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

Université **M**ouloud **M**ammeri De **T**izi-**O**uzou

Faculté De **G**énie **E**lectrique Et D'informatique
DEPARTEMENT D'AUTOMATIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Spécialité :**Automatique et Systèmes**

Présenté par
ARBANE Dehbia
ARAB Katia

Mémoire dirigé par **Saïd Djennoune**

Thème

Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole

Mémoire soutenu publiquement le 09 juillet 2018 devant le jury composé de:

Mr Redouane KARA
Pr, UMMTO, Président.

M r Saîd DJENNOUNE
Pr, UMMTO , Rapporteur.

Mr Amar SI AMMOUR
MCA, UMMTO, Examinateur.

Mr MANSOURI Rachid
Pr, UMMTO, Examinateur.

Mme KASSIM Sarah
Docteur, UMMTO, Invitée.

Ce travail a été préparé au : laboratoire de conception et conduite des systèmes de production (L2CSP)

Remerciements

Nos remerciements chaleureux à notre promoteur, Monsieur **DJENNOUNE Saïd**, professeur à l'Université Mouloud Mammeri de Tizi-Ouzou, pour son soutien, ses réponses à nos diverses questions, et avant tout pour nous avoir proposé ce sujet très intéressant, aussi c'est un honneur pour nous d'avoir eu l'occasion de travailler et d'apprendre aux cotés de personne ayant des qualités humaines exceptionnelles.

On aimera également remercier les membres de jury qui nous feront l'honneur d'évaluer ce travail.

Dédicace

À la Mémoire de mon très cher Père
À qui je dois ce que je suis

J'aurais tant aimé que tu sois là parmi nous pour voir tes souhaits se réaliser. Aucun mot ne saurait témoigner de l'étendue des sentiments que j'éprouve toujours à ton égard.

Je te dédie ce travail et le présent diplôme car c'est à toi que je les dois et c'est grâce à toi que je les ai obtenus.

Que ce rapport soit l'expression de ma grande affection et en témoignage de mon profond amour.

- La meilleure maman du monde.
- Ma sœur et mon frère.
- La meilleure amie qui est une deuxième sœur pour moi avec qui j'ai partagé ce présent mémoire et qui a toujours été la pour moi, merci.
- Cousins et cousines.
- Ma très chère grand- mère.
- Toute la famille.

Katia

Dédicace

Je dédie ce travail :

A la personne qui a tout donné pour que je ne puisse jamais manquer de rien, et qui m'a toujours soutenu et encouragé le long de mon parcours scolaire, ainsi que dans tout ce que j'entreprends dans ma vie, ma chère mère.

A la mémoire de ma grand-mère.

A mes chers petits frères.

A mon père.

A la sœur que je n'ai jamais eue, la personne avec laquelle j'ai partagé ce présent mémoire.

A mon ami proche pour son soutien et ses encouragements.

Dehbia

Table des matières

Table des figures

Liste des tableaux

Notation

Ensembles :

$\mathbb{R}$:	Ensemble des nombres réels .
$\mathbb{R}^n$:	Espace vectorielle de dimension n.
$\mathbb{R}^+$:	Ensemble des nombres positifs.
$\mathbb{Z}^+$:	Ensemble des nombres relatifs (entiers négatifs et positifs).
$\mathbb{N}$:	Ensemble des nombres entiers naturels.
$\mathbb{N}^*$:	Ensemble des nombres entiers naturels non nuls.
$\dot{x}$:	Dérivée du vecteur d'état x .
$\hat{x}$:	Vecteur x estimé.
$\dot{\hat{x}}$:	Dérivée du vecteur x estimé.
$L_f^i h$:	$(i)^{ème}$ dérivée de Lie de h dans la direction de$f$.
$dL_f^i h$:	Le différentiel de $L_f^i h$.

Fonctions et sous-espaces de fonctions :

C^∞ :	Classe des fonctions infiniment dérivables et continues sur un intervalle.
s :	Variable de la transformée de Laplace d'un signal continu($s \in \mathbb{C}$).
$\mathcal{L}$:	Transformée de Laplace .
E_α :	Fonction de Mittag-Leffler à un paramètre.
$E_{\alpha,\beta}$:	Fonction de Mittag-Leffler à deux paramètres .
$\Gamma(.)$:	Fonction Gamma .

Autres opérateurs mathématiques :

D^α :	Opérateur de dérivation d'ordre fractionnaire α.
I^α :	Opérateur de d'intégration d'ordre fractionnaire α.
Δ^α :	Opérateur de différence d'ordre fractionnaire α.

Matrices et normes :

J :	La matrice Jacobienne.
O :	La matrice d'observabilité.
λ_i :	Variation d'exposant de Lyapunov selon i .
$\| . \|$:	La norme euclidienne.
$\| . \|$:	Valeur absolue d'un nombre réel ou module d'un nombre complexe.
$(.)^T$:	Transposée d'un vecteur ou d'une matrice .

Acronymes :

DES :	Data Encryption Standard .
RSA :	Rivest Shamir Adleman .
AES :	Advanced Encryption Standard .
CFE :	Continued Fraction Expansions .
CSK :	Chaos Shift Keying .
MIT :	Massachusetts Institut of Technologie .
FSR :	Feedback Shift Register .

Introduction générale

Avec l'ampleur que prennent les différentes technologies dans la vie quotidienne de chaque individu et le progrès qu'a connu la communication durant ces dernières années, tel l'internet, la communication sans fil et par satellite, les vidéos conférences, la messagerie électronique, la sécurité des échanges d'informations est devenue une préoccupation majeure [1].

Afin d'y remédier, on a recours à la cryptographie, qui joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données.

Les techniques de cryptographie classique sont basées sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. Et la cryptographie moderne comprend le chiffrement symétrique et le chiffrement asymétrique tels que les protocoles le RSA, DES. La majorité de ces protocoles ont déjà été cassés. Pour ces raisons, plusieurs chercheurs essayent de mettre en œuvre d'autres crypto-systèmes.

Durant ces dernières décennies, les systèmes non linéaires chaotiques ont été appliqués à la cryptographie afin d'augmenter le degré de sécurité. L'étude de ces systèmes est liée à la théorie du chaos qui a connu une grande évolution à partir des années 1960 grâce aux travaux du météorologiste Edward Lorenz [2]. Grâce aux propriétés intrinsèques des systèmes chaotiques telle que leur sensibilité aux conditions initiales, les systèmes chaotiques sont de bons candidats pour la cryptographie.

L'idée de l'utilisation du chaos dans les systèmes de communication a été inspirée de la découverte de Pecora et Carroll en 1990 [3]. Ces auteurs ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés d'une manière convenable. Depuis, de nombreuses techniques de cryptage,par addition, par commutation, par modulation...etc, ont été mises au point pour inclure le message clair dans une porteuse chaotique, et par un processus de synchronisation le récepteur est capable d'estimer l'état de l'émetteur, puis de décrypter et enfin de restituer le message clair.

Les chercheurs ont également montré qu'on peut prolonger la synchronisation aux systèmes chaotiques à dérivées fractionnaires. Ces systèmes chaotiques d'ordre fractionnaire ont été mis en application dans le domaine de la transmission sécurisée pour renforcer la sécurisation et rendre la cassure de la clé quasiment impossible.

Notre travail a pour objectif de proposer des schémas de transmissions sécurisées, en

exploitant dans un premier temps les propriétés des systèmes dynamiques chaotiques en utilisatant la synchronisation par observateurs et ce en temps discret et en temps continu puis nous proposons ce schéma de transmission avec l'introduction du calcul fractionnaire dans les systèmes dynamiques chaotiques afin de renforcer le niveau de sécurité de ces crypto-systèmes.

Afin d'aborder ce travail, nous avons divisé ce mémoire en cinq chapitres dont :

Le premier chapitre est consacré à l'introduction et l'étude des systèmes chaotiques par leurs caractéristiques et les outils permettant d'identifier leurs comportements.

Le second chapitre présente des généralités sur la cryptographie et les différentes méthodes de chiffrement existantes. Ce chapitre a pour objectif d'introduire l'utilité et l'utilisation du chaos dans la cryptographie.

Le troisième chapitre introduit l'approche de Pecora et Carroll dans la synchronisation des systèmes chaotiques ainsi que les différentes méthodes de synchronisation telle que la synchronisation par observateurs.

Dans le quatrième chapitre, nous allons introduire les différentes notions sur le calcul fractionnaire dans le cas des systèmes chaotiques en temps continu et en temps discret

Le cinquième chapitre est consacré à l'étude et à la conception de nouveaux schémas de transmissions sécurisées en temps continu et en temps discret, dont chaque schéma de transmission est composé d'un émetteur, un système chaotique d'ordre entier et fractionnaire dit « Système de Lorenz et Hénon-modifié » et à la réception, un observateur « Luenberger »et observateur « retardé étape par étape » qui permettent de reproduire les signaux chaotiques générés par l'émetteur et le message confidentiel de type « signal parole » et ce en utilisant la méthode de cryptage chaotique par inclusion.

Ensuite, nous terminons notre mémoire par une conclusion générale récapitulant nos principaux résultats et quelques perspectives.

Chapitre 1

Systèmes chaotiques

1.1 Introduction

Depuis fort longtemps,la science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos, qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines.

N'ayant pas de définition au sens universel, le chaos est décrit comme étant un cas particulier d'un système non linéaire déterministe, caractérisé par son comportement très sensible aux conditions initiales et bien qu'il soit déterministe, il est imprédictible à long terme, et présente un aspect aléatoire, sans pour autant faire partie des phénomènes aléatoires.

Dans ce chapitre, nous nous intéressons aux systèmes dynamiques chaotiques en spécifiant leurs caractéristiques tout en présentant les méthodes permettant de l'identifier.

1.2 Systèmes dynamiques

1.2.1 Définition

Globalement, un système dynamique, décrit des phénomènes qui évoluent au cours du temps, dont le terme « système » fait référence à un ensemble de variables d'état [4].

1.2.2 Représentation mathématique

En temps Continu

Un système dynamique, dans le cas continu est régi par un système d'équations différentielles.

$$\dot{x}(t) = f(x(t), t) \tag{1.1}$$

Où

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

$$x(t_0) = x_0 \tag{1.2}$$

$x_0 \in \mathbb{R}^n$représente l'état initial du système et t_0l'instant initial.

En temps Discret

Un système dynamique dans le cas discret, est représenté par des équations aux différences, appelées également « équations de récurrences ».

$$\begin{cases} x(k+1) = g(x(k), k) \\ x(k_0) = x_0 \end{cases} \tag{1.3}$$

Où

k est l'instant discret, k_0 est l'instant discret initial, x_0 est le vecteur des états initiaux et $g : \mathbb{R}^n \times \mathbb{Z}^+ \to \mathbb{R}^n$ indique la dynamique du système en temps discret.

1.2.3 Notions sur les systèmes dynamiques

- *Système autonome* : un système est dit autonome lorsqu'il ne dépend pas explicitement du temps.
- *Causalité :* un système est dit « causal », lorsque son entrée ne précède jamais sa sortie.
- Trajectoire temporelle : représente une grandeur décrite en fonction du temps qui peut être par exemple une variable d'état ou une sortie.
- *Trajectoire de phase* : est une trajectoire représenté sur un plan de phase et qui décrit l'évolution du système au cours du temps pour des conditions initiales données.
- *Espace de phase :* est un espace mathématique, souvent multi-dimentionnel, dont chaque axe de coordonnées correspond une variable d'état du système dynamique étudié.
- *Portrait de phase :* est constitué par l'ensemble des trajectoires de phase possibles d'un système dynamique.
- *Point d'équilibre(ou point fixe) :* on appelle point d'équilibre d'un système le point x^* pour laquelle on obtient $f(x^*) = 0$ dans le cas continu , $g(x^*) = x^*$dans le cas discret.

- *Cycle limite :* est un phénomène non linéaire, qui peut être siège d'oscillations, auto-soutenues, caractérisées par leur amplitude et leur période fixes, indépendante de la condition initiale $x_0$et sans excitation extérieure.
- *Tore :* est un cas particulier du cycle limite qui représente les mouvements résultants de deux ou plusieurs oscillations dépendantes que l'on appelle aussi « mouvements quasi-périodiques », la trajectoire de phase ne se referme pas sur elle même.
- *Attracteur* : est une forme géométrique de l'espace de phase vers lequel tendent les trajectoires de phase.

1.3 Théorie du Chaos

Historique

Henri Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème d'interactions de trois corps célestes, et a écrit « Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir et alors nous disons que cet effet est dû au hasard ».

Plus tard, en 1961, Edward Lorenz [2], météorologue et professeur de mathématique au MIT observa par hasard le phénomène qui s'appellera plus tard la théorie du chaos ou le chaos déterministe, à la suite des calculs visant à prévoir les phénomènes météorologiques. Ces prévisions nécessitaient un grand nombre de calculs d'équations différentielles complexes à très grand nombre de variables impossibles à faire à la main, il a utilisé alors un ordinateur, son Royal Mcbee LGP-300 qui est entrée dans l'histoire de la théorie du chaos, et qui a fait de Lorenz le père officiel de cette théorie puisque les calculs des systèmes chaotiques régissant ces phénomènes étaient difficiles à comprendre et à simuler sans ordinateur. Après plusieurs heures de calculs, Lorenz avait obtenu une série de résultats et a décidé de repasser une deuxième fois ces résultats dans l'ordinateur pour s'en assurer. Pour gagner du temps, il avait entrer les variables avec trois chiffres après la virgule, au lieu de six, il pensait qu'une faible variation dans les variables à la base d'un calcul aurait une incidence du même ordre de grandeur sur le résultat final mais à sa grande surprise, les résultats étaient totalement différents de la première série. Il venait de découvrir le comportement chaotique d'un signal non linéaire ; soit, d'infimes différences des conditions initiales d'un système déterministe entraineraient des résultats complètement différents. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon : « Le simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas ».[5]

1.3.1 Définition

Le phénomène du chaos est un phénomène complexe non linéaire, qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales.

Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toute fois converger vers un point fixe ou un cycle limite.Ces trajectoires qui restent denses dans cette région sont très sensibles aux conditions initiales.Les solutions des équations différentielles non linéaires ne peuvent pas être calculés avec exactitude analytiquement car il n'existe pas de méthode de résolution analytique pour ces équations,sauf pour certaines classes particulières.Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation.

1.3.2 Propriétés des systèmes chaotiques

Parmi les caractéristiques principales permettant d'évoquer un comportement chaotique,on peut retenir les propriétés suivantes :

1.3.2.1 Déterminisme et imprévisibilité

Dans le cas des systèmes déterministes, théoriquement la connaissance de l'état initial de l'entrée,et du modèle permet de prédire l'état futur du système.Cependant il est difficile de calculer la solution analytique théorique de certains systèmes non linéaires, qui est le cas pour les systèmes chaotiques déterministes, car ils sont caractérisés par une sensibilité aux conditions initiales, dont une simple erreur de mesure ou un simple arrondi conduit à des solutions différentes, ce qui les rendent imprévisibles, en conséquence la prévisibilité n'est plus liée au déterminisme.

1.3.2.2 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales est l'une des caractéristiques fondamentales des systèmes chaotiques explicitée par Lorenz dans sa célèbre citation :"l'effet papillon".Une légère variation des conditions initiales sur un système chaotique entraine deux trajectoires qui sont initialement voisines,puis qui divergent exponentiellement,par la suite les deux trajectoires sont incomparables,ce qui rend les systèmes chaotiques imprédictibles à long terme. [5]

Il est donc clair que la moindre erreur ou imprécision sur la condition initiale ne permet pas de décider à tout temps qu'elle sera la trajectoire effectivement suivie.

Pour illustrer cette propriété,on prend comme exemple le système de Lorenz décrit par le système d'équations (1.4)

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - y - xz \\ \dot{z} = xy - cz \end{cases} \tag{1.4}$$

Avec :

(x, y, z) : le vecteur d'état.

(a, b, c) : sont les paramètres du système de « Lorenz ».

$(a = 10; b = 28; c = \frac{8}{3})$: sont les valeurs des paramètres pour lesquelles le système présente un comportement chaotique.

Pour deux conditions initiales très proches :

$(x_{01}, y_{01}, z_{01}) = (0.1, 0.1, 0.1)$.

$(x_{02}, y_{02}, z_{02}) = (0.1001, 0.1001, 0.1001)$.

On obtient la figure (1.1)

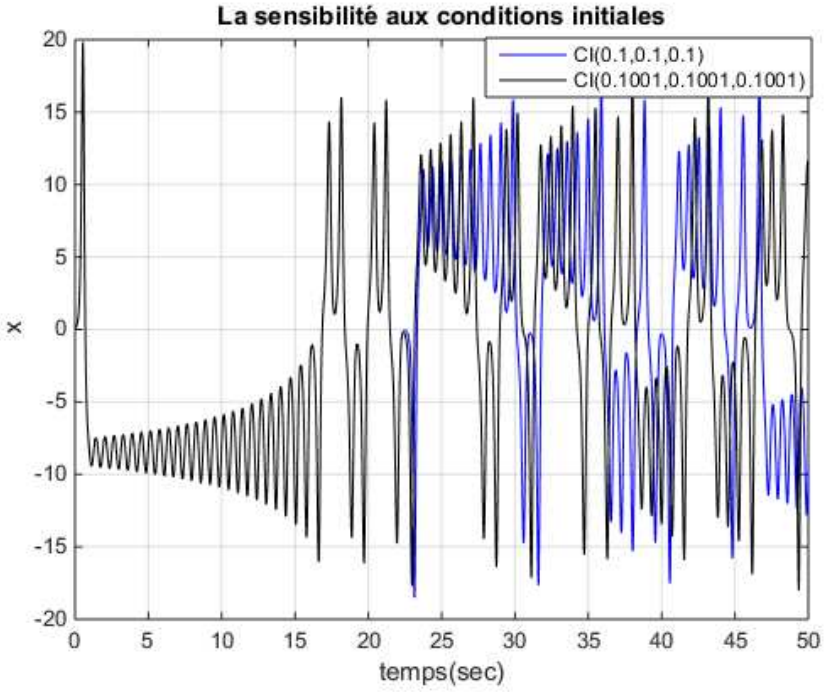


FIGURE 1.1 – Évolution dans le temps pour deux conditions initiales très proches.

La figure (1.1) illustre la sensibilité aux conditions initiales des systèmes chaotiques pour deux conditions initiales très proches. Au départ les deux trajectoires de phase évoluent de la même façon, ensuite elles divergent.

1.3.2.3 Aspect aléatoire

Bien que les systèmes chaotiques soient déterministes, touts les états d'un système chaotique présentent des aspects aléatoires, comme on peut l'observer dans la figure (1.2). Aucune périodicité n'est apparente.

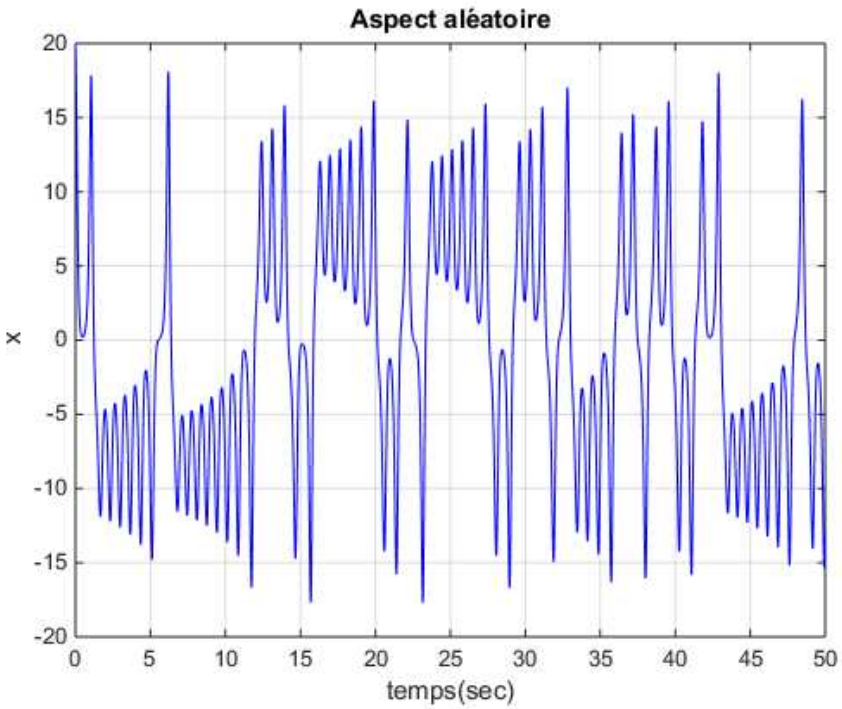


FIGURE 1.2 – L'aspect aléatoire du système de Lorenz .

1.3.2.4 Attracteur étrange

Lorsque Edward Lorenz[2] entreprit graphiquement la solution de son système (1.4) au moyen de son ordinateur, en traçant deux courbes avec deux jeux de conditions initiales très proches,il s'attendait à ce que les deux courbes divergent, mais à sa grande surprise, les deux courbes étaient plus ou moins identiques, elles ressemblaient à deux ailes de papillon.[5]

Le physicien David Ruelle qui s'est penché sur la question a qualifié cette figure « d'attracteur étrange » en remarquant que les trajectoires ne se coupent jamais, et bien qu'elles semblent évoluer au hasard, elle forment des figures indiscutablement reconnaissables.

Par conséquent, lorsque le régime d'un système est chaotique, l'attracteur correspondant est un attracteur étrange qui a des propriétés topologiques différentes de celles d'un attracteur simple .

Un attracteur étrange est caractérisé par son bassin d'attraction et sa dimension fractale.

Le bassin d'attraction

Le bassin d'attraction est l'ensemble de points initiaux de l'espace de phases dont les trajectoires convergent vers l'attracteur et le parcourent d'une façon spécifique et unique.

La dimension fractale

La dimension fractale de l'attracteur selon Hausdorff Besicovutch se présente comme suit. Soit un ensemble de points dans l'espace des phases à n dimensions, qui consiste à recouvrir cet ensemble par des hyper cubés de côté ε, soit le nombre minimum de cubes $N(\varepsilon)$ nécessaires à cette opération qui varie comme [6] :

$$N(\varepsilon) = \varepsilon^{-D} \tag{1.5}$$

Si l'ensemble est celui des points d'un segment de longueur L

$$N(\varepsilon) = L\varepsilon^{-1} \tag{1.6}$$

d'où $D = 1$.

Si l'ensemble est celui des points d'une surface d'aire S

$$N(\varepsilon) = S\varepsilon^{-2} \tag{1.7}$$

d'où $D = 2$.

D est la dimension de Minkowski est définie par :

$$D = lim_{\varepsilon \to 0} \frac{lnN(\varepsilon)}{ln(1/\varepsilon)} \tag{1.8}$$

1.3.2.5 Bornitude des solutions

Toutes les solutions des systèmes chaotiques sont des solutions globalement bornées. En effet, la trajectoire du système chaotique que l'on observe dans l'espace des phases reste confinée dans une région bien définie (attracteur étrange), après une période transitoire de durée variable [7].

On peut qualifier les systèmes chaotiques de stables si leurs conditions initiales sont prises dans le bassin d'attraction, c'est à dire que les trajectoires ne divergent pas vers l'infini mais convergent sur l'attracteur étrange.

Dans l'étude des systèmes non linéaires les cas suivants se présentent :

- Stabilité asymptotique : les trajectoires convergent vers un point fixe.
- Limite de stabilité(réponse oscillatoire sinusoïdale) : les trajectoires convergent vers un cycle limite.
- Limite de stabilité (réponse bornée) : les trajectoires convergent vers un attracteur étrange.

– Instabilité : Trajectoires divergent vers l'infini .

1.3.3 Identification du chaos

Comme il est difficile de calculer la solution analytique des systèmes chaotiques, des méthodes numériques sont utilisées.

Dans cette section, nous présentons quelques outils qui permettent d'identifier le comportement chaotique d'un système dynamique et ses caractéristiques.

1.3.3.1 Exposants de Lyapunov

Les valeurs propres de la matrice d'état dynamique A des systèmes linéaires permettent de caractériser les points d'équilibres et leur stabilité. Les exposants de Lyapunov sont une généralisation de ces valeurs propres et permettent de caractériser un attracteur (ou le comportement d'un système non linéaire, notamment son caractère chaotique ou hyperchaotique).

Les exposants de Lyapunov sont des grandeurs qui quantifient la divergence exponentielle(ou la convergence)de trajectoires proches à un moment donné dans l'attracteur d'un système dynamique et permet de quantifier également la sensibilité aux conditions initiales.Et dans le cas des systèmes en temps continu et des systèmes en temps discret .

Cas continu

Le modèle dynamique autonome (d'ordre n) est défini par [8] :

$$\dot{x}(t) = f(x(t)) \tag{1.9}$$

On note dans la suite $f(x(t)) = f_t(x(0))$ pour préciser la dépendance de l'état initial $x(0)$. On considère un état initial proche de $x(0)$, avec ε petit, et on écrit le développement limité :

$$f_t(x(0) + \varepsilon) = f_t(x(0)) + J_t\varepsilon + O(\| \varepsilon^2 \|) \tag{1.10}$$

Où J_t est la matrice jacobienne de f à l'origine :$J_t = \frac{\partial f_t}{\partial x}(x(0))$.

On peut montrer que la matrice limite

$$\Lambda_{x(0)} = lim_{t\to\infty}(J_t^T J_t)^{\frac{1}{2t}} \tag{1.11}$$

existe et ne dépend pas de $x(0)$.

Les logarithmes λ_i des valeurs propres de la matrice $\Lambda_{x(0)}$ sont appelés exposants de Lyapunov du système (1.9).

Cas discret

Soit un système dynamique discret autonome [9] :

$$x_{k+1} = f(x_k) \tag{1.12}$$

On considère d'abord que ce système est de dimension $n = 1$. Soient deux conditions initiales très proches, x_0 et $\acute{x}_0$. La trajectoire issue de la condition initiale x_0 est $x_k = f^k(x_0)$, est celle issue de la condition initiale $\acute{x}_0$ *est* $\acute{x}_k = f^k(\acute{x}_0)$.

Si les trajectoires x_k et $\acute{x}_k$ s'écartent à un rythme exponentielle aprèsk itérations, alors :

$$\parallel \acute{x}_k - x_k \parallel = \parallel \acute{x}_0 - x_0 \parallel exp(k\lambda) \tag{1.13}$$

$\lambda \in \mathbb{R}$ correspond aux divergences des deux trajectoires. Il vient :

$$\lambda = \frac{1}{k} ln \parallel \frac{\acute{x}_k - x_k}{\acute{x}_0 - x_0} \parallel \tag{1.14}$$

Si l'on considère que les deux conditions initiales sont très proches, leur différence $\epsilon \in \acute{x}_0 - x_0$ tend vers 0 et lorsque k tend vers l'infini, il vient :

$$\lambda_L = lim_{k\to\infty} \frac{1}{k} lim_{\epsilon\to 0} ln \parallel \frac{\acute{x}_k - x_k}{\acute{x}_0 - x_0} \parallel \tag{1.15}$$

Cette relation est équivalente à :

$$\lambda_L = lim_{k\to\infty} \frac{1}{k} lim_{\epsilon\to 0} ln \parallel \frac{\acute{x}_k - x_k}{\acute{x}_{k-1} - x_{k-1}} . \frac{\acute{x}_{k-1} - x_{k-1}}{\acute{x}_{k-2} - x_{k-2}} ..... \frac{\acute{x}_1 - x_1}{\acute{x}_0 - x_0} \parallel \tag{1.16}$$

Ce qui se réécrit aussi :

$$\lambda_L = lim_{k\to\infty} \frac{1}{k} lim_{\epsilon\to 0} \sum_{i=0}^{k-1} ln \parallel \frac{\acute{x}_{i+1} - x_{i+1}}{\acute{x}_i - x_i} \parallel = lim_{k\to\infty} \frac{1}{k} lim_{\epsilon\to 0} \sum_{i=0}^{k-1} ln \parallel \frac{f(\acute{x}_i) - f(x_i)}{\acute{x}_i - x_i} \parallel \tag{1.17}$$

Finalement cette relation devient :

$$\lambda_L = lim_{k\to\infty}\frac{1}{k}\sum_{i=0}^{k-1} ln \parallel \frac{df(\acute{x}_i)}{dx_i} \parallel \tag{1.18}$$

Le terme λ_L est appelé exposant de Lyapunov de la trajectoire $x_k = f^k(x_0)$ et ne doit pas être confondu avec λou λ_i, valeur propre d'un système linéaire. λ_L mesure le taux moyen de convergence ou de divergence de deux trajectoires issues de conditions initiales très proches. S'il est positif, les trajectoires divergent.Très souvent dans la littérature, si $\lambda_L \succ 0$, le système est dit chaotique.Intuitivement cela reflète la sensibilité aux conditions initiales.

La relation (1.17) se généralise aux systèmes de dimension $n > 1$ qui possèdent alors n exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes de l'espace de phase. On a alors $x_k = f^k(x_0)$ avec $x_k = \left[\begin{array}{cccc} x_k^{(1)} & . & . & . & x_k^{(n)} \end{array} \right]^T \in \mathbb{R}^n$et $f = \left[\begin{array}{cccc} f_1. & . & . & . & f_n \end{array} \right]^T$. Les n exposants de Lyapunov λ_{Li}s'écrivent :

$$\lambda_{Li} = lim_{k\to\infty}\frac{1}{k} ln \mid \lambda_i \left(\begin{array}{cccc} J_k. & . & . & . & J_1 \end{array} \right) \mid, i = 1, ..., n \tag{1.19}$$

$\lambda_i \left(\begin{array}{cccc} J_k & . & . & . & J_1 \end{array} \right)$représente la ième valeur propre du produit des matrices $\left(\begin{array}{cccc} J_k & . & . & . & J_1 \end{array} \right)$. Les J_k sont les matrices jacobiennes issues de la linéarisation de f autour de x_k .

Comportement d'un système dynamique non linéaire en fonction des exposants de Lyapunov

En étudiant les exposants de Lyapunov d'un système non linéaire, on peut définir le type d'attracteur généré par le système. Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif (voir Tableau 1.1).

État	Attracteur	Dimension de Lyapunov	Exposant de Lyapunov
Point d'équilibre	Point	0	$\lambda_n \leq ... \leq \lambda_1 \leq 0$
Périodique	Cercle	1	$\lambda_1 = 0, \lambda_n \leq ... \leq \lambda_2 \leq 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0, \lambda_n \leq .. \leq \lambda_3 \leq 0$
Période d'ordre K	K Tore	K	$\lambda_1 = ... = \lambda_k = 0, \lambda_n \leq .. \leq \lambda_{k+1} \leq 0$
Chaotique		Non entier	$\lambda_1 \succ 0 ; \sum_{i=1}^{n} \lambda_i \prec 0$
Hyperchaotique		Non entier	$\lambda_1 \succ 0 ; \lambda_2 \succ 0 ; \sum_{i=1}^{n} \lambda_i \prec 0$

TABLE 1.1 – Classification des régimes permanents selon les exposants de Lyapunov .

Exemple

Considérons le système de Lorenz donné en (1.4) avec les valeurs des paramètres : $a = 16, b = 45.92, c = 4$ et les conditions initiales :$x(0) = 1, y(0) = 1, z(0) = 1$.

Les Lyapunov obtenus sont : $\lambda_1 = 1.50571$; $\lambda_2 = -0.0008$ et $\lambda_3 = -22.5049$.figure(1.3)

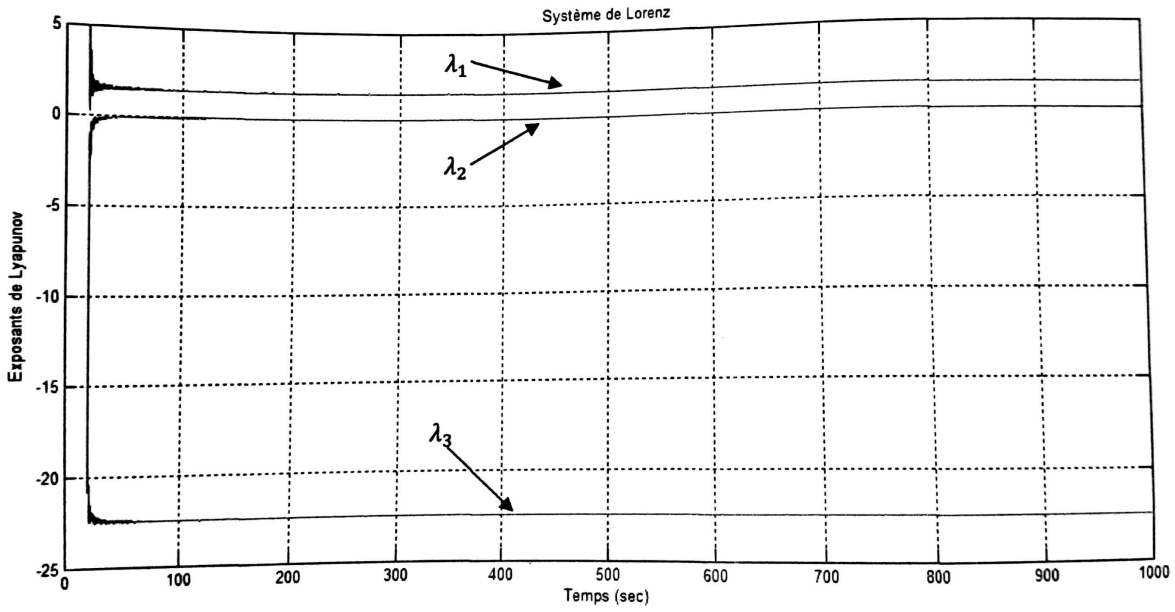


FIGURE 1.3 – Exposants de Lyapunov du système de Lorenz .

On remarque que l'exposant $\lambda_1 = 1.50571$ augmente à une vitesse exponentielle, puis il se stabilise à une valeur fixe .

Le système possède un exposant de Lyapunov positif , donc, le système de Lorenz est un système chaotique.

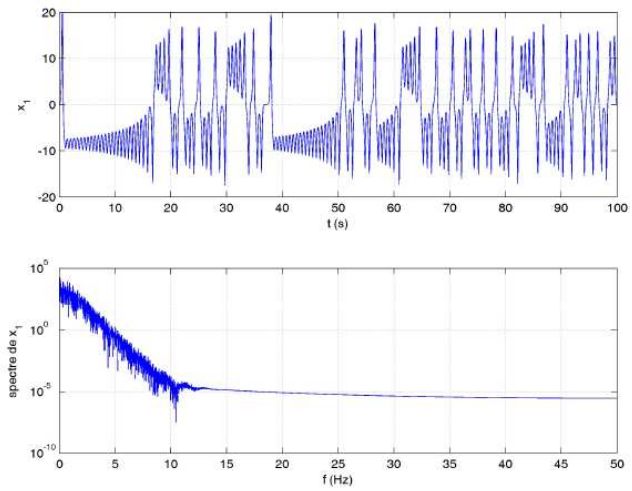
1.3.3.2 Spectre de puissance

Le calcul du spectre de puissance d'un signal sert à extraire ses composantes fréquentielles, en utilisant la transformée de Fourier. En fonction du signal temporel, on calcule la fréquence, l'amplitude et la phase de chaque composante sinusoïdale, en faisant appel aux deux variables réciproques le temps t , et la fréquence f , en utilisant la relation suivante[10] :

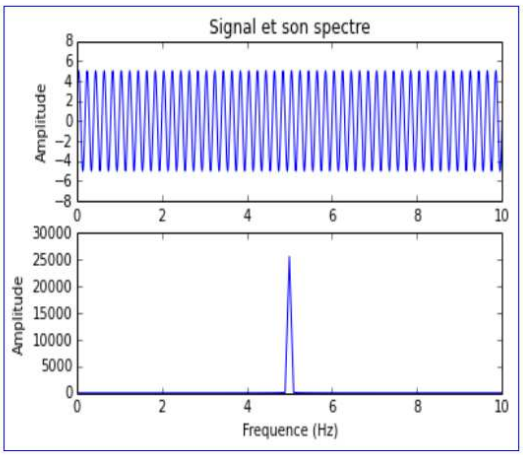
$$\widetilde{X}(f) = \int_{-\infty}^{+\infty} x(t) e^{-2j\pi ft} dt \tag{1.20}$$

– Son module : est représenté par le spectre d'amplitude.
– Son argument t : est représenté par le spectre de phase.

Le calcul du spectre de puissance d'un signal chaotique revient à calculer le spectre de Fourier de l'évolution temporelle d'une des variables du système, sachant que le spectre de Fourier d'un signal périodique ou quasi-périodique est constitué de raies distinctes correspondant aux périodes et harmoniques du système. Cependant pour un signal chaotique, on obtient un spectre continu riche en fréquence, possède une infinité de raies, qui est proche du spectre d'un bruit blanc, illustré par la figure (1.4) qui est très avantageux pour la cryptographie.



Régime chaotique.



Régime périodique.

FIGURE 1.4 – Différence entre le spectre d'un signal périodique et le spectre d'un signal chaotique.

1.3.3.3 Fonction d'auto-corrélation

La fonction d'auto corrélation nommée $C(\alpha)$ permet d'estimer le degré de ressemblance entre la variable x à l'instant t et sa valeur à l'instant $t+\alpha$, et elle est obtenue en faisant la moyenne arithmétique d'un grand nombre de $x(t)$ et $x(t+\alpha)$, sachant que le spectre de puissance correspond à la transformation de Fourier de la fonction d'auto corrélation [10].

Sa relation est citée ci-dessous :

$$C(\alpha) = \frac{1}{t2 - t1} \int_{t1}^{t2} x(t)x(t+\alpha)dt \tag{1.21}$$

En faisant varier progressivement l'intervalleαon obtient la fonction d'auto-corrélation, et donc si $x(t)$ est constant (périodique ou quasi-périodique), $C(\alpha)$ reste non nulle quand $(t \to \infty)$,car le spectre de puissance est formé de raies distinctes,et pour des oscillations périodiques $C(\alpha)$ oscille entre-1 et 1.

Cependant dans le cas des oscillations chaotiques ou le spectre présente une partie continu, $C(\alpha)$ tend exponentiellement vers 0 quand α varie.

Cette propriété assure que les solutions divergent les unes des autres. Si la fonction de corrélation est nulle pour des horizons non nuls, alors c'est un processus non corrélé, et on parle de « bruit blanc déterministe ».

1.3.3.4 Bifurcation

Une bifurcation est un changement qualitatif des propriétés d'un système non linéaire telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents et les paramètres dont la modification quantitative, entraine le changement du régime dynamique de ce système sont appelés paramètres de bifurcation.[11]

Exemple

Sachant que dans les équations de Lorenz par exemple, la résolution du système n'apporte pas toujours le chaos, ce régime n'apparait que pour certaines valeurs des paramètres.Pour illustrer l'influence de ces paramètres, on présente dans cet exemple les résultats de modifications des paramètres « a » ,« c » du système chaotique « Lorenz » décrit pas les équations (1.4) .

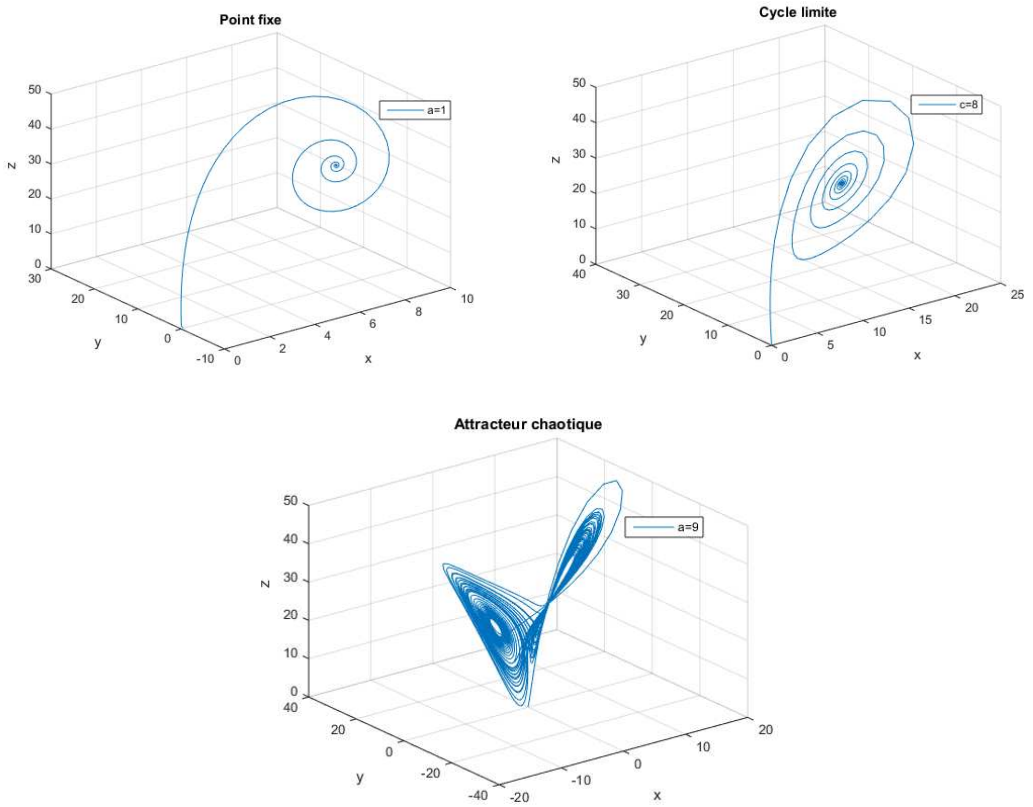


FIGURE 1.5 – Attracteurs de Lorenz pour différentes valeurs de ces paramètres.

Comme illustré sur la figure (1.5)

Lorsque on initialise la valeur de « a » à « 9 » : le système présente un attracteur chaotique.

Lorsque on a initialise la valeur de « a » à « 1 » : le système présente un point fixe.

Lorsque on a initialise la valeur de « c » à « 8 » : le système présente un cycle limite.

Diagramme de Bifurcation

Le diagramme de bifurcation est un tracé, qui permet d'évaluer rapidement l'ensemble des solutions possibles d'un système ainsi que leur stabilité en fonction des variations de l'un de ses paramètres. Il permet également de repérer les valeurs particulières du paramètre qui induisent des bifurcations.

Il présente des intervalles sur lesquelles les solutions asymptotiques évoluent continuellement avec le paramètre, et il classe les valeurs du paramètre sur l'axe des abscisses et les valeurs d'une des variables d'état sur l'axe des ordonnées.

La figure (1.6) illustre le diagramme de bifurcation d'un système quelconque

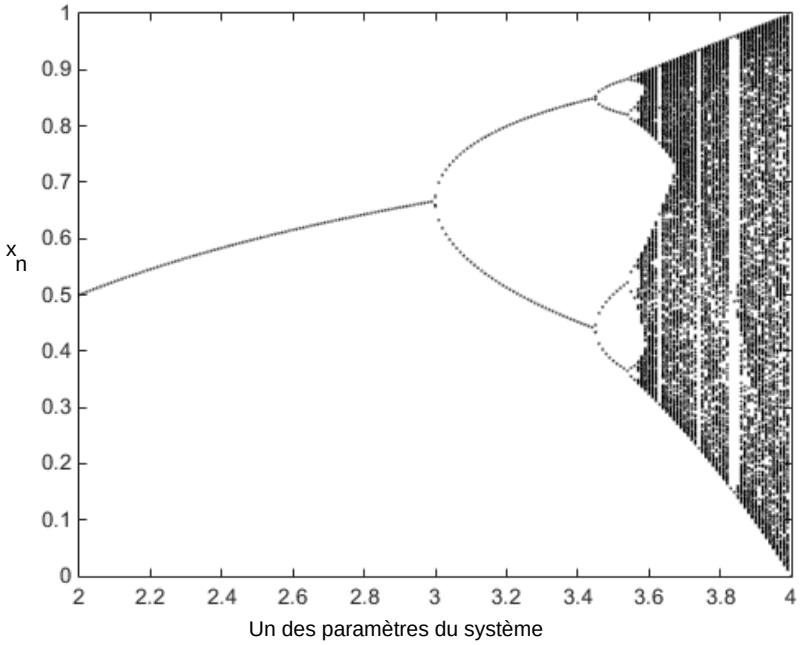


FIGURE 1.6 – Exemple d'un diagramme de bifurcation quelconque.

Route vers le chaos

Varier un paramètre d'un système peut changer son comportement. Il peut passer d'un état stationnaire à un état périodique et devenir chaotique. Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos. L'évolution se fait par des changements discontinus appelé bifurcation.[12]

Feigenbaum a redécouvert une route vers le chaos qui avait été découverte dans les années 60 par Myberg. Cette route est appelée « cascade de doublement de période». Ce scénario est observé avec la suite logistique. Qui est l'exemple le plus connu d'un système non linéaire pour lequel il est possible de tracer un diagramme de bifurcation.

Son équation est donnée comme suit :

$$x_{k+1} = rx(1 - x_k) \tag{1.22}$$

Où $k = 0, 1, 2, ...$, est le temps discret .

x l'unique variable dynamique

$0 \prec r \prec 4$ un paramètre de contrôle qui conduit, suivant les valeurs de r , à une suite convergente soumise à des oscillations ou une suite chaotique.

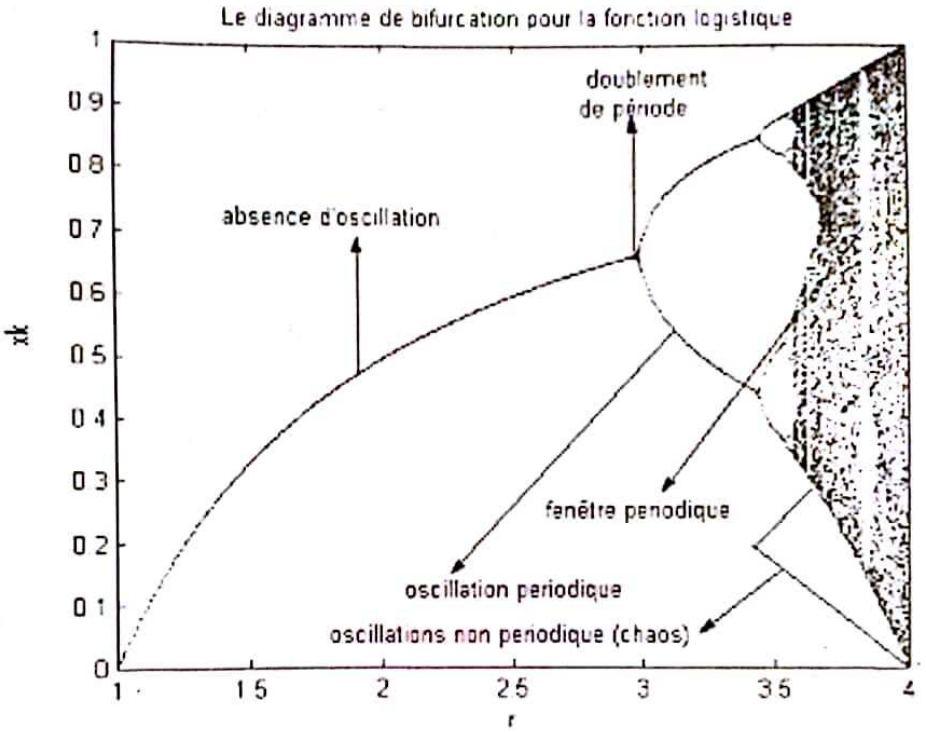


FIGURE 1.7 – Diagramme de bifurcation de la fonction logistique .

On distingue trois scénarios théoriques d'évolution vers le chaos :

– Le doublement de période

L'augmentation d'un paramètre d'un système périodique provoque l'apparition d'un doublement de sa période, :puis elle se multiplie en $4, 8, 16.....$.

Les doublements étant de plus en plus rapprochés,on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie, et c'est à ce moment que le système devient chaotique.

Exemple

La figure (1.8) montre qu'en faisant varier le paramètre « c » du système de Rösseler, décrit par les équations (1.23), on obtient un doublement de période de l'attracteur.

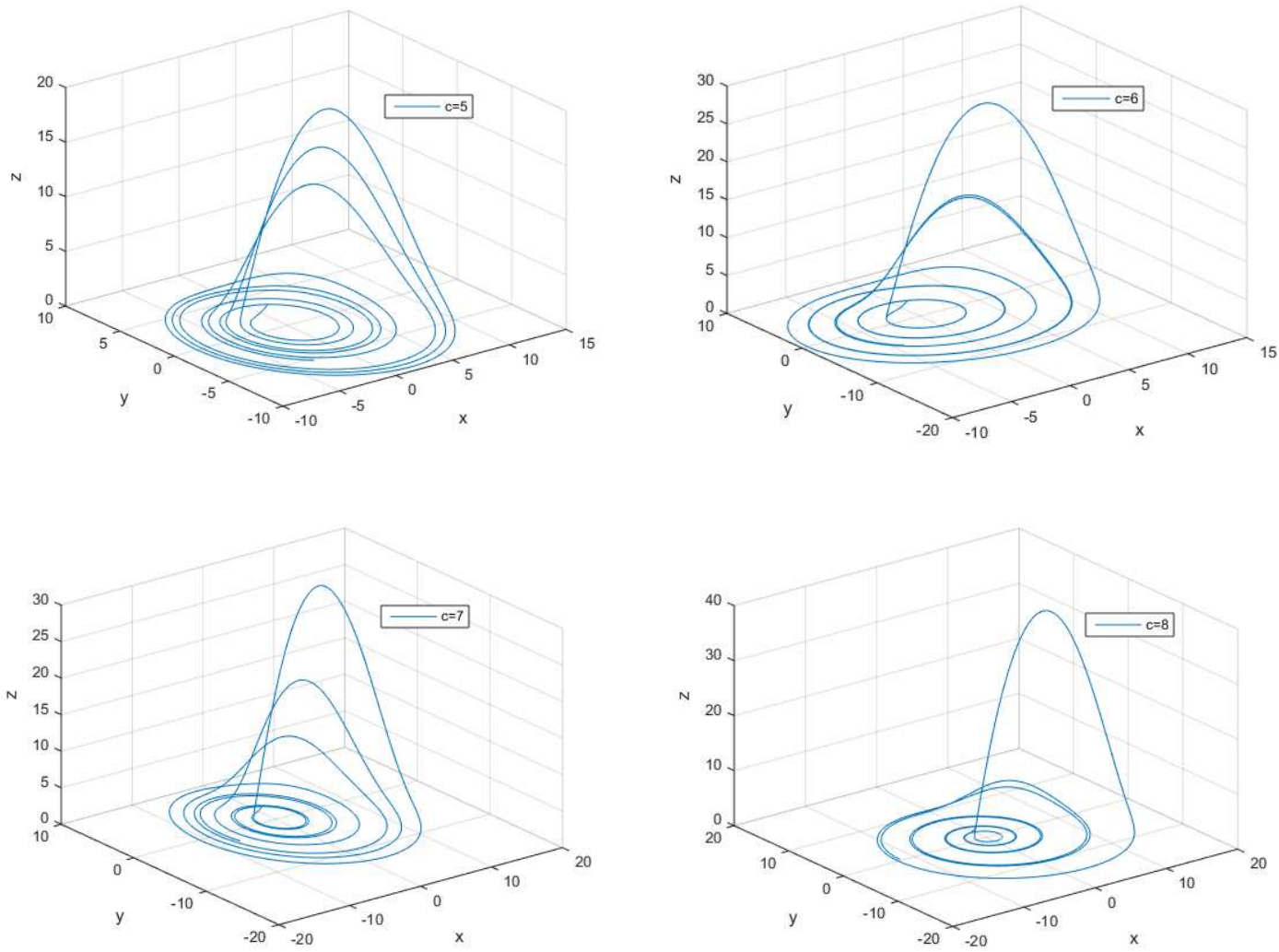


FIGURE 1.8 – Doublement de période de l'attracteur du système de Rössler.

– Intermittence

Les intermittences se caractérisent par l'apparition erratique d'explosions chaotiques dans un système qui oscille de manière régulière.

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise brutalement pour donner lieu à un comportement chaotique. Il se stabilise de nouveau, ensuite pour donner lieu à une autre "explosion chaotique" plus tard.

La fréquence et la durée des phases chaotiques ont tendance à s'accroitre. Plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition.

– Quasi-périodicité

Ce troisième scénario fait intervenir pour un système périodique l'apparition d'une autre période dont le rapport avec la première n'est pas rationnelle. Alors, on change de nouveau le paramètre et il apparait une troisième période, et ainsi de suite jusqu'à l'apparition du chaos.

1.3.3.5 Section de Poincaré

Une application Poincaré, nommée en l'honneur d'Henri Poincaré est un outil mathématique simple permettant de transformer un système dynamique continu en un système dynamique discret via une réduction d'une unité de l'ordre du système, tout en gardant ses propriétés.[13]

Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases par un plan en dimension 3 ou par une droite en dimension 2, afin d'étudier les intersections de cette trajectoire avec ce plan ou cette droite et l'ensemble de points d'intersections situés sur la surface est appelé section de Poincaré.

Le plan de la section doit être choisi de manière à garantir l'existence d'intersections avec la trajectoire et de telle sorte que celle-ci le traverse alternativement dans un sens puis dans l'autre.

On peut identifier le régime de fonctionnement d'un système dynamique en observant l'allure obtenue sur cette section.

- Lorsque le régime est périodique, la section de Poincaré est un point (l'attracteur est un cycle limite).
- Lorsque le régime est bi-périodique, la section de Poincaré est une courbe fermée (l'attracteur est un Tore).
- Lorsque le régime est chaotique, la section de Poincaré,est un ensemble de points répartis sur une surface, ils sont donnés par une structure complexe mais bien définie.

La figure (1.9) illustre le principe de la section de Poincaré pour les trois solutions, périodique, bi-périodique, et chaotique.

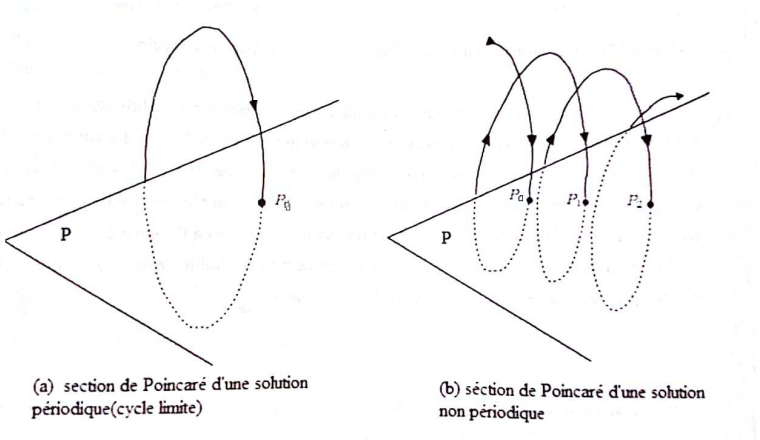


FIGURE 1.9 – Principe de la section de Poincaré.

1.4 Exemples des systèmes chaotiques

1.4.1 Exemple d'un système chaotique en temps continu

Système de Rössler

Le système de Rössler a été proposé par l'Allemand Otto Rössler. Il est lié à l'étude de l'écoulement des fluides. Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique. Les équations de ce système sont les suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \tag{1.23}$$

La figure (1.10) illustre le tracés de l'attracteur de Rössler, les paramètres sont fixés aux valeurs suivantes : $a = 0.2, b = 0.2, c = 5.7$, pour des conditions initiales $x0 =$ (0.2 2 1)

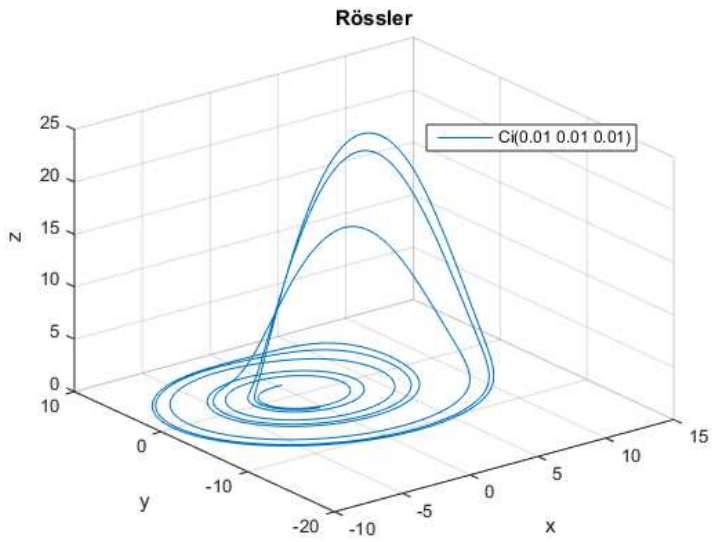


FIGURE 1.10 – Attracteur chaotique de Rössler.

1.4.2 Exemple d'un système chaotique en temps discret

Système de Lozi

La récurrence de Lozi est obtenue en remplaçant $(x)^2$ dans la récurrence du système Hénon par $\mid x \mid$et en modifiant la valeur des paramètres.

René Lozi, propose l'application suivante :

$$\begin{cases} x(k+1) = 1 - a \mid x(k) \mid + y(k) \\ y(k+1) = bx(k) \end{cases} \tag{1.24}$$

L'attracteur chaotique de Lozi est représenté sur la Figure (1.11) pour les valeurs numériques $a = 1.7$et $b = 0.5$.

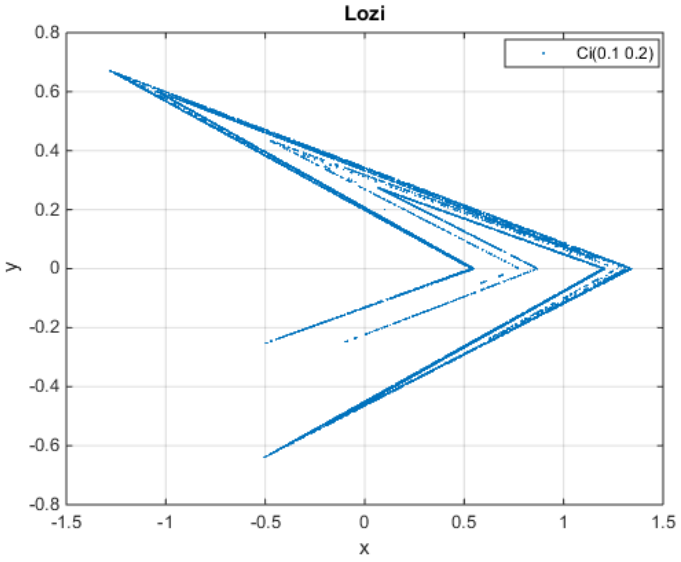


FIGURE 1.11 – Attracteur chaotique de Lozi.

1.5 Conclusion

Un système est chaotique lorsqu'il est régit par des lois déterministes mais que son évolution échappe à toute prévision à long terme. Pour un système continu sans retard et sans entrée il faut également que l'ordre n du système soit supérieur ou égale à trois. Toutefois pour un système discret on obtient le chaos à partir de deux équations. Le comportement chaotique est principalement du à sa sensibilité aux conditions initiales, il est également caractérisé par son spectre de puissance continu, sa fonction d'autocorrection qui à l'infini tend vers zéro et possède au moins un exposant de Lyapunov positif.

Ce chapitre nous a permis d'observer toutes ces caractéristiques accompagnées par divers exemples sur Matlab tel que le système de Rösseler ainsi nous avons pu constater ce qui caractérise un système chaotique des systèmes dynamiques non linéaires.

Dans le prochain chapitre nous énoncerons l'utilité et l'utilisation du comportement chaotique dans le chiffrement,pour des fins de sécurité, et de transmission de données confidentielles.

Chapitre 2

Cryptographie à base des systèmes chaotiques

2.1 Introduction

L'informatique et les technologies ne cessent de prendre de l'ampleur dans la vie personnelle et professionnelle de l'individu moderne, ce qui l'expose au danger des cybercriminalités. Afin de le protéger et de garantir sa sécurité, on recourt à des fonctions de sécurité qui doivent obéir à certaines exigences qui sont ; l'authentification, la confidentialité, l'intégrité et la non-répudiation.

La fonction de sécurité la plus répandue de nos jours, est le chiffrement, mais la plupart des algorithmes de chiffrement actuels ont déjà été cassés et sont donc devenus sans garantie.

La cryptographie chaotique est récente et a démontré une fiabilité de la sécurité tant bien qu'elle a démontré une grande résistance à la cryptanalyse.

Dans ce chapitre, nous allons montrer comment exploiter la théorie du chaos à des fins de cryptographie et de transmission sécurisée tout en citant les méthodes de chiffrement classiques et modernes et les diverses attaques de cryptanalyse.

Voici un schéma classique de transmission dont l'émetteur s'appelle Alice, partage une information avec le récepteur qui s'appelle Bob. L'information partagée entre ces deux derniers est transmise à travers un canal public de manière à ce qu'une tiers personne qu'on nommera Charlie ne pourra pas accéder a cette information.

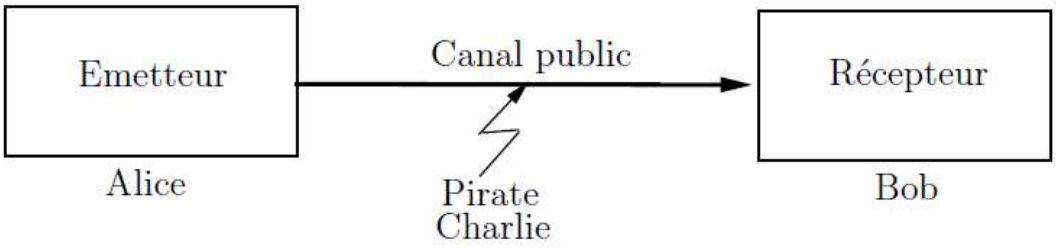


FIGURE 2.1 – Schéma de communication .

2.2 Cryptologie

La cryptologie désigne une science qui vise à mettre en pratique des techniques permettant la réalisation de communications sécurisées en présence de tiers. Elle englobe deux branches indissociables. D'une part, la cryptographie qui se consacre à créer des systèmes appelés crypto-systèmes, visant à assurer les exigences suivantes :

- Confidentialité : les données échangées ne sont disponibles qu'aux personnes autorisées.
- Authentification : les parties en présence sont bien celles qui elles prétendent être.
- Intégrité : les données échangées n'ont pas subi de modifications (volontaires ou non) .
- Non-répudiation : aucune partie ne peut à postériori nier ses actes passés.

D'autre part, la cryptanalyse, à l'inverse, consiste à trouver les moyens afin d'attaquer avec succès les crypto-systèmes.[14]

2.3 Généralités sur la cryptographie

2.3.1 Cryptographie

La cryptographie est une discipline qui traite et étudie les algorithmes et protocoles de transformations de données, servant à cacher des informations sensibles à des fins de sécurité et dans le but de les protéger des éventuelles attaques ou utilisations illégales lors d'une transmission à travers un canal publique.

Principe

Afin d'obtenir une donnée cryptée et protégée, on applique une des fonctions de chiffrement sur la donnée qu'on désignera par « message », une fois que le message a été crypté on obtient un message chiffré.

2.3.2 Notions sur le chiffrement

1. *Stéganographie* : contrairement à la cryptographie, la stéganographie consiste à noyer le message dans un autre et seuls certains mots doivent être lus pour découvrir le texte caché.
2. *Chiffrer* : consiste a transformer un message clair, en un message chiffré en lui appliquant une fonction de chiffrement.
3. *Déchiffrer* : représente l'opération inverse de chiffrement, elle consiste à traduire le message codé en message clair en possédant la clé ou la fonction de déchiffrement.
4. *Décrypter* : consiste à traduire le message codé en message clair sans posséder la clé ou la fonction de déchiffrement.
5. *Message clair* : désigne le message avant d'être chiffré.
6. *Message chiffré* : appelé également cryptogramme, désigne le message après chiffrement.
7. *Crypto-système* : il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.
8. *Clé* : représente les paramètres impliqués et autorisant des opérations de chiffrement et/ou de déchiffrement.

2.3.3 Transmission de données

La transmission de données caractérise une communication d'un signal porteur d'informations, établie entre un émetteur et un récepteur par l'intermédiaire d'un canal de transmission.

2.3.4 Cryptographie dans la transmission sécurisée

Pour pouvoir échanger une information(un message) ; qui peut être un texte, une image ou un son, d'une entité « A » qui est « l'émetteur » vers une entité « B » : « Le récepteur » en toute sécurité, le message est chiffré au niveau de l'émetteur à l'aide d'une fonction de chiffrement (Fc) puis transmis à travers un canal de transmission, vers le récepteur qui, lui seul doit connaitre comment déchiffrer le message en détenant la fonction de déchiffrement (Fd) pour obtenir le message clair, et il existe plusieurs méthodes de chiffrement .

2.4 Méthodes de chiffrement

les méthodes de chiffrement sont classés en deux types, le chiffrement classique qui traite des systèmes reposant sur les lettres et caractères d'une langue quelconque. Ses principaux outils utilisés remplacent des caractères par d'autres et les transposent dans

des ordres différents, avec de différents degrés de difficulté, en revanche le chiffrement moderne utilise des méthodes plus complexes, appelées : « algorithmes » en raison de l'apparition des ordinateurs et il opère directement sur des bits.

2.4.1 Chiffrement classique

chiffrement par substitution

Le chiffrement par substitution consiste à substituer chaque caractère du message clair par un autre caractère, et pour que le récepteur puisse le déchiffrer, il lui faudra appliquer la substitution en inverser, la complexité des systèmes à substitutions dépend de trois facteurs :

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer.
- le nombre d'alphabets utilisés dans le cryptogramme.
- la manière spécifique dont ils sont utilisés.

Et on distingue quatre types de chiffrement par substitution :

– Substitutions mono-alphabétiques : consistent à remplacer chaque lettre du message clair par une autre lettre ou caractère.

– Substitutions poly-alphabétiques : opèrent en remplaçant chaque lettre du message clair par plusieurs caractères ou plusieurs lettres à la fois.

– Substitutions polygrammiques : contrairement aux autres types de substitutions, celles-ci consistent à chiffrer les lettres par groupes et non séparément.

– Substitutions tomographiques : opèrent d'abord par substitutions poly-alphabétiques en remplaçant chaque lettre par plusieurs lettres où symboles puis ensuite elles sont chiffrées séparément par substitution ou transposition.

Exemple : le chiffrement de César

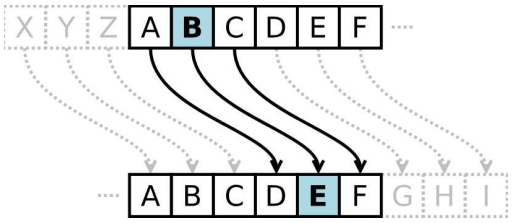


FIGURE 2.2 – Décalage de César .

Le chiffrement de César est la méthode de cryptographie la plus ancienne. Il consiste en une substitution mono-alphabétique, le principe est de décaler l'alphabet clair. Le décalage est la clé du chiffrement.

Pour cette exemple on utilise un décalage de 3, on obtient :

Message clair : Merci pour notre promoteur Monsieur DJENNOUNE

Message chiffré : PHUFL SRXUQ RWUHS URPRW HXUPR QVLHX UGMHQ QRXQH

Chiffrement par transposition

Le principe du chiffrement par transposition repose sur la permutation des caractères,par conséquent le message chiffré diffère du message clair dans l'ordre des caractères et on peut citer plusieurs types de chiffrement par transposition :

- Transposition simple par colonnes : consiste à écrire le message horizontalement sur une matrice prédéfinie, puis pour obtenir le message chiffré on extrait les phrases verticalement.
- Transposition complexe par colonnes : un mot clé secret (avec uniquement des caractères différents) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet. Une fois que le séquence de transposition est obtenue, on chiffre en écrivant d'abord le message par lignes dans un rectangle, puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence.
- Transposition par carré polybique : un mot-clé secret est utilisé pour construire un alphabet dans un tableau.Les coordonnées des lignes et des colonnes correspondant aux lettres du texte à chiffrer sont utilisés pour transcrire le message en chiffres. Avec ce procédé chaque lettre du texte en clair est représentée par deux chiffres écrit verticalement. Ces deux coordonnées sont ensuite transposées en les recombinant par deux sur la ligne ainsi obtenue.

2.4.2 Chiffrement moderne

2.4.2.1 La cryptographie à clé secrète (symétrique)

Le cryptage symétrique est une forme de crypto-système,également appelé cryptage conventionnel ou chiffrement à clé secrète. Il est caractérisé par l'utilisation d'une même clé pour le chiffrement et pour le déchiffrement, qui est choisie préalablement par l'émetteur et le récepteur et qui doit être gardée secrète, car la sécurité de ces algorithmes repose sur cette clé.

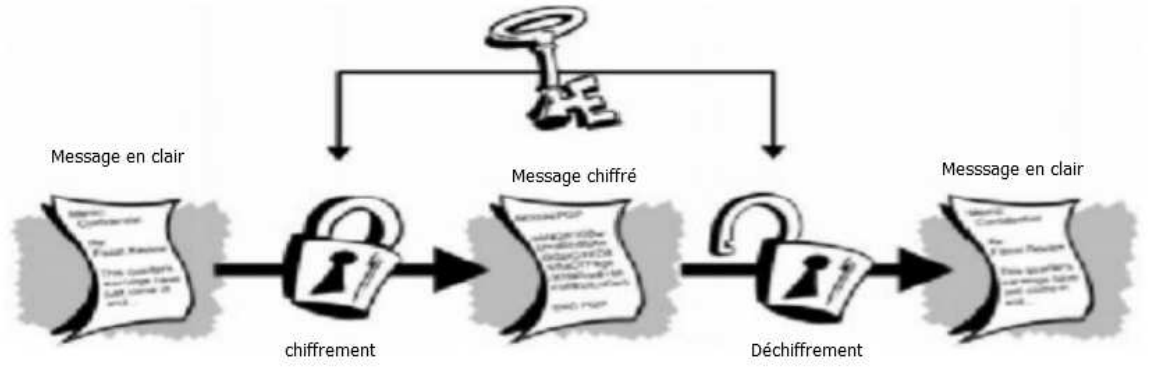


FIGURE 2.3 – schéma du chiffrement symétrique.

Le principal problème du chiffrement symétrique est de maintenir le secret de la clé donc le choix et la transmission de la clé doivent se faire de manière sécurisée. Le second problème apparait lorsque un grand nombre de personnes désirent communiquer ensemble, par conséquent le nombre de clés augmente (pour chaque couple de communicants). Ceci engendre le problème de gestion de clés .

Par exemple :
Dans un réseau de N entités susceptibles de communiquer secrètement, il faut distribuer $N(N-1)/2$ clés.

Il existe deux classes de chiffrement à clé symétrique qui sont généralement distinguées : chiffrement par blocs et chiffrement par flux. [15]

Et les deux crypto-systèmes symétriques les plus utilisés en pratique sont les DES et AES.

•Chiffrement par blocs

Le chiffrement par bloc est le découpage des données en blocs de taille généralement fixe. Les blocs sont ensuite chiffrés les uns après les autres. La taille des blocs a un impact sur la sécurité et sur la complexité : les blocs de grande dimension sont plus sécuritaires mais plus lourds à implémenter. Ils utilisent une clé assez longue parce qu'elles sont moins couteuses. [15]

Le chiffrement par blocs peut être utilisé pour obtenir le même effet qu'un chiffrement par flux. Mathématiquement le chiffrement par flux est plus facile à analyser. La grande majorité des applications cryptographiques symétriques basées sur le réseau utilisent des chiffrements de blocs.

L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire.
2. Découper cette chaine en blocs de longueur donnée.
3. Chiffrer un bloc en l'additionnant bit par bit à une clé.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.Appelé une ronde.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

•Chiffrement par flux

Un chiffrement de flux est un chiffrement qui crypte un flux de données numériques d'un bit ou d'un octet (plutôt petit) à la fois. Leurs avantages principaux surgissent du fait que la transformation (méthode de chiffrement) peut être changée à chaque symbole du texte clair et du fait qu'ils soient très rapides. De plus,ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs.

Si le flux de clé cryptographique est aléatoire, alors ce chiffre est incassable par tout signifie autre que l'acquisition du flux de clé. Cependant,le flux de clé doit être fourni aux deux utilisateurs à l'avance via un canal indépendant et sécurisé. Cela introduit des problèmes logistiques insurmontables si le trafic de données prévu est très important.

En conséquence, pour des raisons pratiques, le générateur de flux binaire doit être mis en œuvre comme une procédure algorithmique, de sorte que le flux de bits cryptographique peut être produit par les deux utilisateurs.

La structure d'un chiffrement par stream repose sur un générateur de clés qui produit une séquence de clés K_1, K_2, ..., K_i. La sécurité du chiffrement dépend de la qualité du générateur : si $K_i = 0$ pour tout i, $M = C$. Mais si la séquence des clés K_i est infinie et complètement aléatoire, on obtient un One-Time-Pad.En pratique, on se situe entre les deux,c'est-à-dire une séquence pseudo-aléatoire. En termes de propagation d'erreur,une erreur dans C_i n'affecte qu'un bit de Mi.La perte ou l'ajout d'un bit de C_i affecte tous les bits suivants de M après déchiffrement. Le générateur de clés peut être considéré comme une machine à états finis. Un exemple de ce type de générateur est le FSR .[16]

La figure (2.4) représente le chiffrement de flux.

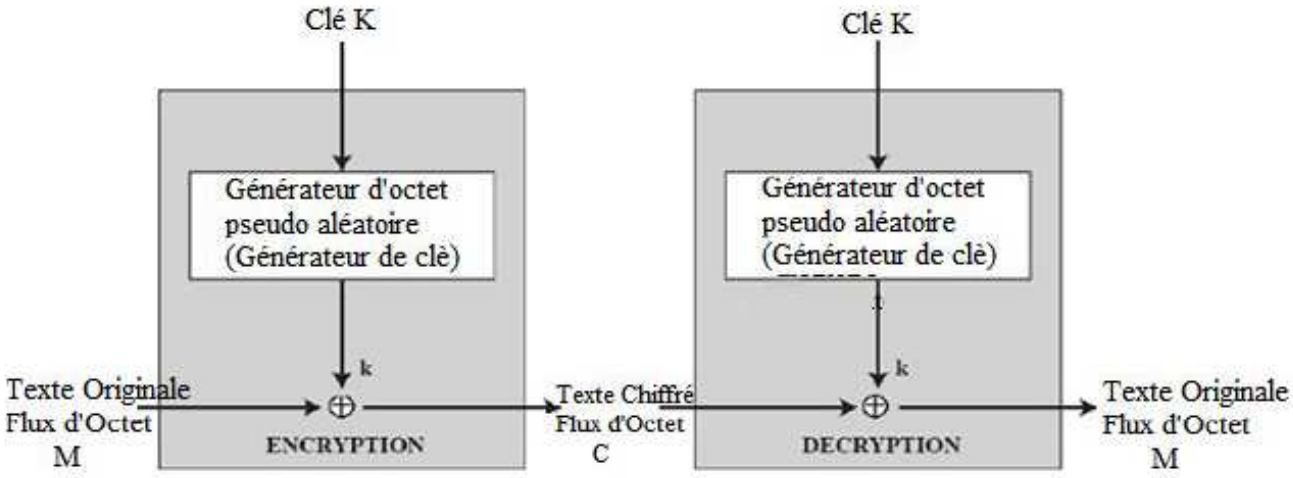


FIGURE 2.4 – Schéma de chiffrement par flux .

•Exemples de protocoles de chiffrement à clé secrète

Algorithme de chiffrement DES

Le DES utilise une clé K de 56 bits, pour chiffrer des blocs de 64 bits, on va obtenir le même bloc chiffres 64 bits.La clé sert donc à la fois pour chiffrer et pour déchiffrer le message. Le bloc de texte clair subit d'abord une permutation initiale. Puis on itère 16 fois une procédure identique, ou la moitié droite est recopiée telle quelle à gauche, et la moitié gauche est transmise à droite en subissant au passage une modification dépendante de la clé. A la fin,on inverse les moitiés gauches et droites (ou bien, comme sur les schémas, on supprime le croisement de la dernière étape), et on applique l'inverse de la permutation

initiale pour obtenir le bloc chiffré. Ces clés sont les mêmes quel que soit le bloc qu'on code dans un message. Cet algorithme est relativement facile à réaliser matériellement et certaines puces chiffrent jusqu'à 1 Go de données par seconde [16]

Quelques avantages de l'algorithme DES :

- Il possède un haut niveau de sécurité.
- Il est complètement spécifié et facile à comprendre rapide et exportable.
- La sécurité est indépendante de l'algorithme lui-même .
- Il repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement, facile à implémenter.

La figure (2.5) représente le chiffrement DES.

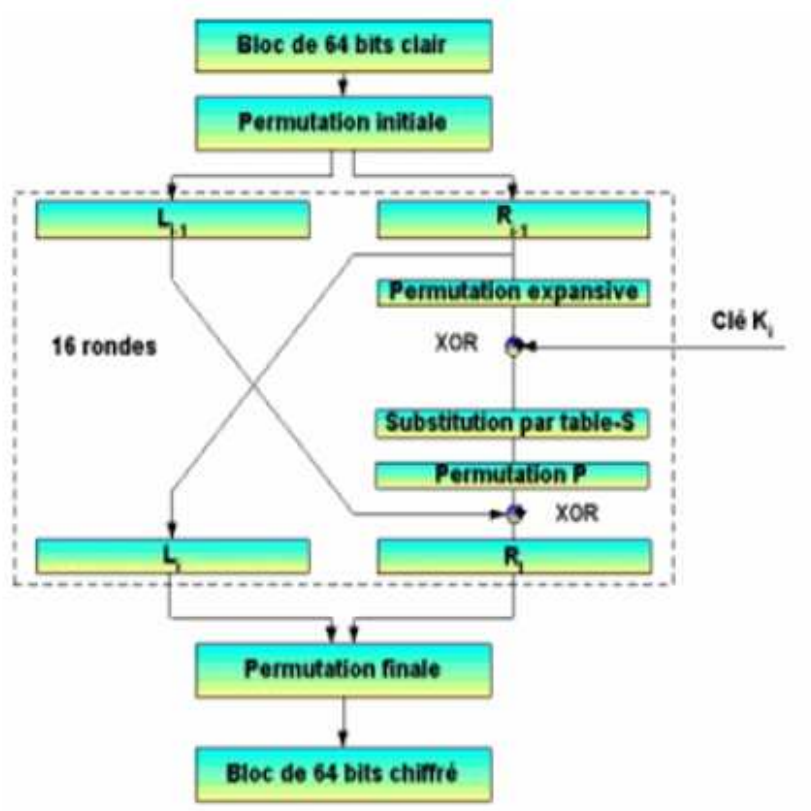


FIGURE 2.5 – Schéma du chiffrement DES.

Algorithme de chiffrement AES

L'Advanced Encryption Standard (AES), aussi connu sous le nom de Rijndael a été publié par l'Institut national de Standards and Technology (NIST) en 2001.AES est un chiffrement par blocs symétrique destiné à remplacer le DES comme norme approuvée pour un large éventail d'applications. Le chiffre prend une taille de bloc en clair de 128 bits ou 16 octets. La longueur de la clé peut être 16, 24 ou 32 octets (128, 192 ou 256 bits). L'algorithme est appelé AES-128,AES-192 ou AES-256, en fonction de la longueur de la clé.

Il possède les propriétés suivantes : [16]

- Plusieurs longueurs de clé et de bloc sont possibles : 128, 192, ou 256 bits.
- Le nombre de cycles ("rondes") varie en fonction de la longueur des blocs et des clés (de 10 à 14) .
- Il est beaucoup plus performant que le DES.
- Il est facilement adaptable à des processeurs de 8 ou de 64 bits .
- Le parallélisme peut être implémenté .

2.4.2.2 Cryptographie à clé publique (asymétrique)

La cryptographie asymétrique à clé publique est apparue pour la première fois en 1976 avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman.

La cryptographie à clé publique utilise une paire de clés, une clé publique pour le chiffrement et une autre clé secrète pour le déchiffrement.

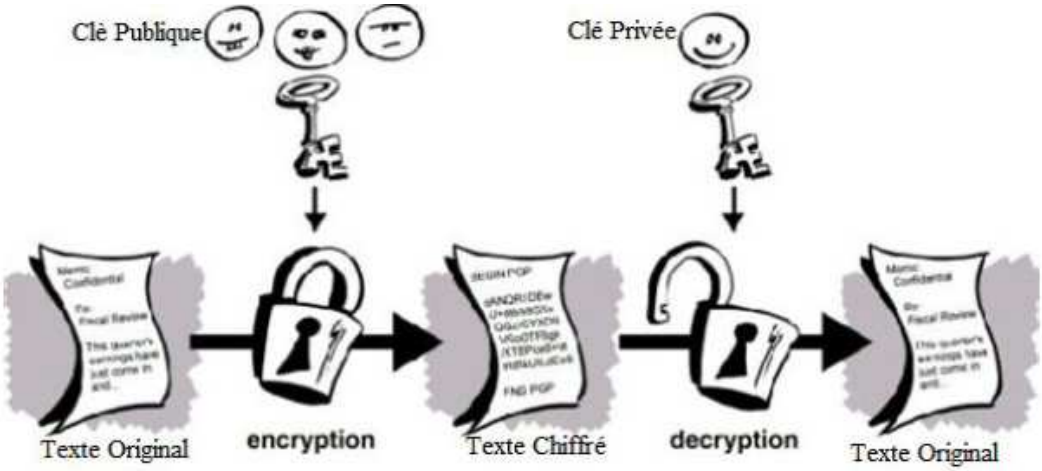


FIGURE 2.6 – Schéma du chiffrement asymétrique.

Avec le chiffrement asymétrique, on choisit une clé aléatoire (clé privée), à partir de cette clé et en appliquant la fonction à sens unique, on déduit la clé publique qu'on transmet à travers un canal non sécurisé.

Lorsqu'une personne désire lui envoyer un message, il lui suffit de chiffrer le message à l'aide de la clé publique. Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privé.

Ce système est basé sur une fonction facile à calculer dans un sens (appelé fonction à trappe à sens unique) et mathématiquement très difficile à inverser sans la clé privée appelé trappe.[15]

Les principaux algorithmes asymétriques à clé publique les plus utilisés sont :
- RSA .
- DSA .
- Diffie-Hellman .

•Exemples de protocoles de chiffrement à clé secrète

L'algorithme RSA

RSA est le premier système à clé publique solide à avoir été inventé, et le plus utilisé en pratique. Publié en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman de l'Institution de technologie du Massachusetts. Le fonctionnement du crypto-système RSA est basé sur la difficulté de factoriser de grands entiers.[16]

Création des clés :
- Génération de deux nombres premiers distincts, p, q.(+-100 chiffres).
- Calculer leur produit n = p · q, appelé module de chiffrement.
- Calculer $\emptyset(n)$ = (p − 1) · (q − 1). (c'est la valeur de l'indicatrice d'Euler en n).
- Déterminer un entier naturel e premier avec $\emptyset(n)$ tel que : 1 < e <$\emptyset(n)$ et gcd (e, $\emptyset(n)$) = 1, appelé exposant de chiffrement.
- Calculer l'entier naturel d, tel que e ∗ d ≡ 1 mod $\emptyset(n)$.
- (e,n) est la clé publique .
- (d,n) est la clé privée.
- p et q doivent rester secrets.

Chiffrement : le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :

$$C = M^e mod n \tag{2.1}$$

Déchiffrement : il s'agit de calculer la fonction réciproque

$$M = C^d mod n \tag{2.2}$$

tel que :

$$e.d = 1 mod[(p-1)(q-1)] \tag{2.3}$$

2.5 Cryptographie Chaotique

Principe

La cryptographie chaotique est l'une des alternatives développées durant cette dernière décennie. Elle répond non seulement aux exigences de la sécurité mais elle a démontré

une grande résistance à la cryptanalyse, comme elle est parfaitement combinée avec le maintien des attributs nécessaires aux algorithmes de chiffrement.Sachant qu'il y a deux types de fonctions chaotiques, part celles qui ont un comportement purement chaotique et qui ne sont pas modélisables, et d'autre part les fonctions chaotiques déterministes qui sont modélisables par des systèmes d'équations qu'on nomme « systèmes dynamiques non linéaires », et ce sont ces dernières qui sont utilisées dans le chiffrement chaotique car leurs attracteurs sont sous forme fractale et rendent l'évolution des trajectoires totalement dépendantes des conditions initiales, et il est donc impossible de prédire ces trajectoires sans connaitre leurs états initiaux, ce qui rend le comportement chaotique imprévisible, et leur sécurité quasi totale.Et pour les introduire dans le chiffrement il faut d'abord choisir une fonction chaotique, ensuite il faut superposer le signal chaotique au flux de données à transmettre selon l'une des techniques choisies pour le cryptage par chaos.

2.6 Techniques de cryptage par chaos

2.6.1 Cryptage par addition

Chronologiquement, cette méthode est la première à utiliser la synchronisation du chaos.L'idée repose sur l'observation des signaux chaotiques.Le principe est d'ajouter le message utile $m(t)$ au signal chaotique $C_x(t)$ et de le récupérer ensuite par la synchronisation chaotique a travers le canal de transmission qui est un canal public. Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $y(t)$ (porteuse chaotique + message), et donc ne cherchera pas à appliquer des techniques de décryptage. Au niveau du récepteur autorisé, ainsi, après la synchronisation grâce au signal reçu, le message original est extrait à l'aide d'une opération de soustraction.[11]

La figure (2.7) illustre la méthode de cryptage par addition.

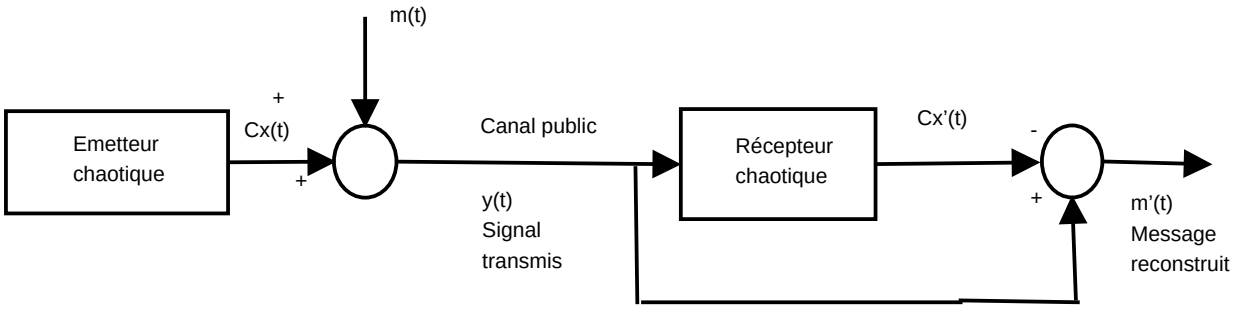


FIGURE 2.7 – Cryptage par addition.

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets.

Le message original doit être au moins de 20 a 30dB inférieur à la sortie de l'émetteur $y(t)$ (la porteuse chaotique plus le message) pour ne pas perturber l'établissement de la

synchronisation au niveau du récepteur, et pour préserver le secret de la transmission, un autre problème qui se pose naturellement, concerne la présence d'un bruit additif au niveau du canal de transmission d'une puissance proche de celle du message, et il revient difficile de détecter l'information. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit.

2.6.2 Cryptage par modulation paramétrique

Cette technique utilise le message contenant l'information pour moduler un paramètre de L'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté sur la figure (2.8).

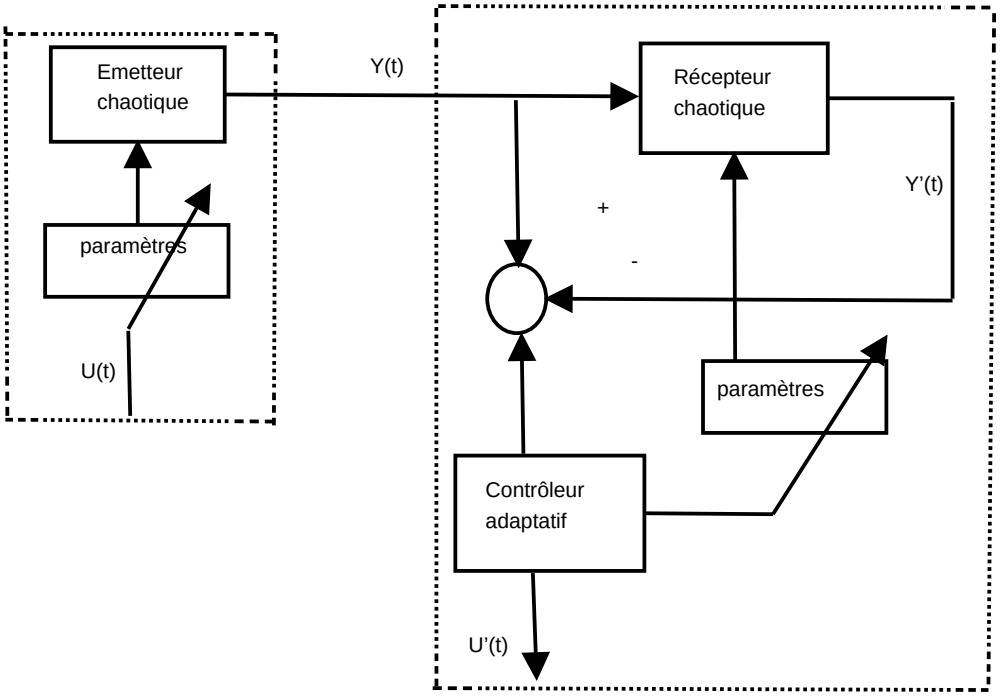


FIGURE 2.8 – Cryptage par modulation paramétrique.

Au niveau de l'émetteur, le fait de moduler un ou plusieurs paramètres impose à la trajectoire de changer continuellement d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques.[17]

Elle n'a pas d'équivalents parmi les systèmes de communication classique. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques.

2.6.3 Cryptage par commutation

Cette technique (en anglais Chaos Shift Keying, CSK) est fondamentalement un cas particulier de la technique de modulation paramétrique pour transmettre un message $m(t)$ numérique sécurisé sur un canal de communication. Dans cette méthode, en fonction de 0 ou 1 à transmettre. L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message, ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents ou avoir deux modèles dynamiques totalement différents. Le fonctionnement c'est selon la valeur de m à l'instant t (c'est –à-dire $m(t) = 0$ ou $m(t) = 1$). L'un des systèmes chaotique (1ou 2) envoie sa sortie $y(t)$ sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges. Le récepteur est constitué de deux systèmes chaotiques ($1'$ et $2'$) identiques à ceux de l'émetteur de sorties respectives $y1'(t)$ et $y2'(t)$. Si $m(t)$ prend la valeur 0, alors le système chaotique $1'$ se synchronise, et le système chaotique $2'$ ne se synchronise pas. Ainsi, l'erreur de synchronisation $e1(t) = y1'(t) - y(t)$ va tendre vers 0, tandis que l'erreur $e2(t) = y2'(t) - y(t)$ sera d'amplitude non nulle. Le processus est symétrique lorsque le message prend la valeur 1.[5]

La figure (2.9) illustre la méthode de cryptage par commutation.

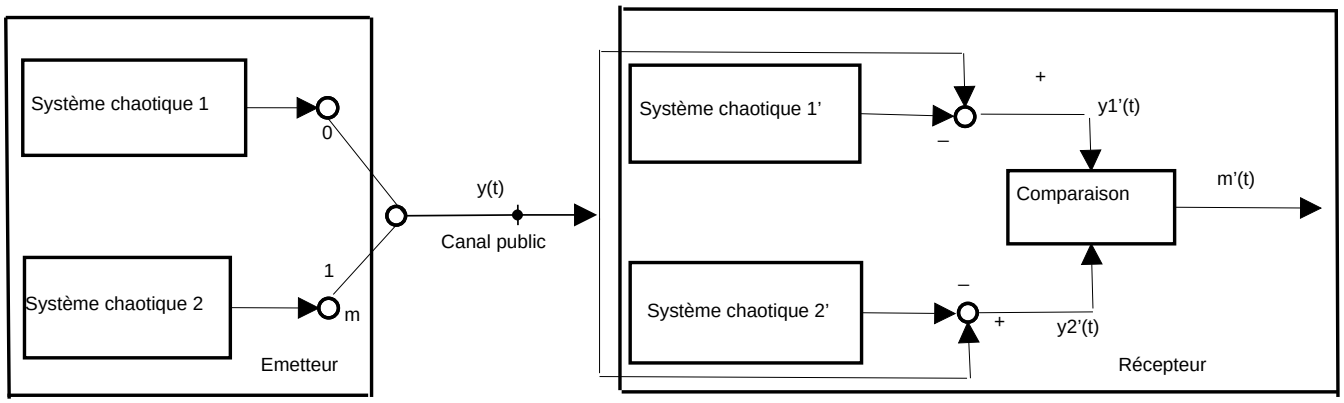


FIGURE 2.9 – Cryptage par commutation.

Cette méthode a l'énorme avantage d'être robuste au bruit : en effet, au niveau du récepteur, on détermine la valeur exacte du message soit en évaluant l'erreur de synchronisation au niveau des deux systèmes chaotiques ($1'$ et $2'$) , soit par corrélation entre le signal $y(t)$ reçu et les signaux $y1'(t)$ et $y2'(t)$.

2.6.4 Cryptage par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur chaotique comme étant une entrée, sans toutefois réaliser une modulation de paramètres, la récupération du message devient alors un problème d'entrée inconnue dans le cas de la théorie du contrôle où les observateurs sont utilisés, dont le système doit satisfaire la condition d'observabilité ainsi que la propriété d'inversion à gauche.

Par conséquent la restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur.Ainsi elle présente beaucoup d'avantages et reste très utilisée en pratique.[5]

2.6.4.1 Observateurs à entrées inconnues

Le schéma de la figure (2.10) illustre un problème classique d'estimation d'état non linéaire à entrées inconnues :

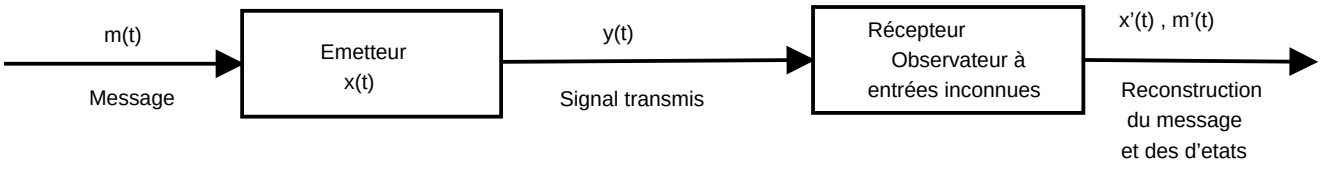


FIGURE 2.10 – Observateur à entrée inconnue

Il faut reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $m(t)$. Différentes techniques de synthèse d'observateurs à entrées inconnues ont été utilisées dans la littérature, et peuvent être utilisées à des fins de décryptage. Parmi les articles utilisant ces types d'observateurs pour décrypter l'information.

2.6.4.2 Décryptage par inversion

Cette technique de cryptage par inclusion consiste à inverser le modèle de l'émetteur afin d'obtenir le récepteur.

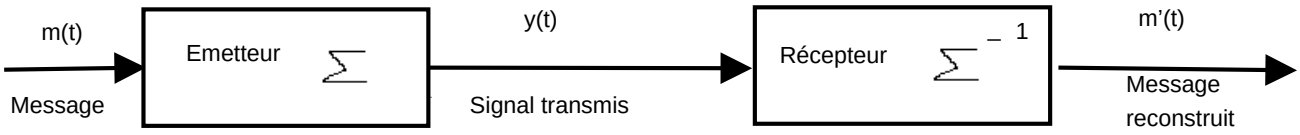


FIGURE 2.11 – Décryptage par inversion

2.7 Cryptanalyse et attaques sur les systèmes cryptographiques

Cryptanalyse

La cryptanalyse est la science qui teste la fiabilité d'une méthode de chiffrement en

estimant les faiblesses des systèmes cryptographiques. Elle consiste à déchiffrer un message chiffré sans posséder la fonction de déchiffrement ou la clé, et le processus par lequel elle procède est appelée « attaque ».

2.7.1 Hypothèse de Kerckhoff

La cryptanalyse des schémas de cryptage peut être effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale, connue sous le nom de principe de kerckhoff est que l'adversaire connait complètement l'algorithme de cryptage,à l'exception de la clé secrète qui est inconnue. Il serait risqué de se baser sur le secret des mécanismes utilisés pour assurer la sécurité d'un système alors que le plus important c'est de garder la clé secrète. Il en existe différents types d'attaques cryptanalytiques, l'objectif est le même c'est de retrouver le texte clair à partir du texte chiffré ou de déduire la clé secrète.

Et il existe plusieurs catégories d'attaques selon la nature de données qu'elle nécessite.

2.7.2 Différentes classes d'attaques

– Attaque sur le texte chiffré uniquement (ciphertext only attack) [18] :
L'attaquant a connaissance du texte chiffré il va essayer de trouver le texte clair et/ou la clé secrète, pour ce la on procède par analyse de fréquence des lettres utilisées dans le texte chiffré, mais il ne fonctionne que pour la plupart des chiffrement classiques basiques.

– Attaque à texte en clair connu (known plaintext attack) :
Le cryptanalyste connait non seulement les messages chiffrés mais aussi les messages en clair correspondants. Alors on cherche à trouver comment les clés ont été utilisées, pour déchiffrer n'importe quel nouveau message chiffré avec la même clé .

– Attaque à texte en clair choisi (chosen plaintext attack) :
Le cryptanalyste a accès aux textes chiffrés et aux textes en clair, il choisit une séquence du texte clair et analyse la séquence correspondante du texte chiffré. Cette attaque est plus efficace que l'attaque à texte en clair connu, car le cryptanalyste peut choisir des textes en clair qui donneront plus d'information sur la clé.

– Attaque adaptative à texte en clair choisi (adaptive chosen plaintext attack) :
C'est une attaque à texte en clair choisi où le choix du texte clair peut dépendre du texte chiffré reçu précédemment (il choisit un bloc initial plus petit et ensuit il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite).

– Attaque sur le texte chiffré choisi (chosen ciphertext attack) :
C'est l'inverse de l'attaque à texte en clair choisi, il choisit une séquence du texte chiffré et analyse la séquence correspondante du texte clair, cette attaque est utilisé contre les systèmes à clé publique pour trouver la clé privée.

– Attaque adaptative à texte en chiffré choisi (adaptive chosen ciphertext attack) :

C'est une attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte en clair reçu précédemment .

– Attaque exhaustive ou attaque par force brute (brute force attack) :
L'adversaire teste toutes les clés possibles de manière exhaustive jusqu'à l'obtention d'un texte clair. Cette attaque est la plus couteuse en terme de calcul et en mémoire à cause de la recherche exhaustive. Plus la possibilités de tester les clés augmentes, plus la probabilité de trouver la clé sera faible et l'attaque couteuse.

2.8 Conclusion

Le cryptage et la communication sécurisée est l'un des champs d'applications prometteur des systèmes chaotiques, en effet la cryptographie chaotique peut s'effectuer sous différents schémas, il s'agit de définir la façon d'introduire le message dans l'émetteur.

Dans ce chapitre nous avons introduit des notions sur la cryptographie et la transmission de données accompagnées des méthodes de chiffrement à clé privé et à clé public, ainsi que le chiffrement à base du chaos qui utilise les propriétés d'un comportement chaotique pour la transmission de données confidentielles.

Une fois que la fonction de chiffrement chaotique est choisie, le problème de la synchronisation du récepteur avec l'émetteur s'impose, ce dernier sera l'objet d'étude du prochain chapitre.

Chapitre 3

Synchronisation des systèmes chaotiques

3.1 Introduction

Les fonctions chaotiques possèdent de nombreuses utilisations potentielles, parmi ces utilisations, on cite la cryptographie. En effet l'utilisation du chaos dans les réseaux de communications a permis de renforcer la sécurité de la transmission des données,pour cela il faut veiller à choisir la fonction de chiffrement adéquate, ensuite à superposer le signal chaotique au flux de données à transmettre, comme il a été cité dans le deuxième chapitre. En revanche la plus grande difficulté réside dans la synchronisation des deux interlocuteurs (l'émetteur et le récepteur), en effet à première vue l'aspect aléatoire du chaos pousse à croire que cela est impossible mais en 1990, L.M Pecora et T.L. Carroll [3], ont réussi à synchroniser deux systèmes chaotiques identiques. Depuis, plusieurs méthodes de synchronisations aux comportements chaotiques ont vu le jour, ainsi que les applications du chaos aux communications sécurisées.

Ce chapitre énonce le principe de la synchronisation chaotique, ainsi que les différentes méthodes les plus répandues.

3.2 Définition

La synchronisation caractérise deux systèmes se comportant de la même façon en même temps, et signifie que chaque système évolue en suivant le comportement de l'autre système.

3.3 Principe de la synchronisation chaotique

Lorsque un message m(t) est injecté à l'entrée d'un émetteur chaotique, celui-ci génère un signal y(t) qui est transmis au récepteur par l'intermédiaire d'un canal. Le récepteur doit donc se charger de récupérer l'information en effectuant l'opération inverse de l'émetteur, il est donc nécessaire de synchroniser les deux systèmes a fin de reconstruire l'information exacte.

En conséquence, la synchronisation consiste principalement à raccorder l'émetteur et le récepteur d'une manière à restituer l'information telle quelle.

La figure (3.1) illustre le principe de la communication chaotique.

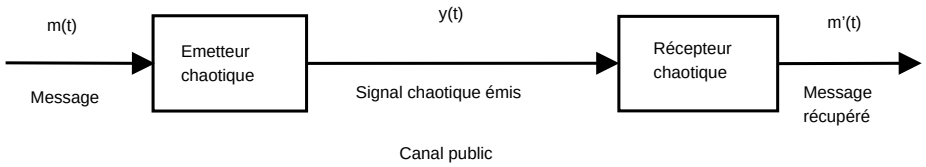


FIGURE 3.1 – Principe de la communication chaotique.

Si on suppose que l'on dispose de deux systèmes chaotiques identiques, le problème qui se pose est la sensibilité aux conditions initiales qui se traduit par une instabilité au sens de Lyapunov, et qui conduit à des signaux totalement différents. Cela signifie qu'il est impossible de reproduire ces conditions initiales dans un système réel.

En 1990, Pecora et Caroll [3] ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés de façon à placer l'émetteur en maître du récepteur afin qu'il force la synchronisation du récepteur en esclave, comme le montre la figure (3.2).

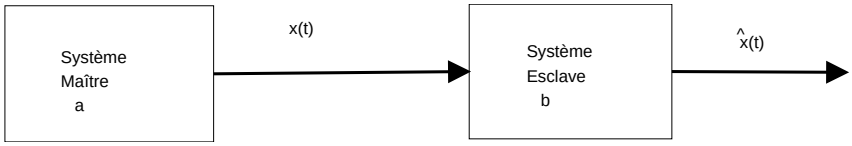


FIGURE 3.2 – Système maître-esclave pour réaliser la synchronisation.

Le système (a) qui est dit maître (émetteur) peut être décrit par [19] :

– Un système différentiel dans le cas continu : (une équation différentielle)

$$\dot{x}(t) = f(x(t)) \tag{3.1}$$

– Une équation aux différences dans le cas discret :

$$x(k+1) = f(x(k)) \tag{3.2}$$

avec le vecteur d'état $x \in \mathbb{R}^n$, la condition initiale $x(0)$ et une sortie $y = h(x)$.

Et le système (b) qui est dit esclave (récepteur) est défini par :

– Un système différentiel dans le continu donné par :

$$\dot{\hat{x}}(t) = \hat{f}(\hat{x}(t), y(t)) \tag{3.3}$$

– Une équation aux différences dans le cas discret :

$$\hat{x}(k+1) = \hat{f}(\hat{x}(k), y(k)) \tag{3.4}$$

avec le vecteur d'état $\hat{x} \in \mathbb{R}^n$ et la condition initiale $\hat{x}(0)$.

Le système esclave est synchronisé avec le système maître dans le cas continu comme dans le cas discret si :

$$lim_{t\to\infty} \parallel x(t) - \hat{x}(t) \parallel = 0 \tag{3.5}$$

Pour tout $(x(0), \hat{x}(0)) \in \mathbb{R}^n \times \mathbb{R}^n$, $x(0) \neq \hat{x}(0)$ Ce type de synchronisation est appelé synchronisation d'état.

3.4 Types de synchronisation

La synchronisation est classée en deux types en fonction de la manière avec laquelle deux systèmes chaotiques sont couplés.

3.4.1 Synchronisation unidirectionnelle

Dans la synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens.

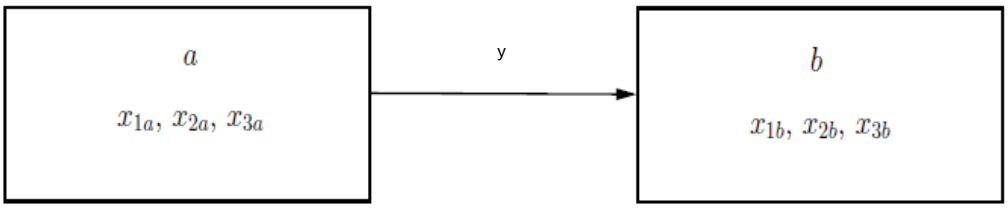


FIGURE 3.3 – Schéma de couplage unidirectionnel.

3.4.2 Synchronisation bidirectionnelle

Dans la synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans les deux sens.

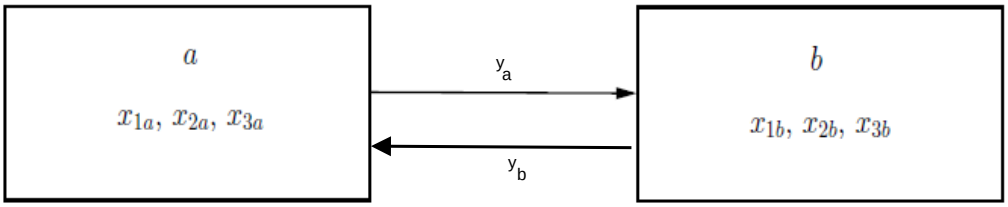


FIGURE 3.4 – Schéma de couplage bidirectionnel.

3.5 Méthodes de synchronisation

Il y a plusieurs méthodes de synchronisations. Dans ce qui suit nous allons citer les méthodes les plus performantes et les plus rencontrées.

3.5.1 Synchronisation par répartition du système

Certains systèmes chaotiques possèdent la propriété d'auto-synchronisation,c'est-à-dire qu'on peut les décomposer en deux sous-systèmes, l'un maître, l'autre esclave. Ces derniers peuvent se synchroniser sous l'effet d'un couplage avec un signal commun. Dans le schéma de synchronisation proposé par Pecora et Carroll[3], un système chaotique représente par (3.6).[19]

$$\dot{x} = f(x) \tag{3.6}$$

Avec $y = h(x)$ comme sortie, est décomposée en deux sous-systèmes dont les états sont $x_1$etx_2 respectivement :

$$\dot{x}_1 = f_1(x_1, x_2) \tag{3.7}$$

$$\dot{x}_2 = f_2(x_2, y) \tag{3.8}$$

Où

$$x = \begin{bmatrix} x_1^T & x_2^T \end{bmatrix}^T \tag{3.9}$$

Le système est partitionné de façon à ce que les exposants de Lyapunov conditionnels du sous-système (3.8) soient négatifs.

Si tous les exposants de Lyapunov conditionnels sont négatifs, alors la trajectoire $x_2(t)$ est asymptotiquement stable. Ceci signifie que les états de plusieurs copies du sous-système (3.8) se synchroniseront à l'aide du même signal $y(t)$.

En particulier,on considère le système décrit par :

$$\dot{\hat{x}}_2 = f_2(\hat{x}_2, y) \tag{3.10}$$

Si les exposants de Lyapunov conditionnels de ce système sont tous négatifs et $\hat{x}_2(0)$ est suffisamment proche de $x_2(0)$,alors l'état $\hat{x}_2$converge asymptotiquement vers x_2, i.e :

$$lim_{t\to\infty} \parallel x_2(t) - \hat{x}_2(t) \parallel = 0 \tag{3.11}$$

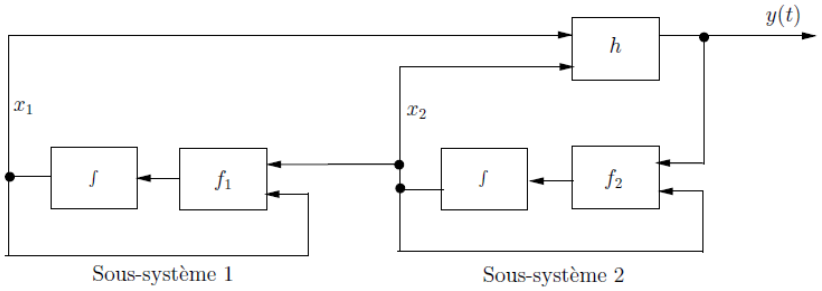


FIGURE 3.5 – Principe de synchronisation de Pecora et Carroll.

3.5.2 Synchronisation par boucle fermée

On l'appelle aussi « méthode de synchronisation par contre réaction » elle consiste à utiliser l'erreur entre l'émetteur et le récepteur pour corriger le comportement du récepteur afin de réaliser la synchronisation.

Supposons les deux systèmes suivants [20] :

Émetteur :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{3.12}$$

Récepteur :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \tag{3.13}$$

Avec g est une fonction de l'erreur entre y et $\hat{y}$,g est choisie afin de garantir la synchronisation entre l'émetteur et le récepteur.

Ce type de récepteur peut être considéré comme la conception d'un observateur. La figure(3.6) illustre la synchronisation par la boucle fermée.

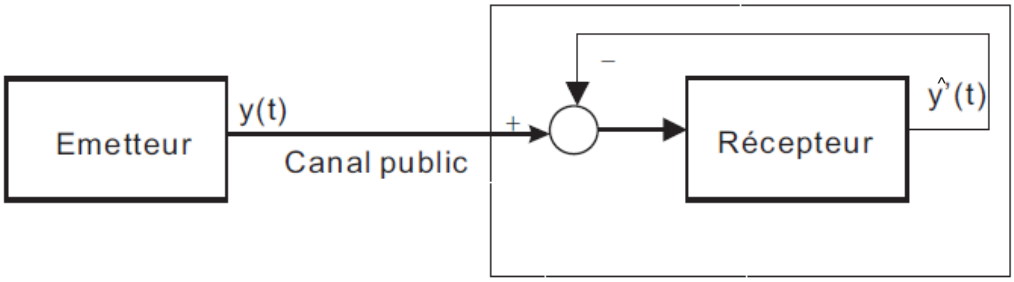


FIGURE 3.6 – La synchronisation par la boucle fermée.

3.5.3 Synchronisation impulsive

Dans un schéma de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation par le récepteur, et dans le but de réduire la redondance du signal transmis, la synchronisation impulsive a été proposée [20]. Elle est réalisée en divisant le signal de transmission en petits intervalles (ou impulsions).

$$\dot{x} = f(x) \tag{3.14}$$

$$y(t) = C_x(t) \tag{3.15}$$

Le signal de sortie (3.15) du système maître de la forme (3.14) est envoyé au système esclave sous forme d'impulsions aux instants discrets prédéfinis dont les variables d'état subissent un saut et un changement d'état. Son schéma est illustré par la figure (3.7)

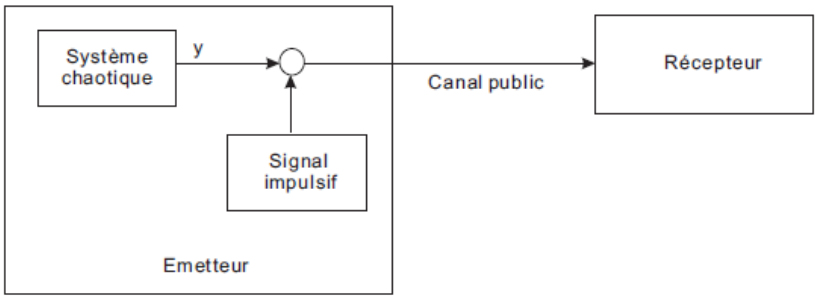


FIGURE 3.7 – Synchronisation impulsive.

3.5.4 Synchronisation par inversion du système

Jusqu'à présent, toutes les approches mentionnées ont pour but de synchroniser seulement les états du système, et elles ne concernent pas l'estimation des entrées inconnues du système. Cependant, la possibilité d'estimer les entrées inconnues est évidemment essentielle à la transmission chaotique de données puisque l'entrée inconnue est généralement le message confidentiel.

Soit la figure (3.8), où l'émetteur peut être écrit de la façon suivante [20] :

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \tag{3.16}$$

$x \in \mathbb{R}^n$, vecteur des états du système d'ordre n.

$u \in \mathbb{R}^m$, vecteur des entrées inconnues d'ordre m.

$f : \mathbb{R}^n \to \mathbb{R}^n \times \mathbb{R}^n$; $h : \mathbb{R}^n \to \mathbb{R}^p$; $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ sont des vecteurs des fonctions analytiques.

Le vecteur d'entrée du récepteur est le vecteur de sortie de l'émetteur,il faut donc concevoir un récepteur de manière à ce que son vecteur de sortie converge au moins asymptotiquement vers le vecteur d'entrée de l'émetteur.

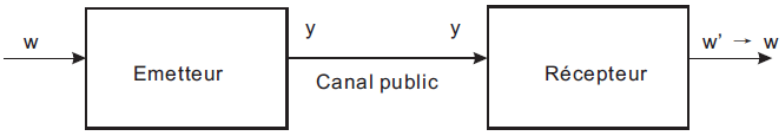


FIGURE 3.8 – Synchronisation par l'inversion du système.

3.5.5 Synchronisation généralisée

Cela correspond à une généralisation du concept de synchronisation identique. Les deux systèmes se synchronisent, au sens généralisé, s'il existe une transformation M telle que [11] :

$$lim_{t \to 0} \parallel x'(t) - Mx(t) \parallel = 0 \tag{3.17}$$

Où x(t) est l'état du système émetteur et x'(t) est l'état du système récepteur.

Et ce indépendamment des conditions initiales.

Si la fonction M est inversible, alors $M^{-1}(x')$ fournit une estimation de l'état x. Mais si cette transformation n'est pas inversible, on ne peut pas estimer x. Cela représente un inconvénient majeur pour certaines techniques de communication, qui utilisent l'état de l'émetteur pour décrypter le message transmis.

3.5.6 Synchronisation retardée

L'état du système esclave converge vers l'état décalé dans le temps du système maître, c'est-à-dire [11] :

$$lim_{t\to 0} \parallel x'(t) - x(t-\tau) \parallel = 0 \tag{3.18}$$

Où x(t) est l'état du système émetteur, x'(t) est l'état du système récepteur et τest un retard positif.

3.5.7 Synchronisation projective

L'état du système récepteur se synchronise avec un multiple de l'état du système émetteur.Il existe donc a et τ tels que [11] :

$$lim_{t\to 0} \parallel x'(t) - ax(t-\tau) \parallel = 0 \tag{3.19}$$

a est le facteur d'échelle, $x(t)$ est l'état du système émetteur, $x'(t)$ est l'état du système récepteur et τ est un retard positif.

Ce type de synchronisation est utilisé pour les systèmes "partiellement linéaires" et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés[11].

3.5.8 Synchronisation de phase

Pour deux systèmes périodiques de phases Φ_1 et Φ_2, la synchronisation est exprimée par la relation[11] :

$$|n\Phi_1 - m\Phi_2| < c. \tag{3.20}$$

où m ,n sont des entiers naturels et c est une constante positive.

Cette notion classique de synchronisation a été étendue aux systèmes chaotiques. Pour définir la phase d'un système chaotique, on peut mentionner l'approche analytique.

Un signal analytique $\Psi(t)$ est une fonction complexe définie par :

$$\Psi(t) = s(t) + j\tilde{s}(t) = A(t)e^{j\Phi(t)} \tag{3.21}$$

où $\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$.$A(t)$ est l'amplitude du signal $\Psi(t)$ et $\Phi(t)$ sa phase.

$$\tilde{s}(t) = \frac{1}{\pi} V.P \int_{-\infty}^{+\infty} \frac{s(\tau)}{t-\tau} d\tau \tag{3.22}$$

Une synchronisation de phase entre deux systèmes chaotiques couplés se produit si

$$|n\Phi_1 - m\Phi_2| < c. \tag{3.23}$$

Dans ce cas, les amplitudes de ces systèmes restent non corrélées.

3.5.9 Synchronisation à base d'observateurs

La synchronisation peut également être réalisée en employant un observateur. Le système maître est un système chaotique quelconque et le système esclave est un observateur d'état correspondant. La Figure(3.9) illustre ce principe de synchronisation.

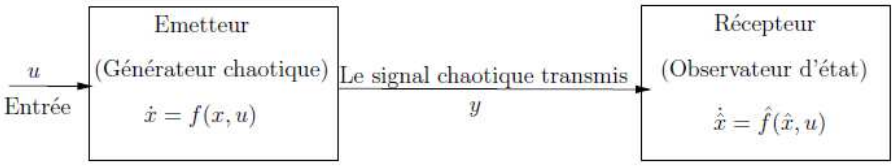


FIGURE 3.9 – Principe de la synchronisation à base d'observateur.

Pour ce principe, nous disons que l'émetteur et le récepteur se synchronisent si le système $\dot{\hat{x}} = \hat{f}(\hat{x}, u)$ (défini au niveau du récepteur) est un observateur convergent pour le système $\dot{x} = f(x, u)$ (défini au niveau de l'émetteur). Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que : $\| x(t) - \hat{x}(t) \| \to 0$, quand $t \to +\infty$.

Exemples d'observateurs pour la synchronisation

Cas Continu

On peut citer l'observateur de Luenberger, l'observateur à mode gilissant, l'observateur à grand gain, observateur impulsif ainsi que l'observateur à entrée inconnue.

Cas discret

On peut citer l'observateur retardé étape par étape appelé également (Observateur Deadbeat).

Définition 3.1

Un observateur est un système dynamique qui permet la reconstruction de l'état d'un système, à partir de ses entrées, de ses sorties, et de la connaissance de son modèle dynamique.

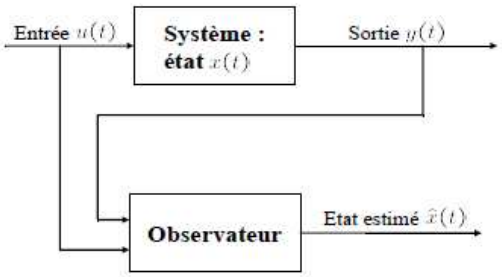


FIGURE 3.10 – Principe d'un observateur.

3.5.9.1 Observabilité des systèmes non linéaires

Cas continu [5]

On considère le système non linéaire autonome suivant :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{3.24}$$

$x \in \mathbb{R}^n$est le vecteur d'état, $y \in \mathbb{R}^p$ est le vecteur de sortie, les fonctions f, h sont des vecteurs de fonctions analytiques de dimensions appropriées.

Pour donner la condition du rang d'observabilité,il faut d'abord définir la dérivée de Lie.

Définition 3.2 : la dérivée de Lie

Considérons h une fonction C^∞ de $\mathbb{R}^n$ dans $\mathbb{R}$. On définit la dérivée de Lie de$h$ dans la direction de f, notée $L_f h$, la dérivée de h le long de la courbe intégrale de f en $t = 0$:

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i(x)} \tag{3.25}$$

Par définition on décrit : $L_f^0 h = h$ et $L_f^k h = L_f(L_f^{k-1} h), \forall k \geq 1$.

Avec :

$$f(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ . \\ . \\ f_n(x) \end{pmatrix} \tag{3.26}$$

Le système (3.24) doit satisfaire la condition du rang d'observabilité $rang(O) = n$
Où

$$O = \begin{pmatrix} dh \\ dL_f h \\ . \\ . \\ dL_f^{n-1} h \end{pmatrix} \tag{3.27}$$

$$rang(O) = rang \begin{pmatrix} dh \\ dL_f h \\ . \\ . \\ dL_f^{n-1} h \end{pmatrix} = n \tag{3.28}$$

n :dimension du système.

Si la condition du rang d'observabilité est vérifiée en x, $\forall x \in U$, U étant un voisinage de x_0, le système décrit par l'équation (3.24) est localement observable en x_0.

Définition3.3 : Observabilité locale

Le système (3.24) est localement observable en$x_0 \in M$ si pour tout voisinage ouvert et suffisamment petit U de x_0 , $I(x_0, U) = \{x_0\}$. Il est clair qu'on peut poser $U = M$.

cas discret [5]

Soit le système non linéaire suivant :

$$\begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k = h(x_k) \end{cases} \tag{3.29}$$

$x_k \in \mathbb{R}^n$, $y_k \in \mathbb{R}^p$,$u_k = (u_{1k}, u_{2k}, ...u_{mk})^T \in \mathbb{R}^m$. Pour toute entrée $u_k \in \mathbb{R}^m$ constante, $f_{uk}(x_k) = f(x_k; u_k)$ est un champ de vecteur C^∞ sur$\mathbb{R}^n$ et les h_i pour $i = 1, ..., p$, les composantes de h qui sont des fonctions définies de C^∞ de $\mathbb{R}^n$sur $\mathbb{R}$.

L'observabilité des systèmes en temps discret se vérifie par le rang d'observabilité suivant :

$$dim(dOh(x0)) = n \tag{3.30}$$

Où l'espace d'observation $O(h)(x_k)$ est défini par :

$$O(h)(x_k) = span(h_i(x_k), h_i \circ f_{u1k}(x_k), ..., h_i \circ f_{u1k} \circ ..... \circ f_{ulk}(x_k))$$

Tel que : $1 \leq i \leq p$, $u_{1k}, ..., u_{lk} \in \mathbb{R}^n$et $x_k \in \mathbb{R}^n$.

Ceci peut être reformulé comme suit :

$$rang[span\{dh, d(f \circ h), ..., d(f^{n-1} \circ h)\}] = n \tag{3.31}$$

n est la dimension du système.

3.5.9.2 Inversion à gauche et conditions de recouvrement d'observabilité

Dans la transmission de données par synchronisation de systèmes chaotiques, il est important de pouvoir estimer l'entrée inconnue du système en plus de la synchronisation des états. En effet, l'entrée inconnue peut être un défaut, une perturbation ou dans notre travail, un message confidentiel. La transmission d'informations avec la méthode par inclusion (Section 2.6) est non seulement un problème d'observabilité mais aussi un problème d'inversion à gauche, c'est à dire reconstruire tous les états ainsi que le message inconnu à partir de la sortie du système et ses dérivées. Deux types d'observateurs continus ont été proposés pour les systèmes à entrées inconnues.

Cas continu [5] Deux types d'observateurs continus ont été proposés pour les systèmes à entrées inconnues. Des observateurs destinés à estimer seulement les états du système (sans tenir compte de l'entrée inconnue), et des observateurs destinés à l'estimation des états et de l'entrée inconnue.

Soit le système :

$$\begin{cases} \dot{x}(t) = f(x,u) \quad , x_0 \in D \subseteq \mathbb{R}^n \\ y(t) = h(x,u) \end{cases} \tag{3.32}$$

Dans lequel $x \in \mathbb{R}^n$ est l'espace d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, et $y \in \mathbb{R}^p$représente le vecteur de sortie du système, $t \in T = [0; t_f]$. Les fonctions $f(x;u)$, $h(x;u)$,$u(t)$ sont considérées suffisamment dérivables. Le problème de l'inversion du système consiste à reconstruire $x$et u ou une partie de ceux-ci à partir de la sortie $y(.)$ du système et de ses dérivées. Le système (3.32) génère le "mapping" suivant (pour la condition initiale x_0 connue) :

$$\emptyset(u) : U \subseteq C^n(T, \mathbb{R}^m) \rightarrow C^N(T, \mathbb{R}^p) : u \rightarrow x(., x_0, u) \rightarrow y(.) = h(x;u)$$

Avant d'introduire les propriétés du système (3.32), on considère un ensemble de fonctions U définies sur le domaine D_α constitué de fonctions et de leurs dérivées d'ordre 1 à α . Alors, nous avons : $U = U(D_\alpha)$ où :

$$D_0 = U_{t\in T} u(t), D_1 = U_{t\in T}(u(t), \dot{u}(t)), ..., D_\alpha = U_{t\in T}(u(t), ..., u(t)^{(\alpha)}), D_i \subseteq \mathbb{R}^{(i+1)m}$$

Définition 3.3 : Le système (3.32) est inversible dans le domaine $D \times D_\alpha \times T$ si pour tout $x_0 \in D$ et deux entrées différentes $u_1(t)$,$u_2(t) \in D_\alpha$, il existe un instant$t \in T$ tel que$h(\emptyset(x_0, u_1)) \neq h(\emptyset(x_0, u_2))$.

Nous écrivons maintenant le système (3.32) de la façon suivante :

$$\begin{cases} \dot{x} = f(x) + g(x)m \\ y = h(x) \end{cases} \tag{3.33}$$

dans lequel l'entrée inconnue (message) m est considérée être bornée, et les champs de vecteurs$f, g : U \subset \mathbb{R}^n \to \mathbb{R}^n$et $h : U \subset \mathbb{R}^n \to \mathbb{R}$ sont des champs de vecteurs analytiques. Le vecteur de sortie de ce système est transmis au récepteur, qui doit générer un vecteur de sortie qui convergera asymptotiquement vers le vecteur d'entrée de l'émetteur. Ce problème constitue le problème d'inversion à gauche.

Dans le système (3.33), on considère que m est continu, ou au moins continu par morceaux. La conception d'un observateur à entrées inconnues est réalisable localement au voisinage de x_0 si les conditions données par les hypothèses suivantes sont vérifiées :

Hypothèse 1 : l'entrée inconnue (message confidentiel) est bornée.

Hypothèse 2 : $span\{dh, dL_f h, ..., dL_f^{n-1}h\} = n$ est de rang$n$.

Hypothèse 3 : $\begin{pmatrix} dh \\ dL_f h \\ . \\ . \\ dL_f^{n-1}h \end{pmatrix} .g(x) = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ \theta \end{pmatrix}$

où θsignie une fonction non nulle presque partout dans $U \subset \mathbb{R}^n \to \mathbb{R}$.

La condition donnée dans l'hypothèse 3 est appelée condition de recouvrement d'observabilité « Observabilité Matching Condition » pour les systèmes continus. Cette condition garantie la propriété d'inversibilité à gauche, c'est à dire la possibilité de retrouver tous les états et le message à partir de la sortie y et de ses dérivées.

Cas discret [5] Plusieurs types d'observateurs ont été proposés pour les systèmes discrets à entrées inconnues. Parmi ces méthodes, on peut citer l'observateur en temps discret retardé étape par étape. Soit le système donné par (3.29), le problème de l'inversion du système consiste à reconstruire $x$et u ou une partie de ceux-ci à partir de la sortie $y(.)$ du système et de ses itérés.

Nous écrivons le système (3.29) de la façon suivante :

$$\begin{cases} x_{k+1} = f(x_k) + g(x_k)m_k \\ y_k = h(x_k) \end{cases} \tag{3.34}$$

dans lequel l'entrée inconnue (message)m_k est considérée être bornée, et les champs de

vecteurs$f, g : U \subset \mathbb{R}^n \to \mathbb{R}^n$et $h : U \subset \mathbb{R}^n \to \mathbb{R}^m$ sont des champs de vecteurs analytiques. La conception d'un observateur à entrées inconnues est réalisable localement au voisinage de $x_0$si les conditions données par les hypothèses suivantes sont vérifiées :

Hypothèse 4 : l'entrée inconnue (message confidentiel) est bornée.

Hypothèse 5 : $span\{dh, d(f \circ h), ..., d(f^{n-1} \circ h)\} = n$ est de rang$n$ en x_0.

Hypothèse 6 : $((dh)^T, (d(f \circ h))^T, ..., (d(f^{n-1} \circ h))^T)^T.g = (0, 0, ..., \theta)^T$.

où θsignifie une fonction non nulle presque partout dans $U \subset \mathbb{R}^n \to \mathbb{R}$.

La condition donnée dans l'hypothèse 6 est appelée condition de recouvrement d'observabilité pour les systèmes discret. Cette condition garantie la propriété d'inversibilité à gauche, c'est à dire la possibilité de retrouver tous les états et le message à partir de la sortie y et de ses itérés .

3.6 Conclusion

Les travaux de Pecora et Carroll ont ouvert la voix à l'utilisation du chaos dans les télécommunications, en montrant que deux systèmes chaotiques identiques peuvent se synchroniser s'ils sont couplés sous certaines conditions. En effet la synchronisation des systèmes chaotiques permet de réaliser des systèmes permettant d'effectuer une transmission sécurisée de données.

Dans ce chapitre, nous avons pu énoncer le concept de la synchronisation chaotique ainsi que ses diverses méthodes.

Chapitre 4

Systèmes chaotiques d'ordre fractionnaire

4.1 Introduction

Le calcul de la dérivée et de l'intégrale d'ordre fractionnaire est une généralisation de la dérivée et de l'intégrale d'ordre entier. Il remonte à la correspondance entre Leibniz et L'Hospital en 1695. En raison de la complexité des calculs et le manque de théorèmes. Il a été marginalement étudié par les chercheurs pendant une longue période. Récemment, il a été considéré comme un outil précieux dans la modélisation de nombreux phénomènes dans divers domaines, de l'ingénierie, de la physique et de l'économie, La dérivée d'ordre fractionnaire offre un excellent outil pour la description de la mémoire des processus dynamiques.

Ce chapitre a pour objectif de définir des notions fondamentales sur le calcul et les dérivées fractionnaires, les systèmes d'ordre fractionnaire et les différentes représentations de ces systèmes. Enfin, nous terminons par une présentation des différentes méthodes de synchronisation des systèmes chaotiques d'ordre fractionnaire.

4.2 Les systèmes dynamiques d'ordre fractionnaire continus

Cette partie contient des définitions fondamentales du calcul fractionnaire en temps continu.

4.2.1 Opérateur de dérivation d'ordre fractionnaire

Un système est dit fractionnaire s'il est modélisé par des équations différentielles comprenant des dérives d'ordre fractionnaire.

Le calcul fractionnaire est une généralisation de l'intégration et de la différentiation à l'opérateur fondamental d'ordre non entier ${}_aD_t^\alpha$ appelé également (opérateur intégro-différentiel d'ordre fractionnaire). Cet opérateur est défini comme suit [21] :

$$ {}_aD_t^\alpha = \begin{cases} \frac{d^\alpha}{dt^\alpha} & \alpha \succ 0 \\ 1 & \alpha = 0 \\ \int_a^t (d\tau)^{-\alpha} & \alpha \prec 0 \end{cases} \tag{4.1} $$

avec $\alpha \in \mathbb{R}$ est l'ordre de dérivation et a et t sont des limites de l'opération .

4.2.2 Fonctions spécifiques à la dérivation fractionnaire

Ces fonctions représentent les outils de base du calcul fractionnaire :

4.2.2.1 La fonction Gamma

L'une des fonctions de base du calcul fractionnaire est la fonction Gamma d'Euler$\Gamma(z)$.La fonction Gamma $\Gamma(z)$ est définie par l'intégrale suivante[22] :

$$ \Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt \tag{4.2} $$

Où :

$z \in \mathbb{C}$;$\Gamma(z)$ est une fonction monotone et strictement décroissante pour $0 \prec z \leq 1$.

Une propriété importante de $\Gamma(z)$ est la relation de récurrence suivante :

$$ \Gamma(z+1) = z\Gamma(z) \tag{4.3} $$

Et en particulier

- La fonction de Gamma Euler généralise la factorielle car $\Gamma(n+1) = n!, \forall n \in \mathbb{N}^*$.
- $\Gamma(1) = \int_0^\infty t^{1-1} e^{-t} dt = \int_0^\infty e^{-t} dt = 1$.
- $\Gamma(0_+) = +\infty$.

4.2.2.2 La fonction Mittag-Leffler

La fonction de Mittag-Leffler est une généralisation de la fonction exponentielle e^z, elle est souvent utilisée dans la résolution des problèmes physiques décrits par des équations à dérivée ou intégrale fractionnaires. Elle est également connue pour avoir un nombre fini de zéros réels, ce qui est applicable à de nombreux problèmes physiques. La fonction de Mittag-Leffler à deux paramètres est définie par la relation suivante [23] :

$$ E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + \beta)}; (z \in \mathbb{C}, \alpha \succ 0, \beta \succ 0) \tag{4.4} $$

Pour $\beta = 1$ on obtient la fonction de Mittag-Leffler avec un seul paramètre

$$E_{\alpha,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)}; (z \in \mathbb{C}, \alpha \succ 0) \tag{4.5}$$

En particulier,si$\alpha = 1$ on trouve la fonction exponentielle

$$E_{1,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{z^k}{n!} = e^z \tag{4.6}$$

4.2.3 Dérivation et intégration d'ordre fractionnaire

Il y a beaucoup d'approches pour la dérivation fractionnaire,les approches qui sont fréquemment utilisées dans les applications sont les suivantes :

4.2.3.1 Dérivée fractionnaire au sens de Riemann-Liouville

La dérivée fractionnaire au sens de Riemann-Liouville est la plus connue et la plus répandue.

Elle est basée sur la $n^{ième}$ primitive d'une fonction f. [24,25]

Considérons la formule de Cauchy pour l'intégration

$${}_aI_t^n f(x) = \int_a^t d\tau_1 \int_a^{\tau_1} d\tau_2 ..... \int_a^{\tau_{n-1}} f(\tau_{n)} d\tau_n \tag{4.7}$$

$${}_aI_t^n f(x) = \frac{1}{(n-1)!} \int_a^t f(t-\tau) d\tau \tag{4.8}$$

Où a et t sont des limites de l'intégration $f(\tau)$.L'équation (4.9) peut-être généralisée pour $n \in \mathbb{R}$.Dans ce cas, nous obtenons la formule de Riemann-Linouville pour l'intégral fractionnaire :

$${}_a^R I_t^\alpha f(t) = \frac{1}{\Gamma(\alpha)} \int_a^t f(t-\tau)^{\alpha-1} f(\tau) d\tau \tag{4.9}$$

Où $\alpha \in \mathbb{R}^+$ est l'ordre d'intégration de la fonction $f(t)$.

La dérivée d'ordre fractionnaire de Riemann-Linouville est défini comme suit [24,25]

$${}_a^R D_t^\alpha f(t) = \frac{1}{\Gamma(m-\alpha)} \frac{d^m}{dt^m} \int_a^t \frac{f(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau \tag{4.10}$$

Où $\alpha \in \mathbb{R}$est l'ordre fractionnaire.Pour $\alpha \succ 0$,$m-1 \prec \alpha \leq m$, $m \in \mathbb{N}$ et pour $\alpha \leq 0$,$m = 0$.[26]

Cette dérivée d'ordre fractionnaire peut aussi être définie à partir de l'équation (4.9) comme suit :

$$ {}_{a}^{R}D_{t}^{\alpha} f(t) = \frac{d^m}{dt^m}({}_{a}I_{t}^{(m-\alpha)} f(t)) \tag{4.11} $$

4.2.3.2 Dérivée fractionnaire au sens de Caputo

Caputo [27] a introduit une autre formulation de la dérivée d'ordre fractionnaire définie par :

$$ {}_{a}^{C}D_{t}^{\alpha} f(t) = \frac{1}{\Gamma(m-\alpha)} \int_{a}^{t} \frac{f^{(m)}(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau \tag{4.12} $$

$$ {}_{a}^{C}D_{t}^{\alpha} f(t) = I^{m-\alpha}(\frac{d^m}{dt^m} f(t)) \tag{4.13} $$

Où $\alpha \in \mathbb{R}$est l'ordre fractionnaire.Pour $\alpha \succ 0$,$m-1 \prec \alpha \leq m$, $m \in \mathbb{N}$ et pour $\alpha \leq 0$,$m = 0$.

$f^{(m)}(\tau)$ étant la dérivée d'ordre entier m de la fonction $f(\tau)$.

4.2.3.3 Dérivée fractionnaire au sens de Grünwald-Letnikov

La définition au sens de Grünwald-Letnikov est basée sur une approche aux différences finies fractionnaires [28,29] où toute la différence par rapport au cas entier se situe dans l'extension de la factorielle à travers la fonction Gamma Euler.

Considérons une fonction continu f(t) sa dériver d'ordre 1 s'écrit :

$$ D^1 f(t) = lim_{h \to 0} \frac{f(t) - f(t-h)}{h} \tag{4.14} $$

La dérivée d'ordre 2 de la fonction f(t) s'écrit sous la forme suivante :

$$ D^2 f(t) = lim_{h \to 0} \frac{f'(t) - f'(t-h)}{h} = lim_{h \to 0} \frac{f(t) - 2f(t-h) + f(t-2h)}{h^2} \tag{4.15} $$

Nous pouvons alors déduire la dérivée d'ordre quelconque qui est donnée par

$$ D^{\alpha} f(t) = lim_{h \to 0} \frac{1}{h^{\alpha}} \sum_{k=0}^{\infty} (-1)^k \begin{pmatrix} \alpha \\ k \end{pmatrix} f(t-kh) \tag{4.16} $$

Où les coefficients $\begin{pmatrix} \alpha \\ k \end{pmatrix}$ sont donnés par :

$$ \begin{pmatrix} \alpha \\ k \end{pmatrix} = \frac{\Gamma(\alpha+1)}{\Gamma(k+1).\Gamma(\alpha-k+1)} \tag{4.17} $$

La dérivée fractionnaire au sens de Grünwald-Letnikov d'une fonction$f(t)$ est définie par la relation suivante :

$$ {}_aD_t^{\alpha} f(t) = lim_{h\to 0} \frac{1}{h^{\alpha}} \sum_{k=0}^{\alpha} (-1)^k \begin{pmatrix} \alpha \\ k \end{pmatrix} f(t-kh) \tag{4.18} $$

Où $h$est la période d'échantillonnage,$\alpha \in \mathbb{R}$est l'ordre fractionnaire .

Définition : (Coefficients binomiaux)

Le coefficient binomial de l'entier naturel α et de l'entier naturel k est défini comme étant l'entier naturel C_{α}^{k}

$C_{\alpha}^{k} = \begin{pmatrix} \alpha \\ k \end{pmatrix} = \frac{\alpha!}{k!(\alpha-k)!}\ Si\ 0 \leq k \leq \alpha$

Et

$C_{\alpha}^{k} = \begin{pmatrix} \alpha \\ k \end{pmatrix} = 0\ Si\ k \prec 0\ ou\ k \succ 0$

$k!$ désigne la factorielle de k.

4.2.4 Propriétés des dérivées fractionnaires et intégrales fractionnaires

Les principales propriétés des opérateurs d'ordre fractionnaire sont les suivantes[30] :

1. Si $f(z)$ est une fonction analytique en z alors sa dérivée fractionnaire $D_z^{\alpha} f(z)$ est une fonction analytique en z et α.
2. Pour $\alpha = n$, où n est un nombre entier,l'opération $D_t^{\alpha} f(t)$ produit le même résultat que la dérivation classique d'ordre entier.
3. Pour$\alpha = 0$, l'opérateurD_t^{α} est l'opérateur identité

$$ D_t^0 f(t) = f(t) $$

4. La dérivation et l'intégration fractionnaires sont des opérations linéaires

$$ D_t^{\alpha}(\gamma f(t) + \delta g(t)) = \gamma D_t^{\alpha} f(t) + \delta D_t^{\alpha} g(t) \tag{4.19} $$

   f et g sont deux fonctions continues , γet δdes nombres réels .

5. La loi additive

$$ D_t^{\alpha} D_t^{\beta} f(t) = D_t^{\beta} D_t^{\alpha} f(t) = D_t^{\alpha+\beta} f(t) \tag{4.20} $$

   αet βsont deux nombres réels.

6. Règle de Leibniz

$$ {}_aD_t^{\alpha}(f(t).g(t)) = \sum_{k=0}^{\infty} \begin{pmatrix} \alpha \\ k \end{pmatrix} f^k(t) D^{\alpha-k} g(t) \tag{4.21} $$

Où $f(t)$ et $g(t)$ ses dérivées sont continues dans$[a,t]$.

4.2.5 La transformée de Laplace

La transformée de Laplace d'une fonction entière f(t) est la fonction F(s) définie comme suit [22] :

$$F(s) = \mathcal{L}\{f(t);s\} = \int_0^\infty e^{-st} f(t)dt \tag{4.22}$$

4.2.5.1 Transformée de Laplace de l'intégrale d'ordre fractionnaire

La transformée de Laplace de l'intégrale d'ordre fractionnaire de Riemann-Liouville d'ordre $\alpha \succ 0$ définie par (4.9) peut notamment s'écrire comme le produit de convolution de la fonction $g(t) = \frac{1}{\Gamma(\alpha)} t^{\alpha-1}$ et $f(t)$.[31]

$$I^\alpha f(t) = D^{-\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_0^t (t-\tau)^{\alpha-1} f(\tau)d\tau = \frac{1}{\Gamma(\alpha)} t^{\alpha-1} * f(t) \tag{4.23}$$

La transformée de Laplace de la fonction$g(t) = t^{\alpha-1}$ est donnée par

$$G(s) = \mathcal{L}t^{\alpha-1} = \Gamma(\alpha)s^{-\alpha}. \tag{4.24}$$

En utilisant la formule de la transformée de Laplace de la convolution :
$\mathcal{L}\{f(t) * g(t)\} = F(s).G(s)$
On obtient la transformée de Laplace de l'intégrale de Riemann-Liouville et celle de Grünwald-Letnikov :

$$\mathcal{L}I^\alpha[f(t)] = s^{-\alpha}F(s) \tag{4.25}$$

4.2.5.2 Transformée de Laplace de la dérivée d'ordre fractionnaire

•Au sens de Riemann-Liouville [32]

$$\mathcal{L}\{{}_a^R D_t^\alpha f(t)\} = \begin{cases} s^\alpha F(s) & \alpha \prec 0 \\ s^\alpha F(s) - \sum_{k=0}^{n-1} s^k ({}_0^R D_t^{\alpha-k-1} f(0)) & \alpha \succ 0 \end{cases} \tag{4.26}$$

Avec $(n-1) \leq \alpha \prec n$ et $n \in \mathbb{N}$.

La transformée de Laplace de la dérivée de Riemann-Liouville est bien connue. Mais son applicabilité en pratique est limitée à cause de l'absence d'interprétation physique des valeurs limites des dérivées d'ordre fractionnaire pour $t = 0$.

•Au sens de Caputo

$$\mathcal{L}\{D_t^{\alpha} f(t)\} = \begin{cases} sF(s) & \alpha \prec 0 \\ s^{\alpha}F(s) - \sum_{k=0}^{n-1} s^{\alpha-k-1} f^{k}(0) & \alpha \succ 0 \end{cases} \tag{4.27}$$

Avec $(n-1) \leq \alpha \prec n$.

Comme cette formule de la transformée de Laplace de la dérivée de Caputo induit les valeurs de la fonction $f(t)$ et ses dérivées en la borne inférieure $t = 0$, pour laquelle une certaine interprétation physique existe, elle semble être la plus appropriée quand on la compare aux autres.[23]

4.2.6 Représentation des systèmes fractionnaires en temps continu

Il existe trois types de représentations des systèmes non entiers continus.

4.2.6.1 Équation différentielle fractionnaire

Un système fractionnaire est représenté par une équation différentielle suivante [32] :

$$y(t) + a_1 D^{\alpha_1} y(t) + ... + a_n D^{\alpha_n} y(t) = b_0 D^{\beta_0} u(t) + b_1 D^{\beta_1} u(t) + ... + b_m D^{\beta m} u(t) \tag{4.28}$$

$$y(t) + \sum_{i=1}^{n} a_i D^{\alpha_i} y(t) = \sum_{j=0}^{m} b_j D^{\beta_j} u(t) + b_0 u(t) \tag{4.29}$$

Où D^{α}désigne l'opérateur de dérivation d'ordre α de Caputo.$u(t) \in \mathbb{R}$et $y(t) \in \mathbb{R}$ désignent respectivement l'entrée et la sortie du système à l'instant t ; $\alpha_i$et $\beta_j \in \mathbb{R}^+$,a_i, $b_j \in \mathbb{R}$ sont les coefficients de l'équation différentielle, n et m sont les nombres des termes de chaque partie de l'équation différentielle.

4.2.6.2 Fonction de transfert fractionnaire

La transformée de Laplace de l'équation (4.29) donne [33] :

$$Y(s) + a_1 s^{\alpha_1} Y(s) + ... + a_n s^{\alpha_n} Y(s) = b_0 s^{\beta_0} U(s) + b_1 s^{\beta_1} U(s) + ... + b_m s^{\beta m} U(s) \tag{4.30}$$

On déduit la fonction de transfert d'ordre fractionnaire suivante :

$$H(s) = \frac{Y(s)}{U(s)} = \frac{\sum_{j=1}^{m} b_j s^{\beta j} + b_0}{1 + \sum_{i=1}^{n} a_i s^{\alpha i}} \tag{4.31}$$

4.2.6.3 Représentation d'état fractionnaire

La représentation d'état d'ordre fractionnaire pour les systèmes non linéaires est définie comme dans le cas entier, on remplace la dérivée entière d'ordre 1 par la dérivée fractionnaire d'ordre α. [34]

$$\begin{cases} D^{\alpha_i} x_i(t) = f_i(x_1(t), x_2(t), ...x_n(t), t) \\ x_i(0) = c_i \qquad\qquad\qquad\qquad\qquad\qquad i = 1, 2, ..., n \end{cases} \tag{4.32}$$

La représentation vectorielle de (4.32) est :

$$D^{\alpha} x(t) = f(x(t), t) \tag{4.33}$$

Où c_i sont les conditions initiales, $\alpha = [\alpha_1, \alpha_2, ..., \alpha_n]^T$et $x \in \mathbb{R}^n . 0 \prec \alpha_i \prec 2$, $(i = 1, 2, ..., n)$.

Remarque : Si les ordres de dérivation de l'équation différentielle fractionnaire qui régit le système (4.33) sont des multiples entiers d'ordre de base α,le système est dit commensurable sinon le système est non commensurable.

4.3 Les systèmes dynamiques d'ordre fractionnaire discrets

4.3.1 Les différences d'ordre fractionnaire

Il existe plusieurs définitions de différences d'ordre fractionnaire dont,la différence au sens de Caputo,la différence au sens de Riemann-Liouville et la différence au sens de Grünwold Letnikov.

Soit l'ensemble $\mathbb{N}_a$ défini par $\mathbb{N}_a = \{a, a+1, ..\}$.

La fonction fractionnaire $t^{\alpha}, t \in \mathbb{R} \setminus \mathbb{Z}\_$, est définie par l'équation [35] :

$$t^{\alpha} = \frac{\Gamma(t+1)}{\Gamma(t+1-\alpha)} \tag{4.34}$$

où $\mathbb{Z}\_ = -1, -2, ...$ et Γest la fonction d'Euler Gamma.

4.3.1.1 Différence de Caputo d'ordre fractionnaire

Soit $\alpha \succ 0$ et $m - 1 \prec \alpha \prec m$, où m est un entier positif, $m = [\alpha]$.

La différence d'ordre α selon Caputo est définie comme suit [36] :

$$ {}_a\Delta_c^{\alpha} f(t) =_a \Delta^{\alpha-m}(\Delta^m f)(t) = \frac{1}{\Gamma(m-\alpha)} \sum_{s=a}^{t-(m-\alpha)} (t-s-1)^{m-\alpha-1}\Delta^m f(s) \tag{4.35} $$

Avec $t \in \mathbb{N}_{a+(m-\alpha)}$,$\alpha \in (0,1]$et f :$\mathbb{N}_a \to \mathbb{R}$.
Si $0 \prec \alpha \prec 1$, alors $m = 1$ et la différence (4.35) peut être réécrite comme suit :

$$ {}_a\Delta_c^{\alpha} f(t) =_a \Delta^{\alpha-1}(\Delta f)(t) = \frac{1}{\Gamma(1-\alpha)} \sum_{s=a}^{t-(1-\alpha)} (t-s-1)^{\alpha}\Delta f(s).t \in \mathbb{N}_{a+1-\alpha} \tag{4.36} $$

avec $\Delta f(s) = f(s+1) - f(s)$ est la différence classique.

4.3.1.2 Différence de Riemann-Liouville d'ordre fractionnaire

La différence d'ordre fractionnaireα au sens de Riemann Liouville, de la fonction f :$\mathbb{N}_{\alpha} \to \mathbb{R}$est définie comme suit [37] :

$$ {}_a\Delta_{RL}^{\alpha} f(t) =_a \Delta^m(\Delta^{-(m-\alpha)} f)(t) \tag{4.37} $$

Si $0 \prec \alpha \prec 1$, alors m=1, l'équation (4.37) peut être réécrite sous forme [38] :

$$ {}_a\Delta_{RL}^{\alpha} f(t) =_a \Delta(\Delta^{-(1-\alpha)} f)(t), t \in \mathbb{N}_{a+(1-\alpha)}. \tag{4.38} $$

4.3.1.3 Différence de Grünwald Letnikov d'ordre fractionnaire

Considérons la différence d'ordre 1 suivante :

$$ \Delta^1 x(k) = x(k) - x(k-1) \tag{4.39} $$

La différence d'ordre 2 est présentée alors comme suit :

$$ \Delta^2 x(k) = x(k) - 2x(k-1) + x(k-2) \tag{4.40} $$

La différence d'ordre entier m peut être alors calculée à partir de la relation suivante [37] :

$$ \Delta^m x(k) = \sum_{j=0}^{m} (-1)^j \begin{pmatrix} m \\ j \end{pmatrix} x(k-j) \tag{4.41} $$

En utilisant la relation (4.41), la différence de Grünwald-Letnik d'ordre fractionnaire est définie ci-dessous [39] :

$$\Delta^{\alpha}x(k) = \sum_{j=0}^{k}(-1)^{j}\begin{pmatrix}\alpha\\ j\end{pmatrix}x(k-j) \tag{4.42}$$

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

Pour modéliser un système chaotique discret d'ordre fractionnaire, on utilisera la définition (4.42). Pour ce faire, considérons le système discret d'ordre entier suivant :

$$x(k+1) = f(x(k)) \tag{4.43}$$

Où f est une fonction non linéaire.

La différence d'ordre 1 pour ce système discret est donnée par

$$\Delta^{1}x(k+1) = x(k+1) - x(k) = f(x(k)) - x(k) \tag{4.44}$$

A partir de l'équation (4.44), nous définissons la différence d'ordre αcomme suit :

$$\Delta^{\alpha}x(k+1) = f(x(k)) - x(k) \tag{4.45}$$

D'autre part, et à partir de l'équation (4.42), nous pouvons déduire que

$$\Delta^{\alpha}x(k+1) = x(k+1) - \alpha x(k) + \sum_{j=2}^{k+1}(-1)^{j}\begin{pmatrix}\alpha\\ j\end{pmatrix}x(k-j+1) \tag{4.46}$$

Pour simplifier dernière équation, introduisons le changement de variable suivant : $p = j - 1$.L'équation (4.46) devient alors :

$$\Delta^{\alpha}x(k+1) = x(k+1) - \alpha x(k) + \sum_{p=1}^{k}(-1)^{p+1}\begin{pmatrix}\alpha\\ p+1\end{pmatrix}x(k-p) \tag{4.47}$$

Définissons le paramètre $C_p = (-1)^{p+1}\begin{pmatrix}\alpha\\ p+1\end{pmatrix}$

En remplaçant l'équation (4.47) dans (4.45) nous obtenons l'équation qui suit :

$$x(k+1) = f(x(k)) - (\alpha-1)x(k) - \sum_{p=1}^{k} C_p x(k-p) \tag{4.48}$$

4.3.2 Représentation des systèmes fractionnaires en temps discret

•Représentation d'état fractionnaire

Une représentation d'état des systèmes discrets non linéaire d'ordre fractionnaire a été proposée. Elle est définie par le système d'équations suivant :

$$\begin{cases} \Delta^{\alpha} x(k+1) = f(x(k), u(k)) \\ x(k+1) = \Delta^{\alpha} x(k+1) - \sum_{p=1}^{L} C_p x(k-p) \\ y(k) = h(x(k)) \end{cases}$$

Où $\alpha \in \mathbb{R}$ est l'ordre de dérivation du système, f et h sont des fonctions non linéaires.

4.4 Systèmes chaotiques d'ordre fractionnaires

L'une des applications importantes du calcul fractionnaire est la théorie du chaos. En effet les systèmes chaotiques d'ordre fractionnaire possèdent des propriétés intrinsèques, qui peuvent être utilisées dans les schémas de synchronisation et de cryptographie. Le choix de l'ordre de dérivée fractionnaire αest effectué de manière à conserver les propriété du comportement chaotique.

4.4.1 Stabilité des systèmes fractionnaires

La stabilité des systèmes d'ordre entier est bien connue, un système est dit stable si les racines du polynôme caractéristique sont à parties réelles strictement négatives, donc situées sur la moitié gauche du plan complexe. Par ailleurs, dans le cas des systèmes fractionnaires linéaires à temps invariant, la définition de la stabilité est différente des systèmes d'ordre entier. En effet, les systèmes fractionnaires peuvent bien avoir des racines dans la moitié droite du plan complexe et être stables. Considérons le système linéaire fractionnaire suivant :[31]

$$\begin{cases} D^{\alpha} x(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \\ x(0) = x_0 \end{cases} \tag{4.49}$$

Avec :

$x(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}^p$et $u(t) \in \mathbb{R}^m$, λsont toutes les valeurs propres de la matrice A.

Le système (4.49) avec entrée, $u(t) = 0$, $u(t)$ est stable si et seulement si

$$| \, arg(\lambda_i) \succ \alpha \frac{\pi}{2} \, |; 1 \leq i \leq n \tag{4.50}$$

L'analyse de la stabilité des systèmes d'ordre fractionnaire a été largement traitée dans le cas où $1 \prec \alpha \prec 2$.

Si $1 \prec \alpha \prec 2$, alors la relation (4.50) décrit une région convexe du plan complexe comme le montre la figure (4.1)

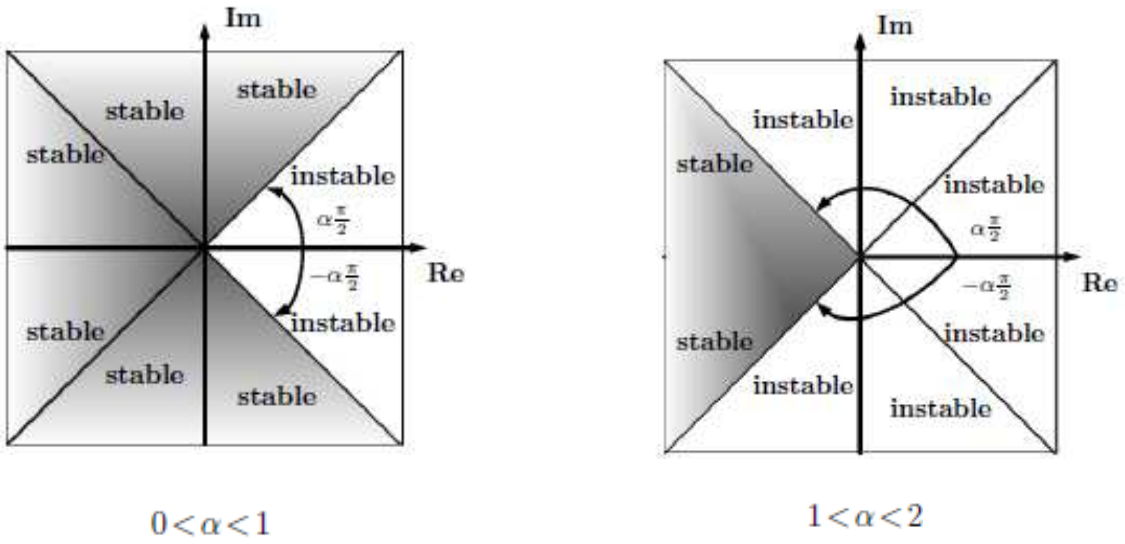


FIGURE 4.1 – Domaine de stabilité des systèmes d'ordre fractionnaires.

Dans le cas du système non linéaire décrit par l'équation (4.51)

$$D^{\alpha}x = f(x) \tag{4.51}$$

Où : $0 \prec \alpha \prec 1$et $x \in \mathbb{R}^n$.

On peut linéariser le système (4.51) sous la forme :

$$D^{\alpha}x = Ax \tag{4.52}$$

Avec A est la matrice Jacobienne de f et ensuite appliqué la condition (4.50).

4.5 Simulation des systèmes d'ordre fractionnaire

La simulation des systèmes d'ordre fractionnaire consiste à simuler l'élément de base qui est l'opérateur d'intégration ou de dérivation d'ordre fractionnaire.

Actuellement, le principe consiste souvent à approximer l'opérateur de dérivation par un transfert entier.

A cet effet, plusieurs méthodes d'approximations sont introduites pour la modélisation de cet opérateur, on distingue essentiellement deux classes selon que la transmittance obtenue est continue ou discrète.[34]

4.5.1 Approche continue

Dans cette approche, il existe plusieurs techniques d'approximation qui sont l'approximation d'Oustaloup[40,41,42] et l'approximation de Charef [43]. D'autres méthodes d'approximation utilisent des techniques d'interpolation, on peut mentionner la méthode de Carlson [44]qui se base sur un processus itératif de Newton, et la méthode de Matsuda [45] qui utilise le principe du développement en fractions continues (CFE), permet d'approximer la réponse du dérivateur généralisé sur un intervalle de fréquences espacées de façon logarithmique. Il existe aussi des techniques d'identification fréquentielles.

La démarche consiste donc à identifier la transmittance d'ordre entier à partir de la réponse fréquentielle "idéale" du dérivateur généralisé.

4.5.2 Approche discrète

Dans le cas discret, l'approximation s'effectue selon deux approches distinctes, les méthodes de discrétisation directe et les méthodes de discrétisation indirecte.

Méthodes de discrétisation directe Parmi ces méthodes, nous pouvons citer la méthode de Grünwald-Letnikov qui est une définition de la dérivée usuelle d'une fonction. Cette méthode permet de faire l'approximation des équations différentielles généralisées par des équations aux récurrences. Ainsi il existe d'autres méthodes d'approximation qui sont basées sur la discrétisation classique dans le domaine fréquentiel ; Euler, Simpson, et El- Alaoui .

Méthodes de discrétisation indirecte La discrétisation indirecte s'effectue en deux étapes :

1. L'approximation continue.

2. La discrétisation de cette dernière au moyen des méthodes usuelles. Cette approche est basée sur des méthodes numériques.

4.6 Différents types de synchronisation des systèmes chaotiques d'ordre fractionnaire

4.6.1 Synchronisation complète

On considère un système chaotique maître- esclave représenté par [46] :

$$\begin{cases} D^{\alpha}X(t) = F(X(t)) \\ D^{\beta}Y(t) = G(Y(t)) + U \end{cases} \tag{4.53}$$

$X(t) \in \mathbb{R}^n$et $Y(t) \in \mathbb{R}^n$ sont les états du système maître-esclave décrit par l'équation (4.53), $F : \mathbb{R}^n \to \mathbb{R}^n$ et $G : \mathbb{R}^n \to \mathbb{R}^n$sont des fonctions vectorielles continues, $U \in \mathbb{R}^n$ est un vecteur de contrôle à déterminer,α et $\beta \in (0, 1]$ sont les ordres de dérivées fractionnaires et D_t^αet D_t^β sont les dérivées fractionnaires de Caputo d'ordre α et β.

On dit qu'il y a une synchronisation complète entre ces deux systèmes si

$$lim_{t\to 0} \parallel Y(t) - X(t) \parallel = 0 \tag{4.54}$$

$e(t) = Y(t) - X(t)$; est l'erreur de la synchronisation complète.

Si $F = G$, la relation devient une synchronisation complète identique.

Si $F \neq G$, la relation devient une synchronisation généralisée.

4.6.2 Anti-Synchronisation

Deux systèmes sont anti-synchronisés si d'une part, le système maître-esclave ont des vecteurs d'état identiques en valeur absolue mais avec des signes opposés et que d'autre part l'erreur d'anti-synchronisation $e(t)$ décrit par l'équation (4.55) tend vers zéro.[46]

$$e(t) = Y(t) + X(t) \tag{4.55}$$

$$lim_{t\to 0} \parallel Y(t) + X(t) \parallel = 0 \tag{4.56}$$

4.6.3 Synchronisation projective

On dit une synchronisation projective si les variables d'état $Y(t) = (y_i(t))_{1\leq i\leq n}$ du système chaotique esclave se synchronisent avec une constante multiple de l'état $X(t) = (x_i(t))_{1\leq i\leq n}$ du système chaotique maître, représenté par l'équation (4.53) tels que :

$$\exists \alpha_i \neq 0, lim_{t\to\infty} \mid y_i(t) - \alpha_i x_i(t) \mid = 0; \forall (x(0), y(0)); i = 1, 2, ..., n. \tag{4.57}$$

Si $\alpha_i = 1$, l'équation (4.53) représente une synchronisation complète.

Si $\alpha_i = -1$; c'est une anti-synchronisation complète.

4.6.4 Synchronisation généralisée

La synchronisation généralisée est considérée comme une généralisation de la synchronisation complète, l'anti-synchronisation et la synchronisation projective, pour synchroniser des systèmes chaotiques de dimensions et de modèles différents. Elle se manifeste par une relation fonctionnelle entre les deux systèmes chaotiques couplés. On considère un couple de systèmes maître-esclave décrit par l'équation (4.53).

Où $X(t) \in \mathbb{R}^n$et $Y(t) \in \mathbb{R}^m$ sont les états du système maître-esclave,n et m sont les dimensions du système, $F : \mathbb{R}^n \to \mathbb{R}^n$ et $G : \mathbb{R}^m \to \mathbb{R}^m$sont des fonctions vectorielles continues, est un vecteur de contrôle à déterminer,α et $\beta \in (0, 1]$ sont les ordres de dérivées fractionnaires et D_t^αet D_t^β sont les dérivées fractionnaires de Caputo d'ordre α et β.

S'il existe un contrôleur $U \in \mathbb{R}^m$ et une fonction $\phi : \mathbb{R}^n \to \mathbb{R}^n$, telles que toutes les trajectoires des systèmes maître et esclave, avec les conditions initiales $x(0)$ et$y(0)$, vérifient[46] :

$$lim_{t\to 0} \parallel Y(t) - \phi X(t) \parallel = 0; \forall x(0), \forall y(0) \tag{4.58}$$

Les systèmes maître-esclave (4.53) se synchronisent au sens généralisé par rapport à la fonction ϕ.

4.6.5 Synchronisation Q-S

La synchronisation Q-S est considérée comme une catégorisation de tous les types de synchronisations précédentes.On considère un système chaotique maître- esclave

Où $X(t) \in \mathbb{R}^n$et $Y(t) \in \mathbb{R}^m$ sont les états du système maître-esclave, n et m sont les dimensions du système. $Q : \mathbb{R}^n \to \mathbb{R}^d$ et $S : \mathbb{R}^m \to \mathbb{R}^d$sont des fonctions.[46]

On dit qu'il y a une synchronisation Q-S entre ces deux systèmes si

$$lim_{t\to 0} \parallel Q(X(t)) - S(Y(t)) \parallel = 0 \tag{4.59}$$

$e(t) = Q(X(t)) - S(Y(t))$; est l'erreur de la synchronisation Q-S.

4.7 Conclusion

L'introduction de la dérivée d'ordre fractionnaire dans le procédé de communication sécurisée à comportement chaotique, engendre des paramètres supplémentaires qui peuvent servir comme clés de sécurité, ainsi d'augmenter la robustesse du système de transmission de données.

Dans ce chapitre nous avons présenté le principe du calcul fractionnaire, comme on a introduit la synchronisation chaotique d'ordre fractionnaire accompagnée par ses diverses méthodes.

Chapitre 5

Application au cryptage de la parole

5.1 Introduction

Dans ce chapitre, nous exploiton les propriétés des systèmes chaotiques dans la cryptographie afin de transmettre des données de manière sécurisée. Le système de cryptage est composé d'un émetteur chaotique et d'un récepteur ainsi que d'un canal de transmission. L'émetteur est représenté par le système de Lorenz dans le cas continu et par le système de Hénon dans le cas discret. L'information transmise est de type "signal parole" qui est injectée dans la dynamique de l'émetteur par la méthode de cryptage chaotique dite "cryptage par inclusion". Le récepteur est un "observateur de Luenberger" dans le cas continu" et observateur étape par étape" dans le cas discret. Les résultats de simulation sont présentés afin d'étudier les performance de ces crypto-systèmes dans le cas entier comme dans le cas fractionnaire, ainsi qu'en temps continu et en temps discret.

5.2 Propriétés générales du signal Parole

Un signal "Parole"est un signal complexe.Son allure varie constamment au cours du temps. Il contient des fréquences graves, moyennes et aigües. Son spectre s'étend de 20 Hz à 20 kHz et varie en permanence entre ces deux fréquences extrêmes.

Le spectre d'un signal est la représentation en fonction de la fréquence des amplitudes des différentes composantes présentes dans le signal.

Le son que nous avons utilisé est un enregistrement du son qu'émet un chien, qui est représenté par la figure(5.1)

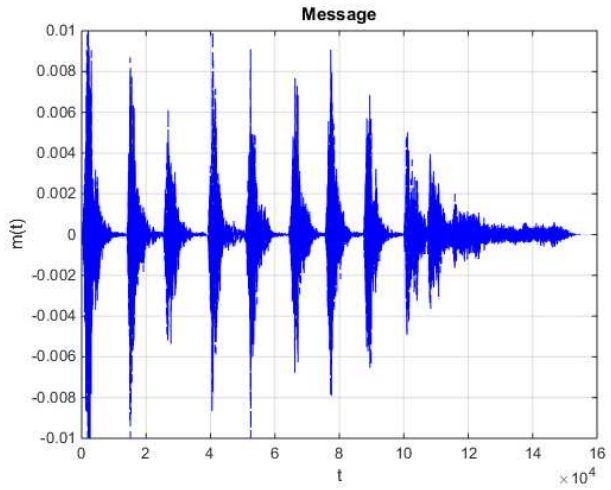


FIGURE 5.1 – Le message.

5.3 Cryptage d'un système chaotique en temps continu

5.3.1 Système « Lorenz »

Le système de Lorenz a joué un rôle historique important puisque son évolution temporelle fait apparaitre un comportement chaotique.De plus, il a constitué le premier et le célèbre système différentiel dissipatif permettant d'observer un attracteur étrange pour certaines valeurs des paramètres.

5.3.2 Cas entier

5.3.2.1 Étude de l'émetteur

Le système de Lorenz est décrit par le modèle suivant :

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -a(1-c)x_1 - (a+1)x_2 - ax_1x_3 + m + p \\ \dot{x}_3 = -bx_3 + x_1(\frac{x_2}{a} + x_1) \end{cases} \tag{5.1}$$

$$\begin{cases} y_0 = x_1 + x_2 - ax_1x_3 + m \\ y_1 = x_1 \end{cases} \tag{5.2}$$

Pour des conditions initiales $(x_1(0), x_2(0), x_3(0)) = (\ 10 \quad 10 \quad 10\ )$

Avec :

a=10, b=28, c=8/3 sont les paramètres du système.

$y_0$et y_1 sont les sorties du système.

m : message à envoyer.

p désigne la perturbation du système, constitué comme suit :
$p = \sum_{k=1}^{N} w_{k+1}(t)$
$\dot{w} = Sw$
$w = [w_1, w_2 ... w_{2N+1}]^T$

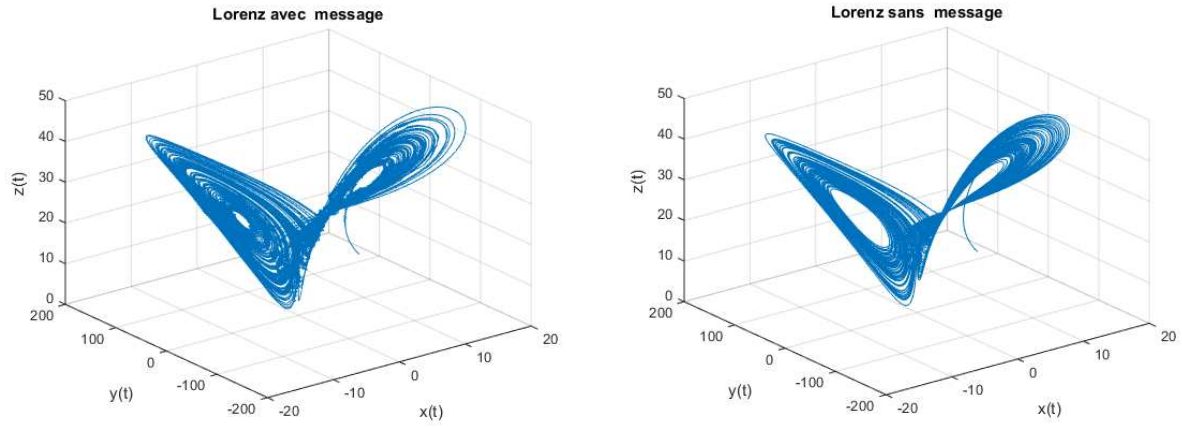


FIGURE 5.2 – Portrait de phase du système de "Lorenz" sans et avec message .

•Processus de Cryptage

Afin de crypter le message, nous l'avons introduit dans la dynamique du système par la méthode de cryptage chaotique dite "méthode de cryptage par inclusion", citée dans le chapitre 2 section (2.6).

Le portrait de phase nous renseigne sur le comportement chaotique du système et comme le montre la figure (5.2), le système en présence du message garde son comportement chaotique.

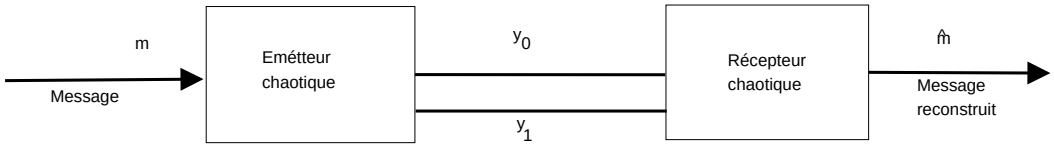


FIGURE 5.3 – Schéma de transmission .

Une fois que le message est introduit dans la dynamique du système chaotique,il est transmis au récepteur par l'intermédiaire de deux canaux de transmission,l'un pour transmettre la sortie "y_0", le second, pour transmettre la sortie "y_1", et ce schéma de transmission est illustré par la figure (5.3). Notons que le message m(t) est aussi présent dans la sortie y(t) envoyé à l'émetteur

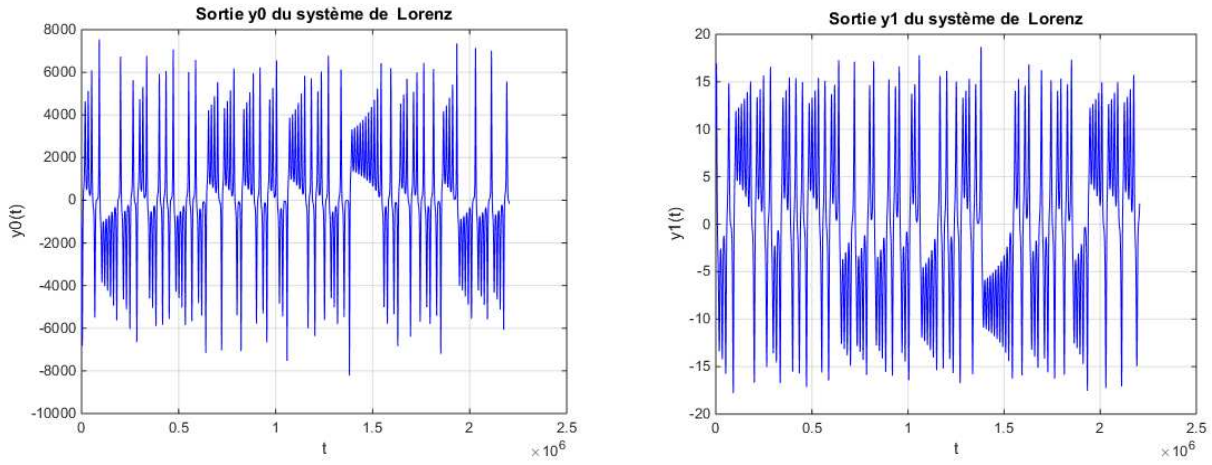


FIGURE 5.4 – Sortie y0 et y1 de l'émetteur,

En observant le tracés des deux sorties sur la figure(5.4), on constate que "y0" , qui contient le message présente un aspect aléatoire. Ce qui signifie que le message est parfaitement noyé dans la dynamique chaotique du système de "Lorenz".

5.3.2.2 Étude du récepteur

•Processus de synchronisation et décryptage

Pour pouvoir restituer le message au niveau du récepteur, ce dernier doit être synchronisé avec l'émetteur. Sachant qu'il existe plusieurs méthodes de synchronisation ; dans notre travail, nous avons utilisé la méthode de synchronisation dite "synchronisation par observateurs" , de type bidirectionnelle citée dans le chapitre 3 section(3.5) l'observateur que nous avons utilisé dans cette partie est l'observateur de Luenberger présenté dans [47] par le système d'équation suivant :

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + g_1(y_1 - \hat{y}_1) \\ \dot{\hat{x}}_2 = -a(1-c)\hat{x}_1 - (a+1)\hat{x}_2 + (y_0 - \hat{y}_0) + g_2(y_1 - \hat{y}_1) + \hat{p} \\ \dot{\hat{x}}_3 = -b\hat{x}_3 + \hat{x}_1(\frac{\hat{x}_2}{a} + \hat{x}_1) \\ \dot{\hat{w}} = S\hat{w} + G_0(y_1 - \hat{y}_1) \end{cases} \tag{5.3}$$

$$\begin{cases} \hat{y}_0 = \hat{x}_1 + \hat{x}_2 \\ \hat{y}_{1=}\hat{x}_1 \\ \hat{m} = y_0 - \hat{y}_0 + a\hat{x}_1\hat{x}_3 \end{cases} \tag{5.4}$$

où $(\hat{x}_1, \hat{x}_2, \hat{x}_3)$ désigne le vecteur des estimés des variables d'état.

$\hat{m}$: le message estimé .

$\hat{p}$: la perturbation estimée.

avec :

$g_1 = 18, g_2 = 392$et $G_0 = [1085, 441, 904, 707]$

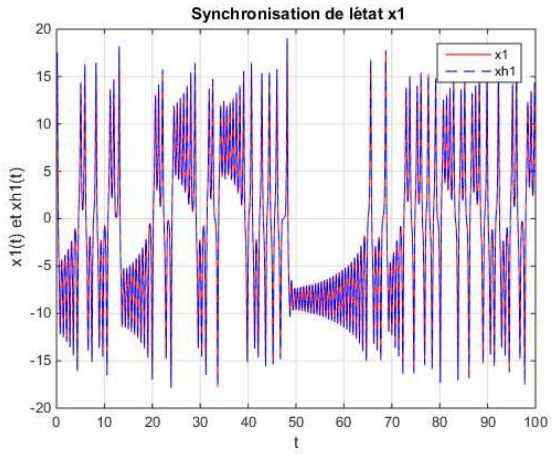


FIGURE 5.5 – Synchronisation de l'état $x_1$et son estimé $\hat{x}_1$

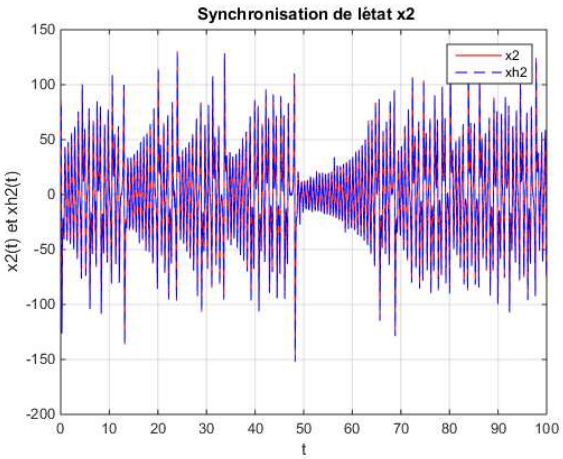


FIGURE 5.6 – Synchronisation de l'état $x_2$et son estimé $\hat{x}_2$

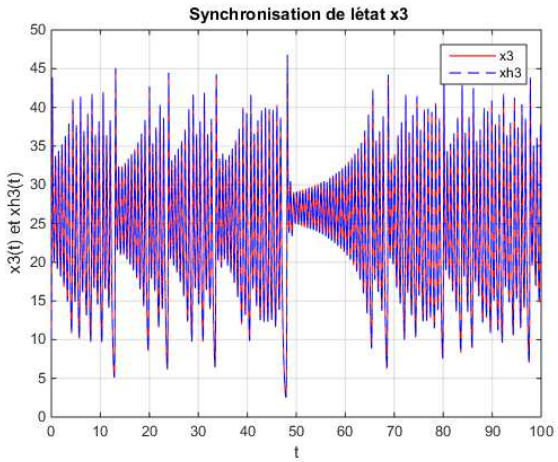


FIGURE 5.7 – Synchronisation de l'état $x_3$et son estimé $\hat{x}_3$

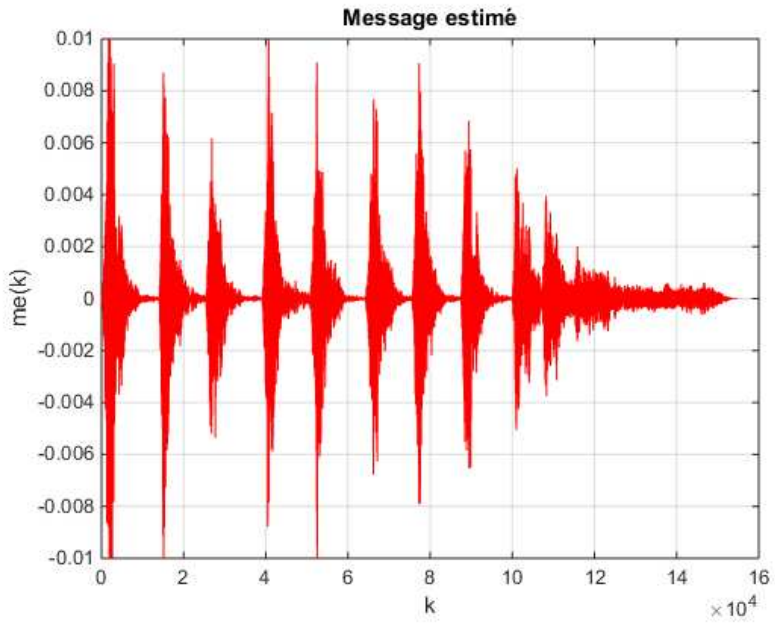


FIGURE 5.8 – Message reconstruit.

On considère le système des variations d'erreurs entre l'émetteur et le récepteur suivant :

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_w \end{bmatrix} = \begin{bmatrix} -g_1 & 1 & 0 \\ -(a(1-c)+1+g_2) & -(a+2) & V_0 \\ -G_0 & 0 & S \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_w \end{bmatrix} \tag{5.5}$$

$\dot{e} = Ae$

$e_1 = x_1 - \hat{x}_1$

$e_2 = x_2 - \hat{x}_2$

$e_w = w - \hat{w}$

S :Matrice d'état du système de perturbation.

$S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

$V_0 = \begin{bmatrix} 1 & 0 \end{bmatrix}$

Le vecteur G_0 ainsi que les paramètres g_1 et g_2 sont des paramètres choisis de manière à satisfaire la stabilité de la matrice A (valeurs propres de A à partie réelle strictement négative). Qui ont été démontré dans l'article [47]

Les états du système sont parfaitement reconstruits comme le montre les figures (5.5), (5.6), et (5.7) par conséquent le récepteur est parfaitement synchronisé. Le message est correctement reconstruit comme le montre la figure(5.8) :

5.3.3 Cas fractionnaire

Dans cette partie nous avons repris le système de "Lorenz", décrit par le système d'équations (5.1), dont nous avons remplacé ses dérivées d'ordre entier par des dérivées d'ordre fractionnaire en utilisant la dérivée fractionnaire au sens de Grünwald-Letnikov citée dans le chapitre quatre section (4.2).

5.3.3.1 Étude de l'émetteur

Le système obtenu après dérivation fractionnaire est le suivant :

$$\begin{cases} D^{\alpha}x_1 = x_2 \\ D^{\alpha}x_2 = -a(1-c)x_1 - (a+1)x_2 - ax_1x_3 + m + p \\ D^{\alpha}x_3 = -bx_3 + x_1(\frac{x_2}{a} + x_1) \end{cases} \tag{5.6}$$

$$\begin{cases} y_0 = x_1 + x_2 - ax_1x_3 + m(t) \\ y_1 = x_1 \end{cases} \tag{5.7}$$

Pour la perturbation, elle est générée comme dans le cas entier. Nous avons pris N=1 , $D^{\alpha}w = Sw$.

$S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

Pour des conditions initiales $(x_1(0), x_2(0), x_3(0)) = (0.1; -0.1; 0.1)$

$\alpha = 0.97$ désigne l'ordre de dérivation fractionnaire du système de "Lorenz" .

Nous avons également utilisé les même valeurs des paramètres a, b, c que dans le cas entier. Cependant le paramètre α est choisi de manière à conserver le comportement chaotique du système. Comme le montre la figure(5.9) où sont tracés, les attracteurs étranges dans le cas avec message et dans le cas sans message.

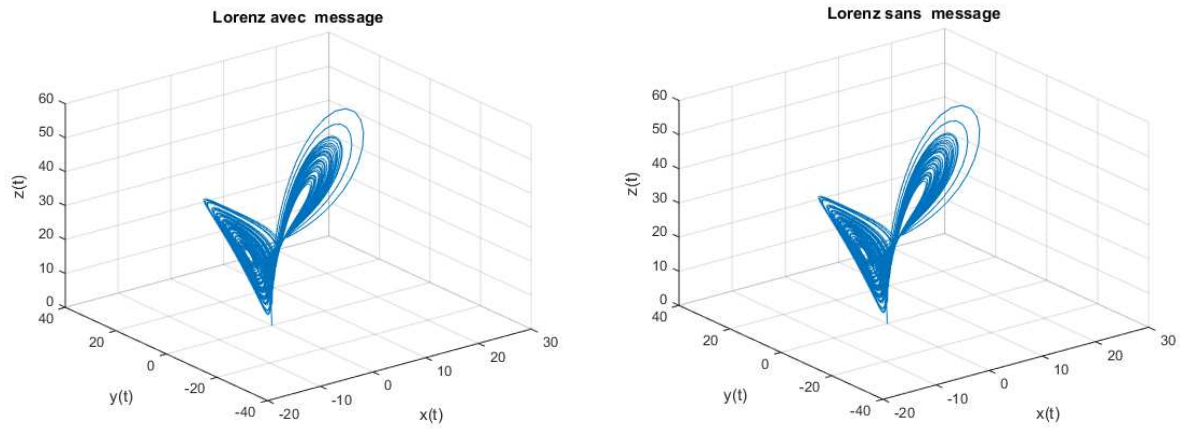


FIGURE 5.9 – Portrait de phase du système de "Lorenz"d'ordre fractionnaire avec et sans message.

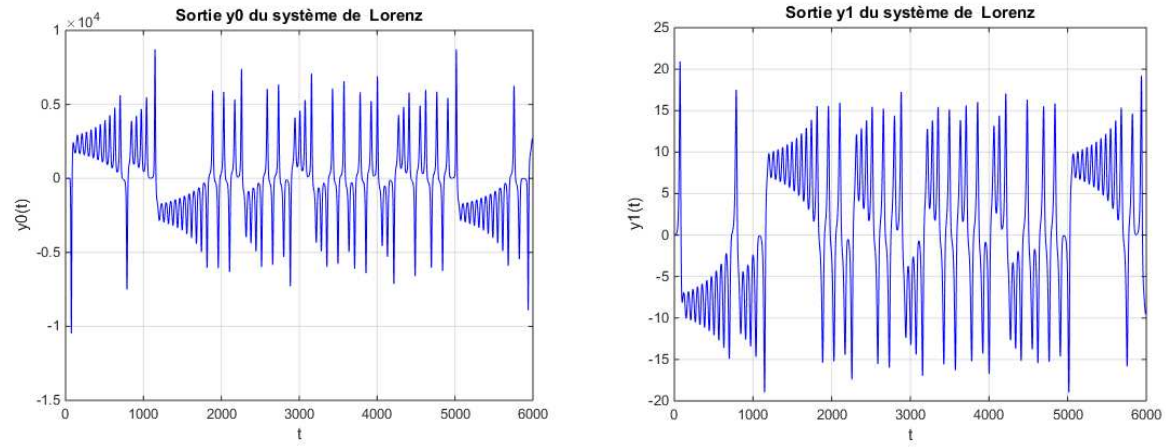


FIGURE 5.10 – Sorties "y_0" et "y_1" de l'émetteur.

En observant la figure (5.10), on remarque que la sortie "y_0" qui contient le message présente un aspect aléatoire ce qui signifie que le message est parfaitement noyé dans la dynamique chaotique de l'émetteur.

•Processus de cryptage

Le message est crypté par la même méthode utilisée dans le cas entier dite "par inclusion".

5.3.3.2 Étude du récepteur

Synchronisation et décryptage

Après cryptage,les deux signaux de sortie sont transmis suivant le schéma de transmission illustré par la figure (5.3). Pour la synchronisation, nous avons utilisé le même observateur proposé dans le cas entier en y appliquant les dérivées d'ordre fractionnaires .

Le modèle qui décrit l'observateur d'ordre fractionnaire est le suivant :

$$\begin{cases} D^{\alpha}\hat{x}_1 = \hat{x}_2 + g_1(y_1 - \hat{y}_1) \\ D^{\alpha}\hat{x}_2 = -a(1-c)\hat{x}_1 - (a+1)\hat{x}_2 + (y_0 - \hat{y}_0) + g_2(y_1 - \hat{y}_1) + \hat{p} \\ D^{\alpha}\hat{x}_3 = -b\hat{x}_3 + \hat{x}_1(\frac{\hat{x}_2}{a} + \hat{x}_1) \\ D^{\alpha}\hat{w} = S\hat{w}_4 + G_0(y_1 - \hat{y}_1) \end{cases} \tag{5.8}$$

$$\begin{cases} \hat{y}_0 = \hat{x}_1 + \hat{x}_2 \\ \hat{y}_{1=}\hat{x}_1 \\ \hat{m} = y_0 - \hat{y}_0 + a\hat{x}_1\hat{x}_3 \end{cases} \tag{5.9}$$

S :Matrice d'état du système de perturbation.

$\hat{p}$: désigne la perturbation estimée.

$\hat{m}$ est le message reconstruit.

g_1, g_2et G_0 sont choisis de telle manière à satisfaire le critère de stabilité des systèmes d'ordre fractionnaire linéaire.

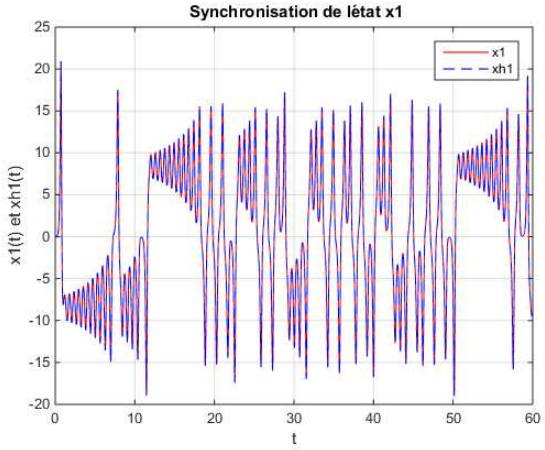


FIGURE 5.11 – Synchronisation de l'état $x_1$et son estimé $\hat{x}_1$.

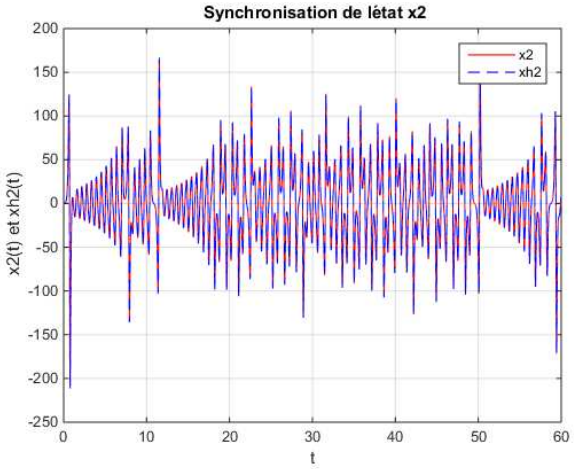


FIGURE 5.12 – Synchronisation de l'état $x_2$et son estimé $\hat{x}_2$.

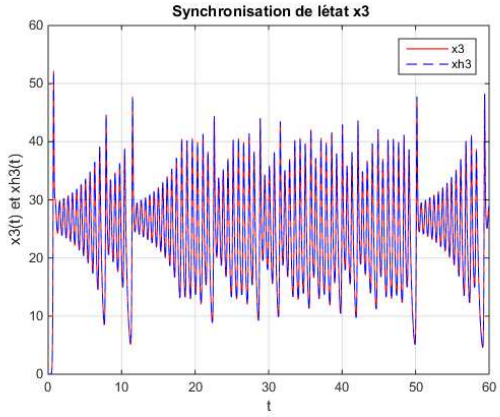


FIGURE 5.13 – Synchronisation de l'état $x_3$et son estimé $\hat{x}_3$.

Les états x_1 et x_2 et x_3 sont parfaitement reconstruit comme le montre les figure(5.11), (5.12), et (5.13) par conséquent le récepteur est parfaitement synchronisé, et le message est totalement reconstruit illustré par la figure(5.14) :

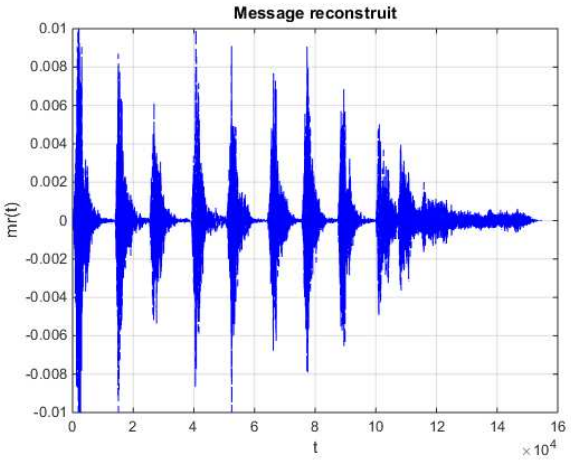


FIGURE 5.14 – Message reconstruit

Afin de mieux illustrer l'utilité de l'ordre de dérivation α pour la transmission sécurisée nous avons varié le paramètre α au niveau du récepteur. En effet pour α de l'émetteur différent de α du récepteur. Le système de cryptage présente une grande sensibilité par rapport au paramètre α. Ce paramètre est utilisé comme clé de sécurité difficile voire même impossible à identifier . Donc l'utilisation des systèmes d'ordre fractionnaire améliore généralement la sécurité.

Pour $\alpha_{rec} = 0.8$ le message n'est plus reconstruit comme le montre la figure (5.15)

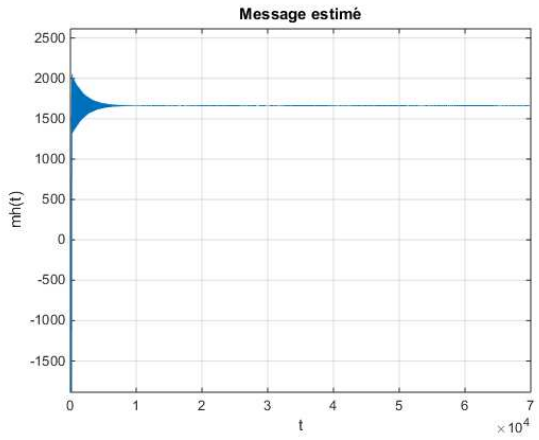


FIGURE 5.15 – Variation du paramètre α.

5.4 Cryptage d'un système chaotique en temps discret

5.4.1 Cas entier

5.4.1.1 Étude de l'émetteur

On considère le système discret hyperchaotique de Hénon modifié d'ordre entier donné par le système d'équation suivant (5.10). [48]

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) + m(k) \\ y(k) = x_2(k) \end{cases} \tag{5.10}$$

où (x_1, x_2, x_3) désigne le vecteur d'état et $y(k)$ sa sortie.

$m(k)$ est le message.

Nous avons tracé le portrait de phase du système avec et sans message pour les paramètres suivants :

a=1.5 et b=0.1

$(x_1(0), x_2(0), x_3(0)) = \begin{bmatrix} -0.1 & 0.5 & 0.1 \end{bmatrix}$:vecteur des conditions initiales.

Le système garde son comportement chaotique même en présence du message dans sa dynamique, comme le montre la figure (5.16).

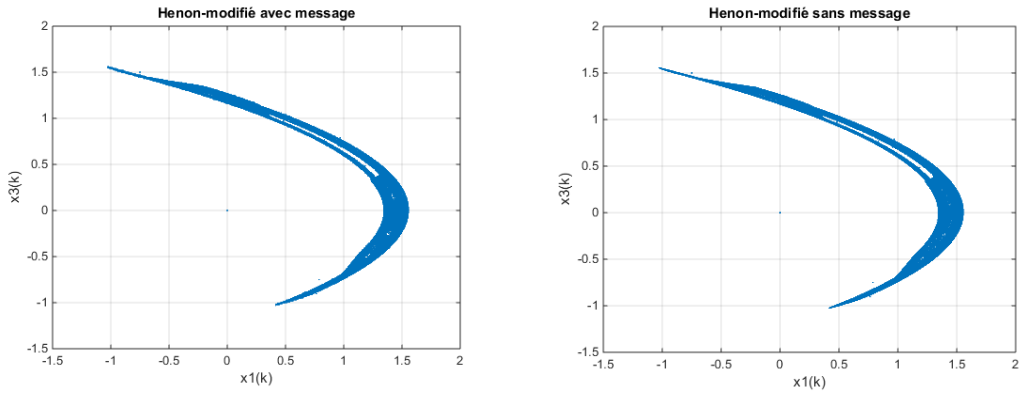


FIGURE 5.16 – Portraits de phase du système d'Hénon modifié avec et sans message.

•Processus de cryptage

L'insertion du message dans la dynamique du système est établie de la même manière que dans le cas continu, en effet la méthode de cryptage utilisé est la "méthode par inclusion ".

Le signal de sortie y(k) est ensuite transmis au récepteur, en suivant le schéma de transmission à un seul canal illustré par la figure (5.17) :

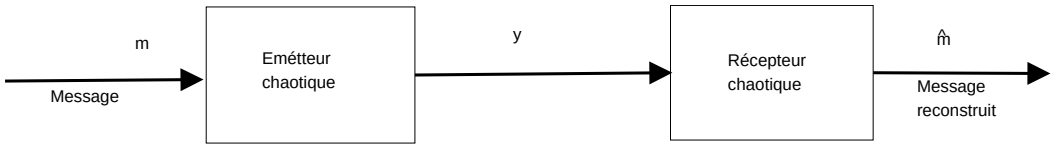


FIGURE 5.17 – Schéma de transmission .

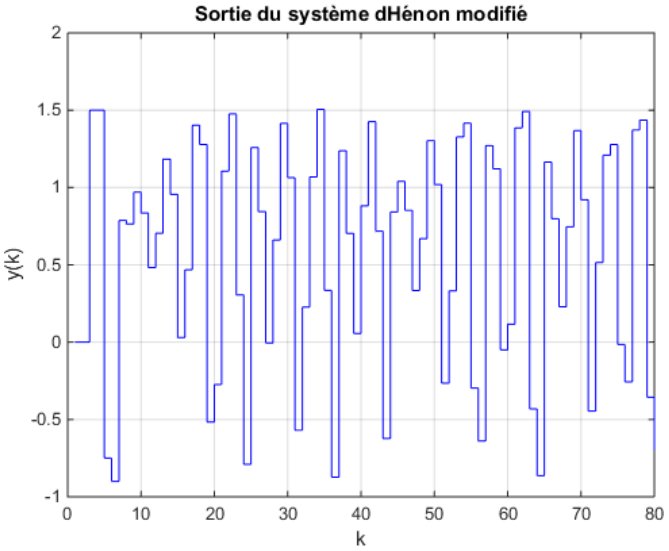


FIGURE 5.18 – Sortie de l'émetteur y(k) .

L'inclusion du message m(k) dans la dynamique de la troisième variable $x_3(k)$ satisfait les conditions d'observabilité et de recouvrement d'observabilité [7,51,52]

5.4.1.2 Étude du récepteur

Processus de synchronisation et décryptage

Pour la synchronisation dans le cas discret nous avons opté pour" l'observateur discret retardée étape par étape ", cet observateur permet de reconstruire tout les états et l'entrée inconnue du système à partir de la sortie du système transmise et de ses itérés [49,50], qu'on désigne par le système d'équation suivant :

$$\begin{cases} \hat{x}_1(k-1) = y(k) \\ \hat{x}_3(k-2) = \frac{1}{b}[a - y^2(k-2) - \hat{x}_1(k-1) \\ \hat{m}(k-3) = \hat{x}_3(k-2) - y(k-3) \end{cases} \tag{5.11}$$

La transmission est réalisée en transmettant la sortie y(k) par l'intermédiaire d'un canal de transmission.

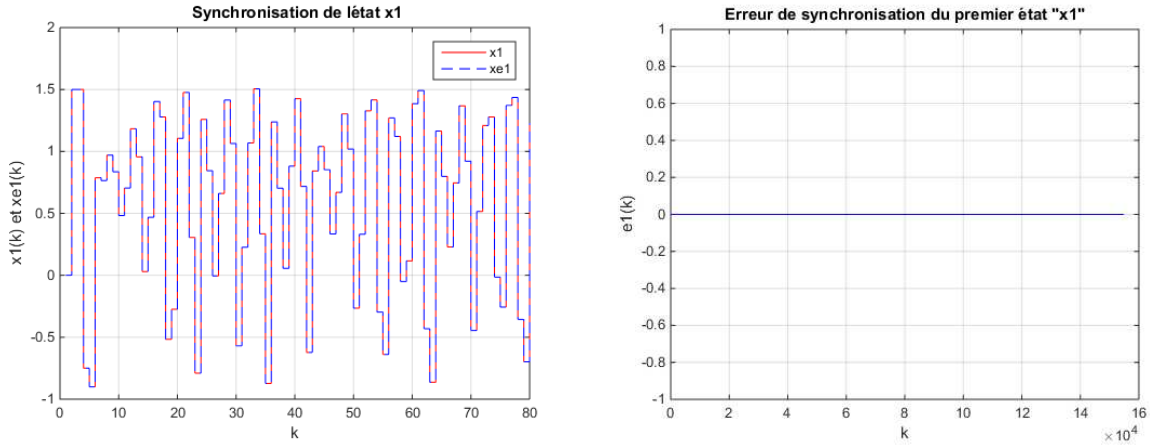


FIGURE 5.19 – Synchronisation de l'état $x_1$et son estimé $\hat{x}_1$et son erreur .

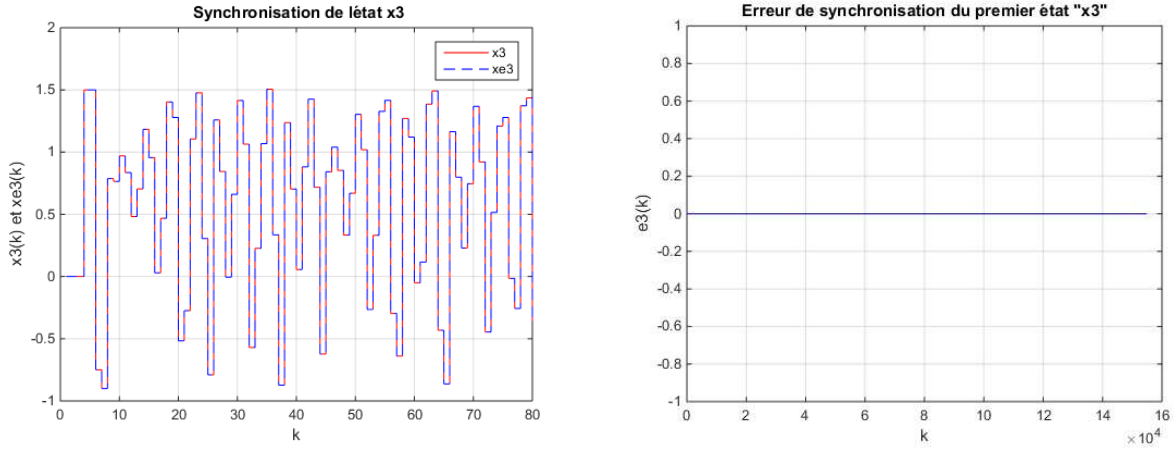


FIGURE 5.20 – Synchronisation de l'état $x_3$et son estimé $\hat{x}_3$et son erreur .

Les états x_1 et x_3 du système sont parfaitement reconstruit comme le montrent les figures (5.19), (5.20), ainsi que les erreurs de synchronisation qui convergent vers zéro par conséquent le récepteur est parfaitement synchronisé, et le message est totalement reconstruit illustré par la figure(5.21) :

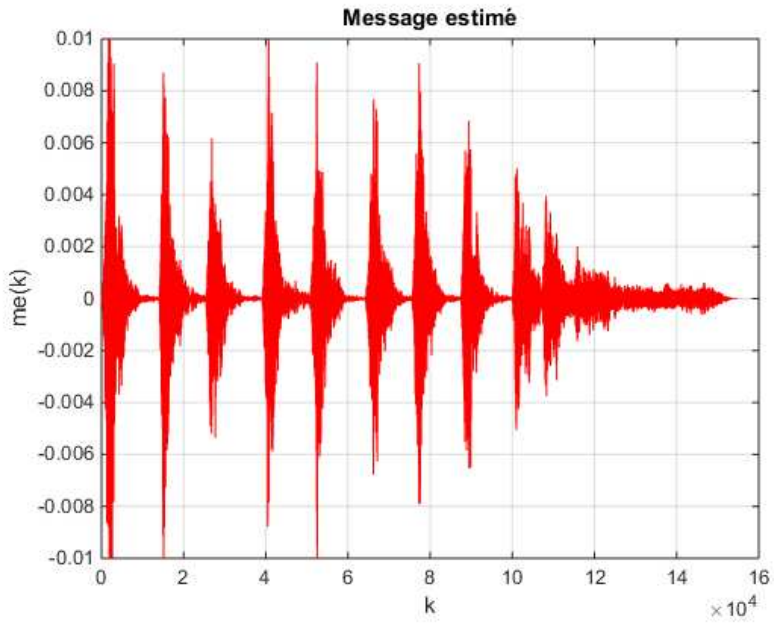


FIGURE 5.21 – Message reconstruit .

5.4.2 Cas fractionnaire

Dans cette partie nous avons repris le système de "Hénon-Modifié", décrit par le système d'équations (5.10), dont nous avons remplacé l'opérateur de différence d'ordre entier par l'opérateur de différence de Grünwald Letnikov d'ordre fractionnaire cité dans le chapitre 4.

5.4.2.1 Étude de l'émetteur

L'émetteur est décrit par le modèle suivant :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \mu_1 \\ x_2(k+1) = x_1(k) + (\alpha_2 - 1)x_2(k) + \mu_2 \\ x_3(k+1) = x_2(k) + (\alpha_3 - 1)x_3(k) + \mu_3 + m(k) \\ y(k) = x_2(k) \end{cases} \tag{5.12}$$

Les mémoires du système d'ordre fractionnaire décrit par l'équation suivantes :
$\mu_1 = \sum_{p=1}^{L} C_{p1} x_1(k-p)$
$\mu_2 = \sum_{p=1}^{L} C_{p2} x_2(k-p)$
$\mu_3 = \sum_{p=1}^{L} C_{p3} x_3(k-p)$
Nous avons choisis comme paramètres :
a=1.5 et b=0.1
Notons que dans le cas discret, nous avons pris des ordres de différence différents (cas non commensurables)

$\alpha_1 = 0.91$, $\alpha_2 = 0.95$, $\alpha_3 = 0.90$

L=5 qui désigne la longueur de la mémoire

et le vecteur des conditions initiales est

$(x_1(0), x_2(0), x_3(0))$=(-0.1,0.5,0.1)

Nous avons tracé le portrait de phase du système avec et sans message qui est illustré par la figure(5.22) qui montre que le système garde son comportement chaotique même après insertion du message.

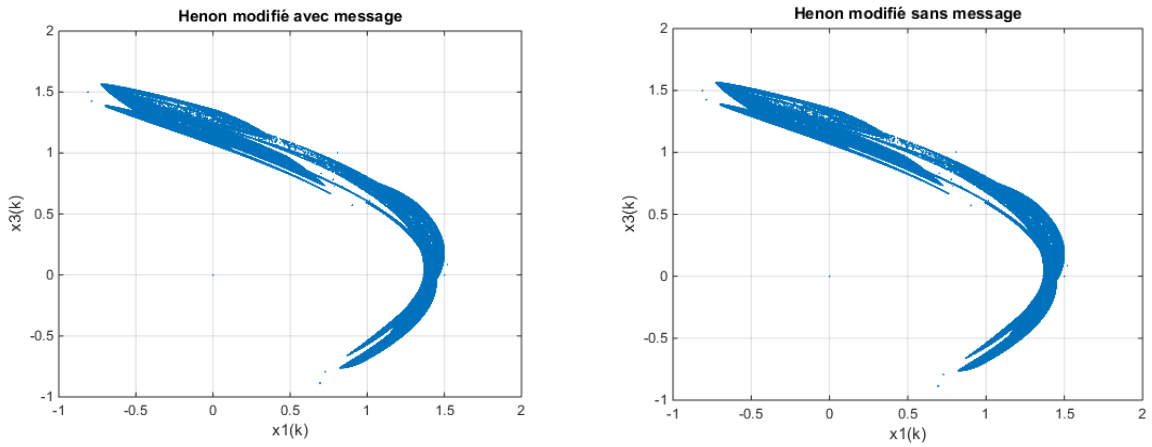


FIGURE 5.22 – Portraits de phase du système d'Hénon modifié d'ordre fractionnaire avec et sans message.

•Processus de cryptage

Le message est crypté par la méthode dite "par inclusion", en l'introduisant dans le troisième état du système, ainsi la sortie du système y(k) est ensuite transmise au récepteur en suivant le même schéma utilisé pour le cas entier illustré par la figure (5.17).

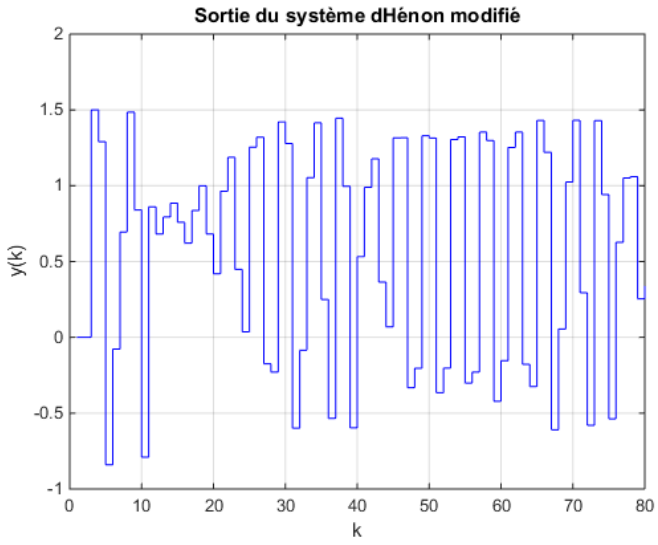


FIGURE 5.23 – Sortie de l'émetteur y(k) .

En observant le tracé de la sortie y(k) représenté par la figure (5.23) on remarque que le signal de sortie présente un aspect aléatoire.

5.4.2.2 Étude du récepteur

•Synchronisation et décryptage

Le récepteur est synchronisé avec l'émetteur par le même observateur utilisé dans le cas entier. En y appliquant la différence de Grünwald Letnikov d'ordre fractionnaire et nous avons obtenu le système suivant :

$$\begin{cases} \hat{x}_1(k-1) = y(k) - (\alpha_2 - 1)y(k-1) + \mu'_2 \\ \hat{x}_3(k-2) = \frac{1}{b}[a - y^2(k-2) - \hat{x}_1(k-1) + (\alpha_1 - 1)\hat{x}_1(k-2) + \mu'_1 \\ \hat{m}(k-3) = \hat{x}_3(k-2) - y(k-3) - (\alpha_3 - 1)\hat{x}_3(k-3) + \mu'_3 \end{cases} \tag{5.13}$$

avec :

$\mu'_2 = \sum_{p=1}^{L} C_{p2}\hat{x}_2(k-p-1)$

$\mu'_1 = \sum_{p=1}^{L} C_{p1}\hat{x}_1(k-p-2)$

$\mu'_3 = \sum_{p=1}^{L} C_{p3}\hat{x}_3(k-p-3)$

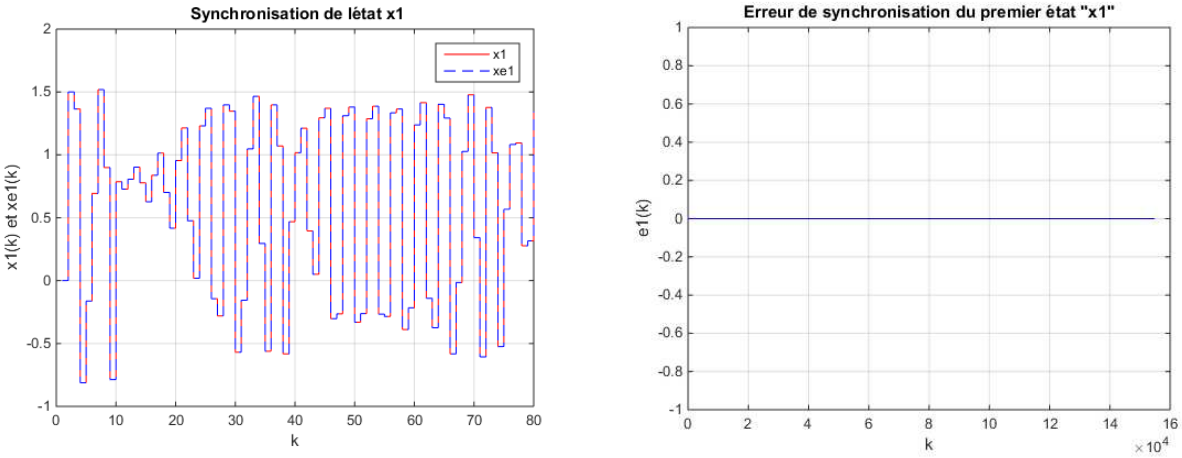


FIGURE 5.24 – Synchronisation de l'état $x_1$et son estimé $\hat{x}_1$et son erreur .

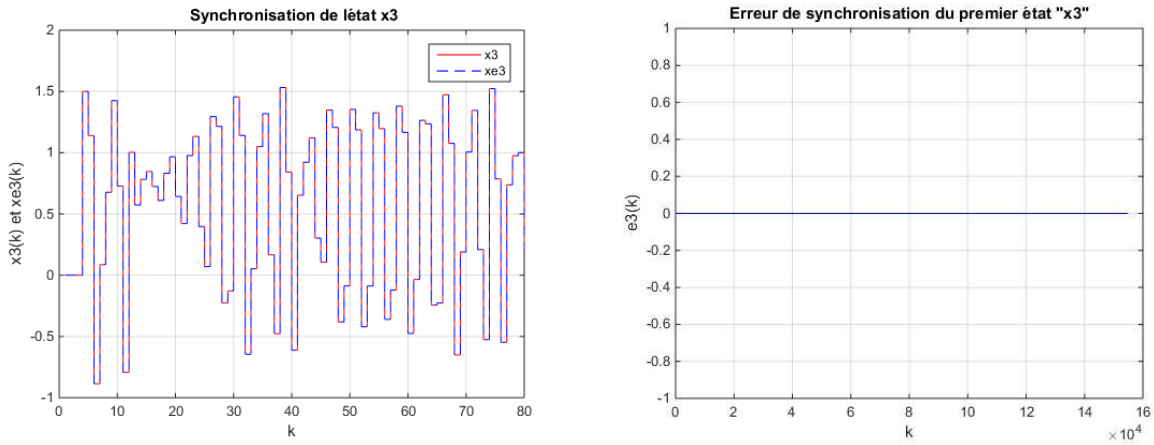


FIGURE 5.25 – Synchronisation de l'état $x_3$et son estimé $\hat{x}_3$et son erreur .

Les états x_1 et x_3 du système sont parfaitement reconstruit comme le montrent les figures (5.24), (5.25), ainsi que les erreurs de synchronisation qui convergent vers 0 par conséquent le récepteur est parfaitement synchronisé, et le message est totalement reconstruit illustré par la figure(5.26) ci-dessous :

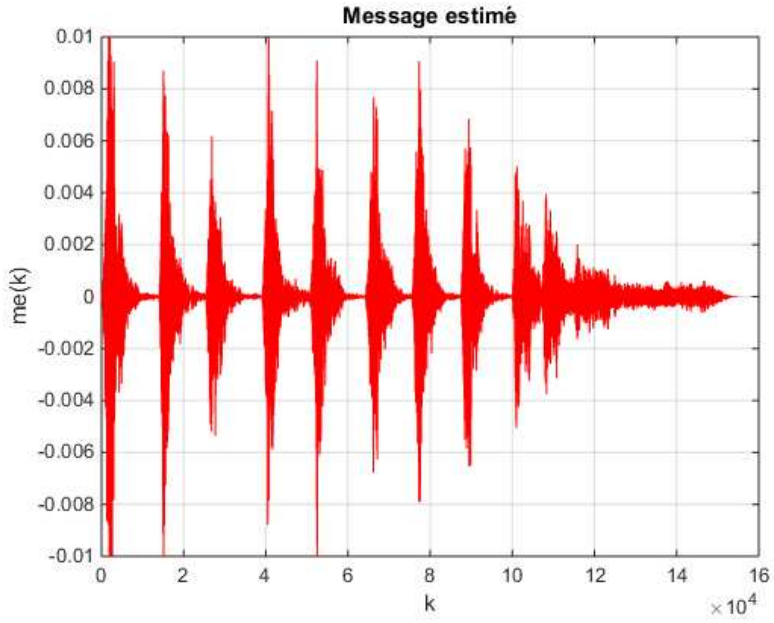


FIGURE 5.26 – Message reconstruit .

Nous avons également varier l'un des ordre de dérivation α_2.Pour $\alpha_2 = 0.959$ et nous avons obtenu le même résultat que pour le cas continu. En effet le message n'est pas reconstruit. Ceci démontre l'avantage d'utiliser les systèmes chaotiques d'ordre fractionnaires dans la transmission sécurisée de données.

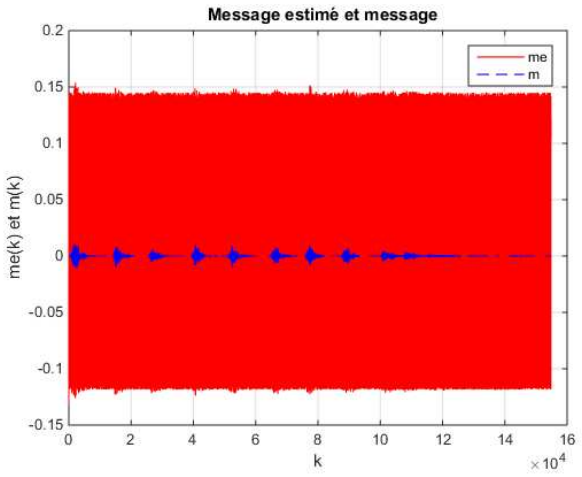


FIGURE 5.27 – Variation du paramètre α.

5.5 Conclusion

A travers ce chapitre, nous avons présenté quelques schémas de transmission sécurisée de la parole, se basant sur la synchronisation des systèmes chaotiques, nous avons étudié le cas des systèmes continus et le cas des systèmes discrets, Nous avons de même exploiter la dynamique d'ordre fractionnaire afin d'améliorer la sécurité

Les résultats de simulation ont montré que l'introduction des dérivées d'ordre fractionnaire(cas continu), différences d'ordre fractionnaire, ainsi que la longeur de la mémoire L (cas discret) a permis de renforcer les crypto-systèmes en termes de sécurité. En effet ces paramètres supplémentaires sont utilisés comme clés secrète.

Conclusion générale

L'objectif de ce travail de mémoire est la conception des schémas de transmission sécurisée, en temps continu et en temps discret, à base des systèmes chaotiques d'ordre entier et d'ordre fractionnaire.

Nous avons d'abord introduit la théorie du chaos et les propriétés d'un système chaotique. Nous avons également cité les différentes classes de cryptographie et les méthodes du cryptage par chaos. Ensuite, nous avons présenté le principe de la synchronisation chaotique dont nous avons introduit ses différentes approches ainsi que la synchronisation par observateurs Et en dernier lieu de la partie théorique, nous avons énoncé les différents théorèmes fondamentaux du calcul d'ordre fractionnaire dans les systèmes dynamiques en temps continu et discret.

Nous avons présenté deux schémas de transmissions en temps continu et en temps discret. Dans le premier schéma de transmission nous avons utilisé le système chaotique de « Lorenz » comme émetteur décrit par des équations différentielles ,et un observateur de Luenberger comme récepteur afin d'accomplir le processus de synchronisation, ensuite nous avons amélioré ce schéma de transmission en introduisant les dérivées d'ordre fractionnaires.

Dans le second schéma de transmission nous avons opté pour le système « Hénon modifié » comme émetteur, et nous avons choisi l'observateur retardé étape par étape comme récepteur pour synchroniser ce dernier avec l'émetteur, que nous avons également améliorer en introduisant les différences d'ordre fractionnaire.

En général le message est considéré comme une entrée inconnue pour l'émetteur. Cette entrée inconnue est reconstruite par le récepteur une fois que celui ci a été synchronisé avec l'émetteur. Nous avons utilisé la technique de cryptage par inclusion. Nous avons testé notre schéma de transmission sécurisée, par l'envoi d'un signal « parole ». La méthode de cryptage par inclusion a présenté plus de sensibilité à la variation de la clé de décryptage(les ordres de dérivation fractionnaires), donc le crypto-système chaotique fractionnaire a prouvé effectivement avec la méthode de cryptage son efficacité en termes de sécurité pour les schémas de transmissions sécurisées.

Les paramètres propres aux systèmes fractionnaires qui sont les ordres de dérivation (cas continu), les ordres de différence et la longueur de la mémoire (cas discret) sont des paramètres supplémentaires utilisés comme clés de sécurité. L'espace de la clé est élargit.

Etant donné qu'il n'existe pas actuellement de méthodes permettant d'identifier ces paramètres additionnels, il serait donc difficile à un intrus de casser les crypto-systèmes présentés.

Comme perspectives, nous nous proposons les pointes suivants :

- Développement de nouvelles approches de synchronisation à base d'observateurs pour les système d'ordre fractionnaire.

-Cryptanalyse pour les crypto-systèmes à base du chaos fractionnaire.

- Application des nouvelles approches dans les schémas de transmission sécurisée de données images, vidéos.

Faire une investigation plus approfondie dans la distinction entre les schémas de transmission sécurisée de signaux analogiques et les schémas de transmission sécurisée de signaux digitaux

- Réalisation en pratique des schéma proposés sur des cartes tels que , Arduino, Rasberry.

Bibliographie

[1] F.Rodriguez-Henriquez,A.D.Pérez,N.A.Saqib,Ç.K.Koç.A Brief introduction to modern cryptography.Chapitre du livre :Cryptographic Algorithms on Reconfigurable Hadware.Springer,Boston MA,pp.7-33,2007.

[2] E.N.Lorenz,Deterministic Nonperiodic Flow,J.Atmos.Sci,20(2),pp.130-141,1963.

[3] L.M.Pecora,T.L.Carroll,Synchronization in chaotic systems,Phys.Rev.Lett.64,pp.821-824,1990.

[4] T. Hamaizia,« Systèmes dynamiques et chaos »,Thèse Doctorat,Université de Constantine 1,2013

[5] H.Hamiche,« Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données »,Thèse Doctorat,Université Mouloud Mammeri Tizi Ouzou,2011.

[6] C.Benhabib, Etude d'un système chaotique pour la sécurisation des communications optiques , mémoire , université de tlemcen faculte de technologie , 2014.

[7] S.Kassim,« contribution a la transmission numérique sécurisée de données a base de générateurs de séquences chaotiques d'ordre non entier »,Thèse Doctorat,Université Mouloud Mammeri Tizi Ouzou,2018.

[8] E.Cherrier,« Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires »,Thèse Doctorat,Institut National Polytechnique de Lorraine,2006.

[9] F.Anstett,« Les systemes dynamiques chaotiques pour le chirement : synthese et cryptanalyse »,Thèse Doctorat,Université Henri Poincare- Nancy 1,2006.

[10] A.Adane ,L.Bourahmoune,« Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire »,Mémoire de Master,Université Mouloud Mammeri Tizi Ouzou,2015.

[11] O.Megherbi,« Étude et réalisation d'un systèmes sécurisé à base de systèmes chaotiques »,Mémoire de Magister,Université Mouloud Mammeri Tizi Ouzou,2013.

[12] Z.Elhadj« Étude de quelques types des systèmes chaotiques :Généralisation d'un modèle issu du modèle de Chen »,Thèse Doctorat,Université Mentourid de Constantine Faculté de Sciences,2006.

[13] G.DA Silva,« Introduction aux systèmes dynamiques et chaos »,Engineering school. Institut Polytechnique de Grenoble, 2004, pp.23. <cel-00556972>.

[14] T.Gaël ,« Design et Analyse de sécurité pour les constructions en cryptographie symétrique » ,Thèse Doctorat,Université de Limoges,2015.

[15] N.Kouadri Moustefai,« Tests de validation pour les crypto-systèmes chaotiques »Mémoire de Magister,Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf,2014.

[16] R.Dumont , « Cryptographie et Sécurité informatique »,cours provisoires,Université de Liège Faculté des Sciences Appliquées ,2009-2010.

[17] C.Benhabib,« étude d'un système chaotique pour la sécurisation des communications optiques » ,Mémoire de Master ,Université de Tlemcen faculté de technologie ,2014 .

[18] Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone,« Handbook of Applied Cryptography ».

[19] A.Zemouche,« Sur l'observation de l'état des systèmes dynamiques non linéaires »,Thèse Doctorat,Université Louis Pasteur Strasbourg I,2007.

[20] G. Zheng,« Formes Normales d'Observabilité Paramétrées par les Sorties : Applications au Cryptage par Synchronisation de Systèmes Chaotiques »,Thèse Doctorat,École Doctorale Sciences et Ingénierie de L'université de Cergy-Pontoise,2006.

[21] D.Idiou,« Implémentation Analogique de Dérivateur et d'Intégrateur d'Ordre Fractionnaire Variable »,Mémoire de Magister, Université Mentouri de Constantine,2008.

[22] M.S .Abd Elouahab , « Les systèmes chaotiques à dérivées fractionnaires »,Mémoire de Magister,Université Mentouri de Constantine,2009.

[23] M.Tidjani,« Synchronisation des systèmes dynamiques chaotiques à dérivées fractionnaires »,Thèse Doctorat,Université Constantinne1,2014.

[24] J.Liouville.Mémoire sur le calcul des différentielles à indices quelconques.J.Ecole Polytechnique 13,pp.71-162,1832.

[25] B.Riemann.Versuch einer allgemeinen auffasung der integration und differentiation.Gesammelte Werke,1876.

[26] K.B.Oldham,J.Spanier.The Fractional calculs.Academic Press,New York,1974.

[27] M.Caputo,Linear models of dissipation whose q is almost frequency independent.Geophysical journal of the royal astronomical society.2(13),pp.529-539,1967.

[28] A.K.Grünwald.Uber begrenzte derivationen und deren anwendung.Zeitschrift fur Mathematik und Physik,12,pp.441-480.1867.

[29] A.V.Letnikov.Theory of differentiation with an arbitrary index.Mat.Sb.3,pp.1-66,1868.

[30] I.Petras,« Fractional-Order Nonlinear Systems »,Springer,2011.

[31] I.N'doye,« Généralisation du lemme de Gronwall-Bellman pour la stabilisation des systèmes fractionnaires »,Thèse Doctorat,l'Université Henri Poincaré – Nancy 1 et de l'Université Hassan II Ain Chock – Casablanca,2011.

[32] I.Pdlubny.Fractional Differential Equations,Academic Press,New York,1999.

[33] R.Mansouri.Contribution à l'analyse et à la synthése des systèmes d'ordres fractionnaire par la représentation d'état.Thèse de Doctorat,Université Mouloud Mammeri Tizi Ouzou,2008.

[34] L.Amimer,« Modélisation et Commande des Systèmes Non Linéaires Fractionnaires par des Réseaux de Neurones Fractionnaires »,Mémoire de Magister,Université Mouloud Mammeri Tizi Ouzou,2015.

[35] D.Mozyrska,E.Pawluszewicz.Local controllability of nonlinear discrete-time fractional order systems.Bull.Pol.Ac. :Tech.,61(01),pp.251-256,2013.

[36] F.Chen,X.Luo,Y.Zhou.Existence results for nonlinear fractional difference equation .Advances in Difference Eq.,ID 713201,pp.1-12,2011.

[37] F.M.Atici,P.W.Eloe.Initial value problems in discrete fractional calculus.Proceedings of the American Mathematical Society,137,pp.981-989,2009.

[38] G.-C.Wu,D.Baleanu,H.-P.Xie,F.-L.Chaos synchronization of fractional chaotic maps based on the stability condition.Physica A :Statistical Mechanics and its Applications ,460,pp.374-383,2016.

[39] A.A.kilbas,H.M.Srivastava,J.J.Trujillo.Theory and application of fractional differential equations.In :vanMilll,J.(ed)North Holland Mathematics studies.Elsevier,Amsterdam,2006.

[40] A. Oustaloup, F. Levron, B. Mathiew, and F. Nanot. Frequency-band complex noninteger differentiator : characterization and synthesis". IEEE Transactions on Circuits and Systems I, vol.47, n°1, pp.25-39, 2000.

[41] A. Oustaloup. La commande CRONE. Editions HERMES, Paris, 1991.

[42] A. Oustaloup. La Dérivation non entière : théorie, synthèse et applications. Editions HERMES, Paris, 1995.

[43] A. Charef, H. H. Sun, Y. Y. Tsao, and B. Onaral. Fractal system as represented by singularity function". IEEE Transactions on Automatic Control, vol.37, n°9, pp.14651470, 1992.

[44] G. E. Carlson and C. Halijak. Approximation of fractional capacitors by a regular Newton process. IEEE Transactions on Circuits and Systems, vol.11, n°2, pp.210-213, 1964.

[45] K. Matsuda and H. Fujii. Optimised wave absorbing control : analytical and experimental results. J. Guidance Control and Dynamics, vol.16, n°6, pp.1146-1153, 1993.

[46] A.Benkhelifa et A.Ghoul« Synchronisation des Systèmes Chaotiques Fractionnaires »,Mémoire de Master,Université de larbi Tébessi – Tébessa ,2016.

[47] G.Oberfon-Pulido,A.Torres-Gonzalez,R.Cardenas-Rodriguez,G.Solis-Perales,Encryption in chaotic systems with sinusoidal excitations.Article ID 782629,7 pages.Mexico.2014

[48] Richter, H. (2002) The generalized Hénon maps : examples for higher dimentional chaos, International Journal of Bifurcation and chaos 12(6) : 1371-1381.

[49] Sira-Ramirez,H. ,Aguilar-Ibaaez,C.and Suarez-Castaan,M(2002).Ewact state reconstruction in the recovery of messages encrypted by the state of nonlinear discrete-time chaotic systems, International Journal of Bifurcation and chaos 12(1) :169-177.

[50] Belmouhoub, I., Djemai. M and Barbot, J-P (2003). An example on nonlineair discrete-time synchronization of chaotic systems for secure communications, European Control Conference (ECC), Cambridge.

[51] S.Kassim,H.Hamiche,S.Djennoune,M.Bettayeb,S.Guermah,M.Lahdir,Secure data transmission scheme based on fractional-order discrete chaotic system,International Conference on Control,Engineering and Information Technology(CEIT'2015).Tlemcen,Algeria,2015.

[52] S.Kassim,H.Hamiche,S.Djennoune,M.Bettayeb,O.Megherbi,A novel robust image transmission scheme based on fractional-order discrete chaotic systems,International Workshop on cryptography and its application (IWCA'16).Oran,Algeria,2016.

Résumé :

Ce présent travail vise à étudier et à concevoir des schémas de transmission sécurisée, en temps continu et en temps discret, à base des systèmes chaotiques d'ordre entier et d'ordre fractionnaire. Ainsi que l'utilisation des systèmes dynamiques chaotiques dans la cryptographie et son application au cryptage de la parole.

Ces schémas ont pour structure de base, un émetteur dont on introduit le message parole confidentiel par la méthode de cryptage chaotique dite « méthode par inclusion », et un récepteur qui lui seul sera apte à reconstruire le message en le synchronisant avec l'émetteur par la synchronisation observateurs.

L'introduction du calcul fractionnaire, a permis de renforcer la sécurité de ces schémas de transmission. En effet, les crypto-systèmes chaotiques d'ordre fractionnaire dont les ordres de dérivation (temps continu) et ordres de différence (Cas discret) peuvent être utilisé comme paramètres de sécurité qui permettent d'élargir l'espace de la clé.

Mots clés : crypto-systèmes, cryptographie, chaos, chiffrement, parole, synchronisation.

Abstract :

This work aims at studying and designing secure transmission schemes, in continuous time and in discrete time, based on the chaotic systems of integer order and fractional order. As well as the use of chaotic dynamic systems in cryptography and its application to speech encryption.

These schemas have as their basic structure, a transmitter whose confidential speech message is introduced by the chaotic encryption method known as the "inclusion method", and a receiver which alone will be able to reconstruct the message by synchronizing it with the transmitter by synchronization observers.

The introduction of fractional calculation has made it possible to reinforce the security of these transmission schemes. Indeed, fractional order chaotic crypto-systems whose derivation orders (continuous time) and difference orders(Discrete case) can be used as security parameters that allow to widen the space of the key.

Key words : crypto-systems , cryptography, chaos, encryption , speech, synchronizing,