

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE MINISTERE DE
L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLEB DE BLIDA



Institut d'Aéronautique et des Etudes Spatiales

Département des études spatiales



Mémoire de Fin d'Etude Master Académique

Option : Télécommunication spatiale.

Intitulé :

« Etude le système de compression-chiffrement continu pour les
Télécommunications et leur Application : Images numériques. »

Présenté par :

Issad souaad.

Ben Abed Imen Bochra.

Encadreur : Mr. Krim

Soutenu le : 15/09/2022 devant le Jury Composé par :

Dr. Azmdroub

Président

IAES

Mme. Azine Houria

Examinatrice

IAES

Remerciements

Avant tout on tient notre remerciement à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

Notre gratitude, nos vifs remerciements et nos respects à notre encadreur Dr. Krim Mohamed, pour tous ses judicieux conseils, son temps qu'il nous a consacré et pour nous avoir toujours orientée vers un esprit purement scientifique. Nous remercions l'ensemble des membres du jury qui nous ont fait l'immense plaisir de juger ce travail. Sincères remerciements au Présidente du jury, Nous exprime également nos remerciements à nos chers parents qui n'ont jamais cessé de nous encourager à bien mener nos travaux. Et à tous ceux qui nous ont encouragé et soutenue moralement et intellectuellement.

Merci à tous

Dédicaces

Je dédie ce travail à :

Mon adorable mère Karima

La femme qui a souffert sans me laisser souffrir ,qui n'a jamais dit non à mes exigences qui n'a épargné aucun effort pour me rendre heureuse qui n'a jamais cessé de formuler des prières à mon égard, qui m'a entouré d'amour, d'affection et m'a doté d'une éducation digne, la femme qui a tout fait pour ma réussite, son soutien, tous les sacrifices qu'elle a consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie. Que ce rapport soit le meilleur cadeau que je puisse t'offrir.

Mon frère chawki et soeur wissem

qui n'ont jamais cessé d'être là pour moi des exemples de persévérance, de courage et de générosité, que dieu les protège et leurs offre la chance et le bonheur.

Ma chère tante Amel

Qui m'a soutenu moralement et Financièrement tout au long de mes études , que dieu te bénisse.

Mes grand-parents mohamed et khadidja

Qui m'ont encouragé et soutenu de tous leurs amour pour atteindre à ce niveau là .

mes chères amies Souaad Lilia Ghozlan Kawter Amina et Houda

Qui m'avez motivé et partagé avec moi tous les moments de fatigue, de tristesse et de joie.

BENABED IMEN BOCHRA

Dédicaces

Je dédie ce mémoire à :

Mon père,

Qui a fait tant de sacrifice pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutien permanent venu de toi.

Ma mère,

Qui a tout fait pour ma réussite, son soutien, tous les sacrifices qu'elle a consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.

Mes Sœurs Selma ,Halima, Ahlam et Nawal ,

qui n'ont cessé d'être là pour moi des exemples de persévérance, de courage et de générosité

Mes chères amies Imen ,Ghozlan, Kawter, Amina

Qui m'avez motivé et partagé avec moi tous les moments de fatigue, de tristesse et de joie.

Mes chats Lili et Lino

Résumé :

Dans le nouveau domaine des technologies télécommunications spatiales, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données confidentielles et assurer la sécurité des données compressés.

Dans l'étude des techniques et dans le contexte de la transmission sécurisé, nous proposons le principe fondamental des systèmes de communication à Base du chiffrement continu qui peut crypter le message transmis : Image par un signal auxiliaire de la séquence nouvelle carte chaotique indépendant du message, ensuite la compression des images numérique est devenue une opération inévitable afin de diminuer leurs tailles en vue d'une transmission et/ou stockage. L'objectif visé pour proposer des techniques de chiffrement des images et compression est d'assurer la sécurité et le compromis d'image entre un taux de compression élevé et une dégradation moindre. Cette dernière est basée sur la technique du Compression par la méthode ondelette du codeur SPIHT, tout appliqué sous simulation sur MATLAB. Les résultats obtenus montrent l'efficacité de ce système de chiffrement continu -compression d'implémentation contre les attaques avancées.

Mots clés : Transmission sécurisé, systèmes de communication, chiffrement continu, Compression, méthode ondelette, codeur SPIHT.

ABSTRACT

In the new field of space telecommunications technologies, where the exchange of multimedia information is developing rapidly, it is essential to be able to have secure systems to protect confidential data and ensure the security of compressed data.

In the study of techniques as well in the context of secure transmission, we indicate the fundamental principle of communication systems based on continuous encryption which can encrypt the transmitted message Image by an auxiliary signal of sequence new chaotic map independent of the message in continuation the compression of digital images has become an inevitable operation in order to reduce their sizes for transmission and/or storage. The aim of proposing image encryption and compression techniques is to ensure security and to compromise the image between a high compression rate and minimum degradation. The latter is based on the technique of Compression by the wavelet method of the SPIHT coder, all applied under simulation on MATLAB. The obtained results show the effectiveness of this continuous encryption-compression implementation against advanced attacks

Keywords : Secure transmission, communication systems, continuous encryption, Compression, wavelet method, SPIHT encoder.

المخلص:

في المجال الجديد لتقنيات الاتصالات الفضائية ، حيث يتطور تبادل معلومات الوسائط المتعددة بسرعة ، من الضروري وجود أنظمة آمنة لحماية البيانات السرية وضمان أمن البيانات المضغوطة. في دراسة التقنيات وفي سياق الإرسال الآمن ، نقترح المبدأ الأساسي لأنظمة الاتصال القائمة على التشفير المستمر الذي يمكنه تشفير الرسالة المرسل: صورة بإشارة مساعدة لتسلسل خريطة فوضوية جديدة مستقلة عن الرسالة ، و كذلك أصبح ضغط الصور الرقمية عملية حتمية لتقليل أحجامها للإرسال و / أو التخزين. الهدف من اقتراح تقنيات تشفير وضغط الصور هو ضمان الأمان وتسوية الصورة بين معدل ضغط مرتفع وأقل تدهور. يعتمد هذا الأخير على تقنية الضغط بواسطة طريقة الموجات الخاصة بمبرمج SPIHT ، وكلها مطبقة تحت المحاكاة على MATLAB. تظهر النتائج التي تم الحصول عليها فعالية تنفيذ ضغط التشفير المستمر ضد الهجمات المتقدمة. **الكلمات المفتاحية:** النقل الآمن ، أنظمة الاتصال ، التشفير المستمر ، الضغط ، طريقة الموجة ، المبرمج SPIHT.

Table des Matières

Remercîments

Dédicaces

Liste des Figures

Liste des symboles

Liste des tableaux

1.Introduction Générale	1
Chapitre I:Généralités sur la cryptographie et La compression d'image numérique	
1. Introduction	7
1.1 La Cryptographie	7
1.1.1 Définitions	7
1.2 Terminologie.....	7
1.3 Principe de la cryptographie :	8
1.4 Rôle de la cryptographie :	8
1.5 Méthodes de la cryptographie Modernes :.....	10
1.5.1 Cryptage conventionnel	10
1.5.1.1 Caractéristiques du cryptage symétrique	11
1.5.2 Chiffrement à clé publique	11
1.6 Méthodes du cryptage des images	12
1.6.1 Méthodes dans le domaine spatial.....	12
1.6.2 Méthodes dans le domaine fréquentiel	13
1.7 Outils élémentaires d'analyse d'un algorithme du cryptage d'image (Mesures de Performance) :	13
1.8 La compression des images :	15
1.8.1 Définition de la compression d'image	15
1.8.2 Principe de la compression d'image :	15
1.8.3 Objectif de la compression :	16
1.8.4 Classification des méthodes de compression.....	18
1.8.5 Méthodes de compression :	18
1) La compression sans pertes.	18
2)La compression avec pertes.	19
1.8.6 Méthodes par transformée	20
1.9 Les normes de compression des images avec et sans pertes.....	20
1.9.1 La norme de compression JPEG	20
1.10 Transformées en ondelettes par SPIHT :	22
1.10.1 Processus de codage SPIHT	23

1.10.2 Principe de L'algorithme SPIHT :	24
1.11 Evaluation de la qualité d'une compression :	25
1.12 Conclusion :	28

Chapitre II: Système Dynamique Chaotique

2. Introduction	30
2.2 Système dynamique :	31
2.2.1 Définition.....	31
2.2.2 Classe système dynamique :	31
A) système dynamique Discrets :	31
B) système dynamique Continus :	32
2.2.3 Trois Sortes De Systèmes Dynamiques :	32
2.2.4 Le chaos :	33
2.3 Propriétés de système chaotiques.....	33
2.3.1 Aspect aléatoire :	34
2.3.2 Sensibilité aux conditions initiales :	34
2.3.3 Imprévisibilité :	34
2.3.4 Exposants de Lyapunov :	35
2.3.5 Bifurcation :	35
2.3.6 Les attracteurs :	36
2.3.6.1 Les différents types d'attracteurs :	36
2.3.6.2 Classes d'attracteurs analogique et numérique :	37
2.4 Les systèmes chaotiques continus et discrets :	38
2.4.1 Systèmes chaotiques continus :	38
A) Système de Lorenz :	39
A.1 Aspect aléatoire du système de Lorenz :	41
A.2 Sensibilité aux conditions initiales du système de Lorenz :	42
B) Fonction carte logistique :	43
B.1 Aspect aléatoire de la fonction logistique :	45
B.2 sensibilité aux conditions initiales de la fonction logistique :	46
B.3 Exposant de Lyapunov de la fonction logistique :	47
2.5 Crypto système basé sur la confusion et la diffusion :	50
2.6 Conclusion :	51

Chapitre III: Simulation Crypto-système basé à Attracteur Lorenz & carte logistique Sous
MATLAB

3. Introduction :.....	54
3.1.2 Modèle Proposé De Chiffrement Et Déchiffrement En Continu	57
3.1.3 Générateur Chaotique Proposé :.....	58
3.1.4 Résultats de compression et interprétations :	60
3.1.5 Compression d'image par ondelette :.....	60
3.2 Compression image par la méthode ondelette (codeur SPIHT) :.....	64
3.2.2 Approche proposée du chiffrement base des attracteurs chaotiques :.....	67
3.2.3 Organigramme de chiffrement image par algorithme carte chaotique et compresser	67
3.3.1 Résultats des Simulations.....	69
3.3.2 Chiffrement en continu a bases des attracteurs chaotiques :.....	69
3.3.3 Crypto-système base sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique :	69
3.3.4 Analyse des résultats:.....	71
3.3.5 Simulation Crypte-compression Images système	78
3.4 Conclusion.....	80

Liste des figures :

Figure 1.1: Chiffrement symétrique.....	10
Figure 1.2: Chiffrement asymétrique.....	11
Figure 1.3: Histogramme d'une image niveau de gris.....	14
Figure 1.4: Histogramme d'une image couleur.....	14
Figure 1.5: Histogramme d'une image chiffrée.....	14
Figure 1.6: Principe de la compression d'image pour la transmission ou stockage.....	16
Figure 1.7: schéma d'un codeur source.....	17
Figure 1.8: Algorithme de compression sans perte les plus utilisés.....	19
Figure 1.9: Méthodes de compression avec perte.....	19
Figure 1.10: principe d'un système de codage par transformation.....	20
Figure 1.11: principe de l'algorithme JPEG avec pertes.....	21
Figure 1.12: principe de l'algorithme JPEG sans pertes.....	21
Figure 1.13: Diagramme en bloc de l'algorithme « SPIHT ».....	25
Figure 2.1: Lyapunov de Lorenz.....	35
Figure 2.2: Attracteur du Système de Lorenz de 50 iteration.....	41
Figure 2.3: Aspect aléatoire du Courbes en x, y, z de l'attracteur de Lorenz.....	42
Figure 2.4: Sensibilité aux conditions initiales pour le Système de Lorenz.....	42
Figure 2.5 : Les projections d'attracteur de Lorenz en 3D.....	43
Figure 2.6: Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique ($N = 1500, \mu=4, x_0=0.1$).....	44
Figure 2.7: application logistique pour $r=4$	46
Figure 2.8: Sensibilité aux conditions initiales de la fonction logistique.....	47
Figure 2.9: Le composant de Lyapunov pour la carte logistique de $1 \leq \mu \leq 3.999$, $N= 1500$, $x_0=0.1$	48
Figure 2.10: Diagramme de bifurcation pour la carte Logistique de $0.1 \leq \mu \leq 3.999$	50
Figure 2.11: Crypto-système basé sur la confusion et la diffusion.....	51
Figure 3.1 : Cryptage d'image par la technique du chiffrement continu à base de L'algorithme Chaotique.....	54

Figure 3.2: Approche Pré-compression.....	55
Figure 3.3 : Approche post-compression.....	56
Figure 3.4: Compression Et Chiffrement Conjoints.....	57
Figure 3.5: Chiffrement Continu pour le System Sécurisé (compression-chiffrement des images).....	58
Figure 3.6: Images satellites des tests (.png).....	60
Figure 3.7 : Images de teste madina (jpg).....	61
Figure 3.8 : processus de compression image par ondelette se compose de Différentes étapes.....	62
Figure 3.9: Conversion d'image RGB a image en niveaux de gris : (a) Image b en couleur (b) Image b en gris.....	63
Figure 3.10 : Conversion RGB à YCbCr.....	63
Figure 3.11: Décomposition l'image originale (YCbCr).....	64
Figure 3.12 : Variation des paramètres d'évaluation (PSNR, MSE et taux de compression) pour niveaux de décomposition et 6.(level 6) Lors de l'utilisation de l'ondelette de codeur SPIHT	65
Figure 3.13: Block diagram of the encryption algorithm.....	68
Figure 3.14: Chiffrement d'image avec l'attracteur de Lorenz.....	70
Figure 3.15: Analyse d'histogramme Des Différents images(compreser,crypter).....	71
Figure 3.16: Analyse d'histogramme Des Différents images(compreser,crypter).....	72
Figure 3.17 : Distribution des pixels adjacent Madina.jpg en claire (X0= 0.2, Y0= 2.5, Z0= 3)	73
Figure 3.18: Distribution des pixels adjacent Madina.jpg chiffrée (X0= 0.2, Y0= 2.5, Z0= 3).....	73
Figure 3.19 : Distribution des pixels adjacent satellite.jpg en claire (X0= 0.2, Y0= 2.5, Z0 =3).....	74
Figure 3.20 : Distribution des pixels adjacent satellite.jpg chiffrée (X0= 0.2, Y0= 2.5, Z0 =3).....	74

Figure 3.21: Analyse d'histogramme Des Différents images(crypter compresser).....76

Figure 3.22: Distribution des pixels adjacent image chiffrée et compressé (image madina) ($X_0= 0.2$, $Y_0= 2.5$, $Z_0= 3$) level 6 ,taux compression =2bpp.....77

Figure 3.23: Distribution des pixels adjacent image chiffrée et compressé (image satellite)($X_0= 0.2$, $Y_0= 2.5$, $Z_0= 3$) $h =0.0001$, $R=28$, $\sigma=10$, et $\beta=8/3$, level 6 taux compression =2bpp.....77

Liste des symboles :

M : texte en clair

C : texte chiffré

D : fonction inverse

ECB : Electronic Code Book

OFB : Output Feedback

CBC : Cipher Block Chaining

CFB : Cipher Feedback

RSA : Rivest – Shamir – Adleman

SSL : Secure Sockets Layer

TLS : Transport Layer Security

NPCR : Number of Pixels Change Rate

UACI : Unified Average Changing Intensity

RLC : RunLengthCoding

VLC : Variable LengthCoding

LZW : Lempel-Ziv-Welch

TCD : Transformation en Cosinus Discrète

JPEG : Joint Photographic Experts Group

JBIG : Joint Bi-level Image Group

MPEG : MovingPictures Experts Group

DWT : Discret Wavelet Transform

CDF : Cohen-Daubechies-Fauvaue

SPIHT : Set Partitioning in Hierarchical Trees

MSE : Mean Square Error

PSNR : Peak Signal-To-Noise Ratio

SSIM : Structural Similarity

Liste des tableaux :

Tableau.3.1 : Comparaison des coefficients de corrélation entre les images en claire et chiffrée image test satellite test75

Tableau.3.2 Comparaison des coefficients de corrélation entre les images en claire et chiffrée image madina75

Tableau.3.3 Comparaison des coefficients de corrélation entre les images en claire et chiffrée et compresser image test satellite test78

Tableau.3.4 Comparaison des coefficients de corrélation entre les images en claire et chiffrée et compresser image madina78

Introduction Générale

1. Contexte

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer une image de façon crypter et compressée est aussi ancien que les communications elles-mêmes. De nos jours le développement énorme des télécommunications et d'Internet, rend la sécurité et compresse d'image numérique de plus en plus importante, il est nécessaire dans plusieurs applications, TV, systèmes médicaux, images militaires,...etc.

Quand on parle de la compression et la cryptographie sont deux techniques opposées et sont la solution la plus courante et la plus acceptable pour sécuriser et protéger les images satellites contre les attaques extérieures et pour garantir une grande confidentialité. En général, le cryptage garantit que les données transmises sont fiables et intégrales en les convertissant de données lisibles en données illisibles via un processus de codage [1], et plus la cryptographie a été dans la plupart des cas perçue comme une chimie noire qui est seulement utilisée par les états et les gouvernements reflétant la complexité et la difficulté et parfois l'impossibilité de la décrypter des images que par des mathématiciens brouillons. À l'inverse, une méthode de compression cherche à réduire la taille des données transférées ou stockées en recherchant et en supprimant des éléments de preuve ou des modèles de données en double. Cependant, la compression de données et le système cryptographique sont profondément connectés et mutuellement utiles, car ils peuvent être utilisés ensemble.

la question qui se pose, pourquoi ne pas avoir les deux en même temps ; compression et chiffrement sachant que la réalisation de ces deux concepts en cascade induit un certain nombre de défis. En effet, la compression des données et leur cryptage ultérieur ou inversement peuvent réduire le taux de compression ainsi que la robustesse de cryptage.

Pour résoudre ce problème, plusieurs approches combinées ont été proposées, cependant ces méthodes entraînent généralement des problèmes de sécurité ou d'efficacité de la compression dans la pratique. Certains d'eux souffre d'une réduction substantielle de l'efficacité de la compression en raison de la réduction de

la corrélation entre les pixels des images causés par les opérations de cryptage d'autre sont moins résistants devant les attaques de texte en clair ou contiennent des failles de sécurité.

L'algorithme de cryptage proposé consiste en un système chaotique de Lorenz qui contient trois équations avec des paramètres de cartes chaotiques (1D et 2D) et un système de rotation efficace pour réduire la complexité habituellement utilisée dans les travaux qui utilisent des cartes chaotiques et donnent plus de simplicité pour comprendre le travail [5]. Grâce aux résultats des tests, l'algorithme de chiffrement proposé est robuste contre les attaques et offre un haut niveau de sécurité, ce qui le rend applicable à bord des satellites d'observation de la Terre (EOS). En plus des images satellites, l'algorithme proposé est mieux adapté au cryptage sécurisé des images numériques normales.

2. Objectifs

Les objectifs de ce mémoire sont de générer une plus petite taille de données pour accélérer leur transmission, assurer sa sécurité et assurer la qualité des données lors de la reconstruction.

Les travaux réalisés présentés on essaye de mettre certains concepts de la théorie du chaos à la disposition du chiffrement continue en particulier l'attracteur de système chaotique Lorenz efficace avec un système de rotation rapide et efficace, des données (textes et images fixes) seront cryptées pour valider le chiffrement. L'un des principaux avantages de notre algorithme proposé est la concentration dans la simplicité d'utilisation et de compréhension par rapport aux travaux récents de cryptage d'images satellites.

Les approche de crypto-compression classiques ont toutes tendances réaliser les techniques de cryptage et de compression de manière disjointe. Cette architecture posait un problème au niveau des étapes de décryptage et de décompression, en occurrence pour les applications en temps réel. Ainsi de nouvelles approches mixtes de crypto compression commencent à prendre de l'essor.

Le concept visite à combiner à la fois les deux techniques de cryptage et de compression de manière à ce qu'elles soient effectuées de manière jointe .le challenge est toujours de procurer pour toutes nos applications un volume de

données de taille réduite ainsi qu'une confidentialités robuste .il s'agit alors de parvenir à trouver une approche efficace de crypto-compression[6]

Afin de mieux cerner l'approche adoptée de notre travail de recherche. Nous avons abordé séparément, les problèmes concernant la sécurité et la compression des images .puis nous avons cherché à intégrer les deux concepts en tenant des contraintes de chacun des deux processus. Les différents aspects peuvent être résumés en ce qui suit :

- L'aspect sécurité et l'authenticité des données pendent la transmission, mais également après réception de celles-ci. Toute information circulant peut être capturée, lue et/ou modifiée.
- Le temps de transfert. En effet, du fait de la quantité importante de données, les tailles des images doivent être compressées avant le transfert
- Des applications exigent que l'image soit associée à des informations contextuelles telles que les images urémiques.

Pour des raisons de confidentialité, certaines images doivent être rendues complètement ou partiellement illisible et non déchiffrables pendent le transfert.

L'objectif de notre travail est d'implémenter une méthode de cryptage moderne et sélectif en mode continue et de l'intégrer au niveau du compression JPEG par la méthode SPIHT . Et ceci afin de tenir compte des contraintes soulignées pour réaliser une transmission sécurisée des images digitale.

3. Organisation du mémoire

Ce mémoire est organisé de trois chapitres comme suit :

Le premier chapitre : présente un aperçu des sujets liés à notre sujet principal qui sont : la cryptographie, le chaos, la compression, et les images numériques.

- Dans le premier sujet, nous présentons les bases de la cryptographie moderne et ses deux principaux types : les chiffrements symétriques, les chiffrements asymétriques.
- Dans le second sujet, nous présentons une brève introduction aux systèmes dynamiques, chaos (carte logistique et Lorenz) et aux quelques concepts de base tels que l'analyse.
- Dans le troisième, nous présentons les bases de la compression et des algorithmes de compression classiques, basées sur la méthode SPIHT .

- Alors que dans le dernier sujet, nous présentons les concepts liés à l'image numérique, les types d'images existants et les formats de fichiers d'images largement utilisés.

Le deuxième chapitre : est dédié à l'étude détaillée de notre système de cryptage chaotique basé sur une nouvelle fonction chaotique définie par une combinaison des deux fonctions : la fonction carte logistique et la fonction lorenz map.

Le troisième chapitre : présente les résultats obtenus en simulant deux modèles de cryptos systèmes chaotiques & compression accompagnés par des interprétations et des analyses des performances.

A la fin de ce mémoire, nous donnerons une conclusion générale, qui contiendra un résumé de ce travail, et les différentes perspectives.

Chapitre I

**Généralités sur la cryptographie et La compression
d'image numérique**

1. Introduction

Dans ce chapitre nous présentons un aperçu sur les éléments clés qui sont directement liés à notre travail : la cryptographie, le chaos et la compression des images et quelques méthodes utilisées dans cette discipline, ainsi que nos motivations pour la compression des images.

1.1 La Cryptographie

1.1.1 Définitions

Déf 1: Le mot cryptographie vient des deux mots grecs kryptós "secret" et gráphein "écrire", c'est-à-dire écrire secrètement. Ce terme générique désigne l'ensemble des méthodes utilisées pour cacher l'information, c'est-à-dire la rendre incompréhensible sans aucun secret.

Déf 2: La cryptographie est l'art de cacher une information pour la rendre inintelligible [9][10] à toute personne ne connaissant pas un certain secret. Autrement dit, c'est l'ensemble des processus de verrouillage visant à protéger l'accès à certaines données afin de les rendre incompréhensible aux personnes non autorisées [11].

1.2 Terminologie

- **Le texte clair :** Texte non crypté. Également appelé texte brut, ou bien le message. (En anglais **Plaintext**)
- **Le chiffrement :** L'action de transformer à l'aide d'une convention secrète, appelée clé, des informations claires en informations inintelligibles par des tiers n'ayant pas la connaissance de la clé est appelée **chiffrement(ou Encryption)**.
- **Le texte chiffré :** Le résultat du processus de chiffrement est appelé **texte chiffré** ou **cryptogramme**. (En anglais **Ciphertext**)
- **Le déchiffrement :** Le processus de reconstruction du texte en clair à partir du texte chiffré en utilisant la convention secrète de chiffrement est appelé **déchiffrement**.
- **La clé :** Chaîne de bits utilisés pour crypter ou décrypter des données ou encore calculer des condensés de messages.

- **Expéditeur** : L'entité qui envoie l'information originale (texte clair).
- **Destinataire** : Entité destinée à recevoir l'information.
- **Canal** : Moyen de transport de l'information d'une entité à une autre.
- **Canal sécurisé** : Canal ou l'adversaire (espion) n'a pas la possibilité de lire, de modifier ou de supprimé l'information.

1.3 Principe de la cryptographie :

Le texte en clair est note M . Ce peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image numérique. Du point de vue de l'ordinateur, M n'est rien d'autre que de l'information binaire. Le texte en clair peut être transmis ou stocké. Dans tous les cas, M est le message à chiffrer.

Le texte chiffré est noté C , C'est aussi de l'information binaire, parfois de la même taille que M et parfois plus grande.

La fonction de chiffrement, notée E , transforme M en C . Ce qui en notation mathématique s'écrit :

$$E(M)=C \quad (1.1)$$

La fonction inverse, notée D , de déchiffrement transforme C en M :

$$D(c)=M \quad (1.2)$$

Comme le but de toutes ces opérations n'est rien d'autre que de retrouver le message en clair à partir de la version chiffré de ce même message, l'identité suivante doit être vérifiée :

$$D(E(M))=M \quad (1.3)$$

Parmi une grande variété de mécanismes de chiffrement, les deux algorithmes principaux en cryptographie standard sont le chiffrement à clé publique (antisymétrique) et le chiffrement à clé secrète (symétrique), présentés dans la section suivante. [16,17]

1.4 Rôle de la cryptographie :

De tout temps la question de la sécurité dans le transfert de données a été un problème envisagé avec le plus grand sérieux. Les militaires ont été, pour des raisons évidentes, Confrontés très tôt à ce genre d'exigences ; jusqu'à très récemment le domaine public n'avait Qu'un droit très limité à la sécurité des données. Mais le changement très marqué de nos moyens de communication,

l'utilisation d'Internet pour des applications commerciales a relancé le problème crucial du droit à la sécurité, car de nombreux concurrents pouvaient avec plus ou moins de facilité s'emparer et déchiffrer nos données. L'utilisateur devait avoir les mêmes privilèges que l'armée dans le traitement de ses données à caractère monétaire. A ce stade, il devenait presque évident que toutes les données puissent être traitées avec autant de sérieux que s'il s'agissait d'argent ou de secret militaire.

L'art et la science de garder un secret sont appelés cryptographie. De nos jours, ce sont les mathématiciens et les physiciens qui étudient la cryptologie et cette science est exploitée par les informaticiens pour les applications.

La cryptographie dans les applications téléinformatiques doit assurer :

- **La confidentialité** : est l'assurance qu'un document ne sera pas lu par un tiers qui n'en a pas le droit lors de la transmission de ce document ou lorsqu'il est archivé. Les documents papiers qui doivent rester secrets sont généralement stockés dans des coffres et sont transportés sous plis cachetés. Pour les documents électroniques, on utilisera le chiffrement.
- **L'authentification** : le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas se faire passer pour quelqu'un d'autre. C'est l'assurance de l'identité d'un objet, Généralement une personne, mais cela peut aussi s'appliquer à un serveur ou une application, ... Dans la vie courante, la présentation de la carte nationale d'identité et la signature manuelle assurent un service d'authentification
- **L'intégrité des données** : l'intégrité d'un objet (document, fichier, message ...) est la garantie que cet objet n'a pas été modifié par une autre personne que son auteur. Sur une feuille de papier toute modification est visible d'un simple coup d'oeil. Sur un document électronique (courrier électronique, fichier Word, ...) non sécurisé, cette détection est impossible.
- **Le non désaveu ou la non répudiation** : Comme ce terme l'indique, le but est que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et le récepteur l'avoir reçu. Les transactions commerciales ont absolument besoin de cette fonction. Le reçu que l'on signe au livreur et la lettre recommandée sont des mécanismes de non répudiation.

Ces exigences sont vitales si l'on désire effectuer une communication sécurisée à travers un réseau informatique tel qu'Internet.

Il n'existe pas une méthode simple et sûre pour permettre de telles exigences, mais un ensemble de techniques permet, en les combinant, de satisfaire ces besoins de sécurité.

1.5 Méthodes de la cryptographie Modernes :

On distingue deux méthodes majeures de la cryptographie modernes : les méthodes à clef secrète c'est la cryptographie symétrique et les méthodes à clef publique/clef privée c'est la cryptographie asymétrique.[1]

1.5.1 Cryptage conventionnel (chiffrement symétrique):

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

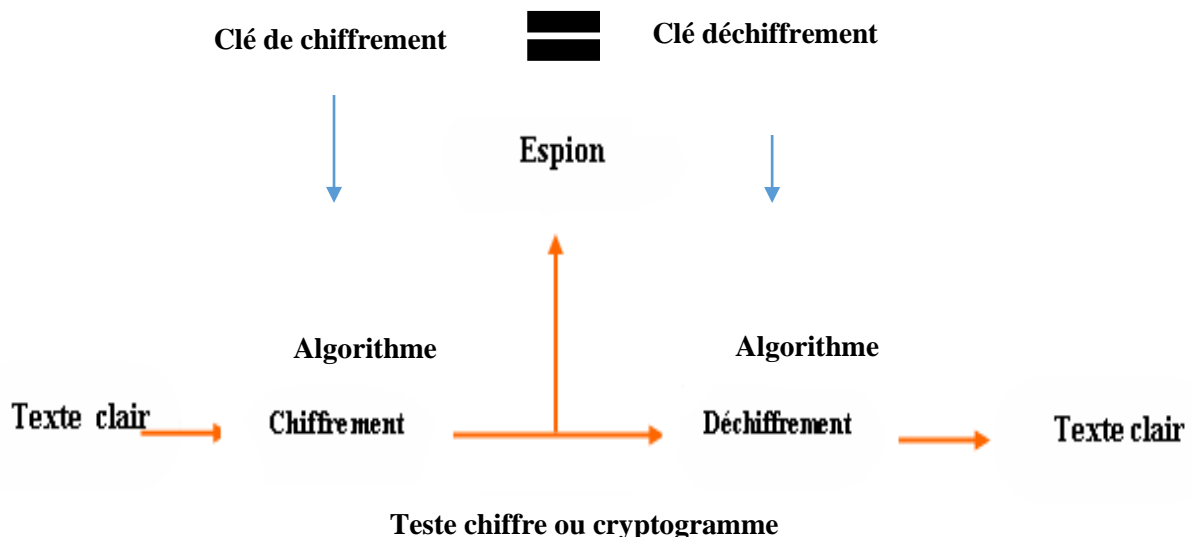


Figure1.1:Chiffrement symétrique [14].

Le cryptage symétrique fonctionne selon deux procédés différents : le cryptage par bloc s'effectue sur des blocs de bits, et le cryptage par flot s'effectue en continu, bit par bit

1.5.1.1 Caractéristiques du cryptage symétrique:

- La rapidité d'exécution.
- La simplicité d'implémentation.
- La sécurisation de la chaîne de transmission de la clé.
- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires [8] .

1.5.2 Chiffrement à clé publique (Chiffrement asymétrique) :

Le cryptage à clé publique est un type de cryptage dans lequel l'utilisateur dispose d'une paire de clés de cryptage, la clé déclarée et la clé secrète [12] [13] [14]. La clé secrète reste un secret. Quant à la clé déclarée, elle peut être distribuée à tout le monde. Les deux touches sont liées à une opération mathématique spécifique (elle varie selon l'algorithme utilisé), cependant, il n'est pas possible d'accéder à l'une des touches par l'autre. L'avantage de ce système est que lorsqu'un message est chiffré avec la clé déclarée, il ne peut être déchiffré qu'au moyen de la clé secrète correspondante.

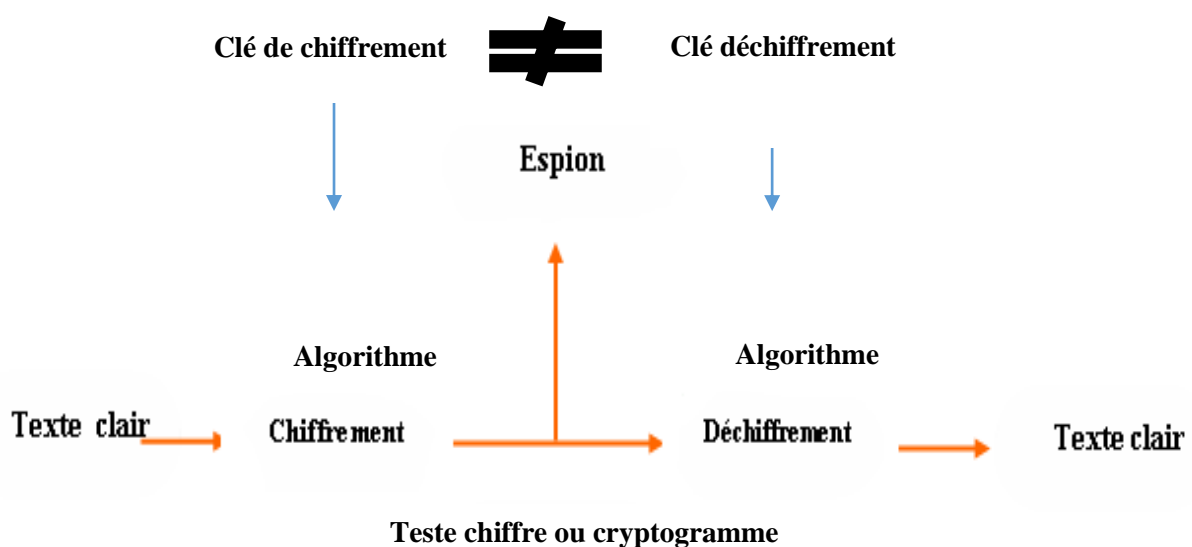


Figure1.2: Chiffrement asymétrique.

1.5.2.1 Caractéristiques du cryptage asymétrique :

- L'élimination de la problématique de la transmission de la clé.
 - La possibilité d'utiliser la signature électronique.
 - L'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisée.
 - Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique.
 - Le temps d'exécution : plus lent que le cryptage symétrique [14].
- Le danger des attaques par substitution des clés d'où la nécessité de valider les émetteurs des clés.
- Taille des clés, plus grande que celle des systèmes symétriques.

1.6 Méthodes du cryptage des images

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

Contrairement aux images, l'utilisation d'une méthode de compression avec perte est totalement interdite lors du chiffrement d'un texte, par conséquent, les chercheurs ont étudié plusieurs méthodes de chiffrement d'image avec/sans perte [23]. D'autre part, les algorithmes de chiffrement des images peuvent être classés selon le domaine d'application comme suit :

1.6.1 Méthodes dans le domaine spatial

Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'image lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles.

Les pixels de l'image peuvent être reconstruits (récupérés) complètement par un processus inverse sans aucune perte d'information.

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

- Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels.
- Dans la deuxième catégorie, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits [23].

1.6.2 Méthodes dans le domaine fréquentiel

Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause généralement une perte d'information [23].

1.7 Outils élémentaires d'analyse d'un algorithme du cryptage d'image (Mesures de Performance) :

1.7.1 Espace de clés

La taille de l'espace de clé est le nombre de paires de clés de cryptage/décryptage qui sont disponibles dans le système de chiffrement [19]. Une condition nécessaire, mais pas suffisante à un schéma de cryptage pour qu'il soit sûr est que l'espace clés soit suffisamment grand pour assurer la sécurité contre l'attaque par force brute [23].

1.7.2 Analyse statistique

1- L'histogramme

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

d'image, l'histogramme de l'image chiffrée doit être uniforme pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme [17].

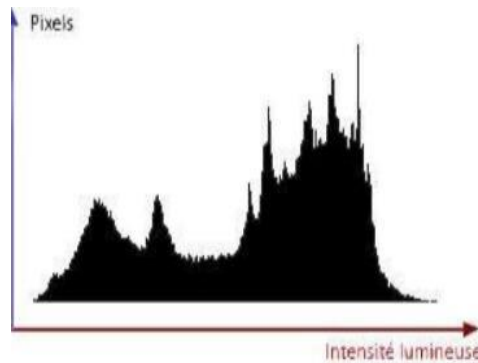


Figure1.3 : Histogramme d'une image niveau de gris [21].

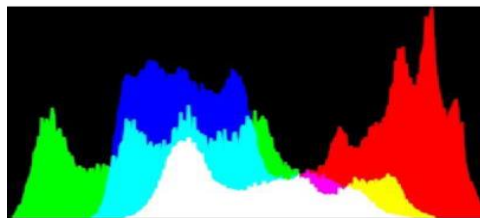


Figure1.4 : Histogramme d'une image couleur [21].

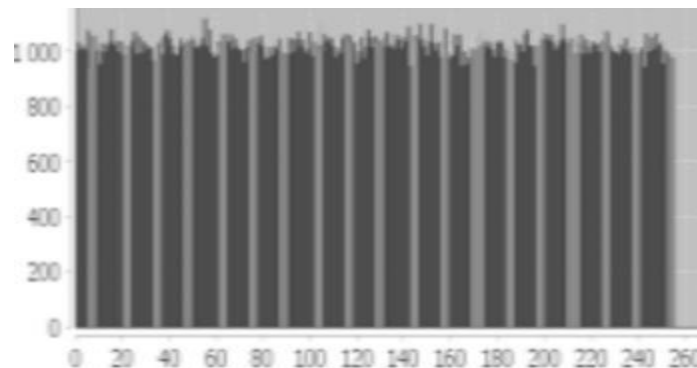


Figure1.5 : Histogramme d'une image chiffrée [25].

2- La corrélation entre les pixels adjacents

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence. Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique [23], et les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes :

$$r_{xy} = \frac{\sum_{i=1}^M \sum_{j=1}^N (x_{i,j,\bar{x}})(y_{i,j,\bar{y}})}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (x_{i,j,\bar{x}})^2 (y_{i,j,\bar{y}})^2}} \quad (1.4)$$

3- L'entropie

L'entropie d'une information est la quantité d'information englobée ou libérée par une source d'information. En particulier, plus la source est redondante, moins elle contient d'information [26]. En absence de contraintes particulières, l'entropie est maximale pour une source dont tous les symboles sont équiprobables. Ainsi, elle est l'une des principales mesures de l'aléatoire de l'information. Les valeurs de l'entropie élevée manifestent un haut degré de caractère aléatoire, et pour tout message codé sur M bits, la limite supérieure de l'entropie est M. La formule utilisée pour calculer l'entropie d'une source m est comme suit [23].

$$h(m) = -\sum p_i \log_2 (p_i) \in [2^n - 1] \quad (1.5)$$

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

1.8 La compression des images :

1.8.1 Définition de la compression d'image

Les méthodes de compression et de codage réduisent le nombre de bits par pixel à stocker ou à transmettre, en exploitant la redondance informationnelle dans l'image [27].

Les principaux critères d'évaluation de toute méthode de compression sont :

- ✓ La qualité de reconstitution de l'image.
- ✓ Le taux de compression.
- ✓ La rapidité du codeur et décodeur (codec).

1.8.2 Principe de la compression d'image :

La compression des données ou le codage source, permet en appliquant des algorithmes de compression spécifiques de réduire la taille d'une image sur une mémoire ou de manière équivalente de réduire son temps de transmission.

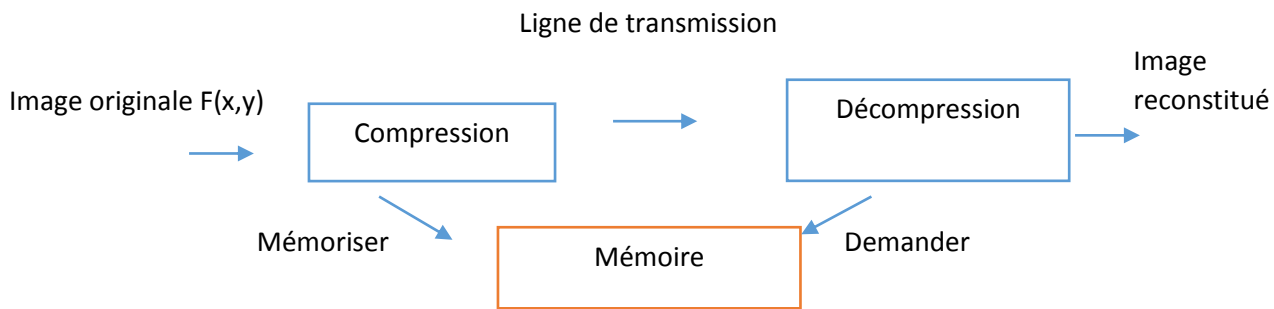


Figure1.6:Principe de la compression d'image pour la transmission ou stockage.

La compression peut être sans perte, l'image restera fidèle à l'image originale, soit elle sera avec perte de qualité pour réduire plus la taille de l'image, dans ce cas-là, la compression sera au prix de la dégradation autorisée, ces types de compression sont faites grâce aux redondances des données présentes sur l'image. Ces redondances sont :

- ✓ **Redondance psycho visuel** : Des détails non perceptible à l'œil humain qu'on peut éliminer (cf. caractéristiques de la vision humaine).
- ✓ **Redondance inter pixel** : La possible corrélation existante entre les pixels de l'image, on dit qu'une image a une redondance inter pixel si c'est possible de prédire la valeur d'un pixel en connaissance de la valeur des pixels voisins (suivants ou précédant), sachant que plus la résolution de l'image est grande plus la probabilité de rencontré des redondances inter pixel est élevée.
- ✓ **Redondance de codage** : séquences de répétition des bits, on rencontre cela généralement à la fin de la compression, pendant l'étape de codage

1.8.3 Objectif de la compression :

Le but de la compression des images est de réduire le nombre moyen de bits par pixel nécessaires à sa représentation. Il est possible dans une certaine limite de réduire ce nombre sans perte d'information. Au-delà, il est nécessaire d'élaborer des algorithmes de compression irréversibles (avec pertes) induisant une distorsion pas ou peu visible dans les conditions normales d'observation des images [28].

Le schéma fonctionnel de la compression est présenté dans la figure1.7 ci-dessous :

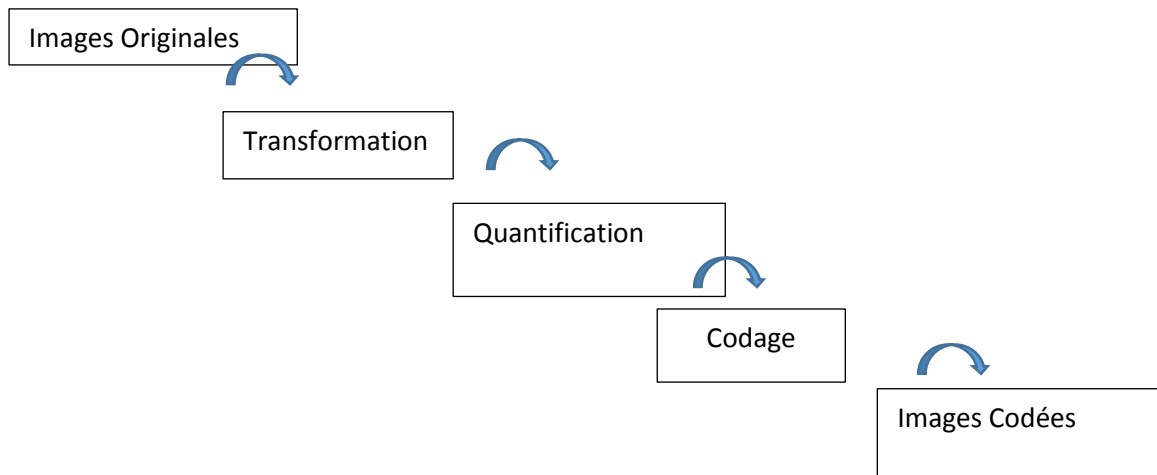


Figure1.7: schéma d'un codeur source [29]

A partir de ce schéma, nous allons revoir chacune de ses étapes à fin de préciser leur rôle.

- 1- Transformation :** La dépendance existante entre chacun des pixels et ses voisins (la luminosité varie très peu d'un pixel à un pixel voisin) traduisent une corrélation très forte sur l'image. On essaie donc de tirer parti de cette corrélation, pour réduire le volume d'information en effectuant une opération de dé-corrélation des pixels. La dé-corrélation consiste à transformer les pixels initiaux en un ensemble de coefficients moins corrélés, c'est une opération réversible.
- 2- Quantification :** La quantification des coefficients a pour but de réduire le nombre de bits nécessaires pour leurs représentations. Elle représente une étape clé de la compression. Elle approxime chaque valeur d'un signal par un multiple entier d'une quantité q , appelée quantum élémentaire ou pas de quantification. Elle peut être scalaire ou vectorielle. Un des résultats fondamentaux des travaux de Shannon concernant la relation : (débit /distorsion) montrent que l'on obtient de meilleures performances en utilisant la quantification vectorielle.
- 3- Codage** Une fois les coefficients quantifiés, ils sont codés. Un codeur doit satisfaire a priori les deux conditions suivantes :
 - **Unicité :** deux messages différents ne doivent pas être codés de la même façon.
 - **Déchiffrable :** deux mots de codes successifs doivent être distingués sans ambiguïté.

1.8.4 Classification des méthodes de compression

La plupart des méthodes de compression visent à enlever la redondance présente dans l'image de manière à diminuer le nombre de bits nécessaires à sa représentation [30].

Plusieurs types de redondance en termes de corrélation peuvent être considérés :

- La redondance spatiale entre pixels ou blocs voisins dans l'image.
- La redondance temporelle entre images successives dans une séquence vidéo.
- Les méthodes de compression peuvent se regrouper, en deux classes :
- Les méthodes sans perte d'informations (sans distorsion ou réversible).
- Les méthodes avec perte d'informations (avec distorsion ou irréversible).

Les expérimentations menées montrent que généralement les méthodes qui atteignent des taux de compression très élevés sont les méthodes avec distorsion. Par contre, les méthodes sans distorsion engendrent des taux de compression très faibles et ne sont utilisées que dans des applications sensibles telles que les images médicales et les images satellites.

1.8.5 Méthodes de compression :

Il existe deux méthodes de compression d'images :

1) La compression sans pertes.

Appelée aussi compression non destructrice, la qualité de l'image après décompression est la même que celle de l'image originale, le taux de compression de ce type est limité. Ce type de compression on le trouve beaucoup dans le domaine où la précision est majeure comme l'imagerie médicale (IRM par ex.) ou la télédétection (imagerie satellite par ex.). Les algorithmes de compression employés sont nombreux, les plus importants sont:

- Codage à répétition : par ex. RLC (RunLengthCoding).
- Codage entropique : basé sur le codage à longueur variable ou VLC (Variable LengthCoding), par ex : le codage de Huffman, le codage arithmétique, etc...
- Codage dictionnaire ou codage Lempel-Ziv-Welch (LZW) : Ce codage ne nécessite plus de connaître les probabilités des symboles comme dans le cas du codage entropique.

La figure (1.8),montre les compresseurs sans perte les plus utilisés en littérature spécialisée du domaine :

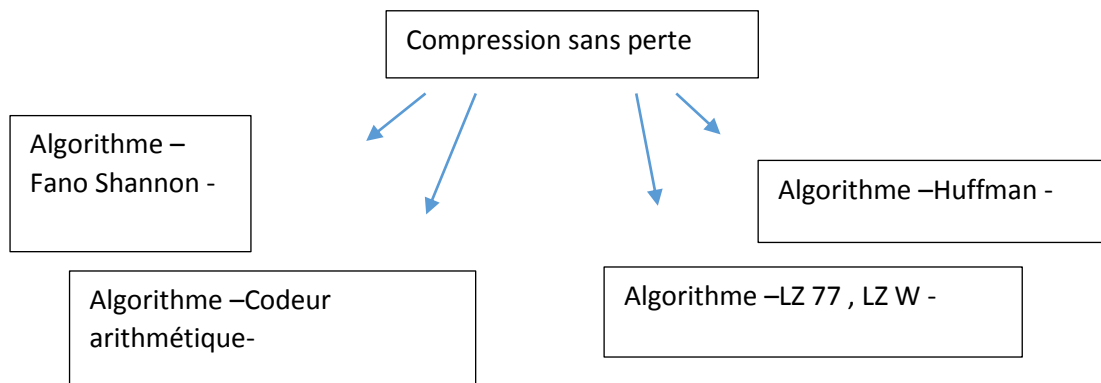


Figure1.8: Algorithme de compression sans perte les plus utilisés.

2) La compression avec pertes.

C'est une compression destructrice, elle permet de sacrifier certains détails de l'image non récupérable en décompression au profit de réduction de poids. Cette dégradation peut être contrôlée selon la qualité qu'on veut obtenir en fonction du taux de compression choisie.

L'objectif des algorithmes de compression avec perte est minimiser cette dégradation de qualité pour un taux de compression donnée. Donc la clé de la compression avec perte est une modification non réversible de la source permettant d'obtenir une nouvelle source dont l'entropie est plus faible. il existe deux catégories principales de compression avec perte :

- Les méthodes directes.
- Les méthodes par transformées.

La figure (1.9) présente un schéma synoptique des méthodes de compression avec perte: [31].

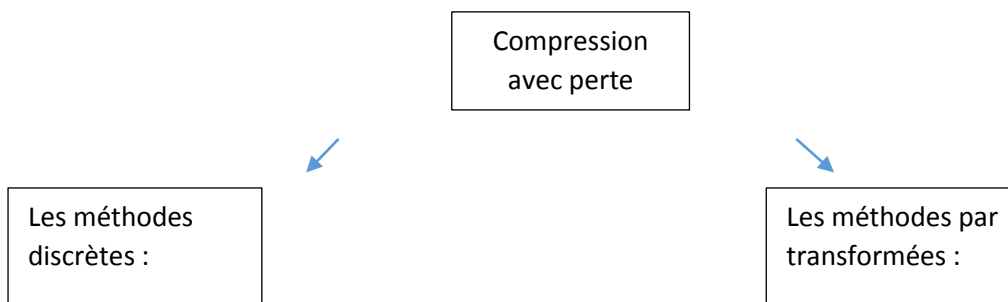


Figure1.9: Méthodes de compression avec perte.

1.8.6 Méthodes par transformée

Dans ces méthodes, l'image de dimension $N_x \times N_y$ est subdivisée en sous images ou blocs de taille réduite (la quantité de calcul demandée pour effectuer la transformation sur l'image entière est très élevée). Chaque bloc subit une transformation mathématique orthogonale inversible linéaire du domaine spatial vers le domaine fréquentiel, indépendamment des autres blocs (transformée en un ensemble de coefficients plus ou moins indépendants). Les coefficients obtenus sont alors quantifiés et codés en vue de leur transmission ou de leur stockage. Pour retrouver l'intensité des pixels initiaux, on applique sur ces coefficients la transformation inverse. Parmi les transformations linéaires existantes [32]:

- Transformation de Karhunen-Loeve (TKL).
- Transformation de Fourier Discrète (TFD).
- Transformation de Hadamard (TH).
- Transformation en Cosinus Discrète (TCD)[27].
- Transformation en ondelettes (TO).

Le principe d'un système de codage par transformation est le suivant la figure 1.10 :

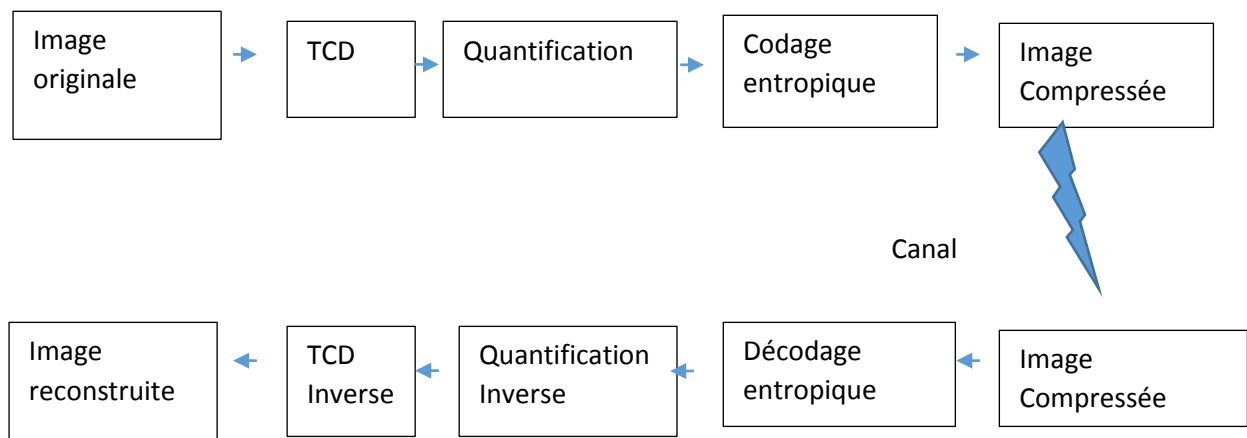


Figure1.10: principe d'un système de codage par transformation

1.9 Les normes de compression des images avec et sans pertes

1.9.1 La norme de compression JPEG

La norme JPEG [34] (Joint Photographic Experts Group) est conçue par le groupe ISO (International Standards Organisation) et le groupe CEI (Commission

Chapitre I : Généralités sur la cryptographie et La compression d'image numérique

Electronic International). Elle est destinée à la compression des images fixes en couleurs et à niveaux de gris en vue de leur stockage sur les supports numériques. Elle a été réalisée dans la perspective de couvrir les applications les plus diversifiées en tenant compte des contraintes réalistes par rapport aux applications les plus visibles : publication, transmission, banques d'images.

Les techniques définies par la norme JPEG se divisent en deux classes :

- les méthodes de compression avec pertes qui sont basées sur la TCD suivie d'une quantification et d'un codeur entropique.
- La seconde classe, concerne les processus de codage sans pertes, cette classe de codeurs n'est pas basée sur la TCD mais sur le codage MICD suivi d'un codage entropique.

Pour les méthodes avec pertes, quatre codeurs ont été spécifiés : un codage de base où l'image compressée puis décompressée n'est plus identique à l'image originale, ce processus utilise la TCD et un codage de Huffman.

Les trois autres types de codage sont une extension de codage de base. Ils diffèrent de codage de base principalement par le codage entropique en utilisant un codage arithmétique ou par restitution progressive de l'image.

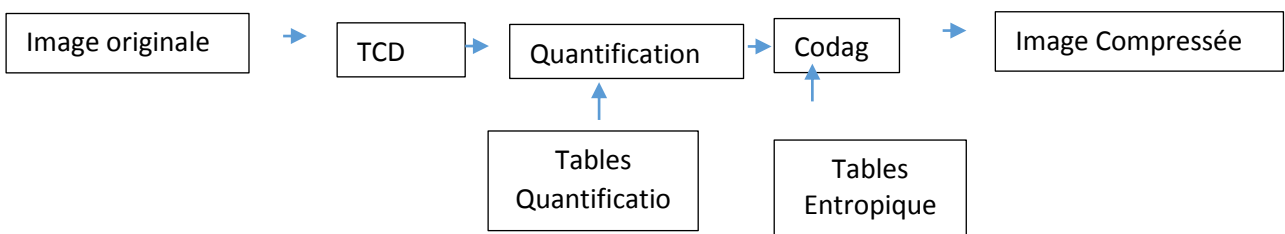


Figure1.11 : principe de l'algorithme JPEG avec pertes[29].

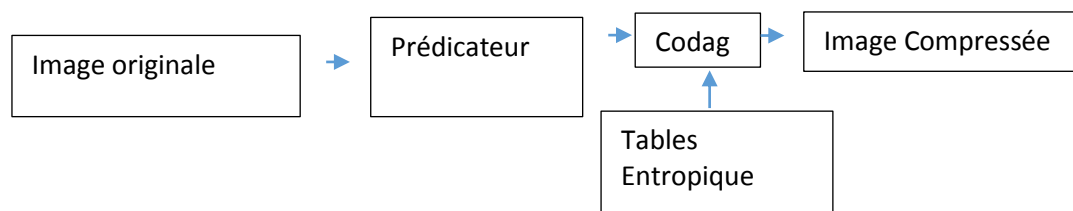


Figure1.12 : principe de l'algorithme JPEG sans pertes[29].

1.9.2 La norme de compression MPEG

Les efforts développés par les équipes du CCITT (Comité Consultatif International de Téléphonie et Télécommunication) pour le H.261 ont été utilisés comme point de départ pour le développement d'un standard de codage d'images animées par ISO, ce standard s'intitule MPEG pour MovingPictures Experts Group.

La première phase de MPEG intitulée MPEG-I spécifie une compression du signal vidéo à un débit de 1.5 Mbits/s. Les deux autres phases ont pour but d'améliorer la qualité du codage vidéo en sacrifiant une augmentation de débit, MPEG-II est destinée à la compression du signal vidéo à des débits d'ordre de 10 Mbits/s, MPEG-III est destinée à la télévision haute définition à des débits de 30 à 40 Mbits/s. Une quatrième phase, MPEG-IV est destinée au codage d'images animées à très faibles débits (10 Mbits/s), MPEG-A tourné vers les applications multimédia. En cours de standardisation.

1.10 Transformées en ondelettes par SPIHT :

Cette méthode SPIHT (Set Partitioning in Hierarchical Trees) proposée par A. Said et Pearlman [41] diffère de ses antécédentes par la manière avec laquelle les coefficients sont classés ainsi que pour le traitement des coefficients significatifs. Un autre point important est que cette méthode, génère un flot binaire intéressant (au niveau de la compression) sans passer par un codage entropique contrairement au codage EZW dont les résultats n'apparaissent qu'une fois associé au codage arithmétique [41], [42].

Le principal avantage de cet algorithme est qu'il est plus rapide en exécution que EZW, et peut donner de meilleurs résultats [41].

L'algorithme (SPIHT ou Set Portioning in Hierarchical Trees) est une méthode de compression d'image basée sur les ondelettes. SPIHT introduit trois listes :

- 1. Liste des pixels significatifs (LSP),**
- 2. Liste des pixels non significatifs (LIP) et**
- 3. Liste des ensembles non significatifs (LIS).**

L'algorithme SPIHT partitionne l'ondelette décomposée en partitions significatives et non significatives selon la fonction suivante (1.10) [26] :

$$S_n(T) = \begin{cases} 1 & , \max_{(i,j) \in T} \{|C_{i,j}|\} \geq 2^n \\ 0 & , otherwise \end{cases} \quad (1.10)$$

ou $S_n(T)$ est la signification d'un ensemble de coordonnées du (T) , et $C_{i,j}$ est la valeur du coefficient à la coordonnée (i, j) .

1.10.1 Processus de codage SPIHT

Le processus d'encodage SPIHT utilise ces listes :

- 1. Initialisation (Initialization):** pour la sortie n , LSP est vide ; plus tard, ajoutez les coordonnées de la racine de départ à LIP ou LIS.
- 2. Passe de tri (Sorting Pass):** A chaque entrée dans LIP, il décidera qu'il est significatif et donne le résultat de la décision de sortie. Si le résultat de la décision est significatif, alors transféré dans le LSP et la coordonnée présente avec leur signe. Si les autres coordonnées vont toutes être significatives, alors ce processus est arrêté.
- 3. Passe de raffinement (Refinement Pass):** dans cette passe, toutes les valeurs de pixel dans LSP sont maintenant $2^n \leq |C_{i,j}|$, et la sortie sera le n ème bit significatif.
- 4. Mise à jour de l'étape de quantification (Quantization-stepupdate):** Dans cette étape, décrémentez n de 1 et passez à l'étape 2

Les processus de décodage sont similaires aux processus d'incorporation mais dans l'ordre inverse. La décompression basée sur le processus SPIHT.

1.10.2 Principe de L'algorithme SPIHT :

L'algorithme SPIHT se déroule en deux passages ; Un pour triage des coefficients significatifs et l'autre pour le raffinement des amplitudes de ces coefficients. Pour chercher les coefficients significatifs, l'algorithme fait le test de signifiante pour chaque liste (LIP, LIS). L'encodeur transmet '1' au décodeur s'il contient un coefficient significatif et '0' sinon. Lorsque le décodeur reçoit '0' il conclut que l'ensemble n'est pas significatif puisque l'encodeur et le décodeur s'il contient un coefficient significatif et '0' sinon, Lorsque le décodeur reçoit '0' il conclut que l'ensemble n'est pas significatif puisque l'encodeur et le décodeur partitionne les coefficients de la même manière. Lorsqu'un ensemble dans (LIS) est significatif, il est divisé en sous-ensembles par une règle commune à l'encodeur et au décodeur, ces nouveaux ensembles sont à leur tour traité de la même manière.

A chaque passage, un nouveau seuil est utilisé, le passage d'un seuil à l'autre se fera par une décrémentation de 1 pour n. Le processus de division s'arrête lorsque tous les coefficients significatifs ont été déterminés ou une fonction de cout est achevée.

Ce nouveau partitionnement semble plus efficace, puisqu'un codage entropique du flux quantifié n'est plus nécessaire, ce qui améliore nettement le temps de calcul. Bien entendu, une méthode avec codage entropique a aussi été étudiée des PSNR meilleur.

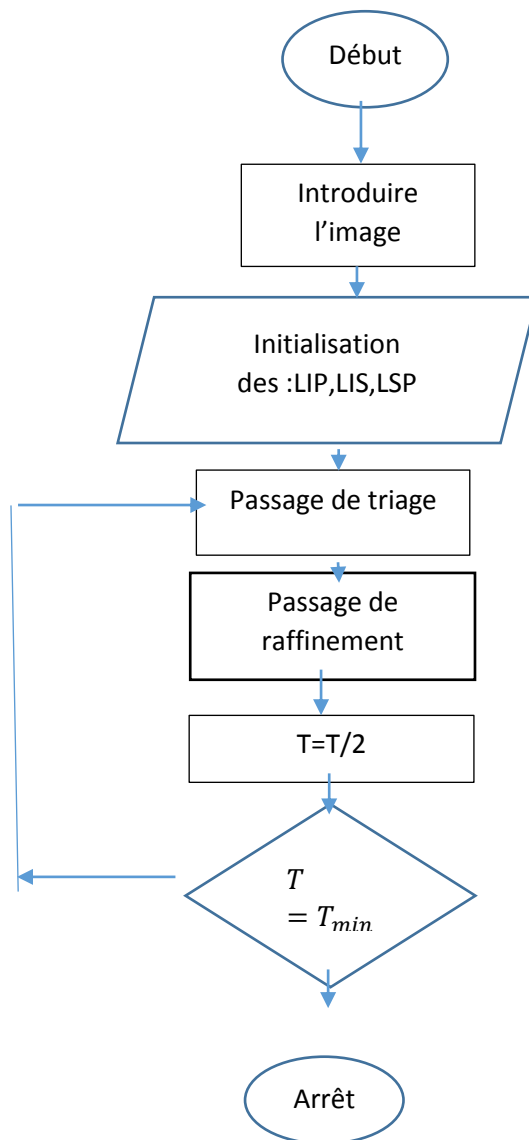


Figure1.13 : Diagramme en bloc de l'algorithme « SPIHT ».

1.11 Evaluation de la qualité d'une compression :

La compression consiste à réduire la taille physique de blocs d'informations, elle s'appuie sur l'analyse de contenu de l'image et tire profit de son organisation interne, afin d'en éliminer les données redondantes qu'elles soient temporelles, spatiales, statistique. Une méthode de compression bien adaptée à l'une des modalités d'imagerie médicale ne l'est pas forcément pour une autre. Où, tout au moins, une méthode peut demander des adaptations différentes selon les modalités. [44,43]

Une motivation majeure des recherches en compression d'images médicales vient de la proportion croissante d'examen acquis numériquement. Il faut les stocker, les communiquer et les visualiser malgré les masses de donnée reçues. Alors existe-t'il une méthode de compression rapide, offrant des forts taux de compression et une très bonne qualité de l'image reconstruite ?

Et pour cela on estime la performance d'une compression effectuée par :

- Taux de compression

Il sert à mesurer l'efficacité d'une méthode de compression

On rappelle RC : rapport de compression.

$$RC = \frac{\text{Nombre de bits utilisées par l'image originale}}{\text{Nombre de bits utilisées par l'image compressées}} \quad (1.11)$$

On définit aussi la quantité T_c appelée taux de compression par :

$$T_c = \left(1 - \frac{1}{RC}\right) \cdot 100 \quad (1.12)$$

L'objectif de la compression d'image est donc d'avoir un taux de compression le plus élevé possible ; toutefois la théorie de l'information donne une limite théorique au taux maximale qu'il est possible d'atteindre sans distorsion pour toute méthode de compression sur une image donnée.

- L'entropie

On définit l'entropie d'un point particulière P d'une image par :

$$H(P) = \sum_{m_i=1}^m p(n_i) \cdot I(n_i) \quad (1.13)$$

Avec :

n_i : les niveaux de gris que peut revêtir le point P ;

m : le nombre totale de n_i ;

$p(n_i)$: la probabilité d'apparition du niveau de gris n_i ;

$I(n_i)$: l'information propre du niveau de gris n_i qui est définit par :

$$I(n_i) = \log_2 \frac{1}{p(n_i)} \quad (1.14)$$

D'où l'entropie sera :

$$H(P) = - \sum_{m_i=1}^m p(n_i) \cdot \log_2 p(n_i) \quad (1.15)$$

Donc :

L'entropie caractérise la quantité d'informations que contient une image. Toutefois, une image, dont tous les pixels ont la même valeur contient très peu d'informations, son entropie est faible. Par contre, une image, dont tous les pixels ont une valeur aléatoire contient beaucoup d'informations et son entropie est forte.

- **Débit**

Représente le nombre moyen de bits nécessaire pour coder un pixel de l'image. Il est défini par l'équation suivante :

$$B_{pp} = \frac{\text{Nombre de bits par pixels dans l'image originale}}{R_C} \quad (1.16)$$

- **Le temps de compression /décompression**

Le temps de compression/décompression nécessaire pour coder/décoder une image est fonction de la complexité de l'algorithme, de l'efficacité de son implémentation et de la puissance de processeur.

- **Mesure de détorsion**

La mesure de distorsion utilisée généralement en compression d'images est l'erreur quadratique moyenne MSE (Mean Square Error). Cette grandeur représente la moyenne des écarts aux carrés entre le pixel I (i, j) et celui de l'image reconstruite \hat{I} (i,j).

Donc : le MSE est défini par la relation suivante :

$$MSE = \frac{1}{N} \sum_{n_i} (n_i - \hat{n}_i)^2 \quad (1.17)$$

Avec :

n_i : le niveau de gris de l'nième point de l'image originale ;

\hat{n}_i : le niveau de gris de l'nième point de l'image transformée ;

N : le nombre total de points constituant chacune des images.

- **Le rapport signal sur bruit crête (SNR) en dB**

Le rapport signal sur bruit (SNR) est largement utilisé pour la mesure de la qualité d'une Image. Il est défini de la manière suivante :

$$SNR = 10 \log_{10} \left(\frac{\sum_{i=0}^{M-1} \sum_{j=0}^{n-1} I^2}{N_x MSE} \right) [\text{db}] \quad (1.18)$$

Le PSNR est habituellement exprimé en décibels est défini comme suit [39]:

$$PSNR = 10 \log_{10} \frac{N_{dgmax}^2}{MSE} [\text{db}] \quad (1.19)$$

Avec :

N_{dgmax} : le niveau de gris maximum et l'exemple couramment utilisé en télévision numérique est $N_{dgmax}=255$;

donc

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad [\text{db}] \quad (1.20)$$

- **Indice de Similarité Structurale (SSIM)**

L'indice de similarité structurelle SSIM (ou SSIM : Structural Similarity) est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale. La similarité compare la luminosité, le contraste et la structure entre chaque paire de vecteurs où l'indice de similarité structurelle (SSIM) entre deux images (I) et (S) [40],[41] est donné par :

$$SSIM(I, S) = I_1(I, S) \cdot I_2(I, S) \cdot I_3(I, S) \quad (1.21)$$

L'indice de similarité structurelle moyenne MSSIM est exprimé comme suit:

$$MSSIM(I, S) = \frac{1}{M} \sum_{j=1}^M SSIM(I_j, S_j) \quad (1.22)$$

1.12 Conclusion :

En conclusion, nous avons le besoin d'images compressées de bonne qualité est en constante augmentation. La compression par la méthode de codeur SHPIT, à son époque avait fourni des taux record. Cependant certaines données importantes doivent être protégées pendant leur transmission ce qui n'est pas assuré par la méthode de codeur SHPIT, c'est pourquoi le besoin de compression et de chiffrement, s'accroît et les chercheurs dans le domaine de la sécurité de l'information accordent une attention croissante à la combinaison de compression et chiffrement.

Chapitre II

Systeme Dynamique Chaotique

2. Introduction :

Depuis fort longtemps, la science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos était synonyme du désordre et de confusion qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines. [46].

Le chaos a ainsi trouvé de nombreuses applications dans différents domaines tel que la physique, la biologie, la chimie l'économie, les télécommunications (Cryptage de l'information)..etc. et particulièrement le cryptage. Pour cette raison, ce chapitre est un tour d'horizon des systèmes chaotiques sans pour autant être une référence. Nous nous intéresserons principalement aux systèmes dynamiques chaotiques sur leurs applications, aspect aléatoire, l'attracteurs étranges et les différentes propriétés de ces systèmes. Il présente essentiellement ce qui est en relation à notre travail de cryptage d'images.

2.1 Notion de chaos :

Avant toute chose, intéressons-nous à la manière dont la notion de chaos a progressivement germé dans l'esprit des scientifiques au fur et à mesure que l'on a progressé dans les époques.

Depuis l'antiquité l'homme s'est rendu compte que quelque chose lui échappait dans le comportement de la nature. pour cela un groupe de scientifiques commence à s'intéresser à des problèmes de tous les jours qui étaient considérés depuis longtemps comme sans solution parce que complètement discontinus et désordonnés (les variations météorologiques, comment se forment les nuages, les arythmies cardiaques, les oscillations du cerveau, ...etc.).

Tous ces phénomènes dans lesquels on ne pouvait déceler a priori aucune logique ont progressivement été regroupés sous le terme de "chaos " .

Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des "comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites.

Ces systèmes sont donc déterministes bien qu'imprévisibles. On le définit parfois également comme un "comportement complexe, apériodique et irrégulier, d'apparence aléatoire".

Divers auteurs, précisent que le chaos est "un comportement effectivement imprévisible à long terme survenant dans un système dynamique à cause d'une sensibilité aux conditions initiales (S.C.I), il peut également être produit "par un système récursif déterministe non linéaire. [47]

2.2 Système dynamique :

C'est une structure qui change au cours du temps. Mathématiquement, un système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état X_n ou n représente la dimension du vecteur, et qui caractérisent l'état instantané du système dynamique. L'ensemble de tous les états possibles est appelé espace d'état ou espace de phase. En plus de l'espace d'état, un système dynamique est défini par une loi d'évolution, généralement désignée par dynamique, qui caractérise l'évolution de l'état du système au cours du temps [48].

2.2.1 Définition :

Globalement, un système dynamique, décrit des phénomènes qui évoluent au cours du temps, dont le terme « système » fait référence à un ensemble de variables d'état. [46]

2.2.2 Classe système dynamique :

Les systèmes dynamiques sont classés en deux catégories :

A) système dynamique Discrets :

Un système dynamique discret est représenté comme suit :

- La condition initiale est : x_0 ;
- Le premier état est : $x_1 = f(x_0)$
- Le deuxième état, qui suit immédiatement le premier, est :
 $x_2 = f(x_1) = f(f(x_0)) = f_2(x_0)$
- Le troisième état est donné par : $x_n = f(x_{n-1}) = \dots = f^n(x_0)$

B) système dynamique Continu :

Un système dynamique continu est décrit par un système d'équations différentielles de la forme :

$$\frac{dx(t)}{dt} = f(x(t)) \quad (2.1)$$

2.2.3 Trois Sortes De Systèmes Dynamiques :

On peut différencier trois sortes de systèmes dynamiques [49] :

a) Les systèmes aléatoires :

Les systèmes aléatoires aussi appelés systèmes stochastiques. Évoluent comme leur nom l'indique au hasard dans tout l'espace sans qu'aucune équation ne les régit, et sans qu'aucune prévision exacte ne soit possible dans le temps.

b) Système déterministe :

C'est un système qui réagit toujours de la même façon à un événement entrant, c'est-à-dire que le système produit le même événement sortant (à sa périphérie). Autrement dit, l'ordre d'arrivée des événements entrants détermine l'ordre des événements sortants [50].

Ce sont des systèmes régis par des lois mathématiques bien connues, on peut donc prévoir exactement l'évolution de ces systèmes dans le temps. Transformé en un système dynamique autonome de dimension $n+1$ [48].

c) Les systèmes dynamiques ou chaotiques :

Ils ont un comportement infiniment complexe. Ils sont irrésistiblement attirés par une figure géométrique de structure également infiniment complexe sur laquelle ils semblent errer au hasard, mais sans jamais la quitter, ni repasser deux fois par le même point. Les attracteurs qui caractérisent ces systèmes, semblent inclure à la fois des lois déterministes et des lois aléatoires, ce qui rend impossible toute prévision à long terme.

2.2.4 Le chaos :

C'est un comportement particulier d'un système dynamique, qui inclut [51, 50]:

- ✓ **La non-linéarité** : Le système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.
- ✓ **Le déterminisme** : Le système chaotique a des règles fondamentales déterministes et non probabilistes.
- ✓ **La sensibilité aux conditions initiales** : Un petit changement sur l'état initial peut mener à un comportement absolument différent sur l'état final (figure 2.1)
Exemple : soient deux états initiaux 3,04326423410 et 3,04326423411, après un certain temps, le résultat dans le premier cas 4.1 et dans le deuxième -2.6.
- ✓ **L'imprévisibilité** : à cause de la sensibilité aux conditions initiales, le système chaotique évolue d'une manière qui semble aléatoire. La figure 2.2 permet de comparer une évolution simple, périodique et prédictible d'un système classique avec une évolution plus complexe, non périodique et non prédictible d'un système chaotique.
- ✓ **L'irrégularité** : Ordre cache comprenant un nombre infini de modèles périodiques instables.

Mathématiquement, le comportement chaotique est expliqué par deux principes importants :

2.3 Propriétés de système chaotiques :

Bien qu'il n'y ait pas de définition mathématique du chaos universellement acceptée, une définition couramment utilisée stipule que pour qu'un système dynamique soit classifié entant que chaotique, il doit comporter les propriétés suivantes [14] :

- Aspect aléatoire.
- Sensibilité aux conditions initiales.
- Imprévisibilité.
- Exposants de Lyapunov.
- Bifurcation.
- Notion d'attracteur.

2.3.1 Aspect aléatoire :

Les systèmes chaotiques se comportent, en effet d'une manière qui peut sembler aléatoire. Cet aspect aléatoire du chaos vient du fait que l'on est incapable de donner une description mathématique du mouvement, mais ce comportement est en fait décrit par des équations non linéaires parfaitement déterministes, comme par exemple les équations de Newton régissant l'évolution d'au moins trois corps en interaction.

2.3.2 Sensibilité aux conditions initiales :

En faisant la troncature de quelques chiffres sur les conditions initiales de son système de prévision météorologique, Lorenz a mis en relief le caractère le plus important des systèmes chaotiques qui est la sensibilité à la condition initiale. Mais en fait c'est avant cette anecdote, que ce phénomène a été découvert. Vers la fin du 19^{ème} siècle, Poincaré montrait que les trois orbites de 3 corps en mouvement sous une force centrale due à la gravité changent radicalement avec une petite modification des conditions initiales. Pour un système chaotique, une très petite erreur sur la connaissance de l'état initial x , dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée.

2.3.3 Imprévisibilité :

En raison de la sensibilité aux conditions initiales, qui peuvent être connues seulement à un degré fini de précision. Le chaos ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase ou chaque point définit un état et le point associé à cet état décrit une trajectoire, appelé également une orbite.

2.3.4 Exposants de Lyapunov :

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches

L'exposant de Lyapunov (λ_{EL}) se définit par :

$$\lambda_{EL}(x_0) = \lim_{n \rightarrow \infty} \sup \frac{1}{n} \log |f(n)'(x_0)| = \lim_{n \rightarrow \infty} \sup \frac{1}{n} \sum_{j=0}^{n-1} \log |f'(x_j)| \quad (2.2)$$

Avec $x_j = f_j(x_0)$

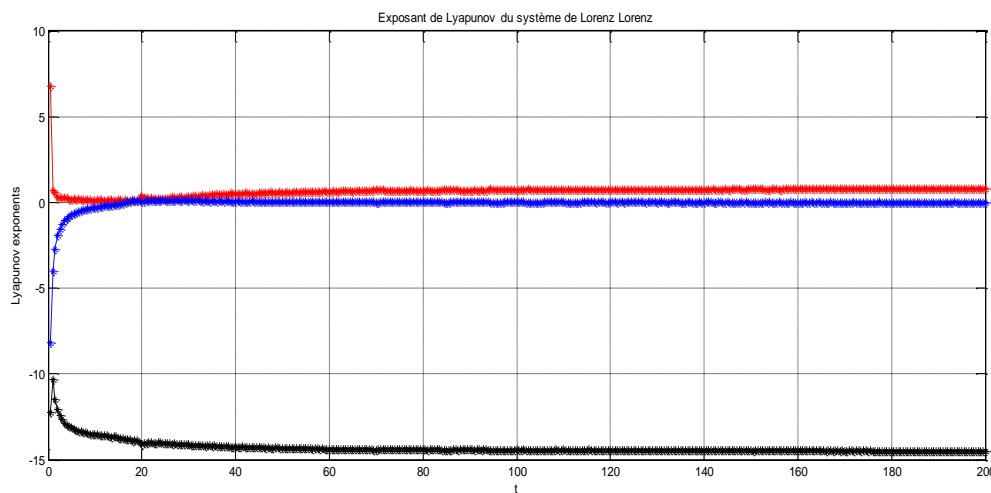


Figure 2.1 : Lyapunov de Lorenz

2.3.5 Bifurcation :

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation.

2.3.6 Les attracteurs :

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. [52]

2.3.6.1 Les différents types d'attracteurs :

Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques. [47]

A) Attracteurs réguliers :

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de trois sortes :

- 1. Un point fixe :** la trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales.
- 2. Un cycle limite :** il représente la trajectoire du pendule idéal dans ce même espace des phases.
- 3. Un tore :** qui correspond à l'attracteur obtenu par les mouvements résultant de deux oscillations indépendantes (par exemple : les oscillateurs électriques).

Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non chaotiques, des trajectoires qui partent de points proches l'un de l'autre dans l'espace des phases restent indéfiniment voisines. On sait donc prévoir l'évolution à long terme de ces systèmes, à partir d'une situation connue.

B) Les attracteurs étranges :

L'attracteur étrange désigne une figure dans l'espace des phases représentant le comportement d'un système dynamique. Il est représentatif d'un système multi périodique si le système possède au moins deux fréquences d'oscillation indépendantes. L'attraction des trajectoires autour de l'attracteur est liée au caractère dissipatif du système réel.

A grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition, deux points ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, il doit se replier sur lui-même. Le processus d'étirement repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais.

Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques.

On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes. On ne peut évidemment représenter que des attracteurs de faibles dimensions (2 à 3) ou des "coupes" d'attracteurs à nombreuses dimensions. [47]

2.3.6.2 Classes d'attracteurs analogique et numérique :

On peut trouver deux classes d'attracteurs: analogique et numérique.

A) Attracteurs analogique :

Exemples : quelque types des attracteurs

1. L'attracteur Lorenz.
2. L'attracteur Rössler.
3. L'attracteur Venderpol.

4. L'attracteur Circuit de Chua.
5. L'attracteur Duffing.
6. L'attracteur Filippov.

B) Attracteurs numérique :

Exemples : quelques types des attracteurs

1. L'attracteur Hénon.
2. L'attracteur Peter de Jong.
3. L'attracteur Hénon-Lozi.
4. L'attracteur Gumowsky-Mira.
5. L'attracteur Pickover.
6. L'attracteur Wallpaper.
7. L'attracteur Clifford.
8. L'attracteur Quadratic.
9. L'attracteur Ikeda.

2.4 Les systèmes chaotiques continus et discrets :

2.4.1 Systèmes chaotiques continus :

Un système chaotique à temps continu est décrit par un système d'équation différentielle de forme [53]

$$\dot{x} = f(t), y = h(t, x, u) \quad (2.3)$$

où : f est le vecteur d'état de dimension n , $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ est une fonction non linéaire qui désigne le champ de vecteur, $h: \mathbb{R}^n \rightarrow \mathbb{R}$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq \mathbb{R}^P$ représente l'entrée du système. Si ce système ne dépend pas de l'entrée, on aura alors. [53]

$$\dot{x} = f(t, x) \quad (2.4)$$

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer les systèmes de Lorenz, henon , etc.

A) Système de Lorenz :

Historique :

Au début des années 60, **Edward Lorenz** un physicien spécialisé en météorologie au Massachusetts Institute of Technology (M.I.T.) travaillait sur un modèle mathématique dont le but était de prédire la température. Un jour, il voulut reproduire sur ordinateur une séquence de résultats obtenus quelques jours plus tôt. Les ordinateurs de l'époque étaient terriblement lents alors pour gagner du temps, il fit démarrer son programme au milieu de la séquence plutôt qu'au début. Il utilisa une des valeurs de son ancienne liste de résultats. Il s'attendait à retrouver les valeurs qu'il avait obtenues précédemment mais à sa grande surprise ce ne fut pas le cas. Lorsqu'il revint une heure plus tard, il constata que les nouveaux résultats s'éloignaient de plus en plus des résultats obtenus quelques jours auparavant. Rapidement il en découvrit la cause. La valeur de la séquence initiale était 0,5061127 et Lorenz avait fait commencer sa suite en tapant seulement les trois premiers chiffres 0,506. Les scientifiques de cette époque se considéraient chanceux lorsqu'ils pouvaient disposer d'une mesure exacte à trois décimales alors pour eux, une quatrième ou une cinquième décimale ne pouvait certainement pas avoir d'effets notoires sur les calculs. Lorenz prouva le contraire. Il découvrit qu'une infime variation sur les conditions initiales de certains systèmes dynamiques (systèmes qui décrivent dans l'espace un état qui évolue dans le temps) pouvait avoir des conséquences tout à fait imprévisibles sur leurs comportements.

Malgré un article publié en 1963 sur le sujet, il faudra attendre jusqu'en 1972 pour qu'on s'intéresse à la découverte de Lorenz. C'est à la suite d'une conférence qu'il donna intitulée «Un battement d'aile de papillon au Brésil peut-il déclencher une tornade au Texas?» que la théorie du chaos devint une sorte de mode. Retenons ici que la théorie du chaos touche divers domaines qui ont tous comme point commun leur sensibilité aux conditions initiales. Même si de très grands noms tels Maxwell, Poincaré, Hadamard et Kolmogorov furent des précurseurs de la théorie du chaos, on attribue généralement ses origines à Edward Lorenz.

Lorsqu'il fait sa découverte, Lorenz travaillait sur un système constitué de douze équations. Il créa par la suite à l'aide des seules variables x , y et z , un modèle

simplifié représentant un phénomène de convection dans une boîte chauffée par le bas, un peu comme les mouvements de l'air qui se produisent l'été lorsque le soleil chauffe fortement le sol et créent de petits nuages blancs appelés cumulus. [52]

- **Système d'équations :**

L'attracteur est défini par le système d'équations suivant :

• **Premier équations du Système de Lorenz :**

$$\begin{aligned} \frac{dx}{dt} &= b * (y - x) \\ \frac{dy}{dt} &= b * x - y - x * z \\ \frac{dz}{dt} &= a * y - c * z \end{aligned} \quad \text{Avec } a, b, c, \text{ constantes.} \quad (2.5)$$

• **Deuxième équations du Figure1.1**

En utilisant la discrétisation, nous pouvons obtenir les équations différentielles. Ici, nous choisissons la méthode d'Euler pour la discrétisation de l'équation. Défini par la définition de la dérivée, pour suffisamment petit [19] :

$$\frac{y(x_{n+1})-y(x_n)}{h} \approx y'(x_n) \approx f'(x_n, y(x_n)) \quad (2.6)$$

Grâce à cela, nous pouvons tirer $(x_{n+1}) \approx (x_n) + h(x_n, y(x_n))$, selon la méthode de l'équation de Lorenz pour l'utilisation de la dérivée par rapport au discret :

$$\begin{cases} x_{n+1} = x_n + \sigma(y_n - x_n)h \\ y_{n+1} = y_n + (Rx_n - y_n - x_n z_n)h \\ z_{n+1} = z_n + (x_n z_n - \beta z_n)h \end{cases} \quad (2.7)$$

Les variables x , y et z représentent les états du système à chaque instant. Avec h , R , σ , et β sont les paramètres du système. Le système présente un comportement chaotique pour $h=0.0001$, $R=28$, $\sigma=10$, et $\beta=8/3$, sont et présente un attracteur du Système de Lorenz.

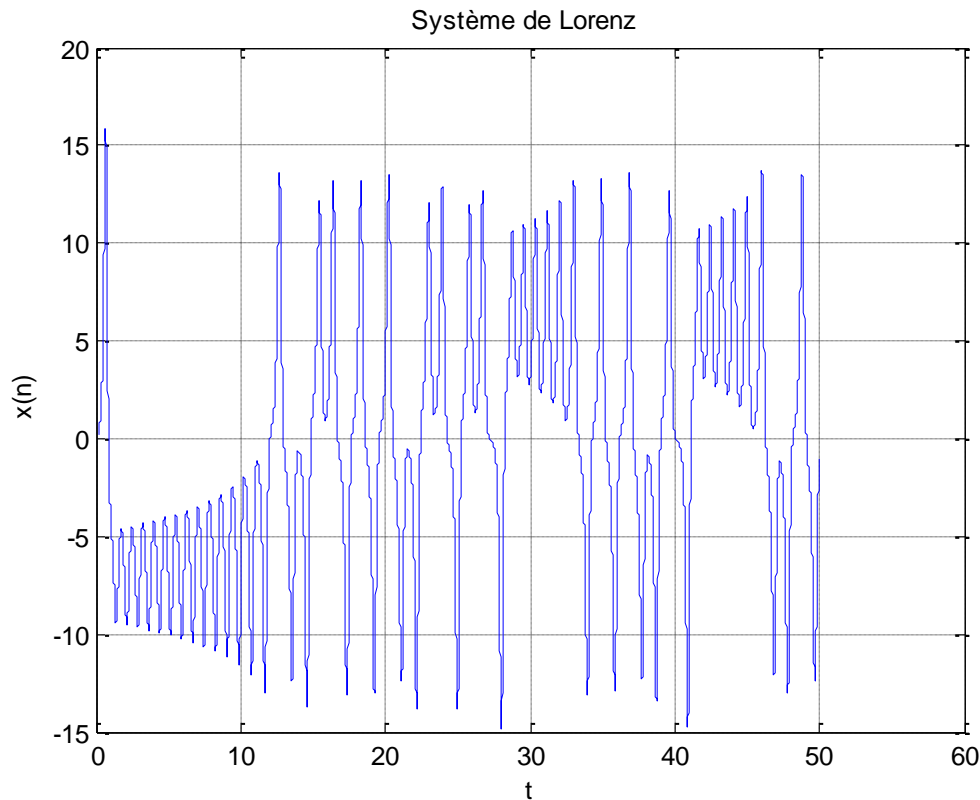


Figure 2.2 : Attracteur du Système de Lorenz de 50 iteration pour $h=0.0001$, $R=28$, $\sigma=10$, et $\beta=8/3$

A.1 Aspect aléatoire du système de Lorenz :

(la figure 2.3) illustre l'aspect aléatoire des états du système (2.5)

- Les différentes courbes de l'attracteur :

Si on programme ces formules avec le logiciel MATLAB 6.5 avec les valeurs $S=10$, $r = 28$, $b = 8/3$, $x_0 = 8$; $y_0 = 3$; $z_0 = 4$; on aura les figures suivantes :

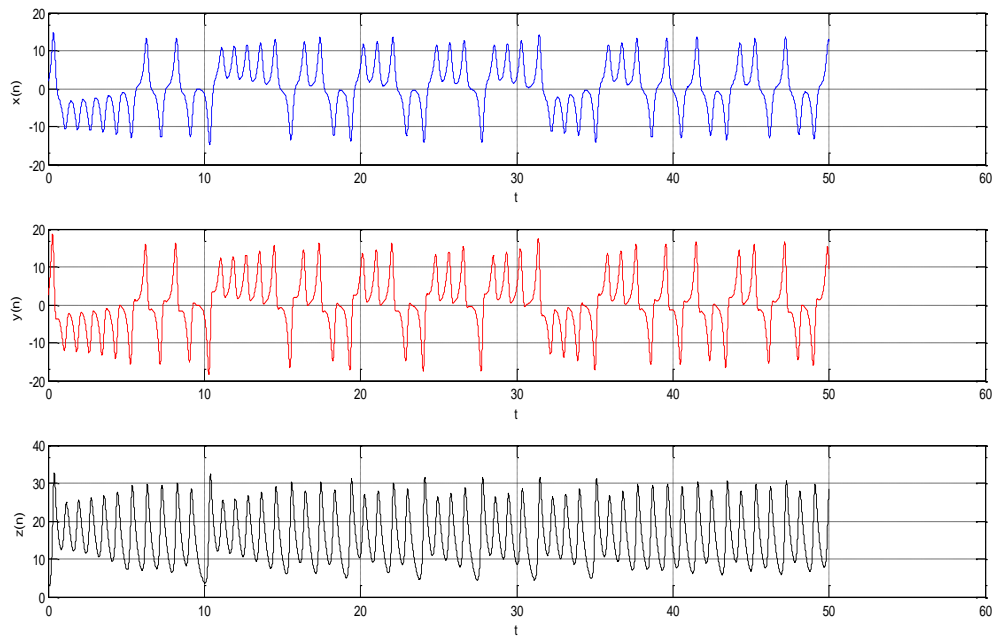


Figure 2.3: Aspect aléatoire du Courbes en x, y, z de l'attracteur de Lorenz

A.2 Sensibilité aux conditions initiales du système de Lorenz :

On a le cas initial: $x_1(0)=0.100$ $x_2(0)=0.101$

En prenant $x_1(0)$ $x_2(0)$ pour conditions initiales très proches, les évolutions des signaux x_1 et x_2 ont un comportement différent au fur et à mesure que le temps augmente, la figure (2.4), illustre les résultats obtenus.

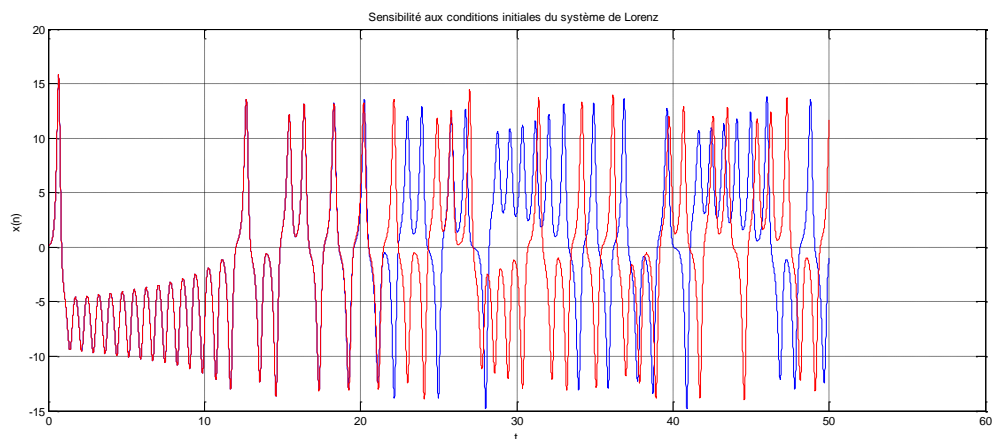


Figure 2.4: Sensibilité aux conditions initiales pour le Système de Lorenz

pour $h=0.0001$, $R=28$, $\sigma=10$, et $\beta=8/3$

Le système chaotique (2.5) présente une courbe attracteur étrange en forme d'ailes de papillon, représenté sur la figure (2.5). 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 donné par le système (2.5) est indépendante du temps t , par conséquent ce type de système est qualifié d'être autonome.

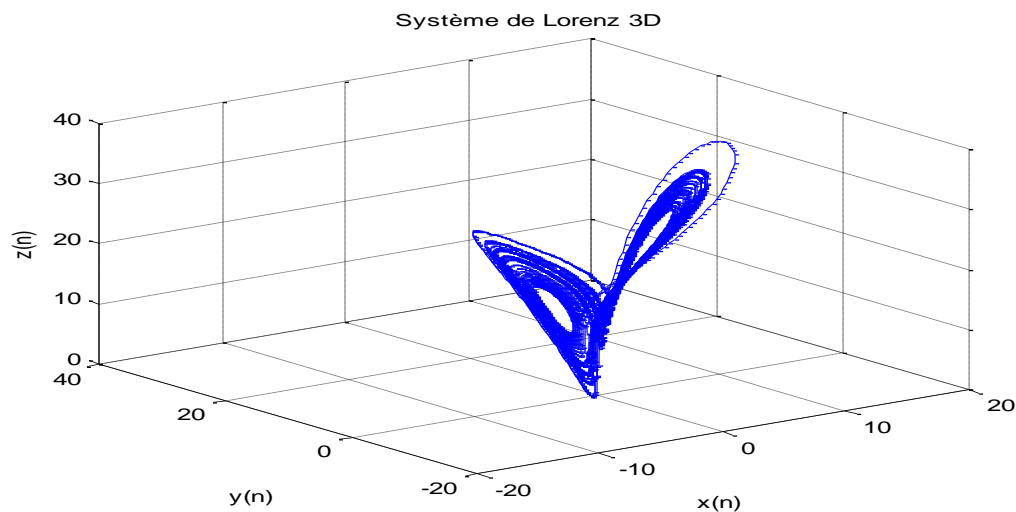


Figure 2.5 : Les projections d'attracteur de Lorenz en 3D

Un système chaotique à temps discret est décrit par un système d'équations aux différences finies, dont le modèle général est le suivant :

$$x(n+1)=x(n), u(n), y(n)=x(n), u(n) \quad (2.8)$$

Il existe plusieurs systèmes chaotiques discret-s. Parmi eux, on peut citer les systèmes de Hénon, Lozi, la fonction logistique, etc...

B) Fonction carte logistique :

- La carte logistique (Logistic Map):

La carte logistique (ou Logistic Map) est devenue un système dynamique discret très utilisé dans plusieurs domaines tels que la biologie, artificielle, télécommunications, l'analyse de données et beaucoup d'autres. Robert May a

montré que cette carte a des comportements chaotiques .La carte logistique est définie par l'équation (2.8) [54]:

$$x_{n+1} = M(x_n) = \mu x_n(1 - x_n) \text{ and } x_n \in [0 \ 1] , \quad (2.9)$$

Avec μ entre 0 et 3.999

Cette carte a également été proposée comme générateur de nombres pseudo-aléatoires par Von Neumann en partie parce qu'elle avait une distribution algébrique connue afin que les valeurs itérées puissent être transformées en une répartition uniforme. Au cours des années, de nombreuses autres réalisations des générateurs de nombres aléatoires basés sur diverses formes de l'équation logistique ont été proposées [55],[56]. C'est sous cette forme qu'il est étudié comme carte logistique. Cette suite, bien que très simple dans son expression, peut conduire à des résultats très différents; Son comportement varie entre les valeurs μ :

μ entre 1 et 3, c'est-à-dire entre 0 et 2, la séquence x_n converge vers $\frac{\mu-1}{\mu}$

et on récupère une séquence x_n convergée à n . μ pour plus de 3, la séquence x_n peut, dans la plage μ comprise entre 2, 4, 8, 16 ... valeurs ou être chaotique.

L'intérêt est du à ses caractéristiques importantes, dont elle est déterministe, sensible aux conditions initiales, son mouvement est ergodique et elle est intégrée avec un nombre infini d'orbites périodiques instable.

La figure (2.7), présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ entre 0 et 3.999.

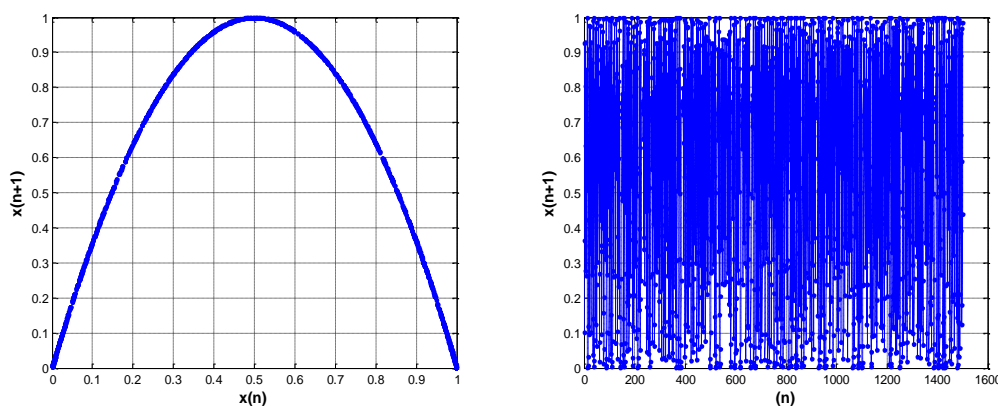


Figure 2.6 : Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique (N = 1500, $\mu=4$, $x_0=0.1$).

Le Diagramme du Cobweb est une procédure spécialement adaptée pour l'analyse qualitative du comportement d'une fonction itérative f à une dimension. ce diagramme est utile pour déterminer l'évolution des itérations de la fonction f pour une condition initiale de donnée et pour une valeur de paramètre donnée.

La carte logistique, décrit par l'équation (2.8) est utilisée dans différentes sortes d'application, telle que : la génération des signaux pseudo aléatoires, l'échantillonnage, l'analyse numérique, synchronisation des systèmes numériques, étalement de spectre, etc. cette dernière été proposée pour la communication à spectre étalé [57], [58] .

Contrairement aux séquences aléatoires, c'est une séquence générée par la carte logistique est reproductible à partir de l'état initiale x_0 . cependant, cette séquence se compose d'un ensemble de cantor dans $[0,1]$. En revanche, plusieurs applications utilisent des séquences de nombre entier de taille $N \gg 1$. Parmi ces application dans la sécurité d'information et étalement / désétalement de spectre à séquence direct DS-SS dans le système DS-CDMA.

Motivés par cette problématique, nous allons définir un nouveau système dynamique chaotique basé sur carte logistique ce système a permis la génération des séquences chaotiques de N entier ($N \in \mathbb{N}$).

B.1 Aspect aléatoire de la fonction logistique :

La figure suivante illustre l'aspect aléatoire du système (2.8) pour $r = 4$. Il est alors impossible de discerner à l'oeil nu cette trajectoire de celle d'une variable aléatoire.

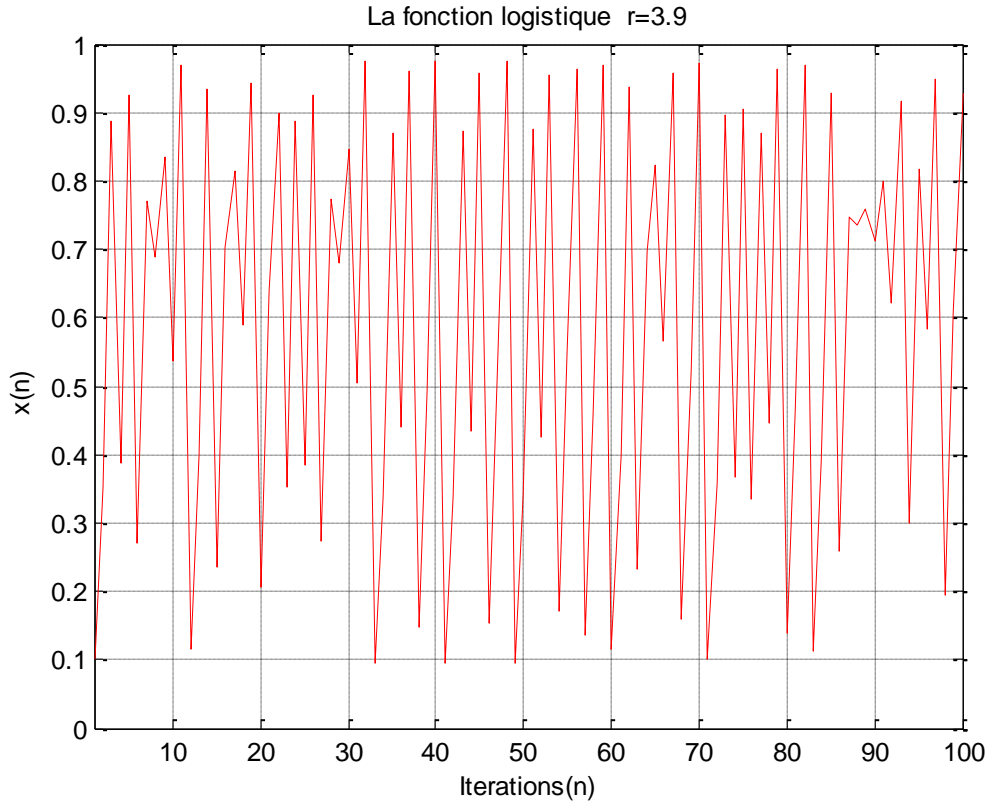


Figure 2.7 : application logistique pour r=4

B.2 sensibilité aux conditions initiales de la fonction logistique :

- Sensibilité aux conditions initiales:

Une caractéristique de la sensibilité aux conditions initiales du système chaotique, qui peut fournir des signaux qui ont des quantités de classe aléatoire non liées, et adapté pour déterminer et produire une régénération [59],[60]. Plus précisément, pour $f(x)$, l'application commence par deux valeurs initiales qui sont proches, disons x et y telles qu'une grande quantité et génèrent les orbites des deux premiers points.

$$E(n) = |f^n(x) - f^n(y)| \tag{2.10}$$

Ou n : Itération.

- La figure 2.9 représente la sensibilité de la nouvelle carte Logistique, avec un coefficient $\mu = 3.999$, la longueur $N = 100$, la valeur initiale des deux séquences chaotique est respectivement 100 et 101, et leur différence une ε est supérieur à zéro ($\varepsilon > 0$).

On a le cas initial:

$$x_1(0) = 0.8$$

$$x_2(0) = 0.8000001$$

En prenant $x_1(0)$ $x_2(0)$ pour conditions initiales très proches, les évolutions des signaux x_1 et x_2 possèdent un comportement différent au fur et à mesure que le temps augmente, on a obtenu les résultats suivants, figure (2.8).

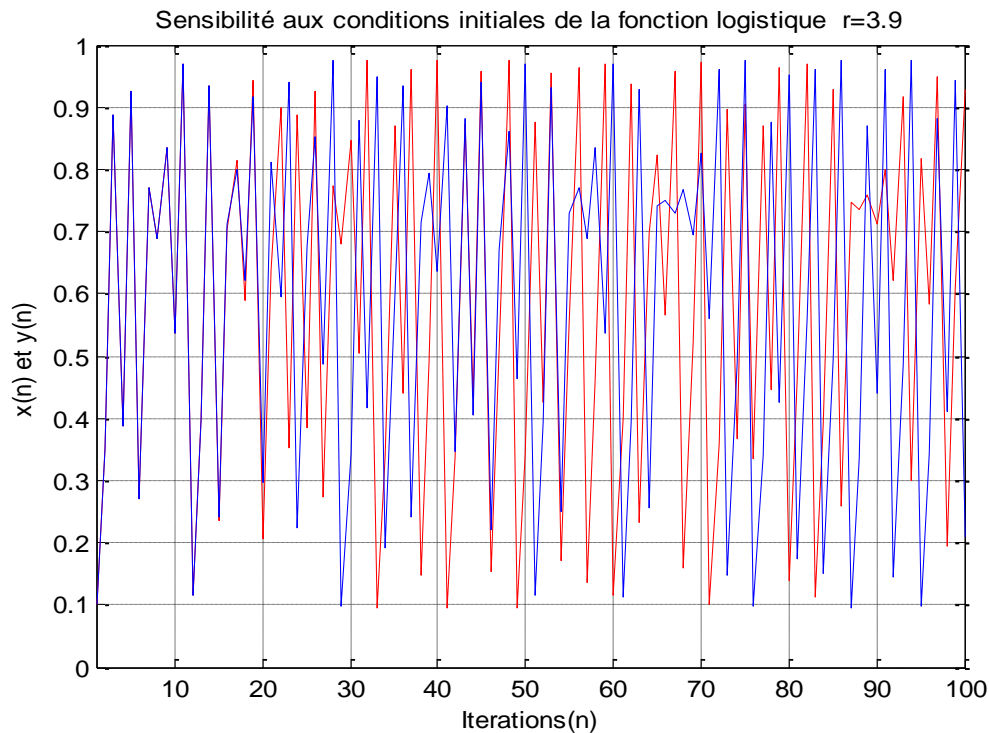


Figure 2.8 : Sensibilité aux conditions initiales de la fonction logistique

B.3 Exposant de Lyapunov de la fonction logistique :

Les systèmes et le chaotique déterministe sont également en contraste caractérisé par une extrême sensibilité aux petits changements dans leurs conditions initiales. Le russe Alexander Lyapunov (1857-1918), qui a introduit la quantité appelée Exposant de Lyapunov (LE). Cet exposant est de quantifier à quelle vitesse le comportement dynamique d'un système est susceptible de différer en fonction des conditions initiales appliquées que nous produisons sur elle. Supposons maintenant que nous changeons ceci en commençant des conditions de ε_0 de telle sorte $f(x_0)$ devient $f(x_0 + \varepsilon_0)$ après $(n+1)$ en des états successive, le changement de celle-ci $f(x_n)$

sera écrit $f(x_n + \varepsilon_n)$ telle sorte que devient successifs après x_0 et x_n soit quantifiée par l'équation (2.20) [Annexe A]:

$$\ln \left| \frac{\varepsilon_n}{\varepsilon_0} \right| = \ln \left| \frac{\varepsilon_n}{\varepsilon_{n-1}} \right| \cdot \left| \frac{\varepsilon_{n-1}}{\varepsilon_{n-2}} \right| \dots \left| \frac{\varepsilon_1}{\varepsilon_0} \right| = \sum_{i=1}^n \left| \frac{\varepsilon_i}{\varepsilon_{i-1}} \right|$$

(2.20)

Ou : $\left| \frac{\varepsilon_i}{\varepsilon_{i-1}} \right| = \left| \frac{f(x_{i-1} + \varepsilon_{i-1}) - f(x_{i-1})}{\varepsilon_{i-1}} \right| \xrightarrow{\varepsilon_{i-1} \rightarrow 0} |f'(x_{i-1})|$

(2.21)

Le composant de Lyapunov d'un 1D map $x_{n+1} = f_\mu(x)$ est défini par l'équation (2.22):

$$\lambda_L(x) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \ln |f'(x_k)|$$

(2.22)

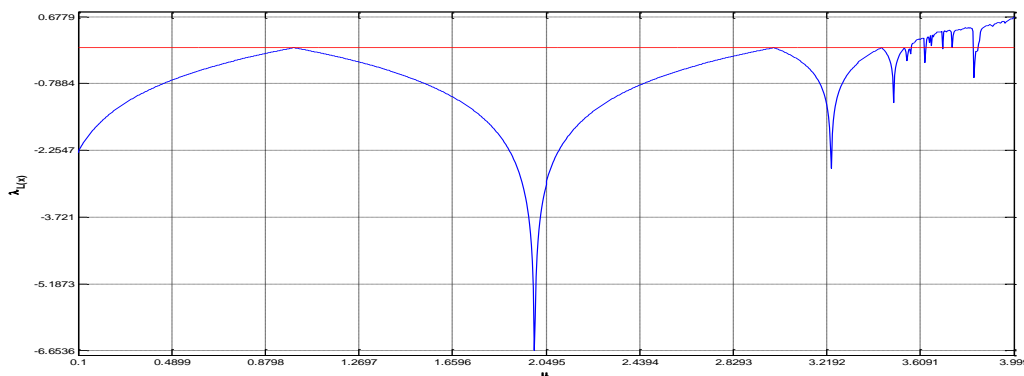


Figure 2.9 : Le composant de Lyapunov pour la carte logistique de $0.1 \leq \mu \leq 3.999$, $N = 1500$, $x_0=0.1$.

L'exposant de Lyapunov montre l'explication des diagrammes chaotiques. Il est souvent utilisé comme une mesure pour former le chaos d'un système dynamique. Simplement dit, cela caractérise le degré auquel le chemin qui commence à diverger très étroitement ensemble dans le temps.

Dans un système avec $LE > 0$, le trajet diverge exponentiellement et donc la dépendance sensible présente un système par rapport aux conditions initiales (fréquemment citées comme caractéristiques des systèmes chaotiques). En outre, si

$LE < 0$, le système est dispersif dans le sens que la trajectoire converge (le système du chaos n'est pas chaotique ci-dessous) et si $LE = 0$, le système est conservateur.

B.4 Diagramme de bifurcation pour la fonction logistique :

Les systèmes dynamiques non linéaires évoluent souvent vers des régimes stationnaires qui varient en fonction de certains paramètres de contrôle. Une faible perturbation de l'un de ceux-ci, lorsque les points d'équilibre du système sont stables, ne change pas son comportement. Cependant, il a des valeurs particulières des paramètres pour lesquelles on observe un changement qualitatif des caractéristiques du système par exemple, nombre de points d'équilibre, perte ou

changement de stabilité d'un point fixe, ou encore l'apparition de nouvelles solutions éventuellement plus complexes comme le chaos. Un changement de nature dans le comportement d'un système dynamique est appelé « Bifurcation », elle surgit lorsqu'un paramètre de contrôle franchit une valeur critique. Ainsi, un système dynamique non linéaire est confronté à bifurquer vers le chaos, lorsqu'on fait varier progressivement l'un de ses paramètres de contrôle, selon trois scénarios de transition possible [61] :

- **L'intermittence** : il s'agit d'un régime qui demeure pratiquement périodique durant de longs laps de temps, et qui se déstabilise brutalement, pour laisser place à une courte bouffée de bruit, puis le régime redevient périodique et ainsi de suite... lorsqu'on augmente la valeur du paramètre de contrôle, les bouffées deviennent de plus en plus fréquentes, et finalement, le chaos domine.
- **Le doublement de période (cascade sous harmonique)** : la variation d'un paramètre de contrôle fait passer le système par une suite de bifurcations, chacune correspondant à l'apparition d'une orbite de période double de la précédente, qui devient alors instable. La succession de ces bifurcations converge de manière géométrique vers un point d'accumulation, au-delà de lequel peuvent être observés des régimes chaotiques, qui n'apparaissent donc que lorsqu'un nombre infini d'orbites périodiques ont été créées.
- **La quasi-périodicité** : ce phénomène intervient lorsque le régime périodique devient quasi-périodique, c'est-à-dire son spectre contient deux fréquences d'oscillation indépendantes. L'influence des oscillations d'une sur l'autre conduit à

un dérèglement de leur mouvement qui peut à son tour perdre sa stabilité et devenir chaotique, soit directement, soit par la survenance d'une troisième fréquence.

Ces scénarios transitoires permettent de comprendre les mécanismes qui conduisent à l'apparition du chaos. Notant que les valeurs des paramètres critiques qui régissent ces changements sont appelées points de bifurcation. Elles peuvent être repérées graphiquement à l'aide d'un diagramme de bifurcation. Prêtons l'exemple de la récurrence logistique diagramme de bifurcation est un résumé visuel de la succession de doubles périodes produite par μ augmente.

La figure.(2.10) montrent que le paramètre de bifurcation μ est représenté sur l'axe horizontal du graphique et l'axe vertical montre les valeurs possibles de population et à long terme de la fonction logistique, Les résultats sont obtenus à partir des programmations sous *Matlab*

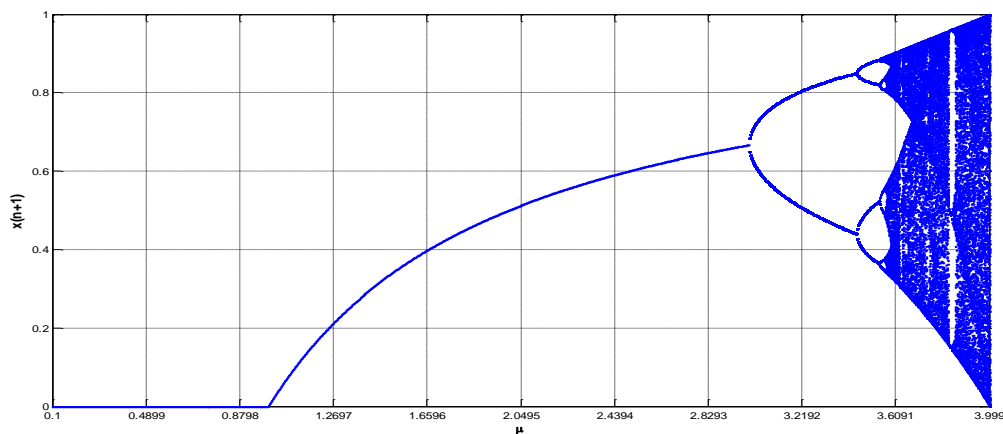


Figure 2.10 : Diagramme de bifurcation pour la carte Logistique de $0.1 \leq \mu \leq 3.999$.

2.5 Crypto système basé sur la confusion et la diffusion :

Les systèmes chaotiques ont une importance dans le domaine de cryptage d'image à cause de la sensibilité aux conditions initiales. Mathématiquement, une carte chaotique est une fonction de l'évolution qui présente une sorte de comportement chaotique. Ces cartes peuvent être paramétrées par un paramètre en temps discret ou continu. Les cartes discrètes prennent généralement la forme de fonctions itérées. Ces fonctions se composent de deux phases : confusion et diffusion (figure 2.11)[62]:

- ✓ Confusion : utilise une carte chaotique 2D qui consiste à permuter les positions des pixels dans l'image sans changer leurs valeurs.
- ✓ Diffusion : consiste à changer les valeurs des pixels dans l'image de sorte qu'un petit changement d'un pixel s'étend à tous les pixels de l'image.

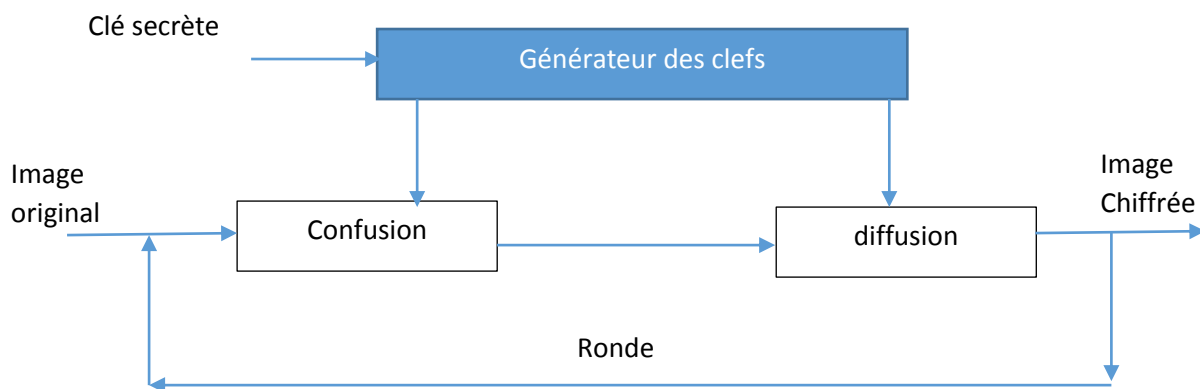


Figure 2.11 : Crypto-système basé sur la confusion et la diffusion.

Ou, dans la phase de confusion, les paramètres de la carte chaotique servent de clé de confusion. Et dans la phase de diffusion, la valeur initiale sert de clé de diffusion.

2.6 Conclusion :

Dans ce chapitre, les systèmes chaotiques ont été présentés, ainsi que leur utilisation à des fins de Crypto-système basé sur la confusion et la diffusion. Nous avons commencé par définir les systèmes dynamiques, ensuite nous avons présenté quelques définitions et propriétés des systèmes chaotiques tel que : la non-linéarité, le déterminisme, la sensibilité aux conditions initiales. Et finalement nous avons détaillé quelques exemples des systèmes chaotiques en temps continu et discret tel que : système de Lorenz.et carte logistique.

Chapitre III

**Simulation Crypto-système basé à Attracteur
Lorenz & carte logistique Sous MatLab .**

3. Introduction :

Le cryptage dans le domaine de l'imagerie numérique est une technique courante pour maintenir la sécurité de l'image. Cette technique essaie de convertir l'image originale une autre image qu'il est impossible de comprendre. En d'autres termes, elle assure qu'aucune personne ne peut connaître le contenu sans une clé pour le décryptage.

Dans ce chapitre on va réaliser un générateur pseudo aléatoire sur la base d'un attracteur Lorenz hybride par carte logistique, afin de réaliser un Chiffrement en continu basé sur les systèmes chaotiques et en suite la sortie Image crypter et compresser en format JPEG par Méthode Ondelette L'objectif principal du générateur chaotique est qu'ils sont parfaits pour le chiffrement, on espère produire une suite potentiellement illimitée de symboles qui a l'apparence d'une suite aléatoire.

La figure 3.1 montre comment l'image d'origine compressée en JPEG est convertie en image cryptée.

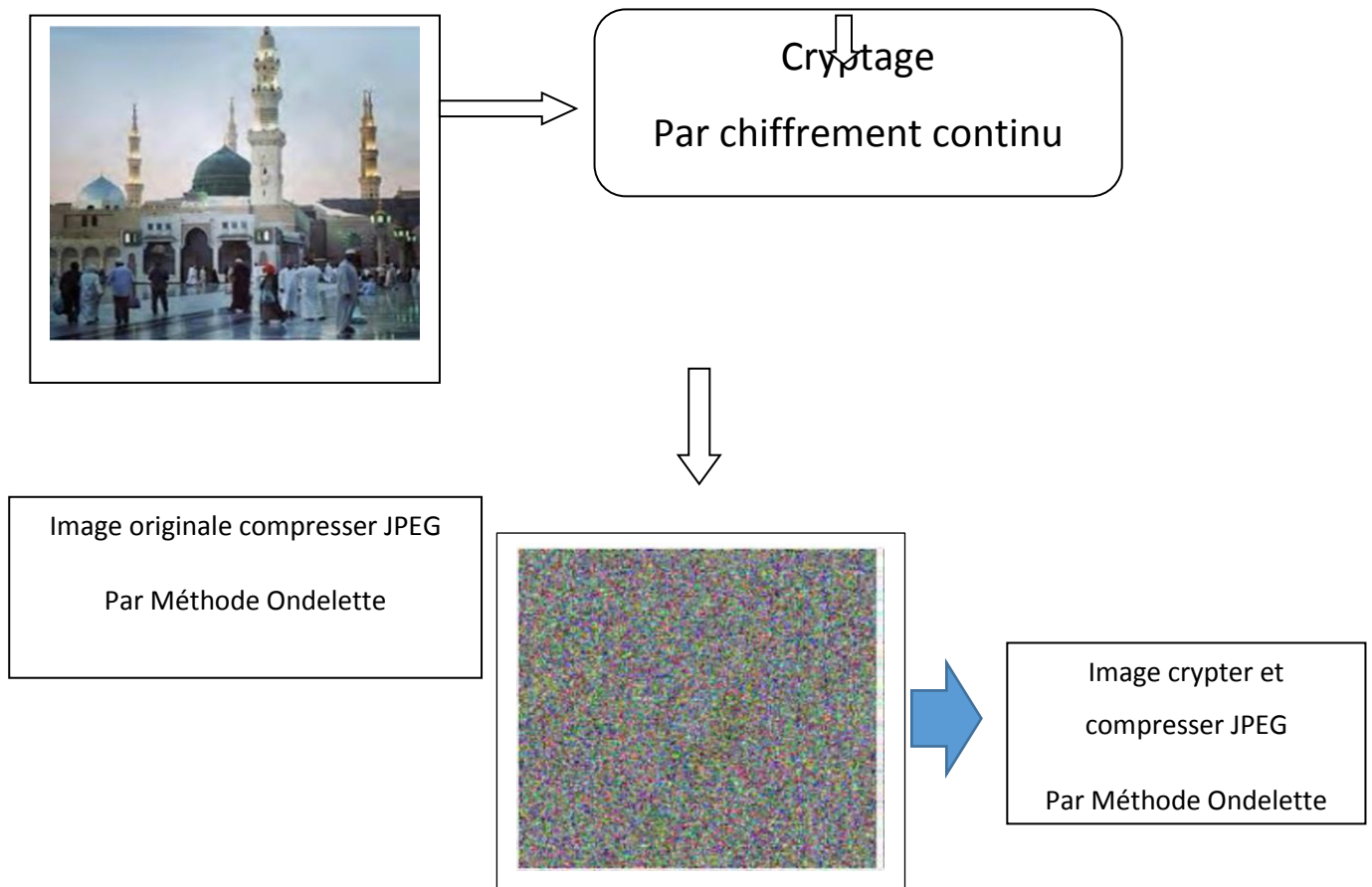


Figure 3.1 : Cryptage d'image par la technique du chiffrement continu
à base de l'algorithme Chaotique

Le cryptage d'image a des applications dans divers domaines, y compris la communication par Internet, l'imagerie médicale et la communication militaire.

3.1.1 Classification des algorithmes de chiffrement sélectif :

Le cryptage sélectif peut être classé, c'est-à-dire lorsque le cryptage et la compression sont appliqués. Le classement peut être considéré comme:

- **Pré-compression :**

Les algorithmes de chiffrement sélectif de cette classe effectuent le chiffrement avant la compression (resp., la décompression avant le déchiffrement) (voir Figure 3.2). Notez que ces algorithmes sont intrinsèquement compatible avec le format et généralement inapplicable pour la compression avec perte. Enfin, dans la plupart des cas, l'exécution du chiffrement avant la compression entraîne une expansion de la bande passante qui a un impact négatif sur l'efficacité de la

compression. Par conséquent, cette classe d'algorithmes n'est généralement pas compatible avec la compression.

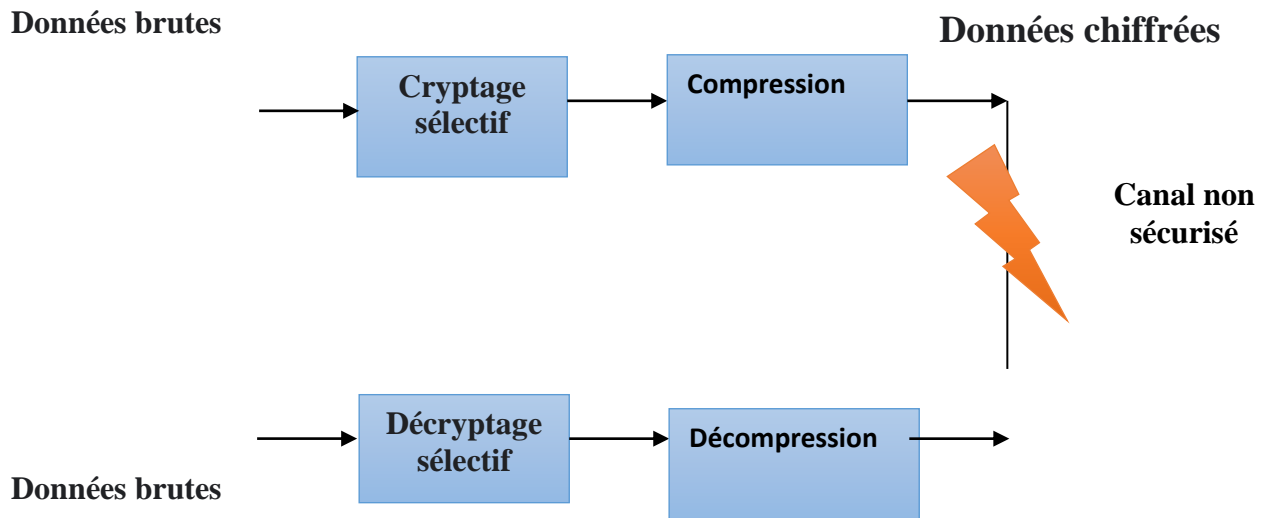


Figure 3.2: Approche Pré-compression.

- **Approche post-compression :**

Les algorithmes de chiffrement sélectif de cette classe effectuent la compression avant le chiffrement (voir Figure 3.3). Cette classe d'algorithmes est généralement compatible avec la compression ; une petite surcharge peut être introduite pour envoyer la clé de cryptage ou des informations sur le cryptage. Le cryptage et le décryptage n'ont pas besoin de modifications côté encodeur ou décodeur. Enfin, il a été suggéré que la classe de post compression est intrinsèquement non conforme au format. Dans cet article, nous donnons des exemples des algorithmes existants qui assurent la conformité au format en utilisant chiffrement à contrainte de modèle.

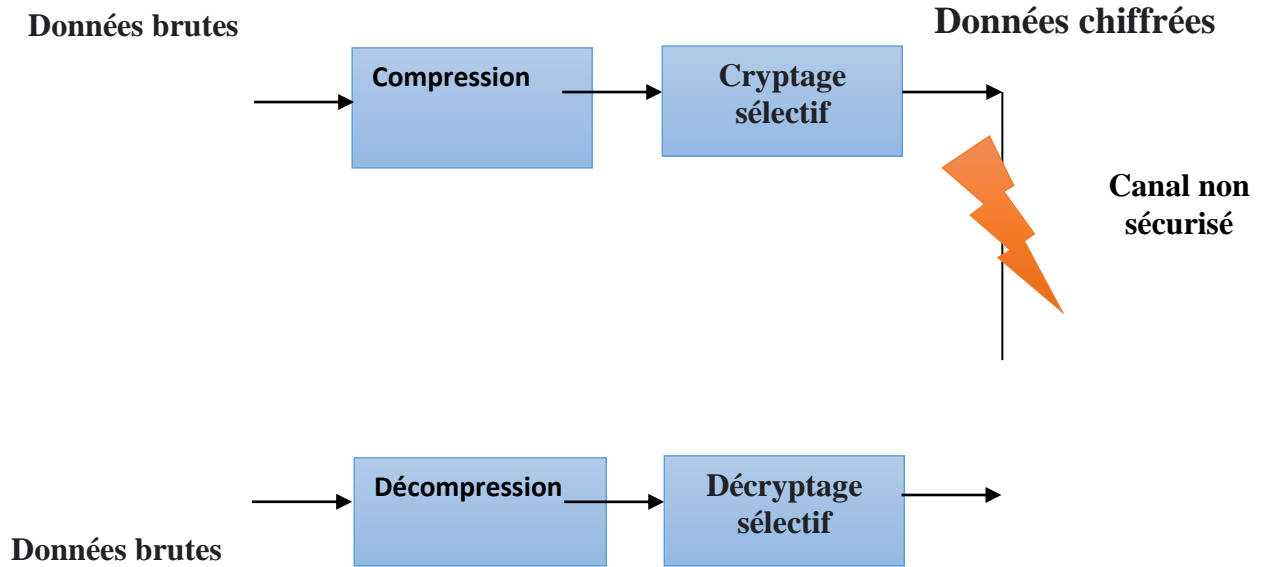


Figure 3. 3 : Approche post-compression.

- **Compression et chiffrement conjoints :**

les algorithmes de chiffrement sélectif de cette classe effectuent une compression et un chiffrement conjoints (resp, une décompression et un déchiffrement conjoints) (voir Figure 3 .5). Les algorithmes de cette classe impliquent des modifications à la fois du codeur et du décodeur qui peuvent avoir un impact négatif sur la conformité du format et la convivialité de la compression.

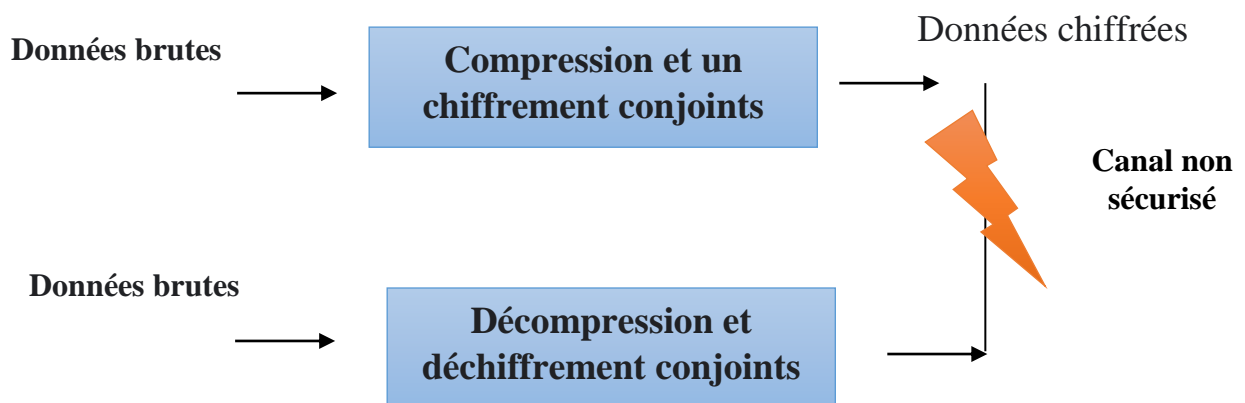


Figure 3.4: Compression Et Chiffrement Conjoints.

3.1.2 Modèle Proposé De Chiffrement Et Déchiffrement En Continu

Mettre les concepts du chaos à la disposition du chiffrement en continu cela signifie construire un générateur chaotique afin de produire un flux chaotique de codons.

Les algorithmes de chiffrement en continu convertissant la donnée à chiffrer un bit à la fois, la réalisation la plus simple d'un algorithme de chiffrement en continue est illustrée par la figure ci- dessous :

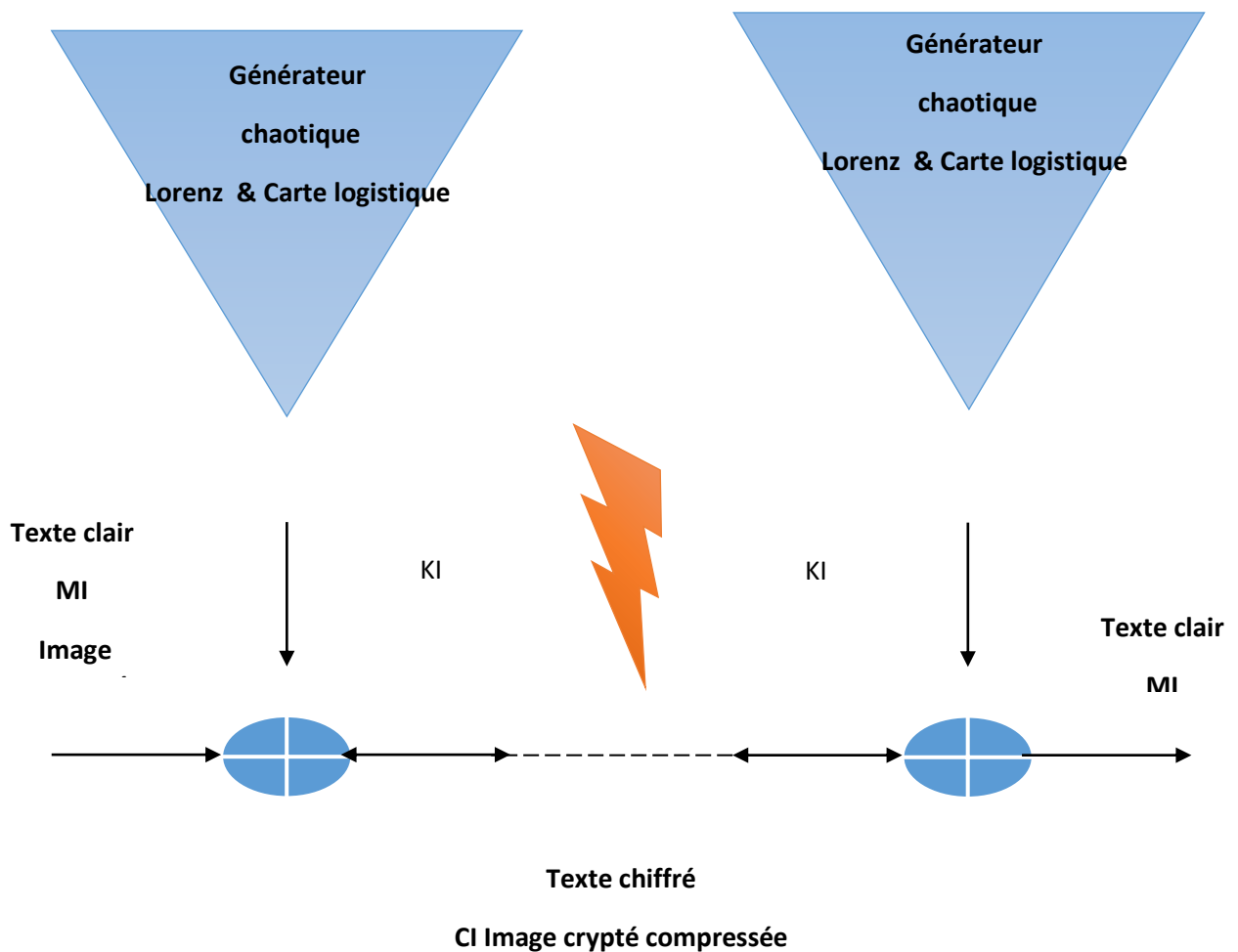


Figure 3.5: Chiffrement Continu pour le System Sécurisé.

(compression-chiffrement des images)

Ce type de générateur engendre un flux de bits appelé (codons) $K_1, K_2, K_3, \dots, K_i$. Ce flux est combiné par "Ou Exclusif" avec le flux de bit du texte en clair $M_1, M_2,$

M_3, \dots, M_i pour produire le flux de bits chiffré qui va être transmis à travers un canal non sécurisé.

$$C_i = M_i \oplus K_i \quad (3.1)$$

Le flux est dit aléatoire car cette suite est arbitraire. Cependant, lorsque la suite arrive à son terme, le générateur ne s'arrête pas de fonctionner. La séquence déjà transmise est à nouveau reproduite (générateur périodique). D'où le qualificatif de pseudo - aléatoire.

Du côté du déchiffrement, les bits chiffrés (C_i) sont combinés par ou exclusif avec un flux identique de codons pour retrouver les bits du texte en clair.

$$M_i = C_i \oplus K_i \quad (3.2)$$

$$\text{Remplacent (3.1) dans (3.2) } \Rightarrow M_i = M_i \oplus K_i \oplus K_i$$

Le premier terme K_0 est appelé le germe (seed en anglais).

La sécurité du système dépend entièrement des détails internes du générateur de codons. Si on ne change pas le germe, on obtiendra toujours la même séquence. Cela se révèle utile, pour la récupération des données émises donc le germe peut déterminer aussi la clef de la séquence.

3.1.3 Générateur Chaotique Proposé :

Le graphe à deux dimensions qui représente chaque équation séparément semble présenter des irrégularités L'idée est d'utiliser ces irrégularités d'une équation différentielle (par exemple dx/dt) pour la génération de codons.

Les différentes phases de la génération de codons sont les suivantes :

1. **Amplification** : On doit tout d'abord amplifier en amplitude la courbe représentative à un seuil à déterminer.
2. **l'échantillonnage** : L'échantillonnage consiste à ne transmettre que des valeurs instantanées de la courbe prises à intervalles réguliers T_e .
3. **Quantification** : La mesure (de l'amplitude) de chaque échantillon est un nombre que l'on met sous forme binaire. La mesure des échantillons est faite avec une certaine précision. La longueur du numéro binaire associé à un

échantillon sera directement liée à cette précision. Plus la mesure sera précise, et plus le nombre d'éléments binaire sera important. La quantification consiste donc à associer une même mesure à toutes les amplitudes d'échantillons compris dans une même plage.

4. **Codage** : Une fois que la courbe qui représente l'équation de l'attracteur est quantifiée, on transmet les numéros des différentes plages occupées par la courbe aux instants d'échantillonnage. Ces numéros sont codés par des mots binaires.

La construction du générateur chaotique est le fruit soit d'une seule équation soit la combinaison des différentes équations afin de produire un flux chaotique de codons.

L'émetteur d'une information doit être certain de l'identité du destinataire et inversement, en précisant certaines valeurs importantes comme la clef,

Cette clé est une fonction de :

- Le seuil d'amplification.
- Période T_e d'échantillonnage.
- Détermination du germe.
- Quantification : La longueur du numéro binaire d'un échantillon.
- Plage de codage.

3.1.4 Résultats de compression et interprétations :

Exemples : Les Images reconstruites :



Figure 3.6 image satellite des tests (png) [65]



Figure 3.7 image de test madina (jpg) [64]

3.1.5 Compression d'image par ondelette :

L'évaluation des résultats obtenus par la méthode de SPIHT sur plusieurs images de différents types a été effectuée selon deux procédés :

- En fonction du PSNR par rapport au débit
- En fonction de la qualité de l'image obtenue.

Chacune des images tests est compressée avec plusieurs débits différents allant de 0.25 jusqu'à 2 bpp en mesurant le PSNR obtenu.

Pour la décomposition en ondelettes nous avons opté sur six (06) niveaux de décomposition avec les filtres d'ondelettes bi-orthogonaux9/7 avec extension symétrique. Les valeurs du PSNR obtenus pour les images : LENA et madina .

L'algorithme de compression d'image par ondelette se compose de différentes étapes.

La Figure 3.10 suivant représente le processus de compression image par ondelette se compose de différentes étapes

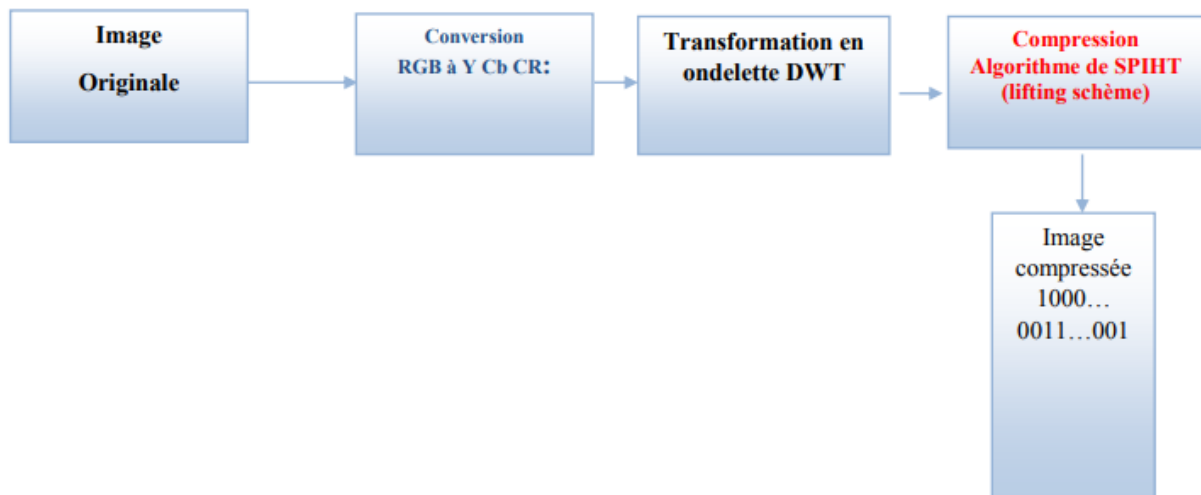


Figure 3.8 : processus de compression image par ondelette se compose de différentes étapes

Les processus de compression image par ondelette se compose de différentes étapes sont :

- **Etape 1 :**

Image originale. Les images utilisées dans cette application, sont des images panchromatiques codées sur 8 bits ($M=N=256$). L'image couleur représente sous forma trois couleurs RGB (R : Red G : green B : Blue) Exemples : Pour notre application, nous avons utilisé les images suivantes :

- Image b codée sur 8 bits, niveaux gris de taille 512x512 pixels.
- Image b codée sur 24 bits en couleur de taille 256 x256 pixels.



(a) Image b en couleur



(b) Image b en gris

Figure 3.9: Conversion d'image RGB a image en niveaux de gris : (a) Image a en couleur (b) Image b en gris

- **Etape 2 :** Conversion RGB à Y Cb Cr : L'œil humain étant plus sensible à la luminance (intensité lumineuse, clarté) qu'à la chrominance (la couleur), pour compresser une image, le format JPEG va « jouer » sur les valeurs de la couleur même et on non pas sur la clarté de l'image, de cette façon la différence de qualité de l'image ne sera que très peu visible (cela dépende du taux de compression) Le système de codage RGB n'est donc pas approprié pour réussir à « jouer » sur la valeur de la chrominance puisque les valeurs de la clarté de l'image sont imbriquées avec ceux de la couleur.

Tandis qu'avec le système de codage YCbCr, la clarté et séparé » de la chrominance. C'est pourquoi l'algorithme va convertir les valeurs RGB en YCbCr, l'algorithme de conversion et suivant : $Y = (0.299 * R) + (0.587 * G) + (0.114 * B)$

$$Cb = (-0.1687 * R) - (0.3313 * G) + (0.5 * B) + 128$$

$$Cr = (0.5 * R) - (0.41874 * G) - (0.0813 * B) + 128$$

Suite à cette étape, il n'y a pas de pertes d'information

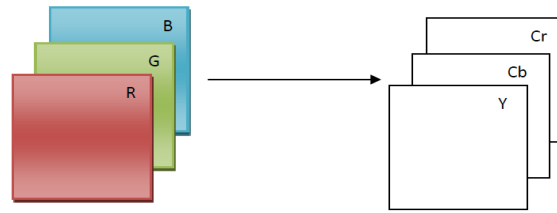


Figure 3.10 : Conversion RGB à YCbCr

- Etape 3** : Transformation en ondelette : - On applique une transformation en ondelette sur L'image originale convertie (RGB à YCbCr). - Rappelons que la transformée en ondelette permet de regrouper les variations de l'image dans un nombre faible de coefficients. c.à.d. Extraction de l'énergie de l'image (les informations nécessaires) et de les stockés dans un petit nombre de coefficients. - La transformation en ondelette est une sorte de filtrage appliqué sur l'image, car les ondelettes sont vues comme des filtres. - La transformée en ondelette DWT comprend plusieurs paramètres, parmi ceux qui nous intéresse, - Le niveau de décomposition et l'ondelette utilisée pour chaque sous échantillonnage de l'image YCbCr.

Cette étape va engendrer une perte de qualité puisqu'elle consiste à pour les information de chrominance) sous échantillonner l'image concrètement le JPEG va garder la moyenne de quatre pixels dans ce cas-là le sous échantillonnage est appelé (2h :2v horizontalement et verticalement) la luminance ne subit pas de sous échantillonnage Sur une photo ou une image quelconque, ne garder en mémoire que la moyenne de chrominance de quatre pixels au lieu des informations entier des quatre pixels, n'est pas dérangeant puisque l'œil ne distingue pas les petites voire moyenne différences de couleur au sein d'un carrée de deux sur deux pixels .

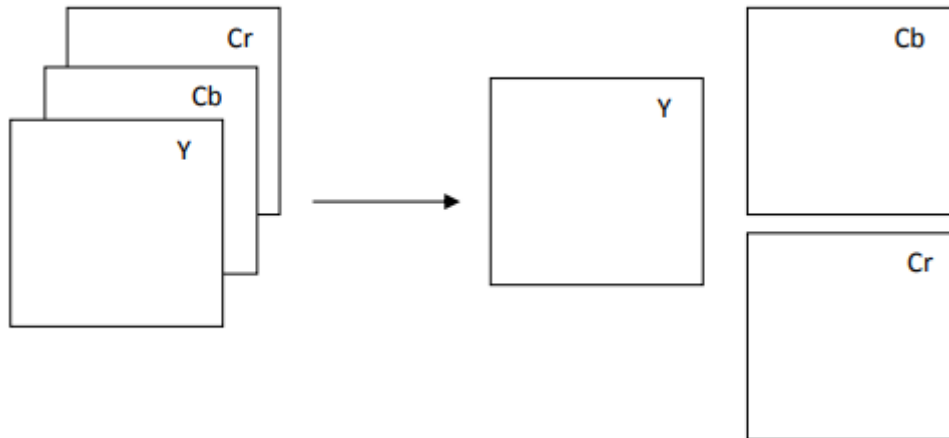


Figure 3.11: Décomposition d'image originale (YCbCr).

Ensuite que les trois sous échantillonnage de l'image YCbCr sont décomposées par la transforme en ondelette CDF9/7 et les coefficients obtenus sont encodés par l'encodeur SPIHT (chaque couche séparément) pour générer une séquence binaire considérée comme des données à stocker ou à transmettre.

3.2 Compression image par la méthode ondelette (codeur SPIHT) :

Pour évaluer ses performances, notre schéma de compression a été appliqué, aux images Satellite et Madina. Méthode de compression repose sur le codeur SPIHT appliqués dans le domaine des ondelettes entières utilisant l'ondelette bi orthogonale CDF9/7 variant le niveau de décomposition (level).

3.2.1 Interprétation des résultats :

Nous généralisons notre algorithme avec la CDF9/7 sur différentes images en couleur. Nous constatons de bonne qualité d'image compressée avec l'ondelette CDF9/7.

Première image satellite des tests type png

			
PSNR =29.90	PSNR =30.13	PSNR =33.29	PSNR =52.09
MSE=66.55	MSE=63.16	MSE=30.47	MSE=0.41
MSSIM=0.47254	MSSIM=0.60869	MSSIM=0.8158	MSSIM=0.99826
Tc=96.88	Tc=93.75	Tc=87.50	Tc=75.00

Deuxième image des tests image madina type jpeg





			
PSNR =30.53	PSNR =31.54	PSNR =35.29	PSNR =41.48
MSE=57.50	MSE=45.65	MSE=19.23	MSE=4.64
MSSIM=0.76341	MSSIM=93.75	MSSIM=0.94471	MSSIM=75.00
Tc=96.88	Tc=0.86829	Tc=87.50	Tc=0.98421

Figure 3.12 : Variation des paramètres d'évaluation (PSNR, MSE et taux de compression) pour niveaux de décomposition et 6.(level 6) Lors de l'utilisation de l'ondelette de codeur SPIHT .

A partir de ces résultats, on peut constater que le PSNR augmente avec le niveau de décomposition pour les différentes ondelettes utilisées sur l'image test. Donc, on peut dire que les performances du codeur SPIHT sont maximales pour de grandes résolutions.

Les résultats de compression des images utilisées dans ces tests prouvent bien les bonnes performances de cet algorithme. Evidemment, on remarque d'importantes disparités du PSNR pour les mêmes débits entre les différentes images.

Le PSNR croît lentement avec le taux en bpp selon une loi qui est approximativement logarithmique. Constatant bien que pour des débits très faibles, les PSNR sont de valeurs très faibles, Ceci est dû essentiellement aux caractéristiques de chacune de ces images. Notons que si nous avons considéré des débits (en bpp) égal ou supérieur à la majorité des PSNR calculés, aussi bien pour les images en niveaux de gris que pour les images en couleur, seront nettement supérieurs à 30dB.

Des images dont les PSNR sont compris entre 30 dB et 50 dB sont jugées généralement comme des images de bonnes qualités. Ces résultats ont montré que l'utilisation d'un niveau de décomposition égal à 6 est suffisante pour la compression d'images en couleur, et donne de meilleurs résultats en termes de PSNR, MSE et MMSIM.

Les résultats de simulation ont indiqué également que l'ondelette est mieux appropriée à la transformation d'images satellitaires.

3.2.2 Approche proposée du chiffrement base des attracteurs chaotiques :

Notre approche de cryptage d'image proposée composée de trois étapes principales, comme le montre la figure 3.13 .

- Première est le mélange de pixels, la seconde est l'opération XOR, et enfin la carte chaotique 3D de Lorenz est effectuée. Ensuite de Carte Chaotique Lorenz combiner avec carte logistique. Mappez, puis effectuez l'opération XOR. L'étape finale est le mélange de pixels, en utilisant une clé aléatoire créée dans le processus de cryptage.
- L'algorithme de décryptage d'image est un processus inverse du processus de cryptage l'Image compressé.
- Dans les sous-sections suivantes, nous aborderons chaque étape en détail.

3.2.3 Organigramme de chiffrement image par algorithme carte chaotique et compresser

Le organigramme suivent représente de l'organigramme du chiffrement avec carte chaotique Lorenz combiner avec carte logistique Lorenz :

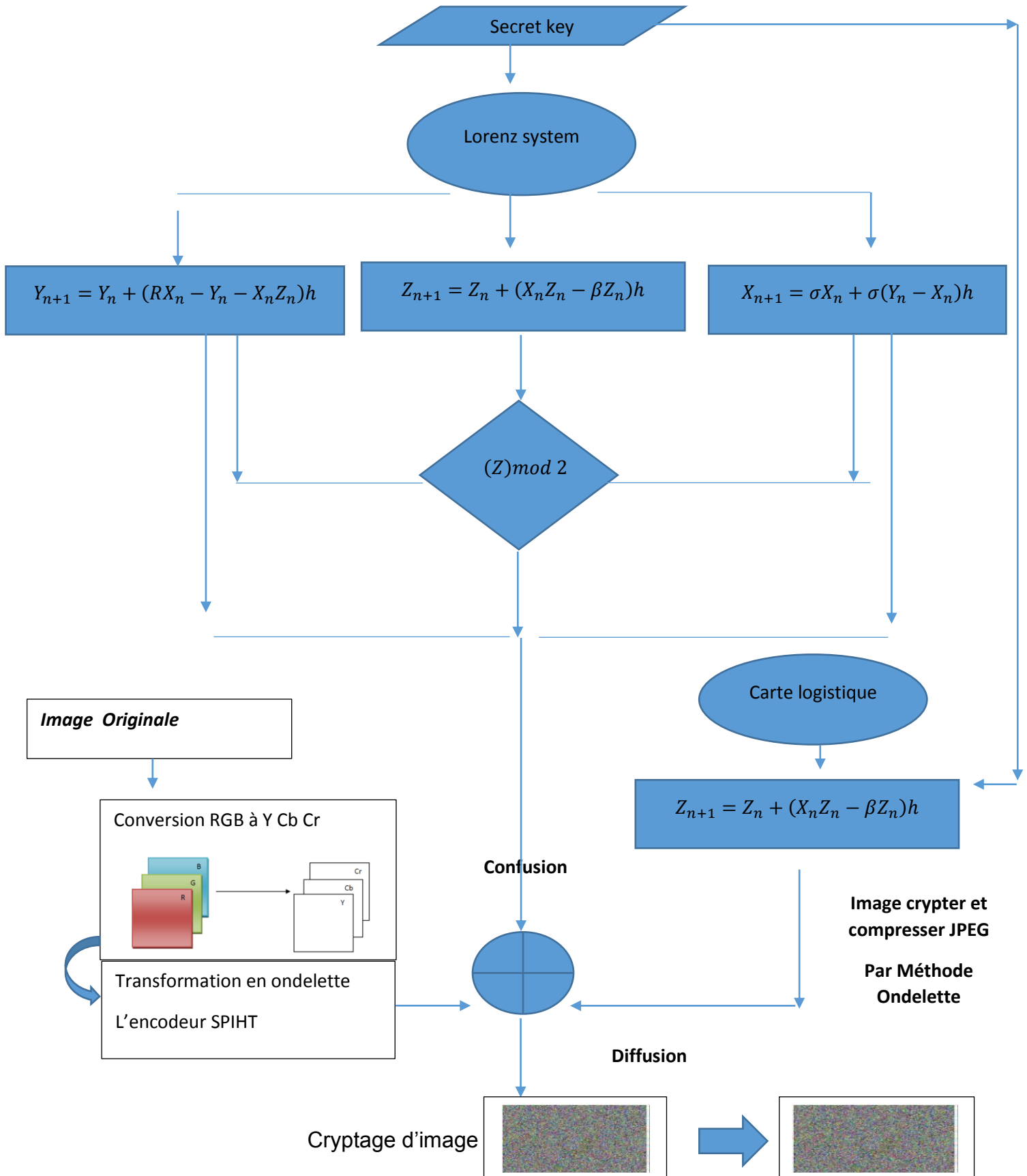


Figure 3.13: Block diagram of the encryption algorithm

3.3.1 Résultats des Simulations



3.3.2 Chiffrement en continu a bases des attracteurs chaotiques :

Dans cette partie on va réaliser un chiffrement en continu basé sur les attracteurs chaotique étudié précédemment pour crypter le texte et les images et voir lequel de ces attracteurs présente le meilleur résultat. Pour notre programme de chiffrement on va utiliser des nombres entiers et positifs codés sur 8 bits pour les codons ainsi que pour le message.

3.3.3 Crypto-système base sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique :

La figure suivant représente la Chiffrement d'image avec l'attracteur de Lorenz

Chiffrement image compresse :

	
<p>Image madina compreser</p>	<p>Image madina crypter</p> <p>(X0= 0.2, Y0= 2.5, Z0= 3)</p> <p>$h=0.0001, R=28, \sigma=10, \text{ et } \beta=8/3$</p>

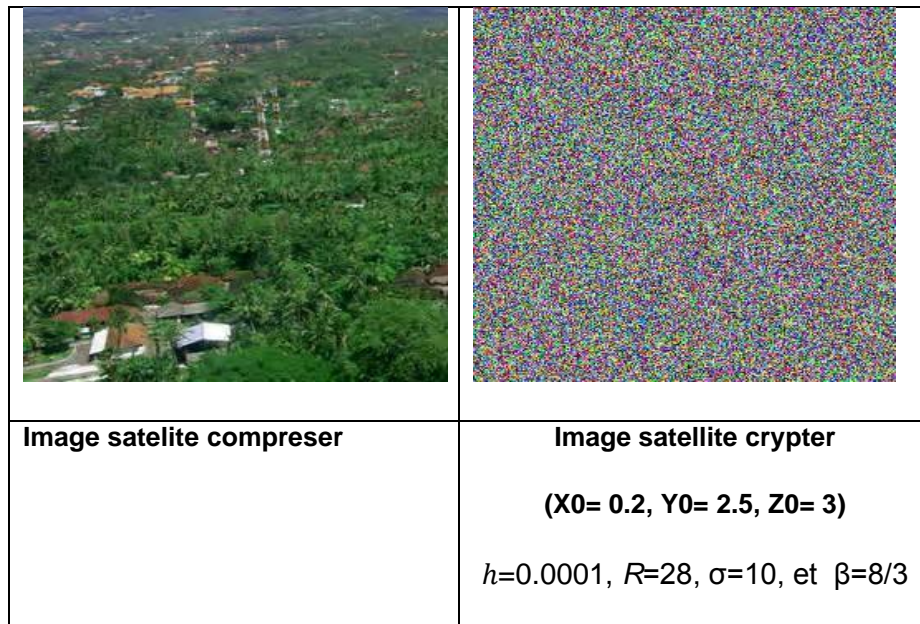


Figure 3.14: Chiffrement d'image avec l'attracteur de Lorenz

Se référant aux résultats obtenus, nous pouvons clairement voir que l'image simple diffère sensiblement de celui correspondant cryptée. Par ailleurs, l'histogramme de l'image cryptée est assez uniforme ce qui rend difficile d'extraire les pixels nature statistique de l'image simple.

Les histogrammes des images claire et chiffrée de Lena montrant ainsi que le crypto système proposé fonctionne de façon correcte.

On constate que :

- Le chiffage change la fréquence des pixels avec une distribution équiprobable pour toute l'image.
- Les pixels sont très corrélés dans l'image en claire et que le chiffage annule toute corrélation entre eux dans l'image chiffrée.
- L'image après chiffage est devenue parasité et ne contenant aucune information visible qui se voit sur l'histogramme des deux images ne contient aucune information sur l'image en claire.

3.3.4 Analyse des résultats:

Résultat de simulation Crypto-système basé sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique :

a) Analyse d'histogramme Des Différents images(compreser,crypter)

L'histogramme de couleur est une caractéristique très importante dans l'analyse d'images. L'analyse de l'histogramme clarifie la manière dont les valeurs de pixel de l'image sont distribuées. Un certain nombre d'images sont cryptées par les schémas de cryptage à l'étude et un test visuel est effectué. Les histogrammes de l'images et de l'image chiffrée sont illustrés aux figures 3.16 et 3.17. Comme le montre cette figure, il est évident que les histogrammes de couleur de l'image cryptée sont presque uniformes et significativement différents des histogrammes de couleur de l'image simple. Par conséquent, il ne fournit aucun indice à utiliser dans une attaque d'analyse statistique sur l'image cryptée.

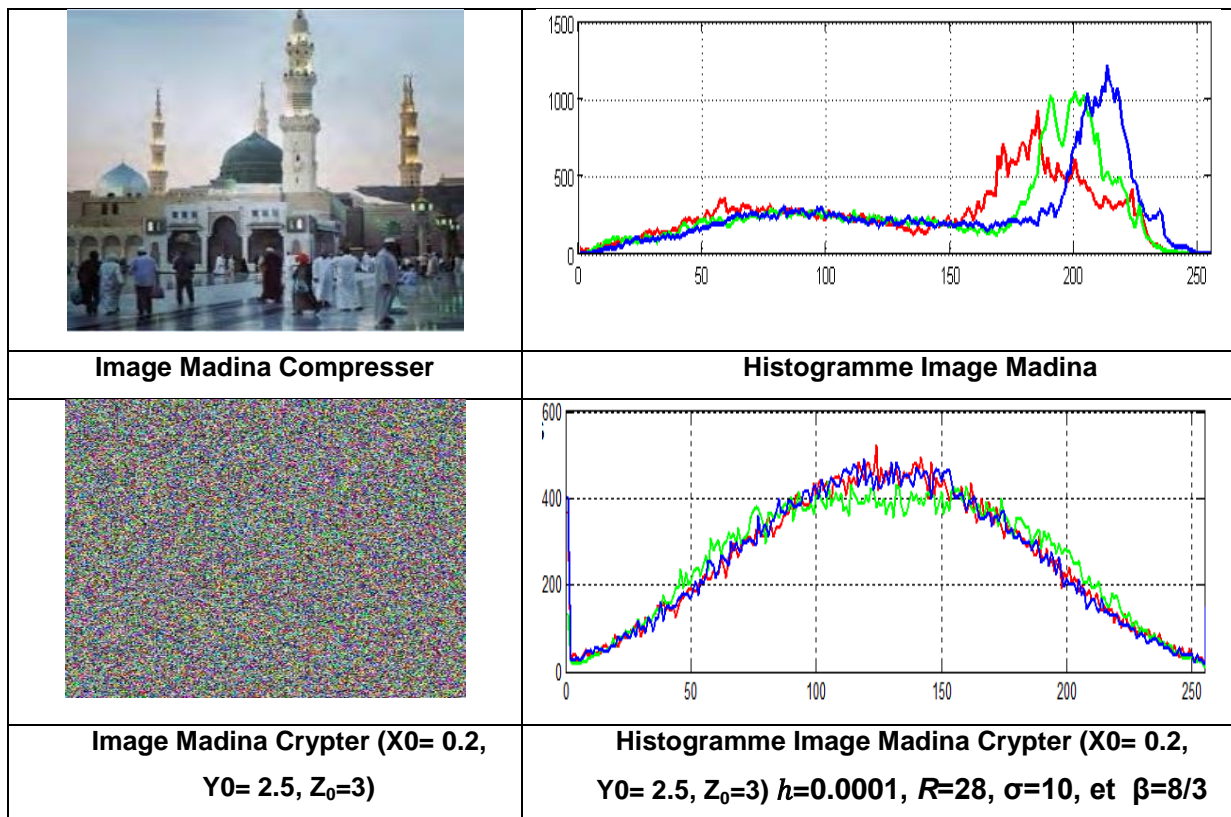


Figure 3.15: Analyse d'histogramme Des Différents images(compreser,crypter)

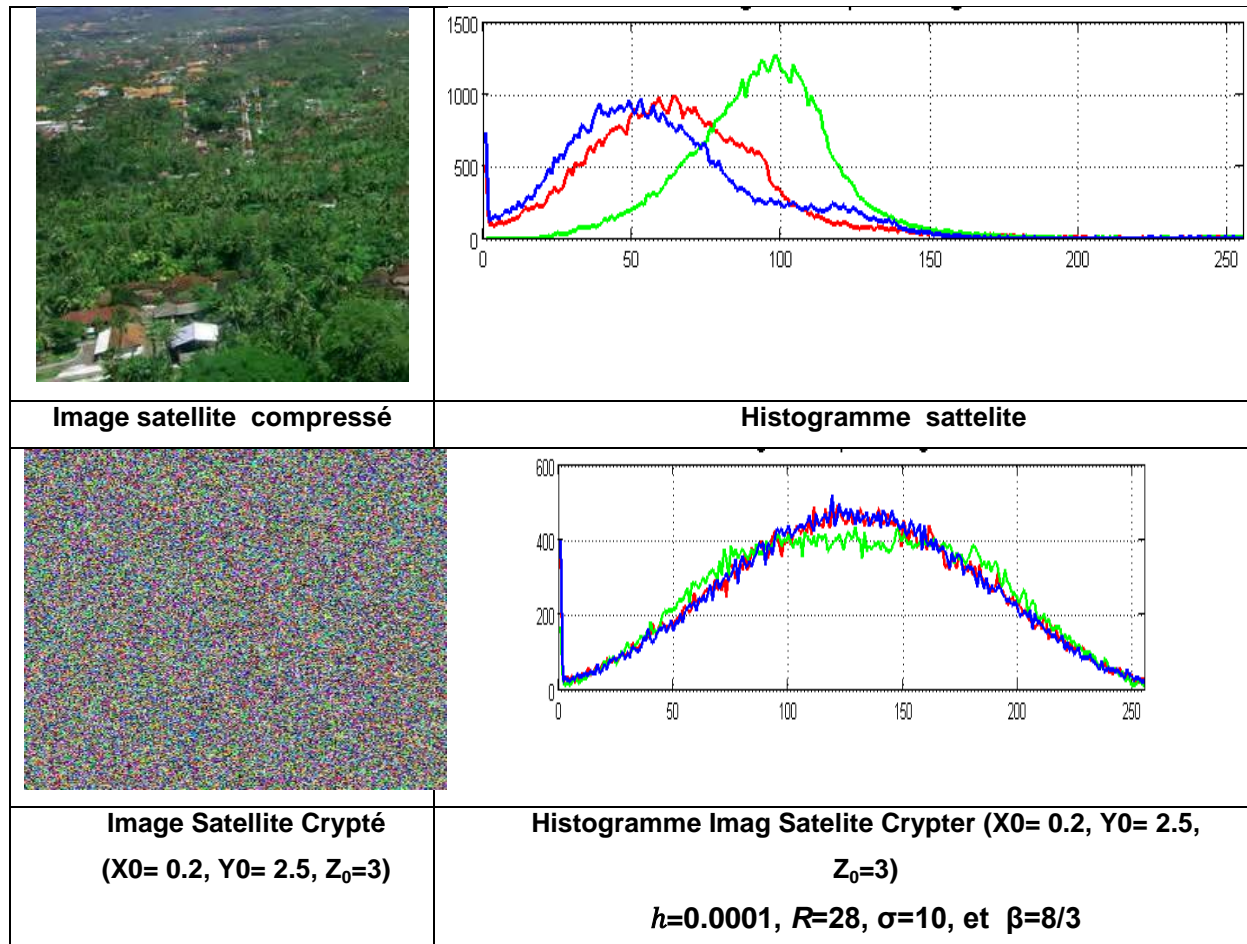


Figure 3.16: Analyse d'histogramme Des Différents images(compreser,crypter)

b) Analyse de la corrélation entre les pixels adjacents Des Différents images (compreser ,crypter)

- Premier Résultats des simulations distribution des pixels adjacent représente dans les figure 3.17,3.18 avec image de tests exemple médina

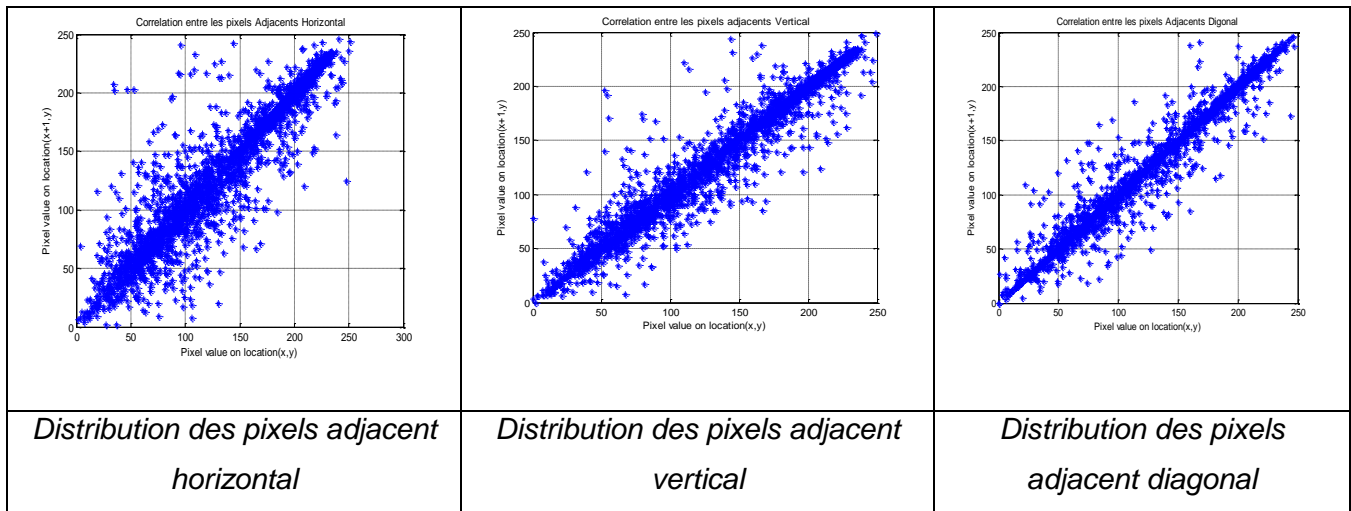


Figure 3.17 : Distribution des pixels adjacent Madina.jpg en claire
($X_0= 0.2, Y_0= 2.5, Z_0= 3$)

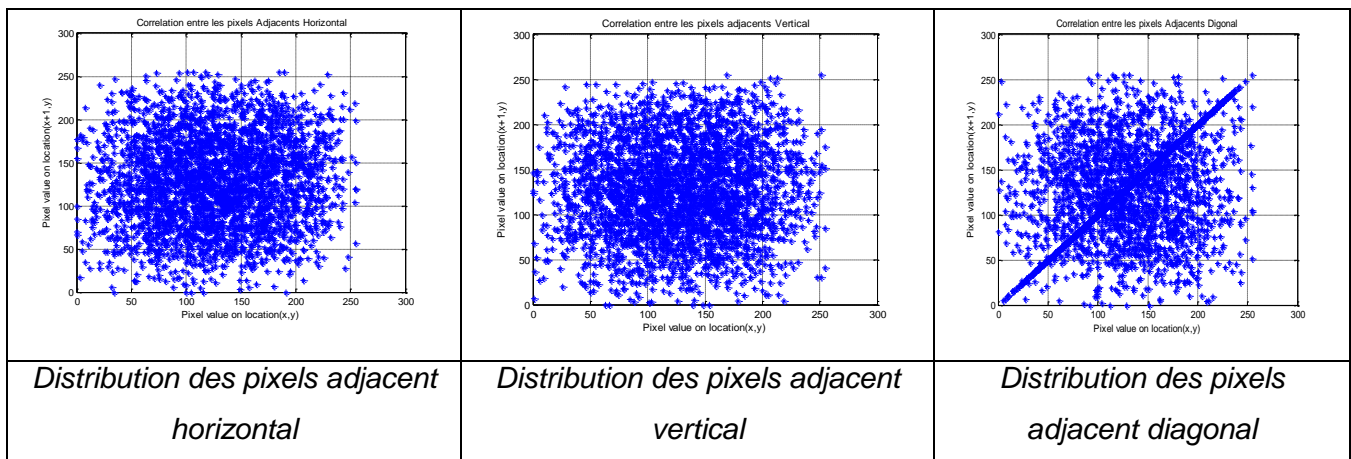


Figure 3.18: Distribution des pixels adjacent Madina.jpg chiffrée
($X_0= 0.2, Y_0= 2.5, Z_0= 3$)

- Deuxième Résultats des simulations distribution des pixels adjacent représenté dans les figure 3.19,3.20 ,avec image de tests exemple teste satellite.

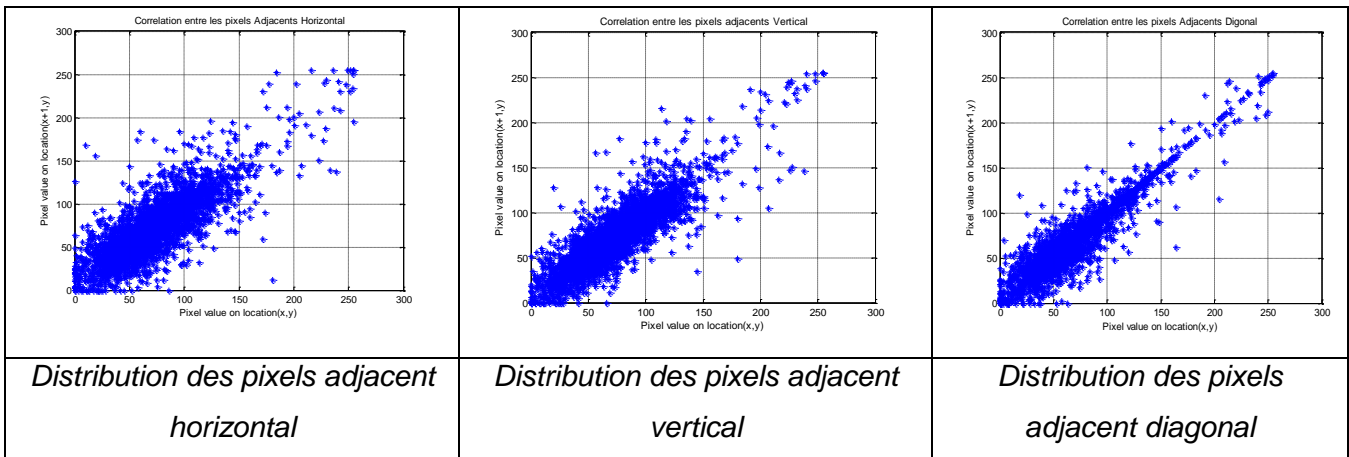


Figure 3.19 : Distribution des pixels adjacent satellite.jpg en claire

($X_0= 0.2, Y_0= 2.5, Z_0=3$)

$h=0.0001, R=28, \sigma=10, \text{ et } \beta=8/3$

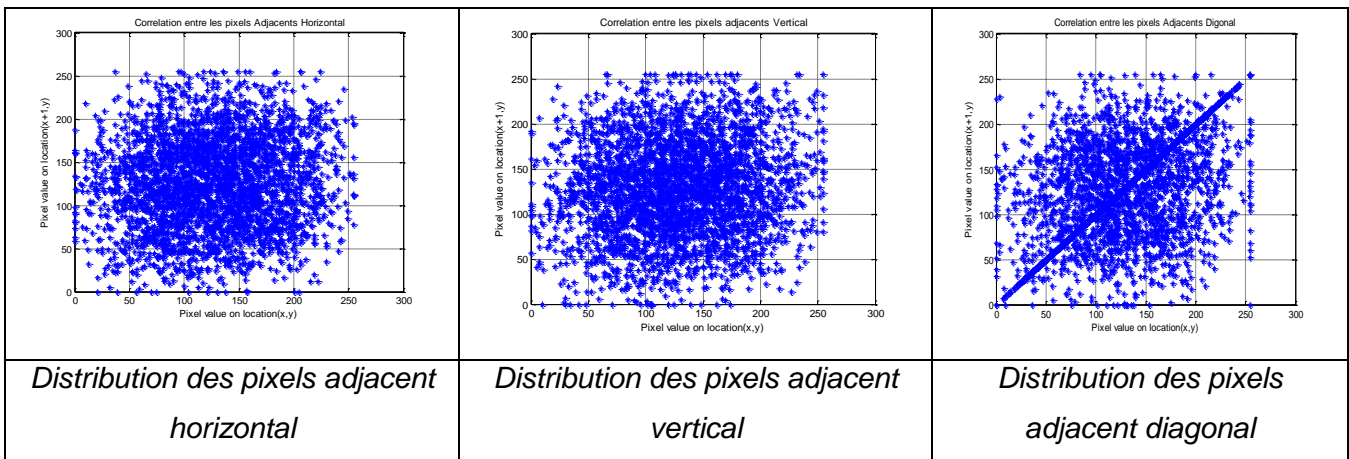


Figure 3.20 : Distribution des pixels adjacent satellite.jpg chiffrée

($X_0= 0.2, Y_0= 2.5, Z_0=3$)

$h=0.0001, R=28, \sigma=10, \text{ et } \beta=8/3$

Tableau.3.1 Comparaison des coefficients de corrélation entre les images en claire et chiffrée image test satellite test

Direction of adjacent Pixels	Image compresses	Type pseudo random generator	Image Encrypted
Vertical (3000)adjexant	0.8604	Lorenz & carte logistique	0.0797
Diagonal (3000)adjexant	0.9394	Lorenz & carte logistique	0.3646
Horizontal (3000)adjexant	0.8020	Lorenz & carte logistique	0.0828

Tableau.3.2 Comparaison des coefficients de corrélation entre les images en claire et chiffrée image madina

Direction of adjacent Pixels	Image compresses	Type pseudo random generator	Image Encrypted
Vertical (3000)adjexant	0.7841	Lorenz & carte logistique	0.0196
Diagonal (3000)adjexant	0.8536	Lorenz & carte logistique	0.0156
Horizontal (3000)adjexant	0.7342	Lorenz & carte logistique	0.0033

Tableau.3.1 et 3.2 Comparaison des coefficients de corrélation entre les images en claire et chiffrées.

On constate que :

- Les pixels adjacents sont très corrélés on que le cryptage créé un désordre très important.
- Les coefficients d'autocorrélation son proche de 1 pour les images en claire et le chiffage l'annule qui prouve le bon fonctionnement de notre système.

- Le tableau 3.1, montre les coefficients de corrélation de l'algorithme proposé sont très faibles ou pratiquement nuls. Ainsi, l'algorithme proposé a résisté aux attaques statistiques.
- Le tableau 3.1 plus performance par rapport le tableau 3.2 donc utilisation image satellite dans la Crypto-système base sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique
- Un bon système de cryptage doit avoir une valeur de corrélation sont très faibles ou pratiquement nuls ce qui est assuré par notre système(3.1

3.3.5 Simulation Crypto-compression Images système

Résultat de simulation Crypto-compression Images système base sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique :

- **Simulation Crypto-compression Images système**

Compression d'une image satellite crypté avec algorithme SPIHT codée avec CDF9/7 pour un taux de 2 bit/pixel . Les résultats de simulation ont indiqué également que l'ondelette est mieux appropriée à la transformation d'images satellitaires.


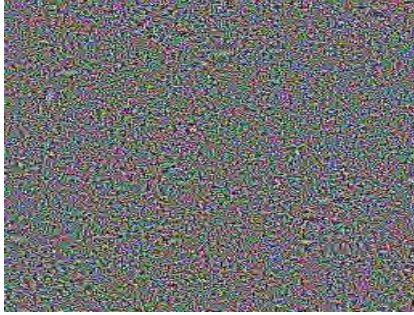
	
PSNR = 26.58 MSE= 141.17 MSSIM=0.83504 Tc=75.00 Taux en bpp 2.000 bpp	PSNR = 26.63 MSE= 143.06 MSSIM= 0.83589 Tc= 75.00 Taux en bpp 2.000 bpp
(a)Image Crypter Medina Compresser	(b)Image Crypter Satellite Compresser

Figure 3.21: Analyse d'histogramme Des Différents images (crypté, compressé)

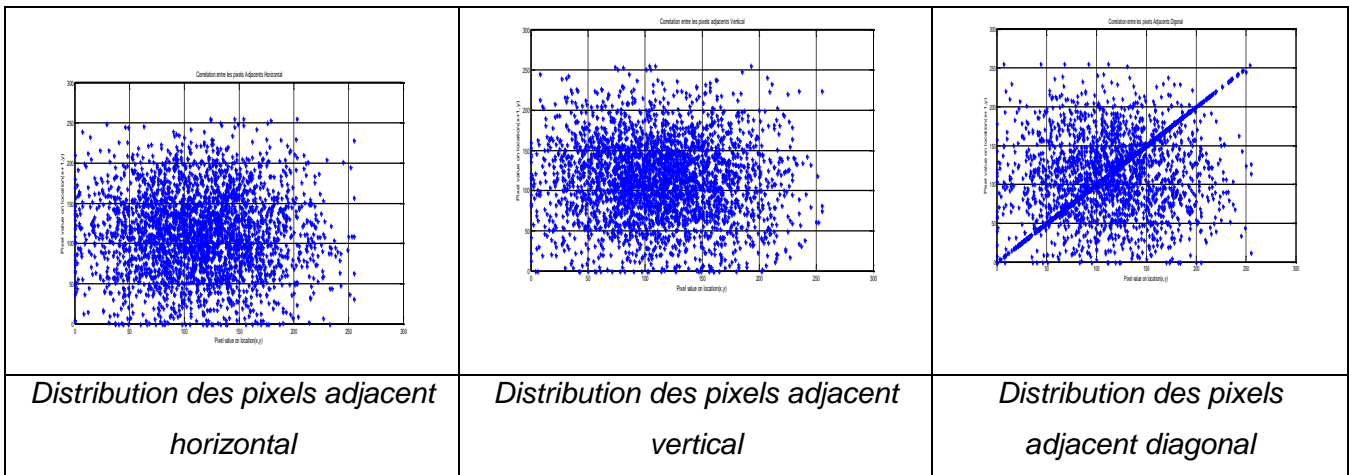


Figure 3.22: Distribution des pixels adjacent image chiffrée et compressé (image madina)

($X_0= 0.2, Y_0= 2.5, Z_0= 3$) level 6 taux compression =2bpp

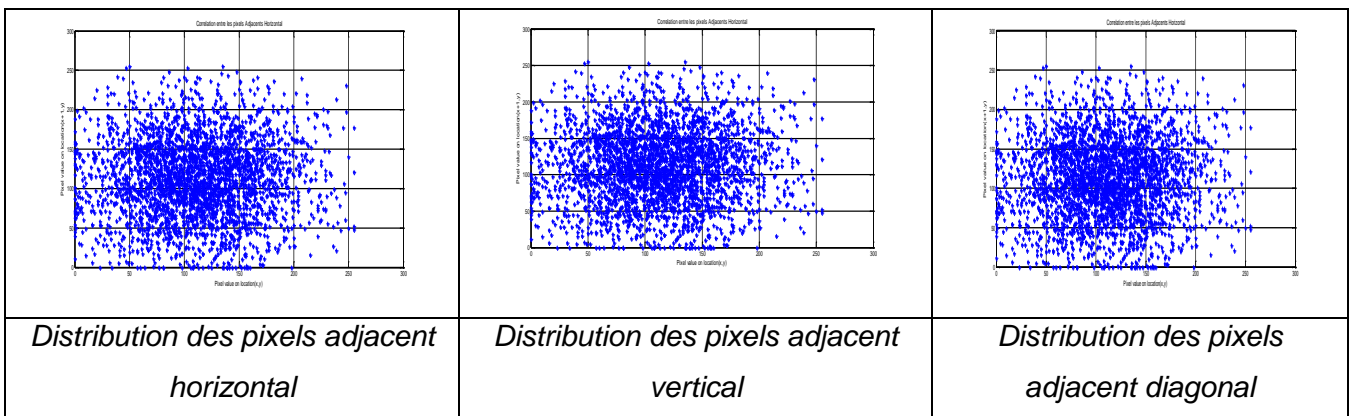


Figure 3.23: Distribution des pixels adjacent image chiffrée et compressé (image satellite)

($X_0= 0.2, Y_0= 2.5, Z_0=3$)

$h=0.0001, R=28, \sigma=10,$ et $\beta=8/3$, level 6 taux compression =2bpp

Tableau.3.3 Comparaison des coefficients de corrélation entre les images en claire et chiffrée et compresser image test satellite test

Direction of adjacent Pixels	Image compresses	Systeme chaotique	Image crypter	Image crypter compresser
Vertical (3000)adjexant	0.8604	Lorenz & carte logistique	0.0797	4.7692e-004
Diagonal (3000) adjexant	0.9394	Lorenz & carte logistique	0.3646	0.3235
Horizontal (3000)adjexant	0.8020	Lorenz & carte logistique	0.0828	0.0290

Tableau.3.4 Comparaison des coefficients de corrélation entre les images en claire et chiffrée et compresser image madina

Direction of adjacent Pixels	Image compresses	Systeme chaotique	Image crypter	Image crypter compresser
Vertical (3000)adjexant	0.7841	Lorenz & carte logistique	0.0196	0.0428
Diagonal (3000) adjexant	0.8536	Lorenz & carte logistique	0.0156	0.3039
Horizontal (3000)adjexant	0.7342	Lorenz & carte logistique	0.0033	0.0090

Tableau.3.3 et 3.4 Comparaison des coefficients de corrélation entre les images en claire et chiffré et chiffre compressé

On constate que :

- Le tableau 3.3, montre les coefficients de corrélation de l'algorithme proposé sont très faibles ou pratiquement nuls. Ainsi, l'algorithme proposé a résisté aux attaques statistiques.
- Le tableau 3.3 plus performance par rapport le tableau 3.4 donc utilisation image satellite dans la Crypto-compression système base sur la confusion et la diffusion basé à Attracteur Lorenz & carte logistique

- Un bon système de cryptage compresser doit avoir une valeur de corrélation sont très faibles ou pratiquement nuls, ce qui est assuré par notre système (3.3).
- Les résultats de simulation ont indiqué également que :
- Les coefficients de corrélation de l'algorithme proposé sont très faibles ou pratiquement nuls. Ainsi, l'algorithme proposé a résisté aux attaques statistiques.
- L'ondelette est mieux appropriée à la transformation d'images satellitaires.

On voit clairement dans le tableau précédent que les résultats des analyses de performances et de sécurité des deux fonctions chaotiques sont encourageants pour les tests d'analyses histogramme et l'analyse de corrélation. Cependant, le système de cryptage basé sur l'attracteurs du Lorenz a une valeur d'espace de clé supérieure à celle du même système basé sur la fonction logistique, ce qui prouve qu'il est mieux résistant aux attaques de force brute. Ensuite la compression basée sur l'algorithme de SPIHT prouve son efficacité. Cependant, cette efficacité est tributaire des caractéristiques des images utilisées. De même, cette efficacité dépend énormément du type d'ondelette utilisée et du nombre de décomposition effectué. Les travaux ont montré qu'un nombre de décomposition égal à six est largement suffisant pour la majorité des cas et que nous ne pouvons pas espérer améliorer davantage en choisissant un nombre plus élevé

3.4 Conclusion

Dans ce chapitre, nous allons proposer l'amélioration des systèmes de la cryptographie pour augmenter les performances de sécurité et de confidentialité des données. Le système proposé est cryptage-compression basée sur la technique de permutation des pixels pour assurer les propriétés de confusion et diffusion. Ainsi l'algorithme proposé basée sur la Attracteur Lorenz & carte logistique. Et son implémentation.

Les résultats des simulations sous MATLAB montrent clairement que l'analyse d'histogramme des images cryptées est uniformément distribuée, donc l'algorithme est sécurisé devant les attaques d'analyse. Et ainsi l'espace clé est suffisamment grand, ce qui rend une attaque force brute infaisable. Par conséquent l'histogramme d'image chiffrée est très uniforme après le cryptage, voire, l'attaquant il ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée. Également l'algorithme proposé a été atteintes beaucoup amélioré sur la corrélation entre les pixels adjacents. Après, nous terminons par un ensemble des tests ont été utilisées pour montrer un changement entre l'image crypté et l'image compresser. Il y a un cryptage efficace pour chiffrer les images. De ce fait l'algorithme proposé montre l'efficacité et la sécurité de notre système proposé. Peut aussi être facilement résisté les attaques en texte clair connues/choisies. Finalement les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées, montrent que l'algorithme proposé offre des performances très favorables.

Finalement, nous avons prouvé la haute performance et la haute sécurité de notre proposition.

Conclusion Générale

Conclusion Générale :

L'utilisation du chaos dans le domaine de télécommunications est étudiée depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires ; il correspond à un comportement borné, de ces systèmes, ce qui le fait apparaître comme du bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée et compressions des images satellite.

Les télécommunications spatiales ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Et ainsi, le besoin d'être en mesure d'envoyer d'images numériques de façon compressée et cryptée est aussi ancien que les communications elles-mêmes. La compression consiste à réduire le nombre moyen de bits par pixel nécessaire à la représentation de celles-ci tout en sauvegardant au mieux leurs qualités visuelles lors de leur décompression. Ce mémoire présente la méthode de compression d'image dans des bases d'ondelettes basé sur le codeur de la technique SPIHT. L'objectif est de réduire le volume d'image générée par les méthodes de compression avec un taux de compression considérable.

La sécurisation de l'information est aujourd'hui, essentiellement fondée sur des algorithmes de calcul dont la confidentialité dépend du nombre de bits nécessaires à la définition d'une clé cryptographique. Différentes méthodes cryptographiques existent dans la littérature. On a des méthodes symétriques et d'autres asymétriques, ces deux méthodes sont généralement utilisées conjointement. Bien que ces méthodes on fait leurs preuves, la puissance croissante des moyens de calcul menace leur confidentialité

L'originalité de cette mémoire repose sur la prise en compte des propriétés de signaux chaotiques issue soit d'équations différentielles soit de récurrences discrètes non linéaire. Le principe du cryptage par chaos consiste à ajouter au message à transmettre un signal chaotique. L'émetteur envoie à un récepteur ce signal chaotique où le message est noyé. Connaissant les caractéristiques du signal chaotique initial, le récepteur sait extraire le message du signal reçu.

Au cours de ce projet, nous avons consisté à concevoir et implémenter un système de cryptage basé sur système chaotique et la méthode de compression

d'ondelettes basé sur le codeur de la technique SPIHT des images numériques. Pour atteindre cet objectif, nous avons d'abord présenté des généralités sur les quatre domaines qui englobent notre travail : cryptographie compressions, chaos et images, Ensuite nous avons présenté un état de l'art sur la cryptographie chaotique en basant sur l'attracteur de Lorenz et carte logistique. Également l'algorithme proposé a été d'utiliser chaotique techniques est d'assurer la confusion et la diffusion opérations et l'objectif principal de cette méthode est d'atteindre un haut niveau de sécurité. Tout d'abord, une complète confusion basée sur les générateurs du système de Lorenz qui a été utilisée pour augmenter la complexité des données chiffrement est appliqué. Ensuite, des rotations carte logistique ont été utilisées pour améliorer la résistance à l'image unique attaques. Les résultats des simulations ont assuré que l'algorithme proposé est capable de résister différentiel, force brute, statistique et image attaques, il est donc hautement sécurisé et efficace. La vitesse de chiffrement et de déchiffrement est rapide par rapport aux autres chiffrements basés sur le chaos algorithmes et adéquats pour l'imagerie satellitaire. Aussi, il faut noter que les attaques utilise contre ce type d'algorithmes sont les mêmes que celles utilise pour le chiffrement continue sauf que dans notre cas, nous avons ajouté d'autres contraintes aux cryptanalyses.

Sur le plan empirique, nous avons prouvé le comportement chaotique d'une nouvelle fonction chaotique définit à partir d'une combinaison des deux fonctions : la fonction logistique en basant sur l'attracteur de Lorenz et la fonction du carte logistique, puis nous avons implémenté un système de cryptage d'image satellite basé sur cette nouvelle fonction proposée.

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

En perspectives de ce travail :

- Faire des comparaisons des résultats du système proposé avec d'autres travaux récents et en utilisant d'autres images de tests.
- Appliquer notre système chaotique sur d'autres types des données à savoir, la vidéo.
- Améliorer notre approche sur tous les formats des messages qui sont très long et les différentes images au minimum de temps, donc on va essayer de construire un système de cryptographie qui sera plus rapide et plus efficace.
- Améliorer notre approche sur tous les formats des images satellites en général et les images couleur entre eux en particulier.

Bibliographie

Bibliographie

- [1] BENIANI Rabab Sécurité des images Numériques compressées JPEG these doctorat 3ème cycle Mathématique et informatique Université Djilal Liebes– Sidi Bel Abbes –2019
- [2] M.NAIM a,* - A. ALI PACHA a – C. SERIEF, An encryption algorithm for satellite images based on chaotic sequences and a rotation system, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf & Satellite Development Center, Oran, Algeria, Communication Science & technology N°23 July 2020 COST <https://www.researchgate.net/publication/349088170>
- [3] Z. Hua, Y. Zhou, C.-M. Pun, et C. L. P. Chen, « 2D Sine Logistic modulation map for image encryption », *Information Sciences*, vol. 297, p. 80-94, mars 2015, doi: 10.1016/j.ins.2014.11.018.
- [4] Z. Hua et Y. Zhou, « Image encryption using 2D Logistic-adjusted-Sine map », 2016.
- [5] S. El Assad, M. Farajallah, et C. Vladeanu, « Chaos-based Block Ciphers: An Overview », 2014.
- [6] M.BENABDELLAH. « Outils de compression et de crypto-compression : application aux images fixe et vidéo » .Thèse de doctorat .Université Mohamed V-Agdal-Maroc.Juin2007.
- [7] Goumidi Djamel Eddine. Fonction logistique et standard chaotique pour le chiffrement des images satellitaires . Magister (école doctorale) en Electronique Spécialité : Télécommunications spatiales Université Mentouri de Constantine (UMC) ; Année 2010
- [8] Floriane Anstett Les systèmes dynamiques chaotiques pour le chiffrement :synthèse et crypt- analyse Centre de Recherche en Automatique de Nancy (CRAN) Thèse juillet 2005.
- [9] B. Schneier. Cryptographie appliquée. *International Thomson Publishing France, Paris*, janvier 2001.
- [10] S. Douglas. Cryptographie :Théorie et pratique. *Vuibert Informatique, Paris*, 2001.
- [11] A. Ali pacha, N. Hadj said . La Cryptographie et ses principaux systèmes de références, *RIST Vol, 12 n'01*, 2002.
- [12] <http://www.hsc.fr/ressources/cours/crypto/crypto.pdf>

- [13] Bruce Schneier traduction de L. Viennot cryptographie appliquée : protocoles, algorithmes et codes sources en C deuxième édition Vuibert informatique.
- [14] Noura Louzzani , Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos, Mémoire de fin d'études pour l'obtention du diplôme De Master en Informatique, Université Mohamed Sadik BENYAHIA de Jijel, 2021
- [15] M.A. FILALI. Etude et implémentation pipeline sur FPGA de l'algorithme de chiffrement AES, *Mémoire de Magister*, Université de Mohamed Boudiaf, Oran, 2014-2015.
- [16] A. Wurcker. Etude de la sécurité d'algorithmes de cryptographie embarquée vis-à-vis des attaques par analyse de la consommation de courant, *Thèse de Doctorat en Informatique*, Université de Limoges, France, 2015.
- [17] J. Emonet. Algorithmes de chiffrement. *Documentation* :version 1.0, 22 juin 2005.
- [18] Dover Publications, New York, NY, 1958 *The Principles of Science: A Treatise on Logic and Scientific Method* p. 141
- [19] *Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone (October 1996) "Handbook of Applied Cryptography". 0-8493-8523-7*
- [20] Stallings, William (1999-01-01). *Cryptography and Network Security: Principles and Practice* p 164 Le 23 mars 2019
- [21] "Dr Clifford Cocks CB". Bristol University. Smart, Nigel (February 19, 2008). Retrieved August 14, 2011.
- [22] Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology. p. 1. Archived (PDF) from the original on 5 March 2013. Retrieved
- [23] A. Beloucif, Contribution à l'étude des mécanismes cryptographiques, thèse En vue de l'obtention du diplôme de Doctorat en Informatique, Université de Batna2, 2016.
- [24] A. Walker, E. Wolfart, R. Fisher, S. Perkins, Image processing learning resources explore with java, http://homepages.inf.ed.ac.uk/rbf/HIPR2/hipr_top.
- [25] Diffie, W.; Hellman, M.E. (November 1976). "New directions in cryptography". *P* 644–654
- [26] Wikipédia, https://fr.wikipedia.org/wiki/Entropie_de_Shannon,
- [27] S. Bres, J-M Jolion et F. Lebourgeois, "Traitement et analyse des images numériques", Edition Lavoisier, 2003.
- [28] N. G. Kingsbury, The dual-tree complex wavelet transform : a new efficient tool for imagerestoration and enhancement, in European Signal Processing Conference, Sept. 1998, pp. 319_322.

- [29] ZITOUNI Athmane, « Ondelettes et techniques de compression d'images numérique », UNIVERSITE MOHAMED KHIDER BISKRA, THESE Doctorat en Sciences en Electronique, 2012/2013
- [30] E. Incerti, "Compression d'images, algorithmes et standards", Edition Vuibert, Paris, 2003.
- [31] D. A. Human. « Method for the construction of minimum-redundancy codes». In Proceedings of the Institute of Radio Engineers, volume 40, Sep 1952.
- [32] Analysis of optical near-field images by Karhunen—Loève transformation Daniel Charraut, Daniel Courjon, Claudine Bainier, and Laurent Moulinier, Applied Optics, Vol. 35, Issue 20, pp.3853-3861 (1996)
- [33] W.Chen, C.H. Smith, and S.C. Fralick. A fast computational algorithm for the discrete cosine transform. IEEE Trans on Communications, COM-25:1004_1009, 1977.
- [34] S. Grgic, M. Mrak, M. Grgic, "Comparison of JPEG Image Coders", Proceedings of the 3rd International Symposium on Video Processing and Multimedia Communications, VIPromCom-2001, Zadar, 2001, Croatia, pp. 79-85.
- [35] M.D. Adams, "The JPEG-2000 Still Image Compression Standard (Last Revised: 2002-12-25)", ISO/IEC JTC 1/SC 29/WG1 N 2412, December 2002.
- [36] S. Hsiang and J. W. Woods, "Embedded image coding using zeroblocks of subband/wavelet coefficients and context modeling," in MPEG-4 Workshop and Exhibition, ISCAS 2000, May 2000.
- [37] M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," IEEE Trans.on Signal Processing, vol. 41, pp. 3445–3462, Dec. 1993.
- [38] Djabri Hamza , Benhmied Youcef. Les techniques de compression d'images de télédétection. UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM , MEMOIRE DE Master en Informatique 2012/ 2013
- [39] Zhijun Fang, Naixue Xiong, Member, IEEE, Laurence T. Yang, Member, IEEE, Xingming Sun, and Yan Yang; "Interpolation-Based Direction-Adaptive Lifting DWT and Modified SPIHT for Image Compression in Multimedia Communications", 2011.
- [40] Benaïssa Mohamed . Bassou Abdesselam. Beladgham Mohammed. Taleb-Ahmed Abdelmalik. Moulay Lakhdar Abdelmounaim .Application of 16-State TCM-UGM and TCM for Improving the Quality of Compressed Color Image Transmission. *I.J. Image, Graphics and Signal Processing*, ,vol.6,No.10,pp.10-17.2014.

- [41] M. Mekouar, " Compression d'images médicales par ondelettes et régions d'intérêt", Mémoire pour l'obtention de la maîtrise en technologie des systèmes, Université du Québec, Montréal, 12 juin 2001.
- [42] S. Saha, « Image Compression – from DCT to Wavelets: A review » ACM Cross words students magazine, Vol.6, No.3, spring 2000.
- [43] NAIT AMARA N. CHOUCANE R « compression d'image fixes par classification de régions en associant les ondelettes et les fractales », mémoire d'ingénieur d'état en électronique, département électronique UMMTO 2008.
- [44] AKROUR.L « compression d'images par fractale dans le domaine de DCT », mémoire d'ingénieur d'état en électronique, département électronique UMMTO 2003
- [45] Z. Maymouna et S. Abla, « Compression des images avec curvelet ». Mémoire master, Université EchahidHamma Lakhdar-El Oued, 2015
- [46] T. Hamaizia, Systèmes Dynamiques et Chaos "Application à l'optimisation a l'aide d'algorithme chaotique", These pour obtenir le titre de Docteur en Sciences de l'Université deConstantine 1, 2013.
- [47] http://math.cmaisonneuve.qc.ca/alevesque/chaos_fract/Lorenz/lorenz.html
- [48] IKHLEF Ameer, 'synchronisation, Chosification et Hyperchaofication des Systèmes Nonlinéaires : Methodes et Applications', thèse de doctorat à l'Université Mentouri de Constanine, Algérie, 2011.
- [49] http://fr.wikipedia.org/wiki/Syst%C3%A8me_dynamique
- [50] http://fr.wikipedia.org/wiki/Syst%C3%A8me_d%C3%A9terministe.
- [51] Abdelkrim Boukabou, 'Méthodes de contrôle des systèmes chaotique d'ordre élevé et leur application pour la synchronisation : Contribution à l'élaboration de nouvelles approches, thèse de doctorat à l'université de Constantine, Algérie, Juin 2006.
- [52] <http://www.cax.free.fr/chaos/chaos.html>
- [53] G. Kaddoum. Contributions à l'amélioration des systèmes de communication multiutilisateurs par Chaos: synchronisation et analyse des performances, *Thèse de Doctorat de l'Université de Toulouse*, 2008.
- [54] Robert M. M. Simple Mathematical Models with very Complicated Dynamics. *Nature*.1976;1-9.
- [55] R. Ursulean, Reconsidering the generalized Logistic map as a pseudo random bit generator, *ELECTRONIKA IR ELECTROTECHNIKA*,.2004; 7(56):10-13.
- [56] Lixiao-ming ;Shen Hai-bin; yan xiao-lang. Characteristic Analysis of a Chaotic Random Number Generator Using Piece-Wise-Linear Map. *Journal of Electronics Information Technology*.2005;27(6): 874-878.

- [57] G Heidari-Bateni, C. D McGillem. A chaotic direct-sequence spread spectrum communication system. IEEE Transaction on Communications. 1994; 42(2): 1524-1527.
- [58] G Heidari-Bateni, C. D McGillem. Chaotic sequences for spread spectrum: an alternative to PN-sequences.inproceeding of the IEEE international conference on selected topics in wirelees communication, Vancouver Canada .1992; 437-440.
- [59] Wai M Tam; Francis C M Lau; Chi Kong Tse. Digital communications with chaos: multiple access techniques and performance. UK; Elsevier. 2007: 8.
- [60] R. Zhu and Y. Ma (eds.), Information Engineering and Applications, Lecture Notes in Electrical Engineering 154, DOI: 10.1007/978-1-4471-2386-6-107, Springer-Verlag London Limited 2012.
- [61] F.Alin.c ontribution à la prédiction et au contrôle des comportements apériodiques dans les convertisseurs électromécaniques : application de la théorie du chaos .thèse de doctorat .Reims 2005.
- [62] LEMMOUCHI Chahra. Utilisation d'une rotation 3D et des systèmes chaotiques pour le cryptage d'images, MEMOIRE de Master en informatique, Université d'Oum El Bouaghi, : 20 Juin 2013.
- [63] <http://selectiveimageencryption.blogspot.com/p/classification-of-selective-encryption.html>
- [64] Mohamed Krim, Adda Ali-Pacha, Naima Hadj-Said. The Quality of a New Generator Sequence Improvent for Spreading the Color Image Transmission System. TELKOMNIKA, February 2018; 16(1):407-419.
- [65] Earth Image Classification Design Using Unmanned Aerial vehicle .TELOMINIKA, Vol.13, No.3, September 2015:1021-1028