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

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

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'AUTOMATIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Spécialité : **Automatique**

Option : **Commande des Systèmes**

Présenté par

Amirouche ADANE

Lylia BOURAHMOUNE

Mémoire dirigé par **Mr Hamid HAMICHE** et co-dirigé par **Mr Saïd DJENNOUNE**

Thème

Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire

Mémoire soutenu publiquement le 09 septembre 2015 devant le jury composé de :

Mr Saïd GUERMAH
MCA, UMMTO, Président

Mr Hamid HAMICHE
MCA, UMMTO, Rapporteur

Mr Saïd DJENNOUNE
Pr, UMMTO, Co-Rapporteur

Mr Amar SI AMMOUR
MCA, UMMTO, Examinateur

Mr Ahmed MAIDI
MCA, UMMTO, Examinateur

Mlle Ouerdia MEGHERBI
Doctorante, UMMTO, Invitée

Ce travail a été préparé au sein du Laboratoire de Conception et de Conduite des Systèmes de Production (L2CSP), UMMTO.

Remerciement

Nos remerciements les plus sincères vont à notre encadreur *Mr H.Hamiche* pour sa disponibilité et sa patience, on salue toutes ses qualités humaines : sa modestie, sa générosité et sa gentillesse… On lui est reconnaissant pour tout ce qu'il nous a apporté sur le plan scientifique et pour tout ce que nous avons appris au près de lui au laboratoire L2CSP.

Nous tenons particulièrement à exprimer notre profonde gratitude à *Mr S.Djennoune*, notre co-encadreur de projet, qui a suivi l'évolution de notre travail avec une disponibilité permanente.

On ne manquera pas de remercier tout les membres du jury pour nous avoir honorés par leur présence et pour avoir accepter d'évaluer notre travail.

Enfin, que tous ceux, qui de près ou de loin, ont participé à l'élaboration de ce travail trouvent ici l'expression de nos meilleurs remerciements.

Dédicaces

On dédie ce modeste travail à nos parents qui ont eu foi en nous et qui ont su être là pour nous soutenir et nous encourager durant le long de nos études.

A tout les membres de nos familles ainsi qu'à tout nos amis(e).

Merci à vous.

Lylia & Amirouche

Sommaire

Liste des figures

Liste des tableaux

Introduction générale

Introduction générale

La cryptographie, véritable science régissant le codage de l'information [1], a connu une réelle explosion avec le développement des systèmes informatiques, passant d'une ère artisanale à des systèmes de très hautes technologies nécessitant une importante puissance de calcul. Elle a connu un plus large essor encore avec l'arrivée des systèmes de communications modernes (Internet,...etc.) [2], où il y a une nécessité absolue de protéger les données échangées des individus. Parallèlement, une autre branche ennemie à la cryptographie appelée la cryptanalyse a été développée, qui est l'art de révéler les textes en clair qui ont été l'objet d'un chiffrement sans connaître la clé de déchiffrement.

De nos jours, les chercheurs portent un grand intérêt pour l'étude des phénomènes chaotiques, ainsi de nombreux travaux ont été fait sur le chaos d'une manière générale [3][4][5]. Ces travaux ont conduit à la généralisation de son utilisation dans divers domaines des sciences.
L'emploi du chaos pour la transmission sécurisée de l'information a été considéré dans les dernières années comme une solution très prometteuse pour augmenter les performances des systèmes de transmission actuels. Ainsi on trouve dans la littérature une multitude d'applications et d'études réalisés concernant plusieurs aspects de la transmission [6] [7]. Grâce à ses caractéristiques quasi-stochastiques, le chaos offre une solution possible pour transmettre des quantités importantes d'informations sécurisées.

L'intérêt d'utiliser des signaux chaotiques réside dans deux propriétés du chaos :
Un signal chaotique est un signal à large spectre et permet donc de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ.

Depuis quelques années, l'utilisation du calcul fractionnaire dans la représentation des systèmes physiques a suscité l'intérêt de la communauté scientifique [10] [35]. Ainsi, les systèmes physiques peuvent être décrits plus correctement par des modèles mathématiques d'ordre non entier. En ce qui concerne les transmissions sécurisées de donnée, les dérivées d'ordre fractionnaire jouent un rôle important dans l'augmentation de la sécurité des et de la confidentialité des données transmises et de nombreux travaux ont porté sur ce sujet [8][9].

Notre travail rentre dans ce contexte, une étude sur une transmission sécurisée de données par un système chaotique d'ordre fractionnaire sera menée. Cette transmission est basée sur la synchronisation de deux systèmes chaotiques à l'aide d'un observateur retardé étape par étape. Nous utiliserons un système chaotique particulier nommé « système de Henon Modifié » qui est un système discret et d'ordre fractionnaire.

Notre travail est structuré comme suit :

Le premier chapitre a pour objet l'étude des notions fondamentales des systèmes chaotiques, abordant des rappels sur les systèmes dynamiques non linéaires avec un accent particulier porté sur les systèmes à temps continu et discret, on retrace également un bref historique de la théorie du chaos. Nous balaierons les différents outils mathématiques qui nous servent à caractériser le comportement chaotique d'un système, tels que les attracteurs étranges, les exposants de Lyapunov et la dimension fractale.
Cette étude est consolidée par des exemples de systèmes chaotiques à temps continu et discret, qui sont simulés sous Matlab, ce afin de mieux illustrer leur fonctionnement et leurs caractéristiques.

Le second chapitre sera consacré à la synchronisation des systèmes chaotiques et aux différentes méthodes de cryptage. Nous parlerons ainsi du principe de la synchronisation de ces systèmes et les différentes méthodes utilisées. Nous citerons aussi des éléments sur la cryptographie et les différentes méthodes de cryptages/décryptage des systèmes chaotiques, ainsi que la cryptanalyse.

Le troisième chapitre sera consacré pour l'étude détaillée d'une transmission sécurisée de données basé sur un système chaotique à temps discret et d'ordre fractionnaire appelé : système de Hénon modifié. En premier lieu, des notions sur le calcul fractionnaires sont abordées et plus précisément sur la dérivation d'ordre fractionnaire. Nous calculons ainsi le modèle d'ordre fractionnaire du système Hénon modifié. Après le calcul du modèle fractionnaire, les équations de ce système seront modélisées sur Matlab afin d'étudier l'ensemble de ses caractéristiques. Ensuite, nous réalisons un programme script sous Matlab qui va nous permettre de réaliser cette transmission sécurisée ainsi que la présentation des résultats de simulations sera donnée. Enfin, des simulations pour l'envoi d'un message défini par un signal sinusoïdal seront données.

Notre travail sera clôturé par une conclusion générale, une annexe qui contient des définitions utiles, et des références bibliographiques assez diversifiées.

Chapitre I

Généralités sur les systèmes chaotiques

I.1 Introduction

La théorie du chaos, au sens large, se définit par une sensibilité extrême à des conditions initiales. Si une infime différence intervient dans ces conditions initiales, un même système peut évoluer en peu de temps d'une façon radicalement différente [11][34].

❖ Découverte du chaos

La découverte de la dynamique chaotique des systèmes non-linéaires remonte aux travaux d'Henri Poincaré sur la mécanique céleste et la mécanique statistique [12], vers 1900. Ces derniers ont suscité peu d'intérêt et sont tombé dans l'oubli. Il fallut attendre 1963 qu'un météorologue du nom d'Edward Lorenz du Massachusetts Institut of Technology, mette en évidence l'aspect chaotique de certains phénomènes météorologiques tels que les mouvements turbulents de l'atmosphère [13]. Alors qu'il cherchait à déterminer les conditions météorologiques futures à partir de données initiales prises sur son ordinateur, il constata qu'une modification minime de ces données entrainait des résultats radicalement différents.

Après avoir modélisé le mouvement des masses d'air par des relations (très simplifiées) de thermodynamique et de mécanique des fluides, il a programmé le modèle sur un ordinateur afin d'obtenir une simulation numérique. A l'époque, cela prenait beaucoup de temps, pour ne pas recommencer les calculs depuis le début, il décida de reprendre son listing et de rentrer en tant que conditions initiales des valeurs prises au cours de la simulation de la veille. La précision donnée par l'ordinateur était de cinq chiffres, alors qu'E. Lorenz a pris en considération trois chiffres. Il tronqua donc ces nombres et repris le calcul. Les résultats de la simulation furent le déclic, d'abord les valeurs semblaient être les mêmes, mais au bout d'un certain temps rien ne concordait. Lorenz venait de mettre en évidence la sensibilité aux conditions initiales [13][14], cette notion joliment illustrée par l'image suivante : **« *le battement d'ailes de quelques papillons peut provoquer des tempêtes aux antipodes* »**. C'est ainsi que les travaux de Poincaré sortirent de l'ombre en fournissant l'ossature mathématique qui allait permettre l'étude des phénomènes non-linéaires. Tous ces travaux lancèrent sur de nouvelles bases les réflexions concernant le déterminisme et la prévisibilité.

❖ Historique du chaos

1890	Henri Poincaré gagne le premier prix du roi Oscar II, étant le plus proche à résoudre le problème de n-corps des orbites des corps célestes. Il a découvert que l'orbite de trois corps célestes agissantes l'une sur l'autres peut engendrer un comportement instable et imprévisible. C'est ici que le CHAOS est né.
1963	Edward Lorenz découvre qu'un simple ensemble de trois équations (non linéaires couplées de premier ordre) peut donner lieu a des trajectoires complètement chaotiques. Ainsi il a mis en évidence un des premiers exemples du chaos déterministe.

1975	Le terme « chaos » a été introduit pour la première fois par Tien-Yien Li et James A. Yorke.
1978	Mitchell Feigenbaum introduit un nombre universel associé au chaos
1990	-Edward Ott, James A. Yorke et Celso Grebogi, introduisent la notion du contrôle du chaos. -Pecora et Carroll : synchronisation des systèmes chaotiques

Tableau (I.1) : Historique du chaos

I.2 Les systèmes dynamiques non-linéaires

Un système dynamique peut être représenté par un ensemble de variables, qui évoluent au cours du temps. Ces variables peuvent être destinées pour l'étude des fluctuations d'état d'un phénomène ou d'un objet quelconque. **La non-linéarité** renvoie d'une manière générale à une rupture de la proportionnalité des causes et des conséquences. Un système physique est dit non linéaire, si la relation entre les grandeurs d'entrées et les grandeurs de sorties ne vérifie pas le principe de superposition.
Un système dynamique en temps continu peut être modélisé mathématiquement par un système d'équations différentielles, alors qu'en temps discret on parle d'un système d'équations aux différences finies.

I.2.1 Modèle mathématique en temps continu

Soit le système défini par les relations suivantes :

$$\begin{cases} \dot{x} = f(x,t,u) \\ y = h(x,t,u) \end{cases} \quad \textbf{(I.1)}$$

Où : $x \in U \subseteq \mathbb{R}^n$ est un vecteur d'état de dimension n , $f: \mathbb{R}^n \to \mathbb{R}^n$ est une fonction non linéaire désignant le champ de vecteurs, $h: \mathbb{R}^n \to \mathbb{R}$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq \mathbb{R}^p$ représente l'entrée du système [15].

I.2.2 Modèle mathématique en temps discret

Comme il a été déjà précisé le système dynamique est dans ce cas représenté par des équations aux différences finies [15], avec le modèle général suivant :

$$\begin{cases} x(k+1) = G(k, x(k), u(k)) \\ y(k) = h\big(k, x(k), u(k)\big) \end{cases} \quad \textbf{(I.2)}$$

Où $G: \mathbb{R}^n \to \mathbb{R}^n \times \mathbb{Z}^+ \to \mathbb{R}^n$ désigne la dynamique du système en temps discret.
En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k :

$$\begin{cases} x(k+1) = G(x(k), u(k)) \\ y(k) = h\big(x(k), u(k)\big) \end{cases} \quad \textbf{(I.3)}$$

I.3 Systèmes non-linéaires chaotiques

L'étude de dynamiques non-linéaires a montré que le chaos apparaissait naturellement dans des systèmes naturels, ou en ingénierie. Il a d'abord été considéré comme irrégulier et souvent attribué à des influences externes aléatoires. En fait, des études approfondies ont révélé que les phénomènes chaotiques étaient caractéristiques des systèmes non-linéaires. Ce qui est apparu comme une surprise pour la plupart des scientifiques est que même des systèmes décrits par des équations simples peuvent avoir des solutions chaotiques. Cependant, tout n'est pas chaotique. Un autre fait curieux est que le même système peut se comporter de façon prévisible ou chaotique, en fonction de petits changements de l'un des paramètres des équations qui le décrivent [16].

I.3.1 Définition du chaos

Bien qu'il n'existe pas une définition du chaos adopté de façon universelle dans la littérature, mais on pourrait dire que c'est un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Caractérisé par une évolution qui semble aléatoire et un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme.

I.3.2 Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires, la figure suivante illustre l'aspect aléatoire du système de Lorenz, dont les équations sont définies en section **(I.3.3)** :

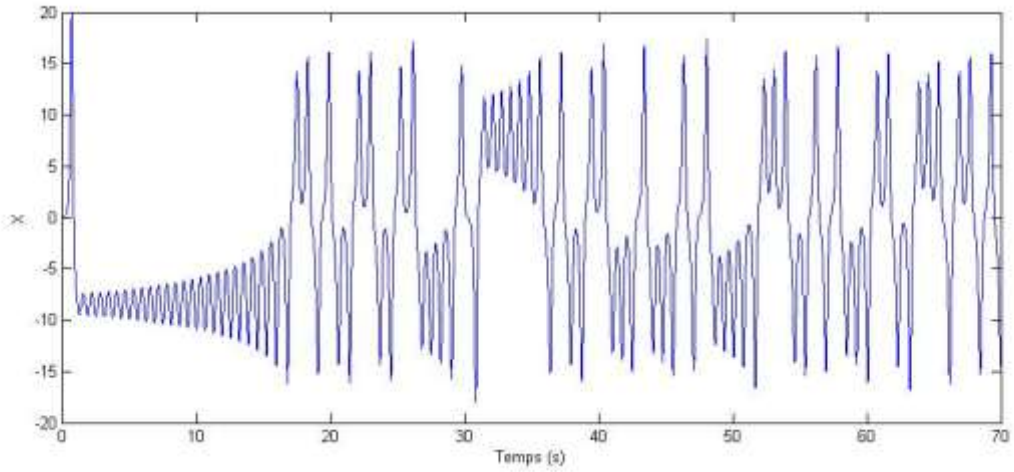


Figure (I.1) : Etat chaotique x du système de Lorenz.

I.3.3 Systèmes chaotiques à temps continu

Pour un système autonome en temps continu, au moins trois variables d'état sont nécessaires pour générer le chaos, c'est à dire que $n \geq 3$. Dans le cas d'un système non-autonome, il faut au moins deux variables d'état et une entrée indépendante [17][16].

Le système de Lorenz est un exemple célèbre de système différentiel au comportement chaotique pour certaines valeurs de ses paramètres. Il s'agit d'un système dynamique non linéaire en temps continu de dimension 3, obtenu des équations de transfert de la chaleur dans un liquide. Le système de Lorenz est défini par :

$$\begin{cases} \dot{x} = a\,(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = x\,y\, -\, c\,z \end{cases} \qquad \textbf{(I.4)}$$

Le système de Lorenz montre un comportement chaotique pour $a = 10, b = 28, c = 8/3$.

On effectue une simulation du système sous le logiciel Matlab, les conditions initiales sont choisies comme suit : x(0) = 0.01, y(0) = 0.01, z(0) = 0.01 et x′(0) = 0.012, y′(0) = 0.01 et z′(0) = 0.01.

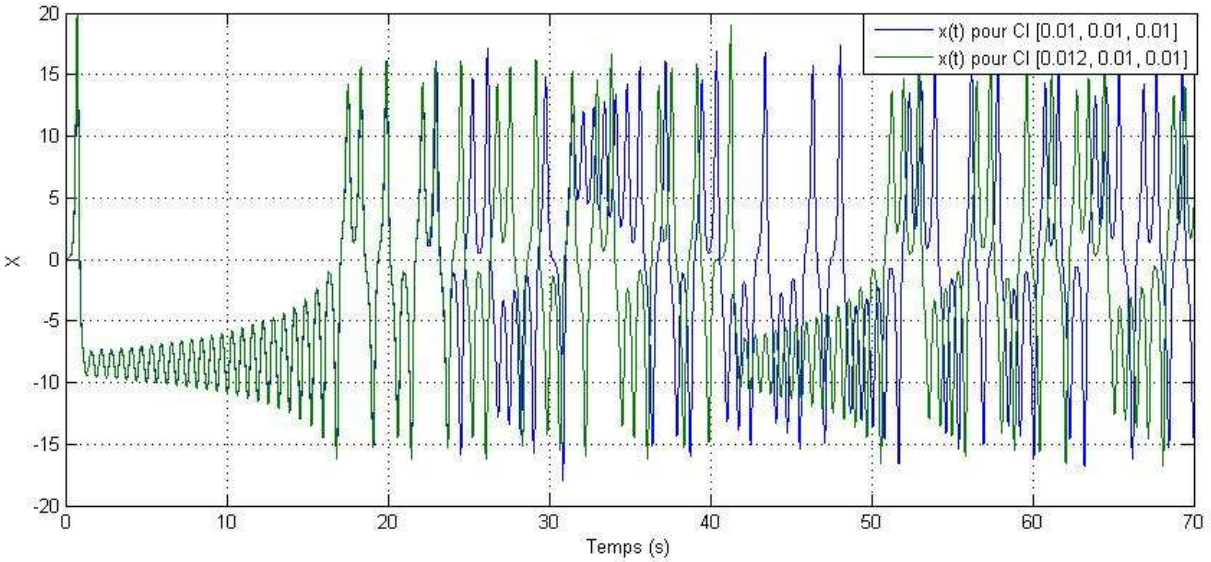


Figure (I.2) : Illustration de la sensibilité aux conditions initiales pour l'état x du système de Lorenz

I.3.4 Systèmes chaotiques à temps discret

Le système de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. Il s'agit d'un système à temps discret qui introduit des itérations dans le plan [17]. Ces itérations sont définies par les relations suivantes.

$$\begin{cases} x_{k+1} = a - x_k^2 + by_k \\ y_{k+1} = x_k \end{cases} \qquad (\mathbf{1.5})$$

Les valeurs des paramètres proposées par Michel Hénon pour observer le phénomène chaotique sont : $a = 1.4 \ et \ b = 0.3$.

Pour simuler le modèle de Hénon on a pris pour conditions initiales $x_0 = 0 \, et \, y_0 = 0$. Ainsi la **Figure (I.3)** montre l'évolution qui semble aléatoire des états $x_k \, et \, y_k$

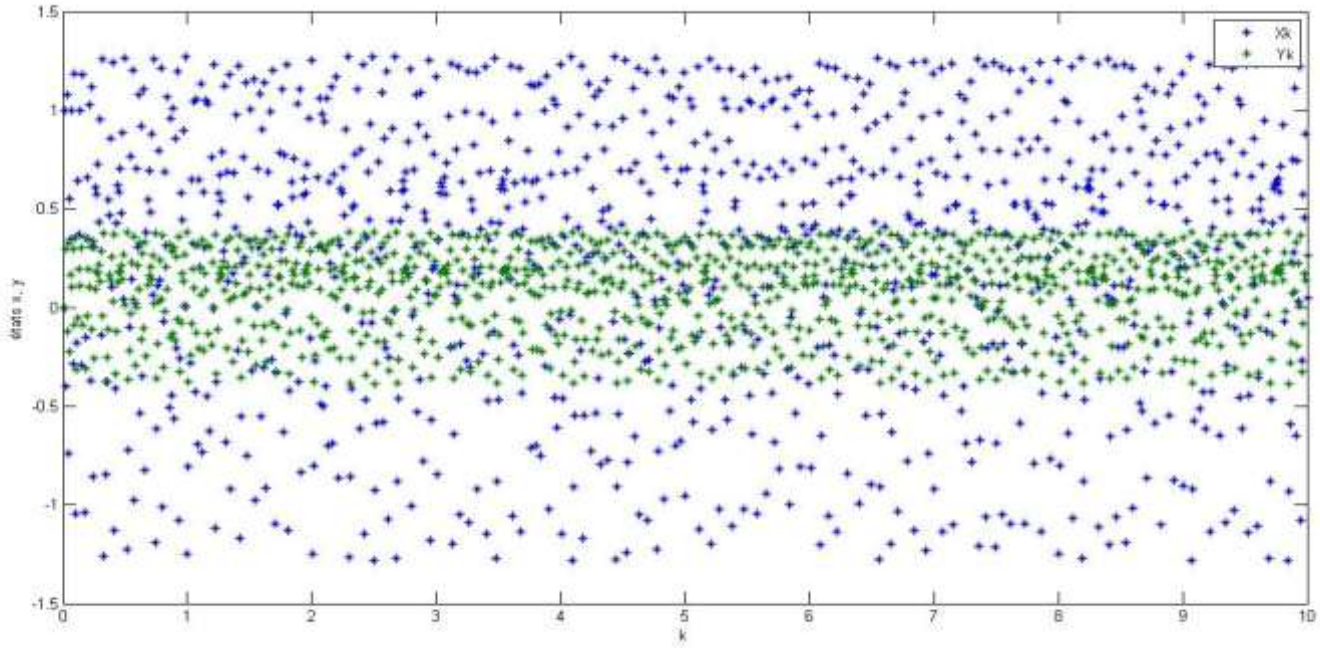


Figure (I.3) : Etats chaotiques x et y du système de Hénon

I.4 Propriétés des systèmes chaotiques

Pour caractériser une dynamique chaotique plusieurs approches sont définies, et permettent l'identification des comportements chaotiques de certains systèmes. L'étude de **l'aspect temporel** de ces systèmes permet de distinguer les propriétés du chaos tels que la sensibilité aux conditions initiales, les attracteurs étranges, les exposants de Lyapunov, etc. **L'aspect fréquentiel** quant à lui, est lié à l'étude du spectre de puissance ou encore la fonction d'auto corrélation des signaux composants le système en question.

I.4.1Sensibilité aux conditions initiales

La sensibilité aux conditions initiales constitue sans aucun doute la caractéristique essentielle du comportement chaotique d'un système : l'évolution est par conséquent imprévisible à long terme. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système.
Edward Lorenz fut l'un des premiers chercheurs à s'en être aperçu pendant qu'il menait des travaux en météorologie portants sur les mouvements turbulents de l'atmosphère [13]. Il démontra ainsi que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes ce qui rend les résultats imprévisibles à long termes.

Soit le système **(I.6)**, qui 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.

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + a\,y \\ \dot{z} = b + z(x-c) \end{cases} \qquad \textbf{(I.6)}$$

Afin d'illustrer la propriété de sensibilité aux conditions initiales, on propose une simulation du système sur Matlab, nous prenons $a = 0.398,\ b = 2\ et\ c = 4$.

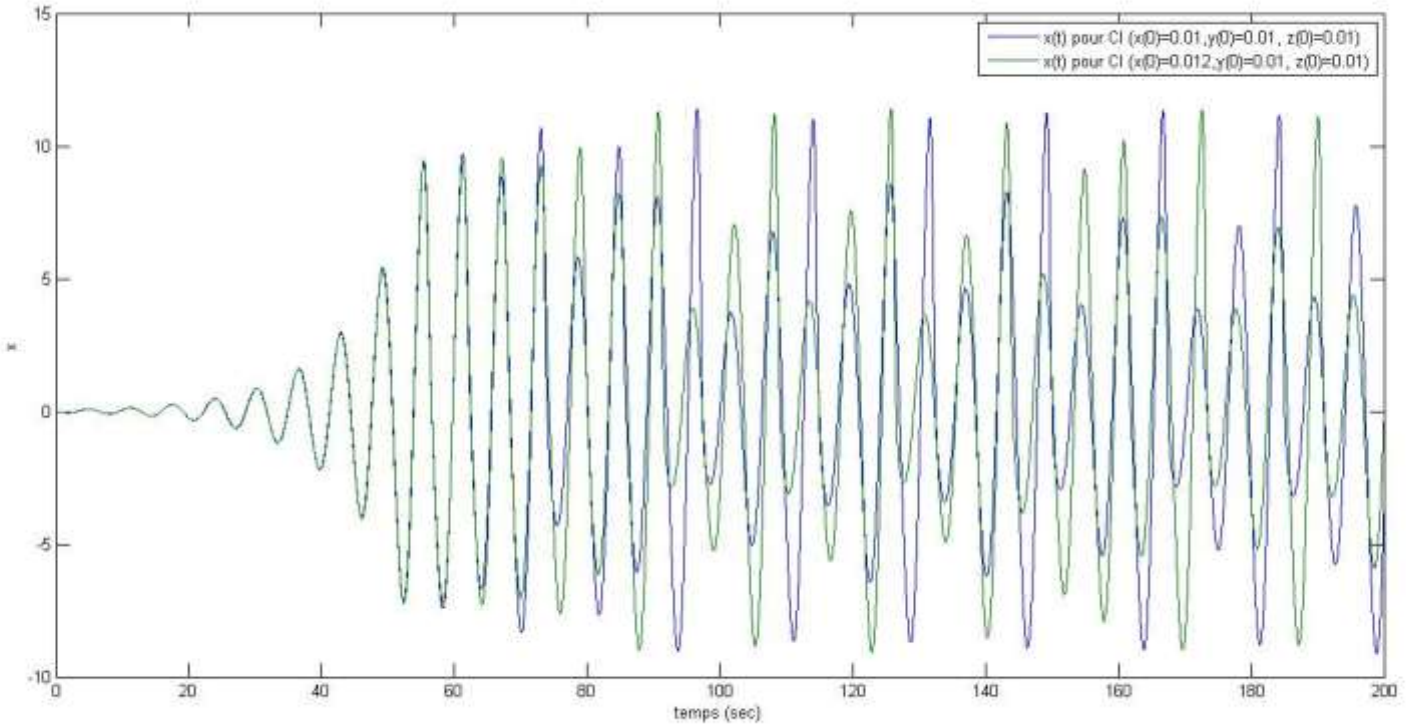


Figure (I.4) : Illustration de la sensibilité aux conditions initiales pour l'état x du système de Hénon

I.4.2 Attracteurs

La région de l'espace de phases vers laquelle convergent les trajectoires d'un système dynamique dissipatif s'appelle "attracteur". Les attracteurs sont des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques. Il en existe quatre types distincts : un point, un cycle limite, un tore ou avoir une structure encore plus complexe de type fractale [19].

- L'attracteur ***"point fixe"*** est un point de l'espace de phase vers lequel tendent les trajectoires, c'est donc une solution stationnaire constante.

- L'attracteur ***"cycle limite"*** est une trajectoire fermée dans l'espace des phases vers laquelle tendent les trajectoires. C'est donc une solution périodique du système.

- L'attracteur ***"tore"*** représente les mouvements résultant de deux ou plusieurs oscillations indépendantes que l'on appelle parfois "mouvements quasi périodiques".

- ***Les attracteurs étranges*** sont bien plus complexes que les autres, on parle d'attracteur étrange lorsque la dimension fractale n'est pas entière. la trajectoire dans l'espace des phases reste confinée dans une région bien définie, après une période transitoire de durée variable.

  L'attracteur de Lorenz et celui de Rössler sont présentés dans les **Figures (I.5) et (I.6).**

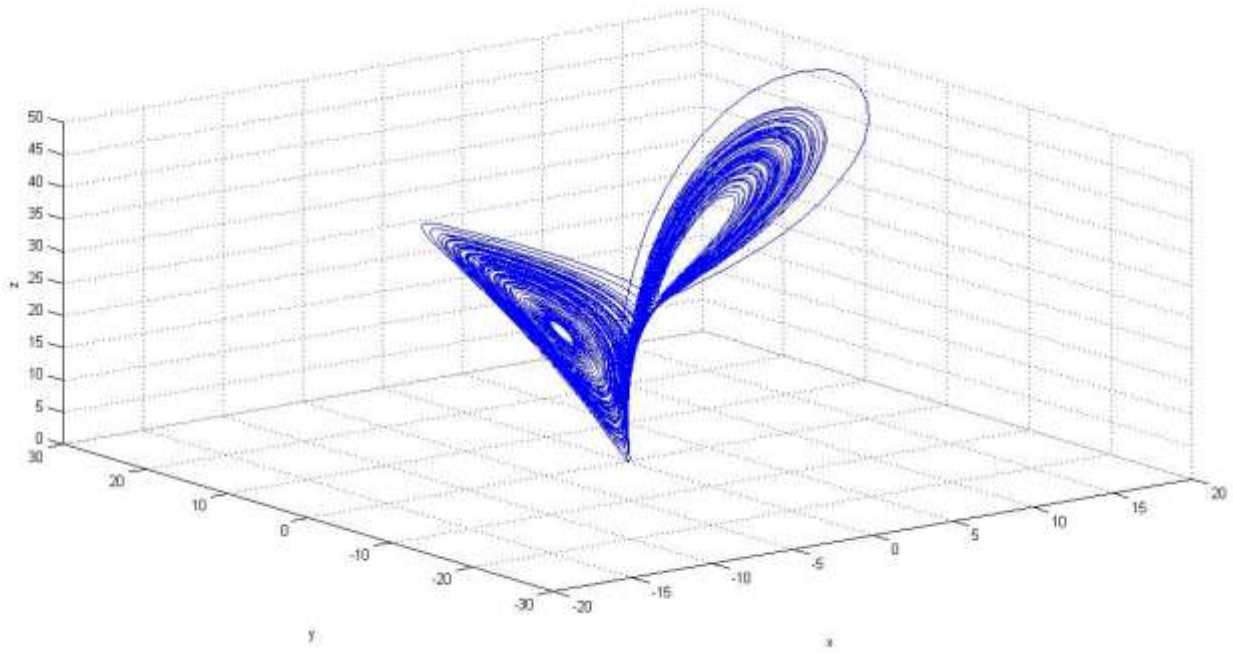


Figure (I.5) : Attracteur étrange de Lorenz

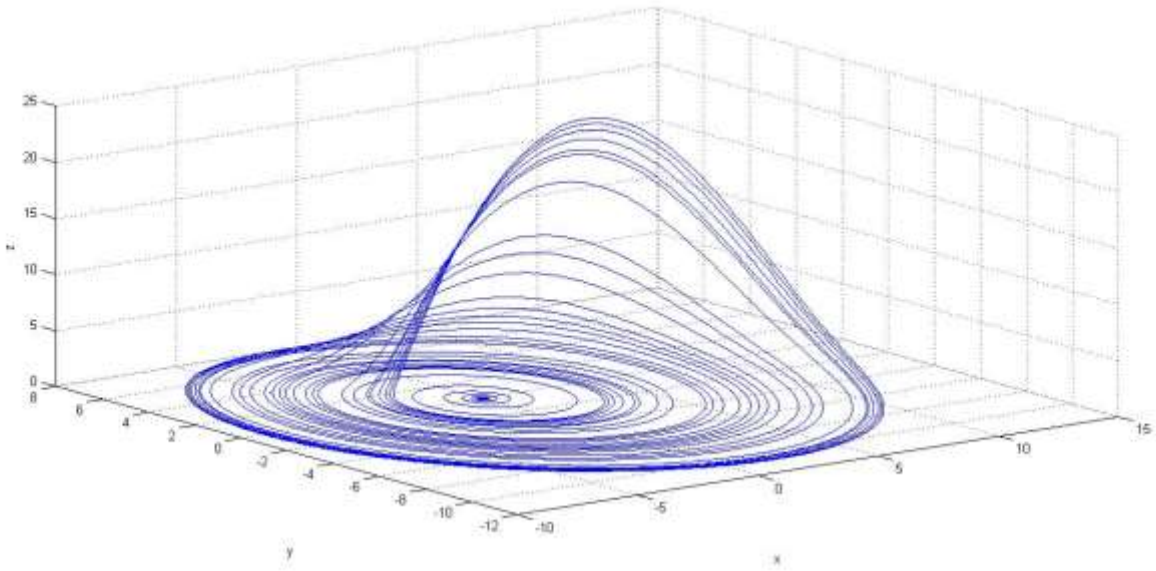


Figure (I.6) : Attracteur de Rössler

I.4.3 Section de Poincaré

Elle permet de caractériser des types de trajectoire dans l'espace des phases de dimension n. Le principe consiste à se ramener à une étude dans $\mathbb{R}^2$ par intersection de la trajectoire dans $\mathbb{R}^n$. On remplace l'étude du système continu $\dot{x} = f(x)$ dans $\mathbb{R}^n$ par celle :

- De l'application ponctuelle T dans $\mathbb{R}^2$ définie ainsi :

$$M_{k+1} = T(M_k)$$

  Où M_k est le k-ième point d'intersection de la trajectoire avec le plan de coupe.
- Ou de l'application G dite de premier retour définie ainsi :

$$x_{k+1} = G(x_k)$$

  Où x_k est l'abscisse du k-ième point d'intersection de la trajectoire avec le plan de coupe.

Les cas typiques observés :

- La solution est périodique dans $\mathbb{R}^n$ (c'est un cycle limite) : La section de Poincaré est un point.
- La solution est quasi-périodique à deux fréquences f_1 et f_2. On distingue deux cas selon que le rapport $\boldsymbol{r = \frac{f_1}{f_2}}$ est rationnel ou pas :
  - **Si r n'est pas rationnel :** la section de Poincaré est une courbe fermée.
  - **Si r est rationnel :** la section de Poincaré se compose de quelques points.
- La solution est apériodique : la section de Poincaré est un nuage de points.

I.4.4 Exposants de Lyapunov

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant les taux de divergence des trajectoires. Dans l'étude des systèmes non linéaires ainsi que les systèmes chaotiques, les exposants de Lyapunov jouent un rôle important, Ils qualifient le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes [20].

I.4.4.1 Exposants de Lyapunov pour un système unidimensionnel

Soit f de $\mathbb{R} \rightarrow \mathbb{R}$ une fonction discrète d'un système dynamique qui applique :

$$x_k = f(x_{k-1}) \qquad \textbf{(I.7)}$$

x_0 et $x_0 + \delta x_0$ deux conditions initiales très proches.

On suppose que l'écart entre les trajectoires de ce système après k itérations et avec l'existence d'un réel λ peut être quantifié par :

$$|f^k(x_0 + \delta x_0) - f^k(x_0)| \approx \delta x_0 e^{k\lambda} \qquad \textbf{(I.8)}$$

D'où

$$\lambda \approx \frac{1}{k} ln \frac{|f^k(x_0+\delta x_0)-f^k(x_0)|}{\delta x_0} \qquad (\textbf{I. 9})$$

Pour $\delta x_0 \rightarrow 0$ on aura :

$$\lambda = \frac{1}{k}\sum_{i=0}^{k-1} ln \left|\frac{df(x_i)}{dx_i}\right| \qquad (\textbf{I. 10})$$

Ainsi :

$$\lambda = \lim_{k\to\infty} \frac{1}{k}\sum_{i=0}^{k-1} ln\,|f'(x_i)| \qquad (\textbf{I. 11})$$

Si $\lambda \leq 0$, la trajectoire de l'évolution du système peut tendre vers un point fixe, avoir un comportement périodique ou quasi-périodique.

Si $\lambda > 0$, le système est chaotique.

I.4.4.2 Exposants de Lyapunov pour un système multidimensionnel

Pour un système de dimension n on parle de spectre d'exposants de Lyapunov dont le nombre est égal à cette dimension.

$\{\lambda_1, \lambda_2, \ldots . \lambda_n\}$

La classification des comportements des systèmes dynamiques selon les exposants de Lyapunov est représentée sur le tableau suivant:

Régime permanent	**Attracteur**	**Exposants de Lyapunov**
Point d'équilibre	Point	$\lambda_n \leq \lambda_{n-1} \leq \cdots\cdots \leq \lambda_1 < 0$
Périodique	Courbe fermée (Cycle limite)	$\lambda_n \leq \lambda_{n-1} \leq \cdots\cdots \leq \lambda_2 < \lambda_1 = 0$
Quasi-périodique	Tore	$\lambda_1 = \cdots\cdots = \lambda_i = 0$ $\lambda_n \leq \lambda_{n-1} \leq \cdots\cdots \leq \lambda_{i+1} < 0$
Chaotique	Attracteur chaotique	$\lambda_1 > 0$ $\lambda_n \leq \lambda_{n-1} \leq \cdots\cdots \leq \lambda_2 \leq 0$
Hyper chaotique	Attracteur chaotique	$\lambda_1 > 0 \; et \; \lambda_2 > 0$ $\lambda_n \leq \lambda_{n-1} \leq \cdots\cdots \leq \lambda_3 \leq 0$

Tableau (I.2): Comportement des systèmes dynamiques en fonction des Exposants de Lyapunov

Remarque I.1

Un attracteur représente par définition la limite asymptotique des solutions partant de toute condition initiale située dans un bassin d'attraction qui est un domaine de volume non nul. Ainsi pour un système chaotique l'existence d'un attracteur nécessite que la dynamique de ce système soit globalement dissipative. Cela signifie que le système doit être caractérisé par une stabilité globale qui correspond à la condition suivante sur le spectre de Lyapunov :

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

Exemple (I.1): Calcul des Exposants de Lyapunov pour le système de Lorenz

Pour calculer les exposants du système de Lorenz on effectue une simulation sur Matlab en utilisant le programme « Lyapunov Exponents Toolbox » [44].

Le système est d'ordre 3 et a pour paramètres : $a = 16,\ b = 45.92,\ c = 4.$
Les conditions initiales sont fixées à : $x(0) = 1,\ y(0) = 1,\ z(0) = 1$

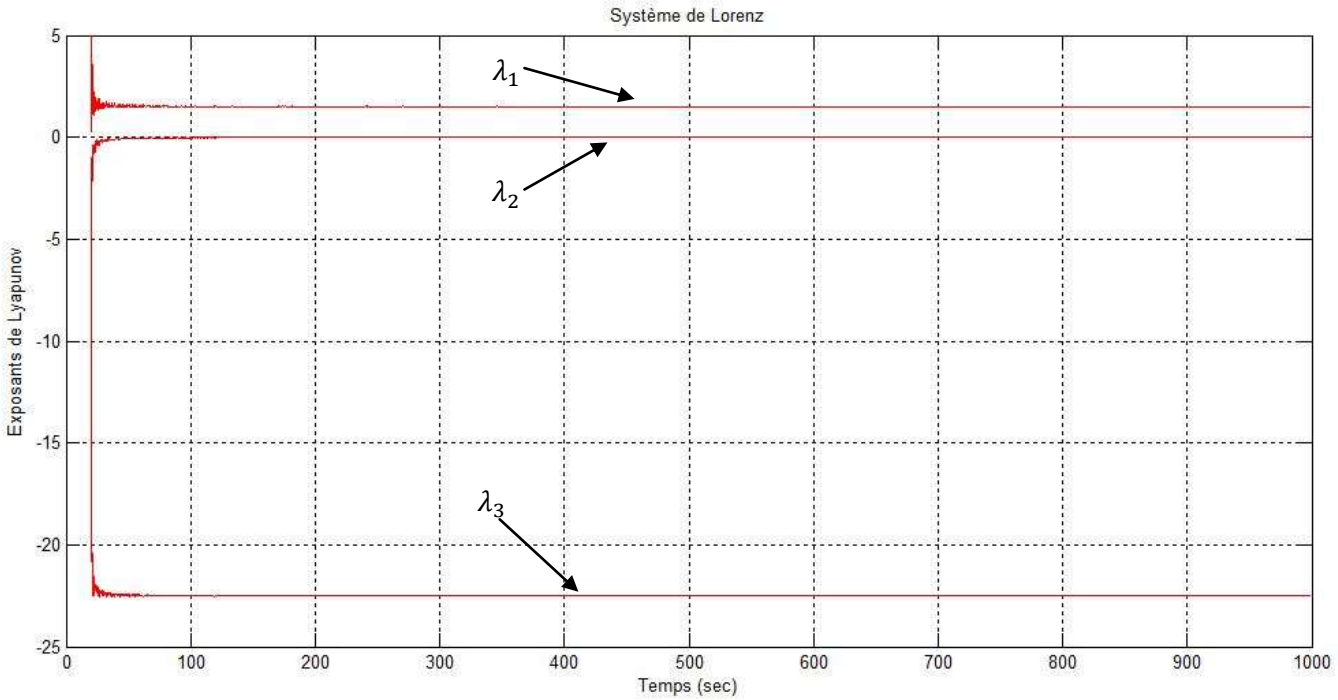


Figure (I.7) : Exposants de Lyapunov pour le système de Lorenz

La **Figure (I.7)** montre l'évolution des exposants de Lyapunov en fonction du temps qui sont :

$$\begin{cases} \lambda_1 = 1.50571 \\ \lambda_2 = -0.0008 \\ \lambda_3 = -22.5049 \end{cases}$$

I.4.5 Bifurcation et route vers le chaos

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique [21].
Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système tel que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées ***valeurs de bifurcation.***

L'exemple le plus connu d'un système non linéaire pour lequel il est possible de tracer un diagramme de bifurcation est l'équation logistique, sa fonction est donnée comme suit :

$$f: [0\ ,1] \rightarrow [0\ ,1] \quad x_{k+1} = f(x_k) = r\ x_k\ (1 - x_k) \qquad (\mathbf{I.12})$$

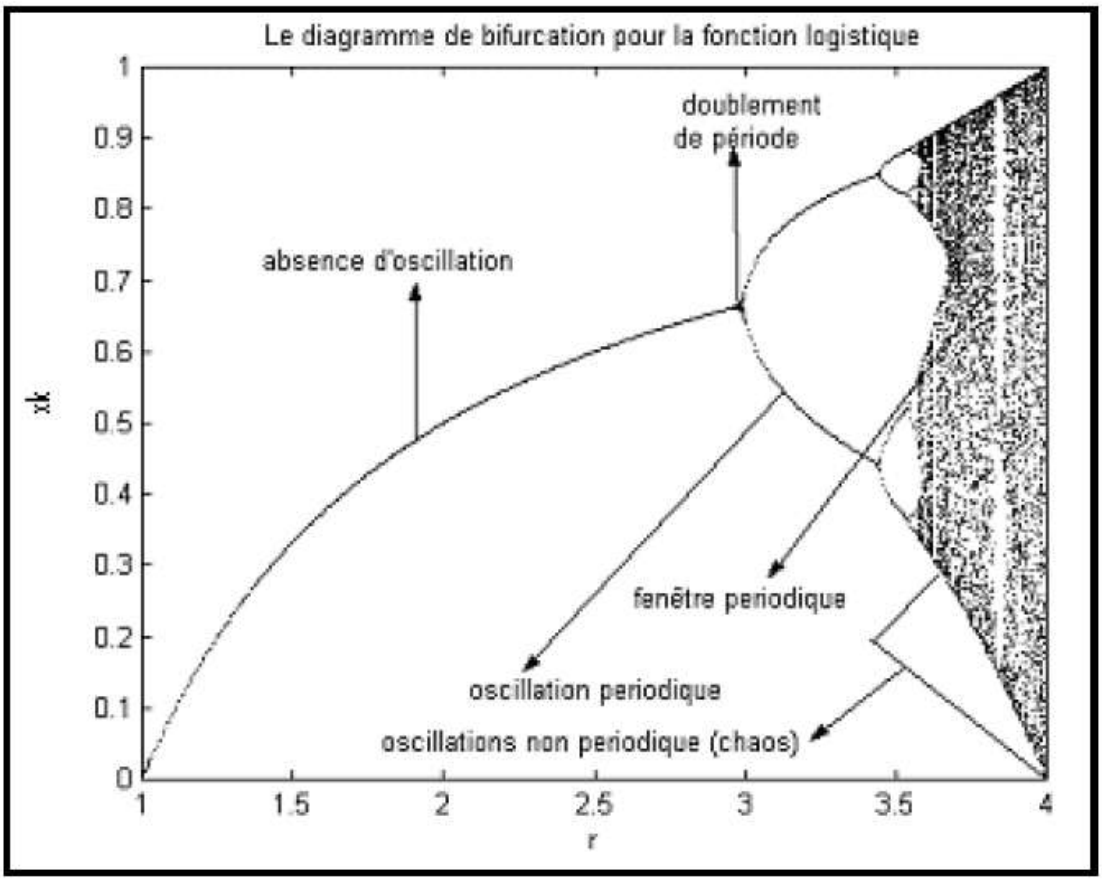


Figure (I.8) : Diagramme de bifurcation de la fonction logistique

Il peut être intéressant d'étudier l'apparition du chaos (ce qu'on appelle le scénario ou la route vers le chaos).
On distingue trois scénarios théoriques d'évolution vers le chaos. Toutes ces évolutions ont permis de classer certains phénomènes expérimentaux comme chaotique déterministe. On obtient l'apparition du chaos en modifiant la valeur d'un paramètre du système que ça soit de manière théorique ou expérimentale.

❖ Le doublement de période

L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de période, la période se multiplie ainsi en 4, 8,16 …

A partir d'une certaine valeur du paramètre les doublements étant de plus en plus rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparait.

❖ **L'intermittence**

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.
Le système conserve pendant un moment un régime pratiquement quasi-périodique (régulier), et il se déstabilise brutalement pour donner lieu à une explosion chaotique.

❖ **La quasi-périodicité**

Ce dernier scénario fait intervenir pour un système périodique l'apparition d'une autre période dont le rapport avec la première n'est pas rationnel.

I.4.6 Spectre de puissance et fonction d'auto corrélation

Le calcul du spectre de puissance de l'évolution des variables d'un système nous permet d'accéder à ses composantes fréquentielles, ainsi avoir une représentation fréquentielle du signal étudié. L'allure de son spectre nous permet donc de caractériser la nature du système ; soit : périodique, apériodique ou chaotique.

Le spectre de puissance (appelé aussi densité spectrale de puissance) d'un signal $x(t)$ correspond au carré du module de la Transformée de Fourier dont le principe général est de décomposer un signal quelconque en une somme de sinusoïdes de fréquences, amplitudes et phases différentes.

Soit $\tilde{X}(f)$ le spectre complexe du signal $x(t)$:

$$\tilde{X}(f) = \int_{-\infty}^{+\infty} x(t) e^{j2\pi f} dt \qquad (\mathbf{I.12})$$

Le spectre de puissance correspond donc à : $\left|\tilde{X}(f)\right|^2$

Dans une dynamique chaotique, le spectre de puissance de l'une des variables du système comporte une partie continue qui correspond à une évolution désordonnée. Ce type de spectre est difficile à différencier de celui d'un bruit blanc.
Afin de mesurer le taux de désordre de ce signal il est nécessaire d'utiliser la fonction d'auto corrélation qui est notée comme suit :

$$C(\tau) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} x(t)\, x(t-\tau) dt \qquad (\mathbf{I.13})$$

Cette fonction permet de mesurer la ressemblance de la variable x à un instant t avec sa valeur à l'instant$(t+\tau)$. La fonction $C(\tau)$ est ainsi obtenue en faisant varier l'intervalle τ dans le but de traduire le taux de similitude du signal avec lui-même quand le temps s'écoule.
Si $x(t)$ est périodique, quasi-périodique ou constante, $C(\tau)$ ne tend pas vers zéro quand τ augmente, car les signaux périodiques (ou quasi-périodiques) gardent leur similitudes internes quand le temps s'écoule, donc le comportement du système reste prédictible.
Si le régime est chaotique, $C(\tau)$ tend vers zéro quand τ augmente.

I.5 Systèmes hyperchaotiques

Un attracteur hyperchaotique est généralement défini, comme étant un comportement chaotique avec au moins deux exposants de Lyapunov positifs, combiné avec un exposant nul le long de l'écoulement et un exposant négatif pour garantir la reliée de la solution. La dimension minimale d'un système hyperchaotique continu est $n = 4$, ce qui rend le l'étude du comportement dynamique des systèmes hyperchaotiques très compliqué [43].

On peut également générer un comportement hyperchaotique à partir d'un système chaotique, pour ce il faut satisfaire les deux conditions suivantes :

- La dimension du système doit être supérieure ou égale à 4 et l'ordre de chaque équation doit être supérieur ou égale à 2 pour le cas d'un système à temps continu, et supérieure ou égale à 3 pour le cas d'un système à temps discret.
- Le système doit avoir au moins deux exposants positifs et la somme de tous les exposants doit être négative.

Exemple (I.2):

L'hyperchaotification du système de Lorenz **(I.4)**, consiste donc à augmenter la dimension du système de 3 à 4. Pour cela, un feedback contrôleur est introduit de la manière suivante :

$$\begin{cases} \dot{x} = \boldsymbol{a}\,(y - x) + u \\ \dot{y} = x(\boldsymbol{b} - z) - y \\ \dot{z} = x\,y - \boldsymbol{c}\,z \\ \dot{u} = -xz + \boldsymbol{d}u \end{cases} \qquad \textbf{(I.14)}$$

d : paramètre du contrôle.

I.5.1 Etude du modèle Hénon modifié

❖ **Le système de Hénon**

Le système de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. Il s'agit d'un système à temps discret qui introduit des itérations dans le plan [22]. Ces itérations sont définies par les relations suivantes.

$$\begin{cases} x_{k+1} = a - x_k^2 + by_k \\ y_{k+1} = x_k \end{cases} \quad (\mathbf{I.15})$$

Les valeurs des paramètres proposées par Michel Hénon pour observer le phénomène chaotique sont : a=1.4 et b=0.3.

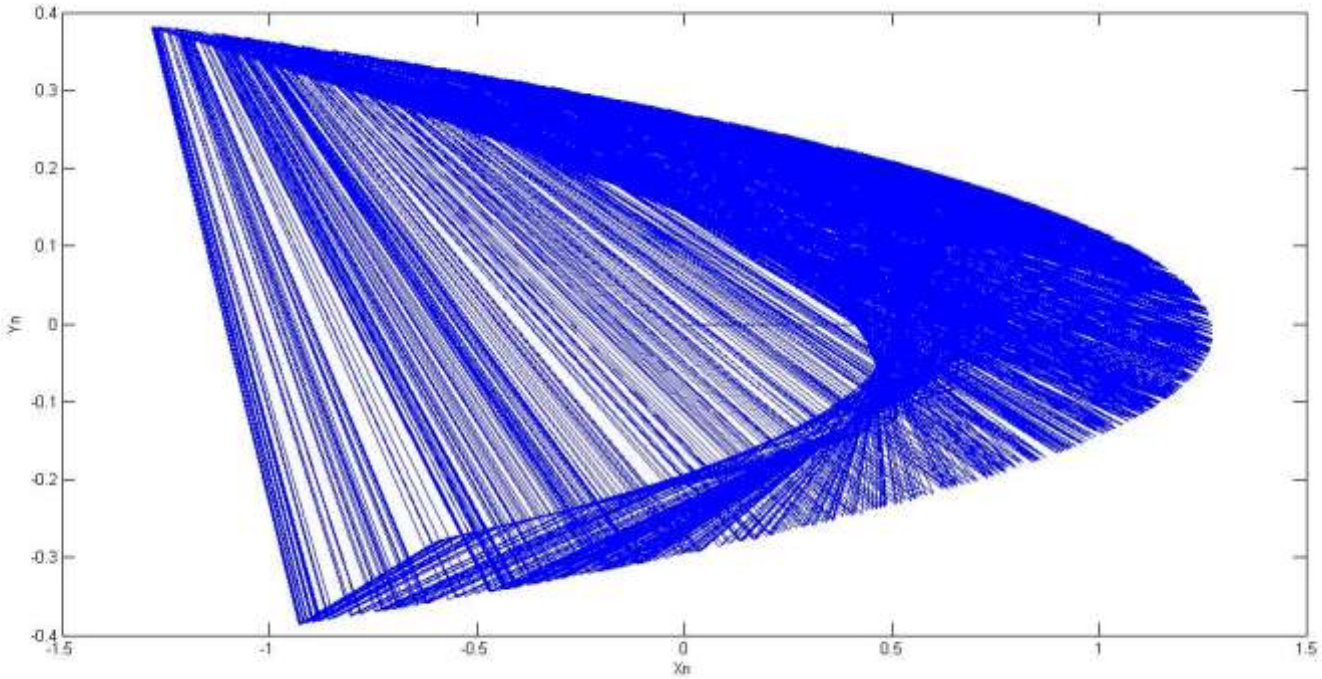


Figure (I.9) : Attracteur chaotique de Hénon.

❖ **Le système Hénon modifié**

Les équations de ce système sont issues du modèle de Hénon, ce système nous intéresse particulièrement dans ce travail puisque il présente un comportement hyperchaotique, ainsi l'étude de ses propriétés et caractéristiques s'impose. Le modèle obtenu est un modèle discret qui contient trois variables.

Le modèle est défini par les relations suivantes :

$$\begin{cases} x_{n+1} = -y_n^2 + az_n + 1.7 \\ y_{n+1} = x_n \\ z_{n+1} = y_n \end{cases} \quad \mathbf{(I.16)}$$

- **Propriétés du système**

Les **Figures (I.10), (I.11) et (I.12)** illustrent les états chaotiques du système :

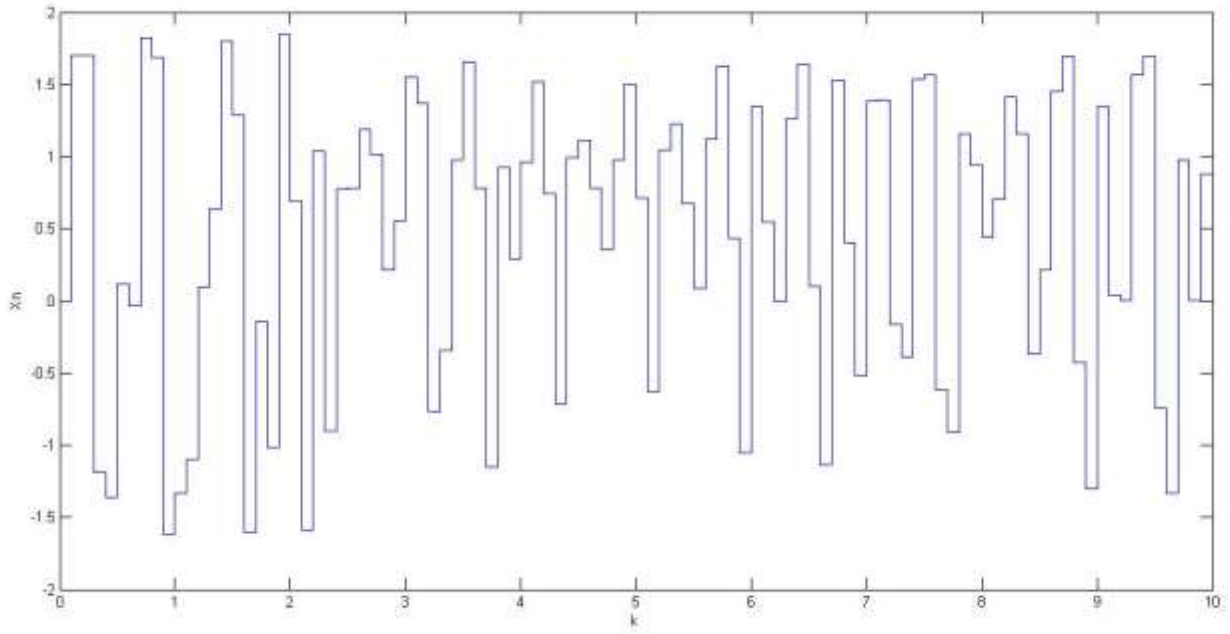


Figure (I.10) : Etat x_n du système.

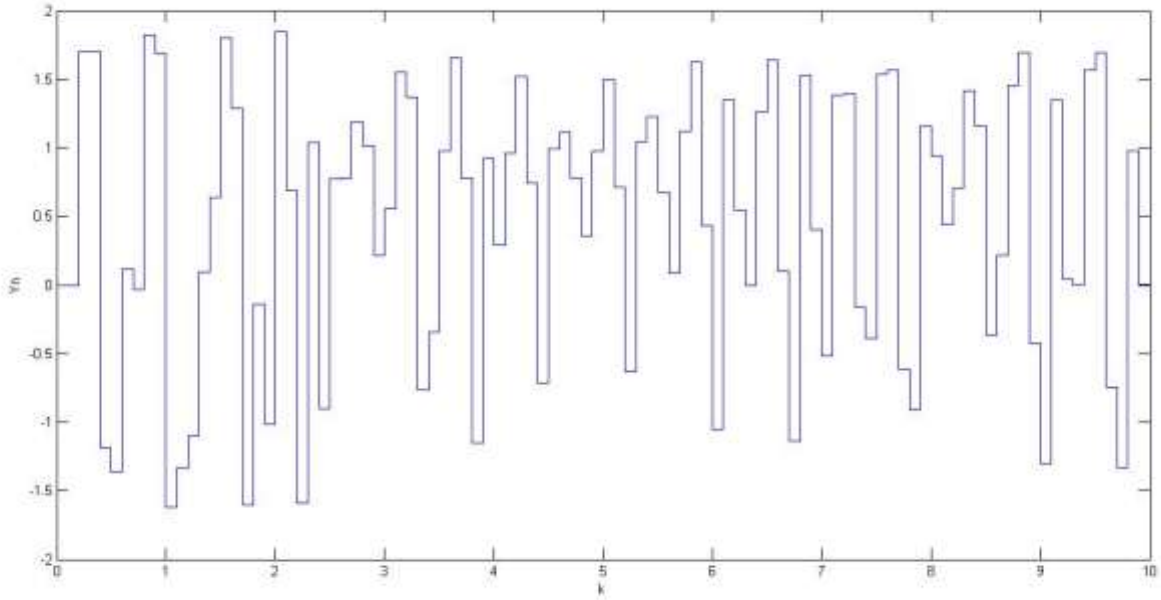


Figure (I.11) : Etat y_n du système.

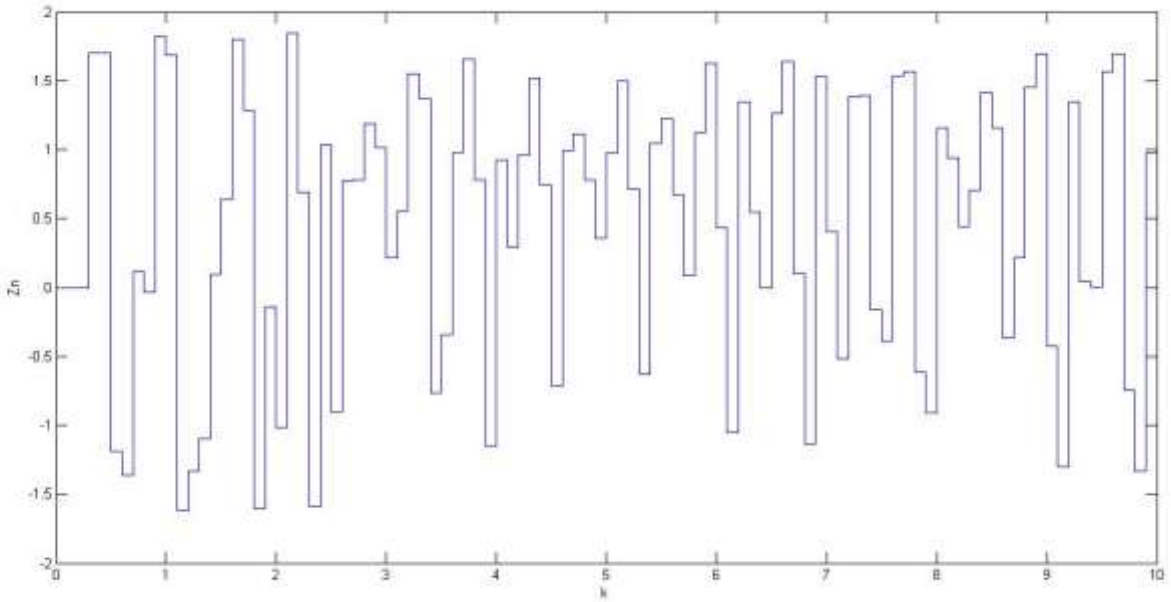


Figure (I.12) : Etat z_n du système.

Sensibilité aux conditions initiales : le Hénon modifié possède une extrême sensibilité aux conditions initiales comme montré dans la Figure suivante :

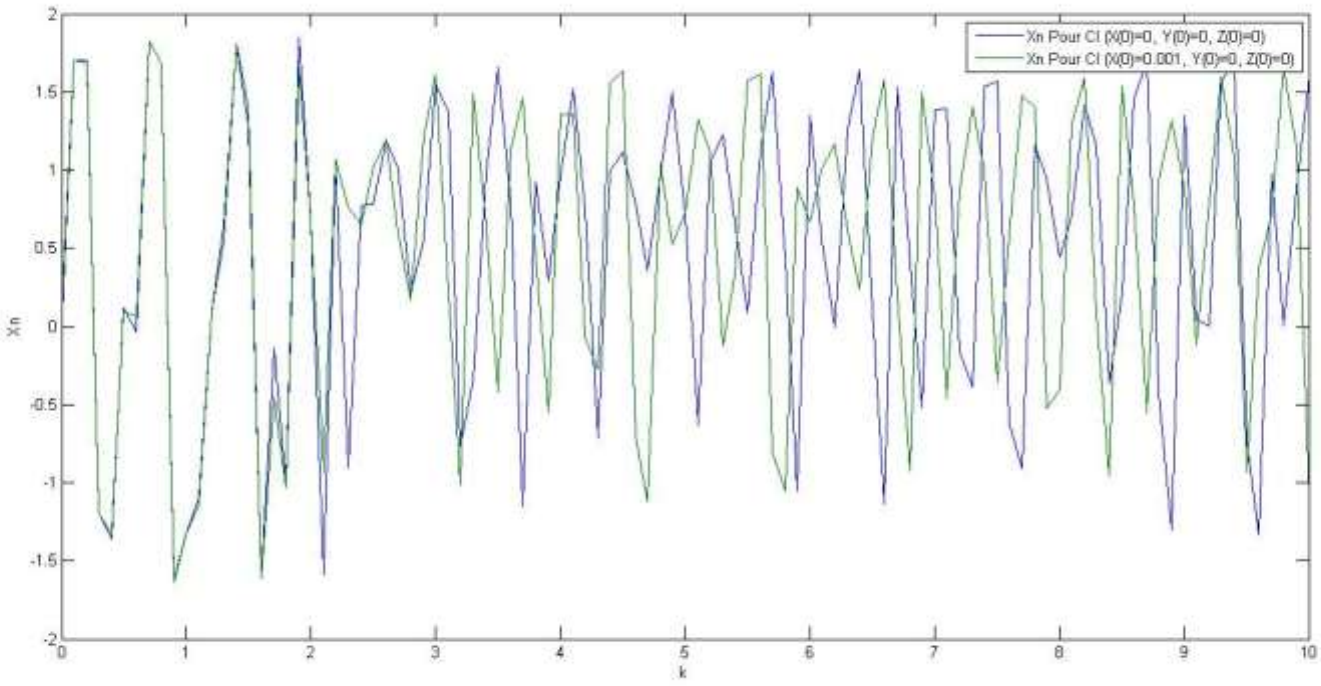
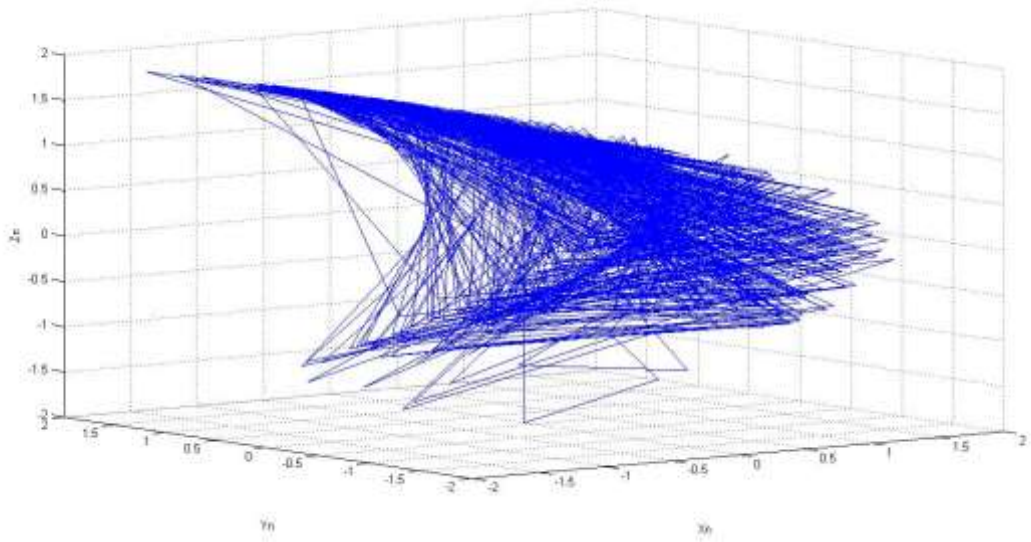
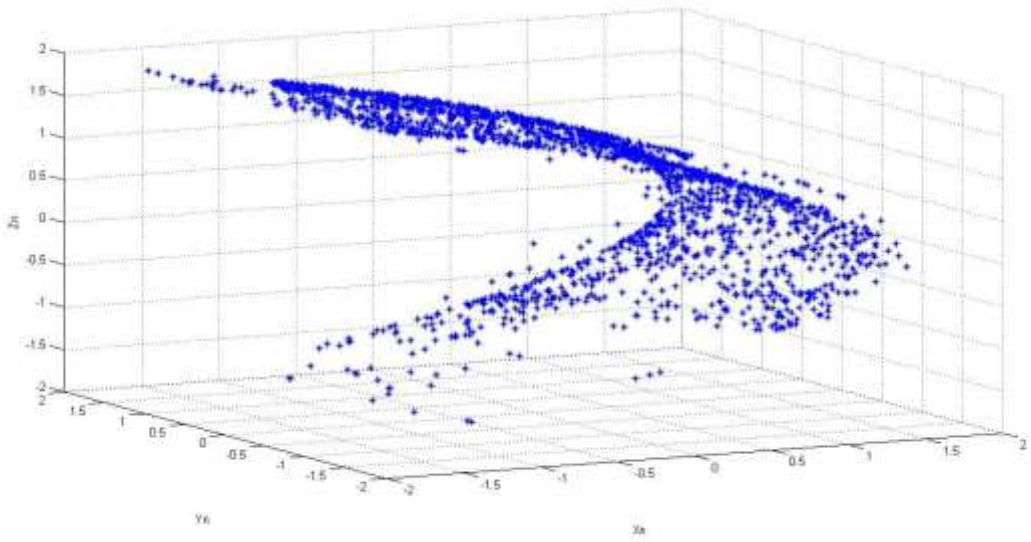


Figure (I.13) : Illustration de la sensibilité aux conditions initiales.

L'attracteur : sur l'espace des phases constitué de trois variable x, y, z on voit la forme de l'attracteur sur la **Figure (I.14),** ce dernier ressemble à celui de Hénon.



I.14 – a



I.14 – b

Figure (I.14) : Attracteur hyperchaotique du système Hénon-modifié.

Les Exposants de Lyapunov :

Pour calculer les exposants du système Hénon modifié, on effectue une simulation sur Matlab en utilisant le programme « Lyapunov Exponents Toolbox ». Le calcul des exposants de Lyapunov nous permet de démontrer le comportement hyperchaotique du système car on voit sur **Figure (I.15)** le tracé des exposants avec deux exposants positifs et un exposant négatif.

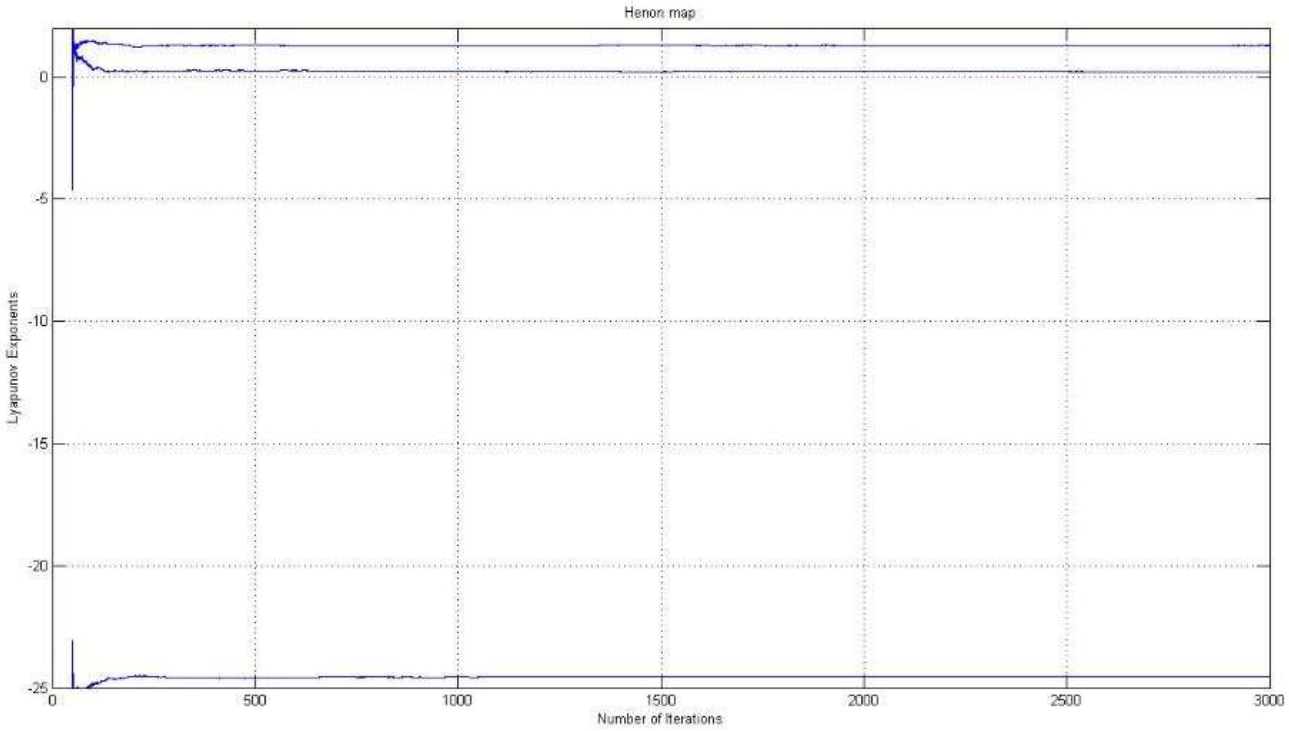


Figure (I.15) : Exposants de Lyapunov du système Hénon modifié.

I.6 Conclusion

Dans ce présent chapitre, nous avons définit le chaos en général, en suite nous avons présenté les propriétés permettant de caractériser les dynamiques chaotiques, telle que la sensibilité aux conditions initiales, le calcul des exposants de Lyapunov et le diagramme de bifurcation…etc.

Cela a été illustré par des exemples de calcul et de simulation effectués sur des systèmes chaotiques à temps continu (système de Lorenz et le système de Rössler), et à temps discret (système de Hénon). Ainsi que le comportement hyperchaotique qui a été illustré par l'étude du modèle Hénon-modifié.

Cependant l'usage du chaos pour la sécurisation de la communication pose directement le problème de synchronisation du récepteur afin de suivre le signal chaotique employé à l'émetteur. Ce qui sera l'objet du second chapitre.

Chapitre II

Transmission sécurisée à base de systèmes chaotiques

II.1 Introduction

La transmission sécurisée est une science aussi vieille que l'existence de l'humanité. Les premiers principes de base de la cryptographie moderne reviennent à Auguste Kerkhoffs, énoncés dans son article intitulé « La cryptographie militaire » publié en 1883 [24], et dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changé. En d'autres termes, aucun secret ne doit résider dans l'algorithme de cryptage mais plutôt dans la clé.

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires qui montrent souvent un comportement non divergeant, apériodique et éventuellement borné. Les signaux qui évoluent dans ces systèmes sont en général, à large bande, ce qui fait apparaître leur trajectoire comme du bruit pseudo aléatoire. En raison de ces propriétés et à cause de la fragilité des cryptosystèmes classiques, les signaux chaotiques fournissent potentiellement une classe importante des signaux qui peuvent être utilisés pour masquer les informations dans une transmission sécurisée, il suffit donc de les mélanger de manières appropriées aux messages en clair qu'on souhaite transmettre confidentiellement.

II.2 Le chaos dans la transmission sécurisée

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données, en particulier pour transmettre des quantités importantes d'informations sécurisées. L'intérêt d'utiliser des signaux chaotiques réside dans deux propriétés du chaos :

Un signal chaotique est un signal à large spectre et permet donc de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ [25].

II.2.1 Schéma synoptique du dispositif de transmission sécurisée

La **Figure (II.1)** illustre d'une façon qualitative le principe de la transmission sécurisée de données à base de systèmes chaotiques.

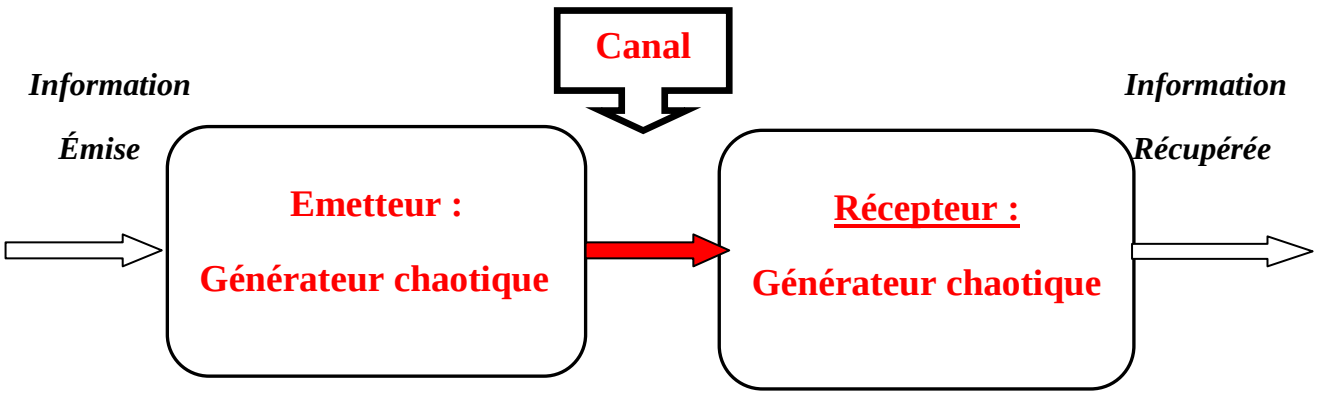


Figure (II.1) : Fondement de la transmission sécurisée à base du chaos

La confidentialité du message, son intégrité et son authenticité, constituent généralement les caractéristiques fondamentales d'une communication sûre et performante. On trouve ainsi différentes méthodes de synchronisation de systèmes et différentes techniques de cryptage ont été mises en place, certaines d'entre elles seront citées dans les sections **(II.3)** et **(II.4).**

II.2.2 Synchronisation des systèmes chaotiques

La synchronisation des oscillateurs non linéaires est un phénomène qui a attiré l'attention des chercheurs depuis le constat et la description de ce phénomène par Huygens en 1673, dans un exemple de deux systèmes mécaniques couplés. Depuis les années 90, de nombreux ouvrages ont été publiés au sujet de la synchronisation chaotique [26] [27], etc. Le phénomène de synchronisation est manifesté lorsque deux systèmes dynamiques évoluent d'une manière identique en fonction du temps. L'une des configurations de synchronisation les plus populaires est la configuration maître-esclave pour laquelle un système dynamique, appelé système esclave suit le rythme et la trajectoire imposés par un autre système dynamique, appelé système maître.

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système. Ce concept repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable, si par un moyen quelconque, deux systèmes puissent échanger de l'énergie, action que l'on nomme couplage (voir **section II.2.3**), ils finiront par se synchroniser [19].

Ainsi la synchronisation peut être définie comme suit :

Soit les deux systèmes :

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{y} = f_2(y) \end{cases} \quad \textbf{(II. 1)}$$

Avec $x(t), y(t) \in \mathbb{R}^n, f_1 \; et \; f_2$ des fonctions non linéaires définies de $\mathbb{R}^n \longrightarrow \mathbb{R}^n$.

Les deux systèmes sont synchronisés si :

$$\lim_{t\to\infty} \|y(t) - x(t)\| = 0 \quad \textbf{(II.2)}$$

Où $y(t) - x(t)$ représente l'erreur de synchronisation.

II.2.3 Synchronisation par couplage

Il est possible de synchroniser deux systèmes chaotiques identiques (1) et (2) par un couplage dit « unidirectionnel », le transfert de l'énergie d'un système à l'autre se fait à l'aide d'un élément de couplage fonctionnant dans un seul sens **(Figure II.1-a).**

Dans le couplage bidirectionnel, le transfert de l'énergie entre les systèmes (1) et (2) se fait dans les deux sens **(Figure II.2-b)** [15].

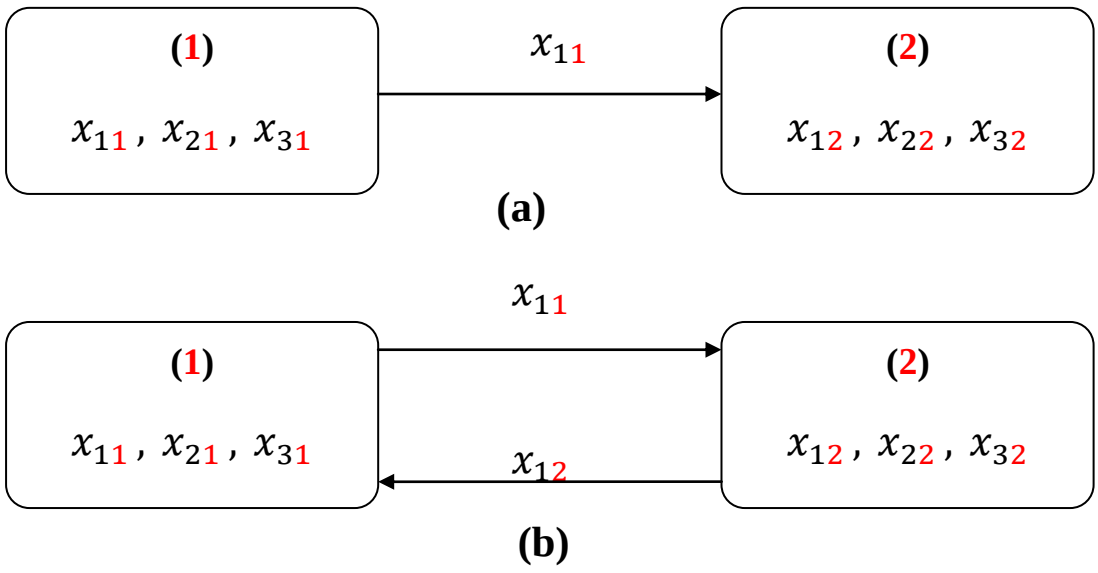


Figure (II.2) : Couplage : - (a) : unidirectionnel

- (b) : bidirectionnel

II.3 Méthodes de synchronisation des systèmes chaotiques

II.3.1 Synchronisation par décomposition du système

Cette méthode a été proposée par les deux chercheurs Pecora et Carroll en 1990 [28][29], ils ont montré que deux systèmes chaotiques identiques peuvent se synchroniser sous certaines conditions. Cette découverte a ouvert la voie pour l'application des systèmes chaotiques dans la communication et encore d'autres méthodes pour synchroniser le chaos.

On considère un système dynamique chaotique de dimension $n \geq 3$:

$$\dot{x} = f(x) \qquad (\mathbf{II.3})$$

On divise le système en deux sous-systèmes S1 et S2

$$\begin{cases} S1: \ \dot{x}_R = f_R(x_R) \\ S2: \ \dot{x}_T = f_T(x_R, x_T) \end{cases} \qquad \mathbf{(II.4)}$$

Où $x_R \in \mathbb{R}^{n_R}, x_T \in \mathbb{R}^{n_T}, n_R + n_T = n.$

S1 est le système conducteur, S2 est appelé le système de réponse.

On divise le sous-système conducteur S1 en deux autres sous-systèmes :

$$\begin{cases} \begin{cases} \dot{x}_{R_1} = f_{R_1}(x_{R_1}, x_{R_2}) \\ \dot{x}_{R_2} = f_{R_2}(x_{R_1}, x_{R_2}) \end{cases} \\ \dot{x}_T = f_T(x_R, x_T) \end{cases} \qquad \mathbf{(II.5)}$$

Cette synchronisation est basée sur la stabilité du sous système de réponse (S2), qui dépend des exposants de Lyapunov (appelés exposants de Lyapunov conditionnels) du système **(II.5)**

Ainsi Pecora et Carroll ont démontré que si tous les exposants sont négatifs, la stabilité du sous-système de réponse peut être garantie.

II.3.2 Synchronisation généralisée

L'application de la synchronisation identique de Pecora et Carroll [28], est soumise à une contrainte qui réside dans la difficulté de réaliser pratiquement un sous-système esclave tout à fait identique à un autre sous-système issu d'une décomposition du système maître.

Pour affranchir cet obstacle, une méthode plus générale est proposée qui est la Synchronisation Généralisée (SG), cette dernière est une généralisation du concept de la synchronisation identique, la SG peut donner une dynamique plus riche car elle peut aussi envisager certains cas désynchronisés, dus aux disparités des paramètres, aux déformations des canaux de transmission et autres.

En conséquence les possibilités d'appliquer la SG pratiquement, peuvent être plus larges que la synchronisation identique [16].

Deux systèmes sont synchronisés au sens généralisé, s'il existe une transformation M telle que :

$$\lim_{t\to\infty}\|\hat{x}(t) - M(x(t))\| = 0 \qquad (\mathbf{II.6})$$

Avec :

$x(t)$: l'état du système émetteur.

$\hat{x}(t)$: l'état du système récepteur.

Indépendamment des conditions initiales, si M est inversible, alors $M^{-1}(\hat{x})$ fournit une estimation de l'état x du système émetteur. Dans le cas contraire il serait impossible de fournir une estimation de l'état x. Ceci présente un inconvénient majeur pour les techniques de communication utilisant l'état de l'émetteur pour décrypter le message transmis.

II.3.3 Synchronisation par boucle fermée

La méthode proposée par Pecora et Carroll présente des bruits à l'entrée du système et une forte sensibilité aux variations de paramètres, ceci est dû au fait que la synchronisation est réalisée en boucle ouverte, ce qui rend cette méthode sensible.
Une autre méthode de synchronisation est proposée, elle est basée sur un bouclage par contre réaction qui permet de récupérer les signaux d'entrées, il peut être réalisée en utilisant l'erreur entre l'émetteur et le récepteur comme indiqué sur la **Figure (II.3)**. Ce qui permet de corriger le comportement du récepteur afin de synchroniser le système [30].

Supposons que l'émetteur s'écrit comme suit :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \qquad \textbf{(II.7)}$$

Le récepteur peut être décrit comme suit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + \varepsilon(y - \hat{y}) \\ \hat{y}(t) = h(\hat{x}) \end{cases} \qquad \textbf{(II.8)}$$

ε est une fonction de l'erreur entre $y - \hat{y}$, cette fonction est choisie de manière à ce que la synchronisation entre l'émetteur et le récepteur soit garantie.

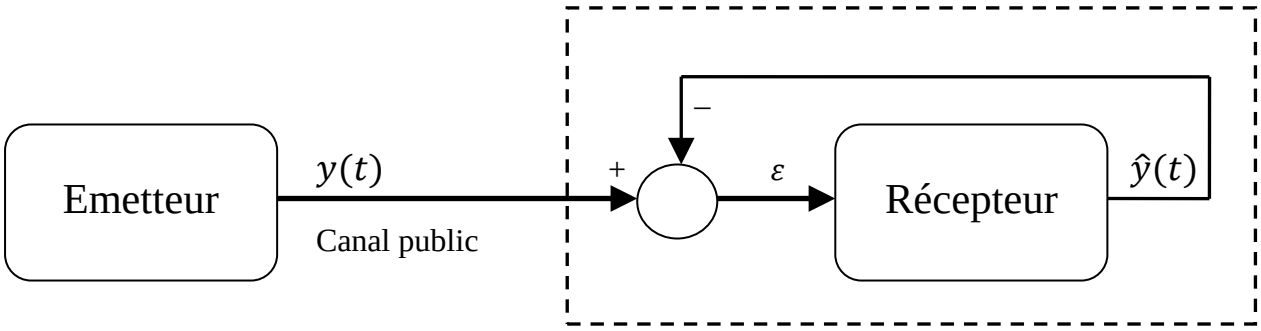


Figure (II.3) : Synchronisation par un contrôle en boucle fermée

II.3.4 Synchronisation à base d'observateurs

L'approche de synchronisation par observateurs est une méthode qui nous intéresse particulièrement dans ce travail. Elle est typique pour estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement, ce à cause de l'inaccessibilité et du facteur économique [31].

Dans cette approche, Le système *maître* est un système chaotique quelconque et le système *esclave* est un observateur d'état correspondant. La **Figure (II.4)** illustre ce principe de synchronisation.

Considérons le système décrit comme suit :

$$\begin{cases} \dot{x} = f(x,u) \\ y = h(x) \end{cases} \quad \textbf{(II.9)}$$

Nous dirons que l'émetteur et le récepteur se synchronisent si le système

$$\dot{\hat{x}} = \hat{f}(\hat{x},u)$$

Est un observateur convergent pour le système (2.8). Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

$$\lim_{t\to\infty}\|x(t) - \hat{x}(t)\| = 0 \quad \textbf{(II.10)}$$

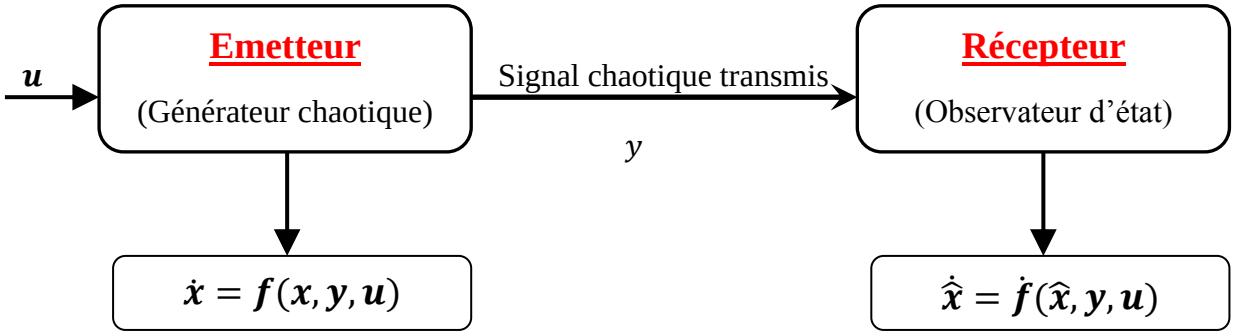


Figure (II.4) : Principe de synchronisation à base d'observateurs

De nombreux travaux de recherche ont été entrepris en exploitant les propriétés des observateurs non linéaires dans les applications de synchronisation des systèmes dynamiques , et plus particulièrement dans les applications de synchronisation des systèmes chaotiques pour la transmission sécurisée de l'information.

II.3.5 Synchronisation impulsive

Dans les méthodes présentées ci-dessus, généralement un des états du système dynamique est transmis dans le but de réaliser la synchronisation par le récepteur. Afin de réduire la redondance du signal transmis (rapport **signal / bruit**), la synchronisation impulsive a été proposée **Figure (II.5)**. Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système subissent des changements soudains [19].

On considère le système maître définit par **(II.3)**, et on définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal $y(t) = Cx(t)$ est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état.

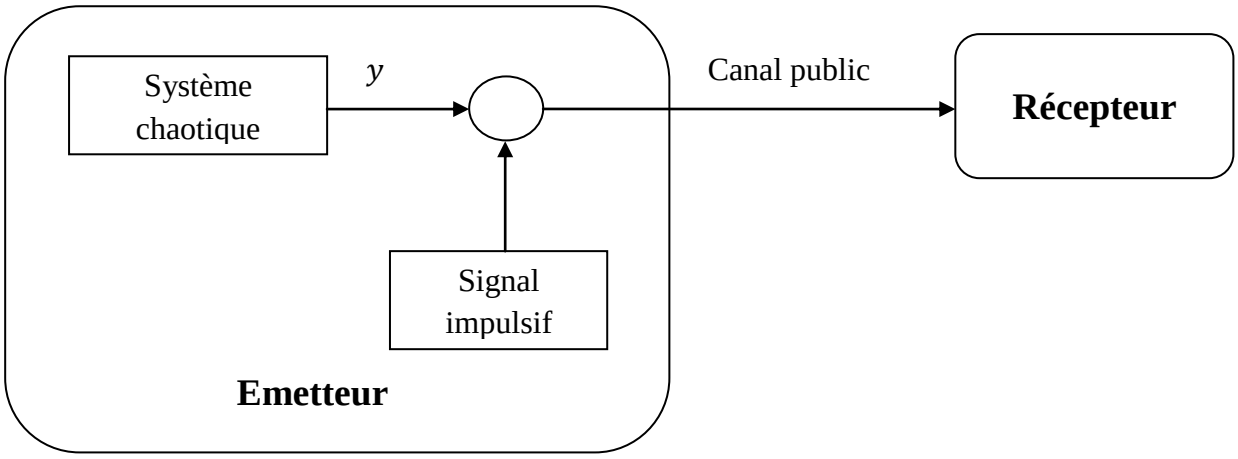


Figure (II.5) : Schéma de la synchronisation impulsive

II.3.6 Synchronisation retardée

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

$$\lim_{t\to\infty}\|\hat{x}(t) - x(t-\tau)\| = 0 \qquad \textbf{(II.11)}$$

Où $x(t)$ est l'état du système émetteur, $\hat{x}(t)$ est l'état du système récepteur et τ est un retard positif [32].

II.3.7 Synchronisation projective

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

$$\lim_{t\to\infty}\|\hat{x}(t) - ax(t-\tau)\| = 0 \qquad (\textbf{II. 12})$$

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

Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés [28][29][33].

II.3.8 Synchronisation de phase

La synchronisation de phase se produit lorsque les oscillateurs chaotiques couplés conservent leur différence de phase, tandis que leurs amplitudes délimitées restent non corrélées.

Pour deux systèmes périodiques de phases $\phi_1$et ϕ_2 [6], la synchronisation est exprimée par la relation suivante :

$$|n\phi_1 - m\phi_2| < \text{c} \qquad \textbf{(II.13)}$$

Avec m, n des entiers naturels et c une constante positive.

Ainsi pour exprimer la phase d'un système en représentant son signal analytique $\varphi(t)$ sous la forme d'une fonction complexe définie par :

$$\varphi(t)=\text{s(t)}+\text{j}\tilde{s}(\text{t})=\text{A(t)}.e^{j\theta(t)} \qquad \textbf{(II.14)}$$

Où $\tilde{S}$(t) est la transformée de Hilbert de la série temporelle $s(t), A(t)$ est l'amplitude de $\varphi(t)$ et $\theta(t)$ sa phase.

II.4 Les techniques de cryptage

La cryptographie par chaos a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage (supérieur à 1 Gbits/s). Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information [15][16].

II.4.1 Cryptage par addition

Cette technique est considérée comme la première proposition d'utiliser le chaos pour sécuriser la communication [16]. L'émetteur est un système chaotique autonome dont le signal $y(t)$ est ajouté au signal du message $m(t)$. La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal publique. Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction. Le schéma représentatif de cette méthode est donné par la **Figure** suivante :

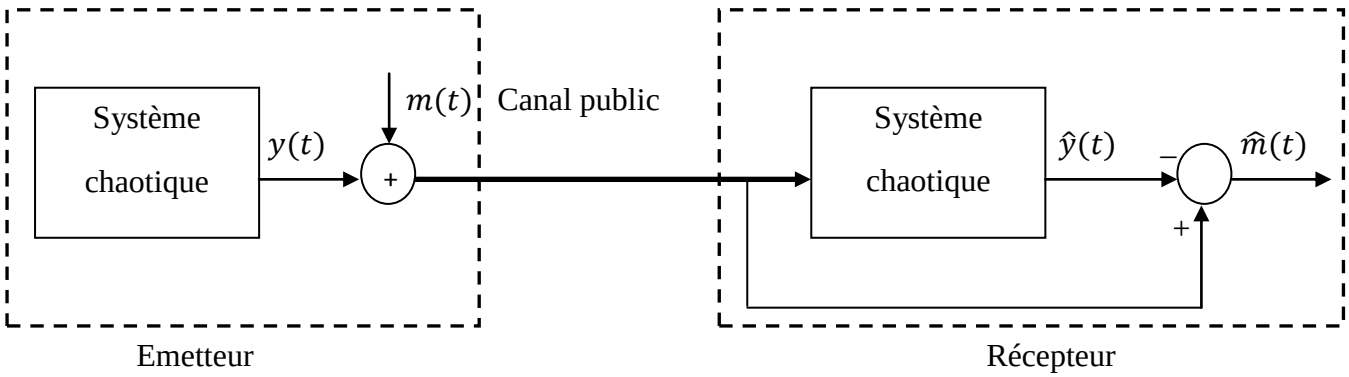


Figure (II.6): Principe du cryptage par addition

Le principal avantage de cette méthode réside dans la simplicité du cryptage, et aussi qu'elle est applicable à des systèmes continus ou discrets. L'inconvénient est qu'il est impératif que l'amplitude du message original soit significativement plus petite que celle de la porteuse chaotique afin d'éviter de perturber l'établissement de la synchronisation et de garantir la sûreté de la transmission.

II.4.2 Cryptage par commutation

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la **Figure (II.7)** où une opération de commutation est employée selon la valeur du message binaire :

Si sa valeur est 0 alors le système chaotique 1 est choisi et le signal de sortie est transmis, sinon la sortie du système chaotique 2 est transmise. Dans ce sens, le message binaire commute avec l'émetteur entre deux attracteurs étranges correspondants aux deux systèmes chaotiques.

Du coté récepteur, il y a deux sous-systèmes chaotiques 3 et 4 qui correspondent respectivement à 1 et 2. Supposant que le canal soit parfait, et que le signal transmis est 0 alors le sous-système 3 se synchronisera avec le système chaotique 1, mais le sous-système 4 ne pourra pas être synchronisé, selon les erreurs de synchronisation **(1,3) et (2,4)**, le signal pourra être récupéré avec succès [15][7].

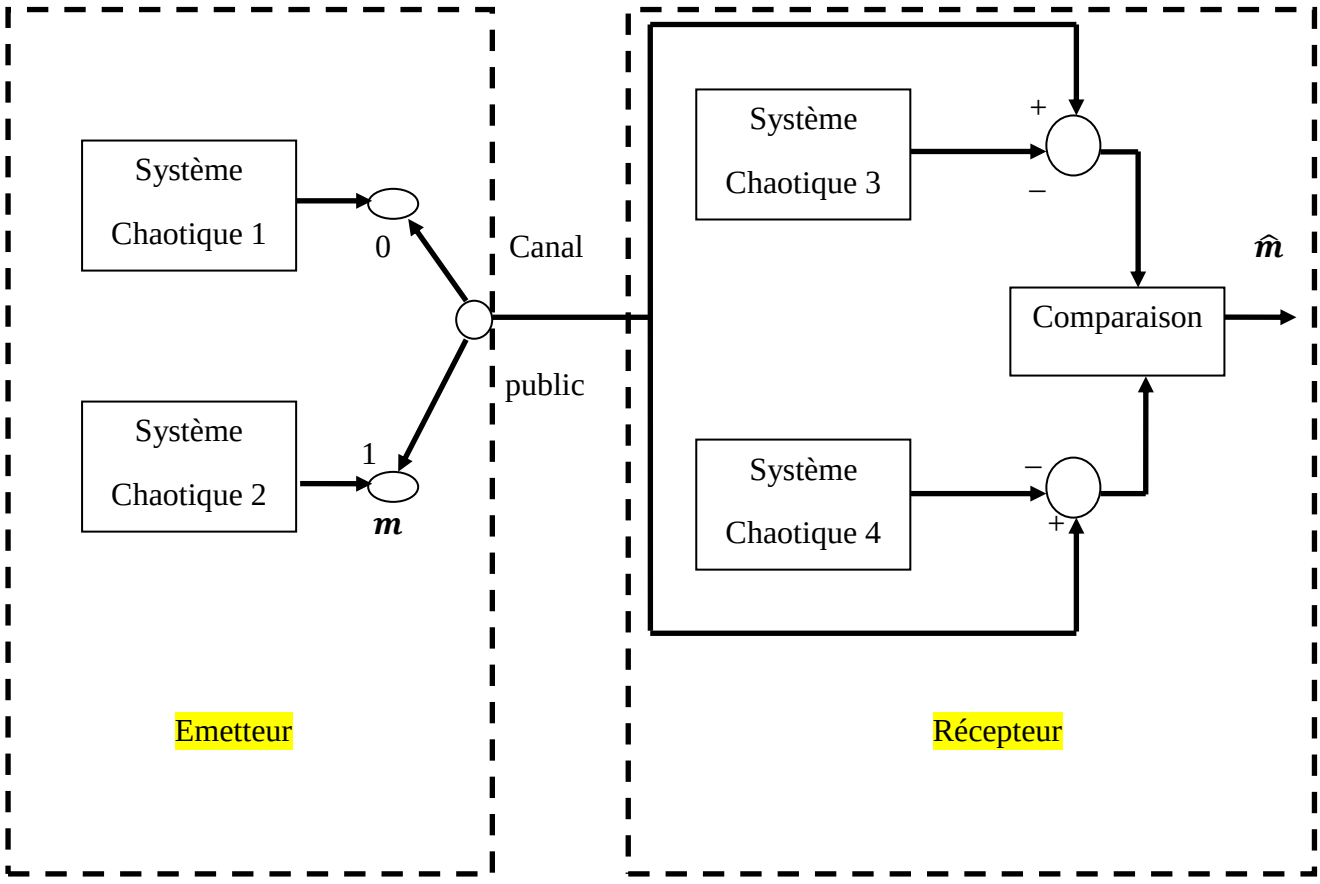


Figure (II.7) : Cryptage par commutation

II.4.3 Cryptage par modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique [36]. 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 à la Figure **(II.8)**

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment 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. Elle n'a pas d'équivalent parmi les systèmes de communication "classique".

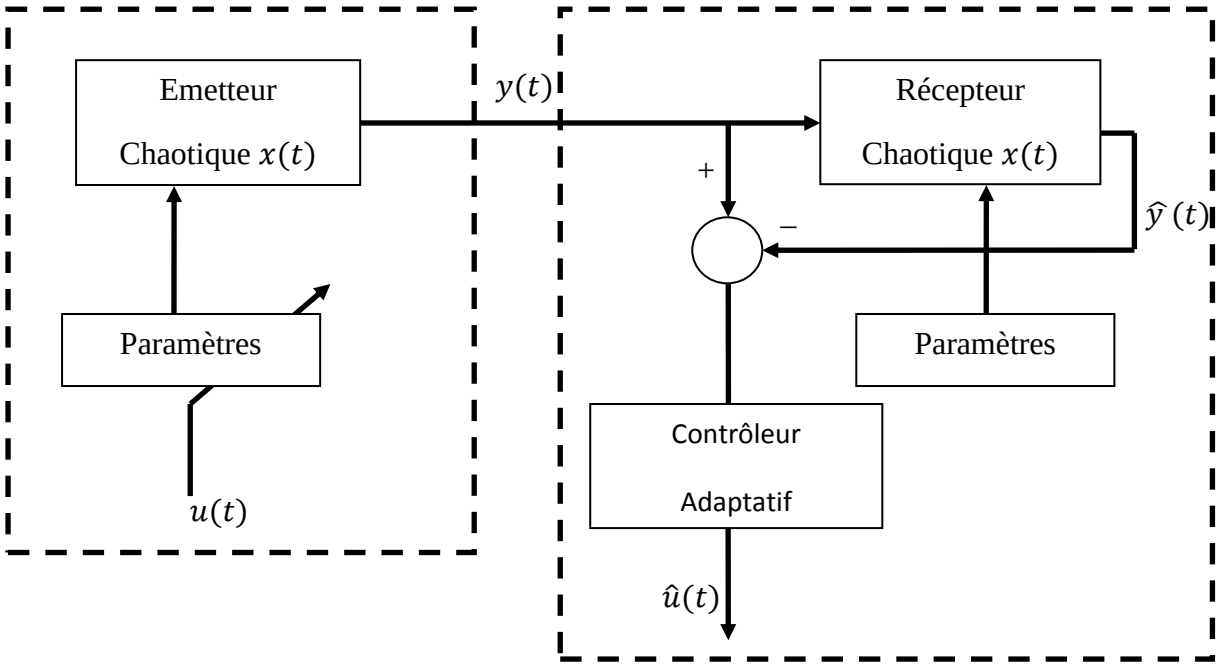


Figure (II.8) : Cryptage par modulation

II.4.4 Cryptage mixte

Cette méthode combine les principes de la cryptographie standard et la synchronisation chaotique. Le message $u(t)$ contenant l''information est crypté grâce à une clé $c(t)$, générée par l'émetteur chaotique. Le message crypté est alors injecté dans la dynamique du système chaotique pour la rendre plus complexe. En suite, un signal $y(t)$ fonction des variables d'état de l'émetteur est transmis au récepteur, qui établie une

synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de la méthode est illustré dans la **Figure(II.9)** [16].

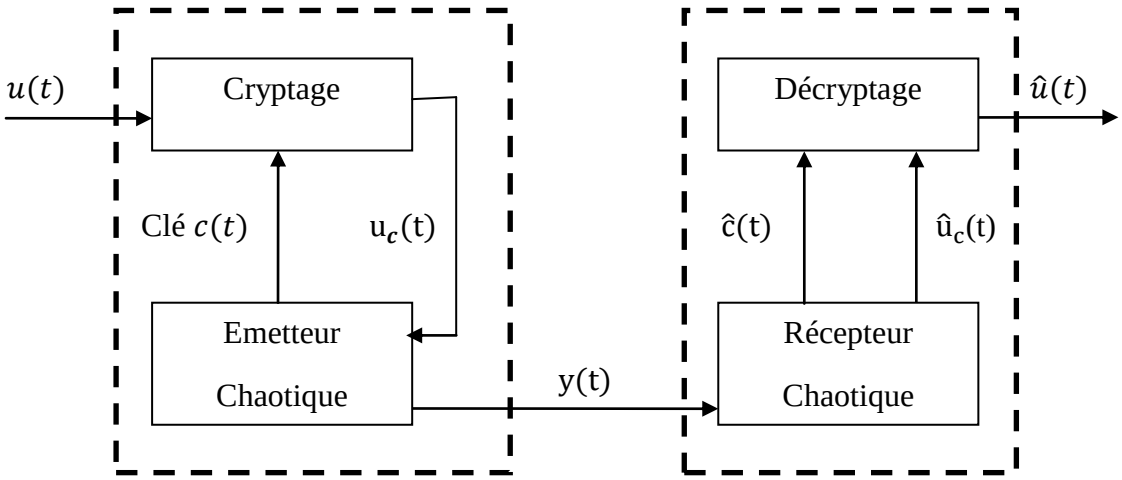


Figure (II.9) : Cryptage mixte

II.4.5 Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du coté de l'émission. Dans ce cas, la restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur [37].

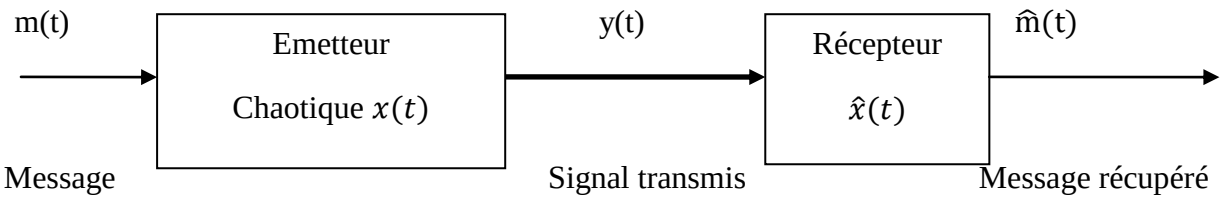


Figure (II.10) : Cryptage par inclusion

II.4.6 Transmission par deux voies

Dans le schéma présenté dans la **Figure (II.11)**, l'émetteur envoie deux signaux au récepteur. Le premier (y_1) est une fonction à valeurs réelles de l'état (x) du système émetteur chaotique, dont l'unique but est de permettre la synchronisation du récepteur. Le second (y_2) envoyé éventuellement sur un autre canal est un signal chaotique qui contient l'information à transmettre.

Parmi les avantages de cette méthode, on peut souligner d'une part que le signal (y_1) ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre coté, le second signal (y_2) contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état (x), soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse [16].

On peut noter également que les deux étapes de synchronisations et de cryptages étant totalement indépendantes, le décryptage n'est pas nécessairement effectué au niveau du récepteur, en même temps que la synchronisation.

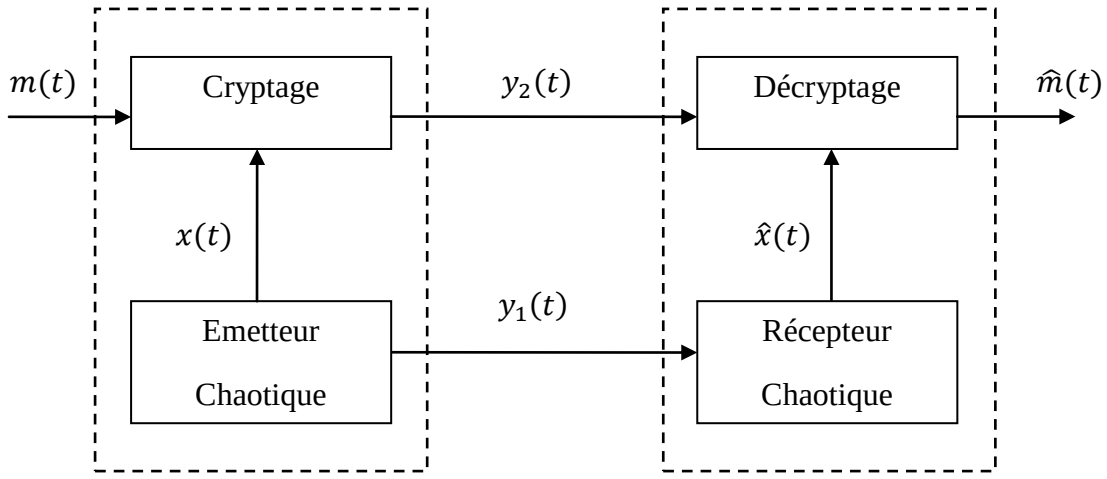


Figure (II.11) : Méthode de Transmission par deux voies

II.5 Cryptanalyse

La **cryptanalyse** est la science qui consiste à tenter de déchiffrer un message ayant été chiffré sans posséder la clé de chiffrement, c'est aussi l'étude de la sécurité d'un cryptosystème en tentant de casser les fonctions cryptographiques qui le composent.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant constamment et en parallèle [18]. En effet de nouveaux cryptosystèmes, plus complexes les uns que les autres sont développés afin de remplacer ceux qui ont déjà été "cassés" par la

cryptanalyse puis encore de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux cryptosystèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un cryptosystème soit supérieure à sa durée de validité. La tendance actuelle est de chercher à prouver la sécurité d'un système sur la base d'hypothèses sur la puissance de calcul requise ou sur la quantité de texte clair ou choisi connue.

La réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque (déchiffrement de la clé secrète, algorithme de chiffrement découvert sans connaître la clé secrète, informations sur le texte clair, etc.). La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées (addition, ou exclusif, etc.), par la mémoire nécessaire et par la quantité de données (texte clair et texte chiffré) requises.

A travers les années, de nombreuses attaques possibles contre les cryptosystèmes ont été identifiées, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques : les attaques actives et les attaques passives.

Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification modification des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi, etc.

Dans les attaques passives, l'adversaire observe les informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le cryptosystème sans l'altérer, telles que le message, la clé secrète, etc. Dans ce cas, l'adversaire touche à la confidentialité des données.

II.6 Conclusion

Ce chapitre nous a permis de faire le lien entre les systèmes dynamiques chaotiques et les systèmes de communication. Nous avons abordé le phénomène de synchronisation et présenté par la suite les principales méthodes utilisées pour la synchronisation des systèmes chaotiques. Pecora et Carroll ont ouvert la voie à l'utilisation du chaos dans les télécommunications. Ces derniers ont montré que deux systèmes chaotiques identiques peuvent se synchroniser s'ils sont couplés sous certaines conditions.

La synchronisation des systèmes chaotiques nous donne accès à la réalisation de différents systèmes permettant d'effectuer une transmission sécurisée d'informations. La sécurité de l'information transmise est assurée par diverses méthodes de cryptages, alors on a mentionné certaines de ces méthodes en présentant leurs avantages et inconvénients.

Chapitre III

Etude du système chaotique d'ordre fractionnaire Hénon Modifié

III.1 Introduction

En général, le comportement des systèmes physiques est décrit par des modèles mathématiques à dérivation et intégration d'ordre entier. Ces systèmes peuvent être encore mieux représentés par des modèles d'ordre non-entier appelé aussi d'ordre fractionnaire.

De nombreuses recherches ont été lancées dans ce sens, aujourd'hui on trouve divers systèmes à temps continu et à temps discret qui sont correctement décrits par des modèles d'ordre fractionnaires tel que des systèmes thermiques [38], systèmes électrochimiques [39]. Le calcul fractionnaire apparait aussi dans le domaine de l'automatique, notamment en robotique, en modélisation, identification et commande [38] [40] [41].

Dans notre travail, la dérivée d'ordre fractionnaire sera utilisée pour le calcul du modèle de Hénon modifié sur lequel notre système de transmission sécurisé est basé.

III.2 Sur le calcul fractionnaire

Le calcul d'ordre fractionnaire est une généralisation de l'intégration et de la différentiation des opérateurs d'ordre non entier. La question des dérivées fractionnaires est abordée en 1695 par Leibniz dans une lettre adressée à l'Hopital, lorsque ce dernier lui demande quelle pourrait être la dérivée d'ordre un demi $(1/2)$ de la fonction $x(t)$, par rapport à la variable t, Leibniz répond que cela mène à un paradoxe dont on tirera profit un jour, ainsi le calcul fractionnaire est alors né [42].

Les opérateurs d'intégration et de différentiation peuvent être représentés par un seul opérateur fondamental noté comme suit :

$$ {}_aD_t^{\alpha} $$

Où : a et t désignent respectivement la condition initiale et la variable par rapport a laquelle on applique l'operateur fractionnaire et $\alpha \in \mathbb{R}$, est l'ordre de l'opération.

L'opérateur intégro-différentiel continu est défini comme suit :

$$ {}_aD_t^{\alpha} = \begin{cases} \frac{d^{\alpha}}{dt^{\alpha}} & \alpha > 0 \\ \mathbf{1} & \alpha = 0 \\ \int_{\alpha}^{t} (d\tau)^{-\alpha} & \alpha < 0 \end{cases} \qquad \textbf{(III.1)} $$

L'équation différentielle fractionnaire est une équation qui contient une ou des dérivées fractionnaires,

Le système fractionnaire est un système qui est décrit par une équation différentielle fractionnaire.

❖ Dérivation d'ordre fractionnaire

Dans ce présent travail, le système d'ordre fractionnaire du modèle dit **Hénon modifié** est calculé selon la définition donnée par Grunwald-Letnikov, qui est donnée comme suit :

La définition au sens de Grunwald-Letnikov est basée sur une approche aux différences finies fractionnaires ou toute la différence par rapport au cas entier se situe dans l'extension de la factorielle à travers la fonction Gamma Euler [10].

$$\Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} dt, (z > 0) \qquad (\mathbf{III.2})$$

Cette définition est basée sur la généralisation de la dérivée classique d'une fonction $f(t)$ d'ordre $n \in \mathbb{N}$ de la forme :

$$D^n(t) = \lim_{h \to 0} \frac{1}{h^n} \sum_{j=0}^{\infty} (-1)^k \binom{n}{j} f(t - jh) \qquad (\mathbf{III.3})$$

$$\binom{n}{j} = \frac{n!}{j!\,(n-j)!} \qquad (\mathbf{III.4})$$

On remplace l'entier n par $\alpha \in \mathbb{R}$ $(\alpha > 0)$, alors l'expression **(III.4)** s'écrit:

$$\binom{\alpha}{j} = \frac{\Gamma(\alpha + 1)}{j!\,\Gamma(\alpha - j + 1)} \qquad (\mathbf{III.5})$$

La dérivée d'ordre fractionnaire d'ordre $\alpha > 0$ est donc :

$$ {}_aD_t^{\alpha} f(t) = \lim_{h\to 0} \frac{1}{h^{\alpha}} \sum_{j=0}^{\left[\frac{t-a}{h}\right]} (-1)^j \binom{\alpha}{j} f(t-jh) \qquad (\mathbf{III.6}) $$

III.3 Passage de l'ordre entier à l'ordre fractionnaire

Soit le système non linéaire à temps discret d'ordre entier représenté par l'équation d'état suivante :

$$ x(k+1) = f\big(x(k)\big) \qquad (\mathbf{III.7}) $$

Où $x(k) \in \mathbb{R}^n$ est le vecteur d'état de dimension n , $f(x)$ est un champ de vecteurs et $k \in \mathbb{N}$ représente le temps discret. Le vecteur d'état s'écrit comme suit : $x(k) = [x_1(k), x_2(k) \ \ldots \ x_n(k)]^T$

Le pas d'échantillonnage est $t_k = kT$ pour $k = 0,1,2,3,\ldots$, où T est la période d'échantillonnage.

On prend $T = 1$

Le premier ordre différentiel pour $x(k+1)$ peut être défini par :

$$ \Delta^1 x(k+1) = x(k+1) - x(k) \qquad (\mathbf{III.8}) $$

On note que cette équation représente l'approximation discrète d'EULER de la dérivation d'ordre entier $\frac{dx(t)}{dt}$

Donc :

$$\Delta^1 x(k+1) = f(x(k)) - x(k) \qquad (\mathbf{III.9})$$

Selon la définition de Grunwald-Letnikov l'operateur différentiel discret d'ordre fractionnaire (avec temps initial égal à zéro) est défini comme suit :

$$\Delta^{\alpha} x(k) = \frac{1}{T^{\alpha}} \sum_{j=0}^{k} (-1)^j \binom{\alpha}{j} x(k-j) \qquad (\mathbf{III.10})$$

Où

$$\binom{\alpha}{j} = \begin{cases} 1 & pour\ j = 0 \\ \dfrac{\alpha(\alpha-1)\dots(\alpha-j+1)}{j!} & pour\ j > 0 \end{cases} \qquad (\mathbf{III.11})$$

Ce résultat mène à la conception de l'espace d'état du système non-linéaire à temps discret d'ordre fractionnaire, en utilisant l'équation suivante :

$$\Delta^{\alpha} x(k+1) = f(x(k)) - x(k) \qquad (\mathbf{III.12})$$

De l'équation **(III.8)** on aura :

$$\Delta^{\alpha} x(k+1) = x(k+1) - \alpha x(k) + \sum_{j=2}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) \qquad (\mathbf{III.13})$$

On change la variable j :

$$p = j - 1$$

Et on remplace dans l'équation **(III.9)**

$$x(k+1) = f\big(x(k)\big) + (\alpha - 1)x(k) + \sum_{p=1}^{k}(-1)^{p+1}C_p x(k-p) \qquad (\mathbf{III.14})$$

Où :

$$C_p = \binom{\alpha}{p+1}$$

Remarque III.1

En général l'ordre fractionnaire α peut être différent pour chaque variable d'état $x_i(k)$. Cependant on note par α_i l'ordre fractionnaire correspondant à la variable d'état $x_i(k)$. Si les ordres α_i sont égaux le système est dit d'ordre commensurable, et s'ils sont différents alors il est d'ordre incommensurable

Le système **(III.14)** présente la propriété d'une longue mémoire infinie, il est facile de vérifier que le coefficient C_p diminue lorsque l'itération p augmente. Pour une utilisation pratique et pour le traitement d'un calcul, on peut utiliser la mémoire principale courte pour définir un système non-linéaire d'ordre fractionnaire plus exploitable. On note par L la longueur limitée de la mémoire, donc le système est écrit comme suit :

$$x(k+1) = f\big(x(k)\big) + (\alpha - 1)x(k) + \sum_{p=1}^{L}(-1)^{p+1}C_p x(k-p) \qquad (\mathbf{III.15})$$

Remarque III.2

Pour $\alpha = 1$, on obtient le système non-linéaire d'ordre entier **(III.7).**

III.4 Le modèle de Hénon-modifié d'ordre fractionnaire

Considérons le système de Henon modifié d'ordre entier :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \quad (\mathbf{III.16})$$

Afin de garantir au mieux la sécurité de la transmission considérée dans notre travail, on propose une alternative qui consiste à augmenter le nombre de clés de sécurité, pour cela on utilise un système chaotique d'ordre fractionnaire.

En utilisant la définition de Grunwald-Letnikov, le système d'ordre fractionnaire correspondant au système d'ordre entier **(III.16)** est donné comme suit :

$$\begin{cases} \boldsymbol{x_1(k+1) = a - x_2{}^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \sum_{p=1}^{L} C_{p1}x_1(k-p)} \\ \boldsymbol{x_2(k+1) = x_1(k) + (\alpha_2 - 1)x_2(k) + \sum_{p=1}^{L} C_{p2}x_2(k-p)} \\ \boldsymbol{x_3(k+1) = x_2(k) + (\alpha_3 - 1)x_3(k) + \sum_{p=1}^{L} C_{p3}x_3(k-p)} \end{cases} \quad (\mathbf{III.17})$$

On pose :

$$\mu_1 = \sum_{p=1}^{L} C_{p1}x_1(k-p) \;\; et \;\; \mu_2 = \sum_{p=1}^{L} C_{p2}x_2(k-p) \;\; et \;\; \mu_3 = \sum_{p=1}^{L} C_{p3}x_3(k-p)$$

Avec : $\begin{cases} 0 < \alpha_1 \leq 1 \\ 0 < \alpha_2 \leq 1 \\ 0 < \alpha_3 \leq 1 \end{cases}$

Une configuration des paramètres du modèle s'impose et ce afin d'avoir un comportement chaotique, dans ce travail on considère différents ordres fractionnaires (cas incommensurable), Le comportement chaotique est obtenu en fixant les clés ; $a = 1.5, b = 0.1,\ \alpha_1 = 0.85,\ \alpha_2 = 0.9,\ \alpha_3 = 0.75$ et $L = 5$.

Les conditions initiales $x_1(0) = 0.1,\ x_2(0) = 0.5,\ x_3(0) = 0.1$ sont choisies à l'intérieur du bassin d'attraction.

III.5 Etude des caractéristiques du modèle obtenu

III.5.1 Attracteur chaotique du système

Les simulations effectuées sous Matlab montrent le comportement chaotique du système d'ordre fractionnaire obtenu. La figure suivante montre l'attracteur chaotique qui prend la forme d'un croissant.

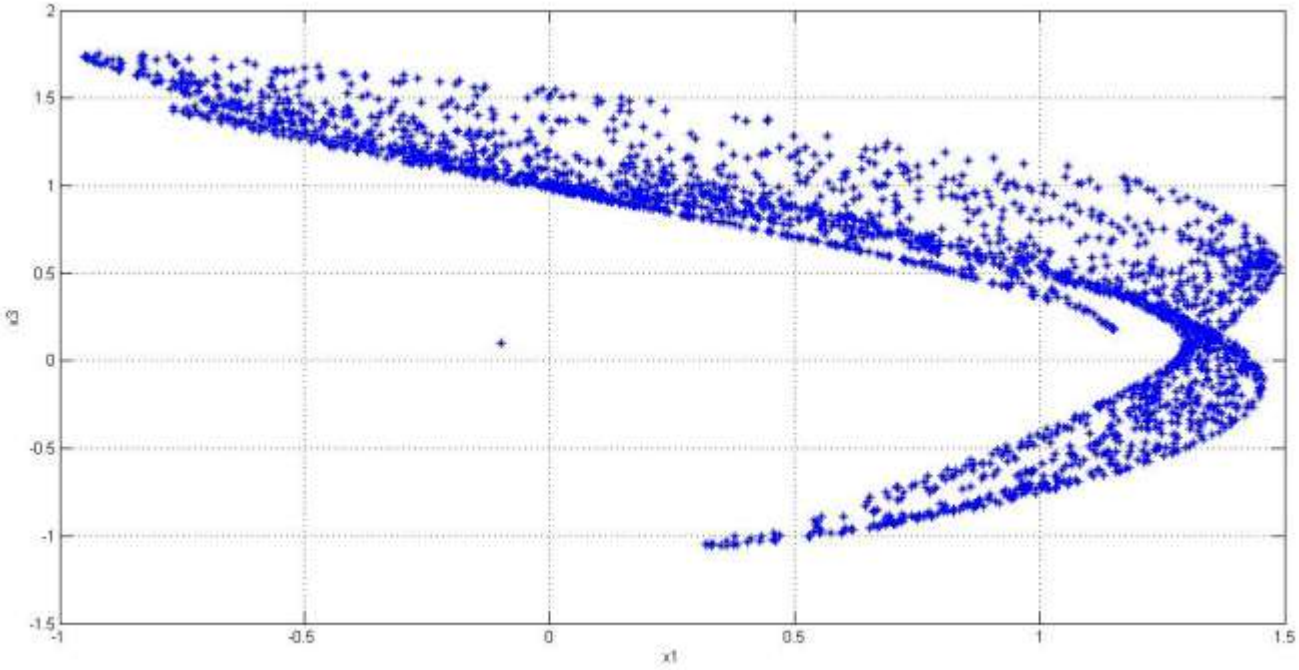


Figure (III.1) : Attracteur chaotique du modèle de Hénon-modifié d'ordre fractionnaire.

III.5.2 Etats chaotiques du système

Les figures qui suivent représentent les états x_1, x_2 et x_3 du système et illustrent l'aspect aléatoire du modèle. Ainsi à partir des ces figures, on constate que tous les états présentent un comportement chaotique.

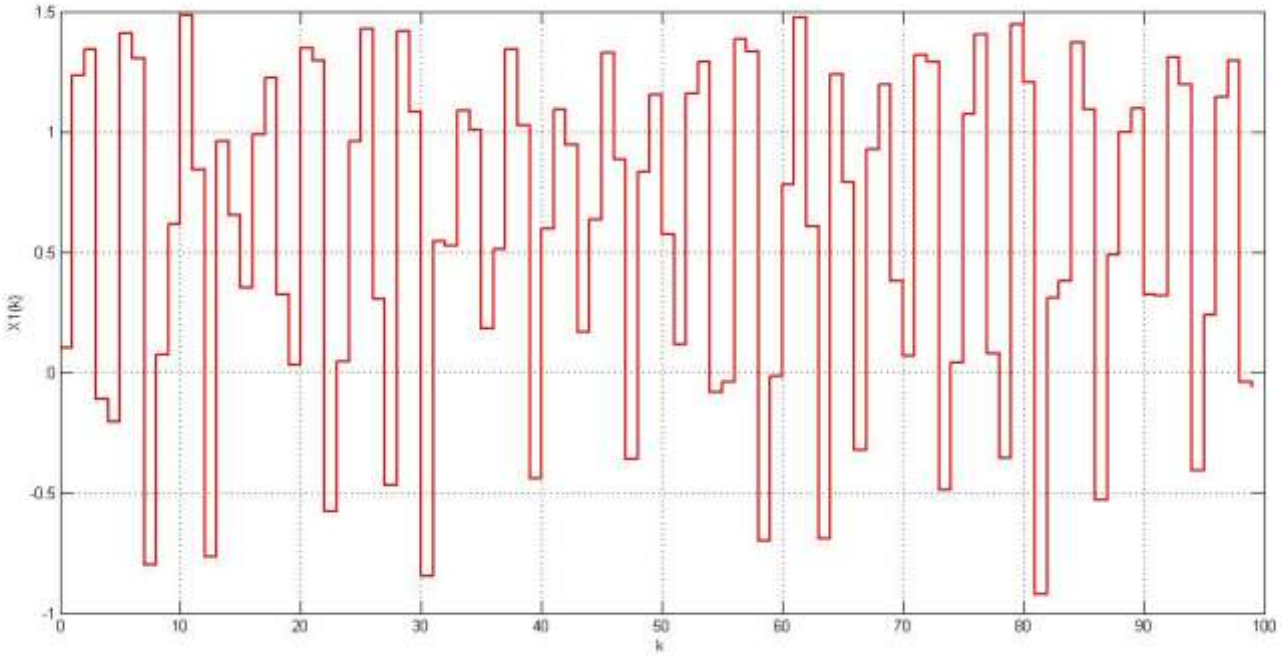


Figure (III.2) : Etat $x_1(k)$ du système de Hénon modifié

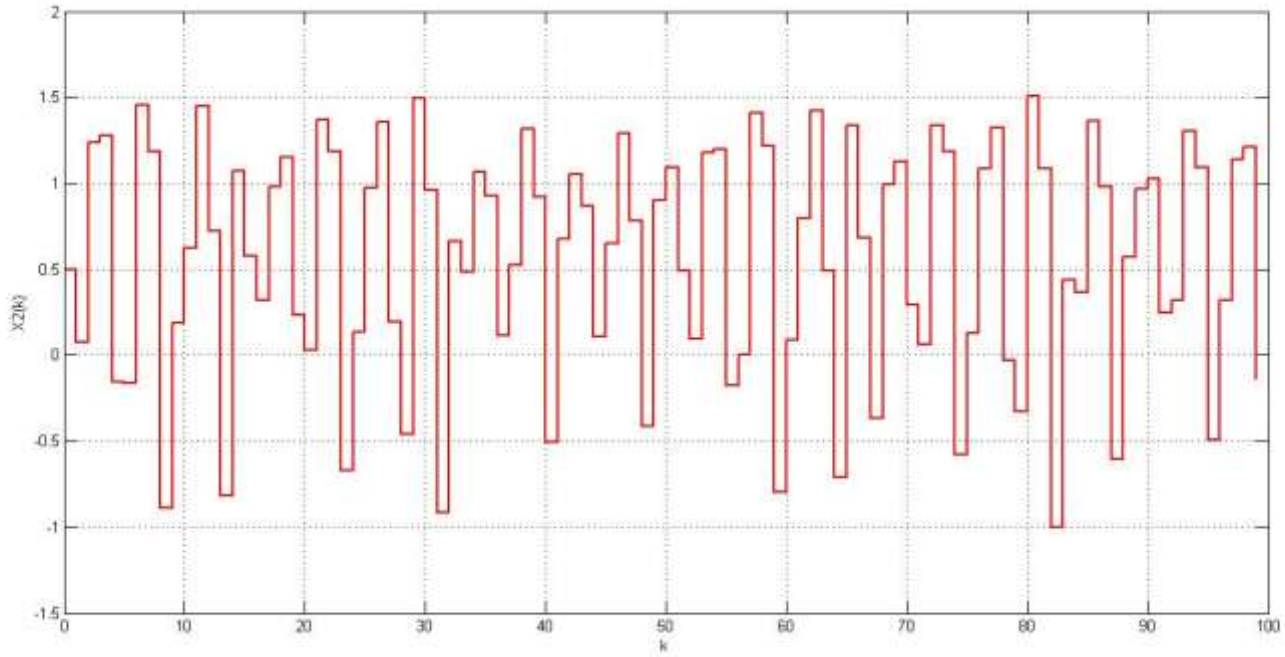


Figure (III.3) : Etat $x_2(k)$ du système de Hénon modifié

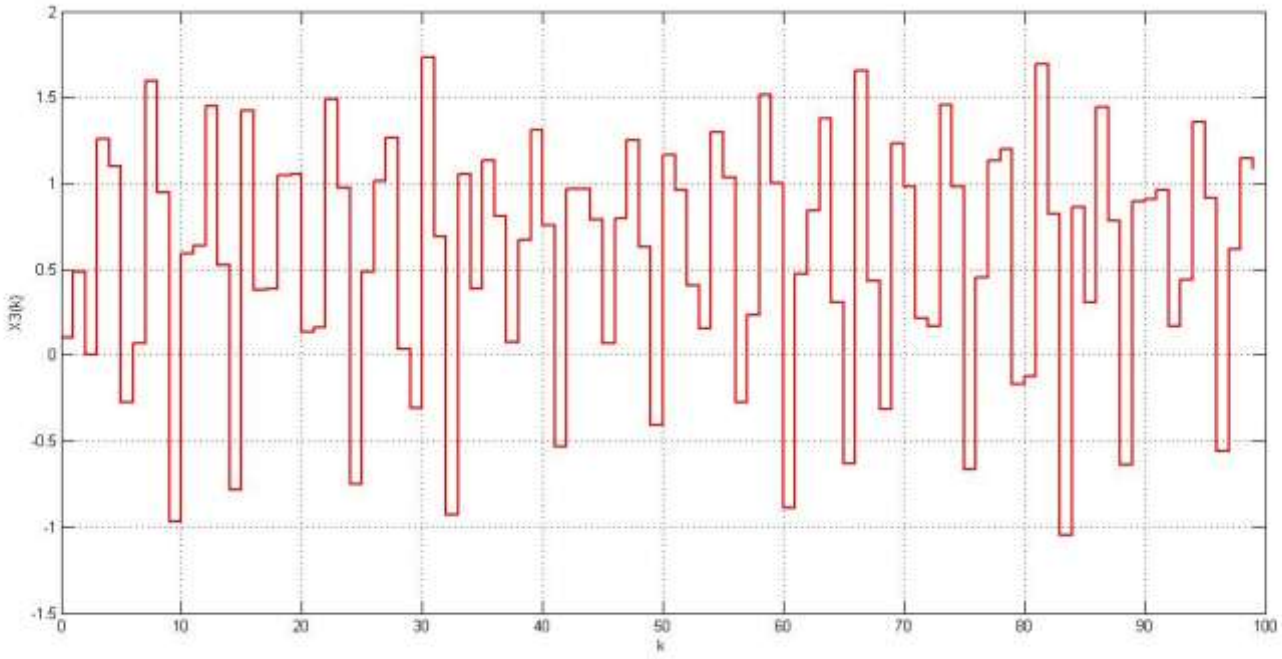


Figure (III.4) : Etat $x_3(k)$ du système de Hénon modifié

III.5.3 Sensibilité aux conditions initiales

La figure ci-dessous illustre la propriété de sensibilité aux conditions initiales, par exemple une modification de l'ordre de 10^{-4} de la valeur de la condition initiale de l'état $x_1(k)$ conduit à une divergence par rapport à l'état considéré

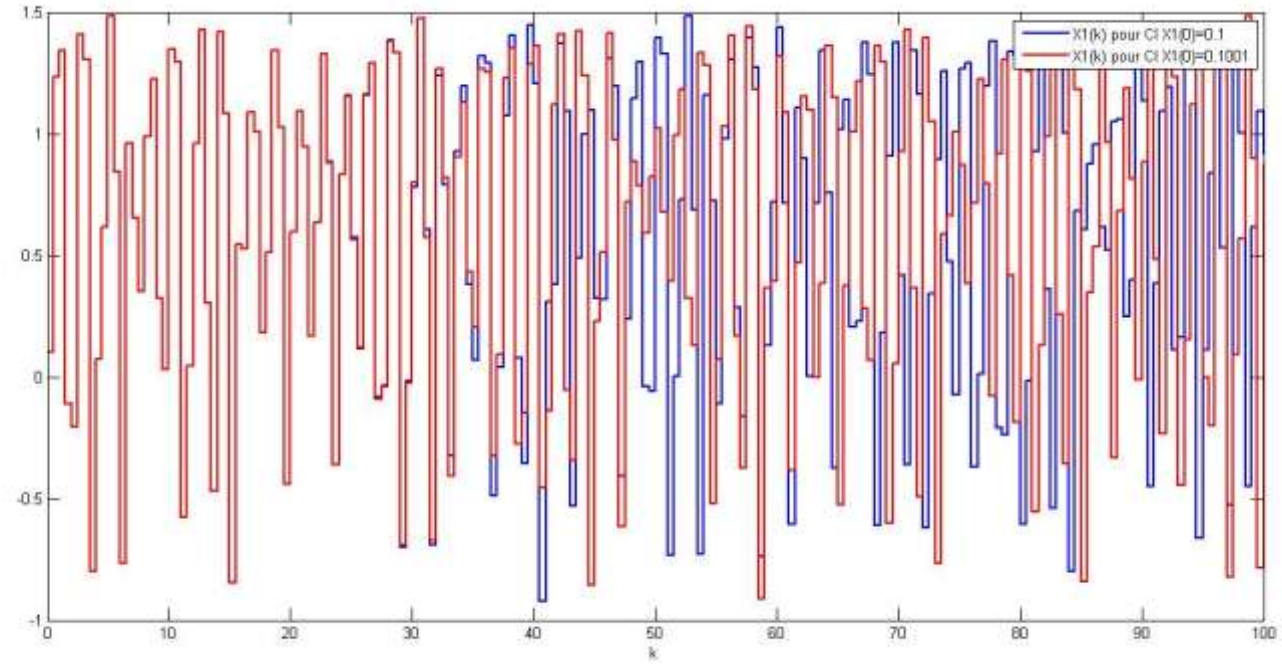


Figure (III.5) : Illustration de la sensibilité aux conditions initiales.

III.5.4 Diagramme de bifurcation

La figure suivante (**Figure (III.6)**), montre le diagramme de bifurcation pour l'état $x_1(k)$ en fonction du paramètre variant a.

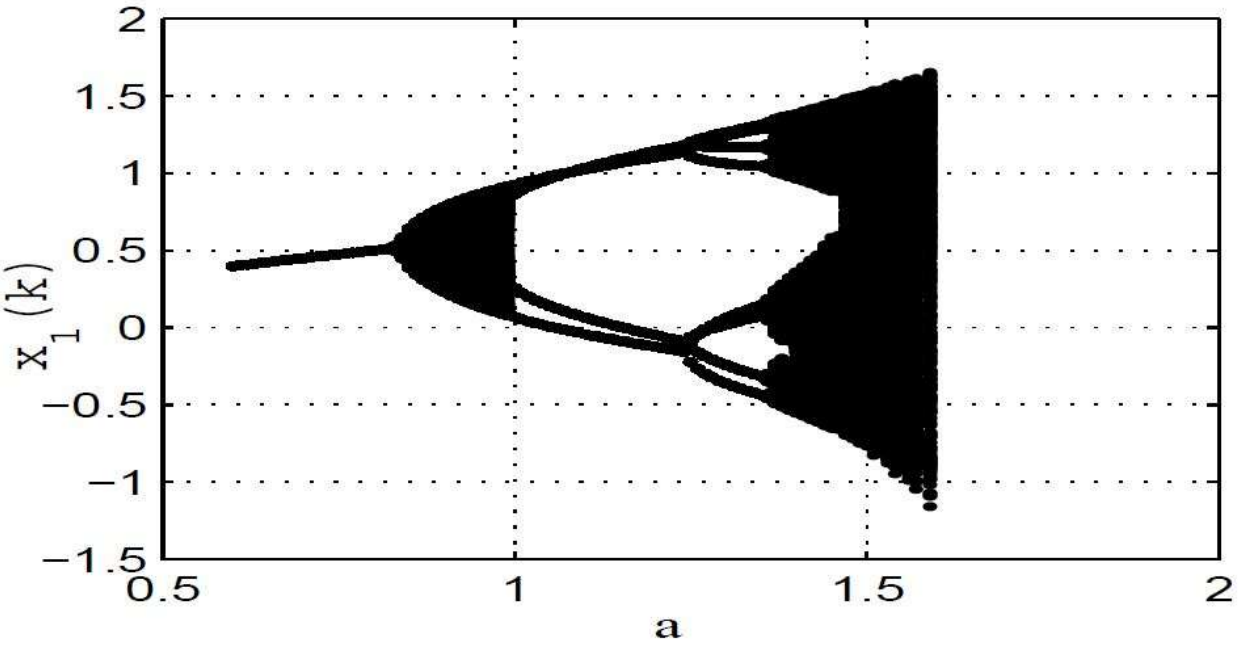


Figure (III.6) : Diagramme de bifurcation de l'état $x_1(k)$

Le système présente un comportement chaotique pour $a \in [1.3, 1{,}7]$. Cependant, durant notre synchronisation le paramètre est fixé comme suit $a = 1.5$.

III.6 Conclusion

L'utilisation du calcul fractionnaire pour l'obtention du modèle de Hénon modifié a été réalisée avec succès tout en préservant le comportement chaotique de notre système, ceci a été démontré et illustré par les résultats de calculs et simulations sous le logiciel Matlab. Mieux encore, la dérivée d'ordre fractionnaire appliquée a engendrée un nombre de paramètres supplémentaires qui vont servir comme clés de sécurité pour la conception du système de transmission. Ceci permet donc d'accroitre la sécurité et la fiabilité de notre transmission qui sera effectué dans le chapitre suivant.

Cependant, l'étude du système résultant nous permet d'avoir accès aux caractéristiques du modèle telles que l'attracteur étrange, la sensibilité aux conditions initiales et le diagramme de bifurcation qui ont été simulé sous Matlab.

Chapitre IV

Transmission sécurisée à base du système chaotique d'ordre fractionnaire Hénon Modifié

IV.1 Introduction

Ce présent chapitre fera l'objet de l'exploitation du système chaotique de Hénon modifié d'ordre fractionnaire (présenté au chapitre précédent) pour la conception d'un nouveau système de transmission sécurisée de données. A cet effet, nous avons élaboré un programme Script sous le logiciel Matlab pour les différents calculs et simulations, les résultats de simulations seront illustrés à la fin de ce chapitre.

IV.2 Etude du système de transmission sécurisée basé sur le système chaotique de Hénon modifié d'ordre fractionnaire

Dans ce travail, nous réalisons un dispositif de transmission sécurisée de données par le biais du système chaotique de Hénon modifié d'ordre fractionnaire. Ce dispositif contient principalement un émetteur, un récepteur et un canal public de transmission. Le schéma de la **Figure (IV.1)** illustre le schéma synoptique de cette transmission.

L'émetteur est constitué du système chaotique de Hénon modifié et du message à envoyé, ce dernier est passé par une fonction de cryptage. Le récepteur est constitué d'un observateur qui servira pour la synchronisation ainsi que la récupération du message via une fonction de décryptage.

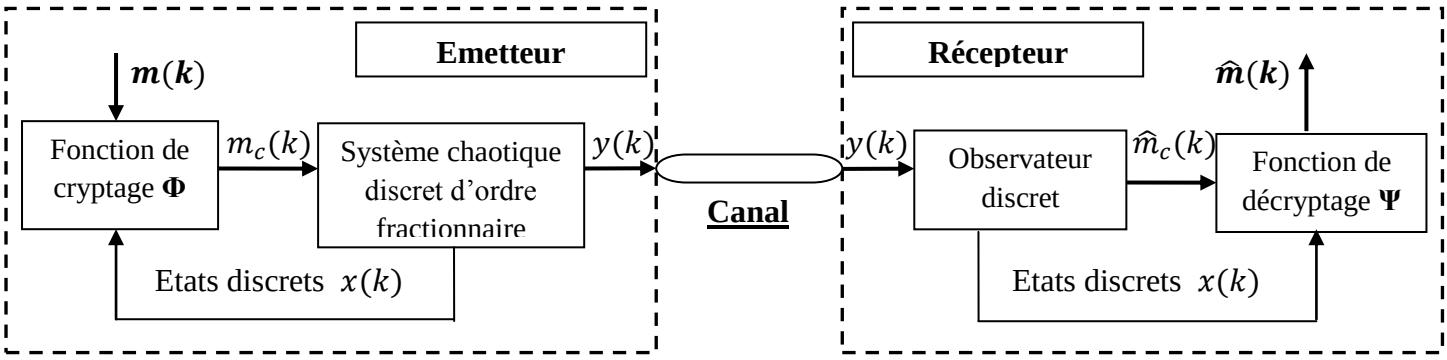


Figure (IV.1) : Schéma synoptique du dispositif de transmission sécurisée

Avec :

$m(k)$: Message original à envoyer, $m_c(k)$: le message crypté

$y(k) = x_2(k)$: Sortie du système émetteur

$\widehat{m}_c(k)$: Message crypté reconstruit, $\widehat{m}(k)$: Message en clair récupéré.

IV.3 Etude de l'émetteur

Afin de pouvoir réaliser une transmission robuste en matière de sécurité, on apporte une modification pour le système **(III.17)** (voir Chapitre III).

Comme montré dans la **Figure (IV.1)**, le message à transmettre $m(k)$ est crypté en utilisant une fonction de cryptage ϕ qui est fonction des états $x_1(k)$ et $x_3(k)$

Pour ce faire et afin de préserver le comportement chaotique du système, le message chiffré $m_c(k) = \phi(x_1(k), x_3(k), m(k))$ est inclus dans la dynamique de la troisième composante de notre système, ainsi on obtiendra un nouveau système régi par les équations suivantes :

$$\begin{cases} x_1(k+1) = a - {x_2}^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \mu_1 \\ x_2(k+1) = x_1(k) + (\alpha_2 - 1)x_2(k) + \mu_2 \\ x_3(k+1) = x_2(k) + (\alpha_3 - 1)x_3(k) + \mu_3 + m_c(k) \end{cases} \quad (\mathbf{IV.1})$$

avec :

$$\mu_1 = \sum_{p=1}^{L} C_{p1}x_1(k-p) \;\; et \;\; \mu_2 = \sum_{p=1}^{L} C_{p2}x_2(k-p) \;\; et \;\; \mu_3 = \sum_{p=1}^{L} C_{p3}x_3(k-p)$$

Le message crypté est défini comme suit :

$$\begin{aligned} m_c(k) &= \phi\big(x_1(k), x_3(k), m(k)\big) \\ &= m(k) + \boldsymbol{c}x_1(k) + \boldsymbol{d}x_3(k) + \boldsymbol{e}x_1^2(k) + \boldsymbol{f}x_3^2(k) + \boldsymbol{g}x_1(k)x_3(k) \quad + \\ &\qquad \boldsymbol{h}x_1^2(k)x_3(k) \end{aligned} \quad (\mathbf{IV.2})$$

Les paramètres $c, d, e, f, g, et\ h$ constituent les nouvelles clés secrètes du système **(IV.1)**.

Le choix des valeurs de ces clés secrètes reste à prendre avec grand soin, et ce afin de préserver le comportement chaotique du système.

Les états du système sont représentés dans les **Figures (IV.2), (IV.3)** et **(IV.4)** :

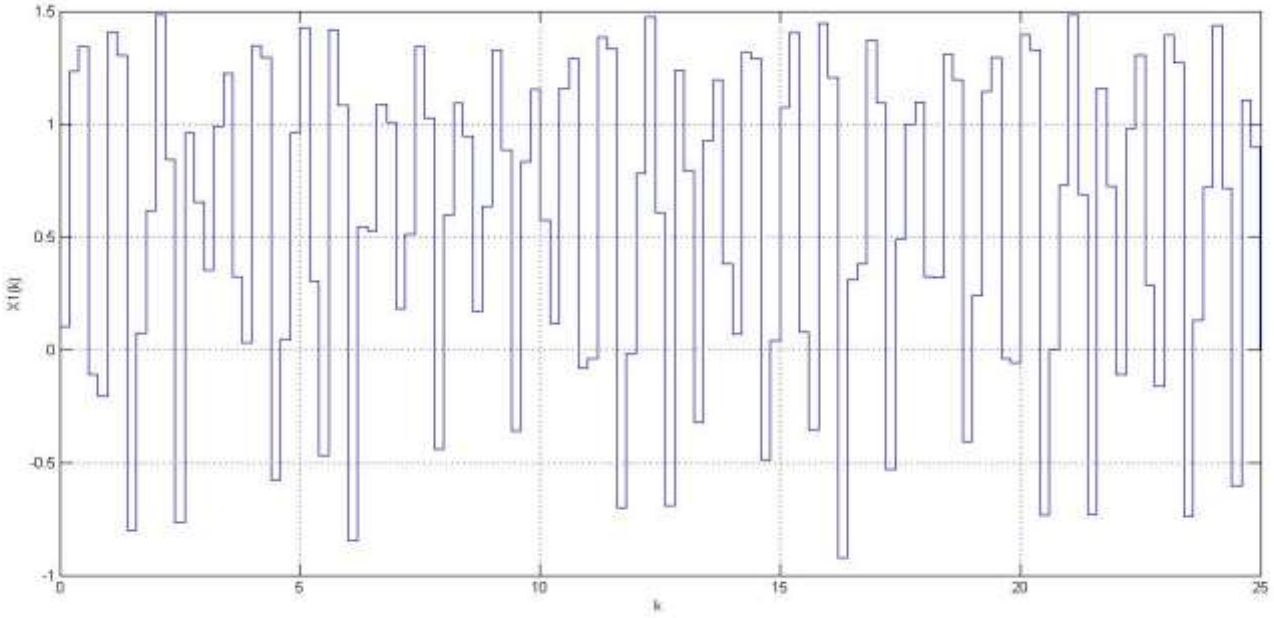


Figure (IV.2) : Etat $x_1(k)$ du système.

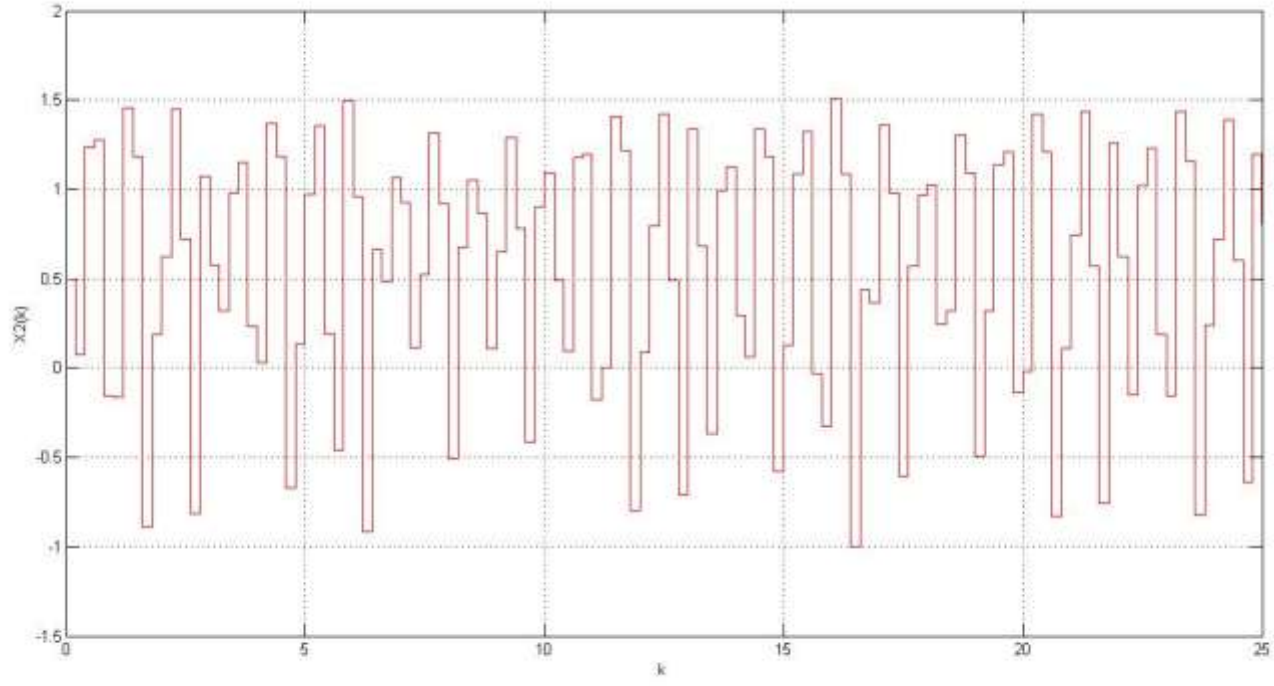


Figure (IV.3) : Etat $x_2(k)$ du système.

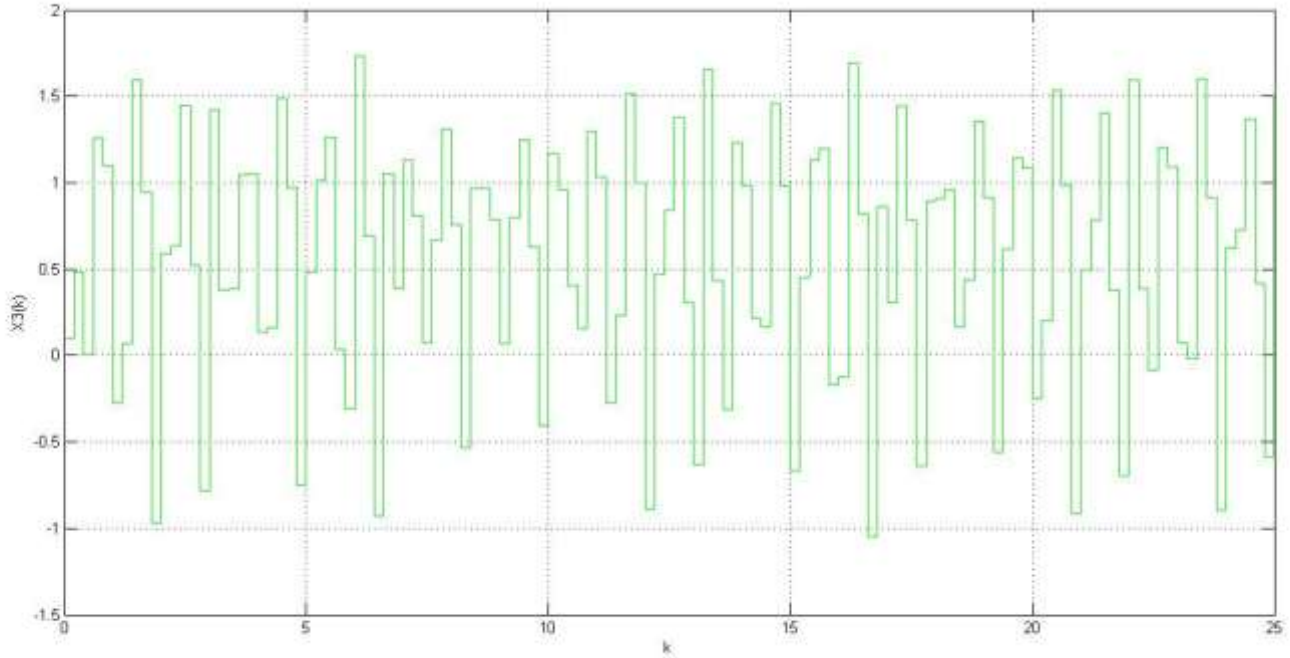


Figure (IV.4) : Etat $x_3(k)$ du système.

IV.4 Etude du récepteur

Dans cette partie, on s'intéresse particulièrement à la reconstruction des états $x_1(k)$ et $x_2(k)$ ainsi que le message $m(k)$. La sortie $y(k) = x_2(k)$ du système est considérée.

Pour la réception nous allons concevoir un observateur discret retardé d'ordre fractionnaire [8]. Ce qui va nous permettre la reconstruction des états du système en plus du message qui va être décrypté en utilisant la fonction de décryptage Ψ qui est l'inverse de la fonction ϕ, ie, $\Psi = \phi^{-1}$. Elle est donnée comme suit :

$$\hat{m}(k) = \Psi\left(\hat{x}_1(k), \hat{x}_3(k), \hat{m}_c(k)\right)$$

$$= \hat{m}_c(k) - \boldsymbol{c}\hat{x}_1(k) - \boldsymbol{d}\hat{x}_3(k) - \boldsymbol{e}\hat{x}_1^2(k) - \boldsymbol{f}\hat{x}_3^2(k) - \boldsymbol{g}\hat{x}_1(k)\hat{x}_3(k) - \boldsymbol{h}\hat{x}_1^2(k)\hat{x}_3(k) \qquad (\mathbf{IV.3})$$

❖ **Reconstruction de l'état $\hat{x}_1 = x_{1o}$**

De la seconde équation du système **(IV.1)**, en appliquant un retard (d'une étape), on déduit l'état $\hat{x}_1$ comme suit :

$$\hat{x}_1(k-1) = y(k) - (\alpha_2 - 1)y(k-1) - \mu_2' \qquad (\mathbf{IV.4})$$

Où

$$\mu_2{}' = \sum_{p=1}^{L} C_{p2}\hat{x}_2(k-p-1)$$

❖ **Reconstruction de l'état $\hat{x}_3 = x_{3o}$**

De la première équation du système **(IV.1)**, en appliquant un retard de deux étapes à la sortie, nous déduisons l'état $\hat{x}_3$ comme suit :

$$\hat{x}_3(k-2) = \left(1/b\right)[\, a - y^2(k-2) - \hat{x}_1(k-1) + (\alpha_1 - 1)\hat{x}_1(k-2) + \mu_1' \,] \qquad (\mathbf{IV.5})$$

Où

$$\mu_1{}' = \sum_{p=1}^{L} C_{p1}\hat{x}_1(k-p-2)$$

❖ **Reconstruction du message $\hat{m} = m_0$**

Encore une fois à partir de la troisième équation du système **(IV.1)**, en appliquant un retard de trois étapes, on peut écrire :

$$\hat{m}_c(k-3) = \hat{x}_3(k-2) - y(k-3) - (\alpha_3 - 1)\hat{x}_3(k-3) - \mu_3' \qquad \mathbf{(IV.6)}$$

Où

$$\mu_3{}' = \sum_{p=1}^{L} C_{p3}\hat{x}_3(k-p-3)$$

Enfin, en utilisant la fonction de décryptage Ψ donnée par **(IV.3)**, le message reconstruit $\widehat{m}(k)$ est :

$$\widehat{m}(k-3) = \widehat{m}_c(k-3) - [\, c\hat{x}_1(k-3) + d\hat{x}_3(k-3) + e{x_1}^2(k-3) + f{x_3}^2(k-3) + g\hat{x}_1(k-3)\hat{x}_3(k-3) + h{x_1}^2(k-3)\hat{x}_3(k-3)\,] \qquad (\mathbf{IV.7})$$

IV.5 Résultats de simulation

Dans ce travail, nous allons simuler notre programme sous Matlab. Pour ce faire, on utilise un signal sinusoïdal comme message à envoyer.

❖ **Reconstruction de l'état $\hat{x}_1 = x_{1o}$**

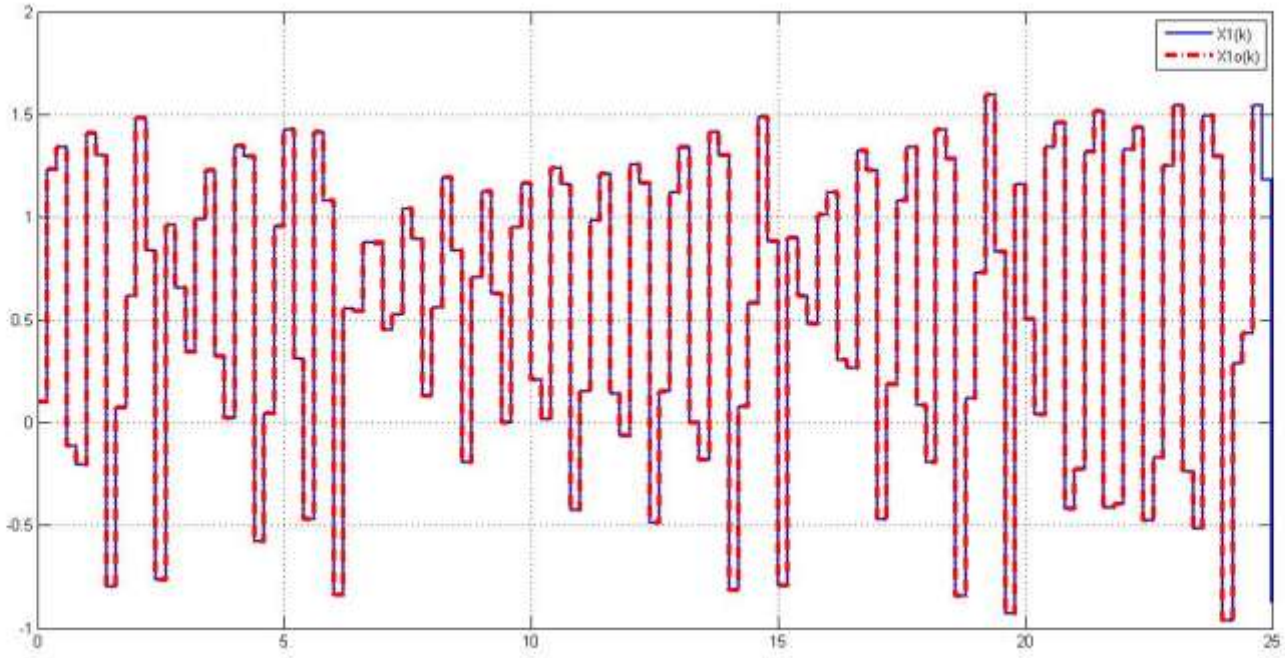


Figure (IV.5) : Etats chaotiques ; $x_1(k)$ (Emetteur) et $x_{10}(k)$ (Récepteur).

❖ **Reconstruction de l'état $\hat{x}_3 = x_{3o}$**

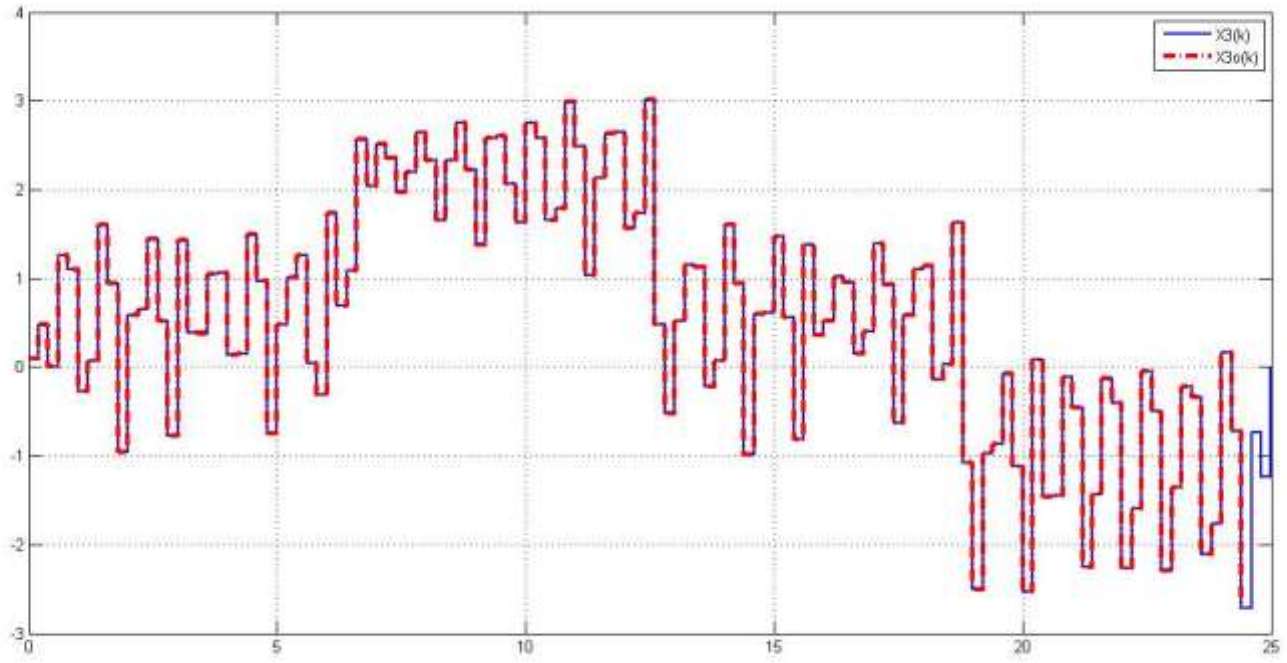


Figure (IV.6) : Etats chaotiques ; $x_3(k)$ (Emetteur) et $x_{30}(k)$ (Récepteur).

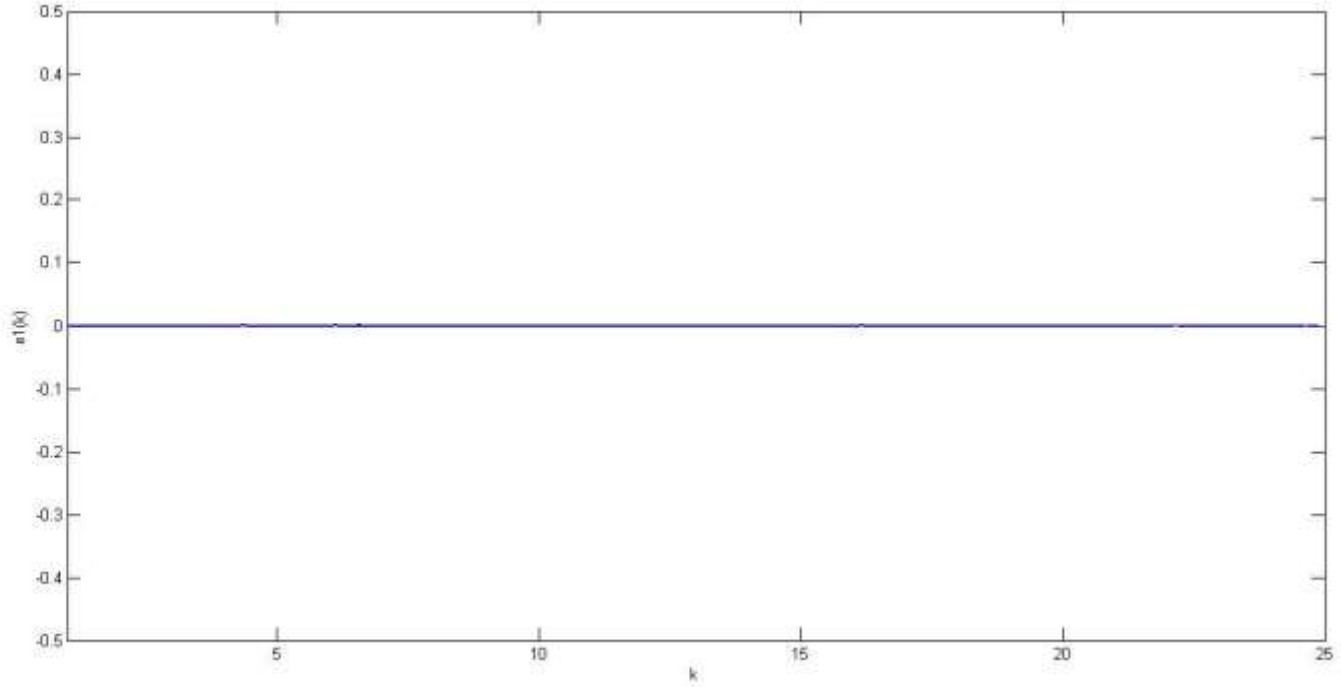


Figure (IV.7) : Erreur de synchronisation (écart $x_1 - x_{10}$)

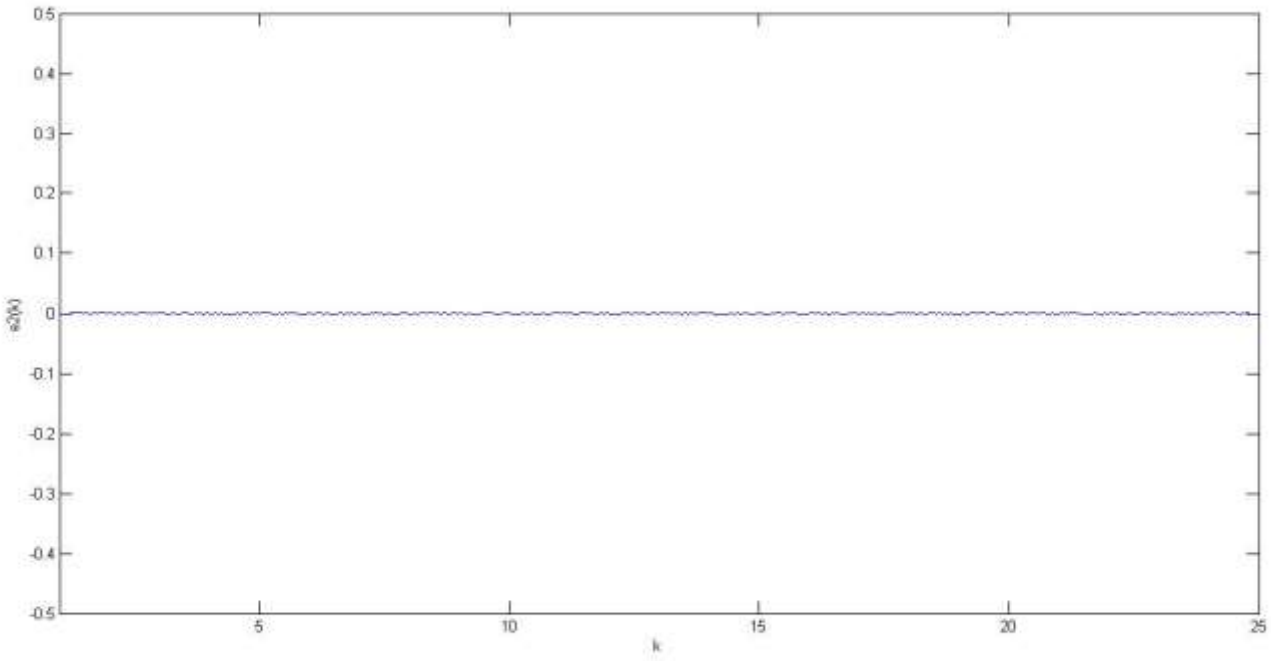


Figure (IV.8) : Erreur de synchronisation (écart $x_3 - x_{30}$)

Observations

La reconstruction des états x_1 et x_3 a été faite avec succès, Ceci dit la synchronisation de l'émetteur avec le récepteur a abouti à la génération d'une erreur de synchronisation quasiment nulle comme montré sur les figures précédentes.

❖ **Reconstruction du message $\hat{m} = m_0$**

Message original

Le message à envoyer pour cette simulation est un signal de forme sinusoïdal, ce dernier a été généré sur Matlab et il est représenté par la Figure suivante :

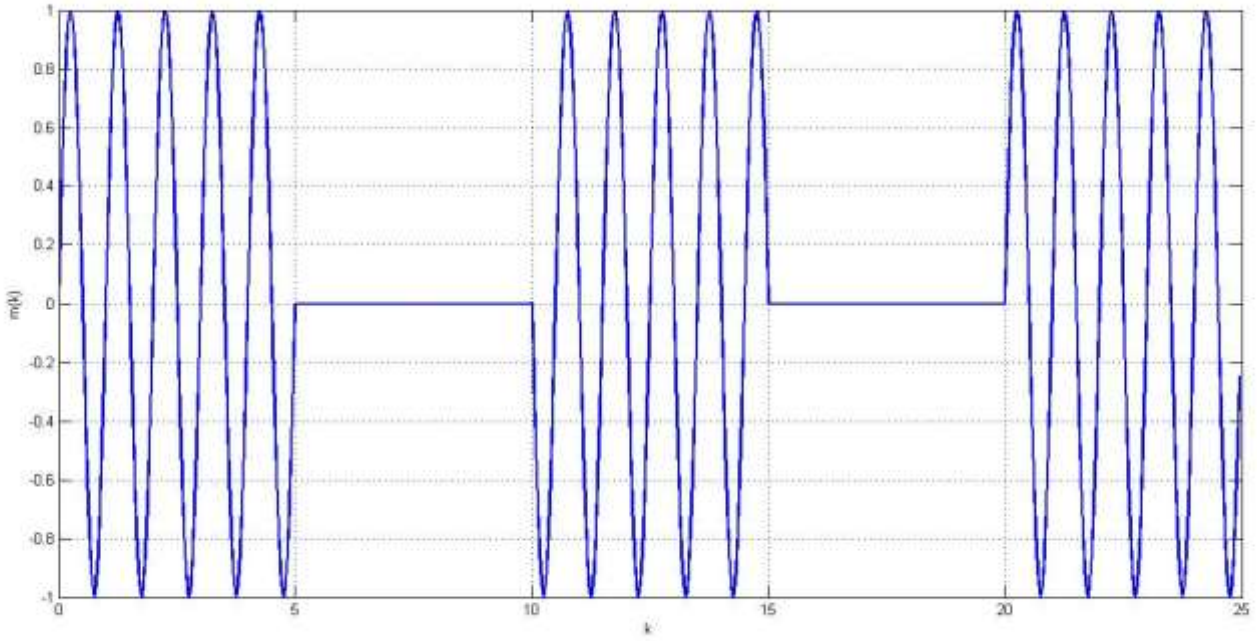


Figure (IV.9) : Message d'origine $m(k)$.

Message crypté

Les paramètres issus de la transformation du modèle en ordre fractionnaire ont servi de clés secrètes pour le cryptage du message. Les valeurs de ces paramètres ont été soigneusement choisies et on est arrivé à les fixer comme suit :

$$c = 1,\ \ d = 0.1,\ \ e = -0.5,\ \ f = 0.1,\ \ g = -0.8,\ \ h = 0.8$$

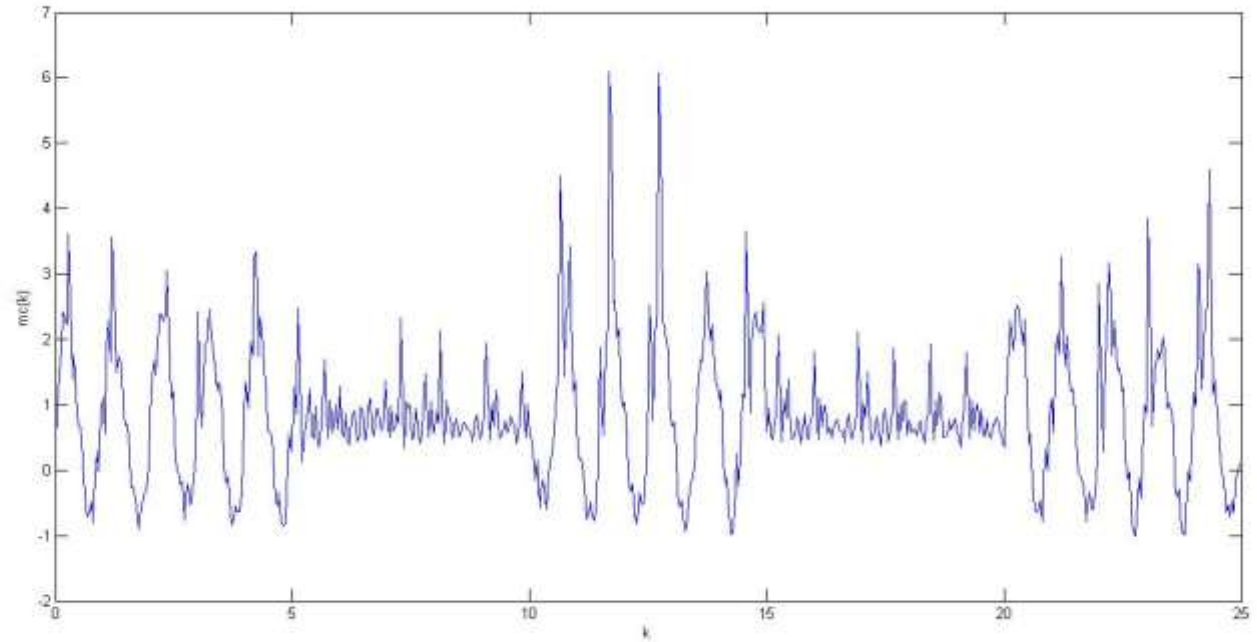


Figure (IV.10) : Message crypté $m_c(k)$.

Message récupéré

La synchronisation étant réussie avec une erreur quasiment nulle, la reconstitution du message a été parfaite, ceci est illustré par les figures suivantes :

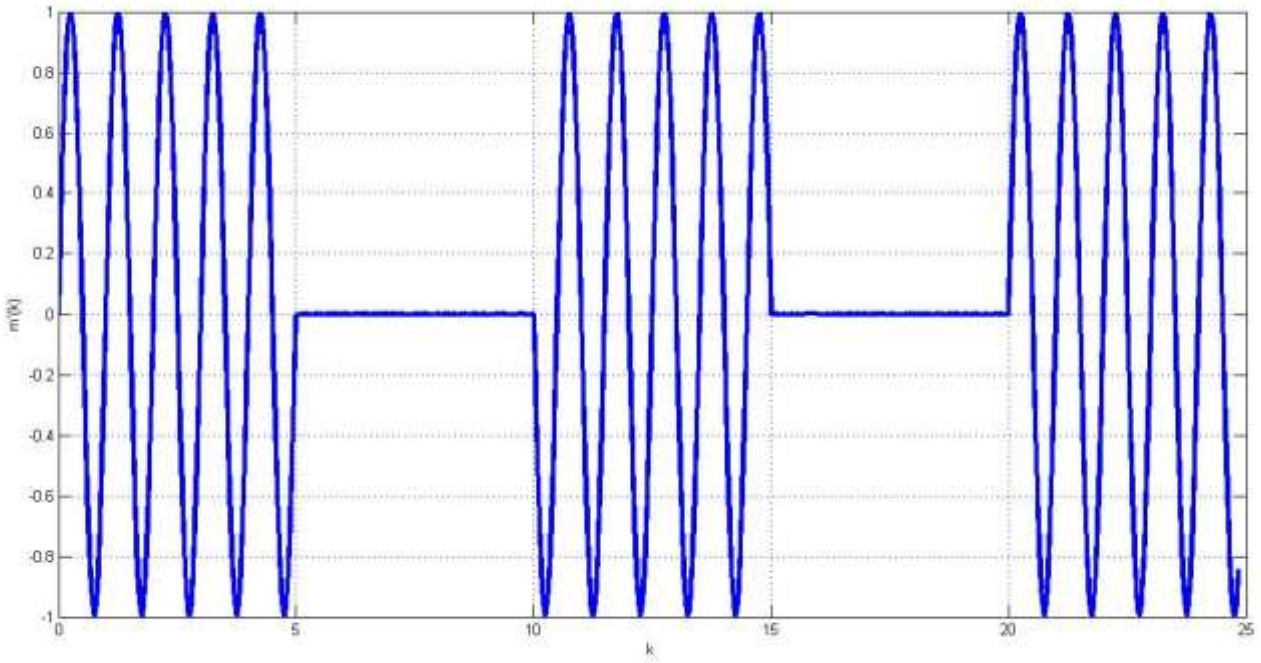


Figure (IV.11) : Message récupéré $\widehat{m}(k)$.

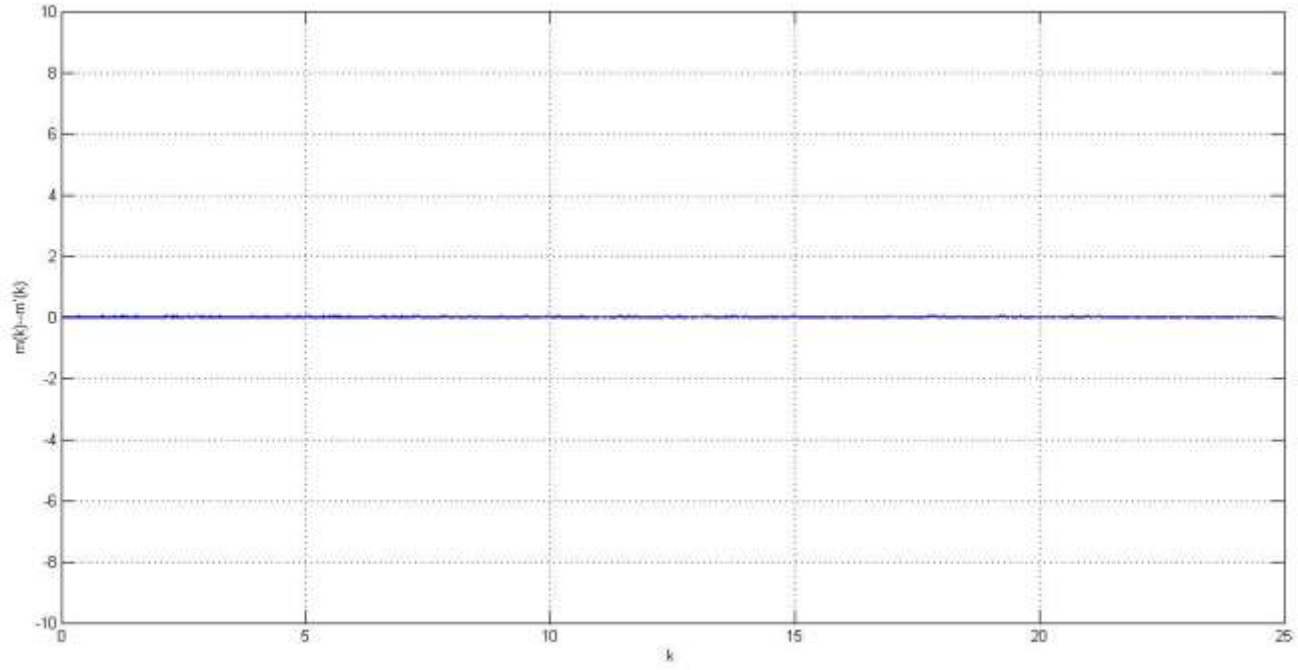


Figure (IV.12) : Erreur de synchronisation (écart $m(k)$- $\widehat{m}(k)$).

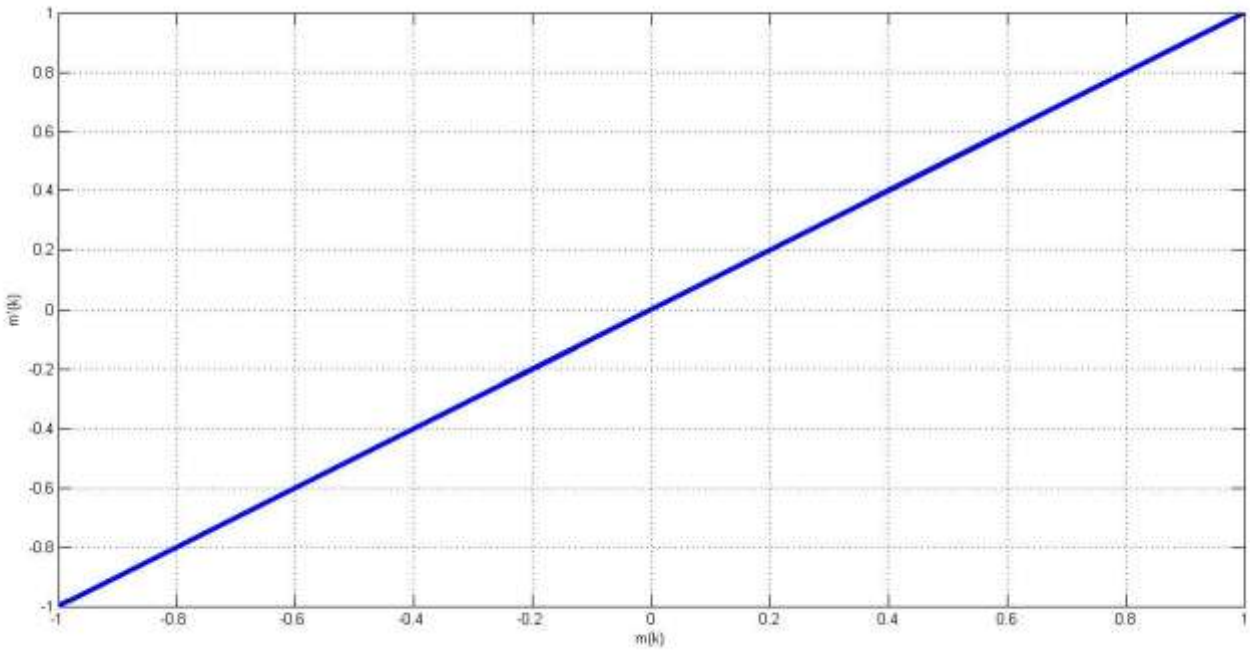


Figure (IV.13) : Plan de phase $m(k)$ en fonction de $\hat{m}(k)$.

IV.6 Conclusion

Dans ce chapitre, nous avons présenté les résultats de simulation de notre dispositif de transmission proposé. Ce dernier est composé de deux parties (un émetteur et un récepteur). La partie émetteur est construite autour du système de Hénon modifié d'ordre fractionnaire auquel on a ajouté le message crypté. Ce dernier a été inclus dans la dynamique du système chaotique en utilisant la méthode de cryptage par inclusion. Le choix de cette technique de cryptage réside dans sa robustesse par rapport aux bruits de canal. La partie récepteur est constitué d'un observateur discret dit retardé étape par étape. Son choix est justifié par sa capacité à reconstruire les états de l'émetteur d'une manière exacte. Autrement dit, les erreurs de synchronisation entre les états de l'émetteur et ceux du récepteur sont nulles. Par conséquent, le message a été reconstruit d'une manière parfaite.

Conclusion générale

Conclusion générale

Les travaux présentés dans ce mémoire ont porté sur l'étude d'un système de transmission sécurisée de données basée sur le système chaotique modifié, discret et d'ordre fractionnaire de Hénon.

Notre travail a été entamé par l'exploration du phénomène chaotique en le simulant par ordinateur. Nous avons ainsi vérifié la sensibilité des systèmes chaotiques même aux faibles variations des conditions initiales, dépisté la route vers le chaos d'un système dynamique en traçant son diagramme de bifurcation, identifié le chaos dans un système dynamique par le calcul de ses exposants de Lyapunov et représenté graphiquement le comportement de quelques systèmes chaotiques célèbres dans le domaine temporel et l'espace des phases.

La découverte en 1990 de Pecora et Carroll sur la synchronisation du chaos a été un déclic, pour la possibilité de l'utiliser dans la sécurisation de la communication. D'où vient l'objectif de la deuxième phase de notre travail. Nous avons cité les méthodes utilisées pour la synchronisation de ces systèmes chaotiques, qui est une étape indispensable pour la transmission de données. Par la suite les notions de cryptage et de décryptage ont été introduites avec un bref passage sur la cryptanalyse.

La troisième phase de notre travail a été consacrée à des notions de base relatives au calcul fractionnaire. L'utilisation des systèmes fractionnaires dans notre cas a pour but l'accroissement de la sécurité de la transmission et cela en augmentant le nombre de clés de sécurité.

La quatrième et dernière phase de notre mémoire a porté sur l'étude complète du système chaotique « Henon modifié », le choix du système est justifié par la simplicité et l'efficacité de son fonctionnement ainsi que par l'apport important dont il contribue en matière de sécurité, en effet la modification des conditions du régime transitoire permet de générer le comportement chaotique. La synchronisation de l'émetteur avec le récepteur est faite à l'aide d'un observateur retardé étape par étape, cette dernière à été bien accomplie et a engendré une erreur de synchronisation nulle, puis l'information est cryptée en utilisant la méthode de cryptage par inclusion, qui consiste à injecter le message dans la dynamique de notre système.

La robustesse du système est renforcée avec l'augmentation des clés de sécurité. Ces nouvelles clés sont obtenues grâce à l'utilisation de la dérivée d'ordre fractionnaire. Enfin, nous avons finalisé notre tâche par des résultats de simulations illustrant les performances du système de transmission proposé en matière de sécurité, de synchronisation et de reconstitution du message envoyé.

En perspectives, notre travail peut être complété par :

- L'étude de la robustesse du système de transmission conçu vis-à-vis des bruits de canal de transmission, et aussi par l'étude de la robustesse vis-à-vis des variations des paramètres de l'émetteur (Hénon-modifié fractionnaire).
- La réalisation expérimentale du schéma de transmission proposé à l'aide de circuits programmables (par exemple une carte Arduino).

Annexe

Annexe

1. Systèmes dynamiques

Un système dynamique peut être représenté par un ensemble de variables, qui évoluent au cours du temps. Ces variables peuvent être destinées pour l'étude des fluctuations d'état d'un phénomène ou d'un objet quelconque.
Un système dynamique en temps continu peut être modélisé mathématiquement par un système d'équations différentielles, alors qu'en temps discret on parle d'un système d'équations aux différences finies.
Dans ces représentations mathématiques interviennent des paramètres qui vont conditionner l'évolution de ce système, ainsi il peut avoir un comportement périodique, pseudopériodique ou chaotique [1].

- **En temps continu [2]**

$$\dot{x} = f(t, x, u)$$
$$y = h(t, x, u)$$

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

- **En temps discret**

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

$$x(k+1) = G\big(k, x(k), u(k)\big)$$
$$y(k) = h(k, x(k), u(k))$$

Où G : $\mathbb{R}^n \rightarrow \mathbb{R}^n \times \mathbb{Z}^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système en temps discret.
En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k :

$$x(k+1) = G\big(x(k), u(k)\big)$$
$$y(k) = h(x(k), u(k))$$

Dans ce qui suit, nous allons donner uniquement quelques notions sur les systèmes continus. Pour le cas discret, les définitions restent les mêmes.

2. Déterminisme

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un événement passé ou présent.
Un système déterministe est un système dont l'état présent est complètement déterminé par les conditions initiales, en contradiction avec un système stochastique pour le quel l'état présent reflète les conditions initiales avec en plus d'une réalisation particulière d'un paramètre aléatoire (bruit et variable interne).

3. Système autonome

Un système dynamique non linéaire est dit autonome lorsqu'il ne dépend pas explicitement du temps. Un système autonome est donné ci-dessous :

$$\begin{cases} \dot{x} = f(x, y) \\ \dot{y} = g(x, y) \end{cases}$$

Un système autonome est indépendant du temps initial, alors qu'un système non autonome ne l'est pas. Dans un système autonome, tout instant peut être considéré comme instant initial, et tout état $x(t)$ du système peut être considéré comme un état initial.

4. Non Linéarité

La non-linéarité renvoie d'une manière générale à une rupture de la proportionnalité des causes et des conséquences.
Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

5. Espace des phases, variables d'état et portrait de phases

De manière simplifiée, l'espace des phases permet de traduire des séries de nombre en une représentation spatiale, de dégager l'essentiel de l'information d'un système en mouvement et de dresser la carte routière de toutes ses possibilités. L'espace des phases est un espace mathématique souvent multidimensionnel. Chaque axe de coordonnées de cet espace correspond à une variable d'état du système dynamique étudié et chaque variable d'état caractérise le système à un instant donné. Pour chaque instant donné, le système est donc caractérisé par un point de cet espace. A l'instant suivant, il sera caractérisé par un autre point et ainsi de suite. Si l'espace des phases est représenté en trois dimensions, cette suite de points peut montrer graphiquement l'évolution du système dans le temps. L'ensemble des

trajectoires possibles constitue le portrait de phases. Celui-ci peut aider à percevoir l'attracteur du système.

6. Système linéaire

Un système linéaire peut être donné par l'expression suivante :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ \dot{y}(t) = Cx(t) + Du(t) \end{cases}$$

$x(t)$: est un vecteur colonne de variable d'états de dimension n (n est la dimension de l'espace d'état).
$y(t)$: est un vecteur colonne de sortie du système de dimension p.
$u(t)$: est un vecteur colonne de dimension m.
$A, B, C\ et\ D$: Sont des matrices constantes de dimensions respectives nxn, nxm, pxn et pxm appelées respectivement matrices d'évolution (d'état), de commande (d'entrée), d'observation (de sortie) et de transmission directe de la commande vers la sortie (de découplage).

7. Système non linéaire

Un système physique est dit non linéaire, si la relation entre les grandeurs d'entrées et les grandeurs de sorties est un système d'équations différentielles avec des coefficients non constants.

$$\dot{x}(t) = f(x(t), u(t))$$
$$\dot{y}(t) = f(x(t), u(t))$$

Avec :
$\dot{x}(t)$: Équation d'état.
$\dot{y}(t)$: Équation de sortie.
$x(t), u(t), y(t)$ Représentent respectivement le vecteur d'état, le vecteur d'entrée et le vecteur de sortie à l'instant t, f est la fonction vectorielle de dimension n.

8. Point d'équilibre

On appelle point d'équilibre du système, le point x^* tel que :

$$f(x^*) = 0\ \ et\ g(x^*) = 0$$

Remarque
Par un changement de variables $\xi = x - x^*$ on peut ramener le point x^* à l'origine.

9. Cycle limite

Les cycles limites sont des phénomènes non linéaires, ce sont des trajectoires fermées isolées. Tout système non linéaire qui a un siège d'oscillations est dit cycle limite, ils sont caractérisés par leurs amplitudes et leurs fréquences indépendantes de la condition initiale, et par le fait d'être sans excitation extérieure.

10. Tore

Cas particulier du cycle limite, le système présente aux moins deux période simultanés dont le rapport est irrationnel (aléatoire), la trajectoire de phase ne s'annule pas sur elle-même.

11. Bassin d'attraction

Le bassin d'attraction est l'ensemble des points de l'espace des phases qui sont sous l'effet de l'attracteur. C'est à dire que toutes les trajectoires qui commencent à ces points tendent vers l'attracteur après un temps fini.

Bibliographie

Bibliographie

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

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

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

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

[5] D. Ruelle « Hasard et Chaos » Odile Jacob, 1970.

[6] J.Y.Chen, K.W.Wong, L.M.Cheng «A secure communication scheme based on the phase synchronization chaotic systems» Physics Reports, 2002: 1-101.

[7] N. Corron, D. Hahs «A new approch to communication using chaotic signals» IEEE Transactions on Circuit and Systems, vol 44, pp. 373–382, 1997.

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

[9] Y. Liu. «Discrete Chaos in Fractional Henon Maps ». International Journal of Nonlinear Science, Vol. 18, pp. 170-175, 2014.

[10] K.B.Oldham, J.Spanier « The fractional calculus : Theory and application of differenciation and integration to arbitrary order ». Academic Press, Inc, 1974.

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

[12] H.Poincaré « Les méthodes nouvelles de la mécanique céleste » Paris: Gauthier-Villars, 1892 (t.1), 1893(t.2), 1899 (t.3)

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

[14] J. Lu, X. Yu, G. Chen « Generating chaotic attractors with multiple merged basins of attraction: A switching piecewise-linear control approach » IEEE Transactions on

Circuits and Systems -I: Fundamental Theory and Application, volume 50, N°2, pp.198-207, 2003.

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

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

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

[18] H.Delfs, H.Knebl. « Introduction to cryptography ». Edition Springer, 2002.

[19] O. Megherbi «Etude et réalisation d'un système sécurisé à base de systèmes chaotiques » Mémoire de magister, Université Mouloud Mammeri Tizi Ouzou, Algérie, 2013.

[20] A.J.Michaels « Digital chaotic communication » Thèse de doctorat, Georgia Institute of Technology, 2009.

[21] H.Zhang « Chaos synchronization and its application to secure communication » Thèse de doctorat, Université de Waterloo, Canada, 2010.

[22] T. Hamaizia «Application à l'optimisation a l'aide d'algorithme chaotique » Thèses de doctorat, Université de Constantine, Algérie, 2013.

[23] J.L.Chabert, A.D.Dalmendico. « Chaos et déterminisme : Les idées nouvelles de Poincaré ». Seuil. Paris, 1992.

[24] A. Kerchoff « La cryptographie militaire, Journal des sciences militaires » pp. 5–83, 1883.

[25] A.Pacha, N. Hadj-Saidi, A. M'hamed, A. Bbelghoraf «Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi» Univéristé d'Oran, Algérie, 2008.

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

[27] E. Ott, T. Sauer and J. A. Yorke «Coping with chaos : Analysis of chaotic data and exploitation of chaotic systems» Wiley-Interscience, NY, 1994.

[28] L.M.Pecora, T.L.Caroll « Synchronization in chaotic systems » Physical Review Letters, February, volume 64, N°8, pp. 821-825, 1990.

[29] L.M.Pecora, T.L.Caroll « Synchronizing nonautonomous chaotic circuits » IEEE Transactions on circuits and systems II: Analog and Digital Signal Processing, volume 40, N°10, pp. 646-650, 1993.

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

[31] A.Zemmouche « Sur l'observation de l'état des systèmes dynamiques non linéaires » Thèse de doctorat, Université de Strasbourg, France, 2007.

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

[33] R.Mainieri, J .Rehacek « Projective synchronzation in three-dimensional chaotic » Physical Review Letters, volume 82, N015, pp. 3042-3045, 1999.

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

[35] K.S.Miller, B.Ross « An introduction to the fractional calculus and fractional differential equations ». Wiley Iterscience Publication, 1993.

[36] J.P. Barbot, I. Belmouhoub and L.Boutat-Baddas, « Observability Bifurcations Applicationto Cryptography, In Chaos in Automatic Control» Taylor and Francis, 2005.

[37] M.L'Hernault « Faisabilité d'un système d'Emission-Réception Analogique pour la Communication Sécurisée pas le Chaos, Thèse de doctorat, Université Pierre et Marie Curie, Paris, France, 2007.

[38] J.Sabatier, O.Cois, A.Oustaloup. « Commande des systèmes non entiers par placement de pôles ». Conférence Internationale Francophone d'Automatique. Nantes, France, 2002.

[39] B.Vinagre, V.Feliu « Modeling and control of dynamic systems using fractional calculus: Application to electrochemical processes and flexible structures ».IEEE Conference on Decision and Control. Las Vegas, UDSA, 2002.

[40] K.S.Miller, B.Ross « An introduction to the fractional calculus and fractional differential equations ». Wiley Iterscience Publication, 1993.

[41] A.Oustaloup . « La dérivation non entière ». Edition Hermès, Paris, France, 1995.

[42] A.Si Ammour « Contribution à la commande par modes glissants d'ordre fractionnaire » Thèse de doctorat, Université Mouloud Mammeri Tizi Ouzou, Algérie,2011.

Sites web

[43] www.scholarpedia.org/article/Hyperchaos
(Systèmes hyperchaotiques) consulté le 06 septembre 2015.

[44] http://www.mathworks.com/matlabcentral/fileexchange/233-let?s_tid=srchtitle

(Logiciel « Lyapunov Exponents Toolbox ») consulté le 06 septembre 2015.