République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D' **I**NFORMATIQUE
DEPARTEMENT D'AUTOMATIQUE

Mémoire de Fin d'Etudes de MASTER PROFESSIONNEL

Domaine : **Sciences et Technologies**
Filière : **Automatique**
Spécialité : **Contrôle, Véhicule et Propulsion Électrique**

Présenté par
Tinhinane BOUSSOUEL

Thème

Conception d'un crypto-système d'images basé sur la carte chaotique de Tent

Mémoire soutenu publiquement le 30/06/2024 devant le jury composé de :

M Ahmed MAIDI
Professeur, Ummto, Président

M Sarah KASSIM
MCB, Ummto, Encadrant

M Ahcene HAMOUDI
MAB, Ummto, Examinateur

M Kahina LARBI
MA, Ummto, Examinateur

REMERCIEMENTS

Je tiens à remercier en premier lieu ma promotrice, Madame Sarah KASSIM, de m'avoir guidé et conseillé tout au long de l'élaboration de ce mémoire de fin d'études.

Je souhaite également remercier toute personne qui, de près ou de loin, a contribué à la réalisation de ce mémoire.

DÉDICACES

Je dédie ce mémoire en premier lieu à mes chers parents. Ce travail est le reflet de tout ce que vous m'avez appris et de tout ce que vous m'avez donné. Il est le fruit de votre soutien sans faille, de vos sacrifices constants et de votre amour inconditionnel.

Je dédie ce modeste travail à la mémoire de ma chère grand-mère maternelle, qui, sans aucun doute, en aurait été très fière. Je le dédie également à ma grand-mère paternelle, dont les conseils et l'encouragement inlassables m'ont toujours épaulé.

Ce mémoire est aussi dédié à ma sœur, mes frères et mes cousins, qui m'entourent de leur présence et de leur soutien quotidien. Merci d'être toujours là pour moi.

TABLE DES MATIÈRES

TABLE DES FIGURES

Symboles et Notation

$\mathbb{R}$: ensemble des nombres réels

K : clé dans le cas d'un algorithme à clé symétrique

K_e et K_d : clés de chiffrement/déchiffrement dans le cas d'un algorithme asymétrique

$E(.)$: fonction de chiffrement

$D(.)$: fonction de déchiffrement

t : variable de temps réel

$x(t)$: vecteur d'état du modèle d'espace d'état en temps continu

k : variable de temps discret

$x(k)$: vecteur d'état du modèle d'espace d'état en temps discret

$\oplus$: XOR (Exclusive OR)

RSA : Rivest-Shamir-Adleman

AES : Advanced Encryption Standard

DES : Data Encryption Standard

SSL : Secure Sockets Layer

TLS : Transport Layer Security

ECC : Elliptic Curve Cryptography

PRNGs : Pseudo-Random Number Generators

RGB : Red Green Blue, un modèle de couleur

JPEG : Joint Photographic Experts Group, un format de fichier image

PNG : Portable Network Graphics, un format de fichier image

BMP : Bitmap, un format de fichier image

TIFF : Tagged Image File Format, un format de fichier image

EPS : Encapsulated PostScript, un format de fichier image

AI : Adobe Illustrator, un format de fichier image

INTRODUCTION GÉNÉRALE

L'étude des systèmes chaotiques, caractérisés par leur sensibilité aux conditions initiales et leur comportement imprévisible mais déterministe, a fasciné les mathématiciens et les physiciens depuis plusieurs décennies [1]. Ces systèmes, dont les trajectoires dans l'espace des phases exhibent une complexité dynamique [2], ont trouvé des applications diverses dans des domaines aussi variés que la météorologie, la biologie et la cryptographie [1].

L'émergence de la cryptographie chaotique représente une convergence intéressante entre ces deux domaines [3]. Cette approche novatrice utilise les propriétés imprévisibles et aléatoires du chaos pour renforcer les protocoles de sécurité [4]. Contrairement aux méthodes traditionnelles qui s'appuient sur des clés statiques, la cryptographie chaotique génère des clés dynamiques à partir de signaux chaotiques, offrant ainsi une résistance accrue contre les attaques cryptanalytiques et une meilleure adaptabilité aux environnements dynamiques et non stationnaires [3][4].

Dans ce contexte, les systèmes chaotiques offrent un potentiel prometteur pour la génération de séquences chaotiques, essentiels pour l'établissement sécurisé de clés de chiffrement [5]. Les dynamiques complexes du chaos permettent également de brouiller efficacement les données sensibles, rendant leur interception et leur déchiffrement considérablement plus difficiles [5][4]. Cette approche non conventionnelle a suscité un intérêt croissant dans la recherche en sécurité informatique, explorant comment exploiter les propriétés uniques du chaos pour répondre aux défis de la sécurité dans un monde numérique de plus en plus interconnecté et exposé aux menaces [6].

Ainsi, ce mémoire se propose d'explorer en profondeur les fondements théoriques des systèmes chaotiques, les principes fondamentaux de la cryptographie traditionnelle et les applications spécifiques de la cryptographie chaotique. En examinant ces domaines interdisciplinaires, il vise à fournir un aperçu détaillé des possibilités offertes par l'utilisation du chaos pour sécuriser les communications et protéger les informations sensibles dans l'ère numérique actuelle.
Ce mémoire se concentre sur la conception d'un crypto-système basé sur la carte chaotique de Tent (Tent map), explorant ses applications potentielles dans le domaine de la sécurité des données.
Nous avons conçu ce système qui exploite les propriétés chaotiques de la carte de Tent pour générer des clés de chiffrement uniques et imprévisibles. Les résultats obtenus démontrent l'efficacité et la robustesse de cette approche chaotique.

Le mémoire est structuré en trois chapitres :

• Le premier chapitre aborde les systèmes chaotiques, en mettant l'accent sur leurs propriétés dynamiques et leur sensibilité aux conditions initiales.

• Le deuxième chapitre examine les principes et les applications de la cryptographie chaotique, étudiant comment les dynamiques chaotiques peuvent être utilisées pour générer des clés sécurisées et brouiller efficacement les données sensibles.

• Le troisième chapitre présente la conception détaillée de notre crypto-système, décrivant son fonctionnement, sa robustesse et sa capacité à répondre aux exigences de sécurité modernes.

CHAPITRE 1

SYSTÈMES CHAOTIQUES

1.1 Introduction

Le chaos, souvent perçu comme une absence d'ordre et de structure, intrigue par sa complexité sous-jacente et ses phénomènes mystérieux [1]. Le but de ce premier chapitre est d'introduire de nombreuses notions et techniques de base de la théorie des systèmes chaotiques dans un cadre aussi simple que possible. Nous allons examiner leur principes fondamentaux en passant bien évidemment par leur mise en équations. Pour une meilleure illustration, Nous allons accompagner ces explications d'une série d'exemples.

1.2 Historique

L'étude des systèmes chaotiques remonte à plusieurs siècles, mais ce n'est que récemment, au cours du XXe siècle, qu'elle a connu un essor significatif. Les premières observations et formulations des concepts liés au chaos remontent aux travaux pionniers de scientifiques tels que Henri Poincaré à la fin du XIXe siècle.

Poincaré fut parmi les premiers à découvrir des exemples de comportements dynamiques non périodiques dans les équations différentielles, jetant ainsi les bases de ce qui allait devenir la théorie du chaos. Cependant, le terme "chaos" lui-même n'a été popularisé qu'au cours des dernières décennies, notamment grâce aux travaux de mathématiciens et de physiciens comme Edward Lorenz, Robert May et Mitchell Feigenbaum [7].

L'une des contributions les plus significatives à la compréhension des systèmes chaotiques est venue des travaux de Lorenz dans les années 1960. En étudiant les équations simplifiées du mouvement atmosphérique, Lorenz a découvert que de petites variations dans les conditions initiales pouvaient entraîner des résultats considérablement différents, un phénomène désormais connu sous le nom de "sensibilité aux conditions initiales" ou "effet papillon" [8].
Depuis lors, les systèmes chaotiques ont été étudiés dans de nombreux domaines scientifiques, y compris la physique, les mathématiques, la biologie, l'économie et même la cryptographie. Leur compréhension a conduit à des avancées significatives dans des domaines tels que la théorie du chaos déterministe, la modélisation du climat, la dynamique des populations et bien d'autres encore [9].

1.3 Systèmes dynamiques

Les systèmes dynamiques, qu'ils soient linéaires ou non linéaires, sont des systèmes physiques dont l'état change au fil du temps en fonction de leur propriétés fondamentales. Modélisés par des équations différentielles, leur analyse permet de saisir le comportement des systèmes complexes au fil du temps à travers des modèles dynamiques. Ces systèmes peuvent être représentés mathématiquement en temps continu et en temps discret [10].

1.3.1 En temps continu

Dans le cas où la composante temps est continue, la dynamique du système est décrite mathématiquement par une équation différentielle ordinaire et un ensemble de conditions initiales : [11]

$$\begin{cases} \dot{x}(t) = f(x(t)) \\ x(t_0) = x_0 \end{cases} \tag{1.1}$$

$x \in \mathbb{R}^n$ est le vecteur d'état.
f est une fonction $\mathbb{R}^n \to \mathbb{R}^n$ appelée champ de vecteur.
Si la fonction f est linéaire, le système dynamique est dit linéaire. Dans le cas inverse, le système est dit non linéaire. Si le temps est exprimé explicitement dans la fonction f, le système est dit

"non autonome".

$x_0 \in \mathbb{R}^n$ représente le vecteur des états initiaux à l'instant initial t_0.

1.3.2 En temps discret

Si un système prends ses valeurs uniquement à des instant régulièrement distribués, celui-ci est dit système discret. Il est présenté par une équation aux différences (fonction itérative), comme suit : [11]

$$\begin{cases} x_{k+1} = f(x_k) \\ x(k_0) = x_0 \end{cases} \tag{1.2}$$

avec k est l'instant discret, k_0 est l'instant discret initial, et x(0) est le vecteur des états initiaux.

1.3.3 Notions sur les systèmes dynamiques

Pour appréhender les subtilités des systèmes dynamiques, il est essentiel de mettre le point sur certaines notions les caractérisant : [12]

- **Système autonome :** système dont les équations n'ont pas de dépendance explicite par rapport au temps.
- **Causalité :** Un système est dit causal lorsque sa sortie ne dépend que de ses entrées actuelles et passées, et non des entrées futures.
- **Trajectoire de phase :** Une trajectoire de phase est la représentation de l'évolution d'un système dynamique dans un espace de phase, où chaque axe correspond à une variable d'état du système.
- **Espace de phase :** Un espace multidimensionnel dans lequel chaque dimension représente une variable d'état du système.
- **Portrait de phase :** Le portrait de phase est l'ensemble des trajectoires de phase possibles d'un système dynamique.
- **Point d'équilibre(ou point fixe) :** on appelle point d'équilibre d'un système le point x^* pour lequelle on obtient $f(x^*) = 0$, état où le système reste inchangé dans le temps. (En discret, $f(x^*) = x^*$)

— **Cycle limite :** Un cycle limite est une trajectoire fermée ou quasi-périodique dans l'espace de phase.

— **Attracteur :** Un ensemble vers lequel les trajectoires d'un système dynamique convergent à long terme.

1.3.4 Systèmes linéaires

Les systèmes linéaires constituent une branche fondamentale des mathématiques appliquées et sont omniprésents dans de nombreux domaines, de l'ingénierie à l'économie en passant par la physique. Un système linéaire est essentiellement un ensemble d'équations linéaires impliquant plusieurs inconnues, et la solution de ce système consiste à trouver les valeurs des inconnues qui satisfont simultanément toutes les équations. Pour un système linéaire invariant dans le temps, la représentation d'état est donnée par : [13]

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1.3}$$

$$y(t) = Cx(t) + Du(t)$$

où :

— $x(t)$ est le vecteur d'état.

— $u(t)$ est le vecteur d'entrée.

— $y(t)$ est le vecteur de sortie.

— A est la matrice d'état (n x n).

— B est la matrice d'entrée (n x m).

— C est la matrice de sortie (p x n).

— D est la matrice de transfert direct (p x m).

— n : La dimension du vecteur d'état $x(t)$, c'est-à-dire le nombre de variables d'état du système.

— m : La dimension du vecteur d'entrée $u(t)$, c'est-à-dire le nombre de signaux d'entrée du système. .

— p : La dimension du vecteur de sortie $y(t)$, c'est-à-dire le nombre de signaux de sortie du système.

1.3.5 Systèmes non linéaires

Les systèmes non linéaires sont des systèmes dans lesquels la relation entre les entrées et les sorties n'est pas proportionnelle, c'est-à-dire que leur comportement ne peut pas être décrit par des équations linéaires simples. Ces systèmes peuvent exhiber des phénomènes tels que la bifurcation, le chaos, et d'autres dynamiques complexes, qui ne sont pas présents dans les systèmes linéaires [14].
Dans tout ce qui suivra, nous allons plus particulièrement nous intéresser aux systèmes dynamiques non linéaire étant donné que la non linéarité est l'une des caractéristiques principales des systèmes chaotiques [11].

1.4 Chaos

Pendant longtemps, les systèmes chaotiques ont été considérés comme étant incontrôlables et inutilisables en raison de l'incapacité à prédire leur comportement à long terme. Cependant, au cours des 30 dernières années, des chercheurs ont réussi à modéliser certains phénomènes chaotiques et ont remarqué l'existence d'un aspect déterministe dans ce qui semblait initialement aléatoire.
Le chaos est l'une des dynamiques les plus complexes que peuvent exhiber les systèmes dynamiques non linéaires. Le comportement chaotique a été observé dans plusieurs systèmes non linéaires évoluant aussi bien en temps continu comme les systèmes de Lorenz, Rossler et Chen qu'en temps discret comme les systèmes de Hénon et de Lozi [15].

1.4.1 Systèmes chaotiques

Le monde qui nous entoure semble souvent imprévisible, désordonné, aléatoire et chaotique. Un système chaotique, qu'il soit simple ou complexe, est caractérisé par sa sensibilité aux conditions initiales et un comportement marqué par une forte récurrence (tendance à revenir à des motifs ou comportements similaires malgré le chaos apparent) [10]. La coexistence de ces deux propriétés engendre un comportement extrêmement désordonné, communément qualifié de "chaotique". Une légère perturbation peut déclencher une instabilité ou un déséquilibre massif à long terme, difficile à prédire. Ainsi, des dispositifs simples peuvent générer des

phénomènes complexes. Un système chaotique se distingue d'un système parfaitement régulier par son caractère imprévisible et non linéaire [13]. Afin de mieux comprendre le comportement de ces systèmes, nous allons énumérer certaines de leurs caractéristiques les plus importantes.

1.4.2 Caractéristiques qualitatives des systèmes chaotiques

1.4.2.1 Non linéarité

Un système non linéaire est généralement insoluble. Toute tentative de le décomposer révèle une complexité interne croissante. La non-linéarité est l'une des caractéristiques fondamentales des systèmes chaotiques. En effet, tout système linéaire ne peut pas être chaotique [15].

1.4.2.2 Non périodicité

Un système exhibant un comportement chaotique évolue le long d'une trajectoire qui ne se répète jamais. En d'autres termes, ses trajectoires ne sont jamais périodiques [12].

1.4.2.3 Déterminisme et imprévisibilité

Le déterminisme implique que le système est dépourvu d'aléa et ne comporte aucun paramètre ou entrée de nature stochastique. Chaque condition initiale détermine entièrement l'évolution future du système, car il est dépourvu de hasard, ce qui le rend déterministe. Cependant, même de légères variations entre deux conditions initiales très proches peuvent engendrer des évolutions totalement différentes. Ainsi, l'évolution du système devient imprévisible, car une petite erreur de mesure ou un arrondi à la 15ème décimale peuvent conduire à des résultats complètement divergents après un certain temps. Ceci est ce que l'on appelle le chaos déterministe [8].
Edward Lorenz, météorologue, fut l'un des premiers à réaliser l'existence du chaos déterministe. En météorologie, cela signifie qu'il est toujours impossible de prédire avec certitude le temps qu'il fera le mois prochain.

1.4.2.4 Sensibilité aux conditions initiales

Edward Lorenz, mathématicien et météorologue américain, s'intéressait particulièrement à la météorologie et aux mouvements turbulents des fluides comme l'atmosphère. En modélisant le mouvement des masses d'air à l'aide de relations simplifiées de thermodynamique et de mécanique des fluides, il réalisait des simulations numériques sur ordinateur, ce qui demandait beaucoup de temps à l'époque [13]. Un jour, par souci de commodité, il a décidé de réutiliser les valeurs précédemment calculées comme conditions initiales, mais en les tronquant pour n'utiliser que trois chiffres significatifs au lieu de cinq. Cela a conduit à une découverte surprenante : de légères variations dans les conditions initiales pouvaient entraîner des résultats radicalement différents. Ce phénomène est maintenant connu sous le nom de chaos déterministe [16]. Cette anecdote illustre comment une infime variation des conditions initiales d'un système peut totalement changer son évolution.
Les exemples abondent, notamment celui de " l'effet papillon ".
Cette sensibilité peut être quantifiée à l'aide de l'exposant de Lyapunov, qui caractérise le taux de divergence ou de convergence des trajectoires proches dans l'espace des phases [7].

1.4.2.5 Aspect aléatoire

Un aspect crucial des systèmes chaotiques est leur nature intrinsèquement aléatoire, qui défie souvent toute tentative de prédiction précise à long terme. Bien que les systèmes chaotiques soient déterministes, leur comportement global peut paraître aléatoire en raison de leur sensibilité extrême aux conditions initiales [11].
Cet aspect est une conséquence directe de leur sensibilité aux conditions initiales.

1.4.2.6 Attracteurs étranges

Pour appréhender le comportement à long terme d'un système chaotique, il est essentiel de préciser en quoi consiste un attracteur étrange, une notion qui englobe des ensembles plus vastes que les simples points fixes ou les orbites périodiques. Les attracteurs étranges représentent une facette captivante des systèmes chaotiques, caractérisés par des motifs complexes et irréguliers qui défient souvent une description conventionnelle. Ces structures, découvertes pour la première fois dans les travaux de David Ruelle et Floris Takens, transcendent les attracteurs simples tels que les points fixes ou les orbites périodiques, et témoignent de la richesse

de comportements possibles dans ces systèmes [11]. Les attracteurs étranges peuvent présenter une fractalité remarquable, se manifestant par des motifs répétitifs à différentes échelles, et leur exploration a ouvert de nouvelles perspectives sur la nature complexe et imprévisible des phénomènes chaotiques [3].

L'émergence d'un attracteur étrange découle de l'interaction de deux processus fondamentaux : d'une part, l'étirement, qui engendre l'instabilité et la sensibilité aux conditions initiales, et d'autre part, le repliement, qui confère à l'attracteur son aspect étrange et fractal.

La principale caractéristique de l'attracteur étrange est son bassin d'attraction [12]. Le bassin d'attraction décrit l'ensemble des conditions initiales qui conduisent à un comportement spécifique de l'attracteur. Ce concept, introduit pour la première fois par Henri Poincaré au début du 20e siècle, est essentiel pour évaluer la stabilité et la convergence des trajectoires dans un système. En examinant le bassin d'attraction, les chercheurs peuvent cartographier les différentes régions de l'espace des phases et déterminer les zones où les trajectoires convergent vers un attracteur donné. Cette approche permet non seulement de comprendre comment les perturbations initiales influencent le comportement global du système, mais aussi d'identifier les conditions qui favorisent la stabilisation de l'attracteur [12].

1.4.2.7 Section de Poincaré

Parmi les méthodes puissantes utilisées dans l'étude des systèmes chaotiques, la section de Poincaré est l'une des plus connues. Les sections de Poincaré sont des sous-espaces qui sont traversés par le système de manière récurrente et transverse afin d'analyser la dynamique du système en réduisant sa dimensionnalité. Cette technique consiste à examiner l'intersection des trajectoires du système avec un plan ou une surface particulière dans l'espace des phases, appelée la section de Poincaré. En d'autres termes, au lieu de suivre l'évolution du système dans tout l'espace des phases, on se concentre uniquement sur les points où la trajectoire traverse cette section [15].

Cette technique révèle souvent des motifs intéressants tels que des orbites périodiques, des points fixes et des bifurcations, qui sont cruciaux pour comprendre la nature du chaos. En observant la distribution des points sur la section de Poincaré et en étudiant comment ces points évoluent au fil du temps, on peut identifier des régularités, des transitions de phase et

des phénomènes chaotiques émergents [8].
Le choix du plan de la section de Poincaré est crucial pour garantir des intersections régulières avec la trajectoire, assurant ainsi une traversée alternée dans les deux sens [17].

- Si le régime est périodique, la section de Poincaré est représentée par un point unique, indiquant un attracteur sous forme de cycle limite.
- Si le régime est bi-périodique, la section de Poincaré prend la forme d'une courbe fermée, reflétant la présence d'un attracteur en forme de tore.
- En cas de régime chaotique, la section de Poincaré se présente comme un nuage de points, décrivant une structure complexe mais distincte.

Cet outil est essentiel pour explorer la complexité des systèmes chaotiques en permettant une visualisation simplifiée de leur comportement dynamique, facilitant ainsi l'analyse et la compréhension des phénomènes chaotiques.

1.4.3 Caractéristiques quantitatives des systèmes chaotiques

1.4.3.1 Exposant de Lyapunov

L'exposant de Lyapunov d'un système, noté λ_i (où i correspond au nombre de dimensions du système), représente une mesure quantitative de la sensibilité aux conditions initiales.
Il évalue le taux moyen de séparation entre deux trajectoires initialement proches dans un système donné [18]. Dans les systèmes instables, ces trajectoires divergent exponentiellement, ce qui signifie qu'une différence initiale entre elles croît au fil du temps selon une loi exponentielle. L'exposant de Lyapunov λ_i mesure cette croissance exponentielle. Chaque exposant de Lyapunov correspond à une dimension du système et indique la force de contraction ou d'étirement dans cette dimension.
Les conditions requises pour l'émergence du chaos dans un système dynamique sont les suivantes : [16]

- Présence d'au moins un exposant de Lyapunov positif, démontrant la divergence des trajectoires.

— Présence d'au moins un exposant de Lyapunov négatif, démontrant le repliement des trajectoires.

— Somme de tous les exposants étant négative, indiquant que le système chaotique est dissipatif, c'est-à-dire qu'il perd en énergie :

$$\sum_{i=1}^{n} \lambda_i < 0 \tag{1.4}$$

où n désigne la dimension du système.

Le signe du plus grand exposant fournit des informations sur l'attracteur du système, comme illustré dans le tableau (1.1).

Attracteur	Exposants de Lyapunov
Point d'équilibre	$0 \succ \lambda_1 \succeq ... \succeq \lambda_n$
Cycle limite	$\lambda_1 = 0,\ 0 \succ \lambda_2 \succeq ... \succeq \lambda_n$
Tore d'ordre 2	$\lambda_1 = \lambda_2 = 0,\ 0 \succ \lambda_3 \succeq ... \succeq \lambda_n$
Tore d'ordre k	$\lambda_1 = ... = \lambda_k = 0,\ 0 \succ \lambda_{k+1} \succeq ... \succeq \lambda_n$
Attracteur chaotique	$\lambda_1 \succ 0,\ \sum_{i=1}^{n} \lambda_i < 0$
Attracteur hyper-chaotique	$\lambda_1 \succ 0,\ \lambda_2 \succ 0,\ \sum_{i=1}^{n} \lambda_i < 0$

TABLE 1.1 – Exposants de Lyapunov pour différents attracteurs

1.4.3.2 Spectre de puissance

Le spectre de puissance, résultant de la transformée de Fourier d'un signal, est largement utilisé pour décrire différents régimes dynamiques. Dans un système présentant du chaos, ce spectre aura une caractéristique principale sous forme d'une bande large, signifiant une distribution étendue de puissance sur un large spectre de fréquences, avec éventuellement quelques composantes périodiques discernables (raies) qui se superposent à cette bande large [14]. Le calcul du spectre de puissance d'un signal sert à extraire ses composantes fréquentielles, en utilisant la transformée de Fourier :

$$X_e(f) = \int_{-\infty}^{\infty} x(t) e^{-2j\pi ft} dt$$

$x(t)$ est le signal d'entrée qu'on souhaites analyser,

$X_e(f)$ est sa transformée de Fourier, représentant ses composantes fréquentielles en fonction de la fréquence f. L'analyse du spectre de puissance d'un signal chaotique implique de calculer la transformée de Fourier de l'évolution temporelle d'une des variables du système. Contrairement à un signal périodique ou quasi-périodique, dont le spectre de Fourier se compose de raies distinctes correspondant aux périodes et harmoniques du système, un signal chaotique produit un spectre continu. Cette caractéristique présente un avantage significatif en cryptographie.

1.4.3.3 Bifurcations et routes vers le chaos

Un système dynamique ne peut passer directement d'un état non chaotique à un état chaotique sans traverser des transitions, car la génération d'un signal chaotique n'est pas instantanée. Cette modification dans les dynamiques du système est connue sous le nom de bifurcation [16] . Les bifurcations sont des transitions qualitatives dans le comportement dynamique des systèmes chaotique. Leur étude approfondie offre un aperçu fascinant de la complexité du chaos déterministe [19]. Les représentations graphiques qui mettent en évidence ces transitions dans le comportement dynamique sont désignées sous le nom de diagrammes de bifurcation.
Le diagramme de bifurcation offre une vue d'ensemble des solutions possibles d'un système, ainsi que leur stabilité, en fonction des variations d'un de ses paramètres. Il permet également de repérer les valeurs spécifiques du paramètre qui conduisent à des bifurcations. Ce diagramme divise les intervalles où les solutions asymptotiques évoluent de manière continue avec le paramètre, classant les valeurs du paramètre sur l'axe des abscisses et les valeurs d'une des variables d'état sur l'axe des ordonnées [13].
Basculer d'un attracteur stable à un attracteur chaotique nécessite le passage par une trajectoire bien spécifique : une suite de bifurcations appelée routes vers le chaos. Il existe une diversité de routes vers le chaos, parmi lesquelles trois scénarios se distinguent fréquemment et sont donc reconnus comme universels :

1.4.3.3.1 L'intermittence

Dans cette séquence, une seule bifurcation gouverne l'oscillation entre des zones de mouvement chaotique et des zones de mouvement régulier. À mesure que le paramètre de bifurcation évolue, cette transition devient plus marquée : les périodes de comportement chaotique

s'étendent progressivement, tandis que les phases de mouvement régulier se réduisent [11]. À un point critique, généralement défini par un seuil dans la valeur du paramètre de bifurcation, le système bascule définitivement vers un état de chaos persistant, où le mouvement irrégulier domine de façon continue.

1.4.3.3.2 La quasi-périodicité

La quasi-périodicité fait référence à un comportement dynamique où un système oscille selon deux (ou plus) fréquences incommensurables, c'est-à-dire que le rapport de ces fréquences est irrationnel. Ce phénomène se produit souvent lors de certaines bifurcations, telles que la bifurcation de Hopf. Au lieu de se fixer à une orbite périodique simple, le système évolue sur un tore de dimension supérieure dans l'espace des phases [20]. Visuellement, cela se manifeste par des trajectoires qui ne se répètent jamais exactement mais remplissent de manière dense une surface toroïdale. La quasi-périodicité est un comportement intermédiaire entre la périodicité régulière et le chaos complet. Dans un diagramme de bifurcation, ce type de comportement est souvent indiqué par des régions de complexité intermédiaire avant l'apparition du chaos [8].

1.4.3.3.3 Doublement de périodes

Le doublement de période, également connu sous le nom de bifurcation de dédoublement de période, se produit lorsque, à mesure qu'un paramètre du système est varié, une orbite périodique stable se déstabilise et donne naissance à une nouvelle orbite dont la période est le double de la période initiale. Ce processus peut se répéter, entraînant des orbites avec des périodes quadruples, octuples, etc [19].

Dans un diagramme de bifurcation, ces événements apparaissent comme une succession de points où la période des orbites double, souvent formant une structure en arbre connue sous le nom de cascade de dédoublement de période. Ce comportement est l'un des signes avant-coureurs typiques de la transition vers le chaos. Au fur et à mesure que les dédoublements de période continuent, ils se produisent à des intervalles de plus en plus rapprochés jusqu'à ce que le système atteigne une dynamique chaotique [21].

1.4.4 Exemples de systèmes chaotiques

1.4.4.1 Exemple de systèmes chaotiques en temps continu

Dans cette partie dédiée aux systèmes en temps continu, le système que nous allons étudier est celui de Lorenz.

Introduit pour la première fois par le mathématicien et météorologue Edward Lorenz [7] en 1963 comme modèle simplifié de la convection atmosphérique, Le système de Lorenz est un ensemble d'équations différentielles non linéaires qui décrivent le comportement d'un système dynamique tridimensionnel. Son évolution temporelle fait apparaitre un comportement chaotique.

Le modèle est décrit comme suit :

$$\begin{cases} \dot{x} &= \sigma(y - x) \\ \dot{y} &= x(\rho - z) - y \\ \dot{z} &= xy - \beta z \end{cases} \tag{1.5}$$

où x, y et z représentent les variables d'état du système et σ, ρ, et β sont des paramètres constants positifs. Ces équations décrivent l'évolution temporelle des variables x, y et z, qui représentent respectivement le taux de convection, la différence de température horizontale et la différence de température verticale. Dans tout ce qui suit, les paramètres sont fixés aux valeurs : $\sigma = 10$, $\beta = 28$, $\rho = 8/3$.

1.4.4.1.1 Sensibilité aux conditions initiales

Cette figure illustre comment une légère modification dans les conditions initiales peut entraîner un chevauchement dans le comportement du système.

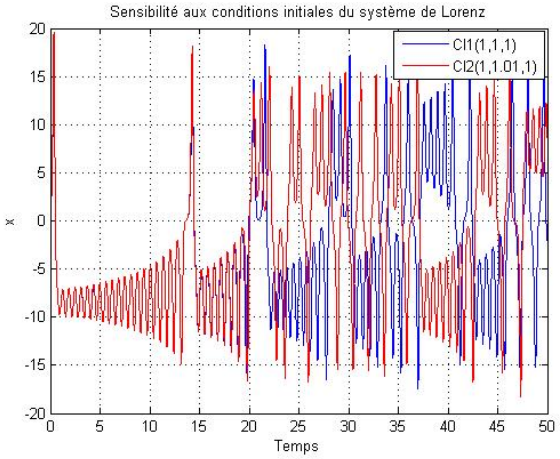

FIGURE 1-1 – Sensibilité aux conditions initiales de l'état x du système de Lorenz

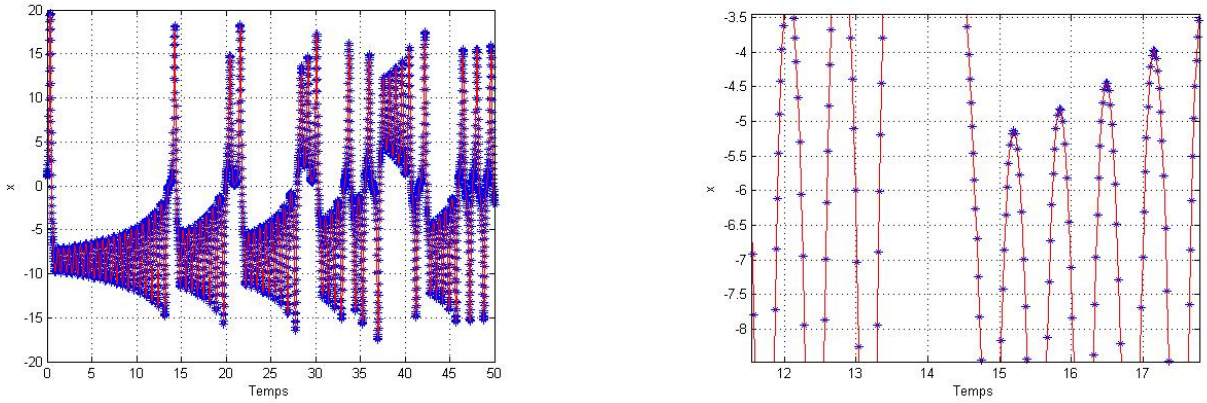

FIGURE 1-2 – Sensibilité de l'état x à deux conditions initiales identiques

1.4.4.1.2 Aspect aléatoire

La figure (1-3) met en évidence l'aspect intrinsèquement aléatoire du système de Lorenz. Elle illustre la nature imprévisible du système. (Conditions initiales fixées à $[x(0),y(0),z(0)]$=[1,1,1])

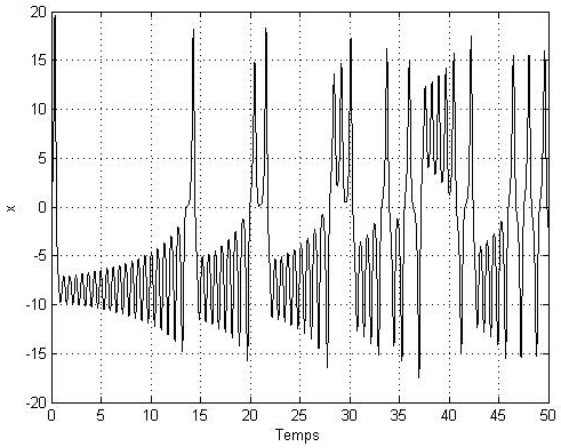

FIGURE 1-3 – Aspect aléatoire de l'état x du système de Lorenz

1.4.4.1.3 Attracteur étrange

L'attracteur étrange de Lorenz, également connu sous le nom d'attracteur de Lorenz, incarne l'une des manifestations les plus saisissantes du phénomène chaotique, révélant un motif géométrique complexe et infiniment répété qui défie toute prédiction déterministe.
Il est tracé à la figure (1-4) pour des conditions initiales $[x,y,z]$ =[1,1,1] . On remarque que l'attracteur chaotique de Lorenz illustre une trajectoire complexe et non périodique, où les orbites

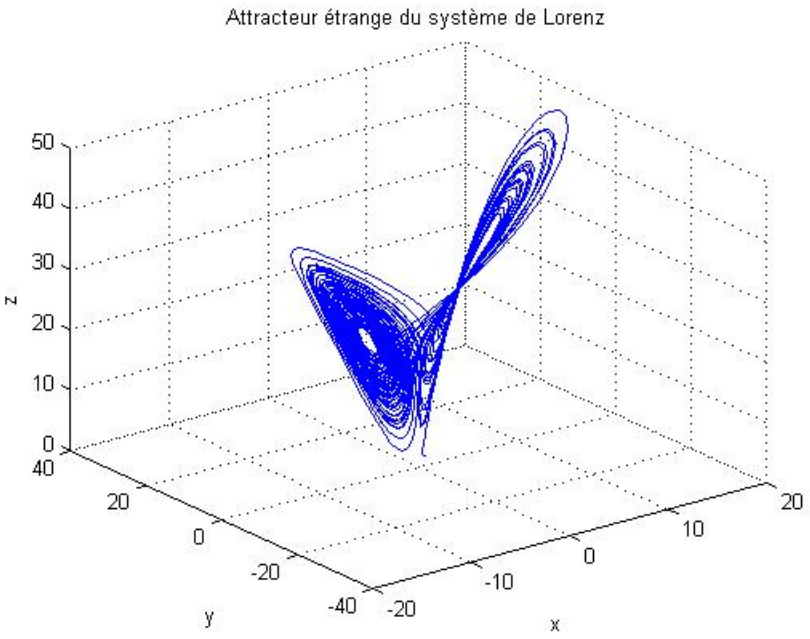

FIGURE 1-4 – Attracteur chaotique de Lorenz

ne se croisent jamais, mais restent confinées dans une structure en forme de spirale double, reflétant la sensibilité extrême aux conditions initiales typique des systèmes chaotiques.

1.4.4.1.4 Exposants de Lyapunov

Avec x(0) = 0.1, y(0) = 0.1, z(0) = 0.1 comme conditions initiales, on obtient la figure (1-5).

Les trois exposants de Lyapunov obtenus sont les suivants : L1 = 0.91448, L2 = -0.00147 et L3 = -14.58.

La somme de L1,L2 et L3 est infèrieure à 0, L1 est supérieur à 0 et il y a présence d'au moins

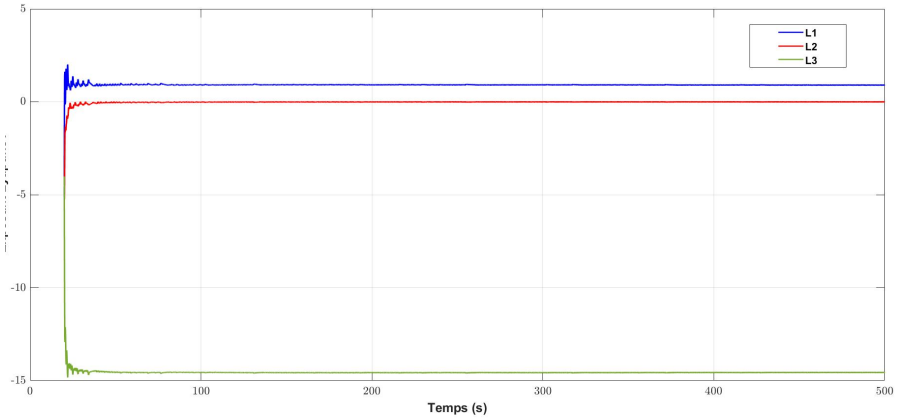

FIGURE 1-5 – Exposants de Lyapunov du système de Lorenz

un exposant négatif (L2 et L3). On en conclu que les conditions requises pour l'émergence du chaos (1.4.3.1) sont vérifiées.

1.4.4.1.5 Bifurcations

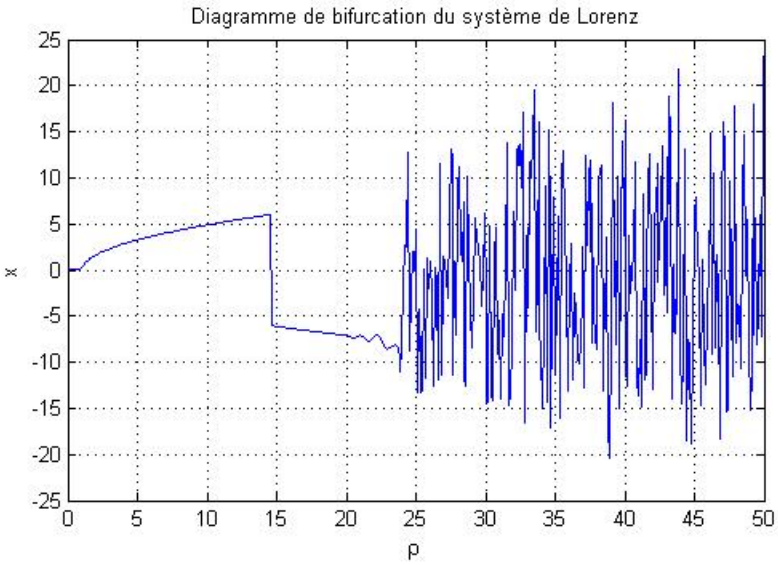

FIGURE 1-6 – Diagramme de bifurcation du système de Lorenz

La figure (1-6) illustre le diagramme de bifurcations de Lorenz. Au fur et à mesure que le paramètre de contrôle ρ augmente, le système passe d'un comportement stable à des oscillations puis rentre dans un régime chaotique à $\rho = 25$.

1.4.4.2 Exemple de systèmes chaotiques en temps discret

Le système qu'on va étudier dans cette section est celui de Hénon.
Le système de Hénon est un exemple classique de système dynamique chaotique à deux dimensions introduit par le physicien Michel Hénon en 1976. Ce système est décrit par un ensemble d'équations itératives simples :

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases}$$

où (x_n, y_n) représentent les coordonnées d'un point dans l'espace, a et b sont des paramètres constants contrôlant le comportement du système, et n est un entier représentant le temps discret. Dans tout ce qui suit, a=1.4 et b=0.3.

1.4.4.2.1 Sensibilité aux conditions initiales

La figure (1-7) illustre la sensibilité aux conditions initiales du système de Hénon.

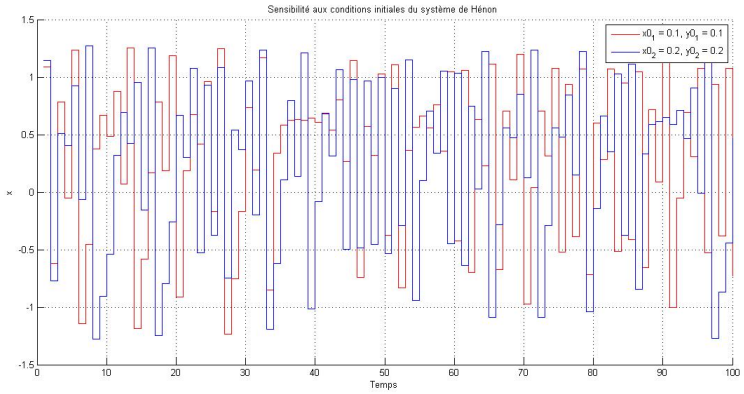

FIGURE 1-7 – Sensibilité aux conditions initiales du système de Hénon

1.4.4.2.2 Aspect aléatoire

La figure (1-8) montre l'aspect aléatoire du système de Hénon. Elle est tracée pour des conditions initiales x_0=0.1 et y_0=0.1.

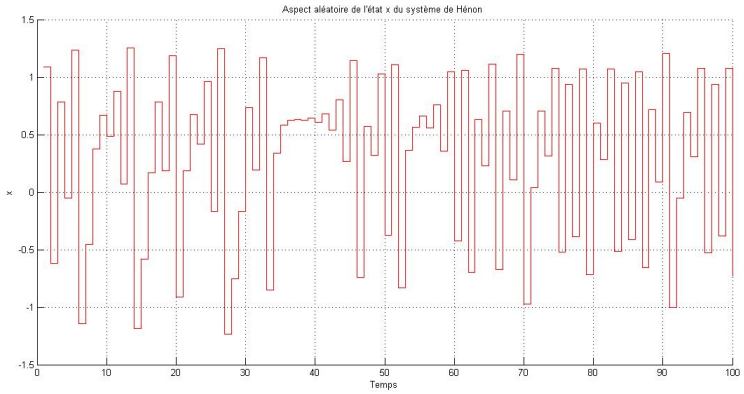

FIGURE 1-8 – Aspect aléatoire de l'état x du système de Hénon

1.4.4.2.3 Attracteur étrange

La figure (1-9) est obtenue pour $[x_0,y_0] = [0.1,0.1]$.

On remarque que l'attracteur étrange de Hénon forme une structure complexe et fractale en deux dimensions, où les trajectoires du système s'enroulent et se replient de manière répétée, illustrant un comportement chaotique confinée dans un espace limité.

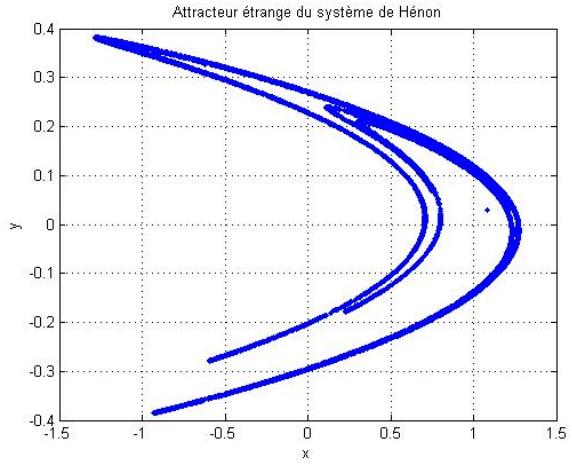

FIGURE 1-9 – Attracteur étrange du système de Hénon

1.4.4.2.4 Exposants de Lyapunov

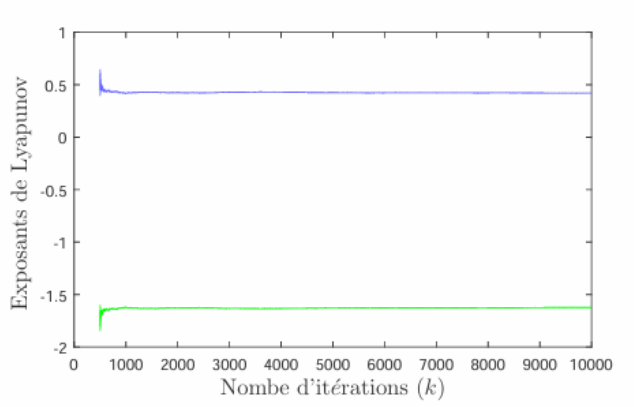

FIGURE 1-10 – Exposants de Lyapunov du système de Hénon

1.4.4.2.5 Spectre de puissance

On observe à travers la figure (1-11) le spectre de puissance des deux états du système de Hénon. Le spectre a une répartition large et continue des fréquences, indiquant une dy-

namique chaotique avec une absence de périodicité dominante et la présence de composantes harmoniques complexes, caractéristiques d'un comportement irrégulier et imprévisible.

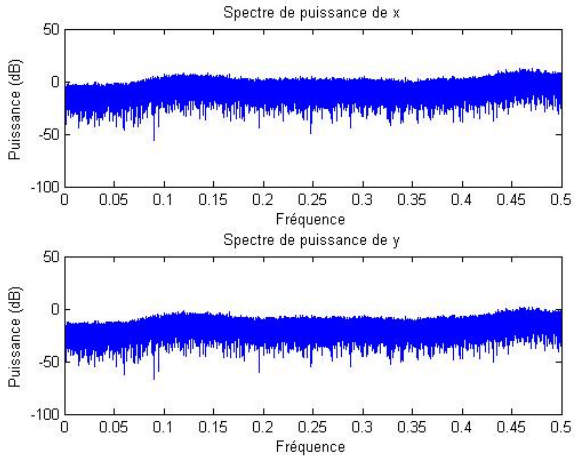

FIGURE 1-11 – Spectre de puissance du système de Hénon

1.4.4.2.6 Bifurcations

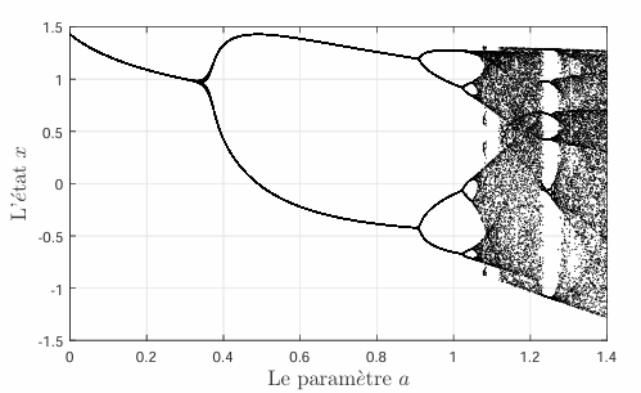

FIGURE 1-12 – Diagramme de bifurcation du système de Hénon

Dans la figure (1-12), le système passe d'un comportement stable à des oscillations périodiques, puis à des bifurcations successives qui mènent à un régime chaotique, caractérisé par des branches fractales et une grande sensibilité aux conditions initiales.

1.4.5 Conclusion

En résumé, l'étude des systèmes chaotiques révèle un monde où des comportements imprévisibles surgissent de règles simples, dévoilant ainsi une complexité fascinante. Dans ce chapitre, nous avons exploré différents aspects de ces systèmes, mettant en évidence leur sensibilité aux conditions initiales, leur comportement non linéaire et leurs attracteurs étranges.

Nous avons observé comment même des modèles élémentaires, tels que le système de Lorenz ou le système de Hénon, peuvent manifester des dynamiques chaotiques, soulignant ainsi leur pertinence dans des domaines scientifiques variés.

Une conclusion fondamentale de notre étude est l'incertitude inhérente à la prédiction à long terme dans les systèmes chaotiques. Malgré nos efforts pour modéliser et simuler ces systèmes avec une précision remarquable, de légères variations dans les conditions initiales peuvent entraîner des résultats radicalement différents, limitant ainsi notre capacité à anticiper l'avenir avec certitude. Cependant, plutôt que de voir cette incertitude comme une entrave, nous devrions la considérer comme une caractéristique inhérente à la complexité de notre environnement. En outre, l'étude des systèmes chaotiques offre des perspectives intrigantes pour la cryptographie, où la complexité inhérente et l'imprévisibilité des systèmes chaotiques peuvent être exploitées pour renforcer la sécurité des communications et des systèmes cryptographiques. C'est ce que nous allons explorer dans le chapitre suivant.

CHAPITRE 2

CRYPTOGRAPHIE CHAOTIQUE

2.1 Introduction

À mesure que le monde se tourne de plus en plus vers le numérique, à l'ère du télé travail et de l'évolution constante des technologies disponibles, la sécurité informatique devient une priorité majeure pour les grandes organisations [22]. Dans cette ère de transformation technologique constante, où nos échanges sont de plus en plus fréquents, rapides et efficaces, la protection des informations confidentielles devient une priorité absolue. C'est dans ce contexte que la cryptologie tient son fondement.

La cryptologie repose sur deux piliers fondamentaux. D'un côté, la cryptographie, de l'autre, la cryptanalyse [23] . Les systèmes chaotiques offrent un potentiel prometteur pour le développement de techniques de chiffrement sécurisées et efficaces en raison de leurs propriétés uniques que nous avons cité en détails dans le précèdent chapitre. La cryptographie basée sur les systèmes chaotiques exploite le comportement imprévisible et aléatoire des systèmes dynamiques chaotiques pour générer des clés de chiffrement et des séquences de chiffres robustes, offrant ainsi une sécurité renforcée contre les attaques cryptanalytiques traditionnelles [23]. Ces systèmes offrent une alternative prometteuse aux méthodes conventionnelles en cryptographie en exploitant la complexité dynamique du chaos pour sécuriser les communications et les données sensibles.

Ce chapitre propose une exploration complète de la cryptographie, couvrant les bases théoriques, les algorithmes de chiffrement et d'autres aspects essentiels pour une compréhension

approfondie. Nous mettons en lumière la cryptographie chaotique, soulignant ses principes et ses applications.

2.2 Historique sur la cryptographie

L'histoire de la cryptographie est une saga captivante qui remonte à l'aube de la civilisation. On pourrait être tenté de croire que la cryptographie n'a gagné en pertinence qu'avec l'avènement de l'informatique et des communications modernes [24]. Cependant, des exemples de documents chiffrés remontent à l'Antiquité, notamment au XVIe siècle av. J.-C, où un potier irakien aurait gravé sa recette secrète sur un pot en supprimant les consonnes et en inversant les lettres pour la dissimuler [25]. Tout au long de l'histoire, diverses méthodes de cryptologie et de stéganographie (l'art de cacher des communications) ont été utilisées. Certaines étaient fascinantes, comme celle du roi de Babylone, Nabuchodonosor, qui écrivait sur le crâne de ses esclaves avant de laisser leurs cheveux repousser pour dissimuler les messages, tandis que d'autres étaient plus simples et utilisaient des techniques comme le chiffrement de César, probablement l'un des algorithmes de chiffrement les plus célèbres, et ce, pendant des millénaires [26].

Dans l'Antiquité, les premières formes de cryptographie étaient rudimentaires mais néanmoins efficaces. Les Égyptiens utilisaient des hiéroglyphes complexes pour dissimuler des messages dans les tombeaux des pharaons, tandis que les Spartiates utilisaient le scytale, un dispositif cylindrique, pour transmettre des messages secrets [27]. Cependant, ce n'est qu'avec l'Empire romain que la cryptographie a commencé à être formalisée. Jules César, par exemple, a utilisé un système de substitution alphabétique, aujourd'hui connu sous le nom de "chiffre de César", pour sécuriser ses communications militaires. Cette technique de chiffrement repose sur le remplacement des lettres des messages par d'autres lettres situées à une distance fixe dans l'alphabet. Cette distance, appelée clé de chiffrement, détermine le décalage utilisé [28]. Par exemple, avec une clé de chiffrement de 3, un tableau de chiffrement serait constitué comme suit :

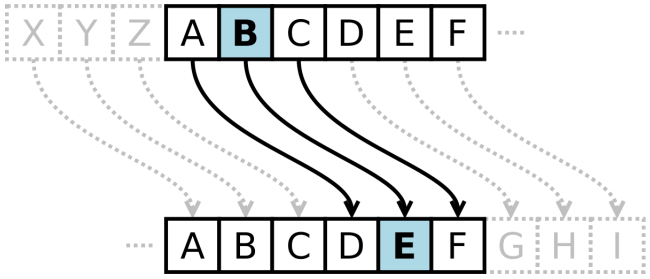

FIGURE 2-1 – Décalage de césar.

Au Moyen Âge, la cryptographie est devenue plus sophistiquée avec l'émergence de techniques telles que la substitution polyalphabétique, qui a été perfectionnée par des cryptographes comme Al-Kindi, un érudit arabe du IXe siècle. La Renaissance a vu l'émergence de cryptographes célèbres comme Blaise de Vigenère, dont le chiffre de Vigenère a été une avancée majeure dans la cryptographie [28]. La révolution de la cryptographie est survenue pendant la

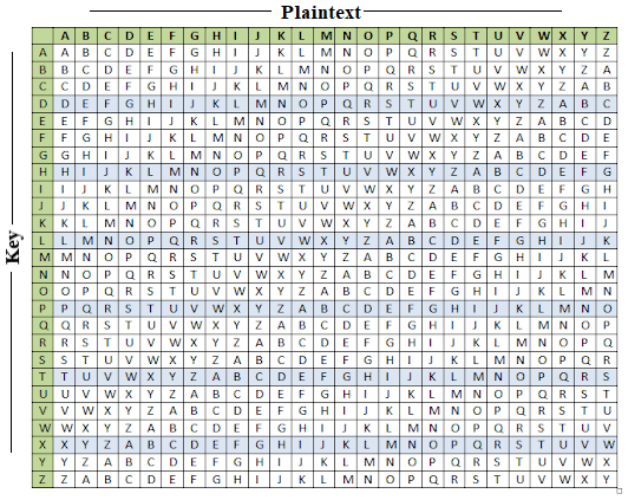

FIGURE 2-2 – Tableau de Vigenère.

Seconde Guerre mondiale avec l'invention de la machine de chiffrement Enigma par les Allemands. Tout comme le chiffrement de Vigenère, Enigma utilise un chiffrement par substitution polyalphabétique. Cependant, Enigma fait appel à une machine électromécanique. Cette machine dans sa version standard est constituée d'un clavier afin de taper le message à chiffrer, du dispositif de cryptage et du tableau lumineux qui affiche la lettre chiffrée. Ainsi, lors de la frappe sur le clavier, un courant électrique passe dans le système de chiffrement pour enfin allumer la lettre chiffrée sur le tableau lumineux [26].

Les efforts pour briser Enigma ont conduit au développement de l'un des premiers ordinateurs électroniques, le Colossus, par les Alliés. Cette époque a également vu l'utilisation généralisée

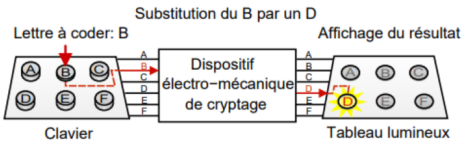

FIGURE 2-3 – Fonctionnement de la machine Enigma.

de méthodes de chiffrement modernes telles que le chiffrement par blocs et le chiffrement à clé publique [29].

Dans les années 1970, Whitfield Diffie, Martin Hellman et Ralph Merkle ont introduit la cryptographie à clé publique, une avancée révolutionnaire qui a permis un échange sécurisé de clés sur des réseaux non sécurisés. Depuis lors, avec l'avènement de l'informatique et d'Internet, la cryptographie est devenue omniprésente dans notre vie quotidienne. Des protocoles tels que SSL/TLS sont utilisés pour sécuriser les communications en ligne, tandis que des algorithmes comme le RSA et le DES sont couramment utilisés pour sécuriser les données sensibles [30].

Vers les années 1990, une méthode de chiffrement innovante émergeait, fondée sur le chaos. Dans cette approche, un système chaotique était utilisé pour produire des séquences de clés aléatoires. En effet, bien que déterministes, les systèmes chaotiques présentent des propriétés statistiques similaires à celles de l'aléatoire, donnant naissance à la cryptographie chaotique.

2.3 Cryptologie

La cryptologie, qui tire son nom des mots grecs pour "science" (logos) et "secret" (kryptos), est l'étude et la mise en pratique des techniques permettant des communications sécurisées, même en présence de tiers indésirables. En d'autres termes, elle assure la sécurité des messages confidentiels [31]. Cette science des secrets, est un domaine fascinant où se confrontent deux esprits vifs : le cryptographe et le cryptanalyste.

Le cryptographe imagine des codes et des procédés ingénieux pour protéger des messages confidentiels ou garantir l'authenticité d'une information. Il tisse des protections solides, comme des serrures complexes, pour que seuls les destinataires légitimes puissent accéder au contenu précieux.

Face à lui se dresse le cryptanalyste. Son objectif : percer les défenses du cryptographe et découvrir le sens caché des messages chiffrés. Il scrute chaque faille, chaque indice, cherchant

la clé qui ouvrira les portes du secret [32].

2.3.1 Cryptanalyse

La cryptanalyse consiste à déchiffrer des informations codées dont on ne dispose pas de la clé correspondante. Pour y parvenir, un arsenal de techniques redoutables, que l'on peut

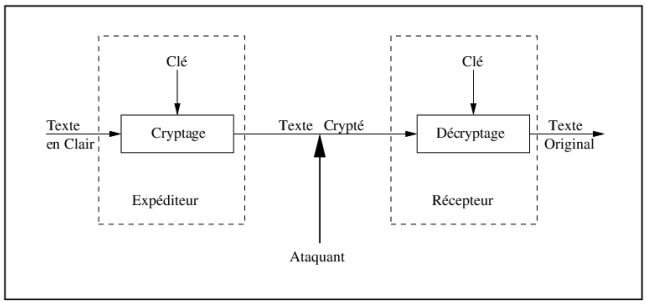

FIGURE 2-4 – Concept de la cryptanalyse.

regrouper en trois grandes catégories, est utilisé : [31]

Attaques par force brute :

- Force brute simple.
- Attaque par dictionnaire.
- Attaque par force brute masquée.

Attaques par analyse :

- Analyse différentielle.
- Cryptanalyse par canal auxiliaire.
- Attaques par rebond.

Attaques par implémentation :

- Attaques par faille logicielle.
- Attaques par canal auxiliaire.

2.3.2 Cryptographie

Cette deuxième branche vise à créer des systèmes de chiffrement, appelés crypto-systèmes, qui permettent de crypter un message de sorte qu'il ne soit accessible qu'avec une clé spécifique (un code permettant de déchiffrer les données) [31].

2.4 Contexte général sur la cryptographie

2.4.1 Concepts de base en cryptographie

— **Chiffrement et déchiffrement** : Processus de conversion du texte original en texte chiffré à l'aide d'une clé (chiffrement) et de la conversion inverse du texte chiffré en texte original à l'aide d'une autre clé (déchiffrement).

— **Clé** : Une valeur utilisée pour chiffrer ou déchiffrer des données. Dans les systèmes de chiffrement symétrique, la même clé est utilisée pour le chiffrement et le déchiffrement. Dans les systèmes de chiffrement asymétrique, des paires de clés publiques et privées sont utilisées

— **Texte chiffré** : connu sous le nom de cryptogramme, c'est le résultat obtenu après avoir appliqué un chiffrement à un texte en clair (le message original).

— **Crypto-système** : Il englobe l'ensemble des clés possibles ainsi que les textes clairs et chiffrés associés à un algorithme spécifique. Cet algorithme se compose en réalité de trois parties :

  — l'une génère les clés K,

  — une autre chiffre le texte en clair M,

  — et la troisième déchiffre le texte chiffré C.

  Le processus de retrouver le texte clair sans la clé de déchiffrement est appelé "décryptage". On utilise également les termes "cryptage" et "crypter" pour désigner l'action de chiffrer un message.

— **Fonctions de hachage** : Génèrent une empreinte numérique unique (hash) à partir de l'image originale. Le hash est utilisé pour vérifier l'intégrité de l'image et s'assurer qu'elle n'a pas été modifiée pendant la transmission ou le stockage.

— **Empreinte numérique** : Trace de notre activité en ligne. Elle regroupe nos données, actions et interactions sur internet.

— **Attaques cryptographiques** : Techniques utilisées pour compromettre la sécurité des systèmes cryptographiques en exploitant des faiblesses dans les algorithmes, les clés ou les implémentations.

2.4.2 Notations

La cryptographie utilise des techniques mathématiques pour sécuriser les données sensibles échangées sur des réseaux publics et privés. Son objectif principal est de garantir la confidentialité, l'intégrité et l'authenticité des informations. Pour cela, elle repose sur des algorithmes de chiffrement qui transforment les données originales en une forme illisible, rendue intelligible uniquement avec une clé de déchiffrement correspondante [33].
Un exemple simple est le chiffrement symétrique, où la même clé est utilisée pour chiffrer et déchiffrer les données. Cela peut être représenté mathématiquement par l'équation [25] :

$$C \equiv E_K(M) \tag{2.1}$$

où M est le message original, E_K est la fonction de chiffrement avec la clé K, et C est le message chiffré.
La propriété de base de la cryptographie est :

$$M = D_{K_d}(E_{K_e}(M)) \tag{2.2}$$

où :

- M représente le message clair,
- C est le message chiffré,
- K est la clé (dans le cas d'un algorithme à clé symétrique), K_e et K_d dans le cas d'algorithmes asymétriques,
- E(.) est la fonction de chiffrement,
- D(.) est la fonction de déchiffrement. Ainsi, avec un algorithme à clé symétrique,

$$M = D(C) \quad \text{si} \quad C = E(M) \tag{2.3}$$

2.4.3 Principe de Kerchoffs

Le principe de Kerckhoffs, énoncé par le cryptographe néerlandais Auguste Kerckhoffs au 19e siècle, stipule que la sécurité d'un système cryptographique ne doit pas reposer sur le

secret de l'algorithme, mais uniquement sur la confidentialité de la clé. En d'autres termes, un système cryptographique doit être considéré comme sûr uniquement si sa sécurité repose sur la confidentialité de la clé, et non sur le secret de l'algorithme lui-même [34]. Ce principe souligne l'importance de concevoir des systèmes cryptographiques basés sur des algorithmes bien connus et largement étudiés, tout en garantissant que la sécurité dépend uniquement de la confidentialité de la clé. Ainsi, même si l'algorithme est rendu public, la sécurité du système reste intacte tant que la clé reste secrète.
Le principe de Kerckhoffs favorise la transparence et la vérifiabilité des systèmes cryptographiques, permettant à la communauté de sécurité de les évaluer et de les analyser de manière approfondie.

2.5 Cryptographie standard

La cryptographie standard, pilier de la sécurité informatique, utilise des algorithmes mathématiques pour protéger les données sensibles. Contrairement à la cryptographie quantique, elle s'appuie sur des techniques éprouvées comme le chiffrement et le déchiffrement pour garantir la confidentialité et l'intégrité des communications. L'univers de la cryptographie standard abrite une multitude de techniques de chiffrement, et parmi elles se distinguent deux piliers fondamentaux : le chiffrement symétrique et le chiffrement asymétrique [35].

2.5.1 Chiffrement symétrique

Le chiffrement symétrique, également connu sous le nom de chiffrement à clé secrète, repose sur l'utilisation d'une clé unique partagée à la fois par l'expéditeur et le destinataire pour chiffrer et déchiffrer les messages [22].
La clé secrète constitue la pierre angulaire de la sécurité. Elle doit être gardée confidentielle par les deux parties, car sa divulgation donnerait accès au contenu des messages chiffrés. Dans la plupart des cas, la clé de chiffrement et la clé de déchiffrement sont identiques. Cette unicité simplifie la gestion et l'utilisation du système, puisqu'une seule clé suffit pour les deux opérations. Avant de communiquer, l'expéditeur et le destinataire doivent s'accorder sur une clé secrète commune. Cette clé peut être partagée via un canal sécurisé, comme une rencontre en personne ou un canal de communication chiffré.

La sécurité du chiffrement symétrique repose entièrement sur la confidentialité de la clé secrète [36]. Si la clé est compromise, un individu malveillant peut intercepter et lire les communications chiffrées. Par conséquent, la longueur et la complexité de la clé sont des facteurs cruciaux pour la sécurité du système. Une clé plus longue et plus aléatoire offre une meilleure protection contre les attaques par force brute ou d'autres méthodes de décryptage [24].

Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement

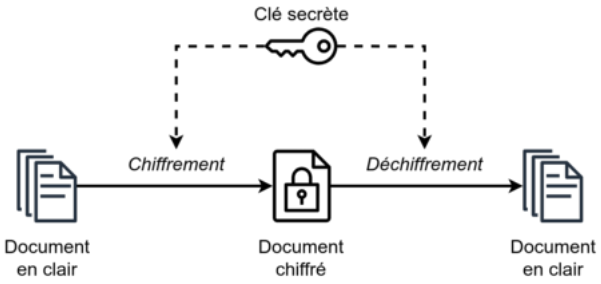

FIGURE 2-5 – Concept du chiffrement symétrique.

par blocs et le chiffrement par flot, détaillés ci-après .

— **Chiffrement par blocs** : Dans un système de chiffrement par blocs, le message est fragmenté en blocs de bits de taille fixe, qui sont ensuite chiffrés successivement. Le processus de chiffrement inclut des substitutions, où les bits d'un bloc sont remplacés par d'autres bits, et des transpositions, où les bits sont réarrangés. Les substitutions augmentent la confusion, rendant plus difficile l'établissement d'une relation directe entre le message original et le texte chiffré. Les transpositions améliorent la diffusion, empêchant que les répétitions du message initial apparaissent dans le texte chiffré [29].

  On distingue également le chiffrement par blocs itératif, où une fonction complexe, combinant substitutions et transpositions et appelée fonction de ronde, est appliquée plusieurs fois. Chaque itération, ou ronde, utilise en entrée la sortie de la ronde précédente (ou un bloc du texte original pour la première ronde) et chiffre cette entrée à l'aide de la fonction de ronde et d'une sous-clé générée à partir de la clé secrète K [35]. La fonction de chiffrement globale est en fait la combinaison de toutes ces rondes successives.

  Un exemple de chiffrement par blocs itératifs est le célèbre schéma DES (Data Encryption Standard). Le DES fonctionne en traitant des blocs de données de 64 bits et en utilisant une clé de chiffrement de 56 bits [36]. Le processus de chiffrement applique 16 rondes successives à chaque bloc de données. Chaque ronde intègre des substitutions non

linéaires et des permutations linéaires afin de brouiller efficacement les données. introduit en 1977, il a joué un rôle historique important dans la cryptographie. Cependant, il présente des failles de sécurité connues et son utilisation a donc diminué au profit de l'AES, plus performant et sécurisé [37].

AES, standardisé en 2001, est considéré comme un algorithme moderne et robuste, offrant une sécurité élevée, une vitesse de traitement adéquate et une adoption internationale. Il fonctionne sur des blocs de 128 bits, utilise des clés de 128, 192 ou 256 bits et s'appuie sur des rondes complexes de substitutions et de permutations pour brouiller les données [24].

— **Chiffrement par flot** : Le chiffrement par flot est une méthode cryptographique où les données sont chiffrées bit par bit ou caractère par caractère, contrairement au chiffrement par blocs qui chiffre des segments de longueur fixe [22]. Il utilise un générateur de clé pour produire une séquence pseudo-aléatoire de bits appelée flot de clé, dérivée d'une clé secrète partagée entre l'expéditeur et le destinataire. Chaque bit du message clair est combiné avec le bit correspondant du flot de clé à l'aide de l'opération XOR (exclusive OR), produisant ainsi le texte chiffré. Pour déchiffrer, le destinataire applique à nouveau l'opération XOR sur le texte chiffré en utilisant la même séquence du flot de clé. Le chiffrement par flot est généralement plus rapide et nécessite moins de ressources, ce qui le rend adapté aux applications de transmission en temps réel. Cependant, il est sensible aux erreurs et dépend fortement de la qualité du générateur de clé [36]. Si le générateur est prévisible ou la clé compromise, la sécurité du chiffrement est menacée. De plus, l'utilisation répétée du même flot de clé peut rendre le chiffrement vulnérable aux attaques par analyse statistique. On peut illustrer ces propos en utilisant le masque jetable, un chiffrement par flot simple et efficace [34].

Deux séquences de caractères de même longueur, l'une représentant notre message secret (le texte clair) et l'autre une séquence aléatoire et secrète (la clé). En combinant ces deux séquences à l'aide d'une opération simple, nous obtenons un message chiffré qui semble incompréhensible. C'est le principe du masque jetable, ou chiffrement par flot, proposé par Vernam en 1917.

La clé est une séquence de caractères aléatoires et de même longueur que le message que

vous souhaitez chiffrer. Cette clé doit être gardée secrète et ne doit être utilisée qu'une seule fois. Le chiffrement s'effectue en combinant chaque caractère du texte clair (mk) avec le caractère correspondant de la clé (Kk) à l'aide d'un "OU exclusif" (XOR). Le XOR est une opération binaire qui compare deux bits et ne donne un résultat "1" que si les bits sont différents [23].

$$ck = mk \oplus Kk \tag{2.4}$$

Le résultat de cette combinaison est le texte chiffré (ck). Il s'agit d'une séquence de caractères qui semble aléatoire et sans signification pour quiconque ne possède pas la clé.
Pour déchiffrer le message, il suffit d'effectuer la même opération XOR en utilisant la même clé sur le texte chiffré (ck). En combinant à nouveau chaque caractère du texte chiffré avec le caractère correspondant de la clé, on retrouve le texte clair original (mk) [33].

$$mk = ck \oplus Kk \tag{2.5}$$

2.5.2 Chiffrement asymétrique

Contrairement au chiffrement symétrique, où une seule clé sert à la fois à chiffrer et à déchiffrer, le chiffrement à clé publique utilise deux clés distinctes : une clé publique (Ke) pour le chiffrement et une clé privée (Kd) pour le déchiffrement [23].
La clé publique (Ke) est, comme son nom l'indique, accessible à tous. N'importe qui peut l'utiliser pour chiffrer un message destiné au récepteur. La clé privée (Kd), en revanche, est gardée secrète par ce dernier. Seule cette clé permet de déchiffrer les messages chiffrés avec la clé publique correspondante.
Alice souhaite envoyer un message secret à Bob. Elle utilise la clé publique de Bob (Ke), accessible à tous, pour chiffrer son message (m) et obtient un message chiffré (c). Alice envoie le message chiffré (c) à Bob par un canal de communication, qui ne doit pas nécessairement être sécurisé, car le message est protégé par le chiffrement. Bob, seul détenteur de la clé privée correspondante (Kd), utilise cette clé pour déchiffrer le message chiffré (c) et retrouve le message original (m) [22]. Un exemple de chiffrement à clé publique est le schéma RSA et le schéma

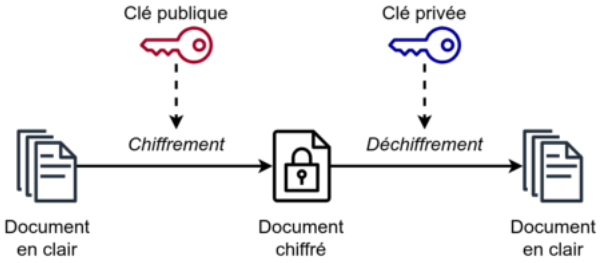

FIGURE 2-6 – Concept du chiffrement asymétrique.

ECC.

RSA (Rivest-Shamir-Adleman) repose sur la difficulté de factoriser de grands nombres en leurs facteurs premiers. Il utilise des clés relativement longues pour une sécurité équivalente. En revanche, ECC (Elliptic Curve Cryptography) est basé sur les propriétés des courbes elliptiques et utilise des opérations sur des points de ces courbes [37].

2.6 Cryptographie chaotique

Les systèmes chaotiques revêtent une importance significative dans le domaine de la cryptographie grâce à leur capacité à produire des séquences de chiffrement imprévisibles et hautement aléatoires [38]. Contrairement aux approches classiques reposant sur des algorithmes déterministes, les systèmes chaotiques tirent parti de leur sensibilité aux conditions initiales pour engendrer un comportement en apparence aléatoire. Cette caractéristique rend extrêmement difficile les attaques cryptographiques basées sur la prédiction ou la recherche exhaustive, car de légères variations dans les conditions initiales entraînent des résultats radicalement différents. De plus, la complexité dynamique inhérente aux systèmes chaotiques renforce leur résistance face aux attaques de force brute et aux techniques de cryptanalyse classiques. En intégrant des éléments de chaos dans les algorithmes de chiffrement, il est possible de concevoir des systèmes cryptographiques robustes et efficaces garantissant un niveau élevé de sécurité pour les communications et les données sensibles [6]. Le chiffrement par chaos brouille le message m_k avec un signal chaotique provenant d'un émetteur (représenté par un état x_k). Seul le signal brouillé y_k est envoyé au destinataire, qui doit ensuite reconstituer le message original à partir de y_k.

- **Phase de chiffrement (émetteur)**
  - Un message m_k est converti en une représentation numérique.

— Un système chaotique génère une séquence de nombres aléatoires (signal chaotique). Cette séquence est décrite par un état x_k.

— Le message m_k est mélangé avec le signal chaotique x_k pour produire un signal brouillé y_k.

— Seul le signal brouillé y_k est transmis au destinataire.

• **Phase de déchiffrement (récepteur)**

— Le destinataire reçoit le signal brouillé y_k.

— Le récepteur utilise un système chaotique identique à celui de l'émetteur pour générer sa propre séquence de nombres aléatoires (signal chaotique).

— L'état du système chaotique du récepteur $\hat{x}_k$ est synchronisé avec l'état de l'émetteur x_k en utilisant le signal y_k. ($\hat{x}_k$ suit dynamiquement x_k, reproduisant ainsi son comportement à chaque instant k).

— Le signal chaotique du récepteur $\hat{x}_k$ est utilisé pour dé-mélanger le message original m_k du signal brouillé y_k.

2.6.1 Techniques de cryptage par chaos

2.6.1.1 Cryptage par inclusion

Le cryptage par inclusion consiste à intégrer discrètement le message secret dans le signal émis par un système, sans en modifier les paramètres fondamentaux [39]. La récupération du message caché s'effectue principalement par deux approches : soit en exploitant l'accès limité des observateurs aux informations internes du système, soit en utilisant des techniques d'inversion du système émetteur lui-même [20].

2.6.1.2 Cryptage par commutation

Cette technique s'applique à la transmission de messages numériques. Dans ce système de communication, le message d'information contrôle le signal transmis en le basculant entre deux attracteurs chaotiques statistiquement similaires. Ces attracteurs représentent respectivement les bits 0 et 1 du message numérique [1]. Ils sont générés par deux systèmes chaotiques de structure identique mais avec des paramètres différents. Lors de la réception, le signal reçu

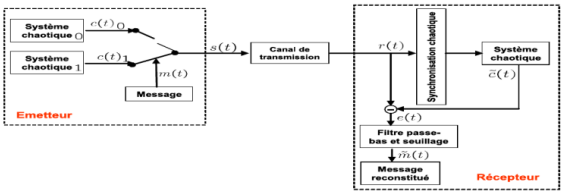

FIGURE 2-7 – Cryptage par commutation

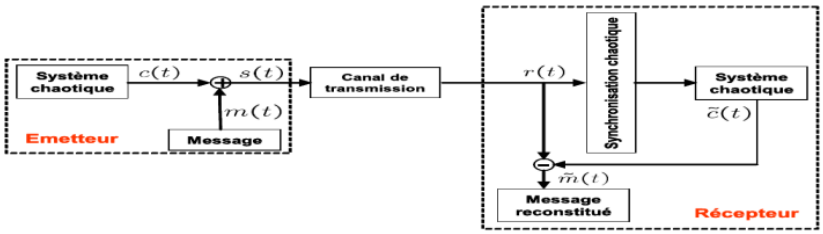

FIGURE 2-8 – Cryptage par addition

permet de reconstituer un système chaotique identique à ceux de l'émetteur. Le message d'information est ensuite récupéré en appliquant un filtre passe-bas, suivi d'un seuillage de l'erreur de synchronisation e(t) [17].

2.6.1.3 Cryptage par modulation paramétrique

L'approche par modulation utilise le message d'information pour moduler un ou plusieurs paramètres θ du système chaotique de l'émetteur. Un contrôleur adaptatif est mis en place au niveau du récepteur pour maintenir la synchronisation avec l'émetteur, même en tenant compte des variations du paramètre modulé [40]. A l'émetteur, la modulation d'un ou plusieurs paramètres entraîne une modification continue de l'attracteur chaotique. Par conséquent, le signal transmis devient plus complexe qu'un signal chaotique standard. Cependant, il est crucial que le processus d'injection du message et la fonction de démodulation des paramètres préservent le caractère chaotique du signal reçu par le récepteur.

2.6.1.4 Masquage par addition

Le chiffrement par addition chaotique utilise deux systèmes chaotiques identiques, l'un chez l'émetteur et l'autre chez le récepteur. Le système chaotique de l'émetteur génère un signal chaotique complexe, noté c(t), qui sert à masquer le message à chiffrer, m(t) [37]. Le message

m(t), généralement beaucoup plus faible que le signal chaotique c(t), est ajouté à c(t) pour créer le signal transmis s(t). Ce signal s(t) est ensuite envoyé au récepteur. La sécurité du chiffrement repose sur la difficulté de séparer le message m(t) du signal s(t) sans connaître le signal chaotique c(t). En effet, la complexité inhérente à c(t) et la faible puissance relative de m(t) rendent le signal transmis quasiment impossible à décrypter sans la clé, c'est-à-dire la connaissance de c(t).

2.6.1.5 Cryptage mixte

Face aux limites des techniques de chiffrement par chaos classiques, le cryptage mixte propose une approche innovante qui combine les principes de la cryptographie standard et de la synchronisation chaotique [41]. Dans ce schéma, le message à chiffrer, noté u(t), est d'abord crypté à l'aide d'une clé secrète, c(t), générée par un système chaotique de l'émetteur. Ce message chiffré est ensuite "injecté" dans la dynamique du système chaotique, augmentant ainsi sa complexité. Le signal résultant, y(t), dépendant des variables d'état de l'émetteur, est transmis au récepteur. Ce dernier établit une synchronisation avec l'émetteur chaotique, lui permettant de reconstituer la clé c(t) et, par conséquent, de décrypter le message u(t) [35].

2.6.2 Étude spectrale

Le but principale de ce mémoire est de concevoir un cryptosystème d'image robuste, et pour y parvenir, nous devons étudier plusieurs aspects afin d'éviter une faille quelconque. De ce fait, nous effectuons également une étude fréquentielle [24].
La distribution du contenu fréquentiel d'une image est une analyse cruciale dans la cryptographie d'images pour plusieurs raisons. Voici pourquoi on se base sur la distribution fréquentielle pour évaluer l'efficacité d'un cryptosystème [22] :

— **Masquage des Informations** : Une distribution uniforme des fréquences après chiffrement signifie que les caractéristiques de l'image originale sont bien dissimulées. Si certaines fréquences dominent dans l'image chiffrée, il pourrait être possible de retrouver des motifs ou des informations de l'image originale, ce qui compromettrait la sécurité du chiffrement.

— **Analyse de la Sécurité** : La transformation de Fourier décompose une image en ses composantes fréquentielles, révélant ainsi les motifs répétés et les structures régulières. En analysant le spectre de puissance (la distribution des amplitudes des fréquences), on peut déterminer si le chiffrement a introduit suffisamment de désordre pour rendre les informations originales indétectables.

— **Résistance aux Attaques** : Les attaques peuvent exploiter les régularités dans les fréquences pour deviner le contenu de l'image chiffrée. Une bonne distribution des fréquences rend ces attaques beaucoup plus difficiles, car elle empêche les attaquants de tirer des informations utiles du spectre de puissance.

— **Diffusion et Confusion** : Une analyse fréquentielle montrant une distribution uniforme des fréquences indique une bonne diffusion des informations originales à travers le texte chiffré.

— **Corrélation Faible ou Nulle entre les Fréquences** : Il ne doit y avoir aucune corrélation significative entre les différentes composantes fréquentielles de la séquence d'image. La faible corrélation entre les fréquences assure qu'il n'y a pas de motifs prévisibles, ce qui est crucial pour maintenir la sécurité et l'intégrité des systèmes cryptographiques.

2.6.3 Comparaison entre séquences pseudo aléatoires et séquences pseudo chaotiques

Caractéristique	Séquences Pseudo-Aléatoires	Séquences Pseudo-Chaotiques
Génération	- Utilisent des algorithmes déterministes PRNGs (Pseudo-Random Number Generators). - Basées sur des formules mathématiques simples et des états initiaux (graines).	- Utilisent des systèmes dynamiques chaotiques (ex : carte logistique, Tent map). - Exploitent les propriétés du chaos déterministe.
Propriétés Statistiques	- Distribution uniforme proche de l'aléatoire véritable. - Valeurs successives statistiquement indépendantes.	- Possèdent une complexité plus élevée et des comportements imprévisibles à long terme. - Sensibilité aux conditions initiales (une petite variation peut entraîner des séquences complètement différentes).
Application en Cryptographie	- Génération de clés de chiffrement, vecteurs d'initialisation.	- Systèmes de cryptographie avancés, sécurité renforcée.
Avantages	- Faciles à générer et à contrôler. - Bien comprises théoriquement. - Largement utilisées et adaptées pour de nombreuses applications pratiques.	- Haute complexité et imprévisibilité. - Grande sensibilité aux conditions initiales. - Avantage en cryptographie et sécurisation des communications.
Inconvénients	- Possèdent une période limitée après laquelle elles se répètent. - Peuvent être prévisibles si l'algorithme et la graine sont connus.	- Plus difficiles à générer et à analyser. - Sensibles aux erreurs numériques et aux perturbations. - Complexité algorithmique plus élevée.

TABLE 2.1 – Comparaison entre séquences pseudo-aléatoires et séquences pseudo-chaotiques

2.7 Conclusion

la cryptographie chaotique se présente comme une alternative prometteuse aux méthodes cryptographiques traditionnelles, offrant une sécurité renforcée, une simplicité d'implémentation et un potentiel de personnalisation. Malgré les nombreux défis rencontrés, la cryptographie chaotique demeure un domaine de recherche actif et prometteur, avec un fort potentiel pour révolutionner la sécurité de l'information. Les recherches futures visent à développer des systèmes chaotiques plus robustes, plus faciles à analyser et plus performants, permettant une adoption plus large de cette approche dans les applications critiques.

CHAPITRE 3

GÉNÉRATION DE SÉQUENCES CHAOTIQUES : APPLICATION AU CHIFFREMENT D'IMAGES

3.1 Introduction

A l'ère du numérique, la protection des données visuelles est devenue un enjeu crucial. Les images numériques, qu'elles soient de nature personnelle, médicale ou confidentielle, représentent des cibles de choix pour les cybercriminels. Face à ces menaces croissantes, la cryptographie d'images s'impose comme un rempart indispensable pour garantir la sécurité de nos informations visuelles. Dans ce troisième chapitre, nous allons explorer le potentiel insoupçonné des systèmes chaotiques pour le chiffrement d'images. Découvrons comment les mathématiques du chaos, avec leurs propriétés uniques de sensibilité aux conditions initiales et d'imprévisibilité, peuvent être exploitées pour créer des algorithmes de chiffrement robustes et résistants aux attaques. Le crypto-système que nous allons concevoir sera basé sur la carte chaotique de Tent (chaotic Tent map).

3.2 Simulation de la Tent map

La Tent map est un système chaotique en temps discret, définie sur l'intervalle [0, 1].
Elle est caractérisée par sa structure morceau linéaire, où elle divise l'intervalle en deux segments et applique une transformation linéaire différente sur chaque segment en fonction d'un

paramètre μ. Elle est linéaire en morceaux, mais non linéaire dans l'ensemble.

La Tent map est définie comme suit :

$$T(x) = \begin{cases} \mu x & \text{si } 0 \leq x < \frac{1}{2}, \\ \mu(1-x) & \text{si } \frac{1}{2} \leq x \leq 1, \end{cases} \tag{3.1}$$

où μ est un paramètre réel positif qui contrôle la pente de la fonction.

Comme nous l'avons exploré en profondeur dans le premier chapitre, les systèmes chaotiques possèdent une multitude de caractéristiques distinctives, illustrées par des simulations Matlab. Nous allons à présent présenter les simulations spécifiques à la tent map. (avec μ fixé à 2)

3.2.1 Sensibilité aux conditions initiales

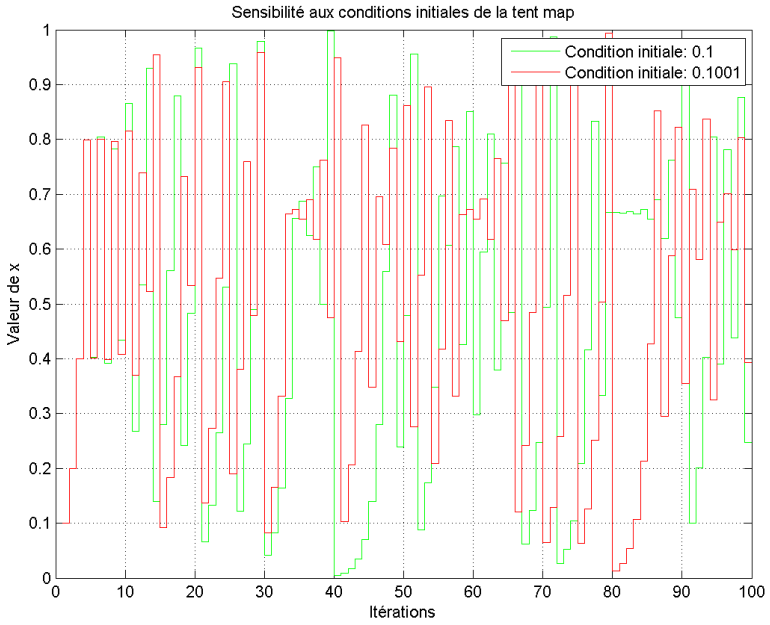

FIGURE 3-1 – Sensibilité aux conditios initiales de la Tent map

3.2.2 Aspect aléatoire

Cet aspect met en évidence l'aléatoire inhérent à notre système chaotique.

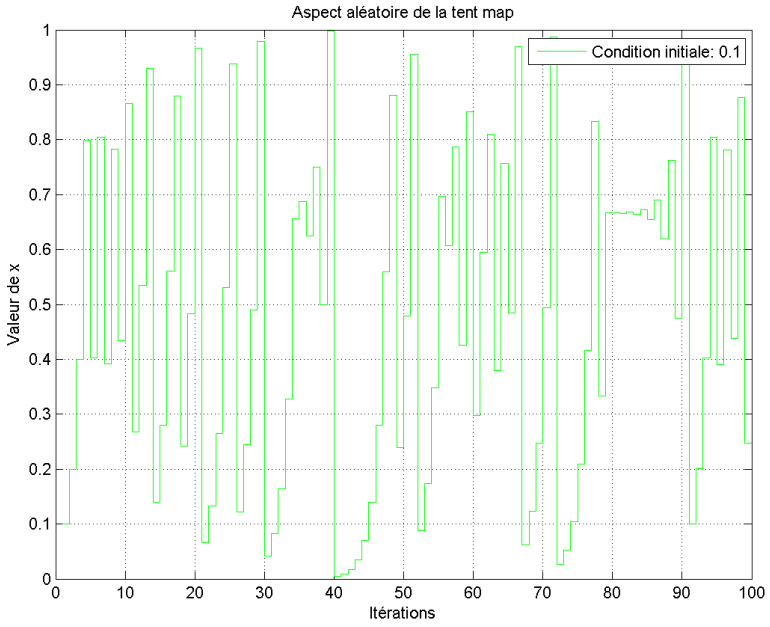

FIGURE 3-2 – Aspect aléatoire de la Tent map

3.2.3 Attracteur étrange

Dans le cas de la Tent map, elle ne possède pas d'attracteur étrange au sens traditionnel du terme. Un attracteur étrange est généralement un ensemble fractal sur lequel un système

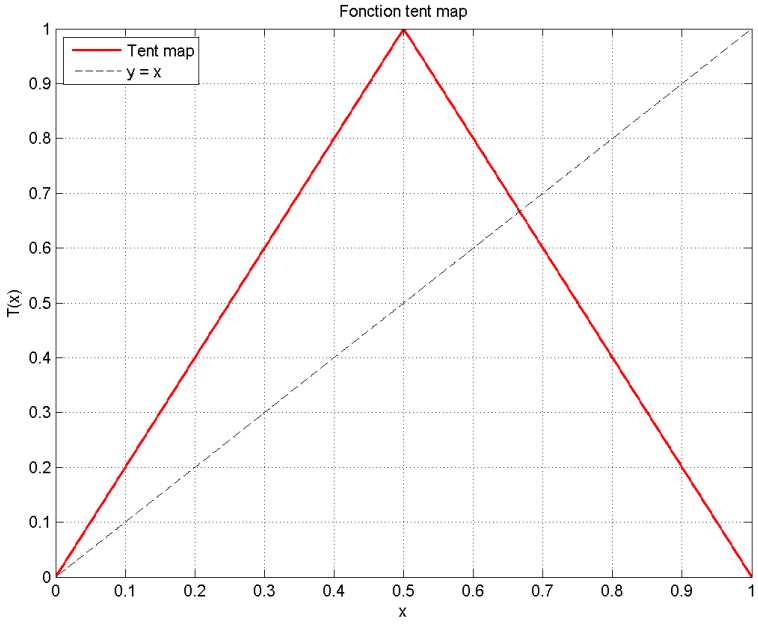

FIGURE 3-3 – Tracé de la fonction Tent map

dynamique évolue de manière non périodique et sensible aux conditions initiales. Bien que la Tent map présente un comportement chaotique, elle n'a pas la structure fractale complexe caractéristique d'un attracteur étrange.

3.2.4 Spectre de puissance

La structure du spectre peut varier en fonction de μ et de la condition initiale x_0. Par exemple, pour des valeurs de μ plus élevées, le spectre de puissance peut présenter une distribution plus large avec des harmoniques plus marquées. Le spectre de puissance joue un

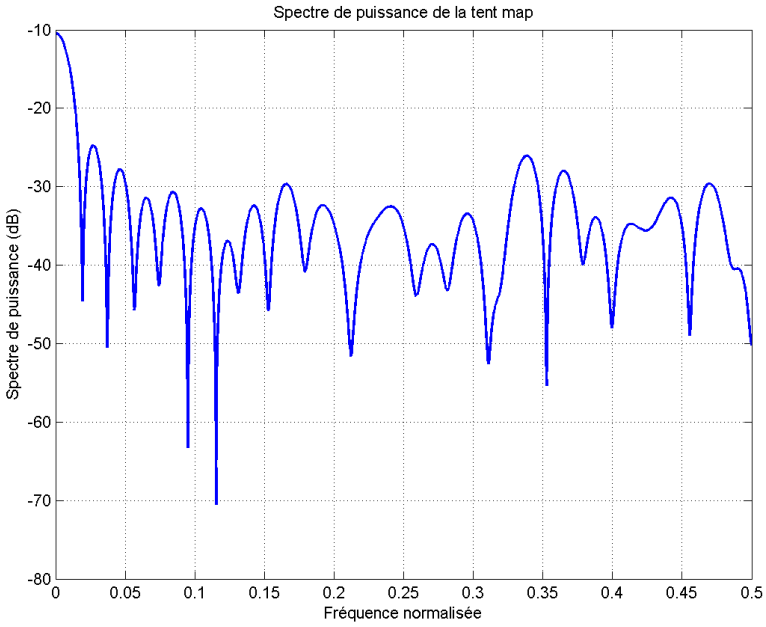

FIGURE 3-4 – Spectre de puissance de la Tent map

rôle crucial dans l'évaluation de la robustesse d'un algorithme de chiffrement basé sur des séquences chaotiques en fournissant une analyse détaillée des caractéristiques fréquentielles du signal chiffré. Un spectre de puissance complexe et uniforme indique que l'algorithme a introduit suffisamment de complexité pour disperser l'énergie du signal original sur une large gamme de fréquences, rendant ainsi les relations entre les données chiffrées difficiles à déterminer. En revanche, des anomalies telles que des pics à des fréquences spécifiques pourraient indiquer des faiblesses dans l'algorithme, permettant potentiellement des attaques basées sur l'analyse fréquentielle pour récupérer des informations sur les données originales.

3.2.5 Diagramme de bifurcations

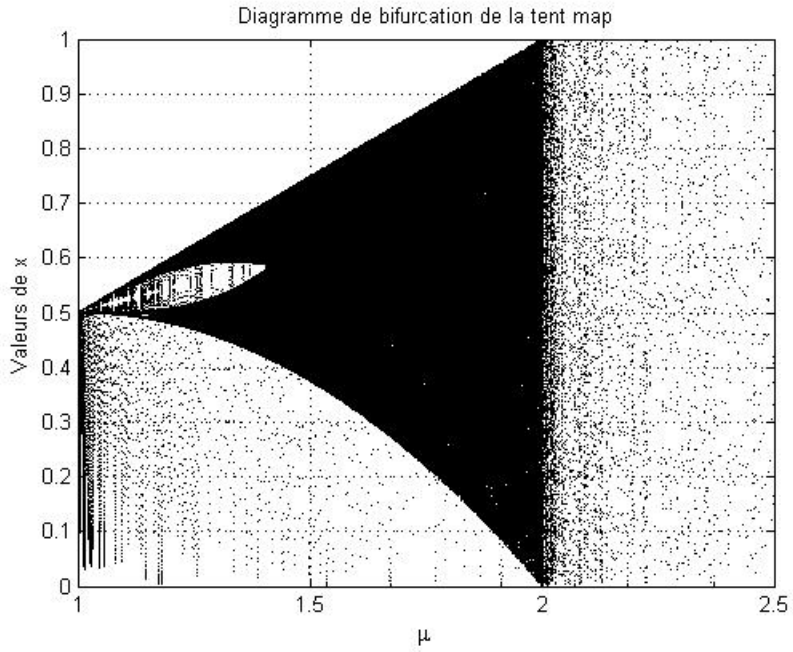

FIGURE 3-5 – Diagramme de bifurcations de la Tent map

3.3 Généralités sur les images

3.3.1 l'image numérique

L'image numérique est composée de minuscules points appelés pixels. Plus l'image contient de pixels, plus elle est détaillée et riche en informations.
[42] Deux notions sont importantes pour comprendre la qualité d'une image : la résolution et la définition.

- **Définition :** la définition correspond au nombre total de pixels d'une image, exprimé généralement en mégapixels (MP). Elle détermine la taille de l'image et la quantité d'informations qu'elle contient. Plus la définition est élevée, plus l'image est grande et peut être imprimée sur un grand format sans perte de qualité. [43]
- **Résolution :** La résolution représente la densité des pixels dans l'image. Elle détermine la précision et la netteté des détails. Plus la résolution est élevée, plus les pixels sont serrés et plus les détails sont fins. [42]

FIGURE 3-6 – Différence de définition entre deux images identiques

FIGURE 3-7 – Différence de résolution entre deux images identiques

Pour stocker, manipuler et partager nos images, différents formats existent, chacun avec ses propres caractéristiques et applications. On distingue les formats bitmap (ou matriciels) et les formats vectoriels. [43]

- **Format bitmap :** Les images numériques au format bitmap, également appelées images matricielles, sont représentées sous forme de matrice de pixels où chaque élément de la matrice représente un pixel de l'image. Par exemple, une image de 100 pixels de large sur 100 pixels de haut serait représentée par une matrice de 100 x 100 pixels, contenant au total 10 000 pixels. Chaque pixel de la matrice possède des informations de couleur, souvent définies par des valeurs RGB (Rouge, Vert, Bleu) dans un modèle de couleur

standard. Les valeurs de ces canaux déterminent la couleur finale du pixel. En fonction de la profondeur de couleur(quantité d'informations de couleur que chaque pixel d'une image peut stocker), une vaste gamme de couleurs peut être représentée. Les formats d'image courants dans cette catégorie incluent JPEG, PNG, BMP, et TIFF. [42]

- **Format vectoriel :** En revanche, les formats vectoriels décrivent les images à l'aide de courbes, de lignes et de formes géométriques définies par des équations mathématiques. Ces formats ne dépendent pas de la résolution, ce qui signifie qu'ils peuvent être agrandis ou réduits sans perte de qualité, contrairement aux images bitmap. Cela les rend parfaits pour les logos, illustrations, dessins au trait et toute image nécessitant des formes nettes et claires. Les formats courants dans cette catégorie sont SVG, EPS, et AI. [43]

3.3.2 Types d'images numériques

Il existe trois catégories principales d'images numériques qui se distinguent par leur mode de représentation des informations de couleur [42].

3.3.2.1 Images binaires

Les images binaires sont les plus simples. Elles ne représentent que deux couleurs : le noir et le blanc.Chaque pixel est codé par un seul bit, indiquant soit la présence de noir (0), soit la présence de blanc (1).

3.3.2.2 Images en niveaux de gris

Les images en niveaux de gris, également appelées images à tons de gris, représentent une gamme de nuances de gris allant du noir au blanc.Chaque pixel est codé par un nombre de bits, généralement 8 bits (256 niveaux de gris), permettant de reproduire une variation plus fine des luminosités [42].

3.3.2.3 Images en couleurs

Les images en couleur, qui sont les plus répandues, représentent une vaste gamme de couleurs perceptibles par l'œil humain grâce à la composante RGB (Rouge, Vert, Bleu). Chaque pixel dans une image couleur est codé par plusieurs bits, généralement 24 bits ou 32 bits, permettant

FIGURE 3-8 – Image binaire de la planète terre

FIGURE 3-9 – Image en niveau de gris

de représenter des millions de couleurs différentes. En utilisant 24 bits, chaque canal de couleur (R, G, B) est codé sur 8 bits, offrant 256 niveaux de luminosité par couleur. Cette combinaison de niveaux permet de créer jusqu'à 16,7 millions de couleurs distinctes (256 x 256 x 256). [43]

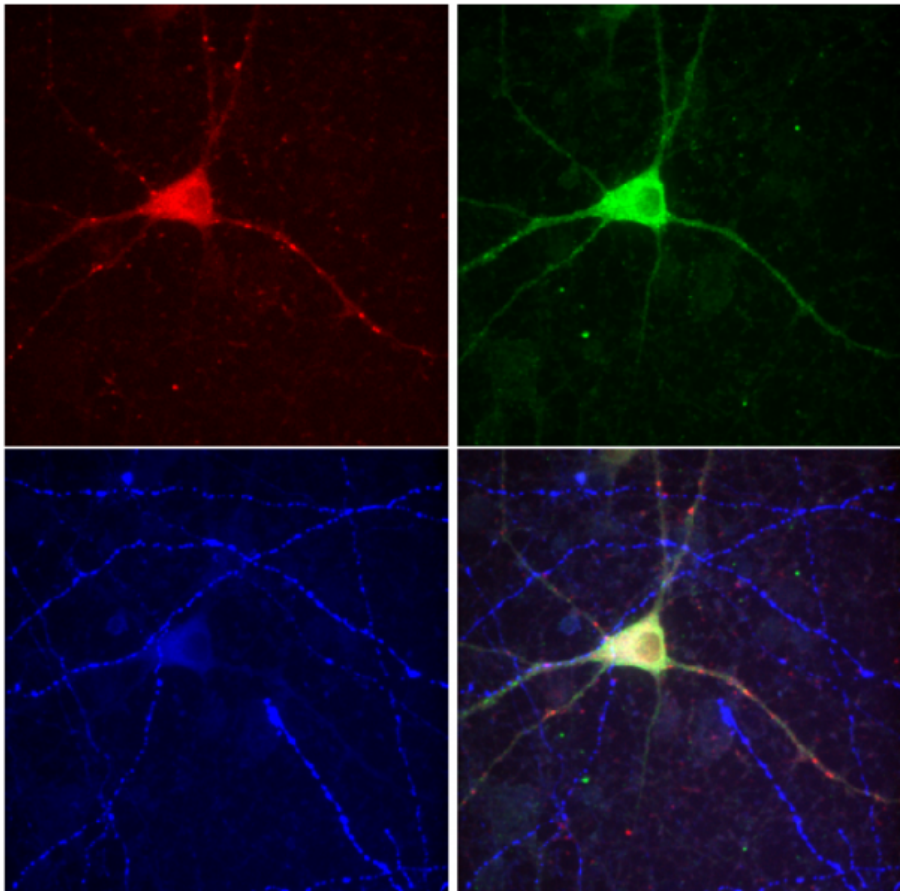

FIGURE 3-10 – Image en couleur ainsi que ces 3 constituants de couleur principaux (RGB)

3.4 Conception du crypto-système

Afin de concevoir notre algorithme de chiffrement, nous devons d'abord générer une séquence chaotique qui servira de clé. Cette clé sera ensuite utilisée pour chiffrer notre image. Dans cette section, nous détaillerons le processus de génération de la clé chaotique (étude de la clé) et expliquerons comment cette clé est appliquée au chiffrement de l'image (étude de l'application sur l'image). Dans tout ce qui suit, nous utilisons une image en niveau de gris de type JPG et de taille 450 x 281.

3.4.1 Étude de la clé

Comme précisé au début du chapitre, la clé de chiffrement est générée en utilisant la carte chaotique de Tent. Initialement, la séquence chaotique commence avec $x(1) = 0.5$ et le paramètre de contrôle $\mu = 1.999$. Pour chaque pixel de l'image, une nouvelle valeur de la séquence est calculée : si $x(i) < 0.5$, alors $x(i+1) = \mu x(i)$; sinon, $x(i+1) = \mu(1 - x(i))$. Cette itération produit une séquence chaotique x. Cette séquence chaotique est générée pour tous les pixels de l'image. Ensuite, les valeurs $x(2)$ à $x(N+1)$ sont restructurées en une matrice de la même taille que l'image et converties en type uint8 (la conversion en uint8 permet de préparer cette matrice pour une opération XOR bit à bit avec l'image d'origine, qui est également de type uint8), fournissant ainsi une matrice chaotique qui est utilisée pour le chiffrement avec l'image originale.

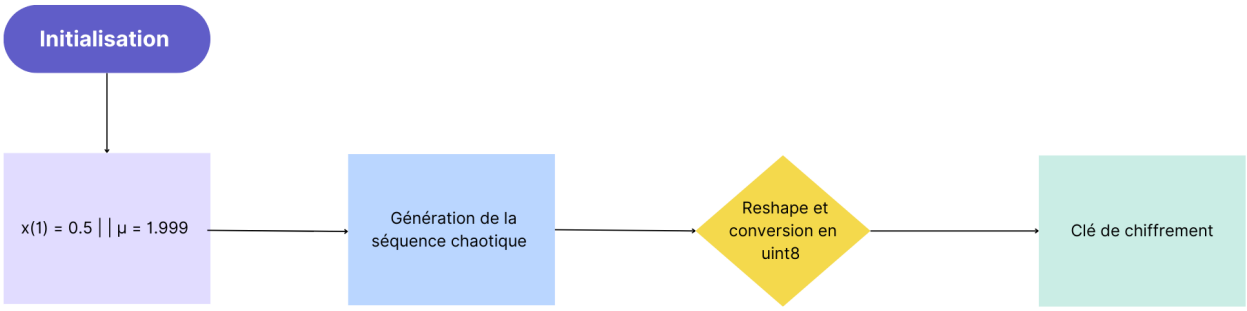

FIGURE 3-11 – Processus de génération de la clé

3.4.2 Étude de l'application sur l'image

Le chiffrement de notre image débute par le chargement de l'image à chiffrer, suivi de la détermination de ses dimensions (largeur et hauteur) pour l'utilisation ultérieure dans le processus de chiffrement. Ensuite vient l'étape de la génération de la clé chaotique, comme expliqué ci-dessus. Le chiffrement réel est effectué en appliquant une opération XOR bit à bit entre chaque pixel de l'image originale et la valeur correspondante de la matrice chaotique. Cette opération XOR mélange les valeurs des pixels de manière à rendre l'image originale illisible à l'œil nu. Ce processus crée une dépendance complexe entre chaque pixel de l'image chiffrée et à la fois les valeurs de l'image d'origine et la séquence chaotique utilisée. Cette approche rend le déchiffrement sans la connaissance de la clé initiale extrêmement difficile, car la séquence chaotique agit comme un élément aléatoire introduit dans le processus de chiffrement. En conséquence, l'image chiffrée devient plus résistante aux attaques cryptographiques, telles que la cryptanalyse. L'opération XOR est choisie non seulement pour sa simplicité d'implémentation mais aussi pour sa capacité à fournir un chiffrement efficace tout en préservant la nécessité d'une clé pour effectuer le déchiffrement correct et récupérer l'image originale sans altération. Enfin, on obtient l'image chiffré.

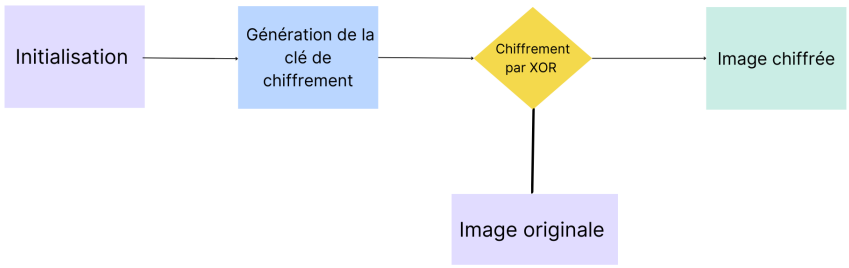

FIGURE 3-12 – Processus de chiffrement de l'image

Dans la figure qui suit, nous présentons l'image originale, l'image chiffrée ainsi que leurs histogrammes respectifs, fournissant une visualisation claire de la distribution des valeurs de pixels avant et après chiffrement. La partie de déchiffrement du programme commence par ré-

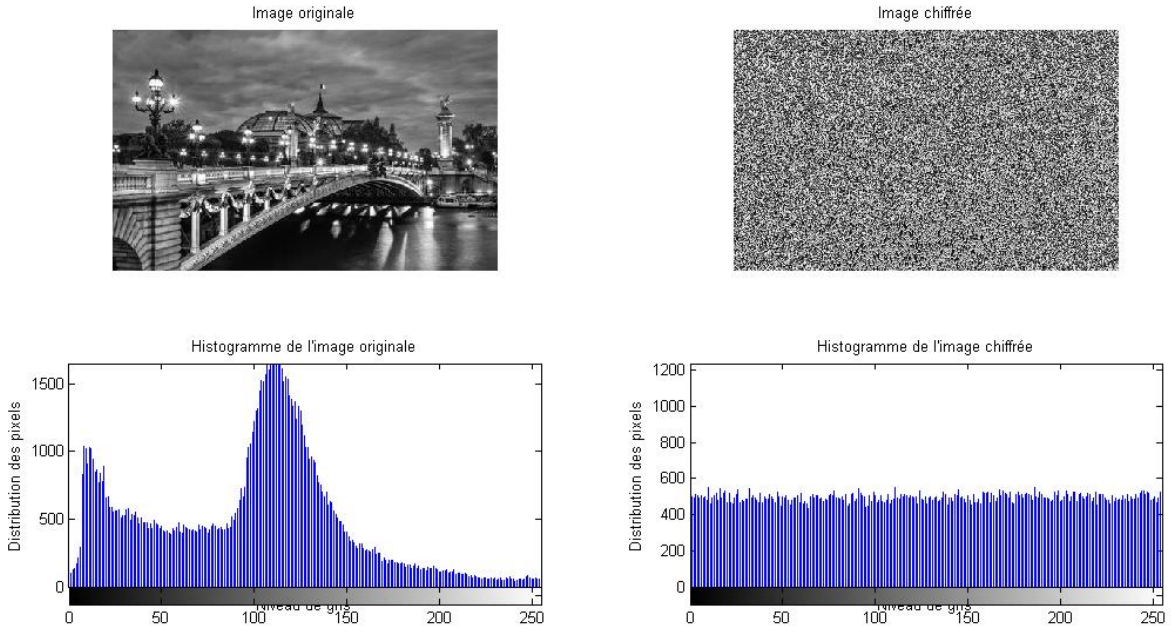

FIGURE 3-13 – l'image originale, l'image chiffrée ainsi que leurs histogrammes respectifs

générer la séquence chaotique utilisée pour le chiffrement en initialisant une nouvelle séquence avec la même condition initiale $x(1) = 0.5$ et le même paramètre de contrôle $\mu = 1.999$. Cette séquence est générée en itérant la carte chaotique (tent map) pour chaque pixel de l'image chiffrée. Une fois la séquence chaotique obtenue, l'image déchiffrée est récupérée en appliquant l'opération XOR bit à bit entre l'image chiffrée et la séquence chaotique convertie en type uint8 et restructurée en une matrice de la même taille que l'image originale. Ce processus inverse l'effet du chiffrement, récupérant ainsi l'image originale.

L'étude de la robustesse de notre cryptosystème fera l'objet de la section suivante, où nous examinerons en détail les résultats des histogrammes et mènerons d'autres analyses complémentaires.

3.5 Étude de la robustesse du crypto-système

3.5.1 Analyse des histogrammes

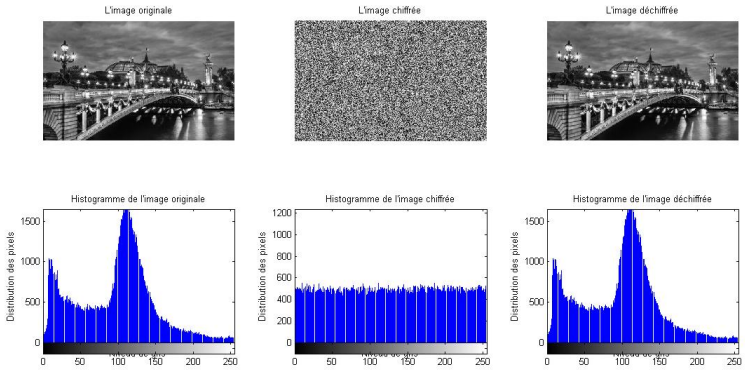

FIGURE 3-14 – Histogrammes des images originale, chiffrée et déchiffrée

L'observation de l'uniformité et de la répartition des valeurs dans ces histogrammes révèle l'efficacité du chiffrement à altérer la structure des données tout en dissimulant les caractéristiques distinctives de l'image originale dans l'histogramme chiffré. La robustesse se manifeste par la capacité du système à préserver les caractéristiques statistiques essentielles lors du déchiffrement, assurant ainsi une restitution fidèle de l'image originale malgré la transformation subie.

3.5.2 Corrélation des pixels adjacents

Le calcul du coefficient de corrélation entre les pixels est utilisé pour évaluer l'efficacité du cryptage dans les systèmes de cryptographie. Un coefficient de corrélation proche de 1 ou -1 indique une forte association entre deux pixels, tandis qu'une valeur proche de 0 suggère que les pixels ne sont pas corrélés et que la valeur de l'un ne peut pas être prédite à partir de l'autre. Ce coefficient est calculé en utilisant la formule suivante :

$$r_{xy} = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}$$

où E est l'espérance mathématique, X et Y sont les valeurs des pixels, μ_X et μ_Y sont les moyennes des valeurs des pixels X et Y, et σ_X et σ_Y sont les écarts-types des valeurs des pixels

X et Y.

Nous avons calculé le coefficient de corrélation pour les images originale, chiffrée et déchiffrée, en prenant en compte les pixels disposés horizontalement, verticalement et diagonalement. Les résultats obtenus sont les suivants :

Direction	**Image originale**	**Image chiffrée**
Horizontale	0.9196	-0.000017
Verticale	0.8975	-0.0043
Diagonale	0.8431	-0.00026

TABLE 3.1 – Coefficients de corrélation des pixels adjacents dans les trois directions.

Le coefficient de corrélation mesuré pour l'image originale est proche de 1, indiquant une forte association entre les pixels. En revanche, pour l'image chiffrée, le coefficient de corrélation est proche de 0, ce qui montre que le chiffrement a significativement réduit la corrélation entre les pixels, rendant l'image chiffrée beaucoup plus aléatoire et difficile à prédire.

Afin de confirmer les résultats du précédent tableau, on représente les distributions des corrélations des pixels adjacents dans les directions horizontale, verticale et diagonale de l'image originale et l'image chiffrée :

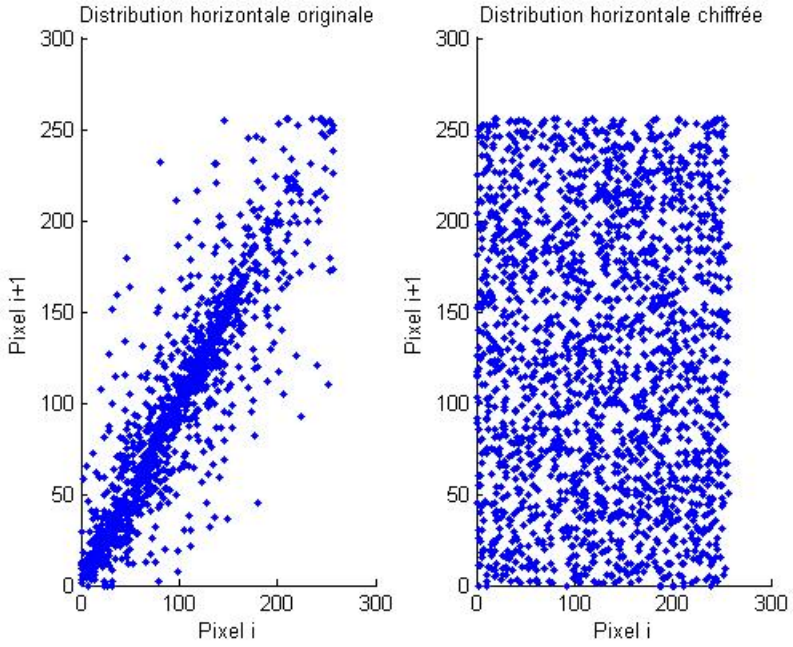

FIGURE 3-15 – la corrélation des pixels horizontalement adjacents dans l'image originale et chiffrée

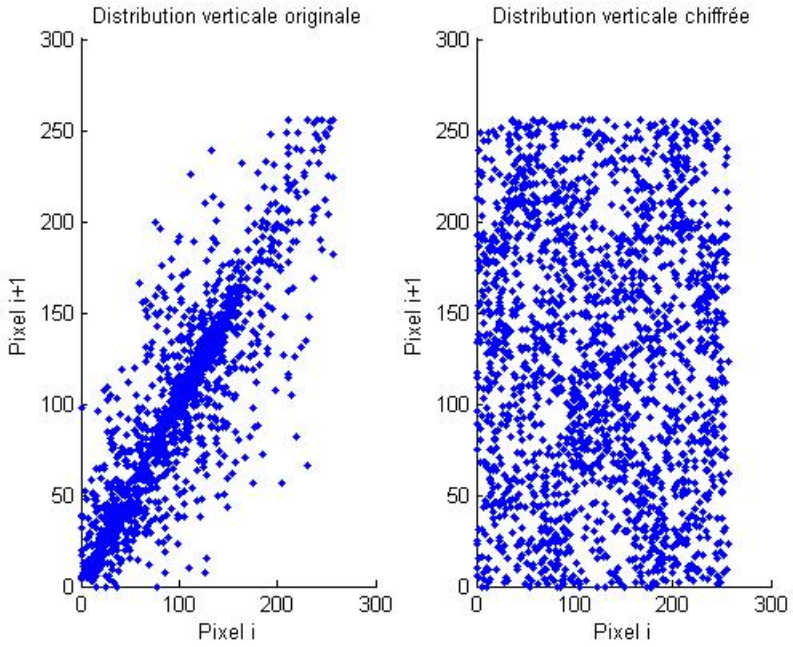

FIGURE 3-16 – la corrélation des pixels verticalement adjacents dans l'image originale et chiffrée

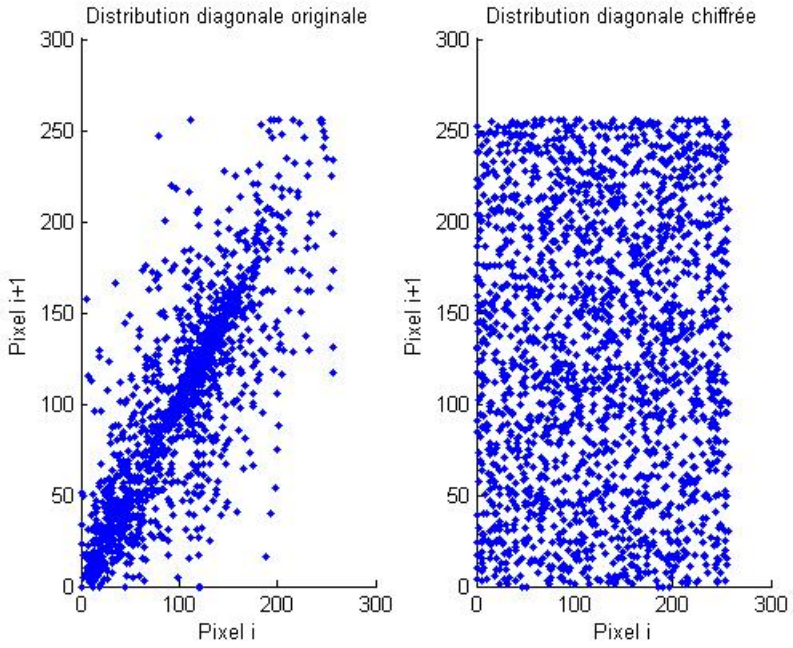

FIGURE 3-17 – la corrélation des pixels diagonalement adjacents dans l'image originale et chiffrée

la distribution des intensités des pixels de l'image originale se concentre sur la diagonale, les pixels sont alors fortement corrélés, tandis que ceux de l'image cryptée sont non-corrélés et ont une distribution uniforme.

3.5.3 Entropie d'information

L'entropie est utilisée pour mesurer la quantité d'information. Plus une information est ordonnée, plus est faible son entropie ; inversement, plus une information est confuse, plus est élevée l'entropie. Les entropies d'informations de notre image originale et l'image chiffrée correspondante sont calculées en utilisant l'équation suivante :

$$H = -\sum_{i=1}^{255} p_i \log_2 p_i$$

où p_i représente la probabilité d'occurrence de chaque niveau de gris. Les résultats obtenus sont listés dans le tableau suivant. À partir de ce tableau, il est clair que l'entropie de l'image chiffrée est proche de 8, donc le crypto-système proposé a une bonne propriété d'entropie d'information.

Image	**Entropie d'information**
Image originale	7.4810
Image chiffrée	7.9985

TABLE 3.2 – Comparaison des entropies d'information entre l'image originale et l'image chiffrée

3.5.4 Analyse différentielle (NPCR, UACI)

Le NPCR (Number of pixel change rate) est une mesure exprimée en pourcentage qui évalue la proportion de pixels modifiés entre une image originale et une image chiffrée.
Quant à l'UACI (Unified Average Change Intensity), il mesure l'intensité moyenne des modifications entre les pixels de l'image originale et ceux de l'image chiffrée.
Les résultats de ces tests sur notre crypto-système sont les suivant : Un NPCR de 99.5556%

Métrique	**Valeur**
NPCR	99.5556%
UACI	29.5312%

TABLE 3.3 – Résultats de l'analyse différentielle : NPCR et UACI

indique que 99.5556% des pixels dans l'image chiffrée diffèrent de ceux de l'image originale. Cette observation suggère que la majorité des pixels ont été altérés durant le processus de

chiffrement. Un UACI de 29.5312% indique que les pixels modifiés présentent en moyenne une intensité de changement de 29.5312% par rapport à leur valeur d'origine. Ce résultat montre que bien que la majorité des pixels aient été modifiés (comme le suggère le NPCR élevé).
Nous avons effectué un test de déchiffrement avec une clé légèrement différente et calculer le NPCR pour étudier la vulnérabilité aux attaques par force brute.
Ci-dessous les résultats obtenus :

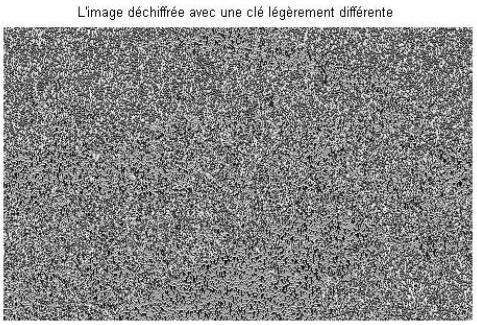

FIGURE 3-18 – Image déchiffrée avec une clé légèrement différente

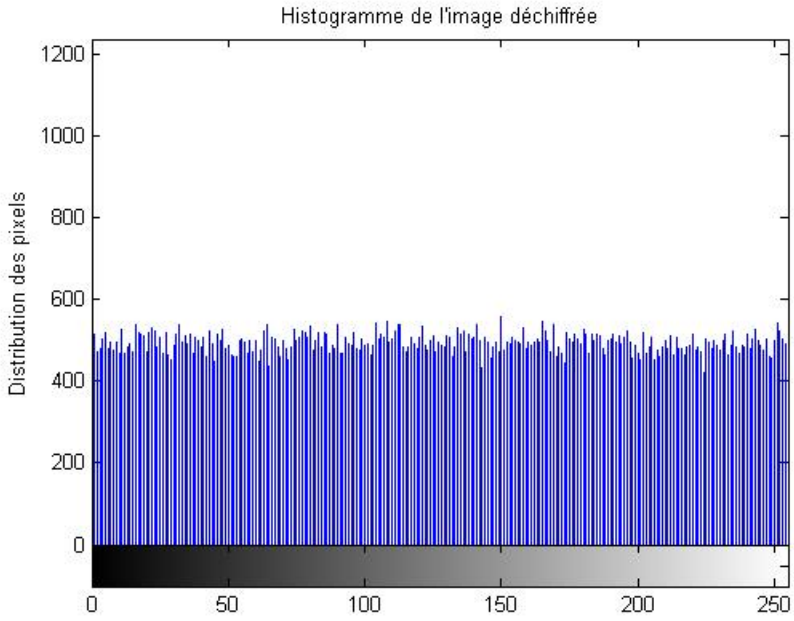

FIGURE 3-19 – Histogramme de l'image déchiffrée avec une clé légèrement différente

Le processus de décryptage a échoué lorsque la clé secrète est légèrement modifiée, l'image décryptée est totalement brouillée. Un NPCR de 99.9589 % indique que la petite modification

Métrique NPCR (%)	**Valeur**
NPCR entre l'image originale et celle déchiffrée avec la clé originale	0.76
NPCR entre l'image originale et celle déchiffrée avec la clé modifiée	99.6315

TABLE 3.4 – Comparaison des valeurs NPCR .

de la clé a entraîné des différences significatives dans l'image déchiffrée. Ainsi, nous concluons que les images chiffrées par l'algorithme proposé présentent une sensibilité extrême à la clé secrète et sont robustes face aux attaques par force brute.

3.6 Analyse de la robustesse de la clé

Pour évaluer l'aléa et l'efficacité d'une clé chaotique, il est important d'appliquer une série de tests statistiques et cryptographiques. Nous allons ici effectuer 3 des tests les plus utilisés pour l'analyse d'une clé chaotique.

- **Analyse du spectre de puissance :**

  La Transformée de Fourier est utilisée pour calculer et afficher le spectre de puissance de notre séquence chaotique. Le spectre de puissance obtenu se caractérise par une réparti-

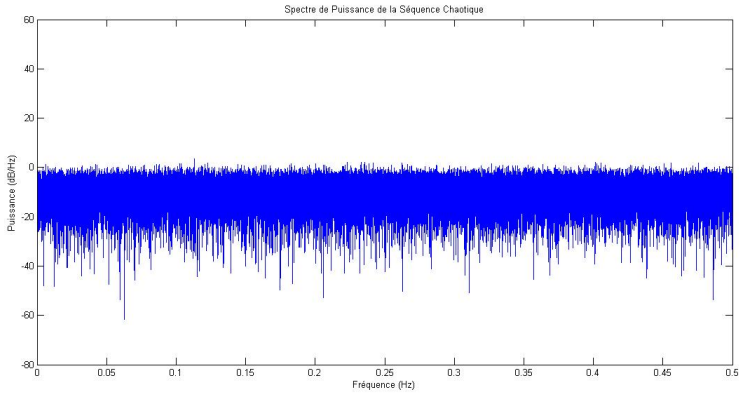

FIGURE 3-20 – Spectre de puissance de la séquence chaotique utilisée pour le chiffrement

tion uniforme de l'énergie à travers une large bande de fréquences, sans pics dominants à des fréquences spécifiques. Un tel spectre indique que la séquence chaotique ne présente pas de motifs répétitifs ni de périodicités discernables, ce qui est crucial pour garantir

un comportement aléatoire robuste. Une densité de puissance uniforme sur l'ensemble des fréquences confirme cette propriété, assurant ainsi une bonne qualité pour une clé chaotique utilisée dans des applications cryptographiques.

- **Test de l'uniformité et de l'indépendance des Bits :**

  L'uniformité des bits fait référence à la distribution des bits de valeur 0 et 1 dans les représentations binaires des pixels de l'image. Une valeur proche de 0.5 indique une distribution uniforme, c'est-à-dire qu'il y a autant de bits 0 que de bits 1, ce qui est idéal pour une image chiffrée car cela suggère une forte randomisation. Le tableau suivant montre les resultats de ce test sur notre clé : Les résultats de l'uniformité des bits entre l'image

Image	**Uniformité des bits**
Originale	0.47425
Chiffrée	0.50036

TABLE 3.5 – Uniformité des bits entre l'image originale et l'image chiffrée

originale (0.47425) et l'image chiffrée (0.50036) révèlent des différences significatives dans la répartition des bits. L'image originale montre une légère prédominance des bits 0 par rapport aux bits 1, typique des images naturelles où la distribution des niveaux de gris n'est pas uniforme. En revanche, l'image chiffrée présente une uniformité presque parfaite entre les bits 0 et 1, indiquant une transformation réussie par le chiffrement. Cette uniformité renforce la sécurité en rendant l'image chiffrée difficile à distinguer du bruit aléatoire sans la clé appropriée, ce qui complique toute tentative d'analyse ou d'attaque statistique.

- **Test d'Autocorrélation :**

  Les graphes d'autocorrélation sont utilisés pour visualiser la corrélation entre les valeurs d'une série (dans ce cas, les valeurs des pixels de l'image) à différents décalages ou retards. La courbe d'autocorrélation de l'image originale présente une décroissance exponentielle, suggérant une forte corrélation spatiale entre les pixels adjacents, caractéristique des motifs ou structures récurrents dans l'image naturelle. À mesure que le décalage augmente, la corrélation diminue, conformément aux attentes pour ce type d'image. En revanche, la courbe d'autocorrélation de l'image chiffrée montre initialement une décroissance suivie d'une stabilisation. Cette évolution indique que le processus de chiffrement a efficacement dispersé les valeurs de pixels, réduisant ainsi la corrélation spatiale. La stabilisation à un

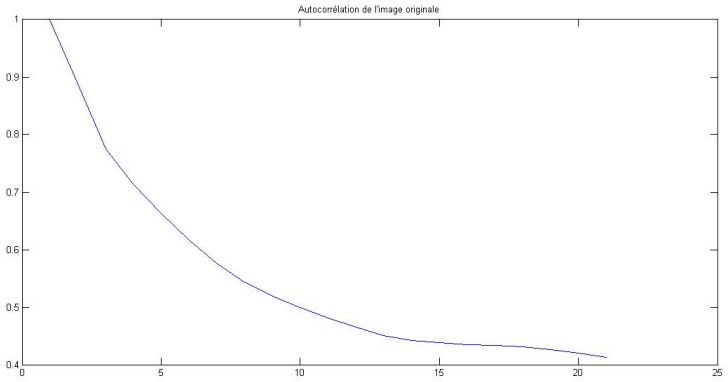

FIGURE 3-21 – Courbe d'autocorrélation de l'image originale

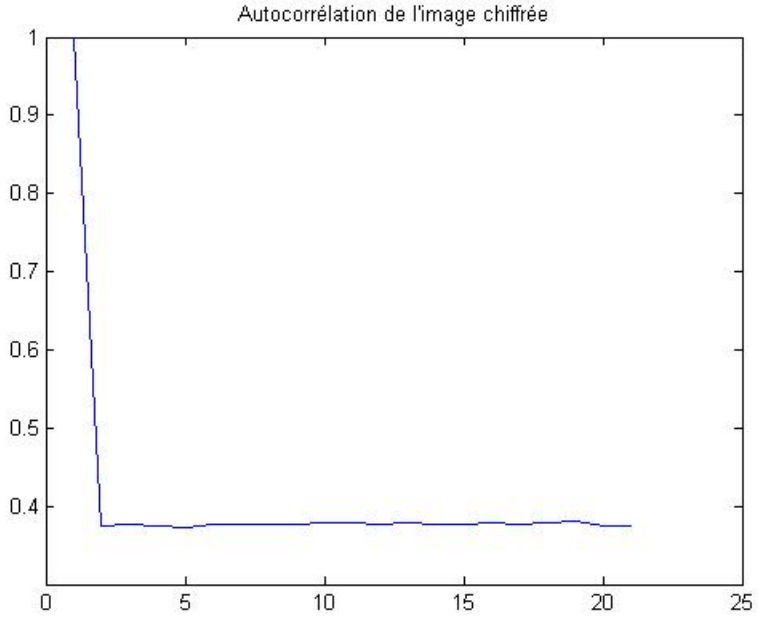

FIGURE 3-22 – Courbe d'autocorrélation de l'image chiffrée

niveau bas de corrélation suggère une diffusion efficace des informations, compliquant la reconstruction des motifs originaux ou des relations spatiales par des méthodes d'analyse statistique ou d'attaque cryptographique. Cette observation sous-tend l'importance d'une bonne propriété de diffusion dans le chiffrement d'image pour assurer la sécurité des données, en rendant ardue toute tentative de récupération non autorisée des informations originales.

3.7 Conclusion

Dans ce chapitre, nous avons exploré le chiffrement d'une image à l'aide d'une carte chaotique de Tent, débutant par la simulation de ce système dynamique non linéaire. Nous avons ensuite examiné l'adaptation de ce concept aux données d'images numériques, en démontrant comment une séquence chaotique peut être utilisée comme clé pour chiffrer efficacement une image. L'étude de la robustesse de cet algorithme a mis en lumière sa capacité à générer des clés sécurisées et imprévisibles, essentielles pour la sécurité des systèmes de cryptographie.
Un cryptosystème utilisant une clé chaotique générée par une Tent map représente une approche prometteuse pour sécuriser efficacement les données sensibles, offrant à la fois résilience et complexité pour contrer les attaques cryptanalytiques modernes. Ce système de cryptographie d'image présente plusieurs avantages significatifs en termes de sécurité et d'efficacité. Tout d'abord, l'utilisation d'une séquence chaotique pour générer la clé offre une imprévisibilité robuste. Les systèmes chaotiques sont sensibles aux conditions initiales, ce qui signifie que de petites variations dans les conditions initiales conduisent à des séquences complètement différentes, renforçant ainsi la sécurité contre les attaques par force brute ou par analyse statistique. De plus, les clés générées à partir de processus chaotiques ont un spectre de puissance large bande, ce qui signifie qu'elles ne présentent pas de pics dominants à des fréquences spécifiques. Cela rend les attaques basées sur la fréquence plus difficiles à exécuter, car la distribution de la puissance est uniforme sur une large gamme de fréquences. En outre, les algorithmes de chiffrement basés sur des clés chaotiques sont souvent simples à implémenter et rapides à exécuter, ce qui les rend adaptés aux applications nécessitant un chiffrement en temps réel ou une faible latence.

CONCLUSION GÉNÉRALE

Ce mémoire a entrepris une exploration approfondie de l'intersection fascinante entre la dynamique chaotique et la sécurité informatique, dévoilant un nouveau paradigme pour la cryptographie moderne. En s'attaquant à cette complexité, nous avons découvert que les systèmes chaotiques, souvent considérés comme imprévisibles et turbulents, recèlent un potentiel immense pour la protection des données sensibles.

Le premier chapitre a exploré les fondements théoriques des systèmes chaotiques, mettant en lumière leur nature dynamique complexe et les caractéristiques qualitatives et quantitatives qui les définissent. En examinant des exemples célèbres comme les systèmes de Lorenz et Hénon, nous avons illustré comment le chaos peut être modélisé et utilisé pour générer des comportements imprédictibles, essentiels dans le domaine de la cryptographie moderne.

Le deuxième chapitre a élargi le cadre conceptuel en introduisant la cryptographie chaotique, situant cette approche dans le contexte plus large de la cryptologie. Nous avons exploré les principes fondamentaux de la cryptographie, comparant les techniques standard avec les innovations chaotiques qui exploitent l'aléa intrinsèque des systèmes chaotiques. Une étude approfondie des séquences pseudo-aléatoires par rapport aux séquences pseudo-chaotiques a souligné les avantages théoriques et pratiques des approches chaotiques dans la sécurisation des données sensibles.

Le troisième chapitre s'est concentré sur la conception spécifique d'un crypto-système utilisant la carte chaotique de Tent. Nous avons débuté par la simulation détaillée de la Tent map, explorant sa dynamique non linéaire et ses capacités à générer des séquences aléatoires. En intégrant ces principes dans le domaine des images numériques, nous avons développé un crypto-système

innovant capable de chiffrer efficacement des données visuelles tout en maintenant leur confidentialité. Nous avons clôture le chapitre avec L'étude de la robustesse du crypto-système et l'analyse approfondie de la sécurité de la clé.

Notre analyse méticuleuse a mis en lumière les caractéristiques qualitatives et quantitatives fondamentales des systèmes chaotiques. La sensibilité aux conditions initiales, l'effet papillon et les trajectoires erratiques, souvent perçues comme des obstacles, se révèlent être des atouts précieux dans le domaine de la cryptographie. Ces propriétés intrinsèques rendent les systèmes chaotiques extrêmement difficiles à prédire et à décrypter, offrant ainsi une couche de protection robuste contre les attaques malveillantes.

C'est avec une conviction profonde envers l'innovation et la sécurité des données que nous clôturons ce mémoire. Nous envisageons un avenir où la théorie chaotique continue d'inspirer de nouvelles stratégies pour répondre aux besoins croissants de protection de l'information dans notre société moderne.

BIBLIOGRAPHIE

[1] H.K. Khalil. *Nonlinear Systems : Third Edition*. Prentice Hall, 2002.

[2] A. Isidori. *Nonlinear Control Systems*. Springer, 3rd edition, 1995.

[3] Kerstin Mathias and Christophe Volos. *Chaotic Secure Communication : Principles and Applications*. Springer, 2005.

[4] Ljupco Kocarev and Shiguo Lian. *Chaos-Based Cryptography : Theory, Algorithms and Applications*. Springer, 2011.

[5] Claudio R. Mirasso and Lucio M. Pecora. *Chaotic Systems : Discrete and Continuous, Complexity, Synchronization, and Cryptography*. Springer, 2013.

[6] M. Ali Oguztoreli. *Secure Communication via Chaos and Nonlinear Dynamics*. Springer, 2014.

[7] Edward N. Lorenz. *The Essence of Chaos*. University of Washington Press, 1993.

[8] Kathleen Alligood, Tim Sauer, and James A. Yorke. *Chaos : An Introduction to Dynamical Systems*. Springer, 1996.

[9] J. M. T. Thompson and H. B. Stewart. *Nonlinear Dynamics and Chaos : Geometric Methods for Engineers and Scientists*. CRC Press, 2002.

[10] Derong Liu and Panos J. Antsaklis. *Stability and Control of Dynamical Systems with Applications*. Birkhäuser, 2003.

[11] Lawrence Perko. *Differential Equations and Dynamical Systems.* Springer, 2001.

[12] Jean-Jacques E. Slotine and Weiping Li. *Applied Nonlinear Control.* Prentice Hall, 1991.

[13] Gilbert Strang. *Introduction to Linear Algebra.* Wellesley-Cambridge Press, 2009.

[14] Steven H. Strogatz. *Nonlinear Dynamics and Chaos : With Applications to Physics, Biology, Chemistry, and Engineering.* Westview Press, 1994.

[15] Oliver Nelles. *Nonlinear System Identification : From Classical Approaches to Neural Networks and Fuzzy Models.* Springer, 2001.

[16] Morris W. Hirsch, Stephen Smale, and Robert L. Devaney. *Differential Equations, Dynamical Systems, and an Introduction to Chaos.* Academic Press, 2012.

[17] Xun Luo and Jinlong Wang. *Chaos in Cryptography and Digital Communication.* Springer, 2015.

[18] M. Rosenstein, J. Collins, and C. De Luca. A practical method for calculating largest lyapunov exponents for small data sets. *Physica D*, 65 :117–134, 1993.

[19] Y. Chen and A.Y.T. Leung. *Bifurcation and Chaos in Engineering.* Springer-Verlag, 1998.

[20] Enrique Alvarez and Simon Haykin. *Chaotic Encryption Systems.* Springer, 2012.

[21] S.S. Sastry. *Nonlinear Systems Analysis, Stability, and Control.* Springer, 1999.

[22] Keith M. Martin. *Everyday Cryptography : Fundamental Principles and Applications.* Oxford University Press, 2012.

[23] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.

[24] Christof Paar and Jan Pelzl. *Understanding Cryptography : A Textbook for Students and Practitioners.* Springer, 2010.

[25] Simon Singh. *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Doubleday, 1999.

[26] David Kahn. *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner, 1996.

[27] Simon Singh. *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor, 2000.

[28] Albrecht Beutelspacher. *Cryptology : An Introduction to the Art and Science of Enciphering and Deciphering Messages.* American Mathematical Society, 1994.

[29] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[30] Ross Anderson. *Security Engineering : A Guide to Building Dependable Distributed Systems.* Wiley, 2001.

[31] William Stallings. *Cryptography and Network Security : Principles and Practice.* Prentice Hall, 2006.

[32] Philippe Guillot. *La cryptologie : l'art des codes secrets.* Auteur, 2013. Date de parution : 23/05/2013.

[33] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography.* Springer, 2nd edition, 2014.

[34] Douglas R. Stinson. *Cryptography : Theory and Practice.* Chapman & Hall/CRC, 3rd edition, 2006.

[35] Bruce Schneier. *Applied Cryptography : Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, 2nd edition, 1996.

[36] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2nd edition, 2014.

[37] William Stallings. *Cryptography and Network Security : Principles and Practice.* Pearson, 7th edition, 2016.

[38] Andreas Ostmann. *Chaos and Cryptography : New Trends in Chaotic Cryptography.* Springer, 2003.

[39] Feng Hao and Denis T. Nichols. *Chaos-Based Digital Communication Systems*. Springer, 2009.

[40] Michiko Hayashi and Masayuki Abe. *Chaotic Dynamics in Cryptography*. Springer, 2007.

[41] Saeed Reza Khalili and Ali Reza Khosravani. *Cryptography Using Chaos and Fractals*. Springer, 2011.

[42] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Pearson Education, 2008.

[43] Wilhelm Burger and Mark J. Burge. *Digital Image Processing : An Algorithmic Approach*. Springer, 2016.