LGERIENNE 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

Memoire

Présenté pour obtenir

LE DIPLOME DE LICENCE

Filière: **Electronique**

Spécialité**: Industrie Electronique**

Par :

Khemidja Salah Eddine

Guendouz Abdelouahab

Badaoui Abderraouf

Intitulé

Etude des suites chaotiques et leurs applications en cryptage d'images

Par la commission d'évaluation composée de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M. Daachi	*MCA*	*Président*	*Univ-BBA*
T. Bekkouche	*MCA*	*Encadreur*	*Univ-BBA*
A. Latoui	*MCA*	*Examinateur*	*Univ-BBA*

Année Universitaire 2020/2021

Table des matières.

Table des matières

Table des matières.

Table des matières

Table des matières

Liste des figures

Liste des figures

Liste de tableau

Introduction Générale

Suite au développement rapide des technologies de l'information, les documents multimédias sont devenus un élément central dans les différents domaines d'application. En effet, ils sont des outils de travail essentiel en biomédical [1], en imagerie satellitaire et astronomique, en production cinématographique, ou encore en informatique industrielle.

Ce développement phénoménal ne s'est pas fait à entraîner des inquiétudes de manipulations illicites puisque n'importe quelle personne peut facilement copier, modifier et distribuer les images numériques sans risque de les détériorer. Ces manipulations illicites sont un problème majeur pour la sécurité d'un système, quel qu'il soit : l'état, une entreprise ou un particulier. D'où, l'importance de protéger ces documents multimédias contre un accès ou une distribution non autorisée.

C'est pour répondre à ce problème qu'a été inventée la cryptographie visuelle. Elle est une branche de la cryptographie qui consiste à transformer une image en d'autres images cryptées n'ayant aucune ressemblance ou corrélation avec l'originale.

Depuis quelques années, le domaine de cryptage d'images connaît un extraordinaire développement et plusieurs techniques ont vu le jour, mais chacune ne peut pas garantir de ne pas avoir de faiblesses ou qu'elle est insensible aux méthodes d'attaque.

La meilleure méthode utilisée dans les temps anciens est la méthode du court Jules, l'un des tsars romains. Dans notre ère actuelle, la nécessité d'utiliser ce «cryptage» scientifique est devenue urgente, car le monde est connecté les uns aux autres via des réseaux ouverts. Alors que ces réseaux sont utilisés pour transférer des informations par voie électronique, que ce soit entre des gens ordinaires ou entre des organisations privées et publiques, qu'elles soient militaires ou civiles [3]. Il doit y avoir des moyens de préserver la confidentialité des informations. De grands efforts ont été déployés dans le monde entier pour trouver des moyens optimaux d'échanger des données alors que ces données ne peuvent pas être révélées.

CHAPITRE 01

INITIATION AUX IMAGES NUMÉRIQUES ET CONCEPTS PRÉLIMINAIRES SUR LA CRYPTOGRAPHIE

1.1 Introduction

En raison de l'importance des images numériques et de la valeur des informations qu'elles contiennent, dans ce chapitre, nous allons référer aux concepts de base de l'imagerie à travers les types des images numériques. Ensuite, nous allons parler des méthodes de codage des couleurs dans les images.

La sécurité informatique est devenue une préoccupation majeure pour tous ceux qui sont intéressés par l'informatique et à cette fin la plupart des développeurs se concentrent sur les techniques de cryptage pour fournir de bons résultats. Dans ce chapitre, nous allons parler sur les bases et les principes de sécurité informatique, la cryptographie et des domaines de convergence entre eux. Ensuite, nous allons discuter les classifications des algorithmes de cryptage en détail avec les types et la présentation des différences entre eux. Puis nous allons parler sur les types des méthodes pour crypter les images, et que nous allons détailler les différents critères pour mesurer l'efficacité des algorithmes de cryptage d'image. Enfin nous allons voir les méthodes modernes pour crypter les images illustrant ces points forts.

1.2. Notions de base sur l'imagerie

1.2.1. L'image numérique

Une image numérique est une mosaïque de points unicolores (pixels) [1], et peut être définie comme une fonction bidimensionnelle, f (x, y), où x et y sont des coordonnées spatiales (plan) pour chaque pixel [2], Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [3].

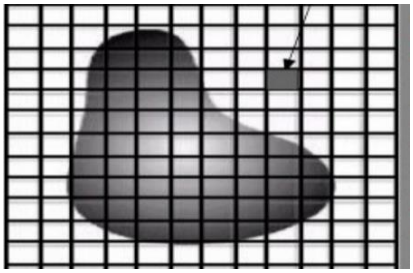


Figure 1.1 : Image numérique [4].

1.2.2. Pixel

Les composants élémentaires d'image sont des points appelés pixels (abréviation de Picture élément) pour former une image. Le pixel représente ainsi le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image [5], et chaque pixel à sa propre couleur (valeur)

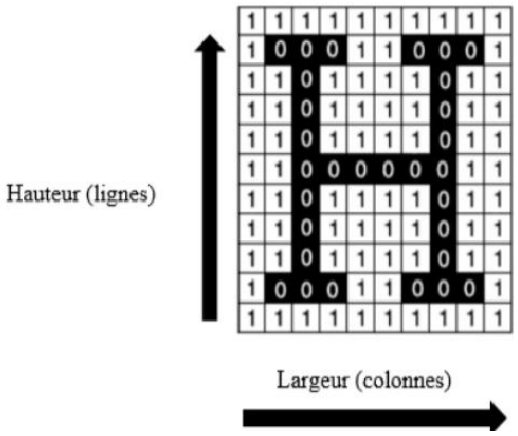


Figure 1.2 : Distribution des pixels par lignes et colonnes [6].

1.2.3. Définition

La définition est le nombre de pixels constituants l'image [3].

1.2.4. La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est «l'octet» [3]. Taille = nombre d'octets pour chaque pixel × définition

1.2.5. Résolution

La résolution d'une image est définie par le nombre de pixels par unité de longueur dpi (dot per inch = point d'encre par pouce) pour une imprimante ou (ppp = pixels par pouce pour un fichier image). Cette résolution dépendra de la qualité de la numérisation.

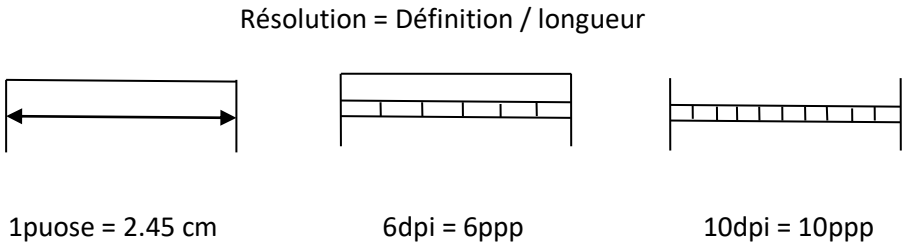


Figure 1.3 : Explication de résolution d'une image [3]

1.3. Les différents types d'image

Il existe deux types d'images numériques :

1.3.1. Matricielle (bitmap)

Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent apparents [6]. Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. Les photos numériques et les images scannées sont de ce type [7].

1.3.2. Vectorielle

Formée de lignes calculées de manière géométrique. Lors d'un zoom avant ou arrière, la forme est recalculée en fonction de notre position sans perdre de qualité [6]. Le processeur est chargé de "traduire" ces formes en informations interprétables par la carte graphique (images Word, Publisher, Corel Draw - format WMF, CGM, etc.)

Les avantages d'une image vectorielle : les fichiers qui la composent sont petits, les redimensionnements sont faciles sans perte de qualité.

Les inconvénients : une image vectorielle ne permet de représenter que des formes simples.

Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes [7].

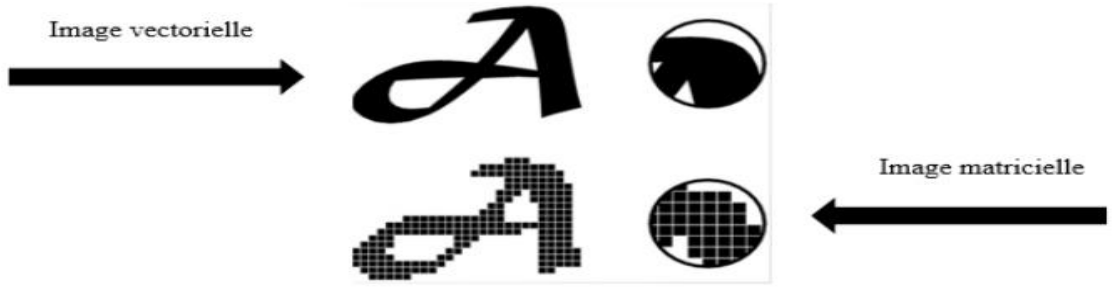


Figure 1.4 : Différence entre image vectorielle et image matricielle [6].

1.4. Les différents modes de couleurs des images

1.4.1. Mode binaire

Appelé aussi Mode bitmap (noir et blanc) : Avec ce mode, il est possible d'afficher uniquement des images en deux couleurs pour chaque pixel : noir et blanc. Il utilise une seule couche [5].Codage en 1 bit par pixel (bpp) : 21= 2 possibilités : [0,1].

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure 1.5 : Codage binaire (0,1) [5].

Figure 1.6 : Image codée en binaire [7].

1.4.2. Mode niveau de gris

A chaque pixel codé en n bits est affecté un nombre binaire variant de «0» (pour le noir) à «2^-n-1» (pour le blanc), avec n le nombre de bits pour chaque pixel.

Il y aura alors «2^N» niveaux de gris.

Si le codage se fait en 8 bits par pixel, il y aura : $2^n = 2^8 = 256$ niveaux de gris allant du blanc au noir.

Si le codage se fait en 16 bits par pixel, il y aura : $2^n = 2^{16} = 65536$ niveaux de gris allant du blanc au noir [3].

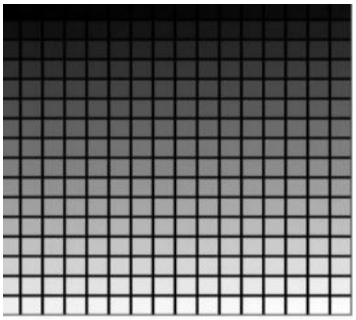


Figure 1.7 : Nuance de 256 gris [5]

Figure 1.8 : Image codée en niveau de gris [5]

1.4.3. Mode couleurs indexées

Permet d'obtenir jusque 256 couleurs fixes, définies à l'avance dans une palette. Il n'utilise qu'une seule couche [5].

Codage en 8 bits par pixel (bpp) : $2^8 = 256$ possibilités.

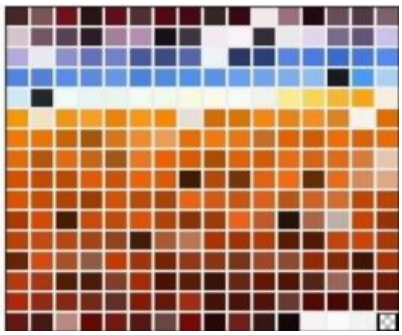


Figure 1.9 : Palette de 256 couleurs utilisées [5].

1.4.4. Les modes colorimétriques RVB / CMJN

Afin de créer des images encore plus riches en couleurs (et donc disposer de plus qu'une palette limitée à 256 couleurs), l'idée de mélanger des couleurs primaires en « couches » est arrivée [5].

Il existe deux systèmes de représentation des couleurs par mélange, selon qu'on les reproduit sur un écran d'ordinateur ou sur support papier via une imprimante :

Figure 1.10 : Les deux modes colorimétriques [5].

1.4.4.1. Mode couleur RVB (lumière éteinte)

Grâce au mélange des 3 couches de couleur (Rouge, Vert, Bleu), il est possible de reproduire un plus grand nombre de nuances qu'avec une palette en mode couleurs indexées [5].

Avec un codage en RVB 8 bits par couche :

Chaque couche utilise 8bits (1 octet), soit 256 nuances possibles : 8 bits pour le Rouge, 8 bit pour le Vert et 8 bits pour le Bleu.

Donc utilisation de $3\ x\ 8\ bits\ =\ 24$ bits Utilisées au total.

$=>\ 256\ x\ 256\ x\ 256\ =\ 2^{24}\ =\ 16{,}7$ Millions possibles !

Avec un codage en RVB 16 bits par couche :

Chaque couche utilise le double, soit 16 bits ! (65535 nuances). $3\ x\ 16\ =\ 48$ Bits utilisées au total.

$=>\ 65535\ x\ 65535\ x\ 65535\ =\ 2^{48}\ =\ 4$ Milliards possibles !

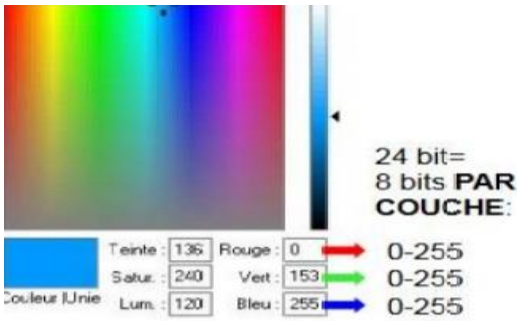


Figure 1.11 : Le mode RVB [5].

1.4.4.2. Mode couleur CMJN (support papier)

Comme les écrans d'ordinateur ne peuvent afficher que du RVB, Photoshop sépare les images CMJN en 4 couches (Cyan, Magenta, Jaune et Noir ou chaque couleur est exprimée en pourcentage) et converti le tout en RVB pour être affiché sur l'écran. Cependant pour L'utilisateur, le fichier possède bien 4 couches distinctes sur lesquels il est possible de travailler [5].

Avec un codage en CMJN 8 bits par couche :

Chaque couche utilise 8 bits (soit 256 nuances possibles) : 8 bits pour le Cyan, 8 bits pour le Magenta, 8 bits pour le Jaune et 8bits pour le Noir.

Donc utilisation de 4 x 8 bits = 32 bits utilisées au total.

$=>\ 256\ x\ 256\ x\ 256\ x\ 256\ =\ 2^{32}\ =$ 4 Milliards possibles !

Avec un codage en CMJN 16 bits par couche :

Chaque couche utilise le double, soit 16 bits ! (65535 nuances). $4\ x\ 16\ =\ 64\ bits$ Utilisées au total.

=> $65535\ x\ 65535\ x\ 65535\ x\ 65535\ =\ 2^{64}$ Possibilités !

1.5. Format d'enregistrement d'une image

Les formats des images ont une relation avec le type d'image lui-même

1.5.1. Les formats matriciels

Nom du format	**Points forts**	**Points faibles**	**Note**
GIF (Graphical Inter change Format)	Possibilité d'animation et de transparence, compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos.
JPEG 2000 Joint Photographic Experts Group	Excellente compression	Compression destructrice	-Spécialement conçu pour les photographies, il est cependant à utiliser avec délicatesse tant sa compression peut brouiller l'image. -Le format JPEG2000, évolution du format original, peut être réglé pour compresser sans pertes. GIF (Graphical Inter change Format)

			Possibilité d'animation et de transparence, compression efficace Limité à 256 couleurs Très
PNG (Portable Network Graphique)	Excellente compression sans perte. Possibilité de transparence. Standard donc pérenne.	Pas très efficace pour les larges photographies	Format destiné à remplacer le format GIF et ses limitations, mais ayant encore du mail à s'implanter dans les habitudes des développeurs. Peut remplacer les JPEG comme les GIF (sauf en ce qui concerne l'animation).
TIFF (Tagged Image File Format)	Compression sans perte efficace. Couche de transparence.	Lourdeur des fichiers non compressés. Format propriétaire.	Format de stockage très utilisé, à éviter pour le Web
BMP (Bitmap)	Format par défaut de window	Disponible uniquement sur la plateforme de Microsoft	Généralement non compressé et de ce fait des fichiers très « lourds »

GIF (Graphical Inter change Format)	Possibilité d'animation et de transparence, compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos.

Table 1.1 : Les formats matriciels [7]

1.5.2 Les formats Vectoriels

Nom du format	**Points forts**	**Points faibles**	**Note**
AI (Adobe Illustrateur)	Reconnu par tous les logiciels graphiques.	Format propriétaire.	Format standard d'Adobe Illustrateur, l'un des plus utilisés du fait de la popularité du logiciel.
PS/EPS (Postscript / Encapsulated Postscript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.
FLA/SWF (Flash)	Très polyvalent, peut utiliser des mp3, des	Format propriétaire et fermé.	C'est le standard de fait des

	JPEG, des vidéos... Très répandu sur le Web.		animations vectorielles sur le Web
PICT (Picture)	Format par défaut de Mac OS, donc encore utilisé.	Disponible uniquement sur la plateforme d'Apple	N'a plus grand intérêt face aux autres formats existants.
PDF (Portable Document Format)	Affiche les documents	Taille prohibitive. Ne peut se lire qu'avec le logiciel Acrobat ou logiciel équivalent	Version simplifiée de PostScript, il a été conçu pour afficher les documents de la même manière quel que soit le système.
SVG (Scalable Vector Graphics)	Format XML donc extensible. Très compressible car format texte. Standard donc pérenne. Permet les animations et la transparence. Peut afficher des images bitmap.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Promis à un grand avenir malgré un démarrage lent, ce format est souvent cité comme capable de rivaliser avec les premières versions de Flash.

Table 1.2 : Les formats vectoriels [7].

1.6 Concepts préliminaires sur la cryptologie

La cryptographie est connue depuis l'Antiquité, lorsqu'elle était utilisée dans les domaines de la guerre et de l'armée. Il a été mentionné que les pharaons ont été les premiers à effectuer le

processus de cryptage de la correspondance entre les secteurs de l'armée. Il a également mentionné que les Arabes ont de vieilles tentatives dans le domaine du cryptage. Les Chinois ont utilisé de nombreuses méthodes de cryptographie et de cryptographie pour transmettre des messages pendant les guerres. Ils avaient l'intention d'utiliser le cryptage pour cacher la vraie forme des messages. Même s'ils tombaient entre les mains de l'ennemi, ils seraient difficiles à comprendre pour lui [8].

Les travaux et recherches dans le domaine de la cryptographie se poursuivent encore en raison du développement rapide des ordinateurs et de la forte croissance des réseaux, en particulier du réseau mondial, Internet

1.7 La cryptographie (Introduction)

La cryptographie est une technique de sécurisation des informations et des communications grâce à l'utilisation de codes afin que seules les personnes à qui les informations sont destinées puissent les comprendre et les traiter. Empêchant ainsi l'accès non autorisé à l'information. Le préfixe « crypt » signifie «caché» et le suffixe graphique signifie «écriture».

En cryptographie, les techniques utilisées pour protéger les informations sont obtenues à partir de concepts mathématiques et d'un ensemble de calculs basés sur des règles appelés algorithmes pour convertir les messages de manière à rendre leur décodage difficile. Ces algorithmes sont utilisés pour la génération de clés cryptographiques, la signature numérique, la vérification pour protéger la confidentialité des données, la navigation Web sur Internet et pour protéger les transactions confidentielles telles que les transactions par carte de crédit et de débit.

Il y a quatre conditions pour réaliser correctement le cryptage

- *Confidentialité*:

Les informations ne sont accessibles que par la personne à laquelle elles sont destinées et aucune autre personne que lui ne peut y accéder.

- *Intégrité*:

Les informations ne peuvent pas être modifiées dans le stockage ou la transition entre l'expéditeur et le destinataire prévu sans qu'aucun ajout aux informations ne soit détecté.

- *Non-répudiation*:

Le créateur / expéditeur d'informations ne peut nier son intention d'envoyer des informations à un stade ultérieur.

- *Authentification*:

Les identités de l'expéditeur et du destinataire sont confirmées. Ainsi que la destination / l'origine des informations est confirmée

1.7.1 Types de cryptographie

En général, il existe trois types de cryptographie:

✓ Cryptographie à clé symétrique:

Il s'agit d'un système de cryptage dans lequel l'expéditeur et le destinataire du message utilisent une seule clé commune pour crypter et décrypter les messages. Les systèmes de clés symétriques sont plus rapides et plus simples, mais le problème est que l'expéditeur et le destinataire doivent d'une manière ou d'une autre échanger la clé de manière sécurisée. Le système de cryptographie à clé symétrique le plus populaire est le système de cryptage de données (DES).

✓ Fonctions de hachage:

Il n'y a aucune utilisation de clé dans cet algorithme. Une valeur de hachage de longueur fixe est calculée selon le texte brut, ce qui rend impossible la récupération du contenu du texte brut. De nombreux systèmes d'exploitation utilisent des fonctions de hachage pour crypter les mots de passe.

✓ Cryptographie à clé asymétrique:

Dans ce système, une paire de clés est utilisée pour crypter et décrypter les informations. Une clé publique est utilisée pour le chiffrement et une clé privée est utilisée pour le déchiffrement. La clé

publique et la clé privée sont différentes. Même si la clé publique est connue de tous, le destinataire ne peut la décoder que parce que lui seul connaît la clé privée

1.8 La cryptanalyse

La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque.

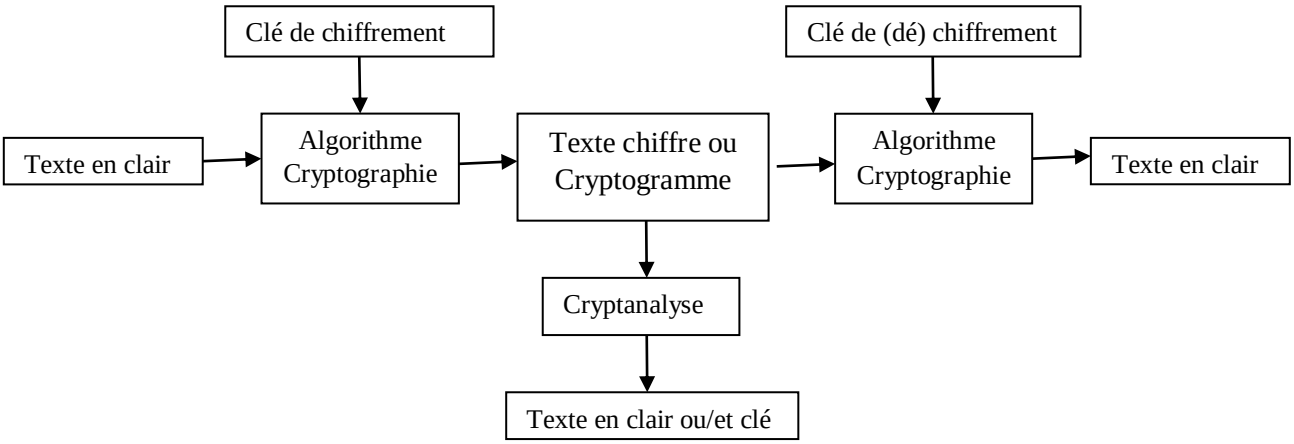


Figure 1.12 : Protocole de chiffrement

- Attaque sur texte chiffré seul (*cipher text - only* en anglais) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.
- Attaque à texte clair connu (*known-plaintext attack* en anglais) : le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
- Attaque à texte clair choisi (*chosen-plaintext attack* en anglais) : le cryptanalyste possède des messages en clair, il peut créer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair chois.

- Attaque à texte chiffré choisi (*chosen-cipher text attack* en anglais) : le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

1.8.1 Familles d'attaques cryptanalytiques

Il existe plusieurs familles d'attaques cryptanalytiques, les plus connues étant l'analyse fréquentielle, la cryptanalyse différentielle et la cryptanalyse linéaire

1.8.1.1 L'analyse fréquentielle

L'analyse fréquentielle, découvert au IX^{e} siècle par Al-Kindi, examine les répétitions des lettres du message chiffré afin de trouver la clé. Elle est inefficace contre les chiffrements modernes tels que DES, RSA. Elle est principalement utilisée contre les chiffrements mono-alphabétiques qui substituent chaque lettre par une autre et qui présentent un biais statistique.

1.8.1.2 L'indice de coïncidence

L'indice de coïncidence, inventé en 1920 par William F. Friedman, permet de calculer la probabilité de répétitions des lettres du message chiffré. Il est souvent couplé avec l'analyse fréquentielle. Cela permet de savoir le type de chiffrement d'un message (chiffrement mono-alphabétique ou poly-alphabétique) ainsi que la longueur probable de la clé.

1.8.1.3 L'attaque par mot probable

L'attaque par mot probable consiste à supposer l'existence d'un mot probable dans le message chiffré. Il est donc possible d'en déduire la clé du message si le mot choisi est correct. Ce type d'attaque a été mené contre la machine Enigma durant la Seconde Guerre mondiale.

1.8.1.4 L'attaque par dictionnaire

L'attaque par dictionnaire consiste à tester tous les mots d'une liste comme mot clé. Elle est souvent couplée à l'attaque par force brute.

1.8.1.5 L'attaque par force brute

L'attaque par force brute consiste à tester toutes les solutions possibles de mots de passe ou de clés. C'est le seul moyen de récupérer la clé dans les algorithmes les plus modernes et encore inviolés comme AES. Il est peu utilisé pour des mots de passe possédant un très grand nombre de caractères car le temps nécessaire devient alors trop important. De même plusieurs brevets rendent cette méthode inefficace, comme celui de Bell ou d'IBM.

1.8.1.6 Attaque par paradoxe des anniversaires

Le paradoxe des anniversaires est un résultat probabiliste qui est utilisé dans les attaques contre les fonctions de hachage. Ce paradoxe permet de donner une borne supérieure de résistance aux collisions d'une telle fonction. Cette limite est de l'ordre de la racine de la taille de la sortie, ce qui signifie que, pour un algorithme comme MD5 (empreinte sur 128 bits), trouver une collision quelconque avec 50% de chance nécessite 2^{64} hachages d'entrées distinctes.

1.9 Type de cryptage

1.9.1 Cryptage conventionnel

Il est également appelé chiffrement symétrique. Il utilise une clé pour le processus de chiffrement et de déchiffrement des données. Ce type de chiffrement dépend de la confidentialité de la clé utilisée. La personne qui possède la clé peut déchiffrer et lire le contenu des messages ou des fichiers. Cela signifie que si quelqu'un veut envoyer un message chiffré à une autre personne il doit trouver un moyen sûr d'envoyer la clé. Si un tiers obtient cette clé, il peut lire tous les messages chiffrés entre les deux personnes. [8]

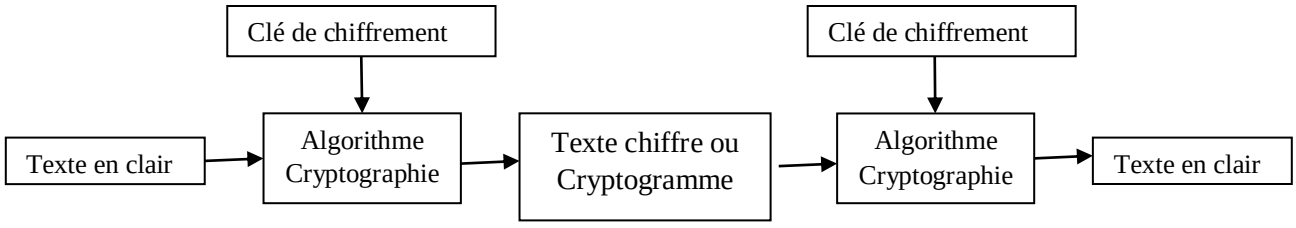


Figure 1.13 : Chiffrement symétrique [11]

1.9.1.1 Systèmes de cryptage conventionnels

1.9.1.1.1César Code

C'est une méthode ancienne inventée par César Jules pour créer des messages cryptés entre les secteurs de l'armée, et elle s'est avérée efficace à son époque. Mais à notre époque moderne et avec le développement des ordinateurs, cette méthode ne peut pas être utilisée pour détecter rapidement le contenu des messages cryptés.

L'exemple suivant illustre le fonctionnement du code César: Si nous encodons le mot "SECRET" et utilisons la valeur clé de 3, nous changeons la position des lettres à partir de la troisième lettre, qui est la lettre "D". Par conséquent, la disposition des lettres sera la suivante:

En conséquence, la disposition des lettres sera la suivante:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Les lettres après avoir utilisé la nouvelle valeur pour eux à partir de la clé "3" sont dans la forme actuelle:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Maintenant la valeur de D à A, B E à, F à C, etc.

De cette manière, le mot "SECRET" sera "VHFUHW". Pour donner à n'importe qui d'autre la possibilité de lire votre message crypté; Vous devriez lui envoyer la valeur clé.

1.9.1.1.2 Data Encryptions Standard (DES)

Ce système a été développé à la fin des années soixante-dix par la National Security Agency des États-Unis, et ce système est devenu faisable pour ne pas l'utiliser avec le développement de systèmes informatiques et l'augmentation de la vitesse de son traitement des données. , car le contenu des messages chiffrés peut être exposé en peu de temps

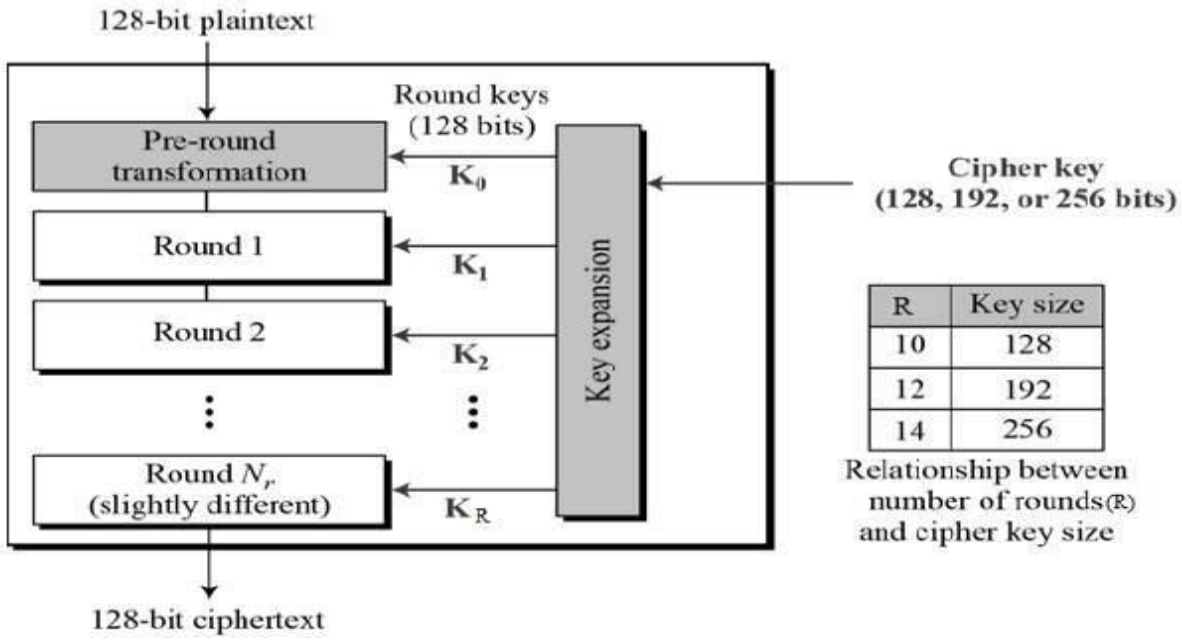
1.9.1.1.3 Advanced Encryption Standard (AES)

La norme de cryptage avancée (AES), également connue sous son nom d'origine Rijndael

(prononciation néerlandaise: [9] est une spécification pour le cryptage des données électroniques établie par le National Institute of Standards and Technology (NIST) des États-Unis en 2001.[12]

AES est un chiffrement itératif plutôt que feistel. Il est basé sur un «réseau de substitution-permutation». Il comprend une série d'opérations liées, dont certaines impliquent le remplacement des entrées par des sorties spécifiques (substitutions) et d'autres impliquent le brassage de bits (permutations).

Fait intéressant, AES effectue tous ses calculs sur des octets plutôt que sur des bits. Par conséquent, AES traite les 128 bits d'un bloc de texte en clair comme 16 octets. Ces 16 octets sont disposés en quatre colonnes et quatre lignes pour être traités comme une matrice Contrairement à DES, le nombre de tours dans AES est variable et dépend de la longueur de la clé. AES utilise 10 tours pour les clés de 128 bits, 12 tours pour les clés de 192 bits et 14 tours pour les clés de 256 bits. Chacun de ces tours utilise une clé ronde de 128 bits différente, qui est calculée à partir de la clé AES d'origine.



R	Key size
10	128
12	192
14	256

Figure 1.14 Une illustration de la structure du système Advanced Encryption Standard

1.9.2 Chiffrement à clé publique (Chiffrement asymétrique)

Le cryptage à clé publique est un type de cryptage dans lequel l'utilisateur dispose d'une paire de clés de cryptage, la clé déclarée et la clé secrète [13] [14] [15]. La clé secrète reste un secret. Quant à la clé déclarée, elle peut être distribuée à tout le monde. Les deux touches sont liées à une opération mathématique spécifique (elle varie selon l'algorithme utilisé), cependant, il n'est pas possible d'accéder à l'une des touches par l'autre. L'avantage de ce système est que lorsqu'un message est chiffré avec la clé déclarée, il ne peut être déchiffré qu'au moyen de la clé secrète correspondante.

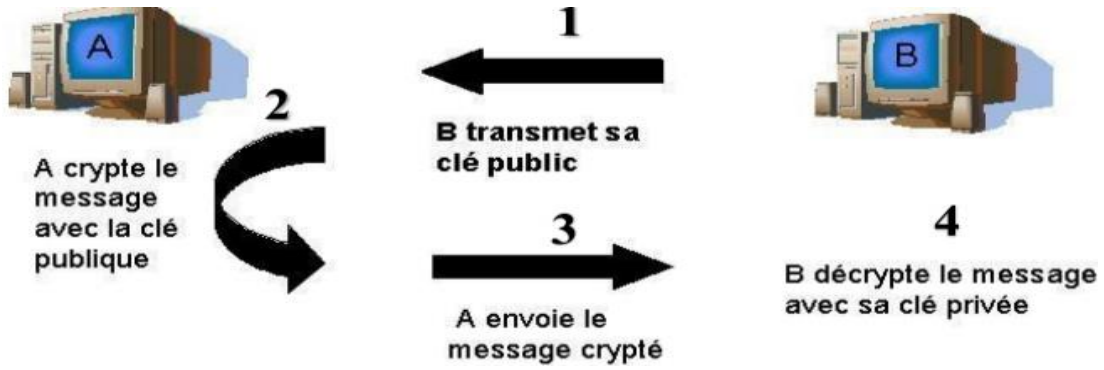


Figure 1.15 : Chiffrement asymétrique [10].

1.9.2.1 Le chiffrement RSA

RSA (Rivest – Shamir – Adleman) est un système de cryptage à clé publique largement utilisé pour la transmission de données sécurisée. C'est aussi l'un des plus anciens. L'acronyme RSA vient des noms de famille de Ron Rivest, Adi Shamir et Leonard Adleman, qui ont décrit publiquement l'algorithme en 1977. Un système équivalent a été développé secrètement, en 1973 au GCHQ (l'agence britannique de renseignement électromagnétique), par le mathématicien anglais Clifford Cocks. Ce système a été déclassifié en 1997 [19].

Dans un système de chiffrement à clé publique, la clé de chiffrement est publique et distincte de la clé de déchiffrement, qui est gardée secrète (privée). Un utilisateur RSA crée et publie une clé publique basée sur deux grands nombres premiers, avec une valeur auxiliaire. Les nombres

premiers sont gardés secrets. Les messages peuvent être cryptés par n'importe qui, via la clé publique, mais ne peuvent être décodés que par quelqu'un qui connaît les nombres premiers [9].La sécurité de RSA repose sur la difficulté pratique de factoriser le produit de deux grands nombres premiers, le «problème d'affacturage». La rupture du cryptage RSA est connue sous le nom de problème RSA. La question de savoir si c'est aussi difficile que le problème d'affacturage est une question ouverte. [21] Il n'existe aucune méthode publiée pour annuler le système si une clé suffisamment grande est utilisée.

RSA est un algorithme relativement lent. Pour cette raison, il n'est pas couramment utilisé pour crypter directement les données des utilisateurs. Plus souvent, RSA est utilisé pour transmettre des clés partagées pour la cryptographie à clé symétrique, qui sont ensuite utilisées pour le cryptage-décryptage en masse

1.9.2.2 Chiffrement SSL

Transport Layer Security (TLS), le successeur du désormais obsolète Secure Sockets Layer (SSL), est un protocole cryptographique conçu pour assurer la sécurité des communications sur un réseau informatique. Plusieurs versions du protocole sont largement utilisées dans des applications telles que le courrier électronique, la messagerie instantanée et la voix sur IP, mais son utilisation en tant que couche de sécurité dans HTTPS reste la plus visible publiquement. Le protocole TLS vise principalement à assurer la confidentialité et l'intégrité des données entre deux ou plusieurs applications informatiques communicantes. Il s'exécute dans la couche application d'Internet et est lui-même composé de deux couches: l'enregistrement TLS et les protocoles de prise de contact TLS.

TLS est une proposition de norme IETF (Internet Engineering Task Force), définie pour la première fois en 1999, et la version actuelle est TLS 1.3 définie en août 2018. TLS s'appuie sur les spécifications SSL antérieures (1994, 1995, 1996) développées par Netscape Communications pour l'ajout le protocole HTTPS à leur navigateur Web Navigator

1.10- Vocabulaire de base

Chiffrement : transformation à l'aide d'une clé de chiffrement d'un message intelligible appelé texte clair ou libellé en un message incompréhensible ou inintelligible appelé texte chiffré ou cryptogramme si on ne dispose pas d'une clé de déchiffrement (en anglais encryption) ; En cryptographie, le chiffrement, parfois appelé à tort cryptage.[24]

Déchiffrement: c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair. [25]

Chiffre : utilisation de la substitution au niveau des lettres ; anciennement code secret, par extension l'algorithme utilisé pour le chiffrement ; [25]

Code : utilisation de la substitution au niveau des mots ou phrases pour coder ;

Coder : utilisation d'un code sur un texte ; [24].

Cryptogramme : message chiffré ; Le destinataire légitime doit pouvoir déchiffrer le cryptogramme et obtenir le texte clair; [25]

Cryptosystème : un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles. [24].

Décrypter : retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux « cassent » des codes secrets), ceci est effectué par un espion (cryptanaliseur, décrypteur ou oreille indiscrète).; [25]

Cryptanalyse : science analysant les cryptogrammes en vue de les décrypter. [24].

Clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations[26].

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair [25].

Confusion : La confusion correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible [26].

1.11 Permutation (transposition)

Chiffrement par permutation (Un chiffrement par transposition) est un chiffrement qui consiste à changer l'ordre des lettres, le chiffrement par transposition demande de découper le texte clair en blocs de taille identique. La même permutation est alors utilisée sur chacun des blocs [27]

1.12 Méthodes du cryptage des images

Il existe deux grandes différences entre les données textuelles et les images numériques rendant les méthodes de cryptage de texte pour la plupart des cas inapplicable au cryptage des images : La différence principale réside dans la taille, en effet la quantité d'informations contenues dans l'image est beaucoup plus volumineuse que celles contenues dans les données textuelles. La deuxième différence concerne la perte de données, lorsqu'une technique de compression est appliquée.

Contrairement aux images, l'utilisation d'une méthode de compression avec perte est totalement interdite lors du chiffrement d'un texte, par conséquent, les chercheurs ont étudié plusieurs méthodes de chiffrement d'image avec/sans perte [16]. D'autre part, les algorithmes de chiffrement des images peuvent être classés selon le domaine d'application comme suit :

1.12.1 Méthodes dans le domaine spatial

Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'image lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles. Les pixels de l'image peuvent être reconstruits (récupérés) complètement par un processus inverse sans aucune perte d'information.

Les algorithmes de cryptage d'image dans le domaine spatial existants peuvent être classés en deux catégories :

- Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels.

- Dans la deuxième catégorie, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits [16].

1.12.2 Méthodes dans le domaine fréquentiel

Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause généralement une perte d'information [16].

1.13 Outils élémentaires d'analyse d'un algorithme du cryptage d'image

(Mesures de Performance)

1.13.1. Espace de clés

La taille de l'espace de clé est le nombre de paires de clés de cryptage/décryptage qui sont disponibles dans le système de chiffrement [17]. Une condition nécessaire, mais pas suffisante à un schéma de cryptage pour qu'il soit sûr est que l'espace clés soit suffisamment grand pour assurer la sécurité contre l'attaque par force brute [16].

1.13.2 Analyse statistique

1.13.2.1 L'histogramme

L'histogramme d'une image désigne un histogramme des valeurs d'intensité des pixels. Cet histogramme est un graphique illustrant le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image grise il y a 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris [18]. Dans un contexte de chiffrement

d'image, l'histogramme de l'image chiffrée doit être uniforme pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme [16].

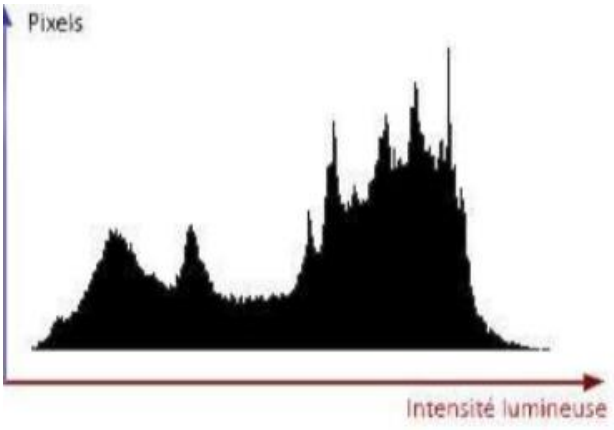


Figure 1.16: Histogramme d'une image niveau de gris [19].

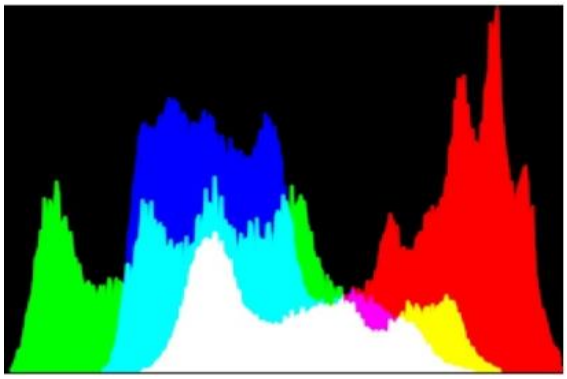


Figure 1.17: Histogramme d'une image couleur [20].

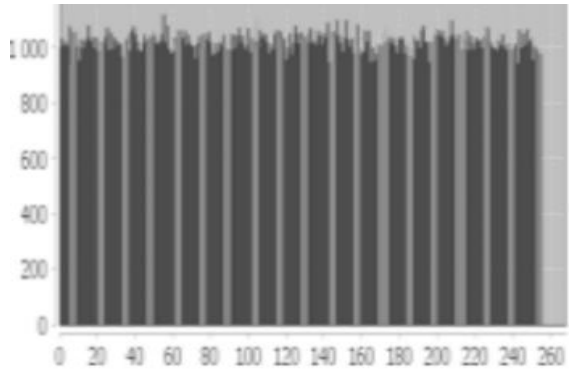


Figure 1.18 : Histogramme d'une image chiffrée [21].

1.13.2.2 La corrélation entre les pixels adjacents

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence. Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique [16], et

les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes : $r = (x)/\sqrt{D(x)}\sqrt{D(y)}$

1.13.2.3 L'entropie

Selon la théorie de Shannon [22], l'entropie d'une information est la quantité d'information englobée ou libérée par une source d'information. En particulier, plus la source est redondante, moins elle contient d'information [23]. En absence de contraintes particulières, l'entropie est maximale pour une source dont tous les symboles sont équiprobables. Ainsi, elle est l'une des principales mesures de l'aléatoire de l'information. Les valeurs de l'entropie élevée manifestent un haut degré de caractère aléatoire, et pour tout message codé sur M bits, la limite supérieure de l'entropie est M. La formule utilisée pour calculer l'entropie d'une source m est comme suit [16]

$$h\,(m) = -\sum pilog\ 2\ (pi)\ intervalle\ [2^n - 1, i = 0] \qquad (2.5)$$

Où pi définit la probabilité d'un pixel et n est le nombre de bits dans chaque pixel. Donc pour un chiffrement d'images au niveau de gris, La valeur de l'entropie doit être très proche de 8.

1.13.3 Analyse de sensitivité

1.13.3.1 Attaques différentielles

Afin de détecter la relation entre l'image originale et l'image cryptée, un adversaire fait un petit changement sur l'image claire, ensuite utilise l'algorithme de cryptage pour crypter l'image avant et après le changement, dans le but de tester comment une petite modification dans l'image originale affecte l'image cryptée. Ce genre d'attaque est appelé attaque différentiel.

Pour assurer la sécurité d'un schéma de cryptage d'image contre l'analyse différentielle, deux mesures quantitatives sont utilisés : le NPCR (Number of Pixels Change Rate) et l'UACI (Unified Average Changing Intensity).

Le NPCR représente le taux de pixels différents entre les deux images chiffrées, tandis que l'UACI représente la différence de l'intensité moyenne. La formule utilisée pour calculer ces deux pourcentages est définie comme suit :

$$NPCR = \sum i,(i,)\ /W \times H \times 100\% \quad (2.6)$$

$$UACI = 1/w \times H\ [\sum (i,)\ i,* |C1(i,j) - C2(i,j)|/255\ ] \times 100\% \quad (2.7)$$

Où W et H représentent la largeur et la hauteur de l'image respectivement. C1(i, j) est l'image cryptée et C2(i, j) est l'image cryptée après avoir changé un pixel de l'image clair. Pour les pixels à la position (i, j), si C1 (i, j) ≠ C2 (i, j), alors f (i, j) = 1 ; sinon f (i, j) = 0. Un NPCR > 99,6094% et un UACI > 33,4635% assure qu'un schéma de chiffrement d'image est sécurisé contre cette attaque [16].

1.13.3.2 Sensitivité de la clé

Un algorithme idéal de chiffrement d'image doit être sensible à la clé. C'est-à-dire le changement d'un seul bit dans la clé secrète devrait produire une image cryptée complètement différente. Pour tester la sensibilité de la clé de chiffrement, nous avons effectué les étapes suivantes [16] :

– Une image originale est chiffrée en utilisant la clé secrète.

– La même image originale est cryptée en faisant une légère modification dans la clé secrète.

– Ensuite, on compare les deux images chiffrées en utilisant les deux mesures NPCR et UACI.

– Ainsi, si les valeurs de l'NPCR et l'UACI obtenues sont supérieurs à 99,6094% et à 33,4635% respectivement : on dit que le schéma est sensible à la clé.

1.14 Conclusion

Dans ce chapitre, nous avons parlé de l'importance des images numériques et de ses types, les méthodes de codage des pixels des images numériques et nous avons parlé des méthodes plus importantes et la plus récentes pour crypter les images numériques.

Chapitre 02

Les Systèmes dynamiques chaotiques

2.1 Introduction

Depuis fort long temps, la science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos, qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines. [28]

N'ayant pas de définition au sens universel, le chaos est décrit comme étant un cas particulier d'un système non linéaire déterministe, caractérisé par son comportement très sensible aux conditions initiales et bien qu'il soit déterministe, il est imprédictible à long terme, et présente un aspect aléatoire, sans pour autant faire partie des phénomènes aléatoires.

Dans ce chapitre, nous nous intéressons aux systèmes dynamiques chaotiques en spécifiant leurs caractéristiques tout en présentant les méthodes permettant de l'identifier. [29]

2.2 Systèmes dynamiques

2.2.1 Définition

Globalement, un système dynamique, décrit des phénomènes qui évoluent au cours du temps, dont le terme « système » fait référence à un ensemble de variables d'état. [30]

2.2.2 Représentation mathématique

- **En temps Continu**

Un système dynamique, dans le cas continu est régi par un système d'équations différentielles.

$$x(t) = f(x(t), t) \qquad (2.1)$$

Où

$X \in Rn$ Est le vecteur d'état t ∈ R+ désigne le temps F : Rn

$xR+\rightarrow Rn$ Désigne la dynamique du système.

$$x(t0) = x0 \qquad x0 \in R^n \qquad (2.2)$$

Représente l'état initial du système et t0 l'instant initial.

- **En temps Discret**

Un système dynamique dans le cas discret, est représenté par des équations aux différences, appelées également «équations de récurrences». [30]

$$x(k+1) = g(x(k), k)\, x(k0) = x0 \qquad (2.3)$$

Où

K est l'instant discret, k0 est l'instant discret initial, x0 est le vecteur des états initiaux et g :$R\hat{}n \times Z+\rightarrow R\hat{}n$ indique la dynamique du système en temps discret.

2.2.3 Notions sur les systèmes dynamiques

– Système autonome : un système est dit autonome lorsqu'il ne dépend pas explicitement du temps.

– Causalité : un système est dit « causal », lorsque son entrée ne précède jamais sa sortie.

– Trajectoire temporelle : représente une grandeur décrite en fonction du temps qui peut être par exemple une variable d'état ou une sortie.

– Trajectoire de phase : est une trajectoire représenté sur une plane phase et qui décrit l'évolution du système au cours du temps pour des conditions initiales données.

– Espace de phase : est un espace mathématique, souvent multidimensionnel, dont chaque axe de coordonnées correspond une variable d'état du système dynamique étudié. [30]

– Portrait de phase : est constitué par l'ensemble des trajectoires de phase possibles d'un système dynamique.

– Point d'équilibre(ou point fixe) : on appelle point d'équilibre d'un système le point x∗ pour laquelle on obtient $f(x*) = 0$ dans le cas continu, $g(x*) = x*$dans le cas discret.

– Cycle limite : est un phénomène non linéaire, qui peut être siège d'oscillations, auto soutenues,

Caractérisées par leur amplitude et leur période fixes, indépendante de la condition initialex0et sans excitation extérieure.

– Tore : est un cas particulier du cycle limite qui représente les mouvements résultants de deux ou plusieurs oscillations dépendantes que l'on appelle aussi «mouvements quasi-périodiques», la trajectoire de phase ne se referme pas sur elle même.

– Attracteur : est une forme géométrique de l'espace de phase vers lequel tendent les trajectoires de phase.

2.3 Théorie du Chaos (Historique)

Henri Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème d'interactions de trois corps célestes, et a écrit « Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir et alors nous disons que cet effet est dû au hasard».

Plus tard, en 1961, Edward Lorenz [29], météorologue et professeur de Mathématique au MIT observa parhasar de phénomène qui s'appellera plus tard la théorie du chaos ou le chaos déterministe, à la suite des calculs visant à prévoir les phénomènes météorologiques. Ces prévisions nécessitaient un grand nombre de calculs d'équations différentielles complexes à très grand nombre de variables impossibles à faire à la main, il a utilisé alors un ordinateur, son Royal Mcbee LGP-300 qui est entrée dans l'histoire de la théorie du chaos, et qui a fait de Lorenz le père officiel de cette théorie puisque les calculs des systèmes chaotiques régissant ces phénomènes étaient difficile à comprendre et à simuler sans ordinateur .

Après plusieurs heures de calculs, Lorenz vait obtenu une série de résultats et a décidé de repasser une deuxième fois ces résultats dans l'ordinateur pour s'en assurer. Pour gagner du temps, il avait entrer les variables avec trois chiffres après la virgule, au lieu de six, il pensait qu'une faible variation dans les variables à la base d'un calcul aurait une incidence du même ordre de grandeur sur le résultat final mais à sa grande surprise, les résultats étaient totalement

différents de la première série. Il venait de découvrir le comportement chaotique d'un signal non linéaire; soit, d'infimes différences des conditions initiales d'un système déterministe entraineraient des résultats complètement différents. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon : « Le simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas». [31]

2.3.1 Définition

Le phénomène du chaos est un phénomène complexe non linéaire, qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales.

Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toute fois converger vers un point fixe ou un cycle limite .Ces trajectoires qui restent denses dans cette région sont très sensibles aux conditions initiales .Les solutions des équations différentielles non linéaires

Ne peuvent pas être calculé sa vecexactitude analytiquement car il n'existe pas de méthode résolution analytique pour ces équations, sauf pour certaines classes particulières .Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation. [31]

2.3.2 Propriétés des systèmes chaotiques

Parmi les caractéristiques principales permettant d'évoquer un comportement chaotique, on peut retenir les propriétés suivantes :

2.3.2.1 Déterminisme et imprévisibilité

Dans le cas des systèmes déterministes, théoriquement la connaissance de l'état initial De 'entrée, du modèle permet de prédire l'état futur du système. Ce pendant il est difficile de calculer la solution analytique théorique de certains systèmes non linéaires, qui est le cas pour les systèmes chaotiques déterministes, car ils sont caractérisés par une sensibilité aux conditions initiales, dont une simple erreur de mesure ou un simple arrondi conduit à des solutions

différentes, ce qui les rendent imprévisibles, en conséquence la pré visibilitén est plus liée au déterminisme.[31]

2.3.2.2 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales est l'une des caractéristiques fondamentales des systèmes chaotiques explicitée par Lorenz dans sa célèbre citation :"l'effet papillon». Une légère variation des conditions initiales sur un système chaotique entraine deux trajectoires qui sont initialement voisines, puis qui divergent exponentiellement, par la suite les deux trajectoires sont incomparables, ce qui rend les systèmes chaotiques imprédictibles à long terme. [31]

Il est donc clair que la moindre erreur oui m précisions sur la condition initiale ne permet pas de décider à tout temps qu'elle sera la trajectoire effectivement suivie.

Pour illustrer cette propriété, on prend comme exemple le système de Lorenz décrit par le système d'équations :

$$\dot{x} = a(y - x)$$

$$\dot{y} = bx - y - xz \qquad (2.4)$$

$$\dot{z} = xy - cz$$

Avec :

(x, y, z) : Le vecteur d'état.

(a, b, c) : sont les paramètres du système de «Lorenz».

$$a = 10 \; ; \; b = 28 \; ; \; c = 8$$

3) : sont les valeurs des paramètres pour lesquelles le système présente un comportement chaotique.

Pour deux conditions initiales très proches :

$(x01, y01, z01) = (0.1, 0.1, 0.1)$.

$(x02, y02, z02) = (0.1001, 0.1001, 0.1001)$.

On obtient la figure (2.1)

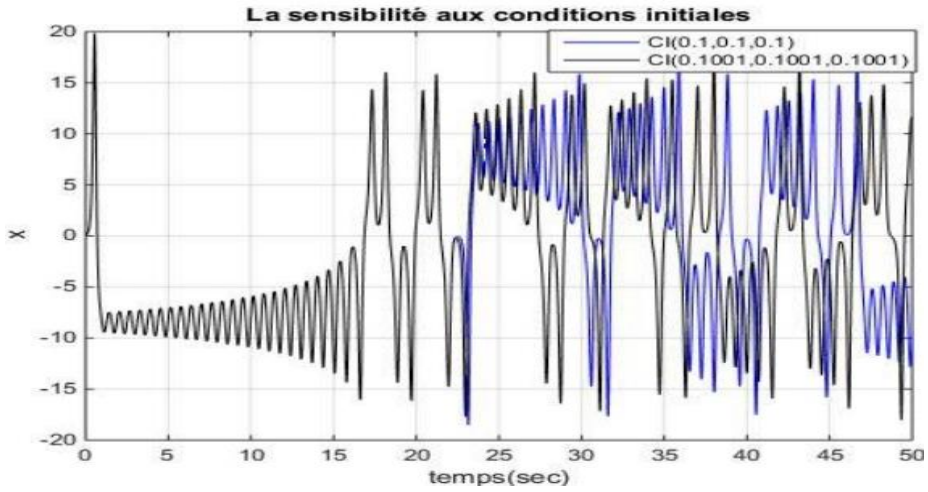


Figure 2.1 – Évolution dans le temps pour deux conditions initiales très proches.

2.3.2.3 Aspect aléatoire

Bien que les systèmes chaotiques soient déterministes, touts les états d'un système Chaotique présentent des aspects aléatoires, comme on peut l'observer dans la figure (2.2). Aucune périodicité n'est apparente

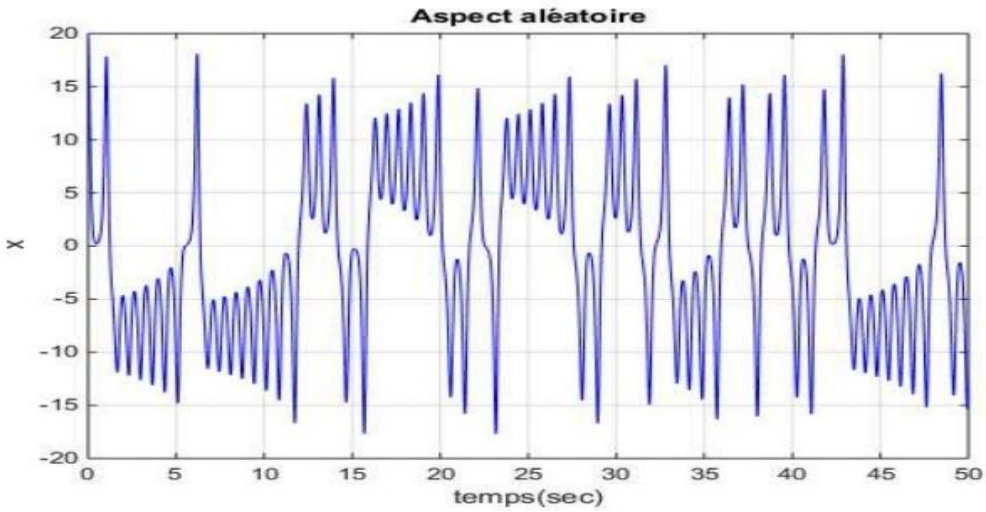


Figure 2.2 – L'aspect aléatoire du système de Lorenz.

2.3.2.4 Attracteur étrange

Lorsque Edward Lorenz [29] entreprit graphiquement la solution de son système (1.1) au moyen de son ordinateur, en traçant deux courbes avec deux jeux de conditions initiales très proches , il s'attendait à ce que les deux courbes divergent, mais à sa grande surprise, les deux courbes étaient plus ou moins identiques, elles ressemblaient à deux ailes de papillon.[31]

Le physicien David Ruelle qui s'est penché sur la question aqualifié cette figure «d'attracteur étrange» en remarquant que les trajectoires ne se coupent Jamais, et bien qu'elles semblent évoluer au hasard, elles forment des figures indiscutablement reconnaissables.

Par conséquent, lorsque le régime d'un système est chaotique, l'attracteur correspondant est un attracteur étrange qui a des propriétés topologiques différentes de celles d'un attracteur simple .

Un attracteur étrange est caractérisé par son bassin d'attraction et sa dimension fractal

- **Le bassin d'attraction**

Le bassin d'attraction est l'ensemble de points initiaux de l'espace de phases dont les trajectoires convergent vers l'attracteur et le parcourent d'une façon spécifique et unique.

- **La dimension fractale**

La dimension fractale de l'attracteur selon Hausdorff Besicovutch se présente comme suit. Soit un ensemble de points dans l'espace des phases à n dimensions, qui consiste à recouvrir cet ensemble par des hyper cubés de côté ε, soit le nombre minimum de cubes N(ε) nécessaires à cette opération qui varie comme. [32]

2.3.2.5 Bornitude des solutions

Toutes les solutions des systèmes chaotiques sont des solutions globalement bornées. En effet la trajectoire du système chaotique quel'on observe dans l'espace des phases reste confinée dans une région bien définie (attracteur étrange), après une période transitoire de durée variable [33].

On peut qualifier les systèmes chaotiques de stables si leurs conditions initiales sont prises dans le bassin d'attraction, c'est à dire que les trajectoires ne divergent pas vers l'infini mais convergent sur l'attracteur étrange.

Dans l'étude des systèmes non linéaires les cas suivants se présentent :

– Stabilité asymptotique : les trajectoires convergent vers un point fixe.

– Limite de stabilité (réponse oscillatoire sinusoïdale):les trajectoires convergent vers un cycle limite.

– Limite de stabilité (réponse bornée) : les trajectoires convergent vers un attracteur étrange.

– Instabilité : Trajectoires divergent vers l'infini.

2.3.3 Identification du chaos

Comme il est difficile de calculer la solution analytique des systèmes chaotiques, des méthodes numériques sont utilisées.

Dans cette section, nous présentons quelques outils qui permettent d'identifier le comportement chaotique d'un système dynamique et ses caractéristiques.

2.3.3.1. Exposant de Lyapunov

L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système. Un système sensible à de très petites variations de la condition initiale aura un exposant positif (système chaotique). En revanche, l'exposant est négatif si le système n'est pas sensible à des petites variations des conditions initiales, les trajectoires se rapprochent et on perd donc l'information sur les conditions initiales.

Un système de dimension n possède n exposants de Lyapunov qui mesurent le taux de divergence suivant un des axes de l'espace de phase. L'apparition du chaos exige l'existence d'un exposant positif selon au moins un axe [34], tout en rendant compte que la somme des exposant est négative (respectivement nulle) pour les systèmes dissipatifs (respectivement conservatifs).

Un exposant de Lyapunov positif (respectivement négatif) selon une direction indique [35], qu'une divergence entre deux trajectoires voisines augmente (respectivement diminue) exponentiellement avec le temps. C'est une caractérisation d'un attracteur étrange ou non. Les différents types d'attracteurs d'un système tridimensionnel en fonction des signes des exposants de Lyapunov sont représentés dans le tableau ci-dessous.

Type d'attracteur	**Signe des exposants de Lyapunov**
Point fixe	- - -
Cycle limite	0 - -
Attracteur étrange	+ 0 -

Méthodes de Calcul des exposants de Lyapunov

Il existe plusieurs méthodes de calcul des exposants de Lyapunov tels que la méthode (QR), (HQR) et (HQRB) [36]. L'une des méthodes les plus utilisées est l'algorithme de Wolf [37].

On considère un système discret à n dimensions

$$X_{k+1} = F(Xk), \qquad k = 0,1,2, \dots \dots \dots \qquad (2.5)$$

Le i-ème exposant de Lyapunov est défini en fonction du taux de croissance du i-ème axe

Principale iv par la formule [10]

$$\lambda_i = \lim_{N\to\infty} \frac{1}{N} \log \frac{\|Vi(N)\|}{\|Vi(0)\|}, \qquad i = 1,2, \dots n \qquad (2.6)$$

Les vecteurs Vi(k) vi sont transformés d'après la formule

$$Vi(k+1) = j(k)Vi(k) \qquad i = 1,2, \dots \dots \dots \qquad (2.7)$$

Où $j(k)$ Est la jacobienne de f au point .

$A\,0 = k$ Les vecteurs $vi, i = 1,2,\dots,n$ sont définis par :

$V1(1,0,0,0,\dots\dots,0)$

$V2(0,1,0,0,\dots\dots,0)$ (2.8)

$Vn(0,0,0,0,\dots\dots1)$

Pour éviter la divergence, à chaque itération les vecteurs V1(k) , V2(k), Vn(k) seront orthonormés par le procédé de Gram Schmidt :

$$v'_1 = \frac{v_1}{\|v_1\|'}$$

$$v'_2 = \frac{v_2 - (v_2, v'_1)v'_1}{\|v_2 - (v_2, v'_1)v'_1\|'} \quad (2.9)$$

$$v'_n = \frac{v_n - (v_n, v'_1)v'_{n-1} - \cdots - (v_n, v'_1)v'_1}{\|v_n - (v_n, v'_1)v'_{n-1} - \cdots - (v_n, v'_1)v'_1\|}$$

Exemple

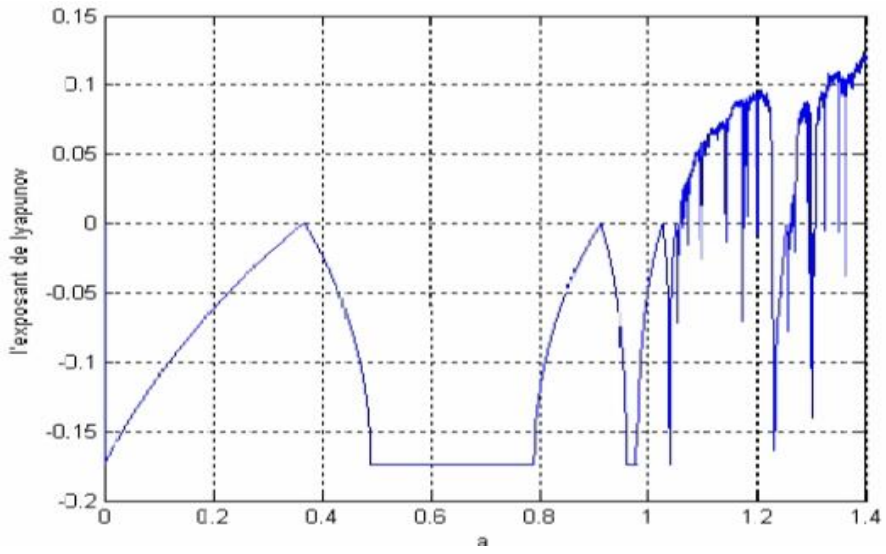


Figure (2.3). Exposant de Lyapunov du système Discret de Hénon

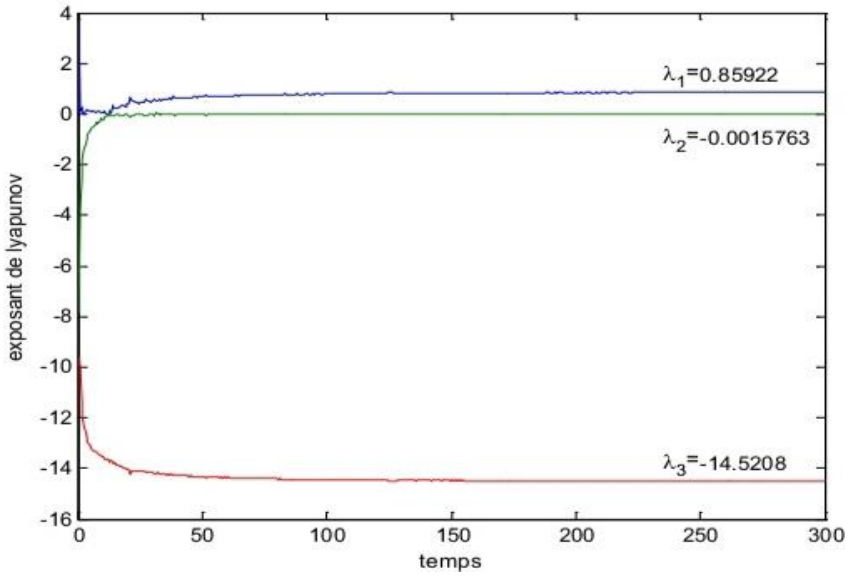


Figure (2.4). Exposant de Lyapunov du système continu de Lorenz

2.3.3.2 Spectre de puissance

Le calcul du spectre de puissance d'un signal sert à extraire ses composantes fréquentielles, en utilisant la transformée de Fourier. En fonction du signal temporel, on calcule la fréquence, l'amplitude et la phase de chaque composante sinusoïdale, en faisant appel aux deux variables réciproques le temps t , et la fréquence f , en utilisant la relation suivante[38] :

$$X(f) = \{x(t)e^{-2j\pi ftdt}[-\infty\,,+\infty\,] \qquad (2.10)$$

– Son module : est représenté par le spectre d'amplitude.

– Son argument t : est représenté par le spectre de phase.

e calcul du spectre de puissance d'un signal chaotique revient à calculer le spectre de Fourier de l'évolution temporelle d'une des variables du système, sachant que les spectre de Fourier d'un signal périodique ou quasi-périodique est constitué de raies distinctes correspondant aux périodes et harmoniques du système. Cependant pour un signal chaotique, on obtient un spectre continu riche en fréquence, possède une infinité de raies, qui est proche du spectre d'un bruit blanc, illustré par la figure (2.4) qui est très avantageux pour la cryptographie.

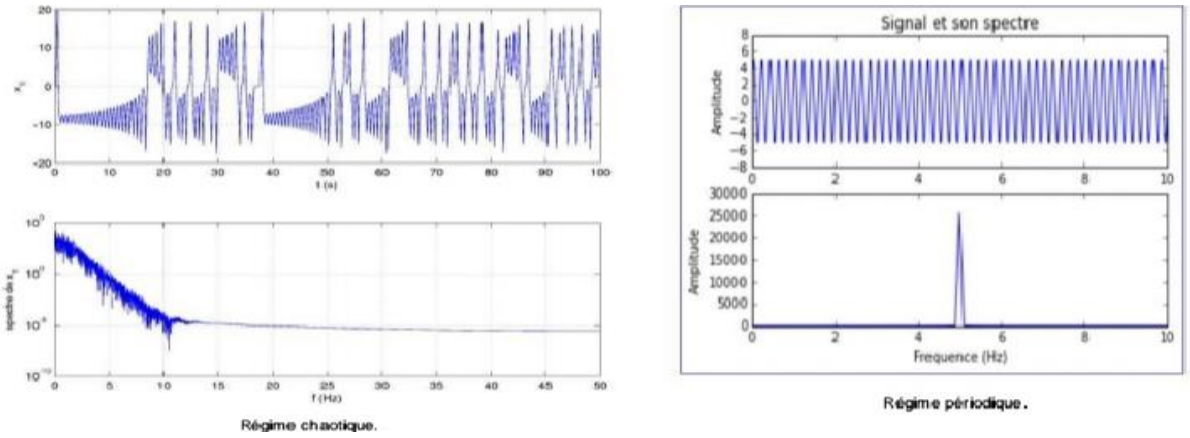


Figure 2.5– Différences entre le spectre d'un signal périodique et le spectre d'un signal chaotique.

2.3.3.3 Fonction d'auto-corrélation

La fonction d'auto corrélation nommée C(α) permet d'estimer le degré de ressemblance entre la variable x à l'instant t et sa valeur à l'instant t+α, et elle est obtenue en faisant la moyenne arithmétique d'un grand nombre de x(t) et x(t+α), sachant que le spectre de puissance correspond à la transformation de Fourier de la fonction d'auto corrélation [38].

Sa relation est citée ci-dessous :

$$C(\alpha) = 1/t2 - t1\{x(t)x(t+\alpha)dt[t2,t1] \qquad (2.11)$$

En faisant varier progressivement l'intervalle α on obtient la fonction d'auto-corrélation, et donc si x(t) est constant (périodique ou quasi-périodique), C(α) reste non nulle quand (t→∞), car le spectre de puissance est formé de raies distinctes ,et pour des oscillations périodiques C(α) oscille entre−1 et1.Cependant dans le cas des oscillations chaotiques ou le spectre présente une partie continu, C(α) tend exponentiellement vers0 quand α varie.

Cette propriété assure que les solutions divergentes les unes des autres. Si la fonction de corrélation est nulle pour des horizons non nuls, alors c'est un processus non corrélé, et on parle de «bruit blanc déterministe». [38]

2.3.3.4 Bifurcation

Une bifurcation est un changement qualitatif des propriétés d'un système non linéaire Telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents et les paramètres dont la modification quantitative, entraine le changement du régime dynamique de ce système sont appelés paramètres de bifurcation. [39]

Exemple :

Sachant que dans les équations de Lorenz par exemple, la résolution du système n'apporte pas toujours le chaos, ce régime n'apparait que pour certaines valeurs des paramètres. Pour illustrer l'influence de ces paramètres, on présente dans cet exemple les résultats de modification des paramètres «a», «c» du système chaotique «Lorenz» décrit pas les équations (1.4) .

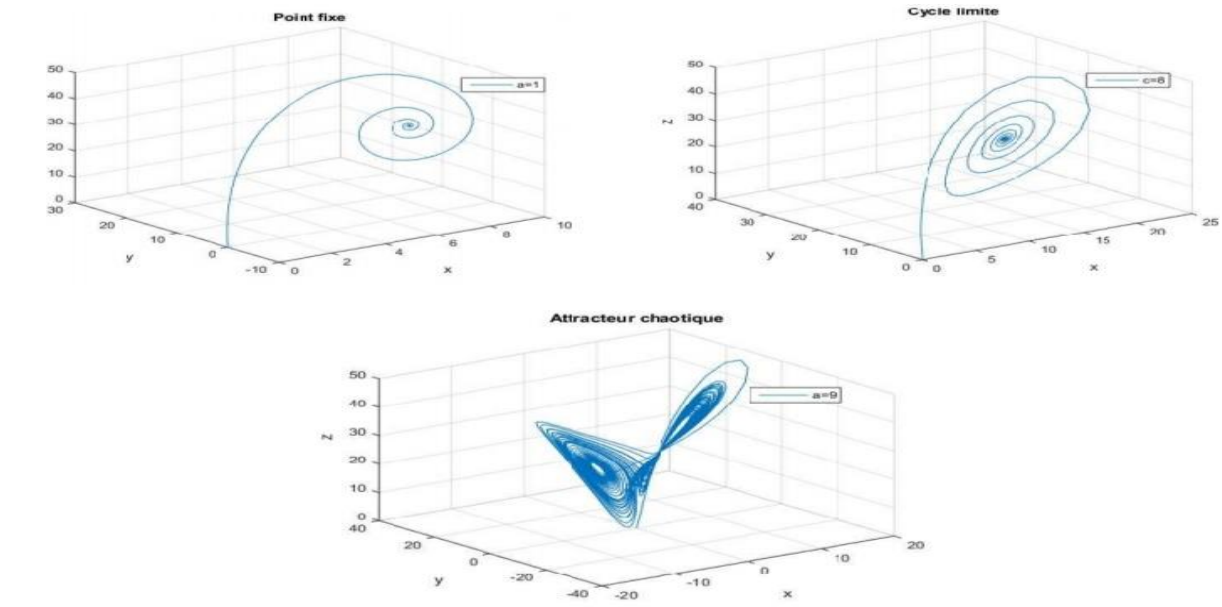


Figure 2.6 – Attracteurs de Lorenz pour différentes valeurs de ces paramètres.

Comme illustré sur la figure (2.5)

Lorsque on initialise la valeur de « a » à « 9 » : le système présente un attracteur chaotique.

Lorsqu'on a initialise la valeur de «a» à «1» : le système présente un point fixe.

Lorsqu'on a initialise la valeur de «c» à «8» : le système présente un cycle limite.

Diagramme de Bifurcation

Le diagramme de bifurcation est un tracé, qui permet d'évaluer rapidement l'ensemble des solutions possibles d'un système ainsi que leur stabilité en fonction des variations de l'un de ses paramètres. Il permet également de repérer les valeurs particulières du paramètre qui induisent des bifurcations.

Il présente des intervalles sur les quelles les solutions asymptotiques évoluent continuellement avec le paramètre, et il classe les valeurs du paramètre sur l'axe des abscisses et les valeurs d'une des variables d'état sur l'axe des ordonnées.

La figure (2.7) illustre le diagramme de bifurcation d'un système quelconque [12]

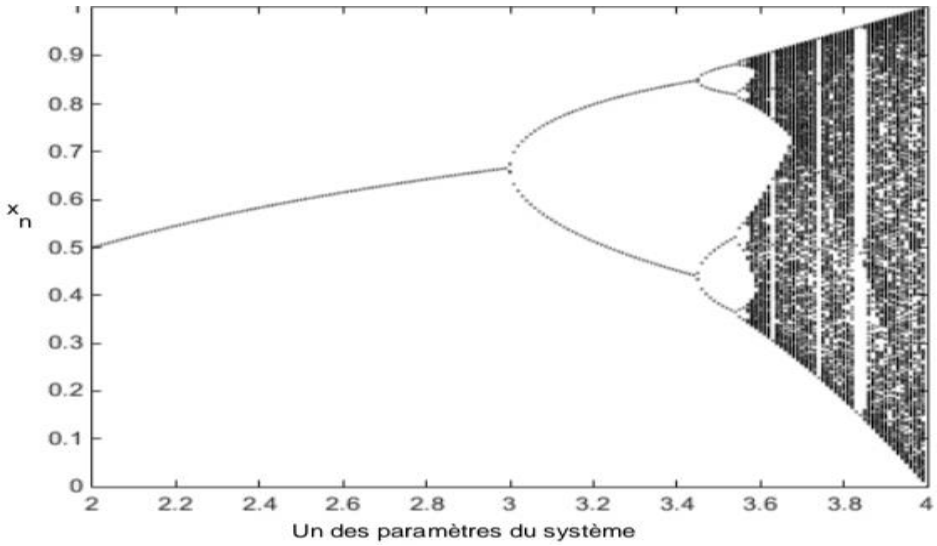


Figure 2.7 – Exemple d'un diagramme de bifurcation quelconque

Route vers le chaos

Varier un paramètre d'un système peut changer son comportement. Il peut passer d'un état stationnaire à un état périodique et devenir chaotique. Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos. L'évolution se fait par des changements discontinus appelé bifurcation. [40]

Feigenbaum a redécouvert une route vers le chaos qui avait été découverte dans les années60 par Myberg. Cette route est appelée « cascade de doublement de période». Ce scénario est observé avec la suite logistique. Qui est l'exemple le plus connu d'un système non linéaire pour lequel il

avec la suite logistique. Qui est l'exemple le plus connu d'un système non linéaire pour lequel il est possible de tracer un diagramme de bifurcation.

Son équation est donnée comme suit :

$$x_{k+1} = rx\,(1 - xk) \qquad (2.12)$$

Où $k = 0,1,2,\ldots..$, est le temps discret.

x l'unique variable dynamique

0≺ r≺4 un paramètre de contrôle qui conduit, suivant les valeurs de r ,à une suite convergente soumise à des oscillations ou une suite chaotique.

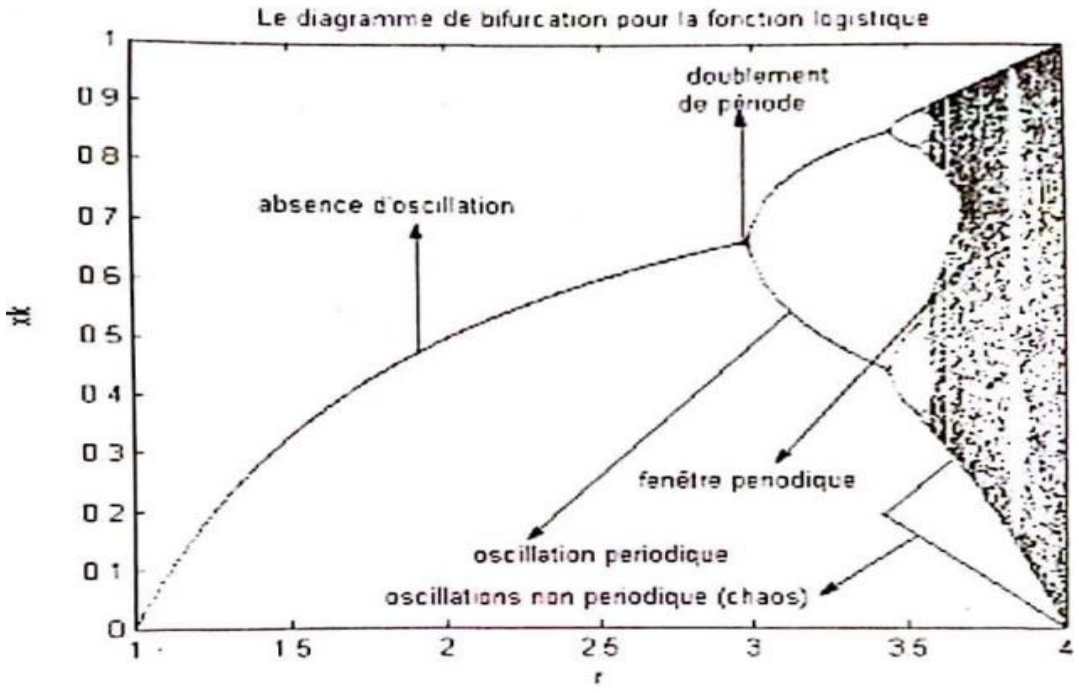


Figure 2.8– Diagramme de bifurcation de la fonction logistique.

On distingue trois scénarios théoriques d'évolution vers le chaos :

– Le doublement de période

L'augmentation d'un paramètre d'un système périodique provoque l'apparition d'un doublement de sa période, puis elle se multiplie en4, 8,16..... .

Les doublement s étant de plus en plus rapprochés, on tend vers un point d'accumulation au quel on obtiendrait hypothétiquement une fréquence infinie, et c'est à ce moment que le système devient chaotique. [40]

Exemple

La figure (2.8) montre qu'en faisant varier le paramètre « c » du système de Rösseler, décrit par les équations (1.23), on obtient un doublement de période de l'attracteur.

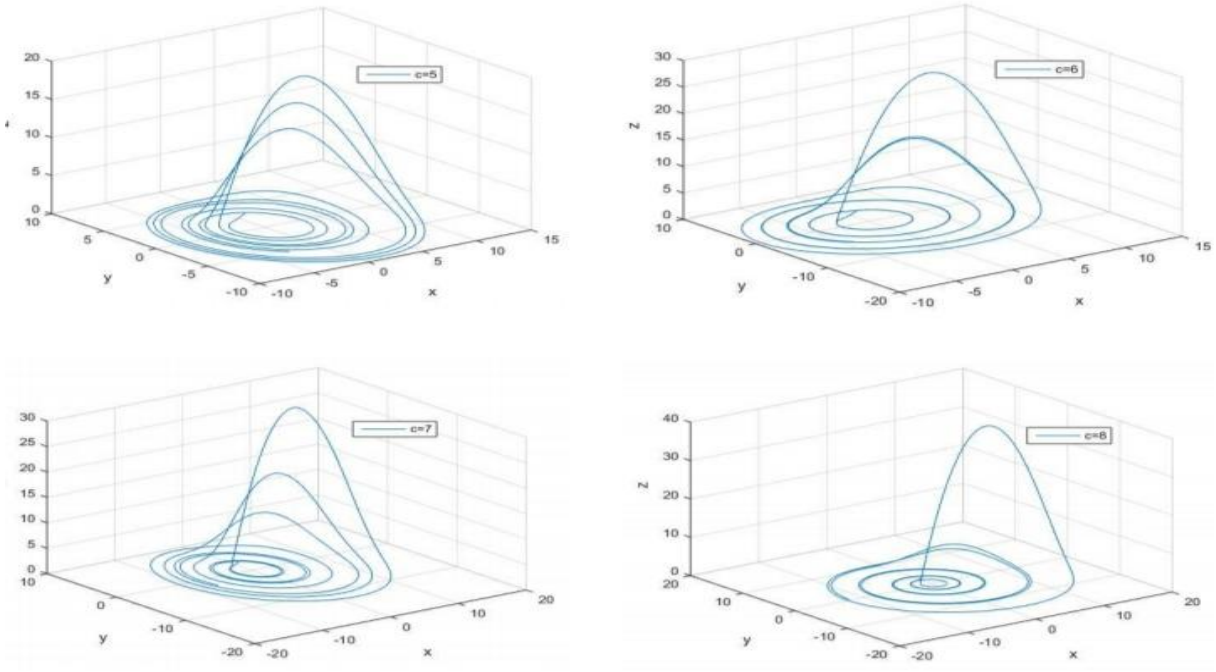


Figure 2.9 – Doublement de période de l'attracteur du système de Rössler.

– Intermittence

Les intermittences se caractérisent par l'apparition erratique d'explosions chaotiques dans un système qui oscille de manière régulière.

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise brutalement pour donner lieu à un comportement chaotique. Il se stabilise de nouveau, ensuite pour donner lieu à une autre "explosion chaotique" plus tard.

La fréquence et la durée des phases chaotiques ont tendance à s'accroitre. Plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition.

– Quasi-périodicité

Ce troisième scénario fait intervenir pour un système périodique l'apparition d'une autre Période dont le rapport avec la première' est pas rationnelle .Alors, on change de nouveau le paramètre et il apparait une troisième période, et ainsi de suite jusqu'à l'apparition du chaos. [41]

2.3.3.5 Section de Poincaré

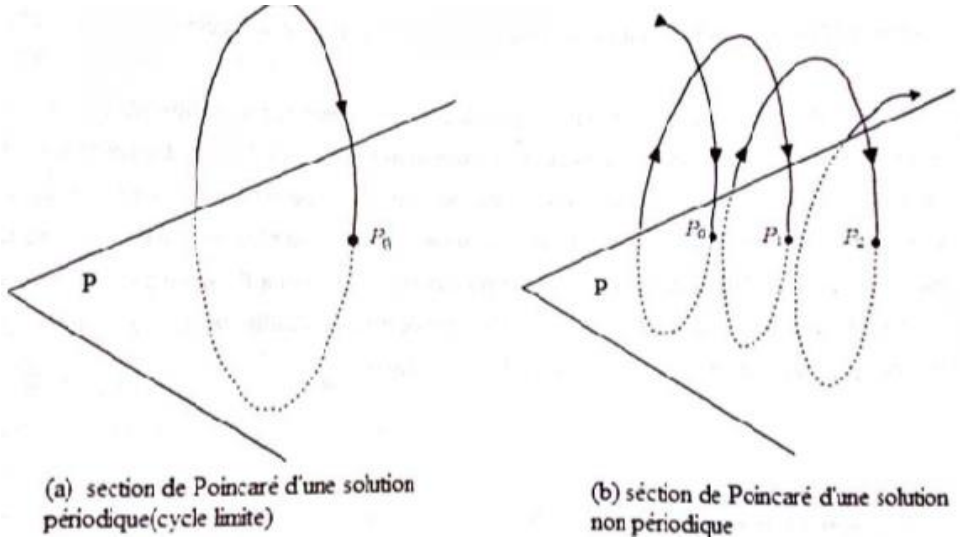
Une application Poincaré, nommée en l'honneur d'Henri Poincaré est un outil mathématique simple permettant de transformer un système dynamique continu en un système dynamique discret via une réduction d'une unité de l'ordre du système, tout en gardant ses propriétés.[41] Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases Par un plan en dimension 3 ou par une droite en dimension 2,afin d'étudier les intersections de cette trajectoire avec ce plan ou cette droite et l'ensemble de points d'intersections situés sur la surface est appelé section de Poincaré.

Le plan de la section doit être choisi de manière à garantir l'existence d'intersections avec la trajectoire et de telle sorte que celle-ci le traverse alternativement dans un sens puis dans l'autre. On peut identifier le régime de fonctionnement d'un système dynamique en observant l'allure obtenue sur cette section.

– Lorsque le régime est périodique, la section de Poincaré est un point (l'attracteur est un cycle limite).

– Lorsque le régime est bi-périodique, la section de Poincaré est une courbe fermée (l'attracteur est un Tore).

– Lorsque le régime est chaotique, la section de Poin caré, est un ensemble de points Répartis sur une surface, ils sont donnés par une structure complexe mais bien définie. La figure (2.9) illustre le principe de la section de Poincaré pour les trois solutions, périodique, bi-périodique, et chaotique. [41]



(a) section de Poincaré d'une solution périodique(cycle limite)

(b) séction de Poincaré d'une solution non périodique

Figure 2.10 – Principe de la section de Poincaré.

2.4 Exemples des systèmes chaotiques

2.4.1 Exemple d'un système chaotique en temps continu

Système de Rössler

Le système de Rössler a été proposé par l'Allemand Otto Rössler. Il est lié à l'étude de l'écoulement des fluides. Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique. Les équations de ce système sont les suivantes :

$$\dot{x} = -(y + z)$$

$$\dot{y} = x + ay \qquad (2.13)$$

$$\dot{z} = b + z(x - c)$$

La figure (2.10) illustre le tracés de l'attracteur de Rössler, les paramètres sont fixés aux valeurs suivantes : $a = 0.2,\ b = 0.2,\ c = 5.7$ pour des conditions initiales $x0 = (\ 0.2\ 2\ 1\ )$

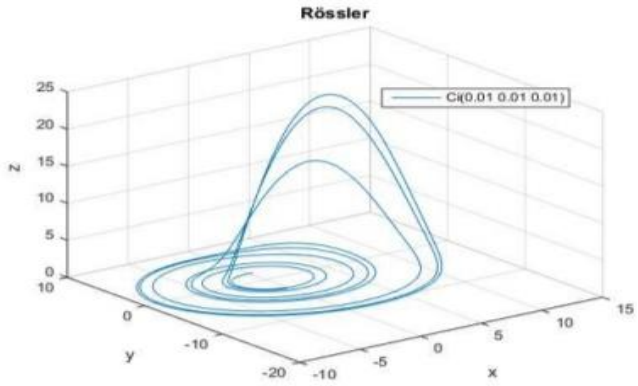


Figure 2.11 – Attracteur chaotique de Rössler.

2.4.2 Exemple d'un système chaotique en temps discret

Système de Lozi

La récurrence de Lozi est obtenue en remplaçant (x)2 dans la récurrence du système Hénon par| x |et en modifiant la valeur des paramètres.

René Lozi, propose l'application suivante :

$$x(k+1) = 1 - a|\,x(k)| + y(k)$$

$$y(k+1) = \; bx(k) \qquad (2.14)$$

Attracteur chaotique de Lozi est représenté sur la Figure (1.11) pour les valeurs numériques $a = 1.7\ et\ \ b = 0.5$.

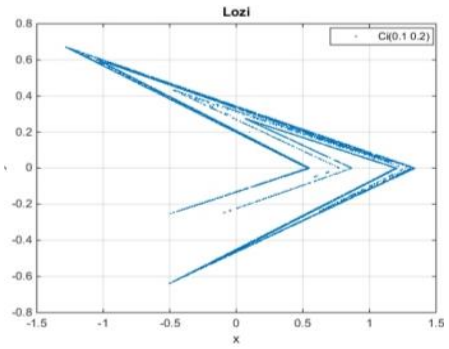


Figure 2.12– Attracteur chaotique de Lozi.

2.5 Les cartes chaotiques

2.5.1. La carte chaotique logistique (la récurrence logistique)

Une récurrence logistique est un exemple simple de suite dont la récurrence n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire, cette récurrence fut popularisée par le biologiste Robert May en 1976. Sa relation de récurrence est :

$$X_{n+1} = \mu(1 - Xn) \qquad (2.15)$$

Elle conduit, suivant les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique [42], comportement selon μ :

Dans le modèle logistique, la variable notée ici Xn désigne l'effectif de la population d'une espèce. En faisant varier le paramètre μ, plusieurs comportements différents sont observés :

. Si $0 \leq \mu \leq 1$, l'espèce finira par mourir, quelle que soit la population de départ.

. Si $1 \leq \mu \leq 3$, la population se stabilisera sur la valeur $\mu-1$

μquelle que soit la population initiale.

. Si $3 < \mu \leq 1 + \sqrt{6}$ (approximativement 3,45), la population oscillera entre deux valeurs. Ces deux valeurs sont indépendantes de la population initiale.

.Si $3{,}45 < \mu < 3{,}54$, la population oscillera entre quatre valeurs, là encore sont indépendantes de la population initiale.

. Si μ est légèrement plus grand que 3,54, la population oscillera entre 8 valeurs, puis 16, 32, etc.

. La plupart des valeurs au-delà de 3,57 présentent un caractère chaotique, mais il existe quelques valeurs isolées de μ avec un comportement qui ne l'est pas. Celles-ci s'appellent parfois les iles de la stabilité. Par exemple autour de la valeur 3,82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs et pour μ légèrement plus grand, entre six valeurs, puis douze, etc. ces comportements sont encore indépendants de la valeur initiale.

. Au-delà de μ = 4, la population quitte l'intervalle [0,1] et diverge presque pour toutes les valeurs initiales [43].

Un diagramme de bifurcation permet de résumer tout cela

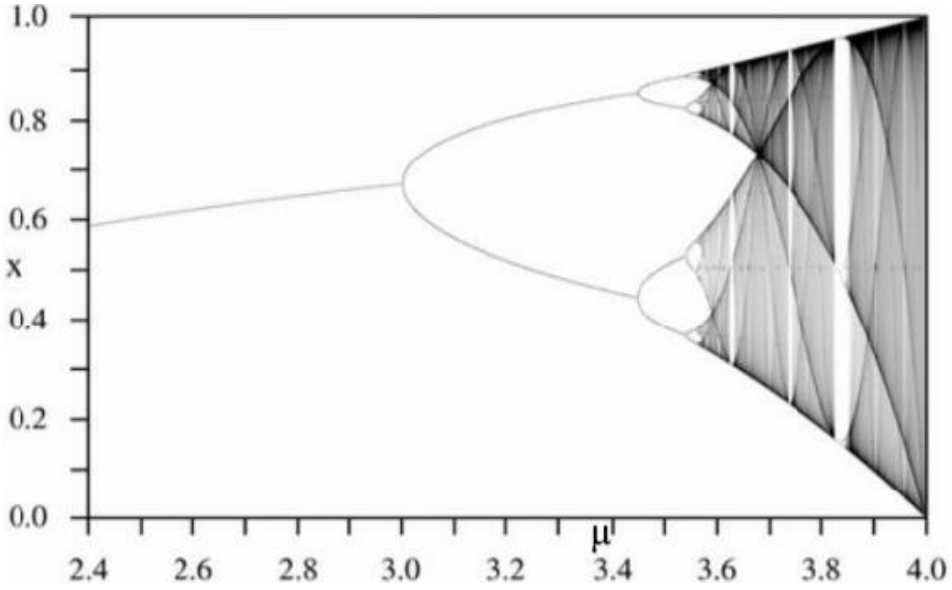


Figure 2.13 : Diagramme de bifurcation de la récurrence logistique [15].

2.5.2 La carte chaotique sine (la récurrence sine)

La récurrence sine d'une (01) dimension a pour représentation d'état :

$$X_{n+1} = Y\ sin(\pi Xn) \qquad (2.16)$$

Avec Y = 1 le comportement chaotique est généré par une manière très similaire à la fonction logistique.

Comme la récurrence logistique, la carte sine est quadratique au voisinage de x = 0,5. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produisent périodiquement dans le même ordre. Elle a le même nombre de Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences.

Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique [43].

2.5.3 La carte chaotique standard (la récurrence standard)

La récurrence standard de deux (02) dimensions a pour représentation d'état :

$$x_{n+1} = x_n + Ks(y_n)$$

$$y_{n+1} = y_n + x_{n+1} \qquad (2.17)$$

Pour K = 0, la carte n'est pas linéaire et seules les orbites périodiques et quasi-périodiques existent. Lorsqu'elles sont tracées dans l'espace des phases, les orbites périodiques apparaissent comme des courbes fermées, et les orbites quasi-périodiques comme des petites courbes fermées dont leurs centres se situent dans une autre courbe fermée plus grande. Ces types d'orbites sont observés suivant les conditions initiales utilisées. La non-linéarité de la carte est augmentée lorsque k augmente [43].

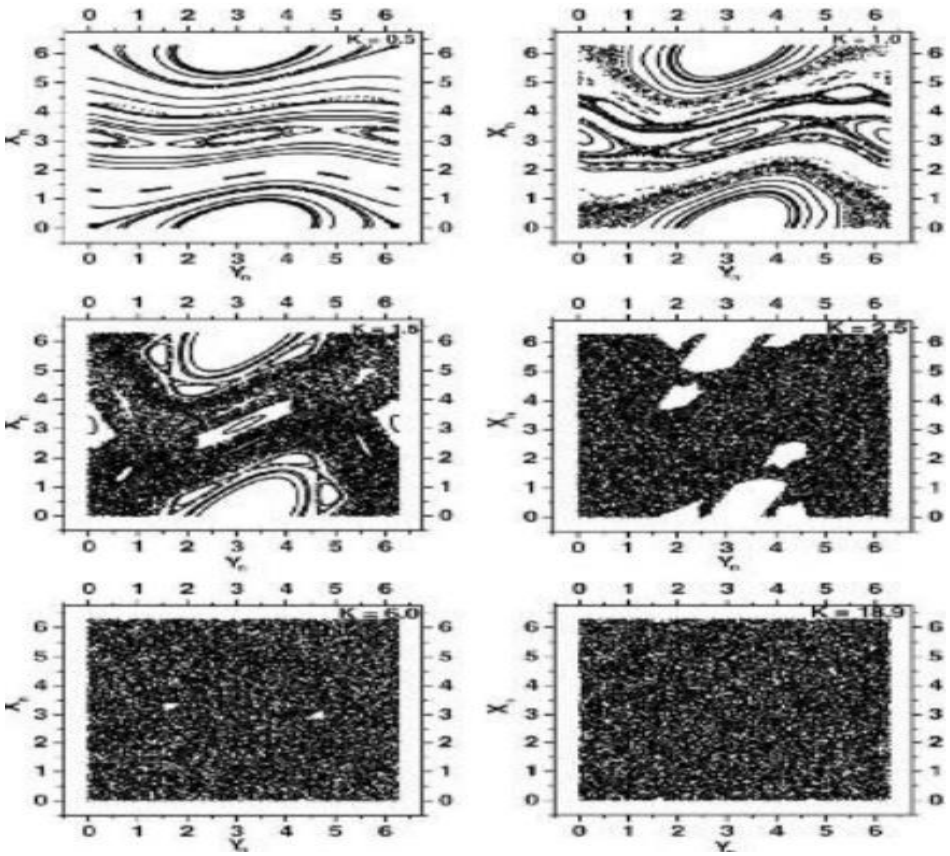


Figure 2.14 : L'espace de phase de la carte standard pour K= 0.5, 1.0, 1.5, 2.5, 6.0 et 18.9 [15].

2.6 Suite chaotique linéaire par morceaux (PLCM map)

La Suite chaotique du système PLCM a gagné récemment une attention particulière de plusieurs chercheurs en théorie du chaos en raison de sa simplicité dans la représentation, son efficacité en implémentation, et son bon comportement dynamique [44]. La suite chaotique PLCM peut être décrite dans l'équation par :

$$zk/y \qquad 0 \leq zk < y$$

$$zk + 1 = F(zk, y) = zk - \frac{y}{0.5} - y \qquad y \leq zk < 0.5 \tag{2.18}$$

$$F(1 - zk, y) \quad 0.5 \leq zk < 1$$

Où zk

$\in (0,1)$ Avec $n \in \mathbb{N}$ et $z0$ comme condition initiale. $\lambda \in (0,0.5)$ est considéré comme étant le paramètre de contrôle. Le système PLCM a une distribution uniforme invariante, une bonne ergodicité et une bonne confusion [45-46], de sorte qu'il peut fournir une excellente séquence aléatoire, qui convient aux systèmes cryptographiques. La distribution de z avec différents du système PLCM est représentée sur la figure 2.9, où les valeurs de z sont uniformément réparties.

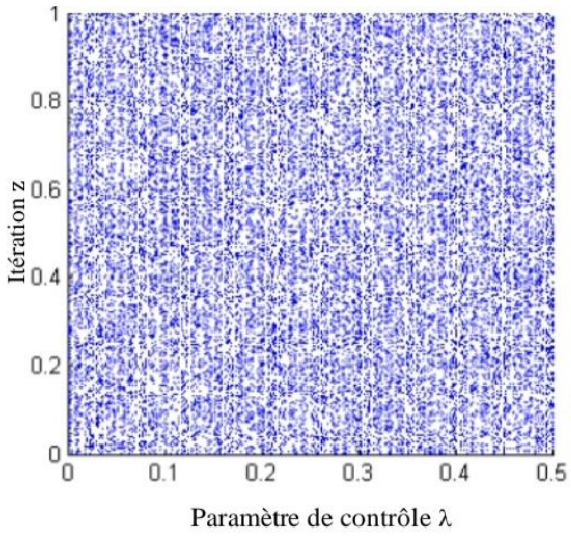


Figure 2.15: Diagramme de bifurcation de la suite chaotique PLCM

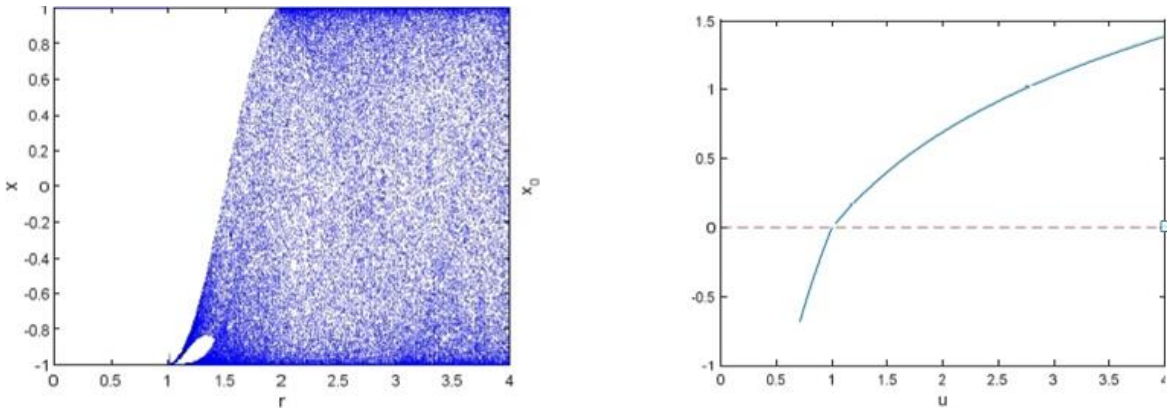
2.7 La carte Chebyshev

Une autre carte unidimensionnelle très utilisée dans les techniques cryptographique à base du chaos, c'est la carte de Chebyshev elle est sous la forme suivante :

$$x_{n+1} = cos\,(\,a \times a\,r\,cos\,(x_{\mathrm{n}}\,)) \qquad (2.19)$$

Où le paramètre $a \in N$. [43]

Son diagramme de bifurcation et le diagramme de l'exposant de Lyapunov sont illustrés aux figures 2.10 (a) et 2.10 (b). On peut constater que, lorsque le paramètre a> 1, il a un comportement chaotique et la plage des séquences chaotiques en sortie est [−1, 1]



(a) (b)

Figure 2.16 Diagramme de bifurcation de la carte Chebyshev(a) et Exposant de Lyapunov de la carte Chebyshev(b)

2.8 Propriétés des suites chaotiques

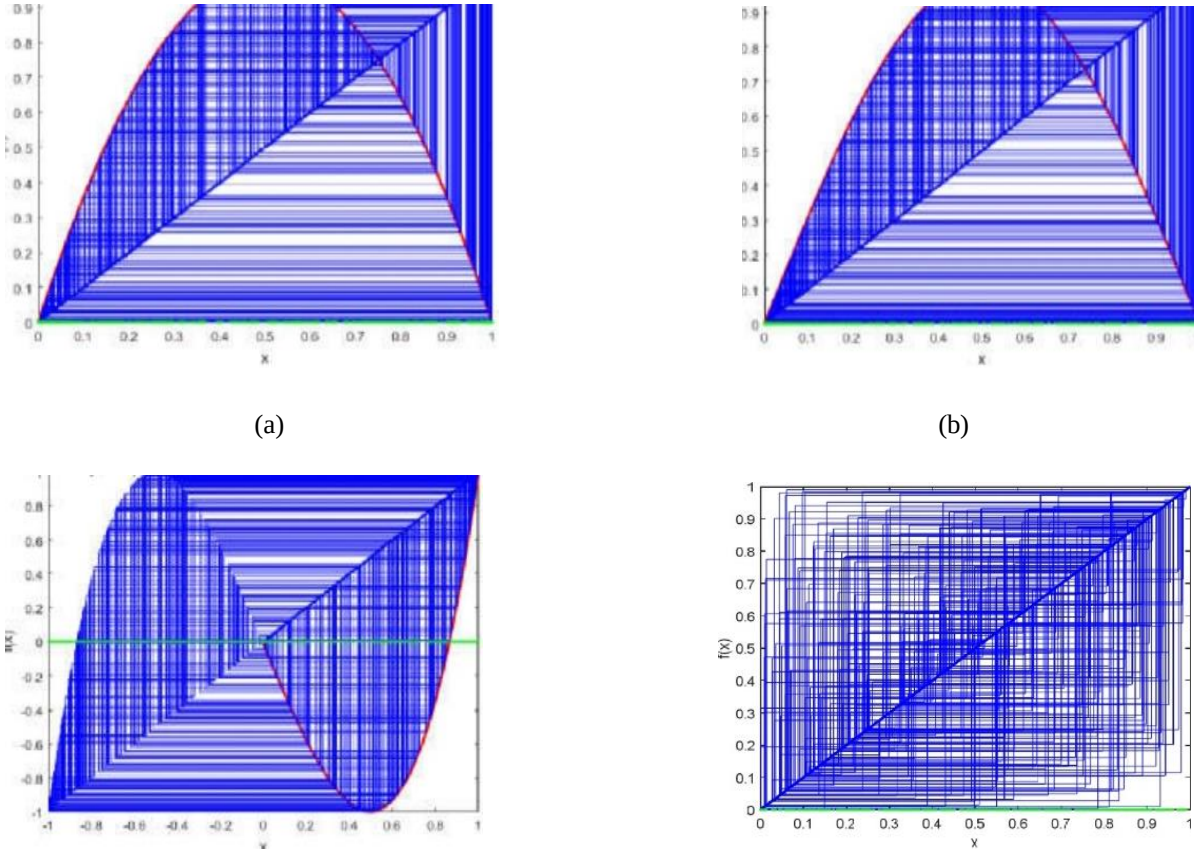
• Sensibilité à la condition initiale : Un changement minime dans la condition initiale provoque en sortie un régime pseudo-aléatoire complètement différent de l'état précédent, c'est le fameux effet papillon dont on a parlé [47], [48].

• Pseudo-aléatoires : une suite chaotique gouvernée par une équation déterministe permet de générer un régime chaotique pseudo-aléatoire.

• Ergodique : un processus chaotique est ergodique, car il possède la même distribution en sortie quel que soit la distribution de la variable présente à l'entrée.

2.9 Le CobWeb

Le plot du Cob Web, ou diagramme de Verhulst [49] est considéré comme l'un des premiers formalisme mathématique permettant de poser le problème de la stabilité d'un processus dynamique. Particulièrement bien adaptée pour visualiser le comportement qualitatif des cartes unidimensionnelles et nous permet d'analyser l'évolution à long terme de tels systèmes sous itération récursive. C'est-à-dire la séquence de valeurs obtenue à partir de $x_{n+1} = f(Xn)$, à partir d'un point initiale pour une valeur de paramètre de contrôle donnée.



(a) (b)

(c) (d)

Figure. 2.17 Le Cob web avec x0 = 0.01. (a) La carte logistique; (b) La carte sinus; (c) La carte de chebyshev; (d)

Les trois premiers graphes de la figure illustrent que, pour des valeurs minime de contrôle, le système affiche une spirales intérieures menant à un point fixe asymptotiquement stable. Puis, on observe un comportement périodique pour quelques valeurs de , représenté par des rectangles répétitifs de plus en plus compliquées. Ensuite le système transite vers un régime instable pour des valeurs [50] de contrôle élevée (comportement chaotique).

Par contre, pour les autres plots qui représentent notre système amélioré. ils affichent tous une orbite remplissant [51] le plan de phase avec des segments de ligne infinis non répétitifs pour toute valeurs de contrôle υ

Ces résultats, montrent l'instabilité de l'attracteur dans la plage élargie et expliquent la chaoticité de notre système améliorée

Conclusion

Un système est chaotique lorsqu'il est régit par des lois déterministes mais que son évolution échappe à toute prévision à long terme. Pour un système continu sans retard et sans entrée il faut également que l'ordre n du système soit supérieur ou égale à trois.

Toutefois pour un système discret on obtient le chaos à partir de deux équations. Le comportement chaotique est principalement du à sa sensibilité aux conditions initiales, il est également caractérisé par son spectre de puissance continu, sa fonction d'autocorrection qui à l'infini tend vers zéro et possède au moins un exposant de Lyapunov positif. Ce chapitre nous a permis d'observer toutes ces caractéristiques accompagnées par divers exemples sur Matlab tel que le système de Rösseler ainsi nous avons pu constater ce qui caractérise un système chaotique des systèmes dynamiques non linéaires.

Dans le prochain chapitre nous énoncerons l'utilité et l'utilisation du comportement chaotique dans le chiffrement, pour des fins de sécurité, et de transmission de données confidentielles

Chapitre 03

Proposition d'une nouvelle suite chaotique appliquée au cryptage d'images

3.1 Introduction

Depuis longtemps, plusieurs chercheurs sont intéressés aux comportements inhabituels des systèmes non linéaires et découvrent que certains systèmes présentaient des instabilités de nature très étranges. Ce fût la découverte des signaux chaotiques qui ont un comportement complètement déterministe mais qui font penser à des allures pseudo aléatoires. Et ces dernières années, la littérature s'est beaucoup intéressée au développement, à la l'analyse et la mise en œuvre des crypto systèmes chaotiques. Les cartes comme la carte logistique sont utilisées dans les algorithmes de cryptage d'image à cause de leur forte sensibilité aux conditions initiales et aux paramètres de contrôle, mais ces derniers présentent des comportements chaotiques seulement pour certaines valeurs de paramètre de contrôle.

De nombreuses méthodes ont été proposées pour résoudre ces problèmes pour surmonter ces problèmes, dans ce présent chapitre, nous donnons une nouvelle méthode permettant de créer un système chaotique simple et efficace. Les simulations et les évaluations de performance montrent que le système proposé est capable de produire un système chaotique avec des meilleures performances et des plages chaotique plus étendues par rapport aux cartes chaotique classiques.

3.2 Modèle de la suite chaotique améliorée

Nous proposons une nouvelle suite chaotique inespérée de la suite chaotique logistique map et l'objectif de cette idée et d'élargir la gamme de paramètre de contrôle r

Pour logistique map $3.95 < r < 4$

Pour la nouvelle suite $0 < r < 30$ et peut y aller jusqu'à l'infini

3.3 Équations des modèles proposés et basée

3.3.1 Expression de la suite logistic map

Logistique (Logistic map) Cette fonction chaotique 1D non linéaire est donnée par l'équation suivante:

$$x_{i+1} = rx_i(1 - x_i) \quad 3.1$$

x_i : est la séquence chaotique d'ordre i

$r \in [0,4]$ Est le paramètre de contrôle. Elle est générée itérativement en partant de

$x_0 \epsilon [0,1]$ Appelée condition initiale.

La suite logistique est vraiment chaotique si $r \in [3.95,4]$ et purement chaotique si $r \cong 4$ La suite montre un bon comportement et elle est fréquemment utilisée dans de nombreuses applications.

3.3.2 Expression de la suite MLM (modified logistic map)

$$x_{i+1} = mod(r.e^{x_i} \times (1 - e^{x_i}), 1) \quad 3.2$$

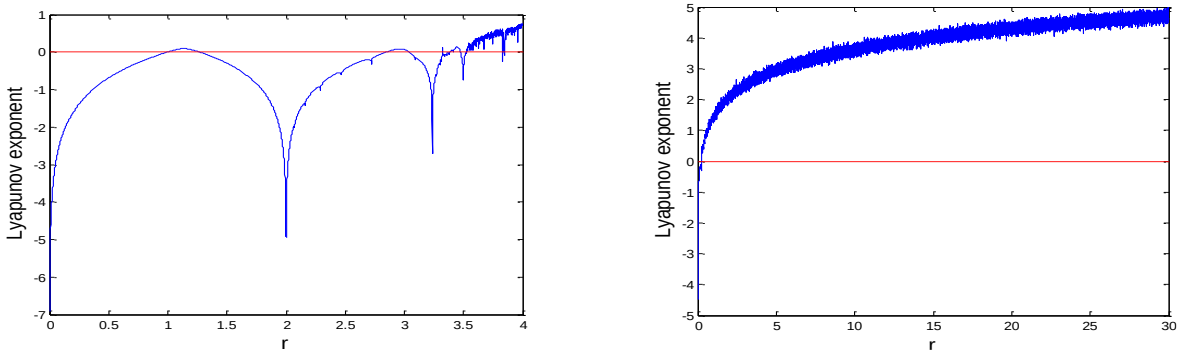
x_0: Valeur initiale $\in$ [0 1]

r : Paramètre de contrôle $\in$ [0 30]

mod : Le résultat du reste de la division

e^{xi} : Fonction exponentielle

3.4 Le diagramme de Lyapunov des deux suites chaotiques



Lyapunov exponent for 1D logistic map *Lyapunov exponent for improved 1D Logistic map*

Figure (3.1) : Le diagramme de Lyapunov des deux suites chaotiques.

Selon les théories de la stabilité des systèmes dynamiques, on dit qu'un système dynamique est stable si, et seulement si, tous les exposants de Lyapunov sont inférieurs ou égaux à zéro. Par contre, s'il y a au moins un exposant positif, le système devient assez instable (chaotique).

Nous remarquons clairement que r à change $3.95 < r < 4$ à $0 < r < 30$

3.5 Le diagramme de bifurcation

On dessine le diagramme de bifurcation de la variable d'état x en fonction du coefficient de contrôle r, où l'on note qu'avec le nouveau système, afin de connaître le comportement dynamique du système où l'on avait des plages chaotiques plus grandes par rapport au chaotique initial Plans.

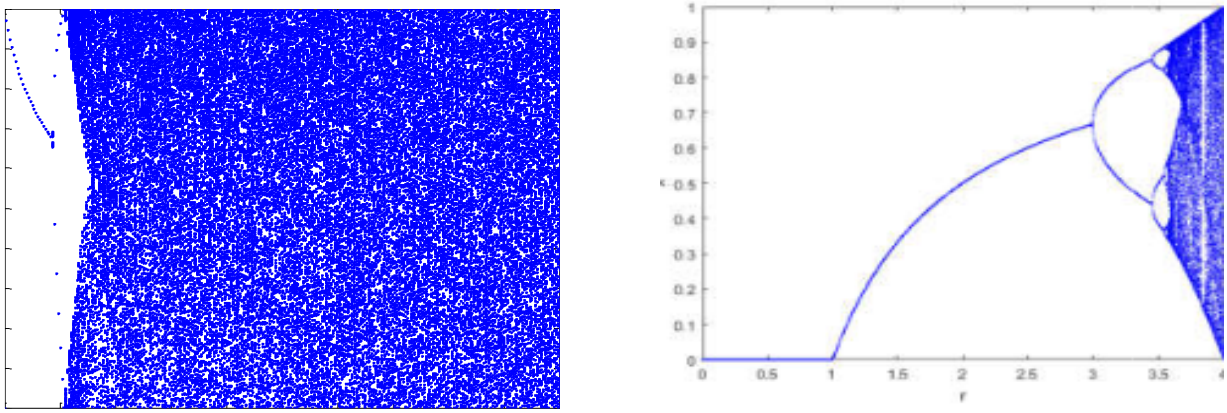


Diagramme de bifurcation de MLM *Diagramme de bifurcation logistique map*

Figure (3.2) : Le diagramme de bifurcation des deux suites chaotiques.

3.6 Le cob web de MLM

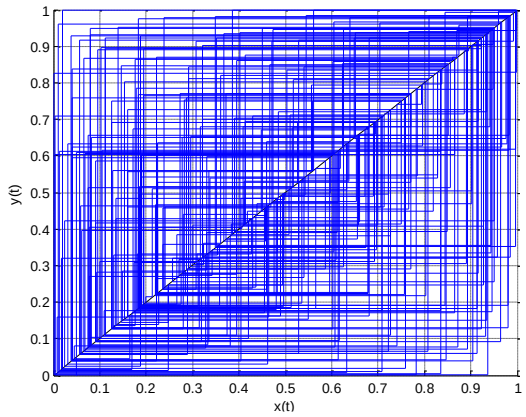


Figure (3.3) : Diagramme de cob web de MLM.

3.7 Technique de cryptage proposée

3.7.1 Schéma de cryptage

Le schéma de cryptage proposé tel que représenté sur la *Figure (3.4)*, peut être réalisé à travers les étapes suivantes

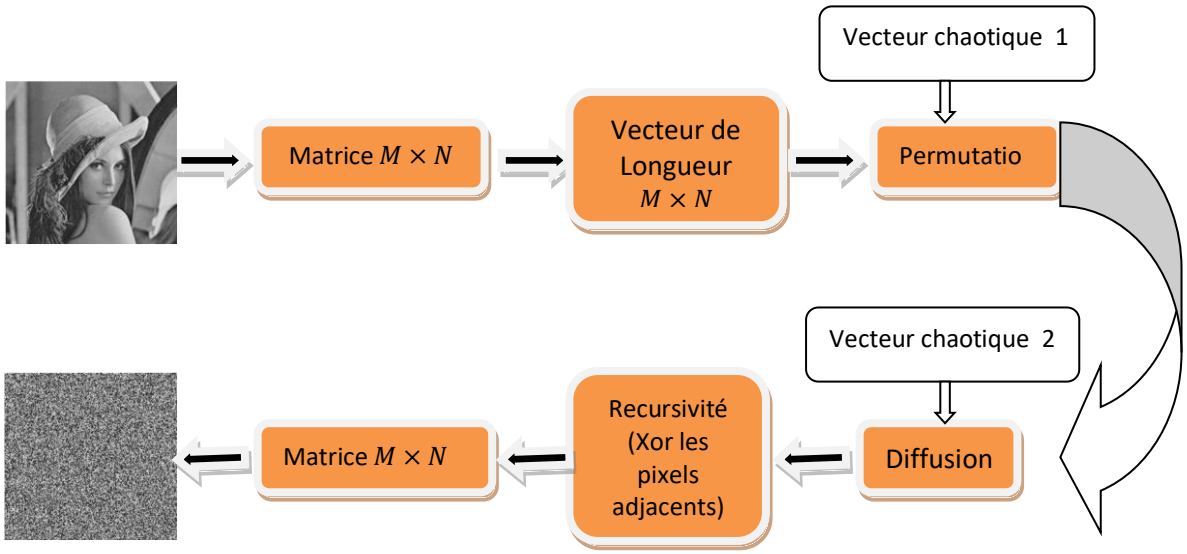


Figure (3.4) Schéma de cryptage proposé.

3.7.2 Algorithme de cryptage

1- Soit p une image de test de taille $m \times n$

2- Convertir cette image en vecteur v de taille $1 \times m \times n$

3- Générer une séquence chaotique de taille $1 \times m \times n$ a base de la suite M , ces valeurs variant entre [0,1] et ayant les paramètres suivants : (x_0, r_0) .

4- Arranger les valeurs de cette suite en ordre croissant

5- Ranger le vecteur v selon l'ordre donner par la suite chaotique MLM pour donner un vecteur v` résultat de permutation

Phase de diffusion :

6- Générer une autre suite chaotique à base de la suite MLM de taille $1 \times m \times n$ ayant comme paramètres chaotiques(x_1, r_1).

7- Convertir les valeurs obtenues ou niveau du gris en multipliant et arrondissant ces valeurs à 255, pour obtenir un vecteur appelé x_1.

8- Effectuer le XOR entre de vecteur x_1 et $v`$ pour donner le vecteur résultant $v``$ de la manière suivante :

Pour $i = 1$ $v``(1) = x_1(1) \oplus v`(1)$

Pour

$i = 2 : m \times n$ $v``(i) = x_1(i) \oplus v`(i) \oplus v``(i-1)$ 3.3

9- Convertir le vecteur obtenu en une matrice de taille $m \times n$ qui est exactement l'image cryptée

3.7.3 Schéma de décryptage

Le processus de décryptage tel que représenté sur la figure 2 prend exactement les étapes du processus de cryptage de manière inverse pour obtenir l'image décryptée

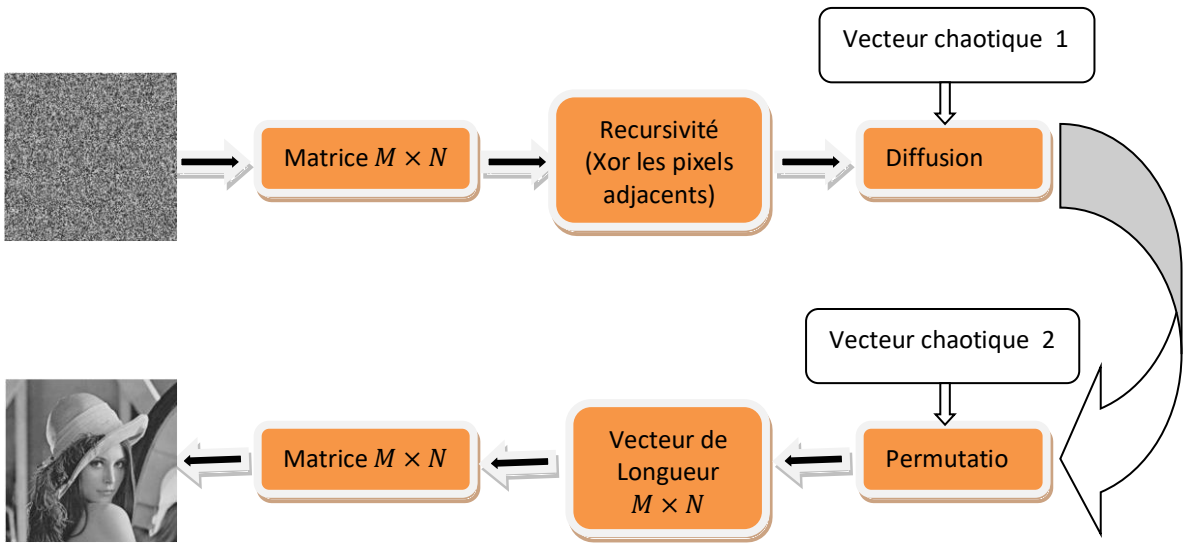


Figure (3.5) Schéma de décryptage proposé.

3.7.4 Algorithme de décryptage

Il fait exactement le travail inverse de l'algorithme de cryptage

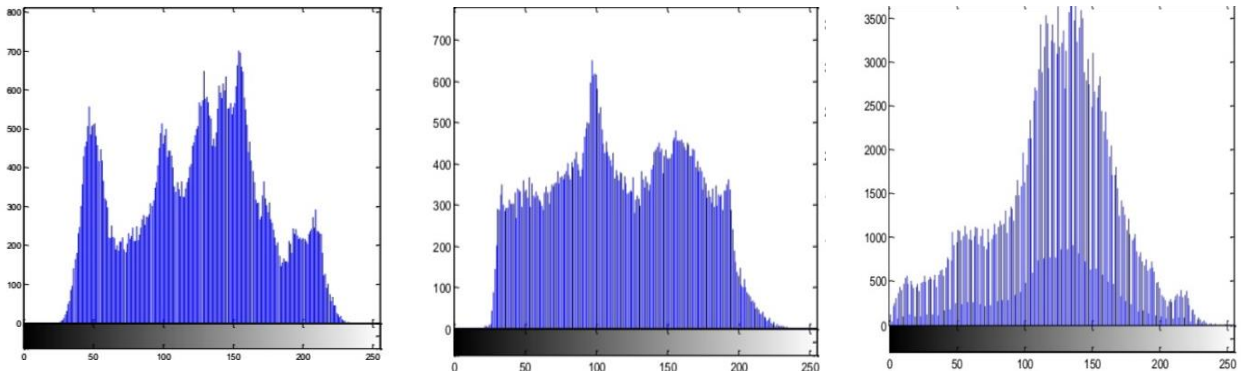
3.8 Résultats de simulation et comparaison

Afin de démontrer l'efficacité de la méthode de cryptage d'image proposée, nous présentons dans cette partie quelques résultats de simulation en considérant des images de test standard Lena (256×256), Barbara(256×256), et Baboon de taille (256×256). Nous avons effectué notre travail sous environnement Matlab R2014a , comme nous avons pris aussi les paramètres chaotiques suivants : $(x_0 = 0.28, r_0 = 10, x_1 = 0.52, r_1 = 20,)$

3.8.1 Analyse d'histogrammes

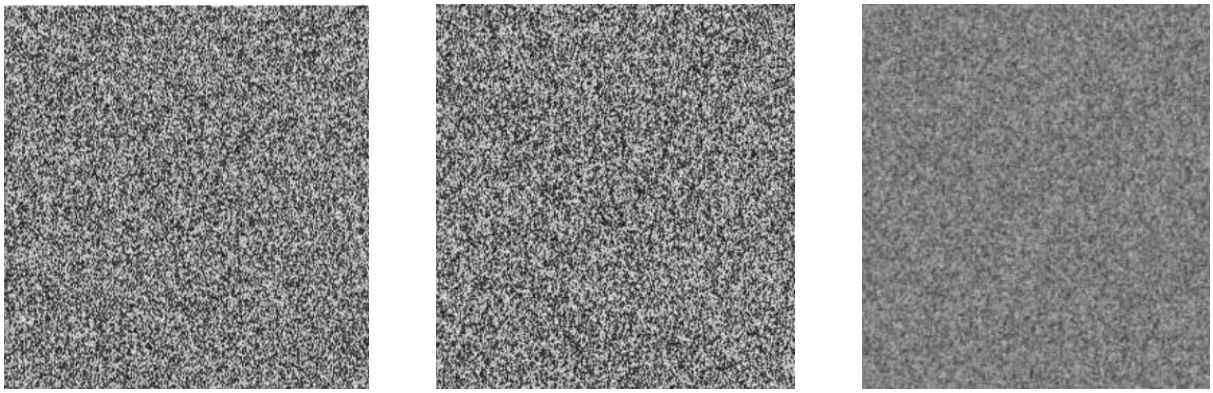
Trois images de tests ont été utilisées dans l'analyse : Lena, Barbara et Living-room. Les tracés des histogrammes des images et les images chiffrées ainsi que leurs histogrammes correspondants sont illustrés dans les figures *Figure (3.6) et Figure (3.7).*

(a)

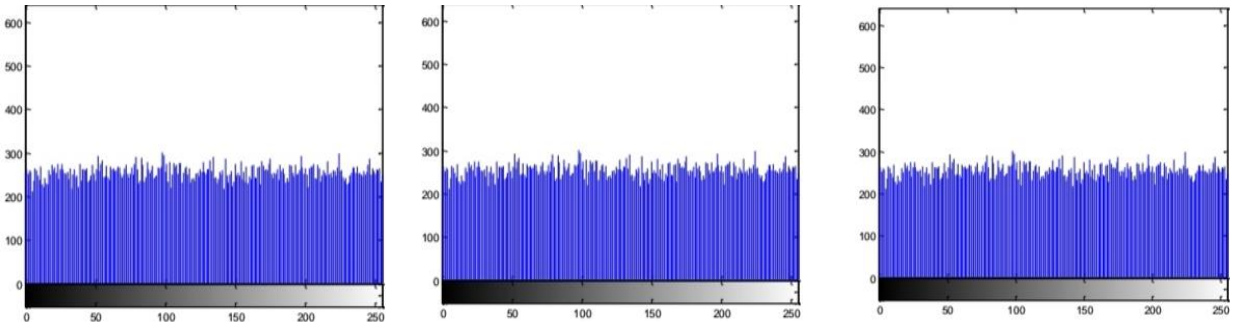


(b)

Figure (3.6) Images originales de test et leurs histogrammes correspondants.



(c)

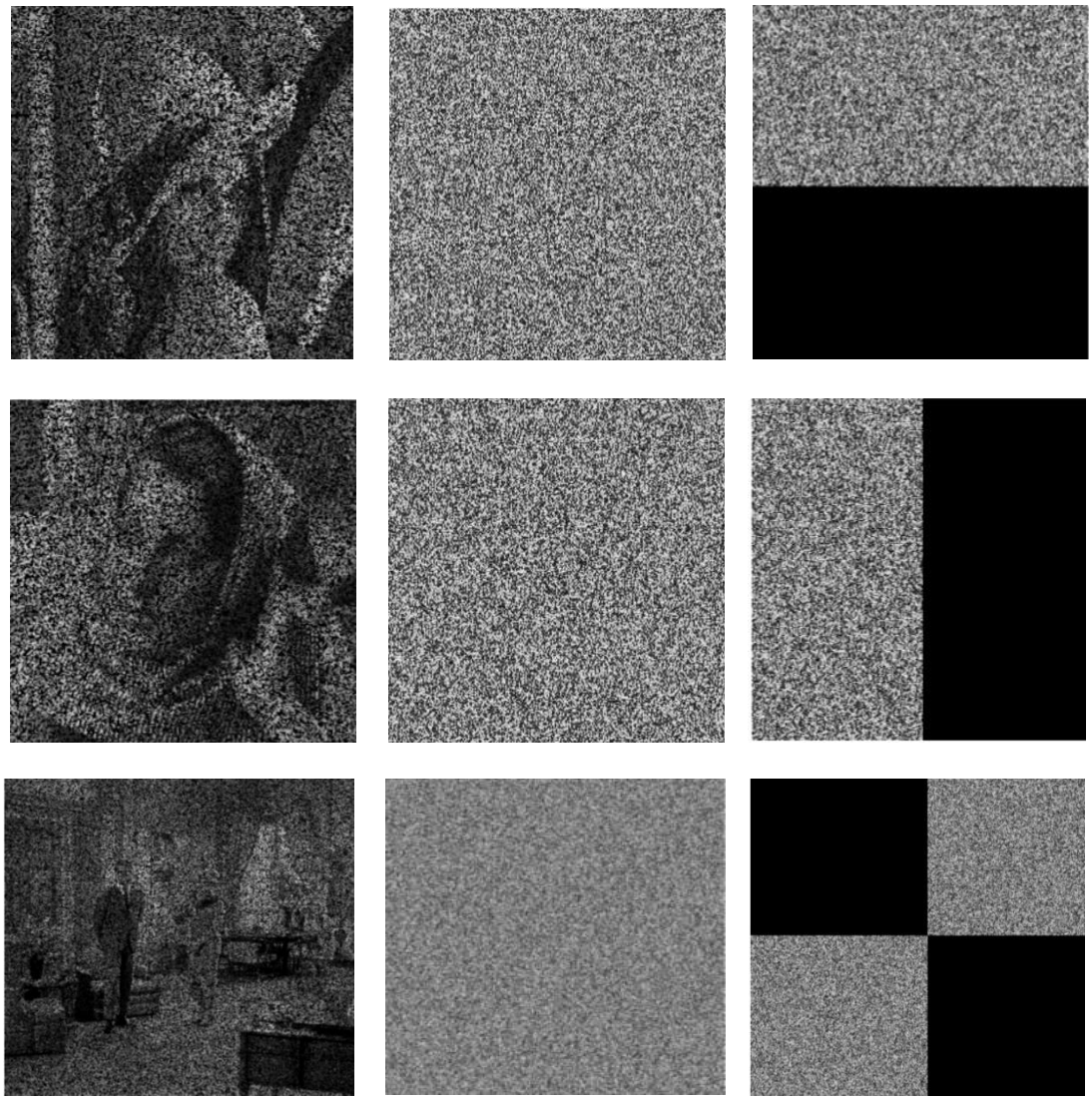


(d)

Figure (3.7) Images cryptées de Lena, Barbara et Living room et leurs histogrammes correspondants.

Nous remarquons sur *Figure (3.7)*, *Figure (3.6* qu'en partant d'histogrammes différents pour des images originales différentes de Lena, Barbara et Living room, nous retrouvons les mêmes histogrammes de leurs images cryptées qui ressemblent à un bruit blanc uniforme, cela confirme que la méthode de cryptage ramène toutes les images originales à des images cryptées ayant les mêmes histogrammes , ce qui empêche les attaquants d'en tirer la moindre information qui pourra révéler l'opération de cryptage et par conséquent, nous pouvons conclure que notre approche résiste aux attaques par l'analyse d'histogrammes.

3.9 Resistance aux pertes des données (Loss data)



(a) (b) (c)

Figure (3. 8): Illustration du test de pertes de données : (a) Images décryptées de Lena, Barbara et Living-room correspondantes (b) Images cryptées de Lena, Barbara et Living-room (c) Leurs images cryptées avec des pertes de données de 50% de Lena, Barbara et Living-room.

Pour tester la résistance de la méthode de cryptage proposé face à l'une des erreurs qui peuvent survenir dans le canal de transmission, telle que la perte des données ou (Loss data), nous considérons le cas où une partie des pixels de l'image cryptée a été perdue au cours de la transmission. D'après les

résultats de simulation illustrés dans la figure 4, Nous remarquons que suite aux différents pourcentages de pertes des donnés atteignant l''image cryptée allant jusqu'a un pourcentage de (50%), l'information sur l'image décryptée n'est pas éliminée totalement, en effet l'image décryptée reste visible et identifiable à l'œil nu malgré qu'elle est bruitée. En conséquence, ces résultats prouvent la robustesse de la méthode proposée vis-à vis du test Loss data et démontre sa résistance face aux erreurs de transmission.

3.10 Sensibilité de la clé

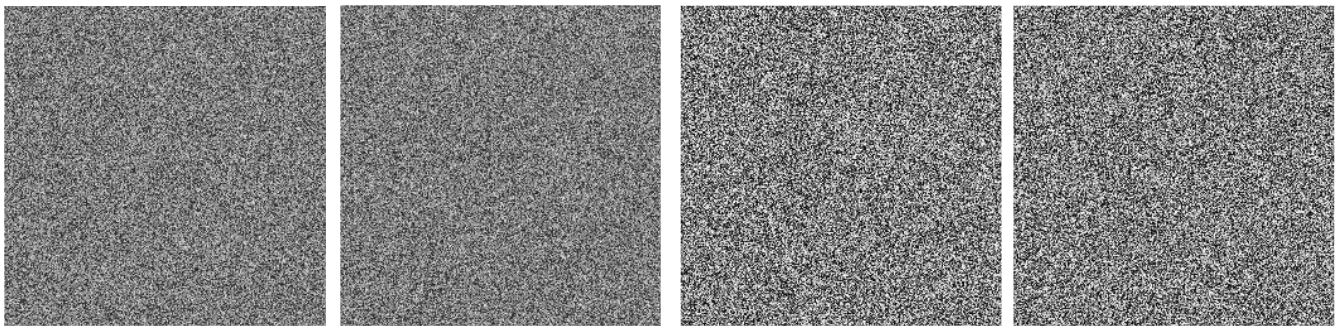
Tout algorithme de cryptage doit être extrêmement sensible au changement de la clé secrète et cela pour garantir la sécurité de la clé contre les attaques par force brute. La sensibilité de la clé d'un crypto système peut être observée par deux méthodes différentes :

1- L'image cryptée doit être très sensible à la clé secrète ; si on utilise deux clés légèrement différentes pour crypter la même image, alors les deux images cryptées doivent être complètement indépendantes l'une par rapport à l'autre (faible corrélation).

2- L'image cryptée ne peut pas être décryptée correctement si la clé secrète est légèrement modifiée à la phase de décryptage

Pour estimer la sensibilité de la clé secrète de l'algorithme proposé, nous supposons que la clé de cryptage k est composée des paramètres des deux suites chaotiques $k(x_0, r_0\,,\ x_1\,,\ r_1\,)$ et la clé de décryptage $k(x_0{}', r_0{}'\,,\ x_1{}'\,,\ r_1{}'\,)$. Pour retrouver l'image originale lors de la phase de décryptage il faut que la clé de cryptage soit égale à la clé de décryptage $k(x_0, r_0\,,\ x_1\,,\ r_1\,) = k(x_0{}', r_0{}'\,,\ x_1{}'\,,\ r_1{}'\,)$. Càd $(x_{0=}x_1{}', r_0 = r_0{}',\ x_1 = x_1{}'\ et\ r_1 = r_1{}')$ cas de la ***Figure (3.9.e).*** Dans ce qui suit nous gardons les mêmes égalités et nous opérons un léger changement dans le premier paramètre $(x_0 + 10^{-15}{}_{=}x_1{}', r_0 = r_0{}',\ x_1 = x_1{}'\ et\ r_1 = r_1{}')$, nous allons voir que l'apparition de l'image décryptée en claire sera à $x_0 + 10^{-16}$, et au dessous de cette valeur l'image apparue décryptée, donc la précision est de l'ordre de 10^{+15}. Cette opération est répétée pour les quatre paramètres à tour de rôle et les résultats de simulation sont bien illustrés dans la *figure (3.9)*.

Nous concluons que les images cryptées par notre algorithme ont une extrême sensibilité à la clé secrète et n'est pas vulnérable aux attaques par force brute.



a *b* *c* *d*

e

Figure (3.9): Image décryptée de Lena avec (a) $x_0'=x_0+10^{-15}$; (b) $r_0'=r_0+10^{-15}$; (c) $x_1'=x_1+10^{-15}$; (d) $r_1'=r_1+10^{-15}$. e) $k = k'$

Les paramètres initiaux sont : $(x_0 = 0.28, r_0 = 10, x_1 = 0.52, r_1 = 20,)$

3.11 Espace de clés

Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espace clé doit être suffisamment grand pour rendre les attaques de force brute impossibles, et la taille de la clé peut être plus longue que la taille de l'image. Dans la technique de cryptage proposée, l'espace de clés est le nombre total de clés différentes utilisées dans la procédure composée et la taille de l'espace clé est : $clé = 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{60}$

$$10 \cong 2^3$$

Donc : $(2^3)^{60} \cong 2^{180}$

Donc $2^{180} > 2^{100}$

Ce qui est supérieur à 2^{100} proclamé dans les systèmes cryptographiques

3.12 Conclusion

Les simulations et les évaluations de performance ont montré que le système proposé est capable de produire un système chaotique avec meilleures performances et des plages chaotiques plus étendues par rapport aux cartes chaotiques classiques. Par la suite, nous avons appliqué notre algorithme déjà proposé dans le chapitre précédant pour confirmer ses applications dans le cryptage des images. Des expériences et des analyses de sécurité ont prouvé que l'algorithme offrait d'excellentes performances en matière de cryptage d'image et d'attaques diverses.

Conclusion Générale

Ce n'est un secret pour personne que la cryptographie basée sur le fouillis a connu un développement majeur ces derniers temps, car la plupart des recherches ont été effectuées sur l'utilisation du fouillis dans les systèmes cryptographiques pour améliorer le temps de chiffrement, la sensibilité du chiffrement des clés de sécurité et tout ce qui concerne la cryptographie par le chaos.

À travers notre travail, nous nous sommes concentrés sur le cryptage des images incolores, afin d'améliorer et de connaître la force de la clé de sécurité, et si elle résiste aux diverses attaques et piratages auxquels elle peut être exposée.

Les résultats expérimentaux que nous avons obtenus ont montré que l'algorithme proposé offre un bon niveau de sécurité. Cela rend une attaque par force brute peu pratique. Ainsi, l'histogramme de l'image cryptée est si uniforme après le cryptage que même un attaquant ne peut pas extraire d'informations de l'histogramme de l'image cryptée. Par conséquent, l'algorithme proposé démontre l'efficacité et la sécurité de notre système proposé.

[1] L. Grazide, L'image électronique,
http://auch2.free.fr/Documents/Informatique/Image_electronique.pdf,.

[2] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition, Pearson Prentice Hall, Upper Saddle River, 2007.

[3] Numeriksciences, http://numeriksciences.fr

[4]- Reenu Batra and Kanishka Raheja" Encryption of Image by Different Techniques: A Survey" February 28, 2019

& CNRS, https://clouard.users.greyc.fr/fetedelascience/documents/image.pdf ,

[5] R. Isdant, Traitement numérique de l'image, 2009, http://raphael.isdant.free.fr/traitement_numerique/2-traitement_numerique_de_l%27image.pdf,.

[6] Léon Robichaud, L'image numérique Pixels et couleurs, support de cours, Département d'histoire, Université de Sherbrooke.

[7] Les formats d'images numériques, Serge WACKER – C2I niveau 1,

http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_image.pdf ,

[8]- Dr .. Turki bin Mohammed bin Abdullah Al-Suraihid" Un aperçu simplifié de la cryptographie " king saoud university. https://fac.ksu.edu.sa/talsuraiheed/blog/24201

[9]-Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology. p. 1. Archived (PDF) from the original on 5 March 2013. Retrieved

[10] Mme L. SAOUDI, initiation à la cryptographie, support de cours du module Sécurité informatique, Département d'informatique, université de Msila, Année 2015/2016.

[11] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.

[12]-Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). *Federal Information Processing Standards Publication 197*. United States National Institute of Standards and Technology (NIST). November 26, 2001. Archived (PDF) from the original on March 12, 2017. Retrieved October 2, 2012

[13]- Dover Publications, New York, NY, 1958 *The Principles of Science: A Treatise on Logic and Scientific Method* p. 141

[14]- *Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone (October 1996)*

"*Handbook of Applied Cryptography*". 0-8493-8523-7
[15]- Stallings, William (1999-01-01). *Cryptography and Network Security: Principles and Practice* p 164 Le 23 mars 2019

[16] 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.

[17] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone, Handbook of applied cryptography, CRC press, 1996.

[18] A. Walker, E. Wolfart, R. Fisher, S. Perkins, Image processing learning resources explore with java, http://homepages.inf.ed.ac.uk/rbf/HIPR2/hipr_top.

[19]- "Dr Clifford Cocks CB". Bristol University. Smart, Nigel (February 19, 2008). Retrieved August 14, 2011.

[21]- Diffie, W.; Hellman, M.E. (November 1976). "New directions in cryptography". *P* 644–654

[22] Claude E Shannon, A mathematical theory of communication, ACM SIGMOBILE Mobile Computing and Communications Review, 5(1) :3–55, 2001.

[23] Wikipédia, https://fr.wikipedia.org/wiki/Entropie_de_Shannon,

[24] Mme L. SAOUDI, initiation à la cryptographie, support de cours du module Sécurité informatique, Département d'informatique, université de Msila, Année 2015/2016.

[25] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.

[26] Wikipédia, https://fr.wikipedia.org/wiki/Confusion_et_diffusion,.

[27] Wikipédia, https://fr.wikipedia.org/wiki/Chiffrement_par_transposition,

[28] T. Hamaizia, Systèmes Dynamiques et Chaos "Application à l'optimisation a l'aide d'algorithme chaotique", These pour obtenir le titre de Docteur en Sciences de l'Université de Constantine 1, 2013.

[29] S. BELKACEM, Chaos based image water marking , These Présentée pour l'obtention du diplôme de DOCTORAT en Science en Electronique, université de Batna 2.

[30] T. Hamaizia,« Systèmes dynamiques et chaos »,Thèse Doctorat ,Université de Constantine 1,2013

[31] H.Hamiche,« Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données »,Thèse Doctorat ,Université Mouloud Mammeri Tizi Ouzou,2011.

[32] C.Benhabib, Etude d'un système chaotique pour la sécurisation des communications boptiques , mémoire , université de tlemcen faculte de technologie , 2014.

[33] S.Kassim,«contribution a la transmission numérique sécurisée de données a base de générateurs de séquences chaotiques d'ordre non entier»,Thèse Doctorat ,Université Mouloud Mammeri Tizi Ouzou,2018.

[34] G. Qi, S. Du, G. Chen, Z. Chen and Z. Yuan, "On a four-dimensional chaotic system," Chaos, Solution and Fractals, Vol. 23, pp. 1671-1682, 2005.

[35] K. Mesbah, "Etude des systèmes dynamiques chaotiques," Thèse de magistère, Université de Constantine, 2005.

[36] H. F. V. Bremen, F. E. Udwadia and W. Proskurowski, "An efficient QR based method for the computation of Lyapunov exponents," Phys. D. 101, pp. 1-16, 1997.

[37] A. Wolf, J.B. Swift, H.L. Swinney and J.A. Vastano, "Determining Lyapunov exponentsfrom a time series," Physica, D. 16, pp. 285-317, 1985.

[38] A.Adane , L. Bourahmoune,«Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire »,Mémoire de Master ,Université Mouloud Mammeri Tizi Ouzou,2015.

[39] O .Megherbi,« Étude et réalisation d'un systèmes sécurisé à base de systèmes

chaotiques»,Mémoire de Magister ,Université Mouloud Mammeri Tizi Ouzou ,2013.

[40] Z. Elhadj «Étude de quelques types des systèmes chaotiques :Généralisation d'un modèle issu du modèle de Chen»,Thèse Doctorat ,Université Mentourid de Constantine Faculté de Sciences,2006.

[41] G.DA Silva, «Introduction aux systèmes dynamiques et chaos»,Engineering school. Institut Polytechnique de Grenoble, 2004, pp.23. <cel-00556972>

.[42] D.E. Goumidi, Fonction logistique et standard chaotique pour le chiffrement des images satellitaires, Mémoire Présenté pour l'obtention du diplôme de Magister, école doctorale en Electronique Spécialité, 2010.

[43]. H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complement aryrule and chaotic maps," Appl. Soft Comput. J., Vol. 12, no. 5, pp. 1457–1466, 1457–1466, 2012

[44]. A. Baranovsky, and D. Daems, "Design of one-dimensional chaotic map swithpre scribed statistical Properties," International Journal of Bifurcation and Chaos, Vol. 5, no. 6, pp. 1585–1598, 1995

[45]. H. Zhou, and X. Ling, "Generating chaotic secure sequences with desired statistical properties and high security," Int. J. Bifurc. Chaos., vol. 7, pp. 205–213, 1997.

[46]. G. Alvarez and al., "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcat. Chaos., Vol. 16, no. 8, pp. 2129–2151, 2006.

[47]. L. Kocarevand, and S. Lian, "Chaos-Based Cryptography - Theory, Algorithms and Applications," Springer-Verlag Berlin Heidelberg, 2011.

[48] Y. Naseer, D. Shah and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed

Chaotic map'', Microprocessors and Microsystems, Vol.65 pp. 1–6, 2019.

[49] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyperchaos' Phys. Lett. A, Vol. 38, pp. 5973–5978, 2018.

[50] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image

encryption'', Optics and Laser Technology, Vol.101, pp.30–41, 2018.

[51] Ch. Pak, K. An, P. Jang, J. Kim and S. Kim , "A novel bit-level color image encryption using improved 1D chaotic map'', Multimedia Tools and Applications, Vol. 78, pp. 12027–12042, 2018.