الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED SEDDIK BENYAHIA JIJEL

Faculté des Sciences et de la Technologie

Département de l'Electronique

N° :……/2022

MEMOIRE DE MASTER

DOMAINE : Sciences et Technologies

FILIERE : Télécommunications

SPECIALITE : Systèmes de télécommunications

Thème

Transmission sécurisée de données par systèmes hyperchaotiques

Présenté Par :

Haider ATAMNA

Kamel ATAMNA

Encadré Par :

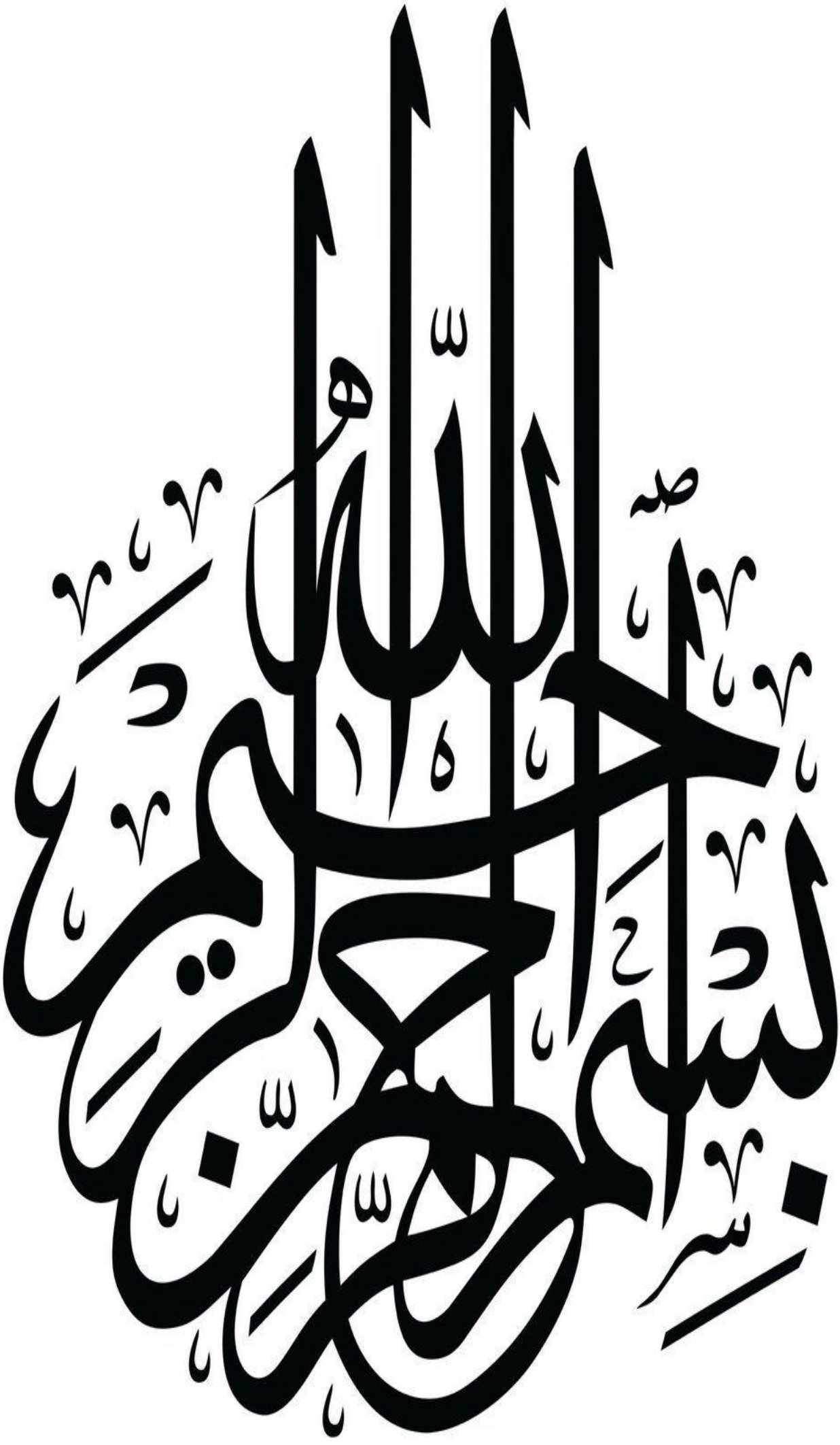
Dr. Morad GRIMES

Date de soutenance : 13/07/2022

Jury de Soutenance

Président : Samira DIB	**Grade : MCB**	**Univ MSB Jijel**
Encadreur : Morad GRIMES	**Grade : MCA**	**Univ MSB Jijel**
Examinateur : Fayçal BOUKERROUM	**Grade : MCA**	**Univ MSB Jijel**

Promotion : 2021 /2022


بسم الله الرحمن الرحيم

Remerciements

*Nous Remercions Avant Tout DIEU **ALLAH** Tout Puissant Et Miséricordieux Pour La Volonté, Le Courage Et La Patience Qu'Il Nous A Donnés Afin De Réaliser Ce Modeste Travail.*

*Nous Exprimons Notre Plus Grande Gratitude Et Notre Respect à Notre Encadreur Mr **GRIMES Morad**, Pour Tous Ses Judicieux Conseils, Son Temps Qu'il Nous a Consacré Et Pour nous avoir guidé et soutenu avec patience et indulgence,*

Notre Remerciement S'étend Aussi Aux Membres Du Jury D'avoir Accepté d'examiner et de juger notre travail.

Dédicaces

À NOS PARENTS,

À NOS FAMILLES,

À NOS AMIS,

À NOTRE FRERE FAROUK,

À TOUS CEUX QUE NOUS AIMONS

ET CEUX QUI NOUS AIMENT.

Résumé

Dans ce mémoire, on s'intéresse à la sécurisation de données par les systèmes chaotiques et hyperchaotiques en raison des propriétés de ces systèmes, telles que leur sensibilité aux conditions initiales et leurs trajectoires qui sont considérées comme bruit pseudo-aléatoire. Pour le cas des systèmes chaotiques nous avons utilisé le système continu de Lorenz et la carte logistique pour chiffrer des images numériques. Une nouvelle méthode de chiffrement a été proposée, elle est basée sur un système hyperchaotique 6D, la matrice Q de Fibonacci et la fonction Cat map. Les résultats obtenus ont démontré l'efficacité de la méthode proposée.

Mots clés : systèmes chaotique, systèmes hyperchaotiques, cryptage, carte logistique.

ملخص

في هذه المذكرة، نهتم بتأمين المعلومات باستخدام الأنظمة الفوضوية والأنظمة عالية الفوضوية نظرا لخصائص هذه الأنظمة مثل الحساسية للشروط الابتدائية ومساراتها التي تعتبر ضجيجا شبه عشوائي. بالنسبة للأنظمة الفوضوية استخدمنا نظام لورينز المستمر والخريطة اللوجستية المنفصلة لتشفير الصور الرقمية. لقد قمنا باقتراح طريقة جديدة للتشفير مبنية على الأنظمة عالية الفوضوية سداسية الابعاد و متتالية فيبوناتشي و دالة Cat map.

أظهرت النتائج المتحصل عليها فعالية الطريقة المقترحة.

الكلمات المفتاحية: الأنظمة الفوضوية، الأنظمة عالية الفوضوية، التشفير، الخريطة اللوجستية.

Abstract

In this thesis, we are interested in securing data by chaotic and hyperchaotic systems because of their properties, such as the sensitivity to initial conditions and their trajectories considered as pseudo-random noise. In the case of chaotic systems, we used Lorenz's continuous system and the discrete logistic map to encrypt numerical images. A new method for encryption was proposed it based on the 6D hyperchaotic system, the Q-matrix of Fibonacci and the function Cat map.

The obtained results show the effectiveness of the proposed method.

Keywords : chaotic systems, hyperchaotic systems, encryption, logistic map.

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des tableaux

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Acronymes

AES	Advanced Encryption Standard
BRIE	Bit Recirculation Image Encryption
CKBA	Chaotic Key-Based Algorithm
CNNSE	Chaotic Neural Network for Signal Encryption
DES	Data Encryption Standard
DH	Diffie-Hellman
DSEA	Domino Signal Encryption Algorithm
ELTM	Enhanced Logistic-Tent Map
HCIE	Hierarchic Chaotic Image Encryption
IDEA	International Data Encryption Algorithm
MSE	Mean Squared error
NMR	Nuclear Magnetic Resonance
PRNG	Générateur de Nombres Pseudo-Aléatoires
PSNR	Peak Signal to Noise Ratio
RSA	Nommé par les initiales de ses trois inventeurs (**R**ivest, **S**hamir et **A**dleman)
TV	Télévision
XOR	Exclusive OR
1D	Unidimensionnel
2D	Bidimensionnel
3D	Tridimensionnel
4D	Quatre Dimensions
6D	Six Dimensions

Table des matières

Chapitre 2 : Systèmes chaotiques et hyperchaotiques

Chapitre 3 : Sécurisation par les systèmes chaotiques

Chapitre 4 : Sécurisation par les systèmes hyperchaotiques

Introduction générale

Ces dix dernières années ont été marquées par une révolution des systèmes de communications grâce au développement de la technologie de l'information avec l'avènement de l'Internet, les communications sans fil, et par satellite. Cette révolution a permis un échange facile des millions de kilo-octets d'informations. Reste qu'avec ces flux de données confidentielles sont transmises via des canaux de communication non sécurisés, et l'information peut à tout moment être interceptée par des individus indésirables.

En effet, la cryptographie joue un rôle capital et le recours aux techniques de cryptage ou de chiffrement pour protéger les données devient incontournable.

La cryptographie est l'art et la science de protection d'une information ou d'un message secret, et ce en brouillant son allure ou sa structure de manière à la rendre insignifiante et incompréhensible aux yeux de personnes non autorisées à connaître son contenu. Diverses approches et algorithmes ont été élaborés et mis en œuvre pour chiffrer et sécuriser les données. On peut citer, entre autres, les algorithmes de chiffrement symétriques et asymétriques. En traitement d'images, l'application de tels algorithmes engendrera un temps de calcul élevé et une implémentation coûteuse. La recherche d'une solution alternative pour sécuriser l'envoi de tels types de données devient alors nécessaire et la théorie du chaos représente, à cet effet, une alternative intéressante.

Le chaos trouve ses fondements dans l'article de Lorenz, où il a connu un développement mathématique dans les années 70 suivi d'un véritable essor scientifique. Le chaos est obtenu à partir de systèmes non linéaires. Il correspond à un comportement borné de ces systèmes ayant l'apparence d'un bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée. L'une des propriétés des systèmes chaotiques est qu'ils présentent une sensibilité aux conditions initiales ; Cela signifie que si l'on modifie légèrement un paramètre d'une équation ou d'un système, un comportement différent peut se produire et c'est ce qui fait leurs forces et qui satisfait certaines exigences des systèmes cryptographiques. Depuis, de nombreux algorithmes de cryptage, fondés sur les propriétés des systèmes chaotiques, ont été proposés. Lorsqu'on évoque le cryptage ou chiffrement de données à base du chaos, il s'agit, en effet, de dissimuler un signal message en le noyant dans un signal chaotique à travers plusieurs étapes et combinaisons successives. Les paramètres du système chaotique utilisé constituent alors les clés de chiffrement secrètes.

Introduction générale

Les travaux réalisés dans ce manuscrit s'inscrivent pleinement dans le contexte de chiffrement des images. L'objectif principal de ce travail est de proposer une méthode de cryptage des images basée sur un système hyperchaotique. La robustesse et l'efficacité de la méthode proposée sont évaluées à l'aide des attaques cryptographiques couramment utilisées, notamment les attaques statistiques et les attaques par analyses différentielles. En effet, les résultats obtenus montrent bien que la méthode proposée peut sécuriser efficacement les images numériques.

De ce fait et dans le but de contribuer à la sécurité des images numériques, nous avons réalisé ce modeste travail qui s'articule sur quatre chapitres :

Le premier aborde des généralités sur la cryptographie. Nous présentons des notions de la cryptographie et des services qu'elle offre puis nous faisons une comparaison entre la cryptographie symétrique et la cryptographie asymétrique.

Le deuxième chapitre est consacré aux systèmes dynamiques, chaotiques et hyperchaotiques. Nous allons présenter les caractéristiques du chaos et leurs propriétés. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle.

Le troisième chapitre est consacré à la simulation et à l'implémentation de deux systèmes chaotiques utilisant le système continu de Lorenz et la carte logistique. L'évaluation de ces deux systèmes est faite moyennant des critères statistique et différentielle.

Dans le quatrième chapitre, tout d'abord nous présentons un algorithme de chiffrement et déchiffrement des images utilisant un système hyperchaotique à 6D et la matrice Q de Fibonacci, ensuite nous proposons une nouvelle méthode de chiffrement en ajoutons la fonction Cat map d'Arnold à l'algorithme de chiffrement. L'interprétation et une étude d'évaluation sont faites pour tester les performances de la méthode proposée vis-à-vis des attaques fréquentes.

Enfin, nous terminons ce travail par une conclusion générale et quelques perspectives ouvertes pouvant être envisagées comme suite à notre travail.

Chapitre 1

Généralités sur la cryptographie

1. Introduction

La confidentialité est une nécessité essentielle pour la transmission sécurisée de données sensibles. Le cryptage est l'un de ses outils de sécurisation pour protéger l'information contre les attaques indésirables en la convertissant en une forme, méconnaissable par ses attaquants. Le but du cryptage est de fournir un moyen facile et peu coûteux de chiffrement et de déchiffrement à tous les utilisateurs autorisés en possession de la clé appropriée et inversement à tous les autres utilisateurs sans l'utilisation de la clé. L'inverse du chiffrement des données est le déchiffrement des données, qui récupère les données originales. Selon le type de texte en clair, les systèmes de chiffrement de données sont classés comme le chiffrement de texte, le chiffrement audio, le chiffrement d'image et le chiffrement vidéo [1].

Dans ce chapitre, nous présentons en particulier les termes utilisés et les notions de base de la cryptologie en plus des classes et des différents algorithmes de cryptographie. Enfin, quelques notions sur la cryptanalyse.

2. Définitions et terminologies

En raison de l'utilisation des termes prises de l'anglais, il existe souvent une certaine confusion concernant les différents termes de cryptographie. Par conséquent, nous définirons les termes qui seront utilisés tout au long de ce travail pour éviter toute ambiguïté [2,4] :

- **Texte en clair (plaintext) :** des données intelligibles et compréhensibles à protégés.
- **Texte chiffré (ciphertext, cryptogramme) :** le résultat du chiffrement du texte en clair.
- **Chiffrer/Chiffrement :** la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré à l'aide d'une convention secrète, appelée clé.
- **Déchiffrer/Déchiffrement :** c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair, en utilisant la convention secrète de chiffrement.
- **Clé :** paramètre d'un algorithme de chiffrement ou déchiffrement, sur lequel repose le secret. On distingue deux types de clés : secrète et publique.
- **Cryptologie :** la science du secret. Elle réunit la cryptographie et la cryptanalyse.
- **Cryptographie :** la science qui utilise les mathématiques pour chiffrer, crypter, coder et déchiffrer des données.

- **Cryptanalyse :** la science qui consiste à analyser le texte chiffré pour obtenir le texte en clair sans connaître la clé. La réussite d'une cryptanalyse peut fournir soit le texte en clair, soit la clé. Un essai de cryptanalyse est appelé attaque.
- **Attaque :** n'importe quelle action qui a le but de menacer la sécurité des données
- **Cryptosystème :** l'ensemble des deux méthodes de chiffrement et de déchiffrement.
- **Algorithme cryptographique** : l'ensemble des fonctions utilisées pour le chiffrement et le déchiffrement.
- **Décrypter :** retrouver l'information intelligible, à partir de l'information chiffrée sans utilisation de la convention secrète de chiffrement. Ce terme ne doit être utilisé que dans le contexte de la cryptanalyse.

2.1. Cryptographie

La cryptographie est l'art de l'écriture secrète qui utilise les mathématiques pour chiffrer et déchiffrer les données. Elle vient des mots grecs Krypto (caché ou secret) et graphein (écriture). La cryptographie est une méthode de transmission ou stockage des données sensibles sur des réseaux non sécurisés (comme l'internet) sous une forme particulière à utiliser uniquement par le destinataire pour les lire et les traiter [5].

2.1.1 Algorithme cryptographique

Un algorithme cryptographique est une fonction mathématique utilisée pour le chiffrement et le déchiffrement. Jusqu'aux années 1970, les algorithmes de cryptographie utilisés consistaient à enchaîner des permutations et des substitutions sur des ensembles de petite cardinalité. C'est ce qui est connu aujourd'hui sous le nom de la *cryptographie classique*. Les algorithmes de chiffrement actuels reposent sur des résultats en algèbre *(étude des corps de nombres, courbes elliptiques, chaos, etc.)* et sur des problèmes algorithmiquement difficiles comme la décomposition d'un nombre entier en facteurs premiers [3].

La philosophie de la cryptographie moderne peut être résumée par les principes de *Kerckhoffs 1883*. "La sécurité d'un cryptosystème ne doit pas dépendre du secret de l'algorithme, mais uniquement du secret de la clé. Les principes fondamentaux des algorithmes cryptographiques reposent sur deux concepts de base que Shannon a déclaré :

a) **La confusion :** vise à rendre le texte le plus illisible possible. Ceci peut se faire par une substitution systématique de symboles, ou par un algorithme de codage aussi complexe que l'on veut.

b) **La diffusion :** vise à faire en sorte que chaque élément d'information en texte chiffré dépende d'autant d'informations en texte en clair que possible. Cela rend la découverte de l'algorithme ou de la clé de cet algorithme plus difficile.

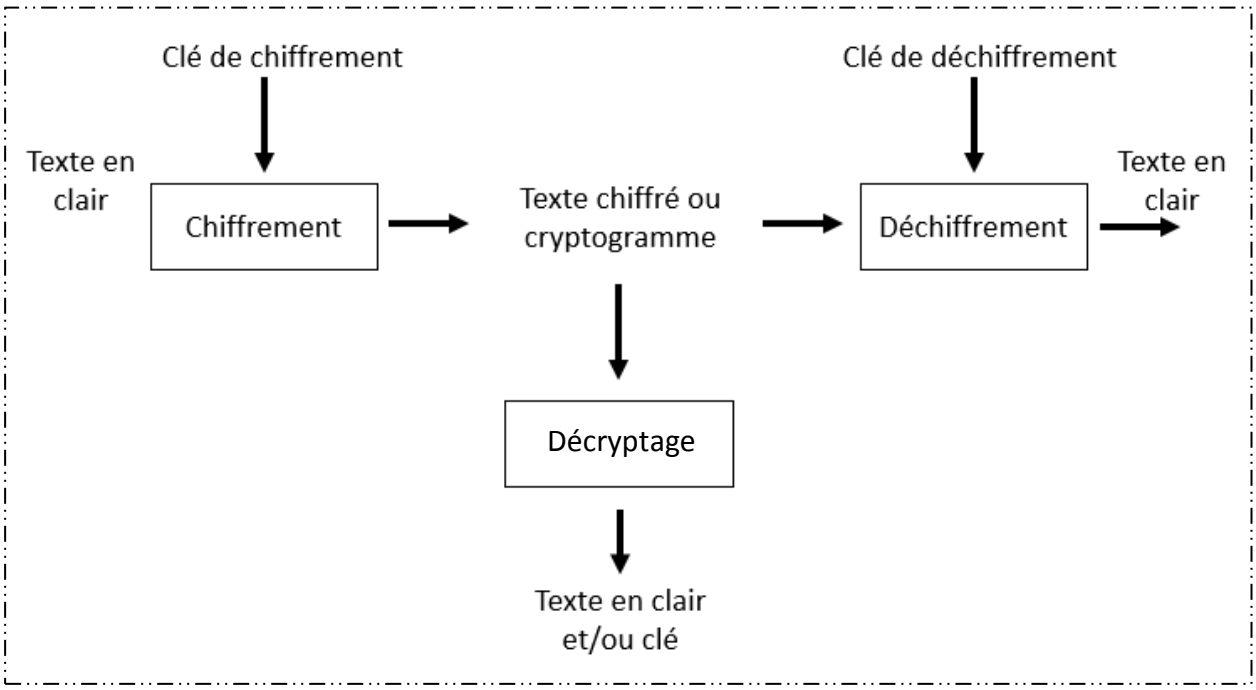


Figure 1.1 : Chiffrement et déchiffrement avec une clé.

3. Objectifs de la cryptographie

Le but fondamental de la cryptographie est d'atteindre les exigences de sécurité pour la transmission d'information, on distingue :

a) **Confidentialité :** assurer que seuls les utilisateurs habilités (autorisés) ont accès à l'information.

b) **Intégrité :** la méthode pour affirmer que le contenu d'une communication ou d'un fichier n'a pas été modifié et aussi que les données échangées sont exactes et complètes.

c) **Authentification :** elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

d) **Disponibilité :** assurer un accès continu aux données et ne peut être bloquées ou perdues.

e) **Auditabilité :** garantir la traçabilité des accès et des essais d'accès et la conservation de ces traces comme preuves exploitables.

f) **Non-répudiation :** elle permet d'assurer qu'un message a bien été envoyé par une source précisée et reçu par un récepteur précisé. Elle permet de garantir qu'un émetteur ou un récepteur ne peut pas plus tard nier faussement qu'il a envoyé ou reçu un message.

4. Classes de la cryptographie

Plusieurs de systèmes de chiffrement ont été imaginés pour défendre contre la curiosité et la malveillance des ennemis depuis des siècles. Ces systèmes peuvent être regroupés en trois catégories principales, comme représentés sur la Figure 1.2.

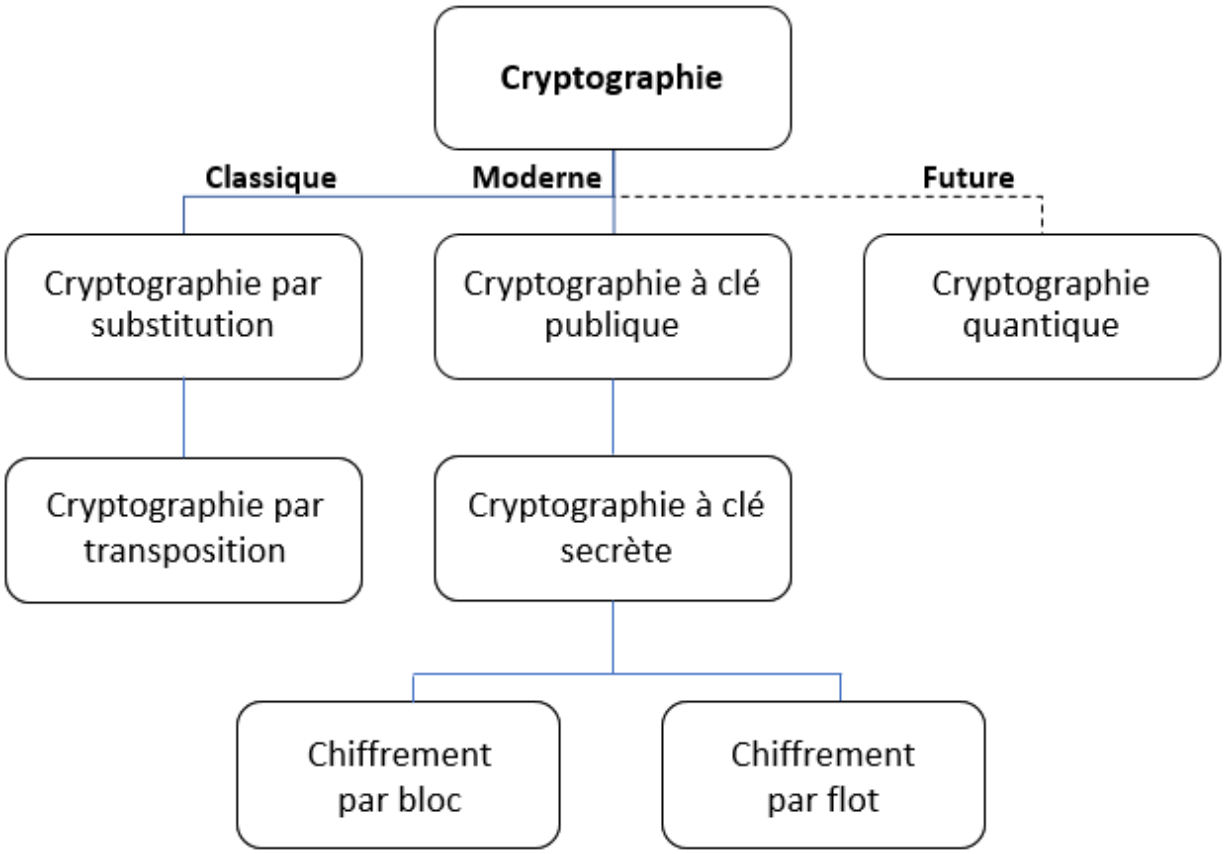


Figure 1.2 : Schéma des classes de la cryptographie.

4.1. Cryptographie classique :

La cryptographie classique décrit la période précédant l'avènement des ordinateurs, durant laquelle, les principaux outils utilisés sont le remplacement de caractères par d'autres et leur transposition dans un ordre différent tout en gardant secret la procédure de cryptage ou

de décryptage. Sans cela le système est complètement inopérant car n'importe qui peut déchiffrer le message chiffré. Ce type de méthode est généralement appelé : le chiffrement à usage restreint, il regroupe deux types de cryptographie [3] :

a) **Cryptographie par Substitution :** consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou nombreuse autre entité. On distingue généralement plusieurs types de cryptosystème par substitution tels que : substitution monoalphabétique, substitution polyalphabétique, substitution homophonique et substitution polygramme.

b) **Cryptographie par transposition :** consiste à modifier l'ordre des éléments d'une information, par exemple l'ordre de pixels d'une image, ce qui permet de les rendre incompréhensibles. Plusieurs types de transposition existent : transposition simple par colonnes et transposition complexe par colonnes.

4.2. Cryptographie moderne

La cryptographie a considérablement évolué avec le développement des ordinateurs, de sorte que les méthodes de chiffrement manuel ont été mises de côté. Malgré ça, les procédés de substitution et de transposition restent toujours d'actualité mais en manipulant, cette fois-ci, des séquences de bits du fait que les ordinateurs ne traitent que des données numériques ce qui rend les techniques de chiffrement actuelles plus sûres, voir même incassables pour certaines techniques, ou du moins prendraient des millions d'années avec la puissance actuelle des meilleurs supercalculateurs. D'autre part, il fait que présentement les algorithmes ne sont plus cachés, mais au contraire sont connus de tous et leur sécurité est liée uniquement aux clés utilisées.

La cryptographie moderne se divise en deux parties nettement particularisées :

- La cryptographie **à clé secrète**, dite également **symétrique.**
- La cryptographie **à clé publique**, ou encore appelée **asymétrique**.

4.2.1. Cryptographie symétrique

Les algorithmes de chiffrement symétriques utilisent la même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette approche est que la clé, qui doit être strictement

confidentielle, doit être transmise de manière sécurisée au correspondant. La mise en œuvre peut être difficile, surtout avec un grand nombre de correspondants, car elle nécessite autant de clés que de correspondants. Il existe deux types de chiffrement symétriques [6,7] :

a) Le chiffrement par bloc (Block cipher)

Les algorithmes de chiffrement par bloc opèrent sur des blocs de données où, le texte en clair est divisé en blocs et fonctionne sur chaque bloc indépendamment. Les tailles de bloc typiques des algorithmes modernes sont de 64 octets, suffisamment petites pour fonctionner mais suffisamment grandes pour dissuader les briseurs de code. Malheureusement, avec la vitesse actuelle des microprocesseurs, casser un algorithme de 64 octets en utilisant la force brute s'avère être une tâche relativement facile.

b) Le chiffrement de flux ou chiffrement par flot (Stream cipher)

Appelé aussi chiffrement en continu, les algorithmes de chiffrement par flot traitent l'information bit à bit, et sont très rapides. Ils sont conçus pour accepter une clé de chiffrement et un flux de texte en clair qui sont utilisés pour produire un flux de texte chiffré. Le chiffrement de flux commence généralement par générateur de nombres pseudo-aléatoires pour effectuer un XOR entre les bits. Ce type de chiffrement est très utilisé dans le contexte de communications téléphoniques.

On distingue quelques algorithmes de chiffrement symétrique très utilisés :

- L'algorithme DES (Data Encryption Standard) ;
- L'algorithme AES (Advanced Encryption Standard) ;
- L'algorithme IDEA (International Data Encryption Algorithm).

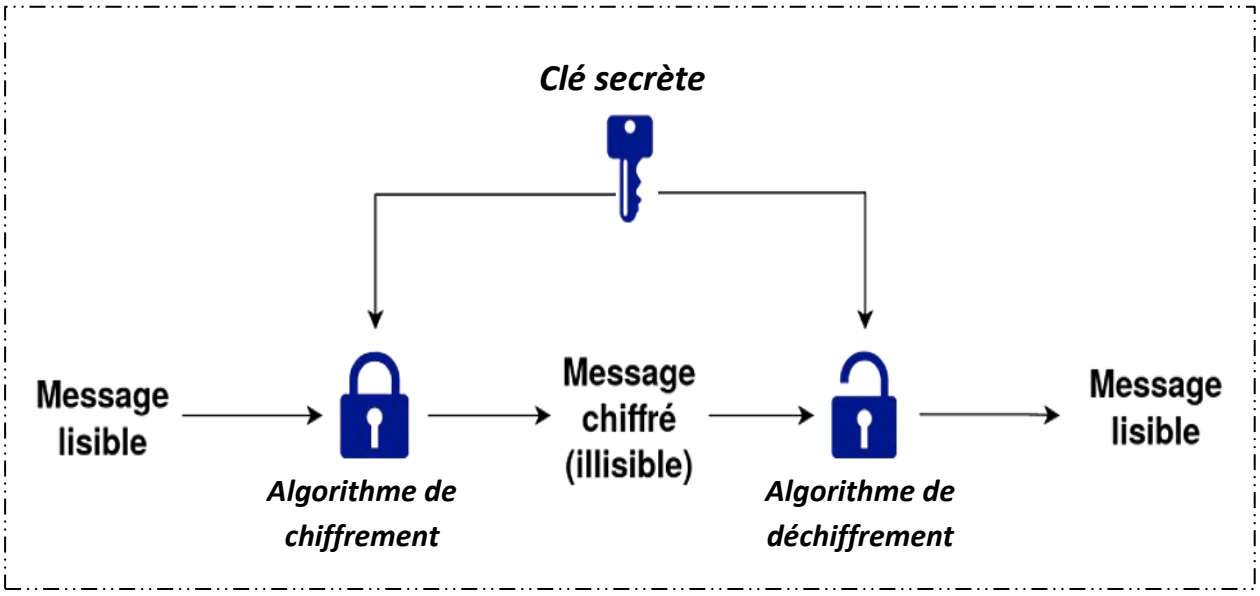


Figure 1.3 : Cryptographie symétrique [8].

4.2.2. Cryptographie asymétrique

Le chiffrement asymétrique utilise deux clés séparées et distinctes, l'une publique, l'autre maintenue secrète. La source peut utiliser la clé publique pour encrypter le message, alors que le destinataire utilisera la clé secrète pour décrypter le message. La clé publique est souvent divulguée sur le réseau afin que tout participant puisse chiffrer mais la clé privée reste en général secrète pour qu'une seule personne (ou machine) puisse déchiffrer le message chiffré. Dans la suite nous citons quelques algorithmes de chiffrement asymétrique les plus utilisés :

- L'algorithme DH (inventé en 1976 par Whitfield **Diffie** et Martin **Hellman**).
- L'algorithme RSA (inventé en 1977 par Ron **Rivest,** Adi **Shamir** et Leonard **Adelman**) ;
- L'algorithme El Gamal (inventé en 1984 par Tahar **ElGAMAL**) ;

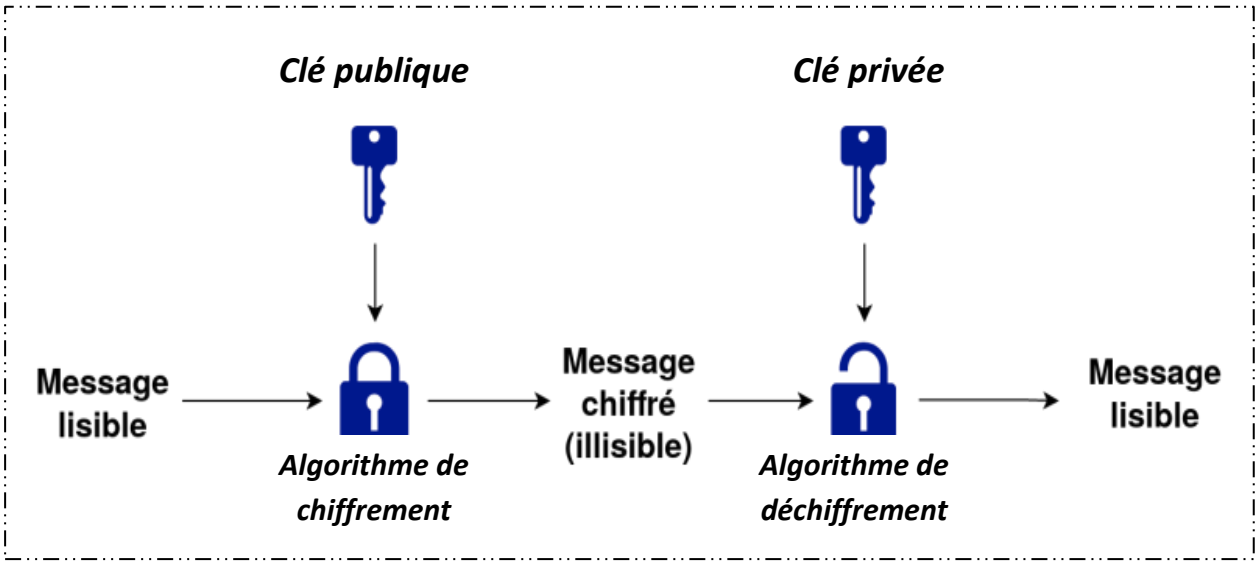


Figure 1.4 : Cryptographie asymétrique [9].

4.3. Cryptographie quantique

Également connu sous le nom de cryptographie à clé inviolable, qui garantit le secret absolu des communications cryptées. La cryptographie quantique, en abrégé BB84, a été développée à partir d'une publication de 1984 par C.H. Bennett et G. Brassard [10]. Plusieurs versions du protocole BB84 sont apparues. Dans le cas le plus simple, on va polariser des photons de valeurs binaires "0" et "1" dont les états de polarisation sont orthogonaux pour coder les données selon deux bases [2] :

- **Base horizontale/verticale :** Les valeurs "0" et "1" correspondent respectivement à des photons de polarisation 0° et 90°.
- **Base diagonale/anti-diagonale :** Les valeurs "0" et "1" correspondent respectivement à des photons de polarisation 45° et 135°.

5. Comparaison entre les cryptosystèmes symétriques et asymétriques

Le tableau ci-dessous présente une comparaison entre les systèmes de chiffrement symétriques et les systèmes de chiffrement asymétriques, en dénombrant les principaux avantages et inconvénients de chaque type de chiffrement [11] :

Type d'algorithme	Exemples	Avantages	Inconvénients
Symétrique (à clé privée)	AES, DES	✓ La rapidité d'exécution. ✓ Adapté au cryptage de flux de données. ✓ La simplicité d'implémentation (gestion d'une seule clé).	○ Echange de la clé secrète. ○ Une clé pour chacun des correspondants : n personnes ⇒ $n(n-1)/2$ clés. ○ Problème de communication de clés entre émetteur et récepteur.
Asymétrique (à clé publique)	RSA, ElGAMAL	✓ L'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisée. ✓ Un couple de clés publique/privée suffisant pour n correspondants. ✓ La possibilité d'utiliser la signature électronique.	○ Temps d'exécution plus long que le cryptage symétrique. ○ Problèmes de gestion de clés publiques. ○ Le danger des attaques par substitution des clés.

Tableau 1.1 : Avantages et inconvénients des cryptosystèmes symétriques et asymétriques.

D'après le Tableau 1.1 on remarque que les deux types ont des inconvénients, c'est pour cela on va étudier les cryptosystèmes chaotiques et hyper-chaotiques dans le prochain chapitre.

6. Utilisations de la cryptographie

Parmi les utilisations de la cryptographie pour pouvoir sécuriser de façon plus sûre on cite :

- Confidentialité des transactions bancaires,
- Protection des secrets industriels, commerciaux ou médicaux,
- Protection des systèmes informatiques contre les intrusions,
- Protection de la confidentialité des communications militaires,
- Protection de la vie privée.

7. Cryptanalyse

Les cryptanalystes sont les adversaires des cryptographes car leur but est de casser un algorithme cryptographique afin qu'une tierce personne puisse le décoder. Les cryptanalystes utilisent un certain nombre de méthodes de base pour leurs besoins [2].

a) **Attaque par texte chiffré uniquement :** le cryptanalyste dispose du texte chiffré de plusieurs messages, tous chiffrés avec le même algorithme. La tâche de la cryptanalyse est de trouver autant que possible le texte brut du message, ou mieux encore, de trouver la ou les clés utilisées pour chiffrer le message, ce qui permettra de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

b) **Attaque de texte en clair connu :** un cryptanalyste a accès non seulement au texte chiffré de plusieurs messages, mais également au texte en clair correspondant. La tâche consiste à trouver la clé utilisée pour chiffrer ces messages ou un algorithme capable de déchiffrer tout nouveau message chiffré avec la même clé.

c) **Attaque à texte en clair choisi :** non seulement la cryptanalyse a accès aux textes chiffrés et aux textes en clair mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé. La tâche consiste à retrouver la ou les clés utilisées pour chiffrer ces messages ou un algorithme qui permette de déchiffrer n'importe quel nouveau message chiffré avec la même clé.

d) **Attaque à texte en clair choisi adaptative :** c'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite.

e) **Attaque à texte chiffré choisi :** Le cryptanalyste dispose de la machine permettant de décoder le ciphertext. Son objectif est de récupérer l'algorithme ou la clé, qui est à la base de la génération du texte chiffré.

f) **Attaque à clé choisie :** le cryptanalyste peut choisir la clé, il est exclusivement au courant de quelques relations entre différentes clés. Cette méthode est difficile et n'est pas très pratique.

8. Conclusion

Ce premier chapitre était consacré aux concepts généraux de la cryptographie qui permettent d'assurer la confidentialité des données, qu'elles soient stockées localement sur une machine ou transmise sur un réseau non sécurisé.

D'abord on a présenté une introduction à la cryptographie, après on a défini les termes les plus utilisés dans ce domaine et on a déterminé les exigences de sécurité que la cryptographie s'efforce à atteindre.

Ensuite, on a indiqué les trois classes de la cryptographie ainsi que les méthodes utilisées dans chaque classe et citant quelques exemples d'algorithmes et faisant une comparaison entre eux.

Enfin, on a mentionné le problème qui fait face la cryptographie, c'est la cryptanalyse. Il oblige les cryptographes à développer les méthodes de chiffrement actuels et à en découvrir de nouveaux afin d'éviter ce problème et d'assurer la sécurité du stockage et de la transmission des données. Un exemple de ces méthodes, est le chiffrement par les systèmes chaotiques et hyperchaotiques qui sera l'objet du prochain chapitre.

Chapitre 2

Systèmes chaotiques et hyperchaotiques

1. Introduction

Le terme « chaos » prend origine du terme « Χάος », utilisé par les Grecs pour décrire l'espace vide infini dont ils ont supposé l'existence avant l'apparition de toutes choses. Les Romains ont repris le terme et interprété l'idée sous-jacente pour concevoir quelque chose d'informe, dans lequel - croient-ils - l'architecte du monde a introduit l'ordre et l'harmonie. De nos jours, dans le langage commun « Chaos » décrit un état de désordre et d'irrégularité. Dans le milieu scientifique le terme "chaos" définit un état particulier d'un système dynamique dont le comportement ne se répète jamais, qui est très sensible aux conditions initiales, et imprévisible à long terme [47].

La première visualisation de phénomènes chaotiques déterministes a été observée par coïncidence par Edward Lorenz en 1961, lorsqu'il a effectué une série de calculs visant à prédire les phénomènes météorologiques. Ce dernier a utilisé son ordinateur (Royal McBean Lgp-300) pour calculer ses prédictions. Après avoir obtenu le résultat final, il a voulu recommencer pour assurer le résultat. Pour gagner du temps, il n'a considéré que trois décimales au lieu de six, estimant que ses résultats varieraient légèrement, mais il a été étonné que ce dernier soit complètement différent du premier. De là, nous avons découvert le comportement chaotique des systèmes non linéaires, une métaphore qui a contribué à l'essor de la théorie de Lorentz : "le simple battement d'aile du papillon au Brésil pourrait déclencher une tornade au Texas " [12].

Le présent chapitre est réservé aux systèmes dynamiques en particulier les systèmes chaotiques et hyperchaotiques.

2. Systèmes dynamiques

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

- Causale, lorsque l'avenir de système ne dépend que de phénomènes du passé ou du présent.
- Déterministe, à partir de l'état du système à un instant initial, on peut calculer son évolution à n'importe quel autre moment.

Les mathématiciens ont classé les systèmes dynamiques en deux catégories [13] :

- Systèmes dynamiques continus.
- Systèmes dynamiques discrets.

2.1. Systèmes dynamiques continus

L'évolution d'un système dynamique continu dans le cas entier est représentée par l'équation différentielle ordinaire suivante :

$$\dot{x} = \frac{dx}{dt} = f(x, t, v) \tag{2.1}$$

où, $x \epsilon E$ (E un ensemble non vide de $\mathbb{R}^n$ appelé espace de phase) est le vecteur d'état, $v \epsilon \mathbb{R}^p$ est un vecteur des paramètres et $f : E \times \mathbb{R}^+ \times \mathbb{R}^p$ est le champ de vecteur, qui représente la dynamique du système (2.1).

Lorsque l'application f est continue et vérifie la condition Lipschitzienne sur un certain intervalle I de la variable x, on peut assurer l'existence et l'unicité de la solution pour toute condition initiale ϵI.

2.2. Systèmes dynamiques discrets

La forme générale d'un système dynamique à temps discret est décrite par une équation aux différences non linéaire suivante :

$$x_{n+1} = f\ (x_n, v)\ ; n \epsilon \mathbb{N} \tag{2.2}$$

2.3. Systèmes non-linéaires

Un système est dit non linéaire s'il ne respecte pas le principe de superposition avec l'existence d'une relation entre les grandeurs d'entrée et de sortie comme équation différentielle avec des coefficients généralement non constants. La majorité des systèmes physiques sont des systèmes non linéaires.

2.4. Systèmes déterministes

Un système est déterministe, lorsque pour tous les mêmes paramètres, les mêmes conditions initiales et les mêmes conditions aux limites, on obtient les mêmes résultats uniques.

3. Notions sur le chaos

On peut définir le chaos comme un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Il montre un aspect fondamental d'instabilité appelé *sensibilité aux conditions initiales*. Cette sensibilité aux conditions initiales rend le phénomène imprévisible. Une autre caractéristique du système chaotique est son évolution qui est *pseudo-aléatoire.*

3.1. Le chaos et l'aléatoire

La différenciation entre chaos et aléatoire nous semble le point le plus important pour comprendre le chaos. En fait, les gens ont tendance à penser que l'imprévisibilité d'un phénomène provient de la pléthore de paramètres entrant dans sa description. Ceci nous amène à une approche probabiliste qui peut être entièrement satisfaite, en conservant par définition un certain aléa. En ce qui concerne le chaos, ce n'est pas le cas, les systèmes chaotiques se comportent de manière apparemment aléatoire. Mais ce comportement est en réalité décrit de manière déterministe par des équations non linéaires pleinement déterministes, c'est-à-dire notamment à l'aide d'outils mathématiques qui permettent des méthodes précises et déterministes.

4. Propriétés des systèmes chaotiques

- **Non-linéarité :** Un système chaotique est un système dynamique non linéaire. Si le système est linéaire, il ne peut pas être chaotique.
- **Déterminisme :** Un système chaotique a des règles fondamentales déterministes plutôt que probabilistes. Son état présent est complètement déterminé par les conditions initiales.
- **Aspect aléatoire :** Les systèmes chaotiques ont tendance à se comporter de manière apparemment aléatoire car on ne peut pas donner une description mathématique du mouvement à long terme, mais il est décrit par des équations non linéaires complètement déterministes.

La figure suivante illustre l'aspect aléatoire du système de Lorenz [14] :

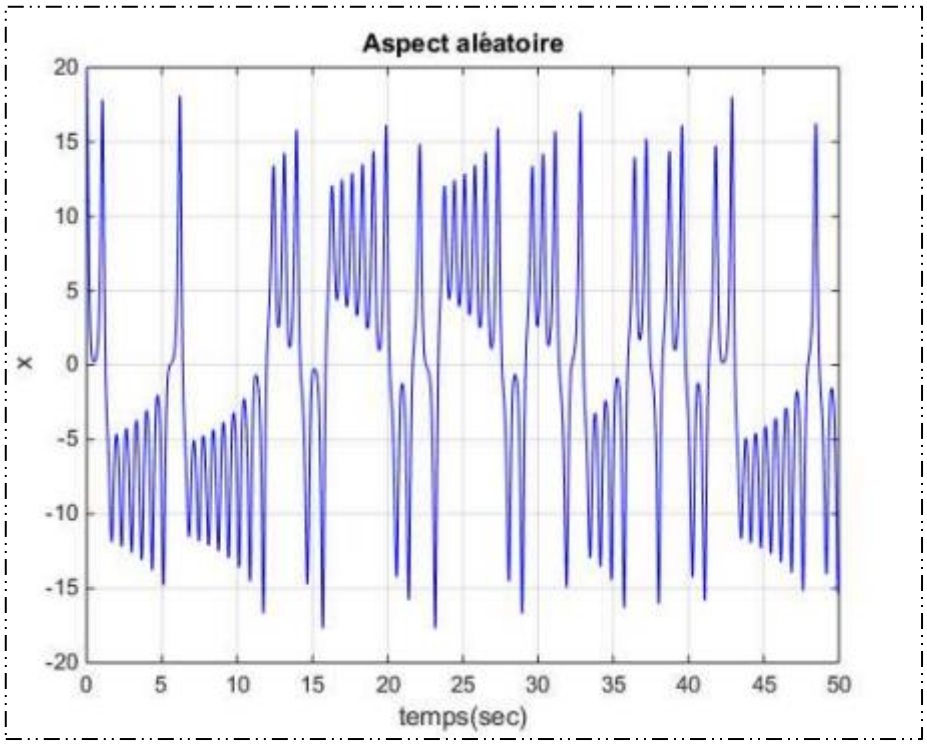


Figure 2.1 : Aspect aléatoire du système de Lorenz.

4.1. Sensibilité aux conditions initiales (SCI)

Initialement, les systèmes chaotiques sont extrêmement sensibles aux perturbations. Ce fait peut être illustré par l'effet papillon popularisé par le météorologue Edward Lorenz. L'évolution d'un système dynamique chaotique est imprévisible car elle est sensible aux conditions initiales. De ce fait, deux trajectoires de phase initialement adjacentes divergent toujours l'une de l'autre, quelle que soit leur proximité initiale. Évidemment, la moindre erreur ou simple imprécision dans les conditions initiales nous empêche de décider à tout moment que ce sera la trajectoire qu'il suivra réellement, nous ne pouvons donc pas faire de prédictions autres que des statistiques sur l'avenir à long terme du système. Ainsi, bien qu'il s'agisse de systèmes déterministes, il n'est pas possible de prédire leur comportement à long terme. La seule façon d'y parvenir est de faire évoluer efficacement le système d'exploitation.

Si cette simulation est faite par ordinateur, alors il y a un problème avec la précision des conditions initiales : en raison de petites erreurs d'arrondissement causées par la précision du type de codage variable, ces conditions initiales peuvent augmenter de façon exponentielle la trajectoire de phases obtenue n’est pas représentative de la réalité [15].

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant les taux de divergence des trajectoires. Ceci est illustré par la Figure 2.2 [16] :

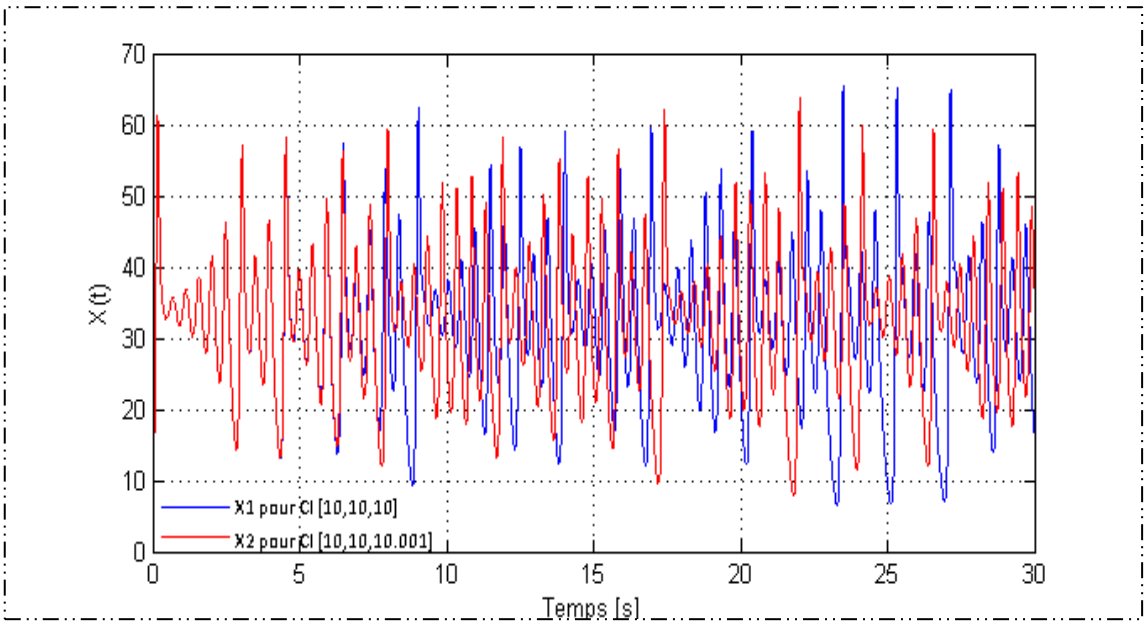


Figure 2.2 : Sensibilité aux conditions initiales pour le système de Lorenz.

4.2. Attracteur étrange

Un attracteur est la région de l'espace de phases vers laquelle convergent toutes les trajectoires d'un système dynamique dissipatif. Les attracteurs sont donc des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques. Un attracteur chaotique dit étrange, est associé à un comportement quasi-aléatoire et caractérisé par un spectre de puissance continu et une fonction d'autocorrélation s'annulant très rapidement. Contrairement aux signaux périodiques pour lesquels la similitude reste présente pour autant que la périodicité n'est altérée ; ce qui a pour conséquence immédiate la périodicité du comportement du système. Le caractère fini de la portée de la fonction d'autocorrélation temporelle pour le régime chaotique met en évidence la perte progressive de la similitude interne et donc l'imprédictibilité [17].

Un attracteur chaotique possède particulièrement la propriété exceptionnelle suivante : *la trajectoire ne repasse jamais par un même état*. Ce qui signifie, entre autres, que cette

trajectoire passe par une *infinité d'états.* Un exemple des attracteurs étranges est celui de Lorenz (Figure 2.3).

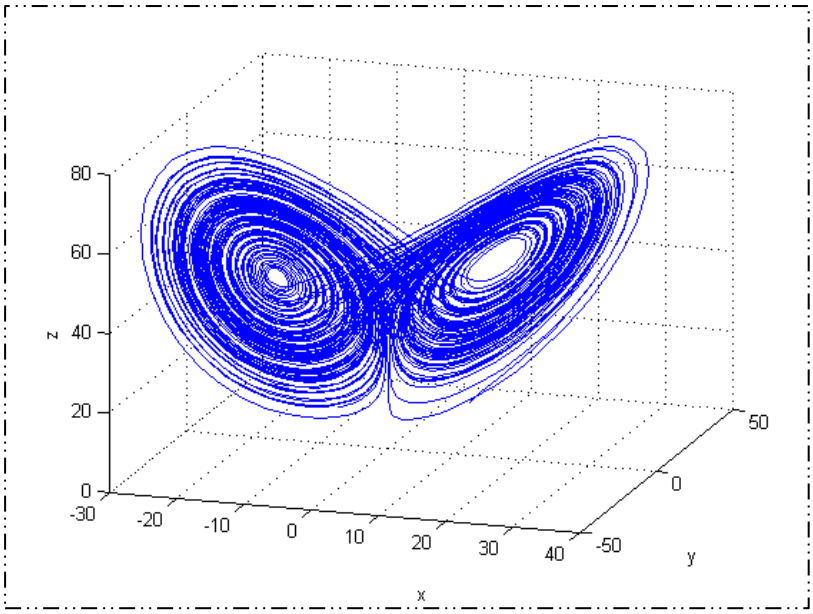


Figure 2.3 : Attracteur étrange de Lorenz.

4.3. Exposant de Lyapunov

Le mathématicien Alexander Lyapounov a étudié le phénomène de la sensibilité aux conditions initiales des systèmes chaotiques et a développé un degré permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier ; cette quantité est appelée « Exposant de Lyapounov » [16].

L'exposant de Lyapunov est un coefficient pour mesurer la sensibilité aux conditions initiales de la série temporelle. Par définition, un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoires voisines de l'espace des phases. Il mesure le taux local d'expansion de l'espace dans lequel l'expansion est maximale, c'est-à-dire en général vers l'attracteur. Un attracteur étrange est un attracteur dont l'un au moins de ses exposants de Lyapunov est positif. Autrement dit, le plus grand exposant est positif pour le système chaotique et négatif pour les autres systèmes.

Deux trajectoires dans le plan de phase initialement séparées par un taux Z_1 divergent après un temps $\Delta_t = t_2 - t_1$ vers Z_2 tel que :

$$|Z_2| \approx \exp(\lambda . \Delta_t)|Z_1| \qquad (2.3)$$

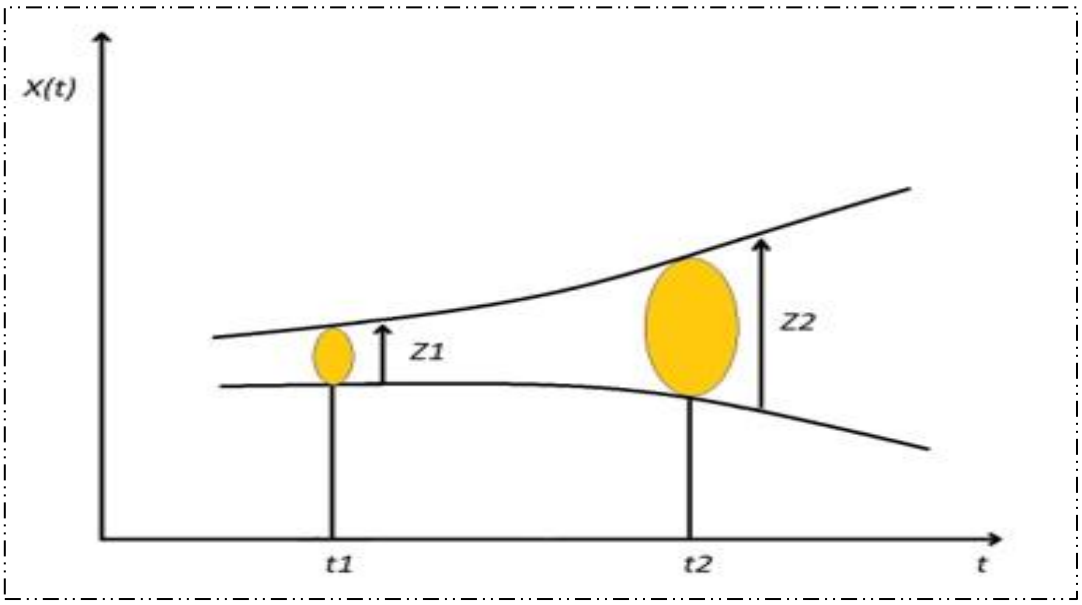


Figure 2.4 : Divergence de deux trajectoires dans le plan de phase.

On considère un système dynamique dont l'espace des phases est de dimension n et on prend à $t = 0$ une hyper sphère infiniment centré en X appartenant à l'attracteur ($X \epsilon \mathbb{R}^n$ avec un rayon ε_0).

Au temps $t >> 0$, cette hyper sphère se transforme en une hyper-ellipsoïde de n demi-axes $\varepsilon_i(t) \approx \varepsilon_0 \exp(\lambda_i\ t), i = 1, 2 \ldots . n$

Les exposants de Lyapunov sont tels que :

$$\lambda_i = \lim_{t\to\infty} \lim_{\varepsilon_0\to\infty} \frac{1}{t} \log\frac{\varepsilon_i}{\varepsilon_0} \tag{2.4}$$

Pour un attracteur *non chaotique*, les exposants de Lyapunov sont tous soit négatifs soit nuls et leur somme est obligatoirement négative. Un attracteur *étrange* (chaotique) possèdera toujours au moins trois exposants de Lyapunov (un exposant par degré de liberté du système), dont un au moins qui est positif (voir Tableau 2.1). On constate donc que les exposants de Lyapunov représentent un outil très utile pour l'illustration de la dynamique d'un système (entre-autre pour déterminer si un système est chaotique ou pas) [18].

Etat stable	Dimension	Exposant de Lyapunov
Point d'équilibre	0	$\lambda_n \leq \ldots \leq \lambda_1 \leq 0$
Périodique	1	$\lambda_1 = 0$ $\lambda_n \leq \ldots \leq \lambda_2 \leq 0$
Période d'ordre 2	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \ldots \leq 3 \leq 0$
Période d'ordre K	K	$\lambda_1 = \ldots = \lambda_k = 0$ $\lambda_n \leq \ldots \leq \lambda_{k+1} \leq 0$
Chaotique	Non entier	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyperchaotique	Non entier	$\lambda_1 > 0$ $\lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tableau 2.1 : Classification des systèmes dynamiques selon leurs exposants de Lyapunov.

4.4. Capacité de mélange :

Intuitivement, il s'agit de la propriété suivante : si l'on se donne deux sous-intervalles quelconques I *et* J de [0 :1], le premier étant considéré comme source et le second comme cible, il existe une orbite dont le premier terme x_0 est dans I, et qui a l'un de ses éléments x_n dans J.

Le caractère arbitraire des intervalles source et cible implique alors qu'en fait il existe une infinité de telles orbites, et que pour chacune d'entre elles, il existe une infinité d'éléments appartenant à l'intervalle cible [19].

5. Bifurcation et routes vers le chaos

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Les graphiques qui représentent les

bifurcations, sont appelés diagrammes de bifurcation. Donc le diagramme de bifurcation est un outil très important pour évaluer les comportements possibles d'un système en fonction des valeurs de bifurcation. La Figure 2.5 illustre le diagramme de bifurcations de la fonction logistique définie sur le segment [0 : 1] par :

$$x_{n+1} = rx_n(1 - x_n) \tag{2.5}$$

où $n = 0, 1, 2..$ dénote le temps discret, et $r \in [0 : 4]$ un paramètre de contrôle.

Selon la Figure 2.5, on peut distinguer trois états différents du système selon la valeur du paramètre r : un régime stable, puis périodique à plusieurs états et enfin un régime chaotique [20].

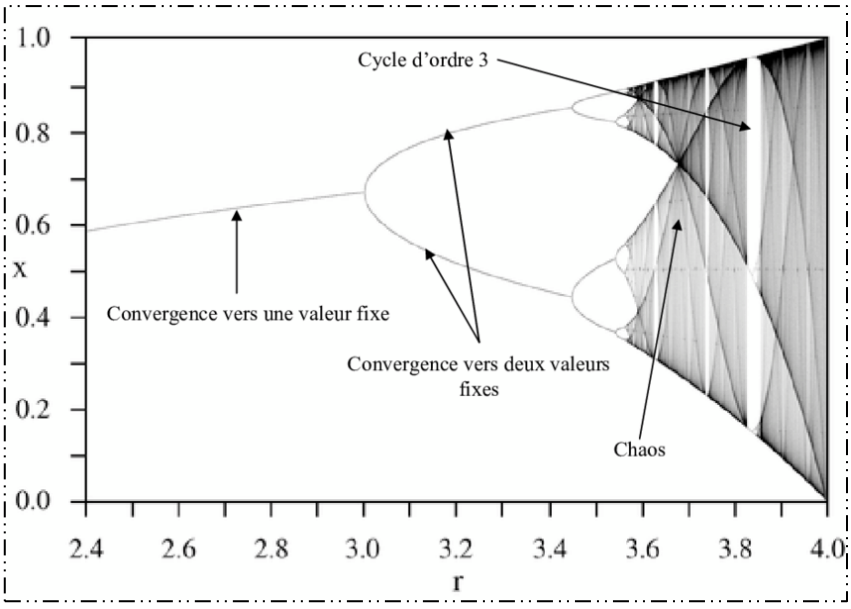


Figure 2.5 : Diagramme de bifurcation de la fonction logistique.

Il peut être intéressant d'étudier l'apparition du chaos (ce qu'on appelle des scénarios ou des routes vers le chaos. Il existe *trois scénarios* théoriques d'évolution vers le chaos. Toutes ces évolutions permettent de classer certains phénomènes comme déterministes chaotiques. On obtient l'apparence du chaos en modifiant la valeur d'un paramètre du système.

a) Doublement de période

Ce scénario de passage vers le chaos est sans doute le plus connu. Par augmentation du paramètre de contrôle, la fréquence du régime périodique double, après est multipliée par 2, 4,

par 8 et par 16 etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique. Il a été étudié en particulier en dynamique de populations par R. May sur l'application logistique, $x_{n+1} = rx_n(1 - x_n)$ [21].

Selon la valeur du paramètre r, la suite converge soit vers un point fixe nul ou pas. Dès que r est plus grand que 3 le système bifurque, c'est à dire qu'il oscille entre 2 valeurs autour du point fixe. On parle de cycle attracteur de période 2. En continuant à augmenter r, ces 2 attracteurs s'éloignent du point fixe jusqu'à ce qu'une nouvelle bifurcation ait lieu. Chaque point se dédouble et on obtient un cycle attracteur de période 4. On dit qu'il y a doublement de période. C'est à partir de cet exemple que Feigenbaum pressentit l'existence d'une forme d'universalité dans cette transition vers le chaos sous forme de cascade de doublement de période.

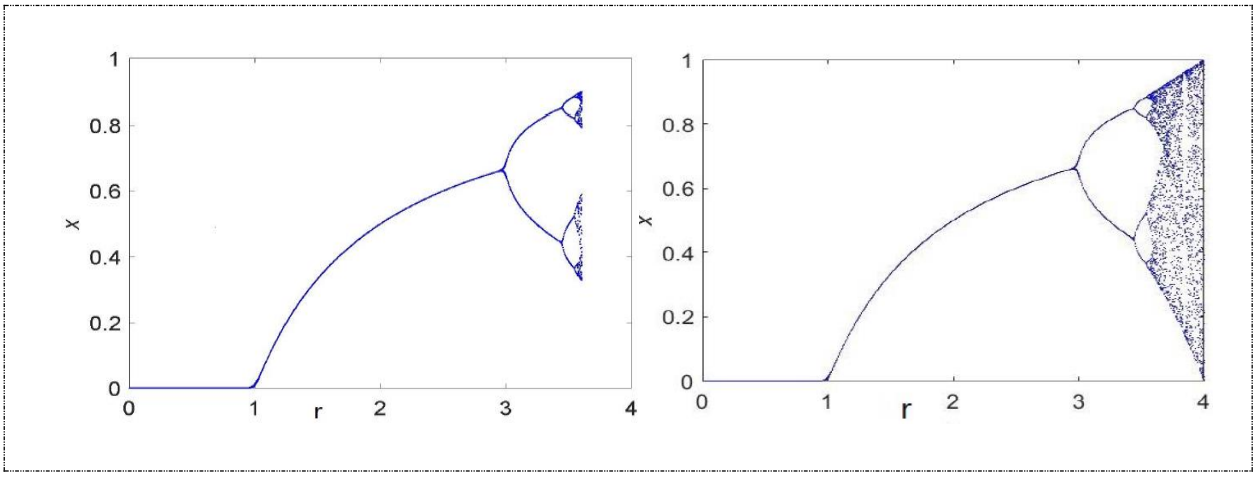


Figure 2.6 : Transition vers le chaos par doublement de période.

b) Intermittence

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière. Le système conserve pendant un certain intervalle de temps un régime périodique ou pratiquement quasi-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, pour donner lieu à une autre « explosion chaotique » plus tard. La fréquence et la durée des phases chaotiques ont tendance à

s'accroître plus on s'éloigne de la valeur critique de la contrainte ayant conduit à leur apparition [16].

c) Quasi-périodicité

Le troisième cas de transition vers le chaos est la quasi-périodicité qui se produit lorsqu'un deuxième système interfère avec un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est pas rationnel, alors le système est dit quasi-périodique. Ce régime peut, à son tour, perdre la stabilité et devenir alors soit directement chaotique, soit par la survenance d'une troisième fréquence.

6. Systèmes hyperchaotiques

Un attracteur hyperchaotique est généralement défini, comme étant un comportement chaotique avec au moins deux exposants de Lyapunov positifs. Combiné avec un exposant nul, le long de l'écoulement et un exposant négatif pour assurer la limite de la solution. La dimension minimale d'un système hyperchaotique continu est quatre [22].

6.1. Système hyperchaotique de Rössler

Le premier système hyperchaotique à quatre dimensions a été proposé en 1979 par Rössler. Ce système est défini par les équations suivantes :

$$\begin{cases} x = -(y+z) \\ y = x + ay + w \\ z = b + xz \\ w = -cz + dw \end{cases} \tag{2.6}$$

Le système suit un comportement hyperchaotique (Figure 2.7), quand les paramètres a, b, c et d prennent les valeurs suivantes : $a = 0.25, b = 3, c = 0.5\ et\ d = 0.05$.

Les conditions initiales peuvent prendre les valeurs suivantes : $x_0 = -10,\ y_0 = -6,\ z_0 = 0,$ $w_0 = 10$. Les quatre exposants de Lyapunov correspondants sont $\lambda_1 = 0.112, \lambda_2 = 0.119, \lambda_3 = 0\ et\ \lambda_4 = -25.118$.

On remarque bien que ce système répond aux conditions de passage du chaos vers l'hyperchaos déjà prédéfinies.

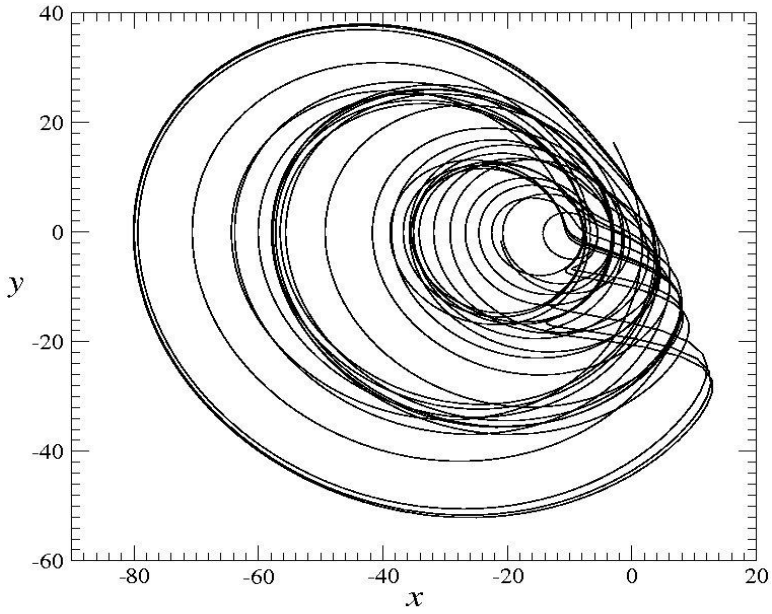


Figure 2.7 : Projection plane de l'attracteur hyperchaotique de Rössler de 4D.

Le caractère hyperchaotique de ce comportement n'est pas si évident à partir de cette projection plane, qui ressemble un peu à un attracteur chaotique "bruyant" [22].

6.2. Comportements hyperchaotiques expérimentaux

Très peu de comportements hyperchaotiques expérimentaux ont été identifiés à ce jour. Comme les systèmes hyperchaotiques (continus) sont au minimum de quatre dimensions nécessairement, l'effet de la fonction de mesure $h : R^m \rightarrow R$ devient de plus en plus critique que pour les systèmes chaotiques tridimensionnel (continu chaotique).

En particulier, quand l'exposant positif de Lyapunov λ_1 est suffisamment plus grand que le deuxième exposant positif λ_2, il y a deux différentes échelles de temps dans la dynamique hyperchaotique. En conséquence, il devient tout à fait difficile de reconstruire d'une façon adéquate le signal du départ.

Ainsi, seulement peu de comportements hyperchaotiques expérimentaux ont été identifiés. L'occurrence du comportement hyperchaotique a été trouvée dans un circuit électronique (Matsumoto et al. 1986), le laser de NMR (le Perron et al. 1988), dans un système de semi-conducteur (le Perron et al. 1989) et dans un système de réaction chimique (Eiswirth et al. 1992) [22].

7. Conclusion

Ce chapitre a été consacré aux quelques généralités sur les systèmes dynamiques, les systèmes chaotiques et hyperchaotiques.

Après une brève introduction sur le chaos, on a mentionné les types des systèmes dynamiques utiles pour la résolution des systèmes chaotiques et hyperchaotiques avec une brève comparaison entre le chaos et l'aléatoire. Les propriétés des systèmes chaotiques sont présentées avec un peu plus de détail. Ces propriétés que possède le chaos, offre la possibilité d'utiliser des systèmes chaotiques dans le domaine de la cryptographie. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul dû à leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des données de grande taille telles que les images.

Le chapitre suivant sera consacré à la sécurisation des données par les systèmes chaotiques continus et discrets.

Chapitre 3

Sécurisation par systèmes chaotiques

1. Introduction

Depuis 1980, l'idée d'utiliser des systèmes numériques chaotiques pour concevoir de nouveaux cryptosystèmes attire de plus en plus l'attention des chercheurs. En fait, plusieurs caractéristiques fondamentales du chaos, telles que l'ergodicité, la capacité de mélange et la sensibilité aux conditions initiales, peuvent être liées aux propriétés de "confusion" et de "diffusion" de la cryptographie classique. Par conséquent, c'est une idée naturelle d'utiliser le chaos pour concevoir de nouveaux cryptosystèmes [23].

Actuellement, il existe deux méthodes pour utiliser le chaos dans la cryptographie :

- Méthodes de chiffrement des communications analogiques, qui sont basés principalement sur les techniques de la synchronisation du chaos.
- Méthodes de chiffrement des communications numériques, où on utilise des circuits numériques ou des ordinateurs pour concevoir leurs algorithmes.

Dans ce chapitre, on s'intéresse au cryptage chaotique numérique des images [24].

2. Le chaos et la cryptographie

Ces dernières années, la cryptographie basée sur la théorie du chaos s'est développée rapidement. Actuellement la majorité des études se concentrent sur l'utilisation du chaos dans des cryptosystèmes en vue d'apporter un progrès (temps de chiffrement, sécurité) par rapport aux procédés standards de la cryptographie (DES, AES), ceci grâce aux caractéristiques des signaux chaotiques tels que : le déterminisme qui indique que ces systèmes sont régis par des règles fondamentales non probabilistes, c'est-à-dire il est possible de regénérer le comportement chaotique. Une autre propriété importante de ces systèmes est la sensibilité aux conditions initiales, c'est-à-dire un petit changement ou une imprécision dans les conditions initiales engendre une des évolutions totalement différentes, cela signifie qu'il est impossible de faire des prédictions à long terme sur le comportement des systèmes chaotiques. Le principe de chiffrement par chaos (voir Figure 3.1) consiste à transmettre un message à travers un signal chaotique d'un émetteur vers un récepteur connaissant les conditions initiales pour extraire le message original [25].

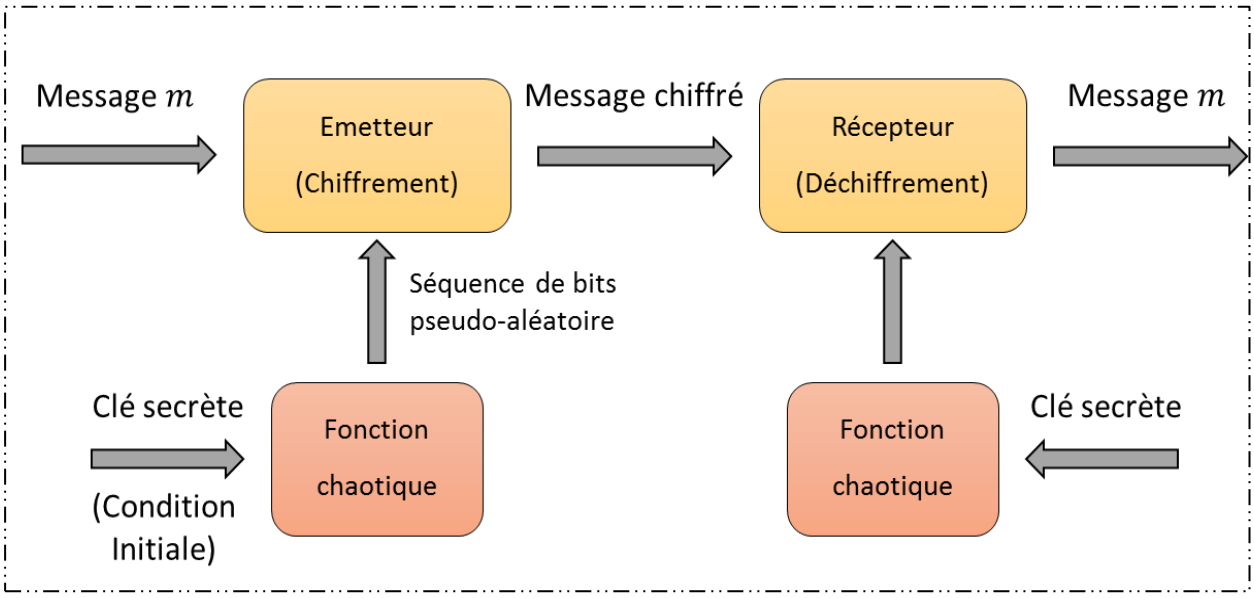


Figure 3.1 : Schéma de principe d'un cryptosystème basé sur le chaos.

3. Correspondance entre chaos et cryptographie :

Le tableau ci-dessous présente la correspondance entre la cryptographie et les systèmes chaotiques [26] :

Théorie du chaos	Cryptographie
Système chaotique.	Système pseudo-aléatoire.
Transformation non linéaire.	Transformation non linéaire.
Nombre infini d'états.	Nombre fini d'états.
Nombre infini d'itérations.	Nombre fini d'itérations.
État initial.	Plaintext.
État final.	Ciphertext.
Conditions initiale et/ou paramètres.	Clé (s).
Indépendance asymptotique des états initiaux et finaux.	Confusion.
Sensibilité aux conditions initiales et paramètres.	Diffusion.

Tableau 3.1 : Correspondance entre chaos et cryptographie.

4. Classes et types des systèmes de chiffrement numérique

Depuis 1990, plusieurs systèmes chaotiques numériques ont été proposés et analysés. Il existe en général trois types des systèmes de chiffrement [27] :

4.1. Systèmes de chiffrement chaotiques continus (bit à bit)

4.1.1. Chiffres chaotiques continus basés sur PRNG

Les systèmes chaotiques peuvent créer des orbites pseudo-aléatoires inattendues. Grand nombre de chercheurs ont considéré les algorithmes et les performances d'estimation de $PRNG$ (Générateur de Nombres Pseudo-Aléatoires) basés sur le chaos dont le XOR est l'opération de base. Ces systèmes chaotiques utilisent en général : la fonction logistique et sa version généralisée, 2D attracteur de Hénon, fonction de Chebyshev, des piecewises linéaires et non linéaires et des systèmes chaotiques *p-adique*.

4.1.2. Chiffrement par approche des systèmes chaotiques inverses

Feldmann et ses collaborateurs ont proposé le modèle général pour concevoir des systèmes de communications chaotiques sécurisés qu'ils ont appelés systèmes chaotiques inverses. Ce modèle peut être utilisé dans les deux cas analogique et numérique.

4.2. Systèmes de chiffrement chaotique par blocs

Les systèmes de chiffrement chaotique par blocs manipulent des blocs de texte en clair et de texte chiffré, où en général, ils sont basés sur des systèmes chaotiques inverses (Backwards) et des systèmes par itérations de la fonction chaotique (Forwards) et *S-Boxes*.

4.3. Autres systèmes chaotiques

Récemment, des nouvelles idées ont été proposées, par exemple l'introduction des automates cellulaires, la recherche du texte en clair dans les séquences pseudo-aléatoires (Searching-Based Chaotic Ciphers), les algorithmes chaotiques à clé publique (Chaotic Public-Key Ciphers), et des méthodes chaotiques pour le cryptage des images qui fera l'objet de la prochaine section.

5. Cryptage chaotique des images

Le développement énorme des télécommunications et de l'internet, rend la sécurité d'image numérique de plus en plus importante, il est nécessaire dans plusieurs applications, TV, systèmes médicaux, images militaires, albums personnels via Internet, etc. Les techniques de cryptage traditionnelles telles que le DES, RSA... ne sont pas généralement convenables pour le chiffrement des images en temps réel, ceci à cause de leur faible vitesse d'exécution.

6. Schémas du chiffrement des images

Fondamentalement, il y a deux méthodes pour utiliser le chaos, dans le domaine du chiffrement des images :

a) Utilisation du chaos comme une source pour créer des bits pseudo-aléatoires avec les propriétés statistiques exigées au chiffrement.
b) Utilisation des fonctions chaotiques en 1D, 2D ou 3D pour faire les permutations et les substitutions secrètes nécessaires à l'image cryptée.

On distingue les algorithmes suivants :

- **BRIE** (Bit Recirculation Image Encryption).
- **CNNSE** (Chaotic Neural Network for Signal Encryption).
- **DSEA** (Domino Signal Encryption Algorithm).
- **CKBA** (Chaotic Key-Based Algorithm).
- **HCIE** (Hierarchic Chaotic Image Encryption).

7. Etude d'un système chaotique continu

Nombreux systèmes chaotiques continus ont été étudiés dans la littérature, parmi ces systèmes, on retrouve le système de Lorenz, le système de Rössler et l'attracteur de Chen. On prend comme exemple des systèmes chaotiques continus le système de *Lorenz. C'*est un système à trois équations différentielles qui devrait représenter approximativement la convection thermique dans l'atmosphère (obtenue à partir des équations de Navier-Stokes) [28]. C'est un exemple bien connu de système différentiel avec un comportement chaotique pour certaines valeurs de paramètres. Le système de Lorenz est représenté par les équations suivantes :

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (3.1)$$

Lorsque les paramètres réels σ, ρ et b prennent les valeurs suivantes : σ = 10, ρ = 28 et b = $\frac{8}{3}$, avec les conditions initiales $x_0 = y_0 = z_0 = 10$, le système (3.1) est chaotique. Dans ce qui suit, nous vérifions quelques propriétés chaotiques de ce système :

7.1. Aspect aléatoire

Nous avons tracé dans les trois sous-graphiques l'évolution dans le temps des coordonnées x, y et z pour $t \in [0 : 20]$, avec la condition initiale $(10,10,10)$. On observe que les trois coordonnées oscillent dans le temps, sans périodicité apparente.

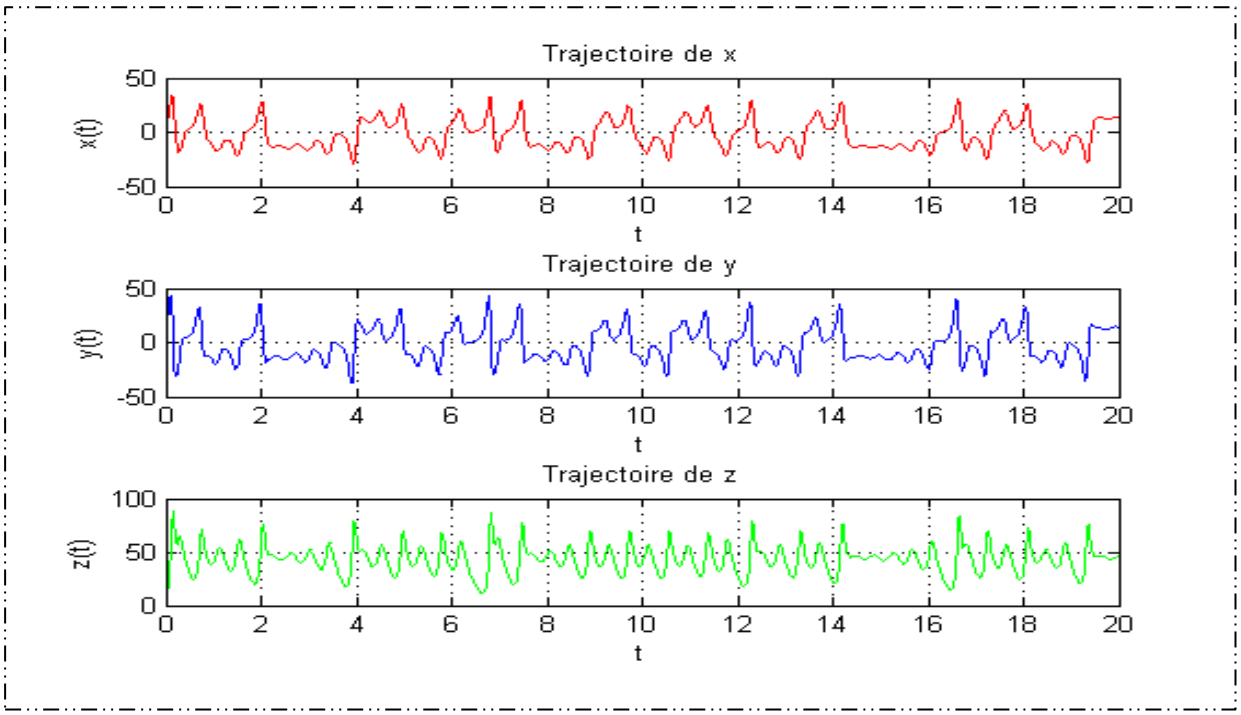


Figure 3.2 : Les trajectoires de x, y et z en fonction du temps.

7.2. Attracteur étrange

Le système chaotique (3.1) présente un superbe attracteur étrange en forme d'ailes de papillon, représenté sur la Figure 3.3. La trajectoire commençant par s'enrouler sur une aile, puis sautant pour commencer à s'enrouler sur l'autre aile, et ainsi de suite.

On observe que la dynamique du système de Lorenz donnée par le système (3.1) est indépendante du temps, par conséquent ce type de système est qualifié d'être autonome [29].

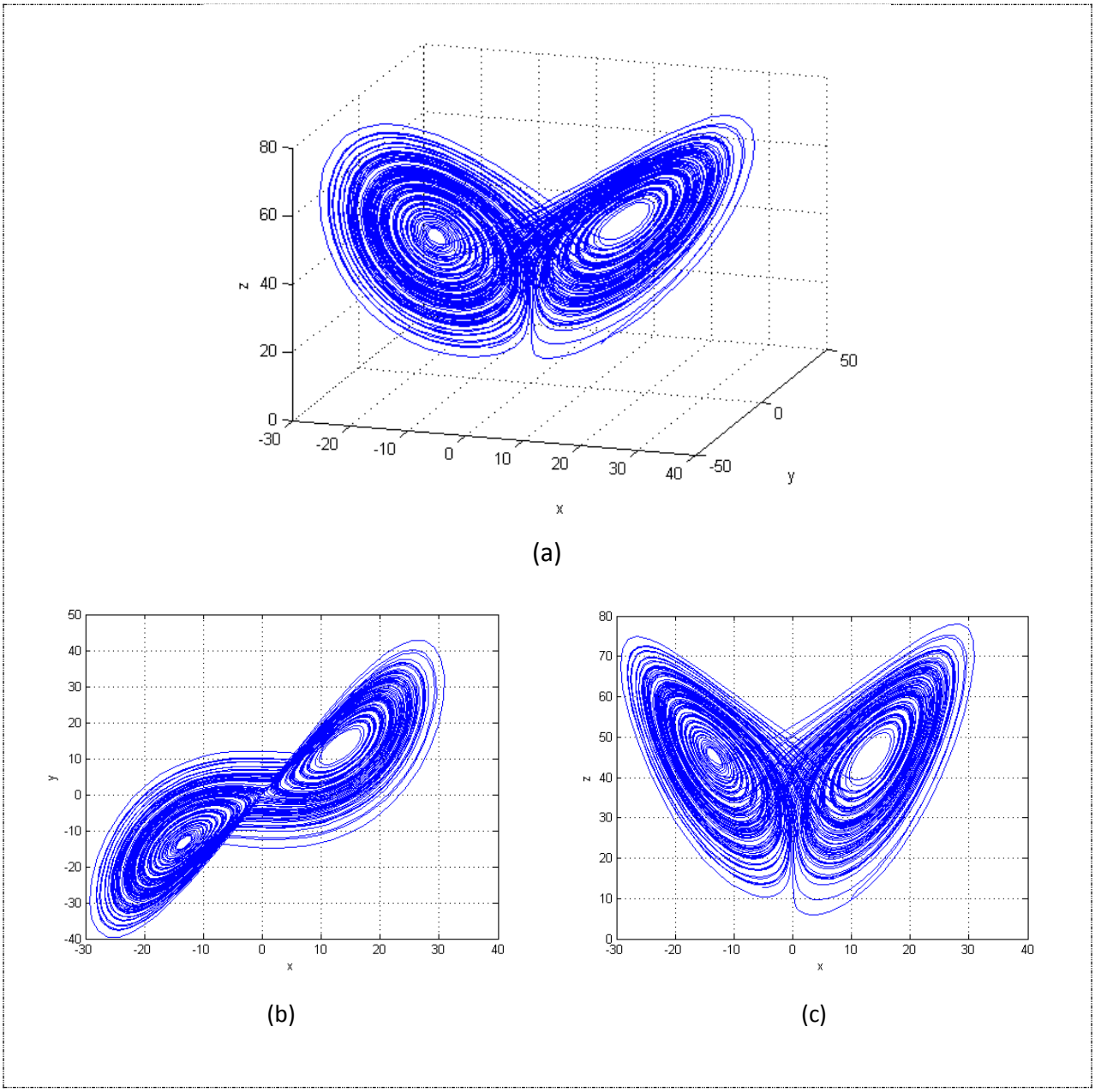


Figure 3.3 : Attracteur de Lorenz (a) en 3D sur les axes (x, y, z) (b) en 2D sur les axes (x, y) et (c) en 2D sur les axes (x, z)

7.3. Exposant de Lyapunov

La Figure 3.4 montre les exposants de Lyapunov du système de Lorenz, les valeurs numériques de ces exposants selon les trois axes (x, y, z) sont $\lambda 1 = 1.482$, $\lambda 2 = 0.000263$, $\lambda 3 = -22.48$ respectivement.

On constate bien qu'il y a un exposant de Lyapunov positif, ce qui signifie que le système est chaotique.

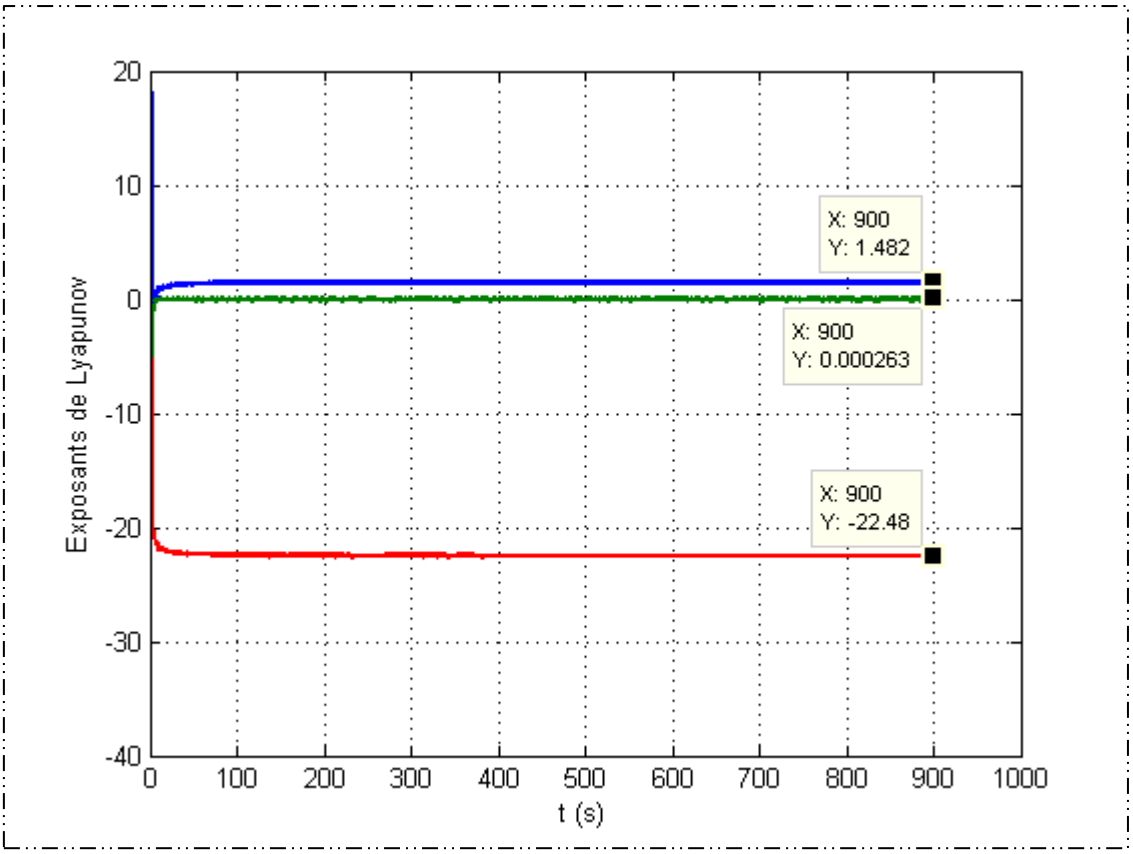


Figure 3.4 : Exposants de Lyapunov du système chaotique continu de Lorenz.

7.4. Sensibilité au conditions initiales (SCI)

Nous avons représenté l'évolution de la coordonnée z pour quatre conditions initiales $zi = 10, zi = 10.001, zi = 10.01, zi = 10.1$. Les quatre trajectoires sont imperceptibles jusqu'à $t = 2.5s$. Ensuite, la trajectoire s'éloigne de la trajectoire de référence. Plus la perturbation est faible, plus la trajectoire s'écarte tardivement de la trajectoire de référence.(voir Figure 3.5)

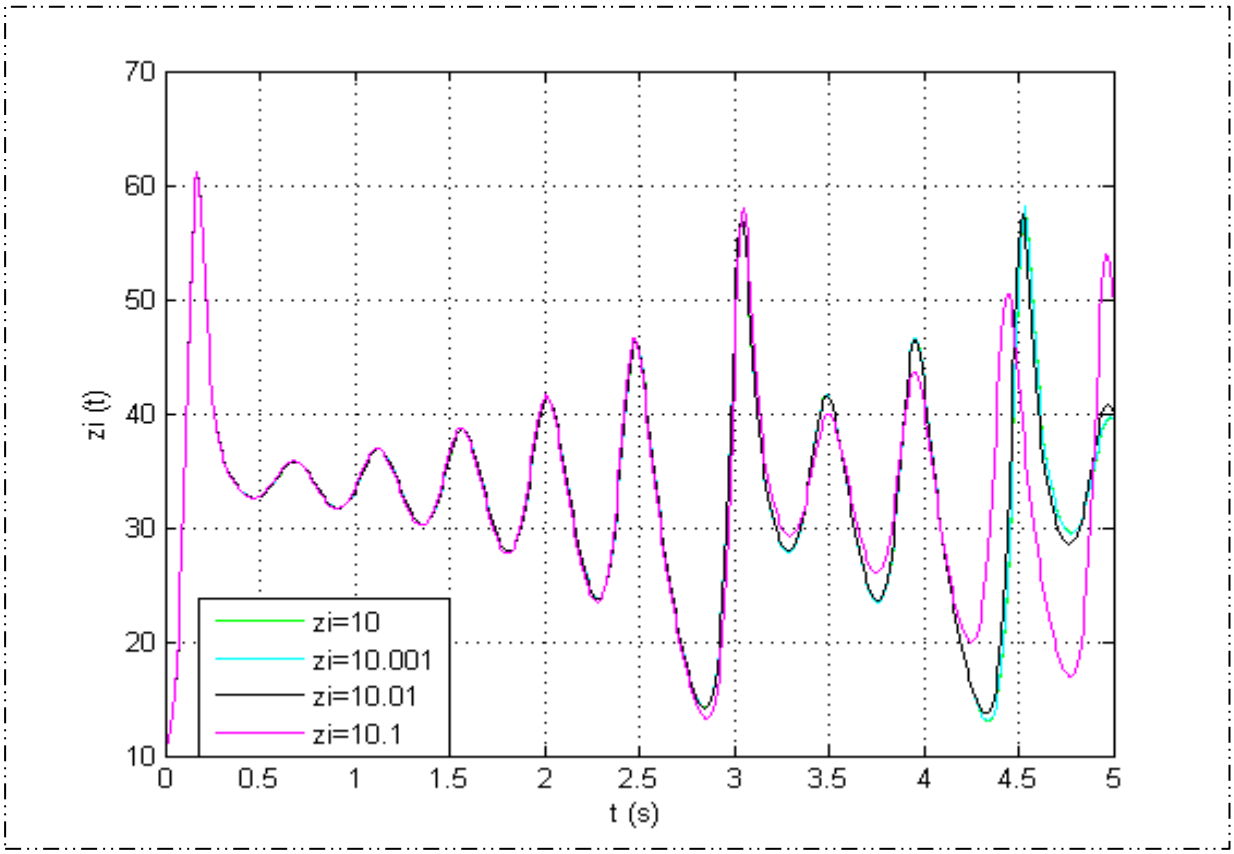


Figure 3.5 : Sensibilité aux conditions initiales du système de Lorenz.

7.5. Chiffrement d'image par système de Lorenz

Pour une transmission sécurisée des données par cryptographie chaotique, nous avons utilisé un algorithme pour chiffrer et déchiffrer les images, sachant que la simulation a été faite avec le logiciel Matlab. Dans ce manuscrit, nous avons utilisé l'image "cameraman.tif", qui est une image en niveaux de gris (256 valeurs). Notre algorithme de chiffrement est :

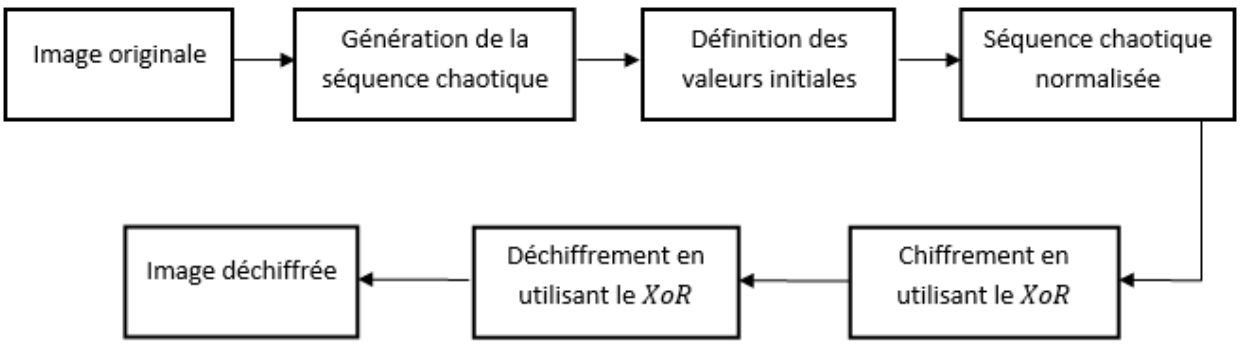
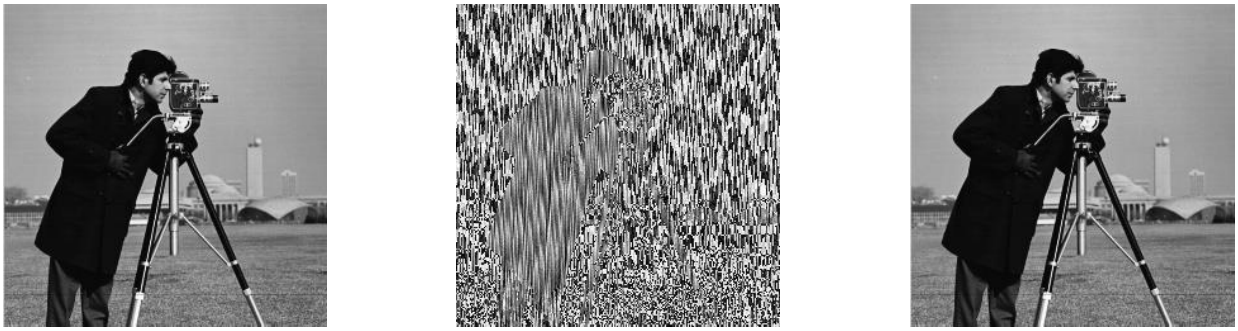


Figure 3.6 : Méthode proposée de chiffrement et de déchiffrement (Lorenz).

Les résultats obtenus après application de cet algorithme sont donnés par la Figure 3.7 :



(a) (b) (c)

Figure 3.7 : Chiffrement/déchiffrement. (a) image originale, (b) image chiffrée et (c) image déchiffrée.

8. Etude d'un système chaotique discret

Il existe plusieurs systèmes chaotiques discrets comme le système de Henon, la fonction de Tent et la fonction Gaussienne discrète, mais le système chaotique discret le plus commun est la fonction logistique qui est l'une des fonctions de Tchebychev.

La fonction logistique très connue dans la théorie des systèmes non linéaires, est une application non bijective du domaine [0, 1] dans lui-même qui sert de récurrence à la suite :

$$x_{n+1} = r x_n (1 - x_n) \tag{3.2}$$

où n = 0, 1, ... dénote le temps discret, x la variable dynamique et r un paramètre réel.

La dynamique de cette application correspond à un comportement très différent ; ainsi selon la valeur du paramètre r, une plus grande variété de régimes permanents se présente, parmi lesquelles on trouve, par ordre de complexité :

- Pour $0 < r < 3$, le système possède un point fixe attractif, il devient instable lorsque r = 3.
- Pour $3 < r < 3.57$, le système évolue périodiquement de période r^k, avec k un entier qui tend vers l'infini lorsque r tend vers 3.57.
- Pour r = 4, le système évolue de manière chaotique.

De même que pour le cas continu, nous présentons dans ce qui suit quelques propriétés du système chaotique discret (3.2).

8.1. Bifurcation

La Figure 3.7 représente le diagramme de bifurcation de la carte logistique créé en faisant varier le paramètre r de 2 à 4.

Comme nous pouvons le voir, il existe différentes régions en fonction de la valeur de r. Ceci est particulièrement intéressant à $r = 3$, car lorsque $r = 3{,}5699$ jusqu'à $r = 4$, la période commence à doubler, conduisant à une dynamique chaotique. Si on fait divers calculs pour voir l'évolution de la fonction paramétrée de r, on s'aperçoit qu'il existe une "chemin" d'un état - ordre - à un autre état - chaos -.

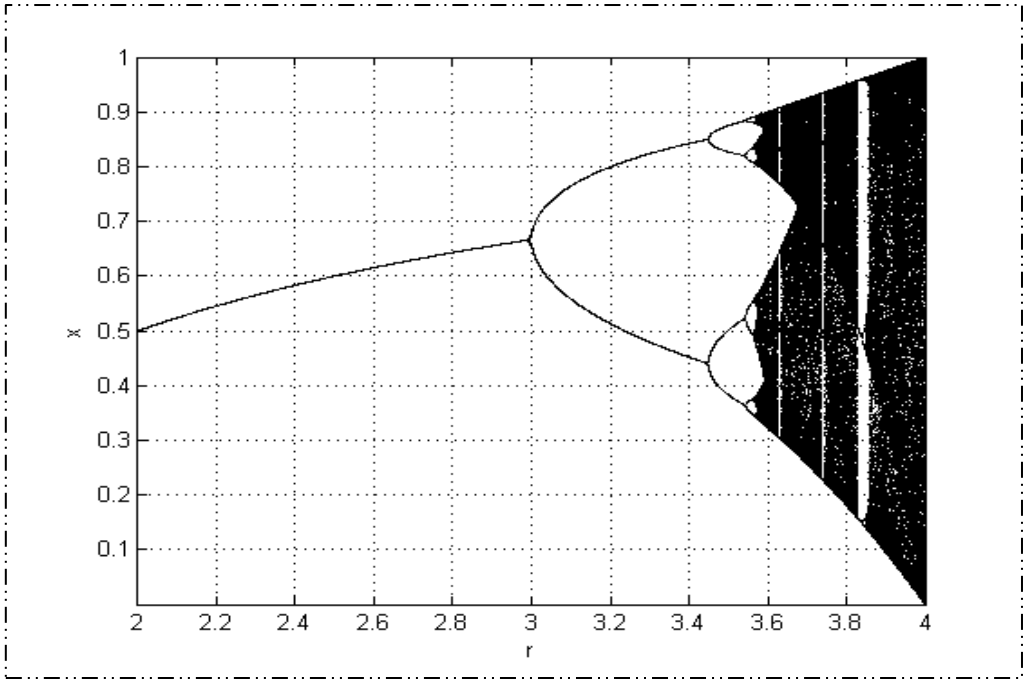


Figure 3.8 : Etude de comportement dynamique pour la fonction logistique.

8.2. Exposant de Lyapunov

Comme il a été déjà mentionné la fonction logistique présente un comportement chaotique à partir d'une valeur spécifique du paramètre r soit r = 4.

Après calcul de l'exposant de Lyapunov de fonction logistique :

$$x_{n+1} = 4x_n(1 - x_n) \tag{3.3}$$

On a obtenu la valeur $\lambda = ln2 > 0$, d'où le comportement chaotique.

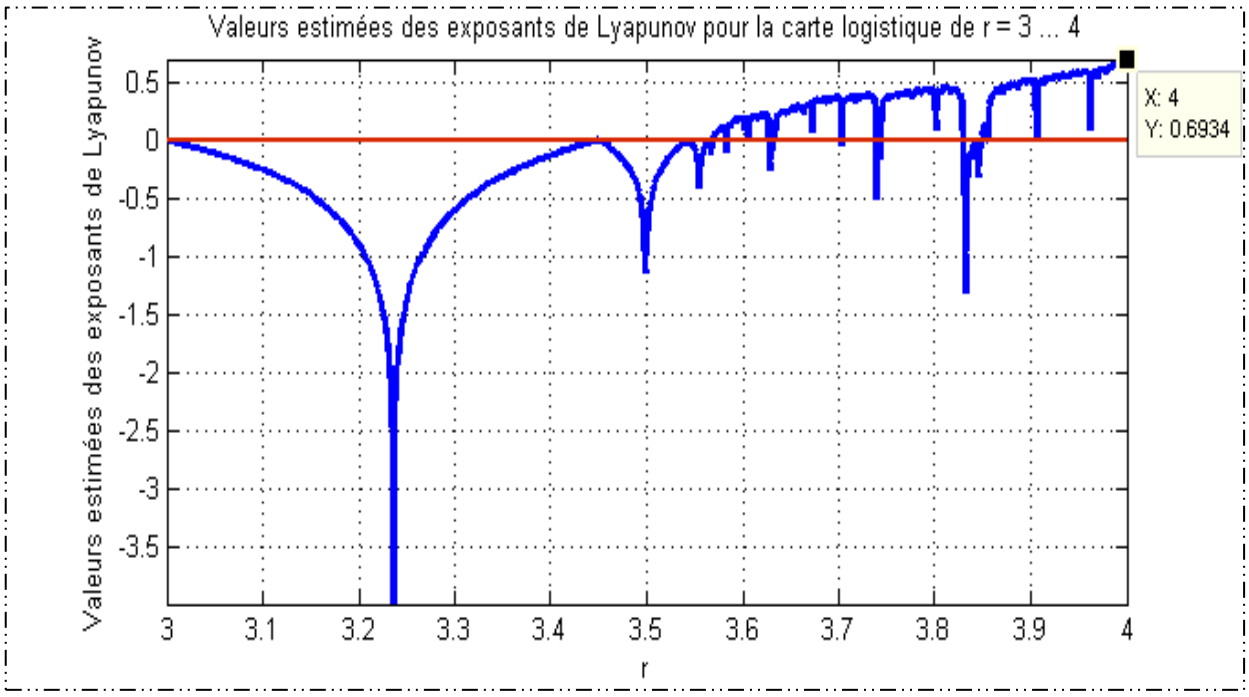


Figure 3.9 : Exposants de Lyapunov pour la carte logistique.

8.3. Chiffrement d'image par la fonction logistique

On s'intéresse aux algorithmes chaotiques 1D, proposés par Yen et Guo, qui sont la base de tous les autres algorithmes qui utilisent la fonction logistique $f(x) = rx(1-x)$, où la condition initiale $x(0)$ et le paramètre de control r jouent le rôle de la clé secrète. Ils sont basés sur l'idée de base suivante [27] :

- Exécution de la fonction logistique pour produire des séquences binaires pseudo-aléatoires $\{b(i)\}$, à partir de la représentation n bits de chaque état chaotique.

$$x(k)=b(nk+0)\times b(nk+1)\ldots b(nk+n-1) \qquad (3.4)$$

- Utilisation de ces séquences binaires chaotiques $\{b(i)\}$, pour contrôler les permutations, et les substitutions pseudo-aléatoires de chaque pixel de l'image.

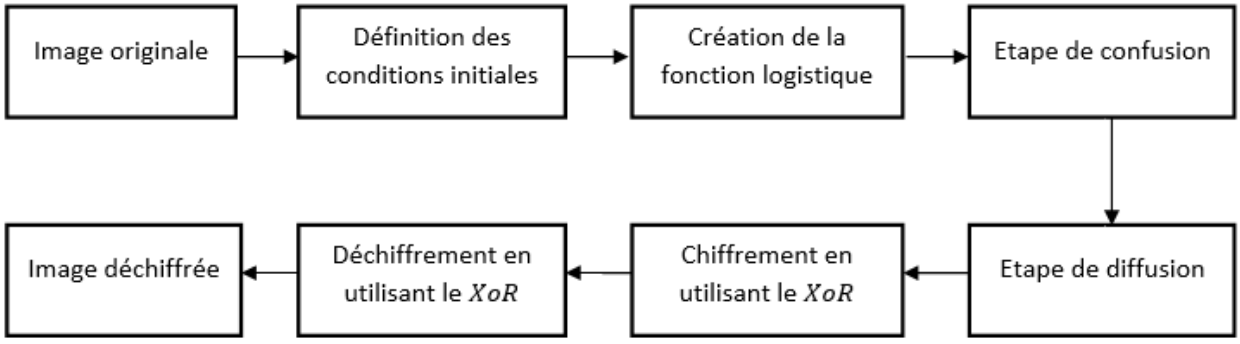
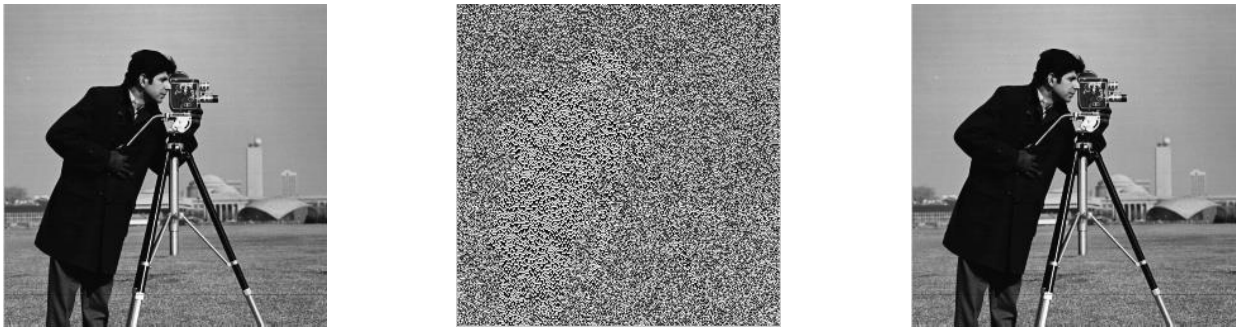


Figure 3.10 : Méthode proposée de chiffrement et de déchiffrement (fonction logistique).

Les résultats obtenus après l'application de notre algorithme ci-dessus sur l'image ''cameraman.tif'' utilisant la fonction logistique sont donnés dans la Figure 3.11 :



(a) (b) (c)

Figure 3.11 : Chiffrement/déchiffrement. (a) image originale, (b) image chiffrée et (c) image déchiffrée.

9. Mesures d'évaluation

La simple inspection visuelle s'avère être insuffisante pour juger la force d'un cryptosystème. L'analyse menée dans ce qui suit a alors pour but d'évaluer le degré de chiffrement des images [2].

9.1. Analyse statistique

9.1.1. Histogramme

L'histogramme d'une image est un graphique illustrant le nombre de pixels dans cette image à chaque valeur d'intensité trouvée. Pour une image au niveau de gris 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. Dans le contexte du chiffrement d'image numérique, l'histogramme de l'image chiffrée doit être uniforme et plat pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme [30].

Comme on peut le constater sur les histogrammes montrés dans la Figure 3.12, l'histogramme de l'image cryptée est uniformément réparti par rapport à l'histogramme de l'image d'origine. Ceci peut s'expliquer par le rôle de l'algorithme de chiffrement utilisé, qui assure que la dépendance des propriétés statistiques de l'image chiffrée et de l'image originale est quasi-aléatoire afin de rendre la cryptanalyse de plus en plus difficile, sauf que l'image chiffrée ne fournit aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir des attaques statistiques sur les méthodes de cryptage d'image fournies.

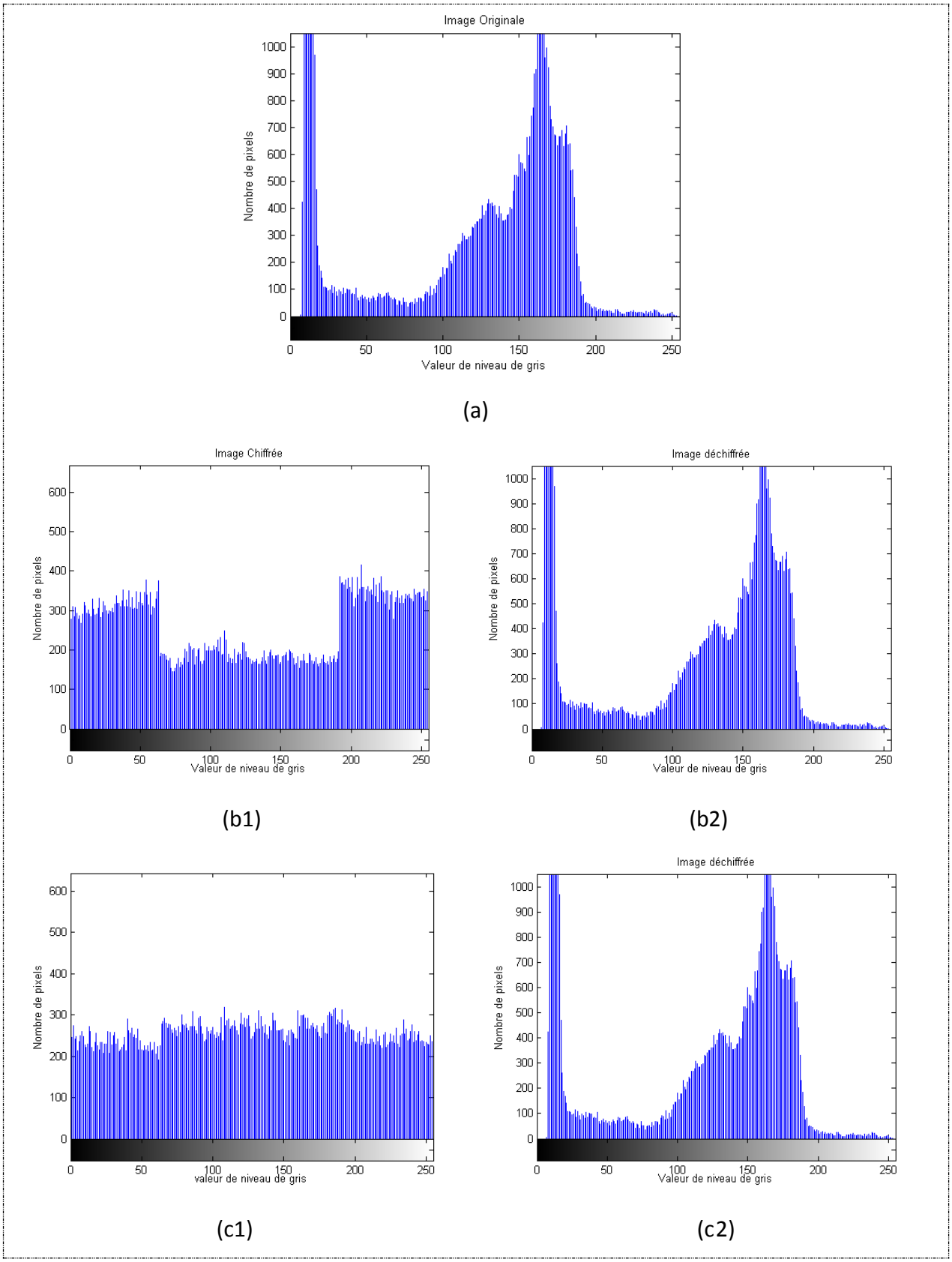


Figure 3.12 : Analyse de l'histogramme des images originales, chiffrées et déchiffrées (a) originale, (b1) (b2) chiffrée et déchiffrée par Lorenz, (c1) (c2) chiffrée et déchiffrée par la fonction logistique.

9.1.2. Corrélation entre les pixels adjacents

La corrélation est une technique qui permet de comparer et estimer les déplacements des pixels d'une image par rapport à une autre image de référence [31]. Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique, et les coefficients de corrélation de chaque paire sont calculés avec la formule suivante :

$$r = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3.5}$$

où :

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{3.6}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \tag{3.7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{3.8}$$

avec :

$\boldsymbol{r}$: la corrélation, $\boldsymbol{cov}$: la covariance, $\boldsymbol{E}$: l'espérance, $\boldsymbol{D}$: la variance, $\boldsymbol{x}, \boldsymbol{y}$ **:** les valeurs des pixels des images.

Le résultat du calcul est une valeur réelle appartenant à l'intervalle [0 : 1]. Si le coefficient est égal à (1), donc les deux images sont similaires. Sinon, si la valeur obtenue est égale à (0) ou proche de (0) alors les deux images sont différentes.

Les résultats statistiques obtenus par le chiffrement par la fonction continue et la fonction discrète sont représentés dans la Figure 3.12 :

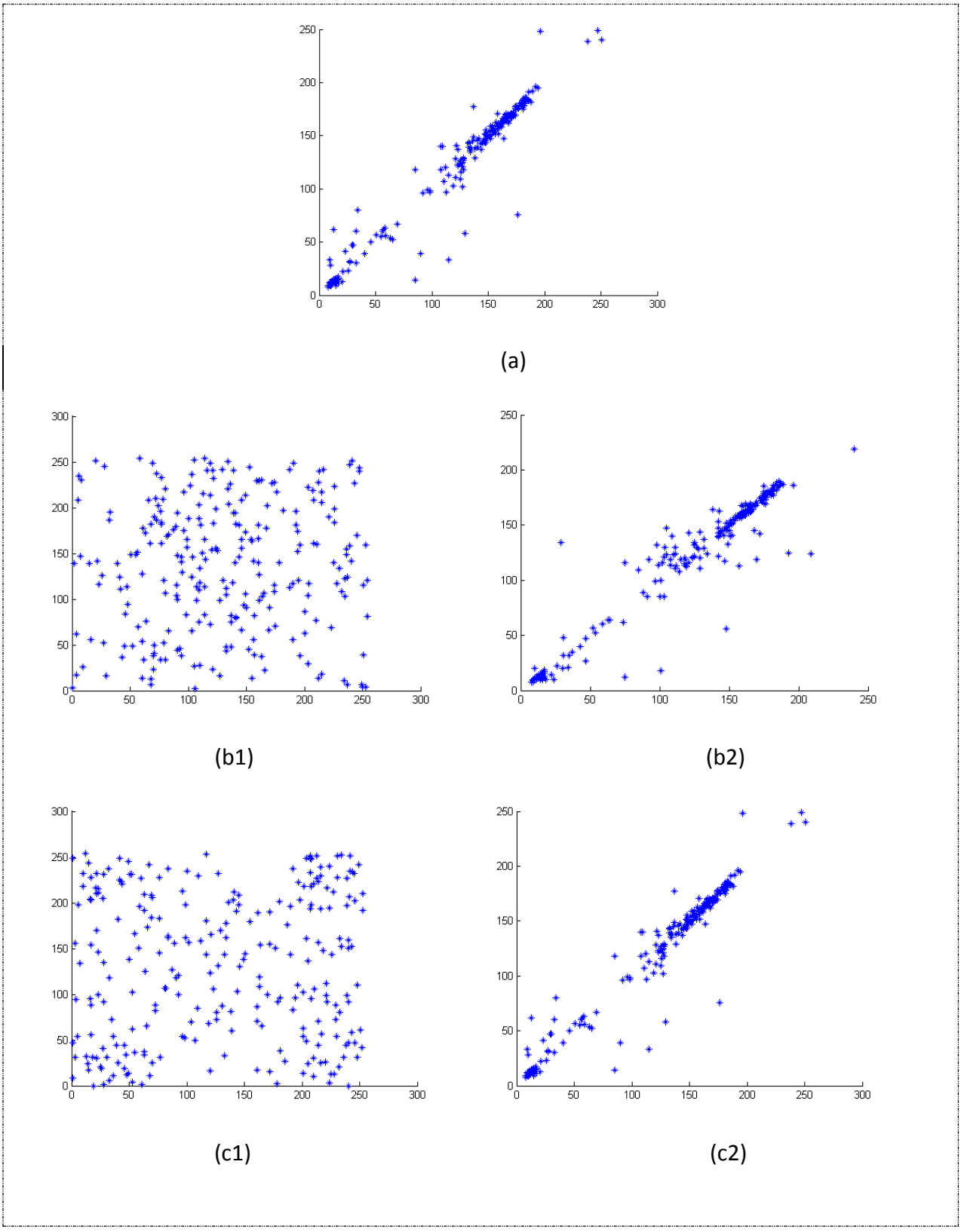


Figure 3.13 : Corrélation de deux pixels adjacents (a) Image originale, (b1) (b2) Images chiffrées et déchiffrées par Lorenz, (c1) Images chiffrées et déchiffrées par la carte logistique.

Les calculs des coefficients de corrélation sont montrés dans le Tableau 3.2 :

Type de chaos	Image originale	Image chiffrée
Système de Lorenz	0.9374	0.0362
La carte logistique	0.9485	0.0208

Tableau 3.2 : Coefficients de corrélation des pixels adjacents entre les images originales et celles chiffrées.

9.2. Analyse différentielle

9.2.1. Entropie

Selon la théorie de Shannon [32], l'entropie de l'information est la quantité d'information absorbée ou libérée par une source d'information. En particulier, plus la source est redondante, moins elle contient d'informations [33]. Sans contraintes spécifiques, l'entropie est maximale pour les sources où tous les symboles sont également probables. C'est donc l'un des principaux indicateurs pour mesurer le caractère aléatoire de l'information. Une valeur d'entropie élevée présente un degré élevé de caractère aléatoire. La formule utilisée pour calculer l'entropie de la source (m) est donnée par :

$$H(N) = \sum_{i=0}^{2^n-1} p(m_i) \log_2\left(\frac{1}{p(m_i)}\right) \tag{3.9}$$

où m_i représente les valeurs des pixels, $p(m_i)$ est la probabilité du symbole m_i et n est le nombre total des pixels dont la valeur est 256 pour les images en niveaux de gris.

Donc, pour le cas des images au niveau de gris, l'entropie doit être très proche de 8.

Les valeurs obtenues après l'application des algorithmes précédents sont données dans le tableau ci-après :

Cryptosystème	Image originale	Image chiffrée
Système de Lorenz	7.0097	7.9335
La carte logistique	7.0097	7.9930

Tableau 3.3 : Valeurs de l'entropie des images originales et chiffrées pour les deux cryptosystèmes.

9.2.2. Erreur quadratique moyenne (MSE)

Le critère de ressemblance est toujours utilisé pour comparer l'image originale I avec l'image chiffrée $\hat{I}$. Ce critère est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et dégradés [34] :

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} (I(m,n) - \hat{I}(m,n))^2 \quad (3.10)$$

où $(M \times N)$ est la taille de l'image, I_p et $\hat{I}_p$ sont les amplitudes des pixels sur les images originale et chiffrée respectivement.

9.2.3. Rapport crête signal sur bruit (PSNR)

Le rapport signal à bruit de crête (Peak Signal to Noise Ratio) représente la mesure de distorsion. Il est largement utilisé dans le traitement d'images pour mesurer la qualité d'une image en calculant le rapport entre l'image originale et le bruit. Il est mesuré en décibels (dB) :

$$PSNR = 10 \times \log_2 \left(\frac{{I_{max}}^2}{MSE} \right) \quad (3.11)$$

Pour une image à niveau de gris, I_{max} désigne la luminance maximale possible ; et MSE est l'erreur quadratique moyenne.

Si MSE est égale à zéro, cela signifie que l'image originale et celle après traitement sont identiques et la valeur du $PSNR$ sera infinie. Plus ce rapport est grand, meilleure est la qualité d'algorithme de chiffrement.

Un $PSNR$ élevé, indique que l'image modifiée est très proche de l'originale. Une valeur de plus de $20\ dB$ est acceptable (varie dans différents cas selon le type de problème). Cependant, le $PSNR$ fonctionne pour la comparaison d'intensité et ne fournit aucune information structurelle [35].

Les valeurs de MSE et $PSNR$ pour les deux systèmes de chiffrement sont données dans le tableau ci-dessous :

Type de chaos	MSE	PSNR (db)
Système de Lorenz	100.6779	28.1355
La carte logistique	107.5199	27.8499

Tableau 1.4 : Valeurs de MSE et $PSNR$ pour les deux systèmes de chiffrement.

Conclusion

Dans ce chapitre, nous avons analysé la sécurisation des données par le chiffrement et déchiffrement de l'image cameraman qui est en niveau de gris, en utilisant deux algorithmes, le premier est basé sur le système continu de Lorenz et le deuxième basé sur la carte logistique (système discret). Les critères d'évaluation de robustesse sur lesquels nous nous sommes basés sont : l'histogramme, la corrélation des pixels, l'entropie, MSE et $PSNR$.

Les résultats obtenus montrent que l'algorithme de la carte logistique présente les meilleures performances en chiffrement vue la distribution uniforme de l'histogramme de l'image chiffrée. On parle ici de dépendance des propriétés statistiques de l'image chiffrée et originale. Dans ce cas la probabilité qu'un cryptanalyste puisse exploiter l'histogramme de l'image chiffrée pour tirer une information utile est quasiment nulle.

Le prochain et dernier chapitre est consacré à la sécurisation de données par les systèmes hyperchaotiques.

Chapitre 4

Sécurisation par systèmes hyperchaotiques

1. Introduction

Le défi et la nécessité de sécuriser parfaitement les informations dans les réseaux informatiques et de communication ont motivés les chercheurs à accroître les efforts et à développer d'autres techniques de cryptage efficaces et rapides basées sur le chaos. En effet, plusieurs techniques de cryptage ont été proposées dans la littérature. Dans ces techniques, le signal chaotique est utilisé pour masquer les messages à transmettre par des systèmes chaotiques possédant un seul exposant de Lyapunov positif. Plusieurs chercheurs ont prouvé que ce masquage n'est pas toujours efficace. Pour remédier à ce problème, de nouveaux systèmes hyperchaotiques de dimension élevée ont été considérés dans la conception des techniques de cryptage plus robustes et plus adaptées aux applications récentes des services de communications modernes.

En général, un système hyperchaotique est un système chaotique qui possède au moins deux exposants positifs. Le comportement dynamique des systèmes hyperchaotiques va donc être très compliqué, c'est pour cela que ces systèmes offrent plus de sécurité dans la communication chaotique.

Dans ce chapitre, nous présentons en premier lieu un système hyperchaotique 6D et la suite de Fibonacci. Puis, nous donnerons leurs utilisations dans le crypto-système développé dans notre travail. Enfin, une analyse et une étude des performances de l'algorithme proposé sont effectuées.

2. Cryptosystèmes hyperchaotiques

Les systèmes de chiffrement chaotique des images numériques sont classés en deux classes principales. La première classe comprend les systèmes de faible dimension comme les cartes chaotiques 1D. La deuxième classe comporte les systèmes de haute dimension, comme les systèmes hyperchaotiques.

Les systèmes de chiffrement de faible dimension sont spécialement désignés pour les données texte et pour les flux des données binaires et non pas pour les données multimédias. En plus, plusieurs travaux ont suggéré que ces méthodes de chiffrement ne sont pas des plateformes adéquates pour chiffrer les images.

Il existe plusieurs types de cryptage basé sur les systèmes hyperchaotiques, tels que [36–38]. Chen et Hu [39] ont proposé une méthode de chiffrement des images médicales utilisant une carte logistique sinusoïdale pour le processus de confusion. L'image chiffrée est divisée en blocs

où un système hyperchaotique est utilisé pour diffuser les blocs d'image. Chai et al. [40] ont utilisé un système hyperchaotique (memristive chaotic) dans le chiffrement d'image, qui a amélioré sa capacité à résister contre l'attaque différentielle. Chai et al. [41] ont présenté un nouvel algorithme de chiffrement d'images basé sur le système chaotique paramétrique utilisant les automates cellulaires élémentaires et la compression de bloc. Tsafack et al. [42] ont conçu un nouveau circuit chaotique 4D et l'ont appliqué au chiffrement d'images. Ramasamy et al. [43], ont proposé un nouvel algorithme basé sur le cryptage par blocs (scrambling) et la transformation zigzag pour le chiffrement d'image. Dans cet algorithme, la clé a été générée à partir de la carte ELTM (Enhanced Logistic-Tent Map) pour diffuser l'image chiffrée.

Malgré le succès de ces techniques, elles présentent certaines limites qui peuvent être résumées comme suit [44]:

1. Faible espace de clés et moins de sensibilité aux conditions initiales.
2. La condition initiale de la carte chaotique ne dépend pas de l'image originale qui conduit à des faiblesses dans la résistance aux attaques différentielles.
3. Certains de ces algorithmes ne résistent pas aux attaques statistiques car l'histogramme de l'image chiffrée n'est pas plat.

Ces limites ont motivé K.M. Hosny, et al. [44] pour proposer un nouvel algorithme de cryptage des images. Cet algorithme (HC-Q) utilise un système hyperchaotique à 6 dimensions et la matrice Q de Fibonacci pour chiffrer les images numériques.

3. Système hyperchaotique 6D

Généralement, l'analyse mathématique montre que les fonctions chaotiques sont non linéaires avec un comportement dynamique. Par conséquent, leurs réponses sont imprévisibles. Des études antérieures montrent que le comportement dynamique des fonctions hyperchaotiques est beaucoup plus compliqué que celui correspondant des fonctions chaotiques de faible dimension. Un système hyperchaotique devrait avoir au moins quatre dimensions. De plus, les fonctions chaotiques de faible dimension ne contiennent qu'un seul exposant de Lyapunov positif, alors que les systèmes hyperchaotiques en ont au moins deux.

Wang et Yu [45] ont défini le système hyperchaotique 6D comme suit :

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) + x_4 - x_5 - x_6 \\ \dot{x_2} = cx_1 - x_2 - x_1x_3 \\ \dot{x_3} = bx_3 + x_1x_2 \\ \dot{x_4} = dx_4 + x_2x_3 \\ \dot{x_5} = ex_6 + x_3x_2 \\ \dot{x_6} = rx_1 \end{cases} \quad (4.1)$$

où a, b, c, d, e et r sont des constants ; x_1, x_2, x_3, x_4, x_5 et x_6 font référence aux variables d'état du système $6D$ hyperchaotique.

Dans ce chapitre, les valeurs constantes sélectionnées sont $a = 10$, $b = \frac{8}{3}$, $c = 28$, $d = -1$, $e = 8$ et $r = 3$. Cette sélection garantit que le système a deux exposants de Lyapunov positifs qui remplissent la condition (la somme de tous les exposants est négative).

4. Matrice Q de Fibonacci

Les éléments de la suite de Fibonacci, F_n sont :

$$F_n = F_{n-1} + F_{n-2}, n > 1 \quad (4.2)$$

où $F_1 = F_2 = 1$.

La matrice Q de Fibonacci est donnée par :

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad (4.3)$$

La n ième puissance de la matrice Q de Fibonacci est la matrice définie par :

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \quad (4.4)$$

où F_n est le nombre de Fibonacci, et les déterminants de la matrice Q de Fibonacci sont :

$$Det(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n \quad (4.5)$$

La matrice inverse Q^{-n} a la forme suivante :

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix} \quad (4.6)$$

5. Algorithme de chiffrement HC-Q

L'algorithme HC-Q [44] utilise un système hyperchaotique 6D et la matrice Q de Fibonacci pour chiffrer/déchiffrer une image numérique. Étant donné que le système hyperchaotique 6D a une haute dynamique complexe comportements et deux exposants de Lyapunov positifs, son utilisation améliore les performances du chiffrement et augmente le niveau de sécurité. La matrice Q de Fibonacci est très simple, rapide et capable de diffuser l'image chiffrée. L'organigramme du chiffrement/déchiffrement HC-Q est illustré dans la figure (4.1).

5.1. Chiffrement

Le cryptage repose sur deux étapes : la confusion et la diffusion. Les arrangements et les valeurs des pixels sont respectivement modifiés dans ces processus. L'étape de confusion est basée sur le système hyperchaotique 6D. Tout d'abord, on calcule la condition initiale du système qui est basé sur l'image originale. Ensuite, un nouveau vecteur est obtenu en itérant le système hyperchaotique, puis on sélectionne trois séquences ($x_1, x_3\ et\ x_5$). Ce vecteur est trié, et la position des nombres triés est utilisée pour confondre l'image originale. Après avoir confondu l'image originale, l'étape de diffusion est effectuée pour obtenir l'image chiffrée. Dans cet algorithme, la diffusion est basée sur la matrice Q de Fibonacci. L'image chiffrée est divisée en blocs, chacun de taille 2 × 2, puis chaque bloc est diffusé à l'aide de la matrice Q de Fibonacci. Deux tours d'étapes de confusion et de diffusion sont effectuées pour obtenir l'image cryptée. L'algorithme (a) dans la figure 4.1 décrit les étapes de chiffrement.

5.2. Déchiffrement

Les étapes de décryptage sont l'inverse des étapes de cryptage. L'image originale peut être récupéré à partir de l'image chiffrée en procédant comme suit :

1. L'image cryptée (C) est divisée en blocs, chacun de taille 2 × 2, puis l'équation de diffusion avec Q^{-10} est appliquée aux blocs d'image en utilisant l'équation suivante :

$$\begin{bmatrix} D'_{i,j} & D'_{i,j+1} \\ D'_{i+1,j} & D'_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} C_{i,j} & C_{i,j+1} \\ C_{i+1,j} & C_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix} mod\ 256 \quad (4.7)$$

où $i = 1:3:5 \ldots : M$ et $j = 1:3:5 \ldots : N$.

2. L'image chiffrée (D) obtenue à l'étape précédente est convertie en vecteur W.

3. Le vecteur S généré à l'étape de cryptage est utilisé pour ramener chaque pixel à sa position d'origine par l'équation suivante :

$$ER(S_i) = W_i\ ,\ i = 1\ :\ MN \tag{4.8}$$

4. Convertir le vecteur ER en matrice pour obtenir l'image décryptée (D).

5. Deux tours d'étapes de décryptage sont effectuées pour obtenir l'image décryptée.

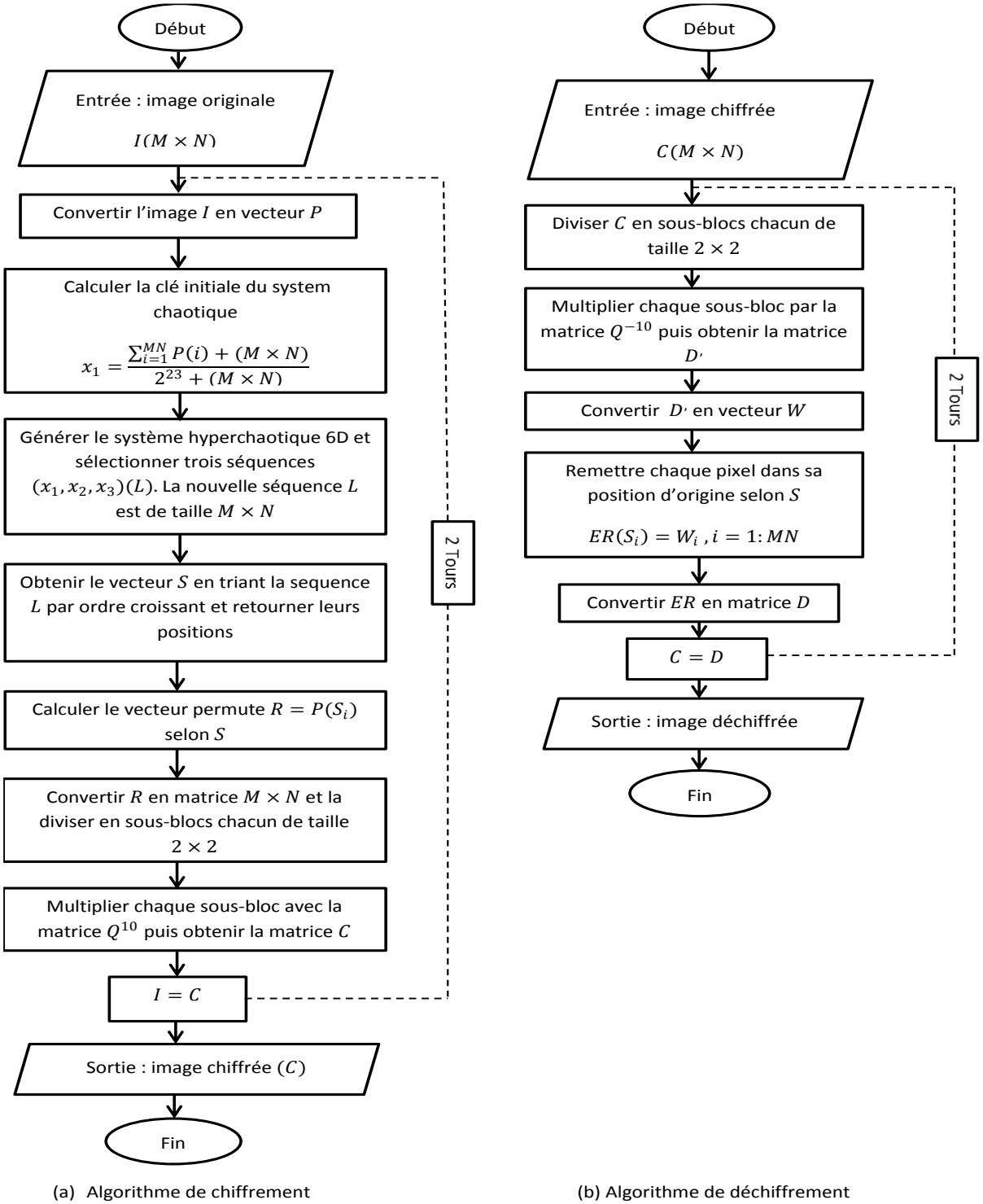


Figure 4.1 : Organigramme de l'algorithme HC-Q.

6. Algorithme proposé

La confusion dans l'algorithme proposé est réalisée en utilisant une carte chaotique à deux dimensions pour rendre la substitution entre les positions des pixels plus complexe. Pour cet objectif, plusieurs cartes chaotiques peuvent être utilisées : la carte standard, la carte de Baker ou la carte Cat. Dans ce travail, la carte Cat (Cat map) a été sélectionnée en raison de sa simplicité par rapport aux autres cartes.

6.1. Arnold's Cat Map

Dans les années 1960, Vladimir Arnold a découvert une carte chaotique en deux dimensions. L'effet de la carte a été vérifié en utilisant une image d'un chat, c'est pour cette raison que la carte a été appelée la carte du chat d'Arnold. La carte du chat d'Arnold est décrite comme suit [46] :

$$\begin{bmatrix} i_{new} \\ j_{new} \end{bmatrix} = \begin{bmatrix} 1 & v \\ u & 1 + u * v \end{bmatrix} * \begin{bmatrix} i \\ j \end{bmatrix} \ mod\ M \tag{4.9}$$

où : i et j représentent les coordonnées d'un pixel. i_{new} et j_{new} sont les nouvelles coordonnées d'un pixel. (u) et (v) sont les paramètres de la carte du chat d'Arnold (clés de la carte). M représente le nombre de lignes et le nombre de colonnes ($M = Nx = Ny$; Nx est le nombre de lignes, Ny est le nombre de colonnes).

Une propriété intéressante de la carte du chat est le théorème de Récurrence de Poincaré. Cela signifie qu'après un certain nombre d'itérations (fréquence), la carte du chat retournera à son état d'origine. La période dépend des paramètres (u) et (v) et de la taille de l'image. Un exemple de la carte chat est représenté dans la figure 4.2. On remarque que la période est égale à 100 itérations.

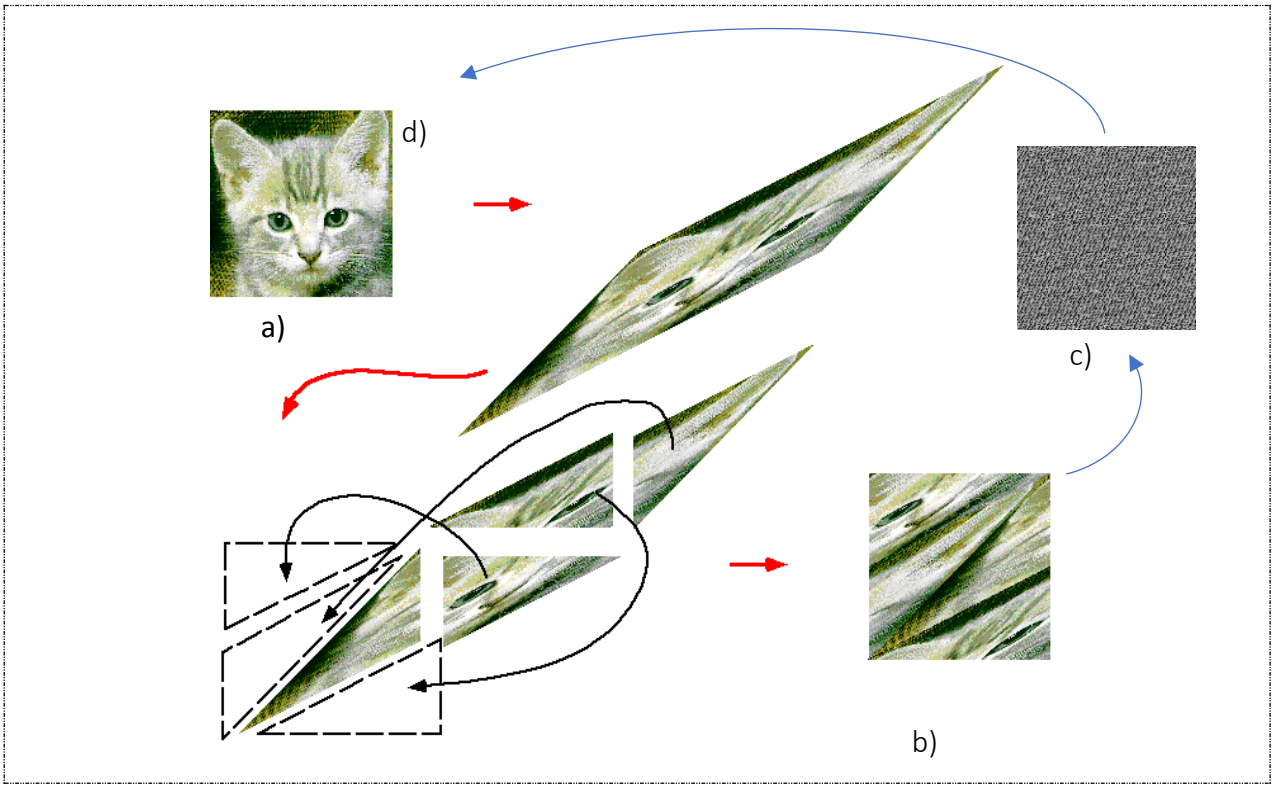


Figure 4.2 : Effet de la carte chaotique chat sur une image. (a) : image originale ; (b) image mélangée par la carte après une seule itération ; (c) image mélangée par la carte après 80 itérations et (d) image mélangée par la carte après 100 itérations.

6.2. Méthode de l'algorithme proposé

Le schéma fonctionnel de l'algorithme proposé est donné dans la figure 4.3. La technique est une combinaison entre l'algorithme HC-Q et la carte chaotique Cat map pour améliorer le niveau de sécurité.

Les étapes de chiffrement de cet algorithme sont :

1) Calculer la fréquence (F) de l'image originale, dans notre cas la fréquence $F = 84$.
2) Etape de confusion : Mélanger les positions des pixels en utilisant la carte Cat map. On réalise 70 itérations de la fonction Cat map sur l'image originale.
3) Etape de diffusion et génération de clés : La diffusion et la génération de clés sont réalisées par l'algorithme HC-Q. Dans cette étape, on chiffre l'image perturbée par la fonction Cat map au lieu de l'image originale.

Pour le processus de déchiffrement, nous introduisons les fonctions inverses pour les différents blocs de chiffrement. Ensuite, on effectue 14 itérations sur l'image déchiffrée pour trouver l'image originale.

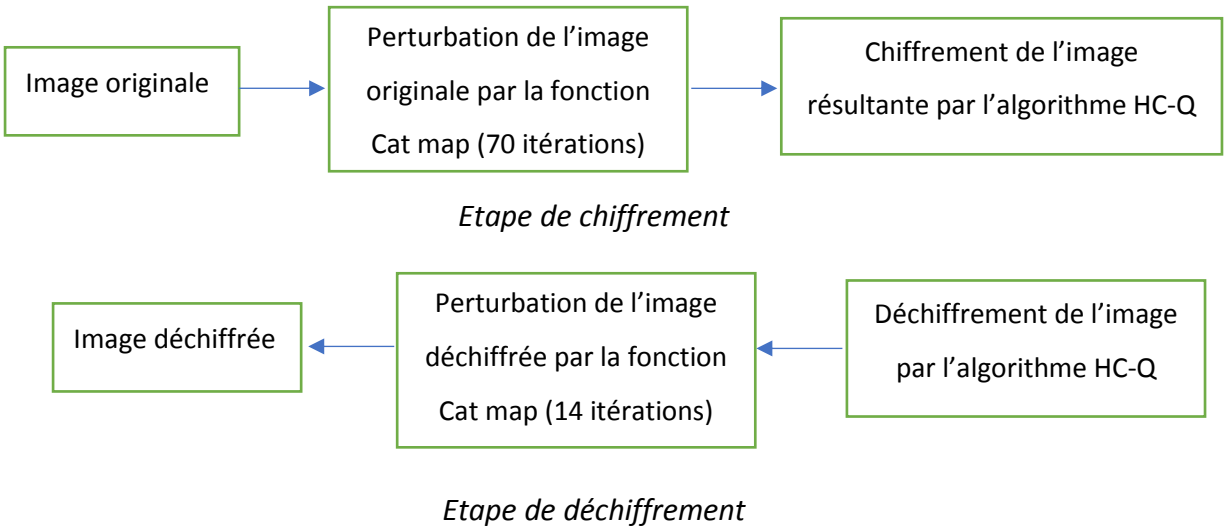
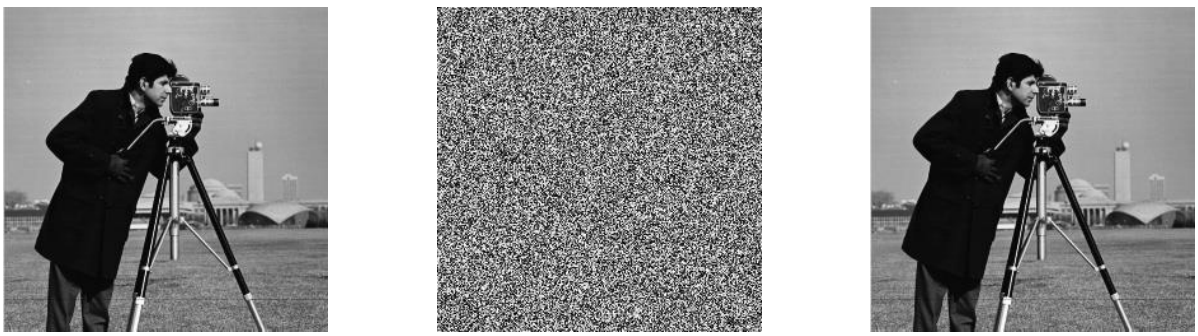


Figure 4.3 : Méthode proposée de chiffrement et de déchiffrement.

7. Résultats et interprétations

L'efficacité des algorithmes étudiés dans ce travail a été testée en utilisant l'image cameraman qui est en niveau de gris et de taille 256×256. Toutes les expériences ont été réalisées sous logiciel MATLAB (R2011a) sur un ordinateur portable équipé d'un processeur Core i5-4310M 2,7 GHz et de 8 Go de RAM.

La figure 4.4 illustre l'image cameraman.tif originale (à gauche), l'image chiffrée obtenue après application de l'algorithme de cryptage HC-Q (au milieu) et l'image déchiffrée (à droite).



(a) (b) (c)

Figure 4.4 : Chiffrement/Image cameraman (a) originale, (b) chiffrée et (c) déchiffrée.

Les résultats obtenus avec l'algorithme de chiffrement/déchiffrement HC-Q amélioré sont montrés dans la figure 4.5. L'image (b) est l'image cameraman après 70 itérations de fonction Cat map, c'est cette image qu'on chiffre au lieu de l'image originale, le résultat de chiffrement est donné par la figure (c). Chez le récepteur, après le déchiffrement de l'image chiffrée avec les mêmes clés de chiffrement, il obtient l'image (d). Le récepteur doit effectuer 14 itérations de fonction Cat map sur l'image déchiffrée pour trouver l'image souhaitée (image originale).

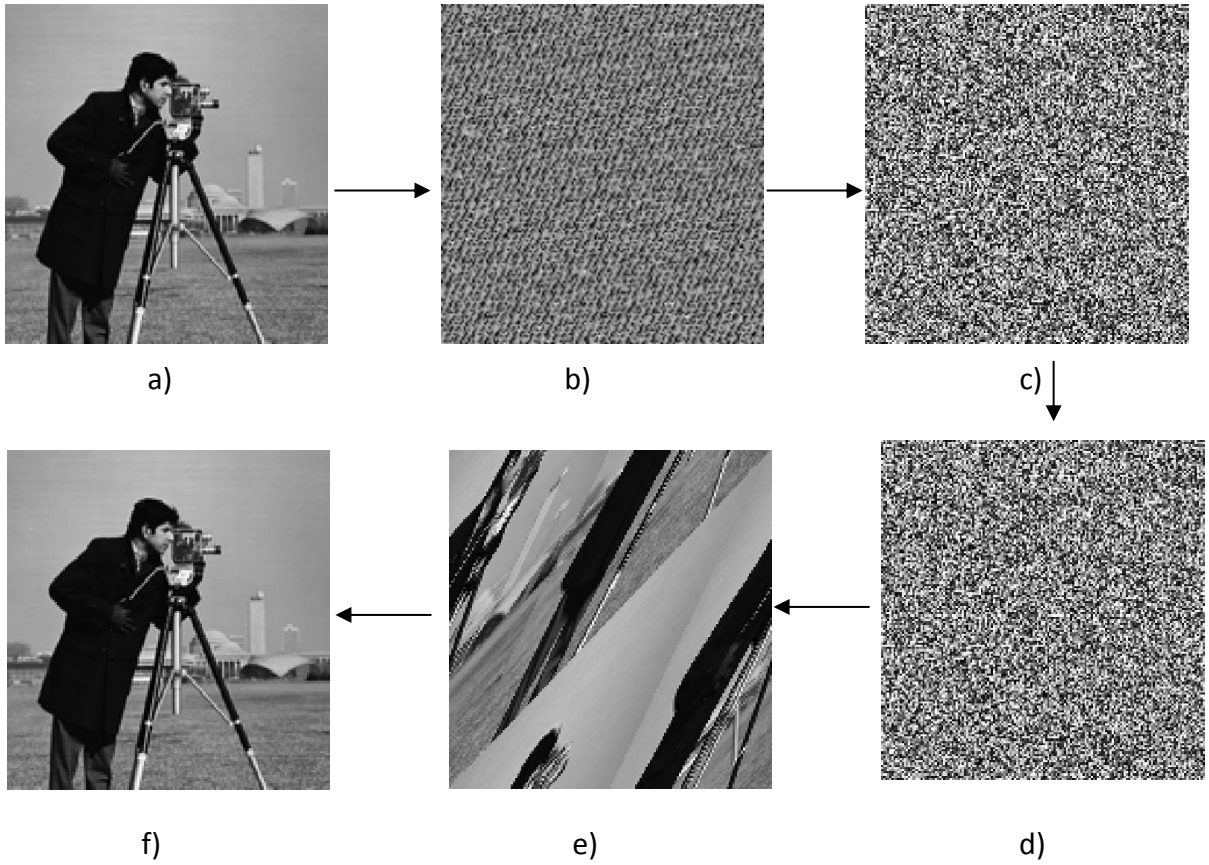


Figure 4.5 : Chiffrement et déchiffrement avec l'algorithme proposé.
a) Image originale, b) cameraman Cat map après 70 itérations, c) cameraman Cat map chiffrée, d) cameraman Cat map déchiffrée, e) cameraman Cat map déchiffrée après 13 itérations et f) cameraman déchiffrée.

A partir de ces images, nous constatons visuellement que les images chiffrées sont suffisamment brouillées. En conséquence, la méthode de chiffrement proposée a une sécurité perceptuelle satisfaisante vis-à-vis du test subjectif, cela ne suffira pas puisqu'un crypto-système chaotique d'image peut être cassé avec succès à l'aide de l'attaque statistique. Pour prouver la robustesse des algorithmes étudiés dans ce chapitre contre ces attaques statistiques, une analyse

statistique a été effectuée en utilisant l'analyse des histogrammes, l'analyse des coefficients de corrélation et l'analyse d'entropie.

7.1. Analyse des histogrammes

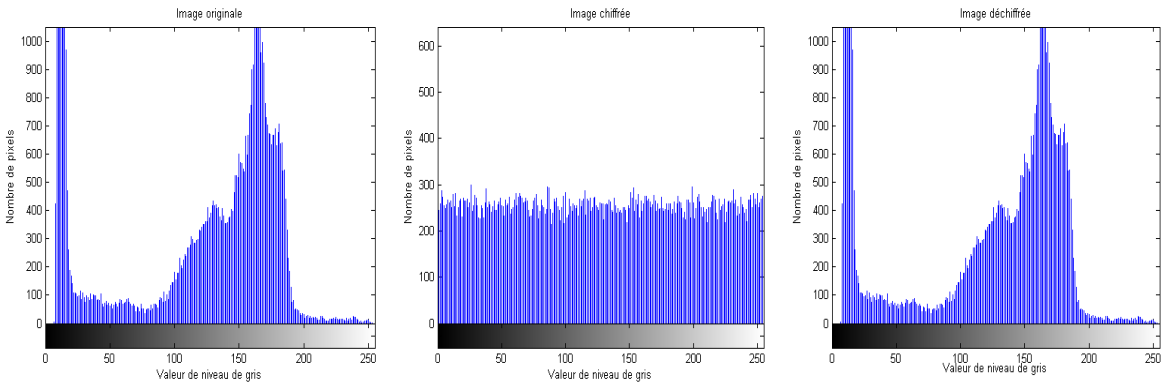
L'histogramme de l'image chiffrée doit avoir deux propriétés [47] :

1. Il doit être totalement différent de l'histogramme de l'image originale.
2. Il doit avoir une distribution uniforme et plate, ce qui signifie que la probabilité d'occurrence de n'importe quelle valeur est la même.

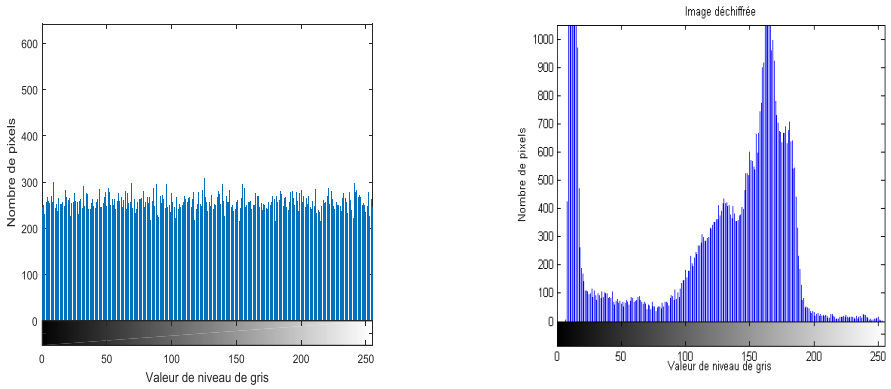
La figure 4.6 a) donne l'histogramme de l'image en clair. Les figures 4.6 b) et c) représentent les histogrammes des images chiffrées et déchiffrées par l'algorithme HC-Q. De même, les figures 4.6 d) et e) représentent les histogrammes des images chiffrée et déchiffrée par l'algorithme HC-Q amélioré.

Les histogrammes des images chiffrées sont entièrement différents de l'histogramme de l'image originale. Il est bien observable que les deux algorithmes respectent les propriétés requises pour les histogrammes des images chiffrées. En outre, les histogrammes des images chiffrées ressemblent bien à un bruit blanc uniforme (tous les pixels ont la même chance d'apparition). Cela confirme que les deux méthodes de chiffrement ne sont pas vulnérables à l'attaque statistique par l'analyse d'histogrammes.

De même, les histogrammes des images déchiffrées sont similaires à celui de l'image originale.



a) b) c)



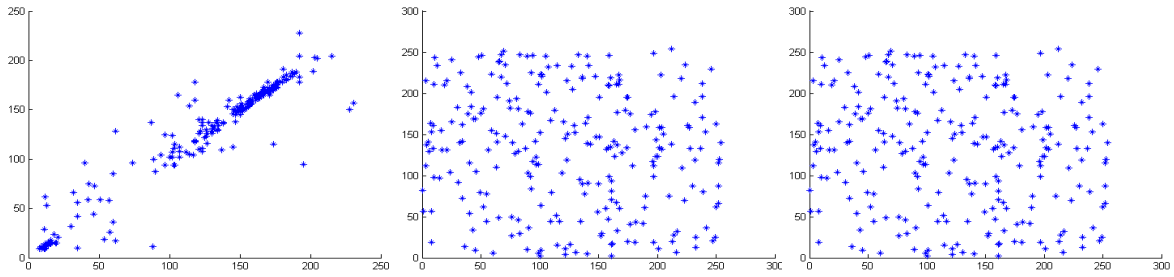
d) e)

Figure 4.6 : Histogrammes des images originale, chiffrées et déchiffrées par les deux algorithmes. a) Image originale, b), c) chiffrée/déchiffrée par HC-Q et d), e) chiffrée/déchiffrée par HC-Q amélioré.

7.2. Analyse de la corrélation entre pixels adjacents

Les pixels adjacents d'une image en clair ont une forte corrélation. Un bon système de chiffrement d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique basée sur la corrélation des pixels adjacents. Afin de tester la performance de notre crypto-système, nous avons choisi au hasard 1000 pixels de l'image en clair et leurs correspondants dans l'image cryptée puis calculé les différents coefficients de corrélation et comparer ces mesures avec celles de l'image originale correspondante.

La figure 4.7 représente respectivement les distributions des corrélations des pixels adjacents de l'image originale et l'image chiffrée pour les deux algorithmes. A partir de cette figure, nous remarquons que la distribution des intensités des pixels de l'image originale se concentre sur la diagonale, les pixels sont alors fortement corrélés, tandis que ceux des images chiffrées sont non-corrélés et ont des distributions uniformes.



a) b) c)

Figure 4.7 : Corrélation entre pixels adjacents.

a) image originale, b) image chiffrée par HC-Q et c) image chiffrée par HC-Q amélioré.

Ces propriétés de corrélation élevée peuvent être quantifiées en tant que coefficient de corrélation pour la comparaison. Le Tableau 4.1 présente les coefficients de corrélation des images en claire et chiffrées utilisant les deux algorithmes. Nous pouvons clairement remarquer que les valeurs des coefficients de corrélation sont proches de 1, cela signifie que les images en clair sont fortement corrélées. Cependant les valeurs des coefficients de corrélation des images cryptées sont proches de 0 (0.0497 pour l'algorithme HC-Q et 0.0311 pour l'algorithme proposé). Se basant sur ces résultats, on peut confirmer que l'algorithme proposé a supprimé avec succès la corrélation des pixels adjacents. Ainsi, il est plus performant que l'algorithme HC-Q car il résiste mieux aux attaques basées sur la corrélation des pixels adjacents.

Image originale	Image chiffrée par algorithme HC-Q	Image chiffrée par algorithme proposé
0.9136	0.0497	0.0311

Tableau 4.1 : Coefficients de corrélation des pixels adjacents entre l'image originale et celles chiffrées.

7.3. Analyse de l'entropie de l'information

Le Tableau 4.2 montre les différentes valeurs d'entropie obtenues des images chiffrées par les deux méthodes de chiffrement. Il est clair que les valeurs d'entropie de ces images sont très proches de la valeur idéale (la valeur idéale égale à 8). Une très bonne valeur de l'entropie est trouvée avec l'algorithme proposé, cela signifie que, les pixels de l'image chiffrée sont statistiquement indépendants les uns des autres. Par conséquent, nous pouvons confirmer que l'algorithme proposé fournit les meilleures propriétés d'aléatoire des données.

Image chiffrée par l'algorithme HC-Q	Image chiffrée par l'algorithme HC-Q modifié
7.9971	7.9991

Tableau 4.2 : Valeurs de l'entropie pour les deux algorithmes.

7.4. Analyse par PSNR

Le Tableaux 4.3 donne les valeurs de $PSNR$ entre l'image originale et l'image chiffrée ou déchiffrée pour les deux algorithmes.

Algorithme utilisé	PSNR (Originale et chiffrée)	PSNR (Originale et déchiffrée)
HC-Q	27.8016	∞
HC-Q modifié	26.8521	∞

Tableau 4.3 : Valeurs de PSNR d'images entre les images originale et chiffrées ou déchiffrées.

D'après le tableau précédent, on voit clairement que l'image originale est différente de l'image chiffrée (la valeur de PSNR est inférieure à 35) cependant elle est parfaitement reconstruite avec les deux algorithmes. En plus, le système de cryptage par la méthode proposée a une valeur de PSNR inférieure à celle de l'algorithme HC-Q, ce qui prouve que la méthode proposée est mieux résistante aux attaques par analyse différentielles.

7. Conclusion

Dans ce chapitre, nous avons présenté deux algorithmes de cryptage basés sur l'hyperchaotique et la matrice Q de Fibonacci. Ainsi, après une brève introduction des différentes étapes de chiffrement et de déchiffrement nous avons soumis l'algorithme proposé à plusieurs tests et analyses pour vérifier sa robustesse vis à vis des attaques communes. Ces critères sont l'histogramme, la corrélation des pixels adjacents, le PSNR et l'entropie.

Les résultats de simulation ont démontré que l'algorithme de cryptage proposé à base de la carte chaotique Cat map présente de très bonnes performances en termes de sécurité et peut ainsi résister aux diverses attaques basées sur les analyses statistiques et différentielles.

Conclusion générale et perspectives

Aujourd'hui, il est important de protéger les données sensibles afin qu'elles ne deviennent vulnérables à un accès non autorisé. Il existe une variété d'algorithmes de cryptage, qui ont prouvé leurs performances et leur efficacité à la sécurisation de données textuelles comme les algorithmes symétriques et ceux asymétriques, mais le problème qui se pose est que ces derniers sont inadéquats pour le chiffrement des données volumineuses et/ou fortement corrélées telles que les images numériques. Une des solutions prometteuses de ce problème est d'utiliser le chaos dans le cryptage en raison de ces caractéristiques particulières comme la sensibilité aux conditions initiales.

Ce travail consiste à réaliser un cryptosystème basé sur les système chaotiques et hyperchaotiques pour la transmission sécurisée des images numériques. Les résultats trouvés des expériences montrent que l'algorithme proposé a la capacité de chiffrer en toute sécurité ce type de données.

Pour ce faire, nous avons commencé ce mémoire par une étude globale sur les différents concepts de la cryptographie. Dans le premier chapitre, on a donné des généralités sur les techniques de cryptage, les algorithmes de chiffrement classiques et modernes ainsi que les algorithmes en cours de développement.

Dans le deuxième chapitre, on a abordé l'état de l'art des systèmes chaotiques et hyperchaotiques, dans lequel nous avons défini les notions de base des systèmes dynamiques et chaotiques, ainsi que leurs conceptions et types employés dans la cryptographie.

Dans le troisième chapitre, nous avons mentionné la relation entre le chaos et la cryptographie, après nous avons étudié deux types des systèmes chaotiques et nous avons fait le chiffrement d'image numérique utilisant ces systèmes. Aussi, les outils d'évaluation de sécurité communs utilisés pour évaluer les performances de des systèmes cryptographiques conçus en termes de niveau de sécurité ont été abordés.

Dans le quatrième chapitre, nous avons proposé et validé une approche robuste capable de chiffrer efficacement les images numériques. En effet, nous avons proposé une nouvelle méthode basée sur un système hyperchaotique à 6D, la matrice de Q de Fibonacci et la fonction Cat map. Les différentes expériences réalisées dans ce mémoire sont faites sous logiciel MATLAB

et les résultats de simulation ont montré que l'algorithme proposé présente un niveau élevé de sécurité et de performance.

Notre projet est loin d'être complet. En guise de perspectives, nous proposons de :

- Adapter notre méthode sur d'autres données numériques à savoir les images couleurs et les vidéos.
- Implémenter cet algorithme dans une chaine de transmission sécurisée.

Références Biblio-webographiques

[1] V. Ullagaddi, « Development of data encryption algorithms for secure communication using public images », Master of Science Degree in Electrical Engineering, University of Toledo, 2012.

[2] M. Kaddouri, « Conception et réalisation d'un crypto-système pour la sécurisation des données médicales. », Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2021.

[3] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[4] https://ram-0000.developpez.com/tutoriels/cryptographie/ (consulté le 17 avril 2022).

[5] R. L. Rivest, « Cryptography », in Algorithms and complexity, Elsevier, 1990, p. 717755.

[6] A. BOUGUESSA, N. HADJ SAID, « Recherche D'une Technique De Stéganographie Basée Sur La Théorie Du Chaos », Thèse de Doctorat, Université des Sciences et de la Technologie d'Oran, 2021.

[7] M. M. Hamel, T. Anteur, « Utilisation croisé d'hyperchaotiques et des séquences d'ADN pour cryptage d'image », Mémoire de Master, Université de Ghardaïa, 2020.

[8] https://librecours.net/module/culture/intro-chiffrement/pres/co/chiffrement-sym.html?mode=html (consulté le 07 avril 2022).

[9] https://librecours.net/module/culture/intro-chiffrement/pres/co/chiffrement-asym.html?mode=html (consulté le 10 avril 2022).

[10] F. Grosshans et P, Grancier, « La cryptographie quantique : l'incertitude quantique au service de la confidentialité », optique quantique vol.71, pp.34-39, 2014.

[11] B. Bouizeri, « Cryptographie : Approche Quantique », Mémoire de Master, Université Mouloud Mammeri, 2017.

[12] C. d. R. Philippe Etchecopar, « Quelques éléments sur la théorie du chaos », 2000.

[13] S. Kaouache, « Synchronisation des systèmes chaotiques et hyperchaotiques **:** Application à la sécurisation des communications », Thèse de Doctorat, Université Frère Mentouri – Constantine, 2020.

[14] A. Dahbia et A. Katia, « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole », Mémoire de Master, Université Mouloud Mammeri, Tizi Ouzou, 2018.

[15] A. Zemouche, « Sur l'observation de l'état des systèmes dynamiques non linéaires », Thèse de Doctorat, Université Louis Pasteur-Strasbourg I, 2007.

[16] O. Megherbi, « Etude et réalisation d'un système sécurisé à base de systèmes chaotiques », Mémoire de Magister, Université Mouloud Mammeri, Tizi Ouzou, 2013.

[17] C. Benhabib, « étude d'un système chaotique pour la sécurisation des communications optiques », Mémoire de Master, Université de Tlemcen faculté de technologie, 2014.

[18] M. BENDAOUD, « Etude et Conception d'un système chaotique basé sur l'oscillateur Colpitts pour les communications sécurisées », Mémoire de Master, Université Aboubakr Belkaïd– Tlemcen, 2019

[19] M. Grimes, S. Haddad, et A. Khebli, « Amélioration du Cryptage Chaotique des Image avec la Fonction CAT MAP », 2007.

[20] https://www.francois-roddier.fr/?paged=13 (consulté le 15 avril 2022).

[21] A. A. Omar et A. Farid, « Conception et étude d'un nouveau système de transmission d'image sécurisée par le chaos », Mémoire de Master, Université Mouloud Mammeri, Tizi Ouzou, 2016.

[22] D. Benzemam, « Systèmes Chaotiques et Hyperchaotiques pour la Transmission Sécurisée de Données », Mémoire de Magister, Univ Tlemcen, 2010.

[23] https://hal.univ-lorraine.fr/tel-01749595 (consulté le 16 avril 2022).

[24] A. Mahamdioua et N. Brahimi, « Cryptage chaotique numérique des images » Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2005.

[25] A. Hank, R. Younsi, « Systèmes chaotiques pour la transmission sécurisée de données », Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2020.

[26] NKAPKOP Jean De Dieu, « Cryptage chaotique des images basé sur le modèle du perceptron », Mémoire de Master en EEA, Université de Ngaoundéré, 2012.

[27] M. Bernou et I. Kerroud, « Les séquences chaotiques pour la sécurité des images : application des systèmes de tatouage numérique robuste basé sur les séquences chaotiques pour la protection des droits d'auteurs », Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2016.

[28] http://courtoisthomas.pythonanywhere.com/memoire/lorenz/system (consulté le 20 avril 2022).

[29] M. Yahia, « Elaboration d'algorithmes de masquage pour les systèmes de communication chaotique », Thèse de Doctorat, Université Mentouri – Constantine,2012

[30] F. HADJI, « Conception et réalisation d'un système de cryptage pour les images médicales », Thèse de Doctorat, Université MOHAMED BOUDIAF-M'SILA, 2018.

[31] A. Beloucif, « Contribution à l'étude des mécanismes cryptographiques », Thèse de Doctorat, Université de Batna 2, 2016.

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

[33] https://fr.wikipedia.org/wiki/Entropie_de_Shannon (consulté le 09 mai 2022).

[34] Z. A. Seghir, « Evaluation de la qualité d'image », Thèse de Doctorat, Université de Mentouri–Constantine, 2012.

[35] A.K. Amzert, O. Belmerabet, « Sécurisation des images médicales sur courbes elliptique », Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2020.

[36] Pak, C. et al. « A novel bit-level color image encryption using improved 1D chaotic map. Multimed » . Tools Appl. **2018**, 78, 12027–12042.

[37] C. Cao, K. Sun, and W. Liu, « A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map ». Signal Process. **2018**, 143, 122–133.

[38] Z. Li, et al., « A novel plaintext-related image encryption scheme using hyper-chaotic system ». Nonlinear Dyn. **2018**, 94, 1319–1333.

[39] X. Chen, C.J. Hu, « Adaptive medical image encryption algorithm based on multiple chaotic mapping ». Saudi J. Biol. Sci. **2017**, 24, 1821–1827.

[40] X. Chai, et al., « An image encryption algorithm based on chaotic system and compressive sensing. Signal Process. **2018**, 148, 124–144.

[41] X. Chai, et al., « An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. Neural Comput ». Appl. **2018**, 32, 4961–4988.

[42] N. Tsafack, et al., « Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption ». Inf. Sci. **2020**, 515, 191–217.

[43] P. Ramasamy, et al., «An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map ». Entropy **2019**, 21, 656.

[44] K.M. Hosny, et al., « New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix », Electronics, vol. 10, n° 9, p. 1066, 2021.

[45] J. Wang, et al., « A new six-dimensional hyperchaotic system and its secure communication circuit implementation ». Int. J. Circuit Theory Appl. **2019**, 47, 702–717.

[46] E. BENSIKADDOUR, « Développement d'un crypto-système basé sur le standard AES et la théorie du chaos pour le chiffrement des images satellitaires à bord d'un satellite d'observation de la terre. », Thèse de Doctorat, Université DJILLALI LIABES, Sidi Bel Abbes, 2019.

[47] H. Kenouni, « Synchronisations des systèmes Hyper-chaotiques à retard sous l'effet des perturbations : Application au chiffrement d'information », Mémoire de Master, Université Mohamed Seddik BenYahia, Jijel, 2016.