الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة د. مولاي الطاهر

كلية التكنولوجيا

قسم: الإعلام الآلي

Mémoire de Master

Spécialité : Sécurité Informatique et Cryptographie

Thème

Prédiction d'un Nouveau Crypto-système d'Image à base de Chao-ADN

Présenté par :

Bencherab Amel

Kaddour Brahim Zine Eddine

Dirigé par :

Mr.Benyahia Kadda

Promotion 2021 - 2022

REMERCIEMENTS

Tout d'abord, nous remercions Dieu le Tout-Puissant de nous donner la force, d'éclairer notre chemin et de nous guider vers le chemin de la connaissance. Nous remercions sincèrement notre directeur de recherche, M. Kadda benyahia, pour le suivi, l’encouragement et les précieux conseils, pour sa gentillesse et surtout pour sa confiance en nous. Nous tenons également à remercier les membres du jury qui ont accepté d'évaluer l'article et de nous faire part de leurs critiques constructives, qui contribueront sûrement à améliorer ce travail. Nous ne pouvons manquer d'exprimer nos sincères remerciements à tous les enseignants qui nous ont encouragés tout au long du processus d'apprentissage.

Dédicaces

On dédie se travail à nos familles, nos parents, nos frères et sœurs,
notre encadreur et nos amis et à tous qui nous ont aidés de loin ou de près
tout au long de ce PFE.

Amel & Zine Eddine

RESUME

Nous proposons une technique de cryptage d'image puissante basée sur un modèle hybride de masquage d'acide désoxyribonucléique (ADN), un système de graphes lorentziens chaotiques 3D. Un schéma logique chaotique est utilisé pour sélectionner diverses opérations algébriques à appliquer aux valeurs de pixel. A l'aide d'une analyse d'histogrammes et de coefficients de corrélation, les performances de la technique proposée sont analysées en termes de résistance aux attaques statistiques. De plus, les principales sensibilités ont été analysées. Les mesures d'entropie et diverses attaques sur les images cryptées, telles que la perte de blocs et l'introduction de bruit, sont également utilisées pour vérifier la robustesse aux attaques.

Abstract

We propose a powerful image encryption technique based on a hybrid deoxyribonucleic acid (DNA) masking model, a 3D chaotic Lorentzian graph system. A chaotic logic scheme is used to select various algebraic operations to apply to pixel values. Using an analysis of histograms and correlation coefficients, the performances of the proposed technique are analyzed in terms of resistance to statistical attacks. In addition, the main sensitivities were analyzed. Entropy measurements and various attacks on encrypted images, such as block loss and noise introduction, are also used to verify robustness to attacks.

ملخص

في هذا العمل، نقدم خوارزمية جديدة لتشفير الصور تعتمد على نموذج هجين لإخفاء الحمض النووي لتحسين نظام التشفير، ونظام فوضوي ثلاثي الأبعاد لورنز، يتم استخدام مخطط منطقي الريبي منقوص فوضوي لتحديد عمليات جبرية متنوعة لتطبيقها على قيم البكسل. باستخدام تحليل الرسوم البيانية ومعاملات الارتباط، يتم تحليل أداء التقنية المقترحة من حيث مقاومة الهجمات الإحصائية. بالإضافة إلى ذلك، تم تحليل الحساسيات الرئيسية. تُستخدم أيضًا قياسات الانتروبيا والهجمات المختلفة على الصور المشفرة، مثل فقدان الكتلة وإدخال الضوضاء، للتحقق من قوة الهجمات.

Table des matières

Liste des figures

Liste des tables

Chapitre 1 :

INTRODUCTION ET FONDAMENTAUX DE SÉCURITÉ

1.1 Introduction

Les humains ont toujours été obsédés par l'information et ont adopté une myriade de tactiques de temps en temps pour dissimuler des informations vitales aux regards indiscrets. L'idée maîtresse de l'écriture des codes secrets ont toujours été populaires depuis que l'homme a quitté la grotte pour vivre en plein air et a commencé vivant en troupeaux. La civilisation a façonné les formes initiales de cryptage nécessaires pour passer l'informations aux générations suivantes, faire la guerre entre tribus, et même accéder au pouvoir.

Au début, même écrire l'information était un moyen de sécuriser l'information car la plupart des gens ne savait pas lire. Puis vint l'âge des symboles secrets où les écrits furent convertis en symboles et chiffres secrets pour les rendre illisibles pour les lecteurs non intentionnels. Ces images capturé plusieurs mots ou messages entiers en un seul et est ainsi devenu extrêmement répandu.

Avec la propagation des civilisations à travers tous les continents, cet art et cette science de l'écriture secrète se sont également développés et certains historiens ont lié l'origine de la cryptographie classique dans des pays comme la Grèce, Rome, l'Égypte et Sparte. [1].

L'armée ou les forces de défense, les politiciens, les religieux, les amoureux et même les artistes utilisation intensive de techniques d'écriture secrètes pour envoyer leurs messages secrets à ceux qu'ils envisageaient les bénéficiaires. Un autre chiffrement renommé qui est devenu viral dans l'Empire romain était le chiffrement de César qui a essentiellement fait le changement de lettre (substitution) pour convertir un message lisible en total charabia. Cette évolution des chiffres s'est poursuivie avec le temps et a produit d'autres chiffres célèbres.

Des cryptogrammes comme Vigenère Cipher, Vernam Cipher, Rail-fence Cipher, et bien d'autres. Les guerres mondiales ont énormément contribué au développement de la cryptographie lorsque les Allemands sont arrivés avec la machine à coder incassable- Enigma (une machine mécanique dédiée à cryptologie) et les puissances alliées ont répondu à ce gigantesque défi par BOMBE (un ordinateur électromécanique)

Cette guerre cryptographique entre les puissances alliées et celles de l'Axe a fait prendre conscience au monde du vrai sens d'une information opportune et correcte. On estime que la rupture les codes Enigma ont raccourci la Seconde Guerre mondiale de plus de deux ans et économisé plus de 14 millions de vies [2]. Après l'âge sombre des guerres mondiales, le monde de la cryptographie n'a plus jamais été le même parce que les ordinateurs sont entrés en jeu à la

fois pour la cryptographie et la cryptanalyse. Cet événement a également marqué la fin de l'âge classique de la cryptographie et le début de la cryptographie qui sera abordée dans la suite.

1.2 Le crypto-système :

L'objectif fondamental de la cryptographie est de permettre la transmission de messages de la source à sa destination via un canal de transmission d'une manière afin que le message tout au long de sa transmission ne puisse être intercepté par quelqu'un.

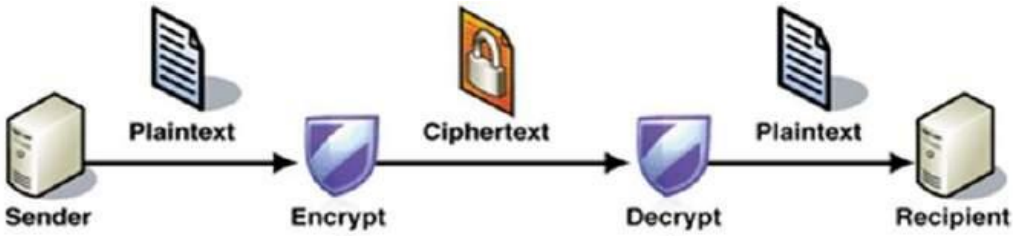


Figure 1.1. Crypto-système

1.2.1 Chiffrement et déchiffrement :

Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement. [**1]**

1.2.2 Les éléments d'un crypto-système :

Un nouveau message d'entrée est nommé texte en clair. Le texte chiffré qui est communiqué est indiqué comme le texte chiffré. La procédure de traduction du texte en clair à son texte chiffré équivalent est reconnue comme chiffrement ou cryptage.

Le rétablissement de l'entrée d'origine à partir d'une entrée cryptée est appelé décryptage ou déchiffrer. L'étude concernant les différents systèmes utilisés pour le cryptage est connue que la cryptanalyse. Les méthodes de décryptage d'un texte en clair dépourvu de toute familiarité de détails de chiffrement établissent le domaine de la cryptanalyse. Ce domaine de la cryptanalyse et la cryptographie sont collectivement appelés cryptologie [2]

Un crypto-système est composé de :

1.Texte en clair :

Texte original intelligible tel qu'il se présentait avant tout chiffrement, révélé après un décodage ou un décryptement réussi.

2.Texte chiffré (cryptogramme) :

C’est le texte obtenu après avoir appliqué l'algorithme de chiffrement sur le texte clair.

3.Clef :

Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message. On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée.

Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser. **[3]**

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs:

- **Les clés symétriques**: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- **Les clés asymétriques**: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

1.3 Cryptographie symétrique :

La cryptographie à clé symétrique utilise la même clé pour le processus d'encodage et de décodage et cette clé est gardée secrète entre les parties communicantes pour assurer confidentialité. Il indique simplement que la clé secrète doit être partagée avant la communication et non par le canal non sécurisé car cela compromettrait l'ensemble du crypto-système.

Néanmoins, les messages peuvent être relayés sur le canal non sécurisé et l’algorithme de chiffrement peut également être rendu public [4]. La figure 1.2 montre une crypto-système symétrique

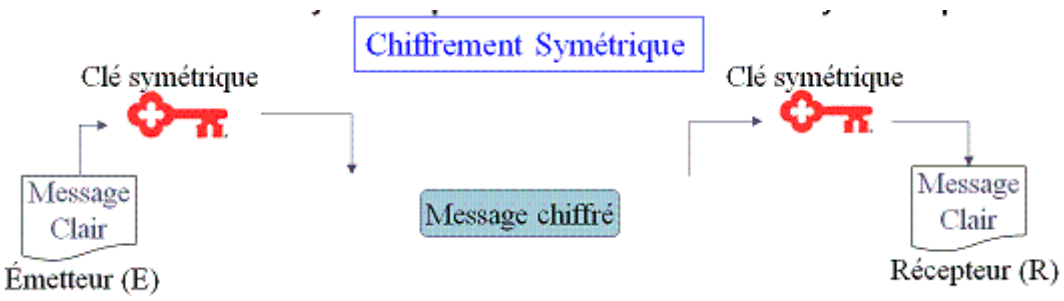


Figure 1.2. Crypto-système à clé symétrique

Une caractéristique cruciale des chiffrements à clé symétrique est qu'ils présentent un effet d'avalanche, ce qui signifie une légère la modification du texte en clair ou de la clé secrète peut entraîner d'immenses changements dans le produit texte chiffré.

Les inconvénients de ce crypto-système sont la distribution et la gestion des clés. Le premier problème fait référence au mode de partage de la clé partagée entre les utilisateurs car dévoiler la clé partagée révélera chaque message envoyé. Par conséquent, la clé doit être partagée avant le communiqué en personne ou par le passage de confiance. Le deuxième problème est également important mais ignoré tout à fait souvent ; il fait référence au problème d'avoir une clé secrète entre une paire d'utilisateurs. Ainsi, si un utilisateur veut converser avec une autre personne, il faut une clé supplémentaire pour cela. Ce problème augmente de façon exponentielle avec le nombre croissant d'utilisateurs et la communication entre eux [5]. Pour gérer tous ces dilemmes, des systèmes de cryptage à clé publique ont été proposés.

1.4 Cryptographie asymétrique :

L'idée centrale de la cryptographie à clé publique est apparue lorsque Whitfield Diffie et son guide Martin Hellman ont publié un article de recherche intitulé New Directions in Cryptography en 1976 pour éliminer le plus gros problème du chiffrement symétrique, c'est-à-dire l'échange de clés entre parties communicantes. Ils ont proposé une nouvelle approche pour échanger la clé secrète à l'aide d'opérations arithmétiques modulaires complexes. Les algorithmes à clé publique utilisent deux clés distinctes pour chiffrer et déchiffrer le texte, d'où le nom de chiffrement asymétrique.

Si une clé est divulguée avec l'algorithme cryptique, même dans ce cas, il est impossible de déduire la seconde clé, et c'est le principe de fonctionnement de la cryptographie asymétrique.[6]

Les deux clés sont mathématiquement corrélées et, à des fins d'identification, elles sont appelées clé publique et clé privée. Comme son nom l'indique, la clé privée est conservée secret et la clé publique est divulguée à tous en la conservant dans un catalogue public ou dans d'autres fichiers accessibles disponibles par voie électronique [6]. Une illustration de Public Key Cryptosystem est montrée dans la figure 1.3 ci-dessous

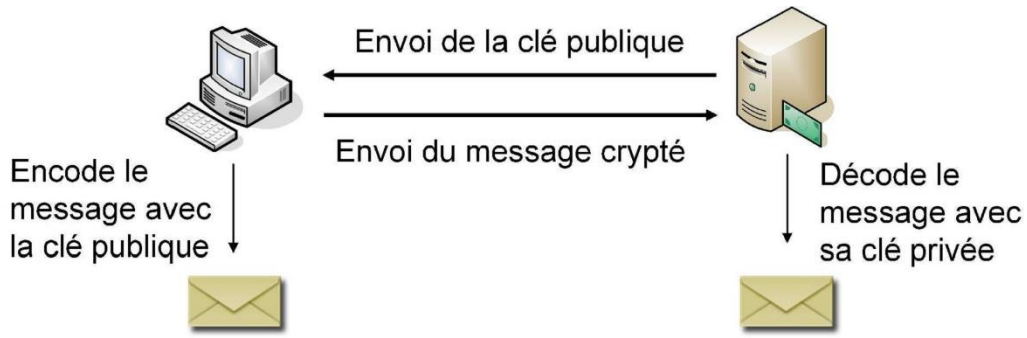


Figure 1.3. Crypto-système à clé symétrique

Certains des algorithmes asymétriques notables sont RSA (du nom de ses inventeurs Ron Rivest, Adi Shamir et Leonard Adleman) et El Gamal Encryption (du nom de son créateur Tahir El Gamal), basés sur la complication informatique de la factorisation des nombres premiers lourds et des logarithmes discrets. [7]. Le seul inconvénient majeur des chiffrements asymétriques est leur vitesse de cryptage et de décryptage plus lente que leurs équivalents symétriques. Les contributions de la cryptographie à clé publique ne se limitent pas à l'échange sécurisé de clés, mais sont étendues à des concepts clés tels que l'authentification à l'aide de fonctions de hachage unidirectionnelles, le tatouage numérique pour protéger les droits de propriété intellectuelle et l'utilisation de la signature numérique pour prouver la validité de la personne associée pour assurer la non-répudiation.[7]

1.5 Cryptanalyse :

La cryptanalyse est le processus de démantèlement des crypto-systèmes en identifiant et en exploitant leur faiblesse. Le cryptage symétrique et asymétrique sont tous deux basés sur le dogme central selon lequel l'algorithme ou le principe de fonctionnement peut être rendu public, mais les clés doivent être gardées secrètes des attaquants pour éviter sa panne. Pour résister aux attaques possibles sur un cryptogramme, le cryptographe doit concevoir le chiffrement en utilisant les objectifs suivants ;

1. Confidentialité : il s'agit de la principale exigence de tout algorithme cryptographique car cela garantit que le contenu du message reste privé ou confidentiel et n'a pas été divulgué intentionnellement ou non à un utilisateur non autorisé.

2. Intégrité : Cela signifie simplement que le contenu du message n'a pas été altéré lors de sa transmission de l'expéditeur au destinataire. Il assure également que le message est protégé de tout accès non autorisé. Habituellement, les fonctions de hachage unidirectionnelles sont utilisées pour parvenir à l'intégrité.

3. Disponibilité : Il promet que les informations sont disponibles pour les utilisateurs authentifiés et autorisés 24 heures sur 24, 7 jours sur 7, 365 jours par an et qu'ils peuvent y accéder où et quand ils en ont besoin. L'accès rapide et fiable à l'information est également l'objectif principal d'un système d'information.

4. Authentification : C'est le processus de validation des personnes impliquées dans la communication. Il peut y avoir plusieurs façons d'authentifier les utilisateurs, comme le nom d'utilisateur et le mot de passe correspondant qui leur sont attribués.

5. Non-répudiation : C'est le concept qui garantit que les parties communicantes ne peuvent pas nier que le communiqué à jamais eu lieu. Par ce biais, l'expéditeur ne peut nier l'envoi d'un message et le destinataire ne peut pas nier avoir reçu le message sur le réseau.

1.6 Cryptographie à base ADN :

La cryptographie à base ADN est utilisée pour une communication sécurisée en raison du vaste parallélisme et de la densité de stockage d'informations extraordinaire qui sont inhérentes à toute molécule d'ADN. Adleman est souvent appelé l'inventeur des ordinateurs à ADN. Son article paru dans un numéro de 1994 de la journal Science décrivait comment utiliser l'ADN pour résoudre un problème mathématique bien connu, appelé le problème du chemin dirigé de Hamilton, également connu sous le nom de problème du "vendeur itinérant". Adleman a choisi de trouver le chemin le plus court entre sept villes. Le succès de l'ordinateur ADN d'Adleman prouve que l'ADN peut être utilisé pour calculer des problèmes mathématiques complexes. L'ADN est utilisé comme support d'information et des opérations basées sur l'ADN sont également simulées sur des ordinateurs à des fins cryptographiques. Les ordinateurs conventionnels peuvent exécuter 100 millions d'instructions par seconde, mais les ordinateurs à ADN peuvent résoudre les opérations à une vitesse 100 fois supérieure à celle des machines conventionnelles. L'ADN possède une haute densité de stockage : 1 gramme d'ADN peut contenir 700 téraoctets de données. De plus, les ordinateurs à ADN peuvent avoir des capacités de traitement parallèle massives.

1.7 Cryptographie à base Chao :

Le chaos est une des dimensions largement utilisée dans les algorithmes de cryptographie. Le phénomène de la théorie du chaos a été introduit pour la première fois par Edward Lorenz en 1972 avec la conceptualisation de "l'effet papillon". De nombreux chercheurs ont observé qu'il existe une relation entre les propriétés du chaos et la cryptographie traditionnelle. G. Alvarez et al. (2006) ont mis en évidence ces relations en termes de certaines propriétés. Q.V. Lawande (2005) a suggéré que la force de la cryptographie réside dans le choix de clés fortes, qui sont des paramètres secrets, utilisés dans le cryptage. La sélection de clés fortes rend difficile pour le cryptanalyste de deviner la clé. Les systèmes chaotiques sont très sensibles aux conditions initiales et aux paramètres du système. Pour un ensemble donné de paramètres en régime chaotique, deux conditions initiales proches conduisent le système vers des trajectoires divergentes. Par conséquent, les cartes chaotiques peuvent être utiles dans le schéma de cryptage/décryptage si les conditions initiales ou les paramètres de contrôle sont choisis comme "clés" et que les "trajectoires" sont utilisées pour le cryptage/décryptage. Puisque les mêmes paramètres sont utilisés pour le cryptage et le décryptage, les schémas de cryptage basés sur le chaos sont des schémas symétriques. L'ergodicité et la sensibilité aux conditions initiales des cartes chaotiques démontrent de très bonnes propriétés de confusion et de diffusion qui sont essentielles pour une approche de cryptage efficace. En outre, les paramètres de contrôle et les conditions initiales des cartes chaotiques forment un très grand espace de clé améliorant la sécurité contre les attaques par force brute.

1.8 contribution :

De nos jours, toutes les données telles que les photos, les dessins, les images médicales et autres contenus multimédias sont stockées sur des ordinateurs numériques et sont également partagées sur les réseaux. Il est très facile de copier, d'accéder et de redistribuer ces informations si un utilisateur malveillant pénètre dans le système. Par conséquent, la cryptographie est devenue une nécessité pour protéger le contenu contre les accès non autorisés. Les exigences des techniques de cryptage d'images sont différentes de celles du cryptage de texte en raison des caractéristiques inhérentes aux données en masse et à la redondance élevée. Les techniques de cryptage doivent être sûres, rapides et permettre la transmission du code avec un stockage efficace. En général, dans les algorithmes de cryptage d'images, les valeurs des pixels sont substituées ou brouillées pour réduire la corrélation entre les valeurs des pixels à l'aide d'une clé externe. L'algorithme de cryptage doit être sensible à la moindre modification de la clé ou

de l'image d'entrée. Un bon algorithme de cryptage doit avoir à la fois les propriétés de confusion et de diffusion pour améliorer la sécurité. Le chaos est largement utilisé dans les techniques de cryptage d'images par les chercheurs pour suggérer des techniques de cryptage d'images sécurisées. Le chaos a la propriété d'être extrêmement sensible au changement des conditions initiales, et d'avoir des propriétés de mélange adaptées à la cryptographie. La cryptographie de l'ADN est également un autre domaine émergeant rapidement comme alternative potentielle pour un cryptage d'image efficace.

Dans ce mémoire, une technique de cryptage d'image robuste basée sur un modèle hybride de masquage de l'acide désoxyribonucléique (ADN), un système de cartes chaotique de Lorenz en 3D. Les cartes logistiques chaotiques sont utilisées pour la sélection de diverses opérations algébriques à appliquer sur les valeurs des pixels. La performance de la technique proposée a été analysée en termes de résistance aux attaques statistiques en utilisant l'analyse des histogrammes et les coefficients de corrélation. En outre, il a également été analysé pour la sensibilité de la clé. La mesure de l'entropie et diverses attaques sur l'image chiffrée comme la perte de blocs et l'introduction de bruit sont également appliquées pour vérifier la robustesse contre les attaques.

La cryptographie de l'ADN est le nouveau domaine émergent. Les chercheurs explorent les opérations de l'ADN et leur utilisation en cryptographie pour un stockage efficace et une meilleure sécurité. Les ordinateurs à ADN pourraient être l'avenir du calcul rapide, sûr et parallèle. Pour explorer l'utilisation de l'ADN dans un large éventail d'applications, les chercheurs simulent les opérations de l'ADN sur des ordinateurs conventionnels afin d'améliorer la sécurité des algorithmes de cryptage. Dans ce mémoire, un algorithme de cryptage à clé symétrique basé sur l'approche ADN est proposé. La séquence de clés originale est petite mais elle peut être étendue à la longueur désirée en utilisant la réplication de l'ADN et la règle du complément de l'ADN guidée sous une séquence chaotique ayant un espace de clés suffisamment grand. La clé étendue avec la règle d'addition et de soustraction de l'ADN est utilisée pour crypter les pixels de l'image. Le processus de cryptage chaotique combiné à l'addition et au complément d'ADN rend la technique suffisamment sûre.

La technique de cryptage d'image basée sur l'ADN proposée par Q. Zhang et al. (2010) a été cryptographiée par H. Hermassiet al. (2013). Il a été constaté que le chiffrement généré ne pouvait pas être décrypté pour retrouver l'image en clair et que l'algorithme pouvait être cassé par une attaque en texte clair. Dans ce mémoire, une nouvelle technique de cryptage d'image

utilisant des opérations ADN et des cartes chaotiques. Le code ADN est décodé par l'ADN pour obtenir l'image finale du code décimal.

1.9 Organisation du mémoire :

Dans ce mémoire, nous avons étudié et proposé un crypto-système pour chiffrer les images.

Dans le 1er chapitre, nous avons d'abord introduit les généralités sur la sécurité des données et l'état de l'art en cryptographie pour mieux comprendre notre projet.

Dans le 2ème chapitre, nous avons introduit la cryptographie basée sur l'ADN pour comprendre la structure de l'ADN et ses avantages en cryptographie.

Dans le 3ème chapitre, nous avons introduit un système chaotique et ses avantages et étudié différents systèmes chaotiques, nous avons présenté les principales caractéristiques du cryptage avec chaos utilisé dans le schéma de Fridrich.

Dans le 4ème chapitre, nous avons proposé un crypto-système basé sur l'informatique ADN et un système chaotique 3D de Lorenz et Nous constatons que notre algorithme a un bon effet de cryptage, et En raison de la longueur de la clé de séquence chromosomique de l'ADN et de la valeur initiale du système 3D de Lorenz, il peut résister attaque par force brute, attaque différentielle et très sensible à la clé secrète. De plus, l'algorithme proposé peut également résister aux attaques les plus connues, telles que l'analyse statistique et les attaques exhaustives.

Toutes ces caractéristiques montrent que notre algorithme est parfaitement adapté au chiffrement d'images numériques.

Chapitre 2 :

La cryptographie à base d'ADN

2.1 INTRODUCTION :

La cryptographie à base d'ADN est un nouveau paradigme qui se propagent et se développent rapidement, elle est apparue en 1994 après l'expérience de Leonard Adleman qui a résoudre Hamiltonian Path problème en utilisant unique molécules d'ADN échouées et une série de procédures adaptées de la biologie moléculaire. Cela a invoqué un nouveau champ de recherche en bio-informatique.

La cryptographie à base d'ADN a des méthodes basées sur des problèmes et des processus biologiques, il est possible de bénéficier des avantages des systèmes cryptographiques classiques et de les rendre plus efficaces sur certaines méthodes grâce à l'utilisation de l'ADN. Il existe deux façons différentes d'utiliser l'ADN en cryptographie : sous sa forme biologique ou sous sa forme numérique. D'une part, l'ADN biologique peut être utilisé pour le stockage et pour y cacher des données. Les informations secrètes sont placées dans une molécule d'ADN et cachées parmi d'autres molécules d'ADN. D'autre part, des nombres aléatoires peuvent être générés à partir de séquences d'ADN numériques. Enfin, la sécurité et la compression sont très importantes lors de la transmission et du stockage de données informatiques. Cependant, la plupart des systèmes de cryptage peuvent augmenter la taille des données, voire accroître la complexité du calcul.[8]

Dans ce chapitre, nous définirons la molécule d'ADN et ses concepts de base, nous présenterons ses structures ainsi que leurs approches.

2.2 DEFINITION D'ADN :

Nom (en biochimie) Acide désoxyribonucléique : une substance autoreproductrice présente dans la presque totalité des organismes vivants et qui constitue le composant principal des chromosomes. L'ADN est porteur de l'information génétique.[9]

Nom (en biologie quantique- métaphysique) Acide désoxyribonucléique : double hélice formée de moins de cinq pour cent d'instructions biologiques, portant la configuration génétique du corps humain. Plus de 90 % est constitué d'énergie quantique et d'instructions qui confèrent une existence sacrée et recèlent les antécédents akashiques ainsi que l'aspect divin chez l'être humain.[9]

Cette longue double hélice semblable à un escalier en colimaçon qui aurait des millions de marches. Les marches de l'escalier sont formées de quatre types de molécules, appelées bases (nucléotides), associées par paire. À chaque marche, la base adénine (A) est couplée à la base thymine (T), ou la base guanine (G) à la base cytosine (C). Chaque molécule d'ADN extrêmement longue est enroulée dans l'un des chromosomes.[10]

Depuis que James Watson et Francis Crick ont découvert l'organisation en double hélice de l'ADN, cette image élégante est devenue une icône culturelle qui exprime notre aptitude à sonder la structure de la constitution humaine et à y découvrir la beauté et la forme traduisant les fonctions responsables de la vie. La représentation de l'ADN éveille une appréciation esthétique et le sentiment d'avoir découvert une vérité intime sur notre nature même d'être vivant et conscient.[9]

2.3 STRUCTURE D'ADN :

La longue chaîne d'ADN est composée d'une succession de nucléotides (contenant des bases) accrochés les uns aux autres par des liaisons phosphodiester. Les 4 bases qui composent l'alphabet du programme génétique sont A, T, G et C. La molécule d'ADN en version 3D est un assemblage de deux chaînes hélicoïdales (ou brins) s'enroulant autour d'un axe. Cette double hélice est maintenue grâce aux liaisons hydrogène entre les bases qui se font face. Ces bases, dites complémentaires (A s'apparie avec T et C avec G) forment comme les barreaux d'une échelle. Les deux brins d'un ADN donnent donc la même information, comme une photo et son négatif.[11]

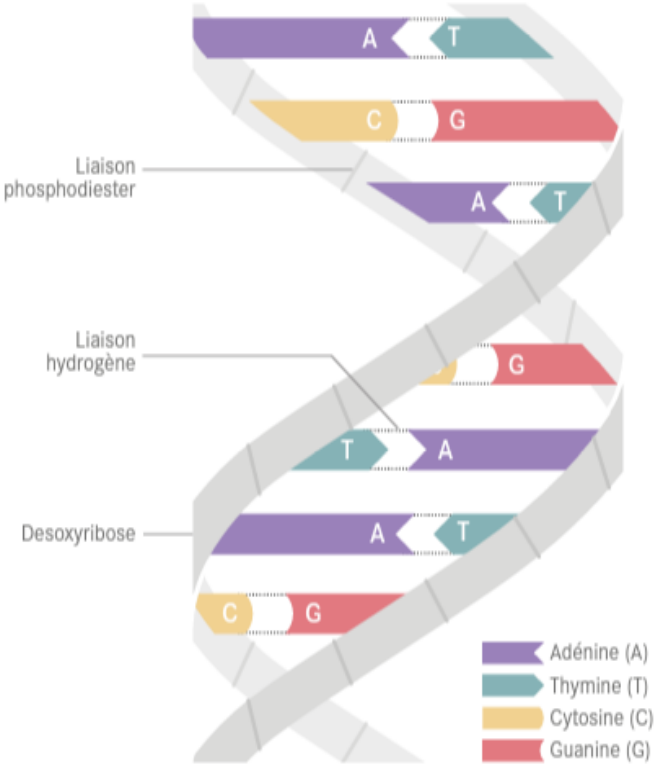


Figure 2.1. Les quatre bases d'ADN

2.4 CODAGE D'ADN :

Les informations sont codées au sein de l'ADN par la disposition des bases (A, T, G et C) suivant une séquence précise. Le code est écrit sous forme de triplets, c'est-à-dire que les bases sont regroupées par trois. Des séquences particulières de trois bases dans l'ADN codent pour des instructions spécifiques, comme l'addition d'un acide aminé à une chaîne. Par exemple, GCT (guanine, cytosine, thymine) code pour l'ajout de l'alanine (acide aminé), et GTT (guanine, thymine, thymine) code pour l'ajout de la valine, un acide aminé. Par conséquent, la séquence d'acides aminés d'une protéine est déterminée par l'ordre des paires de triplet de bases dans le gène correspondant à cette protéine au sein de la molécule d'ADN. Le processus de transformation de l'information génétique codée en une protéine implique la transcription et la traduction.[11]

1re lettre		2e lettre								3e lettre
		U		C		A		G		
U		UUU	Phényl – alanine	UCU	sérine	UAU	tyrosine	UGU	cystéine	U
		UUC	Phényl – alanine	UCC	sérine	UAC	tyrosine	UGC	cystéine	C
		UUA	leucine	UCA	sérine	UAA	STOP	UGA	STOP	A
		UUG	leucine	UCG	sérine	UAG	STOP	UGG	Trypto - phane	G
C		CUU	leucine	CCU	proline	CAU	histidine	CGU	arginine	U
		CUC	leucine	CCC	proline	CAC	histidine	CGC	arginine	C
		CUA	leucine	CCA	proline	CAA	glutamine	CGA	arginine	A
		CUG	leucine	CCG	proline	CAG	glutamine	CGG	arginine	G
A		AUU	isoleucine	ACU	thréonine	AAU	asparagine	AGU	sérine	U
		AUC	isoleucine	ACC	thréonine	AAC	asparagine	AGC	sérine	C
		AUA	isoleucine	ACA	thréonine	AAA	lysine	AGA	arginine	A
		AUG	méthionine	ACG	thréonine	AAG	lysine	AGG	arginine	G
G		GUU	valine	GCU	alanine	GAU	acide aspartique	GGU	glycine	U
		GUC	valine	GCC	alanine	GAC	acide aspartique	GGC	glycine	C
		GUA	valine	GCA	alanine	GAA	acide glutamique	GGA	glycine	A
		GUG	valine	GCG	alanine	GAG	acide glutamique	GGG	glycine	G

Figure 2.2. Codage ADN

2.5 TRANSCRIPTION ET TRADUCTION :

La **transcription** est le processus par lequel l'information codée dans l'ADN est transférée (transcrite) en acide ribonucléique (ARN). L'ARN est une longue chaîne de bases, similaire à un brin d'ADN, sauf que la base uracile (U) remplace la base thymine (T). L'ARN contient donc des informations codées sous la forme de triplets comme l'ADN.[11]

Lorsque la transcription est initiée, une portion de la double hélice d'ADN s'ouvre et se déroule. L'un des brins d'ADN déroulés sert de matrice pour la formation d'un brin complémentaire d'ARN. Le brin complémentaire d'ARN est appelé ARN messager (ARNm). L'ARNm se sépare de l'ADN, quitte le noyau et se déplace dans le cytoplasme cellulaire (partie de la cellule extérieure au noyau, Intérieur d'une cellule). L'ARNm se fixe alors à un ribosome, structure cellulaire minuscule où se produit la synthèse des protéines.[11]

Lors de la **traduction**, le code de l'ARNm (provenant de l'ADN) indique au ribosome l'ordre et le type d'acides aminés à assembler. Les acides aminés sont amenés au ribosome par un ARN beaucoup plus petit appelé ARN de transfert (ARNt). Chaque molécule d'ARNt transporte un acide aminé qui sera ajouté à la chaîne de la protéine en formation. Cette chaîne se replie pour adopter une structure tridimensionnelle complexe sous l'influence des molécules adjacentes, appelées molécules chaperonnes.[11]

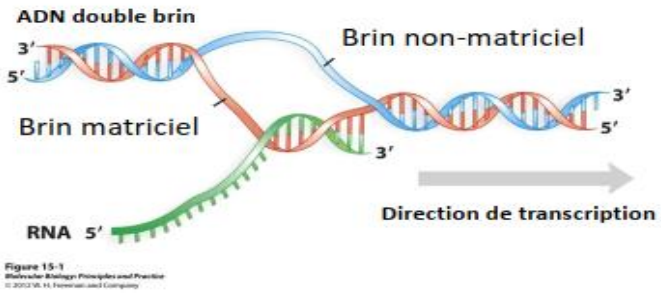


Figure 2.3. La transcription

2.6 LES CHROMOSOMES :

Au moment de la division cellulaire, l'ADN se compacte autour de protéines et s'organise en bâtonnets visibles, les chromosomes. Un chromosome humain débobiné mesure un mètre d'ADN ! Sur ce mètre étalon, certaines fractions sont des instructions qui commandent la synthèse de protéines ; ce sont les gènes. Unités de base de l'hérédité, ils déterminent ce que nous sommes et comment nous fonctionnons (couleur des yeux, groupe sanguin…).[10]

Un chromosome est formé d'un très long brin d'ADN et contient de nombreux gènes (des centaines à des milliers). Les gènes sont disposés sur chaque chromosome suivant une séquence spécifique et chaque gène occupe un emplacement qui lui est propre sur le chromosome (il s'agit de son locus). Outre l'ADN, les chromosomes contiennent d'autres composants chimiques qui influencent la fonction des gènes.[11]

2.7 Appariement :

À l'exception de certaines cellules (par exemple, les spermatozoïdes, les ovules et les globules rouges), le noyau de chaque cellule humaine saine contient 23 paires de chromosomes, soit un total de 46 chromosomes. Normalement, chaque paire se compose d'un chromosome provenant de la mère et d'un autre provenant du père.[11]

On compte 22 paires de chromosomes non sexuels (autosomiques) et une paire de chromosomes sexuels. Les chromosomes non sexuels appariés ont, pour des raisons pratiques, la même taille, forme et position et le même nombre de gènes. Étant donné que chaque chromosome d'une paire de chromosomes autosomiques contient une copie de chaque gène correspondant, en un sens, les gènes portés par les chromosomes autosomiques possèdent une sauvegarde. La 23^{e} paire est la paire de chromosomes sexuels (X et Y).[11]

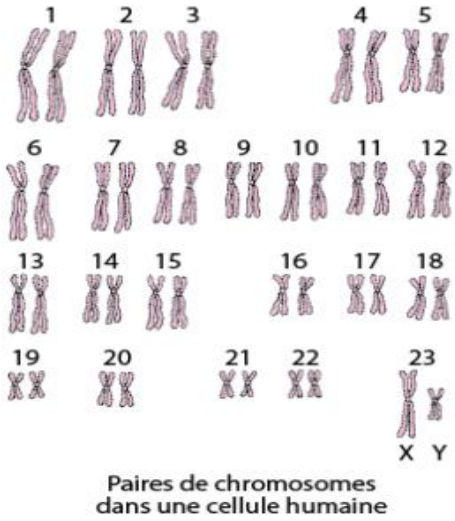


Figure 2.4. Chromosome d'un humain

2.8 LA CRYPTOGRAPHIE A BASE D'ADN :

L'ADN biologique est une molécule très longue, composée d'une succession de nucléotides accrochés les uns aux autres qui forme une chaine très complexe qui peut être utilisé pour le stockage et pour cacher des données à l'intérieur. La cryptographie de l'ADN se développe rapidement. Le regroupement de plusieurs algorithmes et plusieurs techniques et méthodes de chiffrement ainsi que des opérations de calculs dans une approche rend la cryptographie par l'ADN un mécanisme hybride. La cryptographie de l'ADN est très utile car elle requiert les avantages suivants :

A). Capacité à stocker une énorme quantité d'informations : les supports de stockage traditionnels, tels que les cassettes vidéo, nécessitent 1012 nanomètres cubes d'espace pour être stockés, tels que les bandes vidéo, nécessitent 1012 nanomètres cubes d'espace pour stocker un seul bit d'information, les molécules d'ADN n'ont besoin que d'un nanomètre cube par bit. Un gramme d'ADN peut stocker 700 téraoctets d'informations ce qui constitue un stockage à haute densité

B). Traitement parallèle : Les capacités de traitement massivement parallèles des d'ordinateurs à ADN permettent d'accélérer des temps polynomiaux importants, mais autrement solubles, des problèmes en temps polynomial nécessitant relativement peu d'opérations.

C). Performances : L'exécution simultanée de millions d'opérations permet le taux de performance des brins d'ADN d'augmenter de façon exponentielle. L'expérience d'Adleman a été exécutée à 1,014 opérations par seconde, soit un taux de 100 Téraflops (100 trillions d'opérations en virgule flottante par seconde). Le superordinateur le plus rapide du monde ne tourne qu'à 35,8 téraflops.

D). La consommation d'énergie : Les ordinateurs basés sur l'ADN ne nécessitent pas d'électricité. Les processus chimiques qui produisent les unités constitutives de l'ADN se déroulent sans nécessiter d'énergie externe.

Pour crypter à l'aide de l'ADN, l'émetteur et le récepteur crée une table de codage de l'ADN en utilisant la même approche de codage. Le texte en clair est divisé en deux parties égales pour le codage. Un remplissage aléatoire se fait si le texte en clair n'est pas égal. Une table basée sur l'expéditeur est utilisée pour convertir la moitié du texte en clair en une séquence d'ADN, et une table basée sur le récepteur est utilisée pour convertir l'autre moitié du texte en clair en une séquence d'ADN. Le cryptage par ADN est une nouvelle méthode qui utilise l'ADN comme support d'information pour sécuriser les communications de bout en bout.

Prenant l'exemple et l'article de Marc Antonini et son équipe qui travaillent ainsi sur OligoArchive, un projet de trois ans financés à hauteur de trois millions d'euros par la Commission européenne, qui rassemble l'I3S, l'Institut de pharmacologie moléculaire et cellulaire (IPMC), l'école d'ingénieurs Eurocom, l'Imperial Collège à Londres (Royaume-Uni) et enfin la start-up irlandaise Helix Works Technologies Limited. Ensemble, ils visent à obtenir une preuve de concept pour chaque étape du stockage sur ADN : synthétiser et stocker les données, puis être capable de les extraire le plus efficacement possible. Le projet ambitionne de construire un disque ADN : un prototype de bout en bout pleinement fonctionnel qui montre que l'ADN pourrait un jour remplacer les technologies actuelles de stockage d'archives sur bandes magnétiques. [12]

Parmi les principaux écueils à surmonter : le prix. Qu'il soit naturel ou synthétique, l'ADN est composé de séquences de quatre nucléotides, aussi appelés bases. Les systèmes de stockage les utilisent dans un système quaternaire, contrairement au système binaire des ordinateurs. À l'heure actuelle cependant, synthétiser deux cents nucléotides coûte un dollar, sachant qu'encoder une seule image réclame plusieurs milliers de nucléotides. Cela empêche de convertir la masse gigantesque de données à laquelle nous faisons face. [12]

L'équipe d'OligoArchive étudie des solutions pour réduire les coûts : diminuer la quantité de nucléotides nécessaires pour stocker une même quantité d'information. Comme nous l'avons vu, l'ADN se compose de quatre nucléotides différents appelés A, C, G et T. Une première technique simple de codage ADN consiste à leur attribuer chacun deux chiffres binaires : A pour 0 0, C pour 0 1, G pour 1 0 et enfin T pour 1 1. On parle alors de transcodage. [12]

Cependant, si le code ADN synthétique généré pour représenter une donnée numérique ne contient aucune information génétique compréhensible par le monde du vivant, il reste soumis à certaines de ses règles. Par exemple, si un nucléotide est répété trop de fois de manière ininterrompue, son séquençage va subir un certain nombre d'erreurs. Le transcodage ne permet ni de gérer cela facilement ni de contrôler la longueur, et donc le coût, des séquences ADN générées. Pour pallier ces problèmes, les chercheurs proposent d'intégrer un système de codage directement au niveau de la compression des données numériques. Le challenge consiste à créer des séquences de code ADN capables de contenir, en moyenne, encore plus de données numériques sur un même nombre de nucléotides. Ceci réduirait les coûts de synthèse. L'équipe conçoit également des algorithmes qui corrigent automatiquement les erreurs liées au processus de séquençage du code ADN lors du décodage. [12]

« *Lorsque l'on parle au téléphone, les canaux de codage ont parfois des problèmes de bruit qui hachent, voire coupent la communication*, prend comme exemple Marc Antonini. *Le bruit introduit par le séquençage de l'ADN produit en quelque sorte le même phénomène. Nous devons donc rendre l'encodage plus robuste et nous travaillons aujourd'hui dans cette direction. Nous aimerions de plus standardiser les systèmes de compression au-delà de notre groupe d'étude, et nous participons pour cela au comité de standardisation international*

JPEG. » L'équipe se donne trois ans pour apporter ses premières preuves de concept, et ainsi ouvre la voie à un usage concret du stockage sur ADN artificiel. [12]

2.9 OPERATION IMPORTANTES SUR L'ADN UTILISEES DANS LES IMAGES CRYPTOGRAPHIQUES :

Une grande partie de la recherche actuelle en matière de calcul par l'ADN est axée sur la résolution de problèmes difficiles de recherche combinatoire. [VineetGupta (1997)] ont suggéré que pour que l'informatique ADN puisse être appliquée à un plus grand nombre de problèmes, il est nécessaire de prendre en charge les opérations de calcul de base telles que les opérations logiques comme AND, OR et NOT et les opérations arithmétiques comme l'addition et la soustraction. Ces opérations garantissent que seule une sortie unique est générée par des entrées spécifiques, ce qui est la principale exigence des schémas de cryptage et de décryptage. En outre, pour utiliser les opérations de l'ADN, le codage et le décodage des pixels de l'image et le codage numérique des bases de l'ADN sont également nécessaires. Des chercheurs comme [W.C. Chen (2001)], [P.M.J. Allen (1999)] et [W. Piotr (2000)] ont proposé diverses opérations mathématiques basées sur des séquences d'ADN et sur des séquences mathématiques.

2.10 Cryptage d'images à l'aide de l'informatique ADN :

Avec l'évolution de l'informatique ADN, le concept de cryptographie ADN est né. L'informatique ADN prend en charge un parallélisme massif et utilise une très faible consommation d'énergie. Un pixel d'image peut être représenté à l'aide de quatre nucléotides d'ADN et diverses opérations d'ADN peuvent être effectuées dessus à des fins de cryptage. Un certain nombre de techniques de cryptage d'image utilisant des techniques d'ADN ont été proposées dans la littérature qui sont brièvement discutées ci-dessous.

Ayesha Kusoomet al. (2014) ont proposé un schéma de cryptage d'image sélectif dans lequel les images simples sont décomposées en bits les plus significatifs (MSB) et en bits les moins significatifs (LSB). Une carte chaotique unidimensionnelle est utilisée et ses séquences générées sont XORed avec les parties MSB et LSB décodées séparément et finalement ces parties sont combinées pour obtenir l'image chiffrée. En outre, le hachage MD5 128 bits de l'image d'entrée est utilisé pour dériver les paramètres de la carte logistique et la sélection des règles ADN. Pour augmenter l'imprévisibilité de l'image chiffrée, des informations importantes disponibles en clair l'image est chiffrée à l'aide d'une opération d'addition d'ADN quaternaire au lieu d'une opération binaire. Les auteurs ont affirmé que la technique proposée est très robuste contre le bruit et effet de recadrage.

Un algorithme de cryptage d'image utilisant une carte hyperchaotique à quatre dimensions et des opérations ADN a été proposé par X. Huang et G. Ye (2014). Les nombres pseudo-aléatoires sont générés à l'aide d'une carte chaotique 4D qui sont transformées en une séquence d'ADN biologique pour diffuser les blocs d'image. L'image codée par l'ADN est brouillée à l'aide d'une permutation circulaire. Étant donné que la clé secrète utilisée dépend de l'image en clair, les auteurs ont revendiqué la robustesse du schéma de chiffrement proposé pour les attaques de texte en clair/chiffré connues.

Les auteurs de Q. Zhang, L. Liu et X.Wei (2014) ont proposé une technique de cryptage d'image dans laquelle ils ont utilisé le codage de l'ADN et ses opérations avec un système

chaotique quaternaire. Les auteurs ont utilisé le codage de l'ADN quaternaire plutôt que le codage binaire pour améliorer l'efficacité de l'algorithme. En outre, le cryptage de la clé secrète est intégré au processus de cryptage d'image pour améliorer encore la sécurité. La technique proposée a été revendiquée comme étant robuste contre diverses attaques, très sensible à la clé secrète et disposant d'un grand espace de clé.

M. Babaei (2013) a proposé une autre technique de cryptage d'image utilisant la théorie du chaos et des séquences d'ADN. Il a suggéré l'amélioration de la technique de cryptage ponctuel et l'appliquée au texte ainsi qu'aux données d'image. L'auteur a affirmé que la technique proposée est suffisamment sécurisée et fiable pour être utilisée comme méthode de cryptage.[13]

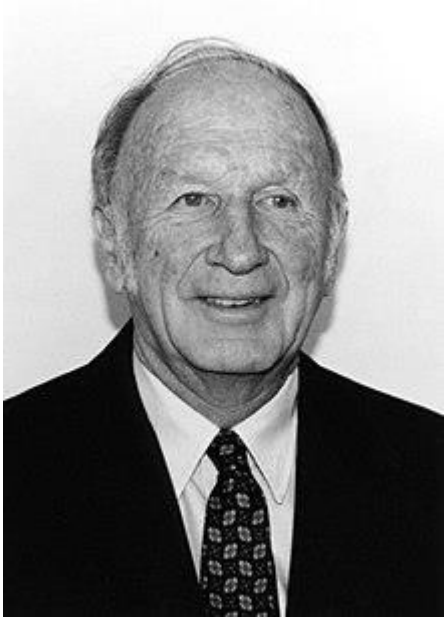
CONCLUSION :

Dans ce chapitre, nous avons présenté brièvement la molécule d'ADN et ses concepts ainsi que sa structure passant à la cryptographie à base d'ADN. Cette dernière n'est qu'à ses débuts. Ces dernières années la cryptographie de l'ADN a connu de grands développements. L'intensification des travaux en cryptographie au cours des dernières années a jeté les bases de l'application des méthodologies de l'ADN à la cryptographie et à la stéganographie. Des recherches et des études sont menées pour identifier une norme cryptographique meilleure et inviolable. À l'heure actuelle, les travaux sur la cryptographie de l'ADN sont axés sur l'utilisation de séquences d'ADN pour coder des données binaires sous une forme ou une autre. Bien que le domaine soit extrêmement complexe et que les travaux actuels soient encore en phase de développement, il y a beaucoup d'espoir que l'informatique de l'ADN soit une bonne technique pour la sécurité de l'information.

Chapitre 3 :
La cryptographie à base de Chaos

Système Chaotique :

3.1 Introduction à la théorie du chaos :



Le chaos peut être considéré comme une sorte d'ordre sans période, abondant, forme irrégulière et complexe mouvement qui existe dans la nature. Le domaine a été lancé par Lorenz en 1963, un météorologue à l'Institut de Technologie de Massachusetts, découvert l'attracteur et connu depuis sous le nom de fameux "effet papillon". Lorenz déduit que les prévisions météorologiques à long terme sont imprévisibles. L'effet papillon" est souvent utilisé dans des systèmes complexes difficiles à prévoir sur une longue période de temps, comme la météo et les marchés boursiers. Cet effet montre que le résultat du développement des choses a une dépendance très sensible sur les conditions initiales, et un très petit écart par rapport aux conditions initiales conditions qui entraîneront de grandes différences dans les résultats. Lorenz a souvent utilisé le terme ***papillons poétiques*** dans ses discours et ses articles pour expliquer la dépendance sensible du chaos aux valeurs : « Un papillon battant des ailes au Brésil peut provoquer une tornade au Texas un mois plus tard. Dans une certaine dynamique du système, une très petite déviation des conditions initiales entraînera de grandes différences dans les résultats." Ce phénomène montre que les résultats du système sont extrêmement sensibles aux conditions initiales. En 1975, le mathématicien américain Yorke et son étudiant diplômé Li Tianyan publié un article qui a donné un nom au phénomène. Sous le nom du chaos [14].

La découverte du chaos dans un système dynamique non linéaire déterministe était connue sous le nom de trois révolutions de la physique au XXe siècle (relativité, science quantique, phénomènes chaotiques).

« La théorie du chaos nous enseigne que nous faisons toujours partie du problème et que la tension et la dislocation se déroule toujours à partir du système entier plutôt qu'à partir d'une « partie » défectueuse. Envisager un problème comme un problème purement mécanique à résoudre peut apporter un soulagement temporaire de symptômes, mais le chaos suggère qu'à long terme, il pourrait être plus efficace d'examiner l'ensemble contexte dans lequel un problème particulier se manifeste [15].

3.2 La naissance de la théorie du chaos :

Le début de la théorie du chaos remonte au mathématicien Français Poinga à la fin du XIXe siècle et au début du 20 e siècle. Jules Henri Poincaré a posé une série de questions sur le problème des trois corps dans le système solaire. En 1913, Poincaré a combine la dynamique et topologie pour étudier et utiliser les diagrammes de phase, topologie et les méthodes de section efficace de l'espace des phases pour souligner que l'interaction gravitationnelle de trois corps peut produire des comportements complexes et surprenants. Certaines solutions d'équations déterministes sont imprévisibles, rendant le problème à trois éléments impossibles à résoudre avec précision, donc le résultat est aléatoire. Poincaré est devenu le premier à découvrir un certain système de chaos et mettre en place les bases de la modernité théorie du chaos [16]

3.3 Les caractéristiques chaos :

1. Sensible aux valeurs et paramètres initiaux. Les légers changements de la valeur initiale et la valeur du paramètre du système chaotique entraînera l'apparition de l'état futur d'un énorme changement, similaire au fameux "effet papillon". Cette caractéristique satisfait la clé exigences en cryptographie.

2. Aléatoire. Il est tout à fait logique que le système soit particulièrement sensible à la valeur initiale, et se caractérise par une instabilité locale du système

3. Certitude. Lorsque la valeur initiale et les paramètres associés d'un système chaotique sont déterminés, la séquence chaotique obtenue est également déterminée. En d'autres termes, le mouvement du système chaotique peut être contrôlé, ce qui est également la base de l'application de chaotique la théorie à la pratique ;

4. Ergodicité. La trajectoire chaotique traversera toute la zone chaotique où elle se trouve

[17].

3.4 Classification du système chaotique :

Le système chaotique peut être classé en deux catégories, Système chaotique (peut avoir au moins unidimensionnel), et système hyper-chaotique (peut avoir au moins quatre dimensions) représenté par des équations aux dérivées partielles ou des équations aux différences comme dans la Figure 3.1.

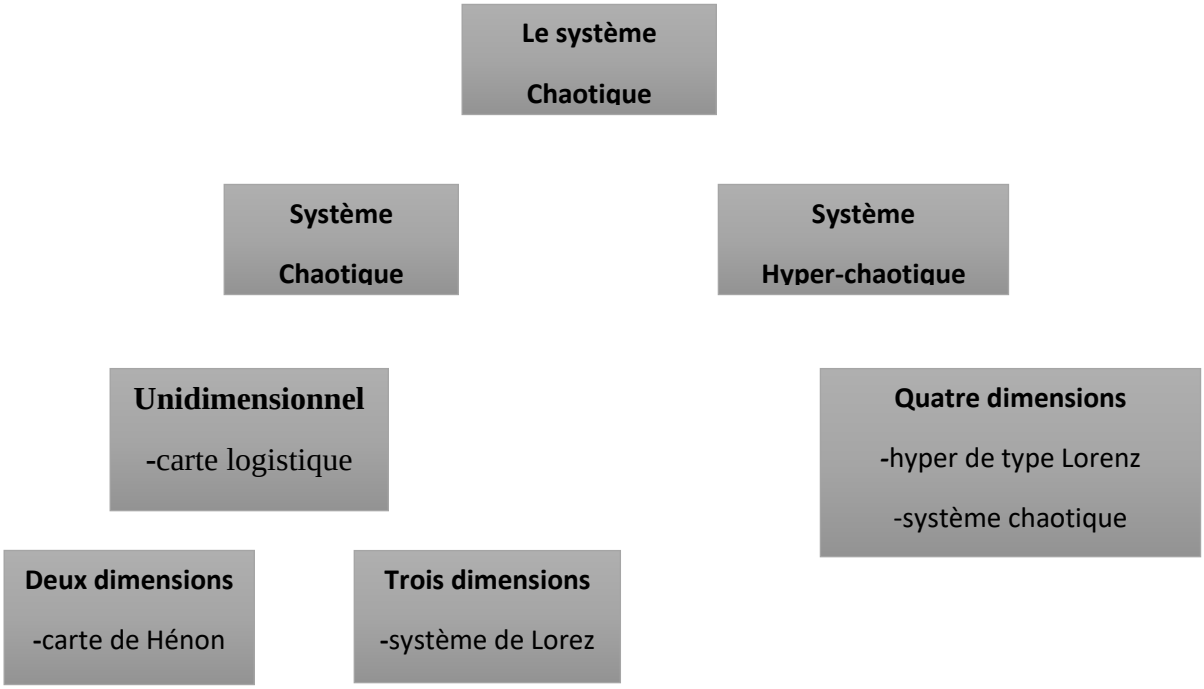


Figure 3.1. Classification du système chaotique avec des exemples

3.5 Système chaotique unidimensionnel :

3.5.1 Carte logistique :

L'équation logistique est également connue sous le nom de modèle de population d'insectes, et elle a été popularisée par le biologiste Robert May dans une étude de 1976. Il est utilisé pour étudier le lien entre le nombre d'insectes individuels et les conditions environnementales. C'est une équation non-linéaire unidimensionnelle à la fois simple et importante. (1) La carte logistique s'écrit comme suit :

$$x_{n+1}=rx(1-x_n) \quad (1)$$

Où **xn** est un nombre compris entre zéro et un qui représente le rapport de la population existante à la population maximale. Les valeurs d'intérêt pour le paramètre **r** (parfois aussi notés μ) sont ceux dans l'intervalle [0,4] de sorte que **xn** reste délimité sur [0,1]. Figure 3.2. montre un diagramme de bifurcation mappé logistique [18].

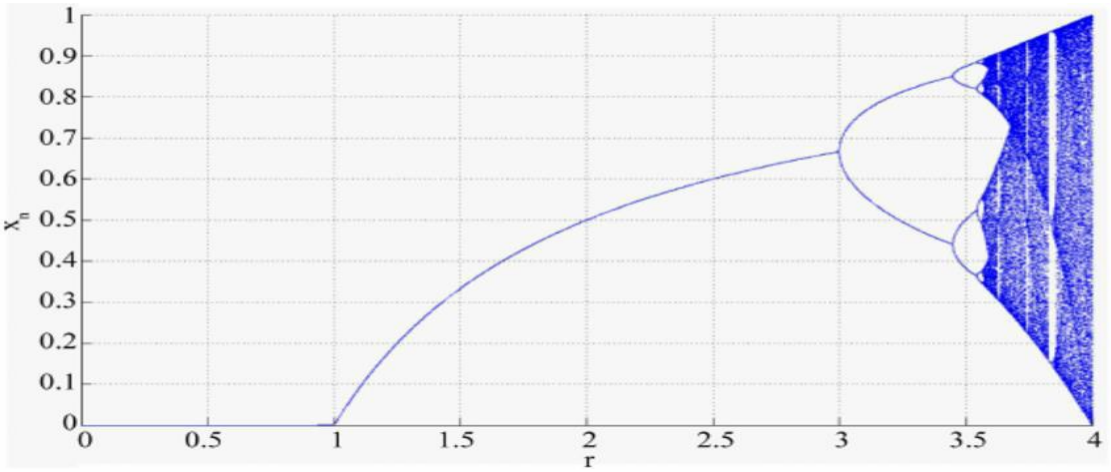


Figure 3.2. Un diagramme de bifurcation de la carte logistique

3.5.2 Tente Coy:

Les expressions mathématiques de tente Coy Où **μ** est une constante réelle positive. Sont affichées ci-dessous comme suit :

$$xn{+}1{=}f(xn){=}\begin{cases}\mu xn & \text{pour } xn{<}12\\ (1{-}xn) & \text{pour } 12{\leq}xn\end{cases} \qquad (2)$$

En choisissant par exemple le paramètre **μ=2**, l'effet de la fonction **μ** peut être considéré comme le résultat de l'opération de pliage de l'intervalle unitaire en deux, alors en étirant l'intervalle résultant [0,1/2] pour obtenir à nouveau l'intervalle [0,1]. En répétant la procédure, tout point **x0** de l'intervalle prend de nouvelles positions successives comme décrit ci-dessus, générant une séquence **xn** dans [0,1]. Figure 3.3. : montre un diagramme de bifurcation pour la carte de tente [19].

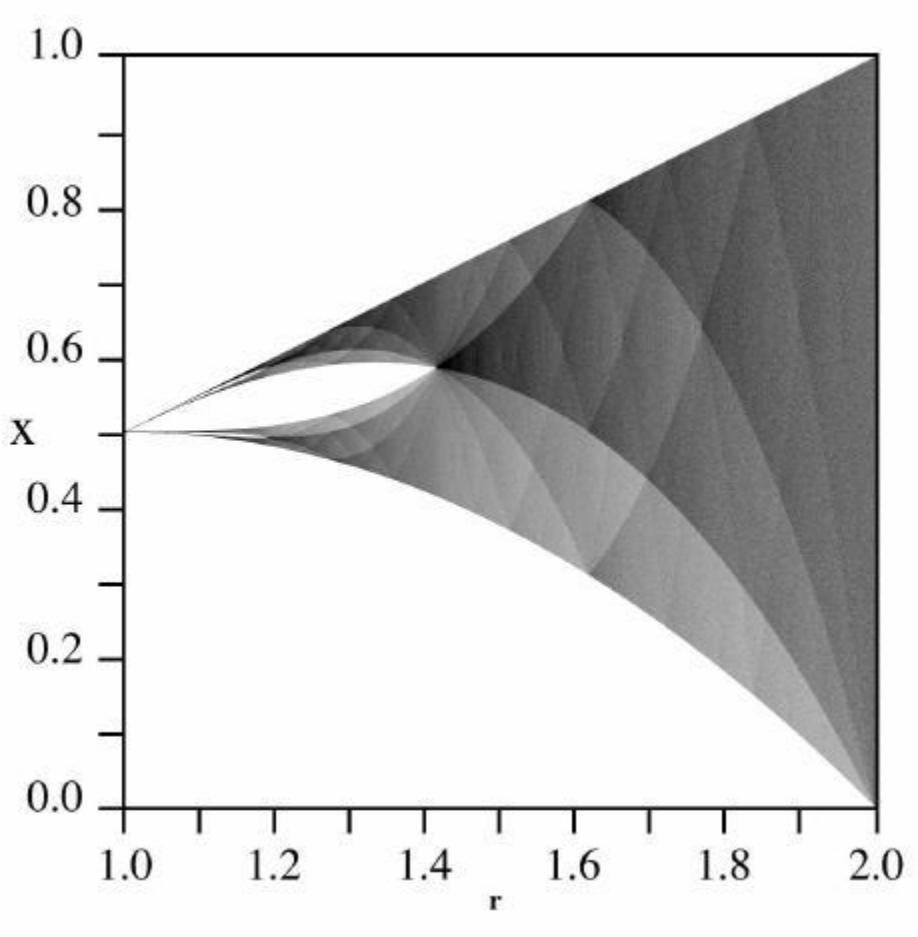


Figure 3.3. Diagramme de bifurcation pour la carte de la tente

3.6 Système chaotique à deux dimensions :

La cartographie bidimensionnelle joue un rôle dans la liaison d'une dimension à une dimension élevée. L'étude des phénomènes chaotiques en cartographie bidimensionnelle permet de comprendre et prédire le comportement de systèmes dynamiques de grande dimension plus complexes.

3.6.1 Plan d'Hénon :

La carte de Hénon est un système dynamique à temps discret également connu sous le nom Hénon Pomeau attracteur /carte. C'est l'un des exemples les plus étudiés de comportement chaotique dans le système dynamique. Un point **(xn, yn)** dans le plan est représenté sur un nouveau point à l'aide de la carte de Hénon, donné par :

$$\begin{cases} x_{n+1} = 1 - a x_{n2} + y_n \\ y_n + 1 = b x_n \end{cases} \qquad (3)$$

La carte dépend de deux paramètres, a et b, qui pour l'application de Hénon classique pourrait avoir des valeurs de a = 1,4 et b = 0,3. Pour les valeurs classiques, la carte de Hénon est

chaotique. Pour les autres valeurs de a et b, la carte peut être chaotique, intermittente ou peut converger vers une orbite périodique. Un aperçu du type de comportement de la carte à différentes valeurs de paramètres peut être obtenu à partir de son orbite diagramme.

La carte a été introduite par Michel Hénon comme un modèle simplifié de la section Poincaré du modèle de Lorenz. Pour la carte classique, un point initial du plan approchera soit un ensemble de points connus sous le nom d'attracteur étrange de Hénon ou divergera à l'infini. L'attracteur de Hénon est un fractale, lisse dans un sens et un ensemble Cantor dans un autre. Les estimations numériques produisent une corrélation dimension de 1,25 ± 0,02[2] et une dimension de Hausdorff de 1,261 ± 0,003[3] pour l'attracteur de la carte classique [20]. L'attracteur de Hénon pour a = 1,4 et b = 0,3 est illustré sur la Figure 3.4. :

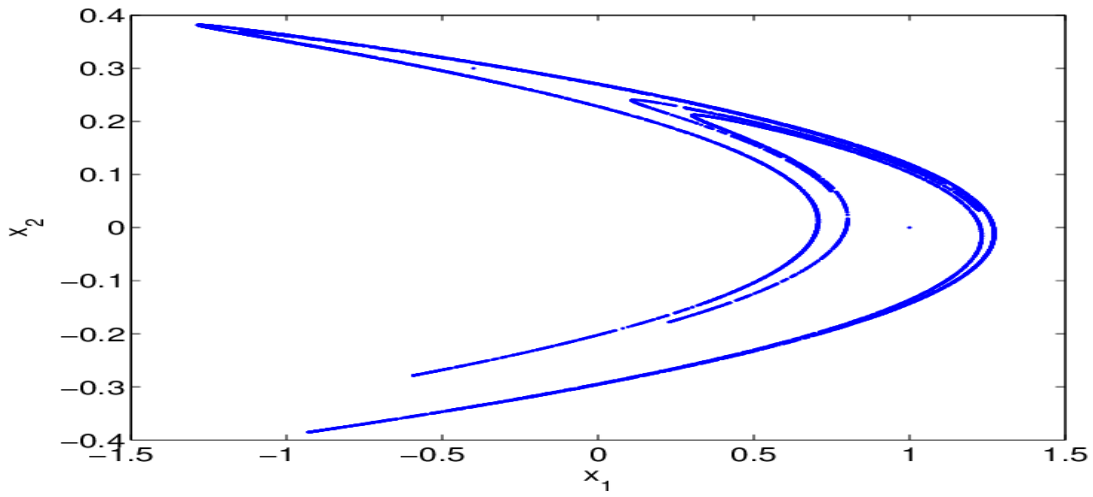


Figure 3.4. Attracteur Hénon

3.6.2 Carte Duffing :

La carte de Duffing (également appelée « carte de Holmes ») est un système dynamique à temps discret. C'est est un exemple de système dynamique qui présente un comportement chaotique. La carte de Duffing prend un point **(xn, yn)** dans le plan et le fait correspondre à un nouveau point donné par

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = -bx_n + ay_n - y_n^3 \end{cases} \qquad (4)$$

La carte dépend des deux constantes a et b. Ceux-ci sont généralement définis sur a = 2,75 et b = 0,2 pour produire un comportement chaotique. La carte de Duffing montrant un comportement chaotique, où a = 2,75 et b=0,15 est illustré dans la Figure 3.5. [21].

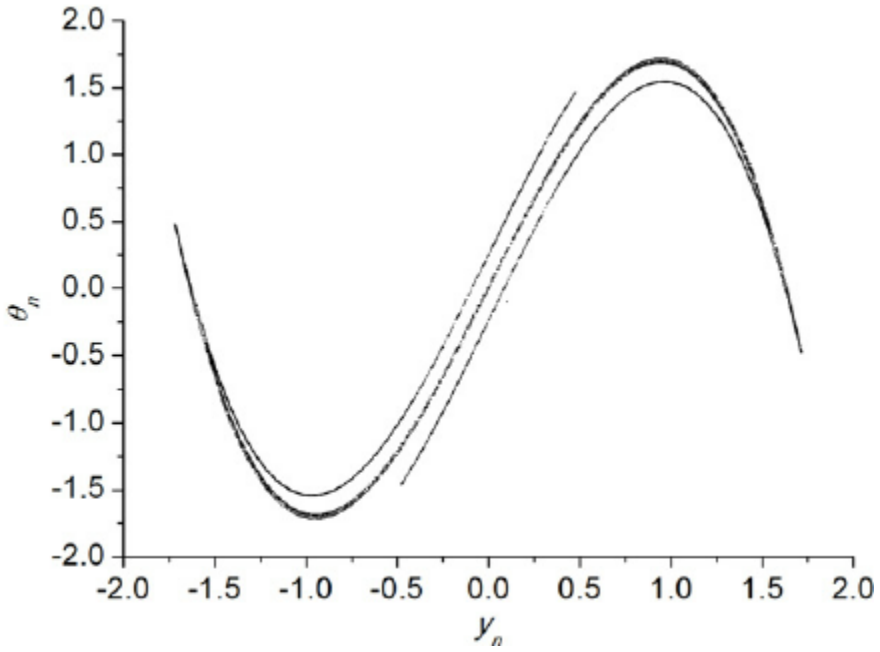


Figure 3.5. Plot de la carte de Duffing

3.7 Système chaotique de trois dimensions :

3.7.1 Système de Lorenz :

Le système de Lorenz est un système d'équations différentielles ordinaires étudié pour la première fois par Edward Lorenz vers 1960, qui est un système dynamique décrit par le système non linéaire suivant de équations différentielles ordinaires :

$$\begin{cases} dx/dt = a(y-x), \\ dy/dt = xz-y, \\ dz/dt = b-xy-cz \end{cases} \quad (5)$$

Les nombres réels a, r, b sont appelés les paramètres de contrôle, tandis que x, y, z sont appelés les variables d'état.

La Figure 3.6. montre l'attracteur impair de Lorenz avec les valeurs a = 28, r = 10 et b = 8/3. La dépendance sensible aux conditions initiales, également connue sous le nom d'effet papillon, est une caractéristique d'un système dynamique qui commence à partir de l'une de plusieurs circonstances initiales alternatives arbitrairement proches sur l'attracteur, provoquant un étalement arbitraire des points itérés [22].

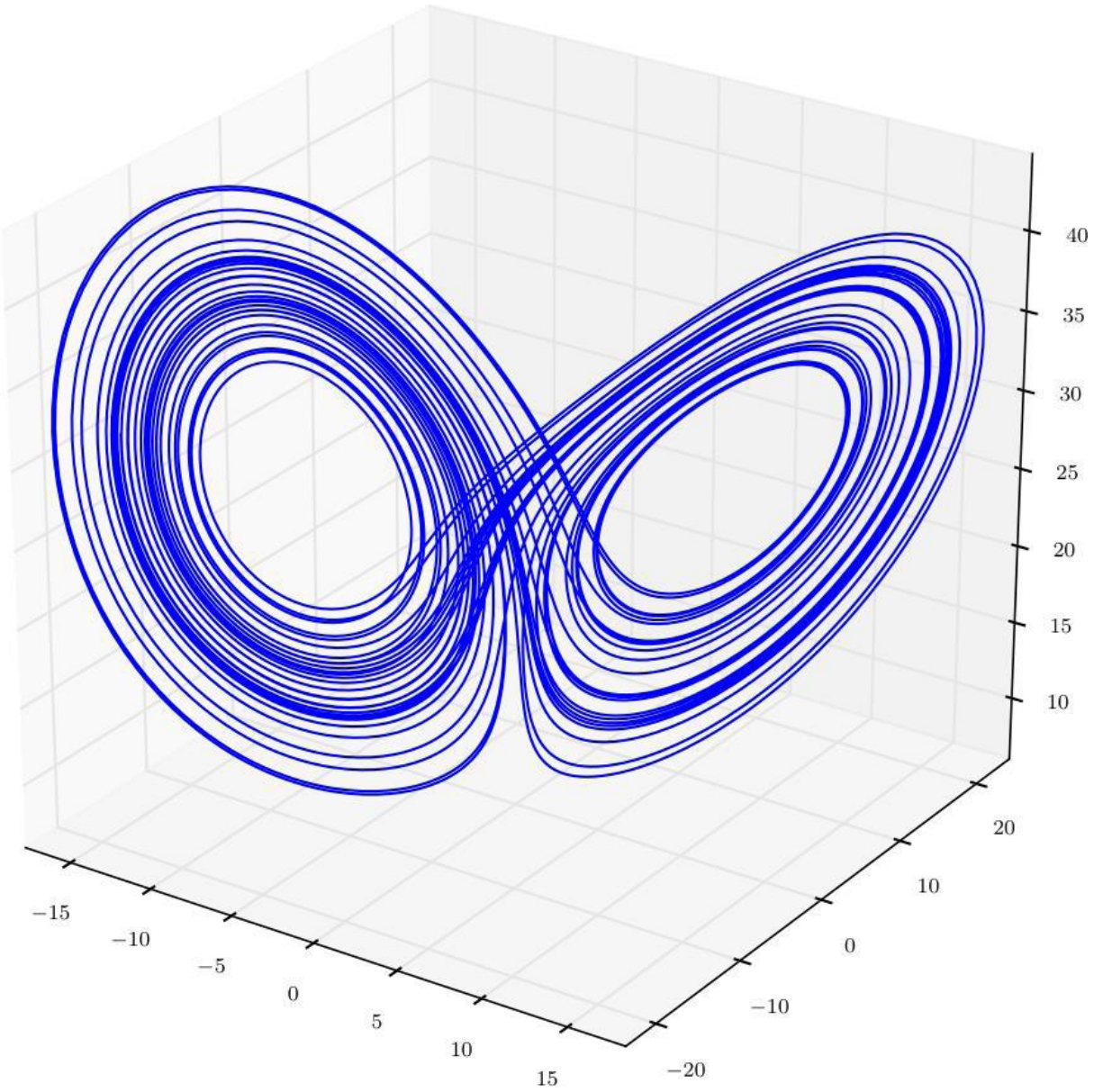


Figure 3.6. Un exemple de solution dans l'attracteur de Lorenz

3.7.2 Système Rössler :

Dans les années 1970, Rössler a étudié le système Rössler. Il s'agit d'un système à trois non linéaires systèmes d'équations différentielles. Ces équations différentielles créent une dynamique en temps continu système à dynamique chaotique liée aux caractéristiques fractales de l'attracteur. Le système Rössler les équations sont les suivantes :

$$\begin{cases} dx/\,dt = -y - z, \\ dy/\,dt = x + ay, \\ dz/\,dt = b + z\,(x - c) \end{cases} \qquad (6)$$

L'attracteur de Rössler pour les valeurs a=0.2 b = 0.2, c = 5.7 est illustré sur la Figure 3.7. [10]

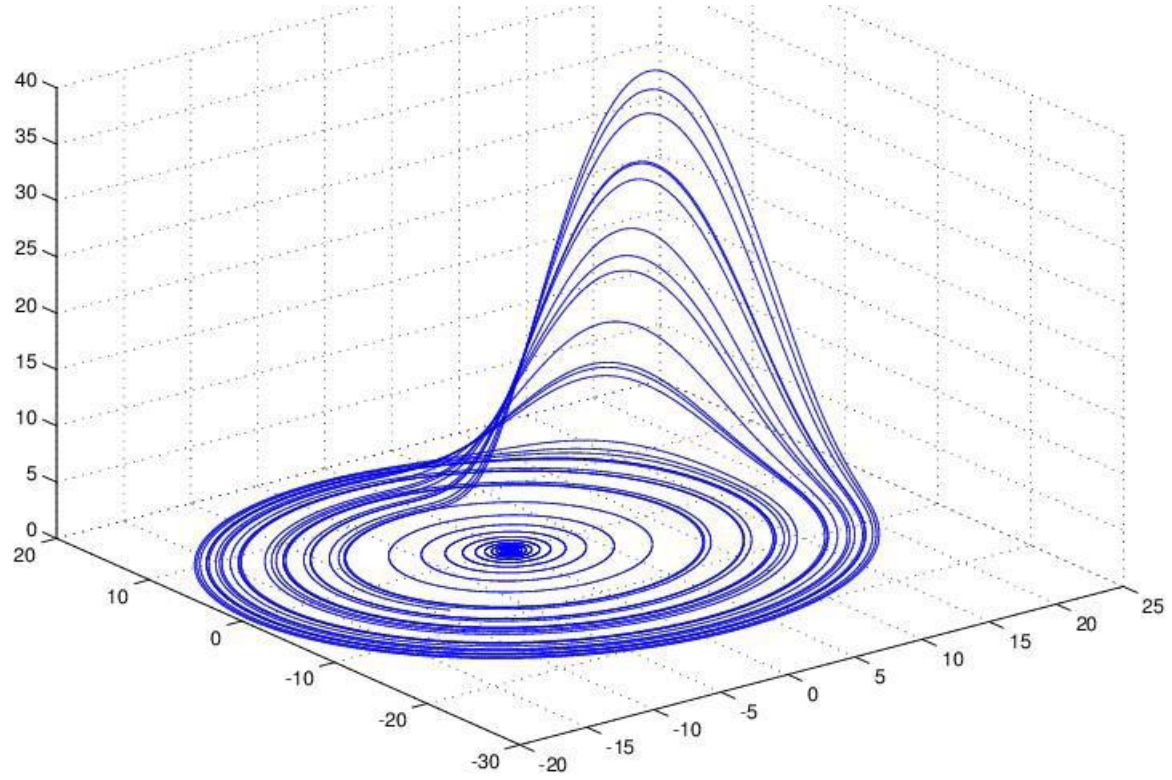


Figure 3.7. attracteur de Rössler

Le comportement des systèmes chaotiques tridimensionnels dépend fortement de la valeur initiale et hautement imprévisible. Après une longue période de mouvement, il se transformera d'un état prévisible mouvement vers un comportement aléatoire inattendu. Les solutions chaotiques se caractérisent par leur sensibilité aux conditions de départ et à l'imprévisibilité de l'avenir.

3.8 Système hyper-chaotique à quatre dimensions :

3.8.1 Système hyper-chaotique de type Lorenz :

Les systèmes hyper-chaotiques peuvent être obtenus en ajoutant une variable d'état supplémentaire à un système chaotique tridimensionnel, en introduisant un contrôleur de rétroaction linéaire w dans l'équation de Lorenz 3D, et en ajoutant une équation d'état différentielle non linéaire du premier ordre par rapport à w, l'équation obtient un nouveau système chaotique de type Lorenz 4D comme suit :

$$\begin{cases} dx/\,dt = a\,(y - x) - ew, \\ dy/\,dt = xz - hy, \\ dz/\,dt = b - xy - cz, \\ dw/\,dt = ky - dw. \end{cases} \qquad (7)$$

Telque x, y, z et w sont des variables d'état et a, b, c, d, e, h sont des paramètres positifs du système.

L'attracteur de système chaotique de type Lorenz 4D est illustré sur la Figure 3.8. [23].

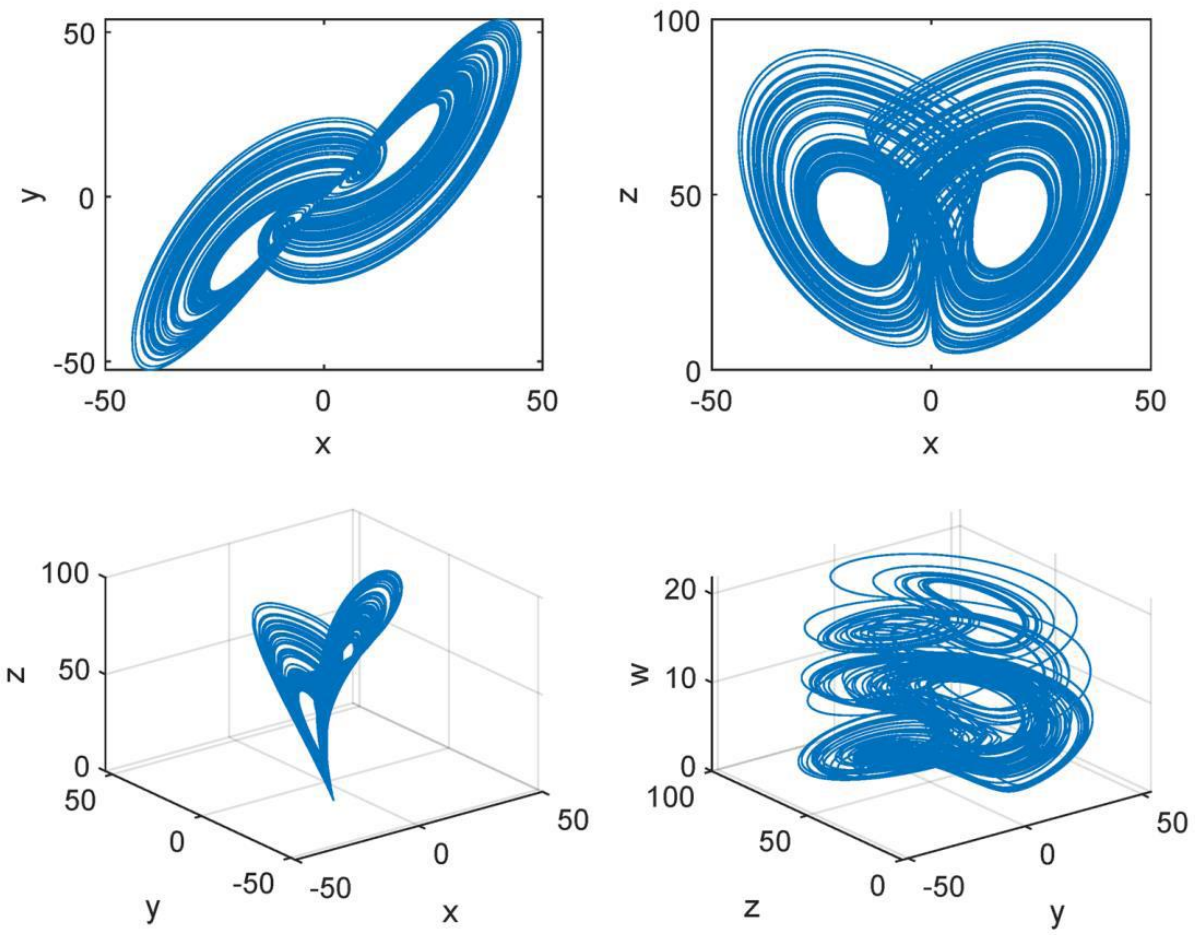


Figure 3.8. Attracteur de système chaotique de type Lorenz 4D

3.9 Chaos et cryptographie :

La cryptographie chaotique est l'application de la théorie mathématique du chaos à la pratique de la cryptographie, qui est l'étude des moyens d'envoyer des informations discrètement et en toute sécurité dans la présence d'un tiers ou d'un adversaire. L'utilisation du chaos dans la cryptographie a attiré l'attention depuis ce temps et a été étudié à l'origine par Robert Matthews en 1989. Des inquiétudes de longue date concernant la sécurité et la vitesse de mise en œuvre, d'autre part, continuent d'entraver sa mise en œuvre.

La cryptographie chaotique et la cryptanalyse chaotique sont les deux techniques qui composent la cryptologie chaotique. Le cryptage des informations pour une transmission sûre est appelé cryptographie, tandis que le décryptage et le décodage des signaux cryptés codés sont appelés cryptanalyse.

Pour utiliser efficacement la théorie du chaos en cryptographie, des cartes chaotiques doivent être construites de telle sorte que l'entropie créée par la carte puisse fournir la confusion et la diffusion nécessaires.

Les systèmes chaotiques et les primitives cryptographiques ont des propriétés similaires qui permettent d'utiliser systèmes chaotiques en cryptographie. Si des paramètres chaotiques, ainsi que des clés cryptographiques, peuvent être traduit symétriquement ou mis sur carte pour générer des sorties acceptables et fonctionnelles, un adversaire aura du mal à trouver les sorties sans connaître les valeurs de départ. Parce que les cartes chaotiques nécessitent un ensemble restreint de nombres dans un environnement réel, elles peuvent ne servir à rien de pratique valeur dans un cryptosystème si le comportement chaotique peut être prévu.

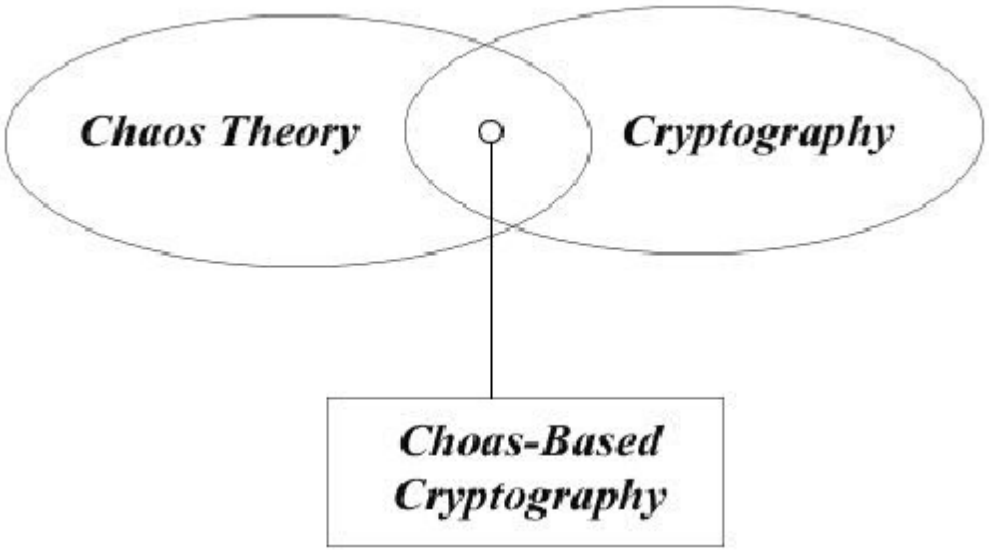


Figure 3.9. le concept de cryptographie basée sur le chaos

3.9.1 Diagramme de Fridrich :

En 1997, Fridrich a proposé un schéma de cryptage basé sur le chaos. Il a été largement référencé depuis 1997 et est devenu la base fondamentale de la plupart des techniques de cryptage d'images basées sur le chaos.

La Figure 3.10. Décrit la structure générale des crypto-systèmes de Fridrich, avec les couches de confusion et la diffusion fonctionnant indépendamment. La notion de cette méthode a été appliquée dans plusieurs articles pour construire des crypto-systèmes robustes.

Le processus de confusion est d'abord appliqué Rc fois à un bloc (ou à l'image entière), puis le processus de diffusion est appliqué Rd fois à la sortie du processus de confusion, et les deux processus sont ensuite répétés R fois.

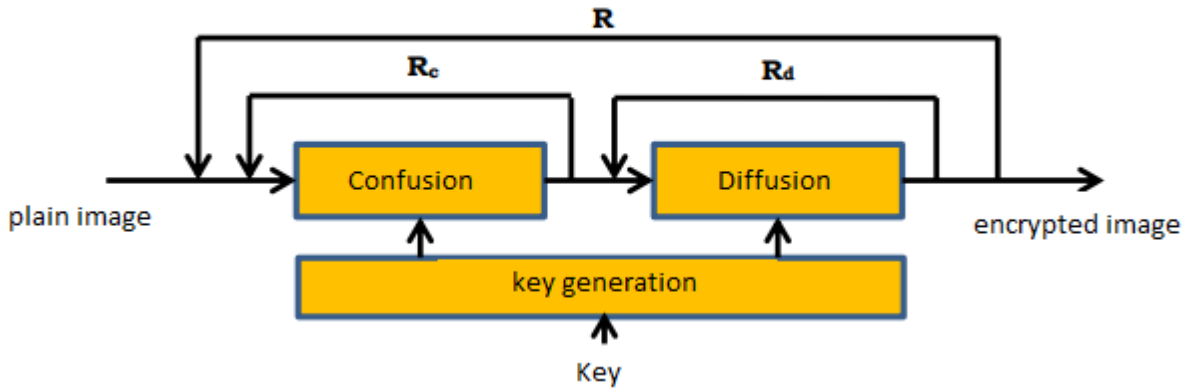


Figure 3.10. Diagramme de Friedrich

En mélangeant au hasard les positions des pixels, la confusion tente de générer une relation complexe entre les statistiques de l'image cryptée et la clé. En décalant les valeurs de pixel, la diffusion tente de construire un lien statistique complexe entre l'image claire et l'image cryptée image (Stallings, 2006)

Une procédure de substitution est utilisée pour créer la confusion. Dans la méthode de Fridrich, la substitution est accomplie en utilisant des cartes de permutation chaotique 2D comme le Cat, le standard ou Baker. Les pixels de l'image sont déplacés en permutation, mais leurs valeurs restent inchangées. En diffusant l'effet de chaque bit de la diffusion gratuite image sur l'ensemble des bits cryptés, le processus de diffusion affecte les caractéristiques statistiques de l'image en clair. Tout crypto-système sécurisé nécessite le processus de diffusion ; sinon, le système est facilement cassé. Les clés des processus de confusion et de diffusion sont générées à l'aide d'un pseudo-aléatoire générateur basé sur des cartes chaotiques (El Assad et al. 2014 ; Fridrich, 1997, 1998) [24].

3.9.2 Type de cryptographie chaotique :

Le concept de cryptographie chaotique ou, en d'autres termes, la cryptographie basée sur le chaos peut être

Divisé en deux grands groupes :

* cryptographie chaotique asymétrique

* cryptographie chaotique symétrique

La majorité des algorithmes basés sur le chaos symétrique sont basés sur l'application de

Cartes chaotiques dans leur processus

3.9.3 Applications :

a) Cryptage des images :

Bourbakis et Alexopoulos en 1991 ont proposé soi-disant le premier projet entièrement destiné schéma de cryptage d'image numérique basé sur le langage SCAN. Plus tard, avec le

Émergence de la cryptographie basée sur le chaos des centaines de nouveaux algorithmes de chiffrement d'images, tous avec l'objectif d'améliorer la sécurité des images numériques ont été proposés. Cependant, il y avait trois principaux aspects de la conception du cryptage d'image qui étaient généralement modifiés dans différents algorithmes (carte chaotique, application de la carte et structure de l'algorithme). Le premier et peut-être le plus point crucial était la carte chaotique appliquée dans la conception des algorithmes. La vitesse du cryptosystème est toujours un paramètre important dans l'évaluation de l'efficacité d'un algorithme de cryptographie, par conséquent, les concepteurs étaient initialement intéressés par l'utilisation d'algorithmes chaotiques simples des cartes telles que des cartes de tente et la carte logistique. Cependant, en 2006 et 2007, la nouvelle image algorithmes de cryptage basés sur des cartes chaotiques plus sophistiquées a prouvé que l'application d'une carte chaotique avec une dimension plus élevée pourrait améliorer la qualité et la sécurité des cryptosystèmes

b) Génération de nombres aléatoires :

Le comportement imprévisible des cartes chaotiques peut être utilisé dans la génération de cartes aléatoires. Certains des premiers générateurs de nombres aléatoires basés sur le chaos ont essayé de générer directement nombres aléatoires de la carte logistique.

c) Fonction Hash :

Un comportement chaotique peut générer des fonctions de hachage

3.10 Techniques de cryptage d'images basées sur le chaos :

Les cartes chaotiques sont non linéaires et déterministes. Ils sont très sensibles aux paramètres d'entrée et une légère modification de ces paramètres entraîne une sortie entièrement différente dans les cartes chaotiques. Un certain nombre d'algorithmes de cryptage d'images utilisant des cartes chaotiques ont été proposé dans la littérature. Une revue de divers algorithmes de chiffrement basés sur le chaos est présentée dans cette section.

Dragon (2014) a proposé un algorithme pour obtenir des boîtes de substitution bijectives (S-boxes) basé sur des cartes chaotiques et une méthode de composition. Les boîtes de substitution de départ peuvent être obtenues à l'aide de cartes chaotiques ou de toute autre méthode disponible. Les boîtes de sortie S sont obtenues en réalisant diverses compositions de cartes de départ. La disposition et la fréquence des boîtes S initiales dans la composition sont basées sur des cartes chaotiques. Étant donné que les cartes chaotiques sont utilisées pour fournir un caractère aléatoire, n'importe laquelle des cartes chaotiques existantes avec un bon pseudo-aléatoire peut être utilisée.

Iqtadar Hussainet al. (2014) a proposé une autre méthode de cryptage d'image basée sur des réseaux de cartes couplés et des boîtes de substitution qui est la version modifiée d'un de leurs travaux antérieurs. Wang et al. (2009) ont déterminé que l'algorithme de chiffrement basé sur la confusion et la permutation comporte deux points faibles : (i) les valeurs de commande pour la permutation sont permanentes dans le chiffrement ; (ii) la séquence de touches est obtenue à partir de la trajectoire chaotique en s'appuyant uniquement sur la touche. Par conséquent, dans ce travail, une technique de cryptage est proposée au moyen de paramètres de commande modifiables. Les emplacements des pixels de l'image sont mélangés en utilisant une carte de tente chaotique et après cela, des réseaux de carte couplés retardés et une transformation en S-box sont utilisés pour résoudre l'association entre l'original image et l'image cryptée.

L'avantage de l'approche est que la confusion et la diffusion du cryptosystème sont améliorées et que le cryptosystème est rendu plus sûr contre les attaques bien connues.

XingyuanWanget al. (2014) ont proposé un algorithme de chiffrement d'images basé sur des boîtes de substitution dynamiques. Le dernier pixel de l'image d'entrée et une clé externe de 256 bits sont utilisés pour générer les paramètres et les conditions initiales de la première S-box. La clé étant dépendante de l'image d'entrée influencera la construction des S-box afin de résister aux attaques différentielles et aux attaques en clair choisies. L'image d'entrée est d'abord divisée en groupes de taille égale selon les rangées et les rangées adjacentes sont dans des groupes différents. Pour chaque groupe, une nouvelle S-box est générée et utilisée. De cette façon, les corrélations entre la verticale les pixels adjacents sont minimisés. La même méthode est appliquée sur les colonnes afin de minimiser la corrélation entre les pixels adjacents horizontaux. Pour améliorer la sécurité, le cryptage est effectué à partir de quatre directions. L'algorithme est résistant aux attaques de texte brut différentiel et choisi.

Xuanping Zhang et al. (2014) ont proposé un schéma de cryptage d'image basé sur une carte chaotique spatio-temporelle. La boîte de substitution circulaire et le tampon de flux de clé sont utilisés pour réaliser le processus de confusion et de diffusion. Les nombres pseudo-aléatoires dans le chiffrement sont produits par un système chaotique spatio-temporel modélisé par un réseau de cartes couplées (CML). La carte chaotique logistique et la carte chaotique linéaire par morceaux sont adoptées dans CML pour produire des nombres pseudo-aléatoires qui sont ensuite convertis en valeurs entières à utiliser pour la construction de la boîte S. La S-box est traitée comme une séquence circulaire avec le pointeur de tête. Les pixels de l'image sont remplacés par les valeurs de la case S sélectionnée en fonction à la fois de la valeur de pixel et le pointeur de tête. Après le processus de substitution, la diffusion est utilisée, le tampon de flux de clés est utilisé pour mettre en cache les nombres aléatoires générés par le système chaotique. Pour chiffrer le pixel, le nombre aléatoire choisi dépend du précédent pixel rendant la diffusion efficace. Les résultats expérimentaux et diverses analyses montrent que l'algorithme proposé est résistant aux attaques.[25]

3.11 Conclusion :

Ce chapitre se concentre sur les techniques de cryptage d'image basées sur le chaos sécurisé. On a défini le chaotique et sa naissance ainsi que ses caractéristiques. La classification de système chaotique est devisée par deux systèmes (chaotique, hyper-chaotique). Nous avons présenté le système de Lorenz qui fait l’objet de notre approche.

Chapitre 4 :
Implémentations et résultats

4.1 Introduction :

Avec le développement rapide d'Internet et de l'innovation dans les technologies, la sécurité des contenus de données multimédias, tels que les vidéos et les images, est devenue un problème sérieux.

Nous avons présenté dans les chapitres précédents un état de l'art autour de la cryptographie à base d'Adn et le chao. Le présent chapitre fait l'objet d'une description détaillée de notre algorithme de cryptage d'image couleur à base de Chao et Adn. Une série des expérimentations a été faite pour démontrer la robustesse de notre algorithme.

4.2. Théorie de base de l'algorithme proposé :

4.2.1. Cryptage des séquences d'ADN :

4.2.1.1. Séquence chromosomique d'ADN :

Chaque organisme vivant possède une séquence d'ADN unique de grande longueur, Dans notre algorithme, nous utilisons cette séquence comme l'un des paramètres de la clé chiffrement. Par exemple, nous utilisons la séquence du chromosome 1 d'Arabidopsis thaliana (ADN linéaire de 30427671 pb, taille de 17,4 Mo [NCBI.nlm.nih.gov]. Qui est une petite plante à fleurs originaire d'Eurasie et d'Afrique, comme le montre la Figure.1&2 [28].

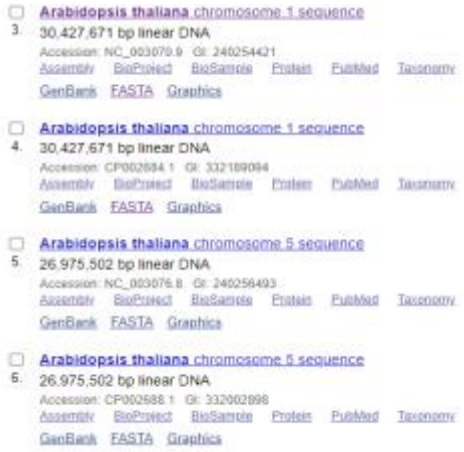


Figure 4.1. Séquence d'ADN de la base de données publiquement disponible du NCBI.

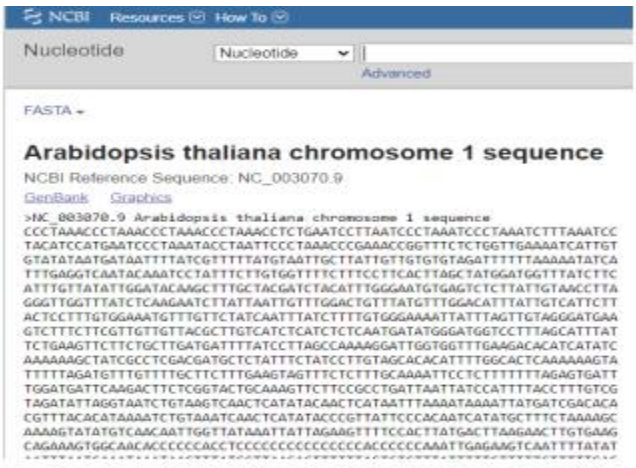


Figure 4.2. Fragment du fichier de séquence d'ADN au format FASTA.

4.2.1.2. Codage et décodage de l'ADN pour l'image :

Une séquence d'ADN contient quatre bases d'acide nucléines A (adénine), C (cytosine), G (guanine) et T (thymine), où A et T sont complémentaires, G et C sont complémentaires. Parce que 0 et 1 sont complémentaires dans le binaire, donc 00 et 11 sont complémentaires et 01 et 10 sont également complémentaires. Nous adoptons le codage suivant dans notre approche

Codage binaire ADN	
A	0 1
T	1 0
C	1 1
G	0 0

Tableau 4.1 Codage ADN

4.2.1.3. Les opérations algébriques pour les séquences d'ADN :

Nous avons défini, les opération XOR, SUB et ADD pour la séquence d'ADN Nous avons utilisé les opérations XOR, SUB et ADD pour fusionner l'image (après qu'on la deviser en système RGB ensuite le shuffling du RGB avec les paramètres de Lorenz et au finale le codage ADN de ce dernier) avec la position de la clé. Par exemple, il existe deux séquences d'ADN [CTAT] et [GCTA], nous adoptons les types des opérations XOR, SUB et ADD qui est montré dans les tableaux 2, 3 et 4 respectivement pour les XOR, SUB et ADD et nous obtenons les séquences [TGTT], [GTAG] et [TGTT] respectivement comme résultat.

XOR	***A***	***G***	***C***	***T***
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Tableau 4.2 : l'opération XOR pour la séquence d'ADN.

SUB	***A***	***G***	***C***	***T***
A	C	T	G	A
G	T	C	A	G
C	A	G	C	T
T	G	A	T	C

Tableau 4.3 : l'opération SUB pour la séquence d'ADN.

ADD	***A***	***G***	***C***	***T***
A	C	G	A	T
G	A	C	T	G
C	G	T	C	A
T	T	A	G	C

Tableau 4.4 : l'opération ADD pour la séquence d'ADN.

4.2.2. Système chaotique 3D :

Dans ce travail, nous avons utilisé le système de Lorentz, qui est décrit par l'équation différentielle suivante :

$$\begin{cases} \frac{dx}{dt} = \sigma\,(y(t) - x(t)) \\ \frac{dy}{dt} = \rho\; x(t) - y(t) - x(t)z(t) \\ \frac{dz}{dt} = x(t)y(t) - \beta\; z(t) \end{cases}$$

Les nombres réels a, r, b sont appelés paramètres de contrôle, tandis que x, y, z sont appelés variables d'état, pour des paramètres de contrôle et des valeurs initiales x0, y0, z0 des variables d'état donnés. Le principe de du système de Lorenz est décrit dans la section 3.7.1.

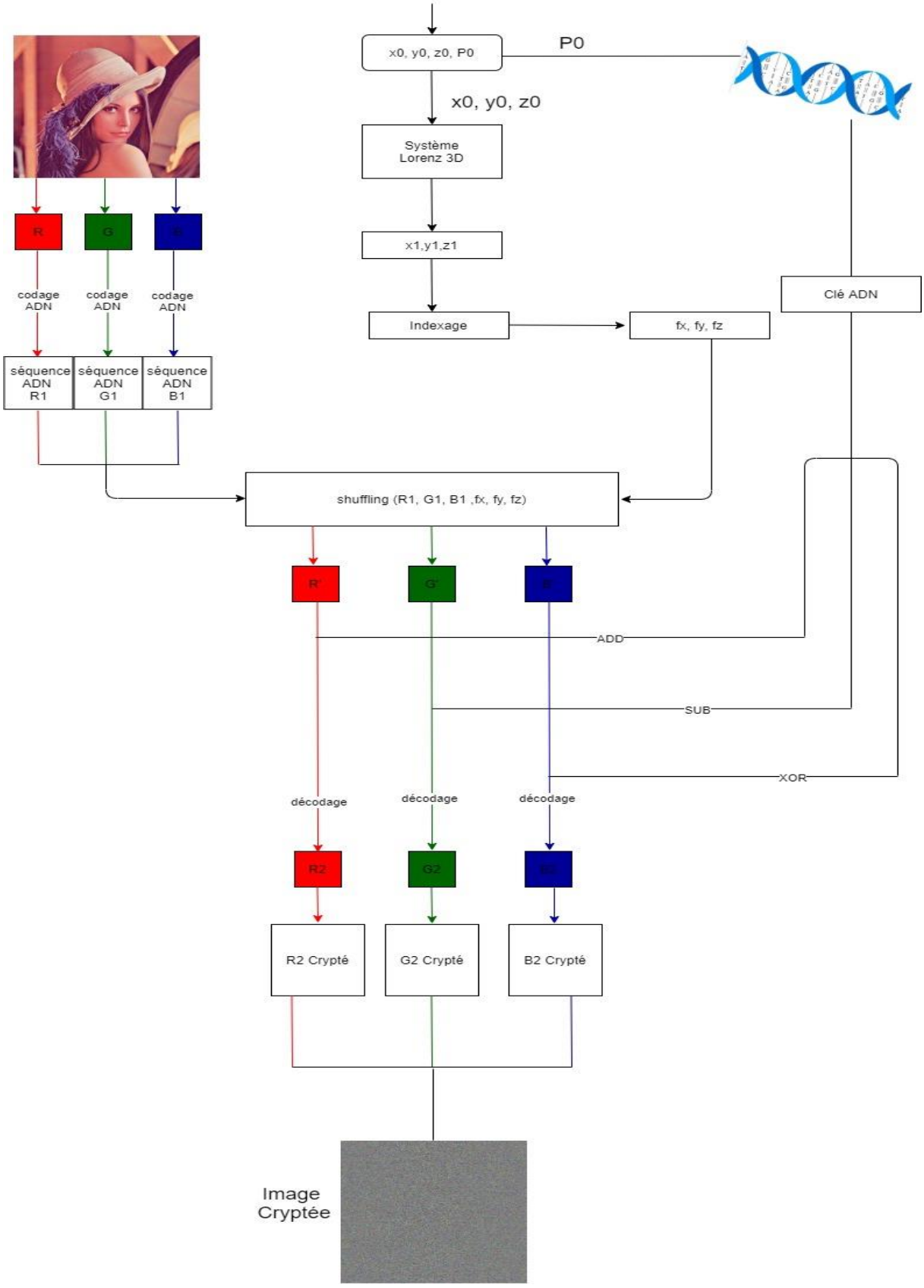


Figure 4.3. Organigramme de l'algorithme de cryptage.

4.3. Description de l'algorithme :

Génération de la clé ADN :

A partir d'une séquence ADN qui est dans notre cas un chromosome humain, nous générons une clé ADN à partir d'une position de départ P_0 de taille M*N*4 ou M, N sont les dimensions de l'image claire.

4.4. Cryptage d'image :

La figure 3 représente notre algorithme de cryptage, Nous détaillons dans la suite les différentes phases de l'algorithme :

Etape 1 : L'image en couleur P(m,n) est lue, tel que m et n sont les dimensions de l'image de largeur et de hauteur, respectivement.

Etape 2 : L'introduction de la clé qui est composée des paramètres de Lorenz K [x0, y0, z0] et une position de départ P_0 de la clé ADN

Etape 3 : Diviser l'image RGB en composants R, G, B et transformer les matrices décomposées de R, G, B en matrices binaires R (m, n × 8), G (m, n × 8) et B (m, n × 8),

Etape 4 : coder respectivement conformément à la règle de codage de l'ADN du tableau 1 et obtenir trois matrices de séquences d'ADN R1(m, n × 4), R1(m, n × 4) et B1(m, n × 4).

Etape 5 : Utilisez les conditions initiales x0, y0, z0 pour itérer le système chaotique, notre algorithme adopte le système chaotique 3D de Lorenz.

Etape 6 : Transformez K en séquence binaire Kb puis générez la matrice Mk (m, n × 8) en répétant Kb, t fois, où $t = \frac{m*n*8}{512}$ Encodez Mk avec la même règle d'encodage et obtenez Mke.

Etape 7 : La partie confusion de notre algorithme est le shuffling, nous utilisons la séquence chaotique indexée pour brouiller les positions des pixels des trois vecteurs d'ADN.

Etape 8 : Nous appliquons les opérations ADN (add, sub, xor comme indiqué dans les tableaux 2, 3, 4 respectivement) entre la clé Mke et les vecteurs R, G, B obtenus par le shuffling en ADN.

Etape 9 : Les vecteurs obtenus après les opérations ADN sont décodés en binaire (4.1). La restauration des pixels donne notre image cryptée.

4.5. Décryptage d'image :

L'algorithme de décryptage de l'image c'est le processus inverse de l'algorithme de cryptage utilise la même clé que l'algorithme de cryptage.

4.6. Expérimentation et résultats :

Présentation de l'environnement :

4.6.1. La machine :

Nous avons travaillé avec une machine dont : le processeur est Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.40 GHz, la mémoire RAM est 8,00 Go, le type de système d'exploitation 64 bits, processeur x64 et l'édition de Windows installé est Windows 10 Professionnel.

4.6.2. Langage de programmation :

Python : est un langage de programmation interprété, multi-paradigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions.

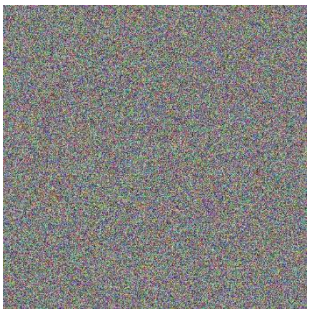
4.7. Résultat de simulation et analyse de sécurité :

Dans ce travail, nous avons utilisé trois images simples, Lena (512 × 512), image médicale (1153 × 1152) et image classée (872 × 871).

Nous avons utilisé Python 3.9 pour simuler les opérations de chiffrement et de déchiffrement et nous avons aussi fixé ces paramètres : X0= 6.377, Y0= 10.286, Z0= 25.746, P0= 20, $Ruledec$ = 4, $Ruledec$ = 5. Les images originales, les images cryptées et les images décryptées sont illustrées dans la figure.4. Comme on peut le voir, il est évident qu'il n'y a aucune comparaison entre l'image originale et celle cryptée.

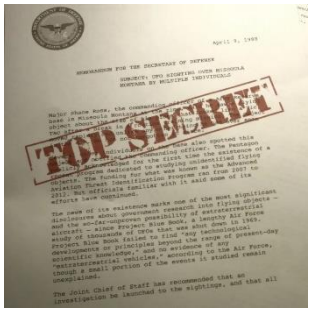
Cela montre que notre algorithme peut obtenir un bon effet de cryptage. Un bon algorithme de chiffrement doit résister à toutes sortes d'attaques connues telles que les attaques exhaustives, les attaques différentielles et les attaques statistiques. Fondamentalement, il doit être sensible aux clés secrètes et l'espace des clés doit être suffisamment grand pour résister aux attaques par force brute. Dans cette section, nous discuterons de l'analyse de sécurité sur le schéma de chiffrement proposé. Une étude comparative du NPCR, de l'UACI et de l'entropie de notre algorithme proposé à quelques algorithmes existants, basés sur des séquences d'ADN, est résumée dans le tableau 5. Ce tableau montre que nous avons obtenu des résultats très motivants par rapport à d'autres algorithmes.

(1) image originale de Lena

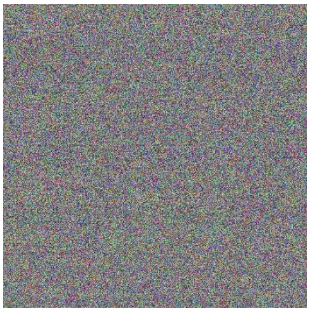


(2) son image cryptée

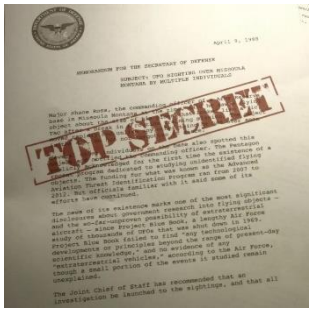
(3) image décryptée



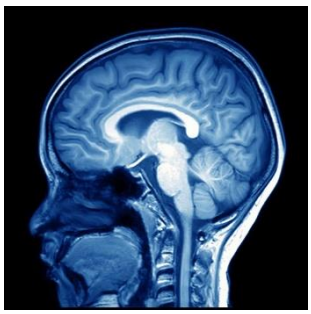
(4) image classée originale



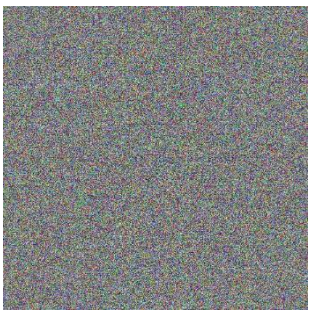
(5) son image cryptée



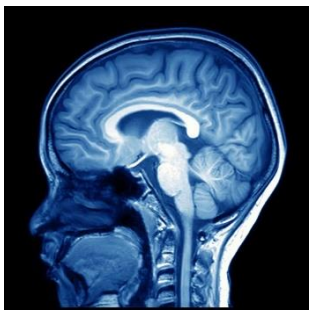
(6) image décryptée



(7) image medicale orignale



(8) son image cryptée



(9) image décryptée

Figure 4.4. Les images cryptées et décryptées

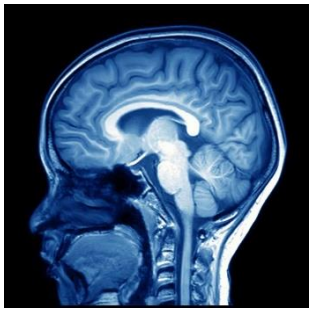
4.8. Analyse de sécurité :

4.8.1. L'espace de clé :

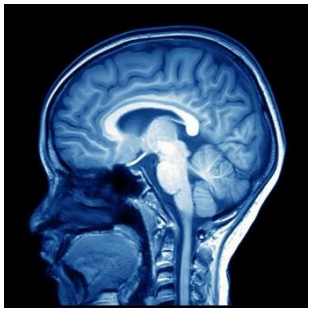
L'algorithme de cryptage d'image proposé utilise (x0, y0, z0, p0) comme clé secrète à quatre paramètres. Si la précision de 10^{-8} est choisie pour chaque paramètre (x0, y0, z0), la taille de l'espace de la clé secrète sera de $10^8 \times 10^8 \times 10^8 = 10^{36}$, en plus le paramètre p0 sert à extraire une clé ADN de longueur dépend de la taille de l'image à chiffrer. Le choix de p0 varie selon la longueur du chromosome utilisé (de 1 à 1000000 pour un chromosome de taille 1000000 bases).

4.8.2. La sensibilité de clé :

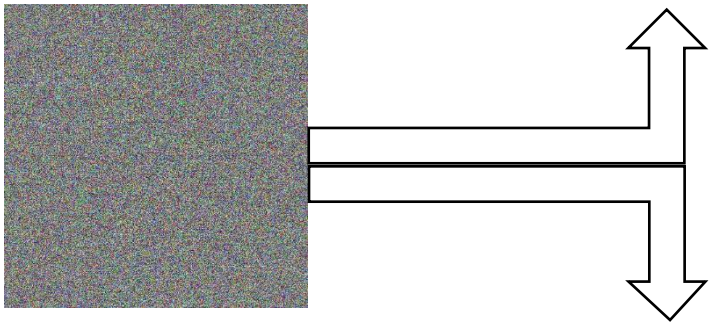
La sensibilité du système de Lorenz à la condition initiale (x0, y0, z0) est de 10^{-6}, en utilisant X0= 0.6377 pour le cryptage de l'image médicale, l'image cryptée illustrée à la Figure.5. (b) est obtenue. Si X0= 0.6377 est utilisé, l'image décryptée est montrée dans la figure (c). En utilisant X0= 0.637700000000001 l'image décryptée est montrée dans la figure (d).



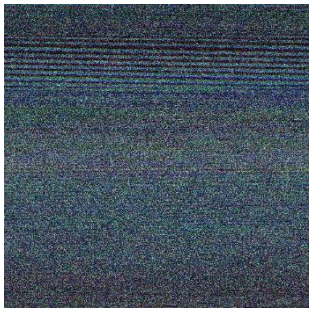
(c) image décryptée avec X0=0.6377



(a) Image originale



(b) image cryptée avec X0=0.6377



(d) image décryptée avec X0=0.637700000000001

Figure 4.5. Différence entre les deux images médicales décryptées avec changement en x0

4.9. L'entropie :

L'entropie d'une image est un indicateur de sa complexité. Si l'image est uniforme et ne possède qu'une couleur, son entropie est nulle. Plus l'entropie est élevée, plus l'image est "aléatoire".

L'entropie est définie comme suit :

$$E = -sum(p.* \log_2(p))$$

Le tableau 5 montre l'entropie d'information de l'image de chiffrement.

Images	Plain image	encrypted image
Lena	7.75019	7.9997
medical image	6.78917	7.9996
Classified image	7.51555	7.9999

Tableau 4.5. L'entropie d'information de l'image de chiffrement.

Nous remarquons que toutes les valeurs des images cryptées sont très proches de 8 (tableau 3), quelles que soient les valeurs des images simples, donc la probabilité de divulgation accidentelle d'informations est mineure et notre algorithme est suffisamment robuste.

4.10. Attaque statistique :

4.10.1 L'analyse des histogrammes :

Les histogrammes des images cryptées et décryptées sont présentés dans la figure.6.

Il ressort de la figure.6 que les histogrammes des images cryptées sont assez uniformes et significativement différents de ceux des images originales. De plus, les images décryptées à l'aide des clés secrètes correctes ne présentent aucune distorsion.

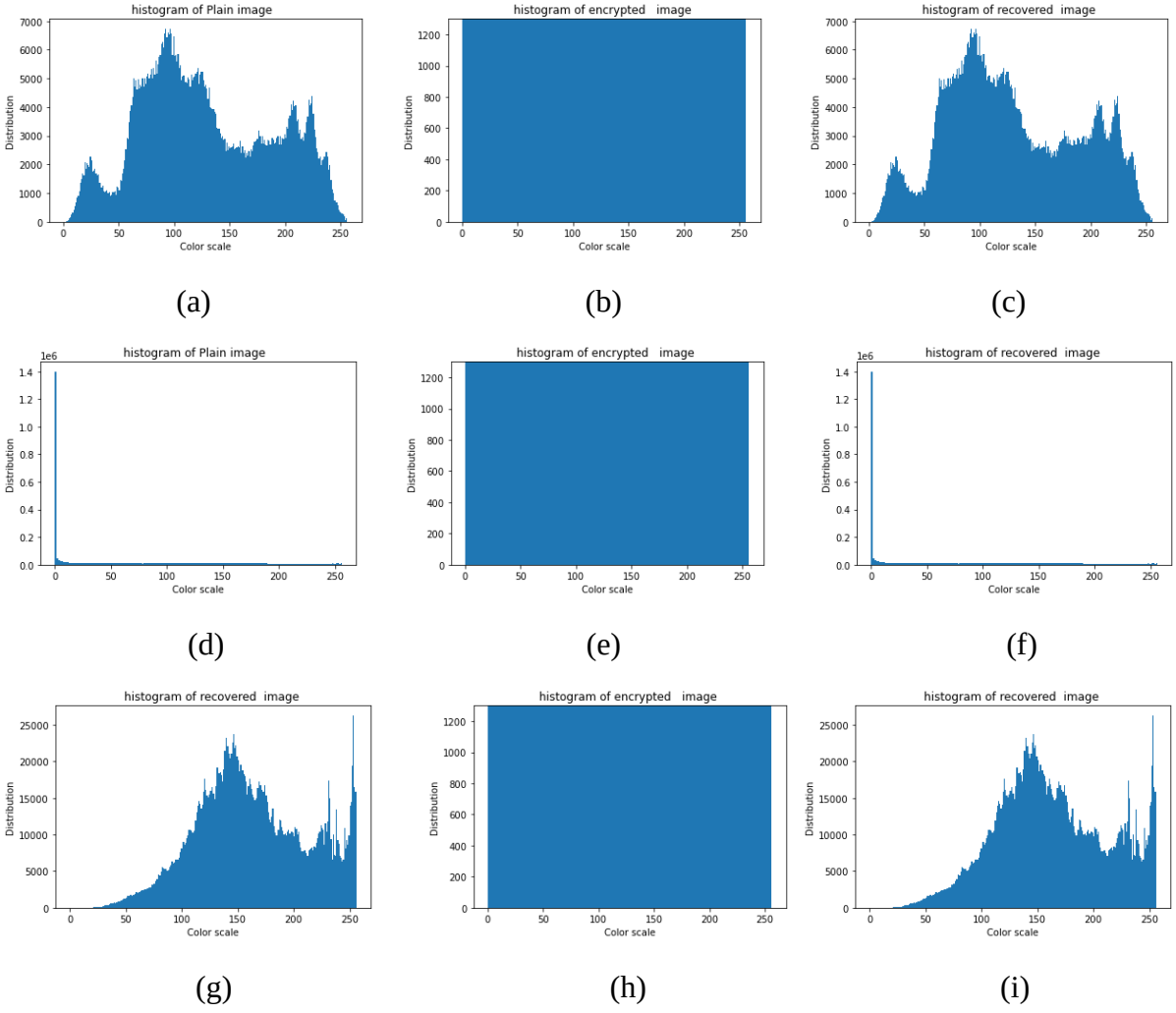


Figure 4.6. Les histogrammes

Figure.6 les histogrammes de : (a) l'image originale de Lena, (b) l'image cryptée de Lena, (c) l'image décryptée, (d) l'image classée originale, (e) l'image classée cryptée, (f) l'image décryptée, (g) l'image médicale originale, (h) l'image médicale cryptée, (i) l'image décryptée.

4.10.2. Analyse du coefficient de corrélation :

En plus de l'analyse des histogrammes, nous avons calculé les coefficients de corrélation existante entre différentes images sources et leurs images cryptées respectives, La corrélation entre les pixels adjacents dans l'image d'origine est incroyablement élevée. Un algorithme de chiffrement efficace permet de réduire la corrélation entre pixels adjacents, de manière à vérifier la corrélation de deux pixels adjacents, on sélectionne aléatoirement 3000 paires (horizontales, verticales et diagonales) de pixels adjacents de la première image et donc de l'image chiffrée. En utilisant les formules suivantes pour le coefficient de corrélation [30].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} X_i$$

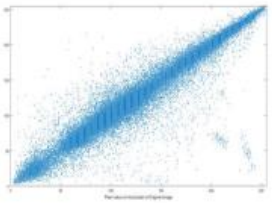
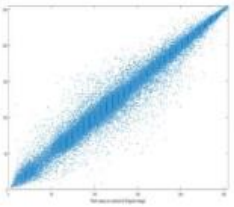
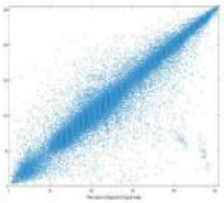
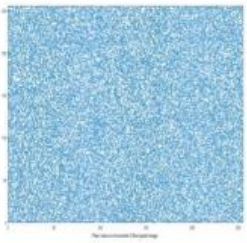
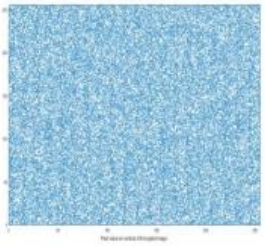
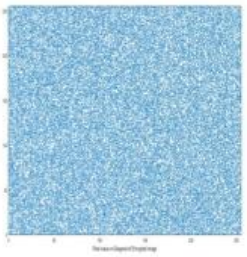
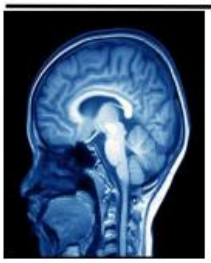
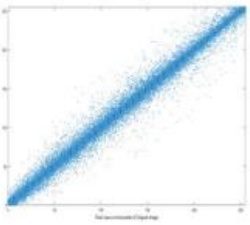
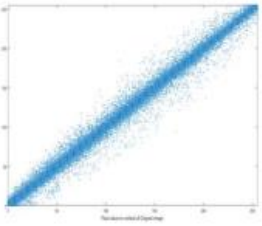
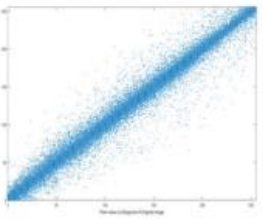
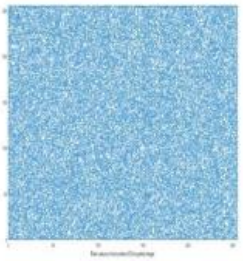
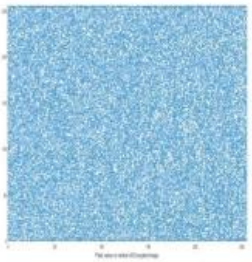
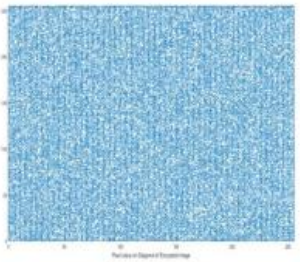
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

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

$$\Gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}$$

Où x et y sont les valeurs de couleur de deux pixels adjacents dans l'image, cov(x; y) est la covariance et D(x) est la variance, et E(x) est la moyenne. Le tableau 4 montre la corrélation de deux pixels horizontalement adjacents dans l'image originale "Lena" et son image cryptée, où les coefficients de corrélation sont respectivement de 0,9468 et 0,0036. Le tableau 4 montre que les corrélations des pixels adjacents dans l'image cryptée sont fortement réduites. De même, d'autres résultats sont présentés dans le tableau 5. D'après les résultats du tableau 5, nous découvrons que le coefficient de corrélation des pixels adjacents dans l'image cryptée est incroyablement petit, qui est proche de 0.

Le tableau suivant regroupe la corrélation de deux pixels adjacents des images étudiées :

Image	Horizontally	Vertically	Diagonally
			
			
			
			

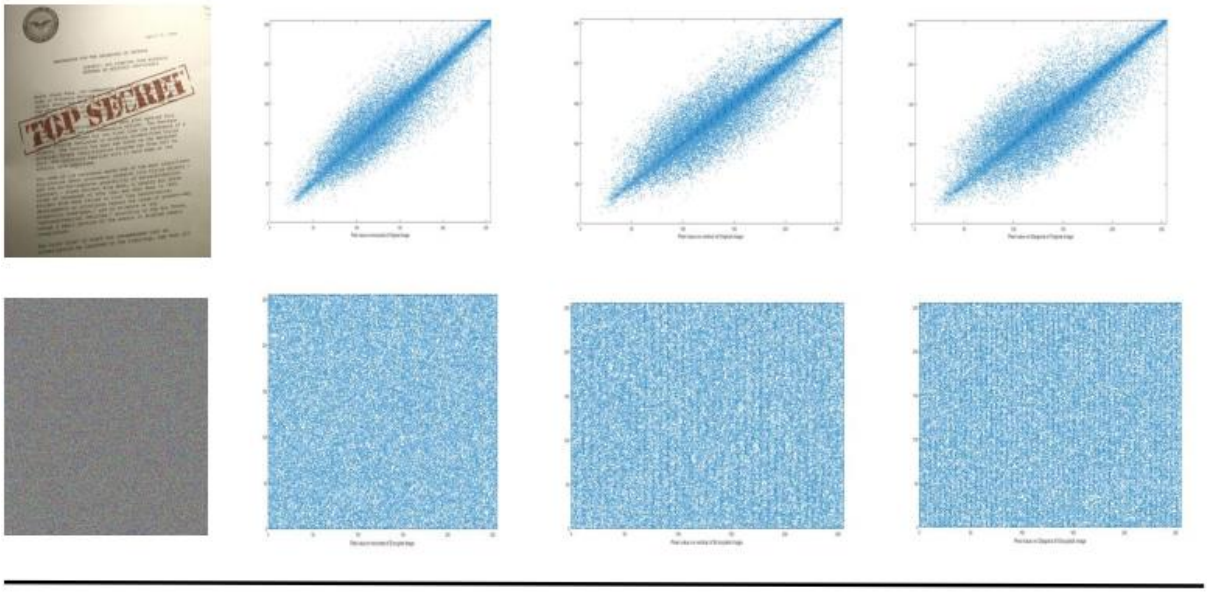


Tableau 6 : Coefficients de corrélation de deux pixels adjacents dans les trois images.

Correlation	Horizontal	Vertical	Diagonal
Lena image	0.9704	0.9881	0.9633
Encrypted Lena image	0.0016	-0.0015	-0.0084
Medical image	0.9978	0.9981	0.9957
Encrypted medical image	0.0027	-0.0081	0.0026
Classified image	0.9780	0.9718	0.9545
Encrypted classified	0.0027	0.0025	0.0036

Tableau 4.6. Coefficients de corrélation

4.11. Attaque différentielle :

En cryptographie, un pixel de l'image simple est comparé à un pixel des images cryptées afin d'extraire une relation utile, qui détermine en outre la clé. Ce type de recherche est nommée cryptanalyse par attaque différentielle [31]. Pour vérifier l'influence d'un changement d'un pixel sur l'ensemble de l'image cryptée par l'algorithme de cryptage d'image numérique proposé, deux mesures courantes ont été utilisées : NPCR et UACI. NPCR signifie le taux de changement du nombre de pixels de l'image cryptée, tandis qu'un pixel de l'image simple est modifié. L'UACI, qui est l'intensité changeante moyenne unifiée, mesure l'intensité moyenne des différences entre les images cryptées. Le NPCR et l'UACI sont calculés, respectivement, en utilisant les deux équations suivantes [32].

$$NPCR = \frac{1}{W \times H}\left[\sum_{i,j} i,j\right] \times 100\%,$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%.$$

Où W et H représentent la longueur et la largeur de l'image, et C1 et C2 sont deux images cryptées dont les images originales correspondantes n'ont qu'une différence d'un pixel et ont même une taille identique. C1(i,j) et C2(i,j) sont les valeurs d'échelle de couleur du pixel situé sur la grille (i,j). Le nombre D(i,j) est fixé par C1(i,j) et C2(i,j) comme suit : Si C1(i,j)= C2(i,j), alors D(i,j)= 0, sinon, D(i,j)=1. Les valeurs NPCR et UACI calculées des images de test sont répertoriées dans le tableau 6. Idéalement, l'UACI devrait être proche de 33,4 %, tandis que le NPCR devrait être proche de 99,6 %. L'expérience présentée dans le tableau 6 montre qu'une légère différence (même une différence d'un pixel) dans deux images simples se terminera par un grand changement dans les images cryptées, puis l'algorithme de cryptage d'image numérique proposé montre de bonnes performances qui peuvent éviter les attaques différentielles.

Tableau 7 : NPCR et UACI des images cryptées lors du changement d'un pixel

Test	UACI %	NPCR %
Lena image	33.451407937453496	99.60568745930989
medical image	33.45666968790152	99.6034507724305
classified image	33.44028642539908	99.6117243703852

Tableau 4.7. NPCR et UACI des images cryptées

Le tableau 6 montre qu'une légère différence (même une différence d'un pixel) dans deux images simples se terminera par un grand changement dans les images cryptées, puis l'algorithme de cryptage d'image numérique proposé montre de bonnes performances qui peuvent éviter les attaques différentielles.

4.12. Conclusion :

Dans ce chapitre, une présentation détaillée de l'approche est faite, des différentes expérimentations réalisées a été discutée. Plusieurs paramètres de performance comme les l'analyse des histogrammes, le coefficient de corrélation, l'espace de la clé, la sensibilité à la clé, l'entropie et les mesures de NPCR et UACI ont été utilisé Dans l'analyse des performances de notre algorithme qui a montré sa robustesse.

Conclusion générale :

Dans ce mémoire nous avons proposé une nouvelle technique de cryptage d'image afin de sécuriser leur transfert.

Nous avons commencé par une introduction générale qui donne une vue globale sur la sécurité, la cryptographie et l'objectif de notre travail.

Le 2ème chapitre, est un état de l'art autour de la cryptographie basée sur l'ADN , nous avons présenté des définitions des différentes notions sur l'ADN pour comprendre sa structure et ses avantages en cryptographie.

Dans le 3ème chapitre, les systèmes chaotiques sont décrits, ses principes et ses avantages. Nous avons présenté les différents systèmes chaotiques utilisé dans le cryptage.

Le 4ème chapitre fait l'objet de notre système proposé, un crypto-système basé sur ADN et un système chaotique 3D de Lorenz. D'après les expérimentations réalisées, les histogrammes, les coefficients de corrélations, la taille de la clé et sa sensibilité faite, nous avons constaté que notre algorithme peut résister à tous types d'attaques.

Nous envisageons d'améliorer notre algorithme pour minimiser ses couts afin de l'utiliser dans un environnement IoT.

Références :

[1] : Renaud Dumont, « introduction à la Cryptographie et à la Sécurité informatique », Université de Liège, Faculté des Sciences Appliquées, 2007

[2] : H.X.Mel, Doris Baker, la cryptographie décryptée Compus Press, 2001.

[3] : Url: http://dspace.univ-tlemcen.dz/bitstream/112/1076/5/chapitre1.pdf Consulté le 08/12/2021 à 15:40.

[4] : E. Williams, "Cryptography 101: Symmetric Encryption", Mar. 31, 2020. Accessed on: June 13, 2020. [Online], Available: https://medium.com/@emilywilliams_43022/ cryptography-101-symmetric-encryption-444aac6bb7a3.

[5] : C. Y. Chen, and H. C. Chao, “A Survey of Key Distribution in Wireless Sensor Networks”, Security and Communication Networks, Vol. 7, No. 12, pp. 2495-2508, 2014.

[6] : W. Stallings, “Cryptography and Network Security Principles and Practice”, 4 th ed., Prentice Hall, 2007.

[7] : Kaushik, Akhil , A novel DNA cryptographic approach ,phd thesis , 2021

[8] Tornea, O. (2013). Contributions to DNA cryptography: applications to text and image secure transmission (Doctoral dissertation, Université Nice Sophia Antipolis; Technical University of Cluj-Napoca (Romania)).

[9] Lee Carroll (2010) the Twelve layers of DNA, Traduit de l'américain par Louis Royer

[10] Florence Klotz, Lucia Le Clech et Diana Russo. réalisation : agence gimmick (novembre 2017) L’ADN, déchiffrer pour mieux comprendre le vivant.

[11] https://www.msdmanuals.com/fr/accueil/fondamentaux/g%C3%A9n%C3%A9tique/g%C3%A8nes-et-chromosomes

[12] https://lejournal.cnrs.fr/articles/stockage-de-donnees-les-promesses-de-ladn-synthetique

[Vineet Gupta (1997)] Vineet Gupta, Srinivasan Parthasarathy and Mohammed J. Zaki (1997), Arithmetic and Logic Operations with DNA, Proc. 3rd DIMACS Workshop on DNA-based Computers (Philadelphia, USA) ,212-20.

[W. Piotr (2000)] W. Piotr, J. M. Jan, R. R. Witold and L. Bogdan (2000), Adding numbers with DNA, International Conference on Systems, Man and Cybernetics, 265–270.

[P.M.J. Allen (1999)] P. M. J. Allen, Y. Bernard, M. P. Philip (1999), Article for analog vector algebra computation, Biosystems, 52, 175–180.
[W.C. Chen (2001)] W. C. Chen, Z. Y. Chen, Z. H. Chen. (2001), Operational rules of the digital coding of DNA sequences in high dimension space, ActaBiophysicaSinica, 17(3). 542–549.

[13] MajidBabaei (2013), A novel text and image encryption method based on chaos theory and DNA computing, international journal of Natural Computing, 12(1), 101-10.

[14] Ming, G, F,Zhu, L, T. (2015). « Chaos Theory in Cryptography ». Beijing Institute of Technology Press
[15] Wahl, C, D. (2019,07,08). A Brief History of Systems Science, Chaos and Complexity. Medium. https://medium.com/age-of-awareness/a-brief-history-of-systems-science-chaos-and-complexity-d9198b1a198d

[16] Wikipedia contributors. (2021, June 10). Chaos theory. In *Wikipedia, The Free Encyclopedia*. Retrieved 08:39, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=1027790119

[17] Gayathri, J., & Subashini, S. (2016). A survey on security and efficiency issues in chaotic image encryption. *International Journal of Information and Computer Security*, *8*(4), 347-381.

[18] Wikipedia contributors. (2021, May 22). Logistic map. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:03, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=Logistic_map&oldid=1024548294

[19] Wikipedia contributors. (2020, March 6). Tent map. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:15, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=Tent_map&oldid=944209609

[20] Wikipedia contributors. (2021, April 26). Hénon map. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:27, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=H%C3%A9non_map&oldid=1019938048

[21] Wikipedia contributors. (2017, July 15). Duffing map. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:33, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=Duffing_map&oldid=790702427

[22] Wikipedia contributors. (2021, May 29). Lorenz system. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:39, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=Lorenz_system&oldid=1025751485

[23] Wikipedia contributors. (2021, June 8). Rössler attractor. In *Wikipedia, The Free Encyclopedia*. Retrieved 09:44, June 18, 2021, from https://en.wikipedia.org/w/index.php?title=R%C3%B6ssler_attractor&oldid=1027472634

[24] Zhang, G., Zhang, F., Liao, X., Lin, D., & Zhou, P. (2017). On the dynamics of new 4D Lorenz-type chaos systems. *Advances in Difference Equations*, *2017*(1), 1-13.

[25] Anchal Jain and NavinRajpal (2012 b), A Two Layer Chaotic Network Based Image Encryption Technique, IEEE NCCCS, Durgapur, Print ISBN: 978-1-4673-1952-2

[26] Paul, S., Dasgupta, P., Naskar, P. K., & Chaudhuri, A. (2017). Secured image encryption scheme based on DNA encoding and chaotic map. International Information and Engineering Technology Association, 4, 70-75.

[27] Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dynamics, 83(3), 1123-1136.

[28] Arabidopsis thaliana.(2021,06,15). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Arabidopsis_thaliana&oldid=1026591731

[29] Watson, J. D., & Crick, F. H. (2010). 1953. A structure for deoxyribose nucleic acid (pp. 82-84). University of Chicago Press.

[30] Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, *52*(11-12), 2028-2035.

[31] Al-Hazaimeh, O. M., Al-Jamal, M. F., Alhindawi, N., & Omari, A. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing and Applications*, *31*(7), 2395-2405.

[32] Al-hazaimeh, O. M. (2014). A novel encryption scheme for digital image-based on one dimensional logistic map. *Computer and Information Science*, *7*(4), 65.