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 : Electronique des systèmes embarqués

Par

- **DABA Zakaria**
- **CHIKH Tawfik**

Intitulé

Face Encryption based on Chaotic Maps

Soutenu le : ……

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
Dr. KHERRAT F	*MAA*	*Président*	*Univ-BBA*
Dr. BEKKOUCHE Tewfik	*MCA*	*Encadreur*	*Univ-BBA*
Dr. BENAMER A	*MAB*	*Examinateur*	*Univ-BBA*

Année Universitaire 2023/2024

First of all, I thank ALLAH for helping me and giving me the courage, will and patience to complete this work.

I would like to thank Dr. BEKKOUCHE Tewfik, supervisor of this thesis, for the support, wise advice and great kindness during the development of this modest work.

I want to take the opportunity to have mercy on my father, and thanking my mom for making shore that I complete my studies journey I love you mom, and to my brother imad for bear with me and my uncle boualem for all his help, and to all my friends fouad,mouhib,ramy thank you all.

Finally, I went to think all members of our families with all our affectionate gratitude for their

support and encouragement.

-DABA ZAKARIA-

First and foremost, I thank Allah, the Almighty, who granted me the courage and strength to complete my work. Without His mercy, this work would not have seen the light of day. To Him belongs my greatest praise for the health and patience He granted me throughout all my years of study.

At the end of this work, I would like to thank Dr. Toufik Bekkouche for supervising my thesis. I would like to express my deep gratitude to him for his valuable help, guidance, attentive advice, and support throughout this work.

I would like to say a huge thank you to my parents for their support and comfort when I needed it, and I also wish to express all my love and gratitude to my sisters, brothers, and my friends Abdel Razak and Zerouti.

Finally, to everyone who contributed, directly or indirectly, to the completion of this work, I express here my profound gratitude.

-Chikh tawfik-

Abstract

The rapid advancement in high-quality image capture transmission and storage has led to their widespread use by both ordinary users and professionals, consequently risking unauthorized access. To address this issue, a technique for image encryption has been proposed. Despite being widely used to protect information, many encryption algorithms encrypt the entire image without considering the varying importance of different regions within it, leading to inefficiency and computational waste.

In this document we studied a region-based selective image encryption technique using a chaotic approach. This proposed technique focuses on encrypting and reconstructing facial regions in the image. Firstly, the face is extracted from the image, followed by encryption and reconstruction into the original image. The second stage involves decryption which is the reverse of the first stage. Selective encryption of facial regions allows for high efficiency and real-time performance. Security analysis indicates that our proposed encryption algorithm demonstrates strong.

ملخص

أدى التقدم السريع في نقل وتخزين الصور عالية الجودة إلى استخدامها على نطاق واسع من قبل كل من المستخدمين العاديين والمحترفين، وبالتالي المخاطرة بالوصول غير المصرح به. ولمعالجة هذه المشكلة، تم اقتراح تقنية لتشفير الصور. على الرغم من استخدامها على نطاق واسع لحماية المعلومات، فإن العديد من خوارزميات التشفير تقوم بتشفير الصورة بأكملها دون مراعاة الأهمية المتفاوتة للمناطق المختلفة داخلها، مما يؤدي إلى عدم الكفاءة والهدر الحسابي.

قمنا في هذه الوثيقة بدراسة تقنية تشفير الصور الانتقائية على أساس المنطقة باستخدام نهج فوضوي. تركز هذه التقنية المقترحة على تشفير وإعادة بناء مناطق الوجه في الصورة. أولاً، يتم استخراج الوجه من الصورة، يليه التشفير وإعادة البناء في الصورة الأصلية. تتضمن المرحلة الثانية فك التشفير وهو عكس المرحلة الأولى. يسمح التشفير الانتقائي لمناطق الوجه بكفاءة عالية وأداء في الوقت الفعلي. يشير التحليل الأمني إلى أن خوارزمية التشفير المقترحة لدينا تثبت قوتها.

Résumé

Les progrès rapides dans la transmission et le stockage de captures d'images de haute qualité ont conduit à leur utilisation généralisée par les utilisateurs ordinaires et les professionnels, risquant ainsi d'être accessibles sans autorisation. Pour résoudre ce problème, une technique de cryptage d’images a été proposée. Bien qu'ils soient largement utilisés pour protéger les informations, de nombreux algorithmes de chiffrement chiffrent l'image entière sans tenir compte de l'importance variable des différentes régions qui la composent, ce qui entraîne une inefficacité et un gaspillage de calcul.

Dans ce document, nous avons étudié une technique de chiffrement sélectif d’images basée sur une région utilisant une approche chaotique. Cette technique proposée se concentre sur le cryptage et la reconstruction des régions du visage dans l'image. Tout d’abord, le visage est extrait de l’image, suivi d’un cryptage et d’une reconstruction dans l’image originale. La deuxième étape concerne le décryptage qui est l’inverse de la première étape. Le cryptage sélectif des régions du visage permet une efficacité élevée et des performances en temps réel. L'analyse de sécurité indique que l'algorithme de cryptage proposé est solide.

Table of Contents

Table of Contents

Table of figures

General Introduction

There has been an increase in demand for securing private and sensitive information, especially in recent years following technological and informational advancements. With the emergence of electronic threats such as malware and cyber-attacks, institutions and companies are under extra pressure to enhance data protection and ensure privacy in communication systems and social networks. Among the most common and widely used types of information are text messages, voice messages, images, videos, and others.

The rapid dissemination of digital images across networks exposes them to unauthorized use, necessitating enhanced protection due to their large size and complexities compared to textual information. They rely on advanced encryption algorithms. Many researchers have developed advanced encryption algorithms to enhance security and address weaknesses in digital image encryption, including public and private encryption techniques, encryption using a single secret key for both encryption and decryption, and encryption using chaos techniques.

In our work, we will focus on encryption using chaos techniques, studying a technique for encrypting facial regions in color images using chaotic maps. This technique will specifically focus on encrypting the facial region only using the Viola-Jones theory, which detects and extracts the facial region in the image, followed by the encryption process.

The manuscript is divided into three chapters according to the following organization:

- Chapter One: We provide a simple definition of digital images and some of their characteristics. We discuss the Viola-Jones theory for detecting facial regions, in addition to a brief explanation of encryption and chaotic maps.
- Chapter Two: in this chapter, we have discussed the cryptographic performance evaluation of such proposed encryption scheme, as we have also detailed some chaotic functions introduced during our simulations carried out by MATLAB.
- Chapter Three: We discuss the working environment used in implementing our application, including hardware specifications and software environment. Then, we explain the process of encrypting and decrypting the facial region. Finally, we close this work with a set of observations and remarks which can contribute to the improvement of this manuscript in future works.

CHAPTER 1

GENERAL INFORMATION ON IMAGE ENCRYPTION

CHAPTER ONE: GENERAL INFORMATION ON IMAGE ENCRYPTION

1. Introduction

Cryptology is the science of information secrecy [1]. In addition to cryptanalysis and steganography, cryptology considers cryptography as one of its main research areas [2]. The term "cryptography" comes from the Latin words "crypto," meaning secret, and "grapy" meaning writing or secret writing. Cryptography involves the development of algorithms whose main goal is to convert a clear image into a cryptic one using a pre-computed key. These transformations are reversible and are called encryption/decryption (or encoding/decoding). In this chapter, we will introduce general concepts about images, basics of image cryptography such as its objectives and the fundamental concept of encryption algorithms, as well as the different categories of encryption algorithms.

2. Image basics

An image may be defined as a two-dimensional function, where x and y are spatial (plane) coordinates, and the amplitude of at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When $x, y,$ and the intensity values of f are all finite, discrete quantities, we call the image a digital image [14].

2.1 Characteristics of digital image

The characteristics of a digital image include the following:

2.1.1 Pixel

It is the basic unit of an image. It is a square point, and the set of these points constitutes the image. Each pixel contains information about the color and brightness of a specific point in the image.

2.1.2 Resolution

The resolution of a digital image refers to the number of pixels per unit area. Higher resolution means a more detailed image, while lower resolution means fewer pixels and less detail.

2.1.3 Dimension

It is the size of the image. To calculate the size of a digital image, simply multiply the number of pixels in the height by the number of pixels in the width of the image.

2.1.4 Different types of images

can be classified into three categories based on their colors:

2.1.5 Binary Images

Binary images are images where each pixel can have only two intensity values. They are displayed in only two colors, black and white. At the digital level **Figure.1.**

Figure.1. Lena Binary image**.**

2.1.6 Gray Image

image in shades of gray, does not contain different colors such as red, green, and blue. Instead, it displays the image in varying shades of gray or simply in black and white **Figure.2**.

Figure.2. Lena Gray image.

2.1.7 Color Image

A color image is a type of image that contains representation of the three primary colors: red, green, and blue. Each pixel in a color image is represented using a set of values for each color, where a specific color value is stored for each color channel (red, green, and blue) **Figure.3**.

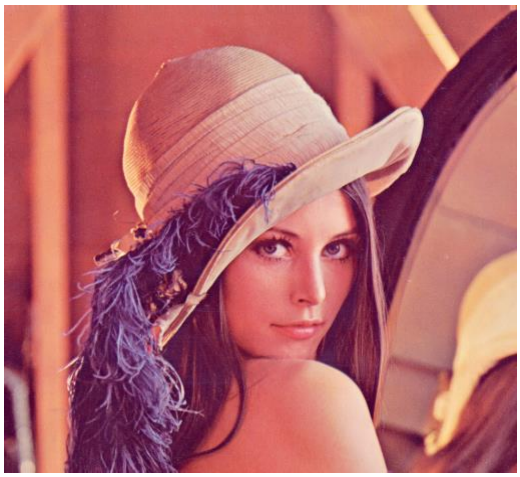

Figure.3. Lena Color image.

2.1.8 Image storage formats

The storage formats of digital images are generally divided into two basic categories: raster images and vector images. A raster image, also known as a bitmap image, is represented as a matrix of points, with these coded points arranged in rows and columns. In contrast, a vector image is described in terms of basic shapes such as lines, circles, rectangles, etc. These shapes are described by geometric attributes and attributes of thickness, color, style, etc.

The most common and important image formats for cameras, printing, and the Internet are JPG, TIF, PNG, and GIF [15].

2.2 Methods of Encryption face area in color images

There is a difference between encrypting the entire image and encrypting only the face region within the image. Encrypting just the face region can indeed be faster and more efficient because it reduces the size of the image to only the area of the face. As a result, processing speed is increased, and encryption time is significantly reduced compared to encrypting the entire image. On the other hand, facial encryption algorithms can be classified according to the application domain: spatial domain or frequency domain [15].

2.2.1 Spatial Domain

Operation on spatial domain in an image is a technique that are based on direct manipulation of pixels on it. In cryptography, image encryption in spatial domain is the process of encrypting the image pixel values directly in such a way that only authorized parties can retrieve the original information and can read it. Among the two broad categories of cryptography namely Symmetric-key cryptography and Asymmetric-key cryptography, typically symmetric cryptography is widely used in case of image encryption **Figure.4.**

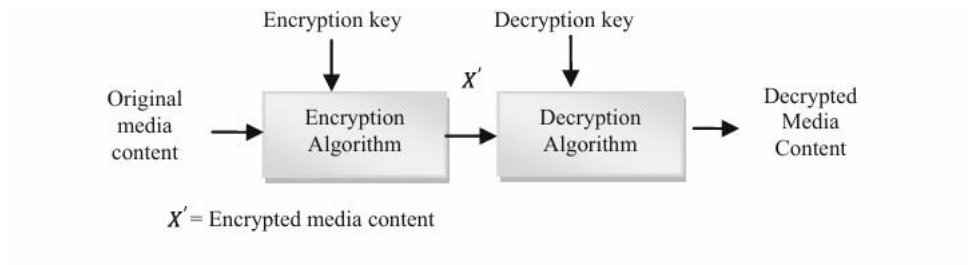

Figure. 4. General encryption and decryption model.

2.2.2 Types of Encryptions on Spatial Domain

Encryption on spatial domain determines the operations on each pixel values. i.e., operation is done in pixel directly. Complete Encryption as well as Partial Encryption can be performed on spatial domain. In complete Encryption technique the whole image values are considered and encrypt each pixel where as in Partial Encryption part of an image is considered for encryption. It may be of two types: region-based encryption and bit plane encryption. In region-based encryption firstly the region or the sensitive area which have to be encrypted is selected using some detection mechanism and only these selected coordinates are encrypted using different encryption technique. In bit-plane encryption single original image is divided into number of bit planes. For a 256 gray level image length of each pixel value is 8-bit. So, 256 gray level images can be converted into 8 different bit planes from MSB (Most Significant Bit) to LSB (Least Significant Bit). Among all the bit planes only some of the bit planes are being encrypted. Now combination of all encrypted and non-encrypted 8-bit planes will give the encrypted image.

2.2.3 Frequency domain

When we talk about image encryption in the frequency domain, we mean that we are working with the frequencies or components of the image, rather than directly manipulating the image data in the spatial domain. To apply encryption in the frequency domain, transformations like the Fourier transform or Discrete Cosine Transform (DCT) are used to convert the image from the spatial domain to the frequency domain. Then, encryption techniques are applied to the frequency components of the image.

When decrypting, the encrypted image must be reconstructed back to the original frequencies. Here lies the challenge, as reconstructing the original image from encrypted frequencies may result in some information loss. This usually happens due to the method used to encrypt the frequencies, which may introduce changes to the original data or lose some fine details during the encryption process.

Therefore, decryption operations must be accurate enough to recover the image with maximum possible precision, but in some cases, there may be some loss in quality or accuracy due to the encryption process.

2.3 Face Detection and Recognition using Viola-Jones algorithm

Identifying and extracting the face from the image is the main objective and the initial work that we should start with, as the aim of this study is to identify and extract the face from the image using the Viola-Jones technique.

2.3.1 Viola-Jones algorithm

A face detection technique that produces speedy, accurate, and effective results is Viola-Jones. The algorithm has been implemented in the software 'MATLAB' using the method (Vision Cascade Object Detector). The main objective of face detection is to identify and locate faces in images. If there are faces present, this process also aims to find them. Working with a variety of face changes, such as orientation, expression, and skin tone, is said to be one of the fundamental problems in facial detection. Furthermore, extrinsic factors including complex backdrops, inconsistent lighting, and the image's quality may play a substantial role in the detection process. Full view frontal upright faces are necessary for Viola-Jones. A window used in the procedure read an input image while searching for traits of a human face. When sufficient features are detected, it is stated that this window type of the image is a face. It is necessary to scale the window and repeat the procedure to bring faces of various sizes. The approach is applied to each window scale separately from the others. Due to the calculating of the various image sizes, this approach is fairly time-consuming. To reduce the number of features every window must be checked, and each window is moved through stages, in order. Early levels have fewer features to check and are thus much simpler to complete than later levels, which end up having more elements and are therefore more difficult. Each level's evaluation of the features is gathered, and if the value obtained falls short of the required amount, the level is failed and this window will not be recognized as a face. The algorithm has very low rates of false positives and very high rates of detection. There are four main phases to the Viola-Jones face detection method, including (Haar-Like Features, Integral Images, ADABOOST, and Cascade Classifier) [16].

2.4 Chaotic Maps

In mathematics the theory of Chaos [3] is the area of study that discusses the nonlinear things that are effectively impossible to predict or control and are highly sensitive to the initial conditions. The important characteristics of a Chaos are as follows:

• it must be sensitive to initial conditions

• it must be topologically mixing

• it must have dense periodic orbits

It can be said that any function that fulfils the above-mentioned behavior are called a chaotic function. The map or the graph obtained by plotting the values which is again found by infinite iteration of that function is called Chaotic Map for that function. In the recent years, researchers have developed many Chaotic Maps [3] by studying different real-life incidents or events. These maps are widely used for different encryption techniques specially for image encryption. The first challenging task in chaotic map-based image encryption is the selection of one or more map(s) which will be suitable according to the designers' encryption objectives. A comparative performance analysis of chaotic based encryption on color image encryption and its cryptographic requirements were discussed in [4]. Here we are going to discuss some of the chaotic maps. Usually, for more security, 2D maps are extended to 3D maps before using it in encryption process. Some of the maps and its 3D extensions are given below: A: Arnold cat map The Well-known Cat map is a two-dimensional invertible chaotic map introduced by Arnold and Aves [5, 6]. The mathematical formula is:

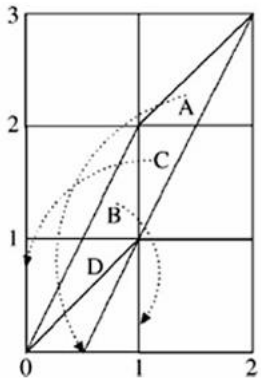

Figure. 5. Geometrical explanation Of Arnold cat map.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ n = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ n \quad (1)$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N \quad (2)$$

The extension of 2D cat map to 3D [10, 11] is,

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod\ N \tag{3}$$

$$A=\begin{bmatrix} 1+a_x a_z b_y & a_z & a_Y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y & a_z b_y & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_{y_z} b_y + a_x a_z b_y + a_x a_z b_y + 1 \end{bmatrix}$$

B: Chen's Chaotic Map

Chen's 3D chaotic map [1] can be expressed

$$\begin{aligned} \dot{x} &= a(y-x) \\ \dot{y} &= (c-a)x - xz + cy \\ \dot{z} &= xy - bz \end{aligned} \tag{4}$$

C: Logistic Map

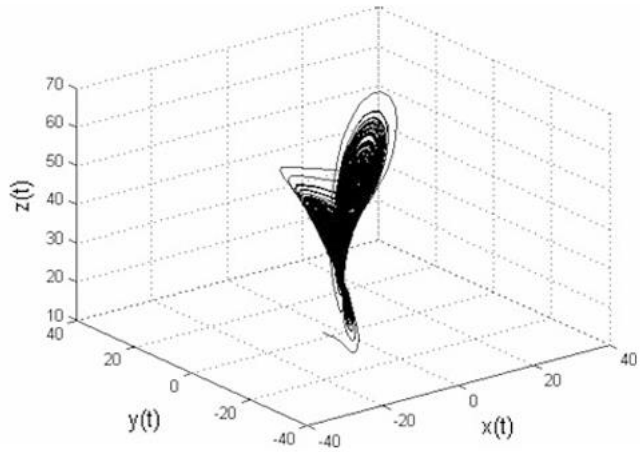

Figure. 6. Chan's chaotic Map With a= 35, b=3 and c=28.

Logistic mapping [6,10,12] was originally proposed by P. Verhulst in 1845, but has become widely known through the work by R. May. It is the simplest among all the chaotic maps **Figure.6.**

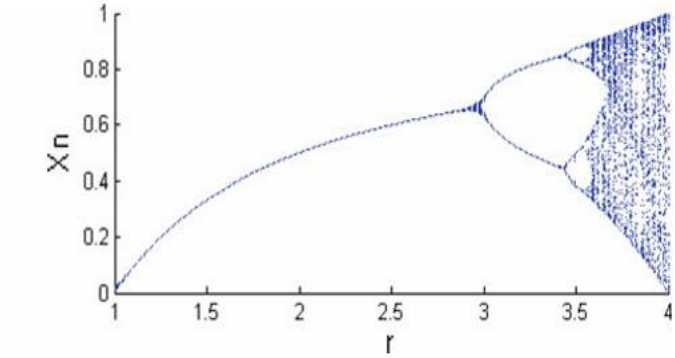

Figure. 7. chaotic logistic Map.

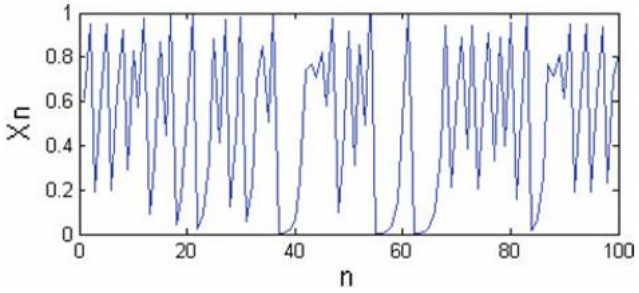

Figure. 8. Chaotic logistic Map sequences.

$$x_{n+1} = rx_n(1 - x_n) \tag{5}$$

Here, r is the constant and xn is the state value **Figure.7.**

Example: Chaotic sequence generated by a Logistic Map with values of r = 3.9999 and initial value of $x_n = 0.60232$ is given in **Figure.8**.

D: Chebyshev map Chebyshev Map [9, 13] is also one type of Chaotic Map which is trigonometric function with Chebyshev polynomial. The equation is,

$$x_{n+1} = T_K(x_n) = \cos(k.\cos^{-1} x_n), \quad x_n \in [-1,1] \tag{6}$$

where k and x(n) are parameter and state value, respectively. Choosing a value of $k \in [2, \infty]$, the system shows chaotic behaviour. The initial value of x_n and theparameter k are used as the key for diffusion module in later stage.

2.4.1 Chaotic Map Based Encryption and Decryption Model

Though there are several Chaotic Map based Image Encryption Techniques are available, but the whole process or techniques can be generalized into three different phases. These three phases are followed in all Chaotic Map based Image Encryption. These are: • Selection of chaotic maps • Confusion • Diffusion For designing these three steps different schemes are

used, depending on the requirements and the objectives of individuals design, i.e., level of security, necessity of key sensitivity, fastness etc. A generalized flow diagram of Chaotic Map based image Encryption process is given in **Figure. 9.** Here initially different chaotic maps and its behavior have to be analyzed. Depending on the user's requirement one or more map(s) have to be selected for using encryption and decryption

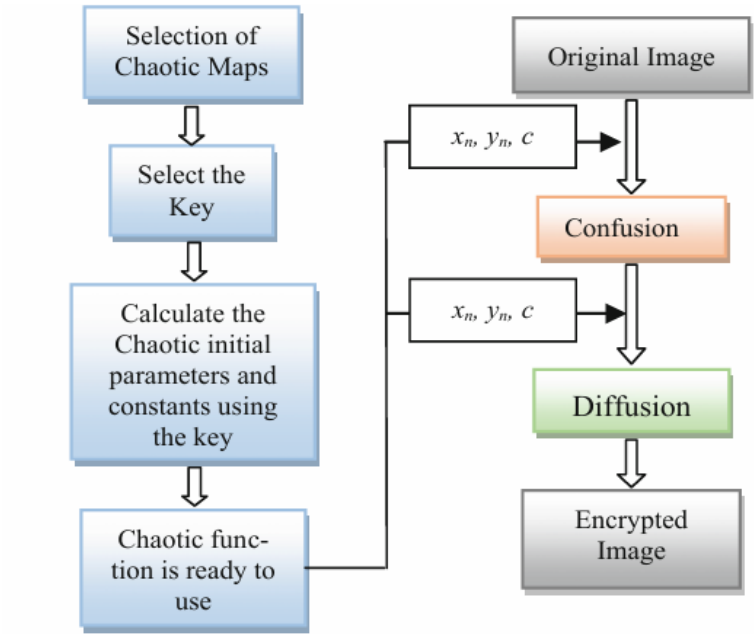

Figure. 9. Chaotic Map based encryption model.

The next step is to select a secret key to be used as initial condition for the chaotic map with effective length considering brute force attack. Then to determine initial parameters and constants of the chaotic maps so that it gives proper chaotic behavior. After that the selected chaotic maps are ready to use in encryption process which produces XN, YN in every iteration. In Confusion stage chaotic mapping functions are applied to the original image to rearrange the pixel values. This process may be repeated several times to give more confusion to the output image. In case of partial image encryption [7, 8], separation of the bit planes and performing confusion to the bit values within the planes are done in this step. The next and final step is the diffusion stage to get the complete encrypted image. In this stage, each pixel values of the output generated by confusion stage is ***XORed*** with the chaotic function values. This step can also be repeated for multiple times to achieve the higher security level. Finally, Encrypted Image is obtained to transmit to the receiver side. Similarly, a generalized decryption process of chaotic map-based image encryption is given in **Figure.10**. In decryption model the process is repeated in reverse order. But the main difference is that here, everything is predefined, i.e., chaotic

maps, key, diffusion technique and confusion technique. The key has to be considered same as used in encryption model. Then to calculate the initial states and constants same process has to be followed. Once the chaotic map is ready to use, first diffusion step has to done on encrypted image in reverse order. The output of the diffusion step will be the input of confusion step. Finally, after completion of confusion step, final decrypted image can be retrieved.

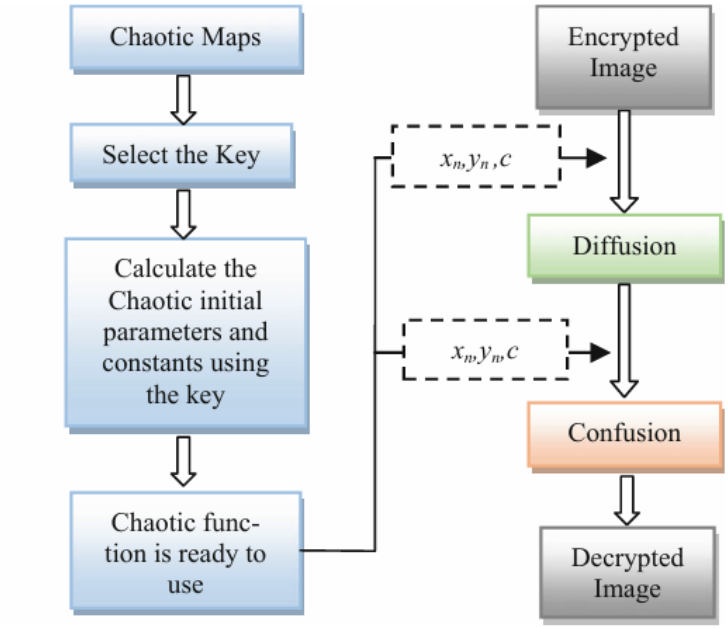

Figure. 10. Chaotic Map based decryption model.

2.4.2 Confusion Phases

In confusion phase, pixel positions of the original image are interchanged using some chaotic maps or mapping functions. Usually, the pixel values are not changed in this phase unless bit-plane confusion is not done. Some of the diffusion techniques used so far in chaotic map-based encryption process are discussed below: Example 1 The 3D Arnolds Cat Map is given by Eq. 2. Here n = 256 is dimension of the image (jump.png). Here $\binom{x}{y}$ represents the original pixel positions and $\binom{x'}{y'}$ represents the new pixel positions after the Arnolds Cat Map transformation (**Figure.11.).**

Figure. 11. example of confusing using Arnold Map a original image b 1st Iteration.

2.4.3 Diffusion Phase

37	34	34	40
30	39	40	38
31	32	33	37
31	15	31	37

$$f'(i,j) = x_n \oplus f(i,j)$$

165	88	197	180
128	251	230	181
49	29	195	34
98	15	229	147

Figure.13. Diffusion of a 4*4 matrix.

Chaotic sequence

10000000
01111010
11100111
10011100
10011110
11011100
11001110
10010011
00101110
00111101
11100010
00000111
01111101
00101010
11111010
10110110

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

$$f(x_{n+1}, y_{n+1}) = f(x_n + y_n)$$

16	1	6	9
15	7	3	8
2	4	11	10
13	14	12	5

Figure.12.Confusion of a 4*4 matrix.

In confusion phase, original image is changed due to the interchange of pixel values but the histogram of both the images are still same. So, it may easier for attacker to retrieve the original image with help of histogram equalization. Hence, diffusion phase is necessary to obtain a complete secure cipher image **Figure.13**. Here **Figure.12.** describes the diffusion process of using chaotic maps. In confusion process only the general view of the image is changed, because of the rearrange mint of the original pixel values. So, we can say that confused image is also an encrypted image. But, histogram of the confused image remains same with the original image, therefore there may be a clue for third party to attack the image if we use this confused image as the final encrypted image.

The main objective of diffusion is to change the image pixel values so that histogram of the original image and encrypted image will be completely different. Example 2 With help of a Logistic map as in **Eq. 2** chaotic sequences are generated and performed XOR operation on the pixels of confusion image **Figure. 14**..

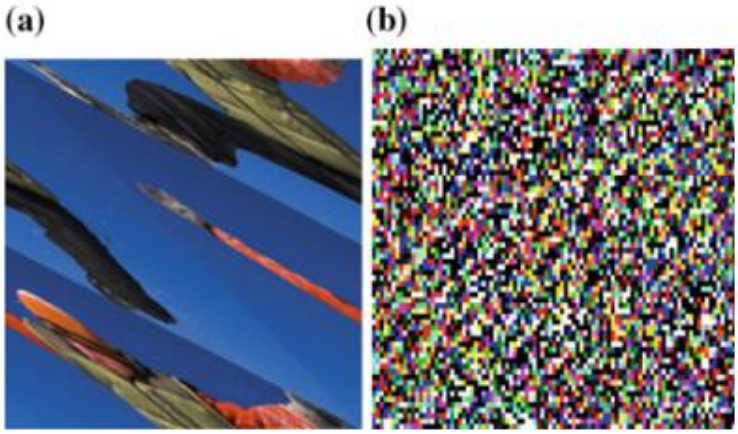

Figure. 14. Example of diffusion using logistic Map. A - confusion image B - after diffusion.

Algorithm: Diffusion

Start

While there exist pixels

$f'(i,j) = x_n \otimes f(i,j)$ *where* x_x *is chaotic sequence*

End loop

End

This process can also be repeated for more than once. Once the diffusion process is completed, the output image is our final encrypted image [17].

2.5 State-of-the-art on image encryption techniques

2.5.1 Method based on permutation

It is a technique that involves changing the location of a part of the image from one place to another, and it relies on three techniques, which are:

2.5.2 Bit permutation

The image can be seen as an array of pixels, each with eight bits for 256 gray levels. In the bit permutation technique, the bits in each pixel taken from the image are permuted with the key chosen from the set of keys by using the pseudo random index generator. The entire array of these permuted pixels forms the encrypted image. The encrypted image obtained from the bit permutation technique is transmitted to the receiver through the insecure channel. At the receiver the encrypted image is decrypted using the same set of keys. As the number of bits in each pixel is eight, we also take the key length equal to eight. The Numbers of permutations obtained with Eich elements Is 8 ! (=40320) [18].

2.5.3 Pixel permutation

In this scheme each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys. The encryption and decryption procedure is same as the bit permutation technique. The size of the pixel group is same as the length of the keys, and all the keys are of same length. If the length of the keys is more than the size of pixel group, the perceptual information reduces. In this work the group of pixels is taken along the row without the loss of generality, i.e., the column wise procedure would yield same kind of results [18].

2.5.4 Block permutation

In this technique the image can be decomposed into blocks. A group of blocks is taken from the image and these blocks are permuted same as bit and pixel permutations. For better encryption the block size should be lower. If the blocks are very small, then the objects and its edges don’t appear clearly. In this block permutation the blocks are permuted horizontally in the image. The permutation of blocks along vertical side is also similar to horizontal side block permutation. At the receiver the original image can be obtained by the inverse permutation of the blocks. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbor’s. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values

of its neighbor's. At the receiver side, the original image can be obtained by the inverse transformation of the blocks [18].

2.5.6 Methods based on matrix transformations

In this section we propose image encryption algorithm using matrix decomposition techniques. We decomposed the input image (which is to be encrypted) using one of the matrix decompositions into a basis component matrix and its weight/strength matrix. For illustration purpose we decomposed image of size m × n into basis matrix of size m × b and strength matrix of size b × n. We can use the order reduction but that can cause the data loss and hence we use full rank decomposition in both NMF and ICA case. At the reconstruction end by operating inverse (multiplication of basis and strength matrix) operation, the reconstructed image is replica of original image. In matrix reconstruction, its components and the order of components is very important. If the order of basis component (Columns of basis matrix) is changed, then it is impossible to reconstruct the image. We exploit this property for the image encryption purpose. In this approach, the columns of weight matrix and the row of basis matrix form the bookkeeping vector. Also, we have added order of scrambled vectors as extra key parameter. This makes the bookkeeping vector unique, which is a major and important characteristic for encryption process. Note that, we have kept basis component, weight component and scrambling order in one stack design which is exceptional and user known only. It is ensured that, the input image can be decrypted only if the ICA, wherein the NMF is replaced by ICA matrix decomposition [19].

2.5.7 Methods based on discrete wavelet transform

Wavelet transform is a time frequency analysis tool, which can not only investigate the time domain characteristics of the local frequency domain processes, but also investigate the frequency domain characteristics of the local time domain processes. Wavelet transform can transform the image into a series of wavelet coefficients, which contain the low frequency coefficients and the high frequency coefficients of the image data. The wavelet coefficients can be efficient compressed and stored. The rough edges of the wavelet can better show the image. So the wavelet transform is often applied in the process of image encryption. Wavelet transform has been widely used in digital image processing in recent years. We use the 2D DWT multi resolution decomposition to the image because the form of a digital image is a 2D matrix. The 2D DWT decomposed image consistent four parts, LL (approximate figure, low frequency part), HL (vertical details), HH (diagonal details) and LH (horizontal details), The basic

information of the digital image is mostly covered in its approximate part (LL low frequency part). Each decomposition is conducted on the basis of decomposition of LL part [20].

2.5.8 Other méthodes

Several existing image encryption algorithms have been proposed based on different technologies, such as: DNA sequencing, cellular automaton. And Frome different Fields such as physiques, biology, et.

2.6 CONCLUSION

In this chapter, we discussed the image and its features, as well as facial encryption techniques in the image and how they work. Studies have shown that encrypting the face in the image is more effective and secure than encrypting the entire image. The Viola-Jones algorithm has helped us in identifying and extracting the face from the image, providing significant facilitation for the success of encryption techniques.

In the second chapter, we will attempt to present some calculations and results regarding the effectiveness of this technique in securing information (images) when sent and stored.

CHAPTER 2

PERFORMANCE MEASURMENT AND CHAOTIC FUNCTIONS

CHAPTER TWO: PERFORMANCE MEASURMENT AND CHAOTIC FUNCTIONS

1. Introduction

Chaos theory consists of studying the behavior of dynamic systems nonlinear [21] represented by deterministic equations which can have a behavior chaotic if they are used iteratively in so-called chaotic sequences [22].in this chapter we will have a look at the performance measurement and chaotic function and see the deference's in the reel time rendering.

1.1 Key sensitivity analysis

A secure encryption system must be sensitive to the secret keys. Being sensitive to secret keys means that if an attacker modifies the keys slightly, the decryption algorithm will not be able to regain the original plain image .In our method, there are two-stage keys including $x01, y01, z01, h01$ and $x02, y02, z02, h02$.Since the second-stage keys $x02, y02, z02, h02$ are determined by the chaotic sequences and the input image, we test the key sensitivity of our proposed encryption algorithm by slightly changing the values of the first-stage keys. Let key1: $x01, y01, z01, h01$ denote the secret keys. We apply a slight change in key1 to generate key 2: $x01 + 10 - 16, y01, z01, h01$, where x01, $y01, z01, h01$ are the same values as in key1. The original Lena image is shown in **Figure. 15.(**a). It is encrypted by key1 to get the cipher image **Figure.15.** (b). Then we used both key1 and key2 to decrypt the cipher image. The decryption results are shown in **Figure.15.** (c) (d). It is obvious to notice that the original image can be recovered using the correct secret key key1, but it cannot be correctly decrypted by key2 which is slightly different from key1.

2. Histogram analysis

Histogram analysis illustrates the distribution of pixel values in the image. The histogram of the plain image is non-uniform since the statistical results can be seen in a normal image. However, to hide the statistical information, the histogram of an encrypted image should be randomly distributed on both axes [23]. Results of our histogram analysis are shown in **Figure.16.** (a)-(c) show the histogram of the RGB channels of the Lena image with statistical information. Instead, **Figure.16.** (d)-(f) show a fairly uniform distribution histogram over three components of the encrypted image because all pixels are evenly distributed in the cipher image, for quantitative analysis, we performed histogram variance tests on both plain Lena image of size 256 × 256 × 3 and its cipher image. The smaller variance of the histogram

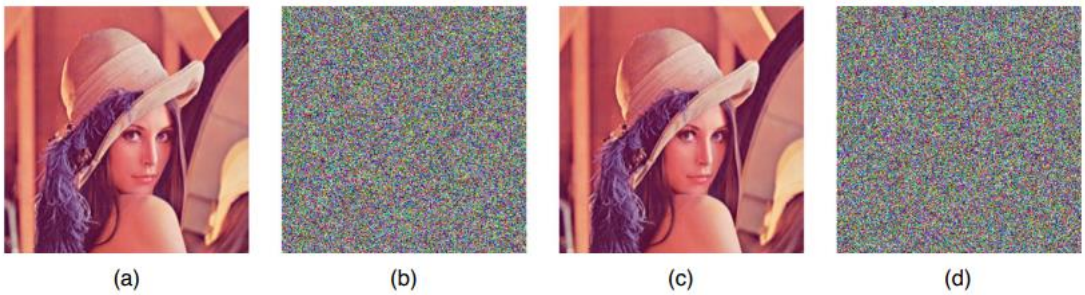

Figure. 15. Key sensitivity results. (a) Original Lena image, (b) encrypted image, (c) decrypted image with right keys, (d) decrypted image with wrong keys.

while the encrypted image has the same histogram which looks like uniform white noise. This confirms that a potential attacker cannot derive any information that can reveal the original face. Therefore, we prove the effectiveness of our proposed algorithm against the histogram analysis test.

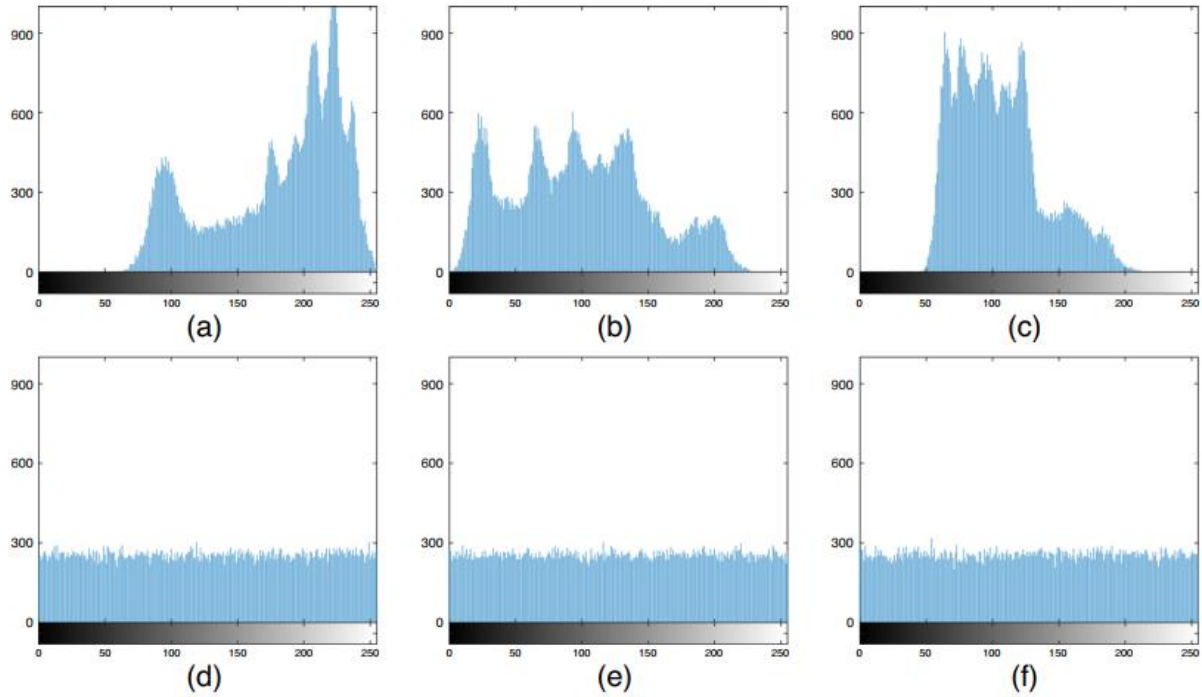

Figure. 16. Histogram analysis of our encryption algorithm. (a) Histogram of red component of the plain image, (b) histogram of green component of the plain image, (c) histogram of blue component of the plain image, (d) histogram of red component of the cipher image

2.1 Loss data test

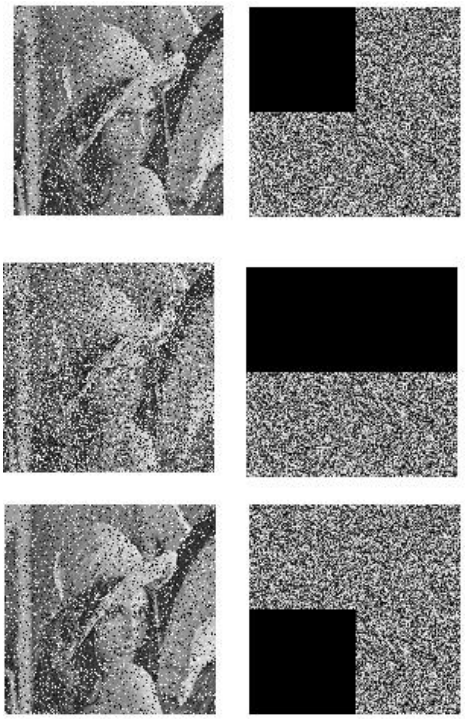

Figure. 17.Loss data test: (a) Encrypted face 1with 25% data loss;50% data loss and 75% respectively (b) Their corresponding decrypted faces.

In this subsection, we explore the results where a portion of the information is lost while transmitting the encoded image from the sender to the receiver. Consequently, we examine the impact of this information loss on the quality of the encrypted image. **Figure.17.** illustrates various simulations demonstrating different levels of loss (12.5%, 25%, and 50%) in the encrypted image, along with the corresponding encoded images for each loss level. Despite the data loss, the decrypted images remain recognizable up to a certain loss rate. This verifies the resilience of the suggested algorithm in the face of a 75% data loss test.

2.2 Key space analysis

For a secure encryption system, it is essential to have sensitivity to secret keys. Sensitivity to secret keys implies that even slight modifications made by an attacker to the keys will render the decryption algorithm unable to retrieve the original image.

Regarding the precision of the input field, which is 256, the key space is calculated as follows:

$$(10^{15}) \times (10^{16}) \times (10^{15}) \times (10^{16}) = (10^{62}) \times (2^{3}) = (2^{186}) \qquad (7)$$

This value is deemed sufficient when compared to the required encryption value of (2^{100}).

2.3 Corrélation coefficients analysis

Correlation analysis consists of horizontal correlation, vertical correlation and diagonal correlation. It shows how adjacent pixels are relative to different axes. The correlation coefficient can be computed by

$$C_{x,y} = \frac{E(x-\mu_x)(y-\mu_y)}{\sigma_x \sigma_y} \tag{8}$$

where x and y are values of adjacent pixels; $\mu x, \mu y, \sigma x$ and σy are the averages and standard deviations of x and y respectively. $E(\cdot)$ is an expectation function. When calculating the correlation coefficients, we randomly select 20000 pairs of pixels from the plain and the cipher image. We select the adjacent right point of each point to calculate the horizontal correlation, the adjacent lower point to calculate the vertical correlation, and the adjacent lower right point to calculate the diagonal correlation.

Table 1 Correlation coefficients of plaintext and ciphertext images

		Plain face			Cipher face		
Image	Direction	R	G	B	R	G	B
Lena	Horizontal	0.9578	0.9465	0.9338	0.0080	–0.0003	0.0026
	Vertical	0.9798	0.9732	0.9579	–0.0058	–0.0011	0.0054
	Diagonal	0.9338	0.9220	0.9047	0.0051	–0.0081	0.0016
All white	Horizontal	NaN	NaN	NaN	0.0064	–0.0066	0.0017
	Vertical	NaN	NaN	NaN	–0.0073	–0.0075	0.0019
	Diagonal	NaN	NaN	NaN	0.0023	0.0021	0.0032
All black	Horizontal	NaN	NaN	NaN	0.0026	0.0013	–0.0019
	Vertical	NaN	NaN	NaN	0.0059	0.0055	–0.0017
	Diagonal	NaN	NaN	NaN	0.0066	–0.0077	–0.0117
Couple	Horizontal	0.9484	0.9300	0.9178	–0.0090	0.0087	0.0002
	Vertical	0.9565	0.9549	0.9459	–0.0063	0.0087	–0.0088
	Diagonal	0.9182	0.8996	0.8875	0.0034	0.0045	0.0098
Female	Horizontal	0.9790	0.9672	0.9534	–0.0198	0.0072	–0.0058
	Vertical	0.9871	0.9811	0.9690	–0.0191	–0.0036	–0.0037
	Diagonal	0.9682	0.9524	0.9304	–0.0147	–0.0014	0.0083
Tree	Horizontal	0.9583	0.9685	0.9605	–0.0095	–0.0103	0.0059
	Vertical	0.9340	0.9450	0.9390	0.0004	–0.0041	0.0039
	Diagonal	0.9143	0.9312	0.9257	–0.0029	0.0007	–0.0133
Beans	Horizontal	0.9759	0.9764	0.9893	–0.0020	0.0066	0.0001
	Vertical	0.9777	0.9806	0.9884	–0.0002	0.0076	–0.0002
	Diagonal	0.9559	0.9600	0.9802	–0.0001	0.0021	–0.0063
House	Horizontal	0.9552	0.9420	0.9742	0.0097	0.0029	0.0032
	Vertical	0.9577	0.9387	0.9663	–0.0076	0.0113	0.0001
	Diagonal	0.9235	0.8891	0.9433	–0.0065	–0.0046	–0.0042
Barbara	Horizontal	0.9427	0.9307	0.9425	–0.0034	0.0009	–0.0042
	Vertical	0.9742	0.9689	0.9743	–0.0004	0.0064	–0.0068
	Diagonal	0.9258	0.9106	0.9257	–0.0034	0.0000	–0.0048

Table 2 Comparison of correlation coefficients in Lena image

Algorithm	Horizontal	Vertical	Diagonal	Average
Plain text	0.9688	0.9836	0.9535	0.9686
Ours	0.0035	–0.0005	–0.0005	0.0015
Ref. [45]	–0.0016	–0.0017	0.0156	0.0063
Ref. [15]	0.0168	0.0445	–0.0022	0.0212
Ref. [53]	0.0373	0.0228	–0.0221	0.0274
Ref. [50]	–0.0015	0.0041	0.0069	0.0042
Ref. [57]	0.0075	–0.0015	–0.0044	0.0045
Ref. [25]	–0.0035	–0.0574	0.0578	0.0396

Table 1 shows the numerical results of the horizontal, vertical and diagonal correlation coefficients in the three channels of our test plain and cipher images. In plain images, the correlation coefficients are close to 1, while in cipher images, the correlation coefficients are close to 0. That means our method can dramatically reduce the relationship between adjacent pixels in three directions. The comparison results with other algorithms are listed in **Table 2**.

In order to intuitively compare the correlation before and after encryption, we draw the point graph of the correlation between adjacent pixels in **Figure.18.** and**.19**., where the abscissa is the gray value of the random pixels, and the ordinate is the gray value of the adjacent pixels. **Figure .18**. shows the diagonally distributed correlation plot of the Lena image with

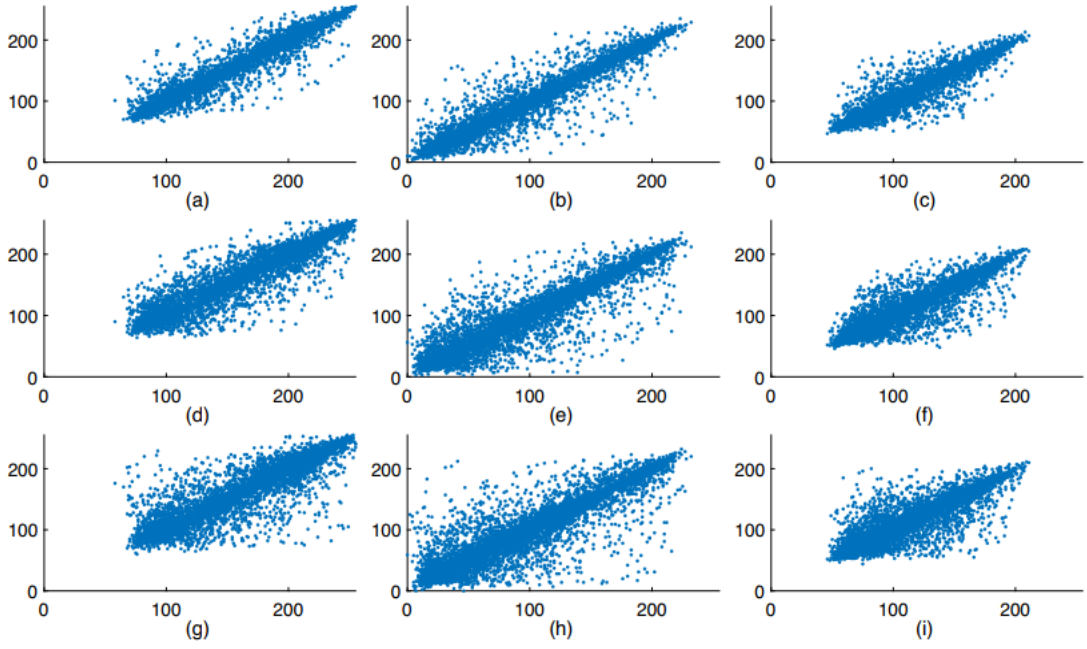

Figure. 18. Correlation plots of the plain image in horizontal, vertical and diagonal adjacency axis.

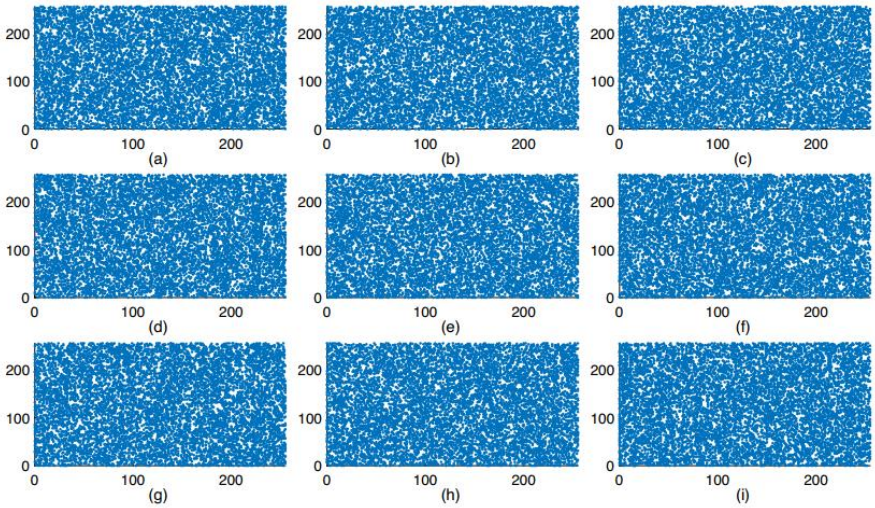

Figure. 19. Correlation plots of the encrypted image in horizontal, vertical and diagonal adjacency axis.

Correlation plots of the plain image in horizontal, vertical and diagonal adjacency axis. (a ,b , c) Pixel correlation coefficient plots of R, G, B channels of the plain image in horizontal direction respectively, (d ,e , f) pixel correlation coefficient plots of R, G, B channels of the plain image in vertical direction respectively, (g, h, i) pixel correlation coefficient plots of R, G, B channels of the plain image in diagonal direction respectively .

Correlation plots of the encrypted image in horizontal, vertical and diagonal adjacency axis. (a,b,c) Pixel correlation coefficient plots of R, G, B channels of the cipher image in horizontal direction respectively, (d,e,f) pixel correlation coefficient plots of R, G, B channels of the cipher image in vertical direction respectively,(g,h,i) pixel correlation coefficient plots of R,G, B channels of the cipher image in diagonal direction respectively

high correlation, whereas**Figure.19.** displays the correlation plot of the cipher image, in which the dots are scattered uniformly. The comparison between **Figure.18.** and **.19.** illustrates that our proposed algorithm can effectively remove the correlation of the plain image hence it has strong resistance to statistical attacks.

2.4 Definition of PSNR

PSNR Peak signal-to-noise ratio (PSNR) is a widely used measurement method to evaluate image quality. It represents the ratio of the maximum possible power of the signal to the destructive noise power that affects its representation accuracy, as shown in Eq (9). The peak signal to noise ratio (PSNR) is usually used as the objective evaluation standard of image quality.

$$PSNR = 10\ log_{10}\left(\frac{I\ max^2}{MSE}\right) \quad (9)$$

$$PSNR = 10\lg\left[\frac{MN\ MAX_{i,j}(I(i,j))^2}{\sum_i \sum_j (I(i,j)-I'(i,j))^2}\right]$$

Here, I(i, j)and I′(i, j) are the pixel values of each point of the original image and the transformed image respectively [24].

2.5 chaotic maps

In mathematics, a chaotic map is a function that exhibits a form of chaotic behavior. It often takes the form of an iterated function and is involved in the study of dynamical systems. Chaotic maps can be parameterized by a continuous-time or discrete-time parameter. According to Alligood et al., a chaotic map is dependent on its domain, and the starting point of the trajectory (the state from which the system starts) is called the initial condition. Chaotic maps clearly illustrate many characteristics of chaotic behavior, such as sensitivity to initial conditions, complex behavior, and the evolution of information in a deterministic and unpredictable manner. Several one-dimensional (1-D), two-dimensional (2-D), and three-dimensional (3-D) chaotic maps are proposed in the literature. In this subsection, we will briefly describe some chaotic maps, such as the logistic map, tent map, and sine map [26].

2.5.1 Logistic maps

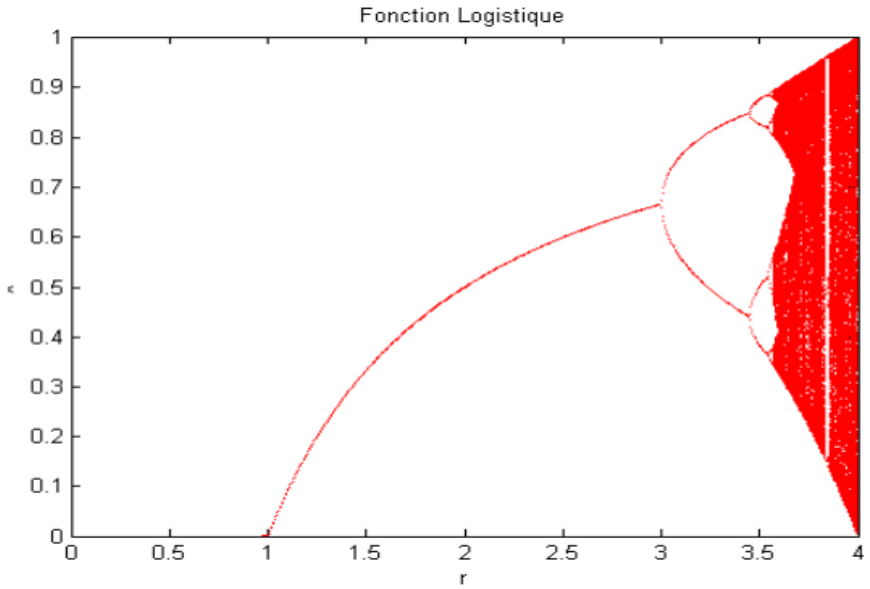

Figure.20. Diagramme de bifurcation pour la fonction logistique.

A logistic recurrence is a simple example of a sequence whose recurrence is nonlinear. Often cited as an example of the complexity that can arise from a simple nonlinear relationship, this recurrence was popularized by the biologist Robert May in 1976. Its recurrence relation is:

$$x_{n+1} + 1 = \mu x_n(1 - x_n) \tag{10}$$

In equation above, (r) is the control parameter that can have values in the interval

$0 < r < 4$ and $x_n \in [0,1]$ [26].

2.5.2 Sine map

The one-dimensional sine recurrence has the state representation:

$$x_{n+1} = \lambda sin(\pi\, x_n) \tag{11}$$

With $\lambda = 1$ chaotic behavior is generated in a manner very similar to the logistic function. Like the logistic recurrence, the sine map is quadratic near ($x = 0.5$). They exhibit probabilistic distribution and evolve towards chaos through almost identical period-doubling. Windows occur periodically in the same order. It has the same Feigenbaum number as the logistic map. Despite the similarities, there are some differences: The Lyapunov exponent is approximately fifty percent smaller, period-doubling bifurcations occur earlier, and periodic windows are wider compared to the logistic map [26].

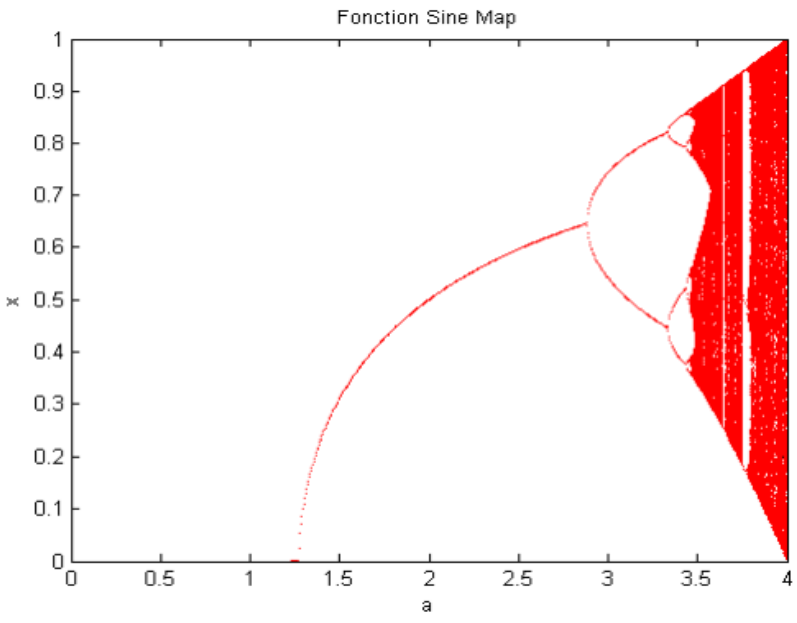

Figure. 21.Diagramme de bifurcation pour la fonction Sine Map.

2.5.3 Tent map

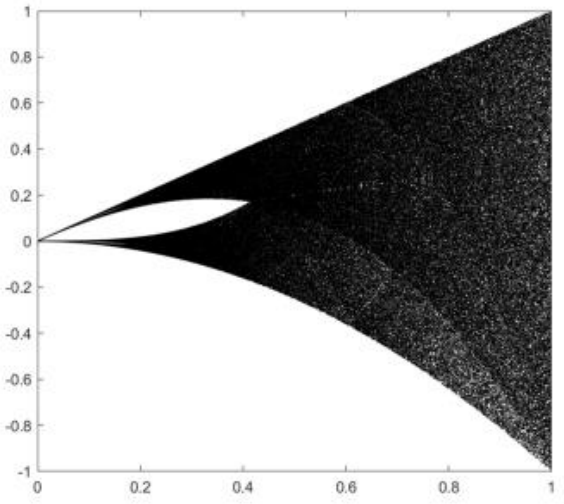

Figure.22. Branching diagram of chaotic mapping of tent map.

Tent map is a piecewise function with linear mapping. It is sensitive (especially for the initial values), unrepeatable, uncertain, unpredictable and other characteristics. The mathematical model of Tent map is shown by Eq (12).

$$x_{n+1} = \begin{cases} \frac{x_n}{\alpha}, 0 < x_n \leq \alpha \\ \frac{1 - x_n}{1 - \alpha}, \alpha \leq x_n < 1 \end{cases} \quad (12)$$

Tent map is in the chaotic state, when $\alpha \in (0,1)\ and\ \in (0,1)\ n\ x$. Usually, the initial value 0 x takes a different value from the system parameter α in order to avoid forming a periodic system. The initial value is $x0$ =0.001, and the iteration is 300 times. When ½ <= $\alpha < 1$, the branch diagram of chaotic mapping of Tent map is shown in **Figure .22.** However, Tent map has few variable parameters, simple structure, vulnerable to attacks, and low security [27].

2.6 Bifurcation

Bifurcation theory is the mathematical study of qualitative or topological changes in the structure of a dynamical system. A bifurcation occurs when a quantitative variation in a system parameter leads to a qualitative change in the system's properties such as stability, the number of equilibrium points, or the nature of steady states. The parameter values at the moment of change are called bifurcation values. In dynamical systems, a bifurcation diagram shows the possible long-term behaviors of a system based on bifurcation parameters [25].

2.6.1 Exposant de Lyapunov

Chaotic evolution is challenging to understand because the divergence of trajectories on the attractor is rapid. For this reason, efforts are made, if possible, to measure or estimate the speed of divergence or convergence. This speed is given by the Lyapunov exponent, which characterizes the rate of separation of two very close trajectories [25].

The Lyapunov exponent is defined by

$$\lambda(x_0) = lim_{n\to\infty}\, sup_{\frac{1}{n}}\, log\,(\|\ f(n)'\,(x_0)\,\|) = lim_{n\to\infty} sup_{\frac{1}{n}} \sum_{J=0}^{n-1} log\,(\|\ f'\,(x_j\,\|) \qquad (13)$$

$$x_j = \boldsymbol{f_j}(\boldsymbol{x_0})$$

2.7 The simulation time

The simulation time (encryption or decryption) depends on several factors, with the most important being the dimensions of the image. The second factor relies on the grayscale levels of the image. The third and most significant factor is the simulation tool, which includes the characteristics of the microcomputers used (clock frequency, RAM, etc.). In our simulations, when dealing with full-color images, the encryption and decryption times tend to be slightly longer.

In our teste we simulate on laptop dell 7320 with an i5 11gen EVO and 16 Gb ddr4 ram contain on SSD with read and write up to 3gb/s.

Table.1. Encryption and decryption time measurement

images	Encryption time	Decryption time
4.1.04.tiff	3.41 seconds	2.38 seconds
4.1.03.tiff	3.26 seconds	2.51econds

3 CONCLUSION

In this chapter, we delved deeper into the theory of image encryption, presenting some calculations on the strength and effectiveness of image encryption. We demonstrated its effectiveness even with images of lower resolution. We also discussed the efficacy of this technique and its robustness against cyber-attacks, where it proved to be highly effective. In the final section of this scientific research, we will discuss a more precise method for encrypting faces, as well as the working environment used, including device specifications and other characteristics.

CHAPTER 3

RESULTS AND DISCUSSION

1. Introduction

In chapter 3, we will implement a facial encryption algorithm in MATLAB 2021B environment. To do this we used the Sipi database [28], and the standard test images are:

4.1.04.tiff'

4.1.03.tiff'

Figure. 23.Standard test images.

2. Proposed facial encryption algorithm

The proposed facial encryption algorithm for color images proceeds through the following steps:

- Consider the size test image.$I(m,n)$
- Either$I'$the face of the test image detected by the Viola Jones size algorithm ().m', n'
- Extract the detected face colors and decompose it into these three components red-green-blue- designated by,$I'_r I'_v\ I'_b$all three having a size of.(m', n')
- Encrypt the three components using the confusion-diffusion architecture using two chaotic logistic map functions with parameters $(,r_{0\,,}x_0)(r_1,x_1)$
- The three Encrypted components are merged to give the encrypted color face.
- Reposition the encrypted face into its place within the entire color image

3. Proposed facial decryption algorithm

The proposed facial decryption algorithm for color images will take the same steps as Those of the encryption phase but in reverse.

4. Simulation test results

Figure.24. illustrates the facial encryption results of standard images **4.1.03 Tiff'** and **4.1.04 Tiff'**. Indeed, we presented the encrypted face in the entire image, as we also illustrated the face area in plain text as well as its corresponding encrypted image.

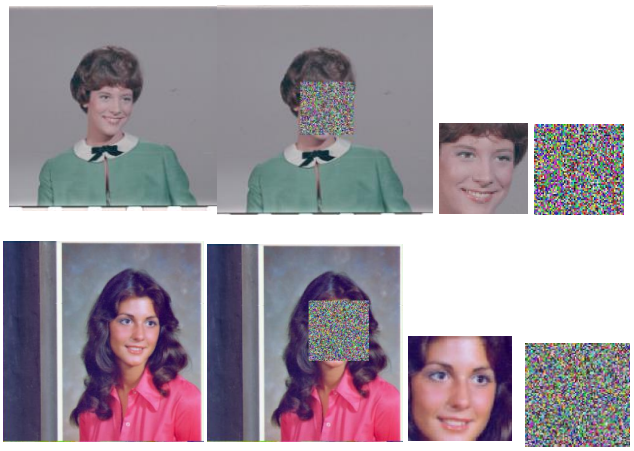

Figure .24. Face encryption results of the two standard images.

Table .1. Summary of PSNR performance metrics and correlation rate

Picture	4.1.04.tiff'			4.1.03.tiff'		
	R	G	B	R	G	B
PSNR (dB)	-40.3513	-39.8836	-38.6801	-38.5540	-38.2188	-38.1712
Correlation rate	-0.0128	-0.0025	-0.0245	0.0086	0.0073	0.0022

The table above summarizes the objective measurements of the correlation rate and the PSNR (dB) calculated between the original face and the encrypted face for the three components (RGB).

4.1 Histogram analysis

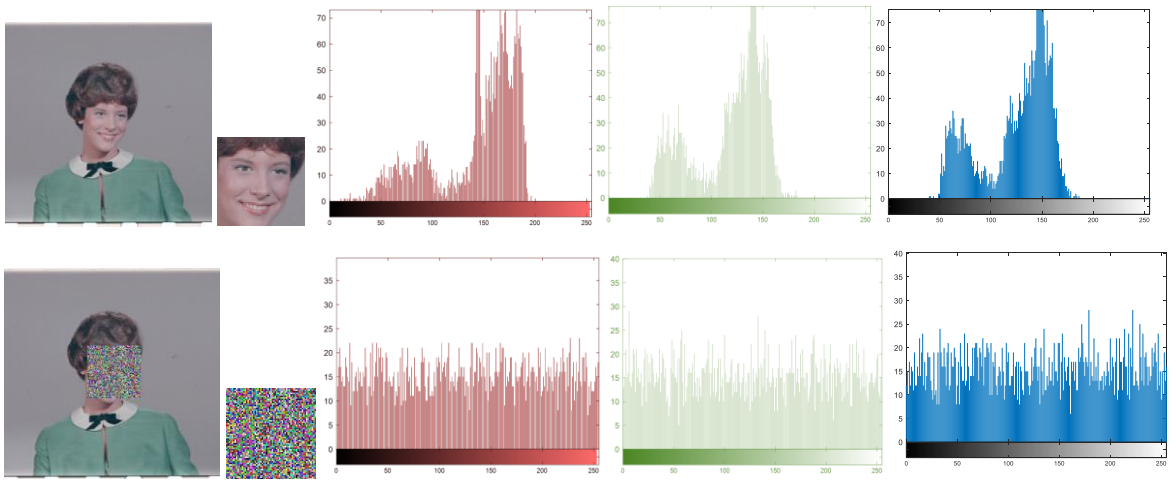

Figure .25. Histogram analysis for the face that matches the image4.1.03.tiff'.

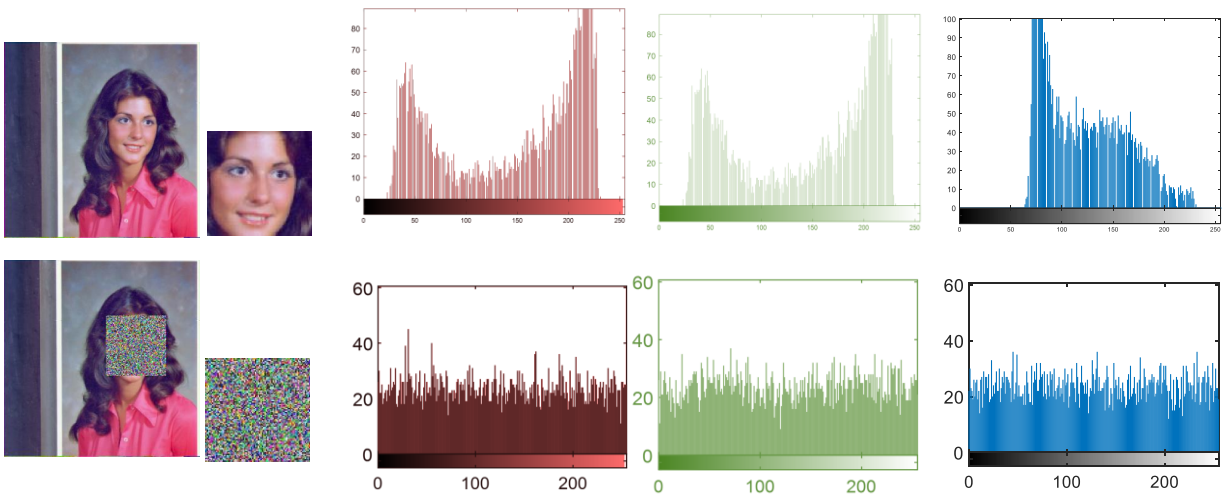

Figure .25. Histogram analysis for the face that matches the image`4.1.04.tiff'.`

Referring to **Figure .24.** and **Figure .25.** regarding the analysis of original histograms and their corresponding encrypted faces of the two test images **4.1.03.tiff'** and **4.1.04.tiff.**' We clearly notice that each component (Red, Green, Blue) has a very specific histogram. In contrast, all components of encrypted faces have a histogram that resembles uniform white noise. However, a possible attacker cannot derive any information that could reveal the original faces. Therefore, we conclude that our proposed algorithm is robust against histogram analysis attacks.

4.2 Loss-data test

We assume that the face encrypted in the image to be transferred between the transmitter and the receiver suffers a loss of a well-determined percentage. We will simulate the influence of this loss on the face deciphered in the entire image. **Figure .26.** illustrates the different cases of loss already mentioned, we note that the decrypted face remains identifiable up to a loss percentage of 50%, which confirms the robustness of the proposed algorithm with respect to the loss data test. We also notice that beyond 50%, the face becomes unidentifiable and this is completely normal given the high percentage of loss.

Figure .26. Loss data test (a) Encrypted face of image4.1.04.tiff'(b) Encrypted face with different loss data 25%, 50%, 75% (c)Those corresponding faces with loss data (d) Those corresponding decrypted face image.

4.3 Execution time of the proposed algorithm

Table .2. Allocated time for encryption and decryption processes

	Allocated time(s)
Proposed encryption algorithm	2.162304
Proposed decryption algorithm	0.952046

4.4 Sensitivity of the encryption key

Figure .27. Sensitivity test: Decrypted face of image 4.1.04.tiff' for (a) $x_0' = x_0 + 10^{-16}$(b)) $r_0' = r_0 + 10^{-15}$ (c)) $x_1' = x_1 + 10^{-16}$ (d)) $r_1' = r_1 + 10^{-15}$ (e) With correct key.

In this proposed facial encryption algorithm, the encryption key is made up of the parameters (x_0, r_0), (x_1, r_1) of the used chaotic Logistic map function. If we assume that the encryption key is $k(x_0, r_0, x_1, r_1)$, the corresponding decryption key is $k'(x_0', r_0', x_1', r_1')$. In the case where the encryption key is the same as the decryption key $k = k'$, the decrypted image is also the same as the original image. For the sensitivity test, we perform an infinitesimal variation in one of the parameters that makes up the decryption key and we keep the others as they are. This is to see its influence on the decrypted image. figure 3.5 clearly illustrates the sensitivity test.

4.5 The encryption key

Taking into account the results obtained in the sensitivity test, we have seen that the sensitivity in the control parameters is of the order of $r_i\ 10^{-15}$

And that of the initial values is of the order of, therefore the precision is of the order of and. The encryption key is: $=x_i 10^{-16}\ 10^{15}10^{16}10^{15} \times 10^{15} \times 10^{16} \times 10^{16}10^{62} \cong (2^3)^{62} = 2^{186}$.

5. Conclusion

In this chapter It consists of extracting the face from the entire image and then encrypting the resulting face using the permutation-diffusion architecture. The simulation results performed on several test images have proven the effectiveness of the proposed method against different cryptographic attacks. Even more, the performance measures found also confirmed the reliability and robustness of the proposed algorithm.

General conclusion

In conclusion, this dissertation explored the area of partial chaotic encryption of areas of interest, highlighting the benefits and challenges of this approach in information security. We examined the fundamentals of chaotic encryption, emphasizing its potential to provide robust, nonlinear protection of sensitive data. During our study, we examined the contribution that the use of chaotic encryption methods and algorithms can bring in the case of an image area instead of the entirety, by highlighting their characteristics and their performances. We also explored key concepts of deterministic chaos, such as sensitivity to initial, which are the basis of chaotic encryption. Using this knowledge, we proposed an approach for partial chaotic encryption of areas of interest. This approach involves applying selective chaotic transformations to specific parts of the data, while leaving other parts intact. This helps protect sensitive information while maintaining the integrity of non-critical parts of the data. However, it is important to emphasize that partial chaotic encryption presents significant challenges. Proper selection of areas of interest and encryption settings is essential to ensure security and accurate data recovery. Additionally, sensitivity to the initial conditions of deterministic chaos can pose problems with the stability and robustness of encryption. We would like to point out that this work was the subject of a scientific conference article published on the partial encryption of areas of interest. This publication demonstrates the importance of this research in the field of the protection of sensitive information and the confidentiality of visual data. Looking ahead, it is necessary to continue research in the area of partial chaotic encryption of areas of interest. Further studies are needed to optimize techniques for selecting areas of interest and to develop mechanisms to control sensitivity to initial conditions. Furthermore, the performance and safety of this approach should be further evaluated through theoretical analyzes and practical experiments.

References

[1]-B. Furht, E. Muharemagic, and D. Socek " Multimedia Encryption and Watermarking, Springer Science & Business Media", 2005.

[2]- Image encryption El-samie, Abd Fathi, E,H, Hossam Eladin Ibrahim, F Mai, Osama, S Saleh, A. Taylor & Francis Group. CRC Press. 2014.

[3]https://en.wikipedia.org/wiki/List_of_chaotic_maps

[4]- K S Tamilkodi, (Mrs) N Rama, "A comprehensive survey on performance analysis of chaotic colour image encryption algorithms based on its cryptographic requirements", International Journal of Information Technology, Control and Automation (IJITCA), vol.5, no.1/2, April 2015.

[5]https://en.wikipedia.org/wiki/Chebyshev_polynomials.

[6]Pawan N. Khade, Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, vol. 9, Issue 3, no 1, May 2012ISSN (Online): 1694- 0814.

[7]- Nitumoni Hazarika, Monjul Saikia, "A Novel Partial Image Encryption Using Chaotic Logistic Map", 2014 International Conference on Signal Processing & Integrated Networks (SPIN),IEEE,2014.

[8]- Monjul Saikia, Nitumoni Hazarika, Margaret Kathing "Partial Image Encryption using Peter De Jong Chaotic Map based Bit-Plane Permutation and it's Performance Analysis" published in ACEEE Fifth International Conference on Recent Trends in Information, Telecommunication and Computing ITC 2014 on Mar 21st at Chandigarh, India ISBN: 978-94-91587-21-3 Search DL ID: 02.ITC.2014.5.5 pp. 1–10 URL: http://searchdl.org/index. php/ conference /view/ 751.

[9]https://en.wikipedia.org/wiki/Chebyshev_polynomials.

[10] Pawan N. Khade, Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, vol. 9, Issue 3, no 1, May 2012ISSN (Online):1694-0814.

[11]- Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solutions and Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[12]- Mayank Mishra, Prashant Singh, Chinmay Garg, "A New Algorithm of Encryption and

Decryption of Images Using Chaotic Mapping", International Journal of Information & Computation Technology. ISSN 0974-2239, vol. 4, no. 7 (2014), pp. 741–746.

[13]- Xin Ma, Chong Fu, Wei-min Lei, Shuo Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", International Journal of Advancements in Computing Technology, vol. 3, no. 5, June 2011.

[14] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd Edition, 2007.

[15] Beloucif, A. (2016). *Contribution à l'étude des mécanismes cryptographiques* (Doctoral dissertation, Université de Batna 2).

[16] Hassan, B. A., & Dawood, F. A. A. (2023). Facial image detection based on the Viola-Jones algorithm for gender recognition. *International Journal of Nonlinear Analysis and Applications*, *14*(1), 1593-1599.

[17] Saikia, M., & Baruah, B. (2017). Chaotic map based image encryption in spatial domain: a brief survey. In *Proceedings of the First International Conference on Intelligent Computing and Communication* (pp. 569-579). Springer Singapore.

[18] Dixit, A., Dhruve, P., & Bhagwan, D. (2012). Image encryption using permutation and rotational XOR technique. *Computer Science & Information Technology*, *2*(3), 01-09.

[19] Khalane, V., Suralkar, S., & Bhadade, U. (2020). Image encryption based on matrix factorization. *Int J Safety Secur Eng*, *10*(05), 655-661.

[20] Andrawus, J., Yusuf, A., & Mustapha, U. T. Accepted Manuscript Fractals.

[21]-Julio Alexander AGUILAR ANGULO-THESE doctorat " Conception d'un Générateur de Valeurs aléatoires en Technologie CMOS AMS 0.35µm" ,ECOLE DOCTORALE Equipe conception de circuit Juin 2015.

[22]-krimmohamed .thése doctorat (Implémentation des séquences chaotiques sur les systèmes de communication moderne :Etalement de spectre à séquence directe DS-SS) université de la séence et de la technologie MOHAMMED BOUDHIAF a Oran .2018/2019 .

[23] Wang X, Liu P (2021) A new full chaos coupled mapping lattice and its application in privacy image
encryption. IEEE Trans Circuits Syst I Regul Pap.

[24] SAHRAOUI, F. (2014). *Sécurité d'image numérique par une approche chaotique* (Doctoral dissertation, Université Ibn Khaldoun-Tiaret-).

[25] Djemaa, A., Boubednikh, A., & Louzzani, N. E. (2021). *Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos* (Doctoral dissertation, université de jijel).

[26] Agaguena Houdjatoulah, T. M. (2023). Etude et simulation d'un système de cryptage d'images à base de chaos.

[27] Liu, Z., Li, J., & Liu, J. (2022). Encrypted face recognition algorithm based on Ridgelet-DCT transform and THM chaos. *Math. Biosci. Eng*, *19* (2), 1373-1387.

[28] Sipi Image Database. https ://sipi.usc.edu/database/, 2023. Accessed on April 11, 2024.