chaotic X-plane from the Rossler function a linear independence relationship will be created between the characters. The Y-plane is used to hide the key from the last step, where the shuffling approach (by using X-plane) is applied to increase the uncertainty in the text file. Therefore, by applying proposed data encryption algorithm in the "hello" text file, the encrypted file will be as follow "¹÷ÒyýÒ", where 6 characters are generated. Where, for decrypting the file the reverse order will be used.

2.3 Data Hiding

Data hiding is a method to hide large amount of information within image, audio, text files and videos. Normally, the data hiding is used with the cryptograph methods, so it is doubly protected from the attackers. In addition, there are many methods to hide the data such as Least Significant Bit (LSB), which replace the least significant bit in the pixel of the carrier image with the secret bit, so the changing is not noticeable to the human vision.
In this section, the chaotic grid and LSB method will be used to design a data hiding algorithm. So, as a first step, the image will be divided into number of blocks that equal N x N where N is the maximum number of data to be hidden in the block. Moreover, the Rossler chaotic function will be used as a chaotic generator as follow: X-plane will be used to shuffle the secret data before embedded the secret data. After shuffling the secret data, the targets will be generated by using Y-plane, where Z-plane is used to choose which target in the block to embed the data. The chosen pixel will be modified by using LSB. Finally, this process will be repeated to the whole image until all the secret data are embedded.
However, the total number of data embedded in the image is depending on the image and block size. For example, if the image size is 256 x 256 and the block size is 8x 8 then the total number of secret data that can be hidden is equal to (32x32) x 8 = 8192 bits in the image only. The proposed model is shown in Figure.6.

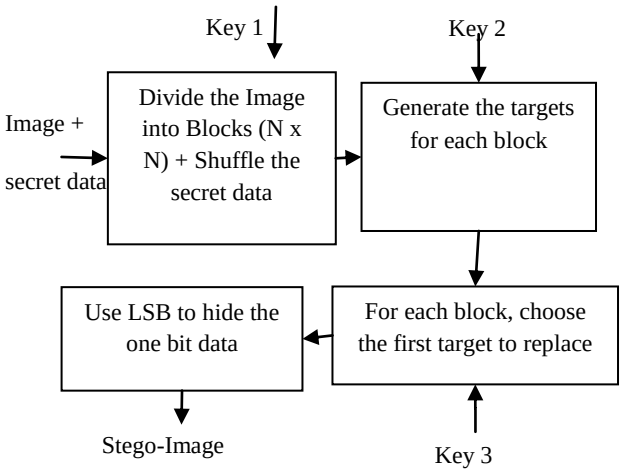

Figure.6: Data hiding algorithm.

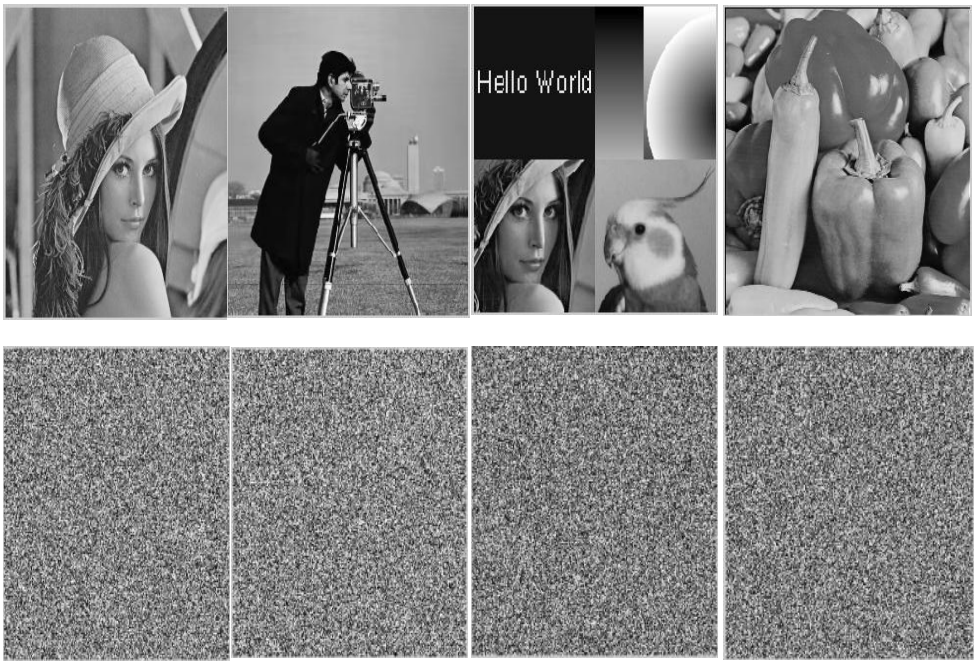

Figure.7: Image Encryption after applying our system, lena, cameraman, montage, peppers.

3. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this section, the three algorithms will be evaluated, in which, the experiments evaluate the ability of the proposed methods; to encrypt the images in the effective way, to encrypt the data and to hide the secret data in the image. So, Lena, Cameraman, Montage, and the Peppers with the size 256x256 are used, as tested images to test the proposed image encryption algorithms.

3.1 Image Encryption

The cipher and original images of the lena, cameraman, montage and peppers are shown in Figure.7, respectively. With input keys Key1= 1.233, Key2= 1.2831 and Key3 =1.3682 for all images.

3.1.1 Keys Space analysis

The key space of our algorithm is depending on the three planes of the Rossler function and the number of targets. So, if the number of possible solutions for the N targets is equal to M then the total key space for the algorithm is equal to $Mx10^{15}$ $x10^{15}$. In which, 10^{15} is a key space analysis for the X and Y-planes, where Z-place is the number of solution for N targets.

3.1.2 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 in the decryption keys. Our sensitive tests keys are as follow: Key1= 1.234, Key2= 1.2832 and Key3 =1.3683. The experiments show that the image can't be retrieve by using a small changing in the decrypted keys. Since, the Rossler chaotic function is highly sensitive for the small changing of the initial conditions and will generate completely different output sequences.

3.1.3 Information Entropy Analysis

The true random variable should generate 28 symbols with equal probability and the entropy value equal 8. Therefore, to evaluate the information entropy and calculate the entropy value, we used a following equation [10]:

$$H(s) = \sum_{s} P(S_i) \log \frac{1}{P(S_i)} \qquad (8)$$

Where P (Si) represents the probability of the symbol Si, in our tests the average entropy of the cipher images for the tested images are 7.9973, 7.9875, 7.9960 and 7.9809 for lena, cameraman, peppers and montage, respectively, which are very close to the optimal value, then the entropy attack is not possible.

3.1.4 Histogram Analysis

The good encryption algorithm should generate uniformly distribution of the histogram, so the attacker can't get any useful information by using image's histogram. In our tests, it's very difficult to get any information from the histogram. Figure.8 shows the histogram analysis of lena, cameraman, peppers and montage images and theirs cipher images, respectively.

3.1.5 Correlation Analysis

Using a correction analysis for some image encryption algorithms could be useful to attack and break the encryption algorithm. For this, we try to test our system by calculating the correlation coefficient for all possible cases in vertical, horizontal and diagonal adjacent.

Where, the correlation coefficient is calculated by using the following formula [10]:

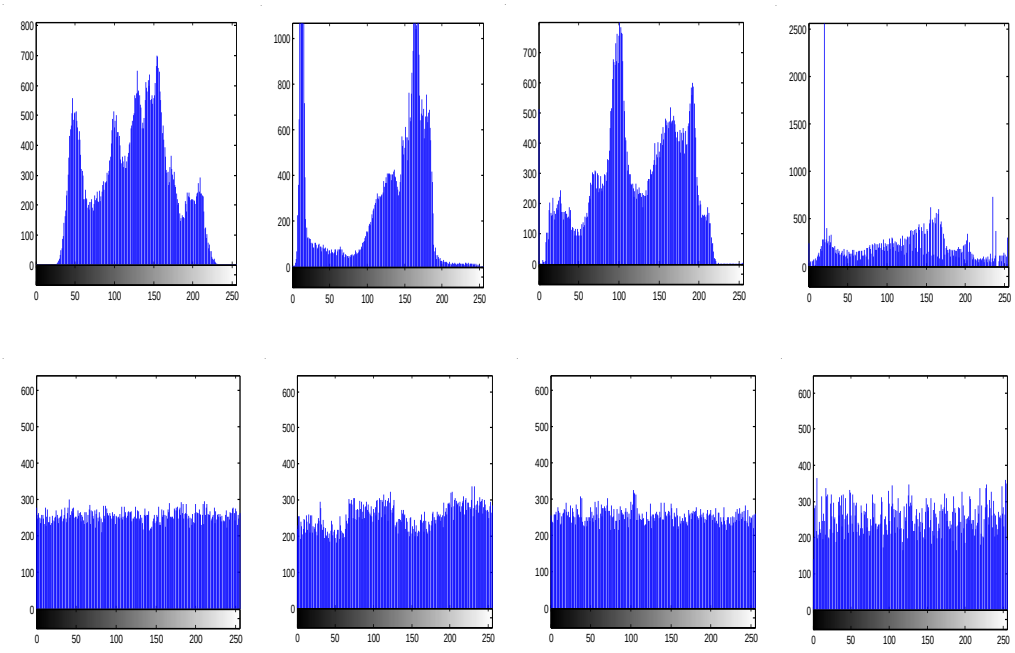

Figure.8: Image histogram after applying our system, lena, cameraman, montage, peppers.

$$r = \frac{Cov(i,j)}{\sqrt{D(i)}\sqrt{D(j)}} \quad (9)$$

$$D(i) = \frac{1}{M}\sum_{i=1}^{M}(i - \bar{i}\,)^2 \quad (10)$$

$$Con(i,j) = \frac{1}{M}\sum_{i=1}^{M}(i - \bar{i})(j - \bar{j}) \quad (11)$$

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.2: Correlation coefficients of adjacent pixels

Image	Lena		Peppers	
Coefficients	Plain image	Cipher image	Plain image	Cipher image
Vertical	0.9603	-0.0081	0.9567	0.0072
Horizontal	0.9257	-0.0025	0.9497	-0.0140
Diagonal	0.9055	-0.0041	0.9147	-0.0019
Image	**Cameraman**		**Montage**	
Coefficients	**Plain image**	**Cipher image**	**Plain image**	**Cipher image**
Vertical	0.9607	-0.0065	0.9737	-0.0089
Horizontal	0.9381	0.0033	0.9363	0.0094
Diagonal	0.9115	0.0068	0.9069	-0.0039

Table.2 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 an efficient way.

3.2 Data Encryption

Our data encryption algorithm considered as a symmetric key algorithm. In addition, the key space of data encryption algorithm is depending on the Rossler function and the size of the bit shuffling block. For example, the number of solutions for the 3x3 blocks is equal to 9!, where the key space of the Rossler planes is equal to 10^{30}. So, the key space for the algorithm is equal to 9! X 10^{30}. On another hand, the size of the encrypted text is larger than the original text, since it depends on the box size.

3.3 Data Hiding

In the proposed data hiding algorithm, the data will be hidden in the above images to test the system performance. So, by using the proposed system, the total number of data to be hidden in the image is depending on the number of targets and the image size. Then, if the image is divided into M blocks and 8 x 8 board are used, the total number of data that can be hidden in the image will be equal to M x 8. In our experiment, four images are used and the PSNR (signal to noise ratio) is calculated for the tested images and the results are as follow: 63.1191, 63.0466, 63.3775 and 64.2490 for lena, cameraman, peppers and montage, respectively.

4. CONCLUSION

In this paper, we used a Rossler chaotic function with the chaotic grid and the N x N random blocks, to build new information security algorithms, which includes image encryption, data encryption and data hiding algorithms. Therefore, to encrypt the image and to hide the data, Rossler chaotic function with the chaotic grid is used. Where, to encrypt the data Rossler chaotic function with N x N random block are used. However, the experimental results show that the proposed algorithms are sensitive to initial conditions and strong against the brute force attacks. After some tests such as entropy analysis, statistical analysis and visual analysis, we show that our algorithms have a high security against different types of attacks.

5. REFERENCES

[1] E .Xu; L. Shao, G. Cao , Y. Ren and T. Qu. "A New Method of Information Encryption," Int. Colloqu'ium on Computing, Communication, Control, and Management, 2009, pp.583-586.

[2] A. A. Shtewi, B. Hasan, A. Hegazy. "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems," Int. Journal of Computer Science and Network Security, vol. 10 no. 2, February 2010.

[3] 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.

[4] 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.

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

[6] 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.

[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] Xing-Yuan, Wang, and Liu Lin-Tao. "Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices." Chinese Physics B 22.5 (2013): 050503.

[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] N. Al-Rousan and H. Al-Najjar. "Digital Image Encryption Algorithm Based on Chaotic Block and Pixel Mapping Table," International Journal of Computer Theory and Engineering, Vol. 4, No.6, June 2013.

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 engineering from Balqa applied university, Irbid, Jordan, 2008. She worked as teacher assistance in computer engineering department 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 energy with emphasis on sun solar system, network coding, wireless sensor networks, image and data encryption and mobile payment systems.