DEMOCRATIC AND PEOPLE'S REPUBLIC OF ALGERIA MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
MOHAMED BOUDIAF UNIVERSITY - M'SILA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

COMPUTER SCIENCE DEPARTEMENT

N° :……..

FIELD: MATHEMATICS AND COMPUTER SCIENCE

FACULTY: COMPUTER SCIENCE

OPTION: Information system and software engineering

Thesis submitted for obtaining the Academic Master degree

By: HACHADI Youness
HADIBI Nisrin

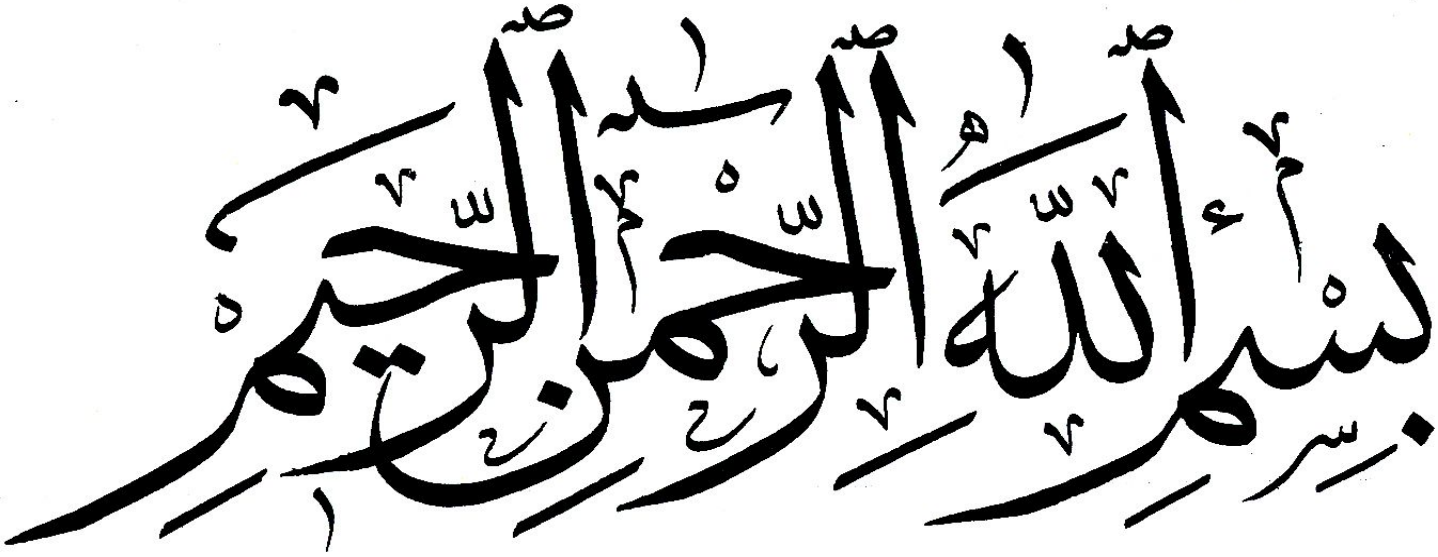
Entitled

Development of a digital image encryption system based on logistics maps

Jury:

……	M'sila University	President
Dr. LAMICHE Chaabane	M'sila University	Reporter
Dr. MOUSSAOUI Adel	M'sila University	Co-Reporter
……	M'sila University	Examiner

College Year: 2019 /2020


بسم الله الرحمن الرحيم

Dedication

We dedicate this work: For all our family members
"Mother father"
"Brothers Sisters"
for their continuous support and we wish them good health and a long life To all our friends, and especially to our best friend Shaima Amaidia, to all our professors who have made every effort to provide us with as much information as possible about our study, to everyone who contributed directly or indirectly to the completion of this work. Finally, we do not forget the distinguished professor Dr. Lamiche Chaabane

HADIBI / HACHADI

Thanks

Above all, we thank ALLAH for giving us the faith, strength, and courage to complete this humble work. I thank our supervisor Dr. Lamiche Chaabane and Co- supervisor Dr. Moussaoui Adel for their methodology and the accuracy of their valuable advice. Thank to our family for their continuous support. I would like to thank all the people who helped me directly or indirectly in completing this letter.

thank you so much

HADIBI / HACHADI

Contents

Liste des figures

General Introduction

General Introduction

Currently, with the great acceleration in the development of Internet and communication technologies, the communication of images in general is a kind that applies strongly and plays a very important role in the transmission of information. However, information security is a sensitive topic for research, discussion and development, and encryption is one of the best alternatives that has proven effective throughout history to ensure confidentiality and security of information.

Problem and objective

Now, it has become clear that we cannot use standard classic encryption methods like RSA, DES, AES, for digital image encryption, because they are designed for textual data. Thus, digital images are characterized by high redundancy, high correlation and voluminous size. The problem posed is how can we design an encryption system to ensure the security of this type of data? In this graduation note and in order to answer this problem, we will implement a chaotic system for the encryption of digital images. This system is based on Clifford Chaotic System and Logistic Map by exploiting the benefits brought by each of them.

Organization of the thesis

We have structured our thesis into three chapters. The first chapter will give a brief presentation on cryptography techniques and its classification, particularly reviewed on symmetric cryptography. In the second chapter takes stock of the basics of digital image. In the third chapter we present the proposed method by Behrouz, Mohadeseh and Vassil in [40]. Then we will end with a general conclusion.

Chapter 1

The cryptography

1. Introduction :

Computer security has become a major challenge, and work in this area of research is increasingly numerous. It is therefore necessary to develop an effective protection tool for transferred data against arbitrary intrusions. Data encryption is very often the only effective way to meet these requirements.

In this chapter, we will present general information on the fundamental concepts of cryptography, classification of cryptographic system, then symmetric encryption algorithms and end with the purposes of cryptography.

2. General Keys on IT Security:

2.1. IT Security:

Means implemented to reduce the vulnerability of a computer system.

2.2 Information System Security (ISS):

All the technical, organizational, legal and human means necessary and in place to restore and guarantee the security of information and the information system.

2.3. Vulnerability:

A weakness (flaw) in the protection of the system, in the form of a threat that can be exploited to intervene on the whole system or an intruder that attacks assets (hardware, software, processes, etc.).

2.4. Threat:

A threat is an individual or application that may exploit a vulnerability to obtain, modify or prevent access to or compromise an asset.

2.5. Attack:

Malicious action that compromises the security of data or computer systems.

2.6. Risk:

The probability that a threat will exploit a vulnerability in the system. Couple (threat, vulnerability).

3. The cryptography:

3.1. Basic concept:

3.1.1. Cryptology:

It is a mathematical science that has two branches: cryptography and cryptanalysis.

3.1.2. Cryptography:

- Science that uses mathematics for data encryption and decryption.
- It is also the study of mathematical techniques related to aspects of IT security (confidentiality, integrity and authenticity)

3.1.3. cryptanalyses:

It is the study of encrypted information, in order to discover its secret. Cryptanalysts are also called «pirates».

3.1.4. Plain text:

Readable and understandable data without specific intervention.

3.1.5. Cipher text (cryptograms):

Unintelligible text resulting from encryption.

3.1.6. Encryption:

A method of concealing plain text by hiding its contents. This operation ensures that only the people to whom the information is intended will be able to access it.

3.1.7. Decryption:

Reverse process of transforming cipher text into plain text.

3.1.8. Key:

The shared secret used to encrypt clear text into encrypted

text and to decrypt encrypted text into plain text.

3.2. Purpose of Cryptography:

Since its inception, cryptography has continued to evolve. Initially given over to the protection of messages exchanged, the range of its applications has expanded to cover only one issue today: the security of information systems. Thus, modern cryptography intervenes in all the major areas of information security, whether through its primary issue: confidentiality but also through the processes of authentication, non-repudiation, data integrity. [01].

- **Confidentiality:** Encrypted text must be legible only to legitimate recipients. It must not be readable by an intruder.
- **Authentication:** The recipient of a message must be able to verify its origin. An intruder must not be able to impersonate someone else.
- **Integrity:** The recipient of a message must be able to verify that it has not been changed on the way. An intruder must not be able to make a false message appear legitimate.
- **Non-Repudiation:** A sender must not subsequently be able to falsely deny having sent a message.

3.3. Classification of cryptosystems :

- **Cryptosystems :**

It is defined as the set of possible keys (key space), possible clear and encrypted texts associated with a given algorithm. Quintuple (P, C, K, E, D), as follow :

- *P :* plain text set
- *C:* Finished set of encrypted texts
- *K :* key space
- For each **K** $\in$ **K**, there is an **ek** $\in$ **E** encryption function, and a corresponding **dk** $\in$ **D** decryption function, such as:

$$D_K(E_K(x)) = x, \text{ for each } x \in P$$

3.3.1. Symmetric cryptography (secret key):

Symmetric cryptography, also known as private key cryptography, has been used for centuries. In this type of cryptography, the decryption key is identical to the key used for encryption, that is, the transmitter and the receiver must have the same key.

The secret of communication is assured only by the key that is used.
The algorithm used is not part of the secret [2].

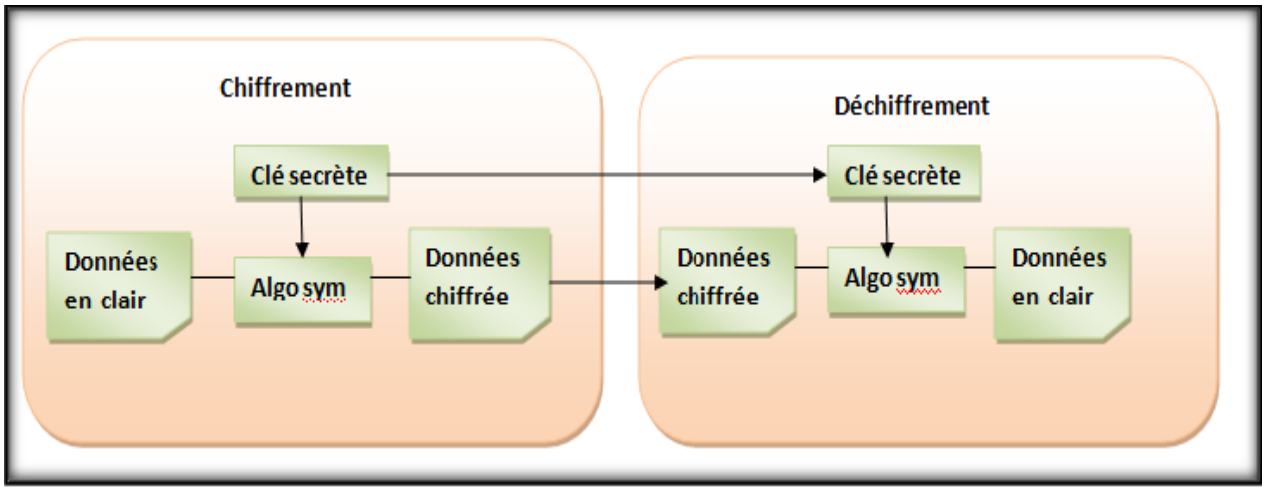


Figure 1.1 : Symmetric encryption.

- **The Characteristics :**
  - The keys are identical : KE = KD = K
  - The key must remain secret.
  - The Most Common algorithms are DES, AES, 3DES, ... etc.
  - At the key generation level, it is chosen randomly in the key space.
  - These algorithms are based on transposition and substitution of clear text bits according to the key.
  - Key size is often 128 bits. DES uses 56, but AES can go up to 256 [3].
- There are two categories of symmetric encryption (encryption and decryption are similar algorithms):
  - **Stream Encryption**: An encryption system that acts on the plain message one bit at a time.
  - **Block ciphers:** This is an encryption system that operates on the plain-text message by groups of bits.

3.2.2. Asymmetric cryptography (Public key):

The principle is that each person (machine) has 2 keys (a PK public key (symbolized by the vertical key) for encryption and a SK secret private key (symbolized by the horizontal key) for decryption) Property: Knowledge of PK

does not allow to deduce SK, and: DSK (EPK (M)) = M, and the best known asymmetric cryptography algorithm is the RSA.

The principle of this kind of algorithm is that it is a one-way trap function. Such a function has the particularity of being easy to calculate in one direction, but difficult or even impossible in the opposite direction. The only way to perform the inverse calculation is to know a hatch. For example, a hatch can be a fault in the key generator. This flaw can be either accidental or intentional on the part of the designer. [4].

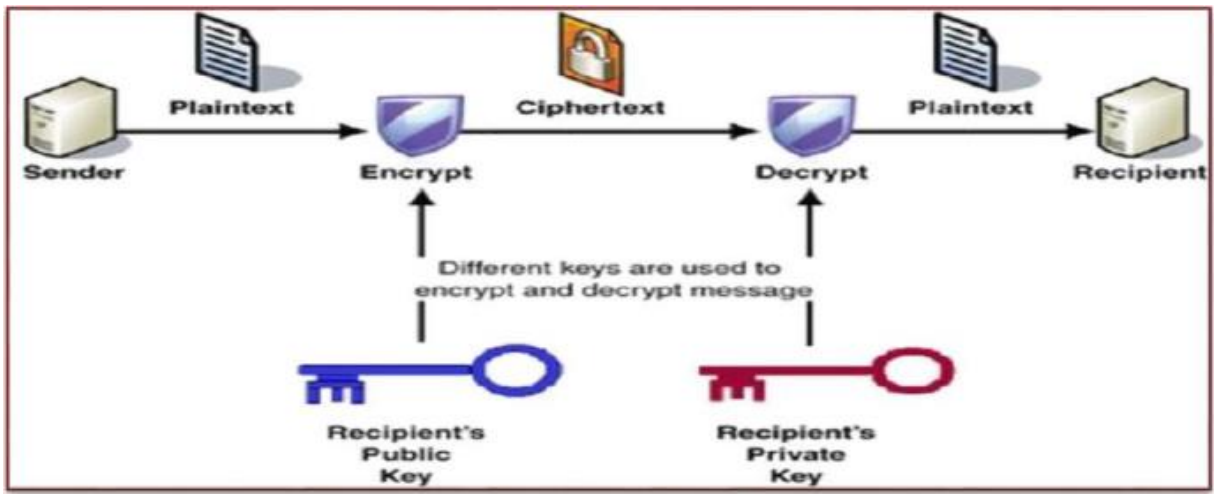


Figure 1.2: cryptography asymmetric

3.2.3. Hybrid encryptions:

Hybrid encryption (the combination of symmetric and asymmetric encryption) of an M message takes place in two steps:

1. Initially, the issuer selects a random K symmetric key. It then uses this K key to encrypt (symmetrically) the M message.

2.Then it figures (asymmetrically) the key K with the public key of the recipient. It sends its recipient M and K's ciphers. The recipient first decrypts the K key, then uses it to find M.

3.4. Symmetric cryptography (secret key):

3.4.1. Stream Encryption:

In flow encryption algorithms, a sequence of bytes or ri bits is produced from the key. This sequence is combined with the bytes or bits of the clear mi to give the bytes or bits of the figure shown ci, according to the formula ci = mi⊕ri [5].

- **Stream Encryption: Algorithms**
  - RC4, the most widespread, designed in 1987 by Ronald Revest, used by the Wi-Fi WEP protocol.
  - A5/1(1994) used in GSM mobile phones to encrypt radio communication between the mobile phone and the nearest relay antenna.
  - E0 used by Bluetooth protocol.
  - Others: FISH - Helix · ISAAC · LEVIATHAN · MUGI · Panama ·SEAL · SOBER · WAKE. [5].

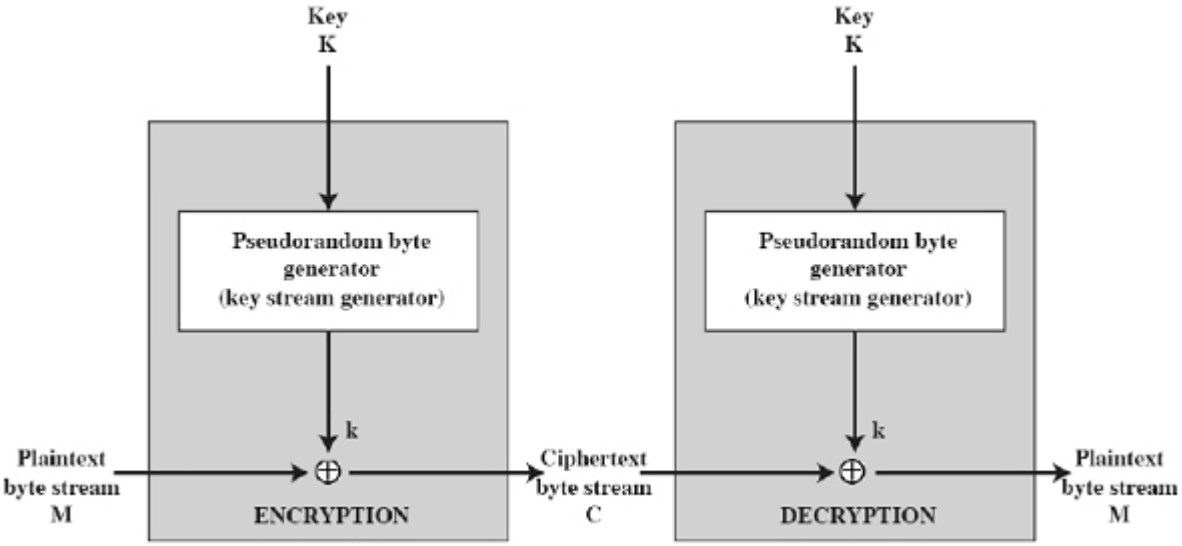


Figure 1.3 : Stream encryption scheme[06].

3.4.2. Block ciphers:

The general idea of block encryption is:

1) Replace characters with a binary code
2) Cut this chain into blocks of given length
3) Encrypt a block by adding bit by bit to a key.
4) Move some bits of the block.
5) Possibly repeat a number of times the operation 3.
6) Proceed to next block and return to item 3 until all message is encrypted.

The most well-known encryption systems in this category are:

DES, **AES** which has become the recommended standard for symmetric encryption

3.5. State of the art in image encryption:

3.5.1. images encryption methods:

There are two main types of methods in image encryption algorithms: scrambling [25] [26] and diffusion [27] [28].

- **Scrambling:**
  Scrambling is achieved by transforming the positions of the pixels. Transforming the positions of the pixels can decrease the correlation between adjacent pixels and achieve encryption. [29]

- **Diffusion:**
  Diffusion is performed by changing the values of the pixels. Diffusion encryption can enhance the randomness and break the statistical characteristics of the cipher images. [29]

Image encryption algorithms can be classified according to the field of application as follows:

I. Methods in the spatial domain:

In the spatial domain, the encryption scheme is applied to the image plane itself, and approaches in this category are based on direct manipulation of the pixels of an image. In these algorithms, encryption destroys the correlation between pixels and makes encrypted images incompressible. Image pixels can be reconstructed (retrieved) completely by a reverse process without any loss of information [42].

Existing spatial domain image encryption algorithms can be categorized into two categories:

- In the first category, a pixel is considered the smallest element, and a digital image is considered a set of pixels.
- In the second category, a pixel can be further divided into bits, on which bit-level operations are performed. For example, a pixel in a grayscale image usually consists of 8 bits [42].

II. Methods in the frequency domain:

The encryption schemes in the frequential domain are based on changing the frame frequency using a transformation, so the reconstruction of the pixels of the original image in the decryption process usually causes a loss of information [42].

3.5.2. Basic tools for analyzing an image encryption algorithm:

I. Key space:

A good encryption algorithm should have large key space to prevent brute-force attacks which is defined to exhaust all the possible keys until the correct one [40].

II. The histogram:

The histogram is a graphical representation of the distribution of pixel luminous intensities [43].

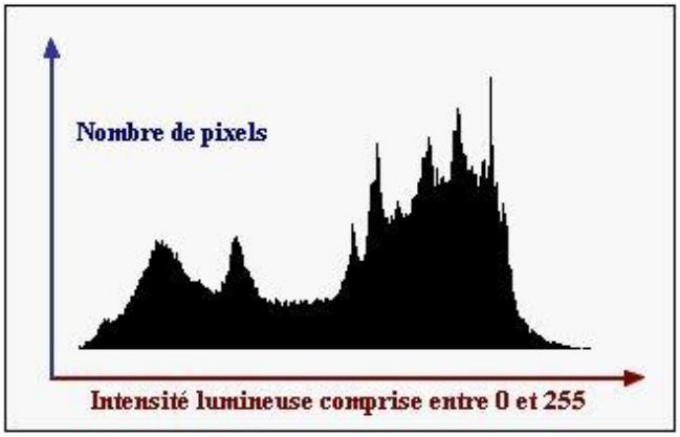


Figure 1.4 : Histogram of a grayscale image [43].

In an image encryption context, the histogram of the encrypted image must be uniform to ensure security against known plain text attack, in other words the attacker will not can't extract information from this histogram.

III. Entropy:

Image information entropy can measure the distribution of image gray values. Image entropy is defined as [40]:

$$H = -\sum_{i=1}^{n} p_{i \log P_i}$$

where P_i represents the probability of occurrence of each pixel and log denotes the base 2 logarithm. The ideal value of the cipher information entropy is 8 [40].

IV. Analysis for Correlation of Adjacent Pixels:

Correlation analysis of adjacent pixels is an important way to test the gray value relationship between adjacent pixels in cipher image. Adjacent pixels in plain image have high correlation and in ciphered image should have low correlation. We calculate the correlation coefficient of the plain an encrypted $r_{P,C}$ by using the following formulas [40]:

$$E(P)=\frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}P(i,j),\quad E(C)=\frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}C(i,j)$$

$$D(P)=\frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[P(i,j)-E(P)\right]^{2}$$

$$\operatorname{cov}(P,C)=\frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[P(i,j)-E(P)\right]\left[C(i,j)-E(C)\right]$$

$$r_{P,C}=\frac{\operatorname{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}}$$

In these formulas $P(i,j)$ and $C(i,j)$ are gray values of the plain pixel and the encrypted one. $E(P)$,$E(C)$, $D(P)$ and $D(C)$ are mathematical expectation of plain pixels $P(i,j)$, mathematical expectation of cipher pixels $C(i,j)$,variance of plain pixels $P(i,j)$ and variance of cipher pixels $C(i,j)$, respectively.

3. Conclusion:

In this chapter, we have provided a brief overview of the different techniques of cryptography. We also focused on the classification of systems cryptographic concerns symmetric encryption algorithms, and then with state-of-the-art encryption techniques image. Finally, we finished we described the basic tools for analyzing an image encryption algorithm as key space and histogram, the entropy, and the last this is correlation between adjacent pixels.

In the next chapter, we will see the basics of digital images.

Chapter 2

Digital Images

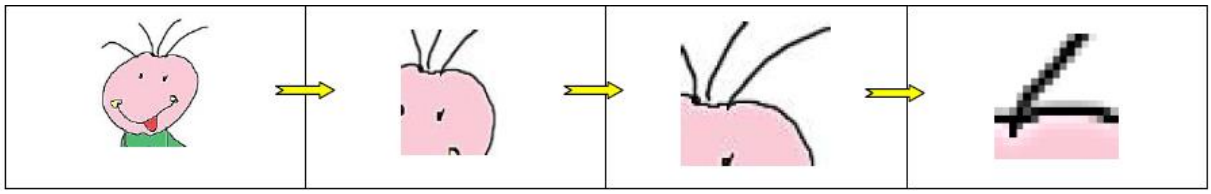
1. Introduction :

Because of the greater use and exchange of digital images, and the value of the important information they contain, in this chapter we will present the basic concepts of imaging through the types of digital images. Next, we will talk about the methods of color coding in images. Then we will talk about the most important and famous formats. Finally, we will conclude with image encryption techniques.

2. Basic notions about imaging:

2.1. Digital image:

A digital image is a mosaic of single-colored points. The more points it has, the better it is defined. When you magnify an image on the screen or print it, you don't change the number of points, you just make them bigger or smaller and therefore visible.[8]



One can be defined as a two-dimensional function, f (x, y), where x and y are spatial (plane) coordinates for each pixel. [9]

These pixels will be assigned binary numbers to define gray hues or colors [10].

2.2 Pixel:

A digital image contains a finite number of points. These points are called pixels (contraction of the English words "picture element"). [11]

A pixel is the smallest unit of a digital image or graphic that can be displayed and represented on a digital display device.

A pixel is the basic logical unit in digital graphics. Pixels are combined to form a complete image, video, text or any visible thing on a computer display.[12]

The size of the pixel defines the resolution compared to the original analog image, i.e. the thinness of the grid. The lower the resolution, the lower the number of pixels in the image, and the more the quality of the digital image deteriorates. [11]

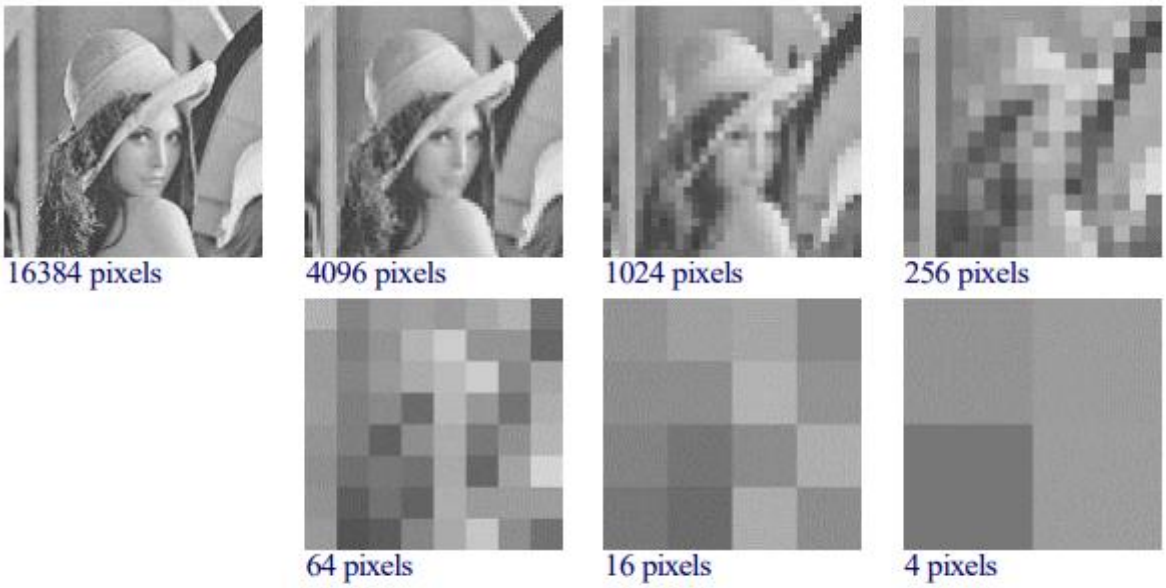


Figure 2.1: variation in the number of pixels. In fact, when viewing the screen, the size is divided by 4 at each step. [11]

2.3. The definition for an image:

The Definition of a digital image therefore corresponds to the product of the number of pixels that compose the image in Length (horizontal axis) by that of its Height (vertical axis).[13]

Définition = (Nombre de pixel en Longueur) x (Nombre de pixel en Hauteur)

2.4. Resolution:

Image resolution is typically described in PPI, which refers to how many pixels are displayed per inch of an image.

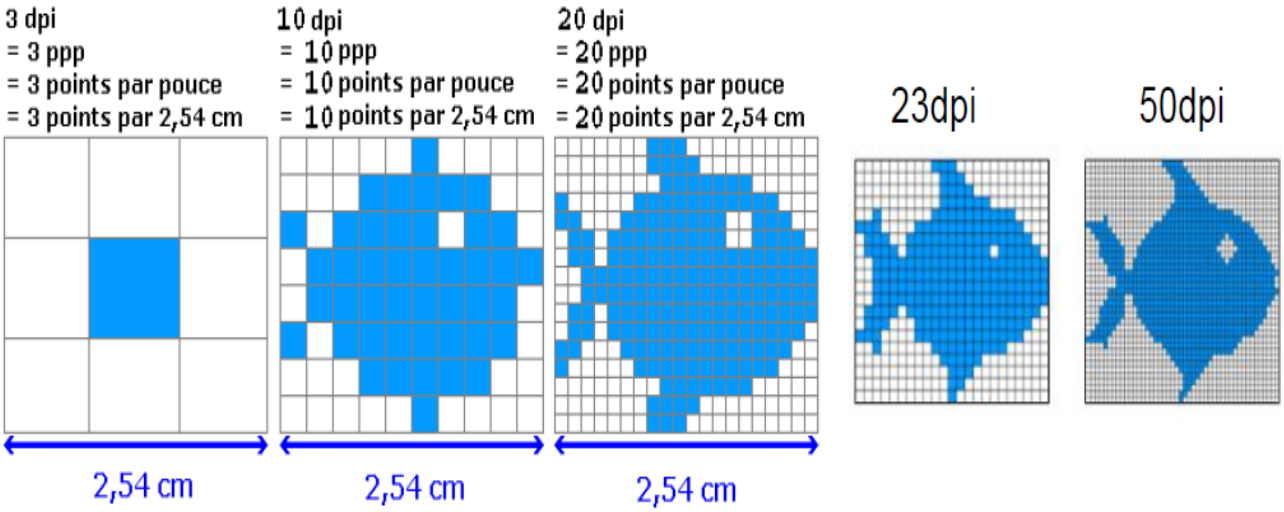


Figure 2.2 : Explanatory diagram of an image resolution [15].

Higher resolutions mean that there more pixels per inch (PPI), resulting in more pixel information and creating a high-quality, crisp image.[14]

2.5. Size:

The size of the image is the place it occupies in binary coding. It's unit is « byte ». [10]

Size = number of bytes for each pixel × definition

3. Types of Digital Images:

3.1. Binary images:

Binary images are the simplest type of images and can take on two values, typically black and white, or 0 and 1. A binary image is referred to as a 1-bit image because it takes only 1 binary digit to represent each pixel. These types of images are frequently used in applications where the only information required is general shape or outline, for example optical character recognition (OCR).

Binary images are often created from the gray-scale images via a threshold operation, where every pixel above the threshold value is turned white ('1'), and those below it are turned black ('0'). In the figure below, we see examples of binary images.[16]

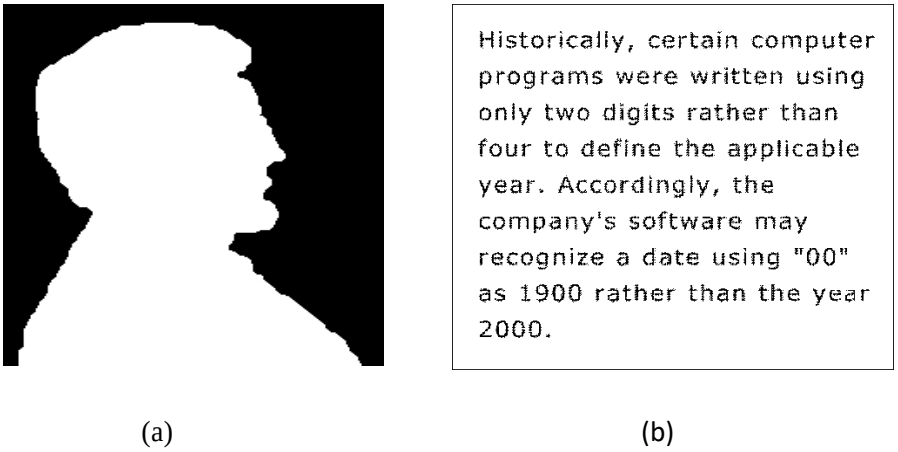


Figure 2.3: Binary images. (a) Object outline. (b) Page of text used in OCR application. .[16]

3.2. Gray-scale images:

Gray-scale images are referred to as monochrome (one-color) images. They contain gray-level information, no color information. The number of bits used for each pixel determines the number of different gray levels available.[16]

If the encoding is done in 8 bits per pixel, there will be: $2^n=2^8=256$ gray levels ranging from white to black.

If the encoding is done in 16 bits per pixel, there will be: $2^n=2^{16}=65536$ gray levels ranging from white to black.[10]

The figure below shows examples of gray-scale images.

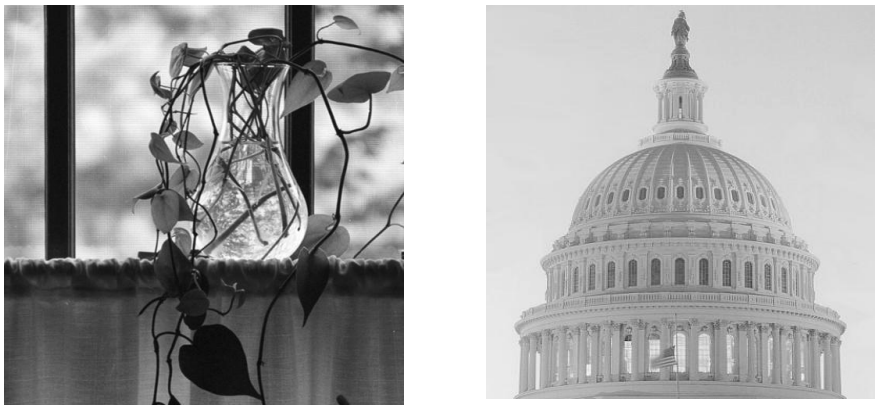


Figure 2.4: Examples of gray-scale images. [16]

In applications like medical imaging and astronomy, 12 or 16 bits/pixel images are used. These extra gray levels become useful when a small section of the image is made much larger to discern details.

3. 3. Color images:

Color images can be modeled as three-band monochrome image data, where each band of data corresponds to a different color. The actual information stored in the digital image data is the gray-level information in each spectral band.

Typical color images are represented as red, green, and blue (RGB images). Using the 8-bit monochrome standard as a model, the corresponding color image would have 24-bits/pixel (8-bits for each of the three-color bands red, green, and blue). The figure below illustrates a representation of a typical RGB color image.[16]

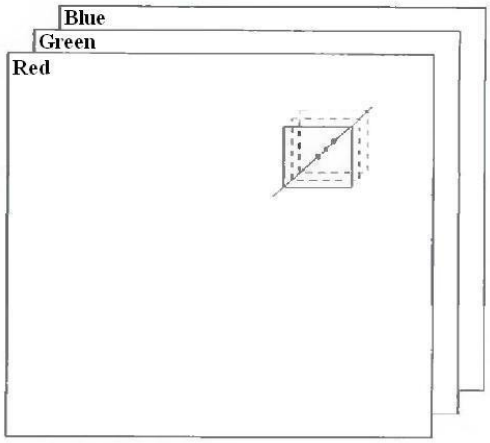


Figure 2.5: Representation of a typical RGB color image.[16]

3.4. Multispectral images:

Multispectral images typically contain information outside the normal human perceptual range. This may include infrared, ultraviolet, X-ray, acoustic, or radar data. These are not images in the usual sense because the information represented is not directly visible by the human system. However, the information is often represented in visual form by mapping the different spectral bands to RGB components.[16]

4. Digital Image File Formats:

Types of image data are divided into two primary categories: bitmap and vector.

- ***Bitmap images*** (also called raster images) can be represented as 2-dimensional functions *f (x, y),* where they have pixel data and the corresponding gray-level values stored in some file format.
- ***Vector images*** refer to methods of representing lines, curves, and shapes by storing only the key points. These key points are sufficient to define the shapes. The process of turning these into an image is called *rendering*. After the image has been rendered, it can be thought of as being in bitmap format, where each pixel has specific values associated with it. [16]

Figure 2.6: difference between vector and matrix image. [17]

Most of the types of file formats fall into the category of bitmap images, for example:

4.1.TIFF (Tagged Image File Format): (.tif, .tiff)

TIFF or Tagged Image File Format are lossless images files meaning that they do not need to compress or lose any image quality or information (although there are options for compression), allowing for very high-quality images but also larger file sizes. [18]

4.2.GIF (Graphics Interchange Format) : (.gif)

GIF or Graphics Interchange Format files are widely used for web graphics, because they are limited to only 256 colors, can allow for transparency, and can be animated. GIF files are typically small is size and are very portable. [18]

4.3.JPEG (Joint Photographic Experts Group) : (.jpg, .jpeg)

JPEG, which stands for Joint Photographic Experts Groups is a "lossy" format meaning that the image is compressed to make a smaller file. The compression does create a loss in quality but this loss is generally not noticeable. JPEG files are very common on the Internet and JPEG is a popular format for digital cameras - making it ideal for web use and non-professional prints. [18]

4.4.BMP (Windows Bitmap) : (.bmp)

BMP or Bitmap Image File is a format developed by Microsoft for Windows. There is no compression or information loss with BMP files which allow images to have very high quality, but also very large file sizes. Due to BMP being a proprietary format, it is generally recommended to use TIFF files.[18]

4.5.PNG (**P**ortable **N**etwork **G**raphics**): (.png)**

PNG or Portable Network Graphics files are a lossless image format originally designed to improve upon and replace the gif format. PNG files are able to handle up to 16 million colors, unlike the 256 colors supported by GIF. [18]

Different color modes have different size data values, as shown:

Image Type	Bytes per pixel	Possible color combinations	Compatible File Types
1 bit Line art	$^1/_8$ byte per pixel	2 colors, 1 bit per pixel. One ink on white paper	TIF, PNG, GIF
8-bit Indexed Color	Up to 1 byte per pixel if 256 colors	256 colors maximum. For graphics use today	TIF, PNG, GIF
8-bit Grayscale	1 byte per pixel	256 shades of gray	Lossy: JPG Lossless: TIF, PNG
16 bit Grayscale	2 bytes per pixel	65636 shades of gray	TIF, PNG
24 bit RGB (8-bit mode)	3 bytes per pixel (one byte each for R, G, B)	Computes 16.77 million colors max. 24 bits is the "Norm" for photo images, e.g., JPG	Lossy: JPG Lossless: TIF, PNG
32 bit CMYK	4 bytes per pixel, for Prepress	Cyan, Magneta, Yellow and Black ink, typically in halftones	TIF
48-bit RGB (16-bit mode)	6 bytes per pixel	2.81 trillion colors max. Except we don't have 16-bit display devices	TIF, PNG

Figure 2.7: Different size data values of different color modes.[19]

5. Digital Image Representation:

The monochrome digital image *f (x, y)* resulted from sampling and quantization has finite discrete coordinates *(x, y)* and intensities (gray levels). We shall use integer values for these discrete coordinates and gray levels. Thus, a monochrome digital image can be represented as a 2- dimensional array (matrix) that has *M* rows and *N* columns [16]:

$$f(x,y) = \begin{pmatrix} f(1,1) & f(1,2) & & f(1,N) \\ f(2,1) & f(2,2) & & f(2,N) \\ \vdots & \vdots & & \vdots \\ f(M,1) & f(M,2) & \dots\dots & f(M,N) \end{pmatrix}$$

Each element of this matrix array is called *pixel*. The spatial resolution (number of pixels) of the digital image is *M* * *N*. The gray level resolution (number of gray levels) *L* is

$$\boldsymbol{L = 2^k}$$

Where *k* is the number of bits used to represent the gray levels of the digital image. When an image can have 2^k gray levels, we can refer to the image as a "*k*-bit image". For example, an image with 256 possible gray- level values is called an 8-bit image. [16]

The gray levels are integers in the interval [0, *L*-1]. This interval is called the *gray scale*. [16] The number, *b*, of bits required to store a digitized image is

$$\boldsymbol{b = M * N * k}$$

Example:

For an 8-bit image of size 512×512, determine its gray-scale and storage size.

Solution: *k*.= 8, *M* = *N* = 512

Number of gray levels $L = 2^k = 2^8 = 256$

The gray scale is [0, 255]

Storage size (b) = *M* * *N* * *k* = 512 * 512 * 8 = 2,097,152 bits

6. Conclusion:

In this chapter, we talked about the importance of digital images and their types, the methods of encoding pixels of digital images, the most famous known formats and their characteristics

In the next chapter, we will explain the method we reproduce the work proposed by Behrouz, Mohadeseh and Vassil in [40] for digital image encryption.

Chapter 3

Image Encryption Based on Permutation and Substitution:

Clifford Chaotic System and Logistic Map [40]

1. Introduction:

Cryptography researchers have proposed several techniques for encrypting digital images. Among them there are algorithms which based on theories like chaos theory, Fibonacci, permutation, and also algorithms which based on different technologies like: DNA sequencing, optics, cellular automaton and Fourier transformation, and many other techniques

In this chapter, we reproduce the work proposed by Behrouz, Mohadeseh and Vassil in [40], image encryption algorithm based on the Clifford attractor and the logistic map. we begin by explaining some of the mathematical principles on which the encryption algorithm was built and their purpose, and then presenting the experimental results and their analysis.

2. Chaos theory:

2.1. Definition:

Chaos theory is a branch of mathematics focusing on the study of chaos states of dynamical systems whose apparently random states of disorder and irregularities are often governed by deterministic laws that are highly sensitive to initial conditions.[30] [31]

2.2. Chaos and Cryptography:

In the past few decades, chaos and non-linear dynamics have been used in the design of hundreds of cryptographic primitives. These algorithms include image encryption algorithms.[32]

The majority of these algorithms are based on unimodal chaotic maps and a big portion of these algorithms use the control parameters and the initial condition of the chaotic maps as their keys. From a wider perspective, without loss of generality, the similarities between the chaotic maps and the cryptographic systems is the main motivation for the design of chaos based cryptographic algorithms.[32] One type of encryption, secret key or symmetric key, relies on diffusion and confusion, which is modeled well by chaos theory.[33]

Chaotic cryptology includes two integral opposite parts: Chaotic cryptography. Chaotic cryptanalysis. Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary.

The new image encryption algorithms based on chaotic maps proved that application of chaotic map with higher dimension could improve the

quality and security of the cryptosystems.

2.3. Chaotic Maps:

In the group of chaotic maps, the 1D chaotic maps have lots of applications because of their simple structures. In this section, we briefly review three 1D chaotic maps: The Logistic, Tent and Sine maps.[07]

2.3.1. Logistic map [07]:

The Logistic map is one of famous 1D chaotic maps. It is a simple dynamical equation with complex chaotic behavior. The mathematical definition can be expressed in the following equation:

$$X_{n+1} = \mathcal{L}(r, X_n) = rX_n(1 - X_n)$$

where r is a parameter with range of [0, 4] and Xn is the output chaotic sequence. To observe its chaotic behaviors, its bifurcation diagram and Lyapunov Exponent a represented in Figure 3.1 (a)and Figure 3.2 (a). In the bifurcation diagram shown in Figure 3.1(a), the dotted line shows its good chaotic behavior and the solid line represents its non-chaotic property.

2.3.2. Tent map [07]:

The Tent map is known as its tent-like shape in the Graph of its bifurcation diagram. It can be defined by the Following equation:

$$X_{n+1} = \mathcal{T}(u, X_n) = \begin{cases} uX_n/2 & X_i < 0.5 \\ u(1 - X_n)/2 & X_i \geq 0.5 \end{cases}$$

Where parameter u ϵ [0, 4].

Its chaotic property is shown in bifurcation analysis in Figure 3.1 (b) and Lyapunov Exponent analysis in Figure 3.2(b). Both analysis results prove that its chaotic range is [2, 4].

2.3.3. Sine map [07]:

The Sine map has a similar chaotic behavior with the Logistic map. The definition can be described by the Following equation:

$$X_{n+1} = \mathcal{S}(a, X_n) = a \sin(\pi X_n)/4$$

Where parameter α ϵ (0, 4].

As shown in Figure 3.1 (c) and Figure 3.2 (c), its bifurcation diagram

and Lyapunov Exponent are similar with those of the Logistic map in Figure 3.1 (a) and Figure 3.2 (a).

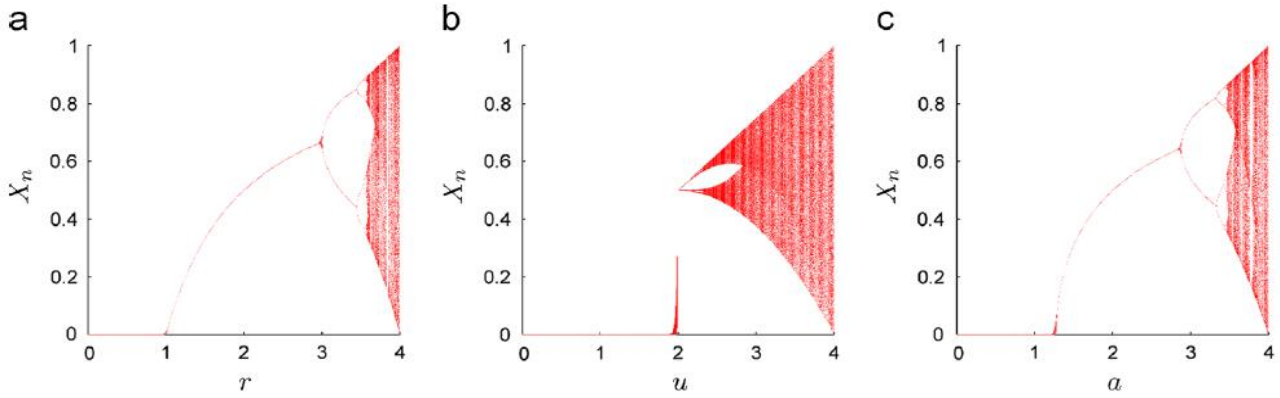


Figure 3.1: The Bifurcation diagrams of the (a)Logistic map; (b)Tent map; (c)Sine map. [07]

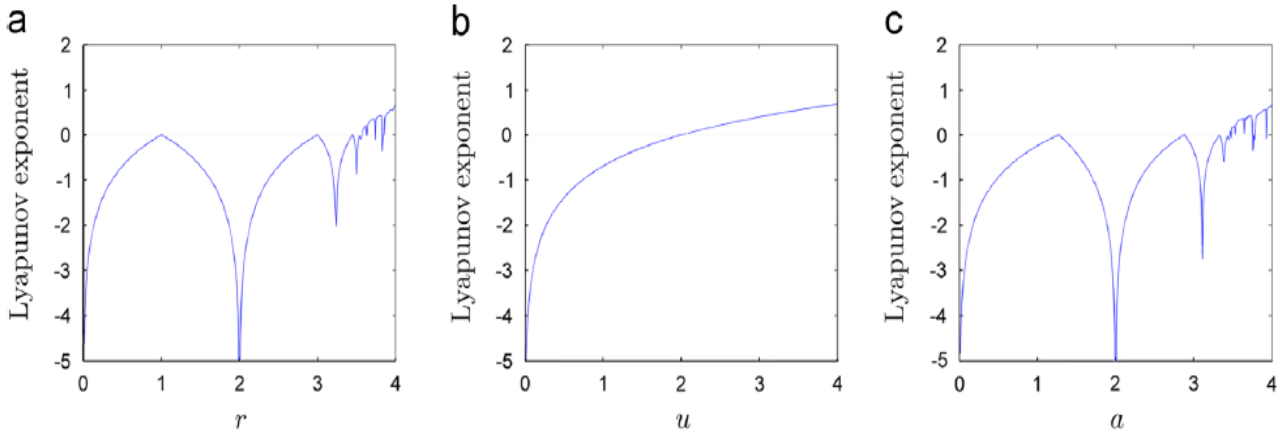


Figure 3.2: The Lyapunov Exponent of the (a)Logistic map; (b)Tent map; (c)Sine map.[07]

3. Logistic Map:

3.1. Logistic Equation:

The logistic equation (sometimes called the Verhulst model or logistic growth curve) is a model of population growth first published by Pierre Verhulst (1845, 1847). The model is continuous in time, but a modification of the continuous equation to a discrete quadratic recurrence equation known as the logistic map is also widely used.[34]

3.2. Logistic Map:

Replacing the logistic equation

$$\frac{dx}{dt} = rx(1 - x)$$

with the quadratic recurrence equation

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

where r (sometimes also denoted μ) is a positive constant sometimes

known as the "biotic potential" gives the so-called logistic map. This quadratic map is capable of very complicated behavior. [35]
While John von Neumann had suggested using the logistic map $x_{(n+1)} = 4x_n(1 - x_n)$ as a random number generator in the late 1940s, it was not until work by W. Ricker in 1954 and detailed analytic studies of logistic maps beginning in the 1950s with Paul Stein and Stanislaw Ulam that the complicated properties of this type of map beyond simple oscillatory behavior were widely noted. [35]
The first few iterations of the logistic map give:

$$x_1 = r x_0 (1 - x_0)$$

$$x_2 = r^2 (1 - x_0) x_0 \left(1 - r x_0 + r x_0^2\right)$$

$$x_3 = r^3 (1 - x_0) x_0 \left(1 - r x_0 + r x_0^2\right) \times \left(1 - r^2 x_0 + r^2 x_0^2 + r^3 x_0^2 - 2 r^3 x_0^3 + r^3 x_0^4\right),$$

where x_0 is the initial value, plotted above through five iterations (with increasing iteration number indicated by colors; 1 is red, 2 is yellow, 3 is green, 4 is blue, and 5 is violet) for various values of r.

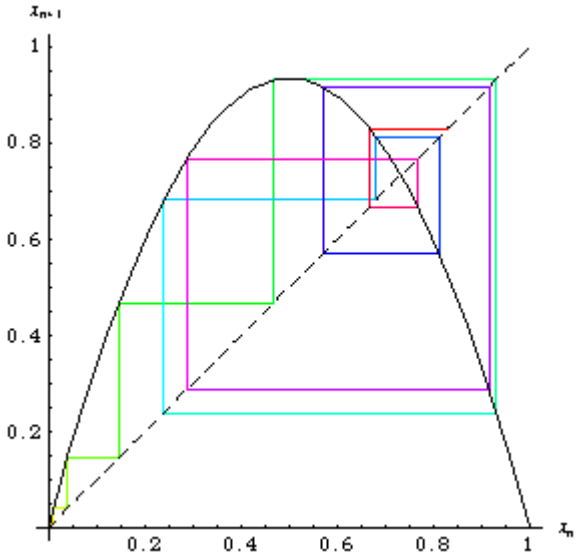


Figure 3.3: Cobweb plots for the logistic map.[35]

Chaotic behavior of the function depends entirely on the value of r, which is constrained to the range of [3.99,4] to make the function operate in the most chaotic region. Bifurcation diagram of the Logistic Map is given in **Figure 3.4**. It can be seen from **Figure 3.4**that as the value of r approaches to 4, the output of the function takes on more distinct values ranging from 0 to 1. Discrete form of the chaotic function used is given in Eqs. (2) and (3). [36]

The aim for using Logistic Map is to benefit from its well-known chaotic behavior to perform more complex pixel permutation, namely better diffusion

operation. One of the functions is used to find new positions of the pixels while the other operates to modify their intensities.

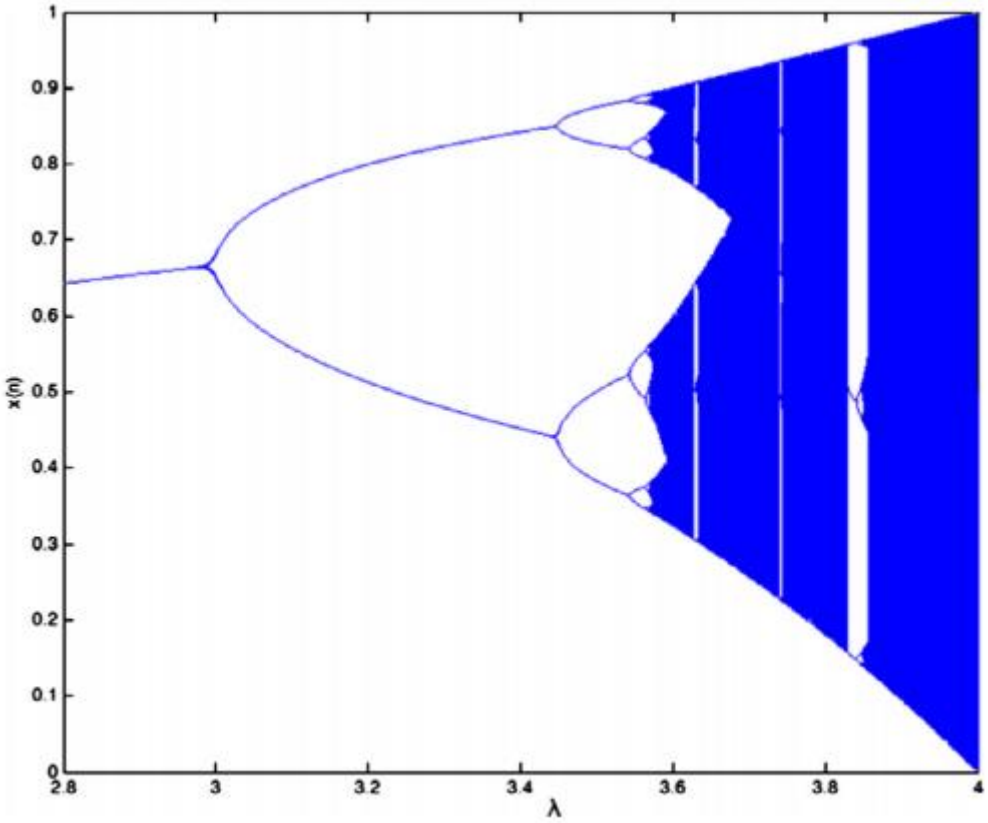


Figure 3.4: Bifurcation diagram of the Logistic Map.[36]

An enlargement of the previous diagram in **Figure 3.4** around r=3.5 in **Figure 3.5**, with value of r at which a 2^ncycle first appears indicated by blue lines.

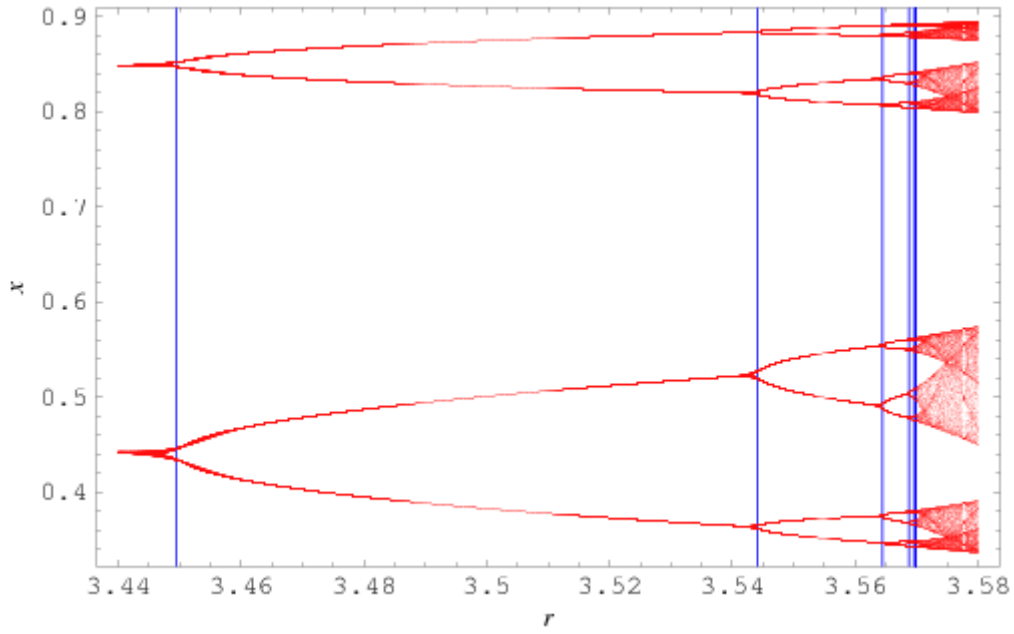


Figure 3.5: Zoom in on the Bifurcation diagram of the Logistic Map.[35]

4. Clifford Chaotic System:

The behavior of the chaotic dynamical system takes place to a set of states, which is called an attractor. There are several types of an attractor like a point, a curve, a manifold or a complicated set with a fractal structure which is called strange attractor [37]. The fixed points of strange attractor are locally unstable but the system is globally stable [38]. Strange attractors can be generated in several ways such as by quadratic or trigonometric maps. Control parameters a, b, c, d, e, f, define behavior of the chaotic system [40].

$$\begin{aligned} x_{n+1} &= \sin(ay_n) + c\cos(ax_n) \\ y_{n+1} &= \sin(bx_n) + d\cos(by_n) \\ z_{n+1} &= \sin(ey_n) + f\cos(ez_n) \end{aligned} \quad (1)$$

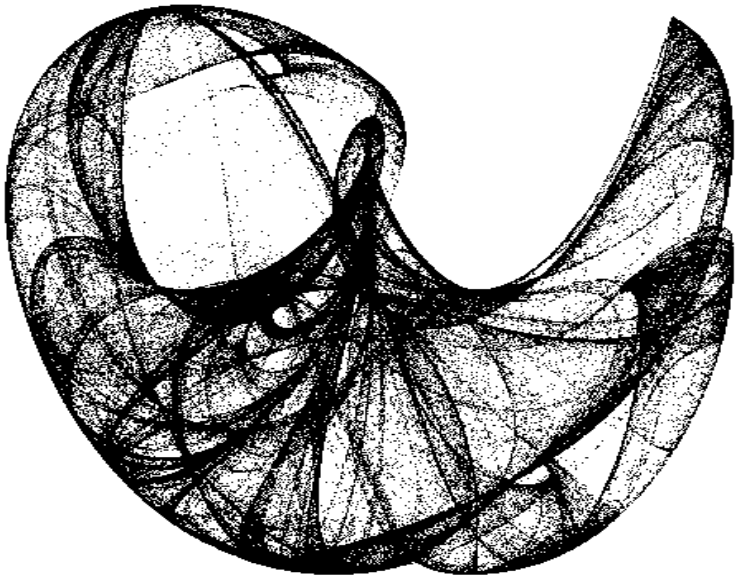


Figure 3.5: Clifford attractor based on (1) [40].

Strange attractors are markedly patterned, when they are geometrically represented. One of the strange attractors with predefined control parameters is shown in **Figure 3.5**. Clifford attractor this dynamical system is used for the encryption purposes in the studied algorithms.

Implementation of image encryption is in two steps: [40]

The first step is image scrambling that the position of the pixels in the image is changed and the second step is pixel substitution. An image can be described by the position and the pixel value. This method can change the position and value of the image pixel and it converts the image from a plain digital image into a noise-polluted image.

Pixel substitution is implemented by XOR or other operation with other sequence or matrix to change plain image pixel value. The main parameters of the Clifford attractor are keys for the process of encryption.

Pixel of image is used as the initial value of Clifford system. Equation in (1) is 3D extension which can be used for encryption of coordinates (pixel position) (x_0, y_0) .and the value of each pixel $P(x_0, y_0)$. New positions and modification value are gained after iterations and quantization. These positions are then used for pixel permutation and the modification value is XOR operated with original pixel value and the value of the previous pixel and encrypted pixel is gained this way [39]. According to **Figure 3.6.**

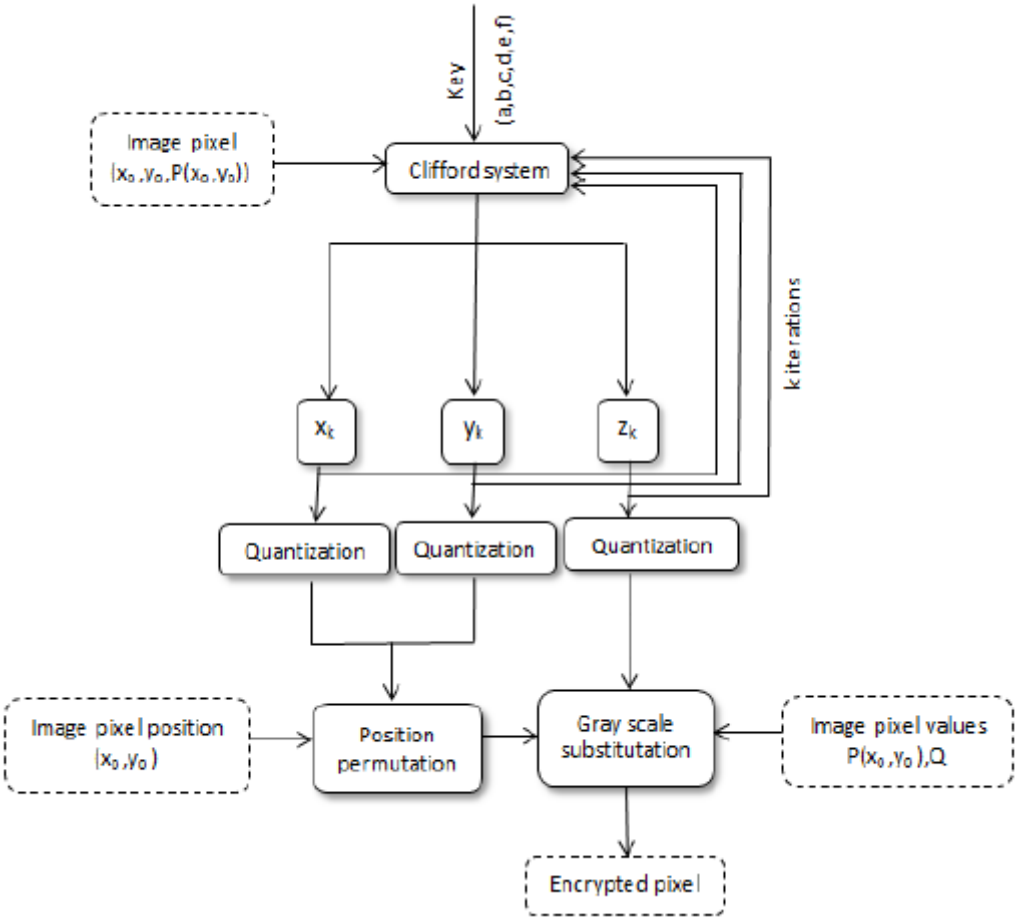


Figure 3.6: Flowchart of encryption Clifford system process suggested in [40]

5. Encryption System based on Clifford system and logistic map [40]:

We use the trigonometric strange attractor which is described by (1). In the new algorithm, first coordinates (x_0, y_0) and value $P(x_0, y_0)$ of pixels put into a Clifford system. Next Logistic map iterate k_2 times with r_1, r_2, r_3 parameters. After quantization step, positions and modification value are gained. **Figure 3.7.**

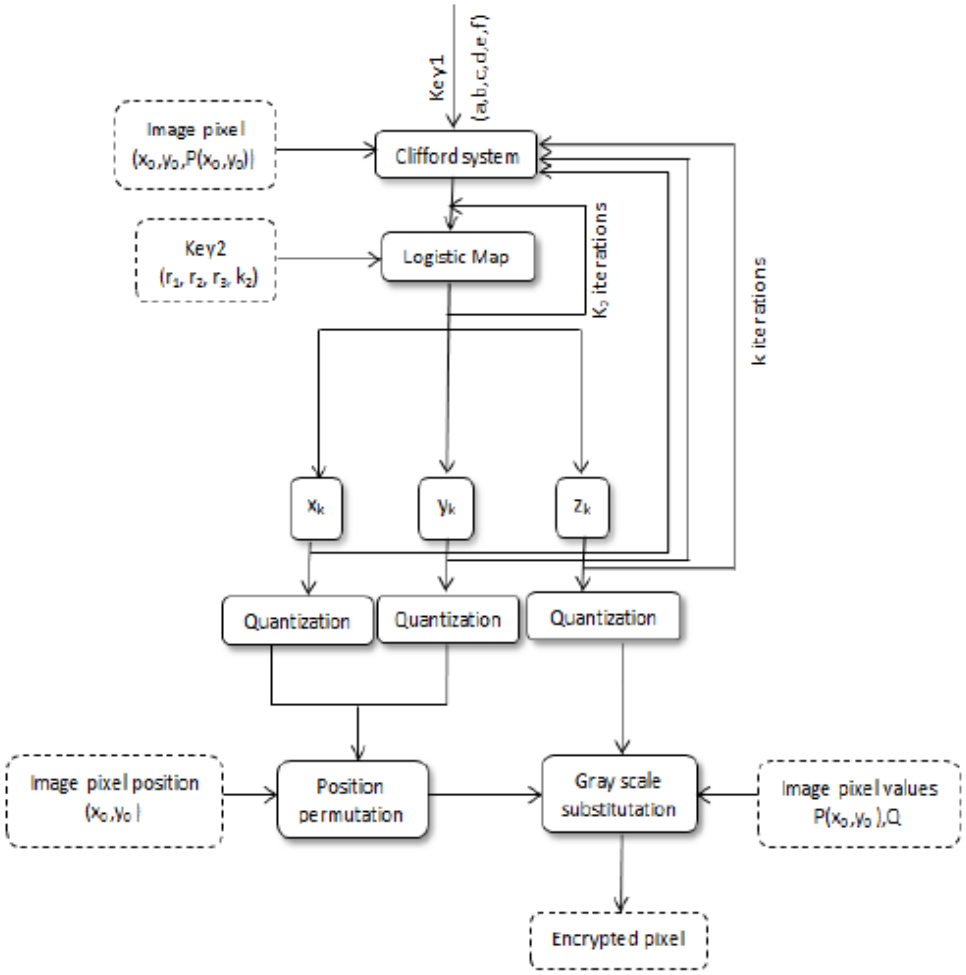


Figure 3.7: Flowchart of Encryption System based on Clifford system and logistic map [40].

Encryption system contains 7 steps as follows [40]:

Step1. Key generation**:** Select parameters a, b, c, d, e, f of Clifford attractor and r_1, r_2, r_3, k_2 of Logistic map.

For Example:

- a = -1.85, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63
- $r_1 = 4$, $r_2 = 4$, $r_3 = 3.95$, $k_2 = 5$

Step2. Image conversion matrix**:** Converts the tested image to a matrix. For grayscale images, the dimension of matrix is [n x m]. n is the height of the image while m is the width. A color image can be converted into grayscale image.

Step3. Initial selection**:** as the initial process of encryption, select a pixel position (x_0, y_0) and a pixel value $z_0 = P(x_0, y_0)$.

Step4. New Clifford system**:** perform Logistic map and Clifford stranger to disorder the position and value pixel of image. Put x_0, y_0 and $z_0 = P(x_0, y_0)$ into the Logistic map with k_2 iterations.

$$x_0 = r_1\ x_0(1-x_0)$$
$$y_0 = r_1\ y_0(1-y_0)$$
$$z_0 = r_1\ z_0(1-z_0)$$

Then Clifford attractor is used to shuffle pixel position and pixel value.
The obtained x_0, y_0, z_0 are the initial values for Clifford equation.

$$x_k = \sin(a y_0) + c\ \cos(a x_0)$$
$$y_k = \sin(b x_0) + d\ \cos(b y_0)$$
$$z_k = \sin(e y_0) + f\ \cos(e z_0)$$

Set $x_0 = x_k$, $y_0 = y_k$, $z_0 = z_k$ and iterate the above equation k times.
The original pixel at coordinates (x_0, y_0) is swapped with the pixel at coordinates.

Step5. Reshaping matrices: Convert 2D matrices x_k, y_k, z_k into 1D matrices.

Step6. Quantization**:** For the obtained vectors in step 5, determine minimum and maximum value of vectors. Then the range is divided between the minimum and maximum.

Step7. Changing values of pixels**:** Pixel value at coordinates (x_k, y_k) is modified by XOR operation of value z_k and then XOR operated with the value of the previous processed pixel Q. This process must be done for every pixel in the image.

$$P(x_o, y_o) \leftrightarrow P(x_k, y_k) \oplus z_k \oplus Q$$

Pseudo code implementation of Behrouz's image encryption [40]

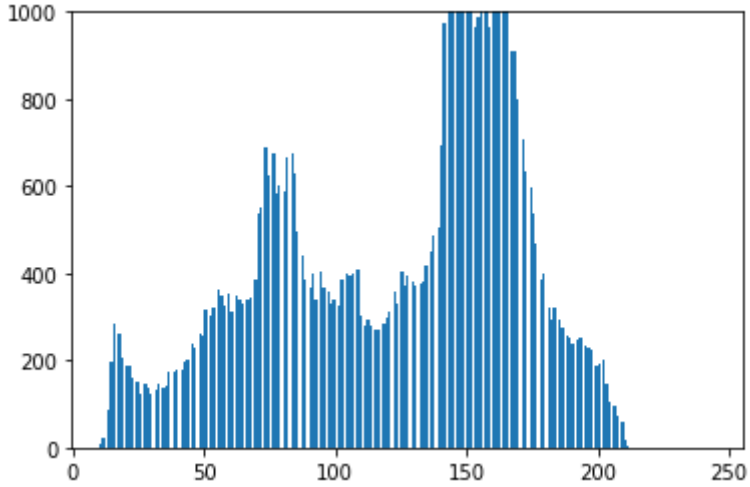
```
Initialization ( a,b,c,d,e,f,k,r1,r2,r3,lgst_round)
Pic ←input_image
r_im ← pic.row
c_im ←
pic.column
for      i → r_im     do
     for     j → c_im     do
          x ←
          i y
          ← j
          z ← pic [i] [j]
          for      n → k      do
               for p → lgst_round do
                    x ← r1 * x * (1-
                    x) y ← r2 * y *
                    (1-y) z ← r3 * z
                    * (1-z)
               end for
               xk [i] [j] ← sin (a * y) + c * cos (a * x)
               yk [i] [j] ← sin (b * x) + d * cos (b * y)
               zk [i] [j] ← sin (e * y) + f * cos (e * z)
          end for
    end
 for
end for
 Q ← 0
 for      i → r_im        do
     for      j → c_im        do
          x_step ← minmax ( xk) / ( r_im -
          1) y_step ← minmax ( yk) / ( c_im
          -1) z_step ← minmax ( zk) / ( 256)
          Xk ← xk [i] [j] – min (xk) /
          x_step Yk ← yk [i] [j] – min (yk)
          / y_step Zk ← zk [i] [j] – min (zk)
          / z_step
          Q_new ← XOR (pic [ Xk[i] [j] ] [ Yk [i] [j] ] , Zk [i]
          [j] ) Q_new ← XOR ( Q_new , Q )
          New_pic [i] [j] ←
          Q_new Q ← Q_new
         end for
 end for
```

6. Simulation Results and Statistical Analysis:

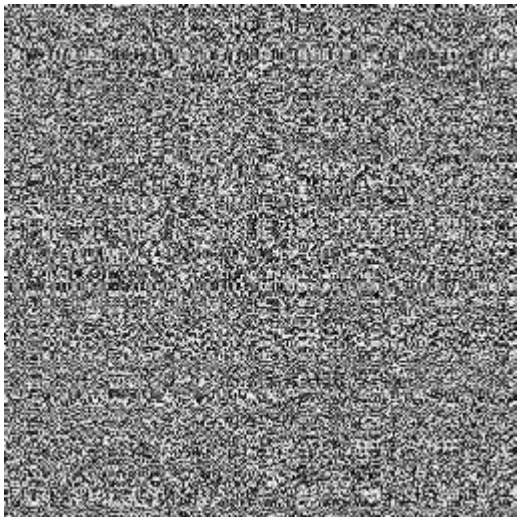
The following tests are realized by PYTHON software on Intel® Core (TM) i3-4005U @, 1.70 GHz PC.

a = - 1.8500001, b=1.48, c = -1.55, d = -1.87, e= -4.32, f =0.63, $r_1 = 4$, $r_2 = 4$, $r_3 = 3.95$, $k_2 = 5$

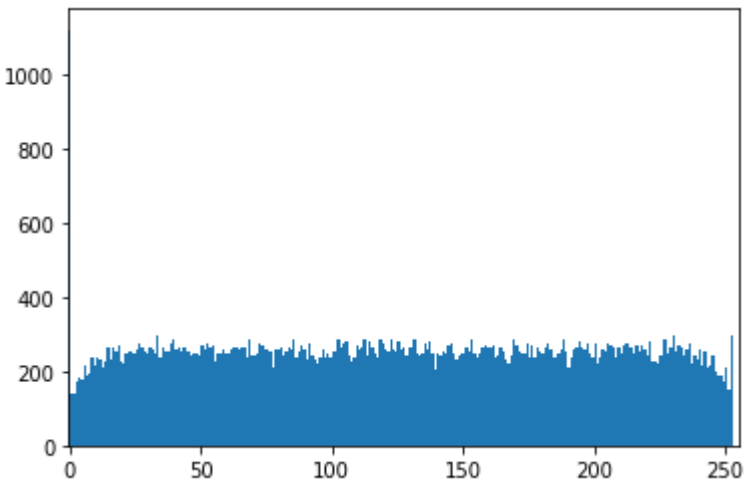
(a)



(b)



(c)



(d)

Figure 3.8: (a) Plain Bird image, (b) Histogram of plain image, (c) Bird image by the encryption system, (d) Histogram of Bird image by the encryption system.

6.1. Key Space Analysis [41]:

A decent encryption algorithm ought to have enormous key space to forestall brute-force attacks which is defined to exhaust all the potential keys until the right one. In the studied strategy we increase the space key by using Clifford system and logistic map. So, the quantity of parameters in the Clifford system is six parameters. Therefore, the size of the key space for the studied system is bigger than Clifford system.

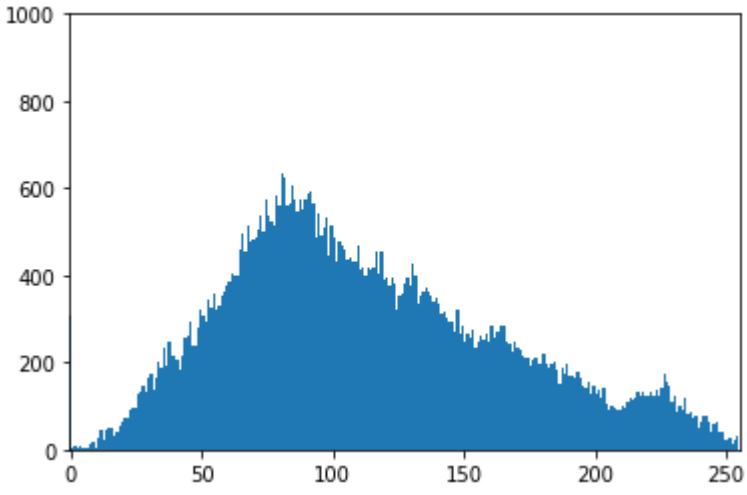
More specifically, this process aims at identifying the key which is used for encryption by means of evolutionary algorithms. Good encryption scheme should have to be resistant opposed to brute-force attack, also the key space must be too large. The total precision of a combinations of one parameter is $10^{16}$and it corresponds approximately to 253 size key space.

More than six attractor parameters are used in the studied scheme; hence the key space is enlarged to more than Clifford system (2^{318}). Also, the key space of studied scheme is large enough to make the classical brute-force attack infeasible.

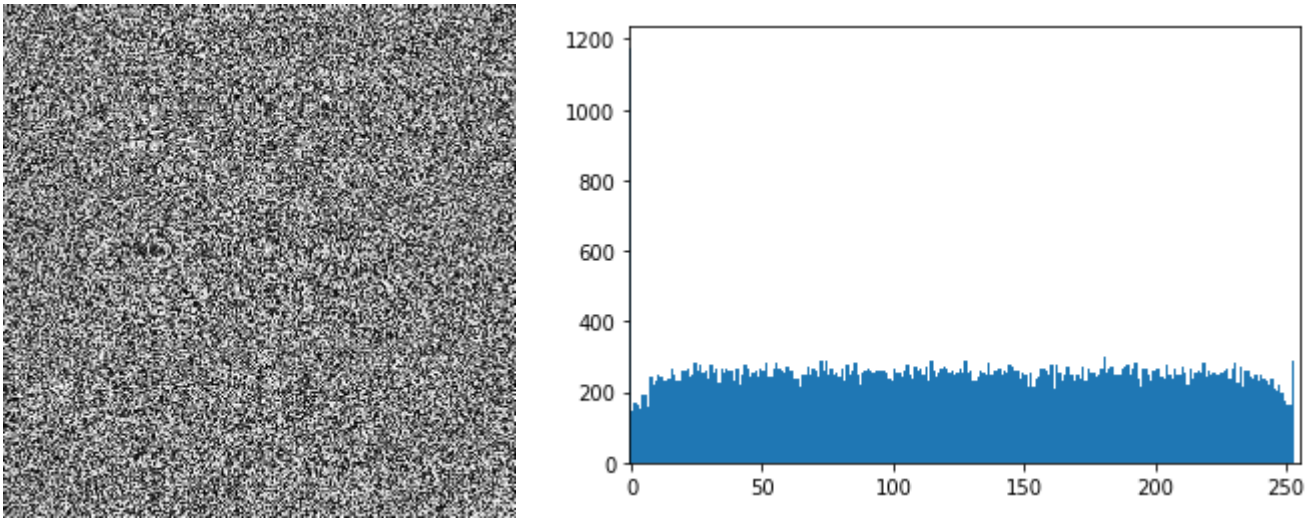
6.2. Encryption and Histogram Test:

Some experimental results are given in this section to demonstrate the efficiency of our scheme. The plain images are “Bird” and “Bridge” with the size 256×256. Their cipher images are shown in Figure 3.8.(c) and Figure 3.9(c). The histogram of the cipher images is shown in Figure 3.8.(d) and Figure 3.9.(d). As we can see, the pixel distribution of the cipher images is fairly uniform, which can greatly reduce the correlation between the pixel values. Both kinds of pictures show that the picture is really well encrypted.

(a)



(b)



(a) **(b)**

Figure 3.9: (a) Plain Bird image, (b) Histogram of plain image, (c) Bridge image by studied encryption system, (d) Histogram of Bridge image by studied encryption system.

7. Experimental results :

7.1. Development environment:

The application was created from a HP DESKTOP-LUAA09K PC:

- Memory: 8192 MB RAM
- Processor: Intel(R) Core (TM) i3-4005U CPU @ 1.70GHz, 1701 MHz, 2 Core(s), 4 Logical Processor(s)
- Operating system: Windows 10 Pro 64 bits

7.2. Programming language: [44][45]

We have chosen the python language to develop our system. This choice of language is motivated by the following reasons:

- ✓ Python is a multi-paradigm programming language.
- ✓ Object-oriented programming and structured programming.
- ✓ Ease of coding: “Code as plain English” is Python’s primary goal. This allows programmers to focus on the design and not on coding. This is perfect for those who are just getting started with machine learning or basic programming. This advantage is very beneficial, especially when faced with complex scenarios.
- ✓ Python is free, unlike MATLAB, which also specializes in data analysis, exploration, visualization, etc. Needless to say, for Python, all you need is a computer, and you are good to go.

- ✓ Python becomes an apt choice for such Image processing tasks. This is due to the commonly used Python libraries for Image manipulation tasks. For example**:**
  _Numpy is one of the core libraries in Python programming, by using basic NumPy operations, such as slicing, masking and fancy indexing, we can modify the pixel values of an image.
  _PIL/PILLOW (Python Imaging Library) is a free library for the Python programming language that adds support for opening, manipulating, and saving many different image file formats...
- ✓ Using OpenCV libraries in Python for image processing functions is faster when compared to MATLAB.

We used the Pycharm IDE programming environment. And used the QTDesigner environment for the creation of the graphical interface. Libraries used:

- ➢ PyQt5
- ➢ PySide
- ➢ Matplotlib
- ➢ Tkinter
- ➢ Numpy
- ➢ Pip-20.2.2

7.3. The interfaces of the developed software:

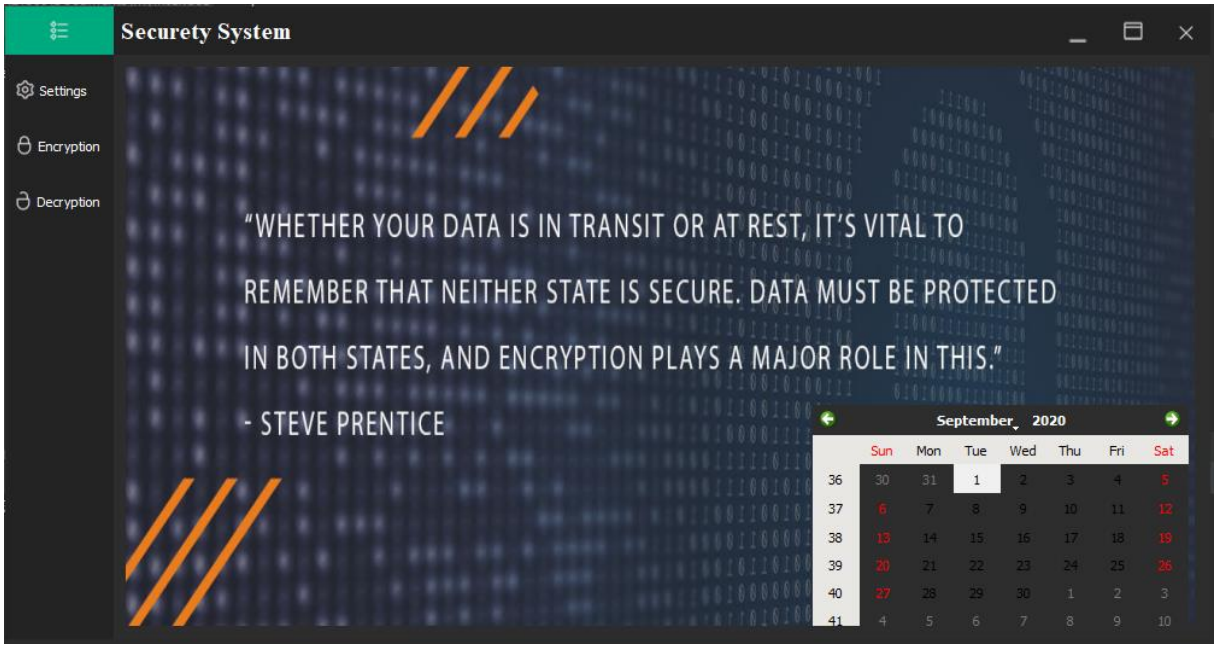


Figure 3.10: Home Page.

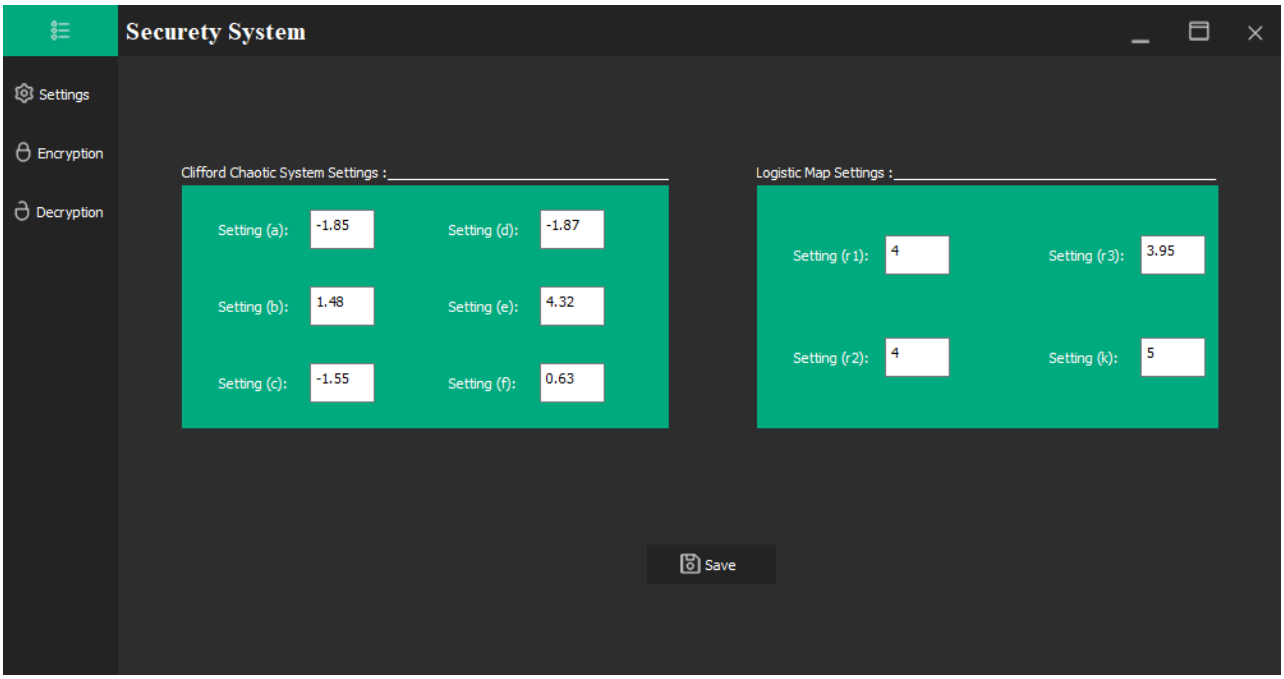


Figure 3.11: Settings Page.

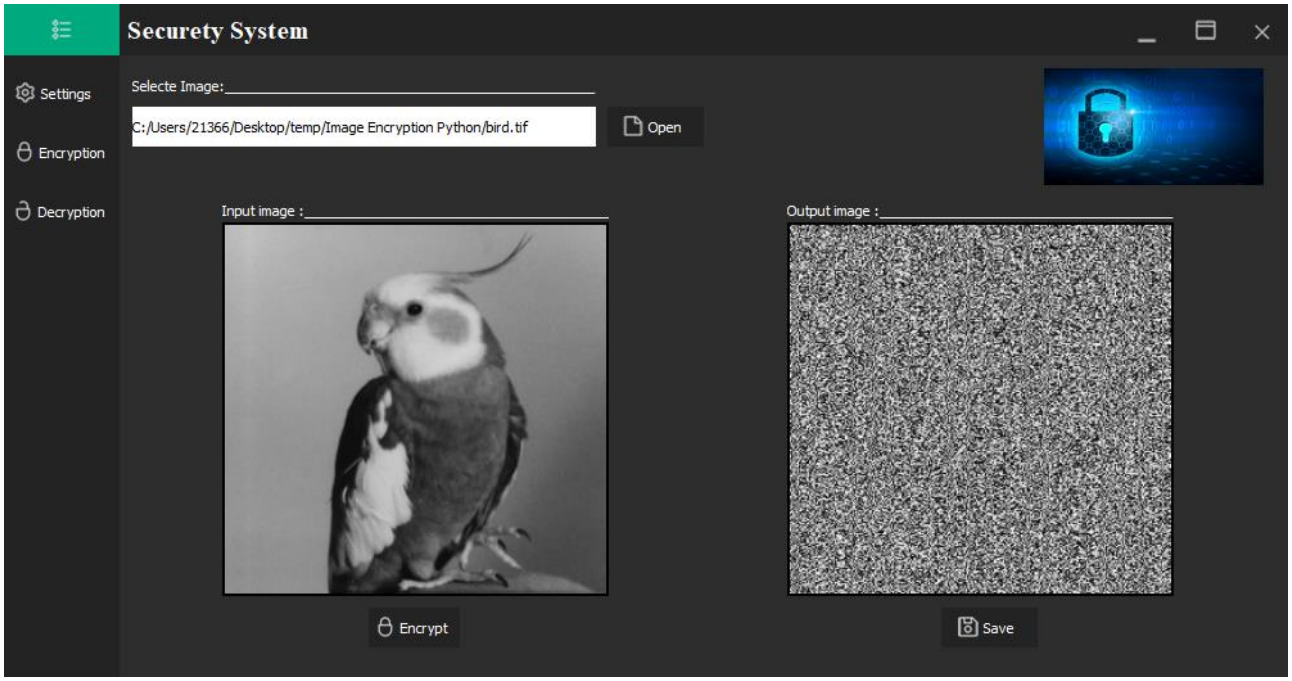


Figure 3.12: Encryption Page.

8. Conclusion :

we have studied in this chapter an image encryption scheme based on the Clifford attractor and the logistic map, Usage of image encryption is in two steps: the initial step is image scrambling that the situation of the pixels in the image is changed and the subsequent step is pixel replacement. Experimental results have indicated that the studied image encryption system has a large key space and a significant level security. Along these lines the examination demonstrates the safety, and the adequacy. Also, the comparisons with existing image encryption schemes that have been made, show that the studied calculation offers truly good results.

GENERAL CONCLUSION

GENERAL CONCLUSION

For the time being, digital images are increasingly being used, leading to an increased transmission of this type of data between networks in general and the Internet in particular, and the confidentiality of this type of data has become essential.

During this paper, we studied an image encryption algorithm based on Clifford attractor and logistic map. The main purpose of this encryption is the combining of properties and benefits between them.

The experimental results clearly show, that the studied algorithm has a high level of confusion. And so, the key space is large enough, which makes a brute force attack unfeasible. Therefore, the encrypted image histogram is very uniform after encryption, or even, the attacker cannot extract the information from the histogram of the encrypted image. Therefore, Behrouz's algorithm shows the efficiency and security of this system.

BIBLIOGRAPHY

[01] Floriane Anstett, ‘’Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse’’, Centre de Recherche en Automatique de Nancy (CRAN), 2006.
[02] Pierre-Louis Cayrel, ‘Chiffrement par blocs’, Université de limoges, France.
[03] R. Dumont. Cryptographie et Sécurité informatique, Université de liége faculté des sciences appliquées 2007, https://www.ulg.ac.be.
[04] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.
[05] Dr N. Chikouche, chiffrement symétrique, support de cours du module Sécurité informatique, Département d'informatique, université de Msila, Année 2016/2017.
[06] R. Dumont. Le chiffrement par blocs. Montefiore Institute ULg.
http://http//www.montefiore.ulg.ac.be/
[07] Yicong Zhou n, LongBao,C.L.PhilipChen Department ofComputerandInformationScience,UniversityofMacau,Macau999078,China
https://www.sciencedirect.com/science/article/abs/pii/S0165168413004258?via%3Dihub
[08] L. Grazide, L'image électronique,
http://auch2.free.fr/Documents/Informatique/Image_electronique.pdf, consulted on18-04-2018.
[09] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition, Pearson Prentice Hall, Upper Saddle River, 2007.
[10] Numeriksciences, http://numeriksciences.fr/, consulted on 18-04-2018
[11] https://www.sites.univ-rennes2.fr/arts-spectacle/cian/image_numFlash/pdf/chap3_tout.pdf
[12] Techopedia https://www.techopedia.com/definition/24012/pixel, consulted on July 26, 2016
[13] https://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/la-definition-pour-une-image/
[14]
https://guides.lib.umich.edu/c.php?g=282942&p=1885350#:~:text=What%20is%20Resolution%3F-,Resolution,high%2Dquality%2C%20crisp%20image
[15] R. Isdant. Traitement numérique de l'image.2009
[16] Image Processing : Lecture 2 ,
https://www.academia.edu/37315655/Types_of_Digital_Images
[17] Léon Robichaud, L'image numérique Pixels et couleurs, Département d'histoire, Université de Sherbrooke
[18] University of Michigan Library, All About Images,
https://guides.lib.umich.edu/allaboutimages, Last Updated: Feb 26, 2020 12:17 PM.
[19] A few scanning tips, by Wayne Fulton, https://www.scantips.com/
[20] Yue, W., Yicong, Z., & Joseph, P. (2014). Design of image cipher using Latin squares. *Information Sciences*, *264*,317-339.
[21] Wang, X., & Lie, Y. (2012). A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. *Optics Communications, 282,* 4033-4042.
[22] Fu, C., Lin, B., Miao, Y., Liu, X., & Chen, J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics Commun, 284,* 5415–5423.
[23] Wu, Y., Noonan, J. P., & Agaian, S. (2011). Shannon entropy based randomness measurement and test for image encryption. *Information Sciences,* 1-23.
[24] Guan, Z. H., Huang, F. J., & Guan, W. J. (2005). Chaos-based image encryption algorithm. *Physics Letters A, 346*,153-157.
[25] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation,” *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.View at: Publisher Site | Google Scholar
[26] C. Fu, J.-J. Chen, H. Zou, W.-H. Meng, Y.-F. Zhan, and Y.-W. Yu, “A chaos-based

digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.View at: Publisher Site | Google Scholar
[27] K. W. Wong, S. H. Kwok, and C. H. Yuen, "An efficient diffusion approach for chaos-based image encryption," *Chaos Solitons & Fractals*, vol. 41, no. 5, pp. 2652–2663, 2009.View at: Publisher Site | Google Scholar
[28] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.View at: Publisher Site | Google Scholar
[29] Xuncai Zhang" Image Encryption Algorithm Based on the H-Fractal and Dynamic Self-Invertible Matrix" https://doi.org/10.1155/2019/9524080 School of Electrics and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China.
[30] *"The Definitive Glossary of Higher Mathematical Jargon — Chaos". Math Vault. 2019-08-01. Retrieved 2019-11-24.*
[31] *"chaos theory | Definition & Facts". Encyclopedia Britannica. Retrieved 2019-11-24.*
[32]Akhavan, A.; Samsudin, A.; Akhshani, A. (2011-10-01). "A symmetric image encryption scheme based on combination of nonlinear chaotic maps". *Journal of the Franklin Institute*. **348** (8): 1797–1813. doi:10.1016/j.jfranklin.2011.05.001
[33] Wang, Xingyuan; Zhao, Jianfeng (2012). "An improved key agreement protocol based on chaos". *Commun. Nonlinear Sci. Numer. Simul*. 15 (12): 4052–4057. Bibcode:2010CNSNS..15.4052W. doi:10.1016/j.cnsns.2010.02.014
[34] *Wolfram|Alpha.*https://www.wolframalpha.com/input/?i=logistic+equation
[35] Weisstein, Eric W. "Logistic Map." From *MathWorld*--A Wolfram Web Resource. https://mathworld.wolfram.com/LogisticMap.html
[36] Computers & Electrical EngineeringVolume 54, August 2016, Pages 471-483. https://doi.org/10.1016/j.compeleceng.2015.11.008
[37] Sprott, J.C. Chaos and Time-Series Analysis, Oxford University Press, 2003, ISBN 978-0-19-850840-3.
[38] International Journal of Future Generation Communication and Networking Vol. 2, No. 3, September, 2009. https://www.researchgate.net/publication/265038721_Improving_Chaos_Image_Encryption_Speed .
[39] Giesl, J., & Vlcek, K. (2009). Image encryption based on strange attractors. *ICGST-GVIP Journal, 9(2),* 19-26**.**
[40] Image Encryption Based on Permutation and Substitution Using Clifford Chaotic System and Logistic Map. Behrouz Fathi-Vajargah, Mohadeseh Kanafchian, Vassil Alexandrov.

[41] Evolutionary Algorithms and Chaotic Systems edited by Ivan Zelinka, Sergej Celikovský, Hendrik Richter, Guanrong Chen

[42] A. Beloucif, Contribution à l'étude des mécanismes cryptographiques, thése En vue de l'obtention du diplôme de Doctorat en Informatique, Université de Batna2, 2016.

[43] Utiliser l'histogramme. PhotoFiltre Studio, http://www.photofiltrestudio.com/doc/histogramme.htm
[44] 10 Python image manipulation tools. https://towardsdatascience.com/image-manipulation-tools-for-python
[45](WIKIPEDIA)https://en.wikipedia.org/wiki/Python_(programming_language)#Features_and_philosophy

ملخص

مع التقدم السريع في استخدام الصور الرقمية في العديد من التطبيقات، من المهم حماية بيانات الصورة السرية من الوصول غير المصرح به. في هذا العمل المخصص لمذكرة نهاية الدراسة، قدمنا خوارزمية تشفير التي يمكن تطبيقها على الصور الرمادية، والتي تعتمد على الدمج بين خوارزميتين ، الخوارزمية الاولى تعتمد على الخريطة اللوجستية الفوضوية والخوارزمية الثانية تعتمد على نظام كليفورد الفوضوي. التحاليل أجريت على هذه الخوارزمية المقدمة لتشفير الصور تبين أنها توفر أداءا تنافسيا للغاية.

الكلمات المفتاحية : الصور الرقمية ، الصورة السرية ، تشفير، خريطة لوجستية فوضوية ، نظام كليفورد.

Abstract

With the rapid advancement in the use of digital images in many applications, it is important to protect confidential photo data from unauthorized access. In this work devoted to the graduation thesis, we have presented an encryption algorithm that can be applied to gray images, and that depends on the combination of two algorithms, the first algorithm is based on a chaotic logistic map, the second algorithm is based on Clifford chaotic system. Analyzes of this presented image encryption algorithm show that it offers a very competitive performance.

Key words: digital images, confidential image, encryption, chaotic logistics map, Clifford System.

Résumé

Compte tenu de l’évolution rapide de l’utilisation des images numériques dans de nombreuses applications, il est important de protéger les données photographiques confidentielles contre tout accès non autorisé. Dans ce travail consacré à la mémoire de fin d'études, nous avons présenté un algorithme de chiffrement qui peut être appliqué aux images grises, et qui dépend de la combinaison de deux algorithmes, le premier algorithme est basé sur une carte logistique chaotique, le second algorithme est basé sur le système chaotique de Clifford. Les analyses de cet algorithme de chiffrement d’image présenté montrent qu’il offre une performance très compétitive.

Mots clés : images numériques, image confidentielle, cryptage, carte logistique chaotique, Clifford System.