Multi-Levels Image Encryption Technique based on Multiple Chaotic Maps and Dynamic Matrix

Baydda Flaeh AL-Saraji
Computer Science
Dept. / Mustansiriyah University,
Baghdad-Iraq

Mustafa Dhiaa AL-Hassani, PhD
Computer Science
Dept. / Mustansiriyah University,
Baghdad-Iraq

ABSTRACT

The rapid development in internet technologies and applications have led to great increase in the amount of information sent and received electronically. Transmitting information on networks have become insecure because of new threats continue to evolve. This research aims to provide an efficient technique with highly protection degree of secret images being transmitted “in a meaningless form” over a communication channel through the use of chaotic maps by taking its advantages over other methods of encryption. Chaotic based encryption algorithm is employed at the present time because of its best security and good performance according to the random sequences that are generated from nonlinear system in a high speed calculations. The obtained results from the experimental tests proved that the proposed encryption algorithm is a powerful and efficient technique according to the higher (Entropy ≤ 8) and (Correlation ≤ 1) with perfect reconstruction of the decryption image.

Keywords

Cryptography, Chaos Theory, Image Encryption, Logistic Maps, Dynamic Matrix.

1. INTRODUCTION

Due to the rapid development in the field of communications multimedia and the increasing use of the Internet, multimedia data security has become very urgent. One of the efficient techniques to achieve the multimedia data security is cryptography, which prevents the unauthorized entities from accessing confidential data. In recent years, the chaos theory and non-linear dynamics have obtained an important role in the cryptography. Cryptography is often used to secure information secrecy through making messages illegible. However, indecipherable messages may make an opponent suspicious and probably lead to his destruction of such a communication manner. In general, the cryptosystem is used for protecting the data against any unauthorized people. Therefore, cryptography allows protection against hackers and spies [1, 2]. The first study of the chaotic functions was in the 1960s and it has shown many magnificent properties. Sequences generated by these functions are very complex, random and these functions a mainly used to improve mathematical models for nonlinear systems. Due to their very sensitive nature to initial conditions and many more interesting feature, it has attracted the interest of many mathematicians [3, 4]. The properties of chaotic systems have been used in very different ways to build new cryptography. All of those proposals can be classified into two big families, which are analog chaos-based cryptography and digital chaos-based cryptography. The first type of chaotic cryptography is based on the chaotic synchronization technique, whereas digital chaotic cryptography is based on one or more chaotic maps in such a way that the secret key is either given by the control parameters and the initial conditions or those values are determined [5].

2. AIM OF THE WORK

This research aims to improve the security level and secrecy provided by the chaotic map based encryption of the image. An N- array key stream generator is proposed in this work, which is based on Multiple- Logistic maps to generate the encryption keys and dynamic matrix using LFSR to increasing the randomness of the image.

3. IMAGE ENCRYPTION USING CHAOTIC –MAP

The basic idea of encryption is to scramble the secret information in such a way that it cannot be understood by unauthorized people; Encryption is the process of encoding data in such a way that hides them from any outsider; it is a simple transfer of plaintext to ciphertext while decryption is the reverse process of encryption, transferring ciphertext to plaintext. A system for encryption and decryption is called cryptosystem [6].The traditional encryption techniques (i.e., RSA, DES, AES and IDEA) are not appropriate options for real-time image data encryption, because images are relatively large in terms of size, practically for the uncompressed formats, these ciphers require a large computational time. Thus, the process of encryption of the image should be quicker to meet the real time constraints. Different encryption techniques that are secure and faster in nature have been introduced by the research community, one of these techniques is Chaos theory [7, 8].

4. CHAOS THEORY

Chaos is derived from the Greek word ‘Xαos’, which meaning a state without predictability or order. A chaotic system is a non-linear, simple, deterministic system, and dynamical, that illustrates completely unexpected behavior and shows randomness. It is used in cryptography for the nature of features is high sensitive to initial conditions of the system, randomness and aperiodicity like the long-term evolution that results from the deterministic nonlinear systems, because of these properties, it has been used to create random numbers. With a very small change in their initial values, the generated series are completely various [9, 10].

With this definition, several conclusions about the characteristics of chaotic system can be drawn [11]:

1. The system is nonlinear which means that the output is not directly proportional to input, and because the system is nonlinear and dynamic it is sensitive to dependence on initial conditions.
2. The system can change at discrete times; it has deterministic (rather than probabilistic) underlying

rules. The states of the system must follow these rules therefore there is no random component in the system.

5. LOGISTIC MAPS

Many methods were developed to design encryption algorithms of the image by using chaotic maps, sequences of chaotic are created during the use of various equations that will show complete randomness to an external observer. The sequence creation is deterministic, since they are sensitive to initial conditions, there for, discusses only the logistic map [12, 13]. The logistic map is a polynomial mapping, a complex chaotic system, the behaviour of logistic map is very simple nonlinear dynamic equations. The 1-D coupled logistic map equation is written as [12]:

$$\mathbf{X_{n+1} = rX_n(1 - X_n)} \qquad \textbf{(1)}$$

The first few iterations of the logistic map (1) give:

$$\mathbf{X_1 = rX_0\ (1 - X_0)} \qquad \textbf{(2)}$$

$$\mathbf{X_2 = rX_1\,(1 - X_1)} \qquad \textbf{(3)}$$

$$\mathbf{X_2 = \ r^2\, X_0\,(1 - X_0)\ \left(1 - rX_0 + rX_n^2\right)} \qquad \textbf{(4)}$$

Where $\mathbf{X_n}$ is the state variable, which generates values in the interval [0,1] and n is the number of iterations, where r is the called system variable and control parameter, $0 < r \leq 4$, as shown in Figure (1).

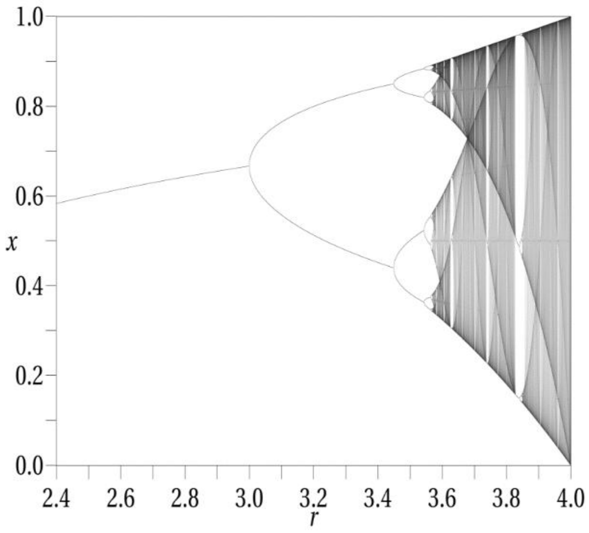


Fig .1 The Bifurcation Diagram of the Logistic Map

The logistic map is one of the simplest chaotic maps; it is highly sensitive to change in its parameter value, where a different value of the parameter r will give quite different pictures, as shown in Figure (2) [12].

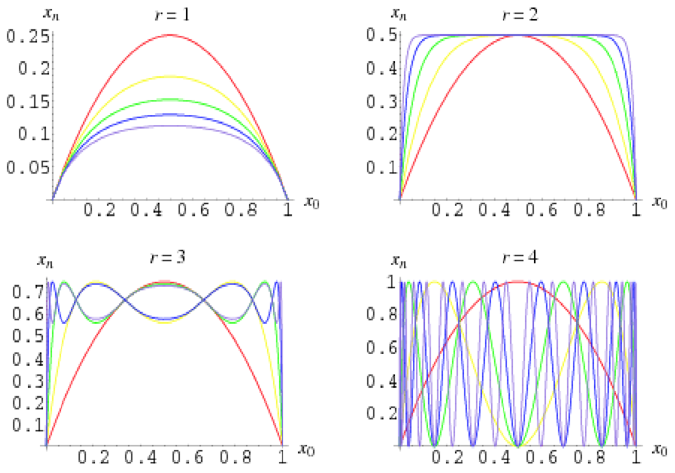


Fig. 2 The Bifurcation Parameter of Logistic Map.

6. THE PROPOSED SYSTEM MODEL

The block diagram of the proposed cryptosystem model, shown in Figure (3), is implemented using Microsoft Visual Basic.net 2013 programming environment. It consists mainly of 2-basic modules: Encryption and Decryption.

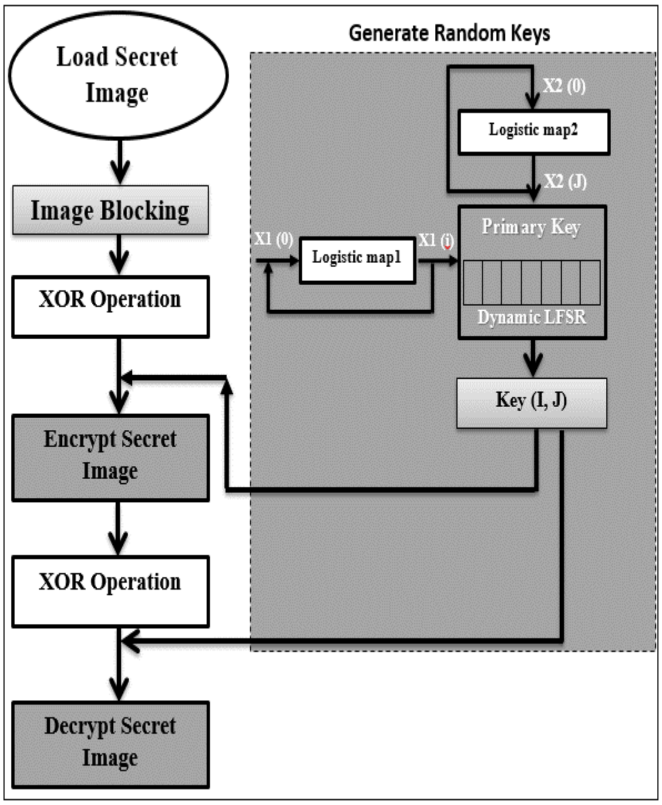


Fig. 3 The Block Diagram of the Multi-Chaotic map encryption and decryption method.

6.1 Chaotic Image Encryption

In order to encrypt a secret image, the chaotic image encryption should perform the sequence of steps that are illustrated by algorithm (1).

Algorithm (1): The Proposed Multiple-Logistic Maps Encryption Method

```
Input  : Secret Image File SI, Common Database.
Output: Encrypt Secret Image ESI [H, W] where H, W represent image Height and Width respectively.

Step1: Select the Secret image file that needs to be sent to the receiver and get its header information.
Step2: Divide the image into group of blocks [3×3].
Step3: The primary key contains all ASCII ('A…Z', 'a…z', /,", [], {},"",…etc).
Step4: Select the primary key either from a Common Database of Key File or directly from variable Length where there is change in each run.
Step5: Convert the Key File to ASCII representation (Sequence of Bytes).
Step7: Convert the ASCII of Key File into its equivalent 2-D binary array called BinKF [M ×N], where M is variable which depends on the Key Length, N = 7 which depends on the ASCII of Key File.
Step8: The initial parameters of the Logistic -Maps (X0, R), such that X0 ∈ [0, 1] & R ∈ [0, 4].
Step9: Apply the Multiple- Logistic Maps to create the generation of factors (Values, Ranges, Max, Min, Increment). The generation of factor Values depends on the [M ×7] in BinKF, the generation of factor Ranges depends on the Length [M] in BinKF, such that Ranges ∈ [0, Max values], the generation of factor Max is the maximum values in generation, Min is the minimum values in generation, the generation of factor Increment is the amount of the increase in Ranges such that Increment = (Max values / number of [M]).
Step10: The resulting values of the equation (1) represent the [M] in BinKF.
Step11: The resulting values of the equation (4) represent the [N] in BinKF.
Step12: Apply the (Linear Feedback Shift Register) to each [M] in the BinKF in order to generate the Keys in first level and increase the randomness.
Step13: Go to step9-step12.
Step14: Create the BinKF for 2nd level.
Step15: Perform the Encryption process of the 1st level (using XOR operations) on the sequences:
        ESI 1[H, W] ⟵ SI [H, W] ⊕ K 1nd.
Step16: Go to step9-step12.
Step17: Create the Keys for 2nd level.
Step18: Perform the Encryption process of the 2nd level (using XOR operations) on the sequences:
        ESI 2[H, W] ⟵ ESI1 [H, W] ⊕ K 2nd.
Step19: Create the Encrypted Secret Image ESI2 [H, W].
```

6.2 Chaotic Image Decryption

In order to decrypt a secret image, the chaotic image decryption should perform the sequence of steps that are illustrated by algorithm (2).

Algorithm (2): The Proposed Multiple-Logistic Maps Decryption Method

```
Input  : Encrypted Secret Image File.
Output: Decrypted Secret Image DSI [H, W], where H, W represent image Height and Width respectively.

Step1: Open the Encrypted Secret Image File ESI [H, W] and then obtains its image data after getting information header.
Step2: Generate the set of all Keys in the same manner in algorithm (1) from K 1nd and K 2nd.
Step3: Perform the Decryption process of the 1nd level (using XOR operations) on the sequences:
        DSI 1[H, W] ⟵ ESI 2[H, W] ⊕ K 1nd.
Step4: Perform the Decryption process of the 2nd level (using XOR operations) on the sequences:
        DSI 2[H, W] ⟵ DSI 1[H, W] ⊕ K 2nd.
Step5: Create the Decrypted Secret Image File DSI 2 [H, W].
```

7. ENCRYPTION TESTS EVALUATION

To test the robustness of the proposed scheme, enciphering tests evaluation was performed. Histogram, information entropy and correlation coefficient analysis were carried out to clarify the good performance of the adopted scheme.

7.1 Histogram Analysis

Histogram is a 2D graphical representation, the horizontal axis refer to the color –level value which begins at zero and goes to the number of color levels where as the vertical axis refer to the number of times of corresponding color level occurred in the image. In other words, histogram shows the number of pixels in an image at each different intensity value found in the image. The histogram of the ciphered image should be significantly different from the histogram of the plain image, and the histogram of the ciphered image should be as uniformed distribution as possible that will indicates more randomness [14, 15].

7.2 Information Entropy Analysis

Entropy refers to information theory, entropy states degree of uncertainty in a system. The Entropy of a message is calculated by equation (5). Entropy is expressed in units of bits. Random messages should have an ideal entropy equal to 8, while in less random messages entropy is less than 8. If the entropy is less than 8, here are degrees of predictability, which is a threat to security. Cipher-images can be considered as random images, so the entropy should ideally be 8 [16].

7.3 Correlation Coefficient Analysis

Correlation is a statistical technique that can show whether and how strongly pairs of variables are related. The correlation coefficients are calculated by the following equation for two variables x and y of length N [17]:

$$R_{XY=}\frac{c_{v(x,y)}}{\sqrt{D(X)\,D(Y)}} \qquad (5)$$

Where $c_{v\,(x,y)}$ is the covariance between the original signal x and the signal y. D(x) and D(y) are the variances of the signals x and y. In numerical computations, the following discrete formulas can be used:

$$C_{V\,(X,Y)=}\frac{1}{N}\sum_{i=1}^{N}\big(X(i)-$$

$$EXYi{-}EX \qquad (6)$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N}(X(i) - \mathrm{E(X)})^2 \quad (7)$$

$$D(Y) = \frac{1}{N}\sum_{i=1}^{N}(Y(i) - \mathrm{E(Y)})^2 \quad (8)$$

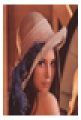
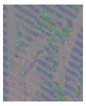
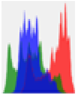
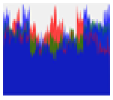
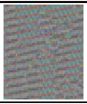
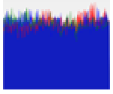
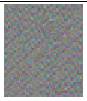
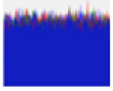
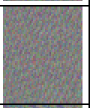
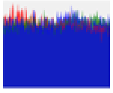
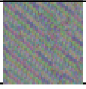
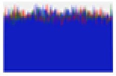
$$E(X) = \frac{1}{N}\sum_{i=1}^{N}(X(i)) \quad (9)$$

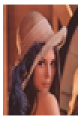
$$E(Y) = \frac{1}{N}\sum_{i=1}^{N}(Y(i)) \quad (10)$$

8. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, the proposed system was tested according to encryption test evaluation, the experimental results of our proposed scheme with Multi- Logistic maps using colored images are presented as shown from in Table (1) and Table (2).

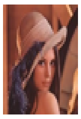
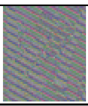
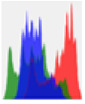
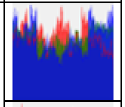
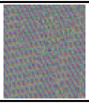
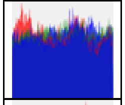
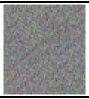
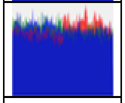
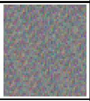
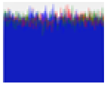
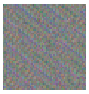
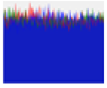
Table.1 The test results for image encryption (Level 1) with different keys.

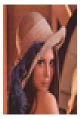
First Level of Encryption						
Original Image (OI)	Key Length	Encrypted Image (EI-1)	Entropy		Histogram	
			OI	EI-1	OI	EI-1
	50		7.5846	7.5999		
	100			7.6232		
	150			7.6338		
	250			7.6422		
	300			7.6561		

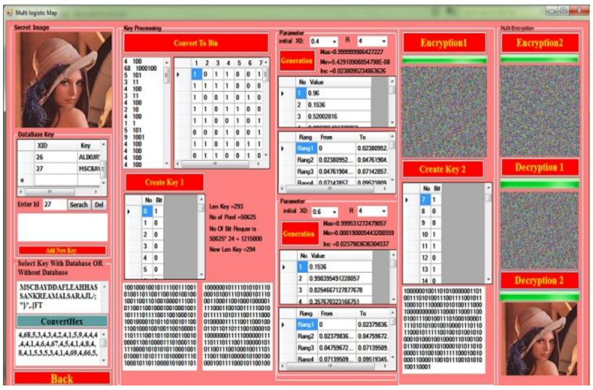
Original Image (OI)	Key Length	Correlation of (OI)	VCorr (EI-1)	HCorr (EI-1)
	50	VCorr (OI) (0.9792) HCorr(OI) (0.9856)	0.8711	0.7295
	100		0.8193	0.7821
	150		0.8018	0.7943
	250		0.8160	0.7711
	300		0.8047	0.7829

The program interface for the chaotic image encryption and decryption are illustrated in Figure (4).

Table. 2 The test results for image encryption (Level 2) with different keys.

Second Level of Encryption						
Original Image (OI)	Key Length	Encrypted Image 2 (EI-2)	Entropy		Histogram	
			OI	EI-2	OI	EI-2
	50		7.5846	7.6015		
	100			7.6440		
	150			7.6487		
	250			7.6532		
	300			7.6877		

Original Image (OI)	Key Length	Correlation of (OI)	VCorr (EI-2)	HCorr (EI-2)
	50	VCorr (OI) (0.9792) HCorr (OI) (0.9856)	0.8191	0.7801
	100		0.7849	0.7764
	150		0.8186	0.7395
	250		0.7972	0.7744
	300		0.8002	0.7820



	XID	Key
	26	ALIKUR'
	27	MSCBAY

Enter Id 27

Select Key With Database OR Without Database

MSCBAYDDAFLEAHHAS SANKREAMALSARAJL/; "]/',.[FT

4,68,5,3,4,3,4,2,4,1,5,9,4,4,4 ,4,4,1,4,6,4,67,4,5,4,1,4,8,4, 8,4,1,5,3,5,3,4,1,4,69,4,66,5,

Len Key =293
No of Pixel =50625
No Of Bit Requer is
50625* 24 = 1215000
New Len Key =294

Parameter
initial X0: 0.4 R 4
Max=0.999999986427227
Min=5.42910908854798E-08
Inc =0.0238095234863626

No	Value
1	0.96
2	0.1536
3	0.52002816

Rang	From	To
Rang1	0	0.02380952.
Rang2	0.02380952...	0.04761904.
Rang3	0.04761904...	0.07142857.
Rang4	0.07142857	0.09523809

Parameter
initial X0: 0.6 R 4
Max=0.999631272479057
Min=0.000190005443208559
Inc =0.0237983636304537

No	Value
1	0.1536
2	0.998395491228057
3	0.0254667127877678
4	0.357670323166751

Rang	From	To
Rang1	0	0.02379836.
Rang2	0.02379836...	0.04759672.
Rang3	0.04759672...	0.07139509.
Rang4	0.07139509...	0.09519345.

Fig.4 The program interface for the Proposed Cryptosystem

9. CONCLUSION

In this paper, the proposed system model is designed in the form of Multi- levels of security to encrypt a color image using Multiple - Logistic chaotic map techniques and dynamic matrix. A Multiple- Logistic chaotic map for multi-level image encryption depends on the image blocking process and consequently the Linear Feedback Shift Register of binary matrix in order to increase the randomness of the encrypt image and then XOR operation, the resulting values with the generation of two Logistic keys from a common DB are with variable length. The Key Length of the original array is variable Length compared with new Key Length for 1nd and 2nd levels of encryption because of applying (Linear Feedback Shift Register) to each [M] in the array. The proposed cryptosystem is ready to be used in quick real time enciphering applications and is appropriate for workable use in the secure transfer of secret information through the web network according to (Entropy ≤ 8) and (Correlation ≤ 1).

10. REFERENCES

[1] Mihir H Rajyaguru, *“Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys”*, International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012.

[2] M.Lakshmanan, and S.Rajasekar*, “Nonlinear Dynamics: Integrability”*, Chaos, and Patterns”, Springer- Verlag Berlin Heidelberg, 2003.

[3] M.Ashtiyani, S.Asadi, P.H.Goudarzi*, “A New Method in Transmitting Encrypted Data by FCM Algorithm”*, Proceeding of ICTTA06 Conference, Syria, (2006).

[4] J.S. Yen and J.I. Guo, *“A New Chaotic Key-based Design for Image Encryption and Decryption”,* IEEE Proc. On Circuits and Systems”, vol. 4, pp. 49-52, (2000).

[5] David Arroyo, Gonzalo Alvarez, and Veronica Fernandez *"On the Inadequacy of the Logistic Map for cryptographic applications"*, Instituto de Fsica Aplicade, Consejo Superior de Investigaciones Cientificas, Serrano Madrid, Span, 2008.

[6] Willam Stallings, *"Cryptography and Network Security: Principles and Practice*", Second ed, Prentice Hall, USA, 2003.

[7] N. K. Pareek, V. Patidar, K.K. Sud*, “Image Encryption Using Chaotic Logistic Map”,* M.L.S. University Computer Centre, Vigyan Bhawan, India, Elsevier, 2006.

[8] Fahad T. Bin Muhaya, *“Chaotic and AES Cryptosystem for Satellite Imagery”,* Prince Muqrin Chair for IT Security,Management Information System Department, Business Administration College, King Saud University, KSA,2011.

[9] Zhang, H. and J.-x. Dong. *"Chaos theory and its application in modern cryptography in Computer Application and System Modeling (ICCASM)"*, International Conference on, 2010.

[10] Amit P., Goseph Z., *“A Chaotic Encryption Scheme for Real-time Embedded Systems: Design and Implementation,* Department of Electrical and Computer Engineering, Iowa State University, Ames, USA, Springer, 2011.

[11] Pengcheng Wei, Huaqian Yang, Qunjian Hang, and Xi Shi *“A Novel Block Encryption Based on Chaotic Map"*, Department of Computer Sience, Chongqing Education of College, Chongqing 400067, China 2002.

[12] Wang Feng-ying, Cui Guo-wei, *“A New Image Encryption Algorithm Based on the Logistic Chaotic System”,* Department of Information Engineer, Inner Mongolia University of Science & Technology, China, © IEEE, 2010.

[13] H. Hermassi, R. Rhouma, S. Belghith, *“Improvement of an Image Encryption Algorithm Based on Hyper-chaos”,* National School of Engineers ENIT, Springer, 2011.

[14] Zhang Yong*, “Image Encryption with Logistic Map and Cheat Image”,* International Conference on Computer Re-search and Development, pp [97-101], March 2011.

[15] RashidahKadir, RosdianaShahril, and MohdAizainiMaarof*, “A Modified Image Encryption Scheme Based on 2D Chaotic Map”,* International Conference on Computer and Commu-nication Engineering, pp [1-5], May 2010.

[16] Alireza Jolfaei, Abdul Rasoul Mirghadri, “An Image Encryption Approach Using Chaos and Stream Cipher”, Journal of Theoretical and Applied Information Technology, (2010).

[17] J. S. Fouda, J. Y. Effa, S. Sabat, and M. Ali, *“A Fast Chaotic Block Cipher for Image Encryption,”* Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 3, pp. 578–588,2014.