

Image Encryption Approach based on Chaotic Image Random Key Generating

Abdulrahman Dira Khalaf¹,

Ali Makki Sagheer²

¹ College of Administration & Economics, ² College of Computer Science & Information Technology

University of Fallujah-Iraq

University of Anbar- Iraq

adk1973@gmail.com

ali_makki@uoanbar.edu.iq

Abstract

An image encryption approach is proposed in this paper. In the beginning initial random numbers algorithm is generated by linear dynamic system using Lorenz map. It is one of chaotic mapping which can give us more suitable random numbers according to initial values. Then, random image key algorithm is proposed to generate new values to use in encryption algorithm. The size of key can be the same size or less than of plain image. At the end block cipher is applied to generate a new cipher from color image which has three channels R, G and B; where, each channel is encrypted by using XOR with image key. Cipher image is sent to the receiver through a public channel, while the initial values are sent through secure channel to avoid the hackers to discover the origin image. The sharing key is used for decoding these images. This technique is a recent approach to reduce the computational requirements for huge volumes of images with a good level of security. Good results have been obtained for encryption and decryption sample of images. Statistical tests are taking into consideration to know the efficiency of this approach, in addition, analysis of space and sensitive key show the power of proposed algorithm for encrypt and decrypt image.

Keywords: Encryption; Decryption; Random Image; Lorenz Map; XOR

I. Introduction

The field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding [1]. Image encryption can be implemented with full encryption or partial encryption. Full encryption encrypts all the components of image while the partial encryption deals with a part of image to encoded features [2]. However, many of these are not secure as they are based exclusively on random permutations making them vulnerable to known or chosen-plaintext attacks [3]. Recently, and many different image encryption methods have been proposed to enhance the security of these images, image encryption techniques try to convert an image to another that is hard to understand [4].

II. Literature Review

Many researches are introduced about image encryption using chaos theory and random key generation. Alsafasfeh Q, Arfoa A. (2011) proposed an image encryption technique based on chaotic theory using two chaotic maps: the Lorenz chaotic system and the Rössler chaotic maps. This technique gives a secure manner as shown in the encryption tests [5]. El-Sayed M. El-Alfy and Khaled A. Al-Utaibi (2011) proposed a technique based on chaotic maps and genetic operators for encrypting color images. The capability of this technique to generate cipher images with low correlation coefficients of adjacent pixels is demonstrated through some experimental results for several benchmark images. It is also shown that the approach is sensitive to any slight changes in the secret key values [6]. Hazem Mohammad Al- Asem AL-Najjar and Mohammad AL-Najjar (2012) proposed an image encryption technique using multi-chaotic attractors to enhance the encryption technique and to increase the complexity of this system to break it [7]. Shoaib Ansari, Neelesh Gupta, and Sudhir Agrawal proposed a cryptography technique based on chaotic map, in the technique; confusion and diffusion are applied on spectral domain on Discrete Cosine Transform (DCT) coefficients, hence, the encryption can be achieved quickly without applying the large number of confusion and diffusion cycle as it is needed in spatial domain. The diffusion template is created by random number generator based on Gaussian distribution. The results proved its robustness with all type of cryptanalytic tests and faster execution [8]. Chaitanaya G. et al (2015) applied the chaotic encryption and chaotic decryption on an image by doing pixel shuffling and using chaotic maps. Chaotic nature ,i.e., randomness property is present in both Henon map and Arnold cat map. Pseudorandom values generation plays an important key role in Henon maps and iteratively pixel shuffling is done in Arnold cat map. A sorting Technique is followed on key values produced by Henon map. By using those sorted positions, shuffle the pixel values are generated by Arnold cat map iteratively. In this way the images are provided with good security for confidential transmission [9].

III. Lorenz Chaotic Attractor

The Lorenz Chaos System of equations is perhaps the first of the nonlinear dynamical systems found to exhibit sensitive dependence on initial conditions and chaos. The Lorenz system is described by the following nonlinear differential equations;

$$\frac{dx}{dt} = a(y - x) \quad (1)$$

$$\frac{dy}{dt} = rx - y - xz \quad (2)$$

$$\frac{dz}{dt} = xy - bz \quad (3)$$

Indeed the Lorenz attractor has played this role in the modern theory of dynamical systems, as the researcher will try to explain. The Lorenz dynamics feature an ensemble of qualitative phenomena, which are thought today, to be present in “generic” dynamics. See figure 1 [10].



Figure 1: The Lorenz attractor

I. Proposed Image Encryption Model

The proposed approach is designed according to two concepts. The first concept generates three random matrices from initial values depending on chaos theory using Lorenz dynamic equation. The second concept converts these matrices into three vectors after making a summation for each row and column, then concatenating these vectors to get three matrices depending on doubles values and string operations to create new values which are used to generate three keys. Random key generating using Lorenz equations proposed as algorithm 1.

Algorithm 1:

1. Read the parameters of Lorenz equations (1, 2 and 3) where $a=10$, $r=28$, $b=8/3$ and $h=0.01$.
2. Input L , x_0 , y_0 and z_0 where: L is the length of one dimension of square matrix.
3. Let $im(1,:) = [x_0 \ y_0 \ z_0]$ represents pixels components image for R, G and B.
4. Let $i = 2$
5. Let $F(1)$, $F(2)$ and $F(3)$ represent to variables of x , y and z respectively. Compute x , y and z
While $i \leq n \times m$
 $F(1) = a \times im(i-1:2) - im(i-1:1)$
 $F(2) = r \times im(i-1:1) - im(i-1:2) - im(i-1:1) \times im(i-1:3)$
 $F(3) = im(i-1:1) \times im(i-1:2) - b \times im(i-1:3)$
 New values of x , y and z will be computed by $im(i,:) = im(i-1,:) + h \times F$
6. End while
7. Convert x , y and z into 2-dimensions matrices
8. End

When $L=256$ Lorenz equations give a good results for random values but take a long time to execute it. For example when running this algorithm to generate a vector that has 65536, it takes a long time rather than $L=128$ to generate a vector that has 16384 therefore, key generating algorithm proposed in this paper to reduce the execution time as shown in algorithm 2.

Algorithm 2:

1. Input initial matrices x , y , z which are generated from algorithm 1
2. Compute summation of each row in x , y and z and save as $A1$, $A2$ and $A3$ respectively.
3. Compute summation of each Column in x , y and z and save as $B1$, $B2$ and $B3$.
4. $C1 = A3 \times B2$, $C2 = A1 \times B3$, $C3 = A2 \times B1$.
5. Concatenate the vectors from step 2-4 to generate three matrices A , B and C .
6. Expand A , B and C to $S1$, $S2$ and $S3$ where $S1 = A1:A5$, $S2 = B1:B5$, $S3 = C1:C5$.
While $i \leq 5$
 $A_i = \text{mod}((A_i - A_{i-1}), 1000)$
 $B_i = \text{mod}((B_i - B_{i-1}), 1000)$
 $C_i = \text{mod}((C_i - C_{i-1}), 1000)$
 $i=i+1$
End while.
7. Repeat step 6 until getting the keys.
8. End.

To explain how this algorithm works, let $m = 2$ and $n = 2$ representing two dimensions. In the beginning, three matrices ($M1$, $M2$ and $M3$) are generated depending on Lorenz equations (1-3) as shown in table 1.

Table 1: Representing three matrices generated by using Lorenz equations

2D array of M1,M2 & M3		1 st column	2 nd column	Σ of columns
M1	1 st row	0.7565000000000000	0.717005002050000	1.473505002050000
	2 nd row	0.7251700000000000	0.728655853556549	1.453825853556549
Σ of rows		1.4816700000000000	1.445660855606549	
M2	1 st row	0.4432000000000000	0.833513517115493	1.276713517115493
	2 nd row	0.6435200205000000	1.019536461282709	1.663056481782709
Σ of rows		1.0867200205000000	1.853049978398202	
M3	1 st row	0.9343000000000000	0.893065071697104	1.827365071697104
	2 nd row	0.912738141333333	0.875226336728996	1.787964478062329
Σ of rows		1.847038141333333	1.768291408426100	

Arrays of M1, M2 and M3 which are generated from input values of $x = 0.7565$, $y = 0.4432$ and $z = 0.9343$. A1, A2 and A3 are new vectors represent summation of rows as shown in figure 2, while B1, B2 and B3 which represent summation of columns where:

A1=[1.473505002050000,1.453825853556549] B1=[1.481670000000000,1.445660855606549]
 A2=[1.276713517115493,1.663056481782709] B2=[1.086720020500000,1.853049978398202]
 A3=[1.827365071697104,1.787964478062329] B3=[1.847038141333333,1.768291408426100]

Only five digits are selected from each one of these double vectors after removing a dot and replacing the white spaces in these vectors by 1:

A1 = '14735' '14538', B1 = '14817' '14457' A1='14735' '14538', B1='14817' '14457'
 A2 = '12767' '16631', B2 = '10867' '1853' A2='12767' '16631', B2='10867' '11853'
 A3 = '18274' '1788', B3 = '1847' '17683' A3='18274' '11788', B3='11847' '17683'

The second stage is to generate three vectors C1, C2 and C3 as shown in figure 2 where:

$C1 = A1 \times B1$, $C2 = A2 \times B2$ and $C3 = A3 \times B3$.

A1=[14735 14538] , B1=[14817 14457] C1=[50649 85973]
 A2=[12767 16631] , B2=[10867 11853] C2=[65858 19116]
 A3=[18274 11788] , B3=[11847 17683] C3=[25245 18914]

For more random A, B and C are re-arranged where $A=[A1, B2, C3]$ $B=[A3, B1, C2]$ and $C=[A2, B3, C1]$. These vectors have two values and have 15 digits where $A=[147351086725245 145381185318914]$, $B=[182741481765858 117881445719116]$ and $C=[127671184750649 166311768385973]$. In the next stage, vectors values of A will be divided into 5 values with 3 digits as shown in table 2 to get Y value which has three digits, then Y is returned to A as a new value. So, the same procedure will be run for B and C.

Table 2: Cutting numbers of A into 5 values

X=A	147351086725245	147351086725	147351086	147351	147
	145381185318914	145381185318	145381185	145381	145
Y	245	725	86	351	147
	914	318	185	381	145

Expanding matrix needs factor value, let us call it Fr, where: $Fr = \lceil 3L/15 \rceil$. When $L=2$ then $Fr=1$, this means the matrix will not expand from (2×15) to be (2×45) , because the proposed

ISI : 000000000

www.IJBICT.com

algorithm is designed to expand key matrix when L is greater than or equal to 6. Therefore only 15 values will have keys matrix. Expanding matrix is used XOR between the components of A, B and C to return new values of these components where $A = B \oplus C$, $B = A \oplus C$ and $C = A \oplus B$ then all values are made with 256 to create three keys in which each of their values should be between (0 and 255); let us call K1, K2, and K3 and let K1', K2' and K3' representing transportation matrices. At the end, XOR between them will generate three keys; let us call key1, key2 and key3.

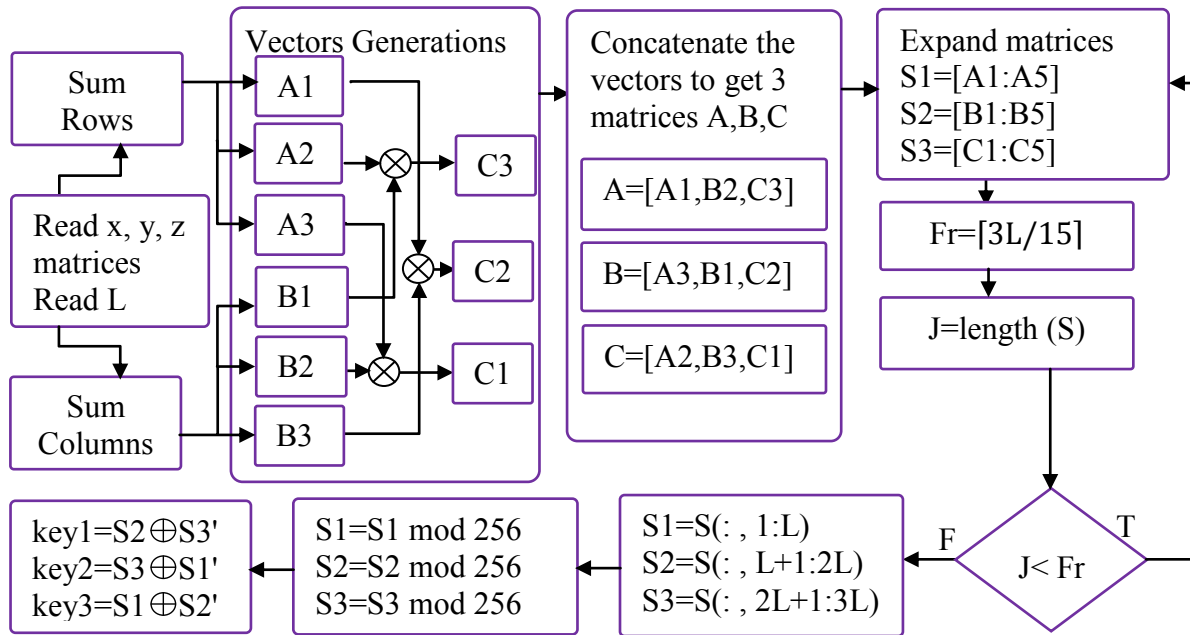


Figure 2: Proposed key generating algorithm

Finally, authors proposed algorithm 3 to complete the encryption of image as following steps:

1. Input RGB image.
2. Extract R, G and B channels from RGB image.
3. Let IR represents the key size according to L in algorithm 2.
4. Let $k_1 = \text{length of IR}$ and $k_2 = \text{length of R}$ then $k = k_2 / k_1$ represent the number of blocks of image encryption for R component such as:
 - $ER = R \oplus IR$, when $i=1$
 - $ER(j) = R(j) \oplus IR(j)$ for $j = 1, 2, \dots, i$, when $i = 4$
 - $ER(j) = R(j) \oplus IR(j)$ for $j = 1, 2, \dots, i$, when $i = 8$
 - \vdots
 - $ER(j) = R(j) \oplus IR(j)$ for $j = 1, 2, \dots, i$, when $i = k$
5. Repeat steps 3 & 4 for G and B.
6. Cipher image will be obtained by concatenate ER, EG and EB
7. Send cipher image with sharing initial key.
8. End.
9. The sender generates three random keys to encrypt three components of color image block by block to obtain cipher image which will be sent to the recipient who has the same procedure to generate a random key after sharing the sender secret key to recover the key.

II. Results and Analysis

These are the results and analysis section. MATLAB (R2013a.) program is used to implement the proposed approach. Color image of type bmp with size of 256×256 is tested by a proposed algorithm. This approach shows good results for many statistical tests such as histogram and correlation. The following tests will discuss feasibility to satisfy properties of good encryption algorithm:

A. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR)

Two important statistical tests are applied here. These tests are MSE and PSNR. Table 3 gives the values of MSE and PSNR for two images.

Table 3: Mean square error and peak signal to noise ratio

Images		Average	R	G	B
Lena	MSE	0.1364	0.1629	0.1379	0.1085
	PSNR	8.7100	7.8804	8.6040	9.6454

B. Differential Attack

Attacker tries to make small change in plain image to get the correlation between the plain and cipher to know the secret key. This case is called the differential attack. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two popular tests to measure the efficient proposed algorithm against differential attack. Table 4 gives NPCR and UACI values for Lena and Baboon images after changing one bit, while Table 5 shows the values after changing one byte.

Table 4: NPCR and UACI for R, G and B after change one bit,
 from $\text{rgb}(200,74,1)=136$ to $\text{rgb}(200,74,1)=137$

Images		R	G	B	Average
Lena	NPCR	99.7208	99.3500	99.3820	99.4843
	UACI	34.5242	32.0960	27.0650	31.2284
Baboon	NPCR	99.6048	99.5987	99.6201	99.6078
	UACI	33.3215	33.5603	33.3107	33.3975

Table 5: NPCR and UACI for R, G and B after change one byte,
 from $\text{rgb}(240,255,3) = 63$ to $\text{rgb}(240,255,3) = 234$

Images		R	G	B	Average
Lena	NPCR	99.7208	99.3500	99.3820	99.4843
	UACI	34.5242	32.0960	27.0652	31.2285
Baboon	NPCR	99.6048	99.5987	99.6201	99.6078
	UACI	33.3215	33.5603	33.3113	33.3977

C. Entropy of Information

Entropy is a widespread test for randomness image encryption over the cipher image. Table 6 illustrates the values of entropy of plain and cipher for sample images .It seems from this Table that the entropy of cipher image which refers to a relative from 8, that means a proposed approach, shows good results.

Table 6: Entropy of plain and cipher sample images

Images	Entropy of plain image	Entropy of cipher image
Lena	7.73291	7.99913
Baboon	7.64026	7.99907

Most researchers try to reach the optimum uniform distribution for histogram of image after applying their algorithms. However, in this paper the researchers try to gain best method to extract the good results here. Figure 3 shows picture's Lena with histogram while figure 4 illustrates the gray scale of red, green and blue channels. After running the proposed algorithms, the histogram of each channel is near from the uniform distribution. Therefore, the proposed one can be satisfied as an efficient approach for encryption and decryption images. Figure 5 and figure 6 show Baboon image with all components before and after encryption.

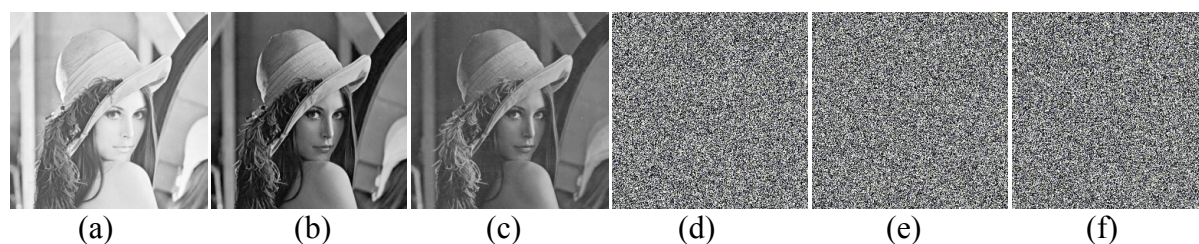


Figure 3: a, b, and c represent R, G and B of plain Lena images while d, e and f are cipher images

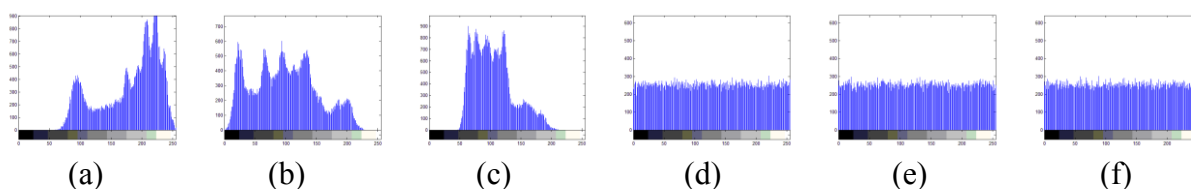


Figure 4: (a-f) histogram of Lena plain and cipher for R, G and B.

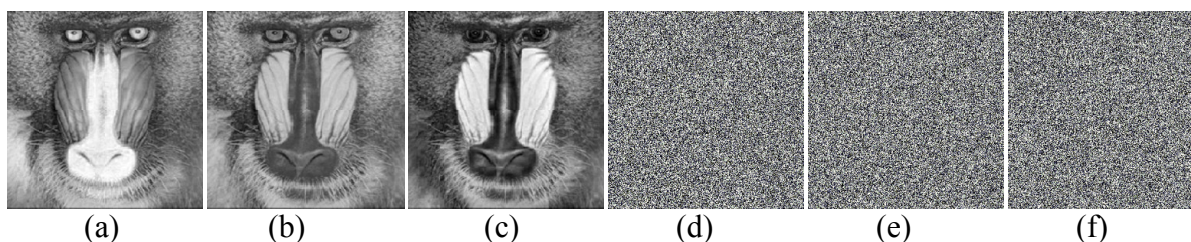


Figure 5: (a-f) represent plain and cipher images of Baboon

with three components R, G and B

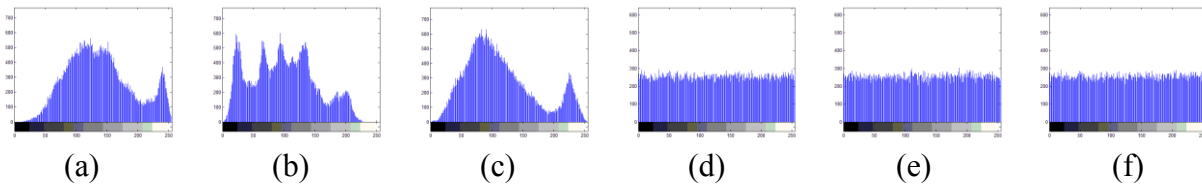


Figure 6: (a-f) histogram of Baboon plain and cipher for R, G and B.

D. Correlation Coefficients

Correlation measures the relation and power of relation between two variables. In this paper, the correlation coefficients between plain and cipher images can be illustrated in Table 7. Table 8 shows correlation among R, G and B for encryption and origin standard images. Randomly, 4000 pixels are selected from origin and encryption image to judge that the cipher image has no relation between pixels. Figure 6 views Correlation coefficient between pixel pairs of Lena image for R, G and B for origin and encryption image including three cases horizontal, vertical and diagonal.

Table 7: Correlation between plain and cipher image

Images	Lena	Baboon	Barbara	Pepper	Elephants	Gold hill	Temple	Boats
Correlation	0.0018	0.0025	0.0043	0.0008	0.0032	0.0016	0.0005	0.0024

Table 8: Correlation coefficients for R, G and B of image according to horizontal, vertical and diagonal

Images		Cipher			Plain		
		R	G	B	R	G	B
Lena	H	0.00175	-0.00104	0.01075	0.95722	0.94321	0.92845
	V	-0.00146	-0.00887	-0.00252	0.97889	0.97137	0.95593
	D	0.00223	0.00467	-0.00056	0.93389	0.91931	0.90068
Baboon	H	0.00784	-0.00324	0.00450	0.97294	0.95311	0.97112
	V	-0.00101	-0.00272	-0.00503	0.96665	0.94467	0.96856
	D	0.00420	-0.00022	0.00357	0.94779	0.91110	0.94644

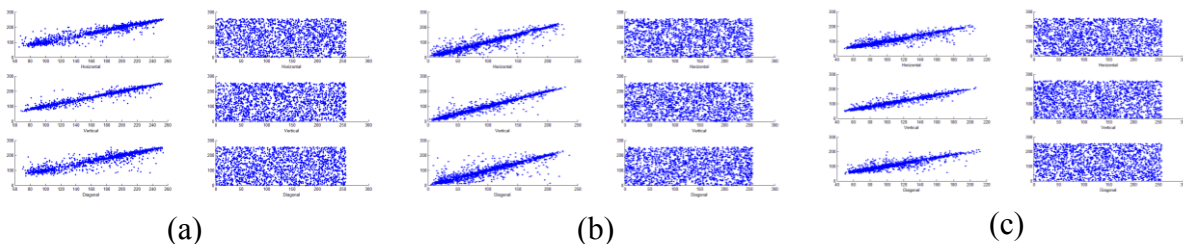


Figure 6: a, b and c are Correlation coefficients between pixel pairs of R, G and B respectively

E. Key Analysis

Space and sensitivity key analysis plays a main role to know the size and security of it. Key space is the total number of different keys that can be used in the encryption technique. The encryption technique should be sensitive to all the secret keys. There are some of initial conditions of chaotic map are used in the proposed image encryption; the initial conditions for $L = 2$, $x_0 = 0.7565$, $y_0 = 0.4432$, $z_0 = 0.9343$, $a = 10$, $b = 8 / 3$, and $r = 28$. The Sub keys generated are:

$A = [147351086725245, 145381185318914]$, $B = [182741481765858, 117881445719116]$

$C = [127671184750649, 166311768385973]$

In this case, the precision is 10, the key space size is $(1015)10 = 10150$, which is extensively enough to resist the brutal force attack. The different secret keys should produce different encrypted images complexity. According to the key sensitivity of the proposed image encryption technique, two different keys from initial parameters can be used to encrypt the original image and two encrypted images are different. For example if Lena image is encrypted using these initial parameter values: $x_0=0.7565$, $y_0=0.4432$, $z_0 = 0.9343$, $a = 10$, $b = 8 / 3$, and $r = 28$, to produce figure 7-b, and it is encrypted with the same initial parameters (except $x_0 = 0.7564$) to produce figure 7-c, then two different encrypted images are shown in figure 7-d.

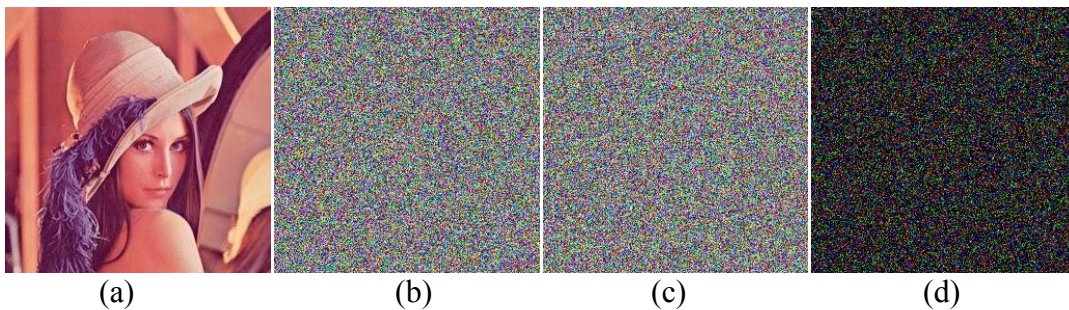


Figure 7: a: image of Lena, b: encrypted image with Key, c: encrypted image with same key after one bit is changed, d the difference between b and c.

III. Conclusions

The main contribution of this paper is the encrypted and decrypted color image depending on the proposed method to generate the random key using Lorenz equations as an input values after some operations to reduce the process time when using only Lorenz equations. Although the proposed algorithm works with any size of key selected by the user, but it gives good results when the size of key is (32, 64, 128 or 256), because image histogram is near to uniform distribution.

References

- [1]. El-Khamy S, El-Nasr M, El-Zein A, (2009) "A Partial Image Encryption Scheme Based on the DWT and ELKNZ Chaotic Stream Cipher". Journal of Basic and Applied Sciences, Vol. 1 No. 3, pp389-394.

International Journal of Business and ICT
Edited in association with the American Society of Competitiveness
2016, Vol.2, No.3-4

ISI : 000000000

www.IJBICT.com

- [2]. Parameshachari B, Soyjaudah K, (2012) "Analysis and Comparison of Fully Layered Image Encryption Techniques and Partial Image Encryption Techniques". In: International conference on information processing. Wireless Networks and Computational Intelligence. Heidelberg: Springer, Vol. 292 pp599-604.
- [3]. Ginesu G, Onali T, Giusto D, (2006) "Efficient Scrambling of Wavelet-based Compressed Images". In: 2nd International Mobile Multimedia Communications Conference; 18-20 September, Alghero, Italy: 43. ACM.
- [4]. Shujun Li, Zheng X, (2002) "Cryptanalysis of a Chaotic Image Encryption method". In: International Symposium on Circuits and Systems; 26-29 May 2002; USA: IEEE, Vol. 2 No. 5, pp708-711.
- [5]. Alsafasfeh Q, Arfoa A, (2012) "Image Encryption Based on the General Approach for Multiple Chaotic Systems". Journal of Signal and Information Processing, Vol. 2 No. 3, pp238-244.
- [6]. El-Alfy E, Al-Utaibi K, (2011) "An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators". In: Seventh International Conference on Networking and Service; 22-27 May 2011; Italy: IARIA, pp 92:97.
- [7]. AL-Najjar H, AL-Najjar A, (2012) "Multi-Chaotic Image Encryption Algorithm Based on One Time Pads Scheme". International Journal of Computer Theory and Engineering, Vol. 4 No. 3, pp350-353.
- [8]. Ansari S, Gupta N, Agrawal S, (2012) "An Image Encryption Approach Using Chaotic Map in Frequency Domain". International Journal of Emerging Technology and Advanced Engineering, Vol. 2 No. 8, pp287-291.
- [9]. Chaitanaya G, Keerthi B, Saleem A, Trinadh A, Kumar K, (2015) "An Image Encryption and Decryption using Chaos Algorithm". Journal of Electronics and Communication Engineering, Vol. 10 No. 2, pp103-108.
- [10]. Ghys E, (2013) "The Lorenz Attractor, a Paradigm for Chaos". In: the series Progress in Mathematical Physics. Basel: Springer, Vol. 66, pp1-54.

Authors



¹ Abdulrahman Dira Khalaf got B.Sc. in Operation Research, Al-Mansour University College (MUC), Iraq (1991-1995) and the degree of Higher Diploma in Computer Qualification by the Information Institute for Postgraduate Studies on 16 of March 2005. M.Sc. in Computer Science from University of Anbar in January 2012. Fields of interest: Information Security, Information Retrieval, Artificial Intelligence, Image Processing and Multimedia Processing.



² Ali Makki Sagheer was born in Basrah-1979. He got B.Sc. of Information System in Computer Science Department at the University of Technology (2001)-Iraq, M.Sc. in Data Security from the University of Technology (2004)-Iraq and Ph.D. in Computer Science from the University of Technology (2007)-Iraq. He is interested in the following Fields (Cryptology, Information Security, Number Theory, Multimedia Compression, Image Processing, Coding Systems and Artificial Intelligence). He published many papers in different conferences and scientific journals.