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 ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Automatique**

Spécialité : **Automatique et Systèmes**

Présenté par

Arezki MELLAH
Sabiha OUBRAHAM

Thème

Application des systèmes chaotiques pour la conception et implémentation d'un algorithme de chiffrement robuste de fichiers texte

Mémoire soutenu publiquement le 24 / 06 / 2024 devant le jury composé de :

M Youcef MESSAR
M. A. A, UMMTO, Président

Mme Ouerdia MEGHERBI
M. C. B, UMMTO, Encadrant

Mme Kahina LARBI
M. A. B, UMMTO, Examinatrice

Mme Hayat HARROUCHE
M. A. B, UMMTO, Examinatrice

Dédicaces

Tout d'abord, je tiens à remercier DIEU

De m'avoir donné la force et le courage de mener

À bien ce modeste travail.

J'ai le grande plaisir de dédie ce modeste travail :

A ma très chère mère, qui me donne toujours l'espoir de vivre et qui n'a jamais cessé de prier pour moi.

A mon très chère père, pour ses encouragement, son soutien son sacrifice afin que rien n'entrave le déroulement de mes études.

A mes frères et mes sœurs,
A mes meilleurs amis
Et mes chers collègues

Et à tous ceux qui m'aident et consultent ce modeste travail.

En fin, je remercie ma binôme, Oubraham Sabiha, qui a contribué à la réalisation de ce modeste travail.

MELLAH Arezki

Dédicaces

Tout d'abord, je tiens à remercier DIEU

De m'avoir donné la force et le courage de mener

À bien ce modeste travail.

Je tiens à dédier cet humble travail à :

Mes chers parents qui ont toujours été à mes côtés et m'ont toujours soutenu tout au long de ces longues années.

Mes chers frères et sœurs qui me poussent toujours à avancer et à continuer, et dont les encouragements nous ont permis d'affronter de nombreuses épreuves.

Mes meilleurs amis :

Sans citer les noms pour ne pas tenter oublier quelqu'un.

Toute la famille et mes amis d'enfance ainsi que ceux du long parcours scolaire et universitaire.

En fin,je remercie mon binôme, MELLAH Arezki qui a contribué à la réalisation de ce modeste travail.

OUBRAHAM Sabiha

Remerciements

Nous remercions, en premier lieu, notre Dieu.

Nous adressons nos sincères remerciements à nos parents et à tous nos enseignants qui nous ont préparés théoriquement et pratiquement durant nos années d'études, ainsi qu'à tout le corps administratif de l'Université Mouloud Mammeri de Tizi-Ouzou.

Nous tenons à remercier tout d'abord notre promotrice, Madame MEGHERBI OUERDIA, pour sa qualité remarquable d'encadrement, sa grande disponibilité, sa précieuse contribution, et pour le temps qu'elle a consacré à la correction de ce mémoire.

Nous remercions également tous ceux qui ont aidé de près ou de loin à l'élaboration de ce travail.

Enfin, nous adressons nos remerciements aux membres du jury qui nous feront l'honneur d'examiner ce mémoire.

Liste des abréviations

AES : Advanced Encryption Standard. Norme de Chiffrement Avancée.

ASCII : American Standard Code for Information Interchange. Code Standard Américain pour l'Échange d'Information.

DES : Data Encryption Standard. Norme de Chiffrement des Données.

ECC : Elliptic Curve Cryptography. Cryptographie à Courbes Elliptiques.

GSM : Global System for Mobile Communications. Système Global pour les Communications Mobiles.

MATLAB : MATrix LABoratory. Laboratoire de Matrices.

PDF : Portable Document Format. Format de Document Portable.

PRNG : Pseudo-Random Number Generator. Générateur de Nombres Pseudo-Aléatoires.

RF : Radio Fréquence.

RNG : Random Number Generator. Générateur de Nombres Aléatoires.

SMS : Short Message Service. Service de Message Courts.

TCP/IP : Transmission Control Protocol / Internet Protocol. Protocole de Contrôle de Transmission / Protocole Internet.

WIFI : Wireless Fidelity. Fidélité sans Fil.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Au cours des dernières années, les avancées technologiques ont apporté des innovations remarquables dans divers domaines, notamment dans la sécurisation des données. Cependant, cette transformation numérique présente un défi permanent : la protection des informations. A mesure que les technologies évoluent, le volume de données générées et stockées augmente de manière exponentielle. Cette prolifération de données, bien qu'elle présente d'immenses opportunités, expose également les informations sensibles à des risques croissants de cyber attaques et de violations de données [1]. La sécurité informatique est devenue une priorité cruciale, car les cybercriminels développent constamment de nouvelles techniques pour exploiter les vulnérabilités des systèmes.

Le texte reste le moyen le plus courant pour échanger des informations, que ce soit sous forme de SMS, d'e-mails, de rapports ou de lettres. Ces communications textuelles sont omniprésentes dans notre vie quotidienne et professionnelle, facilitant la transmission rapide et efficace des informations.

Toutefois, avec l'augmentation des échanges numériques, la protection de ces données est devenue indispensable. Le chiffrement joue un rôle crucial dans cette protection en transformant les informations lisibles en un langage crypté, inaccessible à ceux qui ne possèdent pas la clé de déchiffrement appropriée [2]. Ce processus assure que les informations sensibles, telles que des rapports stratégiques ou des correspondances personnelles, restent sécurisées contre les accès non autorisées et les cybers menaces. En utilisant des techniques de chiffrement robustes, nous pouvons garantir la confidentialité et l'intégrité des communications textuelles dans notre société de plus en plus connectée.

Depuis l'antiquité, la cryptographie vise à sécuriser les informations par des méthodes de chiffrement. Les premières techniques, comme le chiffrement de César, reposaient sur des substitutions simples de lettre. Au moyen âge, des systèmes plus complexes comme le chiffrement de Vigenère sont apparus, utilisant des mots-clés pour varier les substitutions [3]. Avec

l'ère informatique, des algorithmes de chiffrement plus sophistiqués ont été développés, tels que DES [4], AES [5] et ECC.

L'utilisation des systèmes chaotiques dans les algorithmes de chiffrement ouvre de nouvelles perspectives, exploitant la nature imprévisible et pseudo-aléatoire de ces systèmes pour renforcer encore plus les méthodes de la cryptographie. La généralisation aux systèmes chaotiques d'ordre fractionnaire présente des meilleures performances et une meilleure robustesse.

Notre travail consiste à concevoir et implémenter un algorithme de chiffrement de fichiers texte reposant sur les systèmes chaotiques. Cet algorithme est composé de deux systèmes chaotiques : le système de Hénon modifié d'ordre fractionnaire et la fonction logistique d'ordre entier. Un fichiers texte sera chiffré puis enregistré dans un bloc note. L'objectif est d'avoir un algorithme robuste face aux différentes attaques et tentatives d'intrusions.

Afin de mieux illustrer notre contribution, notre mémoire est structuré comme suit :

- Dans le premier chapitre, nous abordons les concepts fondamentaux des systèmes chaotiques. Après une introduction, nous explorons plusieurs notions liées aux systèmes dynamiques, en mettant en évidence les caractéristiques distinctives des systèmes chaotiques. Nous décrivons en détails les propriétés de ces systèmes en illustrant chaque caractéristique par des exemples concrets. Enfin, nous présentons les systèmes chaotiques discrets d'ordre fractionnaire, en nous appuyant sur une modélisation spécifique qui servira de base pour représenter le générateur chaotique utilisé dans notre algorithme.

-Le deuxième chapitre explore la cryptographie chaotique et le chiffrement de fichiers texte. Nous mettons en lumière les similitudes entre les systèmes cryptographiques et les systèmes chaotiques, en soulignant l'importance de ces derniers dans la sécurité des données. Après un bref historique des origines de la cryptographie et des anciennes méthodes utilisées, nous examinons quelques techniques de chiffrement basées sur les systèmes chaotiques, en fournissant des exemples d'application à des textes. Enfin, nous proposons un algorithme de chiffrement spécifique et discutons des résultats obtenus à travers son application.

-Le troisième chapitre se penche sur les analyses de robustesses appliquées à l'algorithme de chiffrement de fichiers texte. Nous commençons par définir la notion de robustesse et exposons ses objectifs spécifiques. Ensuite, nous appliquons différentes analyses de robustesse à notre algorithme, en mettant l'accent sur l'évaluation de sa résilience face à diverses at-

taques potentielles. Nous prenons également en compte le temps d'exécution du programme et discutons de son importance dans les applications en temps réel.

Dans la conclusion générale, nous récapitulons les principaux résultats obtenus et envisageons des perspectives pour de futurs travaux dans ce domaine.

Chapitre 1

Généralités sur les systèmes chaotiques

1.1 Introduction

La théorie du chaos, l'une des disciplines scientifiques les plus modernes, s'est imposée comme l'un des secteurs les plus pointus de la recherche actuelle. Les origines de cette nouvelle théorie remontent aux débuts du $20^{ème}$ siècle dans les domaines des mathématiques et de la physique, mais elle a émergé pleinement dans les années 1960-1970 [6].

Le concept de "chaos" désigne un état particulier d'un système où le comportement ne se répète jamais et qui est extrêmement sensible aux conditions initiales [7], rendant son évolution imprédictible à long terme. Cette découverte a suscité l'intérêt de chercheurs issus de divers horizons, qui se sont interrogés sur la nature et les implications de ce phénomène. Des questions telles que la régulation des arythmies cardiaques, les fluctuations de populations animales, ou encore les mouvements sur les marchés financiers ont incité à explorer le chaos sous un angle scientifique.

Le chaos a ainsi trouvé de nombreuses applications, aussi bien dans les domaines physiques [8] que biologiques, chimiques ou économiques [9]. Dans ce contexte, nous nous focaliserons principalement dans ce chapitre sur les systèmes dynamiques chaotiques. Nous examinerons de près les concepts fondamentaux tels que les espaces de phases, les attracteurs étranges et les bifurcations, ces dernières étant des scénarios de transition vers le chaos. Notre objectif est de fournir des notions élémentaires sur les systèmes dynamiques chaotiques et leurs propriétés, permettant ainsi de mieux appréhender la nature et les manifestations du chaos, ainsi que les moyens de le quantifier.

Nous généraliserons, en outre, notre étude aux systèmes dynamiques chaotiques d'ordre fractionnaire, les raisons derrière l'utilisation des systèmes chaotiques d'ordre fractionnaire dans les systèmes de communication seront abordés ultérieurement dans ce mémoire.

1.2 Les systèmes dynamiques

Un système dynamique est un concept mathématique utilisé pour modéliser les phénomènes qui évoluent avec le temps selon des règles précises. Ces règles peuvent être représentées sous forme d'équations différentielles ou de fonctions itératives. La trajectoire d'un objet en mouvement dans le temps permet de visualiser les propriétés du système telles que les états stationnaires, les attracteurs, les points périodiques et les bifurcations.

Un système dynamique décrit par une fonction mathématique présente deux types de variables : les variables dynamiques, qui sont les quantités fondamentales qui changent avec le temps, et les variables statiques, également appelées paramètres du système, qui sont fixes.

Ce système d'équations peut être classé en deux catégories : continu et discret [10].

1.2.1 Système dynamique à temps continu

Un système dynamique continu est un système dans lequel le temps est une variable continue, et l'évolution du système est décrite par des équations différentielles ordinaires de premier ordre de la forme :

$$\frac{dx}{dt} = f(t, x) \tag{1.1}$$

avec l'état initial $x_0 = x(t_0)$.

Cette expression constitue une forme abrégée du système suivant :

$$\begin{aligned} \frac{dx_1}{dt} &= f_1(t, x_1, \ldots, x_n) \\ \frac{dx_2}{dt} &= f_2(t, x_1, \ldots, x_n) \\ &\vdots \\ \frac{dx_n}{dt} &= f_n(t, x_1, \ldots, x_n) \end{aligned} \tag{1.2}$$

où $f : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ désigne la dynamique du système, $x(t) \in \mathbb{R}^n$ est le vecteur d'état de dimension n, et $t \in \mathbb{R}^+$ représente le temps.

1.2.2 Système dynamique à temps discret

Un système dynamique discret est un système dans lequel le temps est discrétisé en pas distincts, et l'évolution du système est décrite par des équations aux différences finies, avec le modèle général suivant :

$$x(k+1) = g(k, x(k)) \tag{1.3}$$

où $g : \mathbb{Z}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ désigne la dynamique du système en temps discret.

1.3 Définition d'un système dynamique chaotique

Les systèmes chaotiques sont les systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses. Ils sont très sensibles aux conditions initiales [7], ce qui signifie que deux conditions initiales très proches conduisent à deux trajectoires qui s'éloignent rapidement l'une de l'autre.

Ces systèmes peuvent sembler aléatoires, mais en réalité, leur comportement est déterministe, ce qui signifie qu'il est entièrement régi par un ensemble d'équations ou de règles [11].

1.4 Propriétés d'un système chaotique

Il existe plusieurs définitions possibles du chaos. Même si les approches varient en fonction du contexte, elles convergent toutes vers certains points communs caractérisant les systèmes chaotiques, comme la sensibilité extrême aux conditions initiales, le comportement apparemment aléatoire, et la présence de structures complexes. Ci-dessous, nous présentons d'une manière succincte quelques caractéristiques qui permettent de mieux comprendre les points marquants d'un système chaotique [12].

1.4.1 Non linéarité

La non-linéarité est une condition nécessaire, mais non suffisante pour que le chaos se manifeste dans un système. Ainsi, le comportement chaotique doit provenir d'un système non linéaire, mais la non-linéarité ne rend pas nécessairement un système chaotique. Lorsque des non-linéarités sont présentes, plusieurs caractéristiques peuvent apparaître, telles que les cycles limites ou les tores de différents ordres. [13].

1.4.2 Déterminisme

Le comportement chaotique d'un système est le résultat de processus déterministes gouvernés par une ou plusieurs équations, excluant toute intervention aléatoire. Les états passés, présents et futurs du système sont régis par des lois déterministes.

Bien que le déterminisme soit présent dans les systèmes dynamiques chaotiques, il peut y avoir une limite pratique à la prédictibilité en raison de la sensibilité aux conditions initiales et de la complexité des dynamiques. Cela signifie que, même si le comportement global du système est déterminé, les prédictions précises à long terme peuvent être impossibles en raison de la difficulté à connaître les conditions initiales avec une précision suffisante.

1.4.3 Sensibilité aux conditions initiales

Les systèmes chaotiques sont extrêmement sensibles aux conditions initiales. De petites variations dans l'état initial peuvent entraîner des trajectoires complètement différentes au fil du temps [7].

Afin de souligner cette propriété, prenons comme exemple le système de Lorenz. Les équations qui régissent l'évolution de ce système sont les suivantes :

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{1.4}$$

Où σ, ρ, et β sont des paramètres du système. Ces équations montrent comment les variables x, y, et z évoluent au fil du temps.

Nous considérons deux conditions initiales très proches :

- $x_0 = 0.1$
- $x_0 = 0.1 + \epsilon$, avec $\epsilon = 0.0005$

La figure (1.1) illustre le phénomène de sensibilité aux conditions initiales pour des valeurs très proches. Dans un premier temps, l'évolution des deux trajectoires correspondantes aux deux états initiaux très proches, est quasiment la même, mais très vite, elle devient différente et les deux trajectoires divergent.

En utilisant ces équations avec les conditions initiales très proches, on peut observer comment des trajectoires initialement similaires finissent par diverger de manière significative, illustrant ainsi la sensibilité aux conditions initiales caractérisant des systèmes chaotiques.

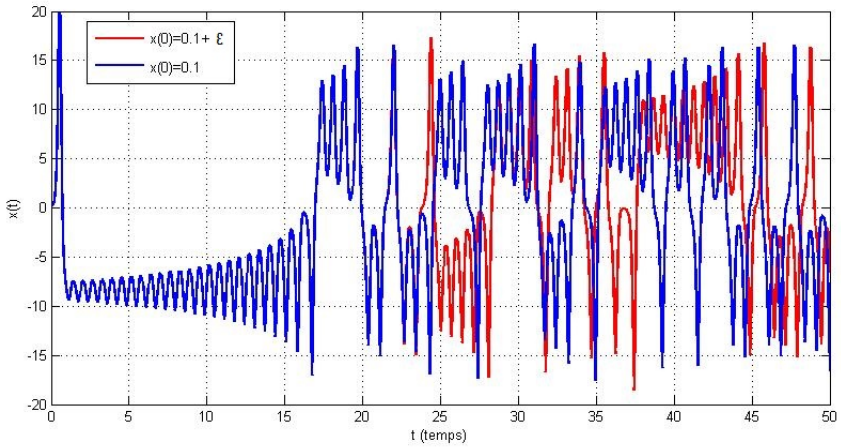


FIGURE 1.1 – Sensibilité aux conditions initiales de l'état x du système de Lorenz.

1.4.4 Aspect aléatoire

Les systèmes chaotiques démontrent un comportement qui semble souvent aléatoire. Cette allure aléatoire découle de notre incapacité à fournir une description mathématique complète de leur évolution.

Cependant, derrière cette apparence d'imprévisibilité se cachent des équations non linéaires parfaitement déterministes.

La figure (1.2) représente l'aspect aléatoire de l'état x du système de Lorenz. On peut observer que le comportement semble aléatoire.

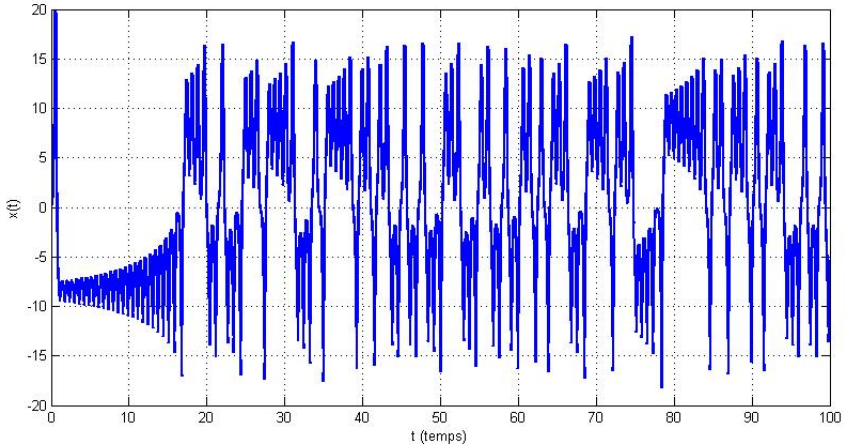


FIGURE 1.2 – Aspect aléatoire de l'état x du système de Lorenz.

1.4.5 Attracteur étrange

Un attracteur dans l'espace des phases est un objet géométrique vers lequel tendent les trajectoires de points de cet espace. Il représente les états vers lesquels évolue un système dynamique à partir d'un ensemble donné de conditions initiales. Plusieurs attracteurs peuvent coexister dans le même espace de phases. On distingue deux catégories principales d'attracteurs : les attracteurs réguliers (point fixe, cycle limite, tore) et les attracteurs étranges (chaotiques) [14]. Le terme "attracteur étrange" a été introduit par David Ruelle et Floris Takens en 1971 [15], pour décrire des attracteurs résultant de bifurcations dans des systèmes dynamiques complexes. Avant leurs travaux, les attracteurs étaient peu étudiés. Les attracteurs étranges se distinguent par leur dimension fractale et leur comportement complexe. Un exemple célèbre est l'attracteur de Lorenz, souvent représenté sous la forme d'ailes de papillon, devenu un symbole de la théorie du chaos. Les caractéristiques de l'attracteur étrange sont alors :

• Contenu dans un espace fini : Les attracteurs étranges ont un volume nul et une dimension fractale.

• Trajectoires complexes : Les trajectoires ne repassent jamais deux fois par le même point (apériodicité).

• Sensibilité aux conditions initiales : Les trajectoires proches divergent de manière exponentielle.

• Bassin d'attraction : Toute condition initiale située dans cette région mène à une trajectoire spécifique sur l'attracteur.

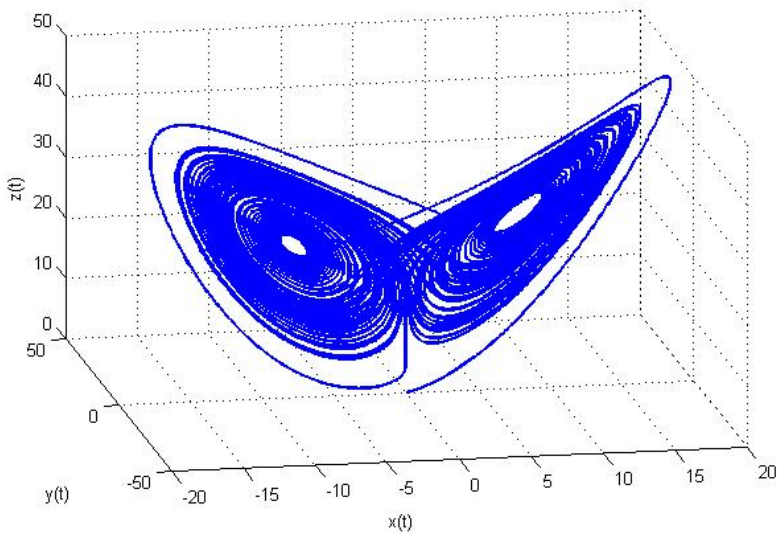


FIGURE 1.3 – Attracteur chaotique étrange de Lorenz.

La figure (1.3) montre l'attracteur chaotique étrange de Lorenz obtenu en espace de phase des états x, y et z, avec les conditions initiales $x_0 = 0.1$; $y_0 = 0.1$ et $z_0 = 0.1$.

La dimension fractale : est une mesure utilisé pour décrire et caractériser des objets ou des phénomènes qui présentent une complexité auto-similaire à différentes échelles, telles que les nuages et les attracteurs étranges.

1.4.6 Spectre de fréquence

Le spectre de fréquence caractérise la nature du système, qu'il soit périodique, apériodique ou chaotique.

Dans le cas des signaux chaotiques, il peut présenter une distribution continue de fréquences sans pics clairs, correspondant à une évolution désordonnée.

Ce type de spectre est souvent difficile à différencier de celui d'un bruit blanc.

La figure (1.4) représente le spectre de fréquence de l'état x du système de Lorenz. Lorsque le système de Lorenz présente un comportement chaotique, son spectre de fréquence est très complexe, caractérisé par une distribution continue de fréquences sans pics clairs.

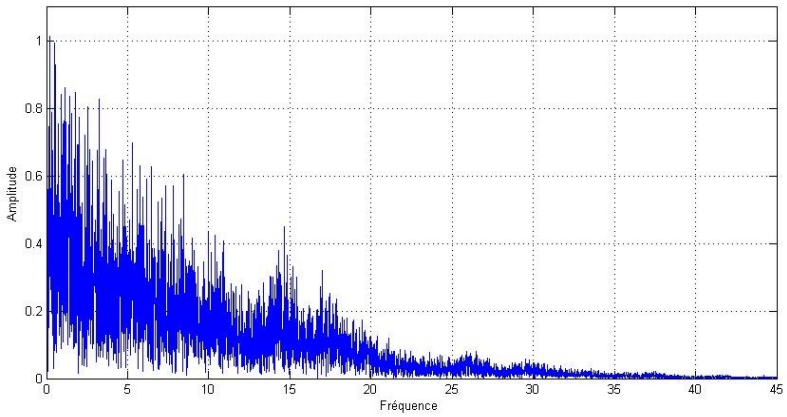


FIGURE 1.4 – Spectre de fréquence de l'état x dans le système de Lorenz.

1.4.7 Les exposants de Lyapunov

Les exposants de Lyapunov sont des coefficients qui permettent de quantifier la vitesse à laquelle deux trajectoires initialement proches dans l'espace des phases d'un système dynamique s'écartent l'une de l'autre au fil du temps. Ces exposants peuvent être positifs, nuls ou négatifs, et ils fournissent des informations cruciales sur le comportement à long terme d'un système dynamique.

Si un exposant de Lyapunov est positif, cela suggère que les trajectoires initialement proches divergeront exponentiellement, indiquant un comportement chaotique dans le système. À l'inverse, si un exposant de Lyapunov est négatif, cela indique que les trajectoires initialement proches convergeront, ce qui signifie que le système est stable. Si tous les exposants de Lyapunov sont nuls, cela peut indiquer un comportement neutre, bien que cela soit rare. Pour un comportement périodique, un exposant de Lyapunov est nul et les autres sont négatifs, tandis que pour un comportement quasi périodique, plusieurs exposants peuvent être nuls, mais il y a généralement des exposants négatifs également [10].

Le tableau suivant résume les différentes configurations d'exposants de Lyapunov :

Type d'attracteur	**Exposants de Lyapunov**
Point d'équilibre	$0 > \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$
Cycle limite	$\lambda_1 = 0, 0 > \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_n$
Tore d'ordre 2	$\lambda_1 = \lambda_2 = 0, 0 > \lambda_3 \geq \lambda_4 \geq \cdots \geq \lambda_n$
Tore d'ordre k	$\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0, 0 > \lambda_{k+1} \geq \lambda_{k+2} \geq \cdots \geq \lambda_n$
Attracteur chaotique	$\lambda_1 > 0, \sum_{i=1}^{n} \lambda_i < 0$
Attracteur hyper-chaotique	$\lambda_1 > 0, \lambda_2 > 0, \sum_{i=1}^{n} \lambda_i < 0$

TABLE 1.1 – Exposants de Lyapunov pour différents types d'attracteurs

1.5 Routes vers le chaos

Le chaos survient en raison d'une instabilité liée à la présence d'un paramètre de contrôle dans les équations d'évolution. La variation quantitative de ces paramètres entraîne un changement qualitatif ou une division dans le comportement du système. Les valeurs des paramètres de contrôle pour lesquelles le système passe vers un régime chaotique sont appelées valeurs de bifurcation.

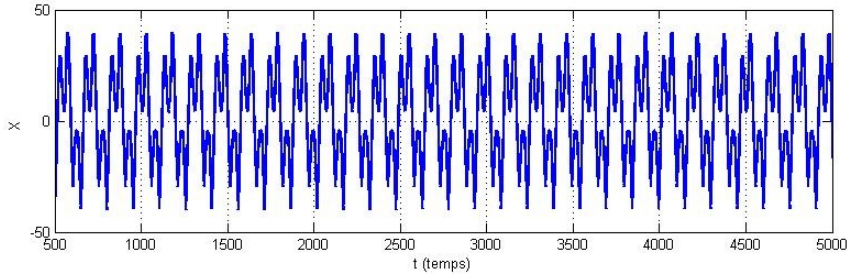
La théorie des bifurcations en général fournit un cadre mathématique puissant pour comprendre les changements qualitatifs dans les systèmes dynamiques [16].

Les graphiques qui illustrent ces ramifications sont appelés diagrammes de bifurcation, comme montré dans la figure (1.6) . Ils sont utilisés pour étudier les dynamiques des systèmes en fonction des paramètres de contrôle, à long terme [17].

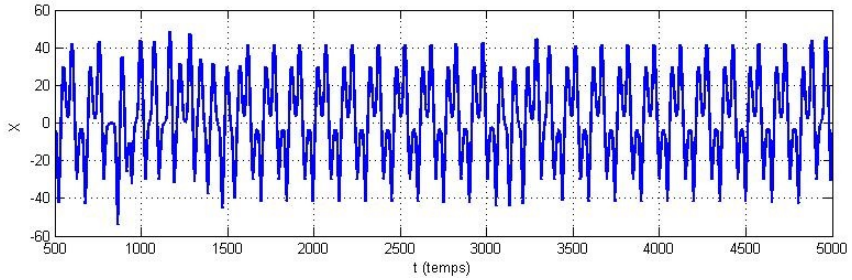
Bien que le chaos puisse émerger de différentes manières dans divers systèmes dynamiques, trois scénarios universels ou types de bifurcations sont souvent observés.

1.5.1 L'intermittence

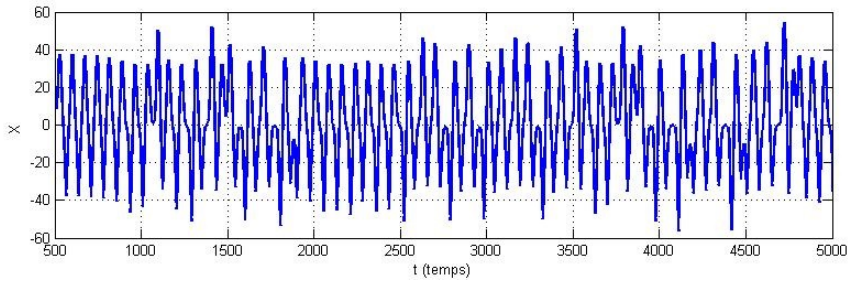
Dans le phénomène d'intermittence, chaque évolution du paramètre de contrôle entraîne des séquences chaotiques entrecoupant un régime périodique stable. À chaque augmentation du paramètre de bifurcation, le comportement chaotique dure plus longtemps, jusqu'à ce qu'il atteigne un seuil critique où le système reste chaotique.



(a) $\rho* = 160$



(b) $\rho* = 166$



(c) $\rho* = 190$

FIGURE 1.5 – Transition vers le chaos par intermittence

Prenons par exemple le modèle de Lorenz dans lequel on remplace le paramètre $\rho = 28$ par un autre ρ^* variant autour de la valeur critique $\rho^* = 166$. Dans la figure (1.5) , on peut voir que pour la valeur $\rho^* = 160$, l'évolution de la variable x montre un comportement périodique. Après la valeur critique, on commence à observer un léger mouvement qui semble aléatoire. Si ρ^* continue d'augmenter, les perturbations deviennent de plus en plus riches en fréquence. Finalement, pour une certaine valeur suffisante de ρ^*, ($\rho^* \geq 167$), l'évolution de l'état x apparaît complètement aléatoire, indiquant un comportement chaotique.

L'intermittence est souvent connue comme la route de Pomeau-Manneville vers le chaos, en référence aux physiciens français Yves Pomeau et Paul Manneville qui l'ont constatée en premier en 1980 [18].

1.5.2 Doublement de périodes

L'augmentation du paramètre de contrôle d'un système conduit le régime périodique vers un doublement de périodes qui se multiplie indéfiniment. Le régime devient apériodique jusqu'à ce qu'il atteigne un régime chaotique. Ce scénario vers le chaos est appelé la route de Feigenbaum [19].

La figure (1.6) illustre comment une simple équation non linéaire peut donner lieu à des dynamiques extrêmement complexes, allant de la stabilité à des comportements chaotiques via une série de bifurcations périodiques.

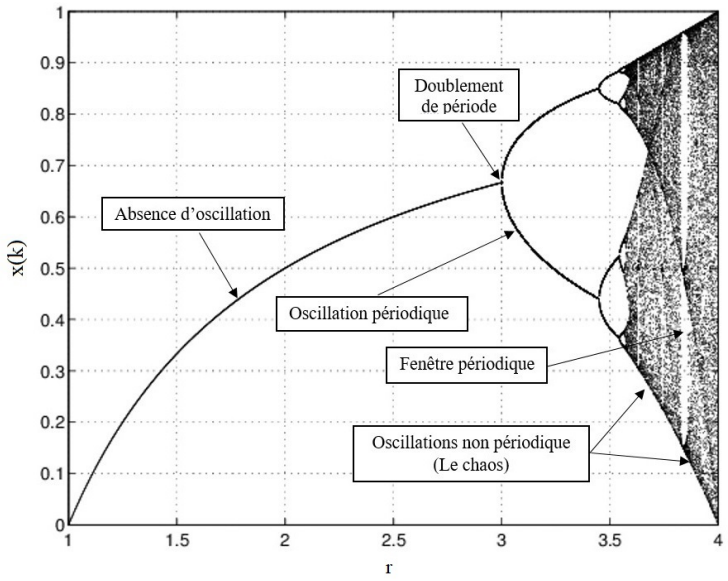


FIGURE 1.6 – Diagramme de bifurcation de la fonction logistique.

On peut distinguer cinq dynamiques différentes :

— Absence d'oscillation ($r < 3$) : la dynamique de système est périodique et stable.

— Oscillation périodique ($3 < r < 3.4$) : la région ou se produit le premier doublement de périodes.

— Doublement de période : On observe une série de bifurcations où le nombre de points dans l'orbite périodique double (passant de 2 à 4, puis 8, ...)

— Fenêtre périodique : il existe des fenêtres où des comportements périodiques réapparaissent avant de retomber dans le chaos.
— Oscillation non périodiques ($r > 3.57$) : le système entre dans un régime chaotique, les valeurs de l'état x deviennent imprévisibles et très sensibles aux conditions initiales, ce qui est caractéristique du chaos.

1.5.3 La quasi-périodicité

Cette route vers le chaos est un concept qui se situe entre la périodicité et l'irrégularité totale. Elle se réfère à des comportements qui semblent périodiques à première vue, mais qui présentent en réalité une légère variation dans leur périodicité. Chaque changement d'un paramètre dans ce système périodique provoque une autre fréquence, jusqu'au chaos. Le rapport entre une fréquence et une autre est irrationnel.

Cette route est appelée la route de Ruelle-Takens-Newhouse vers le chaos [20].

1.6 Exemples de systèmes chaotiques

La génération des signaux chaotiques repose sur divers systèmes dynamiques. En continu, un système chaotique, sans entrée ni retard, doit posséder au moins trois états. En revanche, dans le domaine discret, un système dynamique à un seul état, tel que la fonction logistique peut exhiber du chaos.

Dans cette partie, nous considérons deux cas de systèmes chaotiques : un système chaotique continu, et un autre discret. Ces deux cas illustrent la diversité des systèmes chaotiques et mettent en lumière leurs particularités dans les deux domaines, continu et discret.

1.6.1 Système chaotique continu

Le système chaotique continu se réfère à des comportements chaotiques observés dans les systèmes dynamiques continus, où les variables d'état évoluent de manière continue dans le temps.

Parmi les systèmes chaotiques continus, on compte le système de Lorenz, le système de Chen et le système de Rössler. Dans ce qui suit, nous étudierons le système de Chen et présenterons ses différentes propriétés.

Le système de Chen, découvert par Guanrong Chen en 1999 est constitué de trois équations différentielles ordinaires non linéaires, similaires à celles du système de Lorenz, mais avec une structure et dynamique légèrement différente [21].

Les équations du système de Chen sont les suivantes :

$$\begin{aligned} \frac{dx}{dt} &= a(y-x) \\ \frac{dy}{dt} &= (c-a)x - xz + cy \\ \frac{dz}{dt} &= xy - bz \end{aligned} \tag{1.5}$$

Où x, y et z sont les variables d'état du système, et a, b et c sont ces paramètres de contrôle. Pour les valeurs $a = 35$, $b = 3$ et $c = 28$, le système de Chen présente un comportement chaotique.

La figure (1.7) présente l'attracteur chaotique étrange, observé dans l'espace de phase des états x, y et z, résultant de l'initialisation du système avec les conditions $((x_0, y_0, z_0) = (0.1, 0.1, 0.1))$ et en considérant les valeurs des paramètres mentionnées ci-dessus.

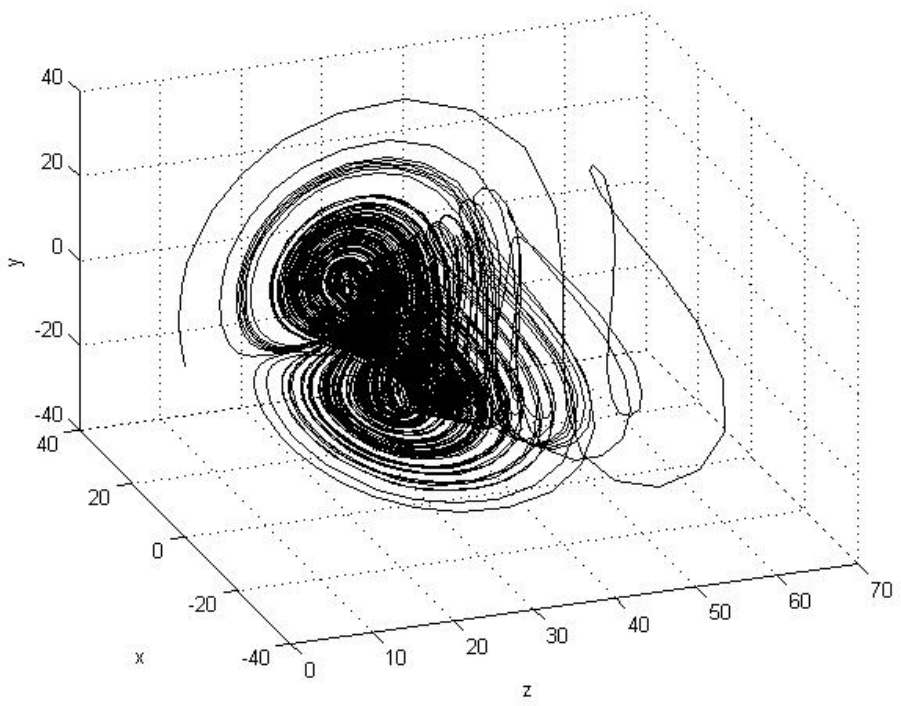


FIGURE 1.7 – Attracteur chaotique étrange de Chen.

La figure (1.8) montre l'évolution chaotique des états x, y et z du système de Chen en fonction de temps.

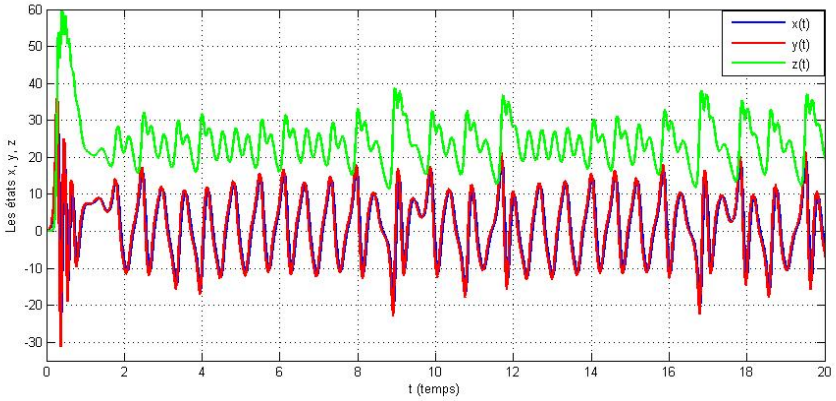


FIGURE 1.8 – Aspect aléatoire des états x, y et z du système de Chen.

1.6.2 Système chaotique discret

Les systèmes chaotiques discrets sont des systèmes dynamiques caractérisés par un comportement imprévisible et complexe, malgré leur définition déterministe et leur simplicité apparente. Ils sont décrits par des équations de récurrence discrètes.

Le système de Hénon, la fonction logistique et le système de Lozi sont tous des systèmes chaotiques discrets.

Dans cette partie, nous prendrons la fonction logistique découverte par Pierre-François Verhulst en 1844. Cette fonction permet de prévoir l'évolution d'une population à partir de la simple connaissance de l'effectif à trois dates différentes. Cela signifie qu'en ayant les données de la population à ces trois moments, on peut déterminer les paramètres de la fonction logistique. Une fois ces paramètres déterminés, on peut utiliser la fonction pour prévoir les effectifs de la population à d'autres moments dans le futur [22].

L'équation de la fonction logistique est donnée par :

$$w_{k+1} = R \cdot w_k \cdot (1 - w_k) \tag{1.6}$$

w_k : la valeur de la séquence à l'étape k.
R : le paramètre de croissance.

Ce système présente un comportement chaotique pour $R = 3.9$, avec une valeur initiale $w_0 = 0.5$, obtenu dans l'espace de phase de l'états w en trois moments différents $w(k)$, $w(k+1)$ et $w(k+2)$.

La figure (1.9) représente l'attracteur étrange de la fonction logistique pour $R = 4$.

La figure (1.10) illustre l'évolution chaotique de l'état w de la fonction logistique.

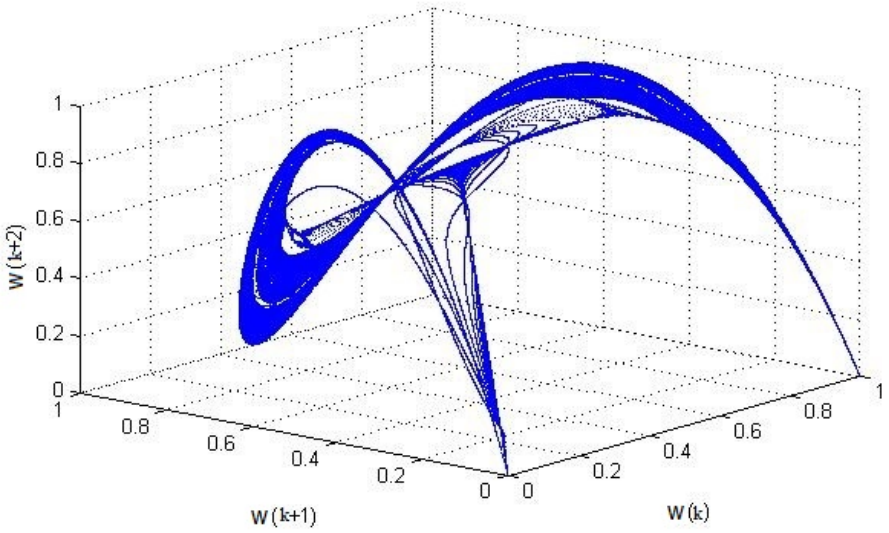


FIGURE 1.9 – Attracteur étrange de la fonction logistique.

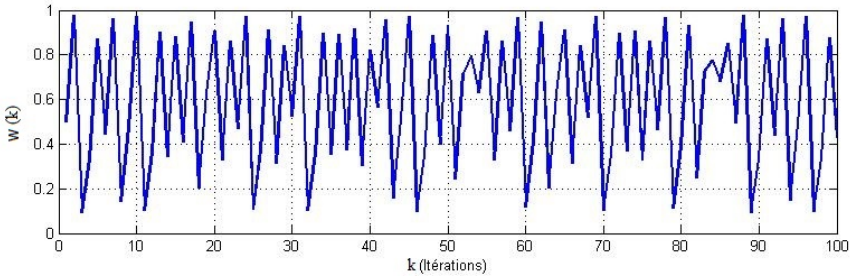


FIGURE 1.10 – Evolution chaotique de la fonction logistique.

1.7 Les systèmes chaotiques d'ordre fractionnaire

Le calcul fractionnaire, une extension du calcul d'ordre entier à un calcul d'ordre non entier, trouve son origine dès le $17^{ème}$ siècle avec des esprits éclairés telles que Leibniz et Euler. Malgré son potentiel conceptuel précoce, les limitations techniques ont entravé son exploration pendant près de trois siècles. Les contributions de mathématiciens tels que Liouville, Riemann et Caputo ont progressivement développé les fondements théoriques du calcul fractionnaire, ouvrant la voie à son application pratique.

L'émergence du calcul fractionnaire dans le domaine de l'ingénierie a été facilitée par des développements tels que le calcul opérationnel d'Heaviside, permettant de résoudre des problèmes d'équations différentielles liés à la diffusion. Depuis les années 1970, des chercheurs comme Oldham et Spanier ont exploré les implications physiques du calcul fractionnaire, mettant en évidence son importance croissante dans des domaines tels que l'automatique, la thermique, l'électricité, la physique, l'ingénierie et la théorie du chaos.

En particulier, le calcul fractionnaire a été identifié comme un outil prometteur pour la transmission sécurisée de données basée sur des systèmes chaotiques.

1.7.1 Représentation des systèmes discrets d'ordre fractionnaire

Plusieurs définitions ont été proposées pour représenter un système discret d'ordre fractionnaire. Nous citerons ci-après les trois définitions les plus utilisées.

1.7.1.1 Définition de Riemann-Liouville

La notation "Riemann-Liouville" fait référence à deux mathématiciens, Georg Friedrich Bernhard Riemann et Joseph Liouville, qui ont tous deux contribué à la théorie des intégrales [23].

La différence d'ordre fractionnaire au sens de Riemann-Liouville est formulée comme suit :

$$a\Delta^{\alpha}_{RL} f(t) = a\Delta^{m}(\Delta^{-(m-\alpha)} f)(t) \tag{1.7}$$

où α est l'ordre fractionnaire.
m est un entier positif.

1.7.1.2 Définition de Caputo

La notation "Caputo" fait référence à Michele Caputo, un mathématicien italien qui a introduit une généralisation de la dérivation d'ordre fractionnaire pour les équations différentielles [24].

$$(a\Delta^{\alpha}_{C} f)(t) = a\Delta^{(\alpha-m)}(\Delta^{m} f)(t) = \frac{1}{\Gamma(m-\alpha)} \sum_{s=a}^{t-(m-\alpha)} (t-s-1)^{(m-\alpha-1)} (\Delta^{m} f)(s) \tag{1.8}$$

où α est l'ordre de différence.

m est un entier positif.

Γ est la fonction gamma présenté comme suit :

$$\Gamma(z) = \int_{0}^{\infty} t^{z-1} e^{-t}\, dt \tag{1.9}$$

1.7.1.3 Définition de Grünwald-Letnikov

Les différences d'ordre fractionnaire de Grünwald-Letnikov sont une méthode pour définir des dérivées d'ordre fractionnaire discrètes, analogues aux dérivées d'ordre entier classiques.

Cette méthode a été proposée par les mathématiciens allemand Ernst Grünwald et le russe Anatoly Letnikov [25].

La différence de Grünwald-Letnikov d'ordre fractionnaire est définie ci-dessous :

$$\Delta^{\alpha}x(k) = \sum_{j=0}^{\alpha}(-1)^{j}\binom{\alpha}{j}x(k-j) \tag{1.10}$$

où $\alpha \in R$ est l'ordre fractionnaire.

En appliquant cette limitation dans notre cas, nous obtenons l'approximation suivante

$$x(k+1) = f(k) + (\alpha-1)x(k) - \sum_{p=1}^{L} C_p x(k-p) \tag{1.11}$$

où $f(k)$ est une fonction de k, $x(k)$ est la valeur de la séquence à l'instant k, α est un paramètre, et C_p sont les coefficients de pondération définis comme :

$$C_p = (-1)^{p+1}\binom{\alpha}{p+1} \tag{1.12}$$

avec la définition de $\binom{\alpha}{j}$ est donnée par :

$$\binom{\alpha}{j} = \begin{cases} 1 & \text{si } j = 0 \\ \frac{\alpha(\alpha-1)\ldots(\alpha-j+1)}{j!} & \text{si } j > 0 \end{cases} \tag{1.13}$$

1.7.2 Modélisation d'un système chaotique discret d'ordre fractionnaire

Prenons exemple le système du Hénon modifié que nous utiliserons dans notre algorithme de chiffrement et qui est donné par le système d'équations suivant :

$$\begin{aligned} x(k+1) &= A - y(k)^2 - B \cdot z(k) \\ y(k+1) &= x(k) \\ z(k+1) &= y(k) \end{aligned} \tag{1.14}$$

où $x(k)$, $y(k)$ et $z(k)$ représentent les variables d'état à l'instant k, et A et B sont des paramètres du système.

En appliquant l'approximation de Grünwald-Letnikov, le système d'ordre fractionnaire correspondant est donné comme suit :

$$\begin{aligned} x(k+1) &= A - y^2(k) - Bz(k) + (\alpha_1 - 1)x(k) + \sum_{p=1}^{L} C_{p1}x(k-p) \\ y(k+1) &= x(k) + (\alpha_2 - 1)y(k) + \sum_{p=1}^{L} C_{p2}y(k-p) \\ z(k+1) &= y(k) + (\alpha_3 - 1)z(k) + \sum_{p=1}^{L} C_{p3}z(k-p) \end{aligned} \tag{1.15}$$

avec :

$$0 < \alpha_i \leq 1; \quad i = 1..3$$

L : taille de la mémoire.

Attracteur étrange

La figure (1.11) montre l'attracteur étrange du système de Hénon modifié d'ordre fractionnaire en plan de phase des états x et z, en prenant compte des conditions initiales $x_0 = 0.1$, $y_0 = 0.1$ et $z_0 = 0.1$ et les paramètres de contrôle $A = 1.65$ et $B = 0.1$.

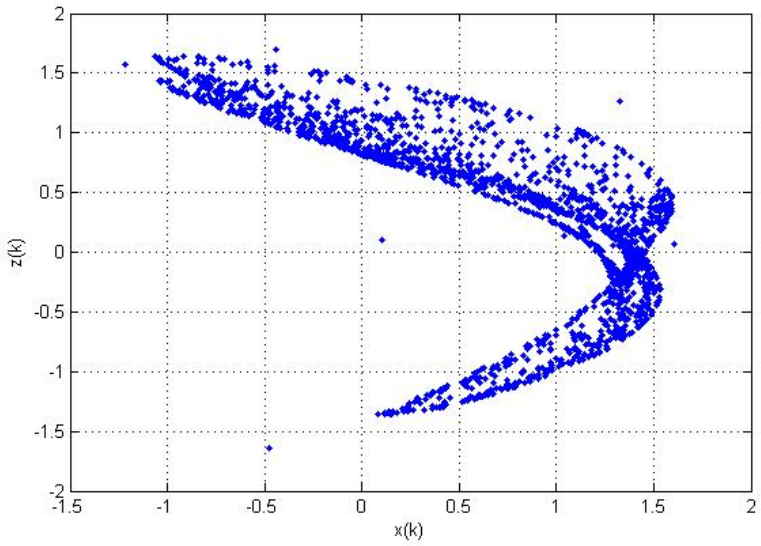


FIGURE 1.11 – Attracteur étrange du système de Hénon modifié d'ordre fractionnaire.

L'évolution des états du système

La figure (1.12) illustre l'évolution chaotique des états x, y et z de système de Hénon modifié d'ordre fractionnaire, avec les conditions initiales citées ci-dessus.

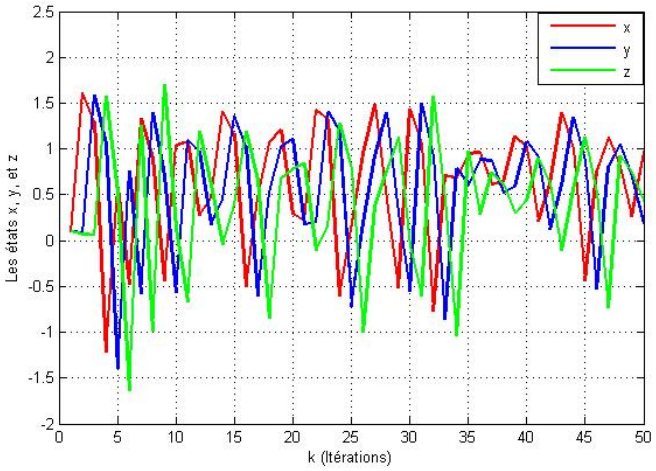


FIGURE 1.12 – L'évolution chaotiques des états du système de Hénon modifié d'ordre fractionnaire.

1.8 Conclusion

Dans ce chapitre, nous avons exploré la théorie du chaos, en définissant les propriétés clés des dynamiques chaotiques, telles que la sensibilité aux conditions initiales, les exposants de Lyapunov, les diagrammes de bifurcation, l'aspect aléatoire et l'attracteur étrange. Ces concepts ont été illustrés à travers des exemples de systèmes chaotiques à temps continu et discret, tels que le système de Lorenz, la fonction logistique et le système de Chen.

Nous avons examiné les concepts fondamentaux des différences d'ordre fractionnaire dans le cadre discret. Nous avons cité les définitions de Riemann-Liouville, de Caputo et celle de Grünwald-Letnikov que nous avons utilisée par la suite pour modéliser un système chaotique d'ordre fractionnaire. Le système de Hénon modifié d'ordre fractionnaire a été étudié comme exemple.

L'application des systèmes chaotiques en cryptographie repose sur l'exploitation des propriétés uniques du chaos pour renforcer la sécurité des données. Les systèmes chaotiques, avec leur sensibilité extrême aux conditions initiales et leur capacité à générer des séquences d'allures aléatoires, offrent un potentiel significatif pour le chiffrement des informations.

Dans le prochain chapitre, nous introduirons la notion de cryptographie et présenterons les différents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques. Nous démontrerons comment ces propriétés chaotiques peuvent être exploitées pour concevoir des algorithmes de chiffrement robustes et sécurisés, transformant ainsi notre compréhension théorique du chaos en applications pratiques pour la protection des communications et des données.

Chapitre 2

Cryptographie chaotique et application au chiffrement de fichiers texte

2.1 Introduction

Dans un monde où la numérisation a envahi tous les secteurs, garantir la confidentialité, l'intégrité et l'authenticité des données sensibles est devenu crucial. Il existe plusieurs méthodes et techniques qui servent à assurer la protection des informations numériques. L'étude et la pratique de ces dernières s'inscrivent dans le domaine de la cryptologie. Elle se divise en deux branches principales : la cryptographie et la cryptanalyse. La cryptographie protège les données en les rendant illisibles pour les personnes non autorisées, tandis que la cryptanalyse étudie les attaques contre les mécanismes de cryptographie, et analyse les réactions face aux tentatives non autorisées d'accès à des informations sécurisées sans les clés nécessaires.

L'utilisation des systèmes chaotiques caractérisés par leur sensibilité aux conditions initiales et leur comportement imprévisible pour le chiffrement„ qualifiée de cryptographie chaotique, offre une robustesse accrue contre les attaques et peut s'avérer plus efficace que les méthodes traditionnelles.

Ce chapitre explorera en profondeur les concepts, les algorithmes et les applications de la cryptographie chaotique. Nous apporterons une vision sur la cryptographie chaotique, présenterons un état de l'art, citerons les méthodes de chiffrement de texte existantes et et conclurons par une application.

2.2 État de l'art

Depuis des millénaires, la cryptographie visant à sécuriser les informations par des méthodes de chiffrement, possède une histoire riche [26]. Les premières traces de cryptographie remontent à l'Antiquité, avec des exemples trouvés sur des tables d'argile près du Tigre en Irak. Vers 500 avant Jésus-Christ, les anciens Hébreux utilisaient des techniques simples comme le chiffre d'Atbash. Les Grecs, employaient le seytale qui est une méthode de transposition. Environ 150 ans avant Jésus-Christ, l'historien grec Polybe inventa le carré de Polybe, un autre procédé de chiffrement par substitution. Au premier siècle avant Jésus-Christ, Jules César utilisait une substitution fixe, connue sous le nom de chiffre de César. Au $XIV^{ème}$ siècle, Léon Battista Alberti, inventa un cadran chiffrant pour des substitutions plus complexes. En 1586, Blaise de Vigenère introduisit le chiffre de Vigenère, utilisant une clé littérale pour déterminer les décalages alphabétiques.

Le $XX^{ème}$ siècle marqua une avancée significative avec le masque jetable introduit par Gilbert S. Vernam en 1917. En 1918, Arthur Scherbius inventa la machine Enigma, utilisée par l'Allemagne pendant la Seconde Guerre mondiale. Cette machine combinait plusieurs rotors pour créer des substitutions complexes. En 1929, Lester S. Hill publia le chiffre polygraphique utilisant des matrices et des vecteurs [27]. Claude Shannon, en 1948, transforma la cryptographie avec sa théorie de l'information [28].

Les années 1990 virent l'émergence de la cryptographie basée sur le chaos, et de la cryptographie quantique [29], [30], exploitant les propriétés de la physique quantique pour offrir une sécurité renforcée par la distribution quantique des clés. Ainsi, la cryptographie a évolué de techniques rudimentaires à des systèmes mathématiquement sophistiqués et technologiquement avancés, s'adaptant continuellement aux défis de chaque époque.

2.3 Cryptographie chaotique

La cryptographie signifie dans la littérature 'écriture des secrets'. Scientifiquement, c'est l'étude des méthodes permettant de préserver des données de manière confidentielle et sécurisée.

L'utilisation des systèmes chaotiques pour chiffrer les informations ou les données sensibles est un sujet d'étude suscitant un intérêt croissant depuis quelques décennies, en raison des propriétés distinctes (comportement non divergent, apériodicité, grande sensibilité, etc.)des systèmes chaotiques.

Le processus commence par la génération de séquences pseudo-aléatoires à partir d'équations chaotiques, telles que la fonction logistique ou le système de Lorenz. Ces séquences sont

ensuite utilisées comme clés pour chiffrer les données. Par exemple, les valeurs générées par une équation chaotique peuvent être appliquées à des blocs de texte clair en les combinant via des opérations telles que l'addition, le modulo ou le OU-Exclusif (XOR), produisant ainsi du texte chiffré difficile à prédire sans connaître les conditions initiales exactes et les paramètres du système chaotique. Cette méthode exploite la sensibilité aux conditions initiales et la dynamique complexe des systèmes chaotiques pour renforcer la sécurité du chiffrement.

Ces méthodes de cryptage sont donc utilisés pour masquer les informations sensibles, les faisant apparaître comme un bruit pseudo-aléatoire.

L'utilisation combinée de ces deux éléments, les systèmes cryptographiques et les systèmes chaotiques, assure une meilleure confidentialité et sécurité [31].

2.4 Similarités entre un système cryptographique et un système chaotique

Les systèmes cryptographiques et les systèmes chaotiques partagent plusieurs similarités importantes, particulièrement en ce qui concerne leurs propriétés dynamiques et leurs comportements pseudo-aléatoire.

2.4.1 Dynamique déterministe / Pseudo-aléatoire déterministe

Les systèmes chaotiques et les systèmes cryptographiques partagent la propriété de dynamique déterministe et de pseudo-aléatoire déterministe. Les systèmes chaotiques, bien que déterministes, produisent des comportements qui apparaissent aléatoires en raison de leur sensibilité aux conditions initiales. De même, un système cryptographique doit générer des sorties pseudo-aléatoires à partir d'entrées déterministes, telles que le texte clair et la clé de chiffrement, rendant ainsi les schémas de chiffrement imprévisibles [32].

2.4.2 Transformation non linéaire

Les deux domaines, théorie du chaos et cryptographie, utilisent des transformations non linéaires pour ajouter de la complexité et rendre les données difficilement prédictibles. Dans les systèmes chaotiques, ces transformations décrivent l'évolution des états du système de manière non linéaire, créant des comportements complexes et imprévisibles. En cryptographie, ces transformations modifient les données pour renforcer la confidentialité des informations, en rendant la relation entre le texte clair et le texte chiffré extrêmement difficile à analyser [33].

2.4.3 Conditions initiales et paramètres / Clé(s)

Dans les deux domaines de théorie du chaos et de cryptographie, les conditions initiales ou les paramètres (comme les clés) contrôlent le comportement du système ou de l'algorithme. Dans les systèmes chaotiques, des conditions initiales légèrement différentes peuvent conduire à des trajectoires complètement différentes. En cryptographie, les clés de chiffrement assurent la sécurité en contrôlant la transformation du texte clair en texte chiffré, garantissant ainsi la confidentialité des données [34].

2.4.4 Sensibilité aux conditions initiales et aux paramètres / Diffusion

La similitude entre les systèmes chaotiques et les systèmes cryptographiques réside dans la sensibilité aux conditions initiales et la propriété de diffusion. Dans un système chaotique, de petites variations initiales entraînent des différences majeures dans le comportement du système. En cryptographie, de légères modifications dans le texte clair ou la clé génèrent des altérations significatives et apparemment aléatoires dans le texte chiffré, un principe connu sous le nom d'effet d'avalanche [35].

2.4.5 Ergodicité / Confusion

L'ergodicité dans les systèmes chaotiques assure une exploration exhaustive et uniforme de l'espace des états, garantissant que toutes les configurations possibles sont atteintes au fil du temps. En cryptographie, la confusion vise à rendre la relation entre le texte clair et le texte chiffré aussi complexe que possible, empêchant ainsi le déchiffrement non autorisé. Les deux concepts, bien que distincts dans leurs domaines respectifs, partagent l'objectif d'assurer une certaine forme de désordre contrôlé pour des applications spécifiques .

2.4.6 Itérations / Rounds

Dans les deux cas, le principe d'appliquer un processus de transformation de manière répétée est partagé. Ce processus itératif amplifie la complexité du système, rendant les prédictions et les analyses beaucoup plus difficiles. Dans un système chaotique, cela conduit à un comportement imprévisible. Dans un système cryptographique, cela augmente la sécurité en rendant le texte chiffré difficile à décrypter sans la clé appropriée.

2.4.7 Structure complexe / Complexité de l'algorithme

La complexité est un facteur clé pour les systèmes chaotiques et cryptographiques. Dans les systèmes chaotiques, une structure complexe permet de rendre les prédictions sur l'évolution du système très difficiles. De même, en cryptographie, une complexité algorithmique élevée rend le décryptage sans la clé extrêmement difficile, augmentant ainsi la sécurité des communications.

2.4.8 Ensemble de nombres réels / Ensemble fini d'entiers

Dans les systèmes chaotiques, l'espace de phase est souvent un ensemble de nombres réels, permettant une représentation continue des états possibles du système. En cryptographie, l'espace de phase est généralement un ensemble fini d'entiers, comme les bits dans un système numérique. Bien que l'un soit continu et l'autre discret, les deux types d'espaces de phase permettent d'explorer toutes les configurations possibles du système, assurant ainsi une couverture complète de leurs dynamiques respectives.

Ci-dessus la correspondance entre la théorie du chaos et la cryptographie est résumée dans un tableau récapitulatif.

Propriétés des systèmes chaotiques	**Propriétés des systèmes cryptographiques**
Dynamique déterministe	Pseudo-aléatoire déterministe
Transformation non linéaire	Transformation non linéaire
Conditions initiales et/ou paramètres	Clé(s)
Sensibilité aux conditions initiales et aux paramètres	Diffusion
Ergodicité	Confusion
Itérations	Rounds
Structure complexe	Complexité de l'algorithme
Ensemble de nombres réels	Ensemble fini d'entiers

TABLE 2.1 – Correspondance entre la théorie du chaos et la cryptographie.

En bref, le lien étroit entre les propriétés des deux théories, à encouragé les chercheurs à proposer une grande variété de crypto-systèmes à base de générateurs chaotiques, en reposant sur des techniques différentes.

2.5 Méthodes de chiffrement à base des systèmes chaotiques

Les méthodes de chiffrement basées sur les systèmes chaotiques exploitent les propriétés et le comportement complexe des systèmes dynamiques chaotiques. Elles offrent une approche intéressante et potentiellement très sécurisée pour la protection des données. L'avantage de ces méthodes réside dans leur résistance potentielle aux attaques cryptanalytiques, en raison de leur sensibilité aux conditions initiales et de la difficulté à prédire leur comportement à long terme.

Les méthodes les plus couramment utilisées sont :

2.5.1 Chiffrement par blocs

Le chiffrement par blocs transforme une chaîne de bits du texte clair en une chaîne de même longueur sous le contrôle d'une clé secrète. Un système de chiffrement est qualifié par blocs s'il divise le texte clair en blocs de taille fixe et chiffre chaque bloc individuellement avec la même clé. Ces algorithmes sont également appelés algorithmes de chiffrement à clé secrète [36].

Dans le chiffrement chaotique par blocs, chaque bloc de données à chiffrer est d'abord converti en une représentation numérique, puis est traité à travers un système dynamique chaotique. Ce système utilise une clé secrète pour initialiser ses conditions initiales de manière à générer une série de valeurs chaotiques. Ces valeurs chaotiques sont ensuite combinées avec les données à chiffrer, généralement par des opérations mathématiques comme des XOR, des additions ou des permutations, pour produire le texte chiffré.

2.5.2 Chiffrement avec fonction de hachage

Les fonctions de hachage sont utilisées pour calculer, à partir d'une donnée d'entrée de taille variable, une empreinte de taille fixe. Cette empreinte est unique pour chaque entrée différente, ce qui signifie que même une petite modification de l'entrée produira une empreinte complètement différente.

Les fonctions de hachage appartiennent à la famille des algorithmes symétriques et doivent agir comme des fonctions aléatoires [37].

2.5.3 Chiffrement par générateurs chaotiques de séquences pseudo-aléatoires

Un élément crucial dans tout cryptosystème basé sur le chaos est le générateur de séquences chaotiques, qui sert à la génération des clés secrètes et au processus de chiffrement des données lors des opérations de substitution et de permutation. La confidentialité des données dépend du degré de chaos (c'est-à-dire de l'aléatoire) des séquences produites par ce générateur de séquences chaotiques.

Les résultats des générateurs de nombres pseudo-aléatoires sont principalement utilisés dans les algorithmes de chiffrement chaotique comme clés, avec lesquelles on applique une opération XOR (ou-exclusif) sur le texte en clair pour générer le texte chiffré [38].

Dans cette approche, un système dynamique chaotique est utilisé pour produire une séquence de valeurs qui semble aléatoire mais qui est déterministe, c'est-à-dire qu'elle est entièrement déterminée par les conditions initiales et les paramètres du système. Ces valeurs chaotiques sont alors transformées en une séquence de bits et utilisées comme clé pour le chiffrement.

De plus, cette approche a pavé la voie à d'autres méthodes de chiffrement qui intègrent également des éléments chaotiques pour améliorer la robustesse et la résistance aux attaques.

2.5.4 Cryptage par permutation chaotique

Le cryptage par permutation, également appelé transposition, est une méthode de chiffrement où les positions des éléments des données (comme les bits, les caractères ou les blocs de texte) sont réarrangées selon une certaine règle ou clé. Ce processus implique l'application itérative d'une série d'opérations non linéaires basées sur des dynamiques chaotiques. Ces opérations modifient de manière complexe l'ordre des bits ou des éléments du bloc de données, introduisant ainsi un haut degré de désordre et de confusion.

Elle est souvent utilisée en combinaison avec d'autres méthodes pour améliorer la sécurité globale du chiffrement [39].

2.5.5 Cryptage par addition

Le cryptage par addition est une méthode simple de chiffrement. Le signal de l'information confidentielle, un texte par exemple, sera additionné au signal généré par un système chaotique [40]. Dans ce processus, un système dynamique chaotique génère une séquence de nombres pseudo-aléatoires, basée sur des équations mathématiques non linéaires. Ces nombres sont ensuite combinés avec les données à chiffrer en utilisant une opération d'addition mo-

dulo, où chaque élément de la séquence chaotique est ajouté aux données de texte clair.

La figure (2.1) présente le principe de cryptage par addition appliqué à un fichier texte. Le contenu de ce dernier m(t) est additionné au signal généré par le système chaotique $x(t)$.

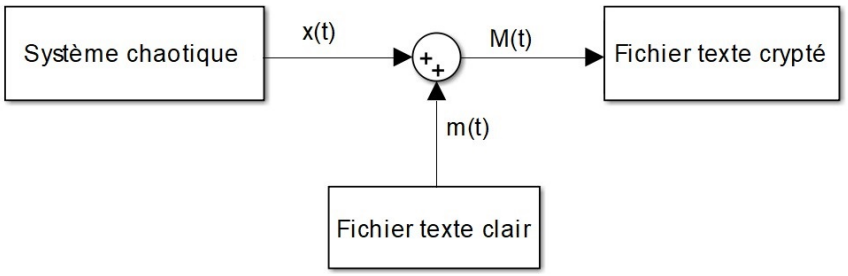


FIGURE 2.1 – Principe du cryptage par addition.

Dans le cas de message texte, le cryptage par addition peut engendrer que chaque lettre du message est décalée d'un certain nombre de positions dans l'alphabet.

2.5.6 Cryptage par commutation chaotique

Cette méthode est principalement destinée aux messages numériques ou binaires. Le cryptage par commutation utilise deux systèmes chaotiques ou plus pour représenter les bits du texte. Pour chaque niveau de texte (0 ou 1), deux systèmes chaotiques différents sont utilisés. L'un des systèmes chaotiques, choisi en fonction de la valeur du bit (0 ou 1), envoie sa sortie au fichier où le texte chiffré est enregistré. Ainsi, la sélection d'un système spécifique pour chaque bit crée le signal de texte crypté [12].
La figure (2.2) présente le principe de cryptage par commutation chaotique utilisant deux systèmes chaotiques.

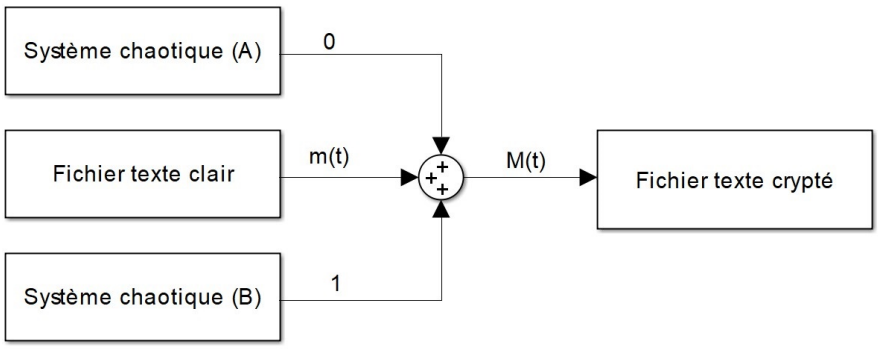


FIGURE 2.2 – Principe de cryptage par commutation chaotique.

2.5.7 Cryptage par modulation chaotique

Le cryptage par modulation est une technique qui encode les données en modifiant certains aspects d'un signal porteur d'information (amplitude, fréquence ou phase) en fonction des informations à transmettre.

Dans cette méthode, le message clair est introduit dans le système chaotique pour moduler un ou plusieurs paramètres de l'émetteur. Il en résulte un mélange multiplicatif entre le ou les paramètres du générateur de chaos et l'information [41].

La figure (2.3) présente le principe de cryptage par modulation chaotique où le signal du fichier texte clair est donné par $u(t)$.

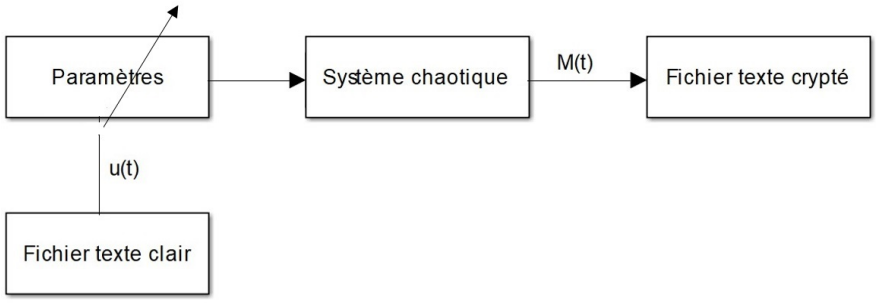


FIGURE 2.3 – Principe de cryptage par modulation chaotique.

2.5.8 Cryptage par inclusion

Le principe du cryptage par inclusion, en général, est de cacher des informations ou des données à l'intérieur d'autres données de telle manière qu'il est difficile pour une personne non autorisée de les détecter. Cette méthode est également appelée stéganographie [42]. Dans le cryptage chaotique par inclusion, les données à chiffrer sont incorporées dans un système dynamique chaotique. Ce système chaotique génère alors une trajectoire complexe et apériodique, qui est utilisée comme texte chiffré ou comme clé de chiffrement [12].

La figure (2.4) présente le principe de cryptage par inclusion où le signal du fichier texte $m(t)$ est inclus directement dans la dynamique de système chaotique.

FIGURE 2.4 – Principe de cryptage par inclusion.

Ainsi, il est clair que le chiffrement par générateur chaotique des séquences pseudo-aléatoires constitue une étape essentielle dans l'évolution de ces techniques de cryptographie moderne.

2.6 Application au chiffrement de texte

Il est vrai que la cryptographie basée sur des systèmes chaotiques est souvent associée au chiffrement des images et des vidéos, principalement en raison de la richesse des données visuelles et de la complexité des médias numériques. Cependant, il convient de noter que les applications au chiffrement des textes existent également, bien que moins discutées dans la littérature. Les systèmes chaotiques offrent des propriétés cryptographiques intéressantes qui peuvent être appliquées de manière efficace au chiffrement des textes, bien que cela soit moins exploré et moins documenté que dans le cas des images et des vidéos.

Megherbi et *al.* ont mis au point un système de communication reposant sur le protocole de transmission Client-Serveur via WiFi, basé sur le système chaotique de Hénon d'ordre fractionnaire. Il intègre un système esclave utilisant l'observateur impulsif d'ordre non entier. L'algorithme de chiffrement combine un vecteur de permutation, une phase de normalisation, ainsi qu'une opération XOR. Ce système est développé sur une carte ESP32 avec un écran LCD et un clavier et fonctionne en mode de transmission unidirectionnel. Les performances du système sont mises en avant par une implémentation aisée, une entropie élevée, une vitesse de transmission rapide, un coût réduit et une important sensibilité aux clé secrètes.

La méthode proposée par Giap et *al.* utilise le protocole de transmission TCP/IP via WiFi. Le système chaotique utilisé est le système de Lorenz, qui est converti en un modèle flou. Pour la gestion du système esclave, ils utilisent un contrôleur en mode glissant ainsi qu'un observateur de perturbations. En termes de chiffrement, la méthode repose sur l'utilisation du deuxième état du système de Lorenz. Le matériel utilisé est une carte de développement ESP8266. La communication est effectuée en mode unidirectionnel (one-way), avec des indicateurs de performance axés sur le rejet des perturbations.

La méthode de Moysis et *al.* utilise une communication par radio-fréquence (RF) avec un générateur de nombres pseudo-aléatoires (PRNG) basé sur deux fonctions sinusoïdales identiques imbriquées. Le système esclave est identique au maître, avec une opération XOR utilisée pour le chiffrement. Le matériel employé comprend un micro-contrôleur ARM Cortex M0+, un écran LCD, et un émetteur-récepteur RF. La communication est bidirectionnelle

(two-way) et les indicateurs de performance mettent en avant le caractère aléatoire des séquences utilisées en chiffrement.

La méthode de Atan et *al.* utilise, pour la transmission de texte, un protocole GSM avec un générateur de nombres aléatoires chaotiques (Chaotic RNG). Le système esclave est identique au maître, et le crypto-système utilise une fonction de sommation pour le chiffrement. Le matériel employé est une carte Arduino MEGA 2560 équipée d'un module GSM shield. La communication est réalisée en mode unidirectionnel (one-way). Les indicateurs de performance de cette méthode soulignent la facilité de mise en œuvre et la vitesse de transmission [43].

2.7 Algorithme de chiffrement proposé

Dans cette partie, nous présentons et décrivons le processus de chiffrement proposé. La structure de l'algorithme de chiffrement comprend quatre éléments essentiels :

1. Texte clair :Cet élément implique le fichier texte original qui est lisible et compréhensible.

2. Les systèmes chaotiques :Ils représentent les générateurs chaotiques, de Hénon modifié d'ordre fractionnaire et la fonction logistique, utilisés pour le chiffrement.

3. Cryptage :C'est le processus de transformation utilisant une combinaison des approches de chiffrement introduites précédemment.

4. Texte crypté :Le résultat final, le fichier texte sécurisé qui est illisible sans les moyens appropriés de déchiffrement.

Les éléments cités ci-dessus sont résumés dans schéma synoptique illustré sur la figure (2.5).

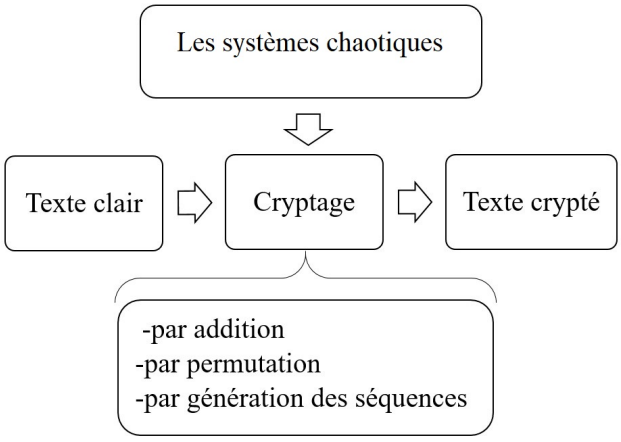


FIGURE 2.5 – Éléments constituant l'algorithme de chiffrement proposé.

Nous décrivons le processus de cryptage à travers les étapes suivantes :

*Etape*1 : Les systèmes chaotiques, Hénon modifié d'ordre fractionnaire défini précédemment dans (1.15) et la fonction logistique indiquée dans (1.6), sont itérés pendant un nombre suffisant de tours pour obtenir des séquences chaotiques $x(k)$, $y(k)$, $z(k)$ et $w(k)$ avec des paramètres de contrôle et des conditions initiales précises.
*Etape*2 : Lecture de fichier texte clair.
*Etape*3 : Les N caractères du fichier texte clair original sont convertis en octets correspondant à leurs codes ASCII.
*Etape*4 : On effectue une addition entre le signal $ca(k)$ des codes ASCII du texte clair qu'on a multiplier fois $d = 0.002$ et l'état $w(k)$ de la fonction logistique chaotique. On nomme le résultat $m(k)$.
*Etape*5 : On applique deux fonctions non linéaires $g_1(k)$ et $g_2(k)$, avec les entrées $x(k)$, $y(k)$ et $z(k)$, N fois pour obtenir deux séquences chaotiques pseudo-aléatoires, avec k_{11}, k_{12}, k_{13}, k_{21}, k_{22} et k_{23} comme coefficients réels et clés de chiffrement secrètes supplémentaires telles que :

$$\begin{aligned} g_1(k) &= k_{11}x(k)^2 + k_{12}y(k)^2 + k_{13}z(k)x(k) \\ g_2(k) &= k_{21}y(k)^2 + k_{22}z(k)^2 + k_{23}x(k)y(k) \end{aligned} \tag{2.1}$$

*Etape*6 : En utilisant les opérations modulo et floor, on convertit $g_1(k)$ et $g_2(k)$ en séquences de nombres entiers positifs nommées $G_1(k)$ et $G_2(k)$.
*Etape*7 : On convertit les éléments entiers positifs des séquences $G_1(k)$ et $G_2(k)$ en binaire et on note les séquences obtenues G_1b et $G_2b(k)$.
*Etape*8 : On effectue une rotation pour $G_1b(k)$ d'un bit vers la droite, et deux bits vers la gauche pour $G_2b(k)$, les séquences résultantes sont notées $G_1d(k)$ et $G_2d(k)$.
*Etape*9 : On trie les éléments de $G_1d(k)$ dans l'ordre décroissant et on sauvegarde les positions des éléments originaux dans un vecteur d'index V, considéré comme vecteur de permutation.
*Etape*10 : Les éléments du résultat de l'addition $m(k)$ sont ensuite triés en fonction du vecteur V, le résultat est converti en binaire et noté M_b.
*Etape*11 : On effectue une opération XOR bit à bit entre les éléments du tableau permuté M_b obtenu et les éléments de la séquence $G_2d(k)$ décalés, on nomme le résultat Mc.
*Etape*12 : Le résultat Mc de l'opération XOR est ensuite converti en décimal (code ASCII).
*Etape*13 : Les codes ASCII sont convertis en caractères.
*Etape*14 : Le résultat final, qui est le texte crypté, est sauvegardé dans un nouveau fichier texte.

La figure (2.6) illustre le schéma proposé pour chiffrer un fichier texte avec deux systèmes chaotique. Il est à noter que le système chaotique (E) est le système de Hénon modifié d'ordre fractionnaire, et le système chaotique (F) est la fonction logistique.

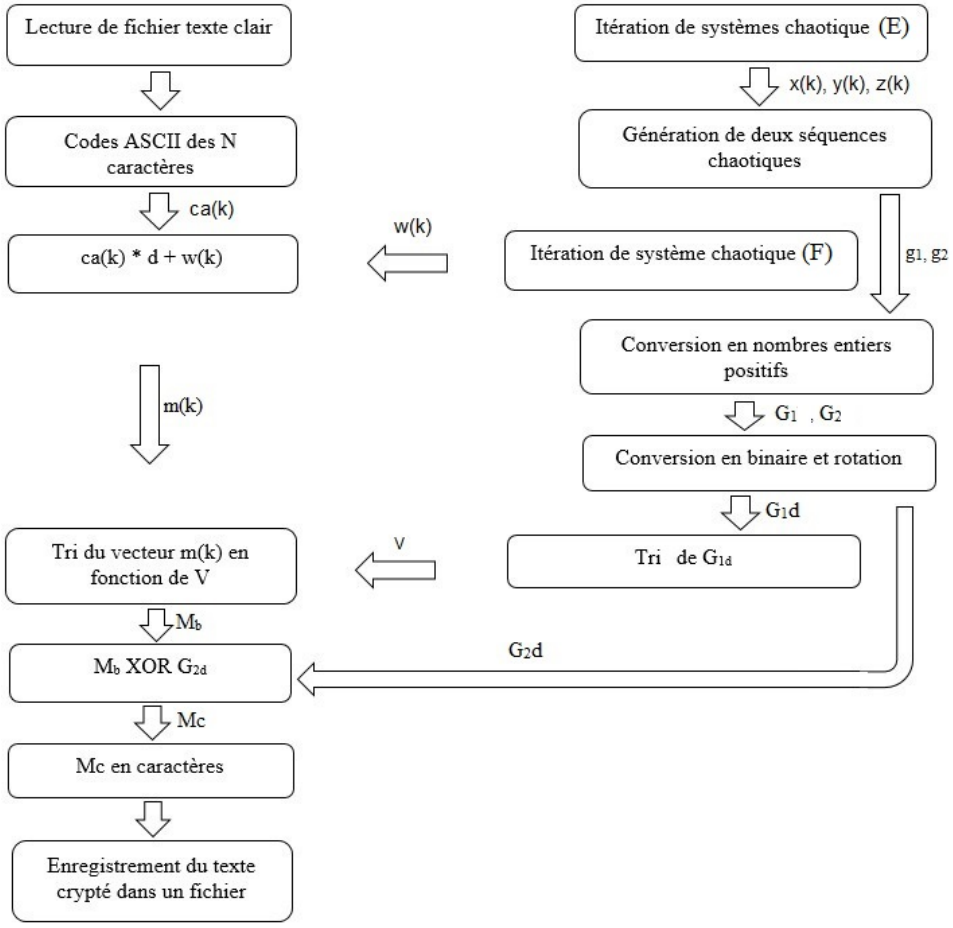


FIGURE 2.6 – Schéma synoptique de l'algorithme de chiffrement de fichier texte proposé.

Ce processus de cryptage transforme le texte clair en un texte crypté, rendant les données illisibles sans les moyens et les clés de déchiffrement appropriés.

2.8 Résultat de chiffrement

La figure (2.7) montre un exemple de fichier texte original, non chiffré. Ce texte est lisible et compréhensible par toute personne ayant accès au fichier. Si un fichier original est intercepté par une personne non autorisée, toutes les informations contenues peuvent être facilement lues et potentiellement utilisées à des fins malveillantes.

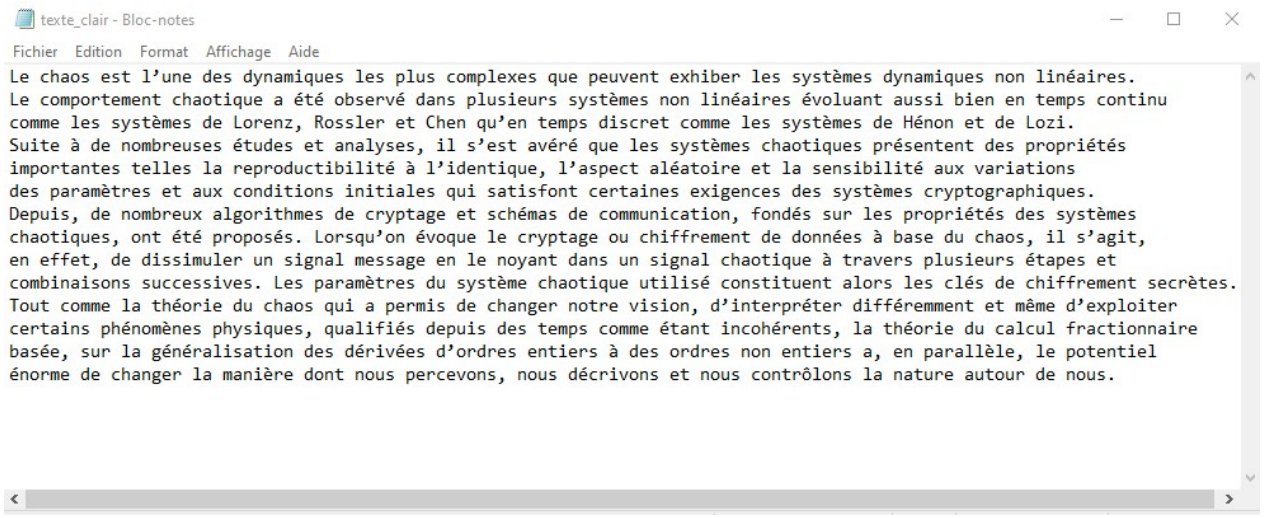


FIGURE 2.7 – Fichier texte clair.

La figure (2.8) montre le fichier texte,considéré comme exemple d'application, après le chiffrement. Le contenu est désormais illisible et incompréhensible sans la clé de déchiffrement appropriée. Cette photo démontre l'efficacité de l'algorithme de cryptage utilisé. Le texte chiffré protège les informations sensibles en garantissant que même si le fichier est intercepté, il reste protégé contre toute utilisation non autorisée.

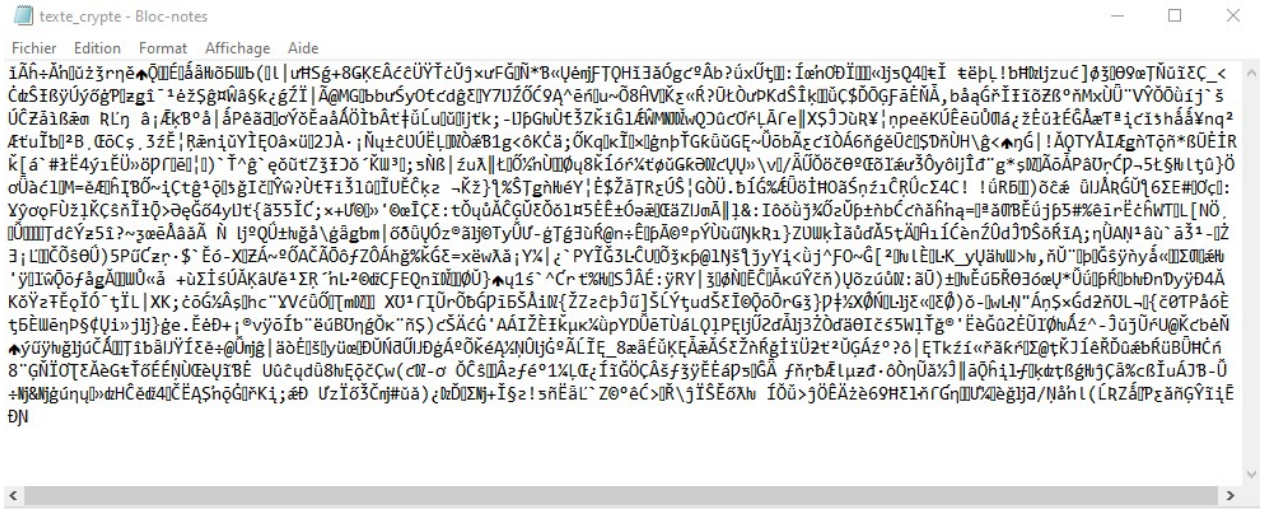


FIGURE 2.8 – Fichier texte crypté.

En conclusion, la comparaison entre le texte clair le texte crypté souligne l'importance cruciale de la cryptographie pour assurer la confidentialité et la sécurité des informations. Le processus de chiffrement transforme les données lisibles en une forme sécurisée, inaccessible sans les moyens appropriés pour les déchiffrer, garantissant ainsi que les données restent protégées contre les accès non autorisés.

2.9 Conclusion

Dans ce chapitre, nous avons exploré la cryptographie chaotique et ses applications au chiffrement de texte. Nous avons défini la cryptographie chaotique, en montrant comment elle utilise les propriétés des systèmes chaotiques pour améliorer la sécurité des communications. Les similitudes entre les systèmes cryptographiques et chaotiques ont été mises en évidence pour souligner l'utilité et l'applicabilité des systèmes chaotiques en cryptographie.

L'état de l'art de la cryptographie a fourni un contexte historique et technique, illustrant les avancées dans le domaine. Plusieurs méthodes de chiffrement basées sur des systèmes chaotiques ont été présentées. Nous avons également abordé des applications pratiques au chiffrement de texte.

Un algorithme de chiffrement de fichier texte basé sur la cryptographie chaotique a été proposé, et ses résultats ont été interprétés pour démontrer son efficacité. En conclusion, la cryptographie chaotique offre une approche prometteuse pour le chiffrement de texte, présentant une alternative sécurisée et innovante aux méthodes traditionnelles.

Cependant ,bien que le simple fait de chiffrer un texte puisse donner une illusion de sécurité, cela ne suffit pas pour garantir que les données sont véritablement protégées. Pour assurer la sécurité d'un fichier texte crypté, il est essentiel de soumettre le système de chiffrement à des tests rigoureux supplémentaires et à des études approfondies. Ces tests incluent l'analyse de la résistance aux attaques statistiques, la analyse différentielle, ainsi que celle de la robustesse face aux attaques par force brute.

Dans le chapitre suivant, nous analyserons la robustesse de notre algorithme pour garantir qu'il offre une protection adéquate contre certaines menaces et attaques fréquentes.

Chapitre 3

Analyses de robustesse de l'algorithme de chiffrement de fichiers texte

3.1 Introduction

Dans un monde où les données numériques sont omniprésentes, la sécurité des informations, des fichiers en particulier, est devenue une priorité absolue pour les individus, les entreprises et les gouvernements. Les algorithmes de chiffrement sont essentiels pour protéger ces données sensibles, en assurant leur confidentialité, leur intégrité et leur authenticité. Toutefois, pour garantir l'efficacité de ces algorithmes, il est impératif de les analyser en profondeur pour identifier et corriger d'éventuelles vulnérabilités [44].

Ce chapitre est consacré à l'analyse de la robustesse de l'algorithme de chiffrement conçu et appliqué aux fichiers texte, en utilisant diverses techniques de cryptanalyse. Nous commencerons par les critères et les méthodes utilisés pour évaluer la robustesse de notre algorithme, en tenant compte des différentes attaques potentielles auxquelles il pourrait être exposé. Ensuite, nous appliquerons des analyses de robustesse, qui ont pour but de comprendre les vulnérabilités des systèmes de chiffrement. Un rappel des principaux paramètres d'entrée de notre algorithme, tels que les clés de chiffrement et les conditions initiales, seront fournis pour assurer une compréhension claire des bases nécessaires à l'évaluation. L'analyse statistique des données chiffrées sera abordée pour détecter des motifs ou des distributions qui pourraient indiquer des faiblesses, et l'analyse différentielle sera utilisée pour examiner l'impact de petites modifications dans les données d'entrée sur les données chiffrées en sortie, afin d'identifier de potentielles vulnérabilité.

Ce chapitre vise à fournir une évaluation exhaustive et critique de la robustesse de l'algorithme de chiffrement de fichiers texte proposé.

3.2 Définition de l'analyse de robustesse

L'analyse de robustesse est le processus d'évaluation systématique de la capacité d'un système ou d'un algorithme à résister à des conditions adverses, des attaques, ou des défaillances. Dans le contexte des algorithmes de chiffrement de fichier texte, cela implique de tester la sécurité et la résistance de l'algorithme face à diverses attaques ciblant ce type d'information pour s'assurer qu'il peut protéger efficacement les fichiers texte contre les tentatives de déchiffrement non autorisées [45][46].

3.3 Objectifs de l'analyse de robustesse

L'objectif de l'analyse de robustesse est de garantir que l'algorithme de chiffrement est suffisamment robuste pour protéger les données sensibles contre une large gamme d'attaques potentielles [47]. Cela inclut :

- Identifier les vulnérabilités de l'algorithme ou de sa mise en œuvre.
- Proposer des améliorations pour corriger les failles identifiées.
- Assurer aux utilisateurs la fiabilité de l'algorithme.
- Garantir l'efficacité de l'algorithme pour protéger les données sensibles.
- Anticiper et bloquer les techniques d'attaque potentielles.
- Protéger les données contre une large gamme d'attaques possibles.

Dans ce qui suit, nous allons tester notre algorithme de chiffrement de texte au moyen de quelques analyses de base.

3.4 Application des analyses de robustesse sur l'algorithme de chiffrement de fichiers texte

Dans cette partie, nous analysons l'approche de chiffrement proposée contre certaines attaques. Pour cela, nous utilisons un fichier texte de 1596 caractères, comme illustré dans la figure (2.7). Les tests sont classifiées en :

. Analyses statistiques incluant l'analyse d'histogramme des codes ASCII permettant d'évaluer la distribution de ces codes dans le texte chiffré, et l'analyse d'entropie qui mesure à quelle degré un signal est aléatoire.

. Analyse différentielle qui vise à examiner comment des petites variations dans les clés affectent le texte chiffré.

. Analyse de l'espace de clés qui évalue la taille de l'espace de clés secrètes.

Les paramètres que nous utiliserons pour nous simulations relatives à l'application des analyses de robustesse incluent les paramètres de contrôle de système de Hénon modifié, nous fixons les valeurs des paramètres à$A = 1.65$ et $B = 0.1$. Les ordres de différences non entier sont choisis égaux à $\alpha_1 = 0.85$, $\alpha_2 = 0.9$ et $\alpha_3 = 0.75$, le choix des paramètres effectué garantit le comportement chaotique de système d'ordre fractionnaires. Pour la fonction logistique, le paramètre de contrôle est $R = 3.9$, qui est une valeur connue pour générer un comportement chaotique. Pour les séquences chaotiques pseudo-aléatoires, nous utilisons les ensembles de paramètres suivants : $k_{11} = 0.21$, $k_{12} = 0.32$, $k_{13} = 0.43$, $k_{21} = 0.44$, $k_{22} = 0.35$, et $k_{23} = 0.26$. On prend les conditions initiales $(x_0, y_0, z_0) = (0.1, 0.1, 0.1)$ et $w_0 = w(0) = 0.1$, dans le but de rester dans le bassin d'attraction. Toutes les simulations sont réalisées en utilisant MATLAB version 2013, qui offre un environnement adéquat pour le calcul fractionnaire et l'analyse des dynamiques non linéaires chaotiques. Ce logiciel contient des fonctions utiles pour le cryptage de fichiers texte, telles que sort pour ordonner les vecteurs, circshift pour la rotation des vecteurs, double pour convertir les données en format numérique par défaut, ainsi que bar pour dessiner l'histogramme et tic-toc pour évaluer le temps d'exécution.

Les principes et les résultats de ces analyses de robustesse sont développés dans la partie qui suit.

3.4.1 Analyses statistiques

L'analyse statistique permet d'analyser les propriétés statistiques de la donnée chiffrée [13]. Cette analyse statistique comprend l'étude des distributions de fréquences via l'histogramme, le calcul de l'entropie pour mesurer la complexité et l'imprévisibilité du texte chiffré, ainsi que l'évaluation des principes de confusion et de diffusion pour assurer la robustesse du chiffrement. Nous développerons ci-dessous, le principe de chaque test.

3.4.1.1 Histogramme

Un histogramme est un graphique qui montre la fréquence d'occurrence des différentes valeurs dans un ensemble de données. Dans le contexte des fichiers texte, l'histogramme vise à comparer les occurrences des codes ASCII dans le texte clair et le texte chiffré. Pour un texte chiffré, un histogramme idéal devrait montrer une distribution uniforme, indiquant que chaque caractère a une probabilité similaire d'apparition, ce qui complique la tâche de l'analyse de fréquences d'apparition pour un utilisateur non autorisé [48].

Les figures (3.1, 3.2) illustrent les distributions des codes ASCII dans les textes original et chiffré.

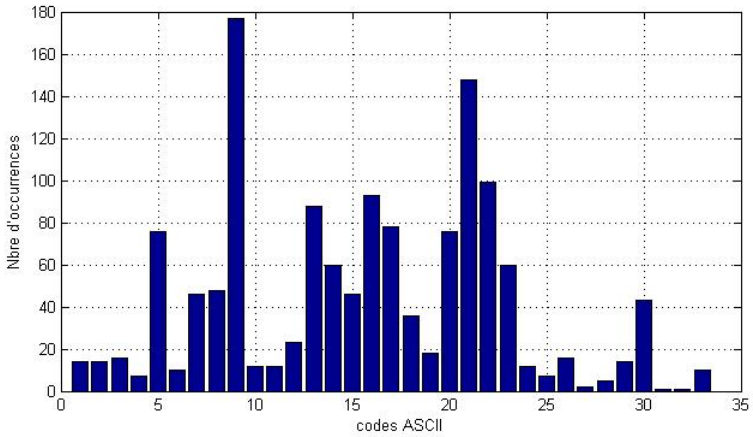


FIGURE 3.1 – Histogramme du texte clair.

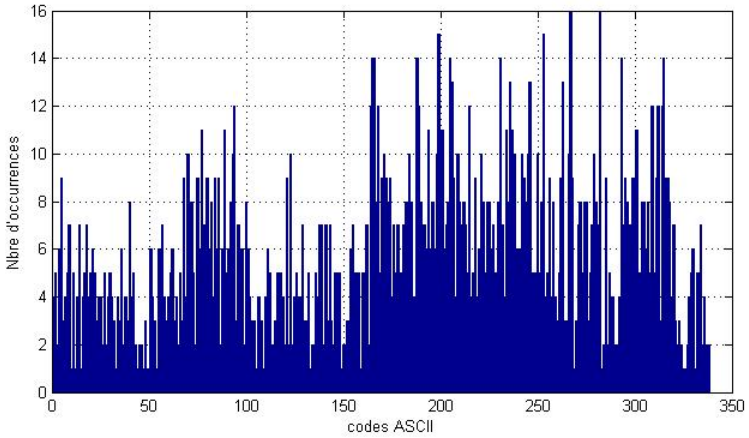


FIGURE 3.2 – Histogramme du texte chiffré.

On peut constater que les distributions des codes ASCII sont différentes. Le texte chiffré affiche une répartition des codes plus uniforme et plus étendue. Cette différence implique que l'algorithme de chiffrement est robuste face aux attaques à base de l'histogramme.

3.4.1.2 Entropie

L'entropie est une mesure quantitative de l'incertitude associée à un ensemble de données. Dans le cadre de l'analyse des fichiers texte, l'entropie permet de quantifier le degré de désordre du texte chiffré. Plus l'entropie est grande, plus le texte chiffré est aléatoire et plus il est sécurisé, car il indique que les caractères sont distribués de manière imprévisible. Au contraire, si l'approche de chiffrement n'est pas suffisamment robuste, l'entropie qui en résulte est réduite et le processus de chiffrement est vraiment exposé et pourrait ne pas contrecarrer les attaques basées sur l'entropie [43].

L'entropie d'un message chiffré m, notée $H(m)$, peut être mesurée comme suit :

$$H(m) = \sum_{k=0}^{2^{M-1}} p(m_k) \log_2 \left(\frac{1}{p(m_k)} \right) \tag{3.1}$$

où 2^M représente le nombre cardinal des symboles d'information, c'est-à-dire tous les caractères possibles dans le message m, et $p(m_k)$ fait référence à la probabilité d'occurrence de l'élément m_k dans le message. Ainsi, si un message m est chiffré avec 2^M éléments potentiels, l'entropie obtenue devrait idéalement être $H(m) = M$.

Dans notre travail, il y a 501 caractères uniques dans le texte chiffré, donc la valeur d'entropie idéale est

$$H = log_2(501) = 8.9687$$

Le tableau (3.1) suivant montre les résultats de l'entropie calculée avant et après le chiffrement.

	Texte en clair	**Texte chiffré**
Entropie	4.3777	8.7928

TABLE 3.1 – Résultats d'entropie dans les textes original et chiffré.

L'entropie élevée du texte chiffré par rapport à l'entropie du texte clair est un indicateur positif que le chiffrement a réussi à transformer le texte clair en une forme hautement aléatoire et sécurisée. D'autre part, l'entropie idéale du texte crypté est de 8.9687, et l'entropie mesurée du texte crypté égale à 8.7928 qui est proche de la valeur l'idéal. Cela montre que notre entropie est presque optimale. L'algorithme de chiffrement proposé est robuste face aux attaques à base de l'entropie.

3.4.2 Analyse différentielle : Sensibilité aux variation des clés secrètes

La fiabilité du chiffrement des informations confidentielles repose en grande partie sur la sensibilité aux clés secrètes qui doit avoir lieu dans des mécanismes de chiffrement et de déchiffrement.

La sensibilité aux clés dans le processus de cryptage signifie que si un même fichier texte original est crypté deux fois, en utilisant des clés secrètes légèrement différentes, les deux fichiers textes chiffrés générés doivent être très différents l'un de l'autre. Cela garantit que de

petites variations dans la clé de chiffrement entraînent des résultats totalement distincts, ce qui renforce la sécurité du chiffrement [43].

Dans notre contribution, la sensibilité aux clés secrètes pour le mécanisme de chiffrement est examinée et confirmée. Le tableau (3.2) présente les clés et leurs valeurs associées ainsi que la précision de chaque valeur.

Clés	**Valeurs**	**Précisions (Pi)**
A	1.65	10^{-15}
B	0.1	10^{-17}
R	3.9	10^{-15}
α_1	0.85	10^{-16}
α_2	0.9	10^{-16}
α_3	0.75	10^{-16}
k_{11}	0.21	10^{-2}
k_{12}	0.32	10^{-2}
k_{13}	0.43	10^{-2}
k_{21}	0.44	10^{-2}
k_{22}	0.35	10^{-2}
k_{23}	0.26	10^{-2}

TABLE 3.2 – La précision des clés secrètes.

Les résultats illustrés montrent que les clés A, B et R, qui sont les paramètres de bifurcation du système de Hénon modifié et de la fonction logistique respectivement, ainsi que les α_i (avec $i = 1..3$), qui représentent les ordres de différences non entiers, possèdent des précisions très élevées, de l'ordre de 10^{-15} à 10^{-17}, signifiant que l'algorithme est sensible même aux plus petites variations. Les clés k_{11}, k_{12}, k_{13} , k_{21} , k_{22} et k_{23} , qui sont les paramètres des séquences chaotiques, ont une précision de 10^{-2}, car ils sont en dehors de la dynamique du système. Bien que cette précision soit moins importante, elle reste suffisante pour des valeurs de cette magnitude, indiquant que ces clés agissent comme des éléments supplémentaires dont les valeurs exactes et précises sont nécessaires pour récupérer le fichier texte original.

Afin de mieux illustrer la sensibilité de notre algorithme face aux variations des clés secrètes, nous considérerons deux cas de figure où nous varions légèrement un paramètre et chiffrons un fichier texte avec la nouvelle clé.

La figure (3.3) montre le texte clair avant d'appliquer le chiffrement.

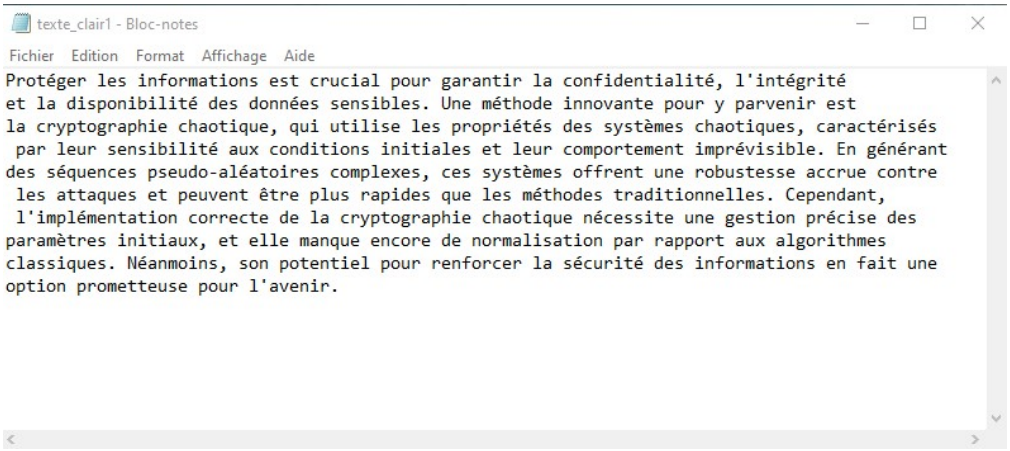


FIGURE 3.3 – Le texte clair (avant le chiffrement).

Nous réalisons d'abord le chiffrement avec les valeurs citées dans le tableau (3.2) . La figure (3.4) illustre le texte chiffré, qui semble bien chiffré et illisible.

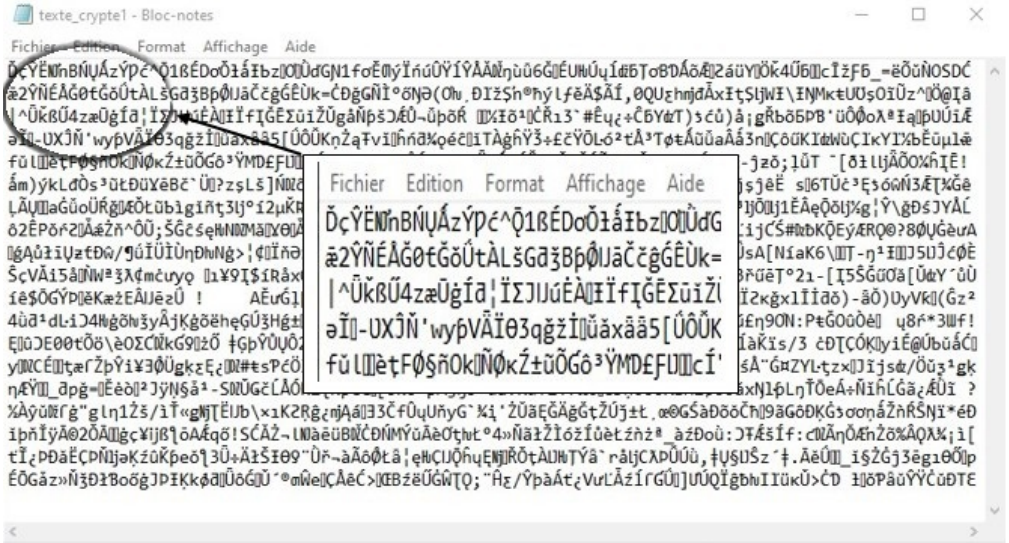


FIGURE 3.4 – Le texte chiffré avec les clés primaire.

Nous appliquons une petite variation pour la clé "A" de l'ordre de 10^{-7}. La figure (3.5) présente le texte après cette variation légère de la clé qui est presque négligeable.

FIGURE 3.5 – Le texte chiffré après la variation de la clé A.

On peut voir que le résultat est complètement différent : le texte chiffré avec cette petite variation ne ressemble en rien au texte chiffré dans la figure (3.4) avant la variation de la clé.

Maintenant, nous effectuons une petite variation pour la clé "α_1" de l'ordre de 10^{-7}. Le résultat est illustré dans la figure (3.6).

FIGURE 3.6 – Le texte chiffré après la variation de la clé α_1.

Il n'y a aucune ressemblance entre cette dernière figure et les autres précédentes, ce qui montre que la variation de la clé α_1 entraîne une grande différence dans le résultat.

La sensibilité aux variations des clés secrètes est extrêmement importante dans notre algorithme de chiffrement. Un léger changement dans la valeur de la clé lors du chiffrement produit un texte totalement différent.

3.4.3 Analyse de l'espace de clés

Un algorithme de chiffrement solide et robuste doit avoir un espace de clés suffisamment vaste pour résister aux attaques à force brute. Cet espace de clés doit être supérieur à 2^{128} [49].

Les attaques à force brute sont des approches ou un intrus ou utilisateur non autorisé tente systématiquement toutes les combinaisons possibles de clés ou de mots de passe jusqu'à ce que la bonne soit trouvée [50].

Notre algorithme de chiffrement comprend douze paramètres en tant que clés secrètes. L'analyse de la sensibilité aux clés secrètes et le tableau (3.2) sont utilisées pour calculer la taille (T) de l'espace de clés en utilisant la formule suivante :

$$T = \prod_{1}^{12} 10^{1/Pi} \tag{3.2}$$

avec Pi : les précision des clés secrètes.

$$T = 10^{17} \times (10^{16})^3 \times (10^{15})^2 \times (10^2)^6 = 10^{107} \approx 2^{355}$$

Cet espace de clés, de taille largement supérieure à celle requise, est suffisamment grand pour dissuader les tentatives d'attaques a force brute.

On peut constater aussi que l'utilisation du système de Hénon modifié d'ordre fractionnaire a permis d'obtenir un espace des clés secrètes 10^{48} fois plus large que si on avait utilisé uniquement des systèmes chaotiques d'ordre entier.

3.4.4 Temps d'exécution

Un algorithme de chiffrement efficace doit être à la fois robuste et rapide, particulièrement pour les applications en temps réel. En effet, dans de nombreux domaines tels que les domaines militaires, la médecine et les télécommunications, les résultats doivent être obtenus presque instantanément, la vitesse est cruciale [51]. Nous avons utilisé la commande tic toc, dans MATLAB, pour calculer le temps d'exécution.

L'algorithme de chiffrement présenté dans notre travail nécessite 1.75 secondes pour crypter les 1596 caractères du fichier texte choisi, en incluant la lecture du fichier texte clair et l'enregistrement du texte chiffré dans un fichier. Sans prendre en compte les actions de lecture et d'enregistrement, le processus de chiffrement nécessite 0.38 secondes.

3.5 Conclusion

Dans ce chapitre, nous avons abordé l'analyse de robustesse d'un algorithme de chiffrement appliqué à un fichier texte. Après avoir introduit le concept d'analyse de robustesse et ses objectifs, nous avons passé en revue les paramètres de simulation considérés dans cette étude.

Nous avons exploré plusieurs types d'analyses, notamment les analyses statistiques et différentielles, qui permettent d'évaluer la sensibilité de l'algorithme. De plus, nous avons abordé l'analyse de l'espace de clés, qui fournit des informations cruciales sur la résistance de l'algorithme face à des attaques à force brute.

Enfin, nous avons clos notre étude en examinant le temps d'exécution du programme et souligné son importance, dans les applications en temps réel où la rapidité est essentielle.

Malgré les tests de robustesse réalisés dans ce chapitre et les résultats prometteurs obtenus, il reste d'autres analyses approfondies à effectuer, comme des analyses de bruit et de corrélation. À partir des résultats obtenus, nous pourrons toujours améliorer et renforcer notre algorithme afin de contrecarrer ces différentes analyses.

Conclusion générale

Dans ce mémoire, nous avons proposé et conçu un algorithme robuste de chiffrement de fichiers texte basé sur les systèmes chaotiques, en particulier sur le système de Hénon modifié d'ordre fractionnaire et la fonction logistique d'ordre entier.

Dans le premier chapitre, nous avons commencé par une exploration de quelques notions sur les systèmes dynamiques en temps continu et en temps discret. Ensuite, nous nous sommes intéressés à un ensemble de systèmes non linéaires dits systèmes chaotiques. Nous avons présenté les propriétés de ces systèmes qui sont très intéressantes pour le chiffrement des données. Parmi ces propriétés, nous pouvons mentionner le déterminisme, qui signifie qu'il est possible de reproduire le comportement chaotique, et la sensibilité aux conditions initiales, qui veut dire que de petites variations dans les conditions initiales provoquent des trajectoires totalement différentes à long terme. Nous avons également abordé la transition vers le chaos dans un système dynamique en expliquant le phénomène de bifurcation avec des exemples. Enfin, nous avons traité la différence d'ordre fractionnaire dans les systèmes chaotiques discrets, en modélisant, comme exemple, le système de Hénon modifié d'ordre non entier.

L'objectif du deuxième chapitre est d'utiliser les systèmes chaotiques dans le domaine de la cryptographie et de les appliquer au chiffrement des fichiers texte. Nous avons d'abord étudié les systèmes cryptographiques en les comparant avec les systèmes chaotiques pour identifier les similarités entre eux. Parmi les caractéristiques des systèmes cryptographiques, nous pouvons citer la confusion, qui vise à rendre la relation entre le texte clair et le texte chiffré très complexe, et la diffusion, qui signifie que de petites modifications dans les clés secrètes engendrent un texte chiffré complètement différent. Nous avons brièvement évoqué les méthodes les plus célèbres de chiffrement reposant sur les systèmes chaotiques.

Ensuite, nous avons présenté en détails l'algorithme de chiffrement de fichier texte ainsi que les étapes qui le constituent. Enfin, nous avons présenté les premiers résultats obtenus après l'application de l'algorithme sur un fichier texte d'extension ".txt". D'après les résul-

tats visuels obtenus, le texte est bien chiffré, son contenu est désormais illisible et embrouillé, montrant l'efficacité de l'algorithme de chiffrement.

Ces résultats ont été complétés et validés par une série de tests et d'analyses de robustesse développés en détails dans le troisième chapitre. Les analyses que nous avons effectuées incluent des analyses statistiques, y compris l'analyse de l'histogramme, qui permet d'évaluer la distribution des codes ASCII dans le texte chiffré, et l'analyse de l'entropie, qui mesure le degré d'aléa dans un signal, une analyse différentielle, qui vise à étudier la sensibilité aux variations des clés secrètes, et enfin, nous avons terminé nos analyses par l'analyse de l'espace de clés, qui mesure la taille de l'espace de clés secrètes.

Nous avons constaté que notre algorithme est bien robuste par rapport aux analyses effectuées. L'histogramme du texte chiffré est plus uniforme et plus étendu, l'entropie est suffisamment élevée, les clés secrètes sont très sensibles aux variations, et finalement, la taille de l'espace de clés secrètes est assez suffisante pour résister aux attaques à force brute.

En guise de perspective, l'algorithme de chiffrement conçu peut être appliqué dans des schémas de communication de fichiers texte.

Notre contribution peut aussi être améliorée à l'avenir par l'application d'autres analyses de robustesse plus approfondies pour la détection des fragilités afin de les éliminer ou au moins minimiser leur impact. En outre, on peut envisager la généralisation de l'approche adoptée pour le chiffrement, la transmission et la sécurité des fichiers texte de différents types, par exemple les fichiers Word, les fichiers PDF et les tableurs Excel, etc.

Résumé

L'objectif de ce mémoire de fin d'études est de développer un algorithme de cryptage basé sur les systèmes chaotiques pour chiffrer un fichier texte.

Pour ce faire, nous avons structuré notre travail en plusieurs parties. Dans un premier temps, nous avons étudié les systèmes chaotiques, nous avons également présenté les systèmes chaotiques d'ordre fractionnaire. Ensuite, nous nous sommes concentrés sur les systèmes cryptographiques et les méthodes de cryptage chaotique, nous avons exploré les concepts fondamentaux de la cryptographie et montré comment les systèmes chaotiques peuvent être intégrés dans des algorithmes de cryptage pour améliorer la sécurité. Nous avons ensuite effectué des analyses de robustesse de l'algorithme proposé, nous avons évalué la résistance de l'algorithme face à différentes attaques potentielles.

Ce mémoire démontre l'efficacité et la pertinence des systèmes chaotiques pour le cryptage de données, en apportant une solution innovante et robuste pour la sécurité de l'information.

Annexe A

Implémentation sur carte Arduino

A.1 Introduction

Le chiffrement est l'une des méthodes les plus efficaces qui garantit la sécurité et la protection des informations à l'ère numérique actuelle [52]. Dans ce contexte, l'implémentation d'algorithmes de chiffrement sur des plateformes matérielles présente un intérêt croissant.

Ce chapitre se focalise sur l'implémentation de notre algorithme sur une carte Arduino Mega 2560. Nous explorerons les différentes étapes nécessaires pour réaliser cette tâche, en commençant par expliquer ce qu'est une carte Arduino, ensuite nous définirons et présenterons le matériel utilisés. Nous passerons ensuite à l'explication de montage initial et de montage avec résultat.

A la fin de ce chapitre, nous serons capables de fournir une compréhension clair et pratique de la manière dont un algorithme de chiffrement peut être intégré dans un système embarqué comme l'Arduino Mega 2560.

A.2 C'est quoi une carte Arduino

Une carte Arduino est un circuit électronique open-source ; les plans de la carte elle-même sont publiés en licence libre avec certains composants de la carte, basé sur un microcontrôleur, conçue pour créer des projets interactifs. Les spécifications matérielles étant open-source, il est possible de fabriquer ou modifier des cartes existantes. Compactes et flexibles, les cartes Arduino comportent des broches d'entrée et de sortie permettant de connecter divers composants électroniques.

Parmi les modèles populaires, on trouve l'Arduino Uno, idéal pour les débutants, l'Arduino Mega, offrant plus de broches et de mémoire pour des projets complexes, et l'Arduino Nano, plus compact. Bénéficiant d'une vaste communauté, Arduino facilite l'apprentissage et le développement dans des domaines variés comme l'automatisation, la robotique, et l'éducation.

Parmi ces types, nous avons choisi une carte Arduino Mega. L'intérêt principal de cette carte est de faciliter la mise en œuvre d'une telle implémentation.

A.3 Détails d'implémentation

Dans notre implémentation, nous avons utilisé une carte Arduino Mega 2560 basée sur un microcontrôleur ATmega 2560, un shield HW-125, une carte SD et un écran LCD comme afficheur du texte.

Le matériel est détaillé dans ce qui suit.

A.3.1 Carte Arduino Mega 2560

L'Arduino Mega 2560 est une plateforme de développement puissante et flexible, idéale pour les projets nécessitant un grand nombre de connexions. Pour pouvoir l'utiliser et la mettre en marche, il suffit de la connecter à un ordinateur à l'aide d'un câble USB qui lui fournit une tension de 5V (ou de l'alimenter avec un adaptateur secteur ou une pile). La carte Arduino Mega 2560 est une carte à microcontrôleur basée sur un ATmega 2560 [53].

Cette carte dispose :
- de 54 broches numériques d'entrées/sorties (dont 14 peuvent être utilisées en sorties PWM (MLI : Modulation de largeur d'impulsion).
- de 16 entrées analogiques (qui peuvent être utilisées en broches entrées/sorties numériques).
- de 4 UARTs (port série matériel).
- d'un quartz de 16 Mhz de fréquence.
- d'une connexion USB.
- d'un connecteur d'alimentation jack.
- d'un connecteur ICSP (programmation "in-circuit").
- d'un bouton de réinitialisation (reset).

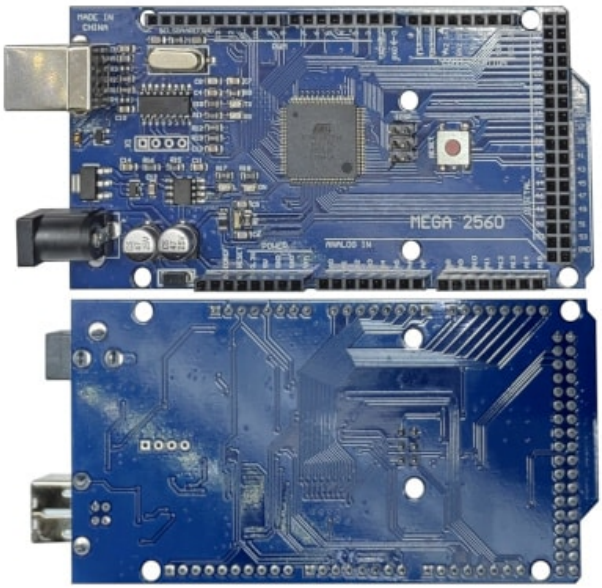


FIGURE A.1 – La carte Arduino Mega 2560.

A.3.2 Écran LCD

Un afficheur LCD est un dispositif qui présente des informations sous forme de caractères alphanumériques, dans un format visuel facilitant leurs lectures et leurs interprétations.

Nous allons utiliser un afficheur LCD afin de visualiser le texte avant et après le chiffrement.

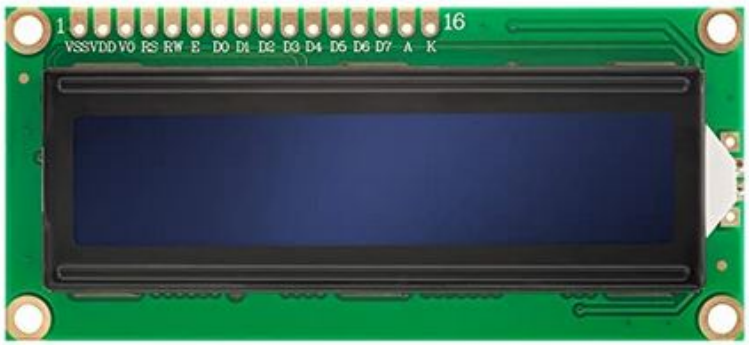


FIGURE A.2 – Écran LCD.

A.3.3 Shield carte mémoire HW-125

Le Shield carte SD HW-125 est une carte d'interface compatible avec Arduino permettant d'ajouter un espace de stockage sur les projets Arduino. Il supporte les cartes SD et les carte micro-SD. Ce module permet de lire et d'écrire des données sur une carte micro-SD. Il utilise l'interface SPI (Serial Peripheral Interface) pour communiquer avec le microcontrôleur.

Ses caractéristiques sont résumées ci-dessous :

• Alimentation (VCC) : 3.3V à 5V

• Interface SPI :

MISO (Master In Slave Out)
MOSI (Master Out Slave In)
SCK (Serial Clock)
CS (Chip Select)

• Compatibilité :

Cartes micro-SD standard SD et SDHC jusqu'à 32GB (FAT16 ou FAT32).
Compatible avec la plupart des microcontrôleurs (Arduino Uno, Mega, etc.).

• Connectivité : Broches de connexion étiquetées (VCC, GND, MISO, MOSI, SCK, CS).

• Dimensions : 28 mm x 28 mm (varie selon le fabricant).

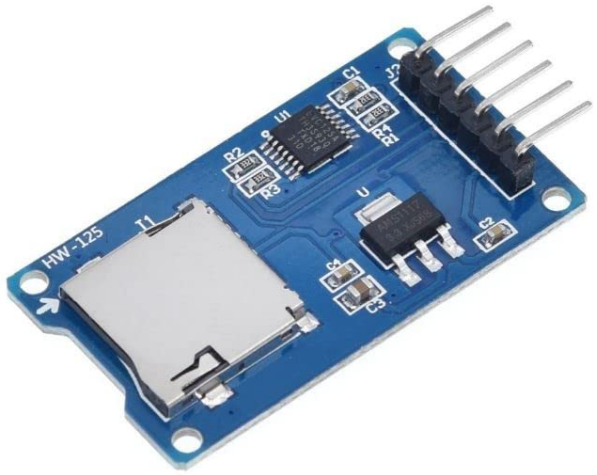


FIGURE A.3 – Le Shield carte mémoire HW-125.

A.3.4 une carte SD

Une carte SD est une forme de stockage de données portable couramment utilisée dans les appareils électroniques tels que les appareils photo numériques, les smartphones, les tablettes et bien d'autres. Elle se présente sous forme d'une petite carte mémoire flash, généralement de la taille d'un timbre-poste, et est conçue pour stocker différents types de données, y compris des photos, des vidéos, de la musique et des documents. Les cartes SD offrent généralement une capacité de stockage allant de quelques mégaoctets à plusieurs téraoctets, selon le type et le modèle. Elles sont faciles à utiliser, durables et souvent compatibles avec une large gamme d'appareils électroniques.

FIGURE A.4 – SD carte mémoire.

A.4 Montage de matériel

Pour notre projet de chiffrement de fichier texte, nous avons utilisé une carte Arduino Mega 2560, un shield carte mémoire HW-125, une carte SD et un écran LCD. La carte Arduino Mega, avec ses nombreuses broches et sa mémoire étendue, est le cœur du système. Le shield facilite les connexions, intégrant le lecteur de carte SD pour le stockage des fichiers texte et l'écran LCD pour afficher le contenu du fichier texte d'abord original puis une fois chiffré. Le programme Arduino lit le fichier texte depuis la carte SD implimantée dans le shield HW-125, applique un algorithme de chiffrement, puis sauvegarde le fichier chiffré sur la carte SD.

La façon dont nous avons réalisé le branchement est résumée dans les tableaux (A.1, A.2) :

Shield de carte SD	**Arduino Mega**
GND	GND
VCC	5V
MOSI	51
MISO	50
SCK	52
SC	53

TABLE A.1 – Connexion du shield de carte SD à l'Arduino Mega

LCD 20×4 I2C	**Arduino Mega**
GND	GND
VCC	5V
SDA	20
SCL	21

TABLE A.2 – Connexion du LCD 20×4 I2C à l'Arduino Mega

Nous avons utilisé le modèle I2C pour la réduction du nombre de fils à 4 au lieu d'utiliser les 16 pins du LCD.

A.4.1 Photo du montage initial

La figure (A.5) illustre le montage initial de l'implémentation.

On peut voir que le texte clair et bien affiché sur l'écran LCD, ce qui montre que le montage est bien installé.

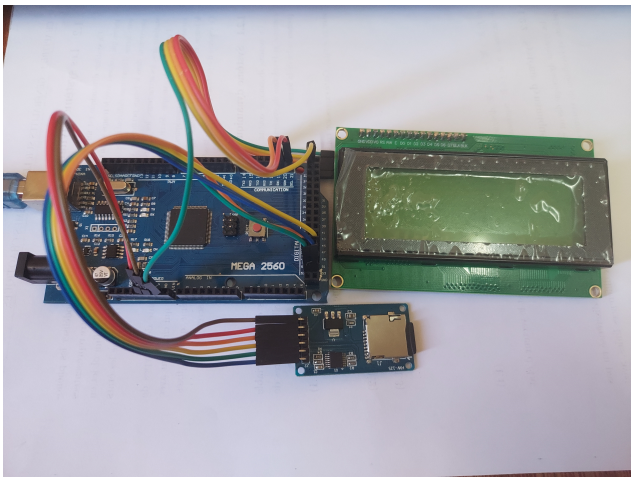


FIGURE A.5 – Le montage initial.

A.4.2 Photo de montage avec résultat

Dans cette partie, nous décrivons le montage final réalisé. Après avoir exécuté le programme Arduino, le fichier texte a été chiffré avec succès, comme indiqué par le message crypté sur l'écran LCD.

La figure (A.6) montre le montage avec le texte clair.

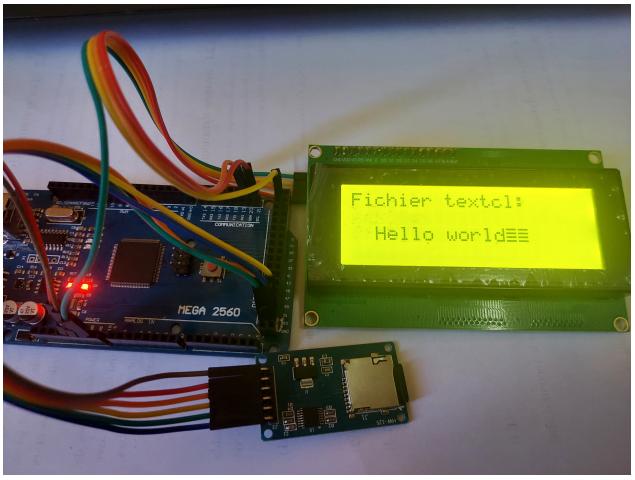


FIGURE A.6 – SD carte mémoire.

La figure (A.7) montre le montage avec le résultat où on peut voir le texte chiffré.

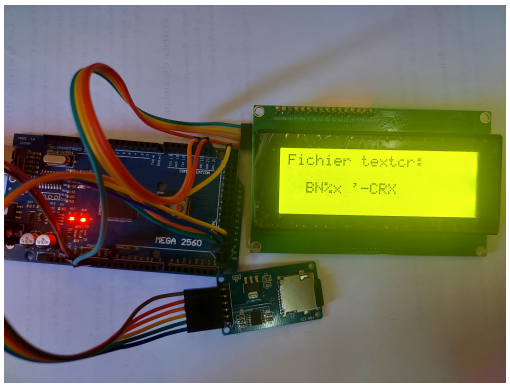


FIGURE A.7 – SD carte mémoire.

A.5 Conclusion

En conclusion, le montage composé de la carte Arduino Mega, du shield carte SD, de la carte SD et de l'écran LCD a permis de développer un système efficace et autonome de chiffrement de fichiers texte. Grâce à la carte Arduino Mega, qui offre une capacité de traitement et de mémoire accrue, nous avons pu lire le fichier texte existant déjà dans la carte SD, appliquer un algorithme de chiffrement, puis sauvegarder le fichier chiffré de retour sur la carte SD. L'écran LCD a joué un rôle crucial en affichant des informations en temps réel, confirmant ainsi le succès de l'opération.

Ce projet démontre la puissance et la flexibilité de programme de chiffrement et des composants Arduino pour des applications de sécurité de données, ouvrant des perspectives intéressantes pour d'autres projets nécessitant la manipulation sécurisée de fichiers.

Pour des fichier plus volumineux, on peut utiliser une carte Arduino plus performante comme la carte Arduino Due ou Arduino Portenta.

Bibliographie

[1] Manuela Tvaronavičienė, Tomas Plėta, and Silvia Della Casa. Cyber security management model for critical infrastructure protection. In *International Scientific Conference „Contemporary Issues in Business, Management and Economics Engineering"*, 2021.

[2] Klaus Schmeh. *Cryptography and public key infrastructure on the Internet*. John Wiley & Sons, 2006.

[3] Florent Chehab. La cryptologie. 2018.

[4] FIPS Pub. Data encryption standard (des). *FIPS PUB*, pages 46–3, 1999.

[5] Vincent Rijmen and Joan Daemen. Advanced encryption standard. *Proceedings of federal information processing standards publications, national institute of standards and technology*, 19 :22, 2001.

[6] Christian Oestreicher. A history of chaos theory. *Dialogues in clinical neuroscience*, 9(3) :279–289, 2007.

[7] Kathleen T Alligood, Tim D Sauer, James A Yorke, and David Chillingworth. Chaos : an introduction to dynamical systems. *SIAM Review*, 40(3) :732–732, 1998.

[8] Abolhassan Razminia, Vahid Johari Majd, and Dumitru Baleanu. Chaotic incommensurate fractional order rössler system : active control and synchronization. *Advances in Difference Equations*, 2011 :1–12, 2011.

[9] Dominique Guegan. Chaos in economics and finance. *Annual Reviews in Control*, 33(1) :89–93, 2009.

[10] Hassan K Khalil. *Control of nonlinear systems*. Prentice Hall, New York, NY, 2002.

[11] Robert C Hilborn. *Chaos and nonlinear dynamics : an introduction for scientists and engineers*. Oxford university press, 2000.

[12] Hamid Hamiche. *Inversion à gauche des systèmes dynamiques hybrides chaotiques : Application à la transmission sécurisée de données.* PhD thesis, Université Mouloud Mammeri, 2011.

[13] Sarah Kassim. *Contribution à la transmission numérique sécurisée de données à base de générateurs de séquences chaotiques d'ordre non entier.* PhD thesis, Université Mouloud Mammeri, 2018.

[14] Moulahoum Mouloud. *Synthése D'Observateurs À Mode Glissant À Entrée Inconnue : Application À La Synchronisation Des Systèmes Chaotiques De Chue.* PhD thesis, Université Mouloud Mammeri, 2014.

[15] David Ruelle and Floris Takens. On the nature of turbulence. *Les rencontres physiciens-mathématiciens de Strasbourg-RCP25*, 12 :1–44, 1971.

[16] Ouerdia Megherbi. *Etude et réalisation d'un système sécurisé à base de systèmes chaotiques.* PhD thesis, Université Mouloud Mammeri, 2013.

[17] Ouerdia Megherbi. *Synchronisation des systèmes chaotiques discrets d'ordre fractionnaire pour la sûreté de communication à base d'observateurs impulsifs.* PhD thesis, Université Mouloud Mammeri, 2018.

[18] Y. Pomeau and P. Manneville. Intermittent transition to turbulence in dissipative dynamical systems. *Communications in Mathematical Physics*, 74 :189–197, 1980.

[19] M. Feigenbaum. Quantitative universality for a class of nonlinear transformations. *Journal of Statistical Physics*, 19 :25–52, 1978.

[20] George Veronis and Linda M Hudon. Summer study program in geophysical fluid dynamics, woods hole oceanographic institution : Chaos. *NASA STI/Recon Technical Report N*, 86 :26580, 1985.

[21] Jinhu Lü and Guanrong Chen. A new chaotic attractor coined. *International Journal of Bifurcation and chaos*, 12(03) :659–661, 2002.

[22] Martial Schtickzelle. Pierre-françois verhulst (1804-1849). la première découverte de la fonction logistique. *Population (french edition)*, pages 541–556, 1981.

[23] Ted Sheehy. Georg friedrich bernhard riemann.

[24] Gastao SF Frederico and Delfim FM Torres. Fractional noether's theorem in the riesz–caputo sense. *Applied Mathematics and Computation*, 217(3) :1023–1033, 2010.

[25] Rudolf Scherer, Shyam L Kalla, Yifa Tang, and Jianfei Huang. The grünwald–letnikov method for fractional differential equations. *Computers & Mathematics with Applications*, 62(3) :902–917, 2011.

[26] J-M d'Hoop. La guerre des codes secrets, des hiéroglyphes à l'ordinateur, 1983.

[27] Lester S Hill. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6) :306–312, 1929.

[28] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4) :656–715, 1949.

[29] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6) :661, 1991.

[30] Charles H Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Theoretical computer science*, 560 :7–11, 2014.

[31] Veronique Guglielmi, PY Besnard, Daniele Fournier-Prunaret, Pierre Pinel, Abdel-Kaddous Taha, and L Beneteau. Un système numérique de cryptographie basé sur les propriétés des signaux chaotiques discrets. In *Proceedings of the GRETSI*, 2003.

[32] Pellicer-Lostao Carmen and López-Ruiz Ricardo. Notions of chaotic cryptography : sketch of a chaos based cryptosystem. In *Applied cryptography and network security*, pages 267–294. IntechOpen London, 2012.

[33] H Masahiko, Takafumi Aoki, Hiroyuki Morimitsu, and Tatsuo Higuchi. Implementation of reaction-diffusion cellular automata. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 49(1) :10–16, 2002.

[34] Gonzalo Alvarez and Shujun Li. Cryptographic requirements for chaotic secure communications. *arXiv preprint nlin/0311039*, 2003.

[35] Mauricio S. Baptista Baptista. Cryptography with chaos. *Physics letters A*, 240(1-2) :50–54, 1998.

[36] Anne Canteaut. Cryptanalyse des chiffrements à clef secrète par blocs. *Journal de la sécurité informatique MISC,(2)*, 2002.

[37] Christina Boura. *Analyse de fonctions de hachage cryptographiques*. PhD thesis, Université Pierre et Marie Curie-Paris VI, 2012.

[38] NW Abderrahim, FZ Benmansour, and O Seddiki. Etude des transmissions chiffrées par synchronisation des systèmes chaotiques. In *international conference on artificial intelegence and information technology*.

[39] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography : principles and protocols*. Chapman and hall/CRC, 2007.

[40] Badis Amarouche and Karim Encadreur Kemih. *Compression et cryptage des vidéos : Application en IoT*. PhD thesis, Université de Jijel, 2021.

[41] John G Proakis and Masoud Salehi. *Digital communications*. McGraw-hill, 2008.

[42] Menezes Alfred, Vanstone Scott, et al. Handbook of applied cryptography, 1997.

[43] Ouerdia Megherbi, Hamid Hamiche, and Maamar Bettayeb. Implementation of a wireless text data transmission based on the impulsive control of fractional-order chaotic systems. *Computers and Electrical Engineering*, 116 :109224, 2024.

[44] Bruce Schneier. *Secrets and lies : digital security in a networked world*. John Wiley & Sons, 2015.

[45] Yehuda Lindell. Introduction to cryptography 89-656. 2006.

[46] Lawrence A Gordon and Martin P Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4) :438–457, 2002.

[47] A KHALDI, Hana BEN CHEIKH, and Khaira BOUZAINE. *Sécurité Des Données Biomédicales Echangées en Télémédecine*. PhD thesis, Université Kasdi Merbah Ouargla.

[48] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3) :379–423, 1948.

[49] Majid Roohi, Chongqi Zhang, and Yucheng Chen. Adaptive model-free synchronization of different fractional-order neural networks with an application in cryptography. *Nonlinear Dynamics*, 100(4) :3979–4001, 2020.

[50] Charles Bouillaguet. *Les attaques cryptographiques sont-elles toujours meilleures que la force brute ?* PhD thesis, Sorbonne Université, 2022.

[51] Miguel Angel Murillo-Escobar, César Cruz-Hernández, Fausto Abundiz-Pérez, and Rosa Martha López-Gutiérrez. Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. *Microprocessors and Microsystems*, 45 :297–309, 2016.

[52] Messaoud Fahem and Denane Lamia. *Conception et réalisation d'un système d'alarme anti-intrusion par barrière laser avec arduino méga 2560.* PhD thesis, Université Mouloud Mammeri, 2016.

[53] Iabbaden Zinedine and Lahlou Farid. *Réalisation d'un module de distribution d'énergie à base d'une carte Arduino méga 2560.* PhD thesis, Université Mouloud Mammeri, 2017.