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

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

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

Mémoire de Fin d'Etudes de MASTER PROFESSIONNEL

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

Présenté par
Rachida MEZINE
Hanane MEZZOU

Thème

Implémentation sur cartes ESP32 d'un système de transmission sans fil de coordonnées GPS à base de systèmes chaotiques discrets

Mémoire soutenu publiquement le 29/09/ 2024 devant le jury composé de :

M Hocine KHATI
Maitre de Conférences classe B, UMMTO, Président

Mme Ouerdia MEGHERBI
Maitre de Conférences classe B, UMMTO, Encadrant

Mme Nacéra ARAR
Maitre Assistante classe A, UMMTO, Examinateur

Mme Kahina LARBI
Maitre Assistante classe B, UMMTO, Examinateur

Remerciements

Tout d'abord, nous tenons à exprimer notre profonde gratitude envers notre Créateur Tout-Puissant, qui nous a accordé la force et le courage nécessaires pour mener à bien ce modeste travail.

Nous sommes profondément honorées d'avoir été encadrées par Madame ***Megherbi Ouerdia****, dont la passion pour la recherche et l'enseignement a éclairé chaque étape de ce mémoire. Nous lui adressons nos sincères remerciements pour son soutien constant et son engagement indéfectible tout au long de ce projet. Sa patience, sa persévérance et sa bienveillance ont été des piliers essentiels sur lesquels nous avons pu compter.*

Nous souhaitons également remercier chaleureusement les membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer ce travail.

Enfin, nous adressons nos remerciements à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce projet.

Dédicaces

Je dédie ce modeste travail à :

À la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ; Maman que j'adore.

À l'homme de ma vie, mon exemple éternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir ; à toi Mon père.

Aucun hommage ne pourrait être à la hauteur de l'amour Dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

Je vous dédie ce travail en témoignage de mon profond amour. Puisse dieu, le tout puissant, vous préserver et vous accorder santé, longue vie et bonheur.

À mes chers frères et ma petite sœur adorée

Je dédie ce travail dont le grand plaisir leurs revient en premier lieu pour leurs conseils, aides, et encouragements.

À la mémoire de grand père Mouloud, ma grande mère Ouerdia et mon oncle Madjid.

À toute ma famille, tentes, oncles, cousins et cousines.

À ma chère binôme, dont la collaboration et l'amitié ont rendu ce travail plus agréable et enrichissant

À mes chères amies avec qui j'ai partagé des moments inoubliables.

À tous ceux qui ont une place dans mon cœur, et tous ceux qui m'ont aidé.

M.Hanane

Dédicaces

Je dédie le fruit de mes années d'études

À ma maman, dont la force et la persévérance m'ont inspirée à chaque étape de ce voyage. Merci pour tous les sacrifices que tu as faits pour que je puisse arriver jusqu'ici. Ce succès est le reflet de ton amour et de ton dévouement.

À mon père, parti trop tôt, mais qui continue de vivre à travers tout ce que je fais. Merci pour ton amour, et tes enseignements qui continuent de me guider.

À mes chers frères et à ma sœur, qui ont été mes compagnons de route, mes alliés et mes plus grands supporters.

À toute ma famille, grands-parents, tantes, oncles, cousins et cousines.

À ma chère binôme, dont la collaboration et l'amitié ont rendu ce travail plus agréable et enrichissant

À tous mes amis avec qui j'ai partagé tant de bons moments, témoins de mes rires, gardiens de mes secrets

À tous ceux qui m'aiment et que j'aime

M.Rachida

Sommaire

Sommaire

Chapitre II: Synchronisation des système chaotique

Chapitre III: Application à la transmission sécurisée de coordonnées GPS

Chapitre IV: Implémentation sur carte ESP32 du schéma de transmission sans fil de coordonnées GPS

Listes des abréviations et acronymes

Liste des abréviations et acronymes

$\frac{dx}{dt} = \dot{x}$ **:** dérivée de la variable x par apport au temps.

R^n : Ensemble des nombre réels entiers.

R^+ : Ensemble des nombre réels positifs.

λ_i :Variation d'exposant de Lyapunov d'ordre i.

$\dot{x}$**:** Dérivée du vecteur d'état.

$\hat{x}$**:** Vecteur estimé.

$\dot{\hat{x}}$ *:* Dérivée du vecteur estimé.

τ : Valeur de temps très petite .

Sign : Fonction signe .

GPS : Global Positioning System

IDE : Integrated Development Environment

LCD : Liquid Crystal Display

I2C : Inter-Integrated Circuit

IoT : Internet of Things

SDA : Serial Data Line

SCL : Serial Clock Line

SDL : Système Dynamique Linéaire

GND : Ground

Liste des figures

Liste des figures

Introduction générale

Aujourd'hui, la communication sécurisée est devenue une préoccupation majeure. Tout système de communication performant nécessite désormais un dispositif de protection pourrésister à d'éventuelles attaques [1]. C'est pourquoi de nouvelles techniques de cryptage sont régulièrement développées.

La cryptographie est la science qui s'intéresse à la protection des messages en les rendant incompréhensibles. Elle a évolué à travers un conflit perpétuel entre deux camps : l'un cherchant à dissimuler l'information et l'autre tentant par tous les moyens de la dévoiler [2]. À chaque fois que le premier camp trouve un moyen de chiffrer ses messages, le second essaie de découvrir la méthode qui lui permettra de déchiffrer l'information. Autrefois, pour dissimuler une information, on mélangeait, permutait ou décalait des lettres, tandis que d'autres remplaçaient les mots par des nombres, tout cela dans le but de rendre la lecture du message impossible. Cependant, la cryptographie n'a cessé d'évoluer : aujourd'hui, le chiffrement des messages se fait de manière mathématique et algorithmique, et plus l'inversion de la transformation est complexe, plus la sécurité est élevée [3].

De nos jours, les chercheurs s'intéressent de près à l'étude des phénomènes chaotiques, et de nombreux travaux ont été réalisés dans ce domaine [4,5]. Ces recherches ont permis de généraliser l'utilisation des systèmes chaotiques dans divers domaines scientifiques, les rendant très intéressants pour le cryptage des données, malgré les difficultés liées à leur synchronisation.

Introduite en 1990 par Pecora et Carroll[6], la synchronisation est une technique qui consiste, dans le cas de deux systèmes chaotiques identiques (émetteur et récepteur), à forcer la trajectoire du récepteur à suivre celle de l'émetteur. Plusieurs méthodes de synchronisation ont été proposées dans la littérature scientifique, basées sur le principe maître-esclave, et permettant de réduire l'erreur entre les signaux émis par le générateur chaotique au niveau de l'émetteur et ceux émis par le celui au niveau du récepteur [6]. Parmi ces méthodes,nous avons opté pour la synchronisation impulsive qui présente plusieurs avantages.

Dans ce travail, nous proposons de concevoir et de réaliser,sur deux cartes ESP32, un système de transmission sécurisé de données GPS basé sur le cryptage par le chaos. Le système est implanté sur une carte électronique de type ESP32. L'intérêt d'utiliser le chaos réside d'une part dans la possibilité d'exploiter les propriétés des systèmes chaotiques pour le cryptage (aspect aléatoire et spectre riche en fréquences, etc.), et d'autre part dans la possibilité de synchroniser les systèmes chaotiques via un observateur.

Pour ce faire, nous utiliserons un système chaotique particulier appelé « système de Lozi ». Deux systèmes chaotiques identiques seront mis en œuvre : l'un servira d'émetteur (générateur de signaux chaotiques) et l'autre de récepteur. Pour récupérer le signal chaotique émis par l'émetteur, le système chaotique au niveau du récepteur sera un observateur impulsif. Il s'agit du système chaotique de Lozi muni d'une loi de commande dite impulsive permettant de synchroniser les deux systèmes chaotiques même en présence de variations dans les conditions initiales.

Le cryptage consiste à intégrer le message chiffré dans le signal chaotique émis par l'émetteur (la première carte), tandis que la récupération du message se fera à l'aide d'une fonction mathématique de décryptage (deuxième carte), grâce à la synchronisation établie.

Notre travail est structuré comme suit :

Le premier chapitre a pour objet l'étude des notions fondamentales des systèmes chaotiques, abordant des rappelssur quelques définitions utiles. Nousprésenteronsles différents outils mathématiques qui nous servent à caractériser le comportement chaotique d'un système, tels que les attracteurs étranges, les exposants de Lyapunov et la dimension fractale. Cette étude est consolidée par des exemples de systèmes chaotiques à temps continu et discret, qui sont simulés sous Matlab, ce afin de mieux illustrer leur fonctionnement et leurscaractéristiques.

Le second chapitre sera consacré à la synchronisation des systèmes chaotiques, les modes de synchronisation,nous parlerons ainsi du principe de la synchronisation de ces systèmes et les différentes types et méthodes utilisées.

Le troisième chapitre sera consacré à l'étude détaillée d'une transmission sécurisée de données GPS basée sur un système chaotique à temps discret appelé « système de lozi » en utilisant la synchronisation à base d'observateur impulsifs.Nous citerons aussi des éléments sur lacryptographie et les différentes méthodes de cryptages/décryptage des systèmes chaotiques.

Le quatrième chapitre présentera la réalisation pratique sur cartes ESP32 du schéma de transmission sans fil conçu et des différents résultats expérimentaux.

Enfin,nous terminons par une conclusion générale et des perspectives

Chapitre I

Généralités sur les systèmes chaotiques

I.1 Introduction

De nos jours, dans le langage commun « Chaos » décrit un état de désordre et d'irrégularité. Dans le langage scientifique le terme « chaos » définit l'état d'un système dynamique dont le comportement ne se répète jamais, qui est très sensible aux conditions initiales et impossibles à prédire sur le long terme. Dans le siècle passé, plusieurs chercheurs se sont intéressés aux comportements inhabituels des systèmes dynamiques non linéaires et on a découvert que certains systèmes présentaient des instabilités de nature très étrange, cela fait la découverte des signaux chaotiques qui ont un comportement complètement déterministe mais qui font penser à des allures pseudo-aléatoires. Ce concept a émergé dans la seconde partie des années 1970 en tant que science des phénomènes non linéaires complexes montrant certaines caractéristiques communes [7].

Il faut aussi noter que le comportement chaotique observé dans le temps n'est dû, ni à une source extérieure de bruit, ni à un degré infini de liberté, ni à un caractère stochastique, autrement dit ce comportement est intrinsèque. Le concept moderne du chaos déterministe est de plus en plus utilisé dans des contextes scientifiques [8], on peut ainsi trouver le chaos dans plusieurs domaines d'application comme les mathématiques, la physique, la chimie, la biologie.

I.2 Définitions et concepts de base

Dans cette partie, nous présenterons et définirons quelques concepts et notions de base liés aux systèmes dynamiques.

I.2.1 Système

Un système est un ensemble d'organes, assemblés pour concourir à un résultat. (Exemple :Système mécanique : masse-ressort) [9].

LaFigure (I.1) présente le schéma synoptique d'un système

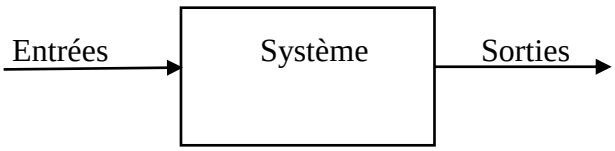


Figure I.1 : Schéma synoptique d'un système

I.2.2 Système dynamique

Un système dynamique est un modèle mathématique d'un phénomène évoluant dans le temps, ce phénomène pouvant provenir de la physique, la mécanique, l'économie, la biologie, l'écologie, la chimie, etc.

Il est constitué d'un espace de phase et d'un espace d'état. Un système dynamique en temps continu peut être modélisé mathématiquement par un système d'équations différentielles, alors qu'en temps discret on parle d'équations aux différences finies [10].

I.2.3 Système autonome

Un système est dit autonome s'il est indépendant du temps initial, alors qu'un système non autonome ne l'est pas.

Dans un système autonome, tout instant peut être considéré comme temps initial, et tout état $x(t)$du système peut être considéré comme état initial.

Soit le système suivant :

$$\dot{x}= \text{f (x, v)} \tag{I.1}$$

Où x est le vecteur d'état et v le vecteur des paramètres

Le système est dit autonome lorsque la fonction f ne dépend pas explicitement du temps [11].

- **Système dynamique en temps continu**

Soit le système défini par les relations suivantes :

$$\begin{cases} \dot{x} = f(x,t,u) \\ y = h(x,t,u) \end{cases} \tag{I.2}$$

Où : $x$est un vecteur d'état de dimension n, f :$\mathbb{R}^n \rightarrow \mathbb{R}^n$ est une fonction non linéaire désignant le champ de vecteurs, h une fonction éventuellement non linéaire qui désigne le vecteur de sortie u et représente l'entrée du système [12].

Un système dynamique continu autonome est généralement exprimé sous la forme d'un ensemble d'équations différentielles ordinaires (EDO) comme suit :

$$\frac{dx}{dt}= \text{f(x)} \tag{I.3}$$

Où

- x est un vecteur d'état représentant les variables du système.
- f(x) est une fonction vectorielle qui décrit la dynamique du système.

- **Système dynamique en temps discret**

Comme il a été déjà précisé le système dynamique est dans ce cas représenté par des équations aux différences finies [12], avec le modèle général suivant :

$$\begin{cases} x(k+1) = G(k, x(k), u(k)) \\ y(k) = h\big(k, x(k), u(k)\big) \end{cases} \quad \text{(I.4)}$$

Où

$x(k)$ représente l'état du système à l'instant$k$.

$u(k)$ est l'entrée du système à l'instant k.

G est une fonction décrivant l'évolution de l'état en fonction du temps k, de l'état actuel x(k), et de l'entrée u(k).

$y(k)$ est la sortie du système à l'instant k.

$h$est une fonction qui lie l'état x(k)et l'entrée u(k) à la sortie y(k).

En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k :

$$\begin{cases} x(k+1) = G(x(k), u(k)) \\ y(k) = h\big(x(k), u(k)\big) \end{cases} \quad \text{(I.5)}$$

I.2.3 Espace d'état

L'espace d'état est l'ensemble des coordonnés nécessaires à la description complète d'un système. Cet espace peut être continu ou discret.

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad \text{(I.6)}$$

tel que

[x,y,z] est le vecteur d'état.

σ, β et ρ sont des paramètres constants.

I.2.4 Espace de phase

L'espace des phases permet de traduire des séries de nombre en une représentation spatiale, de dégager l'essentiel de l'information d'un système en mouvement et de dresser la carte routière de toutes ses possibilités. L'espace des phases est un espace mathématique souvent

multidimensionnel. Chaque axe de coordonnées de cet espace correspond à une variable d'état du système dynamique étudié et chaque variable d'état caractérise le système à un instant donné [14].

I. 2. 5Attracteur

La région de l'espace de phases vers laquelle convergent les trajectoires d'un système dynamique s'appellent '' attracteur ''. Les attracteurs sont des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques. Il en existe quatre types distincts : le point fixe, le cycle limite, l'attracteur quasi-périodique (Tore) et l'attracteur étrange [15].

I. 2. 5 .1 Types d'attracteurs

Il existe plusieurs types d'attracteur ci-dessus nous citons

- ***Point fixe*** : est un point de l'espace de phase vers lequel tendent les trajectoires, c'est donc une solution stationnaire constante.
- ***Cycle limite*** *:*est une trajectoire fermée dans l'espace des phases vers laquelle tendent les trajectoires. C'est donc une solution périodique du système.

- **Différents ordres de cycles limites**

- Cycles limites simples : Trajectoires périodiques dans l'espace des phases, représentant des comportements réguliers.
- Cycles limites multiples : Plusieurs trajectoires périodiques sont existantes, souvent observées lors de bifurcations.
- Cycles limites quasi-périodiques : Trajectoires oscillant avec plusieurs fréquences, formant un tore.
- Attracteur chaotique.

- **Tore :** C'est un cas particulier de cycle limite, le système est caractérisé au moins par deux Périodes simultanées dont le rapport est aléatoire, la trajectoire de phase ne s'annule pas sur elle-même [15].

I.2.6 Système linéaire

On appelle système linéaire, un système dont le modèle mathématique est linéaire (Équations différentielles, aux différences..), qui obéit au principe de la superposition et de proportionnalité [16].

En d'autres termes, les relations entre les entrées et les sorties sont directement proportionnelles et ne présentent pas de comportements complexes ou non linéaires.

Un système linéaire peut être représenté parun système d'équation suivant :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \end{cases} \quad \text{(I.7)}$$

Avec :

$x\,(t)$: Vecteur colonne de variable d'état de dimension n (n : dimension de l'espace d'état)

$y\,(t)$: Vecteur colonne des sorties du système de dimension p.

A : Matrice d'état de taille ($n \times n$).

B : Matrice de commande de taille ($n \times m$).

C : Matrice d'observation de taille ($p \times n$).

D : Matrice de transmission de taille ($p \times m$).

I.2.7 Système non linéaire

La plupart des systèmes physiques présentent des caractéristiques non linéaires en raison de divers facteurs commele changement de phase ou les phénomènes chaotiques.

Un système est dit non linéaire s'il ne respecte pas le principe de superposition et si la relation entre les grandeurs d'entrée et de sortie est une équation différentielle non linéaire avec des coefficients non constants généralement [16].

Il peut être représenté par un système de la forme suivante :

$$\begin{cases} \dot{x}\,(t) = F\,(x\,(t), u\,(t)) \\ y\,(t) = H\,(x\,(t), u\,(t)) \end{cases} \quad \text{(I.8)}$$

I.3 Définition du chaos

Le terme chaos définit un état particulier d'un système modélisé par des équations non linéaires dont le comportement ne se répète jamais et qui est très sensible aux conditions Initiales, et imprédictible à long terme [17].

Il renvoie à un domaine d'étude qui examine les systèmes dynamiques très sensibles aux conditions initiales. De petites variations dans ces conditions peuvent entraîner des résultats très différents dans le comportement futur du système.

Les systèmes chaotiques se caractérisent souvent par un comportement imprévisible, non périodique et apparemment aléatoire, bien qu'ils soient déterministes. Cela signifie que leur comportement est entièrement défini par leurs conditions initiales et leurs règles dynamiques.

I.4 Propriétés d'un système chaotique

I.4.1 Déterminisme

La notion de déterminisme implique la possibilité de « prédire » l'évolution future d'un phénomène en se basant sur des événements passés ou présents. Cependant, le comportement imprévisible des systèmes chaotiques est attribuable à leurs non-linéarités. Contrairement aux phénomènes aléatoires où il est impossible de prévoir la trajectoire d'une particule, un système chaotique fonctionne selon des règles déterministes, sans éléments de probabilité [18].

I.4.2 Non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique [18].

I.4.3 Sensibilité aux conditions initiales

Cette caractéristique indique que de petites modification son variations dans les conditions initiales d'un système, engendrent que les trajectoires restent proches pendant un certain moment puis à partir d'un instant, elles deviennent complètement divergées[19]. Cela signifie que même des erreurs minimes dans la mesure des conditions initiales peuvent avoir un impact significatif sur les prédictions futures du système.

Dans la figure (I.2) nous illustrons cette caractéristique par l'exemple de Lozi.

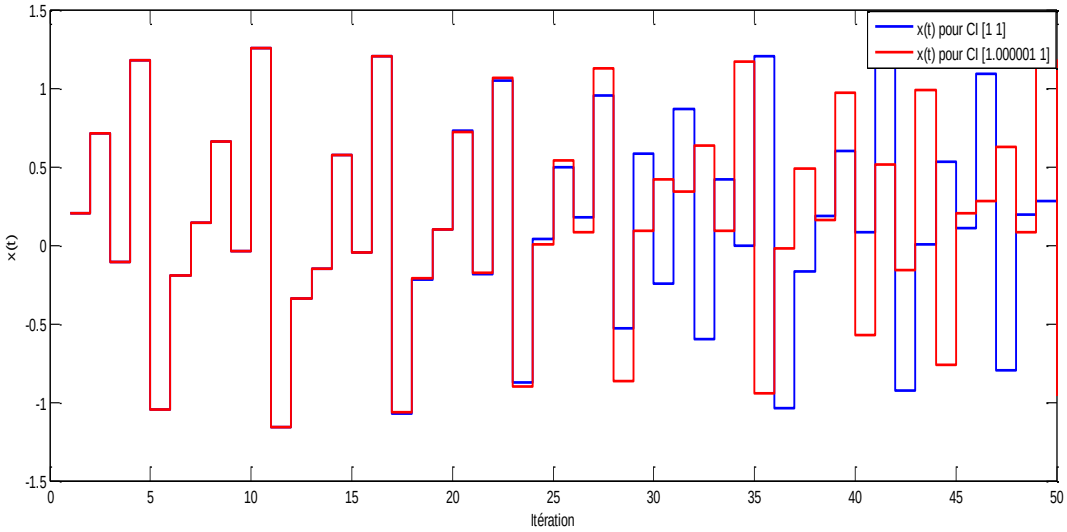


Figure I.2 : Sensibilité aux conditions initiales du modèle de Lozi

-On remarque que les deux trajectoires correspondants aux conditions initiales $(x_1(0), x_2(0) = (1,1)$et $(x_1(0), x_2(0) = (1.000001,1)$sont identiques au début, mais après un certain temps, elles divergent.

I.4.4 Diagramme de bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs de la structure d'un système dynamique.

Tout système régi par des équations différentielles à un comportement asymptotique en fonction de ses paramètres, un changement quantitatif de ces derniers produit un changement qualitatif. Par exemple : déstabilisation d'un équilibre stable, apparition ou disparition d'un cycle ou d'un attracteur, un point d'équilibre dans le plan de phase qui devient un cycle limite [20].

La valeur du paramètre pour laquelle la bifurcation se produit et nommée le point de bifurcation ; on appelle ce changement « bifurcation ».

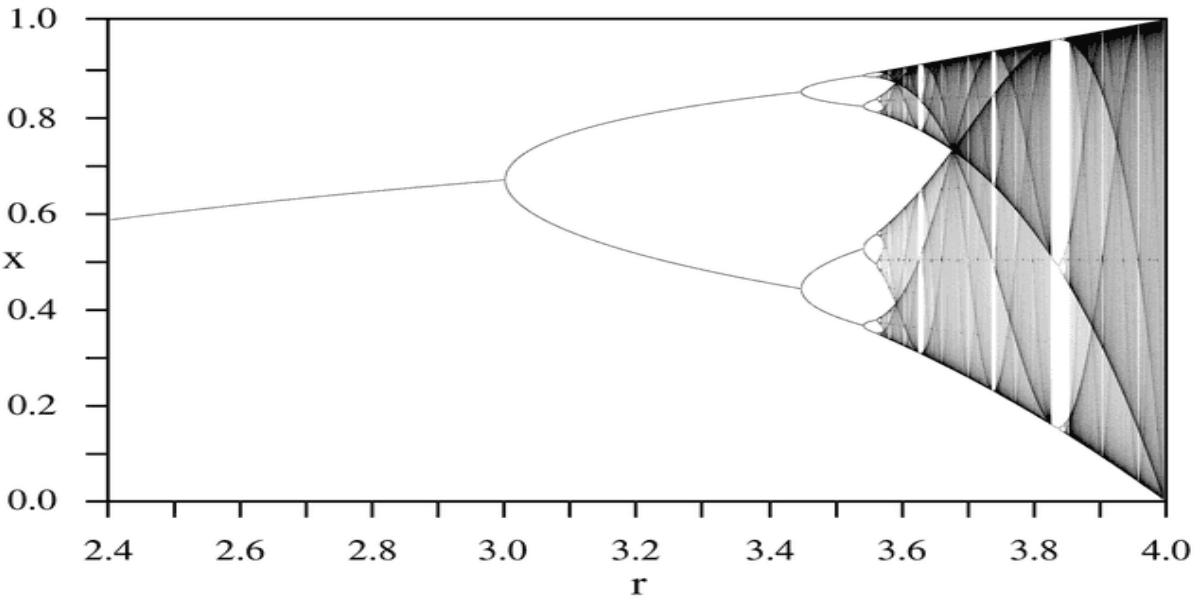


Figure I.3 : Diagramme de bifurcation

I.4.5 Aspect aléatoire

L'une des caractéristiques des systèmes chaotiques est l'aspect aléatoire de son évolution temporelle et son comportement imprévisible. Celui-ci correspond à une évolution complexe, non périodique et non prédictible [9].

La figure suivante illustre le caractère aléatoire de l'évolution de l'une des composantes du système de Lozi par rapport au temps.

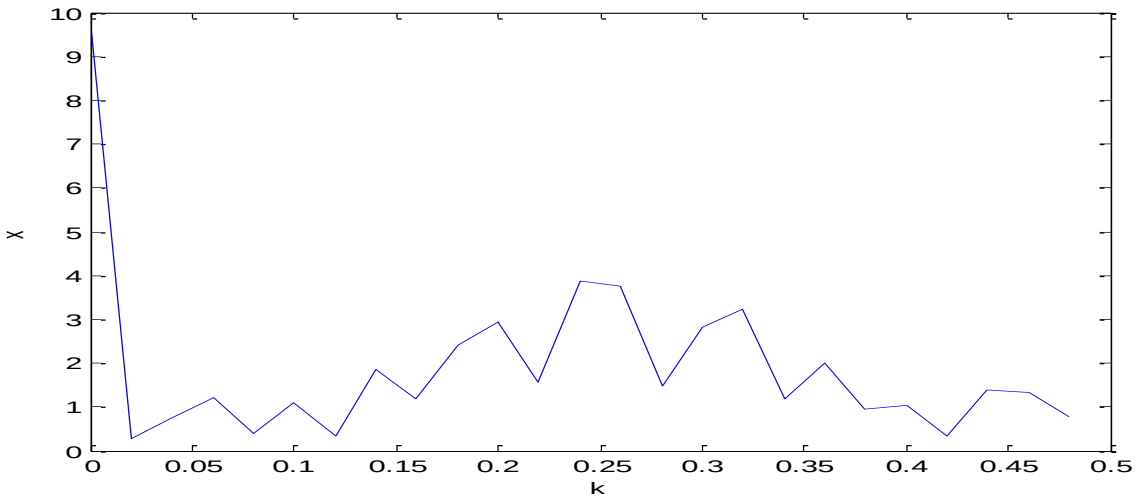


Figure I.4 : Aspect aléatoire du signal (état) x du système de Lozi

I.4.6 Attracteur étrange (chaotique)

Un attracteur est dit chaotique ou étrange lorsqu'il est contenu dans un espace fini et son volume est nul. Il a une forme géométrique complexe qui caractérise l'évolution des systèmes à long terme. Au bout d'un certain temps, tous les points de l'espace des phases donnent des trajectoires qui tendent à former l'attracteur étrange. La dimension de l'attracteur chaotique est fractale [1].

La figure suivante illustre l'attracteur étrange de Lozi :

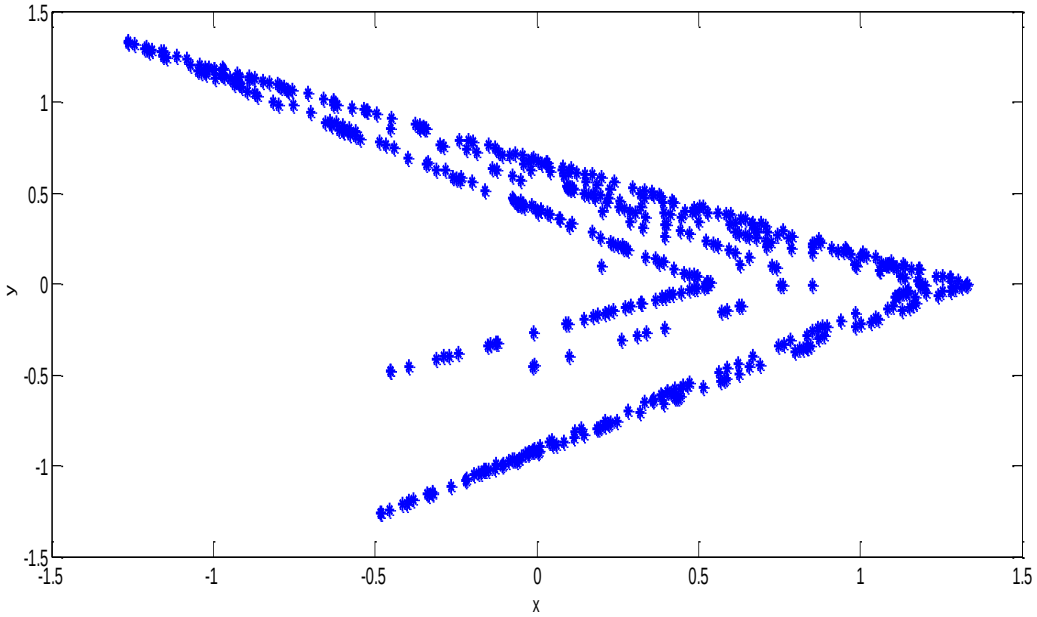


Figure I.5 : Attracteur étrange du modèle de Lozi

I.4.7 Exposants de Lyapunov

L'exposant de Lyapunov est une mesure mathématique utilisée pour étudier la stabilité et l'instabilité des systèmes dynamiques il qualifie le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes [11].

-Lorsqu'un exposant de Lyapunov est positif, cela suggère une tentative de divergence restreinte par les bornes de l'intervalle[11].

-si l'exposant de Lyapunov est négatif, cela signifie que les petites variations de la condition initiale n'ont aucun effet à long terme.

Etat	Attracteur	Dimension de l'attracteur	Exposants de Lyapunov
Point d'équilibre	Point	0	$\lambda_n \leq \ldots \leq \lambda_1 \leq 0$
Périodique	cyrcle limite	1	$\lambda_1 = 0$ $\lambda_n \leq \ldots \leq \lambda_2 \leq 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \ldots \leq \lambda_3 \leq 0$
Période d'ordre K	Tore d'ordre k	k	$\lambda_1 = \ldots = \lambda_K = 0$ $\lambda_n \leq \ldots \leq \lambda_{k+1} \leq 0$
Chaotique	Attracteur étrange	Non entier	$\lambda_1 > 0$ $\sum_{i=2}^{n} \lambda i < 0$
Hyper chaotique	Attracteur étrange	Non entier	$\lambda_1 > 0 \quad \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda i < 0$

Tableau 1: Classification des régimes permanents en fonction des exposants de Lyapunov.

- On dit qu'un système continu ou discret (comme le système de Lozi) est chaotique s'il possède au moins un exposant de Lyapunov positif.

I.5 Routes vers le chaos[21]

Il est reconnu qu'il existe différentes façons par lesquelles un système devient chaotique. En général, elles résultent de différentes bifurcations. Cela étant dit, « rien ne permet d'énoncer avec précision sous quelles conditions nécessaires et/ou suffisantes ces routes prennent place ».

Les routes vers le chaos peuvent être les suivantes :

I.5.1 Doublement de période

En faisant varier (en augmentant) l'un des paramètres d'un système qui a un mouvement périodique fondamental, le processus arrive à une bifurcation où l'évolution du processus double la période jusqu'à l'apparition du chaos.

I.5.2Quasi-périodicité

Ce deuxième scénario fait intervenir pour un système périodique, l'apparition d'une autre fréquence dont le rapport avec la première est irrationnel, un nouveau changement de paramètres fait apparaitre une troisième fréquence, et ainsi de suite jusqu'a atteindre un régime chaotique.

I.5.3 Intermittence

Il s'agit d'un phénomène qui se manifeste dans un système dynamique et périodique par des phases de périodicité stable et des phases chaotiques Après un certain temps, le comportement chaotique prend le dessus et il devient chaotique.

I.6 Exemples de systèmes chaotiques

Il existe plusieurs systèmes qui ont une dynamique chaotique, nous allons prendre comme exemple le système de Lorenz pour cas de système continu et celui de la fonction logistique pour le cas de système discret.

I.6.1 Système chaotique continu

Le système de Lorenz illustre de manière renommée les systèmes différentiels qui présentent un comportement chaotique sous certaines configurations de paramètres.
Le système le Lorenz prend la forme différentielle suivante [23] :

$$\begin{cases} \dot{x}(t) = a\,(y - x) \\ \dot{y}(t) = -xz + cx - y \\ \dot{z}(t) = xy - bz \end{cases} \qquad (I.9)$$

- Les valeurs a=10, b= 8/3 et c sont des paramètres de contrôle du système.
- Les conditions initiales sont choisies et fixées à $(x_0, y_0, z_0) = (0.01\ ,\ 0.01\ ,\ 0.01)$.
- Pour avoir une dynamique chaotique, on fait varier le paramètre c. Le comportement du système de Lorenz pour des valeurs différentes est de c est représenté dans les figures suivantes :

- Pour ***c*** = **10 ,** l'espace d'état présente un point fixe figure (I.6)

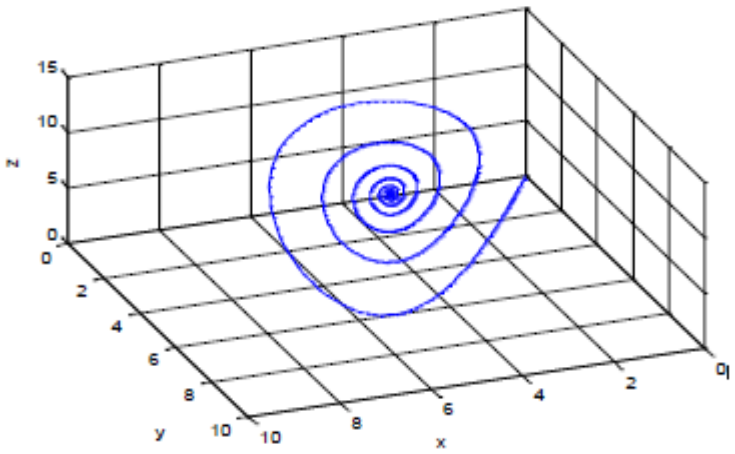


Figure I.6: Point fixe

- La trajectoire converge vers un point d'équilibre ; dans ce cas, le système n'est pas chaotique

- Pour***c*** = **28,** l'espace d'état présente un attracteur chaotique étrange figure (I.7)

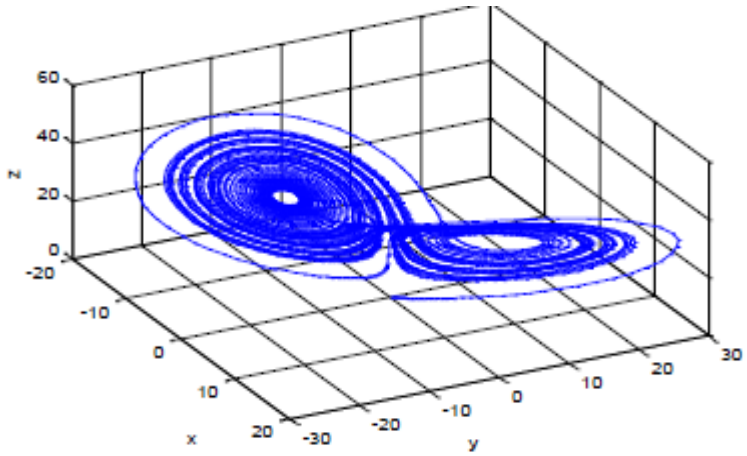


Figure I.7 : Attracteur étrange (sons forme de papillon)

-On remarque que le portrait de phase des trajectoires ressemble à un papillon, c'est un attracteur étrange caractérisant une évolution chaotique du système de Lorenz donc la dynamique du système est chaotique.

- Pour $\boldsymbol{c = 160}$, L'espace d'état présente un Tore voire la figure (I.8)

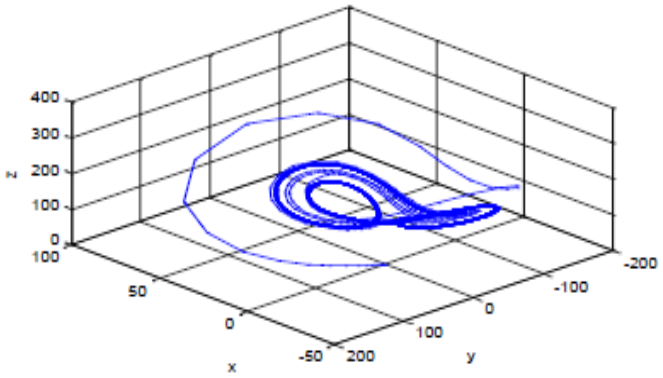


Figure I.8 : Tore

- Les trajectoires convergent vers un attracteur de type tore.

-La figure (I.9) illustre la propriété de sensibilité aux conditions initiales avec une différence de l'ordre de $\sigma = 10^{-6}$ sur la valeur initiale de l'état x.

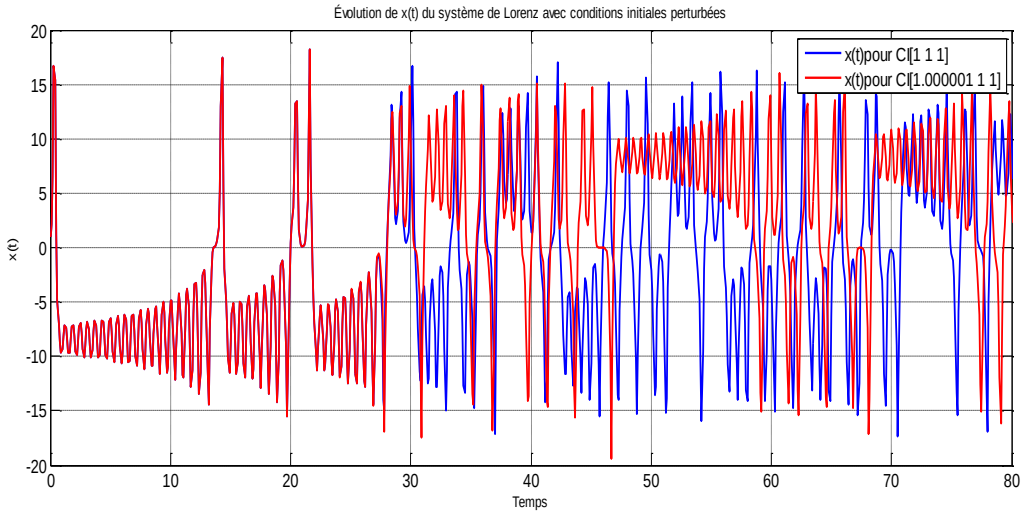


Figure I.9 : Sensibilité aux conditions initiales de l'état x (t) du système de Lorenz

I.6.2 Système chaotique discret

On présente dans cette section un modèle de système dynamique chaotique à temps discret. Ce modèle est appelé application quadratique (ou logistique).

La fonction logistique qui est à temps discret, est présentée sous la forme d'équation aux différences suivantes :

$$x(k+1) = \mathrm{r}.x(\mathrm{k})\,(1 - x(\mathrm{k})) \qquad \text{(I.10)}$$

Où k = 0,1,2,…… dénote le temps discret, et r Є[0; 4] est un paramètre de contrôle , et x la variable d'état .

- Aspect aléatoire

La figure(I.10) suivante illustre l'aspect aléatoire du système

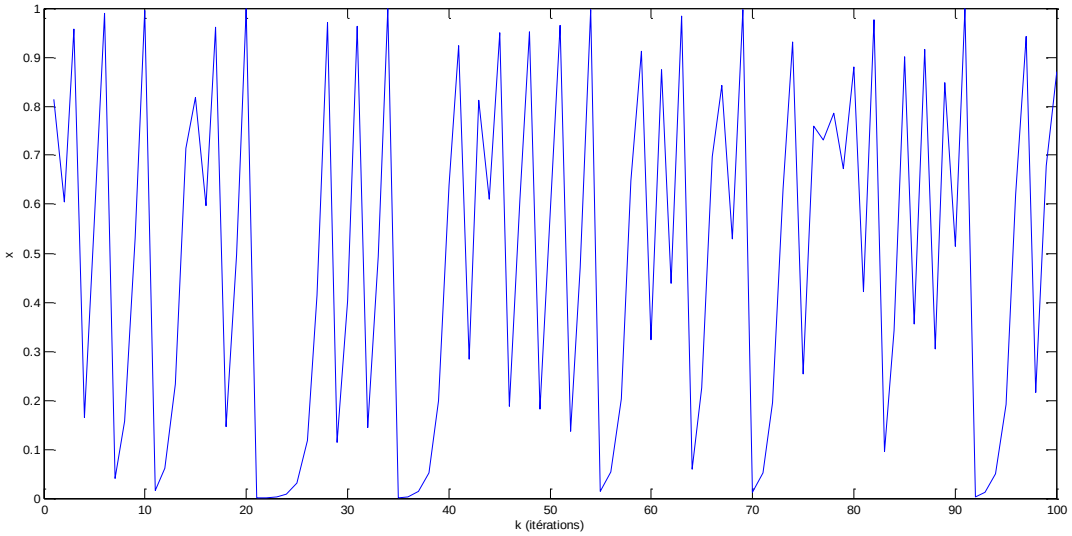


Figure I.10 : Aspect aléatoire du signal x de la fonction logistique

- Exposant de Lyapunov

L'exposant de Lyapunov est un indicateur qui mesure le taux de séparation des trajectoires proches dans un système dynamique. Pour le système (1.9) :

L'exposant de Lyapunov λ est donné par :

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} ln|f'(xi)| \qquad (I.11)$$

où f′(x) est la dérivée de la fonction f .

en appliquant la formule (I.12) pour calculer les exposants de Lyapunov, pour r=4, la dérivée est :

$$f'(x) = 4(1 - 2x) \qquad (I.12)$$

L'exposant de Lyapunov pour la fonction logistique avec r=4 est approximativement 1.386.Donc cet exposant positif indique que le système est chaotique, car des trajectoires initialement proches divergent de manière exponentielle.

I.7 Conclusion

Dans ce chapitre, nous avons présenté et fourni des définitions et notions de base sur la théorie du chaos. Des caractéristiques propres aux systèmes présentant un comportement chaotique telles que la sensibilité aux conditions initiale, aspect aléatoire et attracteur étrange ont été citées et étudiées pour mieux introduire les systèmes chaotiques.

Afin d'être appliqués dans notre cas pour la transmission sécurisée de données, les systèmes chaotiques doivent être synchronisés.

Le principe et l'objectif de la synchronisation des systèmes chaotiques seront l'objectif du chapitre suivant.

Chapitre II

Synchronisation des systèmes chaotiques

II.1 Introduction

Pendant longtemps, le chaos a été considéré comme indésirable par la communauté scientifique. Cependant, dans les années 90, des scientifiques ont réalisé que le chaos pouvait être contrôlé et ont commencé à chercher ses applications possibles [23]. Les signaux issus des systèmes chaotiques sont imprédictibles à long terme, peuvent présenter des propriétés proches de l'aléatoire (autocorrélation réduite), bien qu'issus de systèmes déterministes, ces caractéristiques sont liées aux propriétés requises par les schémas de chiffrement. Cependant les scientifiques ont réalisé que les systèmes chaotiques pouvaient être utilisés dans le domaine des télécommunications, ce qui pose directement le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique employé à l'émetteur[24]. Dans la section précédente, nous avons montré la sensibilité très importante aux conditions initiales des systèmes chaotiques, et à première vue la synchronisation chaotique parait difficile à réaliser. A la différence de la synchronisation classique employée dans les systèmes de télécommunication où l'on cherche à reproduire juste une période d'oscillation, la synchronisation chaotique présente plus de contraintes.

Dans les systèmes de communication, la synchronisation est fondamentale pour une transmission réussie.

Dans ce chapitre, nous présenterons les principales méthodes et types de synchronisation utilisés et nous nous intéressons au type de synchronisation impulsive que nous appliquerons dans le schéma de transmission proposé.

II.2 Synchronisation des systèmes chaotiques

Dans cette partie, nous aborderons la synchronisation chaotique et étudierons son principe.

II.2.1 Définition

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système.

Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante, si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme "Couplage'', les deux systèmes finiront par céder la place à un comportement commun, ils finiront par se synchroniser [10].

La synchronisation de deux systèmes S_1 et S_2 peut être définie comme suit :

$$\begin{cases} S_1 : \dot{x} = f_1(x, u) \\ S_2 : \hat{x} = f_2(x, u) \end{cases} \tag{II.1}$$

Avec x (t), $\hat{x}(t) \in R^n$, $f1$ et $f2$ des fonctions non linéaires définies de $R^n \rightarrow R^n$.

Les deux systèmes sont synchronisés si :

$$lim_{t\to\infty} e(t) = lim_{t\to\infty} |x(t) - \hat{x}(t)| = 0 \qquad \text{(II.2)}$$

Avec :

$x(t)$**:** L'état du système maître (S1).

$\hat{x}(t)$**:** L'état du système esclave (S2).

II.2.2 Historique

Les phénomènes de synchronisation ont fait l'objet de discussions dans divers domaines de recherche de puis $17^{ème}$siècle, lorsque la synchronisation de deux pendules d'horloges attachées à une poutre de support commune a été découverte pour la première fois par Christian Hüygens en 1673 [25], la synchronisation des systèmes dynamique a trouvé son chemin vers de nombreuses applications en théorie et en pratique et plusieurs types de synchronisation ont été étudiés et proposés.

Récemment, les chercheurs de la synchronisation se sont intéressés aux systèmes chaotiques et comme ces derniers sont caractérisés par une sensibilité aux conditions initiales, à première vue, parler de synchronisation pour des systèmes chaotiques semble donc être surprenant, et on peut penser que le chaos est incontrôlable. Cependant, des recherches récentes ont montré que l'on pouvait synchroniser deux systèmes chaotiques en les couplant.

II.2.3 Principe de la synchronisation (Pecora et Carroll)

Pecora et Carroll ont montré qu'une condition nécessaire et suffisante pour que deux sous-systèmes s1 et s2 soient synchronisés est que tous les exposants conditionnels de Lyapunov soient négatifs [26].

L'idée consiste à diviser le système d'origine en deux sous-systèmes, l'un maître et l'autre esclave de telle sorte que les variables dynamiques de départ soient reparties de part et d'autre de chacun des sous-systèmes. Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du signal de départ (système maître) sert à piloter (synchroniser) le premier des deux systèmes dupliqués mis en cascade, qui lui-même permet de synchroniser le second sous-système dupliqué.

II.3 Modes de synchronisation

Il existe deux modes de synchronisation : la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

II.3.1 Synchronisation unidirectionnelle

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques A et B est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [12].

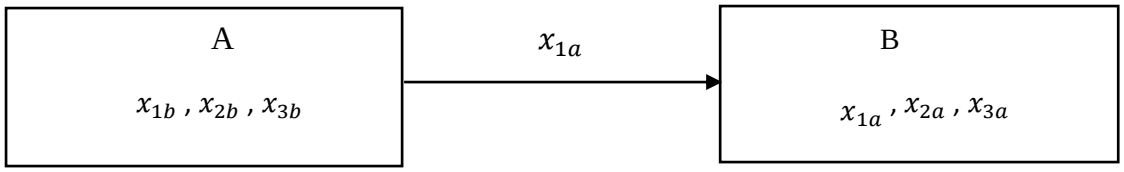


Figure II.1 : Couplage unidirectionnel

II.3.2 Synchronisation bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques A et B est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [12].

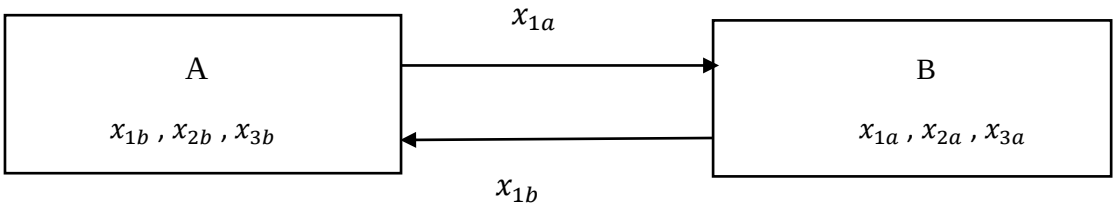


Figure II.2 : Couplage bidirectionnel

II.4 Types de Synchronisation

Plusieurs types de synchronisation ont été proposés dans la littérature. Dans ce qui suit, nous citerons quelques approches en expliquant leurs principes.

II.4.1 Synchronisation complète

On considère un système chaotique maître représenté par [27]:

$$x_m \text{ (k+1)} = \text{F}((x_m\text{(k)}) \qquad \text{(II. 3)}$$

Le système esclave représenté par la formule suivante:

$$x_s(k+1) = G\,(x_s\,(k)) + U \qquad \text{(II.4)}$$

(x_m ,x_s) : sont les vecteurs d'état du système maître et esclave respectivement.

F et G $\in \mathbb{R}^n$: des fonctions non linéaire.

U : est un vecteur de contrôle à déterminer, l'erreur de la synchronisation complète est définie par :

$$e(t) = x_s\,(t) - x_m(t) \qquad \text{(II.5)}$$

Telle que : $\lim_{t\to\infty} || e(t)|| = 0$; où $||.||$ est la norme euclidienne.

- Si F = G, la relation devient une synchronisation complète identique.
- Si F ≠G, c'est une synchronisation complète non identique

On a une coïncidence complète entre les variables d'état des deux systèmes synchronisés [12].

II.4.2 Synchronisation retardée

Dans cette synchronisation, l'état du système esclave tend vers l'état décalé dans le temps du système maître c'est-à-dire [28]:

$$\lim_{t\to\infty} \| x_s(t) - x_m(t-\tau) \| = 0 \qquad \text{(II.6)}$$

Tel que :

- x_m : l'état du système maître.
- x_s : l'état du système esclave.
- τ : un retard positif.

➢ Le maitre : est un système indépendant.

➢ L'esclave : est un système qui est dépendant du système maître.

II.4.3 Synchronisation Projective

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Soit le système suivant :

$$\lim_{t\to\infty} \| x_s\,(t) - a x_m(t) \| = 0 \qquad \text{(II.7)}$$

Où :

a : représente le facteur d'échelle.

x_m: L'état du système maître.

x_s : L'état du système esclave.

Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés [29].

II.4.4 Synchronisation généralisée

La synchronisation généralisée est considérée comme une généralisation de la synchronisation complète, l'anti-synchronisation et la synchronisation projective dans le cas des systèmes chaotiques de dimensions et de modèles différents [30]. Elle se manifeste par une relation fonctionnelle entre les deux systèmes chaotiques.

$$\lim_{t\to\infty} \| x_s(t) - \phi x_m(t) \| = 0 \qquad \text{(II.8)}$$

II.4.5 Synchronisation de phase

Les phases des deux systèmes, maître et esclave sont $\phi_1$et $\phi_2$respectivement. Lasynchronisation de phase entre ces deux systèmes chaotiques est exprimée par la relation :

$$|n\phi_1 - m\phi_2| < \varepsilon \; ; \quad \forall n, m \in \mathbb{Z} \qquad \text{(II.9)}$$

Où :

ϕ_1: la phase du système maître.

ϕ_2: la phase du système esclave.

m et n sont deux entiers naturels.

ε : une constate positive.

Cette notion classique de synchronisation a été étendue aux systèmes chaotiques. Les amplitudes de ces systèmes restent non corrélées [31].

II.5 Techniques de synchronisation

Afin d'atteindre un ou plusieurs types de synchronisation mentionnés ci-dessus, dans ce qui suit, nous citerons quelques approches adoptées en expliquant leurs principes.

II.5.1 Synchronisation par retour d'état

La synchronisation par retour d'état est une technique utilisée pour synchroniser l'état d'un système dynamique avec un autre système similaire en utilisant une loi de contrôle basée sur l'état du système d'origine. L'objectif est de faire en sorte que deux systèmes initialement indépendants évoluent de manière identique au fil du temps, même si leurs conditions initiales sont différentes [32].

Ce système est représenté par une équation dynamique du type :

$$x_m(t) = f\big(x(t)\big) \tag{II.10}$$

Où :

x_m:L'état du système à l'instant t et f(x(t)) décrit la dynamique du système.

Pour le système qui doit se synchroniser avec le système maître ; Il est contrôlé en fonction de l'état du système maître. Sa dynamique est donnée par :

$$x_s(t) = f\big(x_s(t)\big) + K\big(x_m(t) - x_s(t)\big) \tag{II.11}$$

Où :

x_s : L'état du système esclave.

K : un gain qui détermine la force de la correction appliquée pour aligner l'état x_s (t) avec $x_m(t)$.

L'erreur entre les états des deux systèmes est définie comme :

$$e(t) = x_m\,(t) - x_s(t) \tag{II.12}$$

La synchronisation par retour d'état vise à faire converger cette erreur vers zéro, c'est-à-dire

$$lim_{t\to\infty} e(t) = 0 \tag{II.13}$$

II.5.2 Synchronisation par backstepping

La méthode du backstepping est une méthode récursive qui se base sur le choix d'une fonction de Lyapunov avec la conception du contrôleur nécessaire [33].

On considère que le système maître et le système esclave sont définis comme suit :

$$\begin{cases} \dot{x}_{11} = f_1(x_1, x_2) \\ \dot{x}_{12} = f_2(x_1, x_2, x_3) \\ \vdots \\ \dot{x}_{1n} = f_n(x_1, x_2, \dots, x_n) \end{cases} \tag{II.14}$$

Et :

$$\begin{cases} \dot{x}_{21} = f_1(x_1, x_2) \\ \dot{x}_{22} = f_2(x_1, x_2, x_3) \\ \vdots \\ \dot{x}_{2n} = f_n(x_1, x_2, \dots, x_n) \end{cases} \tag{II.15}$$

Où,f_1 est une fonction linéaire ,f_i ($i = 2$,3 , . . . , n) sont des fonctions non- linéaires.

L'erreur de synchronisation est définie comme suit :

$$\begin{cases} \dot{e}_1 = \dot{x}_{21} - \dot{x}_{11} \\ \dot{e}_2 = \dot{x}_{22} - \dot{x}_{12} \\ \vdots \\ \dot{e}_n = \dot{x}_{2n} - \dot{x}_{1n} \end{cases}$$

Alors, la dynamique du système d'erreur s'écrit :

$$\begin{cases} \dot{e}_1 = g_1(e_1, e_2) \\ \dot{e}_2 = g_2(e_1, e_2, e_3) \\ \vdots \\ \dot{e}_n = g_n(e_1, e_2, \dots, e_n) \end{cases} \quad \text{(II.16)}$$

Où : $g_1$est une fonction linéaire et $g_i(i = 2\ ,\ 3\ ,\ .\ .\ .\ ,\ \text{n})$ sont des fonctions non- linéaires. L'objectif est de calculer une loi de contrôle u qui assure la convergence du système e_i $(i = 2,$ 3 , . . . , n) , vers l'origine en utilisant l'algorithme backstepping. Pour cela, le système d'erreur (II.15) doit être décomposé en sous systèmes $(e_1, e_2), (e_1, e_2, e_3), (e_1, e_2, \dots, e_n)$, et pour chaque sous-système on définit une fonction de Lyapunov V positive.

II.5.3 Synchronisation Par observateur [34]

La connaissance des entrées, des sorties et du modèle d'un système dynamique permet la reconstruction d'un ou plusieurs états du système qui ne peuvent être mesurés directement, soit à cause de leur inaccessibilité ou par économie.

La synchronisation par observateur consiste à construire un système esclave qui soit un observateur du système maître, et qui va permettre d'avoir une évolution identique. Dans le cas non linéaire, le problème de la conception d'un observateur est défini comme suit :

Soient les deux systèmes suivant :

$$\begin{cases} s_1 : \dot{x} = f(x) \\ s_2 : \dot{\hat{x}} = \hat{f}(\hat{x}) \end{cases} \quad \text{(II.17)}$$

Si les systèmes $s_1$et s_2 sont synchronisés, on aura :

$$\lim_{t \to \infty} |x(t) - \hat{x}(t)| = 0 \quad \text{(II.18)}$$

$x\ (t)$: État du système.

$\hat{x}\ (t)$: État estimé.

Le principe de la synchronisation par observateur est illustré par la figure suivante :

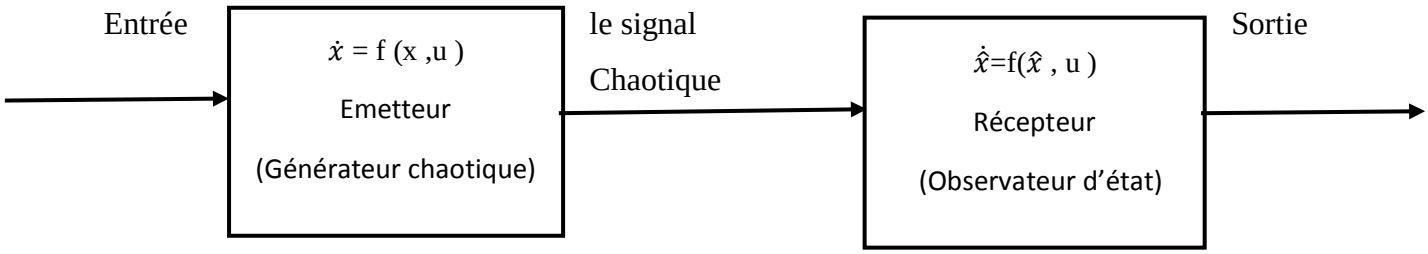


Figure II.3 : Principe de la synchronisation à l'aide d'observateur

II.6 Types d'observateurs utilisés pour la synchronisation

La synchronisation peut être réalisée à l'aide d'un observateur ci-dessus les observateurs sauvent utilisé par la synchronisation de système chaotique.

II.6.1 Observateur à grand gain

Les techniques dites à grand gain peuvent être appliquées sans transformation du système initial. Dans ce cas, la conception de l'observateur se fait directement à partir de la structure du système. Cette technique utilise la théorie de stabilité de Lyapunov pour adapter les techniques développées dans le cas linéaire [35]. La méthode présentée donne des conditions suffisantes de convergence de l'état estimé vers l'état réel du système, pour la classe des systèmes non linéaires décrits par le modèle suivant :

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + G(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \quad \text{(II.19)}$$

Où :

$\hat{x}(t)$: l'estimation de l'état x(t).

$\hat{y}$: l'estimation de la sortie y(t).

G : est la matrice de gain de l'observateur.

La dynamique de l'état comporte une partie linéaire non commandée et une partie non linéaire commandée, vérifiant en général la condition de Lipschitz par rapport à x

$$\|f(x_1) - f(x_2)\| \leq k\|x_1 - x_2\| \quad \text{(II.20)}$$

Où :

k: Constante de Lipschitz

L'observateur à grand gain possède la structure suivante:

$$\dot{\hat{x}} = A\hat{x}(t) + f(\hat{x}(t),u(t)) + K(y(t) - C\hat{x}(t)) \quad \text{(II.21)}$$

L'appellation grand gain provient de la structure de l'observateur : lorsque la fonction non linéaire possède une grande constante de Lipschitz, la moindre erreur entre l'état réel et l'état estimé va se répercuter et croître. Par conséquent, le gain K de l'observateur (II.21) doit être important pour compenser cette amplification de l'erreur. La dynamique de l'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$.

II.6.2 Observateur à mode glissant

Un observateur à modes glissants est un observateur dont le terme correcteur est une fonction sign. Il s'agit de contraindre, à l'aide des fonctions discontinues, les dynamiques du système à converger vers une "surface de glissement"[36].

Soit le système suivant :

$$\begin{cases} \dot{x}(t) = f(x) + g(x)u \\ y(t) = h(x) \end{cases} \quad \text{(II.22)}$$

L'observateur à modes glissants pour ce système s'écrit de la façon suivante :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + Ksign(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad \text{(II.23)}$$

Où :

K : est une matrice de gain de dimension (n $\times p$).

Dans ce cas, on impose l'évolution des dynamiques du système sur une variété, sur laquelle l'erreur d'estimation de la sortie $e = (y - \hat{y})$ converge vers zéro au bout d'un temps fini, et la dynamique du système se réduit de n à $n - p$.

Le principe d'un observateur à modes glissant est illustré dans la Figure (II.4)

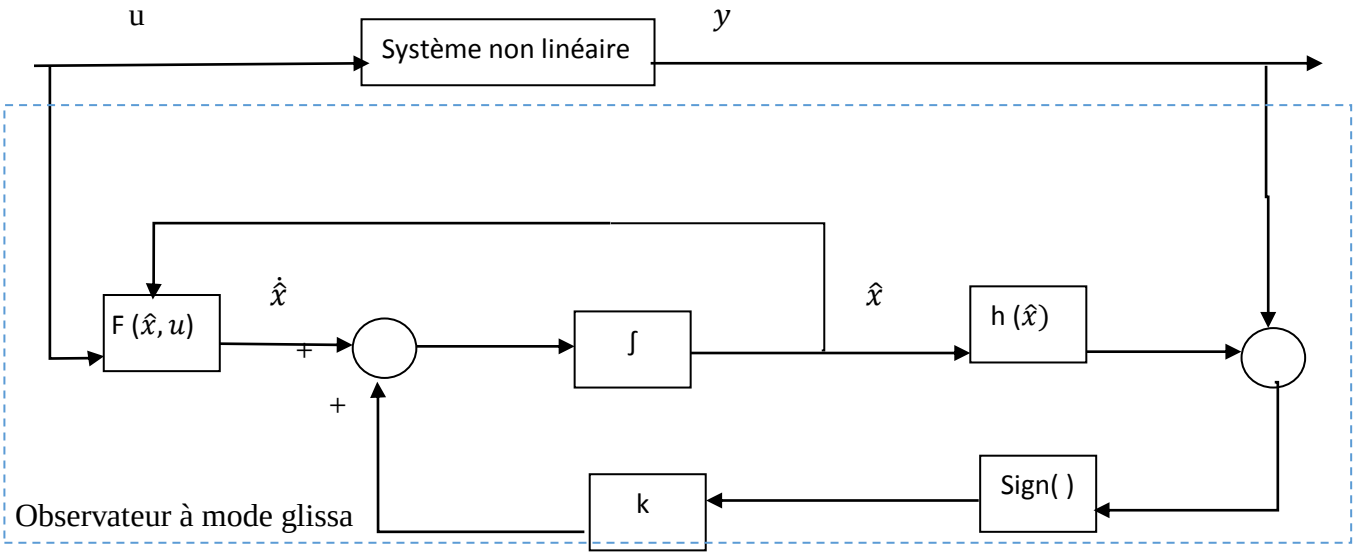


Figure II.5 : Schéma fonctionnel d'un observateur à mode glissant.

II.6.3 Observateur étape par étape

L'observateur étape par étape a été développé pour des systèmes pouvant se mettre sous la forme, appelée forme triangulaire d'observation suivante [37]:

$$\begin{cases} \dot{x_1} = x_2 + g_1(x_1, u) \\ \dot{x_2} = x_3 + g_2(x_1, x_2, u) \\ . \\ . \\ . \\ \dot{x}_{n-1} = x_n + g_{n-1}(x_1, x_2, \dots, x_{n-1}, u) \\ \dot{x_n} = f_n(x_1, x_2, \dots, x_n) + g_n(x_1, x_2, \dots, x_n, u) \\ y = x_1 \end{cases} \quad \text{(II.24)}$$

Où f_n et g_i , pour $i = 1, \dots, n$, sont des fonctions scalaires, $x_i(1, \dots, n)$ sont les états du système, u est le vecteur d'entrée et y est la sortie. La structure de l'observateur proposé est :

$$\begin{cases} \dot{\hat{x}_1} = \hat{x}_2 + g_1(x_1, u) + \lambda_1 sign_1(\bar{x}_1 - \hat{x}_1) \\ \dot{\hat{x}_2} = \hat{x}_3 + g_1(x_1, \bar{x}_2, u) + \lambda_2 sign_2(\bar{x}_2 - \hat{x}_2) \\ . \\ . \\ . \\ \dot{\hat{x}}_{n-1} = \hat{x}_n + g_{n-1}(x_1, \bar{x}_2, \dots, \bar{x}_{n-1}, u) + \lambda_{n-1} sign_{n-1}(\bar{x}_{n-1} - \hat{x}_{n-1}) \\ \dot{\hat{x}}_n = f_n(x_1, \bar{x}_2, \dots, \bar{x}_n) + g_2(x_1, \bar{x}_2, \dots, \bar{x}_n, u) + \lambda_n sign_n(\bar{x}_n - \hat{x}_n) \\ y = x_1 \end{cases} \quad \text{(II.25)}$$

Où les variables $\bar{x}_i$ sont données par :

$$\begin{cases} \bar{x}_1 = x_1 \\ \bar{x}_i = \hat{x}_i + \lambda_{i-1} sign_{eq,i-1}(\bar{x}_{i-1} - \hat{x}_{i-1}) \; pour \; i > 1 \end{cases} \quad \text{(II.26)}$$

Avec $sign_{eq}$ désigne la fonction sign(.) classique filtrée par un filtre passe bas; la fonction $sign_i$ est définie de manière à imposer que le terme correctif ne soit actif que si $\bar{x}_j - \hat{x}_j = 0$ Pour $j = 1, \dots, i$ c'est-à-dire, s'il existe $j \epsilon \{1, \dots, i-1\}$ tel que $\bar{x}_j - \hat{x}_j \neq 0$ alors la fonction $sign_i$ est mise à zéro sinon elle est égale à la fonction $sign(.)$ usuelle. La convergence des erreurs d'observation en temps fini n'est assurée que si le système est à entrées bornées et à états limités pour une durée finie afin de gérer les erreurs.

Si cette condition est vérifiée alors les λ_i peuvent être choisis tel que l'état de l'observateur $\hat{x}$ converge en un temps fini vers l'état x réel du système ; Cependant cette convergence se fait par étapes.

II.6.4 Observateur impulsif

Dans un schéma de synchronisation usuel, un des états du système maître est transmis afin de réaliser la synchronisation avec le système esclave. Dans le but de réduire la redondance du signal transmis ; le signal de transmission est divisé en petits intervalles (impulsions). La synchronisation impulsive est analogue à la synchronisation échantillonnée. Dans cette approche, en raison de l'introduction d'un opérateur de Dirac [38], le problème de synchronisation entre l'émetteur et le récepteur devient celui de stabiliser le système impulsionnel.

Cette méthode sera mieux développée et discutée par la suite pour être appliquée à la réalisation d'un système de transmission sécurisée.

II.7 Synchronisation impulsive de systèmes chaotiques discrets

La synchronisation impulsive illustrée sur la figure (II.5) a été proposée, afin de réduire la redondance du signal transmis. Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système subissent des changements soudains.

L'équation générale de la synchronisation impulsive de système chaotique discret est présentée comme suit :

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(t) + \phi\big(\hat{x}(t)\big); k \neq \mathrm{k}_i \\ \hat{x}(k_i^+) = \hat{x}(k_i) - B(k_i)e(k_i)\,; k \neq \mathrm{k}_i\,, i = 1,2,\dots n \end{cases} \tag{II.27}$$

Où :

A : Matrice d'état.

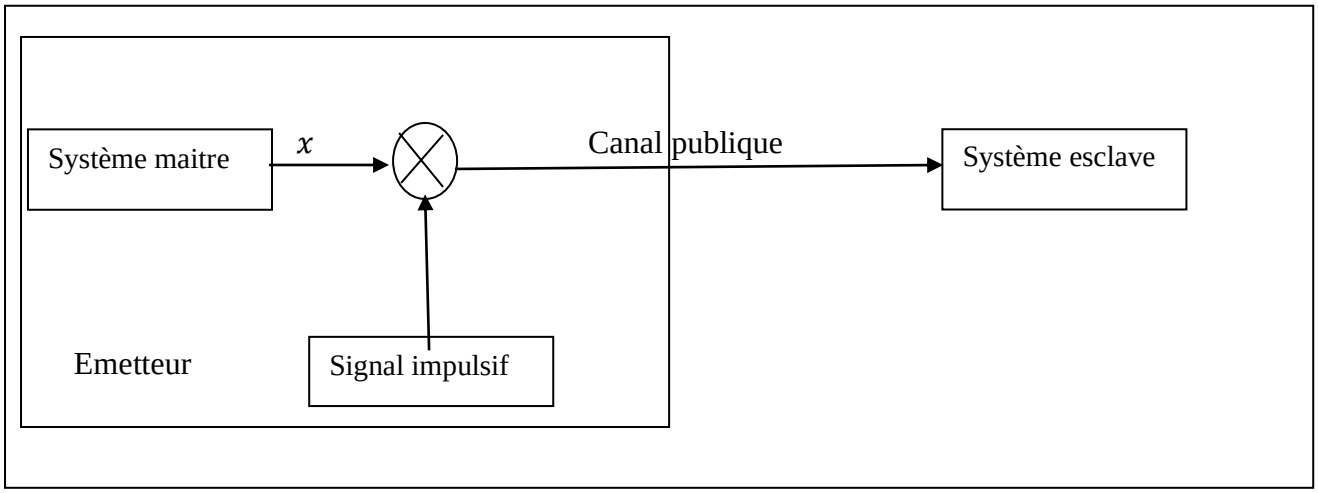
$\hat{x}$: État estimé.

ϕ : Fonction linéaire Lipschitzienne.

$B(k_i)$: Séquence de matrice symétrique de dimension m× m.

Les éléments $B(k_i)$ représentent les sauts des variables d'étatx_1,x_2 ,… ,x_n à l'arrivée de l'impulsion (k_i). Ils peuvent être considérés comme des gains de corrections apportées au système à l'instant(k_i) [39].

e(k) : l'erreur de synchronisation, définie par : e(k) =$x(k) - \hat{x}$(k)



FigureII.5 : Principe de la synchronisation impulsive

Cette technique assure la synchronisation de systèmes chaotiques en utilisant de simples échantillons des états du système maitre, elle est appliquée dans plusieurs systèmes de communication basés sur le chaos.

II.7.1 Exemple illustratif : Dans notre cas nous avons utilisé l'exemple de la synchronisation impulsive de deux systèmes de Lozi

Soit le modèle du système chaotique de Lozi chaotique donné par les équations suivantes :

$$\begin{cases} x_1(k+1) = 1 - a|x_1(k)| + bx_2(k) \\ x_2(k+1) = x_1(k) \end{cases} \quad \text{(II.28)}$$

Où (x_1, x_2) est vecteur d'état et a, b sont les paramètres du système.

Le système de Lozi montre un comportement chaotique par les valeurs des paramètres a=1.7, b=0.5.

- Observateur impulsif

Le modèle d'observateur impulsif pour le système de Lozi (II.28) est représenté par :

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(t) + \phi\big(\hat{x}(t)\big); k \neq \mathrm{k}_i \\ \hat{x}(k_i^+) = \hat{x}(k_i) - B(k_i)e(k_i)\,; k \neq \mathrm{k}_i\,, i = 1,2,\dots n \end{cases} \quad \text{(II.29)}$$

A partir des systèmes **(II.29)** et **((II 30)** on obtient le système d'erreur d'observation suivant

$$e(k) = x_1(k) - \hat{x}_2(k) \qquad \text{(II.30)}$$

II.7.2 Résultats de simulation pour le système de Lozi

Nous allons présenter les résultats de simulation obtenus par simulation sous Matlab/Simulink du système de Lozi et d'observateur impulsif.

Pour obtenir le régime chaotique les paramètres du système sont fixés comme suit :a=1.7, b=0.5 les conditions initiales $(x_1(0), x_2(0) = (0.2\,, 0.1)$ au niveau de l'émetteur et, $\hat{x}_1\ (0)$, $\hat{x}_2(0))$= (0.01 , 0.02) au niveau du récepteur.

❖ **Reconstruction des états de système**

La **figure (II.6)** illustre l'évolution des états des deux systèmes chaotiques (maître et esclave). on peut constater que durant le régime transitoire , les deux états du chaotiques ($x_1 et\ x_1$) et son estime ($\hat{x}_1 et\ \hat{x}_2$) ne sont pas encore synchronisés , mais après un certain nombre d'itérations k , la synchronisation se fait parfaitement dans le régime permanent.

Remarque : xo(k)=$\hat{x}$(k)

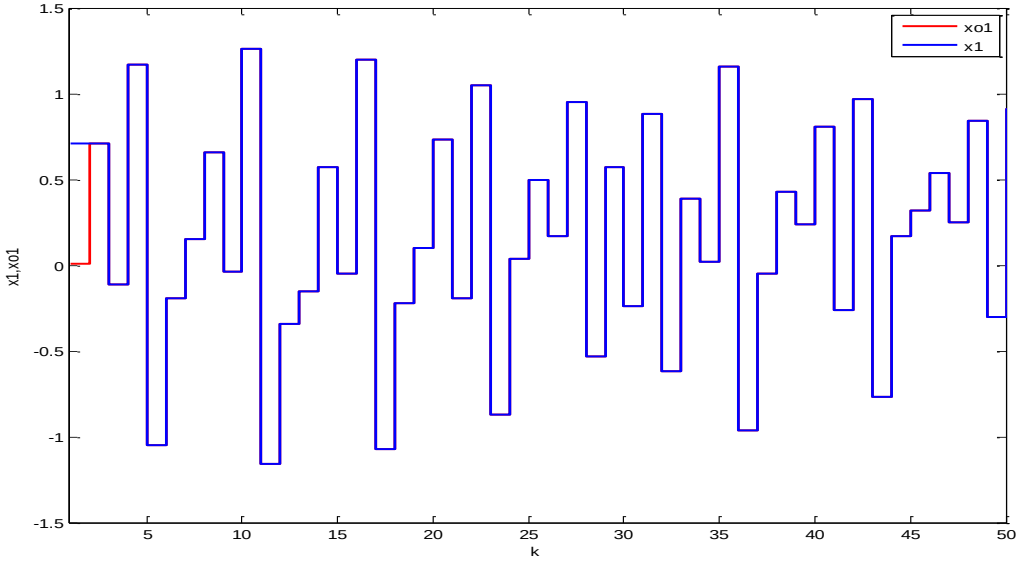


Figure II.6 : Évolution des états$(x_1(k), \hat{x}_1(k))$

La figure (II.7) illustre l'évolution des états des deux systèmes chaotiques. on peut constater que durant le régime transitoire, les deux état du chaotique (x_2) et son estime $(\hat{x}_2)$ ne sont pas

encore synchronisés, mais après certain nombres d'itérations k, la synchronisation se fait parfaitement dans le régime permanent.

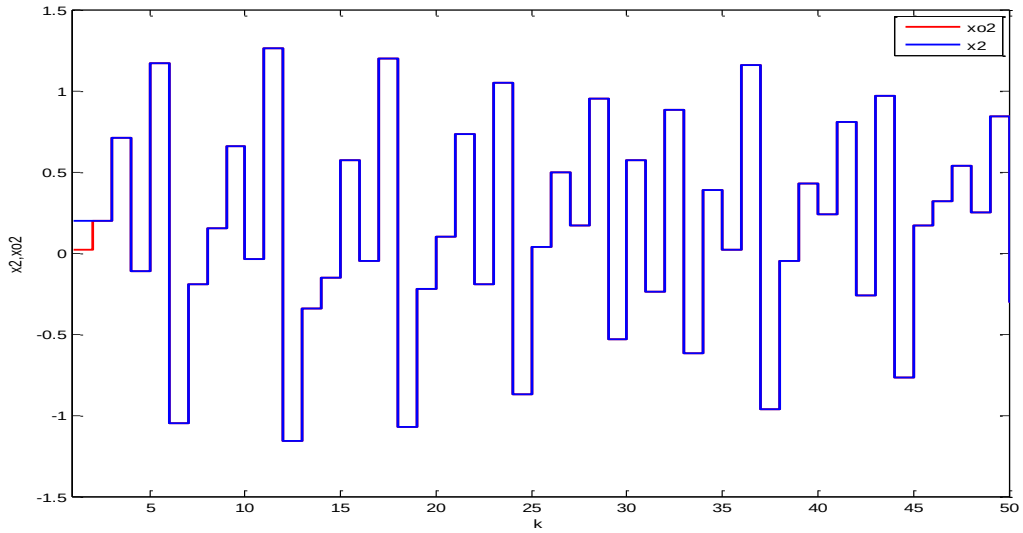


Figure II.7: Évolution des états$(x_2(k), \hat{x}_2(k))$

II.7.3 Résultats de synchronisation pour le système de Lozi

Les figures (II.6 et II.7) représentent l'évolution des erreurs de synchronisation des états et leurs estimées, en mettent en évidence l'écart entre $(x_1(k), \hat{x}_1(k))$ et $(x_2(k), \hat{x}_2(k))$, qui tend vers zéro après k itération .

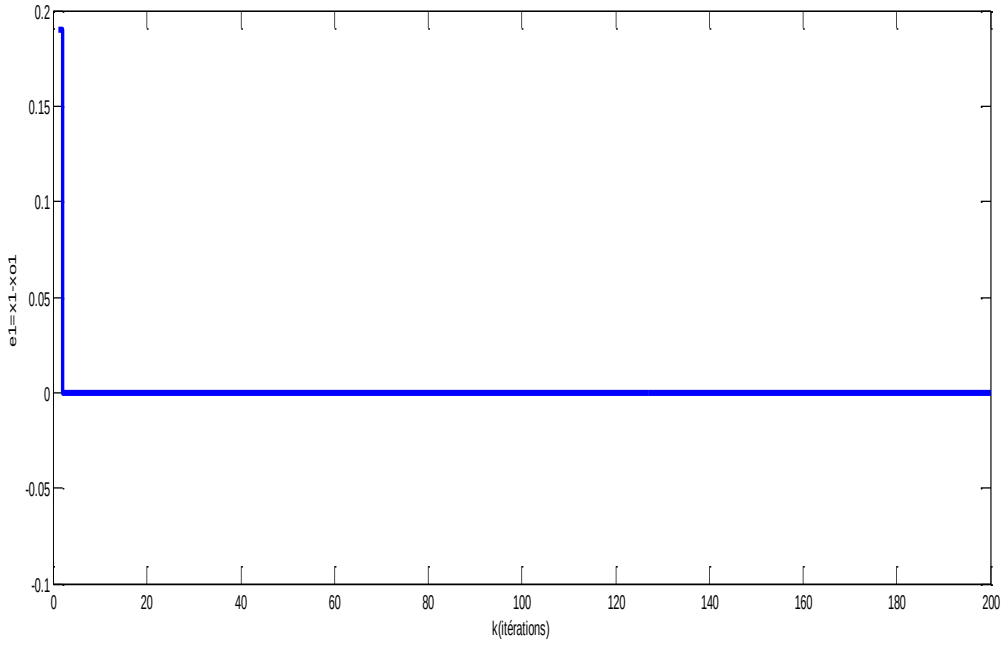


Figure II.8: Erreur d'estimation $e_1 = x_1 - \hat{x}_1$

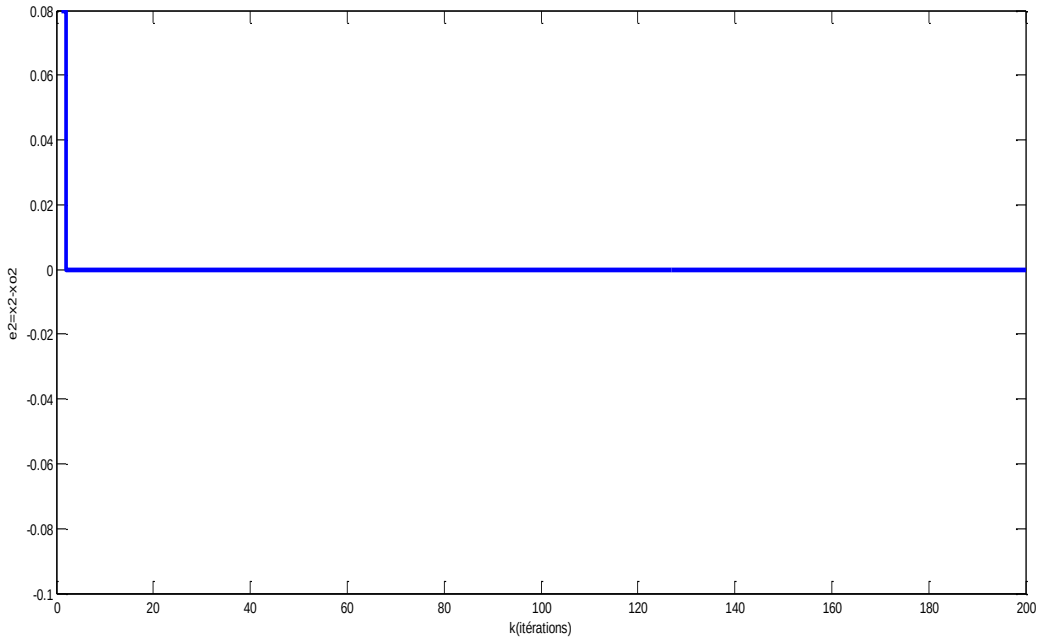


Figure II.9 : Erreur d'estimation $e_2 = x_2 - \hat{x}_2$

II.8 Conclusion :

La synchronisation des systèmes chaotiques nous donne la possibilité de la réalisation de différents schémas permettant d'effectuer une transmission sécurisée d'informations à base de systèmes chaotiques.

Dans ce chapitre, nous avons expliqué le concept de synchronisation des systèmes chaotiques ainsi que les différents modes pour atteindre de synchronisation ; Ajouté à cela nous avons cité les différents types et les techniques de synchronisation.

Dans le chapitre qui suit, la synchronisation impulsive et appliquée pour la transmission sécurisée sans fil de coordonnées GPS.

La structure du schéma de transmission réalisé fera l'objet du prochain chapitre

Chapitre III

Application à la transmission sécurisée de coordonnées GPS

III. Introduction

Les crypto-systèmes (ou systèmes de transmission sécurisée d'information) chaotiques exploitent les propriétés fondamentales des systèmes chaotiques et leur capacité de synchronisation. L'aspect aléatoire des signaux chaotiques est mis à profit pour noyer l'information à transmettre. Par un processus de synchronisation avec la dynamique de l'émetteur, le récepteur est capable d'estimer l'état de l'émetteur [40].

L'étape de synchronisation est fondamentale dans la transmission chaotique: elle permet au récepteur d'estimer les signaux utiles pour la restauration du message.

Ce chapitre est organisé comme suit : La première partie est consacrée à la présentation de la cryptographie chaotique et les méthodes de cryptage utilisées pour cacher et envoyer en toute sécurité l'information au donnée secrète. Dans la deuxième partie, on donne la structure du schéma de transmission (émetteur et récepteur). La dernière partie du chapitre sera consacrée à présenter les résultats de simulation pour illustrer la performance de la méthode proposée.

III.1 Généralités sur la cryptographie

La cryptologie est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

Le principe de la cryptographie consiste à protéger le message en le transformant d'une manière à le rendre incompréhensible. Ce processus est appelé ‘‘chiffrement’’ ou ‘‘cryptage’’. Par ailleurs, le destinataire doit engager un processus appelé ‘‘déchiffrement’’ ou ‘‘décryptage’’ afin de reconstruire le message chiffré. Pour cela, des algorithmes sont utilisés, qui sont en effet des fonctions mathématiques destinées au chiffrement et au déchiffrement du message. Pour transmettre le message d'une manière sûre, un élément ‘‘clé’’ de cryptage est introduit. Cette clé est utilisée par l'expéditeur et le destinataire. On distingue deux types de clés : clé ‘‘secrète’’ et clé ‘‘publique’’.

La cryptanalyse est un domaine de la cryptographie qui détermine les éventuelles faiblesses des systèmes cryptographiques, et cela en tentant de déchiffrer des messages cryptés sans avoir la clé de déchiffrement[41].

III.2 Cryptographie chaotique et techniques utilisées

La cryptographie utilisant la théorie du chaos, a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrement. Le chiffrement d'un message par un signal chaotique s'effectue donc en superposant à l'information initiale un signal. On envoie par la suite le message noyé dans la porteuse chaotique à un récepteur qui lui connaît les caractéristiques du générateur du chaos. Il ne reste alors plus au destinataire que de récupérer le message du signal transmis pour retrouver l'information [42].

Il existe plusieurs méthodes de cryptage à base de la synchronisation chaotique. Parmi ces dernières on peut citer :

III.2.1 Cryptage par addition

Cette technique est considérée comme la première approche utilisée en se basant sur la théorie du chaos pour sécuriser la communication [43]. L'émetteur est un système chaotique autonome dont le message m(t) est ajouté au signal chaotique de sortie y(t). La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public.

Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction.

Le schéma représentatif de cette méthode est donné par la figure suivante :

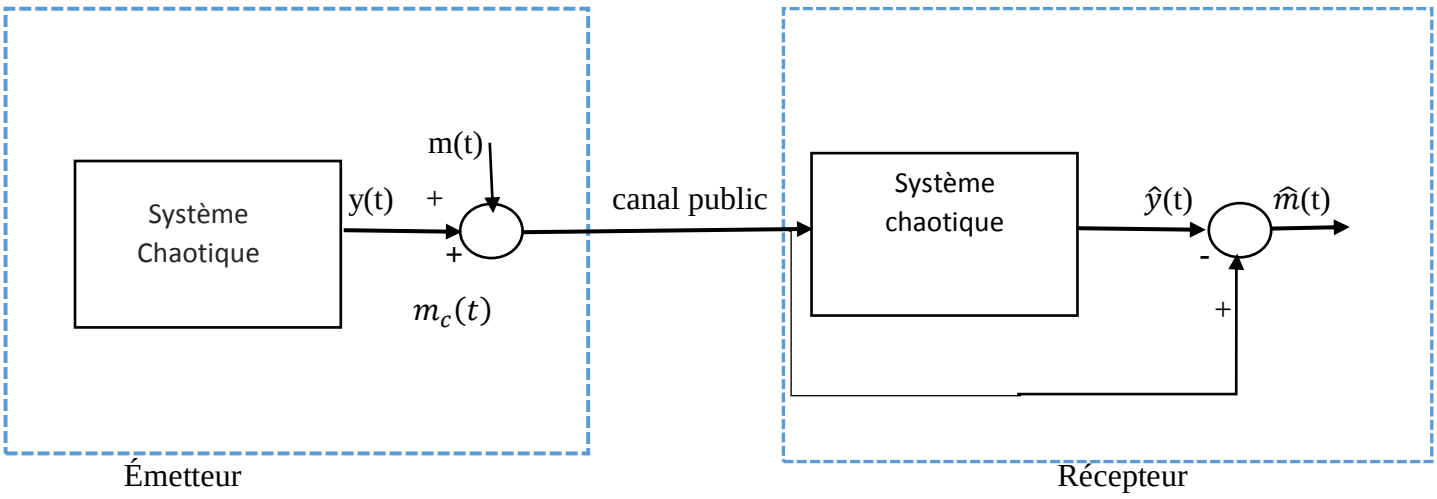


Figure III.1 : Méthode de cryptage par addition

Le cryptage par addition peut être appliqué pour la transmission de messages continus ou discrets. Afin de garantir le secret et pour un cryptage efficace, il faut que l'amplitude du signal utile m soit inférieure à celle du signal chaotique [44].

III.2.2 Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du côté de l'émetteur. Dans ce cas, la restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion à gauche du système émetteur [41].

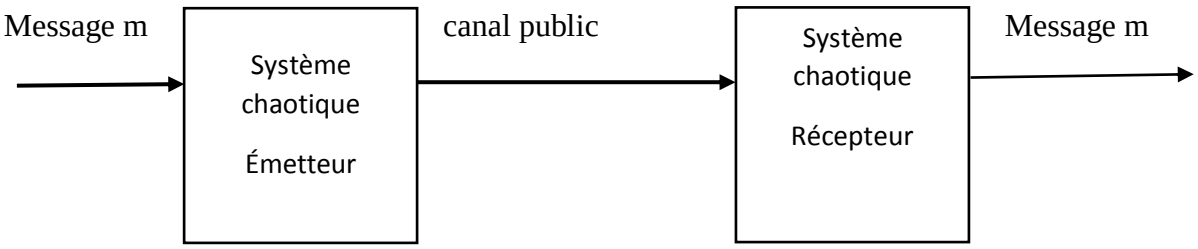


Figure III.2 : Cryptage par inclusion

Cette méthode présente beaucoup d'avantages, telles que la confidentialité des données, et un haut degré protection, mais surtout elle ne nécessite pas plus d'un canal de transmission.

III.2.3 Cryptage par commutation

Le cryptage par commutation chaotique est une méthode de cryptage qui utilise la commutation de différents systèmes chaotiques pour améliorer la sécurité de la transmission de données. L'idée principale est de combiner les avantages de plusieurs systèmes chaotiques différents pour obtenir une meilleure performance de cryptage [45].

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la figure (III.3) ou un processus de commutation est employé selon la valeur du message binaire :

Si la valeur est 0, alors le système chaotique 1 est activé et le signal de sa sortie est transmis. Sinon, c'est la sortie du système chaotique 2 qui est envoyée. Ainsi, le message binaire commute entre l'émetteur et deux attracteurs étranges correspondant aux deux systèmes chaotiques.

Du côté récepteur, il y a deux sous-systèmes chaotiques, 3 et 4, correspondant respectivement aux systèmes chaotiques 1 et 2 de l'émetteur. Supposons que le canal de communication soit parfait et que le signal transmis soit 0 : dans ce cas, le sous-système 3 se synchronisera avec le système chaotique 1, tandis que le sous-système 4 ne pourra pas se synchroniser. En fonction des erreurs de synchronisation entre les paires (1,3) et (2,4), la synchronisation du signal pourrait échouer [46].

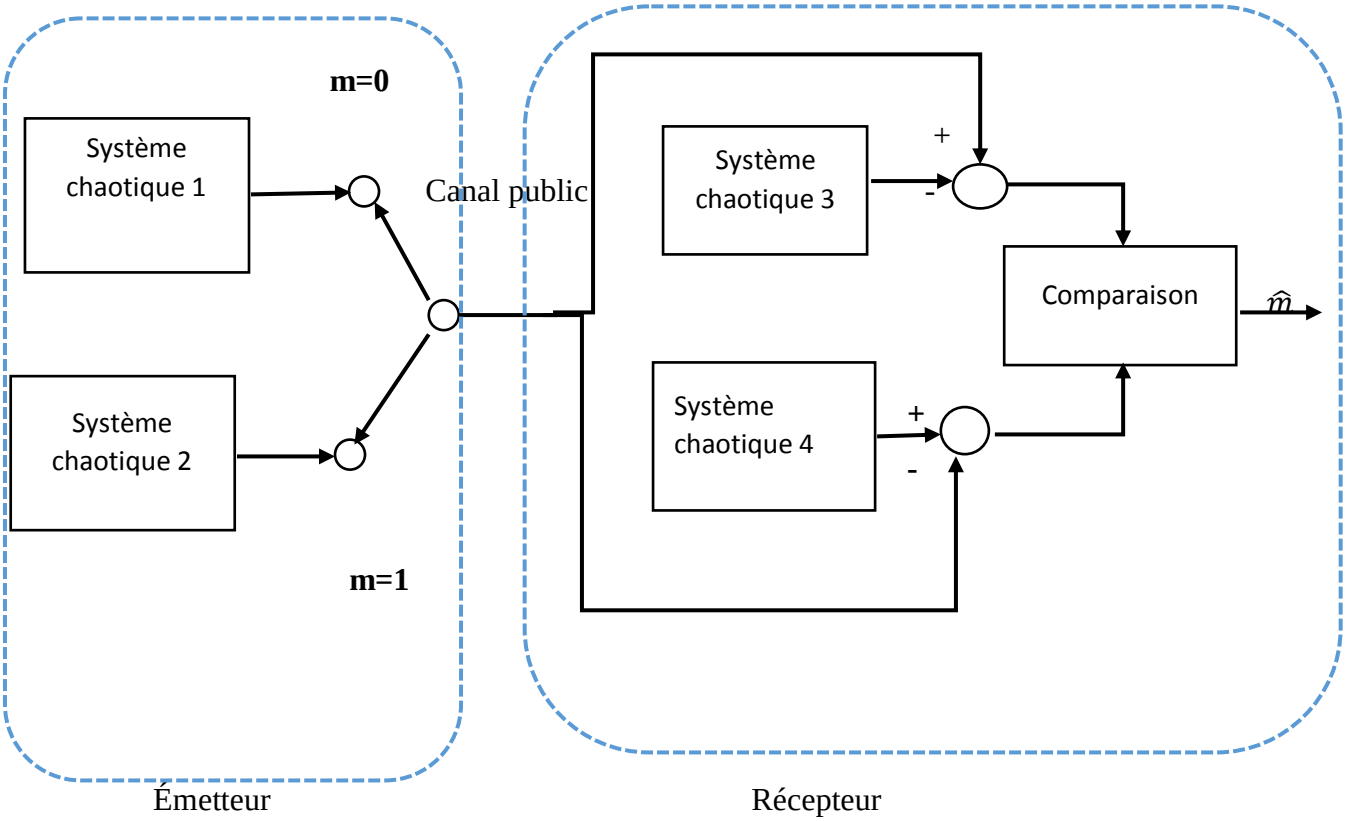


Figure III.3 : Cryptage par commutation

III.2.4 Transmission à deux voies

Dans le schéma présenté dans la Figure (III.4), l'émetteur envoie deux signaux au récepteur. Le premier signal ($y1$) est une fonction réelle de l'état (x) du système émetteur chaotique, dont l'unique objectif est de permettre la synchronisation du récepteur. Le second signal ($y2$), éventuellement envoyé via un autre canal, est un signal chaotique qui contient l'information à transmettre.

Parmi les avantages de cette méthode, on peut noter que le signal ($y1$) ne contient aucune information utile, ce qui permet à la synchronisation de s'établir de manière optimale. En

revanche, le second signal ($y2$) transporte l'information, qui peut être cryptée via une fonction non linéaire de l'état (x) [46].

Il est également important de souligner que les étapes de synchronisation et de cryptage sont totalement indépendantes l'une de l'autre. Ainsi, le décryptage de l'information ne doit pas nécessairement être réalisé au même moment que la synchronisation au niveau du récepteur.

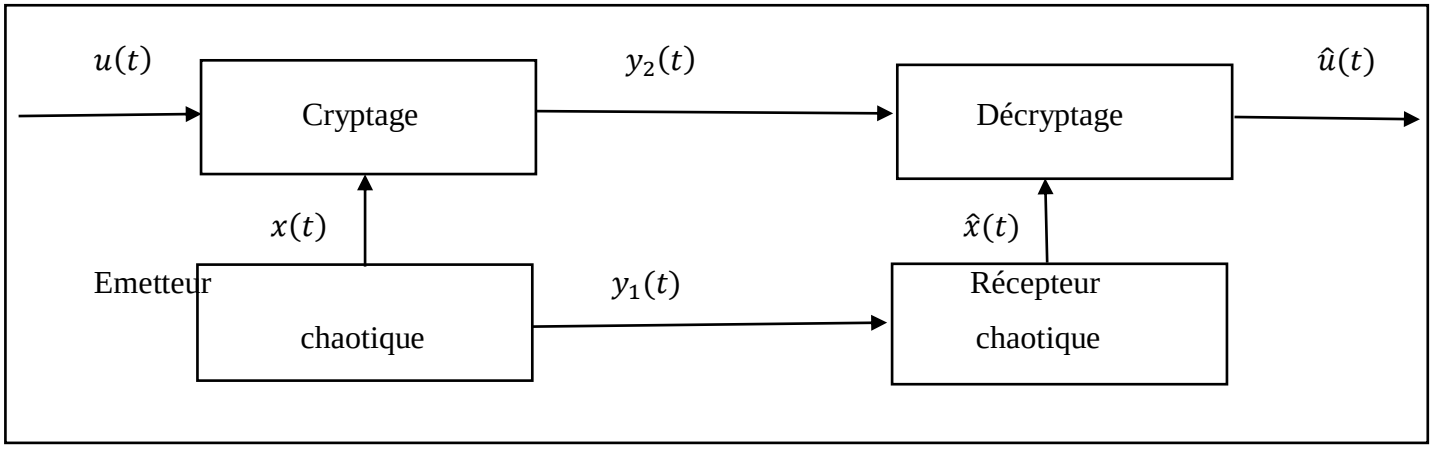


Figure III.4 : Méthode de transmission à deux voies

III.3 Structure de schéma de transmission sans fil des coordonnées GPS

Dans cette partie nous allons décrire la structure de notre schéma de transmission élaboré à base de la synchronisation impulsive, comme illustré sur la figure (III.5). Le système est constitué de deux blocs (émetteur et récepteur) que nous allons détailler dans ce qui suit.

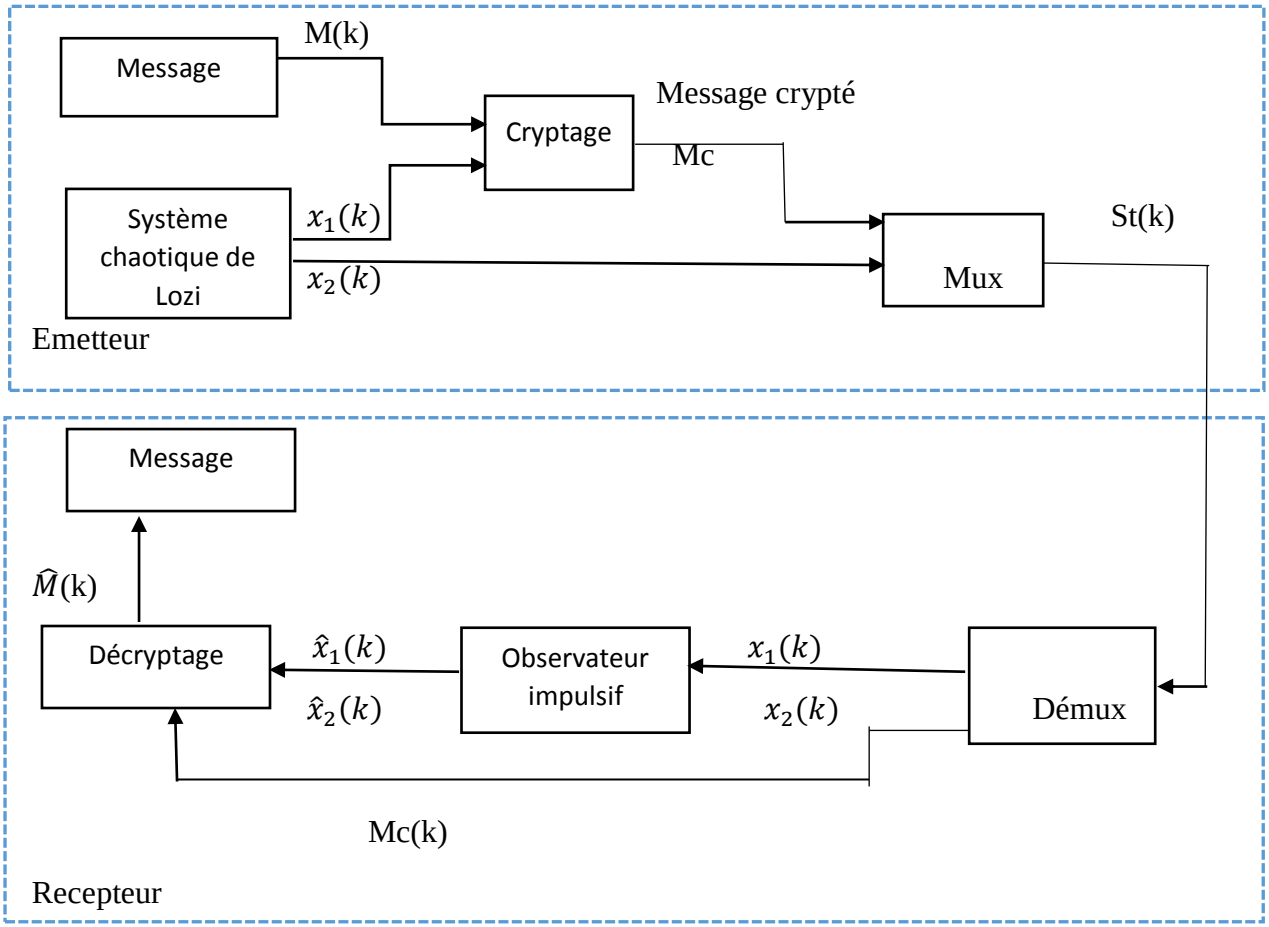


Figure III.5 : Diagramme bloc de la transmission de coordonnées GPS utilisant la synchronisation impulsive

III.3.1 Structure de l'émetteur

Dans cette partie nous présenteront le bloc émetteur ainsi que les éléments le constituant : L'émetteur contient un générateur chaotique qui est le système de Lozi (introduit dans le premier chapitre), Il est caractérisé par les paramètres a=1.7, b=0.5 et les équations (III.1), c'est un système discret qui est connu par sa simplicité à le mettre en œuvre et à l'implémenter.

$$\begin{cases} x_1(k+1) = 1 - a|x_1(k)| + bx_2(k) \\ x_2(k+1) = x_1(k) \end{cases} \quad \text{(III.1)}$$

Où :

x_1 et x_2 sont les états du système .

Pour le message c'est un message M qui contient des données GPS sous forme d'un vecteur, afin de le crypter avec les états du système chaotique de Lozi ; La fonction de cryptage

utilisée est une équation mathématique, elle prend en entrée les états x_1 et x_2 et le message M .L'algorithme de cryptage est défini par l'équation suivante :

$$\text{Mc(k)} = k_1 \times x_1\,(\text{k} + 1) + k_2 \times x_2\,(\text{k} + 1) + k_3 \times \text{m(k)} \qquad \text{(III.2)}$$

Où :

$(k_1, k_2\, et\, k_3)$: sont des clés secrètes supplémentaires

Nous avons choisi d'utiliser un multiplexeur à deux entrées, le multiplexeur a toujours une seule sortie afin d'utiliser qu'un seul canal de transmission.

Lorsque l'entrée de sélection égale à 0 c'est l'état $x_1(k)$ qui est envoyé, si elle est égale à 1 l'état $x_2(k)$ sera envoyé, sinon c'est le message Mc(k) qui est envoyé. Le signal transmis St(k) est ensuite envoyé vers le bloc récepteur défini comme suit :

$$\begin{cases} st(k) = x_1(k+1) & si\ mod\ (k,d) = 0 \\ st(k) = x_2(k+1) & si\ mod\ (k,d) = 1 \\ st(k) = M_c(k) & si\ 2 \le mod\ (k,d) \le d = 0 \end{cases} \qquad \text{(III. 3)}$$

x_1	x_2	Mc	Mc	x_1	x_2	Mc	Mc

Figure III.6: canal de transmission des signaux

La figure suivante illustre le chronogramme d'envoi des signaux x_1 et x_2 et Mc pour la période d=4 telle que d est la période d'envoi des échantillons des états $x_1$et $x_2$pour établir la synchronisation impulsive.

III.3.2 Structure de récepteur

Dans cette partie nous allons développer le bloc de récepteur en présentant les éléments qui le constitue :

Démultiplexeur(DéMUX) : Nous avons utilisé un Démultiplexeur afin de diviser le signal st de synchronisation à l'entrée de l'observateur impulsif et le signal crypté comme entrée du bloc de décryptage.

Observateur impulsif : Dans notre cas, nous utilisons le système de Lozi, qui est discret. Ainsi, l'observateur impulsif est régi par les deux dynamiques suivantes :

A l'arrivée des impulsions :

$$\begin{cases} \hat{x}_1(k+1) = \hat{x}_1(k+1) - b_1(x_1(k) - \hat{x}_1(k+1)); k = \text{k}_i \\ \hat{x}_2(k+1) = \hat{x}_2(k+1) - b_2\big(x_2(k) - \hat{x}_2(k+1)\big) \end{cases} \qquad \text{(III.4)}$$

En dehors des impulsions :

$$\begin{cases} \hat{x}_1(k+1) = 1 - a\,|\hat{x}_1(k)| + \hat{x}_2(k); k \neq \mathrm{k}_i \\ \hat{x}_2(k+1) = b\,\hat{x}_1(k) \end{cases} \quad \text{(III.5)}$$

Où :

x_1 et x_2 sont les états du système de lozi.

$\hat{x}_1$et $\hat{x}_2$ sont les états estimés.

a et b : paramètres du système de Lozi.

B : matrice de commande.

B= $\begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}$, avec : b_1=b_2= -0.9998

Processus de déchiffrement : Une fois les états x_1 et x_2 sont entièrement estimés par l'observateur impulsif, il est possible de retrouver les coordonnées GPS original grâce à un processus de décryptage .Ce processus effectue les opérations inverses de celles du chiffrement en utilisant les états estimés .

La fonction de décryptage dans notre cas est donnée par la fonction suivante :

$$\hat{m}\,(\mathrm{k})=(\,(\mathrm{st(k)}-(k_1*\hat{x}_1\,(\mathrm{k+1}))-(k_2*\hat{x}_2\,(\mathrm{k+1}))/k_3) \quad \text{(III.6)}$$

Où : $k_{1=}$0.2 , $k_{2=}$0.3 , $k_{3=}$0.5

Canal de transmission : Dans notre travail de transmission sans fil, nous avons utilisé le Wi-Fi en suivant le modèle client-serveur. Le module GPS collecte les données de localisation et les envoie en tant que client à un serveur central via une connexion Wi-Fi. Le serveur reçoit ces coordonnées, les traite et les afficher ou les rediriger. Cette architecture permet une communication rapide et fiable entre le client (le module GPS) et le serveur.

III.4 Conclusion

La cryptographie chaotique utilise les propriétés complexes et imprévisibles des systèmes chaotiques pour sécuriser les communications. En appliquant des méthodes comme l'addition, l'inclusion et la modulation, elle permet de chiffrer des informations sensibles, comme les coordonnées GPS, de manière efficace.

Dans le schéma de transmission de coordonnées GPS proposé, l'émetteur génère un signal chaotique à partir du système de Lozi, et crypte les données GPS, puis les transmet avec les

états de synchronisation envoyée par des impulsions à travers un canal unique. Le récepteur, de son côté, récupère via un démultiplexage, les échantillons de signaux de synchronisation qui serrant utilisés par l'observateur impulsifs, ainsi que le message chiffré qui sera l'entrée d'un processus de décryptage pour récupérer les coordonnées GPS originales grâce aux états estimés par l'observateur impulsif.

L'implémentation du schéma de transmission décrit dans ce chapitre sera discutée dans le dernier chapitre de ce mémoire.

Chapitre IV

Implémentation sur carte ESP32 du schéma de transmission sans fil de coordonnées GPS

IV. 1 Introduction

Dans le chapitre précédent, nous avons donné la structure du schéma de transmission sécurisée (émetteur et récepteur), basé sur le cryptage à l'aide d'un système chaotique de lozi et la synchronisation à base d'un observateur impulsif. Nous avons également présenté les différents résultats de simulation.

Le présent chapitre constitue une étape cruciale de ce mémoire, car il met en lumière les résultats de notre réalisation pratique. Ces résultats seront exposés de manière structurée et méthodique, afin de faciliter leur compréhension et leur interprétation.

Enfin, nous procéderons à une discussion approfondie des résultats obtenus.

IV. 2Détails d'implémentation du schéma de transmission des données GPS à base d'oscillateur de lozi sur carte ESP32

Dans cette réalisation, nous avons conçu un programme sur Arduino qui se compose de deux parties. La première partie concerne l'émetteur, composé de trois cartes électroniques, à savoir l'ESP32, un module GPS NEO_M8N et un afficheur LCD de type (20x4) par le biais d'un module I2C. Cette configuration permet aussi de capturer des données telles que la latitude, la longitude, et l'heure d'enregistrement, puis de les transmettre à la deuxième partie, le récepteur.

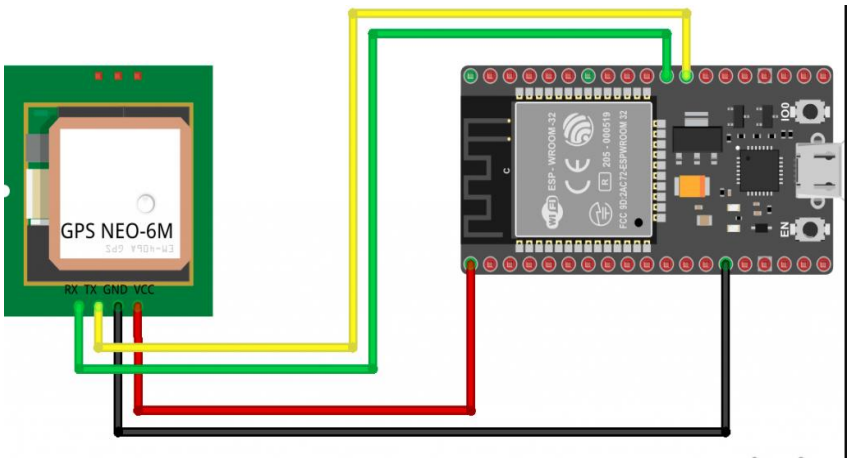


Figure IV.1 : Branchement de la carte esp32 et du module GPS NEO_M8N

Le récepteur, est composé d'une seconde carte ESP32 et au quelle nous relions un afficheur LCD de même type, pour afficher les données GPS et localiser la position de l'utilisateur.

L'interfaçage entre la carte esp32 et afficheurs LCD via le module I2C est présenté sur la Figure (IV.2).

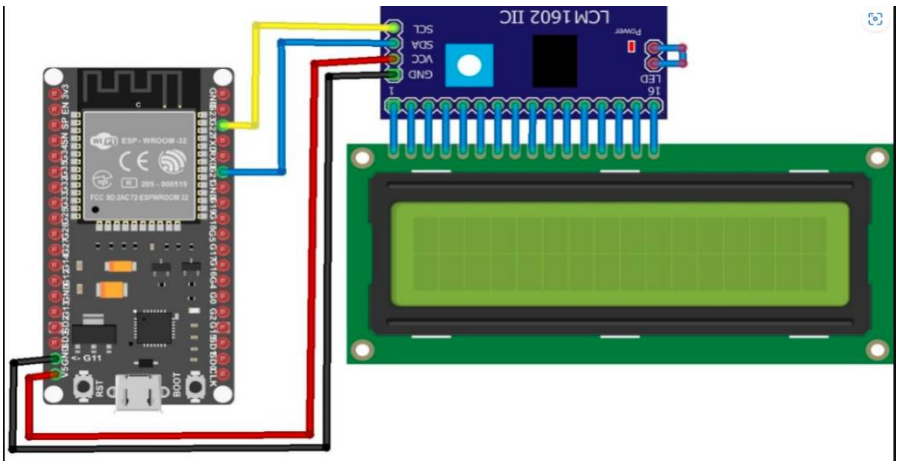


Figure IV.2 : Branchement carte ESP32-LCD via I2C

Le branchement entre l'écran LCD et le module I2C se fait en reliant leurs 20 broches entres elles, et les broches de sortie du module I2C sont reliées à la carte esp32 comme suit :

SDA __ pin20

SCL __ pin21

VCC __ 5V

GND __ GND

La connexion entre les deux cartes ESP32 se fait avec le wifi.

IV. 2. 1 Partie matérielle

Dans cette partie, nous présenterons en détails les différents éléments et composants constituant le système de transmission sans fil implémenté.

IV. 2. 1.1Description de ESP32

La carte ESP32 est un dispositif de développement électronique open-source qui repose sur un microcontrôleur conçu par Expressif Systèmes. Elle est surtout prisée pour les projets de domotique et d'Internet des Objets (IoT) grâce à ses capacités de connectivité sans fil, incluant le Wi-Fi et le Bluetooth, ainsi qu'à sa puissance de calcul élevée. Cette carte est compatible avec divers langages de programmation tels que C, C++, Python et Micro Python, et elle peut être utilisée avec plusieurs Framework de développement, notamment Arduino et l'Expressif IoT Development Framework (ESP-IDF). En résumé, l'ESP32 est un outil polyvalent et puissant, idéal pour des applications nécessitant une connectivité sans fil et une gestion

efficace des données, ce qui en fait un choix privilégié pour les développeurs dans le domaine de la technologie IoT et de la domotique.

La Figure (IV.3) illustre une carte ESP32 à 30 broches, il existe par ailleurs d'autre cartes ESP32 à 38 broches, la différence consiste dans le nombre de broches disponibles pour l'entrée et la sortie (GPIO), ainsi que dans certaines fonctionnalités supplémentaires sur les broches supplémentaires. Voici un résumé des différences :

Figure IV.3 : Carte électronique ESP32 à 30 broches

ESP32 à 30 broches :

- **Nombre de broches GPIO** : 24 broches disponibles.
- **Dimensions** : Légèrement plus compact, donc utile si l'espace est limité dans le projet.
- **Moins de fonctionnalités sur certaines broches** : Il peut manquer certaines broches spécifiques utilisées pour des fonctionnalités comme les capteurs tactiles, DAC (convertisseurs numérique-analogique), ou des broches ADC supplémentaires (convertisseurs analogique-numérique).

ESP32 à 38 broches :

- **Nombre de broches GPIO** : 30 broches disponibles.
- **Plus de fonctionnalités** : Les broches supplémentaires peuvent être utilisées pour des fonctions comme I2S (interface pour audio numérique), DAC, ADC, ou des capteurs tactiles.
- **Meilleure accessibilité des périphériques** : Les broches supplémentaires rendent plus faciles les connexions à des périphériques multiples sans multiplexage ou utilisation de broches partagées.
- **Dimensions plus grandes** : Peut être légèrement plus grand, donc il faut être prudent :(attention à la taille du boîtier si l'espace est une contrainte dans le projet).

A. Caractéristique de la carte ESP32 :

- **Microcontrôleur :** La carte ESP32 est double cœur et est dotée d'un processeur principal fonctionnant à 160 MHz et un coprocesseur à 240 MHz.
- **Connectivité :** Supporte le Wi-Fi 802.11b/g/n et le Bluetooth v4.2.
- **Mémoire :** Dispose de 32 Mo de mémoire flash et de 520 Ko de RAM.
- **Broches d'entrée/sortie :** Comprend 30 broches, dont 16 peuvent être utilisées pour le PWM et 6 pour des entrées analogiques.
- **Mémoire additionnelle :** Supporte la mémoire OTP (One-Time Programmable) pour le flash et la mémoire FRAM (Ferroelectric Random Access Memory).
- **Alimentation :** Peut être alimentée via USB ou par une source externe de 3,3 V.

Ces caractéristiques font de l'ESP32 une plateforme idéale pour des projets d'Internet des Objets (IoT) et de domotique, grâce à sa puissance de traitement et ses capacités de connectivité.

B. Brochage de la carte ESP32

L'ESP32 est équipée de 30 broches numériques qui ressemblent à celles des cartes Arduino, permettant d'ajouter facilement divers composants à vos projets, tels que des écrans LCD, des écrans OLED, des capteurs, des boutons et des buzzers.

La plupart de ces broches prennent en charge des fonctionnalités avancées, telles que l'état d'impédance élevée, ainsi que des résistances pull-up et pull-down internes. Cela les rend particulièrement adaptées pour des applications comme le contrôle des LED et la connexion de boutons ou de claviers matriciels.

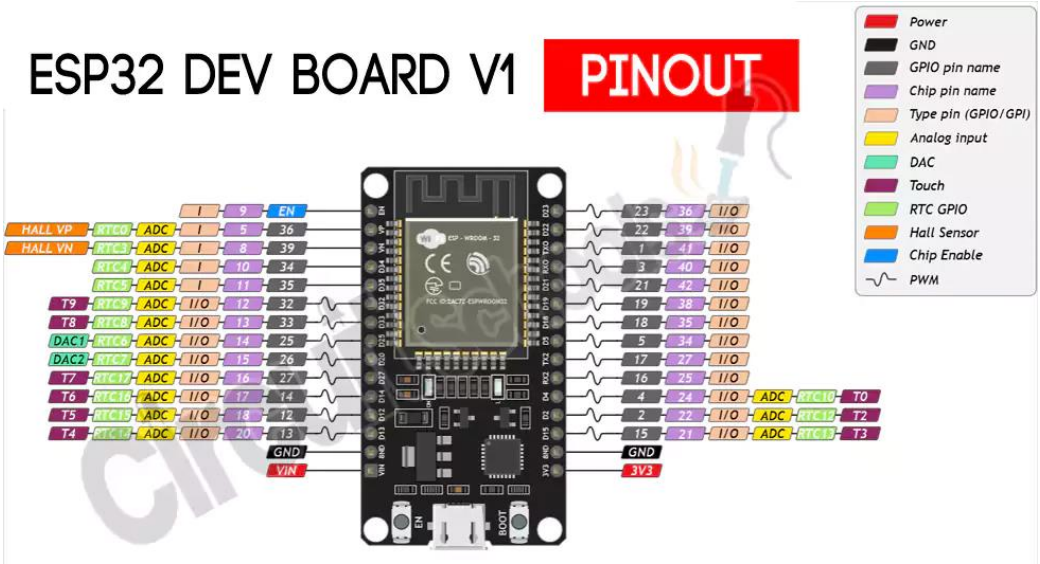


Figure IV.4 : Brochage de la carte ESP32 à 30 broches

Dans notre cas, deux cartes ESP32 à 30 broches sont utilisées, le programme de l'émetteur est chargé dans la première carte, tandis que le programme du récepteur est téléversé dans la deuxième carte.

C. Types de cartes ESP32

Il existe plusieurs modèles de cartes ESP32, chacun conçu pour répondre à des besoins spécifiques dans le développement de projets IoT. Ces différentes variantes permettent aux développeurs de sélectionner la carte mieux adaptée à leurs exigences en termes de puissance, de connectivité et de fonctionnalités spécifiques pour leurs projets.

Voici un aperçu des modèles les plus courants :

- **ESP32-SOLO-1** : Une version simplifiée de l'ESP32, dotée d'un seul cœur, idéale pour des projets nécessitant moins de puissance de traitement.
- **ESP32-WROVER** : Ce modèle est équipé d'une mémoire RAM supplémentaire, ce qui le rend adapté aux applications qui demandent plus de ressources.
- **NodeMCU-32** : Une carte de développement appréciée pour sa facilité de prototypage, grâce à l'intégration d'un convertisseur USB-série et de broches accessibles.
- **ESP32-CAM** : Conçue pour des projets de vision par ordinateur, cette carte intègre une caméra et est souvent utilisée dans des applications de surveillance et de détection.
- **ESP32-S3** : Ce modèle propose des améliorations en matière de traitement et de connectivité, particulièrement adapté aux applications nécessitant des capacités avancées.
- **ESP32-S2** : Une version axée sur la sécurité et la faible consommation d'énergie, idéale pour les dispositifs IoT à faible consommation.
- **ESP32-WROOM-32** : L'ESP32 WROOM-32 est un module microcontrôleur hautement intégré, conçu pour offrir une solution complète et abordable pour les projets IoT. Développé par Expressif Système, ce module intègre une puce ESP32, un véritable concentré de technologie qui lui confère des capacités sans précédent en termes de connectivité, de traitement et de flexibilité. Au cœur de l'ESP32 WROOM-32 trouve un double cœur Xtensa LX6, offrant une puissance de calcul suffisante pour gérer des tâches complexes. Il est accompagné d'une mémoire flash pour le stockage du code et des données, ainsi que d'une mémoire SRAM pour les opérations en cours.

Pour notre prototype, nous avons opté pour le choix de la carte ESP32-WROOM-30 pour sa disponibilité, sa capacité mémoire et le nombre suffisants de ports analogique et numérique pour l'interface avec notre projet. Cette carte présente les caractéristiques principales suivantes :
Processeur : Dual-core Xtensa® 32-bit LX6 jusqu'à 240 MHz.
Mémoire : 520 Ko de SRAM, jusqu'à 16 Mo de mémoire flash.
Interfaces: GPIO, UART, SPI, I2C, ADC, DAC, PWM.
Température de fonctionnement : -40 à 85 °C.

IV. 2.1.2 Module GPS NEO-M8N

Le module GPS Neo-8M est un dispositif compact et performant intégrant un récepteur GPS (Global Positioning System) qui permet de recevoir et de traiter les signaux des satellites pour déterminer la position géographique avec une grande précision. Le module est équipé d'un récepteur GPS sensible qui peut capter les signaux des satellites GPS, GLONASS, et BeiDou. Cela garantit une couverture mondiale et une précision accrue. Il intègre la puce Neo-8M, réputée pour sa fiabilité et ses performances. Cette puce offre des fonctions avancées de positionnement, de navigation et de synchronisation temporelle.

A. Caractéristiques

Tension d'alimentation : 7 ~ 3,6 V
Courant d'alimentation: 67mA
Température de fonctionnement : -40 ~ +85°C
Précision de la position horizontale : 5 m
Taille: 36 mm * 26 mm * 4,5 mm (L * L * H)
Compatible avec divers modules de contrôleur de vol
Cristal RTC intégré
Détection et suppression actives CW
L'antenne en céramique fournit un signal très fort

B. Applications :

- Systèmes de suivi
- Navigation
- Projets IoT
- Projets de cartographie

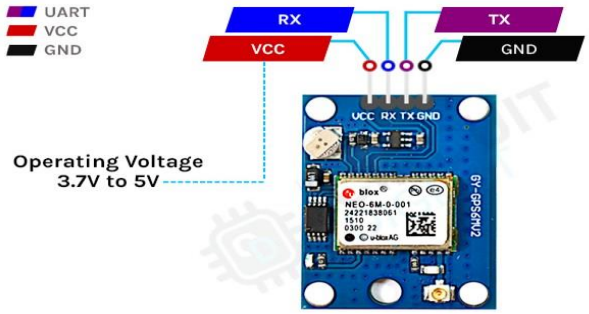


Figure IV.5: Schield GPS NEO-M8N

Dans notre cas, nous utilisons un seul schield GPS NEO-M8N dans l'émetteur qui enregistre les données de navigation à savoir l'altitude, longitude, latitude et l'heure de localisation.

IV. 2.1.3 Afficheur LCD

Un écran LCD est un dispositif d'affichage capable de présenter des images, des données alphanumériques ou graphiques, en exploitant la capacité des cristaux liquides à transmettre ou à réfléchir la lumière.

Les écrans LCD sont plats et consomment peu d'énergie, ce qui les rend populaires dans de nombreux appareils électroniques, tels que les ordinateurs, les smartphones, les téléviseurs, et bien d'autres.

Il existe plusieurs tailles et types d'écran LCD, tels que : écran LCD graphique, écran LCD à matrice de points, écran LCD à écran tactile et écran LCD (16 x 2) ou (20 x 4). Avant d'utiliser l'un de ces écrans il faut d'abord s'assurer de disposer d'une bibliothèque adaptée.

Dans notre cas, nous utilisons deux écrans LCD de type (20 x 4), un au niveau de l'émetteur pour afficher le message crypté et l'autre à la fin de récupération pour afficher les données GPS (latitude, longitude et l'heur de localisation).

A. Ecran LCD (20 x 4)

L'écran LCD 20x4 est un écran qui peut afficher 4 lignes avec 20 caractères par ligne (simultanément). La couleur des caractères est blanche et l'écran a un fond bleu. Cela le rend également lisible dans l'obscurité. Le contraste est réglable. Grâce au module I2C pré-soudé, on a besoin de moins de ports IO. On peut facilement connecter l'écran à un Arduino, Raspberry Pi,ESP32,ESP8266,etc.

Cet afficheur alphanumérique 4 x 20 caractères avec rétro-éclairage (écriture blanche sur fond bleu) est équipé d'un petit module nous permettons de le piloter facilement en I2C via un module Arduino ou Raspberry Pi (non livrés) grâce à des exemples de raccordement et des librairies disponibles en téléchargement.

B. Caractéristiques de l'écran

-Type: LCD

-Format:4lignes de 20 caractères

- Ecriture bleue sur fond noir

- Interface: I2C (module soudé au dos de l'afficheur)

- Contrôleur: HD44780 (afficheur) et PCF8574 (module)

- Alimentation: 3 à 5 Vcc

- Connecteur mâle 1 x 4 broches

- Dimensions 98 x 60 x 20 mm

- Poids: 76 g env.

La figure (IV.6) illustre un afficheur LCD de type (20 x 4).

FigureIV.6 : Afficheur LCD (20 x 4)

IV. 2.1.4 Module I2C PCF8574

Un module I2C, qui signifie Inter-Integrated Circuit, est un dispositif de communication conçu pour être intégré à un écran LCD, permettant ainsi de le contrôler via le protocole I2C. Ce module compact peut être facilement installé à l'arrière de l'écran, simplifiant ainsi la gestion de celui-ci en utilisant le bus I2C. Cela permet de réduire le nombre de connexions

nécessaires et d'améliorer l'efficacité du câblage, rendant l'intégration plus pratique dans divers projets électroniques. Il y a 4 fils pour contrôler l'écran : GND, VCC, SDA, SCL.

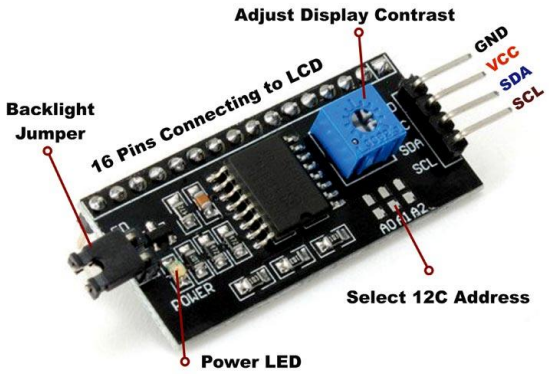


Figure IV.7: module I2C

- **VCC (ou 3V3/5V)** : Alimentation du module. Connecter cette broche à une source de 3.3V.
- **GND** : Relie le module à la masse (le 0V) de notre circuit.
- **SDA** : Ligne de données. Utilisée pour transmettre les données entre le microcontrôleur et le module I2C.
- **SCL** : Ligne d'horloge. Fournit l'horloge pour la synchronisation des transmissions de données sur le bus I2C.

Ces deux dernières (SDA et SCL) doivent être reliées aux broches correspondantes de l'ESP32 que nous avons utilisées.

En résumé, l'utilisation d'un afficheur LCD à commande I2C avec ESP32 offre une simplicité de câblage, une économie de broches, une capacité à brancher plusieurs périphériques et une facilité de programmation.

IV. 2. 2Partie logicielle

Dans cette partie nous nous focaliserons sur l'aspect logiciel en abordant l'environnement utilisé et les configurations requises et effectuées.

IV.2.2.1L'environnement de développement intégré (IDE) Arduino

Le logiciel Arduino est un environnement de développement intégré (IDE) open source et gratuit, disponible en téléchargement sur le site officiel d'Arduino. Il permet aux utilisateurs d'écrire des programmes, de les compiler dans le langage spécifique à Arduino, de les téléverser sur la carte physique, et de communiquer avec celle-ci via un terminal.

Conçu pour être accessible, même pour les novices en programmation électronique, Arduino utilise une version simplifiée du langage C++. Grâce à cet IDE, il est possible de réaliser une multitude de projets, allant des objets du quotidien à des applications plus complexes comme la robotique, les drones ou les systèmes de sécurité.

Le logiciel est compatible avec les systèmes d'exploitation Windows, Mac et Linux, et propose une interface claire et intuitive, facilitant ainsi la programmation des microcontrôleurs Arduino. En somme, Arduino offre une plateforme idéale pour les amateurs et les professionnels souhaitant développer des projets électroniques variés.

La figure(IV.8) suivante illustre l'interface de l'environnement de développement Arduino utilisé dans notre cas pour éditer les programmes de l'émetteur et du récepteur et les télévirser vers les cartes ESP32.

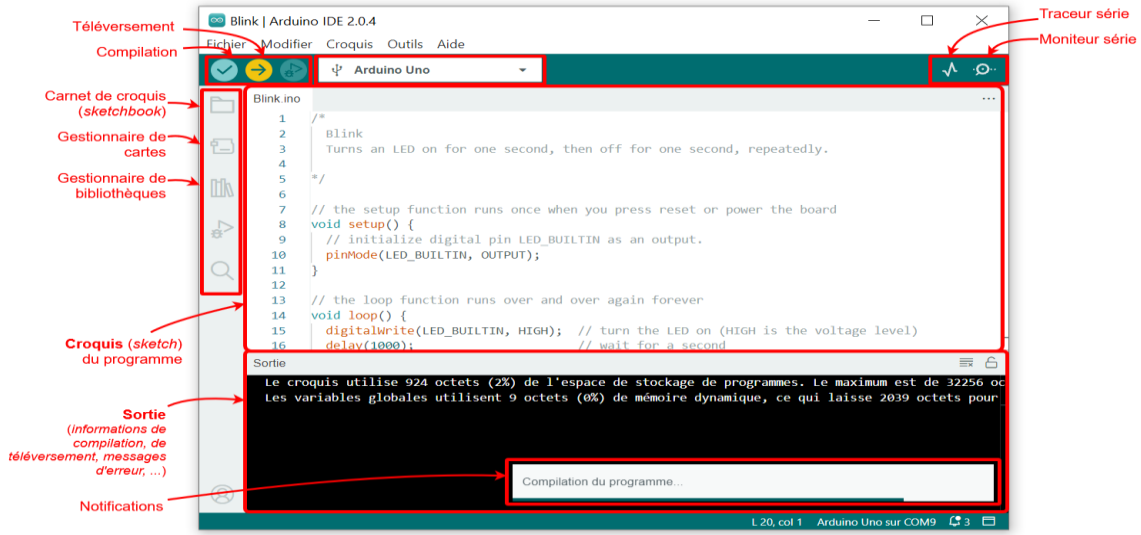


Figure IV.8: Interface de IDE Arduino

IV.2.2.2Configuration des cartes Arduino utilisées

Avant d'effectuer le téléversement des programmes vers les cartes ESP32, il est nécessaire de configurer ces dernières.

Pour programmer la carte ESP32, nous devons installer le package de la carte ESP32 dans l'IDE Arduino. Pour cela, nous cliquons sur Gestionnaire de cartes, nous tapons ESP32 dans la barre de recherche, puis nous cliquons sur le bouton Installer pour démarrer le processus d'installation. Cela téléchargera et installera le package nécessaire pour la carte ESP32.

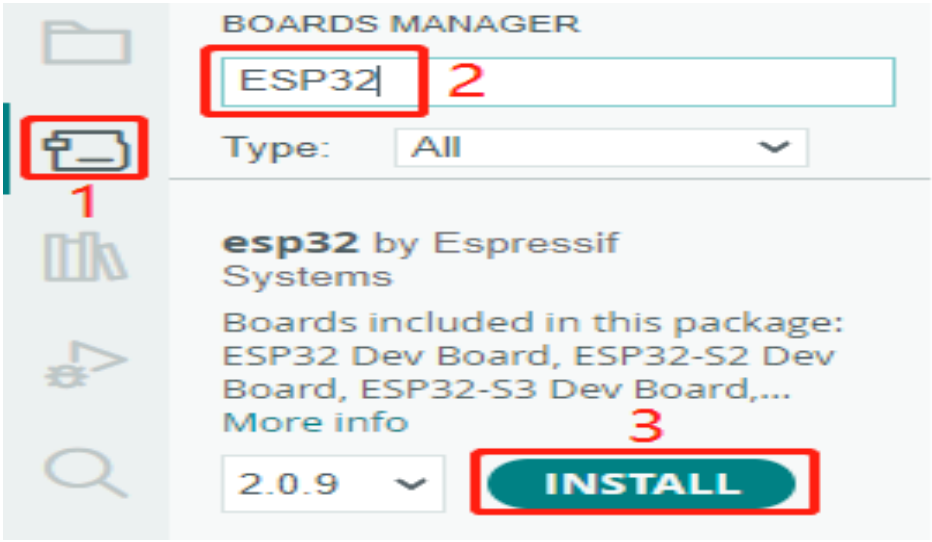


Figure IV.9: Installation du package de la carte ESP32

Ensuite, nous sélectionnons la carte ESP32 Dev Module souhaitée, comme illustré sur la figure (IV.10)**.**

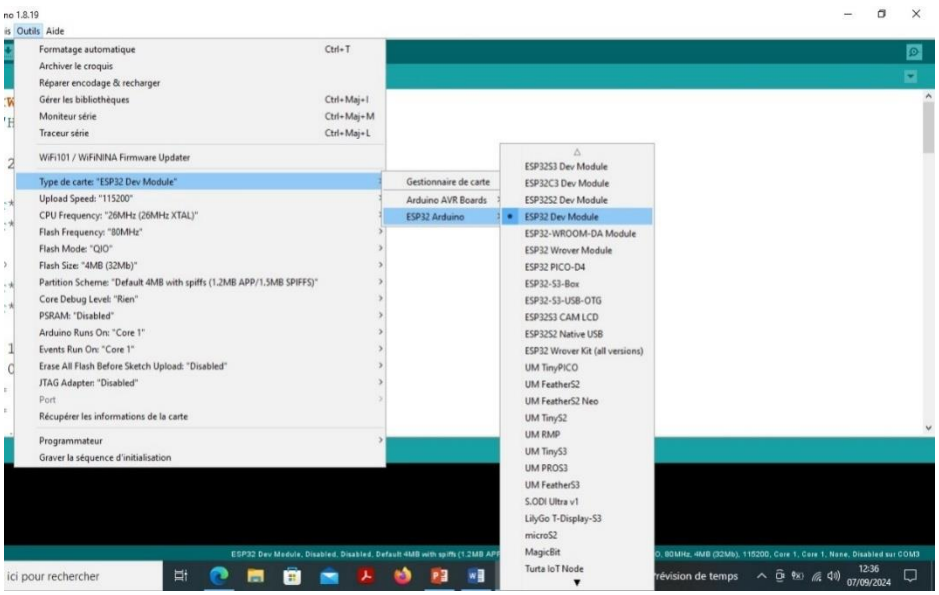
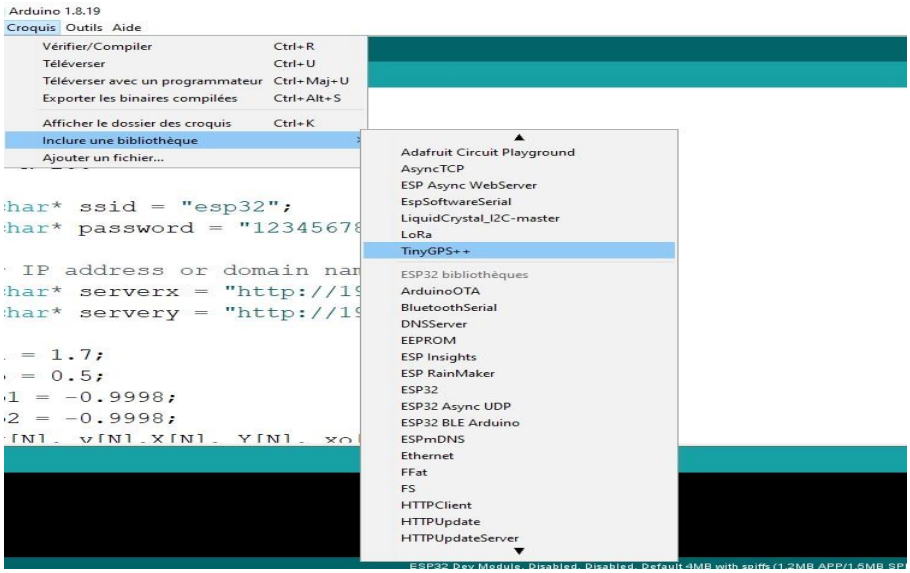


Figure IV.10: Sélection de la carte ESP32

En deuxième lieu il faut télécharger les bibliothèques nécessaires pour chaque composant comme : La bibliothèque " ESPAsyncWebServer " pour la carte ESP32, la bibliothèque " TinyGPS++ " pour le module " Schield GPS NEO-M8N", la bibliothèque "

LiquidCrystal_I2C"pour l'afficheur LCD avec module I2C et le "wifi" pour téléverser les programme dans l'émetteur vers le récepteur.

Les Figures (IV.11), (IV.12), (IV.13) illustrèrent respectivement l'ajout des bibliothèques TinyGPS++ ,WiFi et LiquidCrystal_I2C on fais téléchargées et installées.



FigureIV.11 : Sélection du bibliothèque TinyGPS++

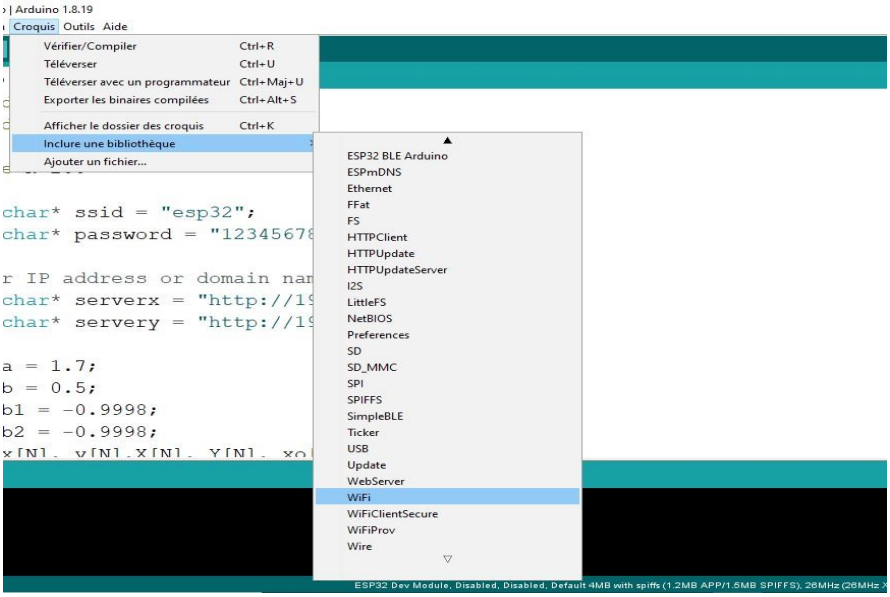
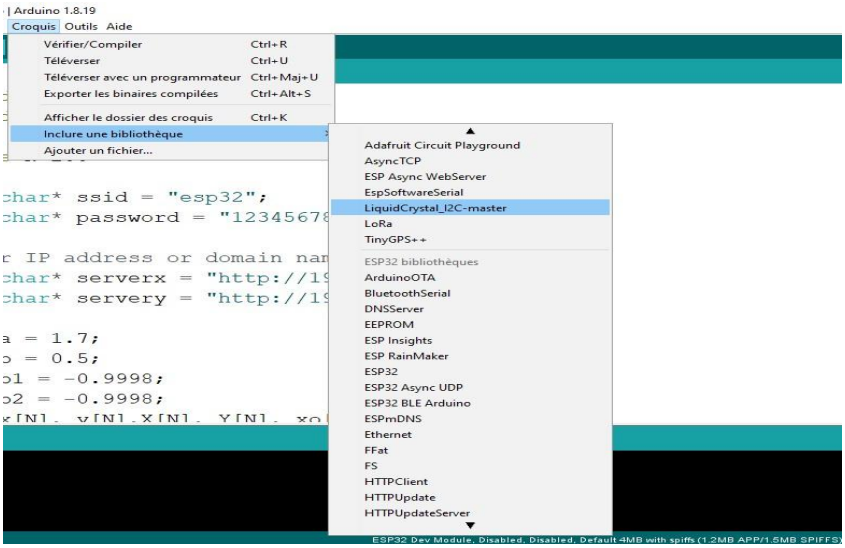


Figure IV.12: Sélection de la bibliothèque wifi



FigureIV.13 : Sélection du bibliothèque LiquidCrystal_I2C

IV. 3 Résultats d'implémentation

Cette section est dédiée à présenter des images des expérimentations et des résultats obtenus. La Figure (**IV**.14) : illustre une image de notre réalisation.

- **Détail du schéma**

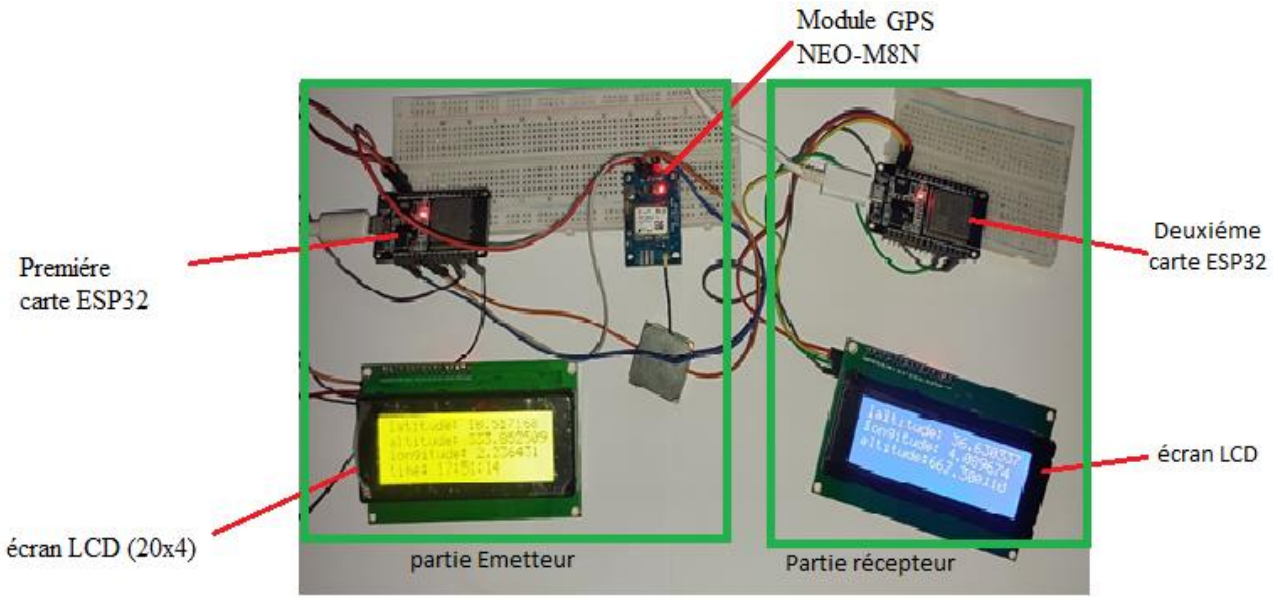


Figure IV.14: Schéma de la réalisation

Le mode de fonctionnement de notre montage est le suivant :

La partie émetteur est composée de deux cartes électroniques, à savoir l'ESP32 et un module GPS. Cette configuration permet de capturer les données (latitude, longitude, altitude et heure d'enregistrement), qui seront ensuite chiffrées par la fonction de cryptage. Le message chiffré est alors affiché sur le premier écran LCD.

Ensuite, le message chiffré et l'état x_1 sont multiplexés à l'aide d'un multiplexeur pour être envoyés dans le canal de transmission vers la partie récepteur.

Une fois le signal reçu, il sera séparé en deux. L'étatx_1 servira à la synchronisation, tandis que le message chiffré sera déchiffré par la fonction de décryptage.

Le message déchiffré sera affiché sur le deuxième écran LCD présent dans la partie récepteur.

La Figure (IV. 15) montre le message crypté, dans la première partie (émetteur), affiché sur le premier écran LCD.

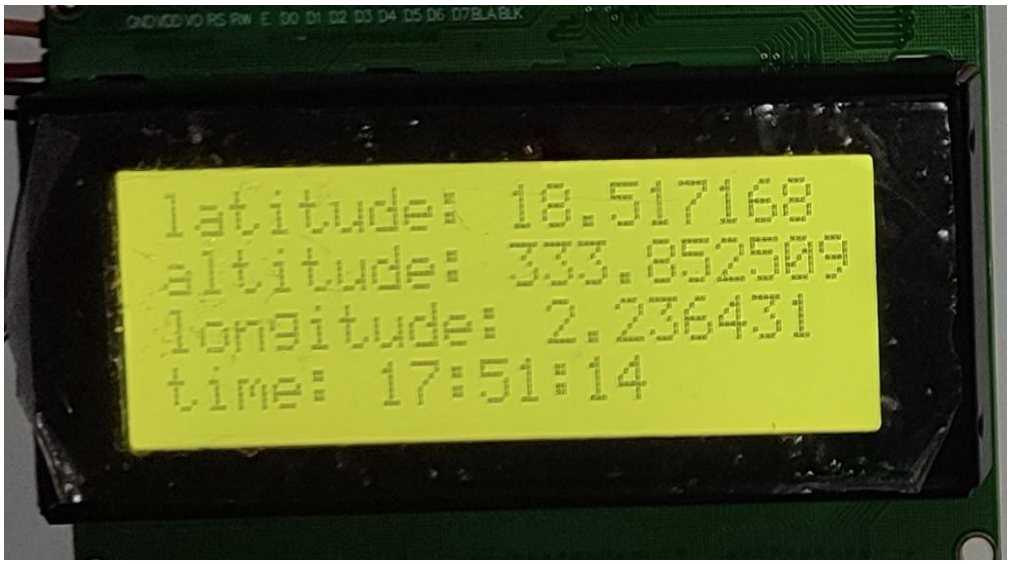


Figure IV. 15 : Affichage des coordonnées GPS crypter sur écran LCD

La Figure (IV. 16)représente la localisation à partir des coordonnées GPS crypter ; Cette dernier est obtenue à l'aide de la fonction de chiffrement.

On remarque que la localisation obtenue est complètement fausse, ce qui prouve que le message est entièrement chiffré et que le cryptage est réussi.

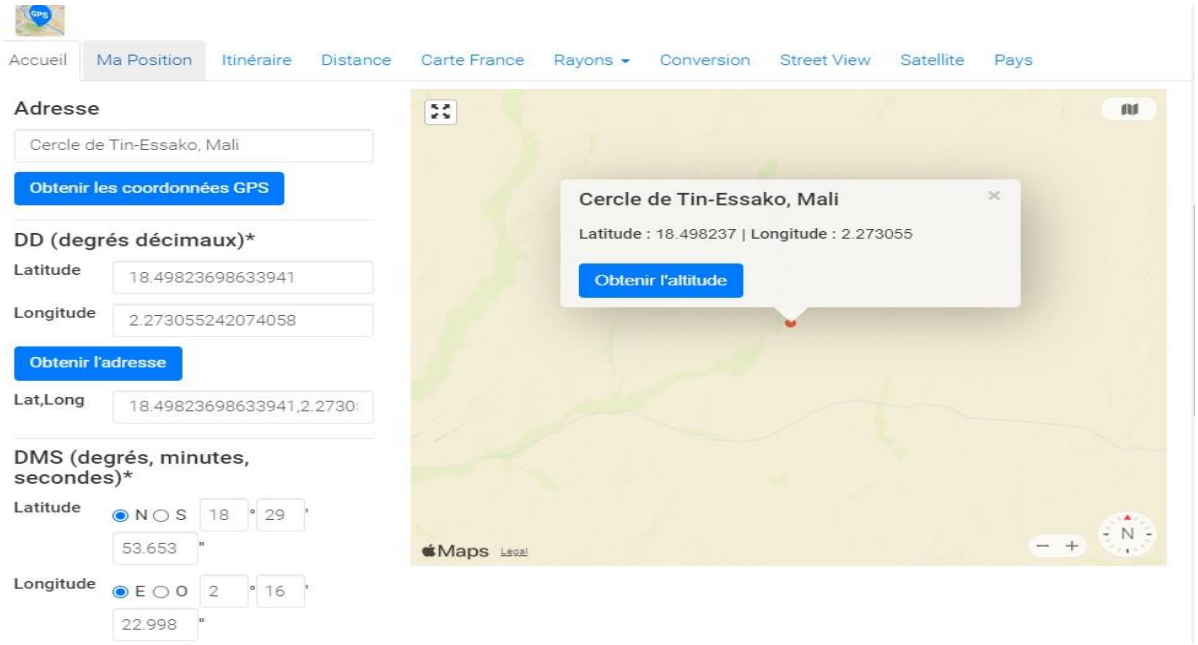


Figure IV.16: Exemple de localisation à partir des coordonnées GPS chiffrées

La figure (IV. 17) Illustre l'affichage sur écran LCD des coordonnées GPS au niveau de récepteur une fois décryptées grâce à l'estimation par faite des états par l'observateur impulsifs.

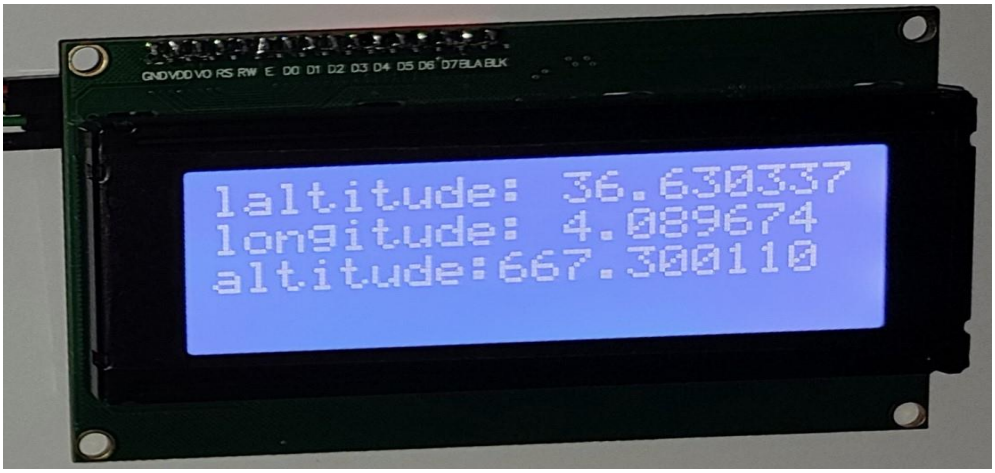


Figure IV. 17 : Affichage des coordonnées reçues et décrypter sur écran LCD

La position exacte de l'émetteur correspondant aux coordonnées décryptées en utilisant le site coordonnées-gps.fr comme il est illustré par la Figure (IV.18) suivante.

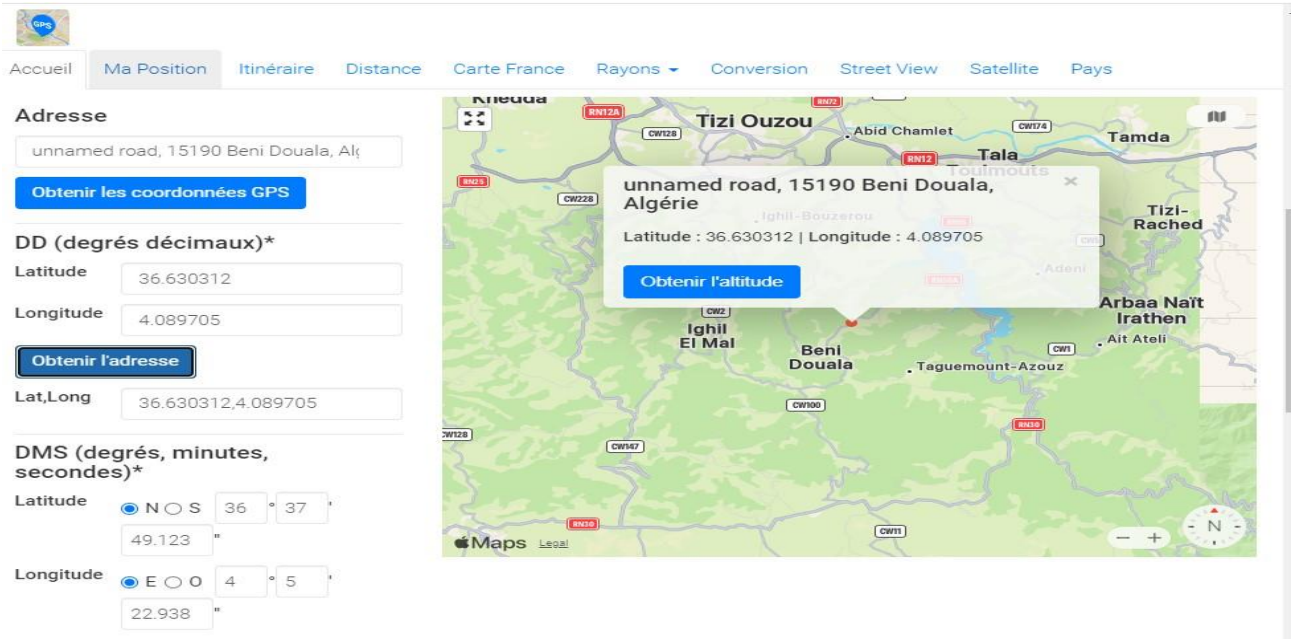


Figure IV.18: Exemple de localisation à partir des coordonnées GPS déchiffrées

IV. 4 Conclusion

Dans ce chapitre, nous avons présenté notre réalisation ainsi que les différents résultats pratiques que nous avons pu obtenir. Les deux blocs de transmission à savoir : l'émetteur et le récepteur ont été codés et implémentés dans des cartes ESP32, en utilisant les bibliothèques appropriées. Ceci nous a permis de tester notre système de transmission. En effet, la synchronisation à l'aide de l'observateur impulsif a bien été établie, par conséquent, le message que nous avons crypté à l'aide des états du système chaotique de Lozi, puis envoyé dans le canal après avoir multiplexé avec le signal de synchronisation depuis l'émetteur a bien été décrypté au niveau du récepteur, et la position de l'émetteur a été déterminée avec succès et précision.

Conclusion générale

Dans ce mémoire, nous avons proposé, étudié et implémenté un système de transmission sans fil de données sécurisées de type coordonnées GPS basée sur les systèmes chaotiques discrets et leur synchronisation impulsive basé sur le chaos. Ce travail nous a offert l'opportunité d'explorer en profondeur le phénomène du chaos. Nous avons également abordé tous les aspects fondamentaux liés à ce phénomène.

Dans le premier chapitre de ce mémoire, nous avons d'abord abordé les concepts fondamentaux des systèmes dynamiques ainsi que les caractéristiques des systèmes chaotiques, telles que la sensibilité aux conditions initiales, le déterminisme, et l'aspect aléatoire de leurs trajectoires. Pour illustrer concrètement les notions discutées, nous avons présenté des exemples de système chaotique connus, tant en temps continu qu'en temps discret, tels que le modèle de Lorenz et la fonction logistique, en les mettant en lumière à la fin du chapitre.

Dans le deuxième chapitre, nous avons introduit le principe de synchronisation, en récapitulant les différents modes et techniques ainsi que les types proposés dans la littérature. Cette étape est essentielle pour une transmission de données. Nous avons ensuite étudié la méthode de synchronisation impulsive. Pour conclure le chapitre, nous avons présenté les résultats de simulations effectuées sous Matlab/Simulink, portant sur le système de Lozi et l'observateur impulsif.

Dans le troisième chapitre, nous avons présenté les principes et les méthodes de cryptage à base de la théorie du chaos, ainsi que la conception de notre système de transmission, qui se compose de deux blocs. Le premier bloc est un émetteur composé d'un système de Lozi, le deuxième bloc est un récepteur que nous avons synchronisé avec l'émetteur à l'aide d'un observateur impulsif. Nous avons ensuite simulé le système de transmission sur Arduino, intégré un message dans l'émetteur en l'ajoutant à un des états du système, et enfin récupéré le message au niveau du récepteur. Enfin, nous sommes passés à la partie réalisation où nous avons présenté le montage effectué.

Dans le quatrième chapitre, nous avons présenté les différents résultats obtenus au cours de la programmation et de l'implémentation de notre travail. Ces résultats démontrent bien que la transmission sécurisée basée sur le chaos, étudiée par simulation est garantie avec succès en pratique. Ces résultats laissent entrevoir quelques perspectives et énormément de possibilités de développement dans le domaine de la communication.

En fait, nous pouvons envisager, à l'avenir de :

- Transmettre les coordonnées sur une longue distance en utilisant un protocole de transmission adéquat
- Analyser la robustesse du schéma de transmission proposé et renforcer la sécurité de l'algorithme de chiffrement à partir de cette analyse.

En conclusion de ce mémoire, nous pouvons affirmer que le chaos est un domaine en pleine expansion et en constante évolution, offrant des innovations de diverses origines. Actuellement, la majorité des recherches se focalisent sur l'application du chaos dans les systèmes de cryptographie, dans le but de répondre aux exigences croissantes en matière de temps de chiffrement et de sécurité. Nous souhaitons que notre modeste travail sert aux promotions à venir afin d'atteindre et réaliser les perspectives citées.

Bibliographie

[1] K. Ahmed Ridha « Systèmes chaotiques pour la transmission sécurisée de données » Thèse de magister, Université Mohamed Khider Biskra, Algérie, 2013.

[2] D.R.Stinson « Cryptography, Theorie and practice ».Chapman and Hall/CRC, ISBN 9781584885085, 2005.

[3] R.Dumont. « Introduction à la cryptographie et à la sécurité informatique ». Note de cours, Université de Liége, 2006-2007.

[4] K.T. Alligood, Tim D. Sauer, James A. Yorke « Chaos an introduction to dynamical systems », Edition Springer, ISBN-13: 978-0387946771, 2000.

[5] J.Gleick. « La théorie du chaos », Edition Flammarion, ISBN : 208081219X, 1999.

[6] H.Dubois, « synchronisation de système chaotiques : étude des méthodes classiques et développement de nouvelles approches » , Thèse de doctorat université de lyon,2022.

[7] P. Bergé « Le chaos ». Magazine Scientifique Européen Archimède, 13 Janvier 1998.

[8] C. Morel « Analyse et controle de dynamiques chaotiques, application à des circuits électroniques non-linéaires » Thèse de doctorat, Université d'Angers, 2005.

[9] S.H. Strogatz, « Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering », Addison-Wesley, 1994.

[10] E. Goncalves, « introduction aux systèmes dynamiques et chaos », Engineering school, Institut Polytechnique de Grenoble, France, Avril 2004.

[11] A.J. Michaels, « Digital Chaotic Communications », Thèse de Doctorat, Georgia Institute of Technology, 2009

[12] H.Hamiche « Inversion à gauche des systèmes dynamiques hybrides chaotiques, application à la transmission sécurisée de données » Thèses de Doctorat, Université Mouloud Mammeri Tizi Ouzou, Algérie, 2011.

[14] J.Vonnez. « Une introduction expérimentale au chaos déterministe » travail de licence ,2000.

[15] I. Talbi, « Systèmes dynamiques non linéaires et phénomène du chaos (application à la cryptographie) », Mémoire de Magister, Université Mentouri de Constantine, 2010.

[16] E.Cherrier « Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires » Thèse de doctorat, Université de Nancy, France, 2006.

[17] O. Megherbi, « Etude et réalisation d'un système sécurisé à base de systèmeschaotiques », Mémoire de Magister, Université Mouloud Mammeri de Tizi Ouzou, 2013.

[18] S.De bievre« le chaos en physique et en mathématiques », thèse de doctorat, Université des sciences et technologies de Lille ,2007.

[19] N.E.Lorenz « The essence of chaos » University of Washington Press, 1993. N. Witkowski.

[20] I. Ameur, « Contrôle, chaotification et hyperchaotification des systèmes dynamiques »,Mémoire de Magister, Université Mentouri de Constantine, 2007.

[21] R.C Hilborn, « Chaos and nonlinear dynamics: an introduction for scientists and engineers », Oxford University Press, second edition, 2000.

[22] H. Dimassi, thèse de doctorat "Synchronisation des systèmes chaotiques par observateurs et applications a la transmission d'informations", Université Paris Sud XI – Université Tunis El-Manar, 2 Sep 2013.

[23] A. Fradkov, A.Y. Pogromsky, « Introduction to control of oscillations and chaos World scientific» Singapore, Series A, vol. 35, 1998.

[24] M. Halimi, « Observation et détection de modes pour la synchronisation des systèmes chaotiques : une approche unifiée », Thèse de Doctorat, Université de Lorraine, Nancy, France,2013.

[25] C. Hugenii , Horoloquim Oscilatorium . 1673.

[26] L.M. Pecora, T.L. Carroll, « Synchronization in chaotic systems », Physical Review Letters, pp. 821-825, February 19, 1990.

[27] J.Lu, "Generalized (complete , lag, anticipated) synchronization of discrete-time chaotic systems",Commun. Nonlinear .Sci .Numer . Simulat .,Vol . 13 (9), pp. 1851 -1859 . (2008)

[28] C.Li, X.Liao, K.W.Wong « Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication», volume 194, N°3-4, pp.187-202, 2004.

[29] Z. Ma, Z. Liu, G. Zhang. "Generalized synchronization of discrete systems", Appl.Math. Mech., vol. 28 (5), pp. 609-614, 2007.

[30] G.Zheng « Formes normales d'observabilité paramétriques par les sorties : Applications au cryptage par synchronisation de systèmes chaotiques » Thèse de doctorat, Université de Cergy-Pontoise, France, 2006.

[31] M. Halimi, "Etude et réalisation d'une transmission sécurisée à base de circuit chaotique de Chua", Mémoire de fin d'études, Université de Jijel, Algérie, Juin 2010.

[32] Tidjani Menacer,Synchronisation des systèmes dynamiques chaotiques à dérivées fractionnaires,Université Constantine 1,(Mai2014).

[33] Tan, X., Zhang, J., Yang, Y. (2003), "Synchronizing chaotic systems using backstepping design," Chaos Solitons Fractals, Vol. 16, pp. 37–45.

[34] R. A. Essedik, observateur à mode glissant d'ordre supérieur et inversion à gauche, Université de Tlemcen, 19 mai 2013.

[35] M.Oueder. Synthèse des observateurs pour les systèmes non linéaires. Automatique. Université de Caen, 2012. Français.

[36] G.M'hammed « Commande et Observateurs d'état des Systèmes non Linéaires », Université Hassan,settat ,2019.

[37] V.Sundarapandian "Sliding controller design for the global chaos synchronization of identical hyperchaotic Yujun systems," Intern. J. Adv. Info. Tech, 2012.

[38] G. Zhang « Formules normale d'observabilité paramétrées par sortie : application au cryptage par synchronisation de systèmes chaotiques », thèse de doctorat de L'université de Cergy-pontoise, année2006.

[39] J.Daafouz and G.Milleriaux, «Poly- quadratic stability and global chaos synchronization of discrcret time hybrid systems, special Issue of Mathematics and computers in simulation, vol.58.pp. 295.307.

[40] M.Abutaha et al, « Cryptography is the science of information security»,International journal of computer science and security (IJCSS),2011

[41] A.Zemouche, « Sur l'observation de l'état des systèmes dynamiques non linéaires »,thèse de Doctorat, université Louis Pasteur-Strasbourg I, France ,2007.

[42] A. Ali-Pacha,N. Hadj-Said « chaos crypto-système base sur l'attracteur de Hénon-Lozi», Institut national des Télécommunication, Evry, France

[43] L. Azib « Système chaotique et hyper chaotique pour la transmission sécurisée des données », thèse de magister, université Abou Baker Belkaid, Tlemcen, 2010.

[44] A.Layec, « Développement de modèles de CAO pour la simulation système des systèmes de communication. Application aux communications chaotiques » Thèse de Doctorat, université de Limoges, année 2006

[45] M.L'Hénault, « Faisabilité d'un système d'Emission-Réception Analogique pour la communication Sécurisée par le chaos, thèse de doctorat, Université pierre et Marie Curie,Paris, France, 2007.

[46] E.Cherrier « Estimation de l'état et des entrées inconnues pur une classe de systèmes non Linéaires » thèse de doctorat, université de Nancy, France, 2006.