République Algérienne Démocratique et Populaire Ministère del'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri De Tizi-Ouzou

FACULTÉ DE GÉNIE ÉLECTRIQUE ET INFORMATIQUEDÉPARTEMENT : ÉLECTRONIQUE

Mémoire de Fin d'Etudes de Master Professionnel

Domaine : **Sciences et Technologie**

Filière : **Électronique**

Spécialité : **Électronique Industrielle**

Thèmes :

Réalisation d'un schéma de communication sécurisé à base de la synchronisation de deux systèmes chaotiques à temps discret sur ARDUINO.

Présenté par :

M^elle^ BOUAROUR Lilia

M^r^ DJADEL Jugurtha

dirigé par :

M^elle^ MEGHERBI Ouerdia

- Mémoire soutenu publiquement le 27 Septembre 2023 devant le jury composé de :

  - M^r^ HAMICHE Hamid

    Président M.C.A, Université Mouloud Mammeri de Tizi Ouzou.

  - M^me^ BOUZBOUDJA Ouardia

    Examinateur.

Promotion : 2023

Remerciements

Nous rendons grâce à Dieu pour sa bonté de nous avoir donné la force, le courage et la santé durant la réalisation de ce mémoire de fin d'étude.

Nos vifs remerciements à tous les enseignants du département électronique, de nous avoir enseigné avec persévérance durant nos Années d'études et de recherches.

Un remerciement particulier et très sincère à Madame MEGHARBI Ouerdia, et Monsieur HAMICHE Hamid car leurs appuis et leurs conseils judicieux nous ont été d'une aide fondamentale. Merci aux membres du Jury d'avoir accepté de Juger ce travail.

Nous tenons aussi à exprimer notre gratitude à nos très chères familles qui nous ont soutenus sur le plan moral et spirituelle durant la réalisation de ce mémoire.

Enfin, un grand merci à toutes les personnes et amis(e) qui ontcontribué de près ou de loin à la réalisation de ce travail.

<< la persévérance est la clé de la réussite >>

Dédicaces

A mes chers parents, Il est difficile d'exprimer avec des mots à quel point vousêtes importants dans ma vie, espérant d'être à la hauteur des valeurs que vousavez semées en moi. Dieu vous protège et longue vie.

A ma mère et ma sœur, Qui m'ont donné de leurs énergies etleurs temps ainsi le courage d'être le meilleur de moi-même. Que dieu vous protège.

A ma tante et son fils mokrane, qui m'ont soutenu sur le plan moral et leursconseils et encouragement durant mon parcours.

A mes chers amis qui ne cessent de m'encourager … Rachid L,
Younes B, Masten T, massi C, Karim B, amine A, massyl H. said G,Jugurtha G, yasmine B, Sylia M, et à tous ceux qui ont été là pour moi.

A mon binôme Lilia, pour son courage et sa patience afin d'accomplir ce travail.

Jugurtha.

Dédicaces

En signe de respect et de reconnaissance, je dédie ce modeste travail :

A ma très chère mère, qui m'a tout donnée, qui m'a soutenue par ces prières son amour et sa tendresse, qui a été toujours présente à mes cotées. A tous les moments qui ont marqués ma vie et continue de l'être pour faire mon
Bonheur.

A mon très cher père, pour ses sacrifices et ses conseils, qui m'a encouragé a aller de l'avant tout au long de mes études.

A mes chers frères et sœur, qui Sont ma joie de vivre.
A mon très cher Soufiane pour son soutien apporté chaque jour.

A mon binôme Jugurtha pour sa vive compassion à ma réussite et surtout Pour sa compréhension et sa patience.
A mes très chers amis, Sylia M, Hanane A, Celia K Ouarda O, Younes B, Rachid L, Zineddine A, en témoignage d'un amour spécial et De soutien permanant au cours des études, pour leur attachement et leurs chaleureux encouragements, ainsi qu'à leur aide apportée pour la réussite de notre projet.

A tous mes amis et plus particulièrement les plus intimes, en témoignage Des moments inoubliables, des sentiments sincères et des liens solides qui Nous unissent.

À toutes les personnes qui ont joué un rôle essentiel, même par de petits gestes, dans la réalisation de ce mémoire.

Lilia.

Sommaire

Sommaire

Sommaire

Table des illustrations

Introduction générale :

En 1963, Edward Lorenz expérimentait une méthode pour la prévision météorologique. Par un pur hasard, il a constaté que de légères modifications des données initiales pouvaient avoir un impact significatif sur les résultats, révélant ainsi le concept de sensibilité aux conditions initiales. À partir de 1975, ces systèmes ont été désignés comme "systèmes chaotiques", marquant le début de l'essor de la théorie du chaos dans les années 70. Cependant, il est important de noter que des travaux antérieurs menés par des scientifiques, tels qu'Henri Poincaré à la fin du XIXe siècle, avaient déjà mis en évidence ce phénomène dans le contexte de l'étude astronomique du problème des trois corps [20] [23].

Récemment, l'utilisation du chaos pour sécuriser la transmission d'informations a été considérée comme une solution très prometteuse pour améliorer les performances des systèmes de transmission existants. Ainsi, on trouve dans la littérature une multitude d'applications et d'études réalisées concernant plusieurs aspects de la transmission. Les caractéristiques chaotiques offrent une solution pour les systèmes où il est important de réduire les probabilités de détection et d'interception, ainsi que pour les applications liées à l'accès multiple.

Cependant, malgré ces avantages, il est essentiel de noter que la synchronisation entre deux systèmes dynamiques chaotiques, nécessaire pour récupérer l'information transmise, s'avère être une tâche difficile a priori.

La protection et la confidentialité de l'information ont toujours été toujours un intérêt de l'humanité. Par conséquent, des techniques de cryptage ont été développées pour rendre les informations incompréhensibles à ceux qui ne possèdent pas la clé secrète. Ces méthodes de cryptage suscitent un vif intérêt dans un large éventail de domaines, que ce soit un militaire, un commercial ou personnelle.

Les systèmes de communication sécurisée occupent une place de plus en plus cruciale dans notre société numérique [44]. Dans ce contexte, la synchronisation de systèmes chaotiques offre une approche novatrice pour garantir la confidentialité et la fiabilité des transmissions de données.

Ce mémoire vise à explorer la réalisation d'un schéma de communication sécurisée basé sur la synchronisation de deux systèmes chaotiques à temps discret, en utilisant la plateforme Arduino.

Le mémoire est structuré comme suit :

Le premier chapitre se concentre sur la définition des systèmes dynamiques de manière générale, ainsi les bases de compréhension nécessaires pour aborder le sujet de la synchronisation des systèmes chaotiques. Les systèmes dynamiques, en tant que modèles mathématiques permettant de décrire l'évolution d'un système au fil du temps, jouent un rôle fondamental dans la compréhension de la dynamique chaotique. Ce premier chapitre offre également une exploration détaillée des systèmes chaotiques, mettant en lumière leurs caractéristiques uniques, telles que la sensibilité aux conditions initiales et la non-linéarité.

Le second chapitre constitue une plongée approfondie dans le domaine de la synchronisation des systèmes chaotiques. La synchronisation est un aspect clé de ce schéma de

communication sécurisée, car elle permet à l'émetteur et au récepteur de reproduire et de coordonner les dynamiques chaotiques pour assurer la transmission réussie des données. Ce chapitre examine les différentes méthodes et techniques utilisées pour synchroniser ces systèmes chaotiques, en mettant en évidence leurs avantages, leurs limites et leur applicabilité dans un contexte à temps discret.

Le troisième chapitre se penche sur la structure du schéma de transmission sécurisé basé sur la synchronisation de systèmes chaotiques. Il décrit les éléments clés de ce schéma, notamment les composants matériels et logiciels nécessaires à sa mise en œuvre sur des cartes Arduino. Ce chapitre explore également les défis liés à l'implémentation pratique de ce schéma, tout en proposant des solutions pour garantir son bon fonctionnement.

Le quatrième chapitre, enfin, est consacré à la présentation et à l'analyse des résultats de simulation et d'expérimentation. Il offre un aperçu des performances du schéma de communication sécurisée en action, en mettant en évidence les avantages et les limites observés lors de tests pratiques et de simulations. Ces résultats serviront de base pour évaluer l'efficacité globale du schéma de synchronisation de systèmes chaotiques à temps discret sur des cartes Arduino.

Ce mémoire se situe à l'intersection de la théorie des systèmes dynamiques, de la synchronisation des systèmes chaotiques et de la mise en œuvre pratique sur des microcontrôleurs Arduino. Il vise à contribuer à la recherche en matière de communication sécurisée en explorant cette approche novatrice et en fournissant une base solide pour son application dans divers domaines de la technologie de l'information et des communications.

Chapitre I :
Généralités sur les systèmes chaotiques.

I.1. Introduction et historique du chaos :

Pendant des siècles, les chercheurs ont débattu pour savoir si les effets de causes données pouvaient être précisément liés ou non. L'avènement de l'astronomie au XVIIe siècle, qui a permis de prédire les trajectoires des planètes, a intensifié ce débat. La physique moderne, cependant, suggère que certains phénomènes ne peuvent pas être prédits avec précision, mais peuvent l'être dans une certaine mesure grâce à la théorie du chaos. Cette théorie englobe des concepts tels que les modèles déterministes, la sensibilité aux conditions initiales, les dimensions fractales et les attracteurs étranges [1].

Au fil du temps, le concept de chaos est devenu plus complexe et a été étudié de manière plus approfondie par les scientifiques et les philosophes. Au XVIIIe siècle, le mathématicien français **Henri Poincaré** a commencé à étudier les systèmes dynamiques non linéaires et a découvert que même de petits changements dans les conditions initiales pouvaient conduire à des résultats très différents. Cette découverte a jeté les bases de la théorie du chaos moderne [2].

Dans le milieu scientifique, le concept a émergé dans la seconde partie des années 1970 en tant que science des phénomènes non linéaires complexes montrant certaines caractéristiques communes, **Henri Poincaré (1892**) qui a démontré que certains systèmes mécaniques, dont l'évolution temporelle est gouvernée par des équations hamiltoniennes, peuvent exhiber un mouvement chaotique [3].

Henri Poincaré Etant le plus proche à résoudre le problème de n-corps, il a découvert que l'orbite de trois corps célestes agissantes l'une sur l'autre peut engendrer un comportement imprévisible. Ainsi est née le chaos.

Alors que **Edward Lorenz** travaillait sur un modèle météorologique simplifié, il a découvert qu'un système déterministe simple pouvait engendrer un résultat imprédictible en raison de sa sensibilité aux variations des conditions initiales, ce qui pouvait être représenté graphiquement par un attracteur étrange. Popularisée par la métaphore de l'effet papillon, la théorie du chaos a montré qu'il existait des systèmes dynamiques à la fois aléatoires et déterministes [4].

Au fil des décennies suivantes, l'étude des systèmes chaotiques s'est étendue à de nombreux domaines, tels que la physique, la biologie, l'économie et la finance. Les systèmes chaotiques ont été utilisés pour modéliser des phénomènes tels que les oscillations du cœur, la turbulence, les mouvements des corps célestes, et les fluctuations des marchés financiers.

I.2. Définitions :

I.2.1. Système dynamique :

Un système dynamique se réfère à un système physique qui subit des changements au fil du temps ou en fonction d'une autre variable, selon l'espace de phase spécifique pris en compte. Par exemple, la trajectoire d'un objet en mouvement à travers le temps est un exemple de système dynamique, de même que l'évolution du nombre d'individus dans une population en fonction du temps, ou encore les variations des valeurs d'une fonction en relation avec une variable x. Ces systèmes dynamiques peuvent être classés en deux catégories distinctes : les systèmes dynamiques discrets, où les changements surviennent à des intervalles distincts, et les

systèmes dynamiques continus, où les changements se produisent de manière constante dans la dimension temporelle ou dans un espace de phase donné.

I.2.2. Système dynamique non linéaire :

Les systèmes dynamiques non linéaires sont des systèmes dont le comportement ne peut être décrit par des équations linéaires. Ces systèmes sont souvent chaotiques et imprévisibles, ce qui les rend difficiles à étudier et à comprendre [5].

Les systèmes dynamiques non linéaires sont présents dans de nombreux domaines, notamment en physique, en biologie, en économie et en ingénierie. Ils peuvent être modélisés mathématiquement à l'aide d'équations différentielles non linéaires [6].

I.2.2.1. Temps continu :

$$\dot{\boldsymbol{x}}(\boldsymbol{t}) = \boldsymbol{F}(\boldsymbol{x}(\boldsymbol{t}), \boldsymbol{t}) \tag{I.1}$$

Où $F : \mathbb{R}^n \times \mathbb{R}^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système Si on associe à cette dynamique un état initial

$$\boldsymbol{x_0} = \boldsymbol{x}(\boldsymbol{t_0}) \tag{I.2}$$

Chaque paire sélectionnée de (x_0, t_0) permet d'obtenir une solution :

$\Phi(. ; x_0 , t_0) : \mathbb{R}^+ \rightarrow \mathbb{R}^n$ telle que :

$$\Phi F\ t_0 ; x_0, t_0 = x_0\ et\ \Phi\ F\ t ; x_0, t_0 = F\ (\Phi F\ t ; x_0, t_0 , t) \tag{I.3}$$

Cette solution appelée souvent trajectoire, fournit les états successifs occupés par le système à chaque instant t

I.2.2.2. Temps discret :

Le temps divisé en intervalles distincts et séparés est appelé "temps discret". Comme indiqué précédemment, un système dynamique à temps discret peut être exprimé par un ensemble d'équations aux différences finies qui suivent généralement ce modèle. L'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues [8]. Elle est représentée par le modèle général des équations aux différences finies sous la forme

$$x(k+1) = G(x(k), k) \tag{I.4}$$

G : □^{n} x □ $^+$ → □n Indique la dynamique du système en temps discret.

On peut également identifier pour chaque couple (x_0, k_0) une solution unique

$$\Phi_G\ (.\ ;\ x_0,\ k_0) : \square + \rightarrow \square n$$

Telle que :

$$\Phi_G\ (k_0\ ;\ x_0,\ k_0) = x_0 \text{ et } \Phi_G\ (k + 1;\ x0\ ,\ k_0) = G\ (\Phi_G\ (k;\ x_0\ ,\ k_0\ ,\ k))$$

(I.5)

I.2.3. Comportement chaotique :

La théorie du chaos est un domaine de recherche qui étudie les systèmes chaotiques et leur comportement. Les scientifiques utilisent des outils mathématiques tels que les attracteurs étranges et les fractales pour comprendre ces systèmes.

En comprenant mieux la nature chaotique des systèmes, les scientifiques peuvent prédire et contrôler leur comportement, ce qui a des applications dans de nombreux domaines, notamment la météorologie, l'économie et la biologie. Le modèle chaotique, ci-dessous, donné par **Otto de Rössler** illustre le caractère chaotique de tels systèmes :

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 + ax_2 + 0.01x_1 \ln(x_3) \\ \dot{x}_3 = c + x_3(x_1 - b) \end{cases}$$

(I.6)

Avec $(x1, x2, x3\ )$ le vecteur d'état et a, b et c les paramètres du système.

Le système de Rössler montre un comportement chaotique pour

$a = 0.2,\ b = 0.2, c = 5.7$ *avec les conditions initiales* $x1(0) = 0.01, x2(0) = 0.01$ *et* $x3\ (0) = 0.01.$

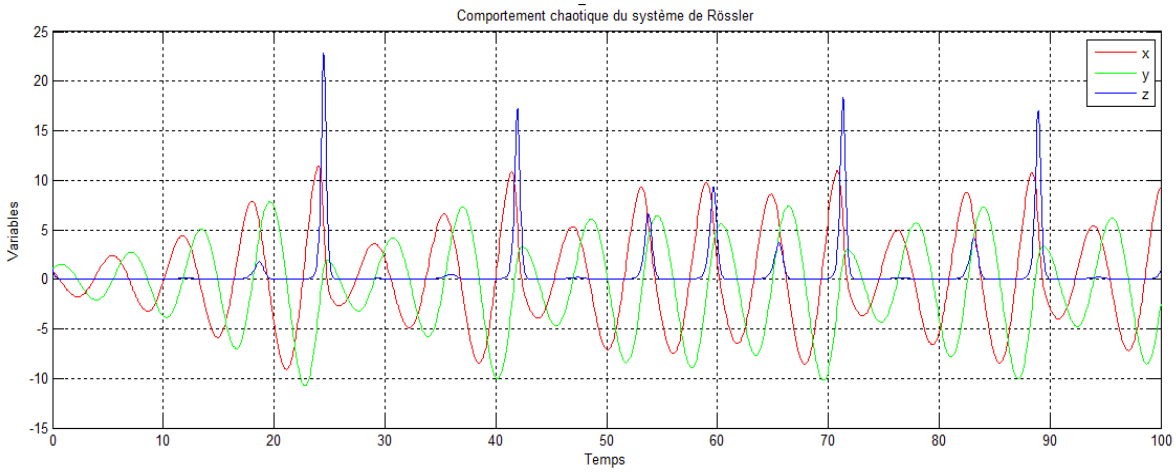

Figure (I.1) : Etat chaotique x_1 du système de Rössler

I.3. Le chaos :

Le concept de chaos tel que compris par les scientifiques ne se réfère pas à l'absence d'ordre, mais plutôt à l'imprévisibilité et à l'incapacité de prédire l'évolution à long terme d'un système en raison de sa forte dépendance à l'égard des conditions initiales. Un système dynamique chaotique est caractérisé par cette sensibilité extrême aux conditions initiales et dépend de multiples paramètres. Contrairement aux systèmes décrits par des équations linéaires ou les lois de la mécanique classique, les systèmes chaotiques ne peuvent pas être déterminés ou modélisés de cette manière. Cependant, ils ne sont pas nécessairement aléatoires et ne relèvent pas uniquement du calcul des probabilités.

Afin de mieux comprendre les systèmes chaotiques, les scientifiques utilisent différentes définitions et propriétés pour les caractériser.

I.3.1 système chaotique :

Les systèmes chaotiques sont des systèmes dynamiques complexes qui présentent une grande sensibilité aux conditions initiales. Cela signifie que de petites variations dans les conditions initiales peuvent conduire à des résultats très différents.

Ces systèmes sont souvent caractérisés par des comportements non linéaires et imprévisibles, ce qui les rend difficiles à modéliser et à comprendre. Les systèmes chaotiques se retrouvent dans de nombreux domaines, comme la météorologie, la physique, la biologie et l'économie.

I.3.2. Propriétés des système chaotiques :

I.3.2.1. Non-linéarité :

Les systèmes chaotiques non linéaires sont définis comme des systèmes dynamiques qui ne peuvent pas être décrits par des équations linéaires.

Ils sont souvent caractérisés par leur comportement imprévisible, leur sensibilité aux conditions initiales, leur dépendance au temps et leur complexité intrinsèque.

I.3.2.2. Déterminisme :

Le déterminisme systémique chaotique est une théorie qui s'intéresse à la complexité des systèmes dynamiques non linéaires. Cette théorie a été développée dans les années 1960 et 1970 par des mathématiciens tels que Edward Lorenz et Mitchell Feigenbaum.

Le déterminisme systémique chaotique se concentre sur la manière dont de petits changements dans les conditions initiales peuvent avoir un impact significatif sur le comportement d'un système dynamique à long terme.

Le déterminisme des systèmes chaotiques est un concept fascinant qui a des implications importantes dans de nombreux domaines différents. Comprendre leur comportement est essentiel pour prédire les événements futurs et prendre des décisions éclairées.

Bien que la prédiction exacte des systèmes chaotiques soit souvent difficile, il est possible de mieux comprendre leur fonctionnement en utilisant des modèles et des simulations. En fin de compte, cela peut nous aider à mieux comprendre notre monde complexe et imprévisible.

I.3.2.3. Aspect aléatoire :

L'aspect aléatoire du système chaotique est dû à la sensibilité aux conditions initiales. Cela signifie que de petites perturbations dans les conditions initiales peuvent avoir un impact important sur le comportement futur du système.

Cela signifie également que même si nous avons toutes les informations nécessaires sur le système, nous ne pouvons pas prédire avec certitude son comportement futur à long terme en raison de la nature imprévisible du système chaotique.

Il existe de nombreux exemples d'aspect aléatoire dans le monde réel. Par exemple, la météo est un système chaotique car de petites variations dans les conditions atmosphériques peuvent entraîner des changements significatifs dans les prévisions météorologiques.

Un autre exemple est le mouvement des fluides, comme les vagues ou les tourbillons. De petites perturbations dans les conditions initiales peuvent entraîner des motifs de flux complètement différents, ce qui rend le mouvement des fluides imprévisible et difficile à modéliser.

L’aspect aléatoire du système chaotique est une caractéristique fascinante qui rend ces systèmes imprévisibles et difficiles à contrôler. Bien que cela puisse présenter des défis, l'aspect aléatoire peut également être utilisé pour résoudre des problèmes complexes et modéliser des phénomènes naturels.

Comprendre l'aspect aléatoire du système chaotique est essentiel pour mieux comprendre les systèmes complexes qui nous entourent et pour développer des solutions innovantes aux problèmes du monde réel.

I.3.2.4. Sensibilité aux conditions initiales :

Les systèmes chaotiques sont des systèmes dynamiques qui présentent une forte sensibilité aux conditions initiales. Cela signifie que de légères variations dans les conditions initiales peuvent entraîner des résultats très différents dans le comportement futur du système. Le concept implique que chaque point individuel d'un système a une signification.

Ce phénomène est communément appelé effet papillon. Par exemple, un papillon battant des ailes au Brésil pourrait potentiellement déclencher une réaction en chaîne d'événements qui aboutit finalement à une tornade au Texas

Le battement d'ailes symbolise une infime altération du point de départ du système, indiquant une légère modification.

Cette sensibilité est due à la nature non linéaire des équations qui décrivent les systèmes chaotiques, ce qui peut conduire à des comportements imprédictibles et apparemment aléatoires.

La sensibilité aux conditions initiales des systèmes chaotiques peut avoir des implications importantes dans de nombreux domaines. Par exemple, de légères variations dans les conditions météorologiques initiales peuvent entraîner des prévisions météorologiques très différentes.

De petites différences dans les conditions initiales d'un marché financier peuvent conduire à des résultats très différents en termes de Prix-là sensibilité aux conditions initiales est une caractéristique clé des systèmes chaotiques, qui peut rendre leur comportement difficile à prévoir. Cependant, en utilisant des outils mathématiques sophistiqués et en recueillant des données précises, les scientifiques peuvent comprendre et prédire le comportement de ces systèmes.

Cela a des implications importantes dans de nombreux domaines, de la météorologie à la finance, et peut aider à améliorer notre compréhension du monde qui nous entoure. Des actions ou de taux de change.

La figure (I.2) illustre la propriété de sensibilité aux conditions initiales sur l'état x_1

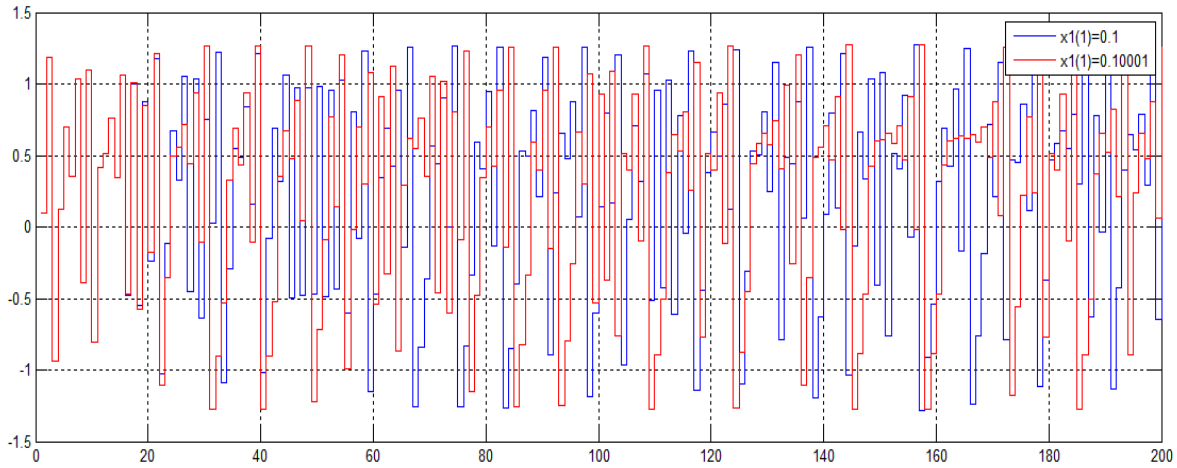

Figure (I.2) : Illustration de la propriété de sensibilité aux conditions initiales sur l'état x_1

I.3.3 Les Exposants de Lyapunov :

Comprendre l'évolution chaotique peut être difficile en raison de sa nature divergente. En raison du mouvement rapide des trajectoires sur l'attracteur, des efforts sont faits pour

déterminer la faisabilité du contrôle d'un tel mouvement rapide. La détermination de la vitesse de divergence ou de convergence est une tâche qui implique une mesure, sinon une estimation. Le taux de vitesse peut être déterminé par l'exposant de Lyapunov, qui est une mesure de la rapidité avec laquelle le comportement d'un système change au fil du temps. Action de séparer deux trajectoires extrêmement proches l'une de l'autre.

Deux trajectoires dans le plan de phase initialement séparées par un taux $Z1$ divergent après un temps

$$\Delta t = t2 - t1 \; vers \; Z2$$

Tel que : $$Z2| \approx e \, \lambda \, \Delta t \, |Z1| \qquad (I.7)$$

Le concept d'exposants de Lyapunov peut être compris comme une extension des valeurs propres, avec un champ d'application plus large. Les solutions périodiques impliquent à la fois des multiplicateurs en virgule fixe et des multiplicateurs caractéristiques. Dans le cas d'un attracteur non chaotique, tous les exposants de Lyapunov ont une signification. Si la somme de deux nombres est négative, on peut en déduire qu'au moins un des nombres est inférieur ou égal à zéro. De plus, le phénomène connu sous le nom d'"attracteur étrange" est présent dans ce scénario. À tout moment, il y aura un minimum de trois exposants de Lyapunov pouvant être identifiés, dont au moins un sera présent. Il est impératif de garder une attitude positive. (Voir le tableau ci-dessus)

Etat stable	**Attracteur**	**Dimension de Lyapunov**	**Exposant de Lyapunov**
Point d'équilibre	**Point**	**0**	**λn ≤ ... ≤ λ1 ≤ 0**
Périodique	**Cercle**	**1**	**λ1 = 0** **λn ≤ ... ≤ λ2 ≤ 0**
Période d'ordre 2	**Tore**	**2**	**λ1 = λ2 = 0** **λn ≤ ... ≤ λ3 ≤ 0**
Période d'ordre K	**K-tores**	**K**	**Λ1 = ... = λK = 0** **λn ≤ ... ≤ λK+1 ≤ 0**
Chaotique		**Non entier**	**λ1 > 0** **∑ i=1 n λi < 0**
Hyper chaotique		**Non entier**	**λ1 > 0, λ2 > 0** **∑ i=1 n λi< 0**

Tableau 1 Classification des régimes permanents selon les exposants de Lyapunov

On constate ici que le nombre d'exposants de Lyapunov nuls indique la dimension d'un attracteur non chaotique. Ainsi, un point fixe est de dimension 0, un cycle limite est de dimension 1 et un tore d'ordre k de dimension k.

I.3.4. Section de Poincaré :

La Section de Poincaré est une notion utilisée en mathématiques et en physique, plus précisément dans le domaine de la théorie des systèmes dynamiques. Elle doit son nom au mathématicien français Henri Poincaré, qui a développé cette idée au début du XXe siècle [9].

La Section de Poincaré est une représentation graphique d'un système dynamique à plusieurs dimensions réduit à une dimension inférieure en utilisant une coupe transversale. Elle permet d'étudier le comportement du système en examinant les intersections de la trajectoire du système avec la coupe. L'idée est de projeter le mouvement du système sur une surface de moindre dimension afin de mieux comprendre les propriétés globales du système [10]. Par exemple, dans le cas d'un système dynamique à trois dimensions, on peut choisir une section transversale bidimensionnelle. Les trajectoires du système seront représentées par des courbes dans cette section. L'étude des intersections de ces courbes avec la section de Poincaré peut révéler des motifs, des bifurcations, des cycles périodiques ou d'autres comportements caractéristiques du système [11].

La Section de Poincaré est une technique puissante utilisée dans de nombreux domaines de la physique et des mathématiques, tels que la mécanique céleste, la théorie du chaos, les oscillateurs, les systèmes dynamiques non linéaires, etc. Elle permet de simplifier l'analyse des systèmes complexes en réduisant leur dimension et en mettant en évidence les caractéristiques importantes du comportement dynamique [12][13].

I.3.5. Notion d'attracteur :

Le concept d'attracteur en mathématiques fait référence à une zone ou à une collection spécifique vers laquelle un système dynamique progresse sur une période de temps. Cet attracteur peut être considéré comme un point focal ou un état stable du comportement du système [10]. Les systèmes dynamiques non linéaires sont souvent corrélés avec les attracteurs, car de légères différences dans les conditions initiales peuvent produire des résultats très disparates sur une période de temps [14]. Un attracteur, dans ce contexte, représente un arrangement particulier vers lequel un système gravite. Il existe plusieurs catégories d'attracteurs, à savoir les attracteurs ponctuels, les attracteurs périodiques et les attracteurs étranges. Les attracteurs ponctuels sont des points individuels vers lesquels le système gravite, tandis que les attracteurs périodiques correspondent à des cycles ou à des motifs répétitifs. Les attracteurs étranges, également connus sous le nom d'attracteurs de Lorenz, sont une forme d'attracteurs chaotiques qui affichent des motifs fractals complexes [15], [16], [17].

La théorie des attracteurs s'est avérée être un outil polyvalent avec des applications dans plusieurs domaines différents, notamment la physique, la biologie, la chimie, l'économie et les sciences de l'environnement. Cette théorie fournit un moyen de modéliser et de comprendre les comportements complexes et dynamiques qui sont présents dans ces systèmes [18][19].

I.3.5.1 Attracteur étrange :

Le concept de l'attracteur étrange est important dans le domaine des systèmes dynamiques non linéaires et de la théorie du chaos. Cette notion a été initialement présentée par Edward Lorenz lors de son étude de la météorologie dans les années 1960. L'exemple

emblématique des équations de Lorenz, également appelées système de Lorenz, est souvent lié à la découverte de l'attracteur étrange [10][20]. Ces équations sont utilisées pour décrire les actions d'un modèle mathématique simplifié de convection atmosphérique. Cependant, leur emploi révélait des propriétés dynamiques à la fois intrigantes et captivantes. L'attracteur étrange de Lorenz est composé de deux lobes primaires qui sont entrelacés, et il a une forme fractale qui se distingue par des motifs récurrents à divers degrés de magnitude. Cela dénote que l'attracteur étrange créé par Lorenz semble complexe et asymétrique, tout en affichant une certaine uniformité et une auto-ressemblance à différents niveaux de grossissement [20].

Les attracteurs étranges ont des implications importantes pour la prévisibilité des systèmes dynamiques. Il est difficile de prédire le comportement futur des systèmes chaotiques à long terme car de petits changements dans les conditions initiales peuvent conduire à des trajectoires radicalement différentes [21].

L'étude des attracteurs étranges à des applications dans divers domaines tels que la physique, la biologie, l'économie, l'ingénierie et même les sciences sociales. Ils permettent de simuler des phénomènes complexes et d'analyser les comportements chaotiques observés dans ces systèmes réels [17][18].

I.3.5.2. Attracteur de Lorenz :

L'attracteur de Lorenz est l'un des exemples les plus célèbres d'un attracteur étrange dans la théorie du chaos et des systèmes dynamiques. Il a été découvert par le mathématicien et météorologue Edward Lorenz dans les années 1960, alors qu'il cherchait à modéliser la convection atmosphérique.

L'attracteur de Lorenz est défini par un système de trois équations différentielles ordinaires, connues sous le nom d'équations de Lorenz :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - xz \end{cases} \tag{I.8}$$

Dans ces équations, x, y et z représentent les variables d'état du système, tandis que a, b et c sont des paramètres fixes. Ces équations décrivent le comportement d'un système dynamique tridimensionnel.

L'attracteur de Lorenz se caractérise par une trajectoire non périodique et une sensibilité aux conditions initiales. Lorsque les paramètres a, b et c sont choisis dans certaines plages spécifiques, le système présente un comportement chaotique. La trajectoire générée par l'évolution des variables d'état forme une structure complexe en forme de papillon avec deux lobes principaux entrelacés.

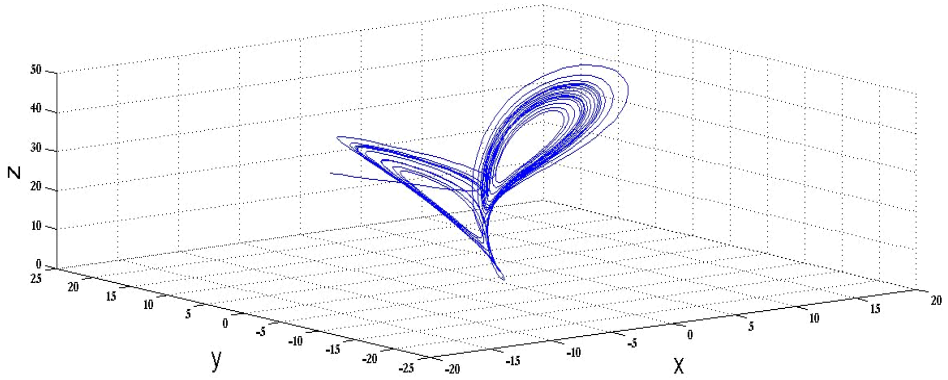

Figure (I.3) : Attracteur de Lorenz

La découverte de l'attracteur de Lorenz a eu un impact majeur sur la compréhension des systèmes dynamiques chaotiques et a montré que de petites perturbations initiales peuvent entraîner des résultats complètement différents à long terme.

I.3.5.3. Attracteur de Hénon :

En 1976, les mathématiciens Michel Hénon et Alain Le Carpentier ont introduit l'attracteur de Hénon, un autre exemple célèbre d'attracteur étrange dans la théorie du chaos et des systèmes dynamiques. Cet attracteur est défini par un ensemble d'équations de récurrence [22] :

$$x(k+1) = y(k) + 1 - ax(k)^2$$

$$y(k+1) = bx(k) \qquad \text{(I.9)}$$

Le système de Hénon montre un comportement chaotique et génère un attracteur étrange pour a= 1.4, $b = 0.3$ $avec$ $x(0) = 0$ et $y(0) = 0$ les conditions initiales du système.

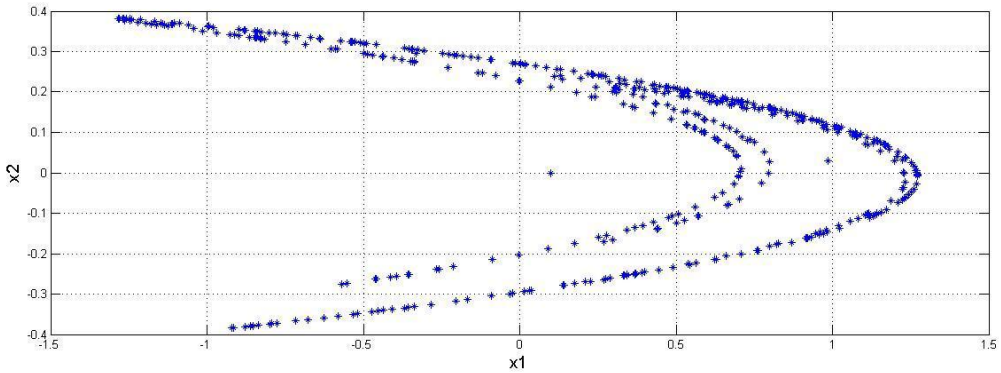

Figure (I.4) : Attracteur de Hénon

Ici, x_n et y_n représentent les variables d'état du système à l'instant n, tandis que a et b sont des paramètres. Les valeurs initiales x_0 et y_0 sont choisies de manière arbitraire.

L'attracteur de Hénon exhibe un comportement chaotique pour certaines valeurs de $a\ et\ b$. Les trajectoires générées par l'évolution des variables
D'état présentent des motifs complexes et une structure fractale. Une visualisation courante consiste à tracer les valeurs successives de $x\ et\ y$ dans un espace bidimensionnel, mettant ainsi en évidence la nature fractale caractéristique de cet attracteur [10].

La découverte de l'attracteur de Hénon a considérablement contribué à notre compréhension de la dynamique chaotique des systèmes non linéaires. Elle a également démontré que des modèles mathématiques relativement simples peuvent engendrer des comportements complexes et imprévisibles. Cette observation a eu un impact significatif sur divers domaines, de la physique à la biologie en passant par les sciences sociales [21].

I.3.5.4. Attracteur de Rössler :

L'attracteur de Rössler est un autre exemple bien connu d'attracteur étrange dans la théorie du chaos et des systèmes dynamiques. Il a été proposé par le mathématicien allemand Otto Rössler en 1976 lors de ses recherches sur la modélisation des oscillations chimiques [23].

L'attracteur de Rössler est décrit par un système d'équations différentielles ordinaires :

$$\begin{cases} \dot{x}_1 = -y - z \\ \dot{x}_2 = x + ay \\ \dot{x}_3 = b + z(x - c) \end{cases} \qquad \text{(I.10)}$$

Dans ces équations, $x, y\ et\ z$ représentent les variables d'état du système, tandis que $a\ , b\ et\ c$ sont des paramètres fixes. Les valeurs initiales $x_0, y_0\ et\ z_0$ sont choisies arbitrairement [10].

L'attracteur de Rössler se caractérise par des trajectoires chaotiques et une structure en forme de spirale. Il présente des propriétés fractales et une sensibilité aux conditions initiales, ce qui signifie que de petites variations dans les conditions initiales peuvent conduire à des trajectoires très différentes à long terme.

La découverte de l'attracteur de Rössler a enrichi notre compréhension de la dynamique chaotique et a eu des applications dans divers domaines, notamment en physique, en chimie, en biologie et en ingénierie. Il a également suscité un intérêt considérable en raison de sa simplicité mathématique et de ses propriétés dynamiques complexes [21].

- La figure (1.5) illustre l'attracteur chaotique du système de Rössler.

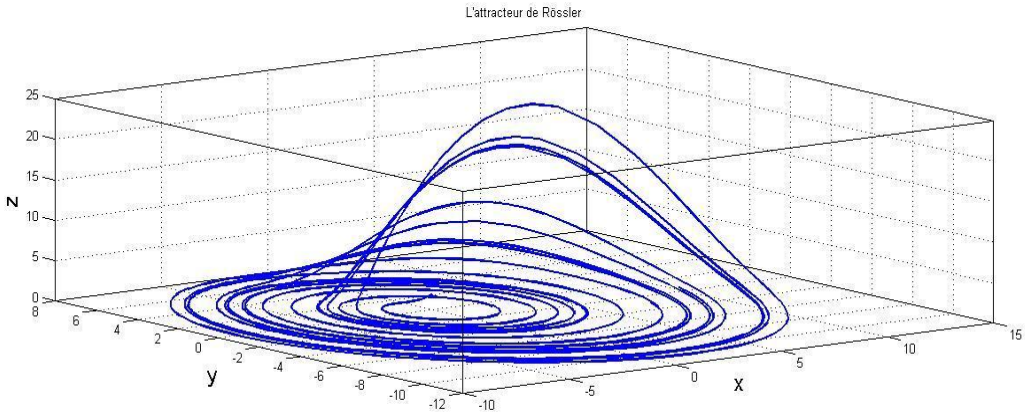

Figure (I.5) : L'attracteur de Rössler

I.4. Bifurcation :

La bifurcation est un concept clé dans l'étude des systèmes dynamiques non linéaires et du chaos. Elle se réfère à un changement qualitatif dans le comportement d'un système lorsque l'un de ses paramètres varie de manière continue. Lorsqu'un système atteint une bifurcation, il peut passer d'un comportement régulier à un comportement chaotique, ou vice versa. Cela signifie qu'une petite variation dans les conditions initiales ou dans les paramètres du système peut entraîner des résultats totalement différents et imprévisibles à long terme [24].

La bifurcation peut être visualisée comme une "route vers le chaos", car elle marque la transition d'un comportement ordonné et prévisible à un comportement complexe et chaotique. Sur cette route, le système peut passer par une série de bifurcations successives, créant ainsi une diversité de comportements dynamiques, tels que des oscillations, des bifurcations périodiques, des attracteurs étranges, etc [18].

Les bifurcations peuvent être étudiées et caractérisées à l'aide d'outils mathématiques tels que la théorie des systèmes dynamiques, les diagrammes de bifurcation et les équations d'évolution. Elles ont des applications dans de nombreux domaines, tels que la physique, la biologie, l'économie et l'ingénierie, où elles aident à comprendre et à modéliser les phénomènes complexes et imprévisibles [21].

I.5. Routes vers le chaos :

La route vers le chaos est un concept complexe qui évoque la transition d'un système stable et prévisible vers un état de désordre et d'imprévisibilité. Elle est souvent associée à des systèmes dynamiques non linéaires, où de petites perturbations initiales peuvent entraîner des résultats très différents à long terme.

Ce phénomène est observé dans divers domaines, de la météorologie à la physique, en passant par l'économie et la biologie. Il met en évidence la sensibilité aux conditions initiales, où de minuscules variations dans les paramètres d'un système peuvent conduire à des trajectoires complètement différentes.

La route vers le chaos est un sujet d'étude fascinant en sciences, car elle remet en question notre capacité à prédire le comportement de systèmes complexes et souligne l'importance de la compréhension des processus non linéaires pour mieux anticiper l'incertitude dans le monde qui nous entoure.

I.6. Conclusion :

Dans ce chapitre, nous avons présenté quelques notions et définitions de base des systèmes dynamiques et le chaos. Telles que les différents types de systèmes dynamiques. Nous avons aussi décrit les principales caractéristiques du chaos : Section de Poincaré, la notion d'attracteur et les exposants de Lyapunov.

Le prochain chapitre se portera sur la synchronisation et le cryptage ainsi que leurs différentes méthodes.

Chapitre II :
Synchronisation des systèmes chaotiques.

II.1. Introduction :

La synchronisation du chaos a été un sujet notable dans la littérature, en particulier depuis les découvertes de Pecora et Carroll [25] [26]. Il a été prouvé que même avec la susceptibilité d'un système aux choix de conditions initiales, Deux systèmes dynamiques indiscernables qui sont structurés dans une configuration maître-esclave peuvent être hautement désordonnés mais capables de se synchroniser parfaitement en l'absence du bruit. Cette possibilité résulte du caractère déterministe du chaos, bien qu'en apparence une trajectoire chaotique soit plutôt assimilable à un signal aléatoire.

Au cours d'une décennie, un modèle ininterrompu de recherche a été noté dans la poursuite de l'utilisation. A des fins de transmission, le désir d'éviter le chaos est surtout motivé par des appréhensions concernant la protection des informations.

La protection des informations est de la plus haute importance, et l'un des moyens de s'en assurer est le cryptage. Le code chaotique peut servir de clé de cryptage à cette fin, Il devient plus simple de maintenir une faible chance de détecter des symboles d'information. De plus, il offre une solution potentielle pour faire face à la rare possibilité de perturbation du signal.

Des points supplémentaires soutenant l'utilisation de systèmes de transmission désordonnés sont fréquemment proposés.

Améliorer le partage des canaux dans un environnement multi-accès (CDMA) tout en gérant la complexité.

Avec l'avènement de la technologie de pointe, le besoin de circuits traditionnels a diminué car il est désormais possible de fonctionner sans une quantité importante de matériel.

II.2. Synchronisation des systèmes chaotiques :

II.2.1. Définition :

L'étude scientifique de la coordination des mouvements entre des systèmes dynamiques chaotiques est connue sous le nom de synchronisation. La synchronisation topologique, qui implique deux attracteurs étranges ayant la même topologie, est un type particulier de synchronisation. Fait intéressant, les scientifiques ont découvert que le cerveau humain peut démontrer une synchronisation topologique, en raison de la nature chaotique de son activité neuronale. Une méthode de synchronisation des systèmes chaotiques consiste à utiliser des observateurs.

II.2.2. Concept et méthodes de synchronisation :

Le processus de synchronisation est basé sur le déterminisme et l'instabilité d'un système chaotique, caractérisé par un ou plusieurs exposants de Lyapunov positifs [27]. Cela permet de créer un système de réplique identique, dans le but d'obtenir une synchronisation

entre les deux systèmes. Le but ultime est que les deux signaux chaotiques produits par les répliques soient indiscernables.

Il existe deux types de synchronisation qui dépendent de la façon dont les deux systèmes chaotiques sont liés : la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

II.2.2.1. Synchronisation unidirectionnelle :

La synchronisation unidirectionnelle est un processus dans lequel les données sont transférées d'un système à un autre dans une seule direction. Cela signifie que les données ne sont transférées que d'une source vers une destination, sans aucune communication de retour de la destination à la source.

Ce type de synchronisation est souvent utilisé dans des scénarios où une source de données est considérée comme la source de vérité et doit être diffusée à d'autres systèmes pour être utilisée. Par exemple, les mises à jour logicielles peuvent être distribuées de manière unidirectionnelle à partir d'un serveur central vers des ordinateurs clients.

Les avantages de la synchronisation unidirectionnelle incluent une réduction de la complexité du système, une amélioration des performances et une meilleure sécurité des données. Cependant, elle peut présenter certains inconvénients, tels qu'une perte de données en cas de panne du système de destination, ou une difficulté à détecter les erreurs ou les conflits de données [27].

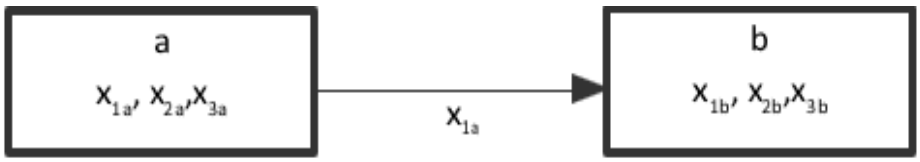

Figure (II.1) : Couplage unidirectionnel

II.2.2.2. Synchronisation Bidirectionnelle :

La synchronisation bidirectionnelle est un processus dans lequel les données sont transférées entre deux systèmes dans les deux directions. Cela signifie que les deux systèmes peuvent envoyer et recevoir des données, et que les modifications apportées à l'un des systèmes sont reflétées dans l'autre système, et vice versa.

Ce type de synchronisation est souvent utilisé dans des scénarios où les deux systèmes doivent être maintenus à jour avec les dernières données, telles que la synchronisation de fichiers entre un ordinateur et un disque dur externe ou la synchronisation de données entre un serveur et un appareil mobile.

Les avantages de la synchronisation bidirectionnelle incluent une meilleure cohérence des données, une amélioration de la collaboration et une meilleure efficacité des processus. Cependant, elle peut également présenter certains inconvénients, tels que la nécessité de gérer les conflits de données qui peuvent survenir lorsque des modifications sont apportées simultanément à deux endroits différents, ainsi que des problèmes de performances si la quantité de données à synchroniser est importante.

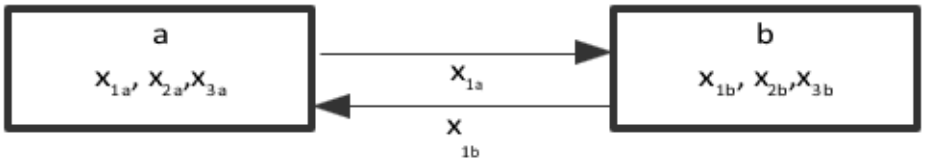

Figure (II.2) : Couplage bidirectionnelle

II.3. Types de synchronisation :

II.3.1. Synchronisation complète :

La synchronisation complète est un processus de synchronisation qui permet de copier intégralement toutes les données d'un système source vers un système de destination. Il existe plusieurs méthodes pour synchroniser des systèmes chaotiques, telles que la méthode du Carroll et Pecora [28]. La synchronisation de systèmes chaotiques peut avoir des applications dans la transmission d'informations [29].

II.3.2. Synchronisation projective :

La synchronisation projective d'un système chaotique est une forme spéciale de synchronisation généralisée, où un système chaotique suit le mouvement d'un autre système chaotique avec une projection linéaire [30]. Plus précisément, la synchronisation projective est établie s'il existe une constante alpha telle que la différence entre les sorties des deux systèmes chaotiques projetées sur un sous-espace de dimension inférieure converge vers zéro [41].

$$\exists a_i \neq 0, \lim_{(t,k)\to\infty} |x_{si} - a_i x_{mi}| = 0, \forall \big(x_m(0), x_s(0)\big) \quad i = 1,2,\cdots,n. \qquad \text{(II.1)}$$

La synchronisation projective est utilisée dans diverses applications, notamment dans la communication sécurisée [31].

II.3.3. Synchronisation retardée :

Lorsqu'un processus de synchronisation subit un retard, on parle de synchronisation retardée. Ce type de retard peut se produire dans diverses formes de synchronisation, telles que la synchronisation audio et vidéo, la synchronisation d'horloge ou même la synchronisation des e-mails.

Dans certaines circonstances, comme lors de la synchronisation audio et vidéo, il peut être nécessaire d'introduire un retard dans la sortie audio pour minimiser l'écart temporel entre les composants audio et visuels. Dans le cas de la synchronisation du courrier électronique, il peut y avoir un retard entre le serveur Exchange et le CUC, ce qui peut entraîner des problèmes de précision de la synchronisation . Le terme est utilisé pour décrire un retard dans le processus de synchronisation, ce qui peut entraîner des problèmes de précision de la synchronisation.

La relation suivante représente l'équation de la synchronisation retardée :

$$\lim_{k\to\infty} \left|\left|x_s(k) - x_m(k-\tau)\right|\right| = 0 \qquad \text{(II.2)}$$

où τ est un retard positif très petit

II.3.4. Synchronisation généralisée :

La synchronisation généralisée d'un système chaotique est un sujet de recherche en physique et en mathématiques. Cette synchronisation est considérée comme une généralisation de la synchronisation complète pour synchroniser des systèmes chaotiques de modèles différents.

Elle se manifeste par une relation fonctionnelle entre deux systèmes chaotiques couplés [32].

$$\lim_{t\to\infty} \left|\left|x_s - \Psi(x_m)\right|\right| = 0 \qquad \text{(II.3)}$$

II.3.5. Synchronisation de phase :

La synchronisation de phase fait référence à la coordination d'une caractéristique dynamique entre les constituants d'un système par le biais de forces externes ou de couplage.

Le terme synchronisation concerne la relation qui se crée entre les phases de deux systèmes en interaction, ou entre la phase d'un système et un signal externe. La synchronisation peut se produire lorsque deux formes d'onde avec la même fréquence ont des angles de phase identiques à chaque cycle. En variante, la synchronisation peut survenir lorsqu'il existe un rapport entier de fréquence entre les signaux cycliques, entraînant le partage d'une séquence répétitive d'angles de phase sur des cycles consécutifs. Divers systèmes présentent une synchronisation de phase, y compris des oscillateurs biologiques comme les lucioles. Il existe différentes méthodologies pour analyser la synchronisation de phase, telles que l'utilisation d'une boucle à verrouillage de phase ou l'évaluation de la synchronisation de phase des signaux provenant de diverses régions du cerveau humain.

L'équation générale de la synchronisation de phase est donnée par :

$$\Delta\theta/\Delta t \;=\; K\, sin(\theta 1 - \theta 2) \qquad \text{(II.4)}$$

II.4. Techniques de synchronisation :

Il existe différentes techniques de synchronisation, dans ce qui suit, nous présentons les deux méthodes les plus fréquentes.

II.4.1. Synchronisation impulsive :

La synchronisation du signal dans la transmission de données est souvent obtenue par synchronisation impulsionnelle. Cette technique implique l'utilisation d'impulsions brèves et rapides pour synchroniser les données entre l'émetteur et le récepteur. Pour maintenir la synchronisation des signaux, ces impulsions sont transmises à intervalles réguliers. La synchronisation par impulsion est largement mise en œuvre dans les systèmes de transmission de données sans fil à haut débit, tels que les réseaux 4G et 5G, ainsi que dans la vidéo numérique [34].

Dans ce schéma de synchronisation, on considère un système maitre de forme générale :

$$\dot{x}(t) = f(x(t)) \qquad \text{(II.5)}$$

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal y(t) = Cx(t) est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état.

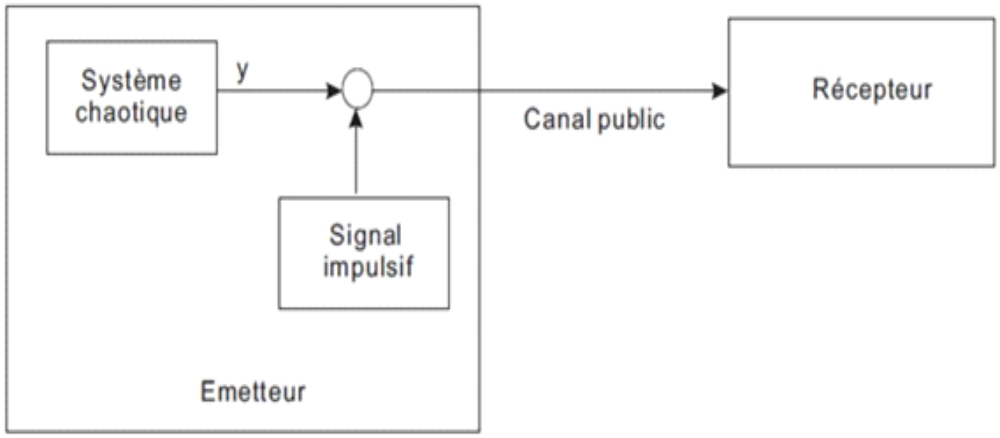

Figure (II.3) Synchronisation impulsive

Les détails concernant cette méthode sont reportés en Annexe.

II.4.2. Synchronisation par boucle fermée :

La synchronisation par boucle fermée est une technique de contrôle utilisée pour maintenir la synchronisation entre deux systèmes ou deux signaux. Elle utilise un mécanisme de rétroaction en boucle fermée pour ajuster l'un des signaux afin qu'il corresponde au mieux à l'autre signal de référence.

Le fonctionnement de la synchronisation par boucle fermée est basé sur une boucle de contrôle comprenant un oscillateur, un diviseur de fréquence, un comparateur de phase et un filtre de boucle. Le signal de référence est utilisé pour régler la fréquence de l'oscillateur, qui est ensuite

divisée en fréquence par le diviseur de fréquence. Le signal de sortie du diviseur de fréquence est comparé au signal de référence à l'aide du comparateur de phase, qui mesure la différence de phase entre les deux signaux. Cette différence de phase est ensuite traitée par le filtre de boucle, qui génère une tension de commande pour ajuster la fréquence de l'oscillateur. Ce processus est répété en boucle fermée jusqu'à ce que la différence de phase entre les deux signaux soit **minimisée** [34].

La synchronisation par boucle fermée est largement utilisée dans les systèmes de communication, notamment pour synchroniser les horloges des équipements de transmission de données, des réseaux de téléphonie mobile ou des systèmes de positionnement par satellite. Elle est également utilisée dans des domaines tels que l'électronique de loisir, la navigation, la métrologie, l'aérospatiale et la défense.

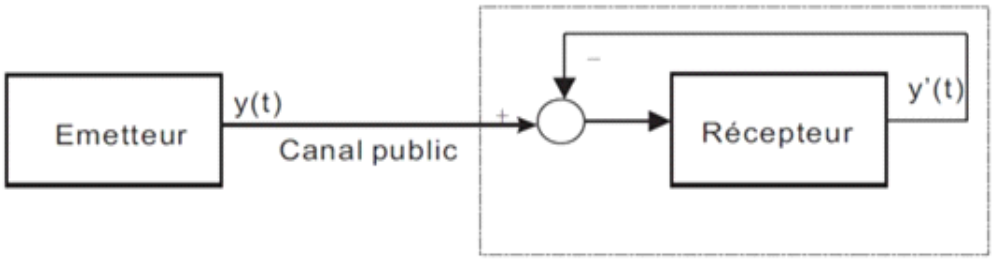

Figure (II.4) : Synchronisation par boucle fermé

II.5.1 Cryptage de données à base de la synchronisation :

Le cryptage de données basé sur la synchronisation est une approche intéressante qui exploite la synchronisation entre deux systèmes pour garantir la sécurité de la communication et du partage de données.

II.5.1.1. Système cryptographique :

Un système cryptographique est un ensemble de techniques et d'algorithmes utilisés pour sécuriser les communications et protéger les données contre les accès non autorisés. Il repose sur des principes mathématiques et des méthodes de chiffrement afin de garantir la confidentialité, l'intégrité et l'authenticité des informations échangées [35][36].

Le fonctionnement d'un système cryptographique implique généralement le Chiffrement ; Décryptage ; Clés ; Protocoles cryptographiques ; Hachage ; et la Signature numérique [37] [38] [39].

II.5.1.2. Similarités entre les systèmes cryptographiques et les systèmes chaotiques :

Les systèmes chaotiques et les systèmes cryptographiques présentent des similitudes intéressantes, bien qu'ils appartiennent à des domaines distincts. Voici quelques similarités entre ces deux types de systèmes :

II.5.1.2.1. Sensibilité aux conditions initiales : Les systèmes chaotiques sont connus pour être extrêmement sensibles aux conditions initiales, ce qui signifie que de petites variations dans les conditions de départ peuvent entraîner des résultats très différents à long terme. De manière similaire, les systèmes

Cryptographiques reposent sur des clés secrètes qui doivent être gardées confidentielles. La divulgation de ces clés peut entraîner la compromission de la sécurité du système cryptographique [35].

II.5.1.2.2. Complexité apparente : Les systèmes chaotiques présentent souvent des comportements complexes et imprévisibles, même s'ils sont déterministes. De même, les systèmes cryptographiques sont conçus pour sembler complexes et difficiles à casser. L'idée est de rendre la tâche des attaquants aussi difficile que possible en rendant la relation entre les clés et les données cryptées difficile à déduire [36].

II.5.1.2.3. Non-linéarité : Les systèmes chaotiques sont généralement non linéaires, ce qui signifie que de petites perturbations dans l'entrée peuvent entraîner des variations importantes dans la sortie. Les systèmes cryptographiques utilisent souvent des fonctions non linéaires dans leurs algorithmes pour rendre la tâche des attaquants plus difficile [37].

II.5.1.2.4. Sécurité par l'obscurité : Dans certains cas, les systèmes chaotiques utilisent des paramètres de contrôle secrets pour générer des comportements chaotiques. De manière similaire, la sécurité des systèmes cryptographiques repose sur le secret de la clé, et non sur la connaissance des algorithmes utilisés [38].

II.5.2. Techniques de cryptage à base de systèmes chaotiques :

Le domaine de la reconstruction des entrées inconnues englobe les tactiques de communication qui tirent parti de la synchronisation des systèmes chaotiques [40][41]. Les systèmes chaotiques sont un sous-ensemble spécialisé de systèmes non linéaires, ce qui signifie que des méthodes applicables aux systèmes non linéaires peuvent également être mises en œuvre sur eux.

L'estimation d'état de systèmes non linéaires à le potentiel d'être une application prometteuse pour un système de communication qui utilise le chaos.

Le processus de transmission d'un message implique la génération d'un signal par l'émetteur, qui est ensuite envoyé via un canal au récepteur désigné. Le destinataire utilise alors une "clé" partagée avec l'expéditeur pour reconstruire le message d'origine.

II.5.2.1 Cryptage par addition :

Le processus de masquage chaotique implique l'utilisation d'un système chaotique indépendant comme émetteur, avec sa sortie y(t) ajoutée au signal de message m(t). Ces deux signaux sont combinés et envoyés via un canal de transmission public au récepteur. Le récepteur est composé d'un système chaotique d'adaptation et d'un soustracteur de base qui permet d'extraire le message après synchronisation des systèmes [42][39]. Il est à noter que cette méthode ne modifie pas l'attracteur étrange du système chaotique avec le message. Un inconvénient de cette technique est que pour réaliser la synchronisation, le message doit être d'au moins 20 à 30 décibels inférieur à la sortie de l'émetteur [40]. Si le bruit du canal est présent à une puissance proche de celle du message, la détection de l'information devient difficile. De plus, cette méthode reste sensible aux attaques extérieures et l'usage du canal de transmission est inefficace du point de vue de l'énergie transmise par rapport à la qualité d'information fournie [34].

Ce schéma représente le cryptage par addition :

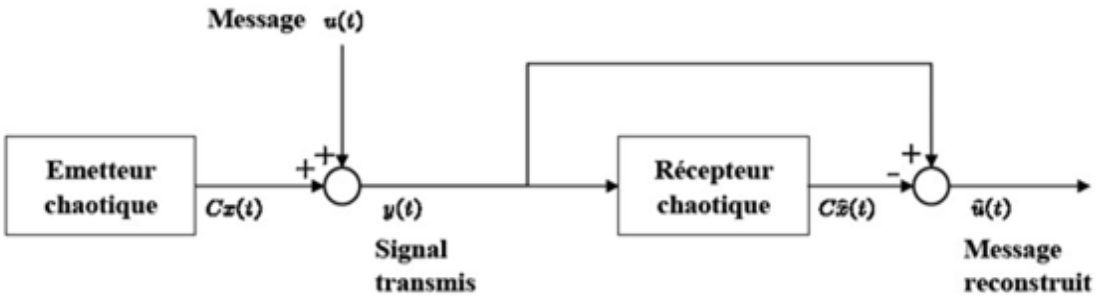

Figure (II.5) : Cryptage par addition

II.5.2.2 Cryptage par commutation :

La cryptographie par commutation du système chaotique est une méthode de cryptage qui utilise des systèmes dynamiques chaotiques pour générer des clés de chiffrement et pour mélanger les données à crypter. Cette méthode consiste à utiliser un système dynamique chaotique pour générer une séquence de nombres aléatoires qui serviront de clé de chiffrement. Ensuite, les données à crypter sont mélangées en utilisant une permutation déterministe basée sur la séquence de nombres aléatoires générée par le système chaotique. Le processus de déchiffrement consiste à appliquer la permutation inverse en utilisant la même séquence de nombres aléatoires. Cette méthode de cryptage est considérée comme très sécurisée car elle utilise des systèmes dynamiques chaotiques qui sont très sensibles aux conditions initiales et aux paramètres de contrôle. Cela signifie que de légères variations dans les conditions initiales ou les paramètres de contrôle peuvent entraîner des comportements chaotiques très différents, ce qui rend très difficile pour un attaquant de retrouver la clé de chiffrement ou les données originales.

Dans le schéma de communication, illustré dans la figure (11), le message d'information est utilisé pour commuter le signal transmis entre deux attracteurs chaotiques statistiquement similaires, qui sont utilisés respectivement pour coder le bit 0 et le bit 1 du message d'information numérique [34].

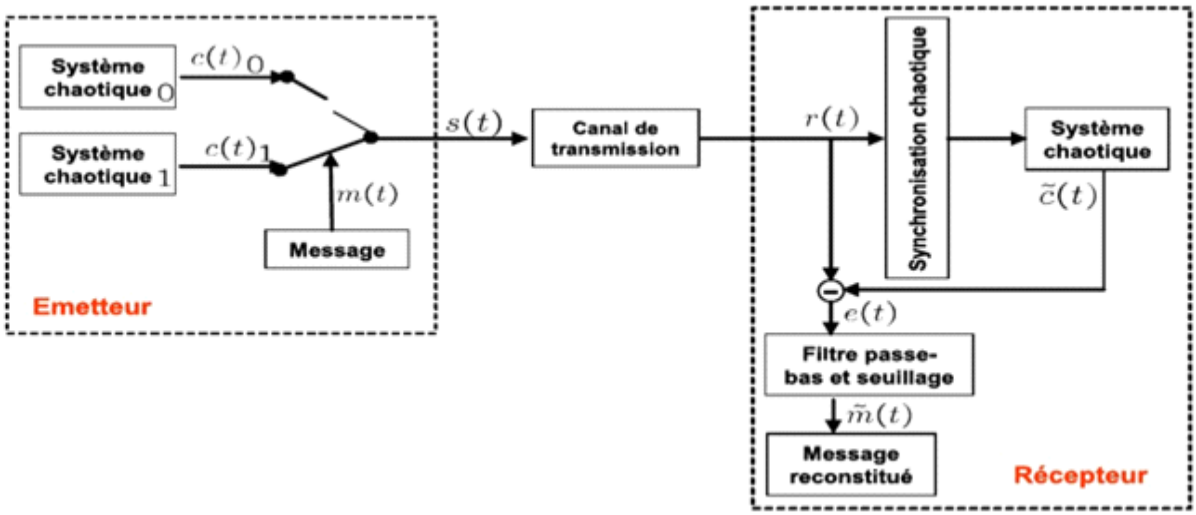

Figure (II.6) : Cryptage par commutation

II.5.2.3. Cryptage par modulation :

Contrairement à l'ajout et à la commutation du cryptage, dans les schémas de modulation chaotiques, un message m(t) est injecté dans le système émetteur, dont la dynamique change constamment avec le message.

Dans ce cas, un contrôleur adaptatif (qui peut également être considéré comme un système dynamique bidirectionnel supplémentaire couplé au système émetteur) est ajouté au système esclave, généralement selon une règle telle que sa sortie m'(t) converge asymptotiquement vers m(t). Afin de suivre la dynamique du système maître, la sortie du contrôleur (c'est-à-dire m(t)) doit être injectée dans le système esclave de la même manière que le système maître. La figure (12) illustre la structure de base d'un système de modulation chaotique typique. Notez que dans certains systèmes modulés chaotiquement, il peut n'y avoir aucune rétroaction s(t) dans le système principal [34][45].

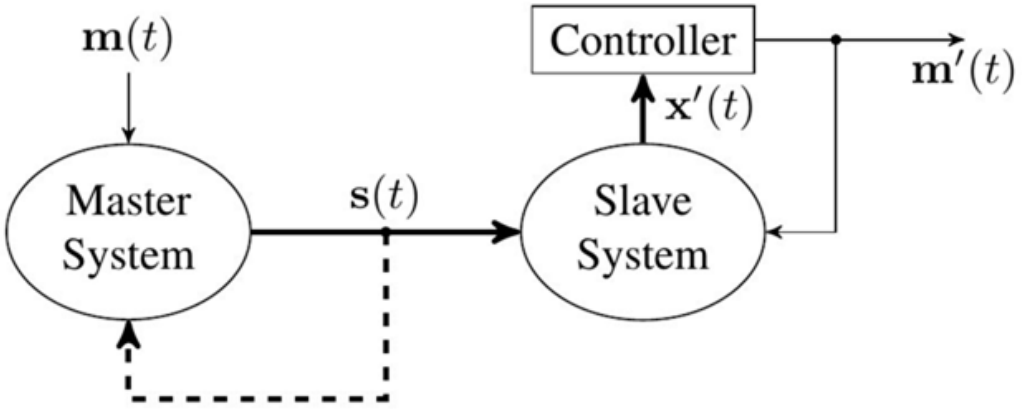

Figure (II.7) : Cryptage par modulation

II.5.2.4. Cryptage par inclusion :

La technique de cryptage par inclusion consiste à intégrer le message dans la dynamique de l'émetteur. Pour restaurer l'information, deux techniques principales sont utilisées : l'utilisation d'observateurs à entrées inconnues ou l'inversion du système émetteur [40]. Cette méthode présente de nombreux avantages et reste largement utilisée dans la pratique [40].

II.5.2.5. Cryptage mixte :

Pour répondre aux problèmes de sécurité rencontrés dans les méthodes précédentes, une nouvelle approche a été proposée, combinant les principes de la cryptographie standard et de la synchronisation chaotique. Dans cette technique, le message u(t) contenant l'information est cryptée à l'aide d'une clé c(t) générée par l'émetteur chaotique. Le message crypté est ensuite injecté dans la dynamique du système chaotique pour augmenter sa complexité. Par la suite, un signal y(t), dépendant des variables d'état de l'émetteur, est transmis au récepteur qui établit une

synchronisation avec l'émetteur. Le récepteur reconstruit ensuite la clé, lui permettant finalement de décoder le message.

Le schéma général de cette méthode est illustré dans la figure (13) [33].

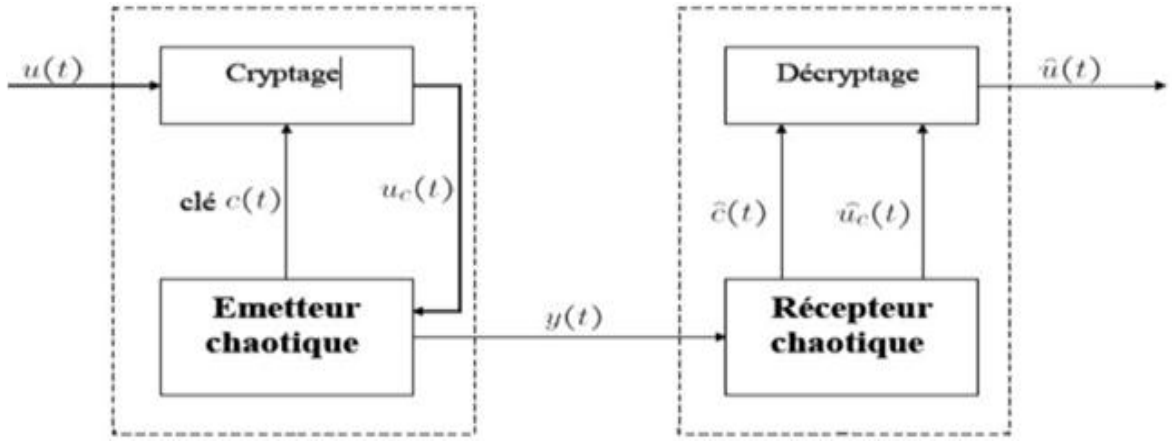

Figure (II.8) : Cryptage mixte

II.6. Conclusion :

Dans ce chapitre, nous venons de voir le principe de synchronisation des systèmes chaotiques ainsi que les différentes méthodes utilisées pour la synchronisation.

Dans le chapitre qui suit nous allons passer à la réalisation du système de transmission de données sécurisées en utilisant une carte Arduino Mega2560.

Chapitre III :

Structure du schéma de transmission et implémentations sur cartes ARDUINO.

III.1 Introduction :

Arduino est une plateforme de développement électronique open-source qui a révolutionné le monde de la création de projets électroniques et informatiques DIY (Do It Yourself) depuis son introduction en 2005. Cette plateforme est largement utilisée par les passionnés d'électronique, les étudiants, les artistes et les ingénieurs pour créer une grande variété de dispositifs interactifs et automatisés.

Les projets Arduino peuvent varier en complexité, allant de simples clignotements de LED à des systèmes sophistiqués de contrôle domotique, de robots autonomes, d'instruments de mesure, et bien plus encore. Arduino a également une communauté mondiale active qui partage des projets, des tutoriels et des conseils en ligne, ce qui en fait une ressource précieuse pour les personnes désireuses d'apprendre l'électronique et la programmation.

Dans ce chapitre on vise à réaliser un système de communication sécurisée basé sur la synchronisation de systèmes chaotiques à temps discret, en utilisant le système de Hénon comme source de chaos. Nous allons présenter les détails de la conception de notre schéma de transmission sur des cartes Arduino.

III.2. Cartes Arduino :

III.2.1. Définition :

Les cartes Arduino sont des plateformes de développement open-source populaires pour la création de projets électroniques interactifs. Elles sont largement utilisées par les amateurs, les étudiants, les ingénieurs et les concepteurs pour créer une variété de dispositifs électroniques et d'objets connectés.

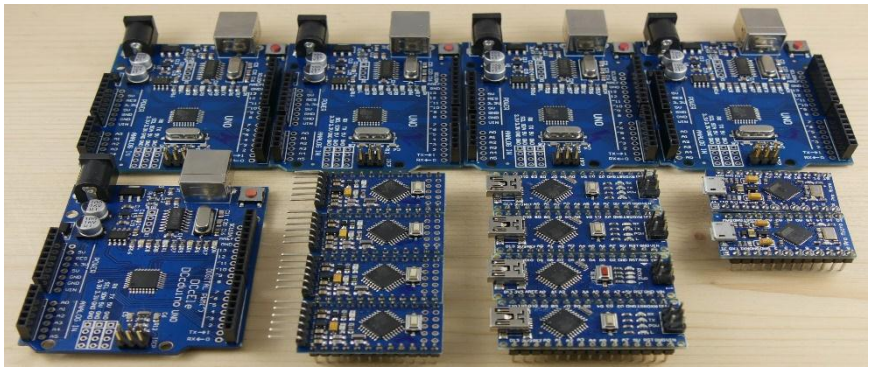

Figure (III.1) : Les cartes ARDUINO

III.2.2. Historique de la carte Arduino :

L'histoire des cartes Arduino est intéressante et témoigne de leur évolution depuis leur création. Voici un bref historique des cartes Arduino :

Début des années 2000 l'histoire des cartes Arduino commence en Italie, où un groupe de chercheurs et d'étudiants, dont Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino et David Mellis, travaillait au sein de l'Interaction Design Institute Ivrea (IDII) à Ivrea, en Italie. Ils ont créé Arduino en tant que plate-forme de prototypage rapide pour leurs projets interactifs [34]. En 2005 la première carte Arduino, appelée « Arduino Serial », est créée. Elle est basée sur le microcontrôleur ATmega8 d'Atmel [35]. Cette carte originale est conçue pour être abordable et facile à utiliser, avec un matériel et un logiciel open-source. Une année après l'équipe Arduino lance l'Arduino Diecimila, qui est la première carte Arduino à utiliser un

convertisseur USB-série intégré (l'ATmega168) pour simplifier la connexion à un ordinateur. Et en 2008 l'Arduino Uno est introduite, dotée de l'ATmega328 et de nombreuses améliorations par rapport aux modèles précédents, notamment une plus grande capacité de mémoire flash et de RAM [34]. En 2010 la popularité d'Arduino ne cesse de croître, et de nombreuses variantes et clones d'Arduino apparaissent sur le marché. Arduino LLC est créée pour gérer la marque Arduino et protéger l'écosystème [35]. L'année 2012 Arduino Due est introduite, utilisant un microcontrôleur ARM Cortex-M3, ce qui marque un écart par rapport aux microcontrôleurs AVR utilisés précédemment. Cela ouvre la porte à des projets plus puissants [34]. Un an plus tard Arduino lance la série Arduino Yun, qui intègre le Wi-Fi, facilitant la connectivité Internet des objets (IoT). Ensuite en 2016 Arduino crée la série MKR pour répondre spécifiquement aux besoins de l'IoT, avec des cartes intégrant des modules de communication tels que le Wi-Fi, le Bluetooth et le GSM. Et en 2020 Arduino annonce l'Arduino Portenta H7, basée sur un microcontrôleur ARM Cortex-M7 et destinée aux applications IoT et à faible consommation d'énergie [34].

L'histoire d'Arduino est marquée par sa croissance constante et sa contribution significative à la communauté des fabricants, des développeurs et des amateurs d'électronique. Elle a permis à des milliers de personnes dans le monde entier de créer des projets électroniques innovants et d'apprendre l'électronique de manière ludique et accessible. Arduino est devenu un acteur clé dans l'Internet des objets et l'automatisation domestique [35].

III.3. Caractéristiques des cartes Arduino :

Les caractéristiques des cartes Arduino peuvent varier en fonction du modèle spécifique, car il existe de nombreuses variantes et générations différentes [36]. Cependant, voici un aperçu des caractéristiques générales que l'on peut trouver sur de nombreuses cartes Arduino :

III.3.1. Microcontrôleur : Chaque carte Arduino est équipée d'un microcontrôleur qui exécute le code que vous programmez. Les microcontrôleurs les plus courants utilisés dans les cartes Arduino sont de la famille des Atmel AVR ou des microcontrôleurs ARM [37].

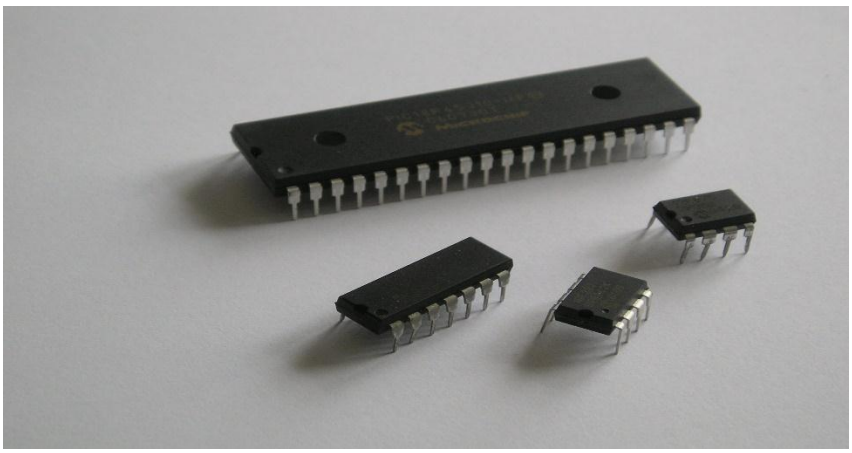

Figure (III.2) : Microcontrôleur

III.3.2. Entrées/Sorties (E/S) : Les cartes Arduino sont dotées de broches d'entrée/sortie numériques (E/S) et analogiques. Les broches numériques peuvent être utilisées pour lire ou écrire des signaux binaires, tandis que les broches analogiques peuvent être utilisées pour lire des signaux analogiques tels que des capteurs de lumière ou de température [34].

III.3.3. Tension de fonctionnement : La plupart des cartes Arduino fonctionnent à une tension de 5 volts, bien que certaines cartes MKR fonctionnent à 3,3 volts.

III.3.4. Mémoire : Les cartes Arduino ont généralement une mémoire flash pour stocker le programme que vous téléchargez, de la RAM pour stocker les données en cours d'exécution du programme, et de l'EEPROM pour stocker des données persistantes [36].

Figure (III.3) : Mémoire

III.3.5. Interface USB : Les cartes Arduino sont généralement équipées d'une interface USB qui permet de les programmer et de les connecter à un ordinateur pour la communication série.

Figure (III.4): Câble USB

III.3.6. Connectivité : Certaines cartes Arduino sont équipées de fonctionnalités de connectivité telles que le Wi-Fi, le Bluetooth ou le GSM pour faciliter la communication avec d'autres appareils ou l'accès à Internet [38].

1.

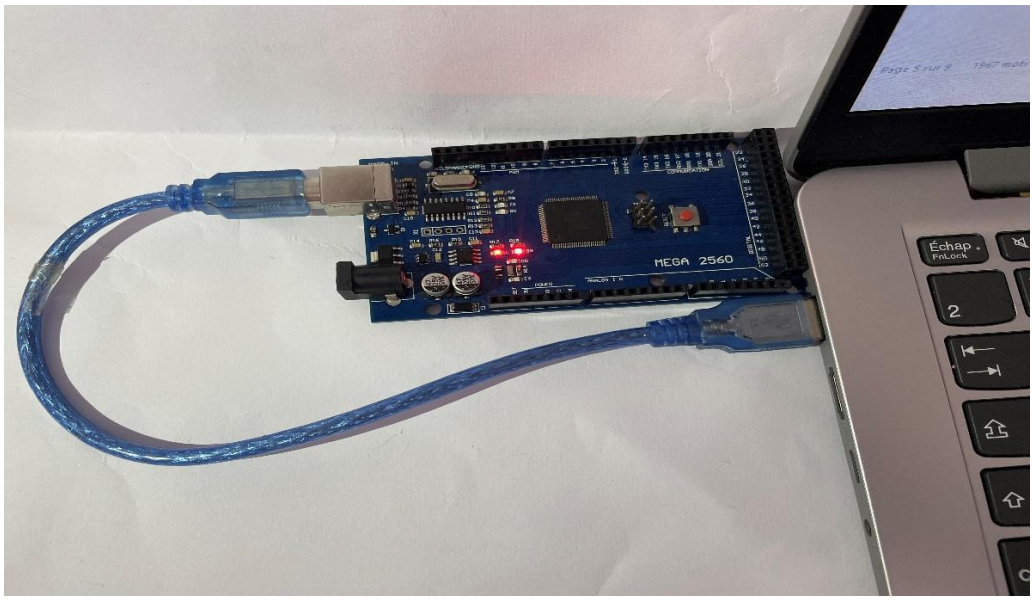

Figure (III.5) : Connectivité de l'ARDUINO

III.3.7. Compatibilité avec les Shields : Les cartes Arduino sont conçues pour être extensibles à l'aide de « Shields », des cartes d'extension qui se fixent au-dessus de la carte principale pour ajouter des fonctionnalités supplémentaires. Les broches des cartes Arduino sont généralement disposées de manière à permettre la connexion facile de ces Shields [39].

III.3.8. Environnement de développement : Les cartes Arduino sont programmables à l'aide de l'environnement de développement Arduino, qui est un logiciel open-source basé sur le langage de programmation C/C++. Cet environnement simplifie la programmation des cartes Arduino.

III.3.9. Polyvalence : Les cartes Arduino sont polyvalentes et peuvent être utilisées pour une grande variété de projets, de l'automatisation domestique à la robotique, en passant par l'Internet des objets (IoT) et bien plus encore [38].

III.4. Types des cartes Arduino :

Il existe de nombreux types de cartes Arduino, chacune conçue pour répondre à des besoins spécifiques [55]. Voici une liste de certains des types de cartes Arduino les plus courants, ainsi qu'une brève description de leurs caractéristiques principales :

III.4.1. Arduino Uno : L'Arduino Uno est l'une des cartes Arduino les plus populaires. Elle est équipée d'un microcontrôleur ATmega328P, dispose de 14 broches numériques, 6 broches analogiques et est largement utilisée pour les projets de base [37].

Figure (III.6) : ARDUINO UNO

III.4.2. Arduino Mega : L'Arduino Mega offre plus de broches d'entrée/sortie que l'Arduino Uno (54 broches numériques et 16 broches analogiques). Elle est idéale pour les projets nécessitant de nombreuses connexions [36].

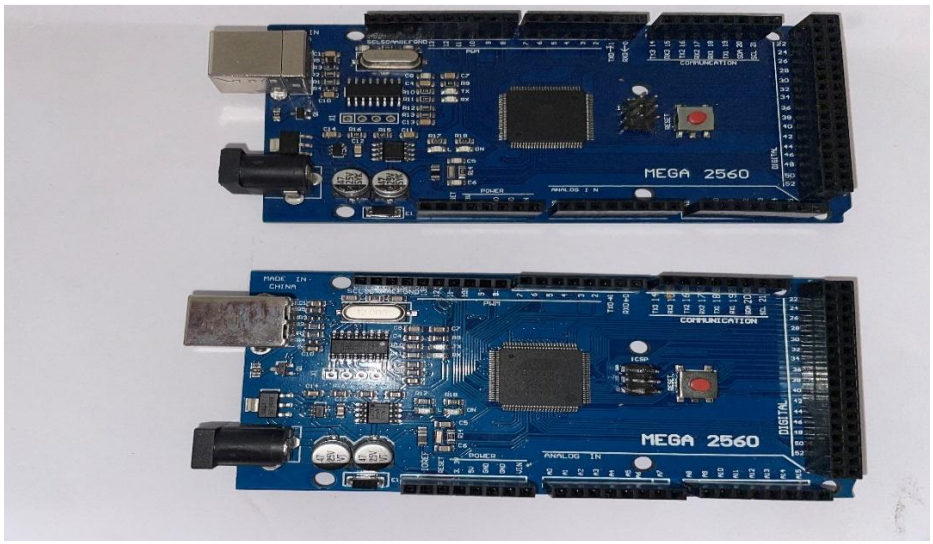

Figure (III.7) : ARDUINO Méga

III.4.3. Arduino Nano : Le Nano est une version compacte de l'Arduino Uno. Il est idéal pour les projets avec des contraintes d'espace tout en offrant des fonctionnalités similaires.

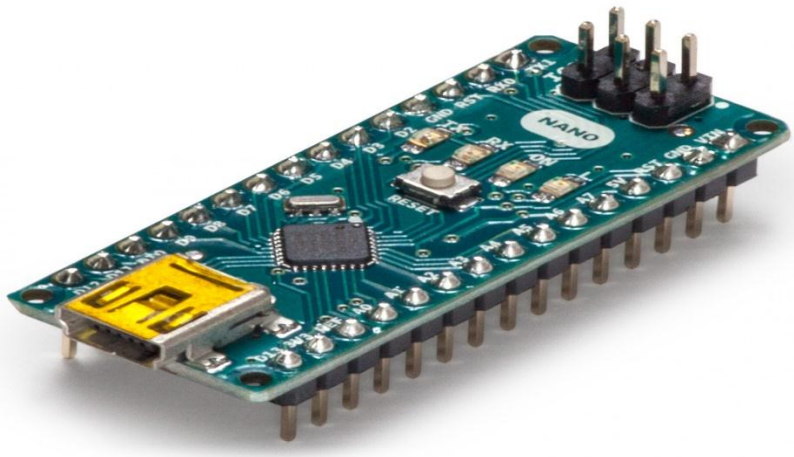

Figure (III.8) : ARDUINO Nano

III.4.4. Arduino Due : Basée sur un microcontrôleur ARM Cortex-M3 SAM3X8E, l'Arduino Due est plus puissant que les modèles basés sur l'ATmega et est adaptée à des projets plus avancés.

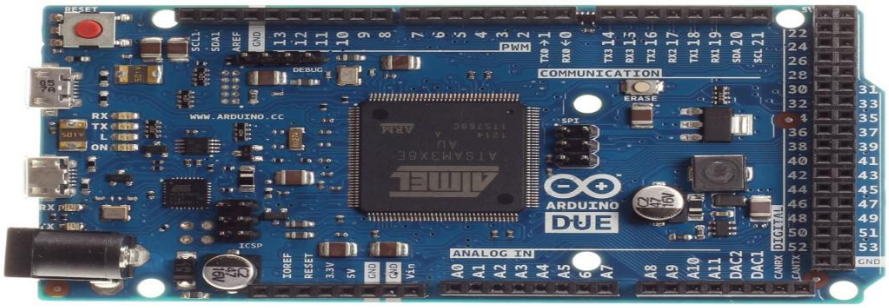

Figure (III.9): ARDUINO DUE

III.4.5. Arduino Leonardo : Cette carte utilise le microcontrôleur ATmega32U4 et peut émuler un clavier ou une souris USB. Elle est souvent utilisée pour des projets d'interface utilisateur.

Figure (III.10): ARDUINO Leonardo

III.4.6. Arduino Pro Mini : Une version minimaliste de l'Arduino basée sur l'ATmega328, idéale pour les projets où l'espace est limité.

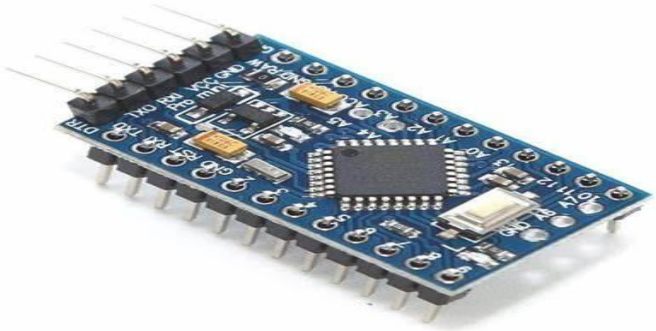

Figure (III.11) : ARDUINO Pro mini

Il existe de nombreuses autres variantes d'Arduino, chacune ayant ses propres caractéristiques et avantages.

III.5. Carte Arduino Mega2560 :

Dans notre projet on a choisi la carte Arduino Mega2560. Après avoir pris en compte les caractéristiques de chaque modèle, ainsi que les exigences spécifiques de notre projet, nous avons fait un choix éclairé. Notre sélection s'est portée sur l'Arduino Mega2560, une carte polyvalente et puissante qui offre une multitude de broches d'entrée/sortie, une capacité de traitement étendue, et la possibilité de gérer des projets complexes et exigeants.

III.5.1. Définition :

La carte Arduino Mega2560 est l'une des variantes les plus populaires de la famille Arduino, et elle est souvent choisie pour les projets nécessitant de nombreuses entrées/sorties et une capacité de traitement élevée [41].

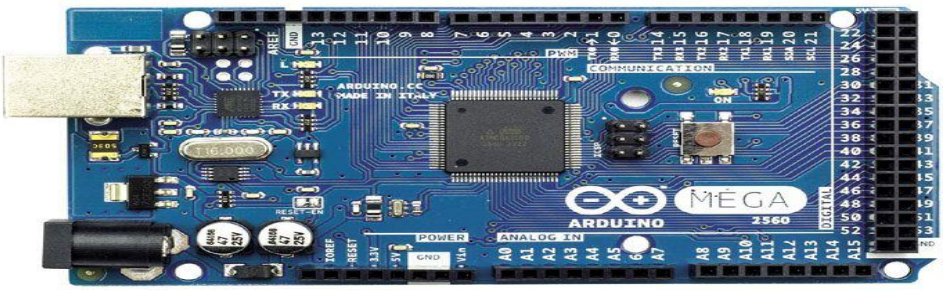

Figure (III.12) : Carte ARDUINO Mega2560

III.5.2. Les caractéristiques de la carte Arduino Mega2560 :

Voici un aperçu des caractéristiques de la carte Arduino Mega2560 :

III.5.2.1. Microcontrôleur : La carte Arduino Mega2560 est équipée d'un microcontrôleur ATmega2560 d'Atmel . Ce microcontrôleur est basé sur une architecture AVR 8 bits et dispose de 256 Ko de mémoire flash, de 8 Ko de RAM et de 4 Ko d'EEPROM [42].

III.5.2.2. Entrées/Sorties (E/S) : La carte Arduino Mega2560 offre un total de 54 broches numériques d'entrée/sortie, dont 15 peuvent être utilisées comme sorties PWM (modulation de largeur d'impulsion) pour la commande de moteurs et d'autres dispositifs. Elle dispose également de 16 broches analogiques pour la lecture de signaux analogiques.

III.5.2.3. Tension de fonctionnement : La carte fonctionne sous une tension de 5 volts.

III.5.2.4. Interface USB : Elle est équipée d'une interface USB permettant la programmation et la communication avec un ordinateur. Elle utilise un convertisseur USB-série pour cette communication.

III.5.2.5. Mémoire : La carte dispose de 256 Ko de mémoire flash, 8 Ko de RAM et 4 Ko d'EEPROM, ce qui en fait une option robuste pour les projets nécessitant beaucoup de

III.5.2.6. Polyvalence : En raison de son grand nombre de broches d'E/S et de sa mémoire étendue, l'Arduino Méga 2560 est adaptée à une grande variété de projets, y compris la robotique, l'automatisation, les projets de contrôle de moteurs, et bien d'autres encore.

L'Arduino Méga 2560 est un excellent choix pour les projets complexes qui nécessitent de nombreuses connexions ou des capacités de traitement accrues. Elle offre une grande polyvalence et convient bien aux projets où l'espace n'est pas un problème et où la complexité est élevée.

III.5.3. Les avantages de la carte Arduino Mega256 :

III.5.3.1. Nombre élevé de broches d'E/S : La carte Arduino Méga 2560 dispose de 54 broches numériques d'E/S, dont 15 peuvent être utilisées comme sorties PWM. Cela permet de connecter un grand nombre de composants et de périphériques externes tels que capteurs, actionneurs, afficheurs, et bien plus encore.

III5.3.2. Nombre élevé de broches analogiques : Elle offre 16 broches analogiques pour la lecture de signaux analogiques, ce qui est utile pour la surveillance de capteurs analogiques comme les capteurs de température, de lumière, ou de pression [43].

III.5.3.3. Mémoire étendue : La Méga 2560 est dotée de 256 Ko de mémoire flash, 8 Ko de RAM et 4 Ko d'EEPROM. Cette mémoire étendue permet le stockage de programmes complexes et de grandes quantités de données [43].

III.5.3.4. Puissance de traitement : Bien qu'elle soit basée sur une architecture AVR 8 bits, la Mega 2560 fonctionne à une fréquence d'horloge de 16 MHz, ce qui lui permet d'exécuter des tâches de traitement relativement rapidement.

III.5.3.5. Compatibilité avec les shields : Comme de nombreuses autres cartes Arduino, la Mega 2560 est compatible avec une large gamme de « shields » (cartes d'extension) conçus pour ajouter des fonctionnalités spécifiques, ce qui facilite l'extension de ses capacités.

III.5.3.6. Polyvalence : En raison de ses nombreuses broches d'E/S, de sa mémoire étendue et de sa puissance de traitement, la Mega 2560 est adaptée à une grande variété de projets, notamment la robotique, l'automatisation, les systèmes de contrôle de moteurs, les stations météorologiques, les projets domotiques et bien plus encore.

III.5.3.7. Communauté et ressources : En tant que membre de la famille Arduino, la Mega 2560 bénéficie du soutien d'une vaste communauté d'utilisateurs, ce qui signifie qu'il existe de nombreuses ressources en ligne, tutoriels et exemples de code disponibles pour vous aider à démarrer rapidement.

III.5.3.8. Amorçabilité : Comparée à certaines autres cartes de développement similaires, la Méga 2560 offre de nombreuses fonctionnalités à un coût relativement bas.

III.6. Structure du schéma de transmission :

La structure d'un schéma de transmission est semblable à l'architecture d'une communication fluide. Elle comprend trois éléments clés :

III.6.1. Émetteur : C'est le point de départ de la communication. Il prend les données, les traite si nécessaire (compression, codage, etc.), puis les transmet sous forme de signaux appropriés par l'intermédiaire d'un canal de transmission.

L'émetteur peut s'écrire sous la forme suivante :

$$x(k+1) = Ax(k) + B + F(.) \qquad \text{(III.1)}$$

III.6.2. Canal de Transmission : Le canal agit comme un support physique (câbles, air, fibres optiques, etc.) par lequel les signaux sont transmis de l'émetteur au récepteur. Ce canal peut être sujet à des interférences, des perturbations ou du bruit [44].

III.6.3. Récepteur : Le récepteur reçoit les signaux du canal de transmission, les décode, les traite si nécessaire (décompression, décodage, etc.), et les présente sous une forme compréhensible pour l'utilisateur ou la machine de destination [44] .

De même le récepteur peut s'écrire de la même manière que l'émetteur autrement dit :

$$y(k+1) = Ay(k) + B + F(.) \qquad (III.2)$$

- La figure du système de transmission est illustrée sur la figure suivante :

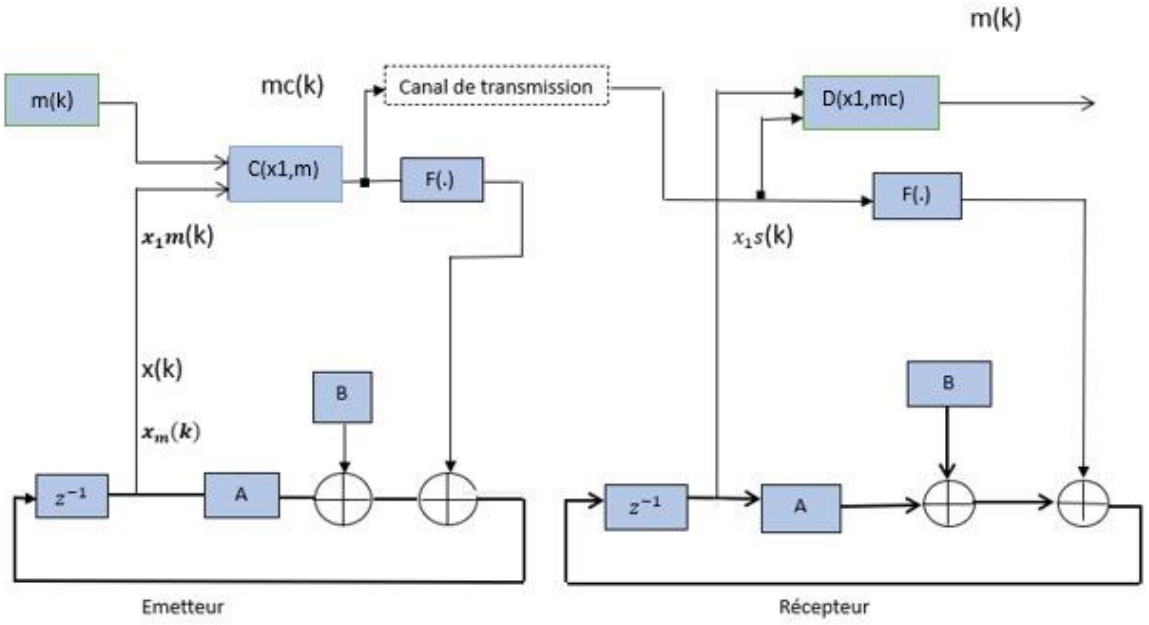

Figure (III.13) : Schéma système de transmission

III.7. Structure de l'émetteur et récepteur :

III.7.1. Structure de l'émetteur :

L'émetteur comprend deux éléments principaux à savoir, le système de Hénon maitre et la fonction de cryptage.

III.7.1.1. Le système de Hénon maitre : Ce système a été largement étudié dans la littérature.il est décrit par le système d'équations suivants :

$$\begin{aligned} x_{2m}(k+1) &= 1 - \left(a.x_{1m}(k)\right)^2 + x_{2m}(k) \\ x_{2m}(k+1) &= b.x_{1m}(k) \end{aligned} \qquad (III.3)$$

$$x_m = \begin{bmatrix} x1m(k+1) \\ x2m(k+1) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix} \begin{bmatrix} x_{1m}(k) \\ x_{2m}(k) \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} -ax_{1m}(k)^2 \\ 0 \end{bmatrix}$$

Les paramètres du système sont donnés comme suit :

$a = 1.4$, b=0.3 avec les conditions initiales du système x_{1m}=0.1, x_{2m}=-0.1

III.7.1.2. La fonction de cryptage : la fonction de cryptage choisie dans notre cas est comme suit :

$$mc(k) = (0.1(k)) + (0.9\, x_{1m}(k)) \quad \text{(III.4)}$$

Le message crypté donne par l'équation (III.2) est injecté comme paramètre du système de Hénon donné par l'équation (III.1) nous obtenant ainsi le nouveau système maitre comme suit : $x_{1m}(k+1) = 0.01 - (a.mc)(k))^2 + x_{2m}(k)$

$$x_{2m}(k+1) = b.x_{1m}(k) \quad \text{(III.5)}$$

Où :

mc (k): c'est le message crypté

III.7.2. Structure du récepteur :

Dans un système chaotique esclave utilisé dans le contexte de la cryptographie, le récepteur joue un rôle essentiel dans la réception des données cryptées et dans le processus de décryptage. Voici les éléments du récepteur :

III.7.2.1. Système Hénon esclave : il est donné par les équations suivantes :

$$x_{1s}(k+1) = 1 - (a.md(k)^2) + x_{2s}(k)$$

$$x_{2s}(k+1) = b.x_{1s}(k) \quad \text{(III.6)}$$

III.7.2.2. Fonction de décryptage :

$$md(k) = (10.md(k) - (9.x_{1s}(k))) \quad \text{(III.7)}$$

Où :

md[k] : est le message décrypté

III.8. Conclusion :

En conclusion, l'implémentation d'un schéma de transmission sur deux cartes Arduino Mega2560 offre une flexibilité et une polyvalence significatives pour une variété d'applications de communication transmission de données. Avec une compréhension solide des concepts et des outils nécessaires.

Le quatrième et dernier chapitre on expose les résultats de simulation et expérimentation.

Chapitre IV :
Résultats de simulation et expérimentation

IV.1. Introduction :

Ce chapitre marque un tournant significatif dans notre exploration de la synchronisation des systèmes chaotiques à l'aide de cartes Arduino en tant qu'émetteur-récepteur. Après avoir établi les fondements théoriques et examiné les aspects pratiques de la mise en place de ces dispositifs, nous nous plongeons désormais dans l'examen des résultats de simulation. Ces simulations représentent le cœur de notre étude, offrant un aperçu précis et détaillé de la manière dont les systèmes chaotiques se comportent lorsqu'ils sont soumis à la synchronisation chaotique à l'aide de cartes Arduino.

Au cours de ce chapitre, nous allons présenter en détail les résultats de nos expérimentations virtuelles, les visualiser à l'aide de graphiques et d'analyses quantitatives, et les interpréter dans le contexte de notre objectif de communication sécurisée et fiable. Ces résultats sont le fruit d'efforts considérables de modélisation, de programmation et de paramétrage soigneux des systèmes chaotiques et des cartes Arduino. Leurs implications sont cruciales pour évaluer l'efficacité de notre approche de synchronisation chaotique.

En fin de compte, ce chapitre constitue une étape cruciale dans la démonstration de la validité et de l'applicabilité de la synchronisation des systèmes chaotiques avec des cartes Arduino en tant que solution viable pour des communications sécurisées et fiables. Les résultats présentés ici contribuent à la richesse de la recherche dans ce domaine en ouvrant de nouvelles voies pour l'intégration de la théorie du chaos dans des applications pratiques et innovantes.

IV.2. Schéma de système de transmission:

Un système de transmission émetteur-récepteur basé sur la synchronisation d'un système chaotique est une approche fascinante pour la sécurisation des communications.

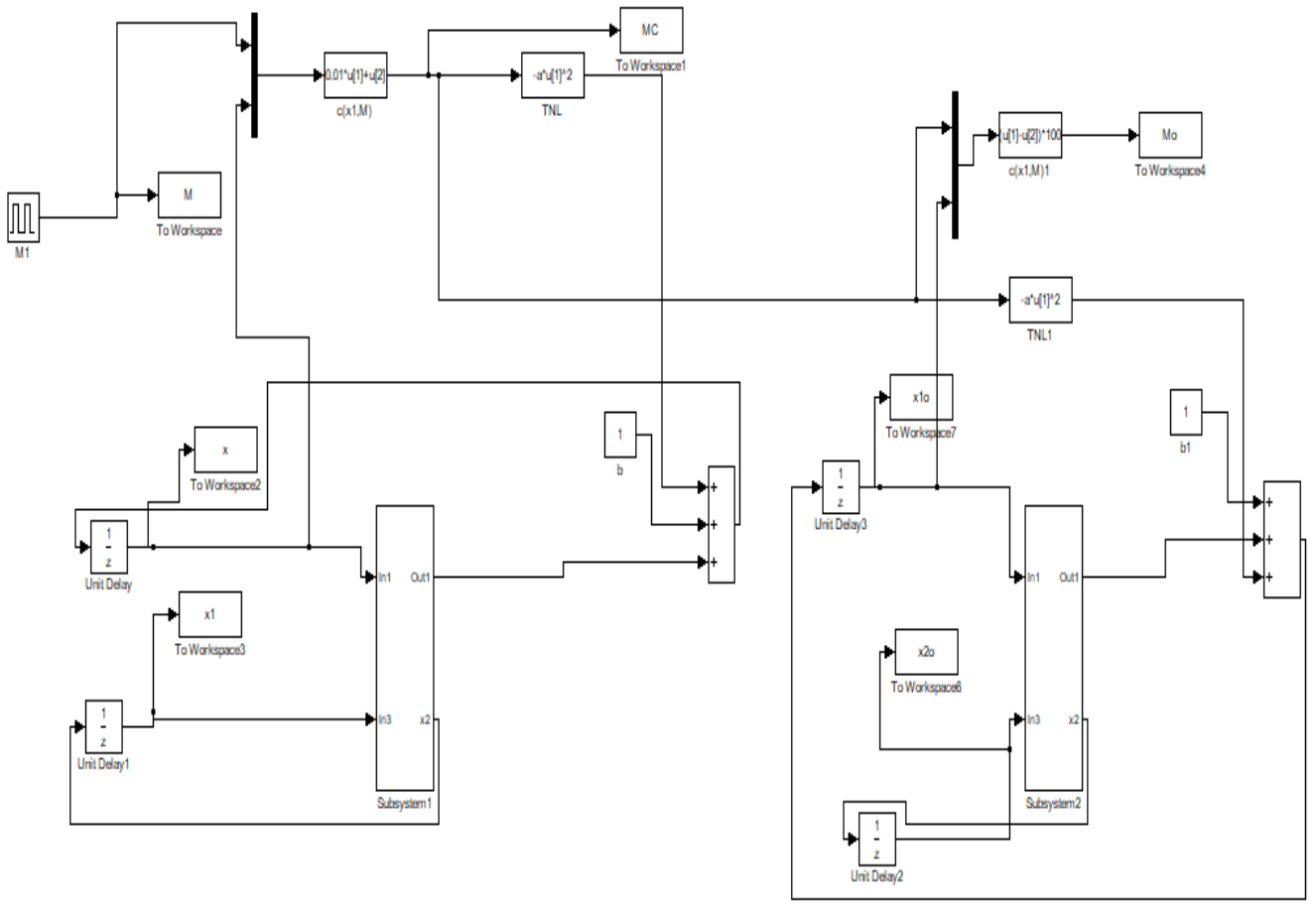

Figure (IV.1) : Schéma du système de transmission chaotique sous Simulink

IV.3. Détails d'implémentation :

- La figure (IV.2) représente une image réelle de notre implémentation :

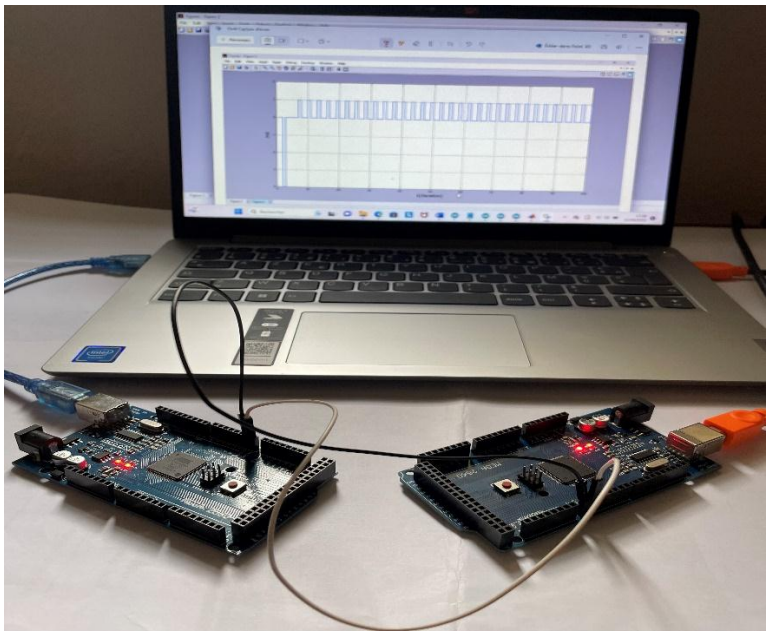

Figure (IV.2) : Implémentation de l'émetteur et récepteur

- Les figures (IV. 3) et (IV.4) representents les états du système chaotique Hénon maitre (emetteur).

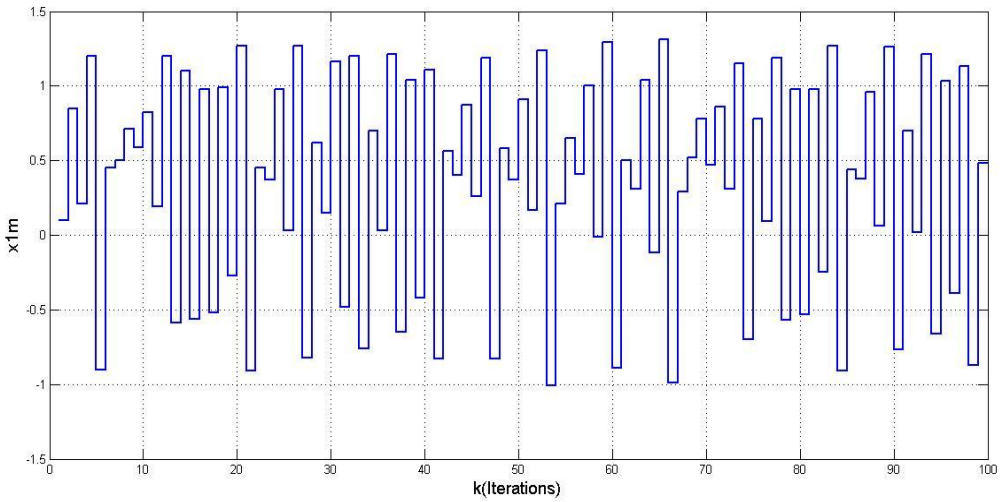

Figure (IV.3) : Etat x_{1m} du système émetteur du Hénon

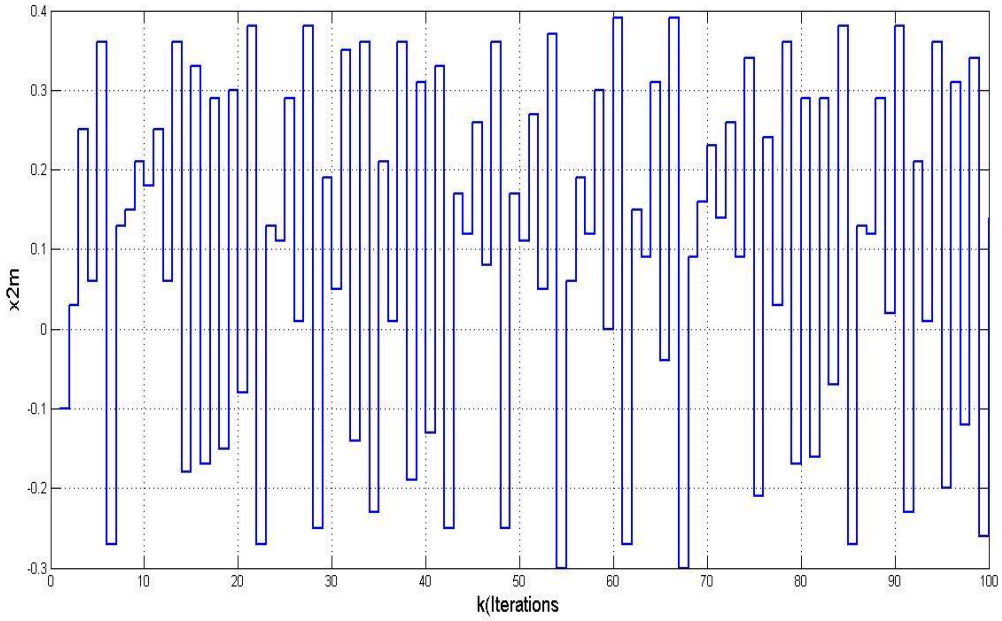

Figure (IV.4) : Etat $x_m(k)$du système émetteur du Hénon

- Les simulations effectuées montrent le comportement chaotique du système de Hénon.
- La figure (IV.5) montre l'attracteur chaotique, obtenu dans le plan de phase des états x1m et x2m, qui prend la forme d'un croissant.

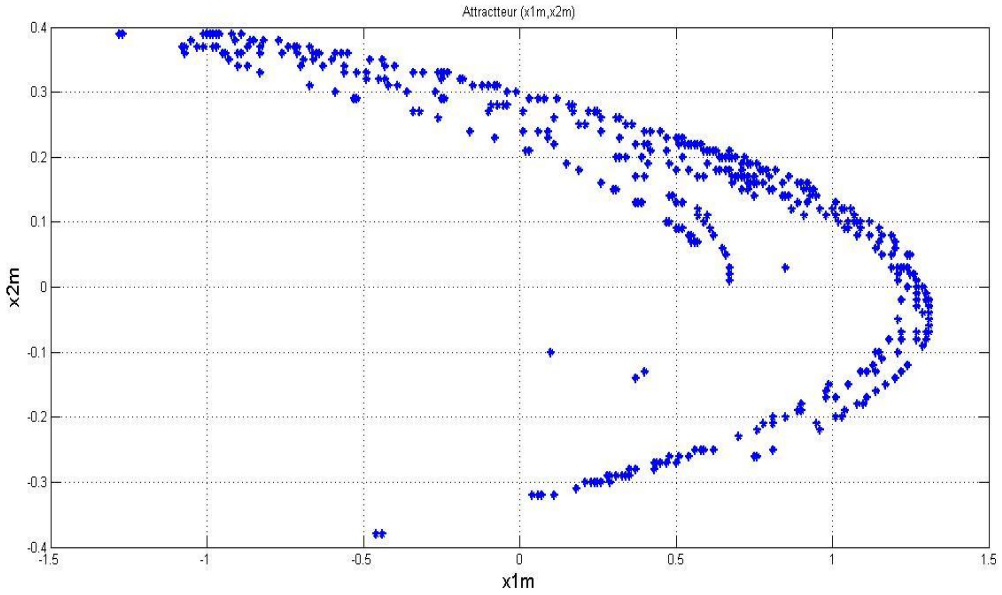

Figure (IV.5) : Attracteur (x_{1m}, x_{2m}) du système Hénon maitre

- Dans notre cas le message envoyé est un message carré d'amplitude 1 et de période 3.

- La figure (IV.6) Illustre l'allure du signal message original.

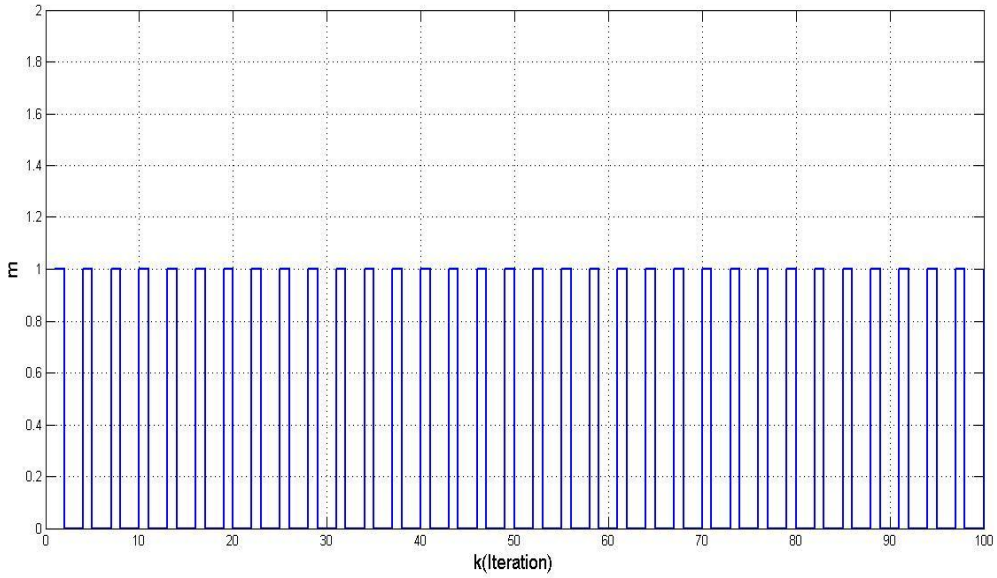

Figure (IV.6) : Message original m(k)

- La figure (IV.7) représente le message crypté d'un signal chaotique en utilisant la fonction de cryptage donné par l'équation (III.4) dans le chapitre précédant.

  Nous remarquons que le message est bien noyé dans le signal chaotique $x_1 m$.

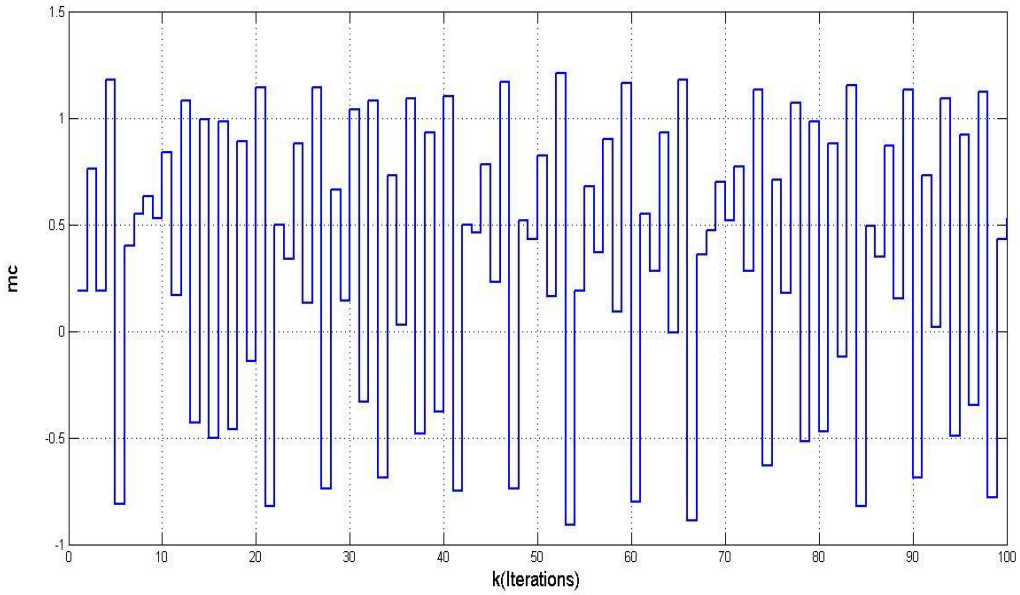

Figure (IV.7) : Message crypté

- La figure (IV.8) represente les états x_1 du système Hénon maitre et esclave (émetteur et récepteur)

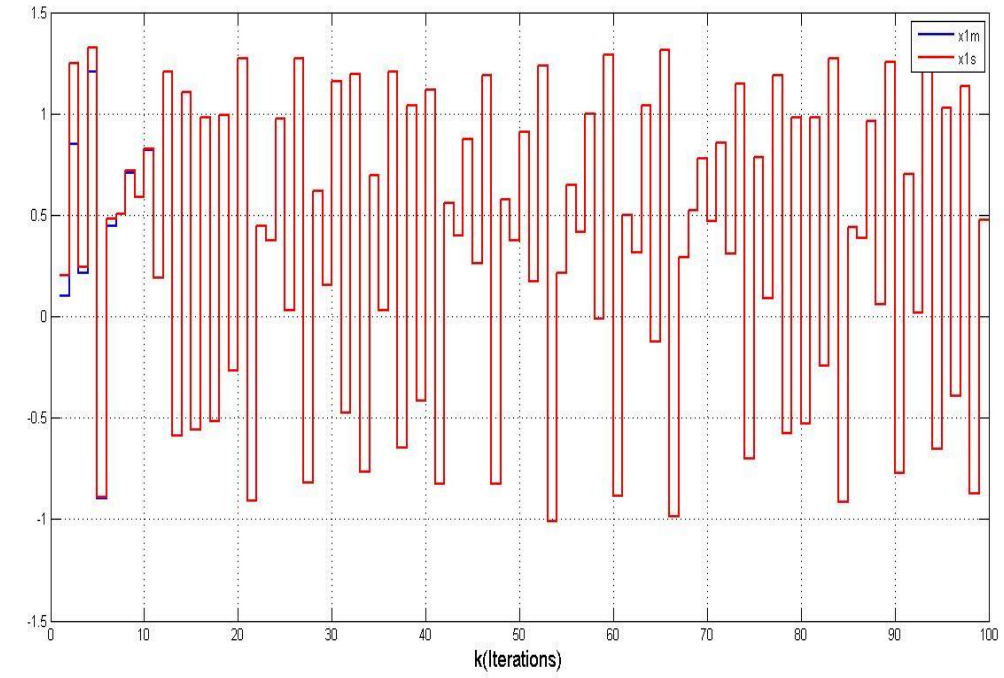

Figure (IV.8) : Etats des systèmes maitres et esclave

- Les états x_1m et x_1s sont synchroniser après un régime transitoire de 11 itérations.

Ceci peut être confirmé par la courbe de l'erreur de synchronisation $e_{1=}x_1m - x_1s$ Illustré sur la figure (IV.9) et qui converge vers zéro après le régime transitoire

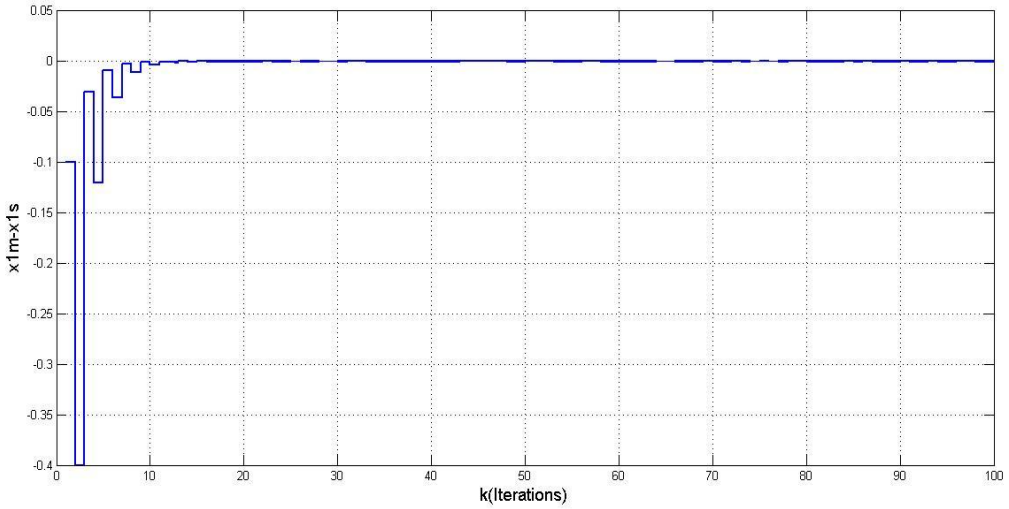

Figure (IV.9) : l'erreur de synchronisation de e_1=$x_1m - x_1s$

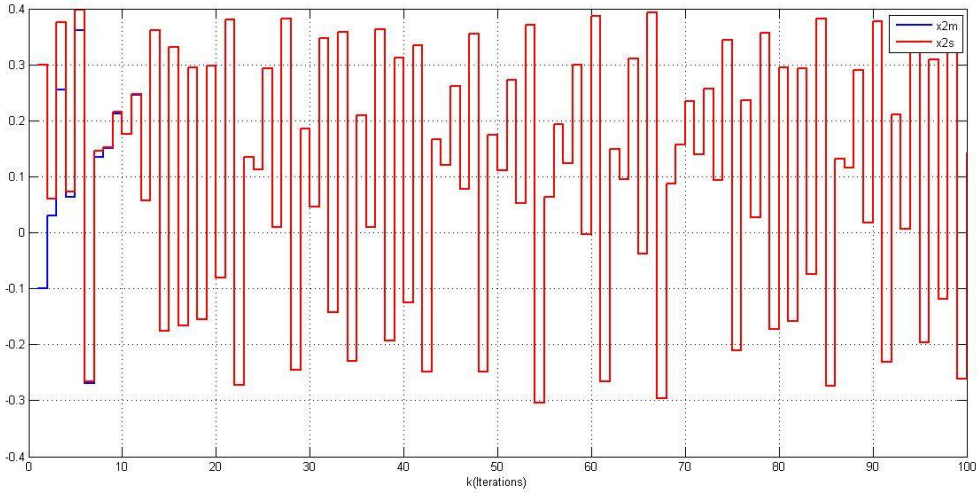

Figure (IV.10) : Etats x_2 des systèmes maitres et esclave

- Les états x_2m et x_2s sont synchroniser après un régime transitoire de 10 itérations.

Ceci peut être confirmé par la courbe de l'erreur de synchronisation de $e_{2=}x_2m - x_2s$ Illustré sur la figure (IV.11) et qui converge vers zéro après le régime transitoire.

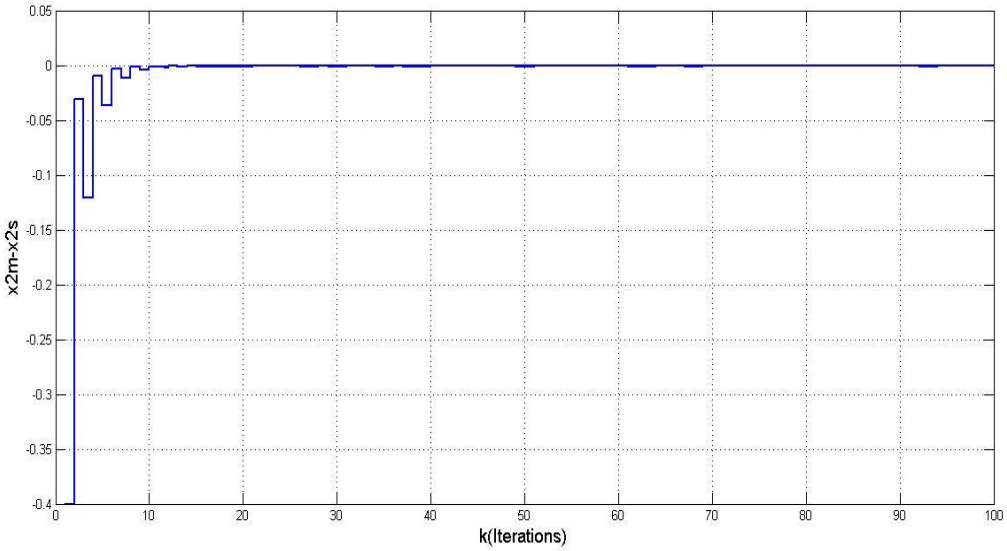

Figure (IV.11) : l'erreur de synchronisation de $e_2 = x_2m - x_2s$

- La figure (IV.12) represente le messaage original $mc(k)$et le message décrypté $md(k)$:

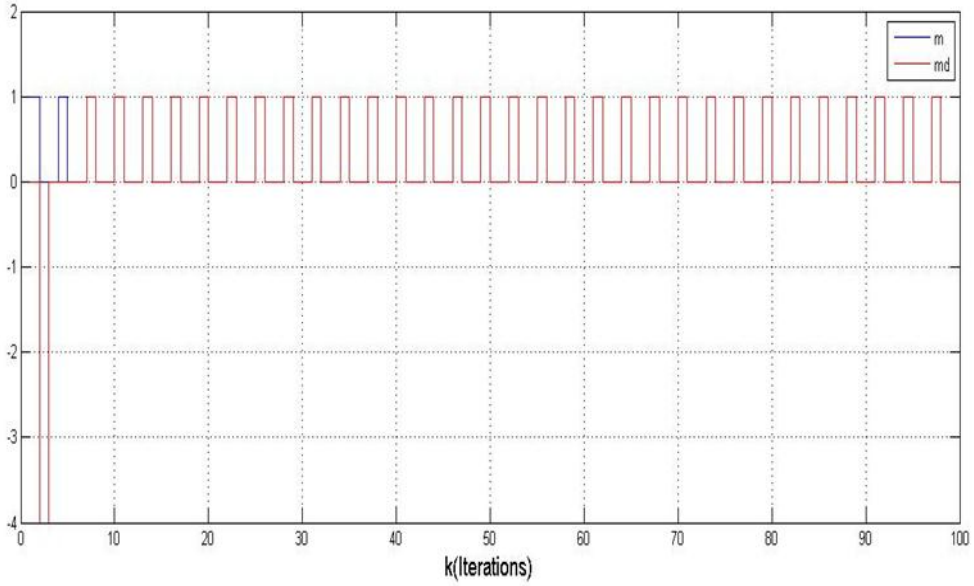

Figure (IV.12): Message original et message décrypté

➢ Nous constatons que le message a été récupéré avec succès.

- La figure ci-dessous illustre l'erreur sur le message $m(k)$.

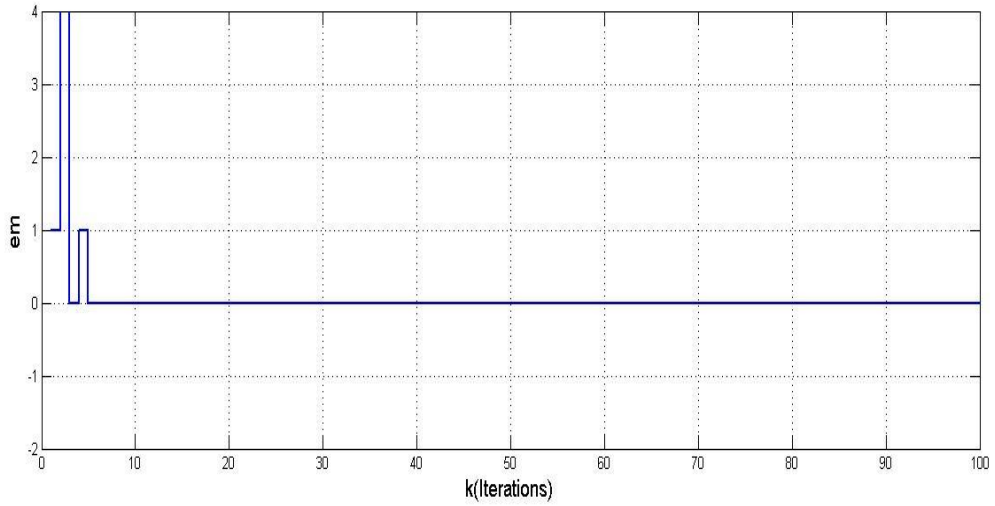

Figure (IV.13) : Erreur sur message

- Par la suite nous avant envoyé un message sinusoïdal de période 135 et d'amplitude 1

La figure (IV.14) montre le message sinusoïdal originale :

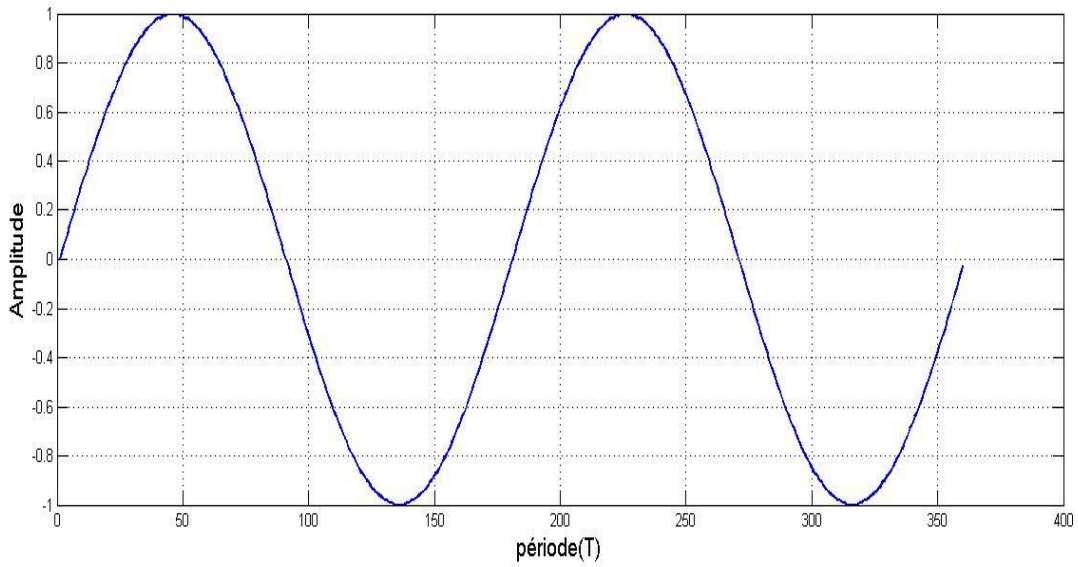

Figure (IV.14) : Message sinusoïdal

- En utilisant la meme fonction de cryptage (III.4), nous obtenons le message crypté montré sur la figure (IV.15) :

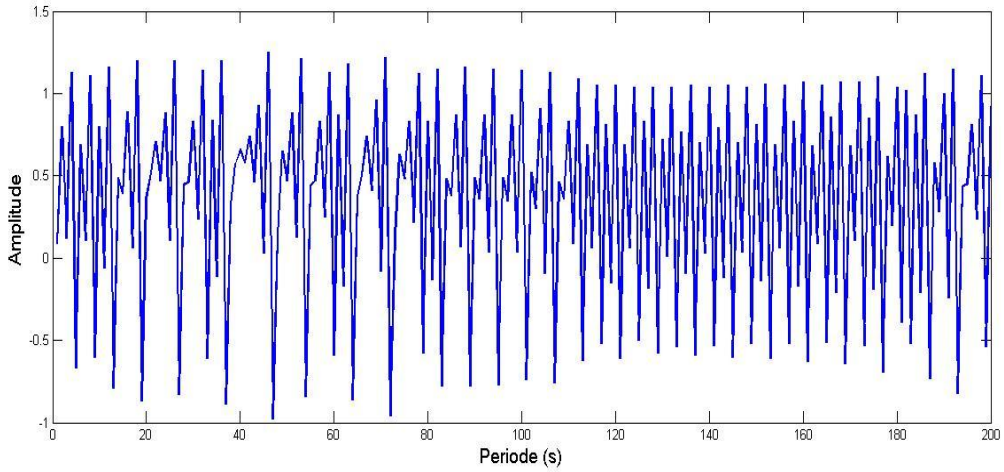

Figure (IV.15) : Le message sinusoïdal crypté

➢ Nous remarquons que message est bien noyé dans le signal chaotique.

- La figure (IV.16) represente le messaage original $m(k)$ et le message décrypté $md(k)$ sinusoidal :

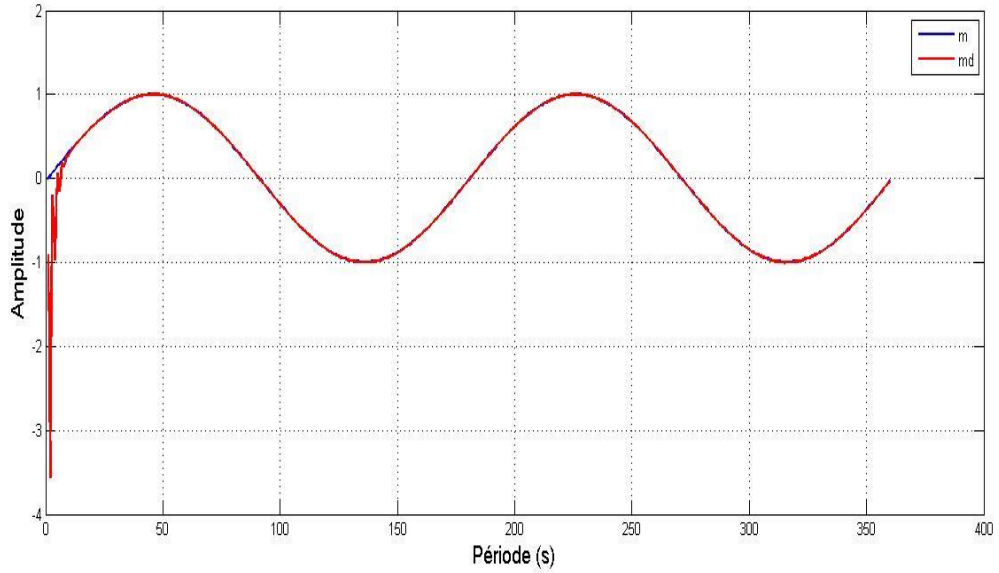

Figure (IV.16) : Le message original $m(k)$ et le message décrypté $md(k)$ sinusoïdal

➢ Nous constatant que le message a était recupéré avec succès.

- La figure ci-dessous illustre l'erreur de synchronisation du message sinusoïdal $m - md$ qui converge vers zéro après le régime transitoire 10s.

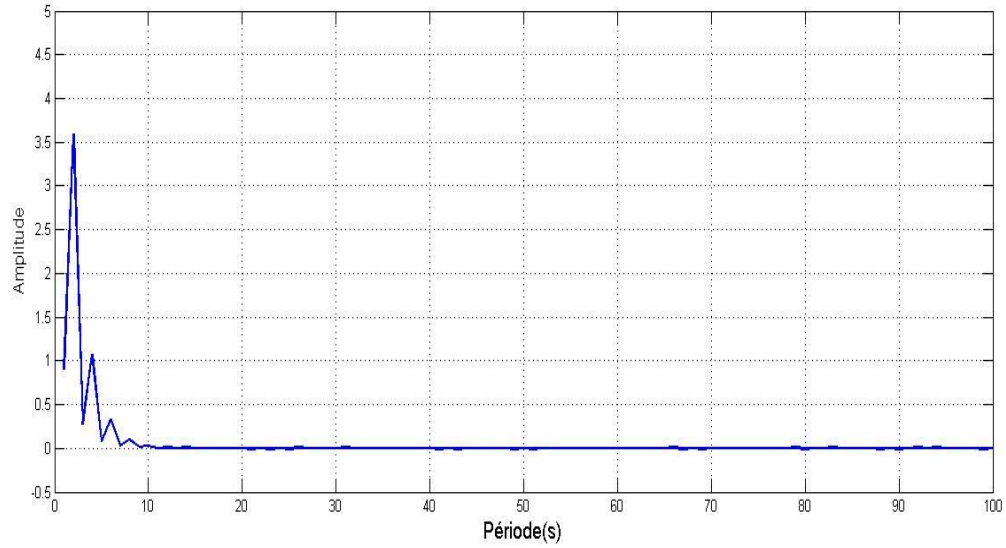

Figure (IV.17) : Erreur de synchronisation $m - md$

Conclusion :

Dans ce chapitre on a pu synchroniser deux systéme de Henon, afin de transmettre des données sécurisées entre un émetteur et un récepteur de signaux chaotiques. Le cryptage a était fait en noyant le message dans le signal chaotique généré par l'emetteur .et la synchronisation entre deux etat du systéme de Henon, les simulations effectuées montrent le comportement chaotique du système de Hénon.

Conclusion générale :

La réalisation d'un schéma de communication sécurisée basé sur la synchronisation de deux systèmes chaotiques à temps discret, à l'aide de la plateforme Arduino, a été l'objet de ce mémoire. Cette étude a permis d'explorer en profondeur les concepts fondamentaux des systèmes dynamiques, des systèmes chaotiques et de la synchronisation, tout en se penchant sur l'implémentation pratique de ce schéma innovant.

Dans le premier chapitre, nous avons défini les systèmes dynamiques de manière générale. Nous avons exploré la notion de dynamique chaotique, mettant en lumière les caractéristiques clés de ces systèmes, telles que leur sensibilité aux conditions initiales et leur comportement non linéaire. Cette compréhension préliminaire a été essentielle pour la suite de notre travail.

Le deuxième chapitre a été consacré à la synchronisation des systèmes chaotiques. Nous avons présenté diverses méthodes de synchronisation, évaluant leurs avantages et leurs inconvénients dans un contexte à temps discret. Ce chapitre nous a fourni les outils conceptuels nécessaires pour concevoir notre propre approche de synchronisation.

Le troisième chapitre a détaillé la structure du schéma de transmission sécurisée proposé, y compris les composants matériels et logiciels nécessaires à son implémentation sur des cartes Arduino. Ce chapitre représente la phase de mise en œuvre concrète de notre travail.

Le quatrième et dernier chapitre a présenté les résultats de simulation et d'expérimentation. Nous avons remarqué que le message envoyé à était récupéré avec succès. Ces résultats serviront de référence pour évaluer l'efficacité globale de notre système de communication sécurisée.

En conclusion, ce mémoire a exploré avec succès la réalisation d'un schéma de communication sécurisée basé sur la synchronisation de systèmes chaotiques à temps discret avec Arduino. Notre recherche a contribué à enrichir la compréhension des systèmes chaotiques et de leur utilisation dans le domaine de la sécurité des communications.

En perspective, notre travail peut-être complété par :

- L’envoie de données plus complexes à savoir les images, vidéos, audios.
- Transmissions de données sans fil (Bluetooth, Wifi…).
- Prise en considération des bruits de canal lors de l’envoie des signaux.

Bibliographie:

[1] S.H. Strogatz. Nonlinear dynamics and chaos: with applications to physics biology,chemistry,and engineering. Livre électronique ISBN ,2e edition, (2018).

[2] S.H. Strogatz. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, (2000).

[3] H. Khalil. Nonlinear Systems (3rd Edition). Prentice Hall, (2002).

[4] C.Jutten « Systèmes asservis non linéaires » cours de troisième année du département 3i option Automatique. Université Joseph Fourier- Polytech Grenoble. 2006.

[5] T.Kathleen "Chaos: Introdution aux systèmes dynamiques ", 1ere édition, 2006.

[6] S.H. Strogatz. Nonlinear dynamics and chaos: with applications to physics biology,chemistry,and engineering. Livre électronique ISBN ,2e edition, 2019.

[7] C.Robert. Hilborn "Chaos et dynamique non linéaire : une introduction pour les scientifiques et les ingénieurs" ox-ford U.P, New York,1994.

[8] F.Laruelle ‘’ Les concepts de fractalité et de chaos généralisés’’ théorie des identités, Presses Universitaires de Fr

ance, 1992

[9] P.Henri "Les méthodes nouvelles de la mécanique céleste." (C'est le livre original où Poincaré a introduit la notion de la Section de Poincaré), Gauthier-Villars, Paris, 1892.

[10] Strogatz, Steven H. "Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering." Westview Press, 2014

[11] G.John, et Holmes.Philip. "Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields." Springer, 1983.

[12] W. Stephen. "Introduction to Applied Nonlinear Dynamical Systems and Chaos." Springer, School of Mathematics, University of Bristol, Clifton, Bristol, UK 2003.

[13] A.Ralph, et M.Jerrold E. "Foundations of Mechanics." Westview Press, American Mathematical Society , 2008.

[14] J.Guckenheimer, et P.Holmes. Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields. Springer-Verlag, (1990).

[15] J.K.Hale, et H.Koçak. Dynamics and Bifurcations. Springer-Verlag,(1991)

[16] E.Ott. Chaos in Dynamical Systems. Cambridge University Press, (2002).

[17] K.T.Alligood, T.D Sauer, et J.A.Yorke, Chaos: An Introduction to Dynamical Systems. Springer-Verlag, (1997).

[18] R.L.Devaney. An Introduction to Chaotic Dynamical Systems. Westview Press, (1989).

[19] R.Abraham, et C.Shaw. Dynamics: The Geometry of Behavior. Redwood City, CA: Addison-Wesley, (1992).

[20] E. N.Lorenz. The Essence of Chaos. University of Washington Press,(1993).

[21] J.Gleick. Chaos: Making a New Science. Penguin Books, (1987).

[22] M.Hénon. A Two-Dimensional Mapping with a Strange Attractor. Communications in Mathematical Physics, (1976).

[23] O.E.Rössler . An Equation for Continuous Chaos. Physics Letters A, (1987).

[24] S. H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. Westview Press, 2014.

[25] J.Christian « Systèmes asservis non linéaires » cours de troisième année du département 3i option Automatique. Université Joseph Fourier- Polytech Grenoble. 2006.

[26] S.Ssastry « Nonlinear Système », Edition Spriger, New York, 1999.

[27] N.Amroune et M.Lainous ‘’ Synchronisation hybride des systèmes chaotiques, mémoire de fin d’études, Centre Universitaire Abd elhafid Boussouf Mila, 2022.

[28] H. Bezziou. ‘’ Synchronisation généralisée des systèmes fractionnaires en utilisant le critère R-H, université mohamed khider biskra, 2020.

[29] https://hal.science/hal-01850439/document

[30] favicon hal.science Hal

[31] S.G.LinShi ‘' Sécurité et réseaux de communication’’, School of Mathematics,South west Jiaotong University, Chengdu 610031, Chine avril (2023).

[32] Mihai Bogdan Luca « Apports du Chaos et des estimateurs d’état pour la transmission sécurisée de l’information », Thèse de Doctorat de l’Université de Bretagne Occidentale, (2006).

[33] Megherbi Ouerdia . Etude et réalisation d’un système sécurisé à base de systèmes chaotiques. Mémoire de Magister, Université Mouloud Mammeri de Tizi-Ouzou, (2013).

[34] K. Si Yahia et M. Kaddour. Conception et réalisation d’un dispositif d’exploration fonctionnelle cardio-vasculaire, Mémoire de fin d’étude, Université Abou bekr Belkaid, Tlemcen (2016).

[35] A.Ould Amara et M.Tighezi . Circuit de mise en forme du signal PCG. Université Abou bekr belkaid ,Tlemcen, Algérie (2015).

[36] A.Adjali et M.Abdi. Synthèse des filtres numériques dans le traitement du signal PCG, Université Abou bekr belkaid ,Tlemcen, Algérie (2015).

[37] N.Dib : Analyse temporelle des déférentes ondes du signal ECG en vue d’une reconnaissance de signatures de pathologies cardiaques. Université Abou bekr belkaid ,Tlemcen, Algérie, (2009).

[38] Hamza Mounir et Ziani Cherif Selmen : étude et réalisation d’un stéthoscope électronique.Université Abou bekr belkaid ,Tlemcen, Algérie, Année 2013.

[39] https://www.bing.com/ckCompatibili +avec+les+shields

[40] https://www.bing.com/ck/ Types+des+cartes+Arduino

[41] https://www.bing.com/ck/ Carte+Arduino+Mega

[42] Mega 2560 Rev3 | Arduino Documentation

[43] Cartes Arduino : Caractéristiques, avantages et inconvénients… (forsimplytech.blogspot.com)

[44] A. Ait Hammi . Etude et réalisation d'un système chaotique basé sur le circuit de CHUA. Mémoire de fin d'étude, Université Mouloud Mammeri Tizi-Ouzou, (2014).

Résumé :

Les systèmes de communication sécurisée jouent un rôle de plus en plus essentiel dans notre société numérique, et le recours au chiffrement devient impératif pour protéger la confidentialité des données. Plusieurs algorithmes de cryptage ont été proposés pour cette fin. Ce qui est intéressant, c'est la similitude entre les systèmes chaotiques et les principes de chiffrement. En effet, les systèmes chaotiques possèdent des caractéristiques telles que le déterminisme, la non-linéarité, l'aspect aléatoire et la sensibilité aux conditions initiales , qui en font des candidats intéressent pour la transmission sécurisée. Cependant, pour les utiliser dans ce contexte, il est crucial que les systèmes chaotiques, à la fois du côté de l'émetteur et du récepteur, soient identiques.

Le défi réside dans le fait que les systèmes chaotiques sont principalement caractérisés par leur sensibilité aux conditions initiales. De légères variations initiales peuvent conduire à des résultats très différents et imprévisibles. Pour surmonter cette difficulté, la synchronisation de deux systèmes chaotiques est nécessaire pour générer des signaux qui évoluent de manière similaire, même en présence de conditions initiales différentes. Dans le cadre de cette étude, nous avons entrepris de mettre en œuvre un système de transmission innovant basé sur des systèmes chaotiques discrets, en utilisant des cartes Arduino.

Plus spécifiquement, nous avons conçu un schéma de transmission sécurisée basé sur la synchronisation de systèmes chaotiques discrets de Hénon. Le processus de cryptage consiste à incorporer un message secret dans la première dynamique du système maître, utilisant une fonction de cryptage dédiée. La récupération réussie des signaux de message de diverses formes a été réalisée en synchronisant les systèmes maître et esclave, tout en employant une fonction de décryptage appropriée. Les résultats expérimentaux obtenus après l'implémentation sur des cartes Arduino illustrent la réussite de cette approche, avec la récupération efficace des signaux de message après une brève période de transition.

Traduction en Anglais:

Secure communication systems play an increasingly essential role in our digital society, and the use of encryption becomes imperative to safeguard data confidentiality. Several encryption algorithms have been proposed for this purpose. What is intriguing is the resemblance between chaotic systems and encryption principles. Chaotic systems exhibit characteristics such as determinism, non-linearity, randomness, and sensitivity to initial conditions, making them interesting candidates for secure transmission. However, to utilize them in this context, it is crucial that chaotic systems, both on the transmitter and receiver sides, match.

The challenge lies in the fact that chaotic systems are primarily characterized by their sensitivity to initial conditions. Slight initial variations can lead to highly different and unpredictable outcomes. To overcome this hurdle, the synchronization of two chaotic systems is necessary to generate signals that evolve similarly, even in the presence of different initial conditions. In this

study, we embarked on implementing an innovative transmission system based on discrete chaotic systems, using Arduino boards.

Specifically, we designed a secure transmission scheme based on the synchronization of discrete chaotic systems of the Hénon map. The encryption process involves embedding a secret message into the master system's first dynamics, using a dedicated encryption function. The successful retrieval of messages in various forms was achieved by synchronizing the master and slave systems, employing an appropriate decryption function. The experimental results obtained after implementing the scheme on Arduino boards illustrate the success of this approach, with the efficient recovery of message signals after a brief transient period.

Les mots clé :

Chaos

Systèmes chaotiques

Systèmes discrets

Sensibilités aux conditions initiales

Synchronisation

Système de Hénon

Attracteur étrange

Emetteur

Récepteur

Transmission sécurisée

Cryptage / Décryptage