REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj

Faculté *des Sciences et de la technologie*

Département d'Electronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : **ELECTRONIQUE**

Spécialité : Industries Electroniques

Par

- **Ramdane Riad**
- **Zoubir Yacine**

Intitulé

Cryptage des signaux image basé sur le les suites chaotiques multi-niveaux

Évalué le /09/2021

Par la commission d'évaluation composée de* :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M.	*MCB*	*Président*	*Univ-BBA*
M. S.E. AZOUG	*MCB*	*Encadreur*	*Univ-BBA*
M.	*….*	*Examinateur*	*Univ-BBA*

Année Universitaire 2020/2021

Abstract:

After the development of the communication system and methods of exchanging digital information, the exchange of secret information has become unsafe. The secrecy of these digital contents is one of the most important issue of existing world. In this work, we study and propose an image encryption algorithm. The proposed algorithm is based on many iterative chaotic maps.The suggested encryption added confusion and diffusion in offered scheme which is one of the most fundamental aspect of encryption technique. We have tested our proposed algoriythm against different performances analysis and compared it with already existing results.These tests showed that the proposed algorithm can provide excellent privacy for digital images.

Résumé:

Après le développement du système de communication et des méthodes d'échange d'informations numériques, l'échange d'informations secrètes est devenu dangereux. Le secret de ces contenus numériques est l'un des enjeux les plus importants du monde existant. Dans ce travail, nous étudions et proposons un algorithme de cryptage d'images. L'algorithme proposé est basé sur de nombreuses cartes chaotiques itératives. Le cryptage suggéré a ajouté de la confusion et de la diffusion dans le schéma proposé qui est l'un des aspects les plus fondamentaux de la technique de cryptage. Nous avons testé notre algorithme proposé par rapport à différentes analyses de performances et l'avons comparé avec des résultats déjà existants. Ces tests ont montré que l'algorithme proposé peut fournir une excellente confidentialité pour les images numériques.

ملخص:

بعد تطور انظمة الاتصال وطرق تبادل المعلومات الرقمية أصبح تبادل المعلومات السرسة غير امن .حيث تعد سرية المحتويات الرقمية واحدة من أهم القضايا في العالم الحالي. في هذا العمل، قمنا بدراسة واقتراح خوارزمية لتشفير الصور. تعتمد الخوارزمية المقترحة على العديد من الخرائط الفوضوية التكرارية، وقد أضاف نظام التشفير المقترح خاصيتا التشويش والانتشار والتان تعدان أحد الجوانب الأساسية لتقنية التشفير. لقد وضعنا الخوارزمية المقترحة تحت اختبارات تحليل الأداء وقارناها بالنتائج الموجودة مسبقا، قد أظهرت هذه الاختبارات أن الخوارزمية المقترحة يمكن أن توفر خصوصية ممتازة للصور الرقمية.

List of acronyms

IDEA	International Data Encryption Algorithm.
DES	Data Encryption Standard.
AES	Advanced Encryption Standard.
ACM	Arnold’s Cat Map.
PLCM	Piece wise Linear Chaotic Map.
2D	two dimensional.
CC	Correlation Coefficient.
MSE	Mean square error.
PSNR	Peak signal to noise ratio.
MAE	Mean absolute error.
NPCR	Number of pixels changing rate.
UACI	Unified average change intensity.

Acknowledgments

First of all, we thank Allah Almighty, who gave us patience and moral strength and enabled us to complete our work.

We express our sincere thanks to ***Dr. Seif El-Din Azouq*** *for agreeing to supervise this work and to lead it with his knowledge, kindness, encouragement, experience, constant presence during the training period, his enlightened advice and the fruitful discussions we had with him.*

We would also like to thank the members of the jury for agreeing to allocate part of their time to review and judge this work.

We cannot forget to thank everyone who supervised our teaching over the five years we spent here in the ***MCIL*** *specialization at the* ***University of Mohamed Bachir Ibrahimi, Bordj Bou Arreridj.***

Finally, our last but not least thank you to our parents and all members of our families with all our affectionate gratitude for their support and encouragement.

List of Figures

List of Tables

Table of contents

III. Simulation results and discussions

Introduction

Introduction

Todays with the development of technology, the exchange of information has become easier with communication networks which created a revolution in the use of information since 1990 [1]. After the transformation of information into digital information due to its efficiency in saving time and effort, the exchanged digital information may be important and confidential, so its privacy is important. This information has become an essential currency for countries.

Digital information is no longer only text messages, but also images and videos. Therefore, it is necessary to search for ways to protect the privacy and confidentiality of these contents. In order to secure the secret information different data security techniques were designed which includes classical and modern encryption schemes. The classical encryption schemes either utilized substitution or permutation [2]. Nowadays, modern encryption mechanisms particularly private encryption schemes use both confusion and diffusion [2]. The most common confusion and diffusion-based block ciphers were the International Data Encryption Algorithm (IDEA)[2], Data Encryption Standard (DES)[1], and Advanced Encryption Standard (AES)[1]. The development of encryption techniques is a discipline in its own right which belongs to the field of cryptography which is one of the branches of cryptology or the science of secrecy [3]. Chaos-based cryptosystems is the new trend nowadays in encryption algorithms. The fundamental characteristics of chaos are quite related with cryptography which make it possible to equally utilize chaos in encryption of digital information.

In order to improve encryption quality, researchers suggested using chaotic image encryption technique on a multi-level basis, that means using multiple discrete dynamical maps in order to increases the encryption randomness and efficiency.

The work plan of our thesis is divided into three chapters:

- Chapter I : Review of cryptography and chaos maps concepts.
- Chapter II : Review of a multilevel chaos image encryption method then presenting the proposed one.
- Chapter III: Showing simulation results and discussions.
- The work thus carried out ends with a conclusion and prospects for the future.

I. Chaos & Cryptography

I.1. Introduction

Chaos is a branch of mathematics that study the behavior of dynamical systems. These systems are highly sensitive to their initial conditions and parameters. These properties attract to make strong cryptosystem algorithms [2]. Cryptography is one of the branches of cryptology or the science of secrecy.[3] Cryptography is the investigation of systems for secure conversation within the sight of attacker.[5]

In this chapter, we will review the elementary concepts of cryptography and chaos and the relationship between them and its application for image encryption and security.

I.2. Basic concepts of cryptography

Image security is based on cryptography [1]. The main goal of cryptography is to guarantee the confidentiality of a message during an exchange between two people through an insecure channel, therefore, if a third party is present in the same communication network, he cannot decipher this message [3]. To accomplish this goal, the message which is often referred to as plaintext is encrypted into an incomprehensible message often referred to as ciphertext [3].

Goals

Cryptography helps to accomplish the following four fundamental goals [1]:

- **Confidentiality** refers to the protection of information from unauthorized access. An undesired communicating party, called an adversary, must not be able to access the communication material. This goal of cryptography is a basic .
- **Data integrity** ensures that information has not been manipulated in an unauthorized way. If the information is altered, all communicating parties can detect this alteration.
- A**uthentication** methods are classified into two categories: entity authentication and message authentication. Entity authentication is the process by which one party is assured of the identity of a second party involved in a protocol, and that the second has actually participated immediately prior to the time the evidence is acquired.

- **Message authentication** is a term used analogously with data origin authentication. It provides data origin authentication with respect to the original message source and data integrity but with no uniqueness and timeliness guarantees.
- **Nonrepudiation** means that the receiver can prove to everyone that the sender did indeed send the message. That is, the sender cannot claim that he or she did not encrypt or sign certain digital information. Fortunately, modern cryptography has developed techniques to handle all four goals of cryptography.

Encryption/Decryption principle

The basic idea of encryption is to modify the message in such a way that only a legal recipient can reconstruct its content.

An encryption system is called a cipher or a cryptosystem. The message for encryption is called plaintext P, and the encrypted message is called ciphertext C [1]. The cryptographic algorithm is composed of an encryption function E and a decryption one D. The encryption function E makes it possible to obtain a ciphertext C from a plaintext P using an encryption key Ke. Similarly, the decryption function D allows decryption using a decryption key Kd.[3]. Therefore, the encryption procedure of a cipher can be described as:

$$C = E_{Ke}(P) \qquad \text{(I.1)}$$

where Ke is the encryption key, and E is the encryption function. Similarly, the decryption procedure is defined as:

$$P = D_{Kd}(P) \qquad \text{(I.2)}$$

where Kd is the decryption key, and D is the decryption function.

Shows the block diagram of the encryption/decryption process.

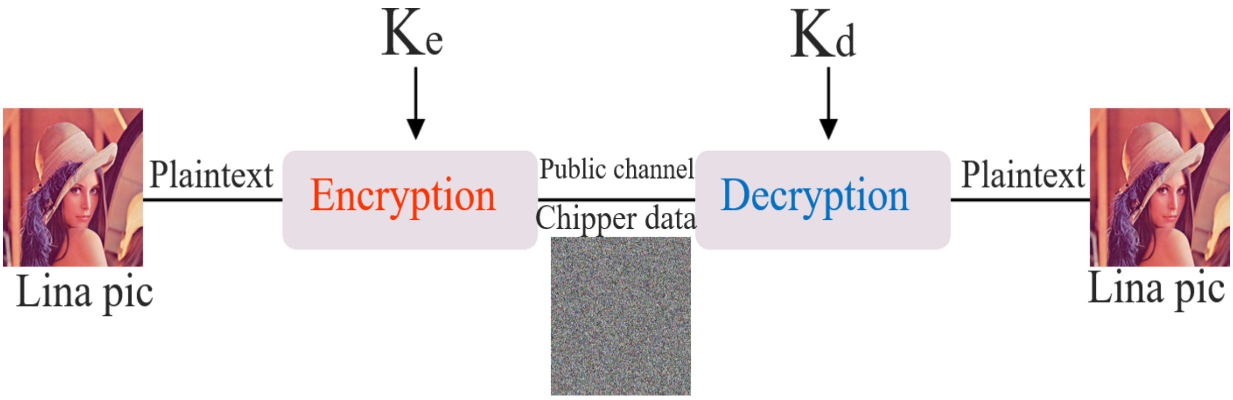

Figure I-1 Encryptions/Decryption of a chipper

I.3. Encryption algorithms classification

Encryption algorithms can be classified in different ways: according to structures of the algorithms, according to keys, or according to the percentage of the data encrypted.[1]

I.3.1. Classification According to Encryption Structure

Encryption algorithms can be classified according to the encryption structure into block ciphers and stream ciphers.

A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length. The fixed length is called the block size. The larger the block size, the more secure is the cipher.

Unlike block ciphers that operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits. So, stream ciphers can be designed to be exceptionally fast, much faster than a typical block cipher. The encryption is accomplished by combining the key stream with the plaintext. Usually, the bitwise XOR operation is chosen to perform ciphering, basically for its simplicity.

I.3.1.1. Classification According to Keys

According to keys, there are two kinds of ciphers(symmetric encryption and asymmetric encryption) following the relationship of Ke and Kd.[1]

I.3.1.1.1. Symmetric encryption

In this case Ke = Kd, the cipher is called a private-key cipher or a symmetric cipher. For private-key ciphers, the encryption/decryption key must be transmitted from the sender to the receiver via a separate secret channel.[1]

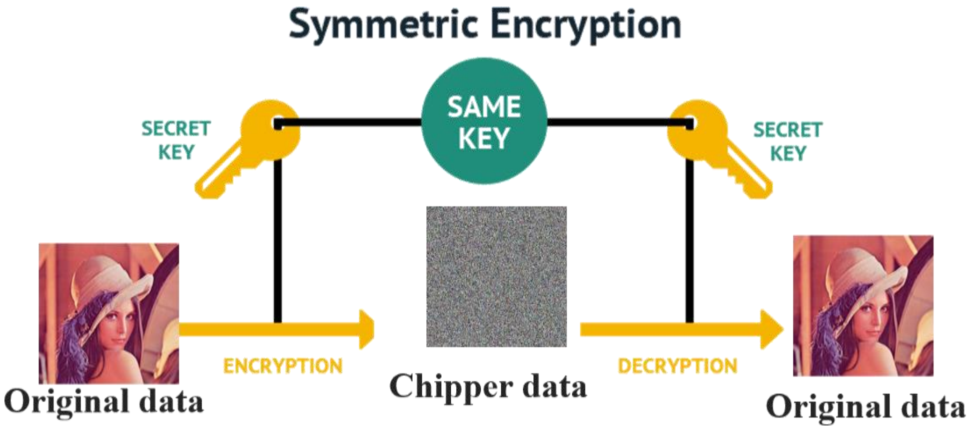

Figure I-2 Model of symmetric encryption

I.3.1.1.2. Asymmetric encryption

In this case Ke ≠ Kd, the cipher is called a public-key cipher or an asymmetric cipher. For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept private, for which no additional secret channel is needed for key transfer.[1]

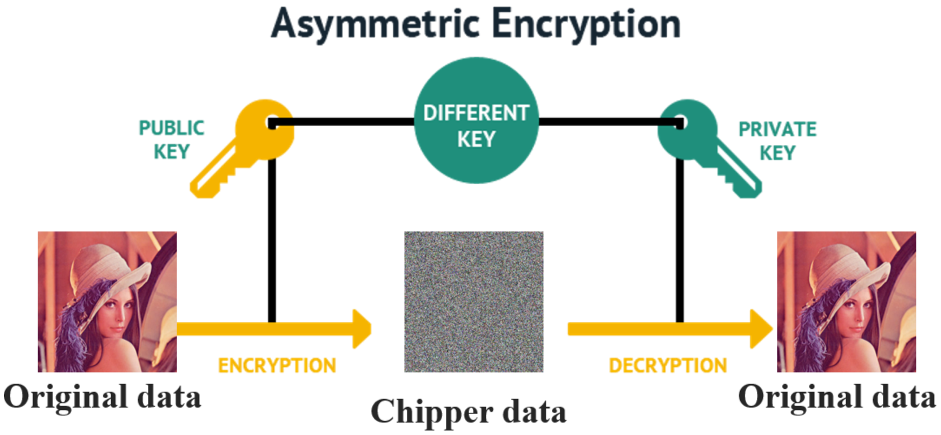

Figure I-3 Model of asymmetric encryption.

I.4. Chaos Theory

Chaos is a natural phenomenon discovered by Edward Lorenz in 1963 while studying the butterfly effect in dynamical systems [8]. The butterfly effect describes the sensitivity of a system to initial conditions as mentioned in Lorenz's paper titled "Does the Flap of a Butterfly's Wings in Brazil set off a Tornado in Texas?" [9].

I.4.1 Chaos in Cryptography

The chaos theory contracts with systems that exhibit a special kind of dynamical behavior in time.[2] There is a set of characteristics that observed the professional in chaotic systems [4], Which can be used in encryption. The most relevant are:

- **Sensitive dependence on initial conditions**: where small changes in the initial values of variables grows in time, and produce unpredictable difference as we compute further, the orbit or path [4].

- **Pseudo-random:** a chaotic sequence governed by a deterministic equation makes it possible to generate a pseudo-random chaotic regime [3].

- **Ergodic:** Statistical measurement of variable that give analogous output irrespective of performance over space or time [2]. A chaotic process is ergodic, because it has the same output distribution whatever the distribution of the variable present at the input.[3].

I.4.2 Confusion and Diffusion principle

If the properties of confusion and diffusion are taken into consideration when designing an encryption algorithm, they will ensure the complexity of the relationship between encrypted text and clear text[3]. This helps to make the algorithm robust against attacks[3]. To achieve this, substitution techniques and permutation techniques are used[6].

I.4.2.1 Confusion

The principle of confusion consists in replacing the character of a plaintext by another different character using a predetermined mathematical function [6]. **Fig I-4** shows a simple example of substitution. The property of confusion hides the relationship between the ciphertext and the key.

This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected. Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

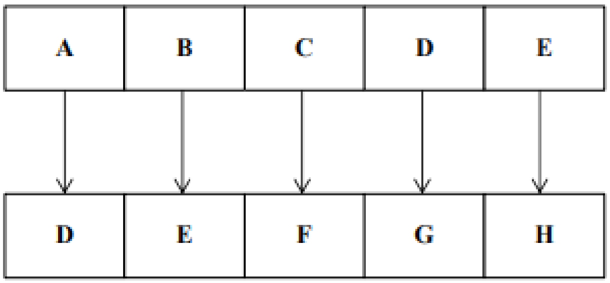

Figure I-4 Exemple of confusion (substitution)

I.4.2.2 Diffusion

The principle of a permutation technique consists in reorganization the order of the characters of a plaintext by changing their positions according to a predetermined arrangement [6].

The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it diffuses the redundancy of plain text by spreading it across the rows and columns [7]. In fig I-5, an example of permutation using Jigsaw permutation.

I.4.3. Discrete chaotic maps

Chaotic maps are simple functions and are iterated quickly. Chaos-based image encryption systems are therefore fast enough for real-time applications. Chaotic maps are charachterized by their bifurcation diagrams. In this type of diagrams we can observe the changes of the dynamic of the discrete map as its parameters changes to identify its chaotic area [4].

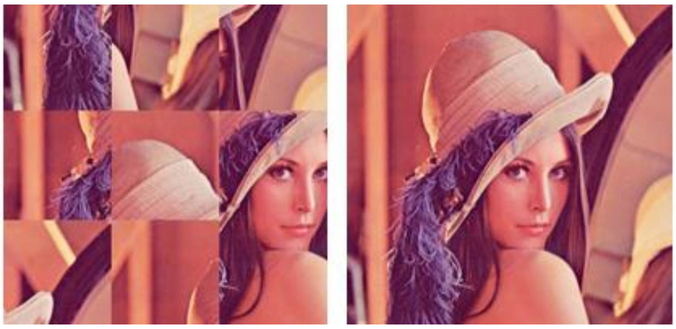

Figure I-5 Example of diffusion (permutation)

I.4.3.1 Logistic chaotic map

One of the most studied one-dimensional discrete maps capable of various dynamical regimes including chaos and defined as [4]:

$$x_{n+1} = rx_n(1 - x_n) \qquad \text{(I.3)}$$

Where r ∈ (0,4) is the control parameter, x_n∈ (0,1) where n € and x_0 as initial condition.

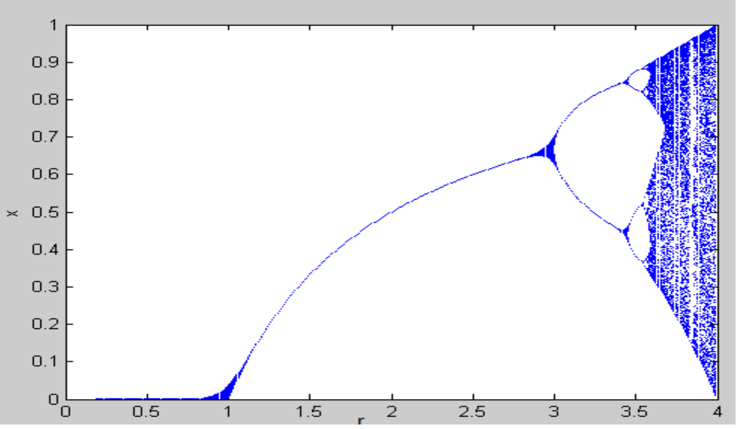

Figure I-6 Bifurcation diagram of Logistic map

Based on this bifurcation , we can see that the sequence becomes chaotic when r ∈ (3.6,4), We can also note “windows” that are easily noticeable wich are non-chaotic intervals [4] .

I.4.3.2 Arnold chaotic map

Arnold Cat Map or ACM is a mixing discrete ergodic system that performs an area preserving stretch and fold mapping discovered by V. Arnold in 1968 using the image of a cat. It is used in cryptography to perform image permutations defined as [8]:

$$x_{n+1} = (2x_n + y_n)\ mod1 \qquad (I.3)$$

$$y_{n+1} = (x_n + y_n)\ mod1 \qquad (I.4)$$

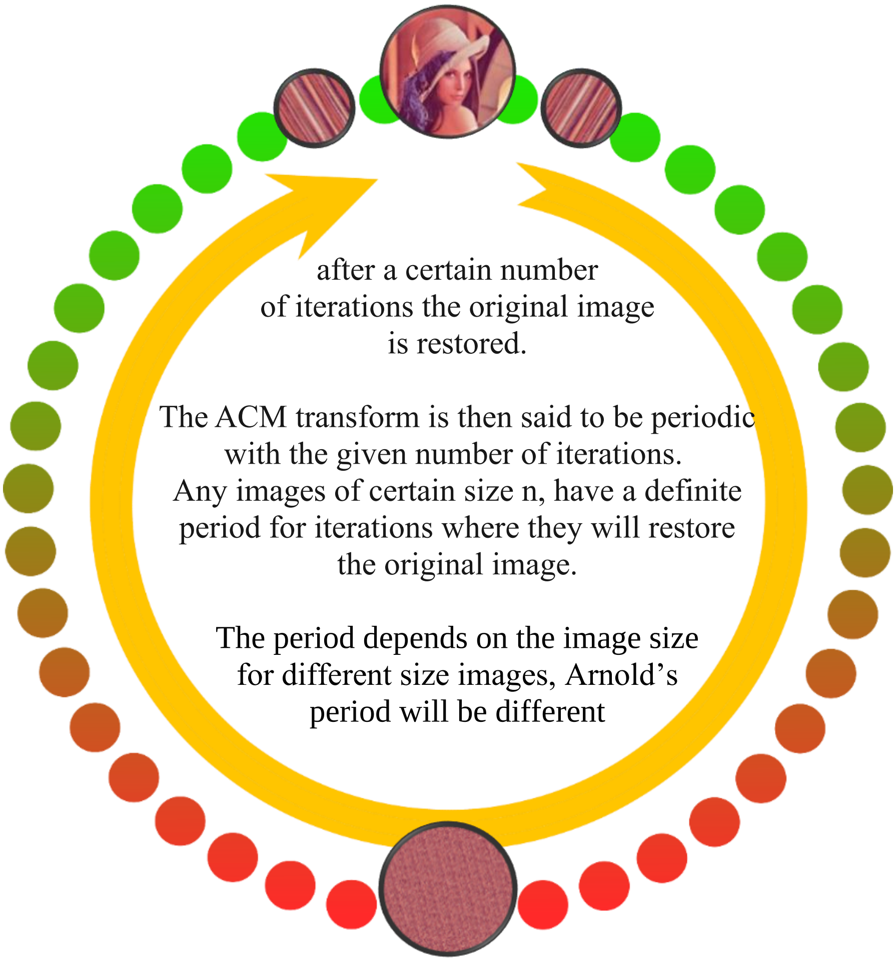
after a certain number
of iterations the original image
is restored.
The ACM transform is then said to be periodic
with the given number of iterations.
Any images of certain size n, have a definite
period for iterations where they will restore
the original image.
The period depends on the image size
for different size images, Arnold's
period will be different

Figure I7- Image changes during the Arnold map cycle

We get the number of iterations of the decryption by calculating: the period of ACM of the image minus the remainder of dividing the number of iterations by the period.

I.4.3.3 Tent chaotic map

A chaotic tent map (CTM) is a linear map which can be defined as:

$$x_{n+1} = f_n(x_n) = \begin{cases} \text{ɥ}x_n & for\ x_n < \frac{1}{2} \\ \\ \text{ɥ}(1 - x_n) & for\ ½ \leq x_n \end{cases} \tag{I.5}$$

where u∈(0,4] and x_n∈(0,1) is the output chaotic sequence. From tent bifurcation diagram shown in Fig I-8 we can see that the Tent map becomes chaotic when r ∈ (0.4,1), and it becomes purely chaotic when r=2.

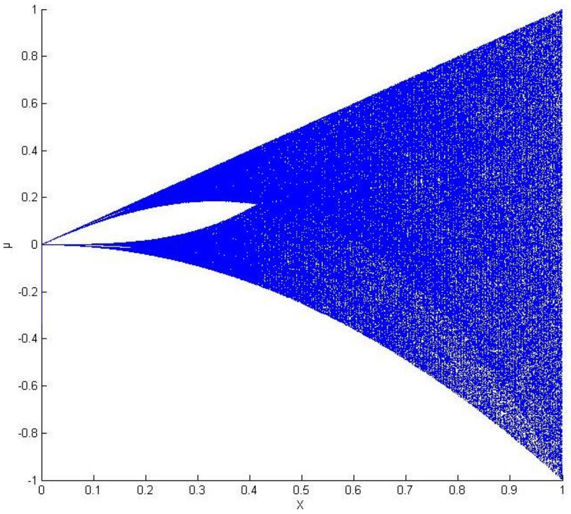

Figure I-8 Bifurcation diagram of Tent map

I.4.3.4 Henon chaotic map

Two-dimensional discrete time dynamical map having good chaotic behavior. This map take points (x_n, y_n) and maps to a new point. Mathematically it can expressed as follows:[2]

$$x_{n+1} = 1 - a{x_n}^2 + y_n \tag{I.6}$$

$$y_{n+1} = bx_n \tag{I.7}$$

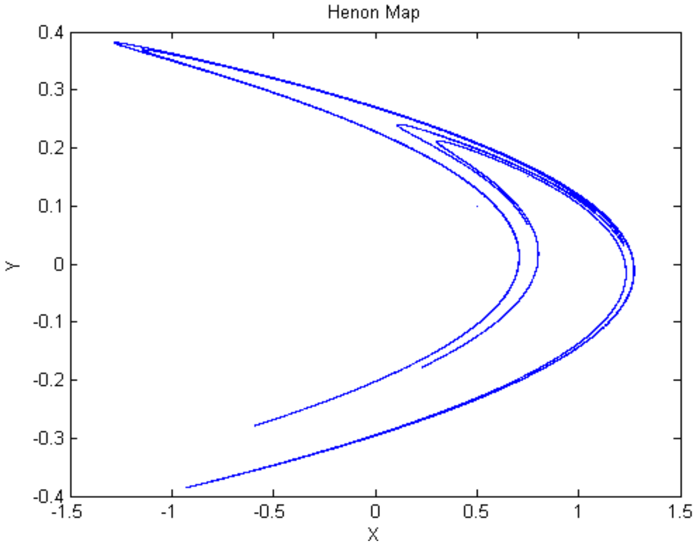

Figure I-9 Henon chaotic map

where x0 and y0 are initial conditions of the map. This system performs chaos when setting parameters to x_0 = 1.61001, y_0 = 2.9996, a = 1.7085, b = 0.32032.

I.4.3.5 Circle chaotic map

Circle map is one dimensional map and exhibit very good chaotic behavior when apply to any data. The mathematical form can be expressed as[2]:

$$\theta_{n+1} = \ mod(\theta_n + \ \Omega \frac{k}{2\pi} sin(2\pi(\theta_n),1) \qquad (I.8)$$

where θ_n = 0.4, Ω = 0.5 and $\theta_{n+1}$is computed as mod 1 and K is constant. This map has basically two important parameters Ω and K, where Ω can be frequency that is being applied externally and K is spring constant.[2]

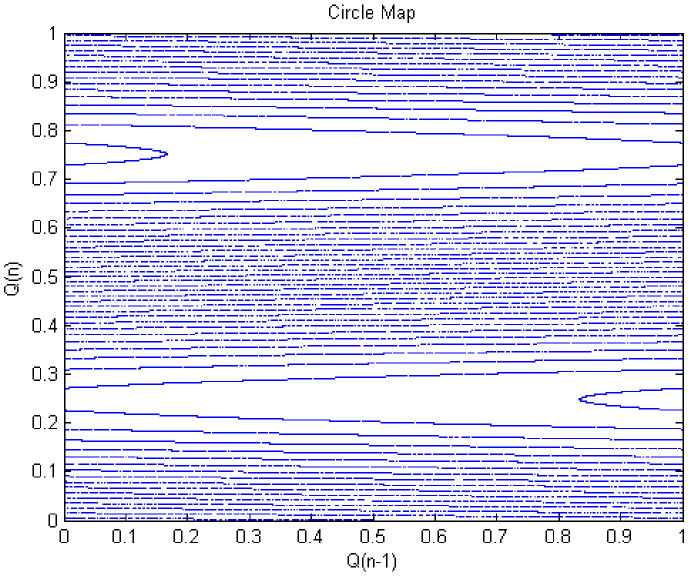

Figure I-10 Circle chaotic map

I.4.3.6 Duffing chaotic map

The duffing map is a two-dimensional discrete time dynamical system that exhibit chaotic behavior. It takes points (x_n, y_n) and give its output.[2] Duffing map equation can be expressed in Eqs. (I.9)– (I.10) respectively[2]:

$$x_{n+1} = y_n \tag{I.9}$$

$$y_{n+1} = -bx_n + ay_n - {y_n}^3 \tag{I.10}$$

where $x_0 = -1.5$, $y_0 = 1.5$, a = 2.738, b = 0.1534.

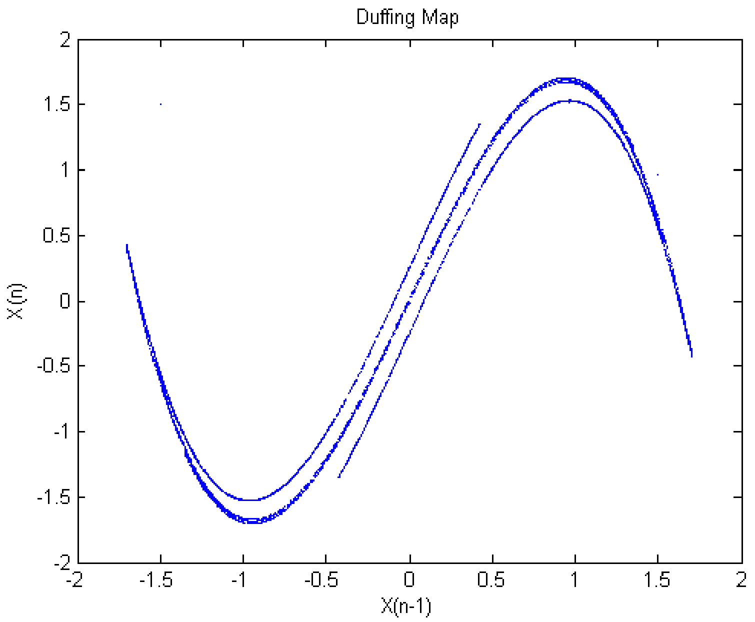

Figure I-11 Duffing chaotic map

I.4.3.7 Piecewise linear map (PWLCM)

Piecewise linear map (PWLM) is a map consists of numerous linear segments, where particular limits are permitted[5]. PWLCM can be represented as[3]:

$$z_{n+1} = (z_n, \lambda) = \begin{cases} \frac{z_n}{\lambda} & 0 \le z_n < \lambda \\ \frac{z_n - \lambda}{0.5 - \lambda} & \lambda \le z_n < 0.5 \\ F(1 - z_n, \lambda) & 0.5 \le z_n < 1 \end{cases} \qquad (I.11)$$

where $zn \in (0,1)$ with $n \in \mathbb{N}$ and $z0$ as the initial condition. $\lambda \in (0,0.5)$ is considered as the control parameter. Piecewise linear map (PWLCM) is chaotic throughout its interval of definition of control parameter λ, unlike the logistic map and the tent map, which is clearly visible in their Bifurcation diagram fig I-12.

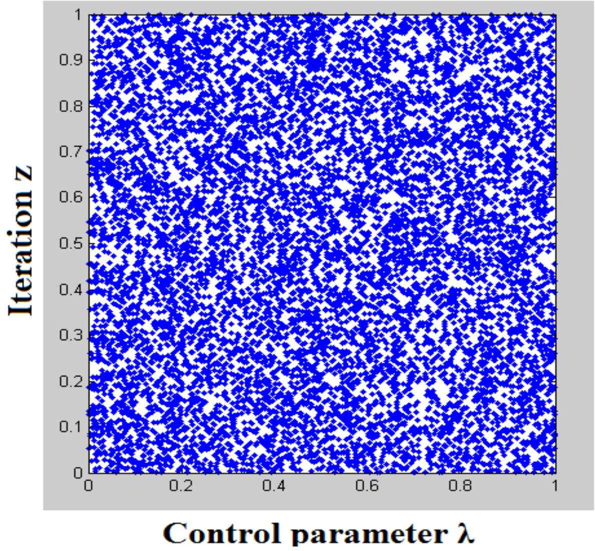

Figure I-12 Bifurcation diagram of PWLCM

I.4.3.8 Chirikov standard map

The Chirikov standard map is an area-preserving map for two canonical dynamical variables, i.j, momentum and coordinate (P,Q). It is described by the equations:

$$p_{n+1} = p_n + k * \sin(Q_n) \qquad \text{(I.11)}$$

$$Q_{n+1} = Q_n + P_{n+1} \qquad \text{(I.12)}$$

where the bars indicate the new values of variables after one map iteration and K is a dimensionless parameter that influences the degree of chaos.

Examples of the Poincare sections of the standard map on a torus are shown in the following Fig I-13 , Fig I-14.

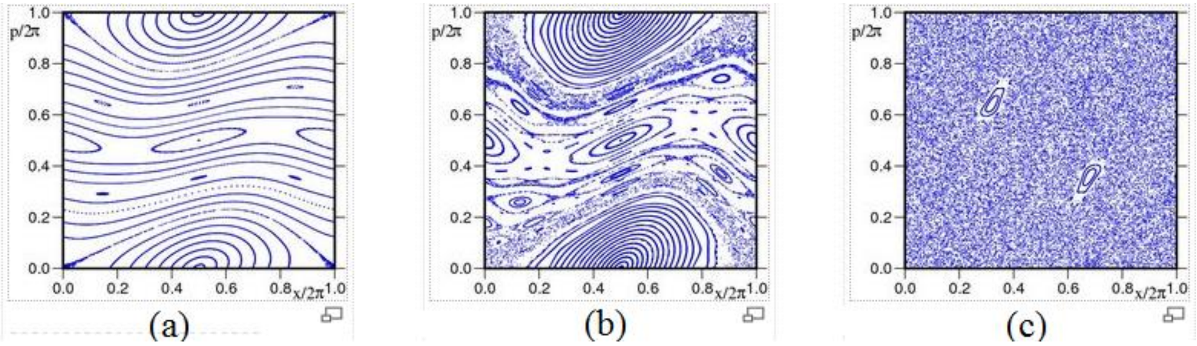

Figure I-13 (a) : when k=0.5 (b): when k=0.971635 (c): when k=5.

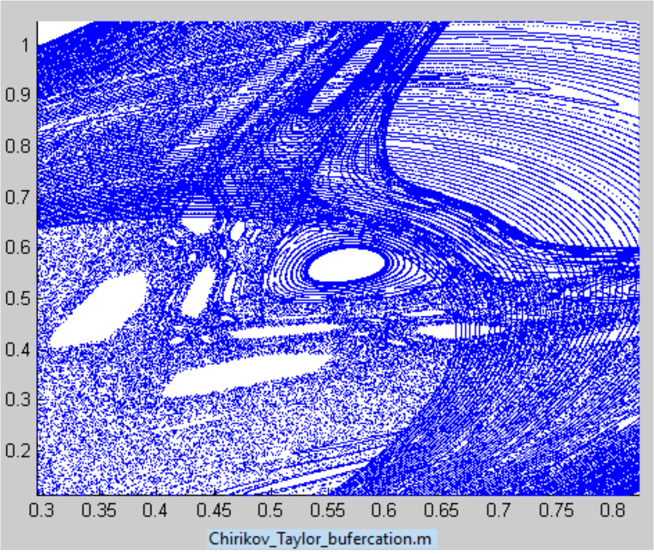

Figure I-14 Chirikov_Taylor_bufercation

I.4.3.9 Gingerbreadman map

In dynamical systems theory, the Gingerbreadman map is a chaotic two-dimensional map. It is given by the piecewise linear transformation:

$$x_{n+1} = 1 - y_n + |x_n| \qquad (I.13)$$

$$y_{n+1} = x_n \qquad (I.14)$$

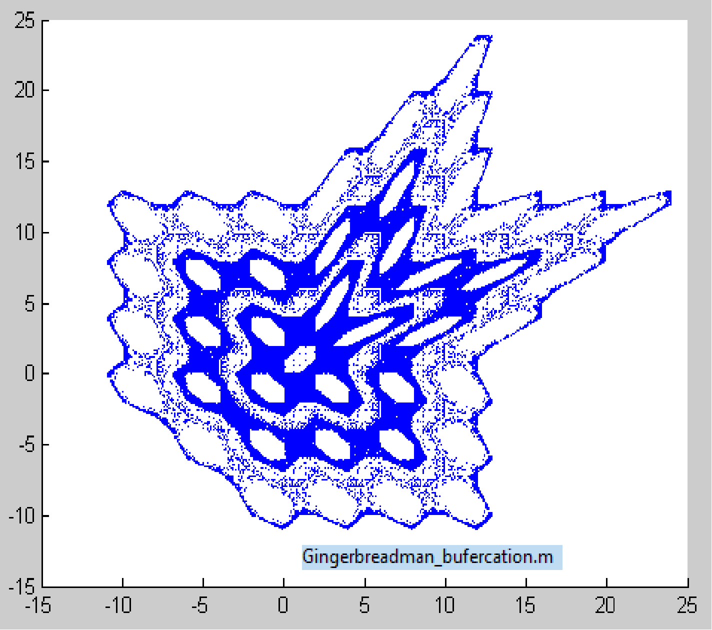

Figure I15- Bufercation diagram of Gingerbreadman map

I.5. Conclusion

In this chapter, we have recalled some of the basic concepts of cryptography and chaotic systems, with which we demystify the remaining chapters. First, we mentioned the basic concepts of cryptography, its goals and encryption/decryption working principle, then we see some classification of encryption algorithms.

In the second part of this chapter, we devoted to talking about chaotic systems, where we began by defining the concept of chaos in cryptography, then we explained Confusion and Diffusion principle and the difference between them. Finally, we have defined all the chaotic maps used in this work.

II. Image encryption based on multi-level discrete chaotic maps

II.1.Introduction

Chaotic maps are sensitive to their initial conditions and this is what distinguishes them in addition to randomness which makes it effective in encrypting images. Using two or more chaotic maps in a multilevel fashion increases efficiency of the encryption algorithm and makes it stronger.

In this chapter, we give some prior necessary definitions about digital images then we present an existing image encryption based on multilevel chaos. Finally, we will present our proposed method.

II.2. Definitions

II.2.1. Digital images

A digital image is a translation of a real image in computer language, which are the numbers, where the image is divided into small parts called pixels. Each pixel has a digital value of one or more bits that expresses its characteristics (brightness or color).

II.2.2. Binary images

Binary image pixels can only take two colors and are usually black and white, Numerically, the two values are often 0 for black, and 1 for white. Often created from gray-level images for simplified processing or printing.

II.2.3. Gray scale images

A grayscale image is an image that contains one color, which is gray, and the difference in the brightness of the pixels that make up this image leads to black and white, and the reason for distinguishing these images from any other type of color image is the lack of information that must be provided for each pixel, as it is for each pixel in the grayscale image Brightness value ranging from 0 (black) to 255 (white).

II.2.4. Color images

The pixels in color images contain more and more accurate information compared to grayscale images, where each pixel contains a mixture of primary colors (RGB). It is possible to construct (almost) all visible colors by combining the three primary colors red, green and blue. Color images in MATLAB are represented by three matrices, each matrix distinguished from the other by one of the three colors.

II.3.Image encryption based on multilevel chaotic maps

Image encryption based on multilevel chaotic maps uses several chaotic maps in succession in order to achieve a vigorous confusion and diffusion capabilities. Using multilevel chaotic maps increases the randomness among the pixel's distribution [3].

II.4.Khan et al method

Khan et al [2] method flowchart is shown in (Fig II-1). The encryption stage uses the following steps to encrypt an image using multiple chaos maps:

1- Read a color image of size 256 × 256 × 3 and transform it to three channels (R, G, B).
2- (R, G, B) channels are divided into blocks of 32 × 32 cells, and each cell of 8 × 8.
3- Pixels are shuffled within each block and for each channel using 2D-Henon map.
4- Blocks are permuted in each respective channel.
5- Pixels are distorted using one dimensional circle map.
6- Bitwise XOR for each channel respectively using 2D discrete time duffing map.

For the decryption stage we follow the precedent steps in reverse order [2]:

a) The 2D Duffing map is XOR bitwise for each channel with the output of step 5 in encryption stage.
b) In second phase reverse process bitwise XOR for each channel with circle map to get back random blocks of each channel.
c) In third phase inverse Rand block is used to get uniform blocks with shuffled pixels as done in encryption stage step 3.

d) In fourth phase inverse Henon chaotic map is treated with the output of third phase to get unshuffled pixels.

e) In fifth phase output of fourth phase is retreated with inverse of first phase in encryption stage.

f) Finally image is treated with cat command to get back into decrypted plain image

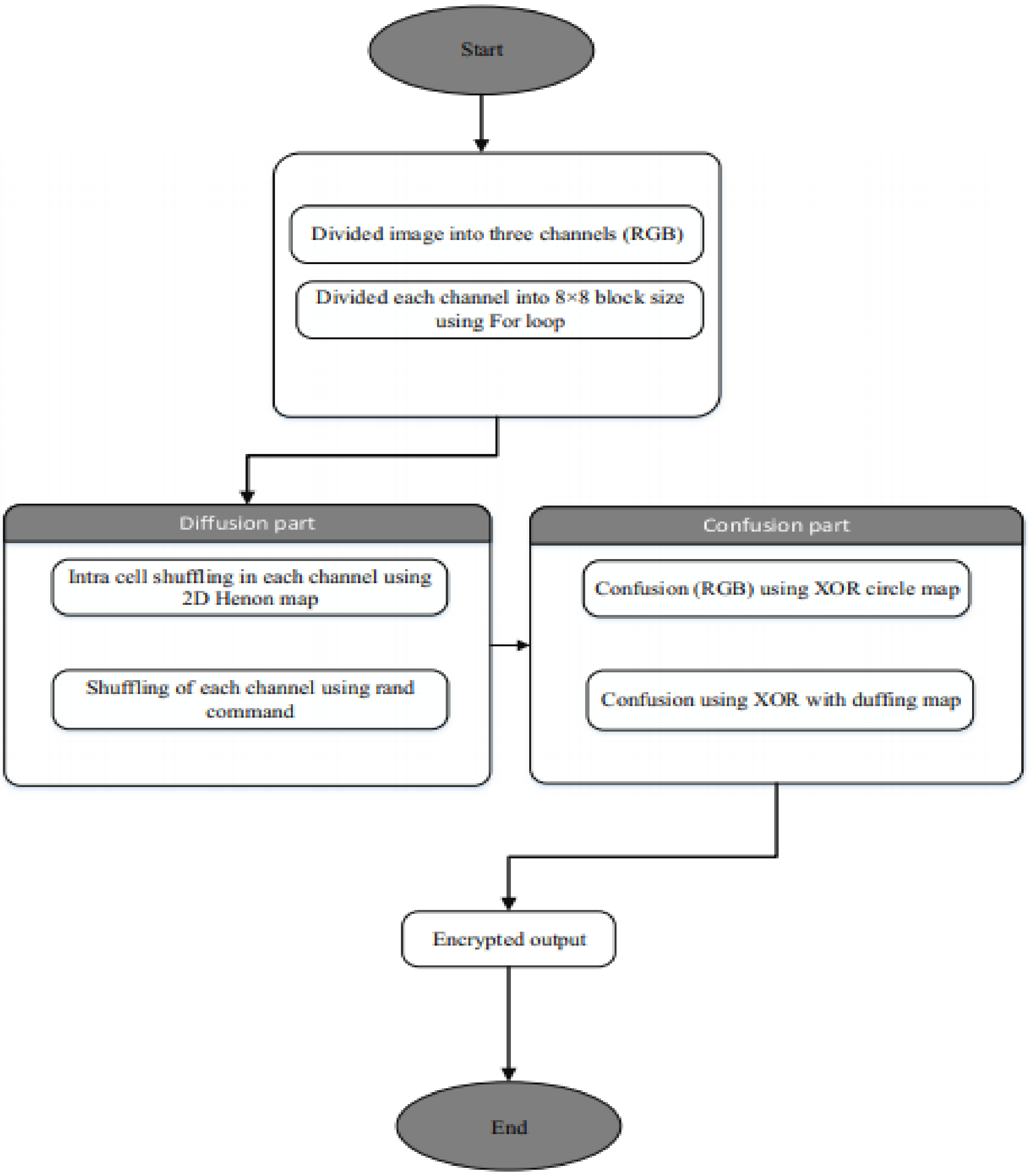
Start
Divided image into three channels (RGB)
Divided each channel into 8×8 block size using For loop
Diffusion part
Intra cell shuffling in each channel using 2D Henon map
Shuffling of each channel using rand command
Confusion part
Confusion (RGB) using XOR circle map
Confusion using XOR with duffing map
Encrypted output
End

Figure II1- Flow diagram for Khan encryption [2].

II.5.Proposed method

Figure II.2 shows the diagram of the proposed algorithm.

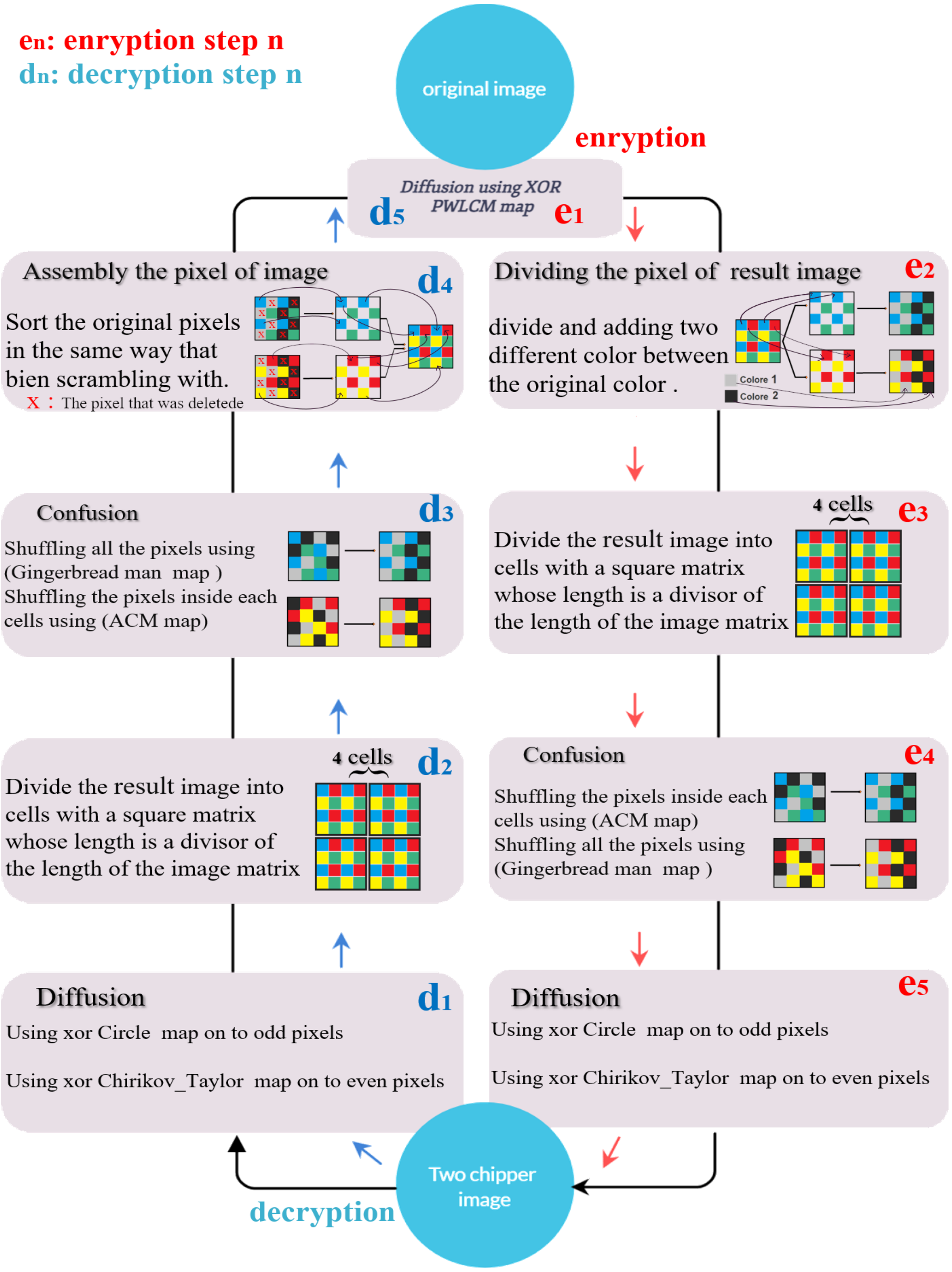
en: enryption step n
dn: decryption step n
original image
enryption
Diffusion using XOR
PWLCM map
d5
e1
Assembly the pixel of image
d4
Sort the original pixels in the same way that bien scrambling with.
X : The pixel that was deletede
Dividing the pixel of result image
e2
divide and adding two different color between the original color .
Colore 1
Colore 2
Confusion
d3
Shuffling all the pixels using (Gingerbread man map)
Shuffling the pixels inside each cells using (ACM map)
4 cells
e3
Divide the result image into cells with a square matrix whose length is a divisor of the length of the image matrix
4 cells
d2
Divide the result image into cells with a square matrix whose length is a divisor of the length of the image matrix
Confusion
e4
Shuffling the pixels inside each cells using (ACM map)
Shuffling all the pixels using (Gingerbread man map)
Diffusion
d1
Using xor Circle map on to odd pixels
Using xor Chirikov_Taylor map on to even pixels
Diffusion
e5
Using xor Circle map on to odd pixels
Using xor Chirikov_Taylor map on to even pixels
Two chipper image
decryption

Figure II2- Proposed encryption/decryption algorithm

II.5.1 Encryption stage

According to the precedent figure II.2, the encryption stage consists of the following steps:

0- Read an image that we want to encrypt (It must be a square image NxN),

1- XOR Diffusion of the image pixels using PLCM (e1 in figure II.2).

2- Dividing the image to two subimage by the following method :

Part1

- We take copy of the pixels values which are located in the odd columns with the odd line (the bleu pixels in figure II.3) ,and take copy of the pixels values which are located in the even columns with the even line (the green pixels in figure II.3).

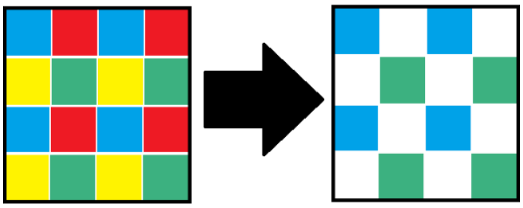

Figure II3- Sub image number 1

- In empty array that has the same size as the original image: each pixel is placed as it was in its previous position between two different values (e2 in figure II.2).
- We call the resulting image, sub image number 1.

Part2

- We take copy of the pixels values which are located in the even columns with the odd line (the red pixels in figure II.4) ,and take copy of the pixels values which are located in the odd columns with the even line (the yellow pixels in fig II.4) .

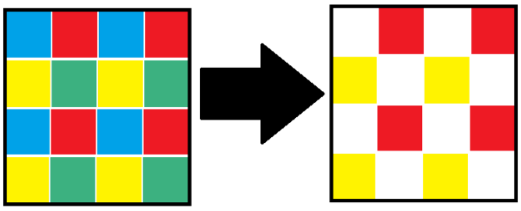

Figure II4- Sub image number 2

- In an empty array that has the same size as the original image: each pixel is placed as it was in its previous position between two different values (e1 in figure II.2, Fig II-5)
- We call the resulting image, the sub image number 2.

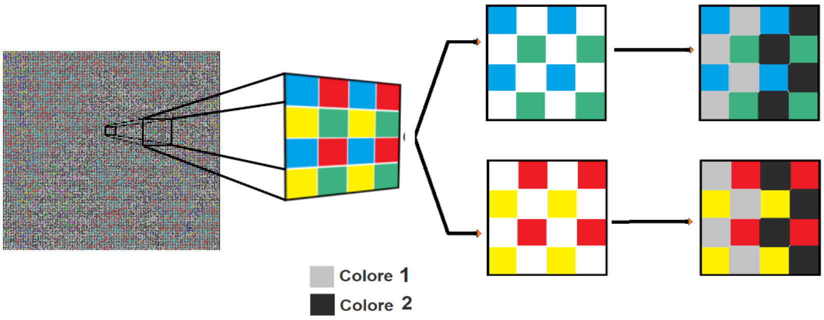

Figure II-5 How to get the two sub-image from diffusional image

3- Divide the two image into cells The number of them is optional, subject to conditions cells with square matrix whose length is a divisor of the length of the image matrix . Example:if size image is 256x256 so possible cell number {1,2,8,16,32,64,128 or 256} .

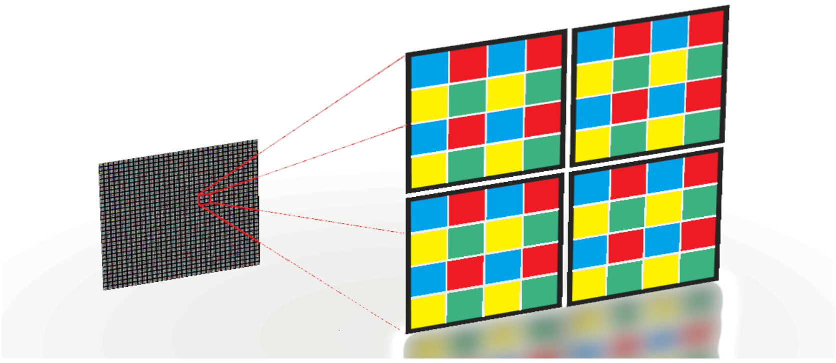

Figure II-6 fourth cells (4x4)

4- Shuffling the pixels inside the cells using (ACM) , then Shuffling all the pixels using (Gingerbread man map).

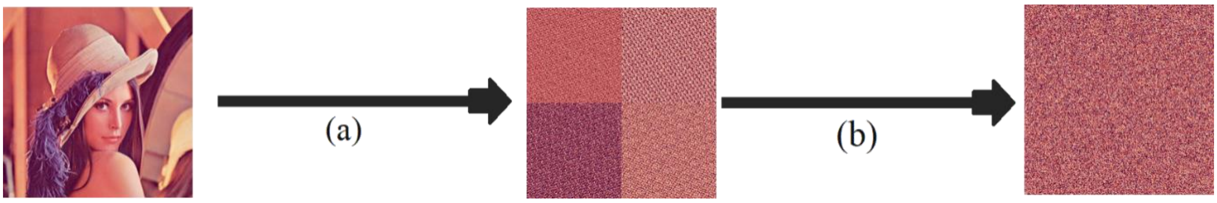

Figure II-7 (a): pixels Shuffled inside each one of the fourth cells using (ACM). (b): all the pixels Shuffled using (Gingerbread man map).

5- Using diffusion xor Circle map on the pixels in the odd lines and using diffusion xor Chirikov_Taylor map on the pixels in the even lines .

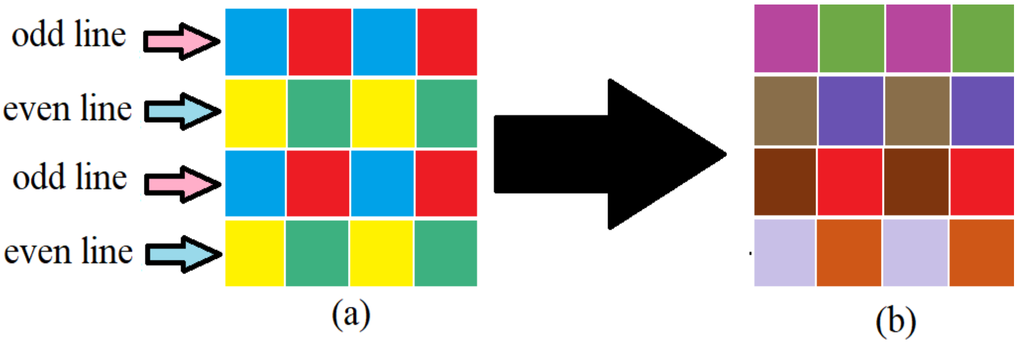

Figure II-8 (a) The image before diffusion , (b) the image after the diffusion process

II.5.2 Decryption stage

According to the precedent figure II.2, the decryption stage consists of the following steps:

0- In the decryption stage, we read two chipper image and transform them into three channels (R, G, B), then follow the encryption stage in reverse order and making sure that the settings (key or password) are correct to obtain the original image.

1- Using diffusion xor Circle map on the pixels in the odd lines and using diffusion xor Chirikov_Taylor maps on the pixels in the even lines.

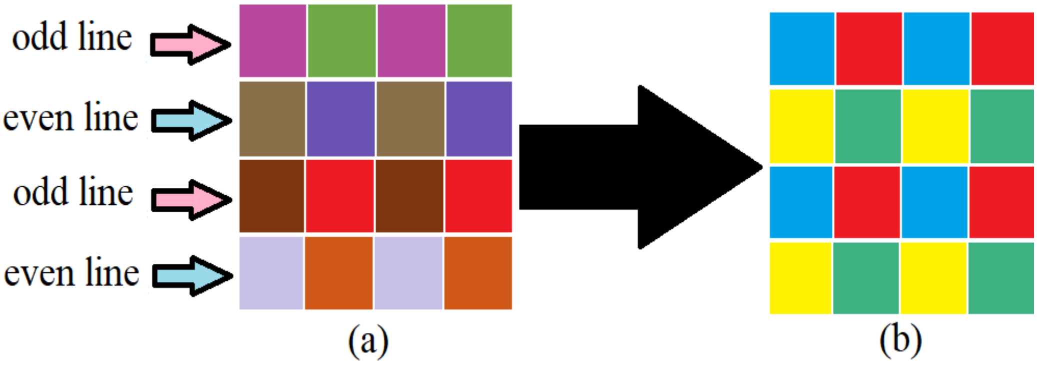

Figure II-9 **(**a) The image before diffusion , (b) the image after the diffusion process

2- Divide the result image into cells with a square matrix whose length is a divisor of the length of the image matrix (same figure II-6) (d2 in figure II.2).

3- In contrast to the encryption process, all pixels are swapped using (Gingerbread man map). Then mix the intracellular pixels using (ACM map).

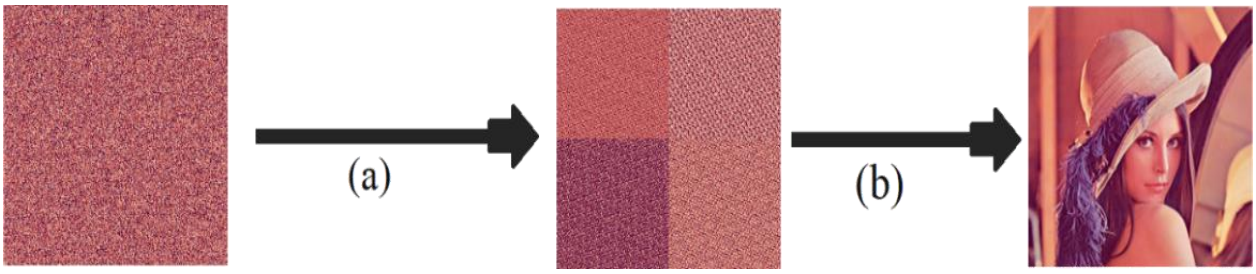

Figure II10-(a): all the pixels Shuffled using (Gingerbread man map) then (b) pixels Shuffled inside each one of the fourth cells using (ACM).

We get the number of iterations of the decryption by calculating: the period of ACM of the image minus the remainder of dividing the number of iterations by the period.

$$\text{The number of iterations of the decryption} = \text{The period of ACM of the image} - \text{Remainder}\left(\frac{\text{The number of iterations of the encryption}}{\text{The period of ACM of the image}}\right)$$

Figure II11- Equation for finding the number of iterations of decryption

The period of ACM of the image can be known by program doing a repetitive loop of the iterations and comparing the result with the original image each time with counting each iteration. If the result equated with the original image, we stop and the last number of iterations is The period of ACM of th image .

4- Sort and assembly the original pixels from the two sub-image in the same way that bien dividing with by the following method :

Part1

- From sub image 1 We take copy of the pixels values which are located in the odd columns with the even line (the bleu pixels in figure II.12) , and we take copy of the pixels values which are located in the even columns with the even line (the green pixels in figure II.12).

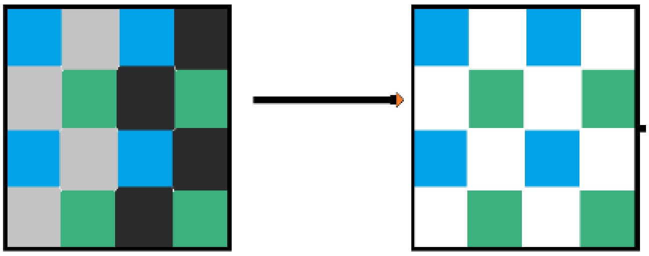

Figure II-12 How we get stored sub-image 1

- From sub image 2 We take copy of the pixels values which are located in the even columns with the odd line (the red pixels in figure II.13) , and we take copy of the pixels values which are located in the odd columns with the even line (the yellow pixels in figure II.13) .

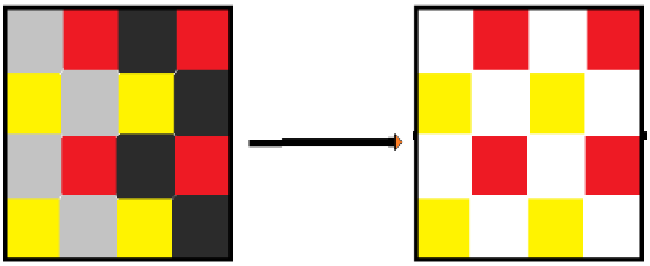

Figure II-13 How we get stored sub-image 2

Part2

- In an empty array that has the same size as the original image: assembling all the pixels from the stored sub-image(1 and 2) , each pixel is placed as it was in its previous position (d4 in figure II.2 , figure II.14).

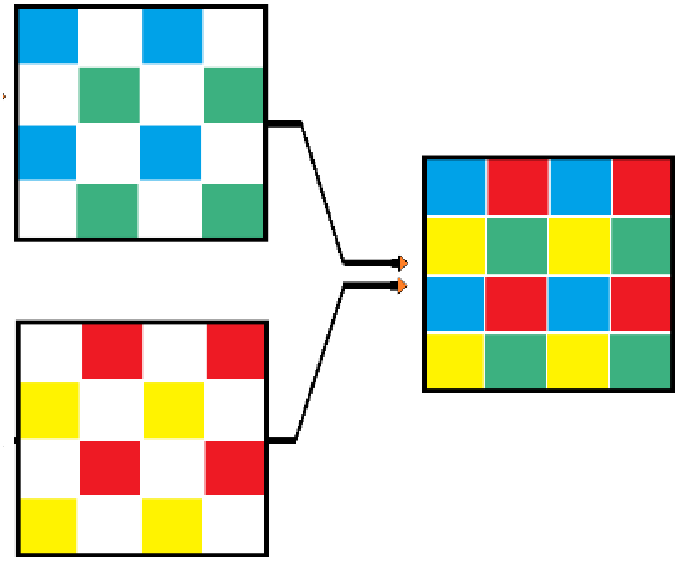

Figure II-14 assembling the all the pixels from the two stored sub-image

5- Diffusion the image using PLCM (Piecewise Linear Chaotic Map).In the event that all the settings "password" are correct, we will finally get the original image that was previously encrypted.

II.6.Conclusion

In this chapter, we have explained and defined the concepts that we need in order to accomplish the required work. Where we gave simplified definitions of digital images, binary images, gray scale images, color images and multilevel chaotic maps, then we touched on Khan method and we mentioned its encryption and decryption steps.Finely, we proposed another method and we mentioned and explained its encryption and decryption steps.

III. Simulation results and discussions

III.1. Introduction

One of the most important goals of cryptography is confidentiality, so we must take care to prevent the eavesdropper from accessing the information by knowing the strength of the proposed algorithm. We can verify this by subjecting it to a group of tests that fall under the title Security Analysis.

In this chapter, we will explain the tests along with conducting a study and comparing all the various results obtained with the results of the Khan algorithm that was previously studied.

III.2. Security analysis

During or after sending secret information may be exposed to hacking and disclosure by an unauthorized person, so we must verify that this does not happen through security analysis. Security analysis play an important role in reliability of encryption algorithms[2]. A weak encryption algorithm results in an easy hack. We have examined our suggested encryption scheme against different statistical analysis that includes histogram analysis, mean square error (MSE), correlation coefficient test, peak signal to noise ratio (PSNR), entropy, plaintext sensitivity analysis[2].

III.2.1. Histogram analysis

Histogram is the way to represent pixel occurrences in digital images[2]. Remembering the true objective to withstand the cipher only assaults and statistical assaults, the histogram ought to be uniform[5]. Uniformity is one of the aspect of encrypted images to hide the actual content of digital images[2]. We took standard Lena image of size 256 × 256 × 3 and divided into three respective channels (RGB)[3]. The histograms of each channel at plain level comprises sharp peaks(see Fig III-1).Whereas histograms of cipher images are distributed equally over the entire region with no sharp peaks (see Fig III-3, Fig III-4 and Fig III-5). The investigation of histograms of encrypted images clearly reveals that the algorithm used does not provide any clue of passive and active eavesdropping to easily obtain any secret information due to uniformity of histograms.

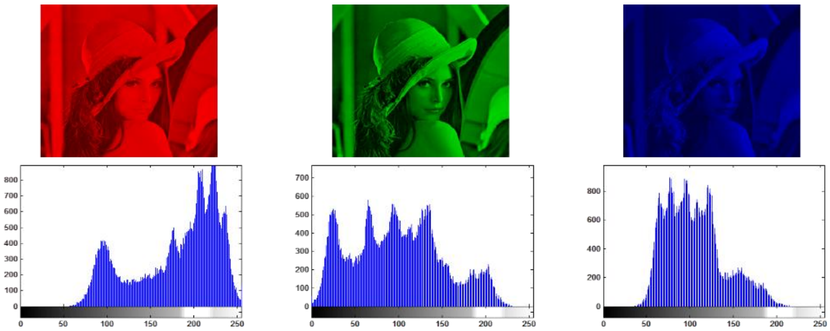

Figure III-1 Histogram of Lenna standard image.

III.2.2 Correlation

The pixels of an original image always have tremendous relationship with their adjacent pixels, either in vertical, horizontal or diagonal directions[5]. So, in order to obtain a fine cipher image, the wave-correlation value between the pixels must be reduced. The value of correlation coefficient (CC) lies within the interval [−1,1]. For totally uncorrelated image the value of CC quite closed to zero, whereas −1 corresponds to negative correlation and 1 belong to positive correlation[2]. For cryptographically secure encryption algorithms CC remains closed to zero[2].

We have added tables to examined the relation of adjacent pixels in three different directions i.e. vertically, horizontally and diagonally (see Fig III-2, Fig III-3, Fig III-4 and Fig III-5 and Tables III-2, III-3 and III-4). The mathematically expressions for correlation coefficient are given by[2]:

$$\gamma_{XY} = \frac{\delta_{XY}}{\sqrt{\delta^2{}_X\delta^2{}_Y}} \qquad \textbf{(III.1)}$$

where δ_{XY} is known as covariance of random variables X and Y, μ_X and μ_Y are expected values of random variables and $\delta^2{}_X$ and $\delta^2{}_y$are variances respectively given below[2]:

$$\delta_{XY}=\sum_{j=1}^{N}\frac{(X_j-\mu_X)(Y_j-\mu_Y)}{N}.\ \delta^2{}_X=\sum_{j=1}^{N}\frac{(X_j-E(X)^2)}{N}.\ \delta^2{}_Y=\sum_{j=1}^{N}\frac{(Y_j-E(Y)^2)}{N}. \qquad \textbf{(III.2)}$$

The linear relationship can be observed among the pixels of plain image (see Figure III-2) and corresponding numerical value of CC is closed to unity (see Tables III-2, III-3 and III-4).

The application of our proposed image encryption scheme make it possible to break the neighboring relation among pixels. The value of CC reduces to zero which shows the strength of our anticipated technique (see Fig III-3, Fig III-4 and Fig III-5 and Tables III-2, III-3 and III-4).

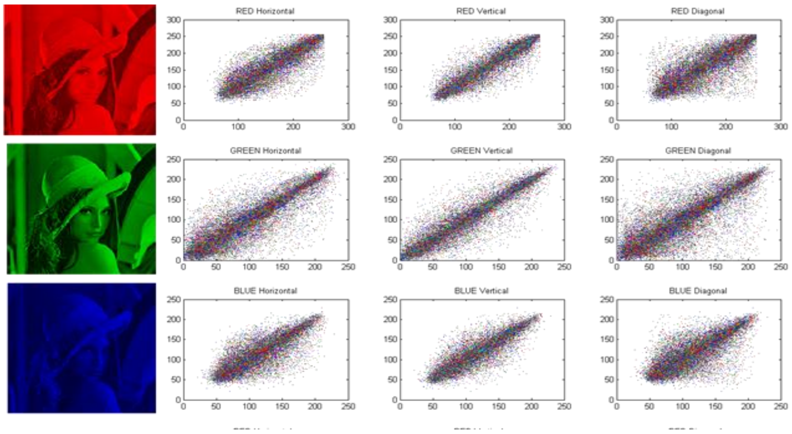

Figure III-2 correlation of Lenna standard image

III.2.3. Mean square error

For authenticity we evaluated mean square error (MSE) for Lena plain and encrypted image which showed reliability of the proposed algorithm. (MSE) can be calculated as in Eq. (III.2).

$$MSE = \frac{1}{\mathrm{M}*\mathrm{N}}\sum_{\mathrm{i}=1}^{M}\sum_{\mathrm{j}=1}^{N}\left(A_{(i,j)} - Q_{(i,j)}\right) \qquad \textbf{(III.3)}$$

where $A_{(i,j)}$ and $Q_{(i,j)}$ show pixels are positioned at i th row and j th column, M×N is the overall extent (size) of image of original and enciphered image respectively, MSE value must be large enough to provide robust security against different cryptographic attakcs[2], (see Tables 5 and 6).

III.2.4. Peak signal to noise ratio

Peak signal to noise ratio (PSNR) can be used to assess the quality of encryption technique. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image [2]. The mathematical expression for PSNR is given in Eq. (III.4).

$$PSNR = 10log_{10}\frac{I^2max}{MSE} \qquad \textbf{(III.4)}$$

where Imaxis maximum value of image, for better security the value for PSNR should be low enough to comply with good security (see Tables III-5 and III-6).

III.2.5. Entropy

Entropy analysis is measurable quantity which measure randomness in the information content of the test image. The entropy can be represented by the following expression:

$$H = -\sum_{j=0}^{\mathrm{N}-1} P(X_j)log_b P(X_j) \qquad \textbf{(III.5)}$$

where $P(X_j)$ represent occurrence of probability of symbol X_j. The theoretical value of entropy is 8 for 8-bit image and practical values through our offered scheme is 7.999, which is quite close to ideal value [3]. (see Tables III-7, III-8 and III-9). This reveals that, our suggested encryption scheme based on multiple chaotic iterative maps is considerably increases the randomness among the pixel's distribution of original image. The histogram of encrypted image is uniform and contain no similarity of plain image which makes it impossible for eavesdropper to extract any information[2].

III.2.6. Mean absolute error

Mean absolute error (MAE) is criterion (model) to inspect pursuance of resisting against differential aggression. We calculated mean absolute error (MAE) between original and encrypted images. MAE value must be large enough to ensure the robustness of cryptosystem. We evaluated our proposed scheme for the size of 256 × 256 × 3 test images. Let $E_{(i,j)}$ and $F_{(i,j)}$ be two grey level pixels at i th row and j th column of an image extent (size) M × N for both plain and enciphered image then Eq. (III.6).for two respectively images can be written as:

$$MAE = \frac{1}{\mathrm{M*N}}\sum_{\mathrm{i}=0}^{M-1}\sum_{\mathrm{j}=0}^{N-1}(E_{(i,j)} - F_{(i,j)}) \qquad \textbf{(III.6)}$$

III.2.7. Differential attacks analysis

The differential assault is one of the most generally utilized and efficient security assaults. The unified average change intensity (UACI) and formally number of pixel change rate (NPCR) are two measures that can be utilized to test whether encoding of image calculation has the capability to resist differential assault[5]. The capability of battling against differential attacks is measured by comparing the differences between two ciphers images i-e., minor change in plain image results completely change in cipher image. Thus, much difference between encrypted forms is expected in order to keep high security[2].

III.2.7.1. Number of pixels changing rate

Number of pixels changing rate (NPCR) actually finds rate of change of pixels' location amid plain and encrypted image. Here we take two encrypted images for NPCR test and had difference of only pixel, we represented cipher image with E1(i, j)and E2(i, j) whose analogous plain image have only pixel difference. An array V(i, j) can be calculated using E1(i, j)and E2(i, j) respectively though NPCR can be evaluated as in Eq. (III.7).

$$NPCR = \frac{(\sum_{i,j} V_{i,j})}{\mathrm{W} * \mathrm{H}} * 100 \qquad \textbf{(III.7)}$$

where $V_{i,j}$ in above equation can be construe as:

$$V_{i,j} = \begin{cases} 0 & E_{1(i,j)} = E_{2(i,j)} \\ 1 & E_{1(i,j)} \neq E_{2(i,j)} \end{cases}$$

III.2.7.2. Unified average change intensity

The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image and expression for UACI is given below:

$$\boldsymbol{UACI} = \frac{\mathbf{1}}{\mathrm{W} * \mathrm{H}} \sum\nolimits_{\boldsymbol{i,j}} \frac{[E_{1(i,j)} - E_{2(i,j)}]}{\mathbf{255}} \qquad \textbf{(III.8)}$$

We have tested Lena image of size 256 × 256 × 3 as a test image for our proposed algorithm. We examined that larger unified average changing rate means our encryption algorithms is quite excellent and mark i.e. encryption performance increases. We showed input image onepixel difference between two source images, the change that is made were almost 0.01% at input side of images for respected ciphered images. Results are tabulated in Tables III-11and III-12.

III.3. Results and discussiomns

Discussing the obtained results from both the proposed algorithm and the reference algorithm and comparing them in terms of security tests.

Table III-1 Encryption settings (parameter)

Name of settings (parameter)	Encryption settings	Decryption settings
Cells length:	256	256
Color number one:	255	255
Color number two:	0	
Pwlcm	x(1)=0.121 p=0.305	x(1)=0.121 p=0.305
Acm_map (number of iteration)	11	181
Gingerbreadman_map	y(1)=0.071 x(1)=3.91	y(1)=0.071 x(1)=3.91
Equation_Circle	o(1)=0.321 k=20000 om=0.39	o(1)=0.321 k=20000 m=0.39
Chirikov_Taylor_map	p(1)=0.15 o(1)=0.5 k=0.39	p(1)=0.15 o(1)=0.5 k=0.39

III.3.1 Correlation results

In the original image, the nearby pixels along the horizontal, vertical and radial orders are distributed in the direction of the main diagonal, which indicates that the pixels in the original image are linearly related and in the case of encoded images, the pixels are distributed in a scattered fashion (see figures III.3, III.4 and III.5).

The results of the numerical values of the correlation coefficient indicate that our proposed scheme is able to add confusion and remove adjacency relationship pixels. The proposed technique separates nearby pixels in the plain text image after encryption is performed. Outperforms registered coding schemes (see tables III.3, III.4 and III.5).

Table III-2 Correlation coefficient of various plain and encrypted images

Image	Plain image			Encrypted image		
	Correlation coefficient			Correlation coefficient		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.9342	0.9725	0.9231	0.0427	0.0033	0.0009
Baboon	0.7977	0.8061	0.8038	-0.0021	0.0044	0.0404
pepper	0.9704	0.9663	0.9564	0.0464	0.0036	-0.0003

Table III-3 Correlation coefficient of red, green and blue channels for various images

Channel	CC	Lena		Baboon		Re f[2]
		Plain	Cipher	Plain	Cipher	
R	HC	0.94794	0.04027	0.86931	0.00121	0.0017
	DC	0.92312	0.00636	0.80606	0.00438	0.0049
	VC	0.97249	0.00589	0.80375	0.04036	−0.0004
G	HC	0.94203	0.04614	0.71640	-0.0012	0.0011
	DC	0.91740	0.00329	0.62158	0.00609	−0.0002
	VC	0.97080	0.00166	0.62746	0.03606	0.0076
B	HC	0.91272	0.04139	0.80746	0.00508	−0.0030
	DC	0.75955	-0.0001	0.78812	0.00337	0.0049
	VC	0.94746	0.00132	0.75955	0.04189	0.0050

We note that there is convergence in terms of results, in which the reference algorithm is slightly better.

Table III-4 Comparison of correlation coefficient different direction

Direction	Horizontal	Diagonal	Vertical
Original Image	0.9518	0.9293	0.9769
Proposed	-0.0021	0.0404	0.0044
Ref[2]	0.0054	0.0054	0.0016

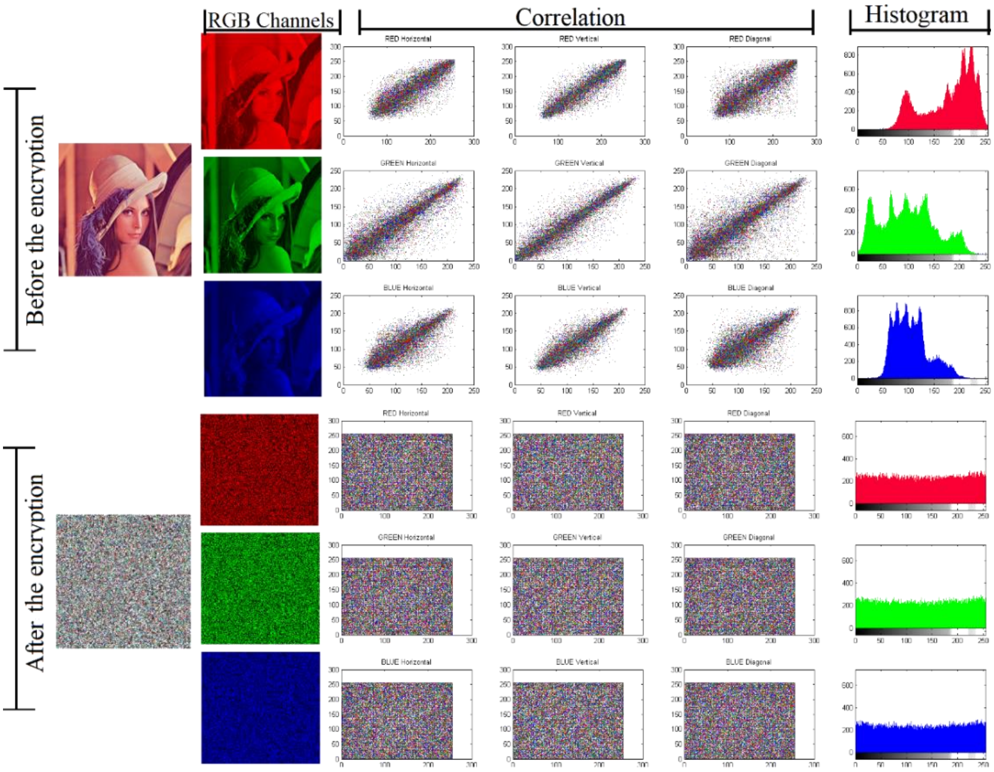

Figure III-3 the correlation and the histogram of three channel of Lenna image after and before encryption

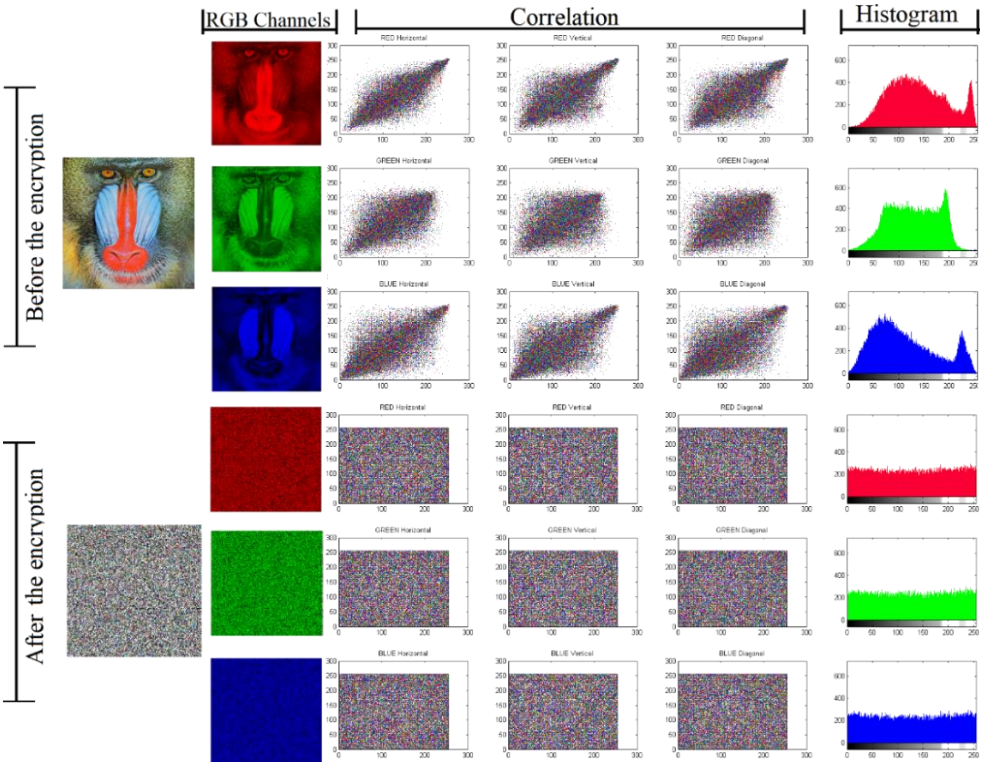

Figure III-4 the correlation and the histogram of three channel of baboon image after and before encryption

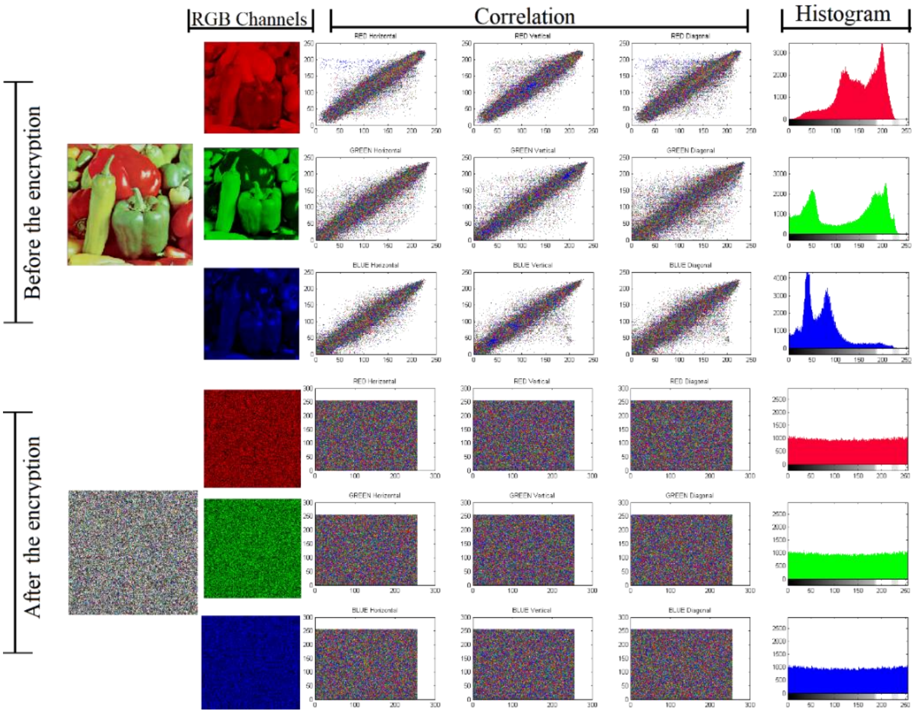

Figure III-5 the correlation and the histogram of three channel of pepper image after and before encryption

III.3.2 MSE and PSNR results

We evaluated mean square error (MSE) and Peak signal to noise ratio (PSNR) for the plain images and encrypted images which showed reliability of the proposed algorithm.

MSE value must be large enough to provide robust security against different , cryptographic attacks, and for better security the value for PSNR should be low enough to comply with good security (see Tables III.5 and III.6).

Table III-5 MSE and PSNR values of red, green and blue channels for various images

Image	Chanels	Size	Projected Techniques	
			MSE	PSNR
Lena	Red	256 × 256	11,345.24	7.58266
	Green	256 × 256	9,775.097	8.22959
	Blue	256 × 256	7,840.227	9.18751
Baboon	Red	256 × 256	9,350.365	8.42251
	Green	256 × 256	8,597.473	8.78709
	Blue	256 × 256	10,439.87	7.94385
Pepper	Red	512 × 512	8,695.342	8.73793
	Geen	512 × 512	11,953.15	7.35597

	Blue	512 × 512	11,847.45	7.39455

Table III-6 Comparison of average MSE and PSNR values with existing values of various images

Images	Size	Projected Technique		Ref[2]	
		Avg.MSE	Avg.PSNR	MSE	PSNR
Lena	256 × 256	09,653.52	8.33325	10,869.73	7.7677
Baboon	256 × 256	09,462.57	8.38448	10,930.33	7.7447
Pepper	512 × 512	10,831.98	7.82948	10,897.50	7.7577

We note that there is convergence in terms of results, in which the reference algorithm is slightly better

III.3.3 Entropy result

The entropy criterion calculates the randomness of the information in the encrypted image. The proposed algorithm showed values ranging from 7.89 to 7.9 which is a good values because its very close to 8 which is the ideal value of a 8-bit image (see Tables III.7,III.8 and III.9).

The result between the proposed algorithm and the reference algorithms can be considered equivalent in terms of results image (see Tables III.9).

Table III-7 Entropy values of red, green and blue channels for various images

Images	Channels	Size	Entropy values
Lena	Red	256x256	7.8998
	Green	256x256	7.9008
	Blue	256x256	7.8997
Baboon	Red	256x256	7.8987
	Green	256x256	7.8974
	Blue	256x256	7.8987
pepper	Red	512x512	7.9023
	Green	512x512	7.9020
	Blue	512x512	7.9026

Table III-8 Entropy values for various

Images	size	Projected Technique Evaluated value
Lena	256X256	7.9012
Baboon	256X256	7.8992
Pepper	512X512	7.9025

Table III-9 Comparison of Entropy value for red, green and blue channels of Lena image

Algorithms	Channels Entropy values		
	Red	Green	Blue
Proposed Algorithm	7.8997	7.9008	7.8990
Ref[2]	7.9973	7.9972	7.9975

III.3.4 MAE Result

Table III-10 MAE test analysis for Lena, Baboon and Pepper images

Images	size	Projected Technique MAE	Ref[[2]
Lena	256 × 256	81	87
Baboon	256 × 256	80.3	92
Pepper	512 × 512	85.19	92

The result can be considered between the proposed algorithm and the reference algorithms are very close in terms of results (see table III.10).

III.3.5 NPCR and UACI result

can be calculated using the equation () , in the result Pixel Number Change Rate (NPCR) The closer the number is to 100, the better

The test result was excellent (see table III-11). Which was better than the result of the reference algorithm (see table III-12)

Table III-11 NPCR and UACI test for chipper images

Images	size	Tests	Red channel	Green channel	Blue channel
Lena	256 × 256	NPCR	0.9965	99.64	99.65
		UACI	0.3410	31.91	29.18
Baboon	256 × 256	NPCR	0.9966	99.66	99.63
		UACI	0.3129	30.26	32.82
Pepper	512 × 512	NPCR	0.9962	99.50	99.50
		UACI	0.3038	35.01	34.82

Table III-12 Comparison of NPCR UACI

Images	size	Tests	Combined layers	Ref[[2]
Lena	256 × 256	NPCR	99.64	99.60
		UACI	31.73	33.37
Baboon	256 × 256	NPCR	99.65	99.61
		UACI	31.47	33.51

We note that the result of the proposed algorithm is better than the result of the reference algorithm

III.4. Conclusion

In this chapter, we study the strength and effectiveness of the proposed algorithm tested against different encryption quality measures.

Then, we showed the simulation results with an explanation of the various attacks that the encrypted image could be exposed to, and compared them with the results of the pre-existing Khan algorithm, where we noticed a convergence in the results of the two algorithms.

Conclusion and future work

Conclusion and future work

The subject of this work is to present an image encryption algorithm based on multilevel chaotic maps.

In the beginning, we recalled the basic concepts of cryptography (encryption/decryption principle) and chaos, where we mentioned the confusion and diffusion principle and the advantages of chaos topology mixing, strange attractor, ergodicity, randomness and dependence on its initial conditions and how they can be exploited in order to produce a strong cryptographic algorithm. We also reviewed all chaotic maps exploited in this work.

Next, we explained the types of images that can be encountered during the encryption process. We reviewed Khan's algorithm concept of encrypting images using multi-level chaotic maps. We also presented and explained our algorithm based on the same concept.

Finally, under the title of security analysis, we showed the simulation results and performed a comparative analysis with Khan's results due to the two algorithms sharing the concept of encoding images based on multi-level chaotic maps. Simulation results are tests like Histogram, Correlation Coefficient, MSE, PSNR, Entropy and NPCR. These tests show how strong or weak the proposed algorithm is.

Finally, we found that the multilevel chaotic map added confusion and diffusion capability to encryption algorithm.

In future work we will try to improve the results of the algorithm, because of the approaching delivery date of this observation, it can be said that the settings in which the encryption was done is preliminary and can be improved, as there was not enough time for testing and finding good settings that can give us better results, the algorithm can also be speeded up by By replacing Arnold's cat map equation with a faster shuffling equation.

Finally, if the algorithm is fast enough and performs well, it can be used to encode videos.

References

1. Image encryption El-samie, Abd Fathi, E,H, Hossam Eladin Ibrahim, F Mai, Osama, S Saleh, A. Taylor & Francis Group. CRC Press.2014.
2. Khan- Majid, Fawad- Masood , *A novel chaotic image encryption technique based on multiple discrete dynamical maps* , Multimedia Tools and Applications , 06 June 2019.
3. Azoug- Seif Eddine , thèse –doctorat Université Ferhat abas –Sétif " Développement et implémentation des techniques de cryptage des signaux image et vidéo ".
4. Vol. 354. Ljupco Kocarev and Shiguo Lian (Eds.) *Chaos-Based Cryptography*, 2011 ISBN 978-3-642-20541-5.
5. Suneja.K et al , *A Review of Chaos based Image Encryption* , Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4
6. B. Schneier, Cryptographie appliquée: algorithmes, protocoles et codes source en C, Vuibert Informatique, 2001.
7. Shannon, C. E. (October 1949). "Communication Theory of Secrecy Systems*".
8. Ali Soleymani,1 Md Jan Nordin,2 and Elankovan Sundararajan1 “A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map”
9. E. Lorenz, Predictability: Does the Flap of a Butterfly’s Wings in Brazil Set Off a Tornado in Texas, American Association for the Advancement of Science.