بسم الله الرحمن الرحيم

صدق الله العظيم

Dédicace

Je dédie cette thèse à :

A mes très chers parents

A ma femme et mes enfants Lina et Basma

A mes frères et sœurs

Aucune dédicace, aucun mot ne pourrait exprimer à leur juste valeur la gratitude et l'amour que je vous porte.

Je mets entre vos mains, le fruit de longues années d'études, de longs mois, de longs jours d'apprentissage.

Chaque ligne de cette thèse chaque mot et chaque lettre vous exprime la reconnaissance et le respect.

Remerciement

Au terme de cette thèse, j'adresse mes sincères remerciements à toute personne dont l'intervention a favorisé son aboutissement.

J'exprime mes profonds remerciements à mon encadrant de thèse, le professeur Abderrahim SAAIDI pour l'aide précieuse qu'il m'a apportée, pour sa patience et son encouragement tout au long de ce travail. Son œil critique a été très crucial pour structurer le travail et pour améliorer la qualité de résultats de différentes étapes. Sans lui rien n'aurait été possible.

Je tiens aussi à remercier, mon encadrant Mr Ali MOUHIB pour sa bienveillance et ses conseils avisés, pour l'aide et l'orientation durant ma préparation doctorale. Je lui témoigne également toute ma gratitude pour avoir consacré du temps précieux à ce travail de recherche.

Mes remerciements les plus sincères vont également à mon co-encadrants de thèse : Mr Ismail AKHARRAZ pour leur disponibilité et leur soutien tout au long de mes années de thèse. Je tiens à leur exprimer ma profonde gratitude.

Je remercie l'ensemble des membres du jury qui m'ont fait l'immense plaisir de juger et d'évaluer ce travail. Sincères remerciements au Président du jury, Mr Khalid SATORI, professeur à la faculté des Sciences Dhar El Mehraz de Fès, aux rapporteurs Mr Mohammed OUANAN Professeur à la faculté des Sciences, Université Moulay Ismail Meknès, Mr Abdelhakim CHILLALI professeur à la faculté Polydisciplinaire de Taza, Université Sidi Mohamed Ben ABDELLAH, Mr My Idriss El OUADGHIRI Professeur à la faculté des Sciences, Université Moulay Ismail Meknès, je tiens à remercier également Mr Majid BEN YAKHLEF et Mr Ismail AKHARRAZ professeurs à la faculté Polydisciplinaire de Taza, Université Sidi Mohamed Ben ABDELLAH pour avoir accepté d'être examinateurs de ma thèse.

Je tiens à remercier vivement aussi Mr Ismail AKHARRAZ le directeur du Laboratoire LSI de la faculté polydisciplinaire de Taza pour son accueilli au sein de son laboratoire, et mis à ma disposition tout ce dont je pouvais avoir besoin pour mener à bien ce travail.

J'exprime également mes remerciements à mes chers parents qui n'ont jamais cessé de m'encourager à bien mener mes travaux. Et à tous ceux qui m'ont encouragé et soutenu moralement et intellectuellement.

Résumé

Au cours des dernières années, le trafic des données ne cesse d'augmenter rapidement sur des réseaux très peu sûr et sous des menaces en forte croissance. La protection des données, et en particulier les images numériques, devient alors un enjeu crucial pour de nombreuses raisons à savoir la disponibilité, la confidentialité et l'intégrité. Actuellement, la technique la plus répandue pour pallier au problème de la confidentialité est le cryptage. Cependant, la plupart des algorithmes disponibles sont conçus pour les données de type texte. En effet, les données images sont considérées comme des données particulières en raison de leurs redondances élevées, leurs fortes corrélations et leurs tailles volumineuses. Par conséquent, certains algorithmes de cryptage traditionnels tels que DES, IDEA, RSA et AES ne sont pas adéquats au cryptage d'image. Récemment, plusieurs techniques de chiffrement ont montré de meilleures performances, en particulier la cryptographie chaotique. Et ceci grâce aux caractéristiques pseudo-aléatoires des signaux chaotiques tels que : bonnes propriétés cryptographiques, reproductibilité, et surtout l'hyper sensibilité aux conditions initiales. Dans cette thèse nous avons amélioré le comportement pseudo-aléatoires de certains systèmes chaotiques, dans l'objectif d'utiliser les nouvelles séquences pseudo-aléatoires générées dans les algorithmes de chiffrement que nous avons développés. L'analyse des performances de la sécurité basée sur les tests standards les plus significatifs à savoir : l'espace clé de cryptage, la sensibilité à la clé secrète, les tests statistiques (entropie, histogramme, corrélation des pixels adjacents) sur l'image claire et l'image chiffrée, et le temps d'exécution, montre l'efficacité et l'efficiences des techniques proposées dans nos algorithmes.

Mots-clés : Cryptographie, crypto-systèmes, confusion, permutation, diffusion, chiffrement, déchiffrement, systèmes dynamiques chaotiques, chiffre de Vigenère, chiffre de Hill.

Abstract

In recent years, data traffic has been growing rapidly on very insecure networks and the increase in illegal eavesdropping. Data protection, and in particular digital images, becomes a crucial issue for many reasons, namely availability, confidentiality and integrity. Currently, the most common technique to overcome the problem of confidentiality is encryption. However, most of the available algorithms are used for text data. In fact, image data are considered as special data because of their high redundancies, their strong correlations and their bulky sizes. As a result, some traditional encryption algorithms such as DES, IDEA, RSA, and AES are not suitable for image encryption. Recently, other encryption techniques have been introduced, particularly chaotic cryptography. This is due to the pseudo-random characteristics of chaotic signals such as: good cryptographic properties, reproducibility and especially the hyper sensitivity to initial conditions. In this thesis we have improved the pseudo-random behavior of some chaotic systems, with the aim of using the new pseudorandom sequences generated in the encryption algorithms that we have developed. The security performance analysis, based on the most significant standard tests, namely: the encryption key space, the secret key sensitivity, the statistical tests (entropy, histogram, correlation of the adjacent pixels) on the plain image and encrypted image, and the execution time shows the efficiency and the efficiencies of the developed techniques.

Keywords: Cryptography, crypto-systems, confusion, permutation, diffusion, encryption, decryption, chaotic dynamical systems, Vigenère cipher, Hill cipher.

ملخص:
في السنوات الأخيرة، تشهد عملية تبادل البيانات تطورا سريعًا عبر شبكات غير آمنة للغاية، ومع زيادة التنصت الغير القانوني التهديدات المتسارعة. أصبحت حماية هاته البيانات، وخاصة الصور الرقمية، مسألة مهمة لعدة أسباب، من بينها الإتاحة، الخصوصية والأمان. فكان للتشفير دور بارز في مجال حماية البيانات من عمليات التجسس والاختراق. إلا أن حاليا معظم الخوارزميات التي تم تطويرها تستعمل بشكل رئيسي لتشفير البيانات النصية ولا تكون
مناسبة للبيانات الخاصة بالصور الرقمية. وهذا راجع بالأساس إلى كثرة تكرار البكسلات المكونة لها والعلاقات القوية بينها بالإضافة إلى أحجامها الكبيرة مقارنة مع البيانات ذات الطبيعة النصية. ونتيجة لذلك، فإن بعض خوارزميات التشفير ليست مناسبة لتشفير الصور الرقمية. في الآونة الأخيرة، تم إدخال تقنيات**AES**و **DES**، **IDEA**، **RSA**التقليدية مثل جديدة لتشفير الصور، نخص بالذكر التشفير الفوضوي. ويرجع ذلك إلى الخصائص العشوائية لإشارات الفوضى مثل: خصائها الجيدة للتشفير، الاستنساخ وخاصة الحساسية المفرطة للظروف الأولية. في هذه الأطروحة، قمنا بتحسين السلوك العشوائي لبعض الأنظمة الفوضوية، وذلك بهدف استخدام تسلسلات عشوائية جديدة ذات درجة عالية من الأمان في خوارزميات التشفير التي تم تطويرها. تحليل الأداء الأمني، بناءً على أهم الاختبارات القياسية: كمساحة مفتاح التشفير، الحساسية للمفتاح السري، الاختبارات الإحصائية وزمن التنفيذ، بين كفاءة وفعالية الخوارزميات المقترحة.

الكلمات المفتاحية: التشفير، أنظمة التشفير، الارتباك، التقليب، الانتشار، فك التشفير، الأنظمة الديناميكية الفوضوية، شفرة فيجنير، شفرة هيل

Liste des abréviations

TIC	**T**echnologies de l'**I**nformation et de la **C**ommunication.
DES	**D**ata **E**ncryption **S**tandard
3DES	**T**riple **D**ata **E**ncryption **S**tandard
AES	**A**dvanced **E**ncryption **S**tandard
RSA	**R**on Rivest, **A**di Shamir et Leonard **A**dleman
1D	**U**nidimensionnelle
CTA	**C**ipher **T**ext **o**nly **A**ttack
KPA	**K**nown **P**lain Text **A**ttack
CPA	**C**hosen **P**laintext **A**ttack
BFA	**B**rute **F**orce **A**ttack
RC4	**R**ivest **C**ipher **4**
SUB	**S**ubstitution
ASCII	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
PWLCM	**P**iece**W**ise **L**inear **C**haotic **M**ap
PELM	**P**seudo **E**nhanced **L**ogistic **M**ap
ECC	**E**lliptic **C**urve **C**ryptography
XOR	e**X**clusive **OR**.
NPCR	**N**umber of **P**ixels **C**hange **R**ate
UACI	**U**nified **A**verage **C**hanging **I**ntensity
CH	**C**hiffre de **H**ILL
TFHC	**T**oorani-**F**alahati **H**ill **C**ipher
PSNR	**P**eak **S**ignal to **N**oise **R**atio
SIPI-USC	**S**ignal and **I**mage **P**rocessing **I**nstitute - **U**niversity of **S**outhern **C**alifornia
UCID	**U**ncompressed **C**olor **I**mage **D**atabase
PSNR	**P**eak **S**ignal to **N**oise **R**atio
MSE	**M**ean **S**quare **E**rror
GPACLE	**G**énérateur **P**seudo-**A**léatoire à **C**arte **L**ogistique **E**tendu
GPACLEA	**G**énérateur **P**seudo-**A**léatoire à **C**arte **L**ogistique **E**tendu **A**méliorée
CC	**C**arte **C**hebyshev
CL	**C**arte **L**ogistique
CS	**C**arte **S**ine
CCA	**C**arte **C**hebyshev **A**méliorée
CLA	**C**arte **L**ogistique **A**méliorée
CSA	**C**arte **S**ine **A**méliorée
EL	**E**xposant de **L**yapunov

Liste des tableaux

Liste des Figures

Table des matières

INTRODUCTION GENERALE

Contexte et problématique

De nos jours, les technologies de l'information et de la communication (TIC) ont connu un grand développement et revêtent une importance primordiale au sein de la société. Les TIC qui offrent des services aussi performants que diversifiés, ont largement contribué à la mondialisation des échanges. L'internet est l'un des outils incontournables dans tous les domaines. Par conséquent, l'échange des informations à aspect professionnel, personnel ou familial apparait souvent une nécessité majeure dans la société moderne. Cependant, cette mondialisation des échanges, pose le problème de la sécurité et de la confidentialité des données numériques transmises à travers les réseaux. Ainsi, assurer la sécurité et la confidentialité est l'une des tâches les plus urgentes auxquelles les organisations sont actuellement confrontées. Et afin de protéger les données personnelles contre tout accès illégitime, la cryptographie [1], qui constitue une solution adéquate pour garantir la confidentialité, et l'intégrité. Qui est l'étude des moyens et des techniques qui permettent de transmettre des données secrètes de manière confidentielle [2] [3]. Le chiffrement est le fait d'appliquer une transformation qui rend l'information inintelligible. Le chiffrement permet donc à partir de données lisibles d'obtenir des données illisibles. Dans le sens contraire, le déchiffrement est l'opération inverse permettant de rétablir et de restituer les données claires à partir de données chiffrées. En général, les transformations mises en œuvre sont des fonctions mathématiques, appelées algorithmes de chiffrement, qui dépendent d'un paramètre appelé clé [4].

L'information qui se transite sur un canal peu sécurisé, n'est pas toujours sous forme textuelles mais également audio, images numériques et autres multimédia. Actuellement, les images numériques sont très utilisées dans plusieurs domaines sensibles à savoir le commerce électronique, les affaires militaires et les dossiers médicaux, et, plus leur utilisation est croissante, plus leur sécurité est un enjeu majeur, surtout avec la multitude des menaces telles que le piratage, l'espionnage et l'escroquerie. Par exemple, il est primordial de sécuriser les plans de bâtisses militaires, les plans de construction d'une banque ou bien les images captées par des satellites militaires, les images médicales…etc. Dans ce contexte, il est devenu nécessaire et impératif de crypter les images numériques avant de les stocker ou les transmettre. Les algorithmes de chiffrement traditionnels tels que le **DES** (**D**ata **E**ncryption **S**tandard) [5]

[6], **AES** (**A**dvanced **E**ncryption **S**tandard) [7] et la **RSA** (**R**on Rivest, **A**di Shamir et Leonard **A**dleman) [8] ne sont pratiquement pas adéquats au chiffrement d'images [9] [10] en raison de certaines caractéristiques intrinsèques des images telles que la taille volumineuse (image de grande taille), la redondance élevée, la forte corrélation entre les pixels adjacents [11].

Par conséquent, il est nécessaire d'être prudent lors de chiffrement de ce type de données, et surtout de garantir un certain nombre de services de sécurité à savoir la confidentialité et l'intégrité, des images transmises.

Pour fournir une solution adéquate aux contraintes de sécurité d'images. Plusieurs techniques de chiffrement ont été développées telles que les méthodes basées sur les systèmes chaotiques [12] [13], qui offrent une bonne combinaison entre le temps d'exécution et la haute sécurité. En effet, l'utilisation des systèmes chaotiques en cryptographie ont attiré l'attention d'un grand nombre de chercheurs, en raison de leur sensibilité aux conditions initiales et de leur non linéarité. En effet, de nombreux algorithmes de chiffrement d'images basés chaos ont été proposés [14] [15] [16] [17]. Particulièrement, les cartes chaotiques unidimensionnelles sont des systèmes chaotiques populaires caractérisées par une simplicité, une rapidité de mise en œuvre dans les systèmes numériques, et une faible consommation des ressources [16]. Cependant, ces cartes présentent quelques faiblesses, à savoir, une distribution non uniforme, l'espace clé réduit et la périodicité [17]. Récemment, plusieurs auteurs ont amélioré avec succès la carte logistique pour surmonter ces faiblesses et de renforcer ainsi la sécurité [15] [18]. Par conséquent, les signaux chaotiques générés présentent de meilleurs propriétés pseudo-aléatoires et ils sont plus favorables à être utilisés comme clés secrètes dans un crypto système robuste. La sécurité obtenue est ainsi maximale, parce que la connaissance de l'image chiffrée ne donne aucune indication sur l'image claire correspondante.

Contribution

Actuellement, on assiste à une flambée d'algorithmes de chiffrement d'images numériques, et dans l'objectif de les améliorer et de les rendre plus performants. Ces dernières années, les chercheurs ont accordé plus d'importance à l'analyse des métriques de sécurité, ils ont remarqué que plusieurs techniques de chiffrement d'images souffrent d'un ou plusieurs problèmes à savoir, la faible sensibilité à la variation de l'image en claire, l'espace de clés

restreint, l'irrésistibilité à l'attaque texte clair choisi et l'irrésistibilité à l'attaque texte claire connu.

Dans ce contexte et en tant qu'objectif général de cette thèse nous avons proposé et validé de nouveaux algorithmes de chiffrement d'images basés sur les signaux chaotiques robustes et qui visent à surmonter les difficultés citées précédemment. En effet, et comme tout crypto système, nous nous sommes assurés que chaque méthode doit offrir les qualités cryptographiques requises suivantes :

- Un grand espace clé : Espace clé doit être suffisamment grand pour résister aux attaques par force brute.
- Sensibilité aux conditions initiales : Un changement infime des valeurs initiales devrait produire un changement radical.
- Faible complexité/rapidité : La complexité globale du système ne devrait pas être très élevée et le temps requis pour le cryptage devrait être raisonnable.
- Haute sécurité : Robustesse contre les attaques statistiques, différentielles, exhaustives et autres attaques connues.
- Forte diffusion : Un petit changement dans un bit d'un pixel devrait apporter des changements radicaux sur l'image chiffrée.
- Forte confusion : pas de corrélation entre les pixels adjacents.

Le travail présenté dans cette thèse s'organise autour de quatre chapitres :

Chapitre 1 : Généralités sur les crypto-systèmes : Fondement théorique et état de l'art.

Ce chapitre est consacré à une présentation des généralités sur les systèmes cryptographiques et à un bref préliminaire des notions de base en mathématiques nécessaires utilisées dans la thèse. Ensuite, il introduit les principaux schémas de chiffrement en cryptographie standard, le chiffrement asymétrique ou à clé publique et le chiffrement symétrique tout en faisant le focus sur les points forts et faibles de ces algorithmes. Puis, les caractéristiques des signaux chaotiques en étudiant le comportement pseudo-aléatoire des suites génératrices sont décrites. Enfin, des modes de chiffrement d'images incluant les systèmes chaotiques proposés sont détaillés dans l'optique de mettre en évidence la puissance de cet outil dans la cryptographie par rapport aux autres méthodes existantes dans la littérature.

Chapitre 2 : Nouveau schéma de chiffrement d'images basé sur la confusion/diffusion et qui utilise la carte Skew Tente améliorée.

La première méthode proposée pour le chiffrement d'images est présentée dans ce chapitre. Nous développons, dans un premier temps, ses différentes étapes (amélioration et validation de comportement pseudo-aléatoire de la carte Skew Tente, élaboration des deux processus de confusion-diffusion). Ensuite, nous présentons les résultats des simulations obtenus.

Nous signalons que des comparaisons, des discussions et des interprétations ont été introduites dans chaque chapitre pour montrer la robustesse et la validation de nos contributions.

Chapitre 3 : Nouvelle technique de chiffrement d'images basée sur un système chaotique 3D et un chiffre de Vigenère dynamique.

Dans ce chapitre nous présentons notre deuxième méthode proposée pour un chiffrement robuste des images couleurs et niveau de gris, nous décrivons, dans un premier temps, ses différentes étapes (Amélioration de propriétés statistiques d'un système chaotique 3D, élaboration d'une nouvelle table de Vigenère dynamique et application des deux mécanismes de chiffrement : Confusion et diffusion), puis, nous analysons et interprétons les résultats obtenus.

Chapitre 4 : Cryptage d'images basé sur une nouvelle variante sécurisée du chiffre de HILL et sur les cartes chaotiques 1D.

Ce chapitre est dédié à notre troisième approche proposée pour le chiffrement d'images. Nous décrivons dans un premier temps son principe (amélioration des propriétés statistiques de trois carte chaotiques 1D, pour produire trois générateurs pseudo-aléatoires performants qui offrent des propriétés pseudo-aléatoires meilleures par rapport aux cartes chaotiques initiales. Dans un deuxième temps, nous proposons une nouvelle variante de CH). Les performances de sécurité sont analysées et évaluées.

Conclusion, synthèse et perspectives.

La thèse ainsi menée s'achève par une synthèse, une conclusion et des perspectives.

Chapitre 1

Généralités et état de l'art des systèmes de chiffrement des données numériques.

Sommaire

1.1 Introduction

Dès que les gens apprirent à partager leurs messages secrets, ils durent découvrir des outils performants qui permettent de communiquer des messages tels qu'ils ne pourraient être lus exclusivement que par le destinataire privilégié. En effet, nous avons eu besoin de protéger des données à caractère confidentiel telles que des données bancaires, des stratégies militaires, ou encore des mots de passe. Il a donc fallu mettre en place des processus de protection efficaces pour protéger ces données sensibles. Les outils utilisés n'avaient alors pour tâche que de rendre difficile voire presque impossible la compréhension des données chiffrées, et seule la complexité des processus de cryptage offre la sécurité nécessaire aux messages. Mais ce n'est qu'après l'avènement de l'informatique que la cryptographie a connu un nouvel essor. En effet, avec l'explosion des développements des réseaux de communication comme la téléphonie mobile et l'internet, le besoin de garantir la confidentialité et l'intégrité des données transmises a connu une croissance considérable dans ces dernières années, et la cryptographie devient une véritable science du secret et a connu une grande avancée, allant des méthodes artisanales, aux méthodes reposants sur des concepts mathématiques de haut niveau (arithmétique, suites récurrentes, chao…). A titre d'exemple les cryptos-systèmes symétriques [5] [19] [20] [21], dont les principaux algorithmes sont DES (Data Encryption Standard) [5] [6] et AES (Advanced Encryption Standard) [21] [22], qui se basent sur les deux mécanismes élémentaires de chiffrement : la substitution et la transposition. Ces crypto-systèmes font l'hypothèse d'une clé secrète partagée au préalable par les correspondants. Mais le problème majeur réside dans les protocoles de partage de la clé. Le seconde intitulé cryptage asymétrique dont l'algorithme le plus répondu est le RSA, proposé par Ronald Rivest, Adi Shamir et Leonard Adleman [8]. Ce cryptage élimine le problème de partage des clés, mais malheureusement beaucoup plus couteux en temps de calcul que les algorithmes symétriques, et consomme plus de ressources informatiques. La dernière catégorie appelée cryptage hybride, fait la combinaison des précédents [23]. Actuellement, une alternative très prometteuse a été développée basée sur des séquences parfaitement pseudo-aléatoires telles qu'elles ne puissent pas être connues du cryptanalyste. Il s'agit bien de la cryptographie chaotique [12] [15] [24] [25].

Dans ce chapitre, nous allons présenter des concepts préliminaires sur la cryptographie, et un état de l'art des méthodes du chiffrement d'images niveau de gris et couleur, tout en mettant le focus sur celles similaires à nos travaux. Nous commencerons par la présentation des généralités dans le domaine de la cryptographie, ensuite nous présenterons succinctement

l'intérêt d'utiliser la cryptographie chaotique comme étant une nouvelle tendance du chiffrement moderne, puis, nous exposerons l'état de l'art sur les techniques de chiffrement des images similaires aux approches développées, enfin, nous terminerons le chapitre par une conclusion.

1.2 Généralités sur les crypto-systèmes

Dans cette section, nous introduisons les terminologies de base de la cryptographie, nous décrivons brièvement les objectifs de la cryptographie et ceux de la cryptanalyse.

1.2.1 Vocabulaire de base de la cryptographie

- **Cryptologie** : (« Cryptology » en anglais) est la science basée spécialement sur les mathématiques, elle comporte deux axes principaux : la cryptographie et la cryptanalyse.
- **Cryptographie** : (« Cryptography » en anglais) est l'étude des techniques mathématiques (Algorithmes) et des protocoles liés à la sécurité de l'information. Dans ce contexte, on entend la confidentialité, l'intégrité, l'authentification, et la non répudiation des données. Ainsi, la cryptographie consiste spécialement en l'élaboration d'un crypto-système ou d'un schéma de chiffrement et déchiffrement.
- **Cryptanalyse :(** « Cryptanalysis » en anglais) est l'art d'étudier des textes-chiffrés ou des systèmes cryptographiques en utilisant des moyens mathématiques en vue de trouver des failles qui permettront l'accès au texte clair à partir du texte chiffré, sans possession de la clé du chiffrement.
- **Chiffrement** :(« Encryption », en anglais) est l'opération qui consiste à transformer, au moyen d'une information appelée clé, un message clair afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître.
- **Déchiffrement** : (« Decryption », en anglais) est l'opération inverse du chiffrement. Il a pour but de récupérer l'information chiffrée en connaissant la clé secrète.
- **Décryptage :** l'opération qui permet de retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.
- **Crypto-système :** (« Cryptosystem », en anglais) est l'ensemble des deux méthodes de chiffrement et de déchiffrement. En cryptographie, l'information à dissimuler est également appelée message ou texte clair (« Plain-Texte », en anglais). Le résultat du

chiffrement d'un texte clair est appelé texte chiffré (« Cipher-Text », en anglais). Le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé.

- **Confidentialité** : (« Confidentiality » en anglais) vise à assurer que seuls les personnes légitimes aient accès aux ressources et aux informations auxquelles ils ont droit. Autrement dit, elle consiste à garder des données secrètes pour tous ceux qui ne sont pas autorisés à les connaître.
- **Intégrité :** (« Integrity » en anglais) a pour but de préserver les données de toute altération non autorisée. Autrement dit, elle vise à assurer que les ressources et les informations ne soient pas corrompues ou détruites par des tiers. L'objectif des attaques sur l'intégrité est de changer, d'ajouter ou de supprimer des informations.
- **Authentification** : (« Authentication » en anglais) permet de garantir à chacun des correspondants que son partenaire est surement celui qu'il croit être.
- **Non répudiation** : (« Nonrepudiation » en anglais) est le moyen qui garantit que l'émetteur d'un texte chiffré ne peut pas plus tard nier l'envoie et aussi le destinataire ne peut pas nier la réception du message.

Les différents processus de la cryptographie sont présentés dans la figure 1.1 suivante :

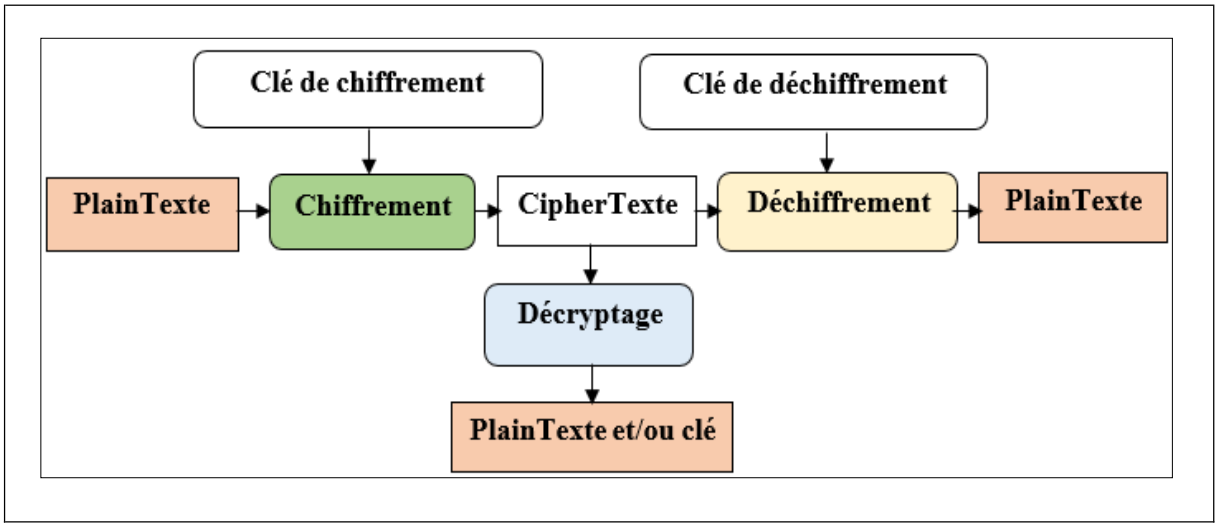

Figure 1.1: Schéma de chiffrement et déchiffrement

1.2.2 Principe de Kirchhoff

Un principe essentiel en cryptographie qui a été préconisé à la fin du XIX^{ème} siècle par le cryptologue français Auguste Kirchhoff [26] [27], il annonce que la technique utilisée pour le chiffrement est susceptible d'être aisément intercepté par l'ennemi. C'est à dire, un crypto-système doit être suffisamment sécurisé, même si tout ce qui concerne le système de

chiffrement est connu, sauf la clé de chiffrement. Autrement dit, aucun secret ne doit résider dans l'algorithme utilisé mais plutôt dans la clé.

1.2.3 Principe de Shannon

Shannon énonça [28] que pour supprimer avec succès les redondances dans un texte clair deux techniques cryptographiques doivent être mise en œuvre à savoir : La confusion et la diffusion.

- **Confusion** : Opération qui sert à rendre la relation entre le Plain-Texte et la clé de chiffrement la plus complexe possible, d'une part, et d'autre part le Cipher-Texte doit être aussi difficile que possible à établir, cela, à pour objectif de rendre le calcul de l'inverse est de complexité élevée, en d'autres termes, elle évite l'analyse du Cipher-Texte par une recherche de redondance et motifs statistique, la confusion est souvent assurée par une substitution.
- **Diffusion :** En cryptographie la propriété de diffusion sollicite que chaque partie du Cipher-Texte dépend étroitement de chaque partie du Plain-Texte d'une part, et de la clé du chiffrement d'autre part, autrement dit, de petits changements en entrée (modification d'un bit) doivent avoir un effet important en sortie. La confusion est souvent assurée par une permutation ou par un effet d'avalanche.

1.2.4 Effet d'avalanche

En cryptographie, l'une des principales propriétés souhaitées pour un schéma de chiffrement robuste est l'effet d'avalanche, ce processus provoque des changements de plus en plus importants en se propageant dans la structure de l'algorithme. Il en résulte qu'une perturbation infinitésimale d'un seul bit en clair ou au niveau de la clé, entrainera un changement radical des données en sortie, comme une avalanche [29]. Ce qui complique toute prédiction sur les entrées par simple observation des sorties et élimine donc toute sorte d'attaques statistiques et différentielles.

1.2.5 Quelques attaques d'un crypto-système

Cette section présente les principaux types d'attaques existant sur les chiffrements, une attaque est souvent caractérisée par les données qu'elle nécessite.

1.2.5.1 Attaque à texte chiffré seul (en anglais Cipher-text Only Attack ou COA)

C'est un modèle d'attaque utilisé en cryptanalyse quand l'attaquant possède uniquement des exemplaires chiffrés des messages, en faisant plusieurs hypothèses sur les messages originaux dont il ne dispose pas. La cryptanalyse est plus ardue par le manque d'informations à disposition. Une attaque ATC réussira quand on peut déterminer le Plain-Texte à partir du Cipher-Texte.

1.2.5.2 Attaque à texte clair connu (en anglais Known Plain-text Attack ou KPA)

L'adversaire possède des textes claires/chiffrés cryptés en utilisant la même clé. L'objectif est de retrouver la ou les clé (s) de chiffrement ou un algorithme qui permet de décrypter n'importe quel nouveau message chiffré avec la même clé.

1.2.5.3 Attaque à texte clair choisi (en anglais Chosen Plain-text Attack ou CPA)

Est un modèle d'attaque en cryptanalyse où l'attaquant peut choisir différents textes chiffrés à décrypter. Ce type d'attaque est plus efficace que KPA, car le cryptanalyste a le droit de choisir des textes en clair qui donneront plus d'informations sur la clé. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.

1.2.5.4 Attaque exhaustive (en anglais Brute-Force Attack ou BFA)

Le principe de ce type d'attaque est que l'adversaire essaie toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque consomme plus de ressources matérielles. C'est-à-dire plus coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive.

1.2.6 Classification des algorithmes de chiffrement

En fonction du nombre de clés utilisées pour le chiffrement et déchiffrement, les algorithmes cryptographiques peuvent être classés en deux catégories. Dans cette section nous présentons les deux types d'algorithmes de chiffrement existants :

1.2.6.1 Chiffrement symétrique (Chiffrement à clé secrète)

Le cryptage symétrique est la technique la plus ancienne et la plus connue. Cette méthode est nommée aussi le chiffrement à clé privée. Pour ce mode de chiffrement, l'expéditeur et le destinataire du message disposent tous les deux de la même clé secrète **K**. D'abord, l'expéditeur utilise la clé secrète **K** pour chiffrer le message nommé **M**. Le message chiffré est appelé **C**, ensuite, le destinataire utilisera la même clé **K** pour déchiffrer le message chiffré **C**, et reconstruire le message original **M**. Comme exemple de ce type d'algorithme nous citons DES, 3DES, AES et RC4 [5] [30] [31]. Les étapes du processus de chiffrement symétrique sont illustrées dans la figure 1.2 ci-dessous :

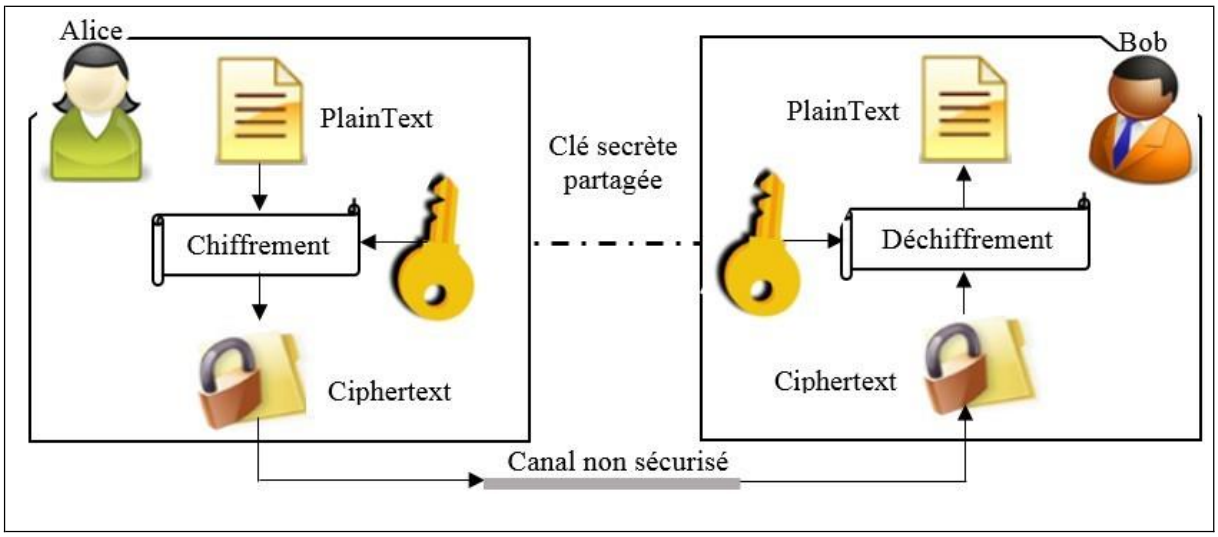

Figure 1.2: Processus de chiffrement symétrique.

Le cryptage et le décryptage d'un message **M** en utilisant la clé secrète **K** avec un algorithme symétrique sont désignés par les équations suivantes :

$$E_K(M) = C \qquad (1.1)$$

$$D_K(C) = M \qquad (1.2)$$

Dans cette section nous présentons succinctement les deux systèmes de chiffrement symétrique standard DES [5] et AES [22].

1.2.6.2 Algorithme de chiffrement DES

DES [5], pour Data Encryption Standard ("standard de cryptage de données"), est un algorithme à clé privée crée très répandu a été inventé par IBM en 1977. Il sert à la cryptographie et l'authentification de données.

Le DES est un algorithme de cryptographie en bloc. En pratique c'est un algorithme de chiffrement par bloc de 64 bits, c'est-à-dire que l'image est d'abord découpée en bloc de 64 bits et que l'on applique l'algorithme à chaque bloc. Comme précisé plus haut, la clé de chiffrement comporte elle aussi 64 bits, même si seuls 56 bits sont utiles, les 8 bits restant étant des bits de contrôle destinés à éviter les erreurs de transmission, les grandes lignes de cet algorithme sont :

- **Phase 1 : Diversification de la clé.**

On diversifie la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés K_1, ..., K_{16} à 48 bits. Les K_i sont composés de 48 bits de K, pris dans un certain ordre.

- **Phase 2 : Permutation initiale.**

Pour chaque bloc de 64 bits de l'image X, on calcule une permutation Y=P(X). Y est représenté sous la forme $Y=L_0R_0$, L_0 étant les 32 bits à gauche de Y, R_0 les 32 bits à droite.

- **Phase 3 : Itération.**

Pour chaque bloc de 64 bits X de l'image, on applique 16 tours d'un même schéma de Feistel. A partir de $L_{i-1}R_{i-1}$ (pour i de 1 à 16), on calcule L_iR_i en posant :

- $L_i = R_{i-1}$
- $L_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Où $\oplus$ est le "ou exclusif" bit à bit, et f est une fonction de confusion, suite de substitutions et de permutations.

- **Phase 4 : Permutation finale.**

On applique à $L_{16}R_{16}$ l'inverse de la permutation initiale. $Z=P^{-1}(L_{16}R_{16})$ est le bloc de 64 bits chiffré à partir de X. le schéma de la figure 1.3. Illustre les différentes étapes de chiffrement par l'algorithme DES.

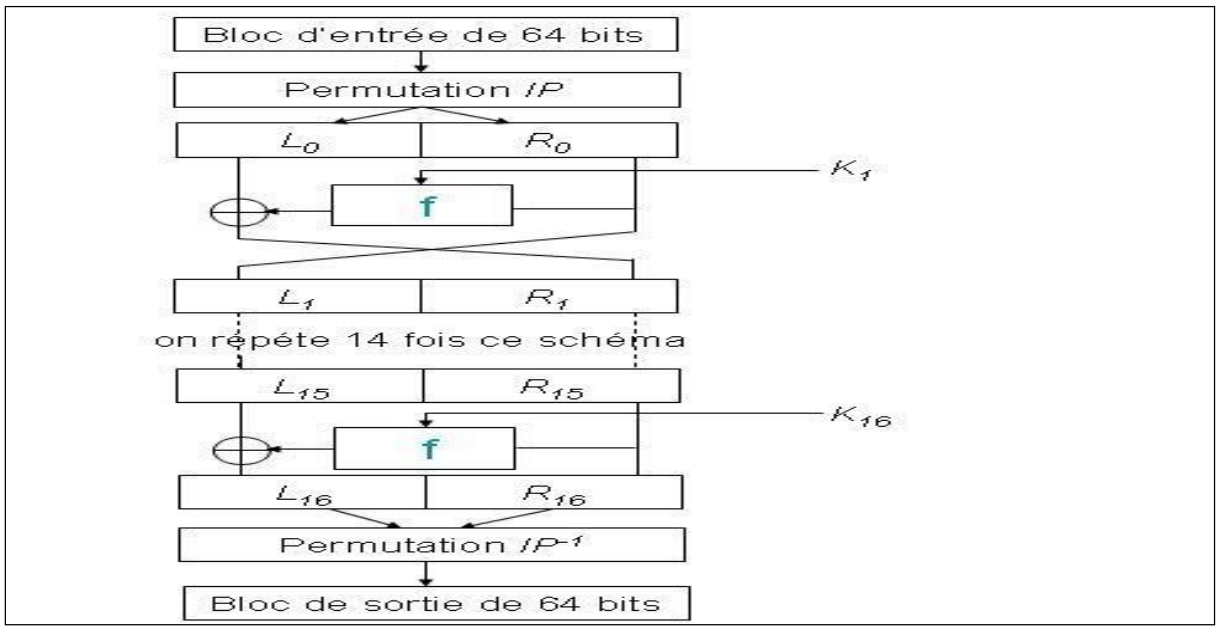

Figure 1.3: Schéma de l'Algorithme DES.

Il est à signaler que le DES est obsolète car d'une part il est trop lent et d'autre part, vue la puissance de supercalculateurs actuels, il est devenu vulnérable à l'attaque par force brute sur sa clé de 56 bits qui est devenue trop courte.

1.2.6.3 Algorithme de chiffrement AES

L'AES [22] (Advanced Encryption Standard) est, comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le DES qui est devenu trop faible face aux attaques connues. L'AES est le successeur du DES, aussi c'est un algorithme de chiffrement en bloc à clé secrète efficace et à faible coût mémoire, basé sur des opérations binaires ; à savoir les permutations et les substitutions. L'AES est exploité dans des applications supportant des fichiers volumineux tels que les images, il opère sur des blocs de 128 bits (Plain-Texte P) qu'il transforme en blocs cryptés de 128 bits (Cipher-Texte C) par une séquence de Nr opérations ou « rounds » (Nr est le nombre de tours), à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de tours diffère (10, 12 et 14, respectivement).

Le schéma de la figure 1.4 décrit succinctement le déroulement servant à crypter un bloc de données avec l'algorithme AES :

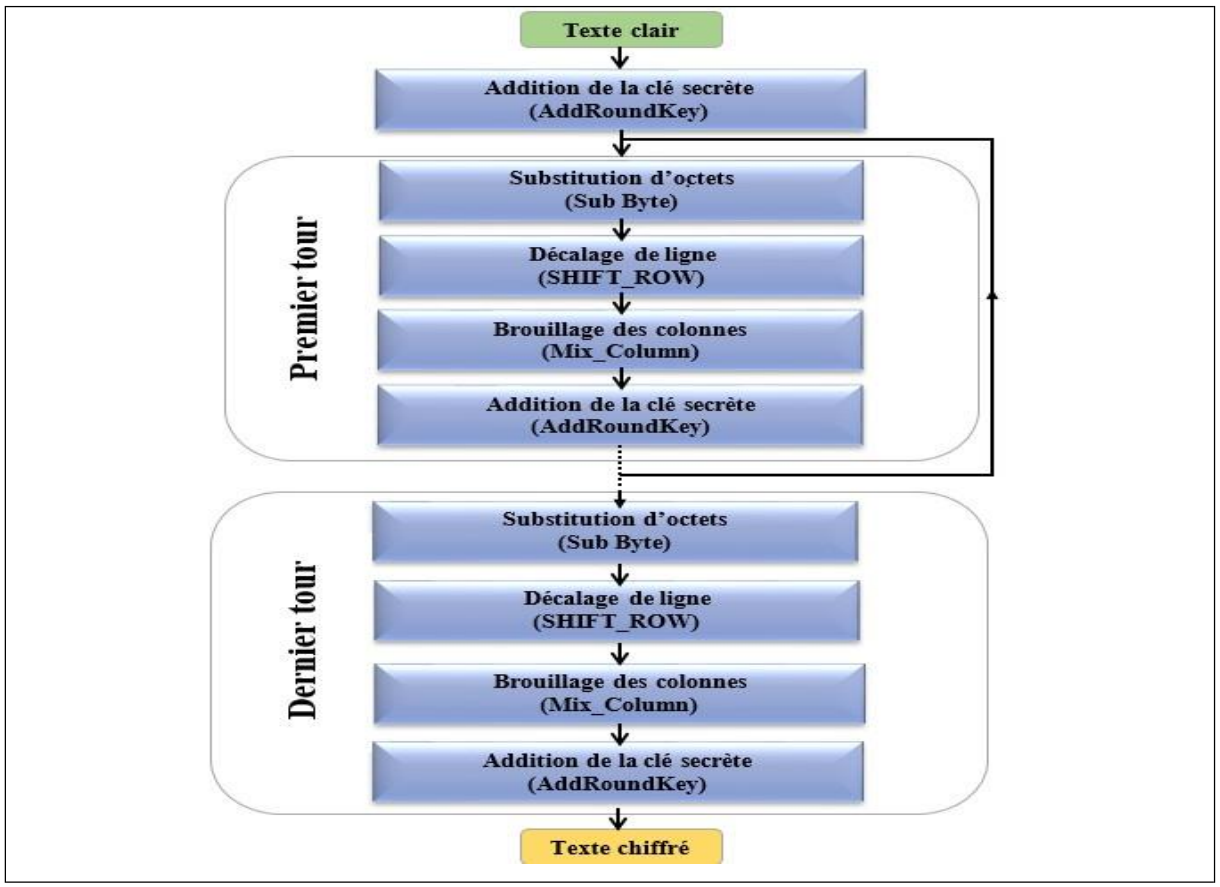

Figure 1.4: Schéma de l'Algorithme AES.

- **Addition de la clé secrète (en anglais AddRoundKey)** : consiste à faire un ou exclusif entre les **n** bits d'un état (Plain-Texte) et ceux de la clé du tour **T**.
- **Substitution d'octets (en anglais BYTE_SUB)** : représente une fonction non-linéaire opérant indépendamment sur chaque bloc à partir d'une table appelée 'table de substitution'.
- **Décalage de ligne (en anglais SHIFT_ROW) :** est une fonction qui réalise des décalages (précisément elle prend l'entrée en 4 morceaux de 4 octets et opère des décalages vers la gauche de 0, 1, 2 et 3 octets pour les morceaux 1, 2, 3 et 4 respectivement).
- **Brouillage des colonnes (en anglais MixColumn) :** est une fonction qui permet de transformer chaque octet d'entrée en une combinaison linéaire d'octets d'entrée exprimée mathématiquement par un produit matriciel sur le corps de Galois **(2^8)**.

1.2.6.4 Avantages et inconvénients du chiffrement symétrique

En général, les techniques de chiffrement symétrique sont très rapides, elles sont caractérisées par une complexité moins élevée par rapport au chiffrement à clé publique tel que

RSA [8], les plus connus sont : DES et AES, en revanche, la gestion des clés des systèmes de chiffrement symétriques pose un grand problème.

1.2.6.5 Chiffrement asymétrique (Chiffrement à clé publique)

Cette technique de chiffrement a été proposée par Diffie et Hellman, en 1976 [30]. Dans un tel schéma, la clé de chiffrement soit identique à la clé de déchiffrement, quiconque est autorisé à utiliser la clé de chiffrement, ou clé publique, ainsi, cette clé est destinée à être divulguée, est accessible pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement, ou clé privée gardée secrète, peut déchiffrer le message chiffré, les systèmes de chiffrement asymétriques les plus connus sont : RSA [8] , El Gamal [10], Crypto système de Merkle Hellman [30]… etc. Le processus de cryptage asymétrique est présenté dans la figure 1.5 ci-dessous.

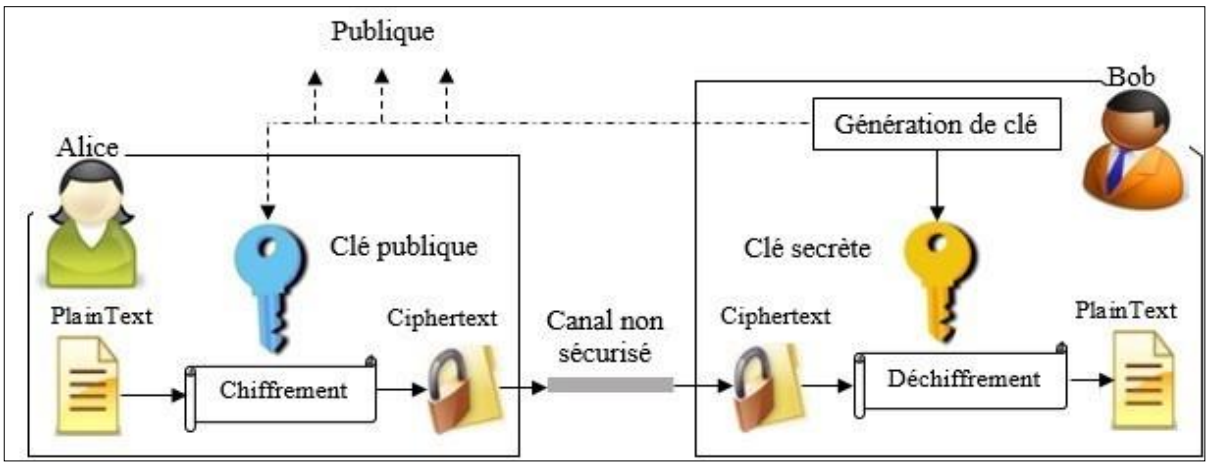

Figure 1.5: Processus de chiffrement asymétrique.

Dans les systèmes de chiffrement asymétrique l'entité **A** (Alice) possède une clé publique **e** et une clé privée correspondante **d**, de telle sorte que mathématiquement il est impossible de calculer la clé secrète **d** à partir de la clé publique **e**. Si l'entité **B** (Bob) souhaite envoyer un message **m** à **A**. Dans un premier temps, elle doit obtenir une copie authentique d'une clé publique **e**, ensuite, elle utilise l'équation de chiffrement (Voir équation 3) pour obtenir le texte chiffré, puis elle transféra le message chiffré à **A**, dans l'autre sens pour déchiffrer le message chiffré Alice applique l'équation de déchiffrement (Voir équation 4) afin de reconstruire le message orignal **m**.

$$E_e(M) = C \tag{1.3}$$

$$D_d(C) = M \tag{1.4}$$

1.2.6.6 Algorithme de chiffrement RSA

Il s'agit d'un algorithme de chiffrement à clé publique développé par Ron Rivest, Adi Shamir et Len Adleman en 1977 [8]. L'algorithme RSA est le plus connu des algorithmes de cryptage asymétrique basé sur le fait qu'il est facile de multiplier deux grands nombres premiers mais difficile de factoriser le un nombre en deux nombres premiers plus grands.

Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés, pour chiffrer les emails, et dans le domaine bancaire. Les étapes de l'algorithme RSA sont :

- Choisir deux grands nombres premiers distincts **p** et **q**.
- Calculer **n=p*q**.
- Calculer **φ(n) = (p-1) (q-1).**
- Choisir un entier naturel **e** premier avec **φ(n)** strictement inférieur à **φ(n)**, appelé exposant de chiffrement.
- Calculer l'entier naturel d, inverse de **e** *modulo* **φ(n)**, et strictement inférieur à **φ(n)**, a appelé exposant de déchiffrement.
- Chiffrement : Le chiffrement d'un message M en un message codé **C** se fait suivant la transformation suivante : $\mathbf{C=M^e \bmod n}$.
- Déchiffrement : il s'agit de calculer la fonction réciproque : $\mathbf{M=C^d \bmod n}$.

Casser le système de chiffrement RSA, revient à retrouver la clé privée **d** à partir de la clé publique ***e***, ce qui nécessite de connaitre les valeurs **p** et **q**. Autrement dit, factoriser le produit le grand nombre **n**. Or **n** est suffisamment grand pour que cela ne soit pas réalisable dans un temps raisonnable. Actuellement, la longueur de **n** varie entre 512 et 2048 bits. Compte tenu de la grande puissance des nouveaux superordinateurs et des avancés mathématiques en matière de factorisation des grands nombres, les tailles des deux nombres **p** et **q** doivent augmenter au cours du temps.

Vu la grande complexité algorithmique du RSA, ce système de chiffrement est en général utilisé pour communiquer une clé de chiffrement symétrique, afin d'assurer un échange confidentiel. Autrement dit, Bob envoie à Alice une clé de chiffrement symétrique qui peut ensuite être utilisée par Alice et Bob pour transmettre et recevoir des données [7].

1.2.6.7 Avantages et inconvénients du chiffrement asymétrique

L'avantage principal du chiffrement à clé publique réside dans la facilité de gestion des clés de chiffrement des utilisateurs, ainsi, le chiffrement asymétrique résout le problème de distribution des clés via un canal non sécurisé que l'on peut rencontrer dans la cryptographie à clé privée, et toutes les communications sont constituées uniquement de clés publiques et aucune clé privée n'est jamais transférée ou partagée. Néanmoins, ces systèmes de chiffrement souffrent principalement de leur grande lenteur. Bien sûr, il ne faut pas une heure pour chiffrer un message mais c'est bien 100 à 1000 fois plus long que certains algorithmes de chiffrement symétriques. Et aussi ils sont vulnérables à une attaque KPA (cela est dû au fait que la clé de chiffrement est publique, par conséquent, un adversaire peut facilement faire de nombreuses tentatives sur des textes clairs et voir si le texte chiffré correspond).

Dans la pratique, les systèmes de chiffrement symétrique et asymétrique sont souvent combinés dans le but d'exploiter leurs avantages du mieux possible pour rendre le chiffrement efficace et plus performant.

1.2.6.8 Algorithmes de chiffrement classiques

Dans cette section, nous décrivons succinctement quelques algorithmes de chiffrement classiques qui reposent en général sur les deux mécanismes fondamentaux du cryptage : la substitution (remplacer certaines lettres par d'autres) et la transposition (permuter des lettres du message afin de le brouiller).

1.2.6.8.1 Code de César

Le système de chiffrement de César [31] est la technique de chiffrement la plus ancienne communément admise par l'histoire, le principe consiste en une substitution mono-alphabétique qui repose sur un décalage de lettres. Voici un exemple :

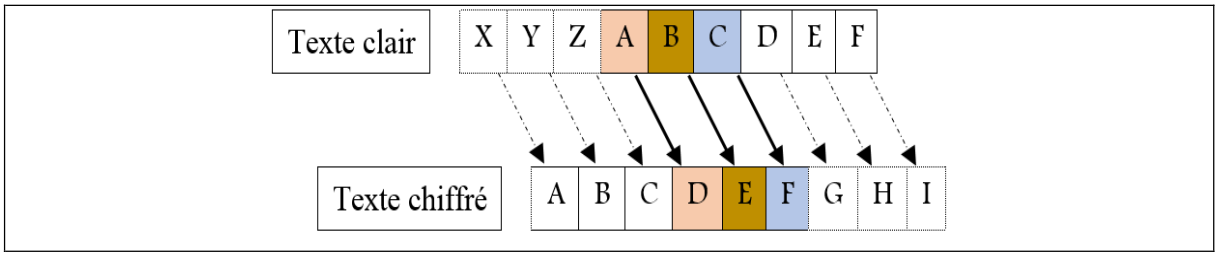

Figure 1.6: Le chiffrement de césar.

Le principe de chiffrement est simple, il consiste à décaler les lettres de l'alphabet d'un nombre **n**. dans la figure 1.9 ci-dessus, on remplace A par D (n=3), on remplace B par E, C par F.... Le point faible du code de César réside dans le fait qu'il n'y a que 26 façons différentes de chiffrer un message. Donc ce code est très peu sûr, puisqu'il est très facile de tester de façon exhaustive toutes les possibilités.

1.2.6.8.2 Chiffre de Vigenère

Vigenère, né en 1523, fut le créateur d'une nouvelle technique de chiffrement des messages qui domina 3 siècles [32] [12]. Vigenère expose le maniement du chiffre carré dans son écrit " Traité des chiffres, ou secrètes manières d'écrire ; Paris 1596 ". Le principe de chiffrement de Vigenère ressemble beaucoup au code de César, à la différence près qu'il utilise une clé plus longue afin de surmonter le problème du code de César dans lequel une lettre puisse être codée d'une seule manière. Pour cela le chiffre de Vigenère utilise un mot clé au lieu d'un simple caractère, ainsi, l'idée de Vigenère est d'utiliser un code de César, mais où le décalage utilisé change de lettres en lettres. Pour cela, une table de 26 alphabets (Appelée carré de Vigenère) sera utilisée, écrits dans l'ordre, décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement le texte à crypter.

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

Figure 1.7: Carré de Vigenère.

Pour chiffrer un texte, on choisit une clé (mot ou phrase), à chaque lettre du Plain-Texte on fait correspondre une lettre de la clé (la clé étant répétée autant de fois que nécessaire). La lettre du Cipher-Texte sera prise dans la colonne correspondante à la lettre du Plain-Texte, et dans la ligne correspondante à la lettre de la clé. Si on pose C le Cipher-Texte, P le Plain-Texte et K la clé, on peut exprimer ce mécanisme par la formule suivante :

$$C = (P + K) \bmod 26 \qquad (1.5)$$

Le déchiffrement est très simple. Il suffit, de pointer la colonne de la lettre de la clé, de rechercher la lettre du Cipher-Texte, à l'extrémité gauche de la ligne, on trouve la lettre du texte claire. Le déchiffrement s'exprime par la formule suivante :

$$P = (C - K) \bmod 26 \qquad (1.6)$$

1.2.6.8.3 Chiffre affine

Pour le chiffrement affine l'idée de base est d'utiliser comme fonction de chiffrement une fonction affine du type :

$$Y = (aX + b) \bmod 26 \qquad (1.7)$$

où les paramètres a et b sont des constantes, X et Y sont des nombres correspondant aux lettres de l'alphabet (A=0, B=1, …, etc.). On remarque aisément que si a = 1, alors on retombe sur le chiffre de César où b est le décalage (le **n** du chiffre de César).

1.2.6.8.4 Chiffre de Hill

Le chiffre affine de Hill est un système de chiffrement simple publié par le mathématicien Lester S. Hill en 1929 [33] [34]. C'est un cryptage polygraphique, c'est-à-dire qu'on ne (dé)chiffre pas les lettres les unes après les autres, mais par paquets, c'est-à-dire que l'on groupe les lettres deux par deux, mais on peut envisager des paquets plus grands.

Les lettres sont tout d'abord remplacées par leur rang dans l'alphabet, ainsi, les lettres $\mathbf{P_k}$ et $\mathbf{P_{k+1}}$ deviennent $\mathbf{C_k}$ et $\mathbf{C_{k+1}}$.

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26} \qquad (1.8)$$

Les composantes de cette matrice doivent être des entiers positifs, de plus la matrice doit être inversible dans l'anneau $\mathbb{Z}/256\mathbb{Z}$. Cependant, sa taille n'est pas fixée à 2. Chaque pair (P_1 et P_2) sera chiffré afin d'obtenir (C_1 et C_2) selon les équations suivantes :

$$C_1 \equiv (aP_1 + bP_2) \bmod 26 \tag{1.9}$$

$$C_2 \equiv (cP_1 + dP_2) \bmod 26 \tag{1.10}$$

Dans le cas général, la clé est une matrice carrée d'ordre m. et les paquets sont des vecteurs de taille m avec m⩾2.

$$\begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ (C_m) \end{pmatrix} = \left(\begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{bmatrix}\right) \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ (P_m) \end{pmatrix} \text{ Ou bien } \tag{1.11}$$

$$C = K.P$$

Le déchiffrement d'un message ne sera possible que si la matrice clé **K** est inversible, et il sera réalisé à l'aide de la matrice inverse $\mathbf{K^{-1}}$ puisque : $\mathbf{P = K^{-1}C.}$

Remarque :

Si le nombre de lettres du texte clair avait été impair, Alice aurait simplement ajouté une lettre arbitraire à la fin du message original. Pour déchiffrer le message chiffré, on procède de la même manière que pour le chiffrement : on prend les lettres deux par deux, puis on les multiplie par la matrice de déchiffrement.

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ (P) \end{pmatrix} = \left(\begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{bmatrix}\right)^{-1} \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ (C_m) \end{pmatrix} \text{ Ou bien } P = K^{-1}.C \tag{1.12}$$

1.3 Cryptographie chaotique

1.3.7 Théorie du Chaos

Depuis la nuit des temps, le chaos était synonyme de confusion et de désordre. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. Dans la littérature, le terme "chaos" désigne un état particulier d'un système dont le comportement s'avère difficile à anticiper, caractérisé par une extrême sensibilité aux conditions initiales ce qui favorise son imprédictibilité à long terme [33] [35]. Historiquement, ce n'est que vers les années 70 que la théorie du chaos s'est imposée sur le devant de la scène scientifique. Ainsi, le terme « chaos » n'a d'ailleurs été introduit qu'en 1975 par les deux mathématiciens Tien Yien Li et James A. Yorke [36]. En effet, la théorie du chaos à contribuer fortement aux progrès de l'informatique. Au début, les spécialistes considèrent le « chao » comme perturbateur et à l'origine des défaillances des systèmes qu'ils conçoivent. L'idée de base est de le contrôler afin de le modifier, ou bien le supprimer. Dans ce contexte, les premiers travaux fondamentaux ont été réalisés par Shinbrot, T et al. [37]. Une fois ces phénomènes avaient été assimilés grâce aux ordinateurs, l'objectif par la suite est porté sur la possibilité d'adapter et d'utiliser les signaux chaotiques crées dans la cryptographie.

En effet, Au cours des dernières décennies, plusieurs chercheurs ont étudié la théorie du chaos dans de nombreux domaines de recherches, notamment les systèmes électroniques, la dynamique des fluides, les lasers, le temps et le climat [37] [38]. La théorie du chaos est une branche des mathématiques qui étudie le comportement de systèmes dynamiques complexes qui sont très sensibles aux changements de leurs paramètres et donnent des résultats imprévisibles. Il existe plusieurs exemples populaires de systèmes chaotiques tels que l'attracteur Lorenz, l'attracteur Rösler, la carte logistique, la carte Henon, la carte des tentes et la carte chaotique PWLCM [39] [40] [21]. En général, la sécurité des systèmes cryptographiques a été construite sur la base de problèmes mathématiques difficiles ou non résolus. La théorie du chaos apparait adéquate à la cryptographie en raison de ses caractéristiques, telles que sa nature déterministe, son imprévisibilité, son aspect aléatoire et surtout sa sensibilité aux conditions initiales. Au cours des deux dernières décennies, l'utilisation du chaos pour concevoir des algorithmes cryptographiques sécurisés a suscité un intérêt considérable [43] [12] [18].

1.3.7.1 Caractéristiques du Chaos

Les systèmes dynamiques non linéaires produisent des signaux chaotiques sous forme d'ondes non périodiques, sous certaines conditions, ils ressemblent à un bruit que ce soit dans le domaine fréquentiel ou temporel. Ce qui les rend imprévisibles. En effet, les orbites chaotiques sont extrêmement sensibles à n'importe quelle modification (même infinitésimale) dans les paramètres de contrôle ou les conditions initiales (l'ensemble forme la clé secrète de chiffrement) d'un crypto-système donné. L'une des principales caractéristiques des systèmes chaotiques est leur hypersensibilité à la clé secrète. Cette hypersensibilité explique le fait que, pour deux systèmes chaotiques identiques, une légère modification des conditions initiales peut entrainer des résultats imprévisibles à long terme. Ce résultat est souvent vulgarisé sous le nom « d'effet papillon ». Cette caractéristique, rend l'utilisation des signaux chaotiques très importante pour la sécurité de l'information. Dans ce contexte plusieurs travaux de recherche, montrent l'intérêt d'utilisation des signaux chaotiques dans la sécurité de données informatiques [41].

1.3.7.2 Conditions d'obtention du chaos

- **Non-linéarité** : Un système linéaire ne peut être jamais chaotique, un système chaotique est toujours un système dynamique non-linéaire.
- **Sensibilité aux conditions initiales** : Un changement infime sur l'état initial peut mener à des comportements radicalement différents dans son état final.
- **Déterminisme :** Le déterminisme est défini comme étant la capacité à « prédire » le comportement futur d'un phénomène à partir d'un évènement passé ou présent.

1.3.7.3 Principe d'une communication sécurisée par chaos

Protéger les données à caractère confidentiel contre des interceptions indésirables a toujours attiré l'attention dans les réseaux de communication. Généralement, l'authentification et la confidentialité de l'information sont réalisées grâce à des algorithmes. Récemment, d'autres techniques de cryptage ont été introduites, tels que la communication par chaos [41]. En effet, le chaos peut générer des comportements dynamiques d'aspects aléatoires. Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication. En général les schémas de chiffrement chaotiques utilisent des nombres pseudo-aléatoires générés à partir des fonctions chaotiques. En effet, une fonction est qualifiée de « chaotique », si elle est non linéaire et surtout si elle est extrêmement sensible aux modifications, même infiniment

faible de la valeur de la clé constituée des conditions initiales et des paramètres de contrôle, les séquences des nombres pseudo-aléatoires générées seront utilisées par les algorithmes qui utilisent le chao pour chiffrer le message clair, la figure 1.8 ci-dessous illustre le principe de chiffrement utilisant le chao :

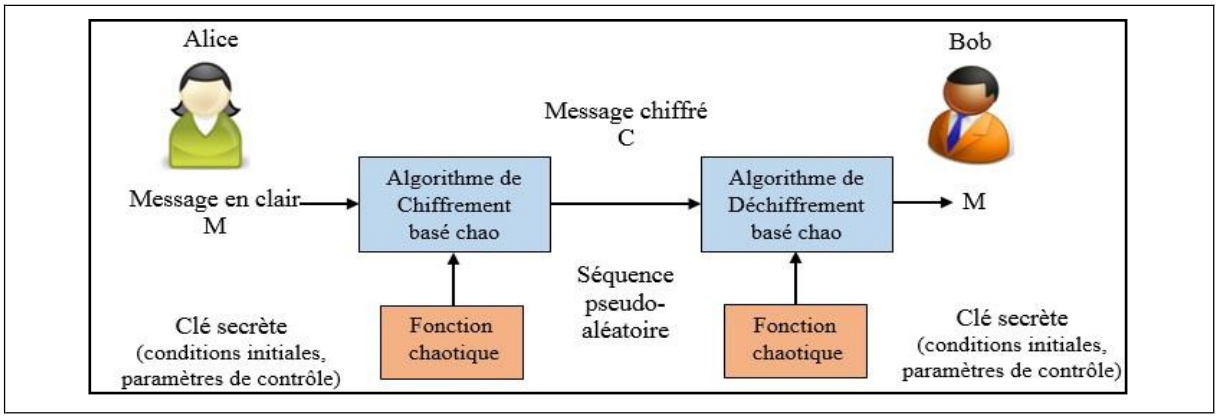

Figure 1.8: Schéma de principe d'un crypto-système basé chaos.

Lorsque Bob reçoit le message chiffé C, la même fonction chaotique sera utilisée avec la même clé secrète pour générer la même séquence pseudo-aléatoires. La mise en œuvre de cette séquence dans l'algorithme de déchiffrement chaotique qui permet à Bob de récupérer le message en clair M (peut être des données numériques, une image, un texte, une vidéo, etc.). Dans la littérature, il existe plusieurs fonctions chaotiques, appelées aussi cartes chaotiques à savoir : logistique, PWLCM (Piece Wise Linear Chaotic Map), sinus, Tchebychev, Skew Tente Map [40] [39] [42] [43] [41]. Ces fonctions chaotiques sont des systèmes récurrents, la propriété de l'hyper-sensibilité à la clé secrète, est à l'origine de nombreux travaux de recherche scientifique, montrant l'intérêt des signaux chaotiques dans la sécurité des systèmes de communications [41]. En bref, la cryptographie par les systèmes chaotiques, est une nouvelle tendance, qui a déjà prouvé une faisabilité et une puissance de chiffrement supérieur, ainsi, chiffrer un Plain-Texte par le chaos se réalise en superposant au texte clair un signal chaotique. De ce fait, le message envoyé par l'entité Alice (Cipher-Texte) est pleinement noyé dans le chaos, à le réception l'entité Bob se chargera de soustraire le chaos du message chiffré pour retrouver le Plain-Texte.

1.3.8 Quelques exemples de cartes chaotiques

Le chaos peut apparaitre simplement après des réitérations des fonctions mathématiques. En effet, plusieurs fonctions existent dans la littérature.

1.3.8.1 Carte logistique

1.3.8.1.1 Définition

La carte logistique est l'une des fonctions chaotiques les plus utilisée dans les systèmes de chiffrement basés chao, considérée comme un exemple simple de suite dont la récurrence non linéaire, cette récurrence fut popularisée par le biologiste Robert May en 1976 [44]. Ainsi, une suite logistique est une suite simple, dont la récurrence est non linéaire, donnée par la relation suivante :

$$f(X_n) = X_{n+1} = \mu X_n(1 - X_n) \qquad (1.13)$$

Avec X_n présente la variable dynamique prenant des valeurs dans l'intervalle $]0,1[$, μ est le paramètre de contrôle du système. Selon la valeur de μ, la suite peut être un point fixe, une suite périodique de période 2, 4, 8, ... Pour μ = 3.569692, ou une suite chaotique pour μ dans l'intervalle [3.56996, 4]. A l'origine le biologiste Robert May [44] a utilisé cette fonction dans le domaine démographique afin de modéliser l'évolution d'une population naturelle (d'où le terme fonction logistique), en faisant modifier le paramètre de contrôle, plusieurs comportements différents sont constatés :

- **1er cas** : $\mu = 0$ ou $\mu = 1$, la suite (X_n) converge vers le point fixe 0. C'est-à-dire l'espèce finira par mourir, quelle que soit la population de départ (condition initiales). Autrement dit : $\lim_{n\to\infty} X_n = 0$.
- **2ème cas** : $1 \leq \mu \leq 3$: Dans ce cas l'effectif de la population se stabilise. Et on distingue deux sous cas :
  - Si $1 \leq \mu \leq 2$, la population finit par se stabiliser autour de la valeur $\alpha = \frac{\mu-1}{\mu}$, quelle que soit la population initiale. Mathématiquement : $\lim_{n\to\infty} X_n = \alpha$.
  - Si $2 \leq \mu \leq 3$, la population finit par se stabiliser également autour α. Et cela après avoir oscillé autour de α pendant quelque temps. La suite converge avec une vitesse linéaire, sauf pour μ = 3 où elle est très lente.
- **3ème cas** : $3 < \mu \leq 1 + \sqrt{6}$ (approximativement 3.45), la population oscillera entre deux valeurs indépendantes de la population initiale.
- **4ème cas** : $3.45 < \mu < 3.54$, la population oscillera dans ce cas entre quatre valeurs, encore indépendamment de la population initiale.

- **5ème cas** : Lorsque μ devient légèrement supérieur à 3.54, la population oscillera entre 8 valeurs, puis 16, 32, etc.
- **6ème cas** : μ > 3.57, la suite présente un comportement chaotique, mais il existe quelques valeurs isolées de μ avec un caractère non chaotique. Celles-ci s'appellent les fenêtres blanches. Par exemple au voisinage de la valeur 3.82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs. Le diagramme de bifurcation présenté dans la figure 1.12 résume graphiquement les différents cas.

1.3.8.1.2 Diagramme de bifurcation

Dans le diagramme de bifurcation, dit de Feigenbaum [45], on représente sur l'axe horizontal la valeur du paramètre **μ** et en ordonnées les valeurs obtenues par la carte logistique entre deux rangs suffisamment élevés, pour un paramètre μ_0 fixé. Cela permet d'observer le comportement asymptotique de la carte logistique, selon la valeur donnée à **μ**.

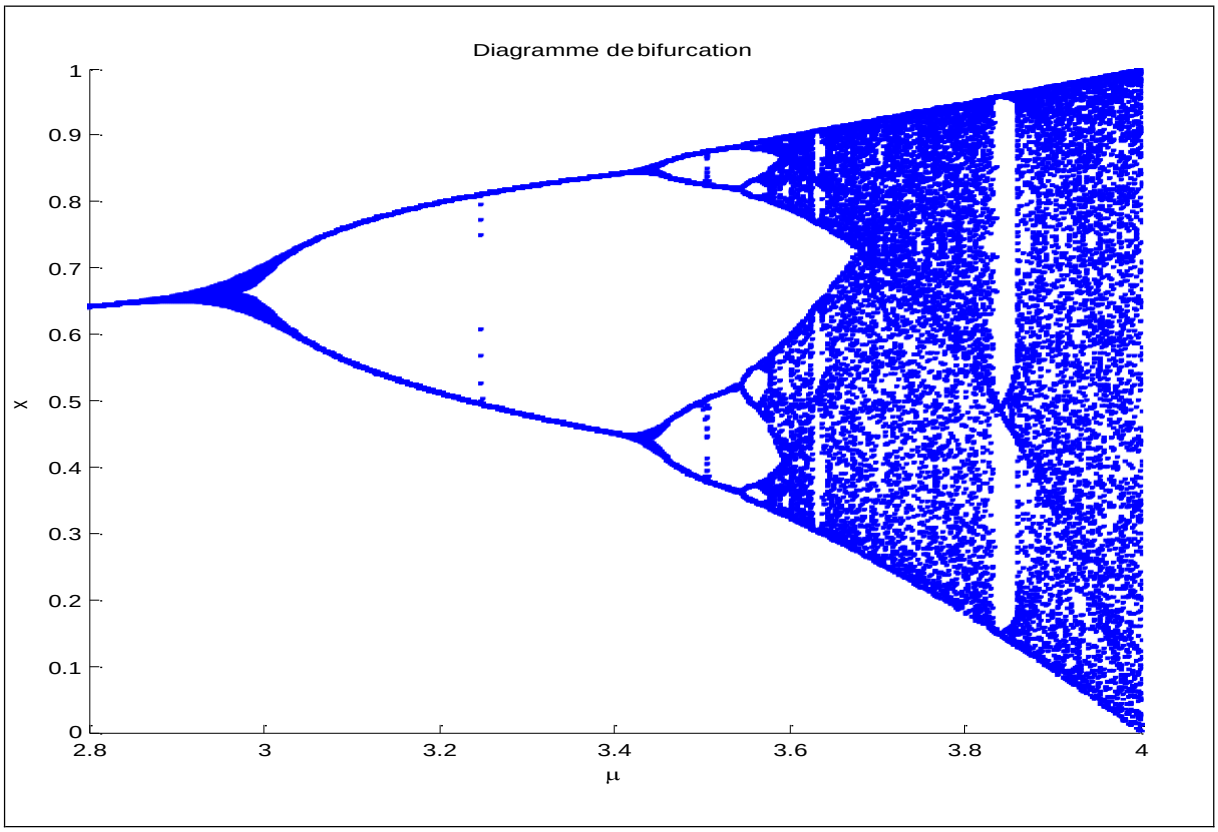

Figure 1.9: Diagramme de bifurcation de la carte logistique [46].

Avant la valeur de μ=3, il n'y a qu'une seule valeur stable, puis, à partir de ce point, le diagramme se divise en deux parties, ensuite, aux alentours de μ = 3.45, les deux branches se dédoublent de nouveau, donnant naissance à 4 branches, puis 8 un peu plus tard et ainsi de suite.

On peut constater que ces dédoublements sont de plus en plus rapprochés, mais surtout qu'à partir de μ = 3.57, la carte logistique va alterner entre une infinité de valeurs, sans période précise : c'est le chaos.

1.3.8.1.3 Exposant de Lyapunov

L'étude de la stabilité ou l'instabilité d'un système dynamique non linéaire a entraîné la création d'exposant de Lyapunov [47] comme étant un outil capable de rendre compte du comportement de l'orbite d'un système dynamique. Poincaré (1890) [48], ainsi l'exposant de Lyapunov est considéré comme un simple issu de déterminer si un système dynamique non linéaire est chaotique ou non. Un système dynamique non linéaire chaotique est caractérisé par son exposant de Lyapunov positif, ce qui prouve sa sensibilité aux conditions initiales [49]. Autrement dit, exposant de Lyapunov présente la divergence de l'écart entre deux trajectoires chaotiques ayants des conditions initiales très voisines. L'exposant de Lyapunov est calculé par la formula mathématique suivante [50] :

$$\lambda = \lim_{n\to\infty} \left(\frac{1}{n}\sum_{i=0}^{n-1} \ln|f'(X_i)|\right) \qquad (1.14)$$

La figure 1.10 ci-dessous présente l'exposant de Lyapunov de la carte logistique :

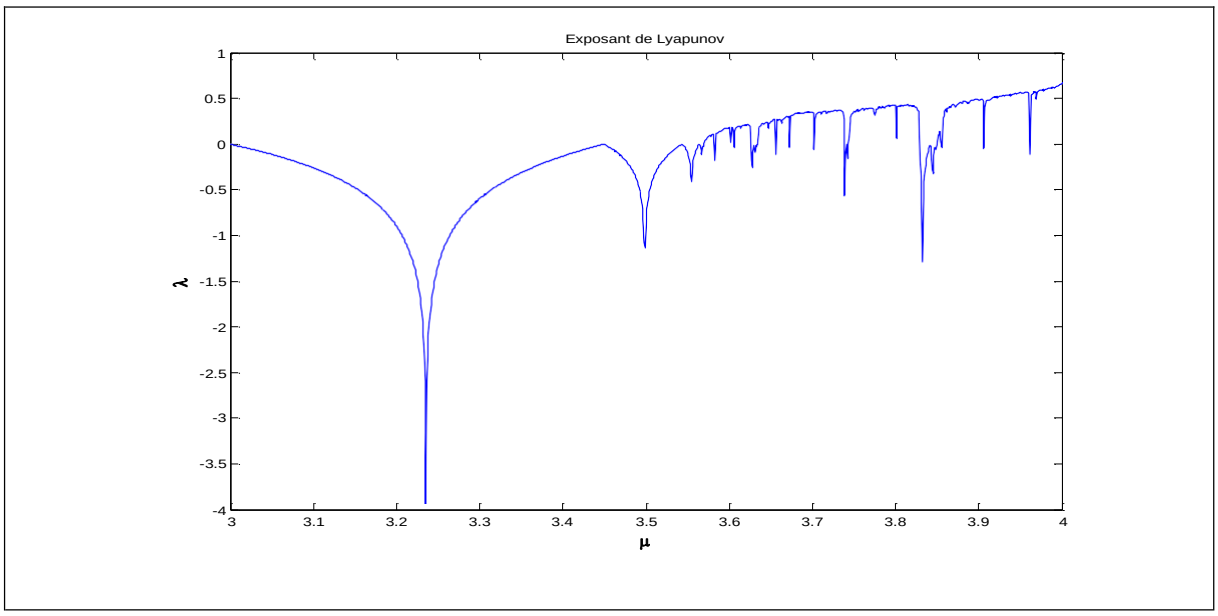

Figure 1.10: Exposant de Lyapunov de la carte logistique.

1.3.8.1.4 Densité de distribution

En cryptographie la distribution des séquences chaotiques générées par des systèmes non linéaires à une grande importance. Le schéma de la figure 1.11 ci-dessous montre la densité de distribution des séquences des nombres réels générés par la carte logistique dans] 0, 1[.

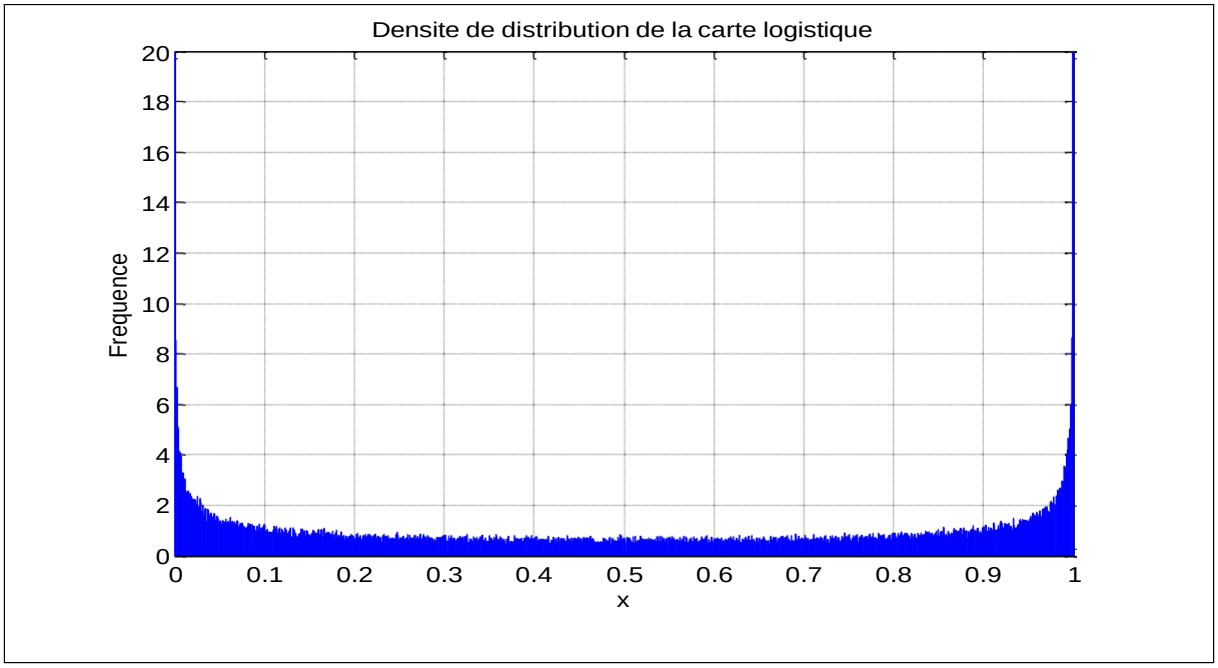

Figure 1.11: Densité de distribution de la carte logistique.

1.3.8.1.5 Sensibilité aux conditions initiales

Nous partons de deux conditions initiales différentes, mais très proches à 10^{-5}, l'erreur augmente de façon exponentielle après les quinze premières itérations. Le schéma de la figure 1.12 ci-dessous montre que les deux orbites X et Y sont identique avant les quinze premières itérations, après l'écart commence à s'élargir.

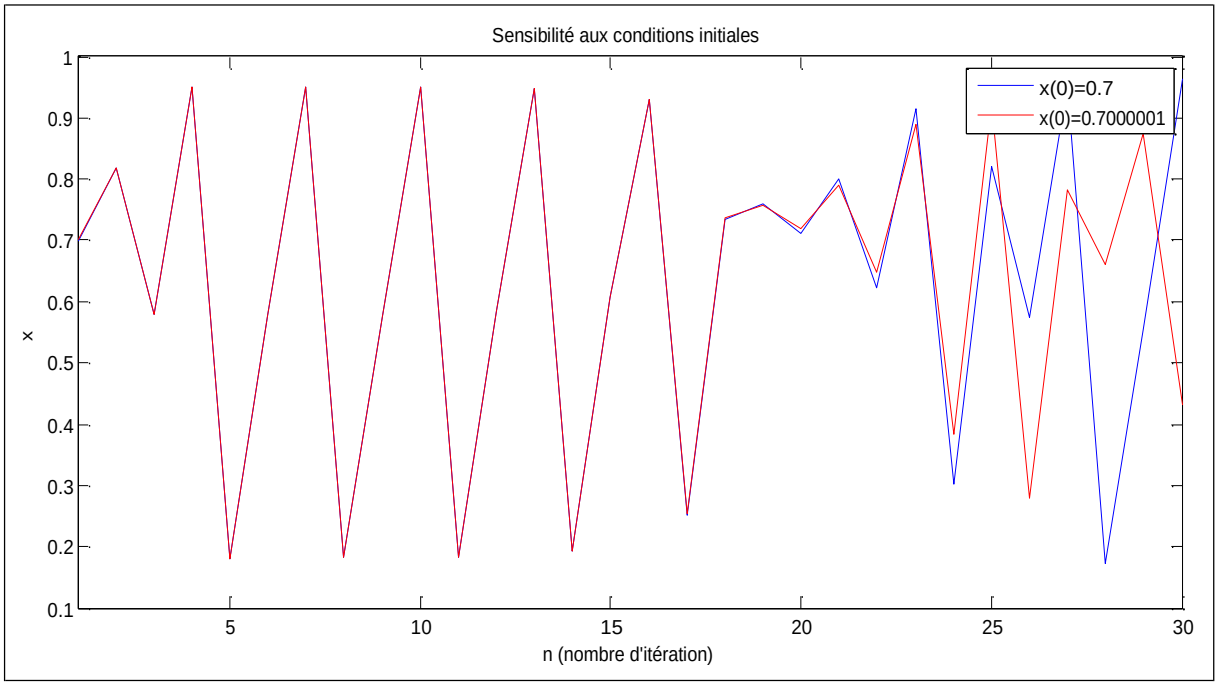

Figure 1.12: Sensibilité aux conditions initiales $\mathbf{x(0) = 0.7;\ x(0) = 0.7000001.}$

1.3.8.2 Carte Sine

La carte Sine est aussi l'un des systèmes dynamiques non linéaire dont le comportement chaotique est similaire à celui de la carte logistique. La carte chaotique Sine est décrite par l'équation suivante [14] :

$$g(X_n) = X_{n+1} = r \sin\ (\pi X_n) \qquad (1.15)$$

avec X présente la variable dynamique prenant des valeurs dans l'intervalle $]0,1[$, $r\epsilon]0,1[$ est le paramètre de contrôle du système non linéaire et X_n est la séquence chaotique de sortie. La figure 1.13 ci-dessous présente le diagramme de bifurcation, l'exposant de Lyapunov, la densité de distribution et la sensibilité aux conditions initiales.

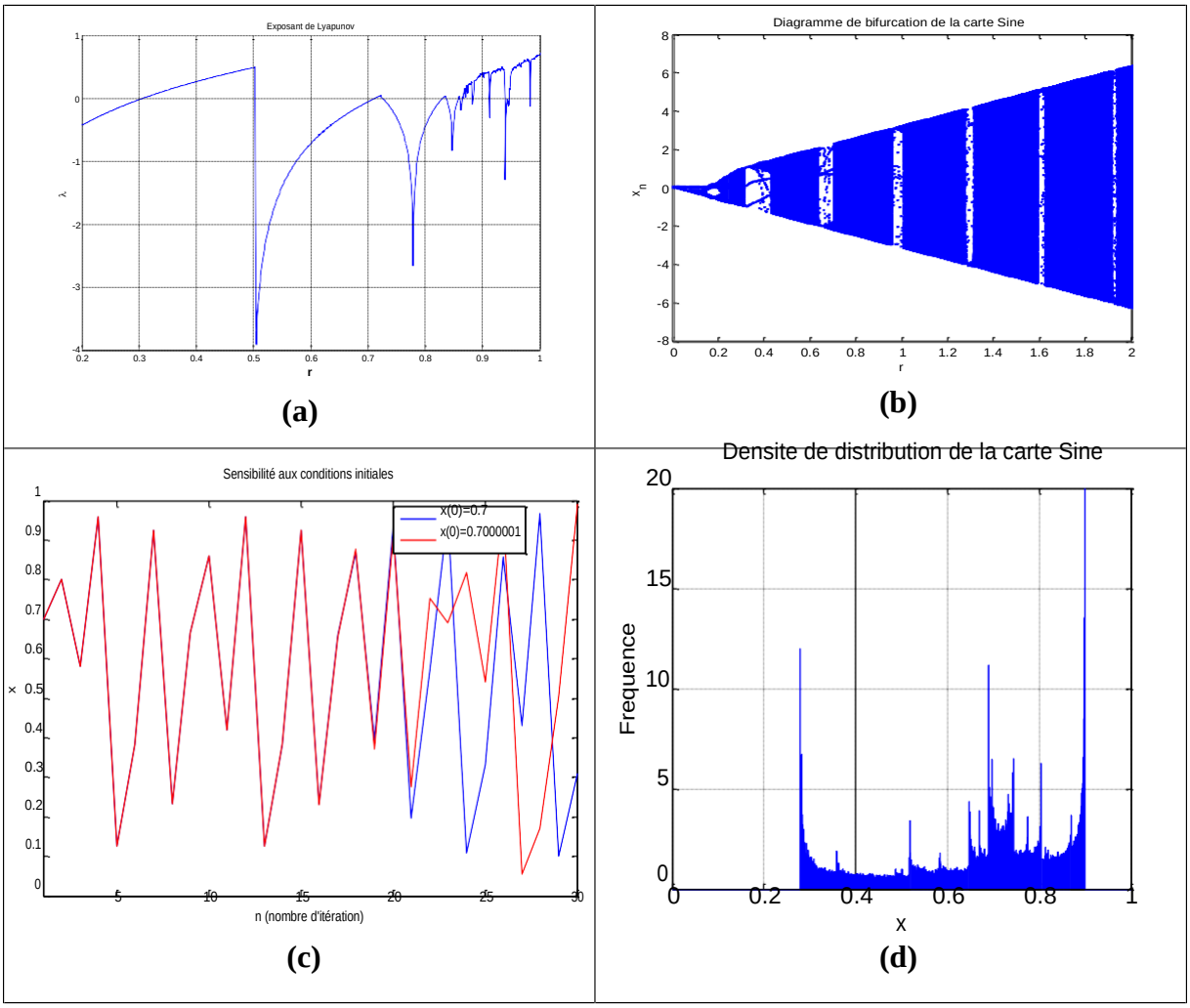

Figure 1.13: (a) : Exposant de Lyapunov ; (b) : Diagramme de bifurcation ; (c) : Sensibilité aux conditions initiales ; (d) : Densité de distribution de la carte Sine.

1.3.8.3 Carte de Tchebychev

La carte Tchebychev fait partie aussi des systèmes chaotiques unidimensionnelles décrite par l'équation suivante [14]:

$$h(X_n) = X_{n+1} = \cos(a \arccos(X_n)) \qquad (1.16)$$

avec X_n présente la variable dynamique prenant des valeurs dans l'intervalle $]0,1[$, $a \epsilon \mathbb{N}$ est le paramètre de contrôle du système non linéaire et X_n est la séquence chaotique de sortie. La figure 1.14 ci-dessous présente le diagramme de bifurcation, l'exposant de Lyapunov, la densité de distribution et la sensibilité aux conditions initiales de la carte Tchebychev.

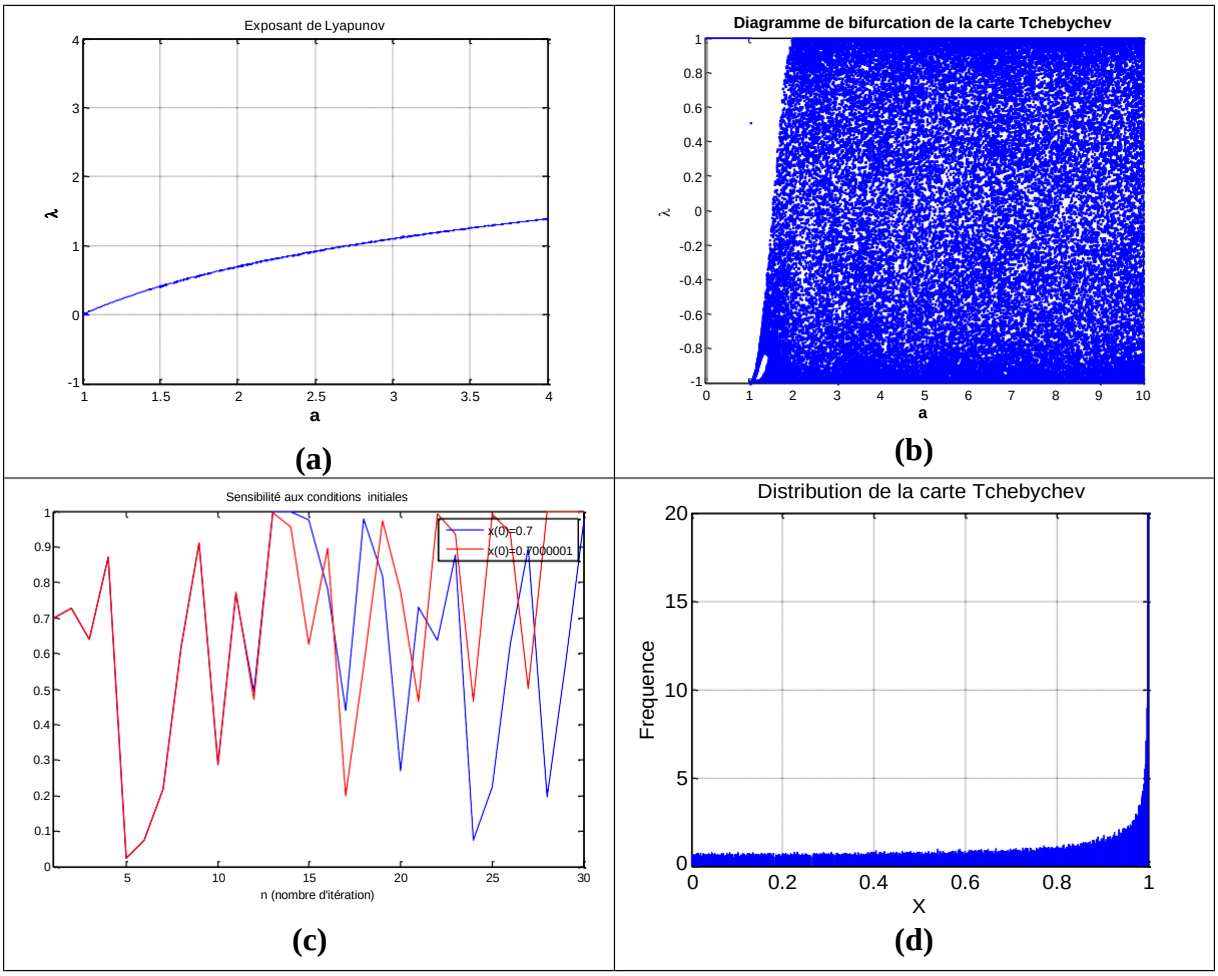

Figure 1.14: (a) : Exposant de Lyapunov; (b) : Diagramme de bifurcation ; (c) : Sensibilité aux conditions initiales ; (d) : Densité de distribution de la carte Tchebychev.

1.3.9 Faiblesses des cartes chaotiques 1D

En général, les cartes logistiques unidimensionnelles sont des systèmes chaotiques populaires caractérisés par leur simplicité, rapidité de mise en œuvre dans les systèmes numériques, et surtout une faible consommation des ressources informatiques. Cependant, ces cartes présentent des faiblesses à savoir, distribution non uniforme, petit espace clé et une périodicité dans l'intervalle chaotique (figures 1.13(b) et 1.14(b)). En effet, les auteurs de [17] [50] ont affirmé que la carte logistique présente certains inconvénients lorsqu'elle est utilisée dans le domaine de la cryptographie, à savoir, des plages chaotiques discontinues, une distribution non uniforme, un espace clé réduit et une périodicité dans les zones chaotiques. Dans le même contexte, plusieurs auteurs ont amélioré avec succès les cartes chaotiques unidimensionnelles pour surmonter ces faiblesses, afin de renforcer la sécurité [15] [18] [14]. Ainsi, Les auteurs de [15], ont proposé un nouveau générateur pseudo-aléatoire basé sur la carte logistique à une seule dimension pseudo-aléatoirement améliorée (PELM), qui produit des

séquences chaotiques avec des propriétés statistiques excellentes. Les auteurs de [18] [15], ont proposé une amélioration fondée sur un entrelacement des cartes logistiques pour renforcer la sécurité et élargir l'espace clé. Les auteurs de [12], ont proposé un nouveau schéma de chiffrement basé sur l'entrelacement de trois cartes logistiques améliorées et l'algorithme de Vigenère.

Dans les travaux présentés dans cette thèse, une amélioration des caractéristiques pseudo-aléatoires de quelques systèmes chaotiques a été effectués. Et ceci, dans l'objectif de créer des systèmes non linéaires capables de produire des séquences chaotiques caractérisées par une uniformité remarquable, une hypersensibilité aux conditions initiales, et surtout des propriétés statistiques excellentes. Les séquences chaotiques ainsi obtenues sont utilisée dans les différentes architectures des crypto systèmes proposés pour les images numériques.

1.4 Etat de l'art

Dans le domaine de sécurité de l'information, la principale différence entre les données format texte et image réside dans la taille. En effet, la quantité d'informations contenues dans l'image [51] est beaucoup plus volumineuse que celles contenues dans les données textuelles, ce qui rend les méthodes de cryptage du texte souvent inapplicable au cryptage des images. Dans ce contexte les systèmes de chiffrement à clé privées tels que DES, AES, BLOWFISH, et ECC [5] [22], ne sont pas efficaces et ne pouvaient pas servir comme systèmes de chiffrement adéquats pour les images numériques en raison de leurs complexité algorithmiques élevée. Par conséquent, les chercheurs ont orienté leur attention vers un système de chiffrement qui devrait offrir les avantages suivants :

1. Espace clé large : l'espace clé doit être suffisamment grand pour résister aux attaques brutales.
2. Forte sensibilité aux conditions initiales : c'est-à-dire un petit changement sur les valeurs initiales devrait produire un changement très élevé.
3. Faible complexité : la complexité du système de chiffrement ne doit pas être très élevée et le temps nécessaire au cryptage/décryptage doit être le minimum possible.
4. Fort effet d'avalanche : Un petit changement dans un bit d'entrée devrait apporter des changements radicaux sur l'image cryptée.
5. Haute sécurité : Robustesse contre les attaques statistiques, différentielle, brutales…etc.
6. Confusion élevée : Aucune corrélation entre les pixels adjacents de l'image cryptée.

Dans cette section, nous présentons une analyse des crypto-systèmes existants dans la littérature pour le cryptage d'image.

1.4.10 Chiffre d'images basé sur le processus de Confusion/Diffusion en utilisant la carte chaotique Skew Tente.

Le comportement dynamique très riche et la bonne combinaison entre la vitesse d'exécution et la haute sécurité des signaux générés par les cartes chaotiques les rend très attractifs pour différentes applications. Dans cette section nous allons introduire un état de l'art sur les principaux algorithmes de chiffrement d'images basés sur l'une des plus fameuses cartes chaotiques appelée Skew Tente utilisée en particulier dans les mécanismes de confusion et diffusion.

Dans ce contexte, les auteurs de [52], ont proposé une nouvelle méthode de chiffrement d'images basée sur la carte chaotique Skew Tente modifiée, dont laquelle les propriétés pseudo-aléatoires sont améliorées afin de produire des meilleures séquences chaotiques qui seront utilisées comme clés de chiffrement et déchiffrement. De plus, dans l'algorithme proposé, les conditions initiales et les paramètres de la carte sont modifiés pendant le chiffrement (car ils dépendent à la fois de l'image originale et de l'image chiffrée), ainsi que la grande sensibilité aux conditions initiales et des paramètres de contrôle. Ce qui offre un algorithme de cryptage très sécurisé.

Dans la référence [53], les auteurs ont conçus un nouvel algorithme de chiffrement d'image basé sur une matrice orthogonale, la carte chaotique, la carte Skew Tente, et l'opérateur logique XOR. Dans ce travail les auteurs ont raffiné la technique présentée par Fawad et al. [54], pour satisfaire les besoins sécuritaires nécessaires d'une image. Les auteurs affirment qu'après une vaste analyse de plusieurs paramètres à savoir : l'inspection visuelle, le coefficient de corrélation, l'entropie, le NPCR, et l'UACI, la technique proposée présente une forte résistance contre les attaques connues à savoir l'attaque brutale, différentielle et statistique. De plus, la technique satisfait bien le processus de diffusion, et les résultats de simulation obtenus sont meilleurs comparés à d'autres techniques récentes.

Dans la référence [13], une nouvelle technique de chiffrement d'image rapide et sécurisée a été proposée. Les auteurs ont introduit trois versions du crypto système basé chaos qui utilise une structure similaire à celle proposée par Zhang et Fridrich [55] [56], dont chaque version est composée de deux couches : une couche de confusion et une couche diffusion. En effet, la couche de confusion est obtenue en utilisant une carte cat. 2D modifiée pour surmonter le

problème du point fixe, pour surmonter certaines autres faiblesses et surtout pour augmenter l'espace de clé dynamique utilisé dans le crypto-système proposé. La première version utilise une carte logistique 32 bits comme couche de diffusion ce qui présente une forte robustesse par rapport à la carte logistique 8 bits. Dans les autres versions, la carte logistique est remplacée par une Carte Skew Tente Finie (CSTF) pour trois raisons : pour augmenter les propriétés de non-linéarité de la couche de diffusion, pour résoudre le problème du point fixe et surtout pour augmenter l'espace clé dynamique. Enfin, toutes les versions du crypto-système proposé sont plus résistantes aux attaques connues et plus rapides que ceux proposés par Zhang. De plus, l'espace clé dynamique utilisé est beaucoup plus grand que celui employé dans les crypto-systèmes proposés dans les références [55] [56]. L'analyse des performances et de sécurité montre que les systèmes cryptographiques proposés sont souhaitables à des applications en temps réel.

Ghebleh and Kanso [57] ont fourni un nouveau procédé pour chiffrer et déchiffrer les images couleur et niveau de gris. Le travail intitulé 'nouveau schéma efficient de cryptage d'image basé sur des cartes Skew Tente chaînées', est basé sur une carte Skew Tente chainée comme générateur pseudo-aléatoires qui sert à générer les séquences chaotiques utilisées dans le processus de chiffrement. En effet, le schéma proposé comprend des opérations de décalage et de mixage étalées en plusieurs rounds pour renforcer la sécurité. Les auteurs affirment qu'une analyse des résultats de simulation démontre des performances élevées du schéma proposé. En outre, le schéma proposé montre des performances supérieures comparées aux autres schémas de cryptage d'image similaires existants, surtout en ce qui concerne les attaques différentielles.

Un nouvel algorithme de chiffrement d'image en couleur basé sur la carte Skew Tente et l'hyper système chaotique du 6 ordre CNN a été proposé dans la référence [58]. Le processus de chiffrement est basé sur la confusion et la diffusion des pixels de l'image originale, la carte Skew Tente est utilisée pour générer la séquence de confusion, tandis que, l'hyper système chaotique du sixième ordre CNN est appliquée pour générer celle de diffusion, pour 6 variables d'état du système (les paramètres de contrôle et les conditions initiales), il y a au total 120 combinaisons. Pour chaque pixel de plain image, une combinaison est choisie pour le chiffrement des trois canaux de couleurs à savoir : rouge, vert et bleu, et la combinaison est déterminée par l'une des variables d'état. Chaque pixel est chiffré par son antécédent et la valeur de combinaison du système CNN.

Les auteurs de l'article [59] ont conçus un nouvel algorithme de chiffrement d'image qui utilise respectivement deux cartes chaotiques, la carte 2D de Henon [60] et la carte Skew Tente pour les processus de permutation et diffusion. Pour ajouter d'autres caractéristiques de sécurité, les auteurs ont appliqué également la S-Box proposé dans l'article [61], pour substituer chaque pixel de l'image claire par un nouveau pixel aléatoire. Les auteurs affirment qu'une analyse approfondie de la sécurité et de la résistance aux attaques statistiques prouvent l'efficience et l'efficacité du schéma proposé.

Les auteurs de l'article [62], ont conçu un nouvel algorithme chaotique qui utilise la carte lattices couplée avec un 'time-delay' pour le chiffrement d'image basé sur l'architecture substitution/ diffusion. Les auteurs ont employé la carte Skew Tente pour mixer les positions des pixels de l'image, puis la carte lattices couplés (DCML) pour appliquer une confusion de la relation entre l'image claire et chiffrée. Dans le mécanisme de génération des clés, un délai dynamique dans le temps est également intégré dans le schéma proposé pour le rendre plus sécurisé.

Dans l'article [63], une approche du cryptage des images couleurs basée sur des cartes chaotiques Skew Tente afin de répondre aux exigences du transfert sécurisé sur des canaux de communication non fiables. Dans le schéma de chiffrement proposé, une clé secrète externe de taille 128 bits et deux cartes chaotiques Skew Tente sont utilisées. Les conditions initiales des deux cartes sont dérivées à partir d'une clé secrète externe. Les auteurs affirment que les résultats expérimentaux en termes d'analyses statistiques et de sensibilité aux clés de chiffrement, prouvent que le schéma de cryptage proposé constitue un moyen efficace et sûr de cryptage et de transmission.

1.4.11 Chiffre d'images à l'aide d'un système chaotique 3D et le chiffre dynamique de Vigenère.

Le chiffrement de Vigenère (CV) [64], est un crypto système symétrique, ce qui signifie qu'il utilise la même clé pour le chiffrement et le déchiffrement. Le cryptage des données numériques par le CV ressemble beaucoup au système de chiffrement de César, à la différence près qu'il utilise une clé plus longue afin de pallier le principal problème du chiffrement de César dont sa faiblesse réside dans le fait qu'une lettre puisse être codée d'une seule façon. Pour cela on utilise un mot clé au lieu d'un simple caractère. D'une manière générale, l'algorithme de chiffrement Vigenère utilisant un tableau carré appelé le carré de Vigenère sous forme d'une matrice carrée de taille 26×26 (Figure 1.7). Au cours des dernières années, plusieurs chercheurs

ont développé des travaux basés sur le CV et les systèmes chaotiques pour Crypter/Décrypter les données numériques.

S. Li et al. [65], ont proposé une technique de cryptage d'image basée sur le concept de CV, mais l'un des problèmes majeurs du schéma proposé était sa vulnérabilité aux attaques statistiques, une cryptanalyse a été réalisée par Y. Zhang et son équipe [66], confirme la vulnérabilité du schéma proposé dans le travail présenté dans l'article [65], et cela après une analyse basée sur une attaque à texte clair choisi et une attaque différentielle. En outre, Les auteurs ont démontré que la clé utilisée peut être révélée facilement. D'autres faiblesses sont présentées dans [65], telles que l'usage d'une carte logistique unidimensionnelle et l'utilisation de la table de Vigenère traditionnelle.

En 2016 Les auteurs de l'article [12], ont développé un schéma de chiffrement d'images basé sur les cartes chaotiques et le CV. Les auteurs affirment que le mécanisme de chiffrement repose sur deux étapes principales : La diffusion et la confusion, la première étape comporte trois niveaux à savoir une diffusion antérieure, une application de CV suivi d'une diffusion postérieure. Tandis que la confusion utilise des cartes chaotiques entrelacées pour permuter les pixels de l'image originale.

Les auteurs du travail intitulé cryptage d'images numérique par le CV basé sur le mixage des cartes chaotiques [67], proposent une technique de chiffrement qui consiste à mettre l'image sous forme d'un vecteur, ensuite appliquer directement le CV comme il a été défini dans les travaux suivants [68] [69]. Dans ce cas, l'image sera découpée en blocs, chaque bloc est une ligne ou une colonne de la matrice image. Les auteurs ont affirmé que ce choix a été effectué afin que l'application de CV ne perde pas sa robustesse vis-à-vis la taille de la matrice image et pour chaque bloc de taille N (avec N un entier positif), ensuite une séquence aléatoire α de dimension N + **K** – 1 sera générée (**K** est un entier positif).

Les auteurs de l'article [70], ont développé une technique de chiffrement d'image basée sur le CV avec décalage circulaire des bits, ils ont testé leur technique sur des images couleurs et niveau de gris, et ils ont affirmé son efficacité et sa robustesse.

Les auteurs de l'article [65], ont développé un algorithme de cryptage d'images basé sur la théorie du chaos et le chiffrement Vigenère. Le processus de chiffrement s'effectue sur le niveau de gris de chaque pixel en triant la séquence chaotique en tant que CV. Après une analyse des simulations les auteurs ont affirmé la validité et l'efficience du schéma proposé.

Dans l'article [71], les auteurs ont abordé une nouvelle technique de chiffrement hybride basée sur le CV qui a pour objectif de rendre ce dernier plus robuste. La méthode utilise une transposition des colonnes, ensuite applique le CV sur le texte transposé. Les auteurs, affirment qu'une analyse cryptographique des paramètres de sécurité a été effectuée sur le texte chiffré et a prouvé la robustesse de la méthode proposée.

1.4.12 Méthode basée sur une nouvelle variante sécurisée de CH et cartes chaotiques 1D

Le chiffre de Hill [33] [34], est une méthode de cryptage linéaire assuré par une matrice carrée inversible de taille n×n à coefficients dans l'anneau $\mathbb{Z}/26\mathbb{Z}$. En effet, après la décomposition du texte clair en blocs de taille n (avec n un entier strictement supérieur à zéro), le texte chiffré est l'image de chaque bloc par la matrice clé. Le CH conventionnel utilise comme clé une matrice carrée d'ordre 2×2 qui, généralement, n'est inversible que si son déterminant est inversible. En effet, si la matrice clé n'est pas inversible, le texte crypté ne peut pas être retrouvé. Le CH présente une résistance contre toute attaque statistique, et attaque brutale. Mais, il est vulnérable aux attaques à texte clair choisi KPCA [72], ceci est dû à la linéarité de l'algorithme. Un autre revers pour le cryptage des images est qu'il révèle certaines tendances et ne cache pas toutes les caractéristiques de l'image (images avec des fonds homogènes) et n'est pas efficace pour les images qui présentent un fond noir. Afin de surmonter ce problème et d'améliorer le CH, plusieurs travaux de recherches ont été publiés.

Les auteurs de [73], ont proposé une nouvelle approche qui sert à intégrer une image dans une autre image en utilisant la méthode de CH modifiée. L'image secrète est réarrangée pour former N matrices 2×2 (avec n un entier strictement supérieur à zéro). Ensuite, une matrice clé de Hill d'ordre 2×2 est multipliée par toutes les N matrices générées, et cela dans $\mathbb{Z}/265\mathbb{Z}$.

Les auteurs de [74], ont proposé une amélioration de CH baptisée HC-PRE (Hill Cipher Modification based on Pseudo-Random Eigenvalues), cette technique utilise des valeurs propres pseudo-aléatoires pour générer des matrices clés dynamiques.

Les auteurs de l'article [75], ont proposé une méthode qui simplifie le calcul de la matrice inversible utilisée pour le déchiffrement, cependant cette technique reste encore vulnérable aux attaques à texte clair/choisi connu.

Les auteurs de l'article [76], ont proposé un algorithme de chiffrement de Hill modifié qui utilisait une matrice clé à usage unique pour chiffrer chaque bloc du texte clair. Dans cet

algorithme, chaque bloc est chiffré en utilisant sa propre clé, cette clé unique est calculée en multipliant la clé actuelle par un vecteur initial secret (IV). L'opération de multiplication est effectuée ligne par ligne, ainsi l'algorithme est nommé Hill Multiplying Rows by Initial Vector (Hill MRIV). Les auteurs ont affirmé que l'algorithme donne un excellent chiffrement des données. Cependant, les auteurs de l'article [72], ont prouvé que l'algorithme est toujours vulnérable à l'attaque à texte claire connu. En outre, Ismail et al. [76], n'ont pas abordés le problème d'utilisation des matrices clés non inversibles qui peuvent conduire à un échec du décryptage.

Les auteurs de l''article [77], ont traité la sécurité d'une image RGB en utilisant le CH combiné avec la transformée en ondelettes discrète, et ils ont choisi la matrice involutive comme clé de chiffrement. Afin de surmonter ce problème, plusieurs articles ont été publiés [77] [78] [79] [80], qui utilisent des matrices involutives. Mais, ce choix risque de rendre l'algorithme vulnérable aux attaques exhaustives [81], faute du faible cardinal de l'ensemble des matrices involutives (car une matrice d'ordre n×n génère n ! matrice involutives) [80]. Les auteurs de l'article [72], ont proposé une amélioration de CH baptisée HILLMRIV, basée sur une matrice clé dynamique. Cette technique modifie chaque ligne de la matrice clé en multipliant la clé courante par un vecteur secret initial. Les auteurs affirment que l'algorithme donne des résultats satisfaisants et une robustesse contre les attaques connues. Mais, il est encore vulnérable aux attaques à texte clair choisi. En 2009 et 2011 les auteurs de [81] [76], ont présenté deux variantes du CH (Toorani-Falahati Hill Ciphers : TFHC1 et TFHC2), ainsi que les protocoles d'échange des messages cryptés. Ces deux variantes utilisent une fonction de hachage unidirectionnelle pour modifier le processus du chiffrement pour chaque texte clair, les auteurs prétendent bien que les deux variantes de CH sont sécurisées contre toute attaque connue. Toutefois, TFHC1 et TFHC2 sont vulnérables contre une attaque à texte clair choisi, ce résultat a été confirmé dans l'article [82].

Les auteurs de [24], ont proposé une nouvelle technique pour générer une matrice auto-inversible utilisée dans le CH. Leur objectif principal est de surmonter le problème d'utilisation d'une matrice clé quelconque, car le message chiffré ne peut pas être déchiffré si la matrice n'est pas inversible. Les auteurs ont affirmé que la complexité de calcul peut être réduite en évitant le processus de recherche de l'inverse de la matrice au moment du décryptage, car ils utilisent une matrice clé auto-inversible pour le chiffrement.

Les auteurs du travail [83], ont également proposé un algorithme de chiffrement avancé de Hill baptisé « AdvHill » capable de résoudre le problème de matrice clé non inversible. Pour

s'assurer que chaque bloc du texte chiffré peut être déchiffré, une matrice clé involutif est utilisée pour le chiffrement. Une matrice clé involutive est une clé qui peut être utilisée pour le chiffrement et le déchiffrement. Cela signifie qu'une matrice clé inverse n'est pas nécessaire pour le déchiffrement, ce qui simplifie définitivement la complexité de calcul et économise le temps de calcul. Cependant, cet algorithme contient encore certains inconvénients majeurs du code de Hill original, tels que la vulnérabilité à l'attaque connue en clair. En outre, cet algorithme ne convient pas non plus pour chiffrer le texte en clair tout en zéro puisque C sera toujours égal à zéro lorsque P est égal à zéro.

1.5 Conclusion

Le fort besoin de confidentialité de la vie personnelle reste toujours en nette progression. Pour cette raison plusieurs chercheurs dans le domaine de cryptographie ont développé des crypto-systèmes robustes pour réaliser ces besoins. Dans ce premier chapitre des généralités sur la cryptographie ont été introduites, ensuite, nous avons détaillé la cryptographie chaotique, avec une description des propriétés chaotiques de quelques carte 1D et leurs points faibles, en fin, nous avons donné un état de l'art de quelques crypto-systèmes existants dans la littérature pour le cryptage des images numériques similaires aux techniques proposées dans la suite de cette thèse.

Chapitre 2

Chiffrement d'images basé sur le processus de Confusion/Diffusion en utilisant la carte chaotique Skew Tente améliorée.

Sommaire

2.1 Introduction

Actuellement, le trafic des données numériques sur les canaux de transmission non sécurisés augmente rapidement. La protection des données numériques, en particulier, des images considérées comme des données particulières en raison de leurs propriétés intrinsèques à savoir, la forte corrélation, la redondance des pixels et la taille volumineuse, devient une nécessité incontournable pour de nombreuses raisons telles que la confidentialité et l'intégrité. Ainsi, la façon la plus habituelle de répondre au problème de sécurité est le chiffrement. En guise d'une recherche en littérature, nous remarquons que plusieurs chercheurs ont constaté qu'il existe un lien étroit entre le chaos et la cryptographie [35]. Les systèmes chaotiques sont caractérisés par leur ergodicité, et surtout leur sensibilité aux conditions initiales et aux paramètres de contrôle pour garantir la sécurité souhaitée des données communiquées. De telles caractéristiques ont suscité l'intérêt des chercheurs à développer de nombreux systèmes de chiffrement d'image à base des systèmes dynamiques chaotiques.

Dans ce chapitre, nous nous focalisons sur une analyse des performances pseudo-aléatoires de la carte Skew Tente améliorée par rapport à l'originale. Puis, on met l'accent sur la mise en œuvre de cette carte dans le processus de confusion/diffusion adopté, suivi des différentes analyses de sécurité.

2.2 Carte Skew Tente

La carte Skew Tente est un simple système dynamique non linéaire avec un comportement chaotique complexe. C'est l'une des cartes chaotiques les plus utilisées, elle est exprimée par l'équation suivante [58]:

$$X_{n+1} = \begin{cases} \dfrac{X_n}{b}, & \text{for } 0 < X_n \leq b \\ \dfrac{1 - X_n}{1 - b}, & \text{for } b < X_n < 1 \end{cases} \qquad (2.1)$$

où $X_{n+1} \epsilon [0,1]$ est l'état du système chaotique, $b \epsilon [0.5,1[$ est le paramètre de contrôle et $X_n \epsilon [0,1]$, avec n est le nombre d'itérations utilisé pour générer la séquence chaotique. Pour résoudre les problèmes mentionnés dans le chapitre 1, nous avons amélioré l'aspect pseudo-aléatoire des séquences générées par la carte Skew Tente classique par une simple

multiplication par 10^5 et une application de l'arithmétique modulaire (mod 1). Ainsi, la carte Skew Tente améliorée est indiqué dans l'équation suivante :

$$X_{n+1}= \begin{cases} \mathrm{mod}\left(\left(\left(\frac{X_n}{b}\right)\times 10^5\right),1\right), & \text{for } 0 < X_n \le b \\ \mathrm{mod}\left(\left(\left(\frac{1-X_n}{1-b}\right)\times 10^5\right),1\right), & \text{for } b < X_n < 1 \end{cases} \qquad (2.2)$$

Pour tester la propriété de la carte Skew Tente améliorée en termes d'exposant de Lyapunov, de densité de distribution et de bifurcation, plusieurs simulations et analyses ont été effectuées (voir figures. 2.1, 2.2 et 2.3). Déterminer si un système dynamique non linéaire est chaotique dépend du calcul du λ. La figure 2.1 ci-dessous montre les exposants de Lyapunov de Skew Tente originale (courbe en bleu) et améliorée (courbe en rouge).

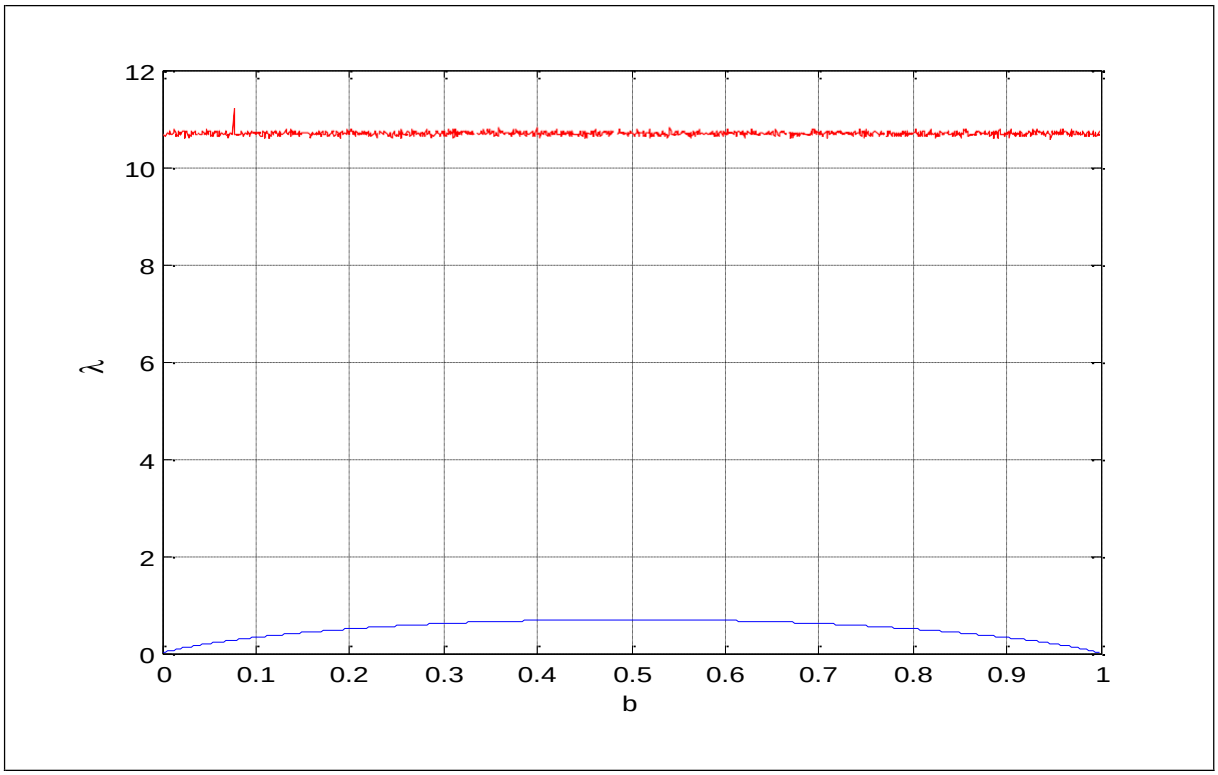

Figure 2.1: Exposant de Lyapunov de la carte Skew Tente (en bleu) et celui de la carte améliorée (en rouge).

Nous pouvons observer dans la figure 2.1 que l'exposant de Lyapunov est assez grand pour la carte améliorée. Par conséquent, le système chaotique amélioré présente une divergence plus élevée et plus rapide entre deux trajectoires chaotiques ayant des conditions initiales très voisines.

Du point de vue de la cryptographie, un bon générateur pseudo-aléatoire doit produire des séquences chaotiques à distribution uniforme. La figure 2.2 ci-dessous montre les densités de distribution de la carte Skew Tente originale et améliorée.

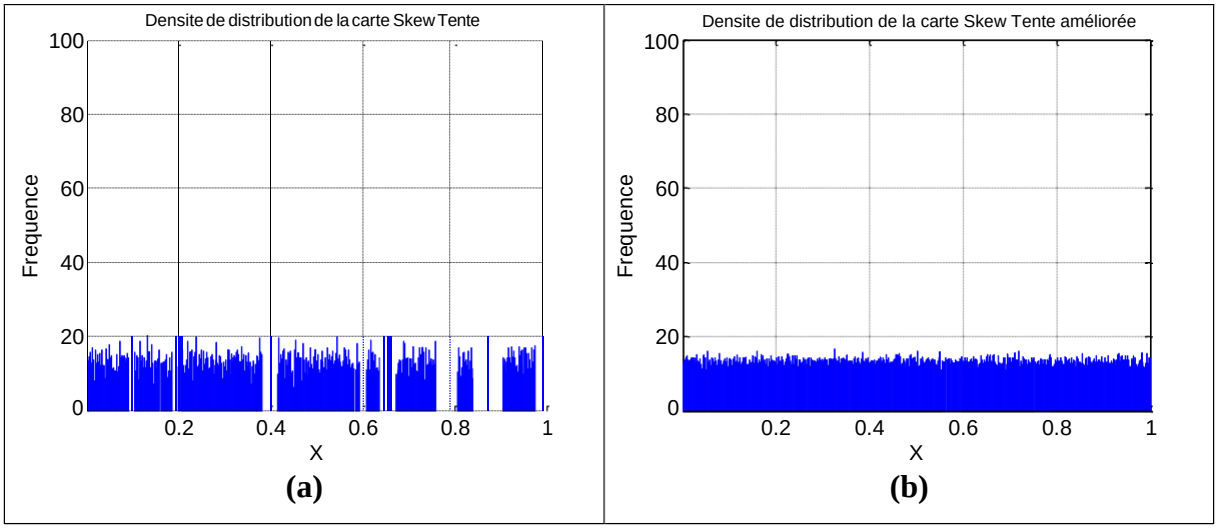

Figure 2.2: Densité de distribution de : a) carte Skew Tente ; b) carte Skew Tente améliorée.

La figure 2.2 montre les densités de distribution des deux cartes chaotiques, on peut observer qu'elles sont uniformément distribuées. Une analyse qualitative de la carte Skew Tente peut être réalisée en étudiant son diagramme de bifurcation, qui représente le comportement asymptotique d'un système dynamique discret en fonction du paramètre de contrôle. La figure 2.3 ci-dessous montre les diagrammes de bifurcation des deux cartes.

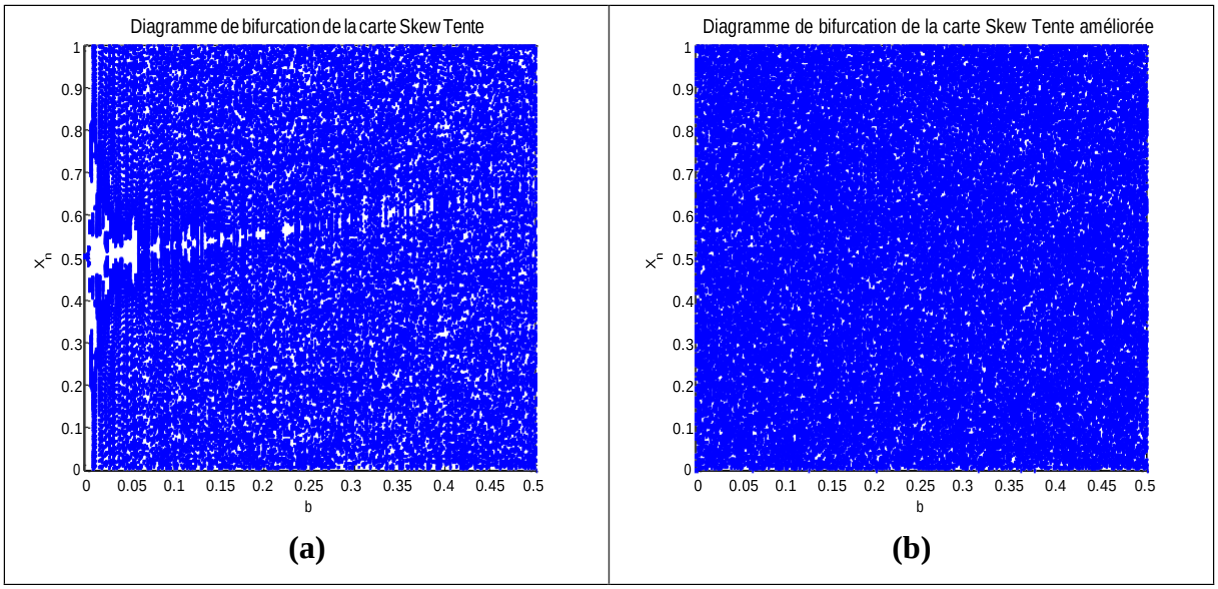

Figure 2.3: Diagramme de Bifurcation de : (a) Carte Skew Tente ; (b) Carte Skew Tente améliorée.

Après avoir comparé les propriétés statistiques des systèmes chaotiques, nous avons constaté que la carte Skew Tente améliorée était plus favorable. En effet, dans la suite de ce travail, nous avons adopté les séquences pseudo-aléatoires issues de la carte améliorée dans le processus de Confusion/Diffusion utilisé dans notre schéma.

2.3 Description du schéma proposé

2.3.1 Génération des clés de permutation

Dans un premier temps, un vecteur chaotique $X=\{X_i, \ldots, X_{255}\}$ de taille 256 est généré à partir de la carte Skew Tente améliorée sous forme de nombres réels dans l'intervalle]0, 1[, puis une séquence d'entier sera créée après un tri croissant des indices de X. Dans la technique proposée, les blocs choisis sont de taille 256, par conséquent la clé de permutation **K** sera comme suit : $K=\{K_i,i=0, \ldots, 255\}$. La figure 2.4 ci-dessous montre la génération d'une clé de permutation de taille 1 × 8 :

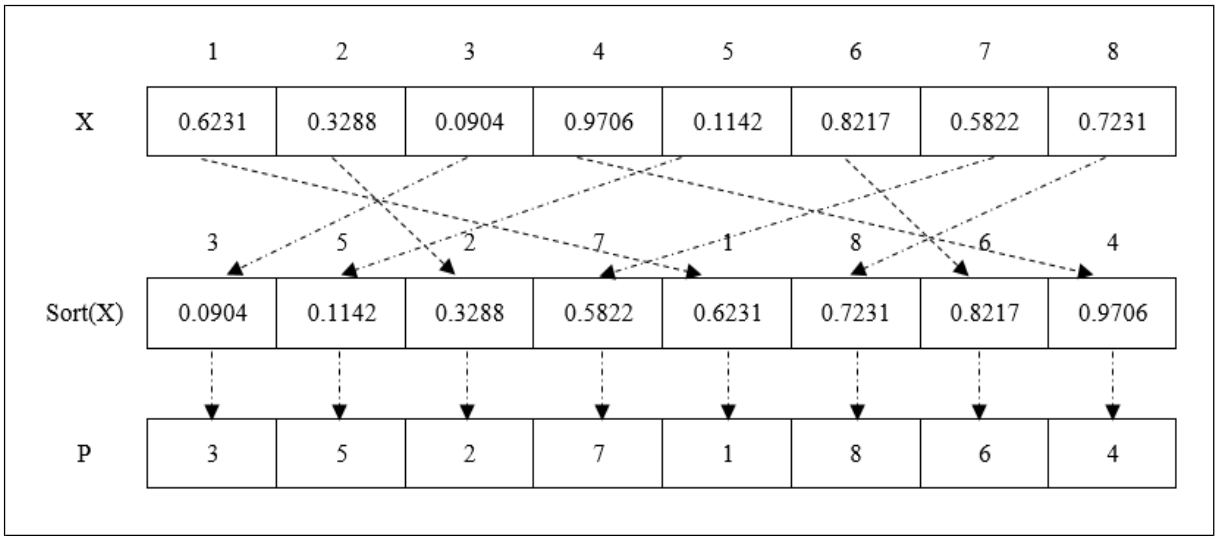

Figure 2.4: Génération d'une clé de permutation de taille 1×8.

2.3.2 Algorithme de chiffrement

Considérons une image couleur P de dimension H×W, avec H étant la hauteur et W la largeur. L'image est divisée en 1×256 blocs. Chaque bloc est crypté comme suit :

- **Étape 1 :** Attribuer un indice à chaque pixel du bloc.
- **Étape 2 :** Choisir une valeur initiale (VI) de la clé **K**.
- **Étape 3 :** Affecter un nouvel indice au premier pixel à l'aide de l'équation suivante :

$$I_0=VI \oplus P_0 \quad (2.3)$$

avec P_0 présente le premier pixel de l'image claire et $\oplus$ est l'opérateur XOR.

- **Étape 4 :** Cryptage du premier pixel à l'aide de l'équation suivante :

$$C_0=K[I_0] \quad (2.4)$$

- **Étape 5 :** Attribuer un nouvel indice aux autres pixels à l'aide de l'équation suivante :

$$I_i=C_{i-1} \oplus P_i \quad (2.5)$$

- **Étape 6 :** Chiffrer les autres pixels à l'aide de l'équation suivante :

$$C_i=K[I_i] \quad (2.6)$$

avec j=1, 2, ...,255. Le diagramme de la figure 2.5 ci-dessous illustre le principe de notre technique :

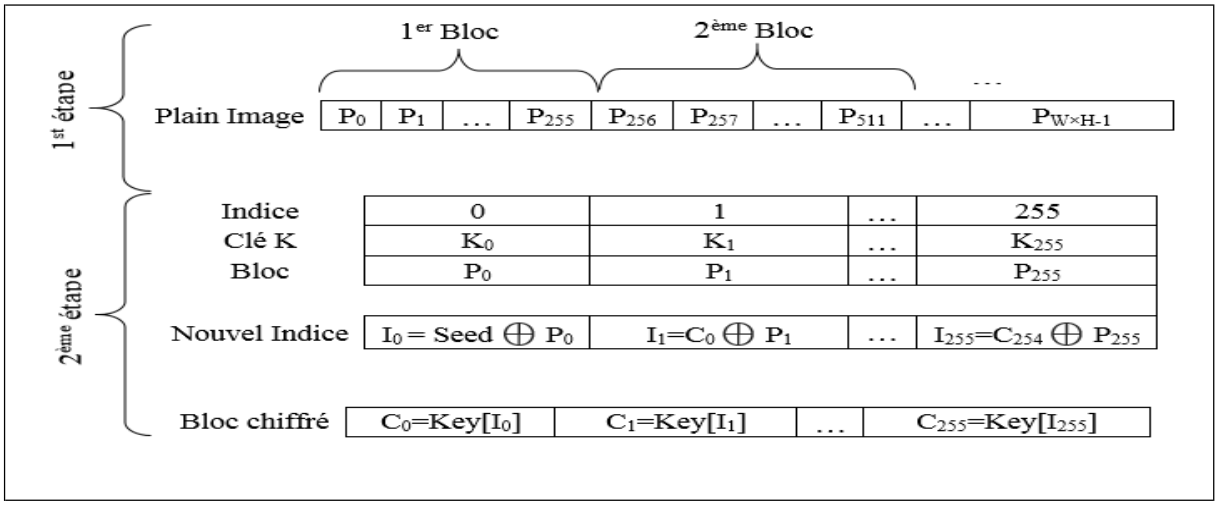

Figure 2.5: Diagramme du crypto système proposé.

Où P_0 est le premier pixel de l'image claire, I_0 est le nouvel indice du premier pixel, C_0 est le premier pixel de l'image chiffrée et j = 1, …, 255. L'algorithme ci-dessous, décrit les étapes citées pour chiffrer l'image claire P.

Algorithme de chiffrement

```
Integer: New_index[0]←VI ⊕ P[0];
 Integer j← 0;
 Pour i← 0 jusqu'à H × W − 1
      C[i]←
      Key[New_Index[j]]; j←j+1
      si (j=256) alors
            j←0
      fin
      New_Index[j]←P[i+1] ⊕ C[i]
Fin
```

2.3.3 Algorithme de déchiffrement

Le processus de déchiffrement s'effectue à travers les étapes décrites dans le mécanisme du chiffrement en ordre inverse. En effet, le déchiffrement commence par le dernier jusqu'au deuxième pixel, par l'algorithme suivant :

Algorithme de déchiffrement

```
Integer: New_index←0, p, j←255,
         B←1;  q← (H × W )/256;
 Pour i← H × W − 1 jusqu'à 1
      New_Index← indiceTab(Key,C[(q-B)×256+j]);
      P[i]← New_Index XOR C[i-1]
            j←j-1 si
            (j=-1)
                  j←255
                  B←B+1
            fin
fin
```

```
Fonction indiceTab (Entier Array [ ], Entier Key)
        Entier returnValue= -1
        Pour i←0 jusqu'à 255 si
          (key = array[i])
                Value = i;
                Sortir;
          fin
         fin
retourne Value;
```

Le premier pixel est obtenu par l'instruction suivante :

$$P_0=VI \oplus C_1 \qquad (2.7)$$

2.4 Résultats expérimentaux et analyses

Dans cette section, nous allons valider notre crypto système en termes d'espace clé, histogramme, entropie, coefficient de corrélation, NPCR et UACI. Toutes les simulations de ce travail ou des travaux présentés dans les deux chapitres suivants, sont effectuées sur un ordinateur personnel. Le tableau 2.1 présente l'environnement matériel, logiciel et la source des images niveau de gris et couleurs utilisées.

Specifications	
Processor	Intel ® Core™ i5-2430M CPU 2.4GHZ
RAM	4GB
Operating system	Windows 8 professional
Programming language	JAVA
Image source	USC-SIPI image data base [84] Uncompressed Color Image Database (UCID) [85]

Tableau 2.1 : Spécifications des simulations.

2.4.1 Test visuel

Un système de chiffrement performant doit assurer une forte sécurité contre tout sorte d'attaque, et pour tout type d'image couleur ou niveau de gris. Le test visuel, est la première évaluation à effectuer sur l'image cryptée. Un système de chiffrement performant doit produire une image cryptée qui ne porte aucune information sur l'image originale. Autrement dit, une tentative d'attaque ne devrait pas pouvoir trouver une relation entre l'image originale et l'image chiffrée. Après des simulations sur un ensemble d'images issues des bases de données USC-SIPI et UCID, nous remarquons clairement que le schéma de chiffrement proposé est capable de crypter correctement les images niveau de gris ou de couleur et même celles dont les pixels sont fortement corrélés. La figure 2.6 montre les résultats des simulations.

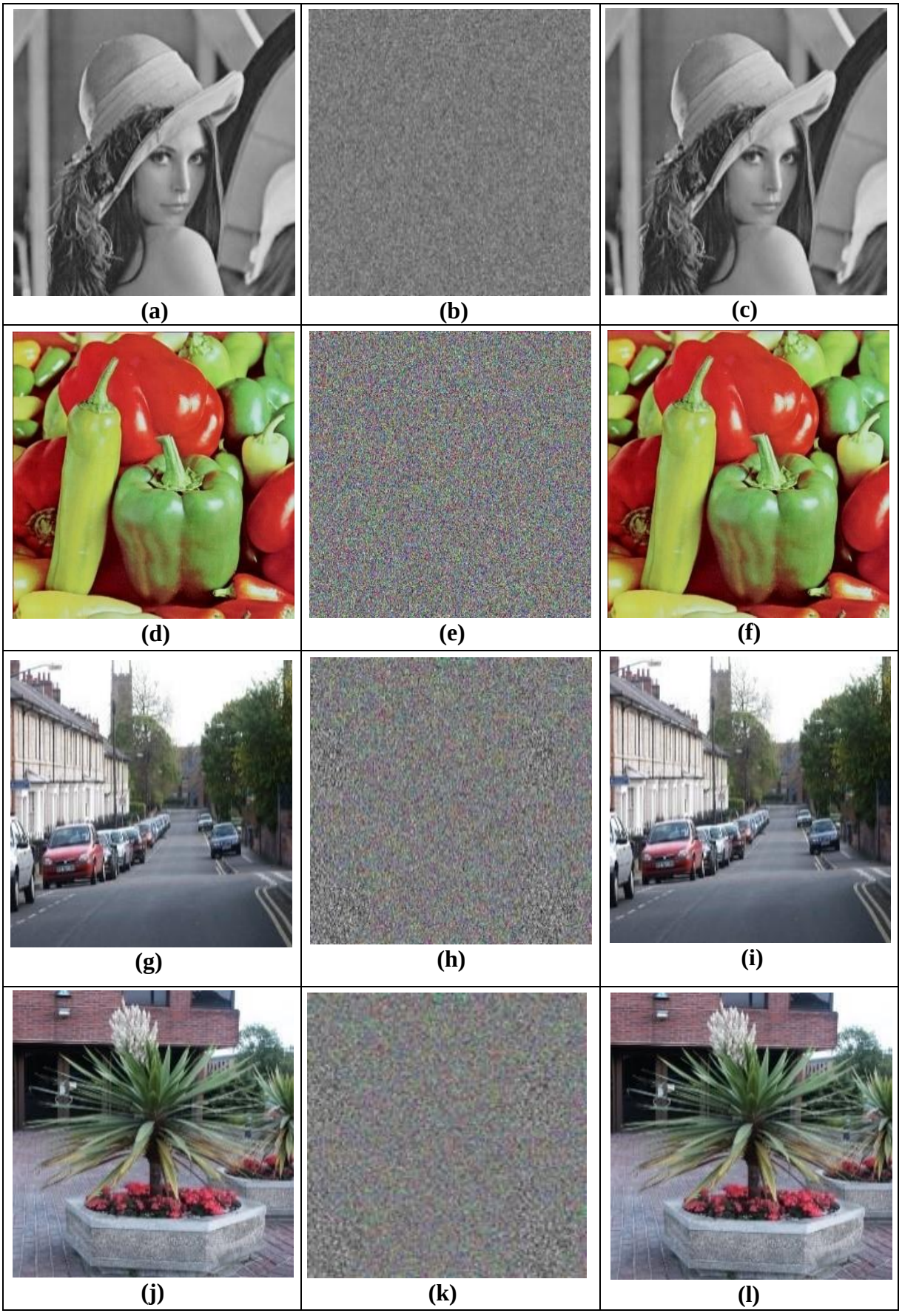

Figure 2.6: (a, d, g, j) images originales ; (b, e, h, k) images chiffrées ; (c, f, i, l) images déchiffrées.

La figure 2.6 montre bien que les images chiffrées sont complétement randomisées. Par conséquent tout attaque sera incapable d'extraire des informations sur l'image originale.

2.4.2 Espace clé

L'attaque brutale est une technique utilisée en cryptanalyse pour trouver la clé de chiffrement. Il s'agit de tester, une à une, toutes les combinaisons possibles. Pour un crypto système d'images meilleur, l'espace clé doit être suffisamment grand, et surtout ne doit pas être inférieure à 2^{100} pour assurer un haut niveau de sécurité [81]. Dans le schéma proposé, la condition initiale et le paramètre de contrôle de la carte Skew Tente améliorée (X_0 et b) sont utilisés comme clés. En effet, X_0 et b sont deux réels à double précision codés chacun sur 64 bits, l'espace clé total est de 128 bits. Ainsi, l'espace de clé est suffisamment grand ce qui rend les attaques brutales infaisables.

2.4.3 Analyse de sensibilité à la clé

En cryptographie la sécurité d'un schéma de chiffrement est étroitement liée à la sensibilité à tout changement de la clé ou de l'image claire, même infiniment petit. C'est-à-dire qu'une légère modification de l'image ou de la clé entraîne un échec du décryptage. Pour tester la sensibilité à la clé de chiffrement, nous cryptons les images "Lena (512 × 512)" de la base de données USC-SIPI et ucid00622 (384 × 512) "de la base de données UCID, avec la clé : X_0 = 0.83294716054979. Cette clé sera légèrement modifiée et sera utilisée pour le déchiffrement. La figure 2.7 montre clairement que l'image cryptée par le X_0 n'est pas correctement déchiffrée à l'aide de la clé $X_0 + 10^{-15}$.

On peut donc conclure que le schéma proposé est sensible à la clé, ce qui signifie qu'un petit changement de la clé générera un résultat complètement différent et ne pourra pas obtenir l'image originale correcte.

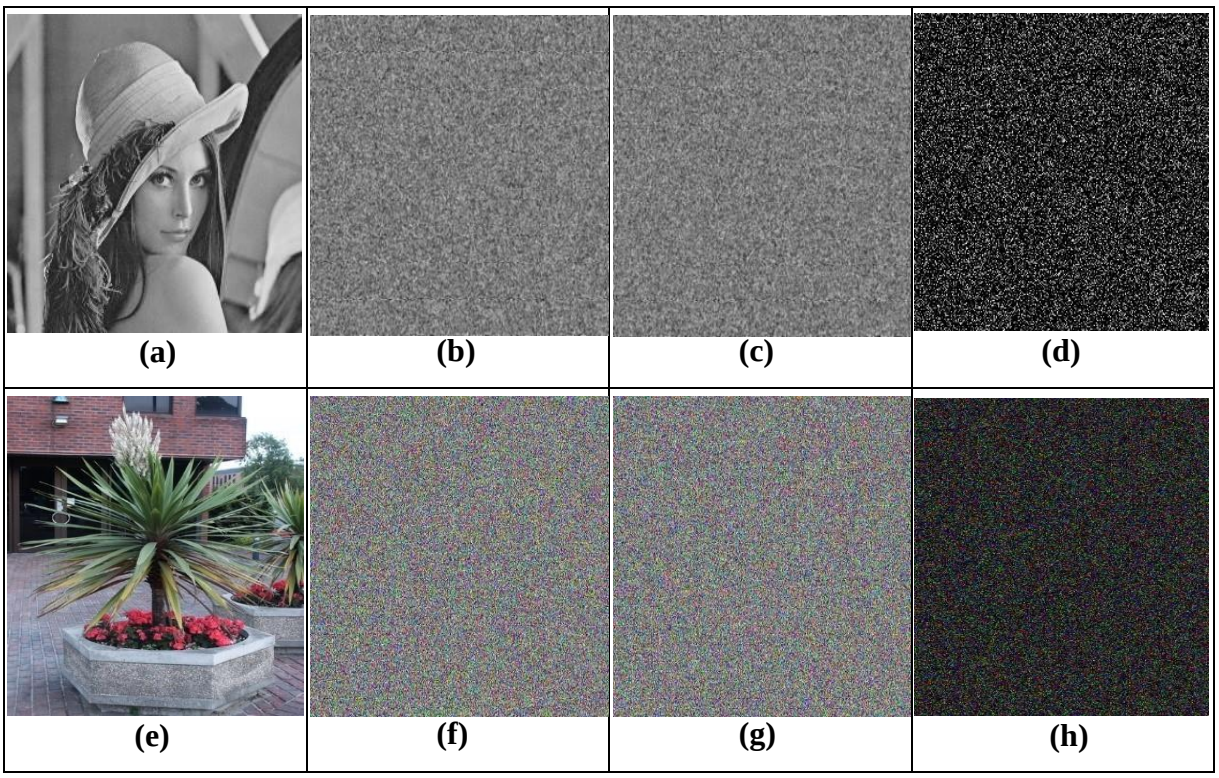

Figure 2.7: Analyse de sensibilité à la clé : (a, e) images originales ; (b, f) images chiffrées par X0 ; (c, g) images décryptées après changement de la clé de X_0 à $X_0 + 10^{-15}$; (d, h) différence entre les images (b) et (c), (f) et (g) respectivement.

2.4.4 Analyse statistique

Afin de prouver la robustesse du schéma de chiffrement proposé face aux attaques statistiques, plusieurs analyses ont été effectuées.

2.4.4.1 Histogramme

Un histogramme d'image est une représentation graphique du nombre de pixels ayant le même niveau de gris. Ainsi l'axe des abscisses représente le niveau de couleur, ce dernier commence de zéro (canal colorimétrique éteint) jusqu'au 255 (canal colorimétrique maximum), chaque barre verticale représente le nombre d'apparition d'un niveau de couleur dans une image. En cryptographie, la distribution de couleur d'une image cryptée a une grande importance. L'histogramme de l'image cryptée peut dans certain cas dévoiler des informations sur l'image originale. Plus précisément, si l'histogramme de l'image cryptée est plat, il ne fournira d'information ni sur l'image originale ni sur la relation entre cette dernière et l'image cryptée.

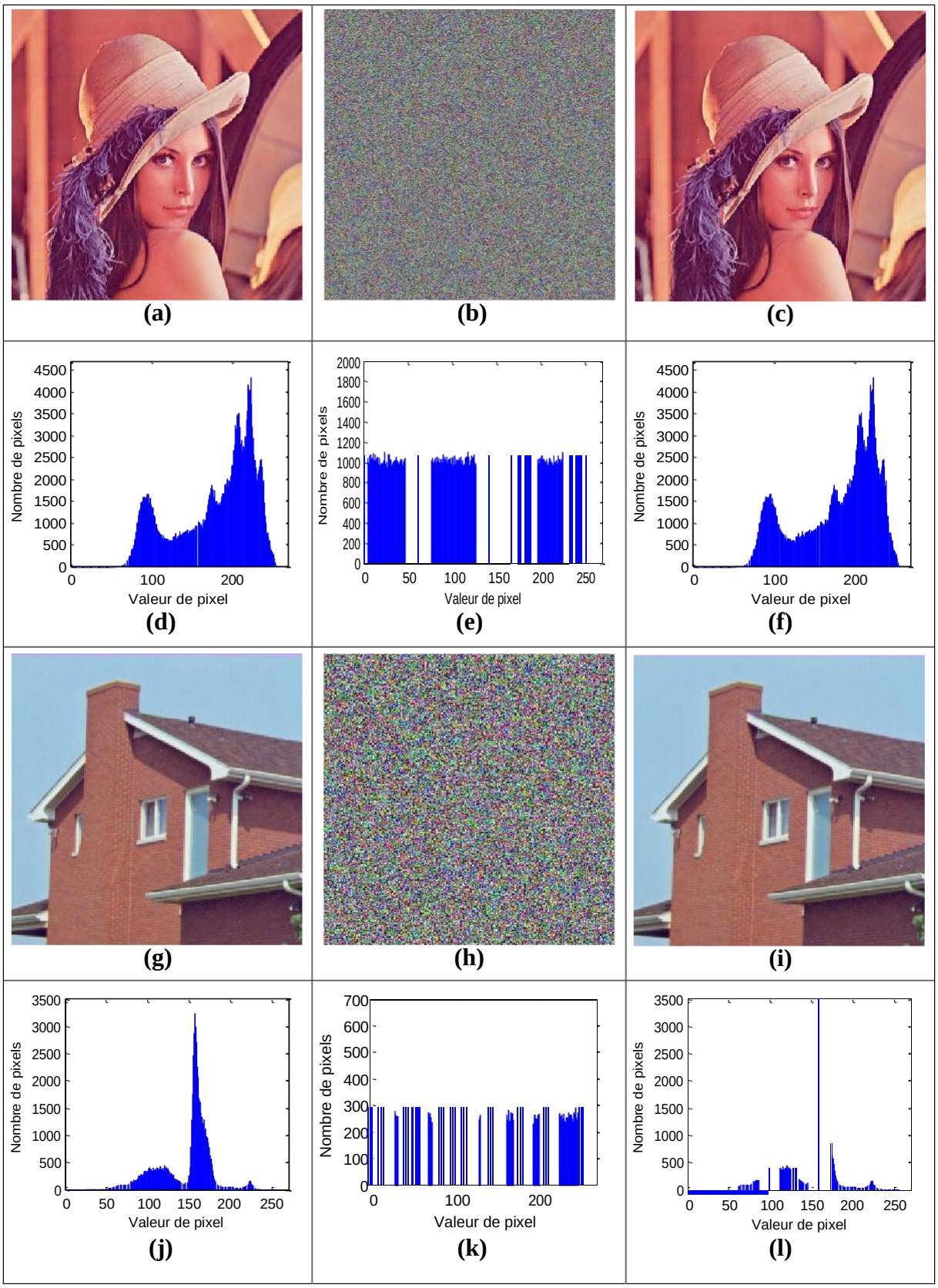

Figure 2.8: Analyse de l'histogramme des images originales/chiffrées (a) Lena, (g) house.

La Figure 2.8 illustre bien que l'histogramme de l'image chiffrée est plat, uniforme et significativement différent de l'histogramme de l'image originale. Par conséquent, il ne fournit

aucun indice à employer dans une attaque par histogramme. Cela est dû au processus Confusion/Diffusion appliqué sur l'image cryptée par notre méthode.

2.4.4.2 Analyse par corrélation

En générale, la corrélation indique la relation linéaire entre deux variables aléatoires. Dans le traitement d'image, elle est souvent utilisée pour étudier la relation entre deux séquences de pixels adjacents. Naturellement, la corrélation entre les pixels adjacents pour l'image originale est très élevée. Dans ce contexte nous avons analysé les corrélations des pixels horizontaux, verticaux et diagonaux voisins pour les images originales et cryptées. Le coefficient de corrélation pour une séquence de pixels adjacents est donné par la formule suivante :

$$r_{\alpha\beta} = \frac{\mathrm{cov}(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \tag{2.8}$$

Où α et β représentent deux vecteurs formés respectivement, par les valeurs des pixels de la séquence choisie de l'image et les valeurs de leurs pixels adjacents.

Les termes $\mathrm{cov}(\alpha, \beta)$, $D(\alpha)$ et $E(\alpha)$ sont calculés par les formules suivantes :

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N} \alpha_i \tag{2.9}$$

$$D(\alpha) = \frac{1}{N}\sum_{i=1}^{N} [\alpha_i - E(\alpha)]^2 \tag{2.10}$$

$$\mathrm{Cov}(\alpha, \beta) = \frac{1}{N}\sum_{i=1}^{N} [\alpha_i - E(\alpha)] \times [\beta_i - E(\beta)] \tag{2.11}$$

Où N est un grand nombre de paires de pixels adjacents sélectionnés aléatoirement dans l'image (dans notre cas N=3000). α_i et β_i sont, respectivement les niveaux de couleurs des pixels collectés. Le tableau 2.2 illustre les résultats des simulations des coefficients de corrélation horizontaux, verticaux et diagonaux de deux séquences de pixels adjacents pour l'image originale et l'image cryptée.

Image	Image originale			Image chiffrée		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena (512×512)	0.9616	0.9761	0.9417	-0.0004	0.0007	-0.0018
Baboon (512×512)	0.8397	0.7195	0.6985	0.0009	0.0061	-0.0019
Peppers (512×512)	0.9653	0.9759	0.9461	-0.0013	0.0001	-0.0002
Cameramen (256×256)	0.9196	0.9549	0.8962	-0.0052	0.0066	-0.0001
ucid00622 (384×512)	0.9164	0.9164	0.8563	0.0026	0.0003	0.0012
Splash (512×512)	0.9432	0.9867	0.9369	0.0045	-0.0017	-0.0113
Male (1024×1024)	0.9772	0.9726	0.9557	0.0019	0.0021	0.0029
ucid00416 (512×384)	0.8937	0.9381	0.8589	0.0029	-0.0007	0.0049
Boat (512×512)	0.8241	0.9434	0.8212	0.0001	-0.0027	0.0039
Girl (256×256)	0.9740	0.9657	0.9516	0.0049	-0.0020	0.0019

Tableau 2.2: Coefficients de corrélation de deux pixels adjacents dans les images originales et chiffrées.

Il ressort du tableau 2.2 que les coefficients de corrélations mesurés pour les images originales sont près de 1, tandis que ceux des images chiffrées sont proches de 0. En se basant sur ces résultats, nous pouvons affirmer que l'algorithme proposé a éliminé avec succès la corrélation des pixels adjacents.

De plus, la corrélation de 3000 paires de pixels adjacents de l'image originale et chiffrée de « Lena (512×512) » et « ucid00622 (384×512) » est illustrée dans la figure 2.9 ci-dessous. Nous pouvons constater qu'il n'y a pas de corrélation détectable entre l'image d'origine et l'image chiffrée. C'est à dire la distribution de corrélation des pixels adjacents de l'image originale et celle de l'image cryptée illustrée dans la figure 2.9, reflète le comportement aléatoire de l'image cryptée.

A partir du tableau 2.2 et de la figure 2.9, on peut déduire que le schéma proposé présente une meilleure capacité de confusion et de diffusion, par conséquent, robuste aux attaques par analyse statistique.

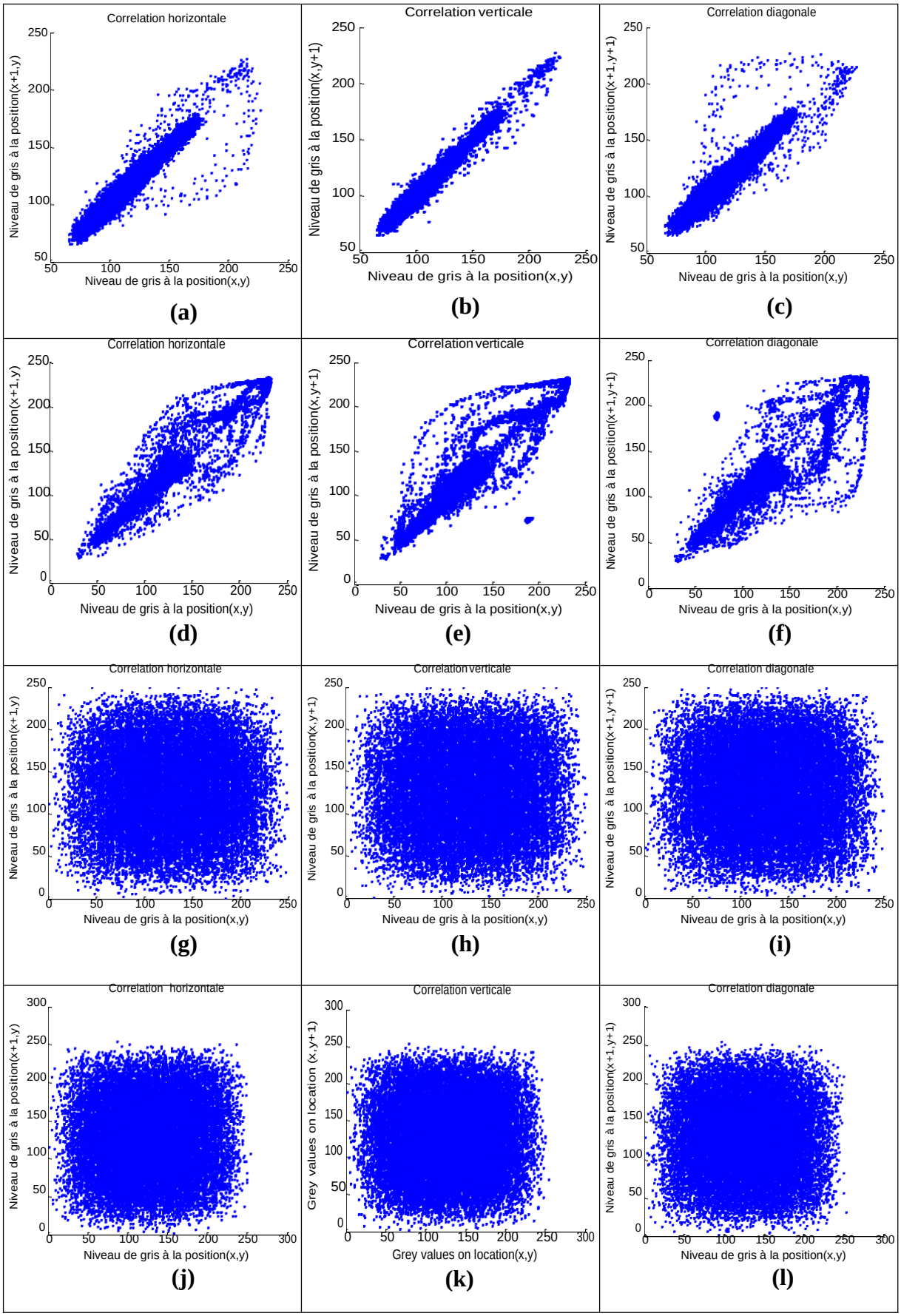

Figure 2.9: Analyse par corrélation.

2.4.4.3 Analyse par entropie

L'entropie d'une information est la quantité d'informations englobée ou libérée par une source d'informations selon la théorie de Shannon [28]. En l'absence de contraintes particulières, la valeur de l'entropie est maximale pour une source d'informations où tous les symboles sont équiprobables. Ainsi, l'entropie est l'une des principales mesures du caractère aléatoire de l'information, autrement dit, l'entropie de Shannon, est une fonction mathématique qui permet de mesurer le comportement aléatoire de l'information. Pour tout message codé sur M bits, la limite supérieure de l'entropie est M. La formule utilisée pour calculer l'entropie est la suivante :

$$e(m) = -\sum_{i=1}^{L} Pr(m_i) \times \log_2 Pr(m_i) \qquad (2.12)$$

où $Pr(m_i)$ est la probabilité du symbole m_i, et L est le nombre total de symboles m_i. Dans notre cas, nous avons choisi des images avec 256 niveaux de gris (codés sur 8 bits), de sorte que l'entropie maximale des informations est d'environ 8. Donc, pour un meilleur crypto système, la valeur de l'entropie doit être très proche de 8. En d'autres termes, une image cryptée sera considérée comme robuste si son entropie tend vers la valeur 8, par conséquent, plus la valeur d'entropie d'une image chiffrée est élevée, plus le système est robuste contre les attaques statistiques. L'entropie des informations pour les images cryptées par notre crypto-système est présentée dans le tableau 2.3 ci-dessous.

Images	Image originale	Image chiffrée
Lena512×512	7.750197	7.999779
Peppers 512×512	7.669825	7.999776
Baboon 512×512	7.762436	7.999781
Cameramen256×256	6.904608	7.999149
House256×256	7.068625	7.999159
Boat 512×512	7.191370	7.999782
Men 1024×1024	7.523736	7.999940
Airplane 512×512	6.663908	7.999769
Sailboat 512×512	7.762169	7.999780
Splash 512×512	7.242830	7.999774

Tableau 2.3 : Entropie de l'image originale et chiffrée.

Il ressort du tableau 2.3, que les valeurs de l'entropie des images cryptées sont très proches de la valeur théorique (qui vaut 8), ce qui confirme l'uniformité des histogrammes des images cryptées, et prouve la résistance de cette technique contre une attaque par entropie.

2.4.5 Analyse par le pic du rapport signal à bruit (PSNR)

En considérant l'image originale comme un signal et celle cryptée comme un bruit, la vérification requiert le calcul de deux indicateurs particulièrement utilisés sont: MSE (Mean Square Error) [86] qui donne l'erreur quadratique moyenne entre les deux images, cette erreur est définie par l'équation (2.13), et le PSNR (Peak Signal to Noise Ratio) [87], le pic du rapport signal à bruit, qui donne une idée plus précise de la dégradation d'une image, il s'évalue selon la formule indiquée dans l'équation (2.14):

$$\mathrm{MSE} = \frac{1}{\mathrm{W} \times \mathrm{H}} \sum_{\mathrm{i,j}} (\mathrm{C}_1(\mathrm{i,j}) - \mathrm{C}_2(\mathrm{i,j}))^2 \qquad (2.13)$$

$$\mathrm{PSNR} = 20 \text{ x} \log_{10}\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right) \qquad (2.14)$$

avec $C_1(i, j)$ est l'intensité de pixel de l'image originale à l'indice (i, j), et $C_2(i, j)$ est l'intensité de pixel de l'image cryptée. Le diagramme ci-dessous illustre les zones de haute, moyenne et

basse qualité de cryptage par rapport à la valeur du PSNR obtenue.

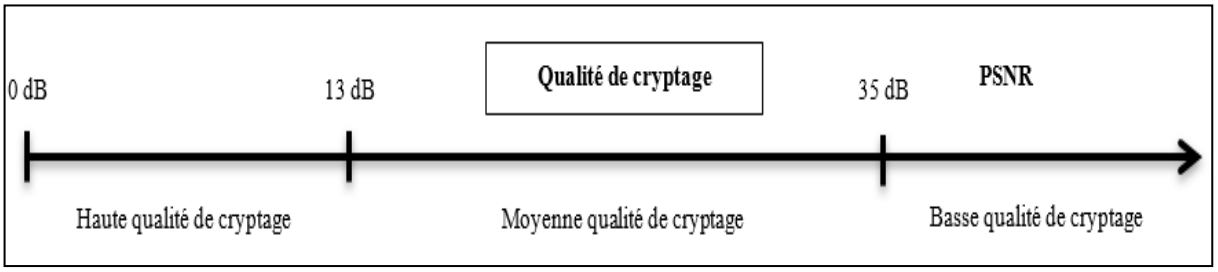

Figure 2.10: Analyse par PSNR.

Le tableau 2.4 montre les valeurs du MSE et PSNR pour différentes images chiffrées par notre crypto-système.

Image	MSE	PSNR
Cameramen 256×256	1.1698e+04	7.4837
House 256×256	8.3683e+03	8.9384
Lena 512×512	8.9270e+03	8.6578
Cameramen 256×256	1.1698e+04	7.4837
Splash 512×512	5.6811e+03	10.6205
Ucid00350 512×384	4.3362e+03	11.7938

Tableau 2.4 : MSE et PSNR.

2.4.6 Analyse différentielle

Un adversaire peut faire un petit changement sur l'image claire, ensuite utilise l'algorithme de cryptage pour chiffrer l'image avant et après le changement, dans le but de tester comment une petite modification dans l'image originale affecte l'image cryptée. Ce genre d'attaque est appelé attaque différentielle. Pour assurer la sécurité d'un schéma de cryptage d'image contre toute attaque différentielle, deux mesures quantitatives sont utilisées : le NPCR (Number of Pixels Change Rate) [87] [88], et l'UACI (Unified Average Changing Intensity) [89]. Le NPCR représente le taux de pixels différents entre les deux images chiffrées qui diffèrent d'un pixel, tandis que l'UACI représente la différence de l'intensité moyenne. Les formules utilisées pour calculer NPCR et UACI sont définies par les deux équations suivantes :

$$\mathrm{NPCR} = \frac{\sum_{i,j} g(i,j)}{W \times H} \times 100 \qquad (2.15)$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|IC_1(i,j) - IC_2(i,j)|}{255}\right) X100 \qquad (2.16)$$

avec $IC_1(i, j)$ est l'image cryptée et $IC_2(i, j)$ est l'image cryptée après avoir changé un pixel de l'image claire. Pour les pixels à la position (i, j), si $IC_1(i, j) \neq IC_2(i, j)$, alors $g(i, j) = 1$; sinon $g(i, j) = 0$.

Une valeur de UACI > 33.4635 et NPCR > 99.6094 assure qu'un algorithme de chiffrement d'image est immunisé contre une attaque différentielle. Le tableau 2.5 ci-dessous montre les résultats des simulations de UACI et NPCR dans notre cas.

Image originale	**Image cryptée**	
	NPCR	**UACI**
Cameramen 256×256	99.620521	33.512345
House 256×256	99.619634	33.570318
Lena 512×512	99.645271	33.473291
Ucid00350 512×384	99.616180	33.461657

Tableau 2.5: Valeurs de NPCR et UACI après le changement de la valeur d'un pixel.

Les résultats présentés dans le tableau 2.5 montrent bien que les valeurs du NPCR sont supérieurs à 99.6094 et celles de UACI sont supérieurs à 33.4635, c'est-à-dire qu'une modification d'un seul pixel de l'image originale entraine un changement radical de tous les pixels de l'image cryptée. On peut dire alors que notre algorithme présente une résistance contre toute attaque différentielle. Ceci est grâce au processus de confusion/diffusion adopté par la méthode proposée.

2.4.7 Temps d'exécution

En plus des performances citées précédemment. Le temps d'exécution est aussi une caractéristique importante d'un algorithme de cryptage d'image, surtout pour l'adopter dans un chiffrement en temps réel. En utilisant les spécificités indiquées dans le tableau 2.1 nous avons obtenu les résultats montrés dans le tableau 2.6, avec une comparaison avec des algorithmes existants :

Image (pixel)	**Méthode proposée**	**Réf.** [12]	**Réf.** [18]	**Réf.** [90]
128×128	0.092	------	------	------
256×256	0.109	0.2973	0.90	0.281
512×384	1.023	------	------	------
512×512	1.215	1.2720	7.86	1.164
1024×1024	3.217000	------	------	------

Tableau 2.6: Temps d'exécution en (seconde).

Il ressort dans le tableau 2.6 que notre méthode possède un temps d'exécution acceptable.

2.5 Comparaison

Pour valider les performances du schéma proposé, nous allons dresser un tableau qui compare les résultats de simulation obtenus avec d'autres approches récentes, en termes de coefficients de corrélation, de PCNR, d'UACI et d'entropie, pour l'image « Lena 256×256 ».

Paramètres	**Réf.** [90]	**Réf.** [91]	**Réf.** [92]	**Méthode proposée**
Corrélation horizontale	0.0230	-0.0230	0.0018	-0.0133
Corrélation verticale	0.0019	0.0019	0.0011	0.00076
Corrélation diagonale	0.0011	-0.0034	-0.0012	0.0077
NPCR	99.5193	99.6200	99.6166	100
UACI	33.5851	33.5100	33.4365	33.5515
Entropie	7.9975	7.9974	7.9994	7.9990

Tableau 2.7 : Comparaison des résultats obtenus avec d'autres méthodes existantes.

2.6 Conclusion

Dans ce chapitre, nous avons suggéré un schéma de chiffrement d'images numérique et niveau de gris. La technique est basée sur une amélioration des propriétés pseudo-aléatoires de la carte Skew tente par une fonction modulaire, qui sera utilisé comme générateur des séquences chaotiques du processus de chiffrement. Les simulations et les évaluations des performances comprenant l'exposant de Lyapunov, la densité de distribution et le diagramme de bifurcation ont prouvé que la carte proposée permet de produire des séquences chaotiques caractérisées par

une densité de distribution uniforme. L’exposant de Lyapunov est considérablement supérieur à celui de la carte Skew tente originale, ce qui rend la carte améliorée extrêmement sensible aux conditions initiales. Les séquences chaotiques générées sont utilisées dans le processus de permutation d’une part, et dans le mécanisme de diffusion d’autre part. L'espace clé utilisé est de 128 bits, ce qui protège notre méthode contre les attaques par force brute. Une analyse statistique a été effectuée sur le schéma de cryptage proposé, démontrant ses propriétés supérieures de confusion qui résistent fortement aux attaques statistiques. Ceci est démontré par un histogramme plat de l’images chiffrée, un coefficient de corrélation proche de zéro des pixels adjacents de l'image chiffrée dans les trois directions (horizontal, vertical et diagonal) et une entropie proche de la valeur théorique (qui vaut 8). Aussi une analyse différentielle a été réalisée, démontrant de hautes performances de diffusion qui résistent aux attaques différentielles, et prouvé par des valeurs de NPCR et UACI proches de celles théoriquement acceptables 99.6 et 33.45 respectivement, et finalement, un temps d’exécution acceptable, nous permet de déduire que le schéma proposé peut être utilisé pour la transmission des données sous forme image avec une sécurité et un temps d‘exécution raisonnable.

Chapitre 3

Chiffrement d'images basé sur le carré de Vigenère dynamique et le système chaotique 3D amélioré.

Sommaire

3.1 Introduction

Actuellement, l'échange des données multimédias via les réseaux de communication, en particulier l'internet, est devenu un élément très important dans la société moderne. Cela, est dû à une grande utilisation de ces données dans divers domaines (médicale, industriel, vision par ordinateur, commerce électronique, …). Alors, ce transfert massif de données multimédias, en particulier les images, engendre un besoin énorme en termes de sécurité. Pour cela une sécurité de haut niveau demeure obligatoire que ce soit pour la sauvegarde, pour la transmission ou pour d'autres applications. Dans ce contexte le chiffrement reste un outil incontournable pour sécuriser une image et garantir sa confidentialité et son intégrité.

Cependant, vu la taille volumineuse, la redondance élevée et la forte corrélation des images, les systèmes de chiffrements standards conçus pour les données format texte tels que RSA [8], DES [5], AES [22] demandent un temps de calcul important, par conséquent ne sont pas adéquats à ce type de données.

Actuellement la cryptographie chaotique constitue l'une des alternatives développées durant la dernière décennie, et qui sont adaptées à la transmission sécurisée des images, cela grâce à leurs caractéristiques intrinsèques telles que l'ergodicité, la sensibilité aux conditions initiales et aux paramètres de contrôle. Ces propriétés sont convenables dans les deux principaux mécanismes de chiffrement [28] qui sont la confusion qui crée une forte relation entre la clé de cryptage et le texte chiffré, et la diffusion qui permet de réduire la forte redondance du texte clair en la propageant sur la totalité du texte chiffré.

La carte logistique 1D est l'un des systèmes chaotiques populaires caractérisées par sa simplicité, sa rapidité de mise en œuvre dans les systèmes numériques, et sa faible consommation des ressources. Cependant, cette carte présente des faiblesses à savoir, une distribution non uniforme, un petit espace clé et la périodicité [17]. Dans ce chapitre une amélioration des caractéristiques pseudo-aléatoires du système chaotique 3D de cartes logistiques étendues est effectuée. En effet, le système obtenu sera utilisé comme un générateur des séquences chaotiques caractérisées par une uniformité remarquable, une hypersensibilité aux conditions initiales, et surtout des propriétés statistiques excellentes. Les séquences chaotiques ainsi obtenues sont utilisée dans l'architecture du crypto-système proposé, basé sur une permutation chaotique pour éliminer la forte redondance des images naturelles, une substitution à partir d'une table de Vigenère dynamique construite à l'aide d'un processus basé

sur des séquences chaotiques, suivi d'une forte diffusion introduite au sein du crypto système proposé qui sera propagée sur la totalité de l'image.

3.2 Description du schéma proposé

Dans ce chapitre nous avons proposé une approche qui permet de crypter les images couleurs après un seul rond, ce qui montre la rapidité, et par conséquent la possibilité de l'utiliser dans des applications à temps réel. Il est bien clair qu'un bon algorithme de chiffrement doit être sensible aux clés de chiffrement, et l'espace clé doit être assez grand pour faire face aux attaques brutales. Ainsi, dans ce travail on utilise un système chaotique 3D constitué de 3 cartes logistiques étendues, dont nous avons amélioré l'aspect pseudo-aléatoire. Le système conçu sera utilisé pour générer les clés de chiffrement, ce qui présente un espace clé largement suffisant contre toutes attaques brutales [93] [94]. Naturellement une image présente une forte corrélation des pixels adjacents. Pour apporter une indépendance statistique entre l'image cryptée et l'image originale, une permutation chaotique a été appliquée sur l'image originale. L'une des considérations les plus importantes pour mesurer la robustesse d'un algorithme de cryptage est l'effet d'avalanche. Notre système cryptographique est robuste contre toute attaque différentielle. Cela rendu possible par un effet d'avalanche inséré qui sera propagé sur la totalité de l'image, de telle sorte qu'une toute petite perturbation sur une valeur initiale (par exemple un changement d'un seul bit d'un pixel de l'image ou de la clé de chiffrement) sera répercutée sur l'image toute entière, cette propriété permet d'apporter un grand effet d'avalanche et par conséquent une forte résistance aux attaques différentielles [95].

3.2.1 Technique de chiffrement

3.2.1.1 Introduction

En général un système de chiffrement parfait doit satisfaire les deux propriétés de Shannon [28]: La confusion correspond à une volonté de rendre la relation entre, d'une part le texte clair et la clé de chiffrement, et d'autre part le texte chiffré, très difficile voire impossible à établir. En effet, ce principe est souvent réalisé par les substitutions, la diffusion s'exprime par le fait qu'une modification même mineure (de l'ordre d'un bit) du texte en clair doit se traduire par une modification très importante du texte chiffré. La diffusion est souvent réalisée par l'effet d'avalanche.

Dans le travail proposé, ces deux propriétés ont été bien adoptées, le schéma de la figure 3.1 illustre le principe du système de chiffrement.

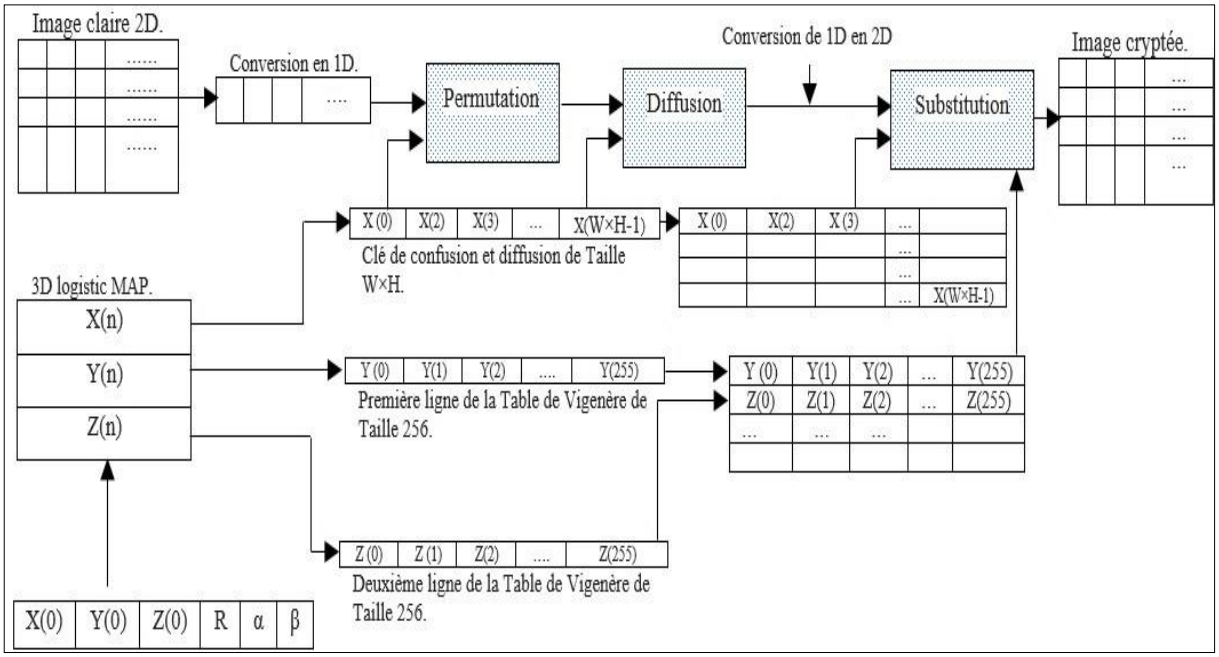

Figure 3.1: Schéma de système de chiffrement proposé dans ce chapitre.

Dans un premier temps l'image originale sera convertie en vecteur de taille W×H (Avec W et H représentent respectivement la largeur et la hauteur de l'image originale), ensuite une permutation sera effectuée sur les pixels via la séquence chaotique X. Puis la même séquence sera utilisée dans le processus de diffusion. Et finalement une substitution sera réalisée à l'aide d'une nouvelle table de Vigenère créée par les deux séquences chaotiques Y et Z.

3.2.1.2 Construction des générateurs Pseudo-aléatoires

Le chao est un phénomène omniprésent dans les systèmes non linéaires déterministes qui présentent une sensibilité extrême aux conditions initiales et qui possède un comportement aléatoire, grâce à ces caractéristiques, plusieurs domaines de recherches sont intéressés par cette dynamique, en l'occurrence la cryptographie.

La carte logistique est l'un des systèmes chaotiques populaire très utilisée dans la cryptographie des images sont expression est donnée par l'équation (3.1) :

$$X_{n+1} = RX_n(1 - X_n) \qquad (3.1)$$

La suite présente un aspect chaotique pour $3.57 < R \leq 4$ et $0.5 < X_0 < 1$. Et un processus de bifurcation lorsque le paramètre de contrôle R est dans l'intervalle]3.57, 4]. Cette carte logistique a une seule dimension peut être étendue en trois dimensions en utilisant le système d'équations (3.2) [90] :

$$\begin{aligned} X_{n+1} &= RX_n(1-X_n)+\beta Y_n^{\prime} X_n + \alpha Z^{\prime}_n \\ Y_{n+1} &= RY_n(1-Y_n)+\beta Z_n^2 Y_n + \alpha X^3_n \\ Z_{n+1} &= RZ_n(1-Z_n) + \beta X^2_n Z_n + \alpha Y^3_n \end{aligned} \qquad (3.2)$$

Ce système appelé (Générateur Pseudo-Aléatoire à Carte Logistique Etendue (GPACLE)) présente un comportement chaotique dans le cas où les paramètres $R, \alpha, \text{et } \beta$ sont comme suit :

$0.53 < R < 3.81$, $0 < \beta < 0.022$, et $0 < \alpha < 0.015$, avec X_0, Y_0 et Z_0 sont dans l'intervalle]0,1[.

Cependant, le GPACLE est caractérisé par sa structure simple, sa facilité d'implémentation. Utilisé généralement pour chiffrer les données de grande taille en temps réel, en revanche, il présente plusieurs faiblesses [17], telle que, la discontinuité, la non-uniformité, la courte périodicité, et l'espace clé faible. Dans ce chapitre nous avons amélioré l'aspect pseudo-aléatoire du GPACLE, par une simple multiplication par 10^5 et une application de l'arithmétique modulaire (mod 1), ce nouveau générateur pseudo-aléatoire nommé (Générateur Pseudo-Aléatoire à Carte Logistique Etendu Amélioré (GPACLEA)), est indiqué dans l'équation (35) [15]:

$$\begin{aligned} X_{n+1} &= \text{mod}(((RX_n(1-X_n)+\beta Y_n^{\prime} X_n + \alpha Z^{\prime}_n)(100000)),1) \\ Y_{n+1} &= \text{mod}(((RY_n(1-Y_n)+\beta Z_n^2 Y_n + \alpha X^3_n)(100000)),1) \\ Z_{n+1} &= \text{mod}(((RZ_n(1-Z_n)+\beta X_n^2 Z_n + \alpha Y^3_n)(100000)),1) \end{aligned} \qquad (3.3)$$

Avec mod est l'opération modulo 1. La comparaison des propriétés pseudo-aléatoires des deux générateurs GPACLE et GPACLEA telle que la densité de distribution, l'exposant de Lyapunov et la bifurcation montrent la qualité et la robustesse de GPACLEA.

En cryptographie, la distribution des séquences des générateurs pseudo-aléatoires à une grande importance. Les deux schémas de la figure 3.2 montrent les deux densités de distribution des séquences X, Y et Z des deux générateurs pseudo-aléatoires GPACLE et GPACLEA.

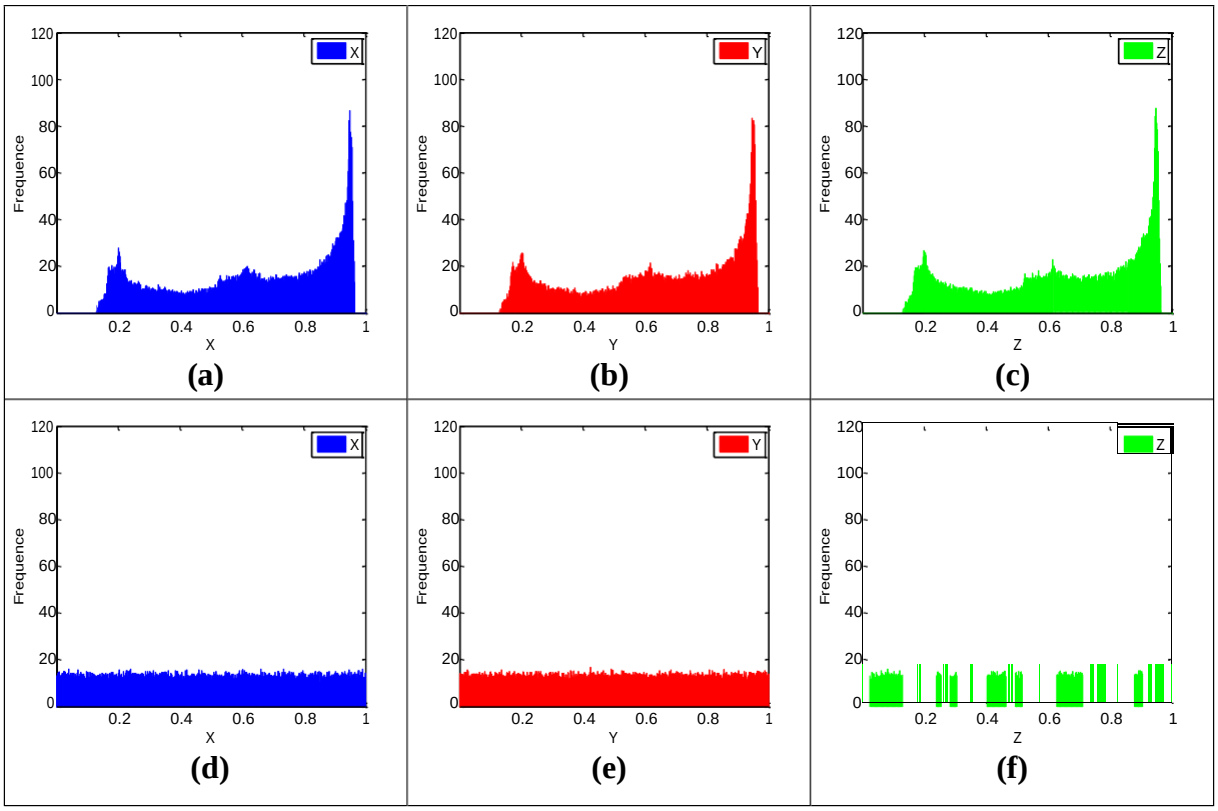

Figure 3.2: (a, b, c) Densités de distribution des séquences X, Y et Z du GPACLE, respectivement ; (d, e, f) Densités de distribution des séquences X, Y et Z du GPACLEA, respectivement.

En analysant les densités de distribution présentées dans la Figure 3.2 ci-dessus, nous confirmons que le GPACLEA présente une densité de distribution uniforme, contrairement au GPACLE qui présente une mauvaise densité de distribution (la quasi-totalité des valeurs sont proches de la valeur 1). Par conséquent le générateur proposé possède de bonnes propriétés statistiques, et est plus recommandé à utiliser pour un système de chiffrement robuste.

Pour déterminer si un système dynamique non linéaire est chaotique ou non on calcul son exposant de Lyapunov. Un système dynamique non linéaire chaotique est caractérisé par son exposant de Lyapunov positif et par conséquent une grande sensibilité aux conditions initiales [15] [18] [41]. Ainsi, nous avons choisi deux orbites chaotiques de GPACLE $_{(X, Y, Z)}$ avec un même paramètre de contrôle R, mais avec des conditions initiales différentes, idem pour GPACLEA $_{(X, Y, Z)}$, soit :

$$\lambda_X = \frac{1}{N} \ln \left| \frac{f^N(X_0 + \varepsilon) - f^N(X_0)}{\varepsilon} \right| \qquad (3.4)$$

avec λ_X est l'exposant de Lyapunov de de la séquence X, X_0 est la condition initiale, $X_0' = X_0 + \varepsilon$ est une autre condition initiale très voisine, $f^N(X_0)$ est la valeur de la séquence X_0 d'ordre N, et N est le nombre d'itération (dans notre cas N=10000), la condition initiale choisie est $X_0 = 0.859571$ et $\varepsilon = 3 \times 10^{-6}$. La figure 3.3 montre les valeurs de l'exposant de Lyapunov pour les deux générateurs GPACLE et GPACLEA pour un paramètre de contrôle $R \in [1.5, 4]$.

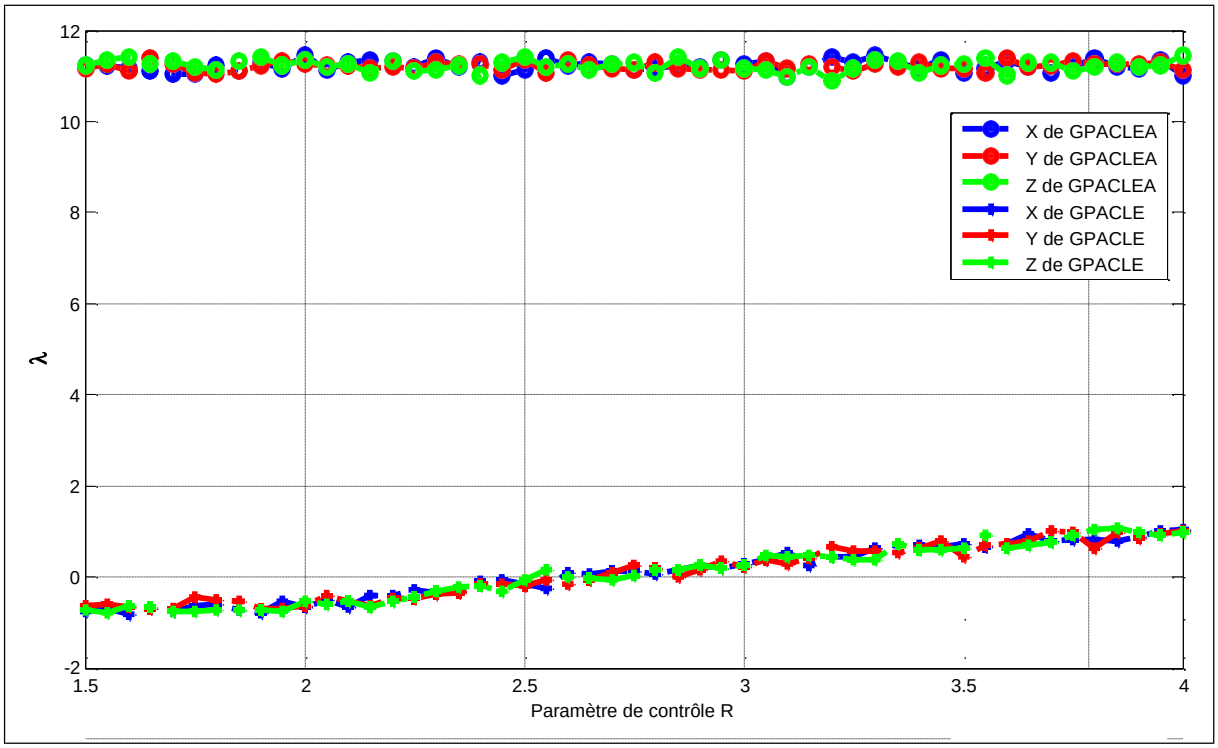

Figure 3.3: Exposant de Lyapunov de GPACLE et de GPACLEA.

En analysant les courbes montrées dans la figure 3.3, nous pouvons remarquer que les valeurs des exposants de Lyapunov obtenues pour GPACLEA ($\lambda_{X,Y,Z} \approx 11.21$) sont meilleures par rapport à celles de GPACLE($\lambda_{X,Y,Z} \approx 1.01$), et par conséquent le générateur proposé présente une divergence exponentielle de l'écart entre deux trajectoires chaotiques ayants des conditions initiales très voisines.

Une analyse qualitative de la carte logistique peut être réalisée par l'étude de son diagramme de bifurcation. Qui représente le comportement asymptotique d'un système dynamique discret en fonction de paramètre de contrôle. Le schéma de la figure 3.4 montre les

diagrammes de bifurcation de la carte logistique 3D étendue des deux générateurs pseudo-aléatoires.

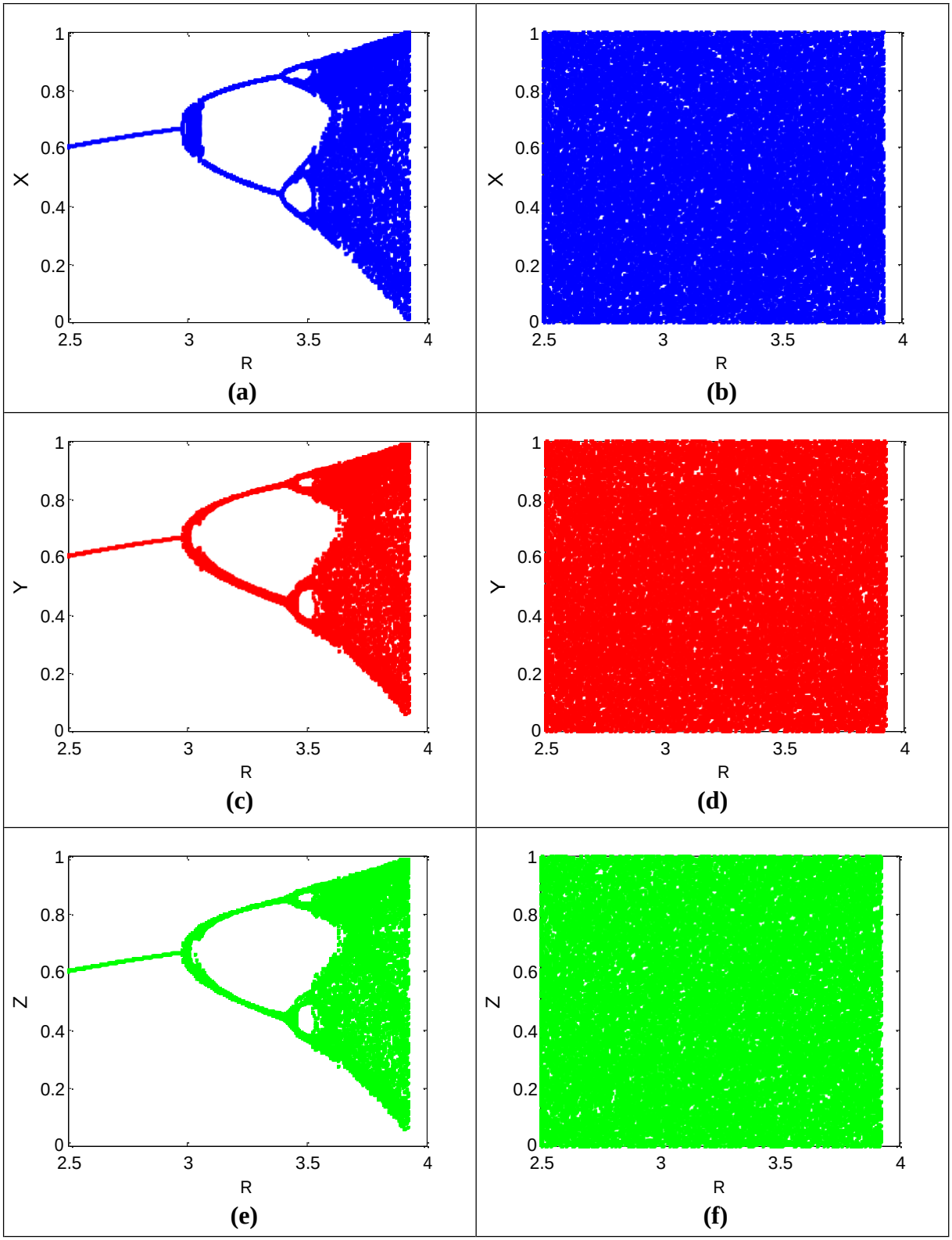

Figure 3.4: (a, c, e) Diagrammes de bifurcation de (X, Y, Z respectivement) de GPACLE, et (b, d, f) Diagrammes de bifurcation de (X, Y, Z respectivement) de GPACLEA.

Après la comparaison des propriétés statistiques des deux générateurs pseudo-aléatoires GPACLE et de GPACLEA, nous avons remarqué que le nouveau générateur est plus favorable à utiliser. En effet, dans la suite de ce chapitre nous avons adopté les séquences pseudo-aléatoires X, Y et Z de GPACLEA pour le chiffrement des images.

3.2.1.3 Permutation chaotique basée sur GPACLEA

Afin de décorréler l'image originale, un processus de permutation sera appliqué sur les pixels adjacents. Nous avons utilisé le processus de génération de clé de permutation décrit dans la figure 2.4, pour obtenir le vecteur de permutation P= $\{p_0, p_1, \ldots, p_{W\times H-1}\}$, avec W représente la largeur et H la hauteur de l'image originale. La permutation chaotique de l'image originale par le vecteur de P est obtenue par l'équation suivante :

$$ImP(i)=ImO(P(i)) \qquad (3.5)$$

avec ImP représente l'image permutée, et ImO représente l'image originale, ainsi, l'image permutée obtenue sera complétement décorrélée et en désordre. Mais elle présente le même histogramme que l'image originale (voir figure 3.5), car il n'y a pas de changement des intensités des pixels. Par conséquent, l'image permutée est faible contre une attaque statistique et une attaque différentielle. D'où la nécessité d'introduire une diffusion et une confusion pour renforcer la sécurité.

Remarque :

Le processus inverse de permutation se réalise par l'équation (3.6) suivante :

$$ImR(P(i)) = ImP(i) \qquad (3.6)$$

avec ImR représentant l'image restaurée après la permutation inverse. La figure 3.5 montre l'image « Lena 512×512 » originale, son histogramme, l'image permutée et l'histogramme correspondant.

La figure 3.5 montre bien que les deux histogrammes de l'image permutée et l'image originale sont identiques. Par conséquent, la permutation est une action qui se contente juste de délocaliser les pixels de l'image originale, sans modifier leurs intensités.

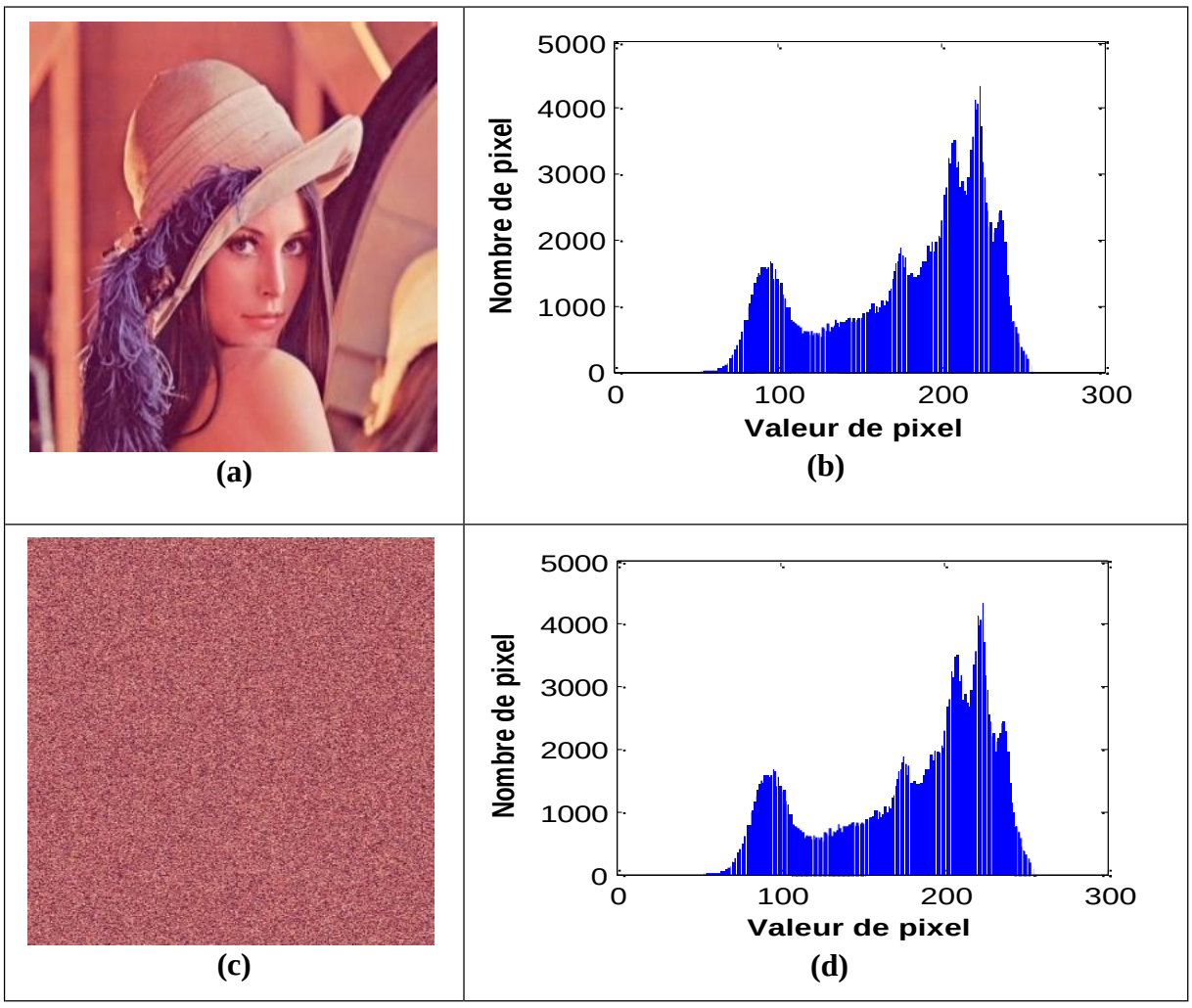

Figure 3.5: (a) Image « Lena 512×512 » originale, (b) son histogramme, (c) image « Lena 512×512 » permutée, (d) son histogramme.

3.2.1.4 Mécanisme de diffusion

Le processus de diffusion repose sur une modification séquentielle des intensités des pixels voisins toute en mixant leurs valeurs avec la clé de diffusion. Soit l'image permutée sous forme de vecteur de taille W×H. le principe de diffusion se résume par les étapes suivantes :

- **Etape 1** : La séquence X= $\{x_0, x_1, \ldots, x_{W\times H-1}\}$, générée à partir de GPACLEA sera utilisée pour obtenir la clé de diffusion K(X)= $\{k_0^{(X)}, k_1^{(X)}, \ldots, k_{W\times H-1}^{(X)}\}$, avec $k_i^{(X)} = \mathrm{mod}(\mathrm{floor}(x_i \times 10^5), 256))$, et i=0, 1, …, W×H-1. La fonction floor(x), retourne le plus grand entier inférieur ou égal à x.

- **Etape 2** : Nous déterminons la valeur initiale C_0, qui est égale à la somme des intensités des tous les pixels ImP_i de l'image permutée, soit :

  $C_0 = \mathrm{mod}((\sum_{i=0}^{W\times H-1} ImP_i), 256)$, avec C_0 sera le premier pixel crypté.

- **Etape 3** : Nous introduisons la diffusion sur la totalité de l'image par la formule suivante :

$$C_j = \mathrm{mod}\left((C_{j-1} \text{ XOR } k^{(X)}_{i-1} \text{ XOR } ImP_{j-1}), 256\right) \quad (3.7)$$

avec j=1, 2, …, W×H-1, C_j est la valeur de pixel crypté a la position j, et ImP_j est le pixel de l'image permutée de rang j. Le processus de diffusion est décrit par le schéma suivant :

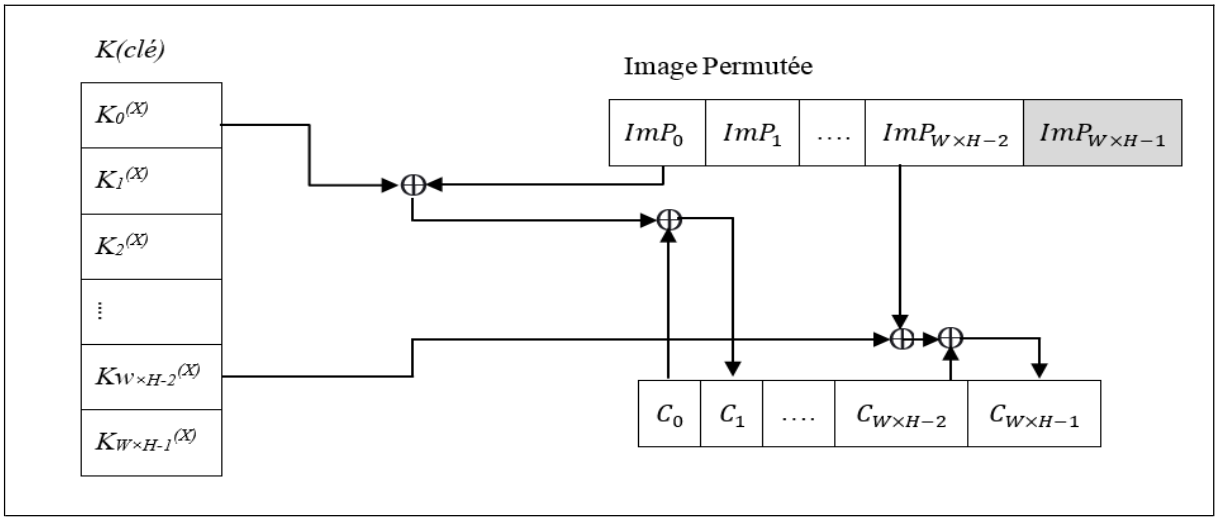

Figure 3.6: Mécanisme de diffusion.

Une analyse du mécanisme de diffusion montré dans la figure 3.6, nous pouvons remarquer que le dernier pixel de l'image permutée n'intervient pas dans le processus de diffusion, ce qui renforce encore la robustesse de l'algorithme contre toute attaque différentielle. L'opération inverse de ce mécanisme de diffusion est déterminée par l'équation (3.8) suivante :

$$ImD_i = \mathrm{mod}\left((C_i \text{ XOR } C_{i+1} \text{ XOR } k^{(X)}_i), 256\right) \quad (3.8)$$

avec i=0, 1, …, W×H-2, ImD_i est la valeur de pixel décrypté a la position i, et C_i est le pixel de l'image cryptée de rang i. Le mécanisme de diffusion utilisé dans le déchiffrement est illustré par le diagramme suivant :

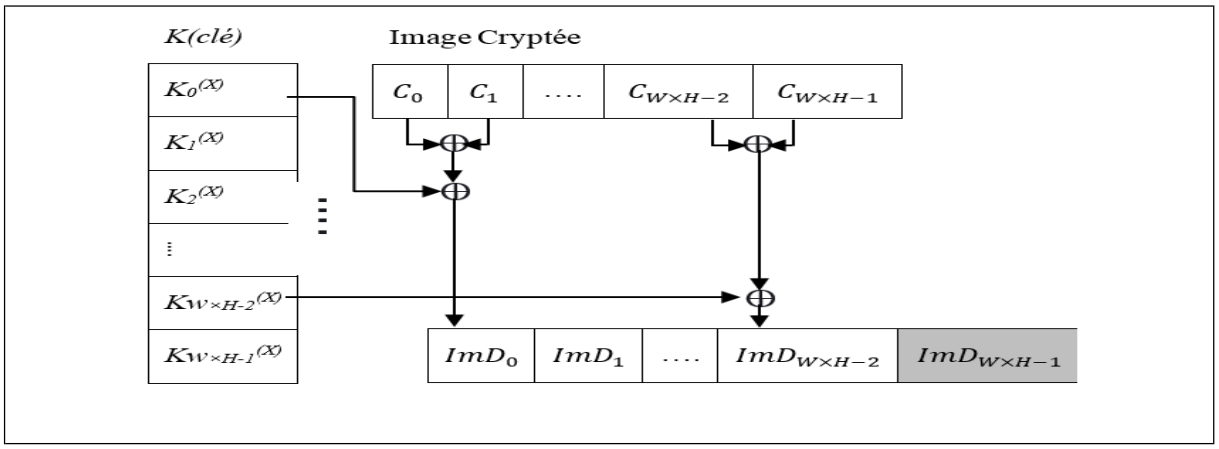

Figure 3.7: Mécanisme de diffusion inverse.

Nous pouvons voir dans la figure 3.7 que le dernier pixel $ImD_{W\times H-1}$ n'est pas récupéré, sa valeur sera obtenue par la formule suivante :

$$ImD_{W\times H-1} = C_0 - \sum_{i=0}^{W\times H-2} ImD_i \qquad (3.9)$$

3.2.1.5 Table de Vigenère

Dans cette section nous allons créer la nouvelle table de Vigenère qui sera utilisée dans la phase de substitution. Le principe de construction est le suivant : La séquence Y= $\{y_0, y_1, \ldots, y_{255}\}$ sera choisie pour créer le premier vecteur clé $K^{(Y)}= \{k_0^{(Y)}, k_1^{(Y)}, \ldots, k_{255}^{(Y)}\}$, avec $k_i^{(Y)} = \mathrm{mod}(\mathrm{floor}(y_i \times 10^5), 256))$, et i=0, 1, …,*255*. Et La séquence Z= $\{z_0, z_1, \ldots, z_{255}\}$ sera choisie pour créer le deuxième vecteur clé défini par :

$K^{(Z)}= \{k_0^{(Z)}, k_1^{(Z)}, \ldots, k_{255}^{(Z)}\}$, avec $k_i^{(Z)} = \mathrm{mod}(\mathrm{floor}(z_i \times 10^5), 256))$, et i=0, 1, …,*255*. Les autres lignes de la table sont créées par des itérations séquentielles indiquées dans l'algorithme 3.

Algorithme de création de la table de Vigenère de taille 256×256.

Pour i 0 jusqu'à 255 faire // Initialisation de la nouvelle table de Vigenère
    $V[0][i] = K^{(Y)}[i]$
    $V[1][i] = K^{(Z)}[i]$
Pour i 2 jusqu'à 255 faire // i pour désigner la ligne// Création des autres lignes de la table de Vigenère.
    Pour j 0 jusqu'à 255 fais // j pour désigner la colonne
        $V[i][j] = V[i-2][V[i-1][j]]$
    Fin
Fin

Pour une table de Vigenère de taille 26×26 (figure 3.8). Soient les deux premiers vecteurs de taille 26, V0 issu de la séquence Y et V1 issu de la séquence Z.

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
V[0][j]	0	8	5	17	19	16	1	23	18	14	25	12	20	10	6	15	3	4	2	7	13	22	21	24	0	9	11
V[1][j]	1	4	13	10	22	16	12	15	1	3	6	23	9	25	17	14	24	11	5	18	8	20	7	19	2	0	21
V[2][j]=V[0][V[1][j]]	2	16	6	12	24	4	10	3	5	19	23	0	25	11	2	15	9	20	1	7	14	22	18	13	17	8	21
V[3][j]=V[1][V[2][j]]	3	11	15	25	0	16	23	22	12	8	2	4	21	9	10	24	6	20	13	1	14	19	18	17	5	3	7
	4	25	9	21	16	20	17	13	11	19	12	4	18	23	0	8	3	22	2	6	15	14	7	1	10	24	5
	5	7	2	18	20	19	13	10	21	14	9	16	1	5	11	8	0	17	25	22	6	24	12	15	4	3	23
	6	11	21	6	14	15	0	4	7	8	12	22	9	17	18	19	25	2	5	1	13	24	23	3	20	16	10
	7	1	12	10	8	0	7	19	21	14	5	15	9	25	22	6	23	18	13	2	11	3	4	20	24	17	16
	8	21	17	22	8	11	7	13	23	19	0	25	12	10	3	4	20	1	18	6	9	14	15	24	16	5	2
	9	4	13	20	14	9	21	22	24	11	1	16	25	15	8	0	3	12	2	19	5	6	23	17	18	7	10
	10	11	3	14	4	0	15	24	5	12	17	1	2	20	19	21	8	10	22	9	7	13	16	18	6	23	25
	11	25	14	0	9	4	3	7	21	15	2	13	20	6	5	23	11	16	17	1	24	8	12	19	22	18	10
	12	25	21	11	17	0	4	5	16	8	14	19	13	24	15	6	2	10	22	3	23	12	20	7	18	9	1
	13	10	12	20	17	25	4	3	16	15	23	24	5	18	11	7	0	13	19	9	22	6	8	21	1	2	14
⋮	14	19	24	12	22	1	0	17	10	2	18	9	4	3	13	16	25	15	23	14	7	5	8	20	21	11	6
	15	22	2	18	21	12	10	19	24	20	9	23	25	17	11	13	14	0	1	7	16	4	15	6	8	5	3
	16	20	12	14	8	3	9	7	11	5	18	21	6	23	4	13	16	19	24	10	15	1	25	17	2	0	22
	17	4	17	13	20	21	9	24	25	10	7	15	19	8	12	11	0	16	5	23	14	2	3	1	18	22	6
	18	3	24	4	1	25	18	0	22	21	11	16	15	5	23	6	20	19	9	2	13	14	8	12	10	17	7
	19	20	22	21	17	6	23	4	1	3	19	16	0	9	18	24	2	14	7	13	12	11	10	8	15	5	25
	20	14	12	8	9	0	10	25	24	1	13	19	3	11	2	17	4	6	22	23	5	15	16	21	20	18	7
	21	24	9	3	19	20	16	25	5	22	18	12	17	0	21	7	6	4	8	15	23	2	14	10	11	13	1
	22	18	13	9	5	15	6	7	10	21	23	11	22	14	16	24	25	0	1	4	20	8	17	19	3	2	12
	23	15	21	18	16	6	25	5	12	14	11	17	10	7	4	13	1	24	9	20	2	22	8	23	19	3	0
	24	25	17	4	0	7	12	6	14	24	22	1	11	10	15	16	13	2	23	8	9	19	21	3	20	5	18
V[25][j]=V[23][V[24][j]]	25	0	9	6	15	12	7	5	13	3	23	21	10	17	1	24	4	18	19	14	11	2	8	16	22	25	20

Figure 3.8: Table de Vigenère 26×26.

Le chiffrement s'effectue de la manière suivante, soient :

- Texte claire (colonne) :
- Clé (ligne) :
- Texte chiffré :

4	5	2	10	7	12	7	13
8	**15**	**3**	**12**	**17**	**2**	**9**	**17**
11	10	25	19	25	11	24	12

Le déchiffrement consiste à repérer la valeur de la clé sur la colonne de gauche et on parcourt la ligne jusqu'à trouver la valeur du texte chiffré. Puis on remonte la colonne pour lire la lettre claire correspondante (tout en haut).

- Texte chiffré :
- Clé :
- Texte claire

11	10	25	19	25	11	24	12
8	**15**	**3**	**12**	**17**	**2**	**9**	**17**
4	5	2	10	7	12	7	13

A noter qu'une table de Vigenère 256×256 améliorée a été créée pour le chiffrement des images.

3.2.2 Technique de déchiffrement d'image chiffrée

Le déchiffrement se réalise d'une manière similaire dans le sens inverse. Le processus commence par la substitution inverse à l'aide de la table de Vigenère, l'image ainsi obtenue sera convertie en vecteur, afin d'appliquer le mécanisme de diffusion inverse sur le vecteur obtenu, ensuite, la permutation inverse sera effectuée sur le vecteur obtenu, et enfin une conversion vecteur-matrice sera réalisée pour récupérer l'image originale.

3.3 Résultats de simulation et analyse de sécurité

3.3.1 Environnement de travail

Toutes les simulations sont effectuées sur un ordinateur personnel. Le tableau 3.2 montre l'environnement matériel et logiciel, les valeurs des conditions initiales, les valeurs des différents paramètres, la base de données des images utilisées et d'autres spécifications.

Spécifications	
Processeur	Intel ® Core™ i5-2430M CPU 2.4GHZ
RAM	4GB
Système d'exploitation	Windows 8 professionnel
Langage de programmation	JAVA
Base de données des images	USC-SIPI [84] et UCID [85]
Taille des images couleurs choisies	128×128, 256×256, 512×512, 384×512 et 512×384
Conditions Initiale :	Valeurs :
• x_0	• 0.85914789414578
• y_0	• 0.75831478921547
• z_0	• 0.91514781245891
Paramètres de contrôle :	Valeurs :
• R	• 3.79
• α	• 0.0149
• β	• 0.019

Tableau 3.1 : Environnement de travail.

3.3.2 Test visuel

Le test visuel, est la première évaluation à effectuer sur l'image cryptée. Un système de chiffrement performant doit produire une image cryptée qui ne porte aucune information sur

l'image originale, autrement dit, un adversaire ne devrait pas pouvoir trouver une relation entre l'image originale et chiffrée.

Figure 3.9: Test visuel.

La figure 3.9 montre les image claires leurs résultats du chiffrement et du déchiffrement. Nous pouvons remarquer qu'il n'existe aucune similarité perceptuelle entre l'image originale et l'image cryptée correspondante.

3.3.3 Espace clé

L'attaque exhaustive consiste à essayer toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque est très coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive. Les clés utilisées dans notre approche sont : R, α, β, x_0, y_0 et z_0 des nombres réels à double précision codé chacun sur 64 Bits. Au total l'espace clé est de 384 Bits. Dans notre cas une attaque exhaustive nécessite 2^{384} essaies ce qui met largement la technique proposée dans ce chapitre à l'abri d'une attaque exhaustive [81].

3.3.4 Sensibilité à la clé

La sensibilité à la clé de chiffrement est une caractéristique essentielle pour tout algorithme de cryptage afin de tester sa résistance à une attaque brutale. Pour cela, nous avons crypté l'image « Lena 256×256 » en niveau de gris, en utilisant les clés x_0 =0.85914789414578, y_0=0.75831478921547, z_0=0.91514781245891, R=3.79, α=0.0149 et β=0.019, l'image cryptée est affichée dans la figure 3.10(a). Ensuite nous avons essayé de décrypter avec les mêmes clés légèrement modifiées (x_0=0.85914789414579, y_0=0.75831478921547, z_0= 0.91514781245891, R=3.79, α=0.0149 et β=0.019), ce test a été effectué sur plusieurs image de tailles différentes. La figure 3.10 illustre les résultats de simulation.

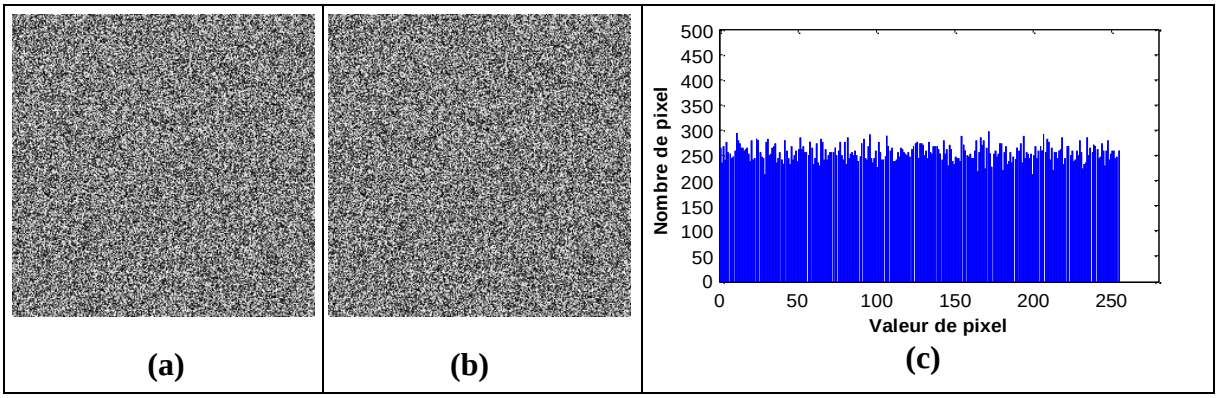

Figure 3.10: (a) « Lena 256×256 » niveau de gris cryptée avec la clé x_0 =0.85914789414579, (b) « Lena 256×256 » décryptée avec x_0+10^{-14}, (c) Histogramme de (b).

On constate dans la figure 3.10, qu'une modification infinitésimale (de l'ordre de 10^{-14}) sur les clés de cryptage, a produit une image complétement différente de l'originale, et avec un histogramme plat. Ce qui assure une hypersensibilité du schéma proposé à toute perturbation de la clé. Par conséquent, notre méthode est à l'abri des attaques brutales.

3.3.5 Analyse par histogramme

L'histogramme de l'image fournit l'information sur la distribution des niveaux de couleurs des pixels. Un intrus peut attaquer un algorithme de chiffrement par une analyse statistique en faisant analyser les histogrammes d'une image cryptée pour extraire quelques informations utiles de l'image claire. En effet, une image bien cryptée doit présenter un histogramme plat et uniformément distribué. Plus précisément, si l'histogramme de l'image cryptée est uniforme, alors il ne fournit ni information sur l'image originale ni relation entre cette dernière et l'image cryptée. Pour cela, nous avons analysé individuellement les trois canaux de couleurs rouge, vert et bleu de l'image « Pepper 512×512 ».

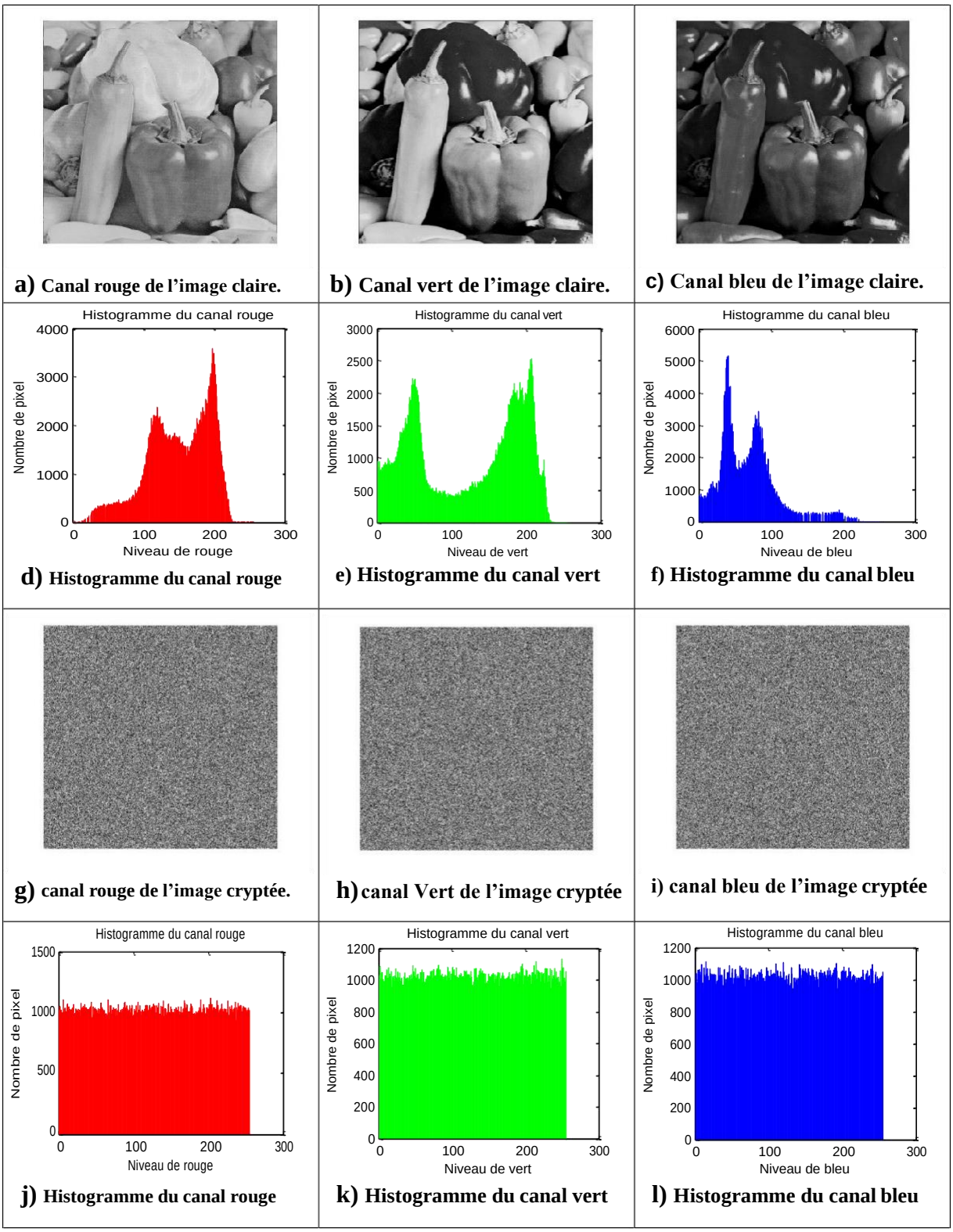

Figure 3.11: Analyse par histogramme.

Il ressort donc de la figure 3.11, que les histogrammes des trois canaux R, G et B des images chiffrées sont uniformément distribués par rapport aux histogrammes des trois canaux R, G et B de l'image originale. L'algorithme de chiffrement utilisé fait de sorte que la

dépendance des propriétés statistiques des images chiffrées et des images originales soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile car l'image chiffrée ne fournit aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir une attaque statistique sur le procédé de chiffrement d'images proposé.

3.3.6 Analyse par corrélations

En générale, la corrélation indique la relation linéaire entre deux variables aléatoires. Dans le traitement d'image, elle est souvent utilisée pour étudier la relation entre deux pixels adjacents. Naturellement, la corrélation entre les pixels adjacents pour l'image originale est très élevée. Dans ce contexte nous avons analysé les corrélations des pixels horizontaux, verticaux et diagonaux voisins pour les images originales et cryptées. Les équations qui donnent le coefficient de corrélation sont décrites dans le chapitre II section IV.4.b. Le tableau 3.2 illustre les résultats des simulations des coefficients de corrélation horizontaux, verticaux et diagonaux. La figure 3.12 montre les distributions de deux pixels adjacents.

Image	**Image originale**			**Image cryptée**		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
House	0.9782337	0.9529324	0.9362445	0.0067335	0.0006498	-0.0015399
Lena	0.9615757	0.9761491	0.9416661	-0.0014036	-0.0016485	-0.0056780
Pepper	0.9652828	0.9759218	0.9460511	0.0002810	0.0015651	0.0021876
Baboon	0.8396515	0.7194739	0.6984868	-0.0011286	0.0010581	-0.0036633

Tableau 3.2 : Coefficient de corrélation des pixels adjacents de l'image originale et cryptée.

Il ressort du tableau 3.2, que les coefficients de corrélation pour les images originales sont au voisinage de 1 ce qui montre que les pixels sont fortement corrélés. Alors que pour les images chiffrées les coefficients de corrélation sont au voisinage de 0 ce qui prouve que les pixels adjacents sont décorrélés pour les images chiffrées.

Dans le même contexte une évaluation concernant la distribution de la corrélation des pixels adjacents de l'image originale et celle de l'image cryptée illustrée dans la figure 3.12, reflète le comportement aléatoire de l'image cryptée.

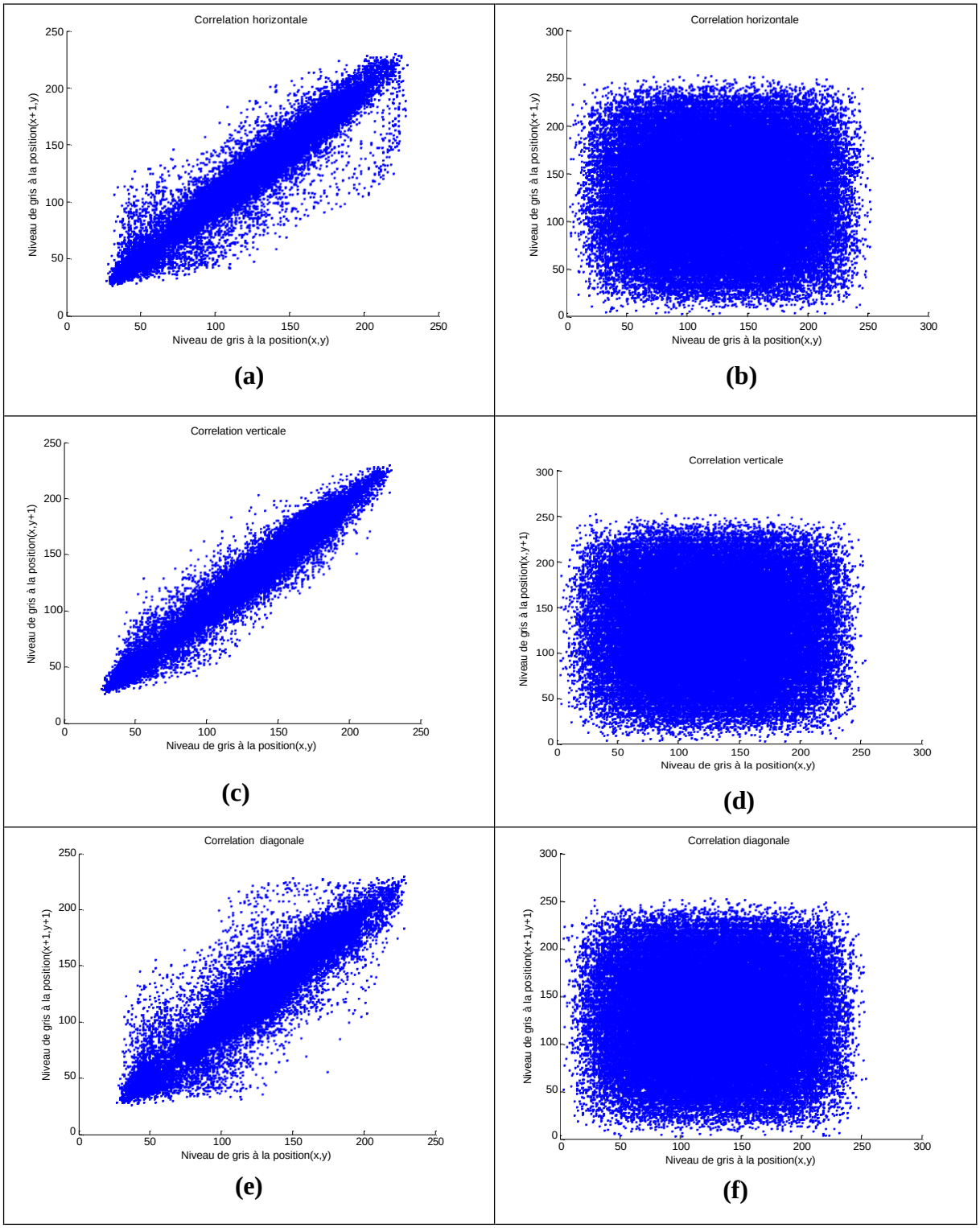

Figure 3.12: Distribution de la corrélation des pixels adjacents de « Lena 256×256 » originale dans les directions, (a) Horizontale, (c)Verticale, (e) diagonale : Distribution de la corrélation des pixels adjacents de l'image « Lena 256×256 » cryptée dans les directions, (b) Horizontale, (d) Verticale, (f) diagonale.

Une simple analyse des distributions des pixels adjacents montre bien que l'image cryptée a une distribution totalement aléatoire. Elle est différente de celle de l'image originale,

ceci conduit à dire que l'algorithme de cryptage proposé fait en sorte que la dépendance des propriétés statistiques de l'image cryptée et de l'image originale soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile.

3.3.7 Analyse par entropie

Selon la théorie de Shannon [28], 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. L'entropie est maximale pour une source dont tous les symboles sont équiprobables. Ainsi, pour une source d'information l'entropie est l'une des principales mesures de l'aléatoire de l'information. Une valeur élevée de l'entropie reflète un haut degré de caractère aléatoire, et pour tout message codé sur M bits, la valeur maximale de l'entropie est M. L'équations qui donne l'entropie est décrite dans le chapitre II section IV.4.c. Le tableau 3.3 ci-dessous montre les résultats des simulations de l'entropie pour les images originales et celles des images cryptées correspondantes.

Image	Originale	Cryptée
House256×256	7.068625071	7.999084298
Lena512×512	7.750197479	7.999791665
Peppers512×512	7.669825514	7.999772330

Tableau 3.3 : Entropie de l'image originale et l'image cryptée.

Il ressort du tableau 3.3, que les valeurs de l'entropie des images cryptées sont très proches de la valeur théorique (qui vaut 8), ce qui confirme l'uniformité des histogrammes des images cryptées, et prouve la résistivité de notre approche contre une attaque par entropie.

3.3.8 Analyse différentielle

Afin de détecter la relation entre l'image originale et l'image cryptée, un adversaire fait un petit changement sur une image claire, ensuite utilise l'algorithme de cryptage pour crypter cette image avant et après le changement, dans le but de tester comment une petite modification dans l'image originale affecte l'image cryptée. Ce genre d'attaque est appelé attaque différentielle. Pour assurer la sécurité d'un schéma de cryptage d'image contre toute attaque différentielle, deux mesures quantitatives sont utilisées : NPCR et l'UACI.

Le NPCR représente le taux de pixels différents entre les deux images chiffrées qui différent d'un pixel, tandis que l'UACI représente la différence de l'intensité moyenne. Les formules utilisées pour calculer NPCR et UACI sont définies dans le chapitre II section IV.6.

En effet, Une valeur de UACI > 33.4635 et NPCR > 99.6094 assure qu'un schéma de chiffrement d'image est immunisé contre une attaque différentielle. Le tableau 3.4 ci-dessous montre les résultats des simulations de UACI et NPCR pour les images originales et images cryptées correspondantes.

Image originale	**Image cryptée**	
	NPCR	**UACI**
Cameramen 256×256	99.641221	33.677555657
House 256×256	99.610705	33.486124674
Lena 512×512	99.610814	33.573320176
Peppers 512×512	99.613217	33.583128686

Tableau 3.4 : Valeurs de NPCR et UACI après le changement de la valeur d'un pixel.

Le tableau 3.4 montre que la valeur du NPCR est supérieure à 99.6094 et celle du UACI est supérieure à 33.4635. Ainsi la modification d'un seul pixel de l'image originale entraîne un changement radical de tous les pixels de l'image cryptée, alors on peut dire que notre algorithme présente une résistance contre une attaque différentielle.

3.3.9 Analyse par le pic du rapport signal à bruit (PSNR)

En considérant l'image originale comme un signal et celle cryptée comme un bruit, la vérification de la qualité de décryptage requiert le calcul de deux indicateurs particulièrement utilisés sont : MSE (Mean Square Error) donne l'erreur quadratique moyenne entre les deux images et le PSNR (Peak Signal to Noise Ratio), le pic du rapport signal à bruit, qui donne une idée plus précise de la dégradation d'une image. MSE et PSNR s'évaluent selon les formules indiquées dans le chapitre II section IV.7. Le tableau 3.5 montre les résultats des simulations obtenus.

Image	**MSE**	**PSNR**
Cameramen 256×256	11762.830184936	7.425685335
House 256×256	8337.192377726	8.920605380
Lena 512×512	8944.887575785	8.615054743
Peppers 512×512	10102.421716054	8.086548671

Tableau 3.5 : PSNR et MSE.

3.3.10 Temps d'exécution

En plus des performances citées précédemment, le temps d'exécution est aussi une caractéristique importante d'un algorithme de cryptage d'image, surtout pour l'adopter dans un chiffrement en temps réel. En utilisant les spécificités indiquées dans le tableau 3.1 nous avons obtenu les résultats montrés dans le tableau 3.6 et une comparaison avec des algorithmes existants :

Image (pixel)	**Méthode proposée**	**Réf.** [12]	**Réf.** [96]	**Réf.** [90]
256×256	0.109	------	0.90	0.281
512×512	1.215	0.8645	7.86	1.164

Tableau 3.6 : Temps d'exécution en seconde.

Le tableau 3.6 montre que notre méthode possède un temps d'exécution acceptable. Par conséquent le système de cryptage proposé est adéquat à des applications en temps réel.

3.4 Comparaison et discussion

Afin de valider les performances du schéma proposé, nous allons comparer les résultats de simulation obtenus avec d'autres approches récentes, en termes d'espace clé, entropie, coefficient de corrélation, NPCR, UACI et PSNR.

Approche	**Méthode proposée**	**Réf.** [12]	**Réf.** [96]	**Réf.** [90]
Espace clé	2^{384}	2^{448}	2^{216}	2^{240}

Tableau 3.7 : Espace clé de la méthode proposée et d'autres existantes dans la littérature.

Le tableau 3.7 montre que l'espace clé est assez grande que 2^{100} [81]. Par conséquent, le schéma proposé peut résister à toutes sortes d'attaques exhaustives.

Image	**Entropie**				
	Originale	**Méthode proposée**	**Réf.** [12]	**Réf.** [96]	**Réf.** [90]
Baboon 512×512	7.762436	7.999784	7.999773	7.999766	7.9981000
Lena 512×512	7.750197	7.999791	7.999767	7.999767	7.9994000
Airplane 512×512	6.663908	7.999755	7.999780	7.999786	7.9991000
Pepper 512×512	7.669825	7.999772	7.999772	7.999772	7.9983000
Girl 256×256	6.898139	7.999073	7.999016	7.999178	-------
House 256×256	7.068625	7.999084	7.999127	7.999017	-------

Tableau 3.8 : Entropie de la méthode proposée et d'autres existantes dans la littérature.

Nous pouvons remarquer que les valeurs d'entropie obtenues sont meilleures pour certaines images. Cela est dû à la robustesse du générateur pseudo-aléatoire utilisé et à l'amélioration apportée à la table de Vigenère.

Méthodes	**Lena 512×512**			**Baboon 512×512**		
	Horizontale	**Verticale**	**Diagonale**	**Horizontale**	**Verticale**	**Diagonale**
Méthode proposée	-0.0014036	-0.00164	-0.00567	-0.00112	0.00105	-0.0036
Réf. [12]	0.0000279	-0.00178	-0.00385	0.000081	0.01020	0.00271
Réf. [96]	-0.0045587	-0.01948	0.009401	0.000559	0.00275	0.00146
Réf. [90]	0.000800	0.00210	0.000500	0.001600	0.00480	0.00240

Tableau 3.9 : Comparaison des coefficients de corrélation.

Il ressort du tableau 3.9 que le coefficient de corrélation a été considérablement réduit, cela est dû à la permutation chaotique et à la confusion appliquée par la table de Vigenère améliorée. Vu que les coefficients de corrélation sont très proches de zéro ceci élimine toute attaque par corrélation.

Image	UACI & NPCR							
	Méthode proposée		**Réf.** [12]		**Réf.** [96]		**Réf.** [90]	
	NPCR	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**
Baboon	99.6132	33.5893	99.6125	33.4397	99.6117	33.4833	99.23	33.31
Lena	99.6108	33.5733	99.6047	33.4761	99.5994	33.4709	99.63	33.59
Airplane	99.6150	33.5820	99.6079	33.4695	99.6107	33.4380	99.48	33.35
Pepper	99.613217	33.5831	99.6060	33.4797	99.5998	33.4793	99.30	33.00

Tableau 3.10 : Comparaison des constantes différentielles.

D'après le tableau 3.10, il semble clair que les valeurs de NPCR et UACI sont meilleurs que d'autres obtenues dans la littérature. Cela est dû au mécanisme de diffusion appliqué et au générateur pseudo-aléatoire amélioré que nous avons utilisé.

Image	PSNR			
	Méthode proposée	**Réf.** [12]	**Réf.** [96]	**Réf.** [90]
Baboon	8.770528602	8.771542313	8.776262857	9.521307186
Lena	8.615054743	8.611692609	8.616901712	9.236306195
Airplane	7.973539604	7.971561784	7.985145007	8.001615162
Pepper	8.086548671	8.075978269	8.073717583	8.871923922

Tableau 3.11 : Comparaison du PSNR.

D'après le tableau 3.11, le PSNR obtenu par la méthode proposée a une faible valeur. C'est-à-dire que c'est très difficile de reconstruire l'image originale à partir de l'image cryptée sans possession de la clé (une valeur faible du PSNR implique que l'image est randomisée). Cela est dû à la structure adoptée dans notre algorithme basée sur une couche de permutation, une couche de diffusion et une couche de substitution.

3.5 Conclusion

Dans ce chapitre, à l'aide d'un système chaotique 3D dont les propriétés statistiques ont été améliorées, d'une nouvelle table de Vigenère, et d'un bon mécanisme de diffusion, nous avons proposé un nouvel algorithme de chiffrement d'images couleur et niveau de gris. Grâce

aux bonnes propriétés statistiques de GPACLEA l'algorithme proposé nous offre un excellent processus de confusion et de diffusion ce qui assure une sécurité élevée. La confusion et la diffusion ont été obtenues en utilisant la permutation, la substitution et l'effet d'avalanche inséré par le mécanisme de diffusion, par conséquent toute modification apportée à un bit d'un seul pixel aléatoire sera répercutée sur l'image entière. Ceci se justifie par la valeur de la constante statique UACI. En outre les valeurs des coefficients de corrélation qui sont proches de zéro, confirme que la dépendance des propriétés statistiques de l'image cryptée et celle originale est presque aléatoire. L'histogramme plat de l'image cryptée reflète une valeur d'entropie maximale. En fin un espace clé large (2^{384}) et une grande sensibilité à la clé due à l'utilisation de la carte chaotique étendue améliorée, met à l'abri notre approche contre toute attaque brutale.

En se basant sur les résultats obtenus, nous pouvons affirmer que la technique proposée est adaptée pour les applications de chiffrement d'image. Dans le chapitre qui suit, nous allons introduire notre troisième contribution, qui consiste en un schéma de chiffrement pour les images numériques basée sur une nouvelle variante sécurisée du chiffre de HILL et cartes chaotiques 1D.

Chapitre 4

Cryptage d'images couleurs basé sur une nouvelle variante sécurisée du chiffre de HILL et des cartes chaotiques 1D.

Sommaire

4.1 Introduction

Au cours des dernières années, les technologies de l'information et de la communication ont connu un immense développement. Surtout avec l'expansion de l'internet, le transfert sécurisé d'information est devenu nécessaire et très utilisé dans le monde virtuel afin de protéger ces données à caractère personnel ou confidentiel. Récemment, les réseaux ont fortement évolué et sont reconnus inévitables pour la communication moderne. Les informations multimédias transmises sur ces réseaux sont des données qui présentent des particularités remarquables, du fait de leur quantité importante d'information. En particulier, la transmission des images soulève un nombre important de problèmes. Nous citons, la confidentialité, et l'intégrité [1]. Ainsi, une forte sécurité doit être assurée en raison des menaces telles que le piratage, l'espionnage et l'escroquerie. Le cryptage d'image est différent du texte en raison de certaines caractéristiques intrinsèques, telles que la forte corrélation entre les pixels adjacents et la redondance. Par conséquent, les systèmes traditionnels tels que DES [5], AES [22] et Blowfish [97] ne conviennent pas pour le cryptage d'images. Actuellement, de nombreux mécanismes de chiffrement d'image ont été proposés dans la littérature en utilisant diverses méthodes. Ainsi, l'utilisation des systèmes chaotiques en cryptographie ont attiré l'attention d'un grand nombre de chercheurs, en raison de leur sensibilité aux conditions initiales et de leur non linéarité. En effet, de nombreux algorithmes de chiffrement d'image basés chaos ont été proposés [77] [12] [90]. Particulièrement, la carte chaotique unidimensionnelle (1D) est l'une des systèmes chaotiques populaire caractérisée par sa simplicité, sa rapidité de mise en œuvre dans les systèmes numériques, et sa faible consommation des ressources. Cependant, cette carte présente des faiblesses à savoir, la distribution non uniforme, l'espace clé réduit et la périodicité [17]. Récemment, plusieurs auteurs ont amélioré avec succès la carte logistique pour surmonter ces faiblesses, afin de renforcer la sécurité [15] [25].

Le Chiffre de HILL (CH) [98] [34] est l'un des algorithmes à clés symétriques qui a montré des avantages pour le cryptage de données. Cependant l'algorithme original est vulnérable aux « Attaque à Texte Clair Choisi » [51]. Un autre revers pour le cryptage des images est qu'il révèle certaines tendances et ne cache pas toutes les caractéristiques de l'image (images avec des fortes corrélation des pixels adjacents). De plus, CH dans sa version originale et presque toutes les versions proposées nécessitent l'existence d'une matrice clé inversible de déchiffrement [24]. Cela peut devenir une problématique car une matrice clé inversible n'existe pas toujours. Dans l'objectif de rendre le CH plus sécurisé et efficace au chiffrement des images

numériques, plusieurs travaux de recherches ont été réalisés [72] [99] [24] [100] [79] [77].

Dans ce chapitre, nous allons proposer un nouvel algorithme de chiffrement d'image couleur et niveau de gris basé sur des cartes chaotiques 1D et le CH. La nouveauté de l'approche proposée consiste à améliorer les propriétés chaotiques des cartes 1D qui serviront à produire des séquences chaotiques caractérisées par une uniformité remarquable, une hypersensibilité aux conditions initiales, et surtout d'excellentes propriétés statistiques. Les séquences chaotiques obtenues sont utilisées dans l'architecture du crypto système proposé pour générer les paramètres d'un vecteur de translation, et ceux d'une matrice clé de chiffrement sous forme d'entiers quelconques dans l'anneau $\mathbb{Z}/256\mathbb{Z}$ sauf l'élément situé à la fois dans la première ligne et la première colonne qui doit être impaire pour qu'on puisse déterminer son inverse dans l'anneau $\mathbb{Z}/256\mathbb{Z}$ qui sera utilisé dans le processus de déchiffrement. La méthode offre un chiffrement pixel-par-pixel contrairement au CH conventionnel qui chiffre les couples de pixels adjacents deux à deux ce qui présente une solution adéquate au problème du chiffrement des images présentant des fonds noirs ou fortement homogènes. Notre algorithme évite le problème du faible espace clé des cartes chaotiques 1D classiques. De plus, une analyse de sécurité est présentée pour vérifier la robustesse du processus de chiffrement par rapport aux attaques connues.

4.2 Description de la méthode proposée

Dans cette section on va s'intéresser premièrement, à la validation du système chaotique utilisé pour générer les séquences pseudo-aléatoires employées dans le processus de chiffrement. Ensuite nous détaillerons les deux mécanismes de chiffrement et déchiffrement proposés dans notre schéma.

4.2.1 Cartes chaotiques unidimensionnelles (1D)

Les cartes chaotiques 1D sont caractérisées par une structure simple et une facilité d'implémentation, de sorte qu'elles sont largement utilisées dans le chiffrement des données de grande taille en temps réel. Hélas, elles présentent plusieurs faiblesses [17], dont je cite, la discontinuité, la non-uniformité, la courte périodicité, et l'espace clé faible. Pour surmonter ces faiblesses nous avons amélioré le comportement chaotique des cartes chaotiques 1D classiques : Carte Logistique CL, Carte Tchebychev CC et Carte Sine CS . Et ceci à travers une simple multiplication par une fonction d'ajustement $G(k)$ avec $5 \leq k \leq 10$ et une application de

l'arithmétique modulaire (mod 1). Le tableau 4.1 ci-dessous montre les cartes chaotique 1D classiques et améliorées.

Carte chaotique	Expression	Paramètres
CL	$x_{n+1} = F_L(\mu, x_n) = \mu x_n(1 - x_n)$	$\mu \in [0,4]$: Paramètre de contrôle. x_0 : Valeur initiale. x_n : Séquence chaotique de sortie.
CLA	$x_{n+1} = F_1(\mu, x_n, k) = \mod((F_L(\mu, x_n) \times G(k)), 1)$	
CC	$y_{n+1} = F_C(r_1, y_n) = \cos(r_1 \arccos(y_n))$	$r_1 \in \mathbb{N}$: Paramètre de contrôle. y_0 : Valeur initiale. y_n : Séquence chaotique de sortie.
CCA	$y_{n+1} = F_2(r_1, y_n, k) = \mod((F_C(r_1, y_n) \times G(k)), 1)$	
CS	$z_{n+1} = F_S(r_2, z_n) = r_2 \sin(\pi(z_n))$	$r_2 \in]0,1[$: Paramètre de contrôle. z_0 : Valeur initiale. z_n : Séquence chaotique de sortie.
CSA	$z_{n+1} = F_3(r_2, z_n, k) = \mod((F_S(r_2, z_n) \times G(k)), 1)$	

Tableau 4.1 : Cartes chaotiques 1D classiques et améliorées.

CLA, CCA et CSA présentent respectivement Carte Logistique Améliorée, Carte Chebyshev Améliorée et Carte Sine Améliorée. $F_L(\mu, x_n)$, $F_C(r_1, y_n)$, et $F_S(r_1, z_n)$ présentent respectivement CL, CC et CS, tandis que $F_1(\mu, x_n, k)$, $F_2(r_1, y_n, k)$ et $F_3(r_2, z_n, k)$ présentent les cartes chaotiques améliorées.

Dans cette section on va effectuer une analyse comparative permettant l'évaluation et la validation des propriétés chaotiques des cartes 1D classiques et améliorées en termes de l'exposant de Lyapunov (Figure 4.1), de densité de distribution (Figure 4.2) et du diagramme de bifurcation (Figure 4.3).

L'un des outils mathématiques qui servent à caractériser le comportement chaotique d'un système dynamique non linéaire est l'exposant de Lyapunov. Lorsque l'exposant est positif, la carte est chaotique, et plus cette valeur est grande, plus on aura des performances chaotiques. Les exposants de Lyapunov des cartes chaotiques unidimensionnelles classiques et de leurs améliorations sont montrés dans la figure 4.1 ci-dessous :

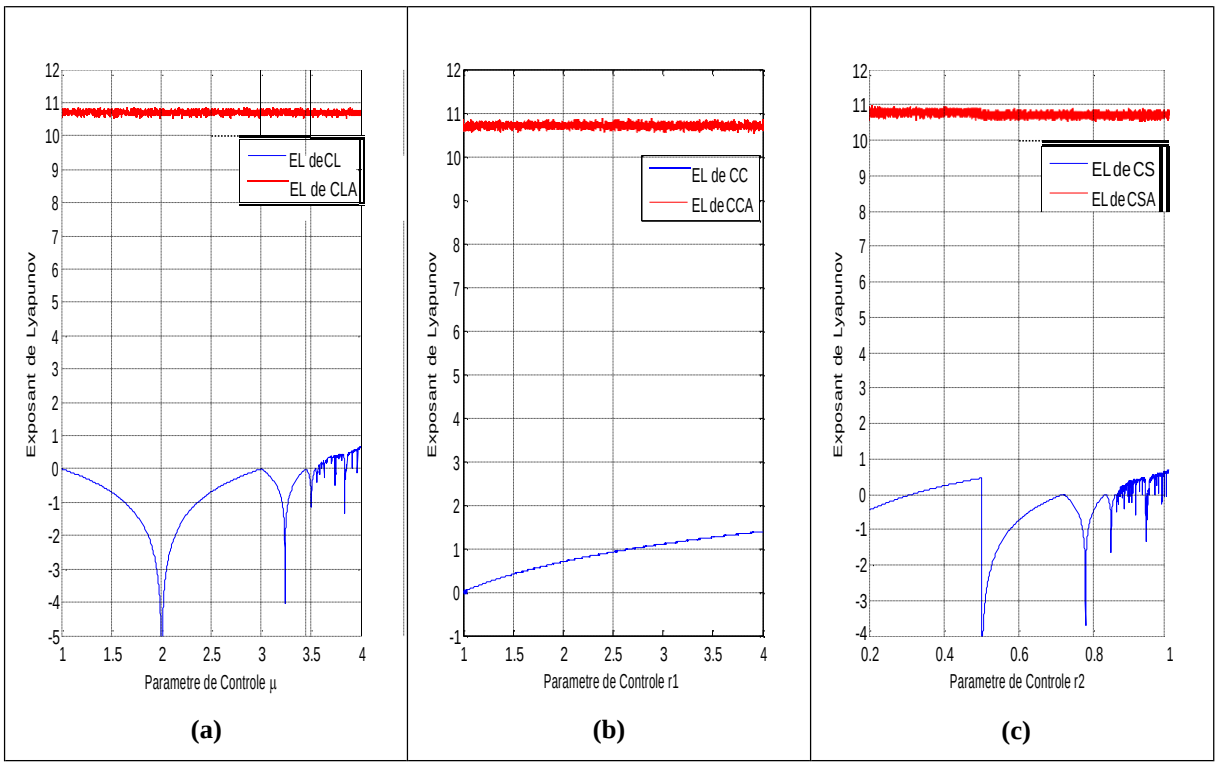

Figure 4.1: Exposant de Lyapunov de : (a) CL et CLA ; (b) CC et CCA ; (c) CS et CSA.

Dans la figure 4.1 les valeurs des exposants de Lyapunov obtenues pour les cartes 1D améliorées (courbes rouges) sont meilleures par rapport à celles des cartes 1D classiques (courbes bleues). Par conséquent, les cartes chaotiques améliorées 1D présentent une forte dépendance aux conditions initiales (une des propriétés du chaos), et aussi une divergence exponentielle de l'écart entre deux trajectoires chaotiques ayants des conditions initiales très voisines.

En cryptographie, la distribution des séquences chaotiques à une grande importance. Une carte chaotique performante doit produire une répartition uniforme des valeurs dans l'intervalle]0,1[. Les densités de distribution des cartes chaotiques 1D et celles de leurs améliorations sont montrées dans la figure 4.2 suivante :

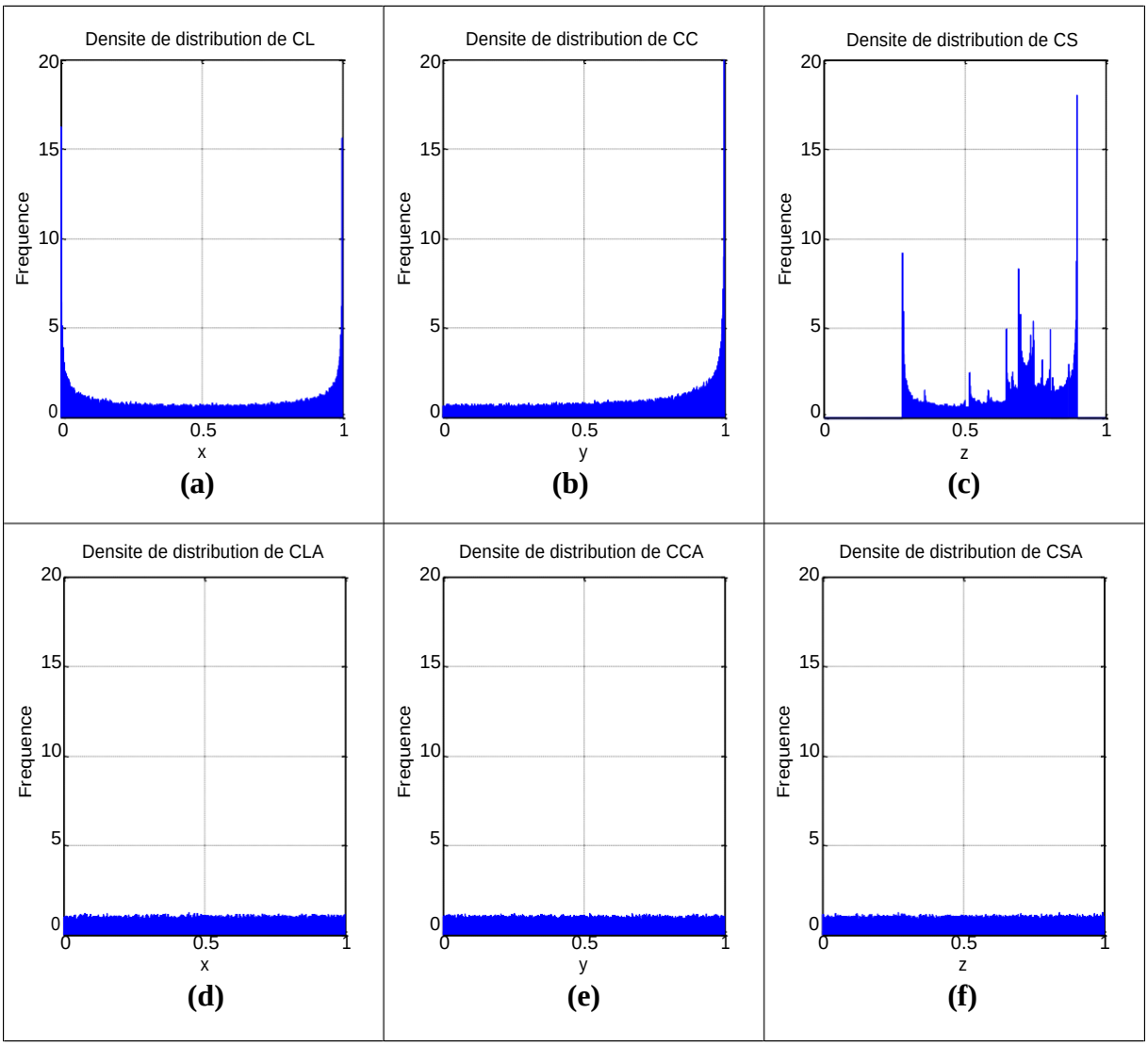

Figure 4.2: Densité de distribution de : (a) CL ; (b) CC; (c) CS ; (d) CLA ;(e) CCA ; (f) CSA.

Il apparait que le système chaotique proposé présente une densité de distribution uniforme, contrairement aux trois cartes 1D qui présentent de mauvaises densités de distribution. Et par conséquent, les cartes chaotiques améliorées possèdent d'excellentes propriétés statistiques.

Une analyse qualitative d'une carte chaotique peut être réalisée par l'étude de son diagramme de bifurcation. Qui représente le comportement asymptotique d'un système dynamique discret en fonction de paramètre de contrôle. Le schéma de la figure 4.3 ci-dessous montre les diagrammes de bifurcation des trois cartes chaotiques 1D classiques et améliorées.

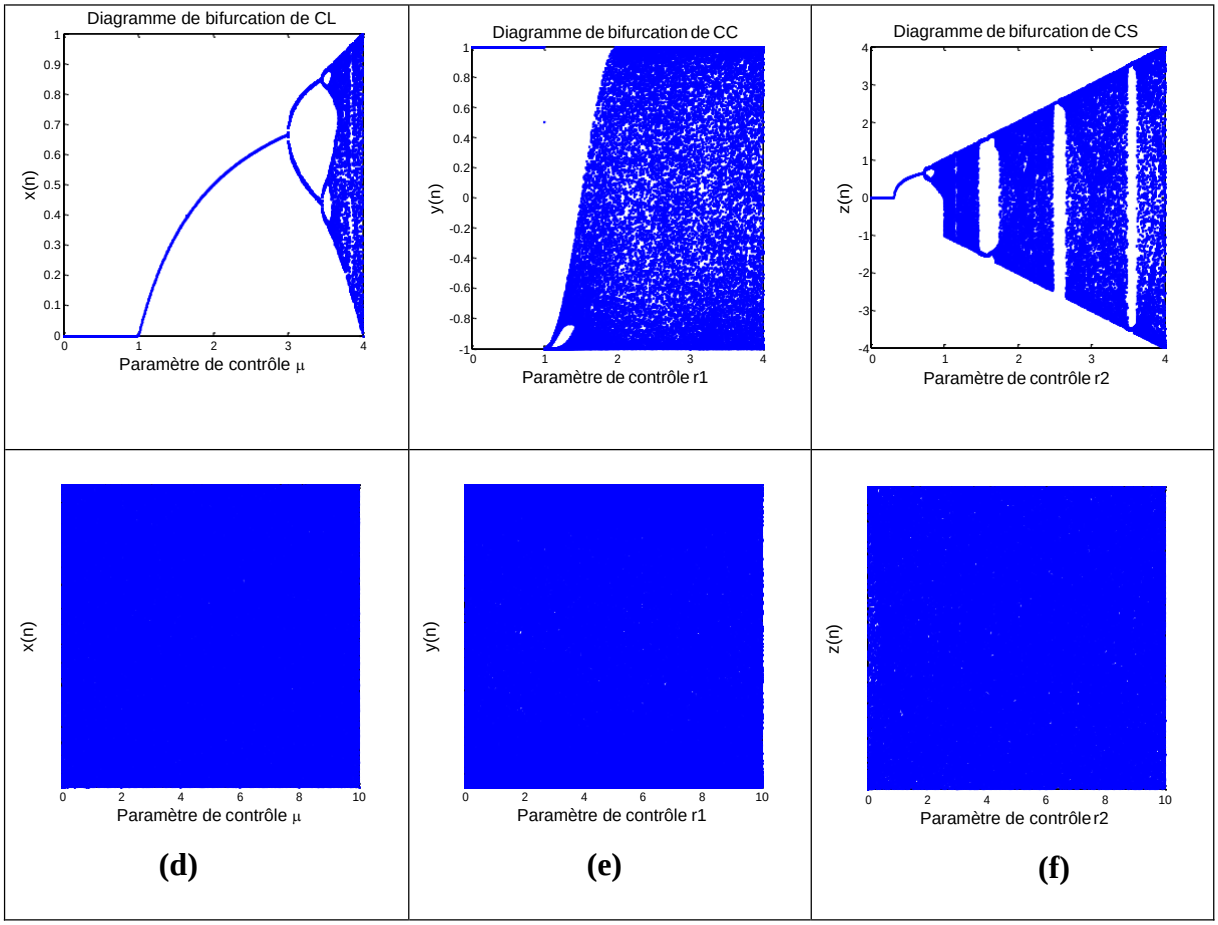

Figure 4.3: Diagramme de bifurcation de : (a) CL; (b) CC ; (c) CS; (d) CLA ;(e) CCA; (f) CSA.

Les diagrammes de bifurcation des cartes chaotiques CL, CC et CS indiqués respectivement dans la figure 4.3(a), 4.3(b) et 4.3(c) ne présentent le comportement chaotique que sur des intervalles limités (zone chao) lorsque le paramètre de contrôle varie dans l'intervalle $[0,4]$. Par contre, ceux des cartes chaotiques améliorées CLA, CCA et CSA indiqués respectivement dans la figure 4.3(d), 4.3(e) et 4.3(f) montrent un comportement chaotique assez large.

Une comparaison des propriétés chaotiques des cartes chaotiques 1D et celles des cartes chaotiques améliorées en termes de densité de distribution de l'exposant de Lyapunov, et de bifurcation montrent la qualité et la robustesse de CLA, de CCA et de CSA. Par conséquent, l'amélioration adoptée possède d'excellentes performances chaotiques, et est favorable à être utilisé dans des systèmes cryptographiques robustes. Ainsi dans la suite de cet article nous avons adopté les séquences pseudo-aléatoires provenant des cartes chaotiques améliorées pour le chiffrement des images numériques.

4.2.2 Processus du chiffrement

L'objectif principal du système de chiffrement d'images numériques proposé dans ce chapitre, est d'avoir un niveau élevé de confusion en utilisant une forte relation entre l'image chiffrée et la clé, une forte diffusion en utilisant un mode de chainage puissant, et d'un espace clé assez large pour mettre le crypto système à l'abri des attaques exhaustives [81]. Dans le schéma proposé le chiffrement de chaque pixel de l'image claire est assuré par le produit d'un vecteur constitué du couple pixel-clé et d'une matrice de Hill d'ordre 2×2 d'une part, et de l'ajout d'un vecteur chaotique d'autre part (voir équations 4.2 et 4.4). Outre le pixel crypté, ce processus génère un bruit qui sera incorporé dans le pixel voisin (Voir équations 4.1 et 4.3). En effet, le chiffrement d'un pixel dépend fortement de son voisin. Et par conséquent, la modification d'un seul pixel de l'image originale entraîne un changement radical de tous les pixels de l'image cryptée, ce qui offre une forte résistance face aux attaques différentielles [100]. La clé utilisée est constituée de : μ, r_1, r_2, β, x_0, y_0 et z_0 des nombres réels à double précision codé chacun sur 64 bits, au total l'espace clé est de 384 bits, donc toute attaque exhaustive demande 2^{384} opérations, ce qui assure une résistance face aux attaques brutales. Le schéma proposé comprend six étapes :

- **Etape 1 :** Choix de μ, r_1, r_2, β, x_0, y_0 et z_0.
- **Etape 2** : Génération des trois matrices clés K_1, K_2, et K_3 à partir des trois cartes chaotiques CLA, CSA, CCA respectivement avec :
  - $K_1(i) = \mathrm{mod}(\mathrm{floor}(x_i \times 10^6), 256)$,
  - $K_2(i) = \mathrm{mod}(\mathrm{floor}(y_i \times 10^6), 256)$,
  - $K_3(i) = \mathrm{mod}(\mathrm{floor}(z_i \times 10^6), 256)$,

  avec $\mathrm{floor}(x)$ est une fonction qui renvoie le plus grand entier inférieur ou égal à x, $\mathrm{mod}(x, y)$ renvoie le reste de la division entière de x par y et $i = 1, \dots, w \times h$.
- **Etape 3** : Génération des paramètres h_{11}, h_{12}, h_{21} et h_{22} de la matrice clé de Hill d'ordre 2×2 à partir de CLA. Avec h_{11} doit être un entier impair pour qu'on puisse calculer son inverse dans l'anneau $\mathbb{Z}/256\mathbb{Z}$.
- **Etape 4 :** Extraction des pixels P(i, j) de l'image originale. Avec $i = 1, \dots, w$. Et w est la largeur de l'image. $j = 1, \dots, h$. Avec h est la hauteur d l'image.
- **Etape 5 :** Conversion de l'image en vecteur de taille $w \times h$.
- **Etape 6 :** Chiffrement du premier pixel $P(1)$ et bruitage de son voisin $P(2)$ comme suit :

$$\begin{pmatrix} C(1) \\ T(1) \end{pmatrix} = \left(\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} P(1) \\ K_1(1) \end{pmatrix} + \begin{pmatrix} K_2(1) \\ K_3(1) \end{pmatrix} \right) \bmod 256 \quad (4.1)$$

$$S(2) = (T(1) + P(2)) \bmod 256 \quad (4.2)$$

avec $C(1)$ est le premier pixel chiffré, et $S(2)$ est le deuxième pixel randomisé.

- **Etape 7 :** Chiffrement des autres pixels de l'image comme suit :

$$\begin{pmatrix} C(i) \\ T(i) \end{pmatrix} = \left(\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} S(i) \\ K_1(i) \end{pmatrix} + \begin{pmatrix} K_2(i) \\ K_3(i) \end{pmatrix} \right) \bmod 256 \quad (4.3)$$

$$S(i+1) = (T(i) + P(i+1)) \bmod 256 \quad (4.4)$$

avec $i = 1, \dots, w \times h - 1$.

La figure 4.4 ci-dessous, montre le principe de chiffrement d'images par notre méthode.

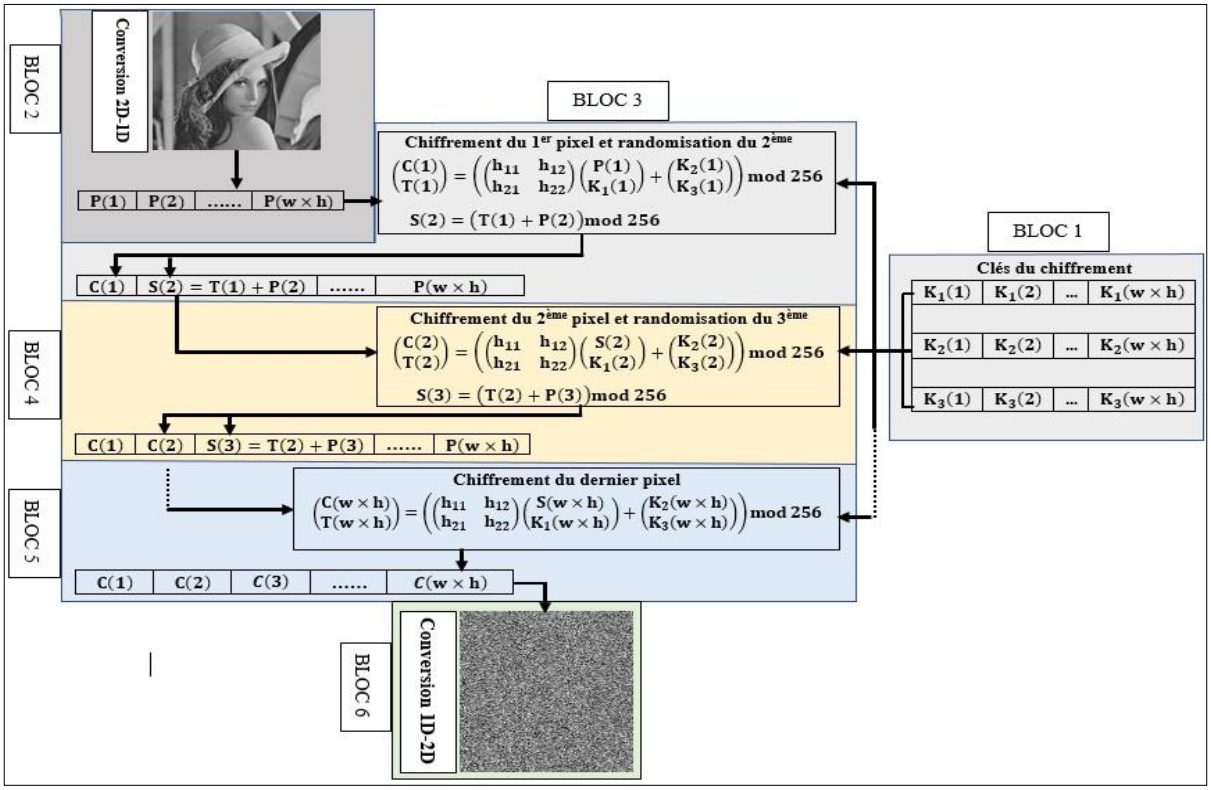

Figure 4.4: Schéma du chiffrement.

Le schéma de la figure 4.4 illustre le principe de chiffrement qui repose sur les blocs suivants :

Bloc 1 : Ce bloc montre les trois clés utilisées K_1, K_2 et K_3.

Bloc 2 : La matrice obtenue après l'extraction des pixels de l'image claire sera convertie en vecteur $P(i)$.

Bloc 3 : Le processus de chiffrement commence par le premier pixel $P(1)$, et est assuré par le produit d'une matrice clé de Hill $H = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix}$ avec le vecteur $\begin{pmatrix} P(1) \\ K_1(1) \end{pmatrix}$ dont $P(1)$ est le premier pixel de l'image claire et $K_1(1)$ est l'élément correspondant de la clé K_1, suivi d'une addition d'un vecteur chaotique $\begin{pmatrix} K_2(1) \\ K_3(1) \end{pmatrix}$ pour un chiffrement adéquat des images qui présentent un fond noir ou homogène (voir équations 4.1 et 4.3). Ainsi, nous obtenons le premier pixel crypté $C(1)$ et le paramètre $T(1)$ qui sera utilisé pour randomiser le pixel adjacent. En effet, le bruit ajouté sert à casser la forte corrélation entre les pixels adjacents, ceci est prouvé par un coefficient de corrélation faible (voir tableau 4.2) et d'une distribution totalement aléatoire des pixels adjacents de l'image cryptée dans les directions, horizontale, verticale, et diagonale (voir figure 4.8).

Bloc 4 : Le processus de chiffrement est appliqué sur le pixel randomisé $S(2)$ pour produire le pixel crypté $C(2)$ et générer le bruit $T(2)$ qui sera utilisé pour bruiter le pixel adjacent.

Bloc 5 : Le processus décrit dans les blocs 3 et 4 se poursuit jusqu'au dernier pixel crypté $C(w \times h)$.

Bloc 6 : Le vecteur constitué des pixel cryptés $C(1), C(2), \ldots, C(w \times h)$ sera converti en matrice pour construire l'image cryptée. A noter que le système de chiffrement proposé est valable pour chiffrer les images en niveau de gris et couleurs [84].

4.2.3 Processus du déchiffrement

Le processus de déchiffrement commence lorsque le destinataire reçoit l'image chiffrée, par extraction des valeurs des pixels cryptés $C(i, j)$, suivi de la détermination de l'inverse h_{11}^{-1}, et finalement application des équations (4.5) et (4.7) pour restaurer les valeurs des pixels originaux.

Les étapes de la méthode proposée pour le déchiffrement sont :

- **Etape 1 :** Extraction des pixels cryptés de l'image chiffrée C.
- **Etape 2 :** Conversion de l'image cryptée en vecteur de taille $w \times h$.
- **Etape 3 :** Déchiffrement du premier pixel $C(0)$ comme suit :

$$P(0) = (h_{11}^{-1}(C(0) - h_{12} \times K_1(0) - K_2(0)))\ \bmod\ 256 \quad (4.5)$$

$$tmp = (h_{21} \times C(0) + h_{22} \times K_1(0) + K_3(0)) \bmod 256 \quad (4.6)$$

avec tmp est une variable temporaire qui sera calculée à chaque itération, ensuite utilisée pour déchiffrer le pixel suivant.

- **Etape 4 :** Déchiffrement des autres pixels de l'image cryptée comme suit :

$$P(i) = (h_{11}^{-1}(C(i) - h_{12} \times K_1(i) - K_2(i)) - tmp) \bmod\ 256 \quad (4.7)$$

$$tmp = (h_{21} \times C(i) + h_{22} \times K_1(i) + K_3(i)) \bmod 256 \quad (4.8)$$

avec $i = 0,1, \dots, w$ et $j = 0,1, \dots, h$.

- **Etape 5 :** Conversion du vecteur image P en matrice pour restaurer l'image originale.

4.3 Résultats de simulation et analyse de sécurité

Plusieurs simulations visant à évaluer les propriétés du schéma proposé, notamment la sensibilité à la clé du chiffrement, l'analyse par histogramme, les coefficients de corrélation, l'entropie, le PSNR, le NPCR, l'UACI et l'analyse de la vitesse, ont été effectuées. Les simulations ont été réalisées à l'aide des images de la base de données USC-SIPI [84] et de la base de données non compressées d'images couleur (UCID) [85]. Toutes les simulations ont été effectuées sous l'environnement indiqué dans le tableau 3.1. Les paramètres utilisés comme clé sont les suivants : x_0 = 0.75147854321781, y_0=0.92791237172793, z_0 = 0.61247892775319, μ=3.9745453232121279 ; r_1=0.14785214785423 et r_2 = 0.61247892775319. Les résultats de simulation sont illustrés dans la figure 4.5. Les première et quatrièmes rangées affichent les images en clair, les deuxième et cinquième indiquent les images chiffrées et les troisième et sixième affichent les images déchiffrées. Nous remarquons clairement que les images chiffrées sont complétement randomisées, totalement différentes des images originales, de plus il n'existe aucune caractéristique dans l'image chiffrée qui puisse être extraite ou utilisée pour identifier l'image originale.

4.3.1 Robustesse aux attaques brutales

La clé utilisée dans notre schéma est constituée des trois valeurs initiales x_0, y_0, z_0 et les trois paramètres de contrôles des trois cartes chaotiques μ , r_1 et r_2, au total six nombres réels à double précision codé chacun sur 64 bits, alors l'espace clé est de 384 bits. Du point de vue

cryptographique, la taille de l'espace de clé ne doit pas être inférieure à 2^{100} [81], pour assurer un niveau élevé de sécurité. Dans notre cas une attaque exhaustive nécessite 2^{384} essaies, ce qui met le schéma proposé largement à l'abri d'une attaque exhaustive.

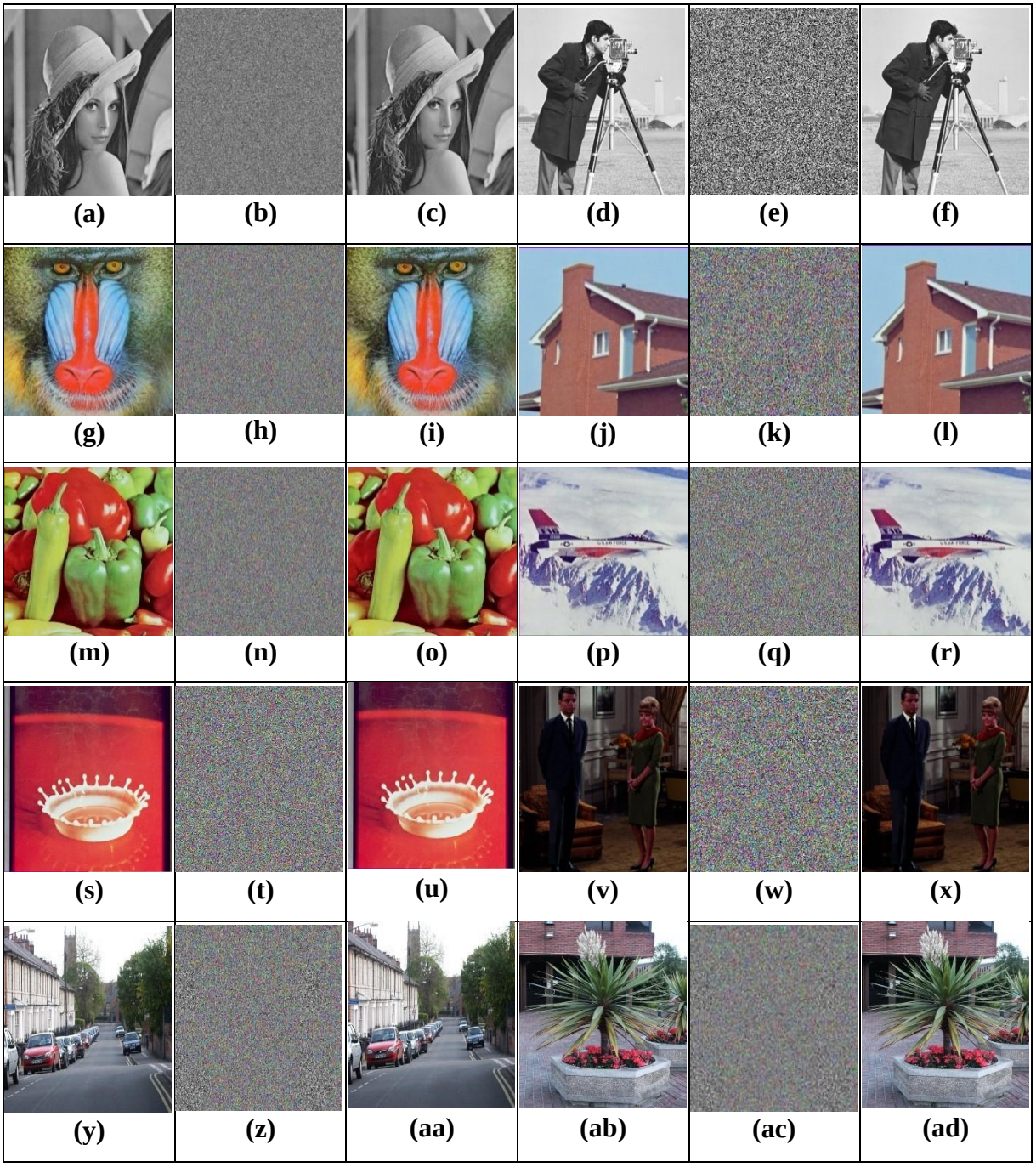

Figure 4.5: (a, d, g, j, m, p, s, v, y, ab) Images originales ; (b, e, h, k, n, q, t, w, z, ac) Images chiffrées ; (c, f, i, l, o, r, u, x, aa, ad) Images déchiffrées.

4.3.1 Sensibilité à la clé de chiffrement

Un schéma de chiffrement d'image robuste doit être sensible à la clé. C'est à dire une modification d'un seul bit dans la clé secrète devrait produire une image chiffrée totalement

différente. Pour évaluer la sensibilité du schéma proposé à la clé de chiffrement, nous avons effectué les étapes suivantes :

- **Etape 1 :** Une image claire est chiffrée en utilisant la clé de cryptage.
- **Etape 2 :** La même image originale est chiffrée en effectuant un léger changement dans la clé secrète.
- **Etape 3 :** Une différence a été effectuée sur les deux images chiffrées obtenues.

Figure 4.6 ci-dessus montre les résultats des simulations.

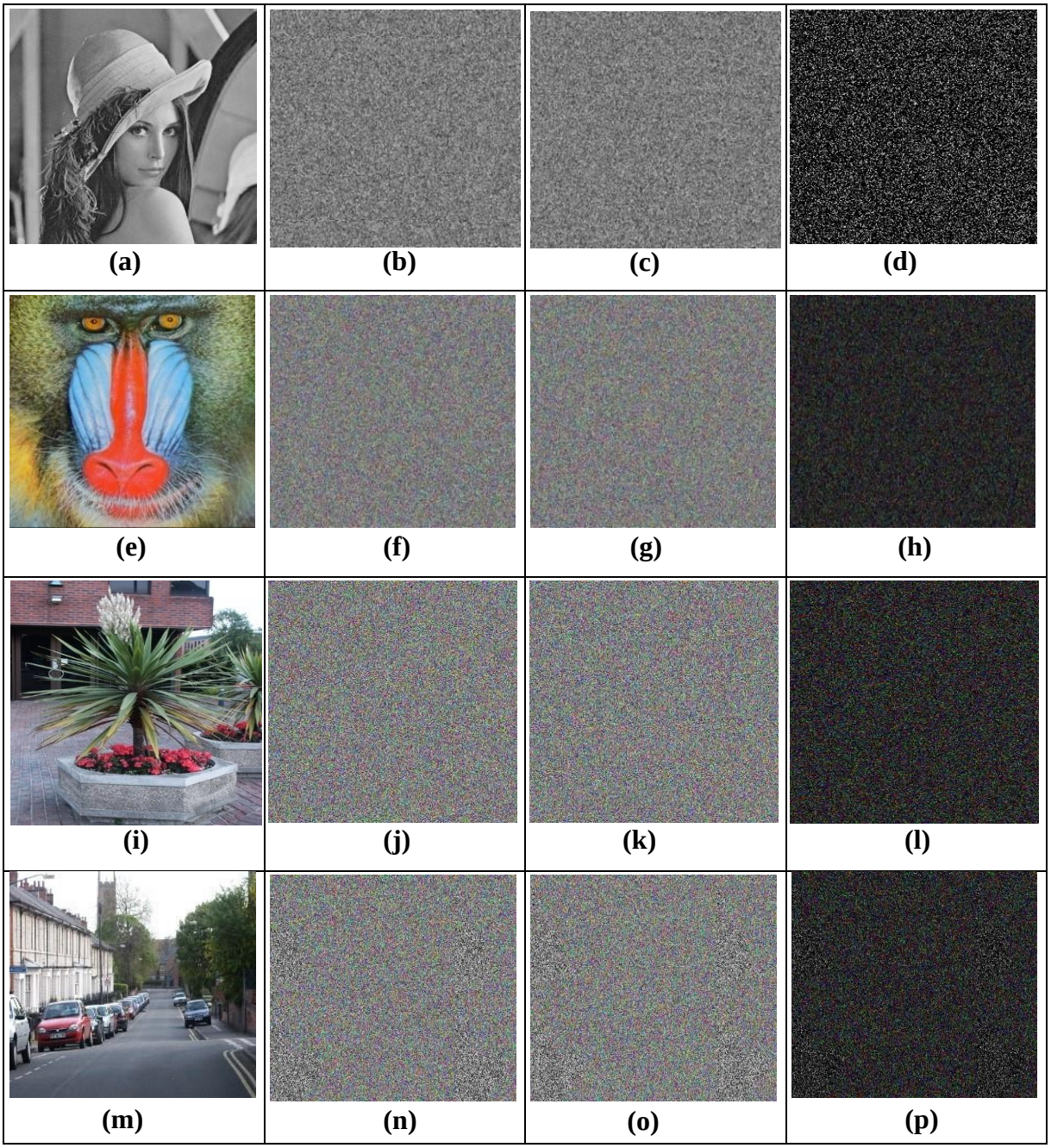

Figure 4.6: Sensibilité à la clé secrète : (a), (e), (i), (m) images originales; (b), (f), (j), (n) Images chiffrées par x_0 ; (c), (g), (k), (o) Images chiffrées par la clé secrète $x_0 + 10^{-15}$; (d), (h), (l), (p) Différence entre les images chiffrées (b) et (c), (f) et (g), (j) et (k), (n) et (o), respectivement.

4.3.2 Analyse Statistique

Dans cette analyse, trois testes sont effectués, notamment l'histogramme, le coefficient de corrélation, la distribution des pixels adjacents dans les trois directions horizontale, verticale et diagonale, et finalement une analyse par entropie.

4.3.2.1 Analyse par histogramme

Quatre images de tests ont été choisies dans cette analyse : Lena 512×512, Baboon 512×512 et Cameramen 256×256 de la base de données [84]. Les tracés des histogrammes sont montrés dans la figure 4.7 ci-dessous :

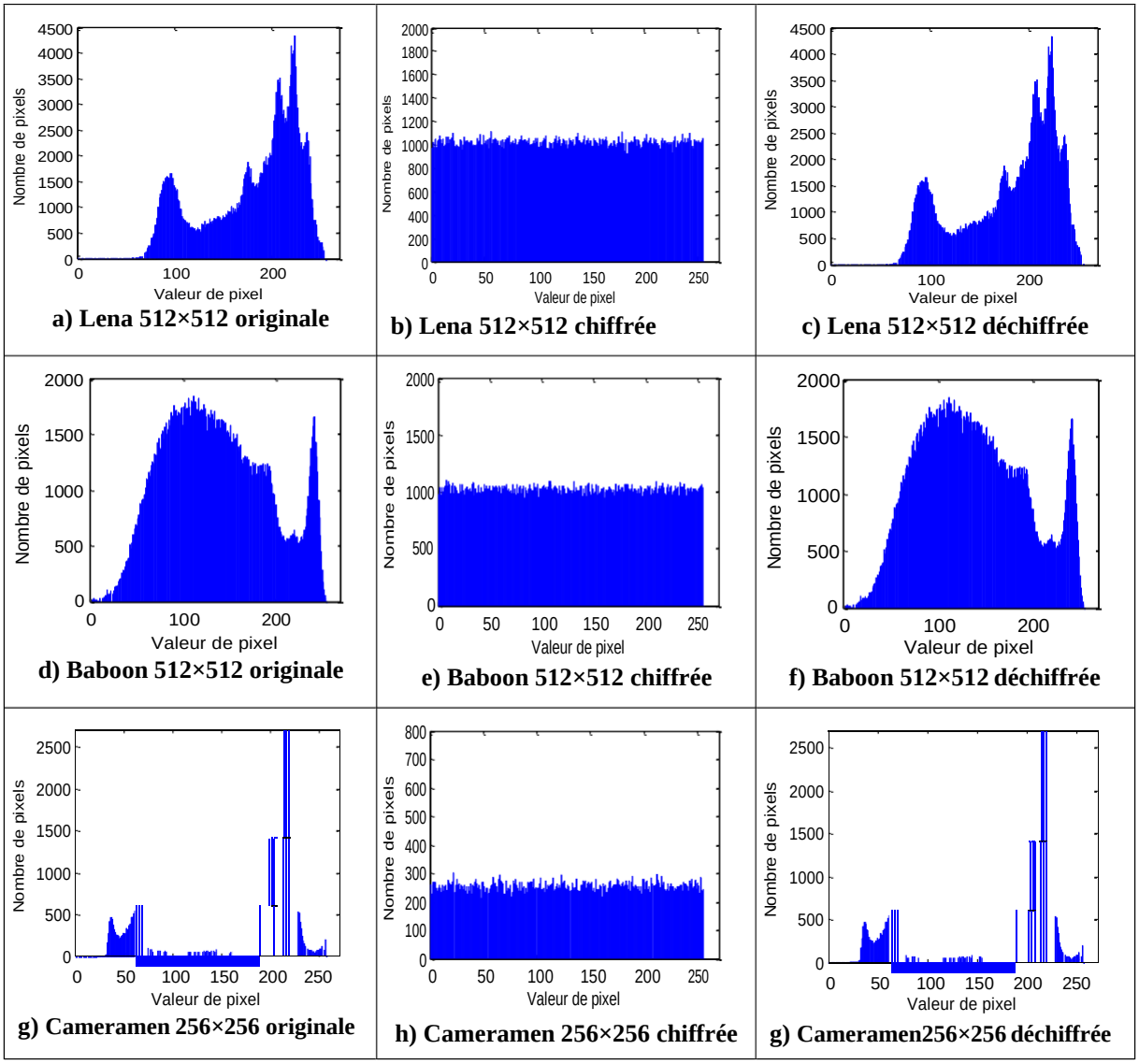

Figure 4.7: Analyse par histogramme.

Il ressort de la figure 4.7 ci-dessus, que les histogrammes des images chiffrées sont plats et uniformément distribués après le cryptage. Subséquemment, il empêche le cryptanalyste

d'extraire des informations sur l'image originale en utilisant les histogrammes des images chiffrées.

4.3.2.2 Analyse par corrélation

En plus de l'analyse par histogramme comme étant un test visuel, nous avons aussi calculé et analysé la corrélation entre les paires de pixels adjacents dans les trois directions horizontale, verticale et diagonale pour l'image originale et chiffrées. Les coefficients de corrélation sont calculés par les formules mathématiques indiquées dans le chapitre II section IV.4.b. La liste des coefficients de corrélation des images claires et leurs chiffrées en utilisant le schéma proposé sont montrés dans le tableau 4.2.

Image	**Image originale**			**Image chiffrée**		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Lena (512×512)	0.9616	0.9761	0.9417	-0.0005	0.0006	-0.0029
Baboon (512×512)	0.8397	0.7195	0.6985	0.0015	0.0061	-0.0028
Peppers (512×512)	0.9653	0.9759	0.9461	-0.0033	0.0003	-0.0009
Airplane (512×512)	0.9692	0.9648	0.9453	-0.0033	0.0013	0.0060
Boat (512×512)	0.8241	0.9434	0.8212	0.0002	-0.0037	0.0042
House (256×256)	0.9782	0.9529	0.9362	0.0020	-0.0057	-0.0081
Tree (256×256)	0.9682	0.9451	0.9225	0.0002	-0.0007	-0.0031
Couple (256×256)	0.9395	0.9567	0.9089	-0.0028	0.0009	0.0014
Girl (256×256)	0.9740	0.9657	0.9516	0.0067	-0.0018	0.0014
Sailboat (512×512)	0.9745	0.9694	0.9540	-0.0011	-0.0014	0.0037
Splash (512×512)	0.9432	0.9867	0.9369	0.0045	-0.0027	-0.0104
Ucid (512×384)	0.8937	0.9381	0.8589	0.0035	-0.0008	0.0050
Ucid (384×512)	0.9164	0.9164	0.8563	0.0027	0.0004	0.0028

Tableau 4.2 : Coefficients de corrélation pour l'image originale et chiffrée.

Le tableau 4.2 liste les coefficients de corrélation des images originales et leurs cryptées en utilisant la technique proposée. Les coefficients de corrélations mesurées des images claires sont près de 1 tandis que ceux des images chiffrées sont proches de 0. En se basant sur les résultats obtenus, nous pouvons affirmer que le schéma proposé a supprimé avec succès la corrélation des pixels adjacents dans les trois directions.

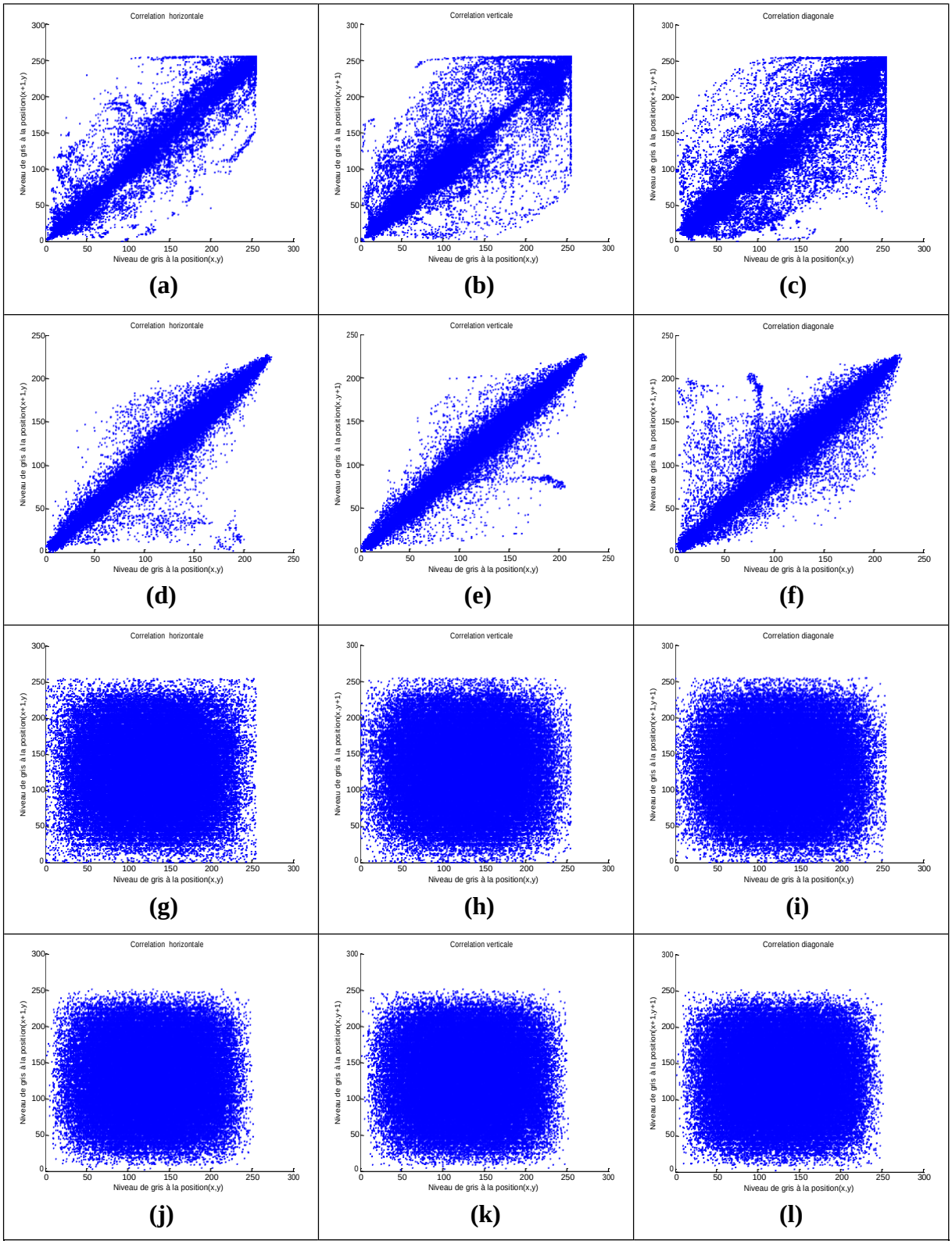

Figure 4.8: Analyse par corrélation : (a, b et c) Corrélation de deux pixels adjacents de l'image ucid00418 512×384 ; (d, e et f) corrélation de deux pixels adjacents de l'image Pepper 512×512 ; (g, h et i) Corrélation de deux pixels adjacents de l'image ucid00418 512×384 chiffrée ; (j, k et l) corrélation de deux pixels adjacents de l'image Pepper 512×512 chiffrée.

4.3.2.3 Analyse par entropie

Un autre paramètre qui mesure la robustesse d'un schéma de chiffrement vis-à-vis des attaques statistiques est l'entropie définie par Shannon [28]. La formule mathématique qui permet de calculer l'entropie est indiquée dans le chapitre II section IV.4.c. Le tableau 4.3 montre les résultats des simulations obtenues pour des images claires et chiffrées de différentes tailles.

Image	**Entropie de l'image originale**	**Entropie de l'image cryptée**
Lena (512×512)	7.7502	7.9998
Baboon (512×512)	7.7624	7.9997
Peppers (512×512)	7.6698	7.9998
Couple (256×256)	6.2945	7.9990
Airplane (512×512)	6.6639	7.9998
House (256×256)	7.0686	7.9992
Tree (256×256)	7.5371	7.9993
Jelly beans (256×256)	6.5835	7.9990
Girl (256×256)	6.8981	7.9990
Male (1024×1024)	7.5237	7.9998
Splash (512×512)	7.2428	7.9998
ucid00416 (512×384)	7.4287	7.9996
ucid00622 (384×512)	7.6799	7.9995

Tableau 4.3 : Entropie de l'image originale et celui de l'image chiffrée correspondante.

Il ressort du tableau 4.3 que les valeurs de d'entropie sont proches de la valeur théorique qui vaut 8. Donc on peut confirmer que le schéma proposé dans ce chapitre fournit de meilleures propriétés aléatoires et prouve la distribution uniforme des niveaux de couleur des histogrammes (figure 4.7). Par conséquent, la technique proposée peut surmonter avec succès l'analyse de l'entropie.

4.3.3 Analyse par PSNR (Peak Signal to Noise Ratio)

Outre les trois facteurs testés dans les sections précédentes, le calcul du PSNR est aussi un paramètre important du fait qu'il mesure la qualité des schémas de chiffrement. Ce facteur est donné par la formule indiquée dans le chapitre II section IV.7. Ce paramètre reflète la difficulté de restaurer l'image originale à partir de l'image chiffrée « détruite » sans avoir utilisé la clé de chiffrement. Le tableau 4.4 résume les résultats des différentes mesures obtenues après les tests qui ont été effectués sur l'images originale issues des deux bases de données [84] et [85].

Image originale	PSNR	MSE
Lena (512×512)	8.6173	8940
Baboon (512×512)	11.8866	4244
Peppers (512×512)	10.8373	5404
Cameraman (256×256)	7.4564	11772
Airplane (512×512)	9.5339	7296
House (256×256)	11.4487	4694
Tree (256×256)	9.7417	6955
Jelly beans (256×256)	10.2108	6243
Girl (256×256)	8.7561	8727
Couple (256×256)	6.2945	15383
ucid00416 (512×384)	9.1252	8016
ucid00622 (384×512)	10.5276	5803

Tableau 4.4 : Valeurs de PSNR et MSE.

Le tableau 4.4 montre que les valeurs du PSNR sont strictement inférieures à 13 dB [101], ce qui signifie que l'image a été complètement randomisée. On sait que plus le PSNR est faible, plus l'algorithme de chiffrement est meilleur.

4.3.4 Analyse différentielle

Afin d'évaluer le changement d'un bit dans la clé secrète ou dans un pixel de l'image originale sur l'image chiffrée. Deux paramètres quantitatifs ont été mesurés, à savoir, le taux de changement de nombre de pixels (NPCR) et le changement moyen de l'intensité unifiée (UACI). En général, une attaque différentielle est une procédure où l'intrus apporte une légère modification telle que la modification d'un seul pixel de l'image cryptée, puis observe son effet sur le résultat obtenu. Après ce changement, si le cryptanalyste est en mesure d'obtenir des informations pertinentes à partir de l'image cryptée sur l'image originale alors le schéma utilisé est pratiquement inefficace et vulnérable à une analyse différentielle. NPCR et UACI sont calculés par les formules mathématiques définies dans le chapitre II section IV.6. Les mesures de NPCR et UACI en utilisant les images tests issues de la base de données USC-SIPI [84] et UCID [85] sont illustrées dans le tableau 4.5, où il apparaît clairement que la valeur de NPCR et UACI obtenue par le schéma proposé sont extrêmement proches des valeurs espérées (les valeurs espérées de NPCR de UACI sont respectivement de 99.6 et 33.4). C'est à dire, une petite modification d'un seul pixel de l'image originale provoque un changement radical de tous les pixels de l'image cryptée. Nous pouvons donc dire que notre algorithme a une résistance contre une attaque différentielle.

Image originale	Image chiffrée	
	NPCR	UACI
Cameramen (256×256)	99.6205	33.5123
House (256×256)	99.6196	33.5703
Lena (512×512)	99.6453	33.4733
Peppers (512×512)	99.6316	33.4214
Baboon (512×512)	99.6372	33.4542
Airplane (512×512)	99.6290	33.5402
Tree (256×256)	99.6125	33.5307
Jelly beans (256×256)	99.6138	33.5205
Girl (256×256)	99.6156	33.5172
ucid00416 (512×384)	99.6201	33.5102
ucid00622 (384×512)	99.6210	33.5092

Tableau 4.5 : Valeurs NPCR et UACI après la modification de la valeur d'un pixel.

4.3.5 Temps d'exécution

Indépendamment des considérations de sécurité, le temps d'exécution est aussi un facteur important pour tester les performances d'un système de cryptage d'image. Afin de valider et de montrer l'efficacité du schéma proposé en termes de temps d'exécution, et grâce à ses propriétés intrinsèques [102], nous avons choisi l'image « Lena 256×256 ». Les résultats obtenus sont illustrés dans le tableau 4.6. Nous avons également analysé la rapidité du schéma proposé sur les images issues de la base de données UCID [85] (en moyenne, le schéma proposé prend environ 0.125 seconde pour chiffrer une image couleur de dimensions 384 × 512 et 512 × 384). Comme on peut voir dans le Tableau 4.6, le schéma proposé a un temps d'exécution acceptable.

Image	**Méthode proposée**	**Réf.** [103] **(Temps de chiffrement/Déchiffrement)**	**Réf.** [104]	**Réf.** [105]	**Réf.** [12]
Lena (256×256)	0.0754	1.2615	0.208	0.000006	0.2973298

Tableau 4.6 : Temps d'exécution.

Le tableau 4.6 montre la comparaison des résultats obtenus par le schéma proposé avec d'autres méthode en termes de temps d'exécution. On constate que le schéma proposé est plus rapide en temps d'exécution que la plupart des schémas disponibles dans la littérature. Le travail

indiqué dans [103] présente un temps d'exécution meilleur, et le schéma proposé vient en deuxième position.

4.4 Comparaison et discussion

Dans ce travail, les performances du schéma proposé sont comparées à celles d'autre techniques de chiffrement mentionnées dans les articles [12] [102] [104] [103] [105]. La comparaison est effectuée en utilisant l'image "Lena 512×512". Le tableau 4.7 montre la comparaison de la méthode proposée avec d'autres mentionnées dans la littérature, en utilisant différents critères de mesure tels que l'entropie, le coefficient de corrélation, le NPCR et l'UACI.

Méthode	**Correlation coefficient**			**NPCR**	**UACI**	**Entropie**
	Horizontal	**Vertical**	**Diagonal**			
Méthode proposée	-0.0004541	0.0005994	-0.0029000	99.645271	33.473291	7.9998
Réf. [11**]**	0.0148000	0.0092000	-0.012400	99.625900	31.974600	7.9968
Réf. [104]	0.0024000	0.0029000	-0.0039000	99.612100	33.471100	7.9993
Réf. [106]	-0.0030859	0.0025108	-0.0000938	99.683600	33.530300	7.9973
Réf. [103]	-0.000319	0.0012010	0.0052710	99.614715	33.5788652	7.9994
Réf. [12]	0.00002793	−0.0017885	−0.0038550	99.604797	33.4761272	7.9997

Tableau 4.7 : comparaison des résultats obtenus avec d'autres schémas existants.

Le tableau 4.7 montre que l'entropie de l'algorithme de cryptage d'image proposé est extrêmement proche de la valeur idéale 8. Par conséquent, le schéma proposé fournit les meilleures propriétés d'aléatoire et résiste aux attaques basées sur l'entropie. En observant les valeurs NPCR et UACI du tableau 4.5, nous pouvons voir que les valeurs de NPCR et UACI du schéma de chiffrement d'image proposé sont très proches des valeurs espérées (NPCR (99.6) et UACI (33.4)) par rapport aux autres valeurs présentées dans les autres algorithmes [103] [102] [105]. Ainsi, le schéma proposé résiste bien aux attaques différentielles. Enfin, en observant les valeurs de coefficient de corrélation dans les trois directions, nous remarquons que les résultats obtenus du coefficient de corrélation sont très proches de zéro. En fin, nous pouvons conclure que le schéma proposé est acceptable et peut être utilisé pour des applications de cryptage d'image.

4.5 Conclusion

Dans ce chapitre, un nouveau schéma de chiffrement d'image basé sur une variante sécurisée de CH et trois cartes chaotiques 1D améliorées a été proposé. Premièrement, nous avons amélioré la carte logistique, la carte de Tchebychev et la carte sinus, pour produire trois générateurs pseudo-aléatoires puissants offrant des meilleures propriétés pseudo-aléatoires par rapport aux cartes chaotiques initiales. En effet, l’exposant de Lyapunov, le diagramme de bifurcation et la densité de distribution le prouvent. Ensuite, nous avons suggéré une version améliorée de CH, basée sur une matrice clé de taille 2×2, capable de chiffrer les pixels un par un au lieu du bloc de pixels. Afin de chiffrer chaque pixel, nous avons utilisé un bruit généré par une randomisation des pixels précédents. En conséquence, une légère modification de l'image originale ou de la clé produit une image cryptée complètement différente. Donc, la méthode proposée est sécurisée aux attaques différentielles. L'espace clé de taille 384 est suffisamment grand pour rendre les attaques par force brute irréalisables dans un délai raisonnable. De plus, les résultats des simulations présentés par un histogramme plat de l'image cryptée assurent une valeur d'entropie très proche de la valeur théorique 8. De plus, un coefficient de corrélation proche de zéro, un temps de cryptage court, une distribution aléatoire des pixels adjacents de l'image cryptée montrent l'efficacité et l'efficience du schéma proposé.

Conclusion générale et perspectives

Actuellement, la transmission des images numériques sur divers supports de communication constitue un défi pour la mise au point des méthodes de sécurité crédibles pour une protection efficace des informations confidentielles et sensibles. Par conséquent, la sécurité des images numériques est devenue un sujet de recherche très sollicité. La confidentialité peut être réalisée grâce à des algorithmes de chiffrement qui permettent de transformer les informations compréhensibles à un format inintelligible. Récemment, ce champ attire l'attention de plus en plus de spécialistes, et nombreuses méthodes ont été développées.

Subséquemment, le travail de cette thèse consiste dans un premier temps à comprendre certaines propriétés cryptographiques, accompagné par une description de quelques méthodes classiques de chiffrement, telles que DES, AES, RSA, César, Vigenère…etc. La théorie du chao a été introduite comme une nouvelle tendance moderne de chiffrement. Cela grâce à sa nature déterministe, son imprévisibilité, son aspect aléatoire et surtout sa sensibilité aux conditions initiales. Une étude de quelques cartes chaotiques célèbres telles que la carte logistique, carte Sine et carte Tchebychev a été faite dans le premier chapitre.

Nous avons proposé dans le 2ème chapitre un schéma de chiffrement d'image basé sur une amélioration des propriétés pseudo-aléatoires de la carte Skew tente par une fonction modulaire, qui sera utilisée comme générateur des séquences chaotiques qui constituent la clé de chiffrement. La technique utilisait les deux processus fondamentaux de chiffrement à savoir la permutation et la diffusion. Dans le 3ème chapitre, une autre technique de chiffrement d'images basée sur l'amélioration des caractéristiques chaotiques 3D, d'une nouvelle table de Vigenère dynamique et d'un meilleur mécanisme de diffusion. Dans le dernier chapitre, un autre schéma de chiffrement basé sur une variante sécurisée de CH et trois cartes chaotiques 1D améliorées a été proposé. Premièrement, une amélioration des propriétés pseudo-aléatoires de la carte logistique, la carte de Tchebychev et la carte sinus a été effectuée. Ensuite, nous avons suggéré une version améliorée de CH, basée sur une matrice de clé de taille 2×2, capable de chiffrer les pixels un par un au lieu du bloc de pixels.

Ces trois techniques de chiffrement offrent un excellent processus de confusion et de diffusion ce qui assure une sécurité élevée. La confusion et la diffusion ont été obtenues en

utilisant la permutation, la substitution et l'effet d'avalanche inséré par le mécanisme de diffusion, par conséquent toute modification apportée à un bit d'un seul pixel aléatoire sera répercutée sur l'image entière. Ceci se justifie par la valeur des constantes statiques NPCR et UACI. En outre, les valeurs des coefficients de corrélation qui sont proches de zéro, confirment que la dépendance des propriétés statistiques de l'image cryptée et celle originale est presque aléatoire. Les histogrammes plats de l'image cryptée reflètent une valeur d'entropie maximale. Des espace clé largement grands et des fortes sensibilités, mettent à l'abri les approches proposées contre toute attaque brutale. Et finalement, des temps d'exécution acceptables, nous permettent de déduire que les schémas proposés peuvent être utilisés pour la transmission des informations avec une sécurité et un temps d'exécution raisonnable.

En contrepartie, on constate que dans les trois techniques proposées un fort effet d'avalanche a été introduit, de telle sorte qu'une modification même infiniment petite de la clé ou d'un pixel de l'image originale entraîne un changement radical de l'image chiffrée. Ce mécanisme permet de rendre ces techniques plus robustes contre les attaques différentielles. En perspectives de ce travail, nous envisageons d'étudier les contraintes de toute modification accidentelle ou inattendue, induites sur le canal de transmission et son effet parasite sur l'image chiffrée transmise lors de déchiffrement par le récepteur.

Bibliographie

[1] L. O. M. Kobayashi, S. S. Furuie et P. S. L. M. Barreto, « Providing integrity and authenticity in DICOM images: a novel approach,» *IEEE Transactions on Information Technology in Biomedicine,* vol. 13, n14, pp. 582-589, 2009.

[2] R. L. Rivest, «Chaffing and winnowing: Confidentiality without encryption,» *CryptoBytes (RSA laboratories),* vol. 4, n11, pp. 12-17, 1998.

[3] P. Laud, «Symmetric encryption in automatic analyses for confidentiality against active adversaries,» *IEEE Symposium on Security and Privacy. Proceedings IEEE,* pp. 71-85, May 2004.

[4] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino et E. W. Felten, «Let we remember: cold-boot attacks on encryption keys,» *Communications of the ACM,* vol. 52, n15, pp. 91-98, 2009.

[5] D. Coppersmith, «The Data Encryption Standard (DES) and its strength against attacks,» *IBM journal of research and development,* vol. 38, n13, pp. 243-250, 1994.

[6] E. Biham et A. Shamir, «Differential cryptanalysis of DES-like cryptosystems,» *Journal of CRYPTOLOGY,* vol. 4, n11, pp. 3-72, 1991.

[7] J. D. J et V. RIJMEN, «AES, Proposal: The Rijndael Block Cipher. ,,» *Technicalreport.*

[8] R. L. Rivest, A. Shamir et L. Adleman, «A method for obtaining Digital Signature and Public-Key Cryptosystems,» *Communications of the ACM,* vol. 21, n12, pp. 120-126, 1978.

[9] R. Fischlin et C. P. Schnorr, «Journal of Cryptology,» *Stronger security proofs for RSA and Rabin bits,* vol. 13, n12, p. 221–244, 2000.

[10] T. El Gamal, «A public key cryptosystem and a signature scheme based on discrete logarithms,» *IEEE transactions on information theory,* vol. 31, n14, pp. 469-472, 1985.

[11] F. Sun, S. Liu, Z. Li et Z. Lü, « A novel image encryption scheme based on spatial chaos map,» *Chaos, Solitons & Fractals,* vol. 38, n13, pp. 631-640, 2008.

[12] R. Bansal, G. Shailender et S. Gaurav, «An innovative image encryption scheme based on chaotic map and Vigenère scheme,» *Multimedia Tools and Applications* , pp. 1-34, 2016.

[13] M. Farajallah, S. El Assad et O. Deforges, «Fast and secure chaos-based cryptosystem for images,» *International Journal of Bifurcation and Chaos,* vol. 26, n102, p. 1650021, 2016.

[14] C. Pak et L. Huang, «A new color image encryption using combination of the 1D chaotic map,» *Signal Processing,* vol. 138, pp. 129-137, 2017.

[15] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño et R. Méndez-Ramírez, «A novel pseudorandom number generator based on pseudorandomly enhanced logistic map,» *Nonlinear Dynamics,* vol. 87, n11, pp. 407-425, 2017.

[16] H. Wang, B. Song, Q. Liu, J. Pan et Q. Ding, «FPGA design and applicable analysis of discrete chaotic maps,» *International Journal of Bifurcation and Chaos,* vol. 24, n104, pp. 145-154, 2014.

[17] D. Arroyo, G. Alvarez et V. Fernandez, «On the inadequacy of the logistic map for cryptographic applications,» *arXiv preprint arXiv:*, vol. 805, p. 4355, 2008.

[18] I. S. Sam, P. Devaraj et R. S. Bhuvaneswaran, «An intertwining chaotic maps based image encryption scheme,» *Nonlinear Dynamics,* vol. 69, n14, pp. 1995-2007, 2012.

[19] W. Tuchman, «A brief history of the data encryption standar, ACM Press/Addison-Wesley Publishing Co,» *New York, NY, USA,* pp. 275-280, 1997.

[20] J. Katz, A. J. Menezes, P. C. Van Oorschot et S. A. Vanstone, «Handbook of applied cryptography.,» *CRC press,* 1996.

[21] M. Rhee, «Internet Security Cryptographic Principles, Algorithms and Protocols,» *Republic of Korea: Seoul National University: John Wiley & Sons Ltd,* 2003.

[22] J. Daemen et V. Rijmen, «AES proposal: Rijndael,» 1999.

[23] S. Gupta et J. Sharma, « A hybrid encryption algorithm based on RSA and Diffie-Hellman,» *IEEE International Conference on Computational Intelligence and Computing Research. IEEE,* pp. 1-4, 2012 .

[24] J. Overbey, W. Traves et J. Wojdylo, «On the keyspace of the Hill cipher,» *Cryptologia,* vol. 29, n11, pp. 59-72, 2005.

[25] M. Machkour, A. Saaidi et M. L. Benmaati, «A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher,» *3D Research,* vol. 6, n14, p. 36, 2015.

[26] W. Stallings, «Cryptography and network security: principles and practice,» *Upper Saddle River: Pearson,* pp. 92-95, 2017.

[27] A. Kerckhoffs, «La cryptographic militaire,» *Journal des sciences militaires,* pp. 5-38, 1883.

[28] C. E. Shannon, «Communication theory of secrecy systems,» *Bell system technical journal,* vol. 28, n14, pp. 656-715, 1949.

[29] S. Zhu et C. Zhu, « Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system,» *Multimedia Tools and Applications,* vol. 77, n121, pp. 29119-29142, 2018.

[30] U. M. Maurer et S. Wolf, «Diffie-hellman oracles.,» *In Annual International Cryptology Conference (pp.). Springer, Berlin, Heidelberg,* pp. 268-282, 1996, August.

[31] D. Luciano et G. Prichett, « Cryptology: From Caesar ciphers to public-key cryptosystems,» *The College Mathematics Journal,* vol. 18, n11, pp. 2-17, 1987.

[32] A. K. Bhateja, A. Bhateja, S. Chaudhury et P. K. Saxena, «Cryptanalysis of vigenere cipher using cuckoo search. Applied Soft Computing,» vol. 26, pp. 315-324, 2015.

[33] L. S. Hill, «Concerning Certain Linear Transformation Apparatus of Cryptography,» *The American Mathematical Monthly,* vol. 23, pp. 135-154, 1931.

[34] L. S. Hill, «Cryptography in an Algebraic Alphabet,» *The American Mathematical Monthly,* vol. 36, n16, pp. 306-312, 1929.

[35] P. L. M. et C. T. L., «Synchronization in chaotic systems,» *Phys. Rev. Lett.,* vol. 64, n1821 , 1990.

[36] T. Y. Li et J. A. Yorke, «Period three implies chaos,» *The American Mathematical Monthly,* vol. 82, n110, pp. 985-992, 1975.

[37] T. Shinbrot, C. Grebogi, J. A. Yorke et E. Ott, «Using small perturbations to control chaos.,» *Nature,* vol. 363, n16428, p. 411, 1993.

[38] R. Sneyers, « Climate Chaotic Instability: Statistical Determination and Theoretical Background,» *Environmetrics,* vol. 8, n15, pp. 517-532, 1997.

[39] K. Alligood, T. Sauer et J. Yorke, «Chaos an Introduction to Dynamical Systems,» *New York: Springer-Verlag,* 1996.

[40] X. Zeng, R. Pielke et R. Eykholt, «Chaos theory and its application to the Atmosphere,» *Bulletin of the American Meteorological Society,* vol. 74, n14, pp. 631-639, 1993.

[41] C. F. Barenghi, Introduction to chaos: theoretical and numerical methods., 2010.

[42] R. May, «Simple mathematical models with very complicated dynamics,» *Nature,* vol. 261, pp. 459-467, 1976.

[43] O. RÖssler, «An equation for continous chaos,» *Phys. Lett. A,* vol. 57, p. 397, 1976.

[44] S. A. Levin et R. M. May, «A note on difference-delay equations,» *Theoretical Population Biology,* vol. 9, n12, pp. 178-187, 1976.

[45] http://fr.wikipedia.org/wiki/Théorie_du_chaos.

[46] J. Oden, Le chaos dans les systèmes dynamiques, cours, 2007.

[47] H. D. Abarbanel, R. Brown et M. B. Kennel, «Lyapunov exponents in chaotic systems: their importance and their evaluation using observed data,» *International Journal of Modern Physics B,* vol. 5, n109, pp. 1347-1375, 1991.

[48] P. H, «Sur le problème des trois corps et les équations de la dynamique,» *Acta Mathematica,* vol. tome 13, pp. 1-270, 1890.

[49] G. L. Baker, G. L. Baker et J. P. Gollub, «Chaotic dynamics: an introduction,» Cambridge university press, 1996.

[50] E. I. Olivares, R. Vazquez-Medina, M. Cruz-Irisson et J. L. Del-Rio-Correa, «Numerical calculation of the lyapunov exponent for the logistic MAP,» *In 2008 12th International Conference on Mathematical Methods in Electromagnetic Theory IEEE,* pp. 409-411, 2008.

[51] B. Furht, D. Socek et A. M. Eskicioglu, «Fundamentals of multimedia encryption techniques,» *Multimedia Security Handbook. CRC Press,* p. 93–131, December 2004.

[52] C. Li, G. Luo, K. Qin et C. Li, «An image encryption scheme based on chaotic tent map,» *Nonlinear Dynamics,* vol. 81, n11, pp. 127-133, 2017.

[53] J. Ahmad, M. A. Khan, F. Ahmed et J. S. Khan, «A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation,» *Neural Computing and Applications,* vol. 30, n112, pp. 3847-3857, 2018.

[54] F. Ahmed, M. Y. Siyal et V. U. Abbas, «A perceptually scalable and jpeg compression tolerant image encryption scheme,» *Fourth Pacific-Rim Symposium on Image and Video Technology. IEEE,* pp. 232-238, 2010, November.

[55] L. Zhang, X. Liao et X. Wang, «An image encryption approach based on chaotic maps,» *Chaos, Solitons & Fractals,* vol. 24, n13, pp. 759-765, 2005.

[56] J. Fridrich, «Symmetric ciphers based on two-dimensional chaotic maps,» *International Journal of Bifurcation and chaos,* vol. 8, n106, pp. 1259-1284, 1998.

[57] M. Ghebleh et A. Kanso, «A novel efficient image encryption scheme based on chained skew tent maps,» *Neural Computing and Applications,* pp. 1-16, 2017.

[58] A. Kadir, A. Hamdulla et W. Q. Guo, «Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN,» *Optik-International Journal for Light and Electron Optics,* vol. 125, n15, pp. 1671-1675, 2014.

[59] J. Khan, J. Ahmad et S. O. Hwang, «An efficient image encryption scheme based on: Henon map, skew tent map and S-Box.,» *6th International Conference on Modeling, Simulation, and Applied Optimization(ICMSAO). IEEE*, pp. 1-6, 2015, May.

[60] M. Hénon, «A two-dimensional mapping with a strange attractor,» *In the Theory of Chaotic Attractors. Springer, New York, NY*, pp. 94-102, 1976.

[61] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal et U. Y. Bhatti, «Some analysis of S-box based on residue of prime number,» *Proc Pak Acad Sci*, vol. 48, n12, pp. 111-115, 2011.

[62] Y. Tang, Z. Wang et J. A. Fang, «Image encryption using chaotic coupled map lattices with time-varying delays,» *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, n19, pp. 2456-2468, 2010.

[63] T. Sarika et C. Deepak, «Adapted Encryption Algorithm with Multiple Skew Tent Map,» *IJCSM*, vol. 2, n14, pp. 422-428, April 2013.

[64] C. J. Mendelsohn, «Blaise de Vigenère and the" Chiffre Carré",» *Proceedings of the American Philosophical Society*, pp. 103-129, 1940.

[65] S. Li, Y. Zhao, B. et J. Wang, « Image scrambling based on chaotic sequences and Vigenère cipher,» *Multimedia Tools Appl* , vol. 66, n13, p. 573–588, 2013.

[66] Y. Zhang, X. Di, W. Wen et H. Nan, «Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher,» *Nonlinear Dyn*, vol. 78, n11, p. 235–240, 2014.

[67] Z. Amrani, S. Chitroub et A. Boukhari, «Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques,» *4th International conference on computer integrated manufacturing CIP.*, 2007.

[68] P. William, C. Jean-Jacques et D. Michel, «Transfert sécurisé d'images par chiffrement de Vigenère,» *Centre d'électronique et de micro optoélectronique de Montpellier, UMR CNRS 5507, STINIM, université de Montpellier II, France.*

[69] P. William et R. José Marconi, «Sécurisation d'image par crypto-tatouage,» *Laboratoire LIRMM, UMR CNRS 5506, Université Montpellier II, France.*

[70] I. Saputra, N. A. H. Mesran et R. Rahim, «Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File,» *International Journal of Engineering Research & Technology (IJERT)*, vol. 6, n11, pp. 266-269, 2017.

[71] Q. A. Kester, «A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher,» *arXiv preprint arXiv:1307.7786.*, 2013.

[72] Y. Rangel-Romero, R. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes, L. Martínez-Ramos, M. Mecate-Zambrano et F. Rodríguez-Henríquez, «Comments on "How to repair the Hill cipher,» *Journal of Zhejiang University Science A*, vol. 9, n12, pp. 211-214, 2008.

[73] B. Karthikeyan, J. Chakravarthy et V. Vaithiyanathan, «An enhanced Hill cipher approach for image encryption in steganography,» *International Journal of Electronic Security and Digital Forensics*, vol. 5, n13-4, pp. 178-187, 2013.

[74] A. Mahmoud et A. Chefranov, «Hill cipher modification based on pseudo-random eigenvalues,» *Applied Mathematics & Information Sciences*, vol. 8, n12, p. 505, 2014.

[75] A. V. N. Krishna et K. Madhuravani, «A modified Hill cipher using randomized approach,» *International Journal of Computer Network and Information Security*, vol. 4, n15, pp. 56-62, 2012.

[76] I. A. Ismail, M. Amin et H. Diab, « How to repair the Hill cipher,» *Journal of Zhejiang University-Science A*, vol. 7, n112, pp. 2022-2030, 2006.

[77] C. Samson et V. U. K. Sastry, «An RGB image encryption supported by wavelet-based lossless compression,» *IJACSA* , vol. 3, p. 36–41, 2012.

[78] B. Acharya, M. Sharma, S. Tiwari et V. K. Minz, «Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem,» *Procedia Computer Science*, vol. 2, pp. 242-247, 2010.

[79] S. K. Naveenkumar et H. T. Panduranga, «Chaos and Hill Cipher Based Image Encryption for Mammography Images,» *Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE,* pp. 1-5, March 2015.

[80] M. N. A. Rahman, A. F. A. Abidin, M. K. Yusof et N. S. M. Usop, «Cryptography: A New Approach of Classical Hill Cipher,» *International Journal of Security and Its Applications,* vol. 7, n12, pp. 179-190, 2013.

[81] G. Alvarez et S. Li, «Some basic cryptographic requirements for chaos-based cryptosystems,» *International journal of bifurcation and chaos,* vol. 16, n108, pp. 2129-2151, 2006.

[82] L. Keliher et A. Z. Delaney, «Cryptanalysis of the toorani-falahati hill ciphers,» *IEEE Symposium on Computers and Communications (ISCC). IEEE,* pp. 436-440, July 2013.

[83] B. Acharya, S. K. Panigrahy, S. K. Patra et G. Panda, «Image encryption using advanced hill cipher algorithm,» *International Journal of Recent Trends in Engineering,* vol. 1, n11, pp. 663-667, 2009.

[84] http://sipi.usc.edu/database/database.php?volume=misc.

[85] G. Schaefer et M. Stich, «UCID - an uncompressed color image database, in: In storage and Retrieval Methods and Applications for Multimedia,» *Proceedings of SPIE,* p. 472–480, 2004.

[86] M. Joshi et K. Singh, «Color image encryption and decryption for twin images in fractional Fourier domain,» *Optics Communications,* vol. 281, n123, pp. 5713-5720, 2008.

[87] V. Rozouvan, «Modulo image encryption with fractal keys,» *Optics and lasers in engineering,* vol. 47, n11, pp. 1-6, 2009.

[88] Y. N. J. P. &. A. S. Wu, «NPCR and UACI randomness tests for image encryption,» *multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), Cyber journals,* vol. 1, n12, pp. 31-38, 2011.

[89] H. S. Kwok et W. K. Tang, «A fast image encryption system based on chaotic maps with finite precision representation,» *Chaos, solitons & fractals,* vol. 32, n14, pp. 1518-1529, 2007.

[90] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem et M. Lee, « Image encryption using a synchronous permutation-diffusion technique.,» *Optics and Lasers in Engineering,* vol. 90, pp. 146-154, 2017.

[91] L. Xu, Z. Li, J. Li et W. Hua, «A novel bit-level image encryption algorithm based on chaotic maps,» *Optics and Lasers in Engineering,* vol. 78, pp. 17-25, 2016.

[92] Y. Zhang et D. Xiao, «An image encryption scheme based on rotation matrix bit-level permutation and block diffusion,» *Communications in Nonlinear Science and Numerical Simulation,* vol. 19, n11, pp. 74-82, 2014.

[93] L. Q. X. Y. Y. B. Wang, «An image encryption scheme based on cross chaotic map,» *Congress on Image and Signal Processing IEEE,* vol. 3, May 2008.

[94] N. K. Varshney, «RC6 based data security and attack detection,» *In Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems Springer, Cham,* vol. 1, pp. 3-10, 2016.

[95] S. Lian, J. Sun et Z. Wang, «Security analysis of a chaos-based image encryption algorithm,» *Physica A: Statistical Mechanics and its Applications,* vol. 351, n12, pp. 645-661, 2005.

[96] M. Kumar, S. Kumar, R. Budhiraja, M. K. Das et S. Singh, «Intertwining logistic map and Cellular Automata based color image encryption model,» *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) IEEE,* pp. 618-623, March 2016.

[97] P. Singh et K. Singh, « Image encryption and decryption using blowfish algorithm in matlab,» *International Journal of Scientific & Engineering Research,* vol. 4, n17, pp. 150-154, 2013.

[98] H. L, «Concerning certain linear transformation apparatus of cryptography.,» *The American Mathematical Monthly,* vol. 38, n13, pp. 135-154.

[99] X. Chen, K. Makki, K. Yen et N. Pissinou, «Sensor network security: a survey,» *IEEE Communications Surveys & Tutorials,* vol. 11, n12, 2009.

[100] C. H. Lin, C. Y. Lee et C. Y. Lee, «Comments on Saeednia's improved scheme for the Hill cipher,» *Journal of the Chinese institute of engineers,* vol. 25, n17, pp. 743-746, 2004.

[101] Mairal, J; Elad, M; Sapiro, G, «Sparse representation for color image restoration,» *IEEE Transactions on image processing,* vol. 17, n11, pp. 53-69, 2008.

[102] D. Munson, «A note on Lena,» *IEEE Transactions on Image Processing,* vol. 5, n11, pp. 3-3, 1996.

[103] G. Hanchinamani et L. Kulkarni, «An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher,» *3D Research,* vol. 6, n13, 2015.

[104] K. A. K. Patro, A. Banerjee et B. Acharya, «A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1-D chaotic maps,» *In International Conference on Next Generation Computing Technologies. Springer, Singapore,* pp. 396-418, October 2017.

[105] Z. E. Dawahdeh, S. N. Yaakob et R. R. bin Othman, « A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher,» *Journal of King Saud University-Computer and Information Sciences,* vol. 30, n13, pp. 349-355, 2018.

[106] M. Mollaeefar, A. Sharif et M. Nazari, «A novel encryption scheme for colored image based on high level chaotic maps,» *Multimedia Tools and Applications,* vol. 76, n11, pp. 607-629, 2017.

[107] M. Toorani et A. Falahati, «A secure cryptosystem based on affine transformation.,» *Security and Communication Networks,* vol. 4, n12, pp. 207-215, 2011.

[108] S. Suri et R. Vijay, «A synchronous intertwining logistic map-DNA approach for color image encryption,» *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-14, 2018.

[109] P. Stavroulakis et M. Stamp, Handbook of information and communication security, Springer Science & Business Media, 2010.

[110] S. P. Singh et R. Maini, «Comparison of data encryption algorithms,» *International Journal of Computer Science and Communication,* vol. 2, n11, pp. 125-127, 2011.

[111] V. U. K. Sastry et N. R. Shankar, «Modified Hill Cipher for a large block of plaintext with Interlacing and Iteration,» *Journal of Computer Science,* vol. 4, n11, pp. 15-20, 2008.

[112] E. Ott, C. Grebogi et J. A. Yorke, «Controlling chaos,» *Physical Review Letters,* vol. 64, p. 1196–1199, 1990.

[113] Q. A. Memon, «Synchronized choas for network security,» *Computer Communications,* vol. 26, n16, pp. 498-505, 2003.

[114] S. Lian, J. Sun et Z. Wang, «A block cipher based on a suitable use of chaotic standard map,» *Chaos, Solitons and Fractals,* vol. 26, n11, pp. 117-129, 2005.

[115] H. L, «Cryptography in an algebraic alphabet,» *The American Mathematical Monthly,* vol. 36, n16, pp. 306-312, 1929.

[116] A. Kumar, D. S. Jakhar et S. Makkar, «Comparative Analysis between DES and RSA Algorithm's,» *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 2, n17, pp. 386-391, 2012.

[117] Z. Kotulski et J. Szczepanski, «Discrete chaotic cryptography (DCC),» *Annalen der Physik,* vol. 6, n15, pp. 381-394, 1997.

[118] P. N. Khade et M. Narnaware, «3D chaotic functions for image encryption,» *IJCSI International Journal of Computer Science Issues,* vol. 9, n13, pp. 323-328, 2012.

[119] E. Cherrier, M. Boutayeb et J. Ragot, «Observers-based synchronization and input recovery for a class of nonlinear chaotic models,» *IEEE Transactions on Circuits and Systems,* vol. 53, n19, pp. 1977-1988, 2006.

Liste des publications

➢ Articles

[1] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « A new image encryption combining 3D chaotic system and a dynamic Vigenère cipher,» *International Journal of Tomography & Simulation™,* vol. 31, n11, pp. 90-114, 2018.

[2] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps,». *Journal of Information Security and Applications*, vol 47, pp. 173-187, 2019.

[3] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Image encryption based on Arnold transformation,» *Gulf J. Math*, vol. 4, n4, pp. 103-107, 2016.

[4] M. Essaid, I. Akharraz, A.Saaidi et A. Mouhib, « A new color image encryption algorithm based on iterative mixing of color channels and chaos,» In Proceedings of International Conference on Applied Mathematics, *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, n5, pp. 94-99, 2017.

[5] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map,» *Procedia Computer Science*, vol. 127, pp. 539-548, 2018.

[6] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system,» *In Proceedings of The 5th IEEE international conference on Wireless Technologies, embedded and intelligent Systems-WITS'2019-, 2019.*

[7] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Chaotic image encryption scheme based on dynamic substitution and diffusion operations,» *In Proceedings International Conference on Intelligent Systems and Advanced Computing Sciences (ISACS'19)* (soumission en cours).

➢ Conférences nationales

[1] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Cryptage d'image: Etude comparative,» Journée nationale de la cryptographie (CrypTa'15). 13 Mai 2015, FPT Taza.

[2] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Cryptage d'image: Etude comparative,» 2ème Séminaire en sciences et Techniques de l'Ingénieur (SSTI), 28 Mai 2015, FPT Taza.

[3] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Cryptage d'image : Cryptage sélectif des visages,» 2ème Workshop en Imagerie, Systèmes et Applications (WISA). 30-31 octobre 2015, FPT Taza.

[4] M. Essaid, I. Akharraz, A. Saaidi et A. Mouhib, « Cryptage d'image basé sur permutation, substitution et confusion par générateur à congruence linéaire,» 3ème Colloque International sur la Modélisation et Analyse en Mécanique Energétique (CIMAME'2016). 28-29 avril 2016, FPT Taza.