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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

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

Mémoire de
MASTER PROFESSIONNEL
Domaine : Sciences et technologies
Filière : Génie électrique
Spécialité : Electronique Industrielle

Présenté par :

M^elle Assia BERKANE

Thème

Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotiques discrets

Mémoire soutenu publiquement le : 27/09/2016 devant le jury composé de :

M. Y. Attaf Périsedent.
M. Djerire Examinateur
M. Hamid HAMICHE Encadreur
Melle Ouerdia MEGHERBI Co- Encadreur

Promotion : 2016

Remerciement

Nous 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 prés de lui au laboratoire L2CSP.

Nous tenons particulièrement à exprimer notre profonde gratitude à Mlle Ouerdia Megherbi, 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'évoluer notre travail.

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

Dédicace

Je dédie ce travail à ma famille qui m'a soutenu durant toutes mes années d'études en m'incitant toujours à aller de l'avant, ainsi qu'à tous mes amis.

Assia

Sommaire

LISTE DES FIGURES

LISTE DES FIGURES

Introduction générale :

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateurs et nature d'information à transmettre. Actuellement, tout système de communication performant nécessite un système de sécurisation afin de le protéger vis à vis des attaques possibles. Pour cela, de nouvelles méthodes de cryptage sont développées. Le cryptage des informations est maintenant utilisé pour interdire l'accès ou la modification des informations sensibles et garantir la confidentialité dans les communications. Certaines de ces nouvelles méthodes utilisent le chaos dans les systèmes de transmission.

Le chaos est caractérisé par un certain nombre de caractéristiques telles la sensibilité aux conditions initiales et l'imprévisibilité, ce qui rend les systèmes chaotiques très intéressants dans le cryptage des données [1].

Introduite en 1990 par Pecora et Carroll [1], la synchronisation est une technique qui, étant donné deux systèmes chaotiques, consiste à forcer la trajectoire d'un système à suivre celle de l'autre système. Plusieurs méthodes de synchronisation ont été proposées dans la littérature scientifique, elles se basent sur le principe du maître-esclave et permettent de réduire l'erreur entre les trajectoires de l'émetteur et du récepteur [1].

La cryptographie est une science qui s'intéresse à la protection des messages à transmettre, et ce en le rendant incompréhensible. La cryptographie a évolué grâce au conflit qui a toujours opposé deux camps, l'un cherche à dissimuler une information et l'autre essaie par tous les moyens de trouver ce que on lui cache [1], à chaque fois que le premier trouve le moyen de chiffrer ses messages, le second essaie par tous les moyens de trouver l'astuce qui va lui permettre de décrypter l'information. Autrefois pour dissimuler une information, on mélangeait, permutait ou décalait des lettres, d'autres remplaçaient les mots par des nombres dans le bute de rendre la lecture du message impossible [1]. La cryptographie n'a pas cessé d'évoluer. Actuellement, on chiffre le message clair d'une façon mathématique et algorithmique, plus l'inversion de la transformation est difficile plus la sécurité est élevée, et vice- versa [1].

Dans ce travail, nous proposons de concevoir et de réaliser un système de transmission sécurisé de données basé sur le cryptage par le chaos. L'intérêt de l'utilisation de chaos réside d'une part, dans le fait de la possibilité d'exploiter les propriétés des systèmes chaotiques dans le cryptage (sensibilité aux conditions initiales,…), et d'autre part sur la possibilité de la synchronisation par observateur impulsif.

Le cryptage se fera en noyant le message utile dans le signal chaotique émis par l'émetteur, la récupération du message se fera par une fonction mathématique de décryptage du signal chaotique clair.

Ce travail comporte quatre chapitres.

- Le chapitre I est consacré aux généralités et aux notions de base sur les systèmes chaotiques.
- Le chapitre II traitera des généralités sur la synchronisation des systèmes chaotiques, ainsi que le principe de transmission à base du chaos. .
- Le chapitre III expose l'étude du schéma de transmission proposé.
- Le chapitre IV présente les résultats de simulations.

Enfin, on termine par une conclusion générale et des perspectives .

Chapitre I

I.1 Introduction

La théorie du chaos fait partie des sciences les plus récentes est devenue l'un des domaines les plus avancés dans la recherche contemporaine. Les origines de cette nouvelle théorie s'étendent aux mathématique et physique des débuts du $20^{ème}$ siècle, mais elle a émergé dans les années 1960-1970 [1].

Durant des années, le chaos était considéré comme incontrôlable et même inutilisable, malgré la mise en équation de certains phénomènes et la démonstration du déterminisme dans des aspects d'apparence aléatoire [1].

La théorie du chaos est définie comme une étude des systèmes dynamiques non-linéaires complexes et les systèmes complexes qui sont exprimés par des récurrences et des algorithmes mathématiques et qui sont dynamiques (non constants) et non périodique. Elle inclut l'étude qualitative et quantitative d'un comportement instable non périodique et aléatoire des systèmes dynamiques non linéaires déterministes. Le chaos peut être vu aussi comme un système avec des propriétés stochastiques. Dans toutes les définitions qui peuvent exister pour le chaos, un phénomène fondamental est indispensable. La sensibilité aux conditions initiales [1].

En effet, en programmant son ordinateur et en changeant par 10^{-4} les conditions initiales des prévisions météo, Edward Lorenz a découvert que pour certaines équations ou système d'équations non linéaires les résultats montrent une grande sensibilité aux conditions initiales. On peut dire que cette anecdote est la base du chaos déterministe [1] [2].

La théorie du chaos influence l'explication de plusieurs phénomènes et trouve son application dans plusieurs domaines tels que :

- Economie : Prévision des cycles économiques, des mouvements commerciaux et des marchés financiers.
- Météo : Prévisions météo logiques.
- Santé : prévisions des crises d'épilepsie.
- Sciences sociales : Comportement des systèmes sociaux.
- Cryptage de l'information.

I.2 Historique de la théorie du chaos

La signification scientifique du chaos n'a était citée qu'à la fin du XIX^{e} siècle par Henri Poincaré (1854-1912), car depuis les travaux d'Isaac Newton (1642-1727), la science était dominée par le déterminisme. Moyennant la connaissance des conditions initiales d'un système donné, les scientifiques pensaient pouvoir prédire complètement et précisément le futur du système en question. Un siècle après Newton, pierre-Simon Laplace (1749-1827) définit le sens absolu du déterminisme, il affirmait que l'état présent de l'univers permettait en principe de prédire complètement son futur. Mais Poincaré allait donner tort à Laplace, il avait en effet montré que, malgré un caractère déterministe, le problème des trois corps en mécanique céleste (exemple Terre-lune-soleil) ne pouvait pas donner lieu à la prédiction [2].

On a ainsi pu tester la stabilité de ce système en comparant les trajectoires suivies par un des corps à partir de deux positions initiales très proches : ces trajectoires restent proches l'une de l'autre à court terme et on peut donc prédire les éclipses, mais elles deviennent complètement différentes à long terme, une toute petite différence initiale a donc produit un effet considérable. C'est dans cette extrême sensibilité aux conditions initiales que réside l'origine de l'imprédictibilité du chaos déterministe. Poincaré avait remarqué cet effet puisqu'il a écrit : « Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir et alors nous disons que cet effet est du au hasard » [2].

L'idée que les petites causes peuvent avoir quelquefois de grands effets a été notée par les historiens et autres depuis longtemps, par exemple dans la fameuse expression " pour manque d'un clou un royaume a été perdu ".en 1860 James Maxwell a discuté comment les collisions entre molécules dures de la sphère pourraient mener à l'amplification progressive du rendement aléatoire microscopique dans les gaz [1].

En 1898 Jacques Hadamard a noté la divergence générale de trajectoires dans l'espace, et Pierre Duhem a discuté la signification générale possible de ceci en 1908, il a donné le résultat qu'on ne peut jamais atteindre une prédiction complète du système chaotique, et cela à cause des conditions initiales aléatoires nécessairement présentes dans le théorème de Hadamard [2].

En 1961, Edward Lorenz, météorologue et professeur de mathématiques au MIT (Massachussetts Institut of Technology) observa par hasard le phénomène qui s'appellera plus tard la théorie de chaos déterministe, à la suite de calculs visant à prévoir les phénomènes

météorologiques. Ces prévisions nécessitaient un grand nombre de calculs d'équations différentielles complexes à très grand nombre de variables impossible à faire à la main, il a utilisé alors un ordinateur, son Royal Mcbee LGP-300 qui est entré dans l'histoire de la théorie du chaos, et qui a fait de Lorenz le père officiel de cette théorie puisque les calculs des systèmes chaotiques régissant ces phénomènes étaient difficiles à comprendre et à simuler sans ordinateur. Après plusieurs heures de calculs, Lorenz avait obtenu une série de résultats et a décidé de repasser une deuxième fois ces données dans l'ordinateur pour s'assurer du résultat. Pour gagner du temps, il avait entré les variables avec trois chiffres après la virgule au lieu de six, il pensait qu'une faible variation dans les variables à la base d'un calcul aurait une incidence du même ordre de grandeur sur le résultat final, mais à sa grande surprise les résultats étaient totalement différents de la première série. Il venait de découvrir le comportement chaotique d'un système non linéaire : soit, d'infimes différences dans les conditions initiales d'un système déterministe entraineraient des résultats complètement différents. Pour mieux comprendre l'importance de cette sensibilité aux conditions initiales Lorenz a eu recours à une métaphore qui contribua au succès médiatique de la théorie du chaos : «le simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas » [2].

En 1971, le physicien belge David Ruelle et le mathématicien Floris Takens ont également publié un article dans lequel ils avaient analysé les états finaux des modèles mathématiques de systèmes qui dissipent une partie de leur énergie en chaleur. Les résultats ont montré que l'ensemble des états finaux d'un tel système a une nature fractale : C'est un attracteur étrange. Le mouvement sur un tel attracteur dépend énormément des conditions initiales ; c'est la propriété appelée effet papillon par Lorenz. En appelant bifurcation le point ou une faible variation d'un paramètre induit un changement qualitatif de la solution d'une équation, Ruelle et Takins ont montré qu'un tout petit nombre de bifurcations suffit à produire un comportement chaotique et donc à engendrer la turbulence. Quatre ans plus tard, l'étude expérimentale d'un fluide en rotation par les physiciens Jerry Gollub et Harry Swinnay, du City Collège de New York, montrait que l'apparition de la turbulence suit bien dans ce cas la description de Ruelle et Takens mais le mot Chaos n'a pas encore était utilisé ; il était introduit par le mathématicien Yorke en 1975 et la théorie du chaos déterministe sera alors appliqué à l'étude de phénomènes dans dive [2].

I.3 Définition des systèmes dynamiques

Un système dynamique est un système physique qui évolue. Il peut évoluer dans le temps ou par rapport à une autre variable suivant l'espace de phase considéré.

La trajectoire d'un objet en mouvement dans le temps est donc un système dynamique, ainsi que le nombre d'individu d'une population quelconque dans le temps, encore les valeurs d'une fonction par rapport a une variable x [2].

On a deux types des systèmes dynamiques (discret ou continu) [2].

I.3.1 Notions des systèmes dynamiques

Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non-linéaire. Du point de vue mathématique, la notion générale de système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état. Ces variables ont la propriété de caractériser complètement l'état instantané du système dynamique. En associant en plus le système de coordonnées, on obtient l'espace d'état qui est appelé également l'espace des phases. Conjointement avec l'espace d'état, un système dynamique est défini aussi par une loi d'évolution, généralement désignée par la dynamique, qui caractérise l'évolution de l'état du système dans le temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique [3] [4].

a. Systèmes dynamiques linéaires

Un système physique est dit linéaire si la relation entre les grandeurs d'entrée et de sortie peut être définie par des équations différentielles linéaires (à coefficients constants).Ces deniers vérifient alors les principes de proportionnalité des effets aux causes, et de superposition [3].

b. Système dynamique non linéaire

Un système non linéaire est un système qui n'est pas linéaire, c'est-à-dire (au sens physique) qui ne peut pas être décrit par des équations différentielles linéaires à coefficients constants. Cette définition, ou plutôt cette non-définition explique la complexité et la diversité des systèmes non linéaires et des méthodes qui ne sont pas une théorie générale pour ces systèmes, mais plusieurs méthodes adaptées à certaines classes de systèmes non linéaires [3].

I.3.2 Définition du chaos

Bien qu'il n'existe pas une définition du chaos adoptée de façon universelle dans la littérature, on pourrait dire que c'est un phénomène qui peut apparaitre dans les systèmes dynamiques déterministes non linéaires caractérisés 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 [4].

I.3.3 Classes des systèmes chaotiques

Il existe plusieurs systèmes chaotiques qui sont utilisés pour générer les signaux chaotiques. Dans ce paragraphe, nous présenterons deux classes : Les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

I.3.4 systèmes chaotiques continus

Un système chaotique à temps continu est décrit par un système d'équation différentielle de forme [3] :

$$\acute{x} = f(t, x, u), y = h(t, x, u). \tag{1}$$

où : $x\ est$ le vecteur d'état de dimension n, f : $R^n \rightarrow R^n$ est une fonction non linéaire désignant le champ de vecteur, h : $R^n \rightarrow R$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq \Re^p$ représente l'entrée du système. Si ce système ne dépend pas de l'entrée, on aura alors.

$$x = f(t, x) \tag{2}$$

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer les systèmes de Lorenz, Rössler, Bogdanov, le circuit de Chua, etc.

a. Système de Lorenz

Le système de Lorenz est généré par le système d'équations suivant :[9]

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \tag{3}$$

Cet exemple a été publié en 1963 dans un journal météorologique.

Les variables x, y et z représentent les états du système à chaque instant. a, b, c sont les paramètres du systèmes. Le système présente un comportement chaotique pour a=12, b=26, c=9 et présente un attracteur étrange en forme d'ailes de papillon [4].

b. Système de Rössler

Le système de Rössler est donné par les équations suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \quad (4)$$

x, y, et z sont les variables d'états du système .a, b, c sont les paramètres réels .Les paramètres et les conditions initiales de cette équation ont été choisis de la manière suivants : a=b=0.1, c=12 $(x_0, y_0, z_0)=(0.01,0.01,0.01)$

L'ensemble des trajectoires de ce système définissent un attracteur étrange aux propriétés fractales sur le long terme [4].

I.3.5 Systèmes chaotiques discrets

Un système chaotique à temps discret est décrit par un système d'équations aux différences finies, dont le modèle général est le suivant :

$$x(k+1) = G\big(x(k), u(k)\big)\,,\ y(k) = h(x(k), u(k)). \quad (5)$$

La dynamique du système en temps discret. Parmi les systèmes chaotiques discrets, nous pouvons citer les systèmes de Hénon, Hénon modifié, Lozi, la fonction logistique, etc.… [4]

a. Système de Hénon :

Introduit par l'astronome Michel Hénon en 1976, il est présenté par des équations le suivant [4] :

$$\begin{cases} x(k+1) = y(k) + 1 - a * x(k)^2 \\ y(k+1) = b * x(k) \end{cases} \quad (6)$$

Tel que $(x(k),y(k)) \epsilon R^2$ Représente le vecteur d'état.

Pour les valeurs a=1.4 et b=0.3le système présente un comportement chaotique

Les conditions initiales prises sont $x_0=0.1$, $y_0=0$

Pour d'autres valeurs de a et b, il peut être chaotique, intermittent ou converger vers une orbite périodique [4].

b. Système Hénon-Heiles ou Hénon modifié

Il est donné par les équations suivantes :

$$\begin{cases} x(k+1) = a - y^2(k) - bz(k) \\ Y(k+1) = x(k) \\ Z(k+1) = y(k) \end{cases} \quad (7)$$

Pour avoir un comportement chaotique, les paramètres du système sont donnés comme suit :

a=1.76 et b=0.1 et les conditions initiales du système : $x_0= 0.1$, $y_0= 0.1$, $z_0 =0.1$ [4].

I.4 Propriétés de systèmes chaotiques

Bien qu'il n'y ait pas de définition mathématique du chaos universellement acceptée, une définition couramment utilisée stipule que pour qu'un système dynamique soit classifié en tant que chaotique, il doit comporter les propriétés suivantes [4].

- Aspect aléatoire
- Sensibilité aux conditions initiales
- Notion d'attracteur
- Exposants de Lyapunov
- Fonction d'auto corrélation et spectre de puissance
- Bifurcation

I.4.1 Aspect aléatoire

Les systèmes chaotiques se comportent, en effet d'une manière qui peut sembler aléatoire. Cet aspect aléatoire du chaos vient du fait que l'on est incapable de donner une description mathématique du mouvement, mais ce comportement est en fait décrit par des équations non

linéaires parfaitement déterministes, comme par exemple les équations de Newton régissant l'évolution d'au moins trois corps en interaction. Les figures ci-dessus illustrent les aspects aléatoires du système chaotique continu (4) et discrets (6) [4].

a. Aspect aléatoire du système de Rössler

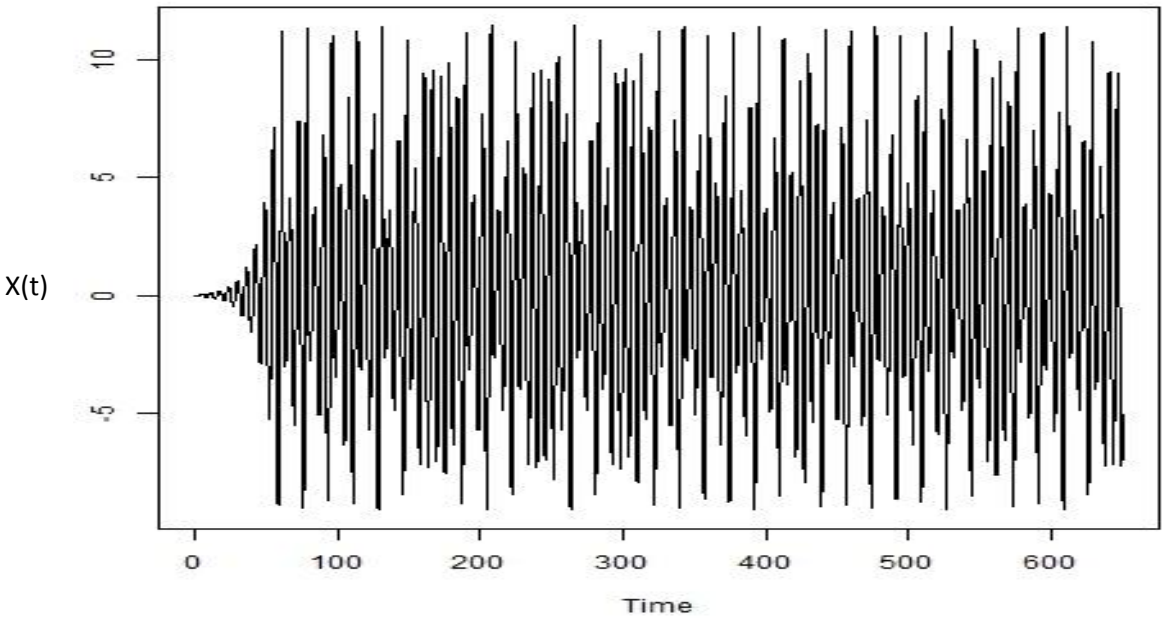


Figure (1) : *Aspect aléatoire du système de Rössler.*

b. Aspect aléatoire du système de Hénon :

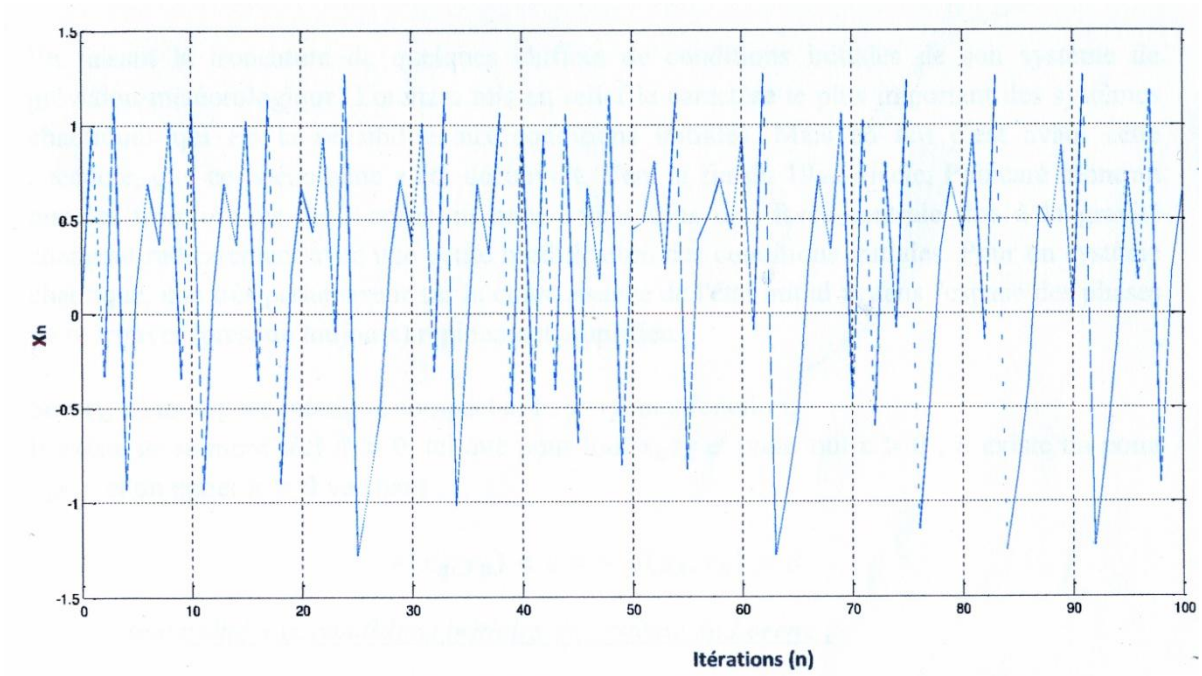


Figure (2) : *Aspect aléatoire du système de Hénon*

I.4.2 Sensibilité aux conditions initiales

En faisant la troncature de quelques chiffres sur les conditions initiales de son système de prévision météorologique, Lorenz a mis en relief le caractère le plus important des systèmes chaotiques qui est la sensibilité à la condition initiale. Mais en fait c'est avant cette anecdote, que ce phénomène a été découvert. Vers la fin du 19^{éme} siècle, Poincaré montrait que les trois orbites de 3 corps en mouvement sous une force centrale due à la gravité changent radicalement avec une petite modification des conditions initiales. Pour un système chaotique, une très petite erreur sur la connaissance de l'état initial x, dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée [5].

- **Stabilité aux conditions initiales du système de Lorenz :**

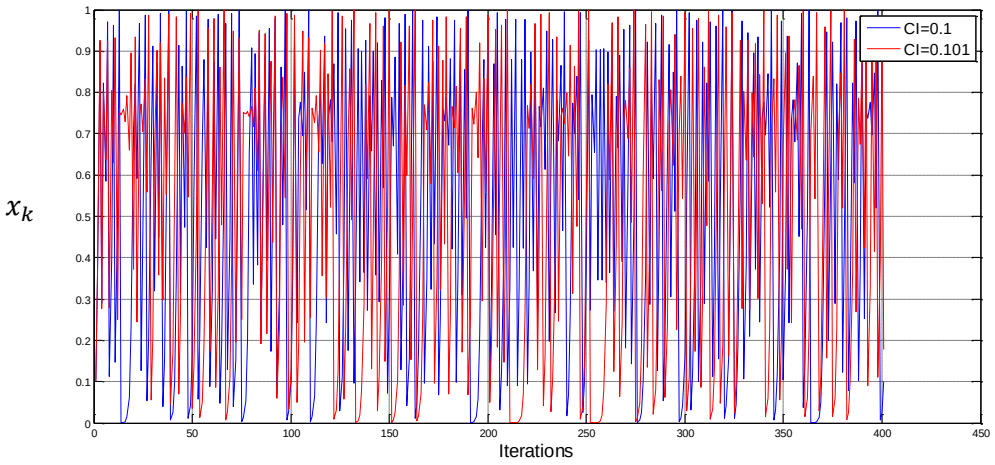


Figure (3) : *Sensibilité aux conditions initiales (Système de Lorenz)*

Remarque :

On a le cas initial :

$$\begin{cases} x_1(0) = 0.100 \\ x_2(0) = 0.101 \end{cases}$$

En prenant $x_1(0) et\, x_2(0)$ pour conditions initiales très proches, les évolutions des signaux $x_1\ etx_2$ Sant comportement différent au fur et à mesure que le temps augmente, on a obtenu les résultats suivants, figure (3).

I.4.3 Notion d'attracteur

Avant d'expliquer la notion d'attracteur, il faudrait d'abord définir ce qu'est l'espace des phases. Les trajectoires dynamiques des systèmes chaotiques sont fréquemment situées dans un espace appelé espace de phase. Les régions de l'espace sans l'existence permanente des dynamiques chaotiques seront inutiles puisque les points dans ces zones tendent vers l'infini et ne contribuent pas à la continuité du processus chaotique. Les variables qui construisent cet espace doivent contenir toute information sur la dynamique du système [5].

On peut maintenant définir un attracteur comme étant une limite asymptotique des solutions de toute condition initiale localisée dans un domaine de volume non nul ou bassin d'attraction [6].

Les trajectoires complexes dans l'espace de phase qui attirent les solutions du système chaotique sont alors des attracteurs. L'ensemble de points attirés vers l'attracteur constitue le bassin d'attraction. Autrement dit, l'attracteur est une géométrique de l'espace de phase (formant une structure feuilletée) indiquant le comportement d'un système chaotique. L'attracteur peut être étrange avec structure fractale (une courbe ou surface de forme irrégulière ou morcelée qui se crée en suivant des règles déterministes ou stochastiques impliquant une transformation ponctuelle de type homothétie interne) ou point fixe ou encore cycle limite. Parmi les premiers exemples des attracteurs étranges mentionnés dans l'histoire du chaos, on cite l'attracteur de Lorenz. Ci-dessous, nous donnerons des exemples d'attracteurs étranges pour les différents systèmes chaotiques continus où discrets [5].

a. Attracteur de Lorenz

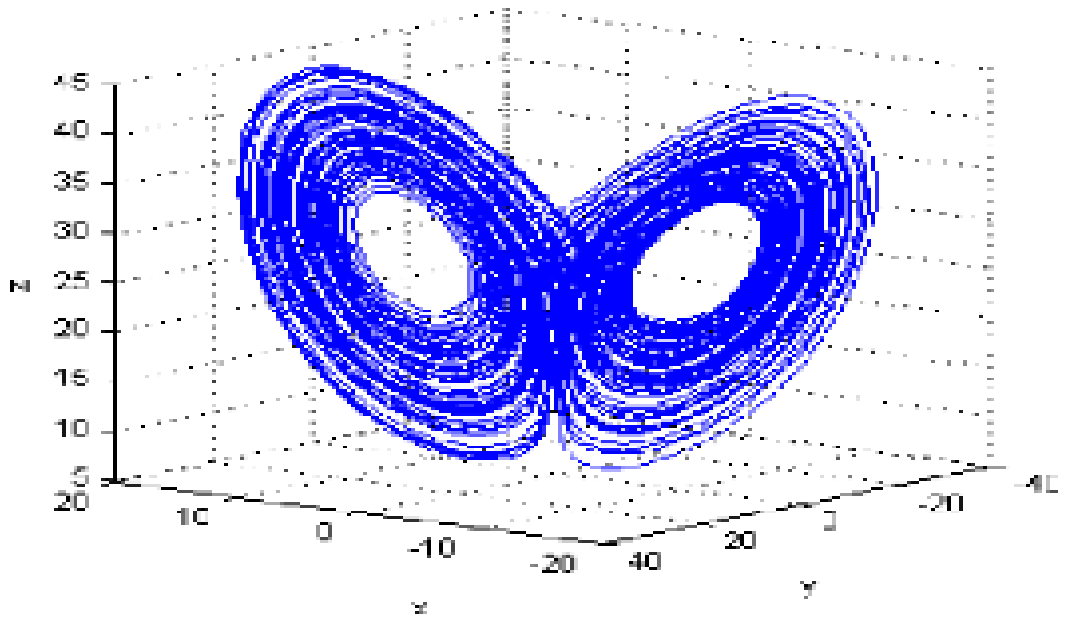
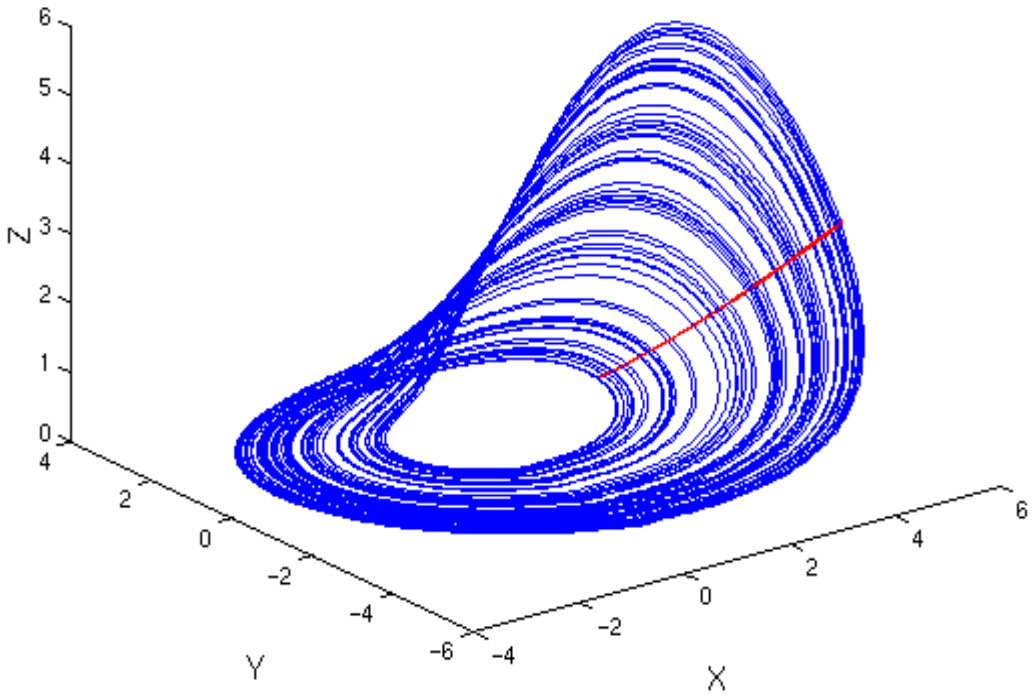


Figure (4) *: Attracteur de Lorenz*

b. Attracteur de Rössler



Figure(5) : *Attracteur de Rössler*

c. Attracteur de Hénon

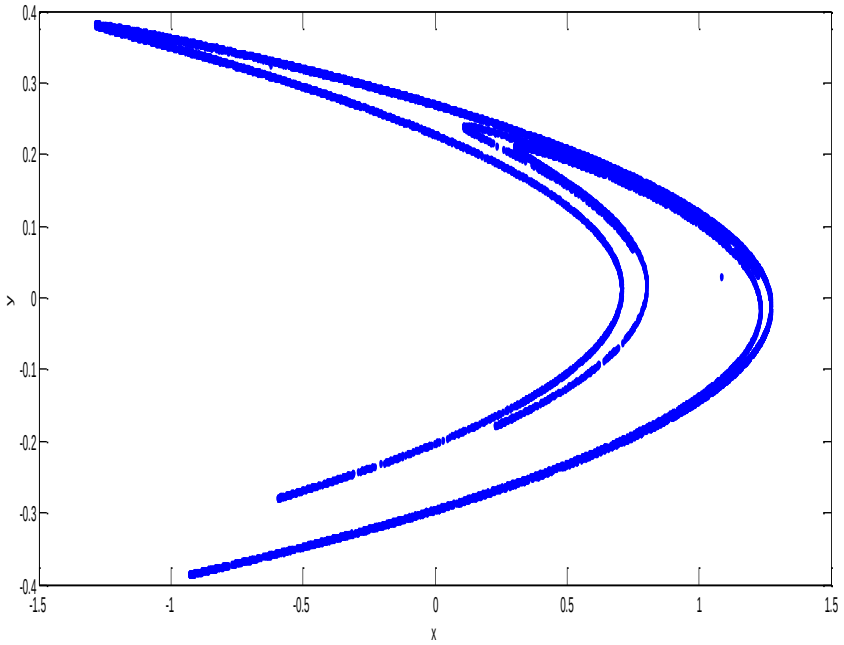


Figure (6): *Attracteur de Hénon*

d. Attracteur de Hénon-Heile

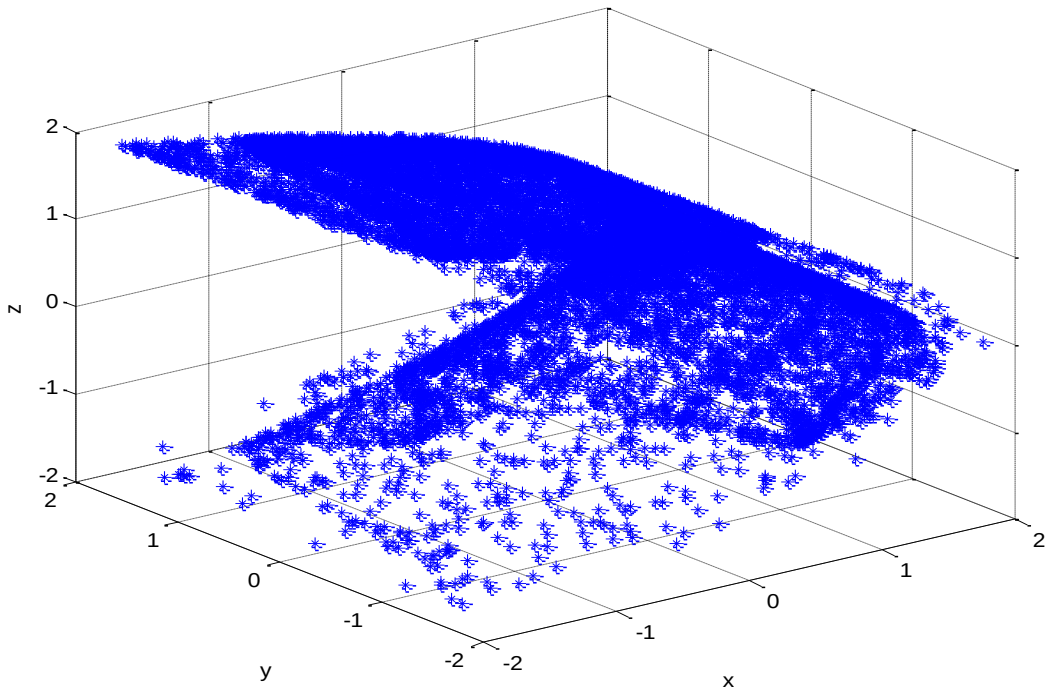


Figure (7) : *Attracteur de Hénon-Heiles*

I.4.4 Exposants de Lyapunov

Les exposants de Lyapunov permettent de caractériser le chaos temporel et plus particulièrement la sensibilité aux conditions initiales que présente un attracteur étrange. Autrement dit, nous allons exposer comment calculer le taux de divergence entre l'évolution des trajectoires issues de conditions initiales proches au sein de cet espace borné qu'est l'attracteur étrange [6].

a. Exposant pour une application unidimensionnelle

Considérons un système dynamique discret faisant intervenir une application f et deux conditions initiales très proches, x_0 et $x_0 + \varepsilon_0$

La première itération conduit à : $x_1 + \varepsilon_1 = f(x_0) + \left(\frac{df(x_0)}{dx}\right)\varepsilon_0$ (8)

D'où l'on déduit : $\varepsilon_1 = \left(\frac{df(x_0)}{dx}\right)\varepsilon_0$ (9)

Après n itérations, il vient :

$$\boldsymbol{\varepsilon_n = \frac{df^n(x_0)}{d_x}\varepsilon_0 = \left(\prod_{i=0}^{n-1}\frac{df(x_i)}{dx}\right)\varepsilon_0} \quad (10)$$

Les termes $\left(\frac{df^n(x_0)}{d_x}\varepsilon_0\right)^{1/2}$ caractérisent la divergence. On définit alors l'exposant de Lyapunov par :

$$\lambda(x_0) = \lim_{n\to\infty}\frac{1}{n}ln\left|\frac{df^n(x_0)}{dx}\right| = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}ln|f'(x_i)| \quad (11)$$

Un exposant positif indique que la divergence entre deux trajectoires voisines augmente exponentiellement avec un temps.

Il est possible d'étendre cette définition à une dimension plus élevée d'espace des phases. Pour un espace de dimension *p*, il ya *p* exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes du système. Ils sont définis partir de la matrice Jacobienne de l'application *f* au point x_0 et de ses valeurs propres [6].

b. Exposant pour une application multidimensionnelle

Il s'agit de généraliser les concepts du paragraphe précédent à des trajectoires multidimensionnelles de type f :$R^m \to R^m$:$x_{i+1=}$f (x_t).

Il faut savoir qu'un système m-dimensionnel possède m exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes du système, de sorte qu'en moyenne un hyper- volume initial V_0 évolue selon une loi de type suivant [7] :

$$V = V_0 e^{(\lambda 1+\lambda 2+.....+\lambda m)\, t} \tag{12}$$

Il est nécessaire qu'au moins un des λ_i soit positif, pour avoir étirement et donc sensibilité aux conditions initiales selon au moins un axe. Mais il faut également que la somme des λ_i soit négative, En effet, dans le cas contraire, le volume initiale finirait par remplir tout l'espace dans lequel il est immergé. On n'aurait alors plus un attracteur de faible dimension, et donc plus affaire à du chaos déterministe [7].

Pour pouvoir définir et calculer λ_i, considérons une hyper-sphère dans l'espace m-dimensionnel de rayon ε (petit) de conditions initiales et examinons son évolution. On s'intéresse à : On pose $x'_0 = x_0 + \varepsilon$ et on opère un développement en série limité d'ordre 1 de $f'(x_0)$ au voisinage de x'_0 [7].

$$x_t \quad x'_t = \frac{df^t(x_0)}{d_x}(x_0 \quad x'_0) = J^t(x_0)(x_0 \quad x'_0) \qquad \text{(J.Malek)} \tag{14}$$

où $J^t(x_0)$ dénote la matrice Jacobienne de $f^t(x_0)$ au point x_0, il s'agit d'une matrice m x m. Si elle est diagonalisable, alors il existe une matrice inversible P_t telle que :

$$D^t{}_m = P_t^{-1} J^t P_t \tag{15}$$

D'où $D^t{}_m$ est une matrice diagonale contenant les valeurs propres de J^t. Dénotons celles-ci par : $\Lambda^t{}_i, i = 1,.....,m$. On définit alors les m exposants de Lyapunov de la manière suivante :

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} In[\Lambda_i^t] \qquad (i=1 \ldots m)$$

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

Etat stable	Flor	Dimension de Lyapunov	Exposants de Lyapunov λ_i
Point d'équilibre	Point	0	$\lambda_n \leq \ldots\ldots \leq \lambda_1 \leq 0$
Périodique	Cercle	1	$\lambda_1=0$ $\lambda_n \leq \ldots\ldots \leq \lambda_2 \leq 0$
Périodique d'ordre 2	Tore	2	$\lambda_1=\lambda_2=0$ $\lambda_n \leq \ldots\ldots \leq \lambda_3 \leq 0$
Périodique d'ordre K	K-tores	K	$\lambda_1=\ldots=\lambda_k=0$ $\lambda_n \leq \ldots\ldots \leq \lambda_{k+1} \leq 0$
Chaotique	Attracteur Chaotique	Non entier	$\lambda_1>0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyperchaotique	Attracteur Hyperchaotique	Non entier	$\lambda_1>0$ $\lambda_2>0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tableau 1: *Attracteurs et exposants de Lyapunov.*

Le logiciel LET (Lyapunov exposent Toolbox) (12) nous a permis de calculer les exposants de Lyapunov sans passer par les méthodes de calculs mathématiques relativement longues que nous venons de citer.

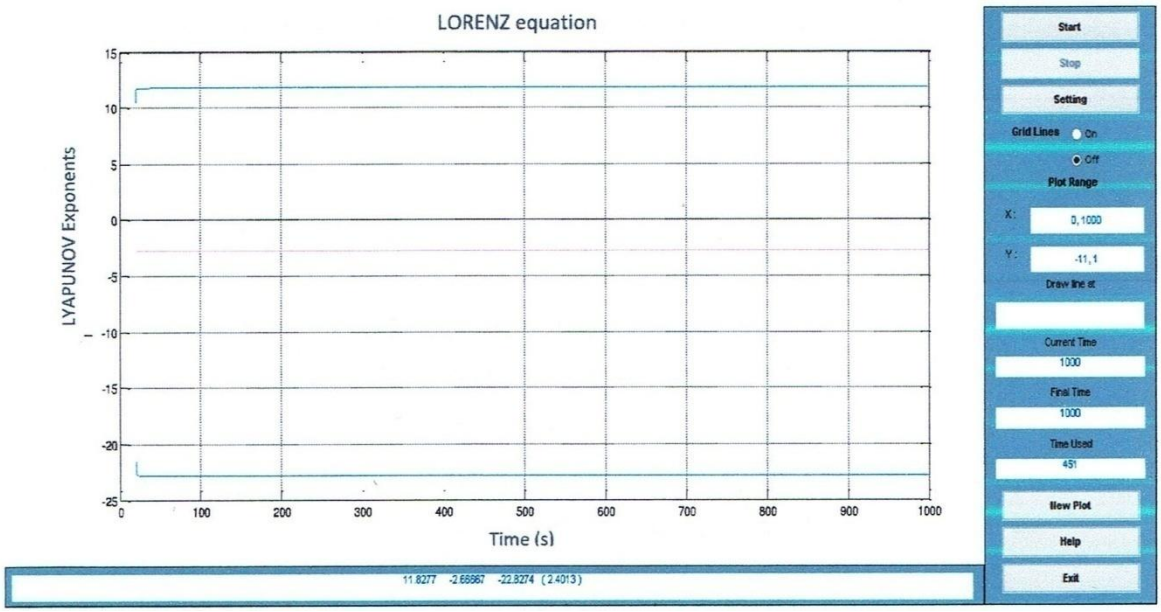


Figure (8) : *Exposants de Lyapunov (système de Lorenz)*

D'après la figure (8), nous avons 3 exposants de Lyapunov dont un positif :

λ_1=11.8277

λ_2=-2.66667

λ_3=-22.8274

et $\lambda_1+\lambda_2+\lambda_3$=-13.66637.

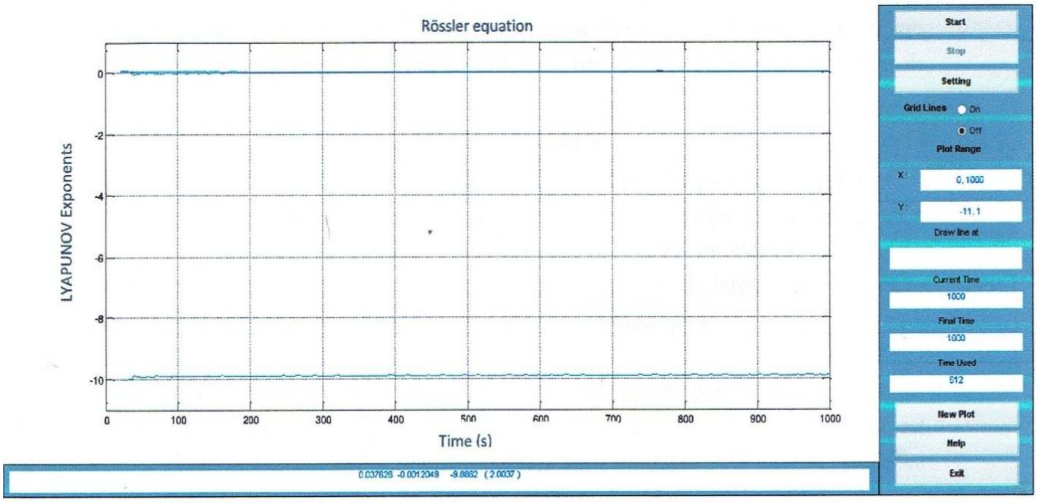


Figure (9) : *Exposants de Lyapunov (système de Rössler)*

D'après la figure (9), nous avons 3 exposants de Lyapunov dont un positif

λ_1=0.037626

λ_2=-0.0012049

λ_3=-9.8862

et $\lambda_1+\lambda_2+\lambda_3$=-9.8497789

I.4.5 Fonction d'autocorrélation et spectre de puissance

Le spectre de puissance (ou densité spectrale d'énergie) d'un signal f(t) est fonction :

$$v \to |TF[f](v)|^2$$

Tf : transformée de Fourrier

$|TF[f](v)|^2$ Mesure le « poids » de la fréquence v dans la décomposition du signal $f(t)$ en superposition de signaux élémentaires $\left(e^{i2\pi vt}\right)$

Dans le cas d'un système dynamique, le signal f peut être une variable X^i (t) de l'espace de phase. Un signal périodique ou quasi périodique (signe d'un attracteur en cycle ou tore limite) sera caractérisé par des pics isolés dans le spectre de puissance (pics correspondant à la fréquence fondamentale et aux différentes fréquences de battement présentes dans le signal)[8].

Un système chaotique présentera des signaux avec des oscillations irrégulières. Ce qui caractérise les oscillations chaotiques sera la présence de bandes larges « continues » dans le spectre. Le système peut « passer continument » d'une fréquence à l'autre dans la bande. Elles caractérisent donc une certaine perte d'information sur l'état initial due à la sensibilité aux conditions initiales. Il faudra néanmoins différencier cela d'un fond continu (bande continue qui s'étend sur tout ou presque tout le spectre) qui caractérise plutôt un bruit blanc, c'est-à-dire des fluctuations totalement aléatoires caractérisant une perte totale d'information à très court terme. De manière équivalente, on pourrait étudier la TF inverse du spectre de puissance comme suit [8].

$$TF^{-1}\left[|TF[f]|^2\right](t) = \int_{-\infty}^{+\infty} \overline{f(t-\tau)f(\tau)}d\tau = R_f(t) \tag{17}$$

$R_f(t)$: Fonction d'autocorrélation de f. On rappelle que la fonction d'autocorrélation $R_f(t)$ en t, mesure la ressemblance du signal f avec lui-même décalé dans le temps d'une valeur de t. pour un signal quasi périodique (signe d'un attracteur en tore limite), on s'attend donc à une fonction d'autocorrélation présentant des oscillations régulières avec de larges ventres centrés sur les différentes périodes présentes dans le signal et leurs harmoniques [8].

Pour un signal chaotique, on s'attend à une fonction d'autocorrélation présentant de fins petits pics (en sinus cardinal) formant une figure d'oscillations irrégulières. Cette autocorrélation est caractéristique de la propriété de mélange topologie (on a des petits pics d'Autocorrélation est caractéristique de la propriété de étrange qui est ergodique si le système passe par un point, il repassera dans le voisinage de celui-ci, mais de manière irrégulière et non périodique). Pour un bruit blanc, on s'attend à un unique pic extrême fin en 0 [8].

a. Autocorrélation pour le système de Lorenz

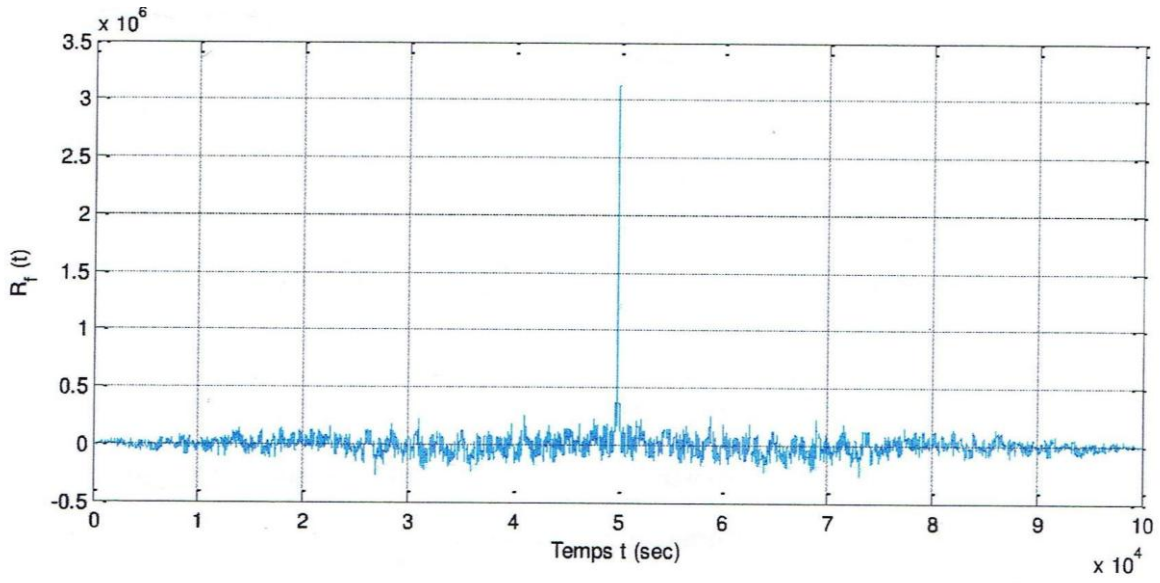


Figure (10) : *Autocorrélation d'un signal issu du système de Lorenz*

b. Autocorrélation pour le système de Rössler

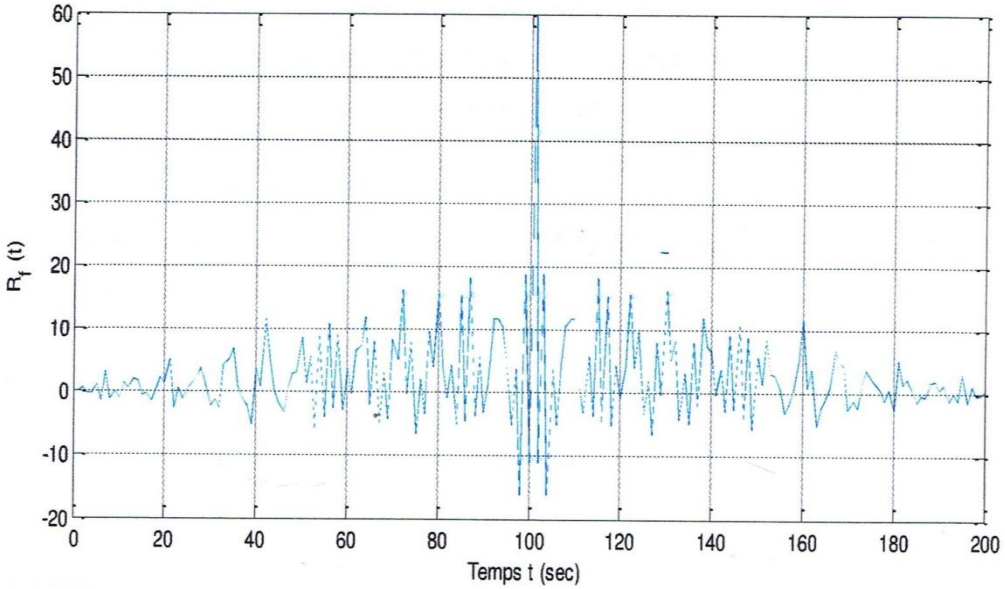


Figure (11) : *Autocorrélation d'un signal issu du système de Rössler*

c. Exemple d'Autocorrélation pour le système de Hénon

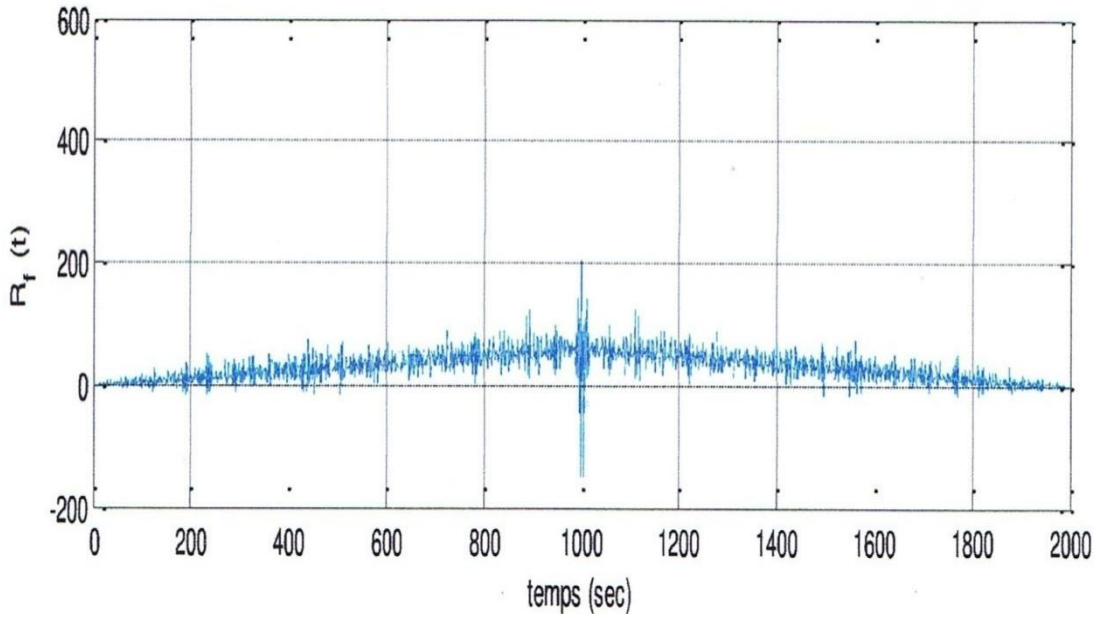


Figure (12) : *Autocorrélation d'un signal issu du système de Hénon*

La fonction d'auto corrélation a une portée finie, la similitude temporelle avec lui-même diminue et finit par disparaitre à des instants suffisamment futurs du signal, ce qui correspond à l'imprédicibilité et aussi à l'origine de l'écartement de deux trajectoires initialement voisines qui perdent toute similitude au bout d'un temps fini, ce qui correspond à la sensibilité aux conditions initiales des systèmes chaotiques[8].

Il est plus simple de représenter le spectre d'amplitude $|TF[f(v)]|$ plutôt que le spectre de puissance $|TF[f(v)]|^2$.

d. Aspecter d'amplitude du système de Lorenz

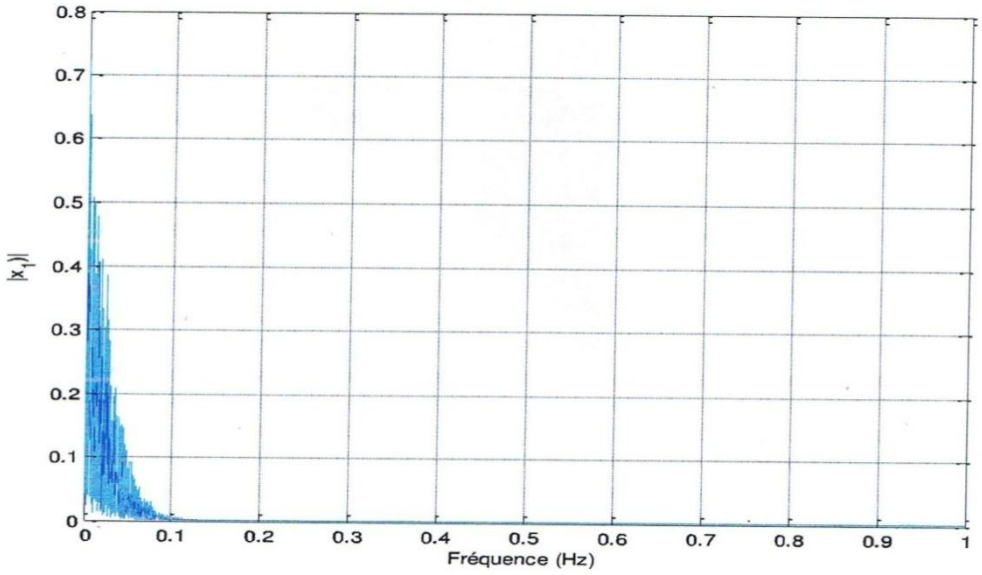


Figure (13) : *Spectre d'amplitude du système de Lorenz*

I.4.6 Bifurcation

Le passage d'un point fixe à un cycle limite de période -2, puis à un cycle limite de période -4, est un événement important dans la dynamique d'un système. On dit qu'il y a une bifurcation lorsqu'un tel changement qualitatif des solutions se produit à l'occasion de la variation d'un paramètre. Les graphiques qui représentent ces bifurcations, sont logiquement appelés diagrammes de bifurcation. Cette notion est centrale dans l'étude du chaos. Lorsque l'on examine de tels graphiques, il faut faire attention aux axes. Sur un axe nous prenons le paramètre, et sur l'autre la variable d'état, formant l'espace paramétrique [9].

Un diagramme de bifurcation délimite des zones de l'espace paramétrique dans lesquelles le comportement qualitatif du système est similaire. On voit apparaître aussi un enchainement très rapide de doublements de période qui mène à une situation chaotique. Ce mécanisme de doublements de période est une des routes vers le chaos. Un exemple de diagramme de bifurcation (système de Hénon modifié) est représenté sur la figure 14 [9].

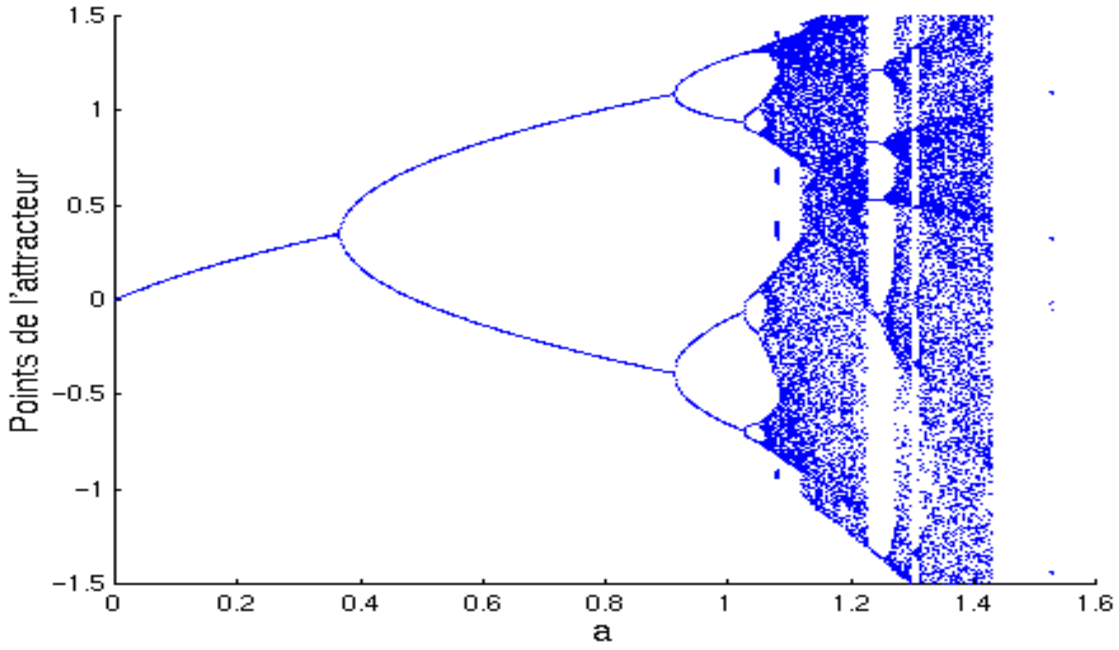


Figure (14) : *Diagramme de bifurcation pour le système de Hénon-Helies*

Dans notre exemple du Hénon modifié :

- Pour a croissant de 0 à 0.8 : le système a tendance à se stabiliser autour d'une seule valeur, il est attiré par un cycle limite de période -1.
- Pour 0.8<a<1.06 : le système finit par osciller entre 2 valeurs, on dit qu'il possède un cycle de période-2 (dédoublement de période).
- Pour 1.06<a<1.37 : la longueur du cycle augmente de plus de plus en plus rapidement.
- Pour 1.37<a<1.8 : la longueur du cycle s'allonge et devient tellement complexe que l'on peut difficilement suive son évolution, le système passe dans une phase chaotique.

Des bifurcations dans les phénomènes chaotiques peuvent engendrer une structure fractale. Les fractales et le chaos déterministe sont deux domaines mathématiques qui présentent beaucoup de points communs, bien que leurs caractéristiques soient différentes (imprévisibilité et sensibilité aux conditions initiales pour le chaos et autosimilarité et invariance d'échelle pour les fractales) [9] [8]. Ainsi de nombreux phénomènes chaotiques présentent des structures fractales (par exemple, dans leurs attracteurs étranges), même si beaucoup d'objets fractals ne sont nullement chaotiques (triangle de Sierpinsky, courbe de Koch…) [9].

I.5 Scénarios vers le chaos

Le chaos nait toujours d'une instabilité liée à la présence d'un paramètre de contrôle dans les équations d'évolution. Lorsque ce dernier prend une valeur particulière dite critique, le système subit une bifurcation ; il change brusquement de comportement dynamique.

Une succession de bifurcations peut alors conduire à un comportement chaotique.
Les différents processus qui conduisent au chaos sont :

La cascade sous harmonique ou dédoublement de période, l'intermittence ou transition de Pomeau-Mannevielle et la quasi-périodicité [10].

- **Cascade sous harmonique ou dédoublement de période : cf paragraphe sur la bifurcation**

Il existe un système simple qui illustre bien le mécanisme d'évolution vers le chaos par cascade sous harmonique. C'est l'oscillateur étudié dans les années 1980 par l'électronicien américain Léon Chua. Dans ce système, les grandeurs électroniques évoluent en étant alternativement croissantes puis décroissantes [10].

Dans la figure(15) nous avons représentés l'évolution d'une tension u prélevée dans le circuit pour différentes valeurs d'un paramètre de contrôle, en pratique une résistance r.

La réalisation expérimentale du circuit de Chua montre que la période des oscillations varie par doublements successif, lorsque r dépasse des paliers r_1, r_2, r_3, au fur et à mesure que l'on augmente r. La période qui vaut initialement T_0, devient$2T_{0,}4T_0$, etc : elle s'allonge indéfiniment. Le circuit devient apériodique, son évolution atteint un régime chaotique [10].

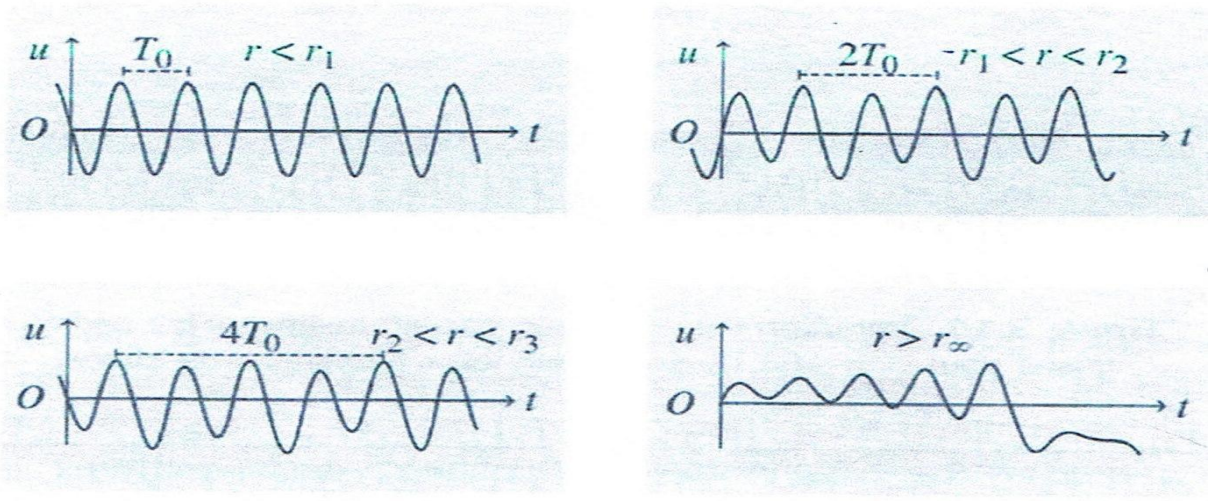


Figure (15) : *Cascade sous harmonique dans le montage de Chua*

- **Intermittence ou transition de Pomeau-Manneville**

Ce processus de transition d'un régime périodique à un régime chaotique par intermittence a été découvert par les physiciens Français Yves Pomeau et Paut Manneveille en 1980.

Dans leur publication, ces auteurs reprennent les équations du modèle de Lorenz de la convention, mais utilisent le paramètre r qu'ils font varier autour de la valeur critique r_c=166.06. Le calcul par simulation de l'évolution de la variable z montre l'apparition du chaos par intermittence : Pour r=166, z a un comportement périodique, alors que si r est légèrement supérieur à r_c, ce comportement est interrompu par des « bouffées » irrégulières de courte durée, dont l'apparition semble aléatoire. Si *r* continue d'augmenter, ces perturbations sont de plus en plus fréquentes et plus longues, si bien qu'au final l'évolution de

Z apparaît complètement aléatoire et donc chaotique (figure 16) [11].

- **Quasi-périodicité**

Un système est Quasi-périodique s'il est constitué de deux oscillateurs, de périodes respectives T_1 et T_2 telles que leur rapport ne soit pas un nombre rationnel, le système semble présenter alors un mouvement périodique, mais il ne repasse jamais par le même état ; au mieux il se rapproche indéfiniment de ce dernier. La transition vers le chaos par Quasi-périodicité intervient quand un oscillateur interagit avec un système initialement périodique : Au fur et à mesure que le paramètre de contrôle (ou d'interaction) augmente, le système adopte un comportement Quasi-périodique jusqu'à devenir chaotique.

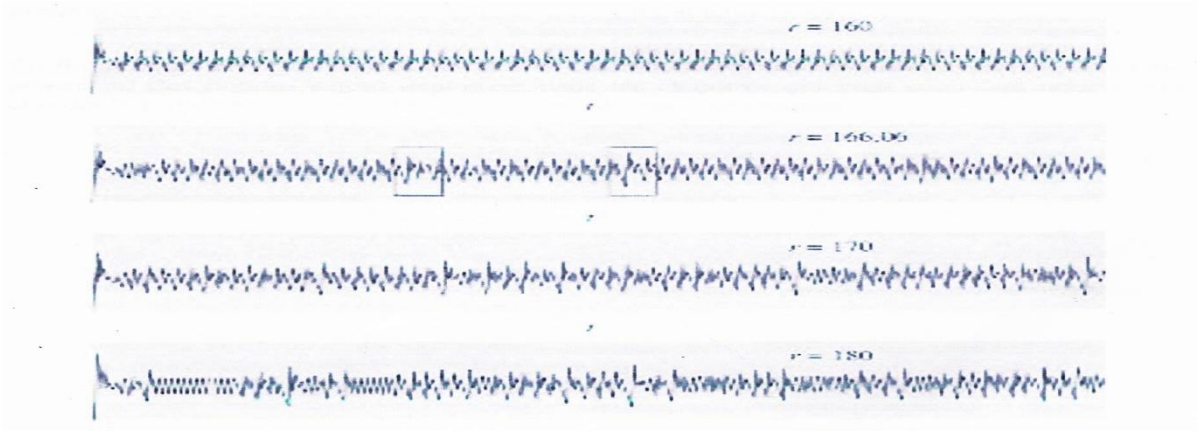


Figure (16) : Transition vers le chaos par intermittence ; les cadres grisés pour r=166..06 soulignent les (bouffées) de turbulence du chaos.

Conclusion

Dans ce chapitre, nous avons présenté quelques notions sur le chaos. La première partie est consacrée à la définition des systèmes dynamiques chaotiques linéaires et non linéaire. Toujours dans cette partie, nous avons défini les systèmes chaotiques continus et discrets avec leurs propriétés.

A la fin de ce chapitre, les scénarios de transition vers le chaos des systèmes dynamiques ont été présentés. Ces notions seront exploitées dans les chapitres qui suivent où nous allons aborder le problème de la synchronisation des systèmes chaotiques.

Chapitre II

II.1 Introduction

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maitrise de la synchronisation des systèmes chaotiques. Un signal chaotique se présente sous forme d'un bruit blanc dans les deux domaines temporel et fréquentiel. Ce qui différencie un signal chaotique d'un bruit aléatoire est la notion de déterminisme [11]. En effet, le bruit ne peut être décrit que comme un processus aléatoire alors qu'un système chaotique est représentable par des équations différentielles. Ainsi il est possible de synchroniser deux systèmes chaotiques. Pecora et Carroll ont été les premiers en 1989 [11] à synchroniser deux systèmes chaotiques L'utilisation des systèmes chaotiques dans la transmission sécurisée correspond à noyer le message codé dans un signal chaotique. A la réception l'opération inverse est effectuée à savoir l'extraction puis le décodage du message ainsi reçu [11].

II.2 Définition de la synchronisation

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système. D'une façon générale, la synchronisation peut être décrite de la manière suivante [11].

Considérons les deux systèmes suivants :

$$\dot{x} = f_1(x, u) \tag{1}$$

$$\dot{\hat{x}} = f_2(\hat{x}, u\ ) \tag{2}$$

Avec $\boldsymbol{x} \in \boldsymbol{R^n}, \hat{\boldsymbol{x}} \in \boldsymbol{R^n}$, dans lesquels $\boldsymbol{f_i} : \boldsymbol{R^n} \times \boldsymbol{R^n} \to \boldsymbol{R^n}$ **s**ont des champs de vecteurs non linéaires ,les deux systèmes sont dit synchronisés si :

$e = \left| \hat{x}(\mathrm{t}) - x(\mathrm{t}) \right| \to 0$ quand $\mathrm{t} \to \infty$

Où *e* représente l'erreur de synchronisation.

II.3 Méthodes de synchronisation

Les méthodes traditionnelles de synchronisation chaotiques sont en général basées sur l'utilisation de circuits identiques. Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante .Si, par un moyen quelconque, on leur permet d'échanger

de l'énergie, qui est l'action que l'on nomme « couplage », les deux systèmes finiront par céder la place à un comportement commun ; c'est la synchronisation [12].

On distingue deux types de synchronisation, classés selon le sens dont l'énergie est échangée entre les deux systèmes chaotique : La synchronisation par couplage unidirectionnel et la synchronisation par couplage bidirectionnel.

Nous allons présenter dans ce qui suit les deux modes de synchronisation ainsi que les différentes méthodes proposées par la communauté scientifique[13].

II.3.1 Synchronisation par couplage unidirectionnel

Lors d'une synchronisation par couplage unidirectionnel, l'énergie est transférée d'un système à l'autre entre deux systèmes identiques a et b à l'aide d'un élément de couplage fonctionnant dans un seul sens, comme un buffer [13].

La figure 17 illustre ce mode de synchronisation :

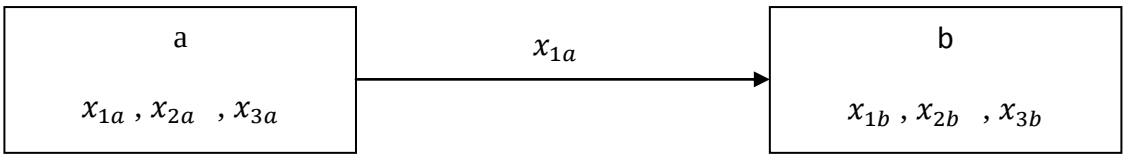


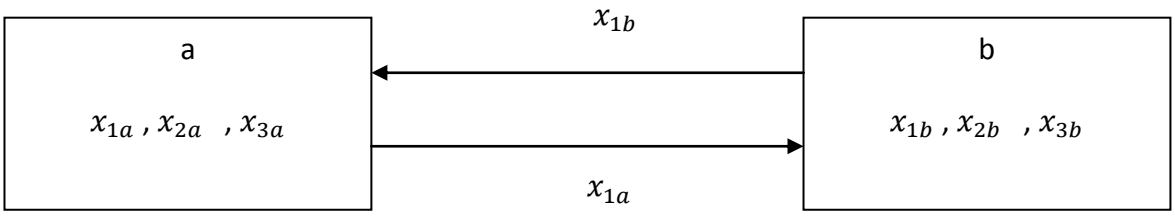
Figure (17) : *Schéma de couplage unidirectionnel.*

Où $(x_{1a}; x_{2a}, x_{3a}, x_{1b}, x_{2b}, x_{2b})$ sont les états des systèmes (couplage unidirectionnel)

II.3.2 Synchronisation par couplage bidirectionnel :

Lors d'une synchronisation par couplage bidirectionnel, l'élément de couplage permet l'échange de l'énergie dans les deux sens, ceci peut être par exemple une simple résistance [13].

La figure 18 illustre ce mode synchronisation



Figure(18): *Schéma de couplage bidirectionnel*

II.3.3 Synchronisation par décomposition du système (synchronisation identique)

La synchronisation identique proposée par Pecora et Carroll [13] a l'avantage de représenter une solution simple et performante de la synchronisation dont l'objectif est que l'esclave reproduit le plus fidèlement possible l'état du maître, après un régime transitoire.

Ce concept repose sur le constat qu'un système chaotique possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc impossible de construire une réplique identique à ce système et d'essayer de synchroniser. L'idée consiste à diviser le système d'origine en deux sous-systèmes de telle sorte que les variables dynamiques de départ soient réparties de part et d'autre de chacun des sous-systèmes [13], [14] .Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du système de départ (système maître) sert à piloter (synchroniser) le premier des deux sous-systèmes dupliques mis en cascade qui lui même permet de synchroniser le second sous-système dupliqué .Considérons un système dynamique autonome, en temps continu, de dimension « n » représenté par la relation suivante [13], [14], [15].

$$\dot{x} = f(u) \qquad (3)$$

U∈R^n

Avec U(t)= (U_1(t)……U_n(t)) et F(u)= (F_1(u),…..F_n (u)).

Ce système est divisé arbitrairement en deux sous-systèmes :

$\dot{x}$=G(x, y_1) et $\dot{y}$=H (x_1, y) (4)

Avec : x(t)= (u_1(t)…u_m(t))= (x_1(t)…x_m(t)).

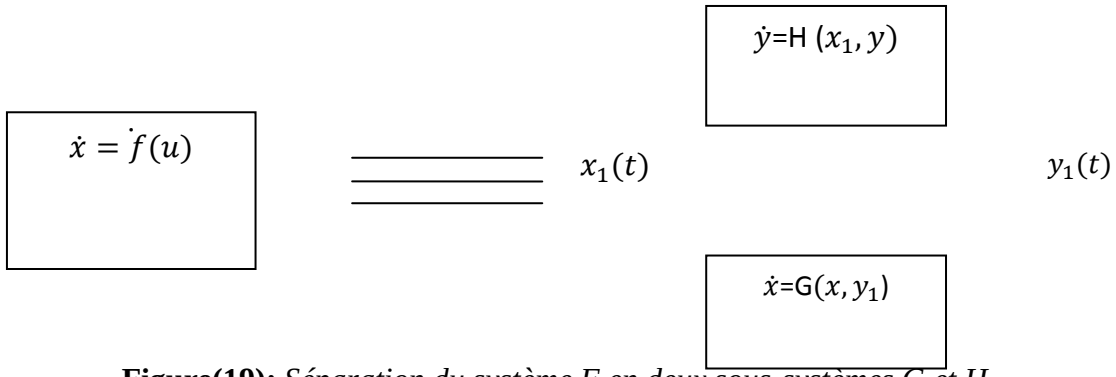
Y(t)= (u_{m+1} (t),…..u_n(t))= (y_1(t),….y_p(t))

Tel que : m + p =n

Soient :

$$\begin{cases} \dot{x}_1 = G_1(x, y_1) \\ . \\ . \\ .\dot{x}_m = G_m(x, y_1) \end{cases} \quad (5) \qquad \text{et} \qquad \begin{cases} \dot{y}_1 = H_1(x_1, y) \\ . \\ . \\ \dot{y}_p = H_p(x_1, y) \end{cases} \quad (6)$$

La figure 19 illustre plus en détails le processus de séparation ne deux sous-systèmes.



Figure(19)*:* *Séparation du système F en deux sous-systèmes G et H*

Le sous-système « G », dont les variables d'états sont décrites par le vecteur *x*, H dont les variables d'états x(t) et y_1(t) sont données par le vecteur *y*.

Ces deux sous-systèmes sont ensuite dupliqués et mis en cascade comme le montre la figure suivante figure 20 :

Soient « Ĝ » et « Ĥ » ces deux sous-systèmes.

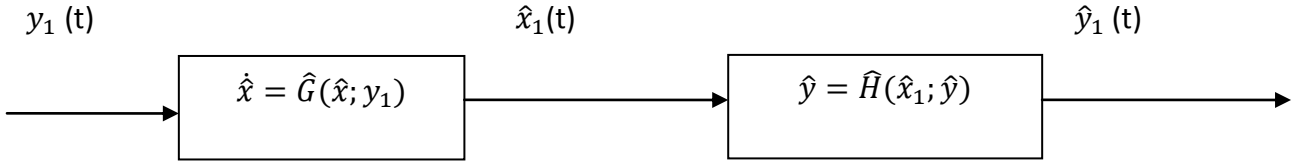


Figure. (20) *:* *Mise en cascade des deux sous-systèmes dupliqués*

L'objectif maintenant est de synchroniser le signal $\hat{y_1}$(t) avec le signale y_1(t) provenant du système d'origine comme le montre la figure (21).

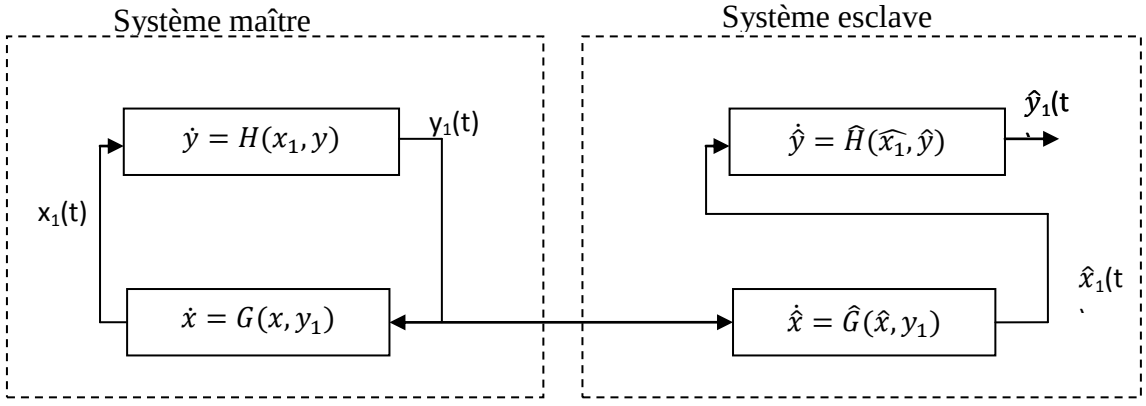


Figure (21) : *Principe de synchronisation par décomposition en sous-systèmes.*

Si l'ensemble des quatre sous-systèmes est considéré comme un système unique alors ce dernier peut être décrit par les équations d'états suivantes :

$$\begin{cases} \dot{x}=\mathrm{G}(x,y_1) \\ \dot{y}=\mathrm{H}(x_1,\ y) \\ \dot{\hat{x}}=\hat{\mathrm{G}}(\hat{x},\hat{y}_1) \\ \dot{\hat{y}}=\hat{\mathrm{H}}(\hat{x}_1,\hat{y}) \end{cases} \tag{7}$$

On parle alors de synchronisation par cascade.

La condition nécessaire pour obtenir la synchronisation est que tous les exposants conditionnels de Lyapunov (CLE) du sous-système « Ĝ » soient négatifs. Les « CLE » représentent les exposants de Lyaponov dans le cas d'un système non autonome. Dans notre cas, le sous-système « Ĝ » est piloté par le signal y_1(t). Les « CLE » caractérisent la stabilité du sous-système non autonome « Ĝ » et s'ils sont tous négatifs, les signaux $\hat{x}_1$(t) et x_1(t) se synchronisent et [15].

$$\lim_{t\to\infty}|\hat{x}_1(t)-x_1(t)|=0 \tag{8}$$

La condition exposée précédemment est une condition nécessaire et suffisante pour obtenir la stabilité locale. En effet, la synchronisation du sous-système Ĥ dépend aussi du choix des paramètres statiques (par exemple les valeurs des composants d'un circuit) et les conditions initiales des variables dynamiques du système maitre (x(t=0), y(t=0)) et du système esclave ($\hat{x}$ (t=0), $\hat{y}$ (t=0)). La difficulté réside dans les conditions initiales qui, dans la pratique, ne sont pas contrôlables [15], [16], [17].

II.3.4 Synchronisation complète

On considère un système maitre représenté par les équations suivantes [16] :

$$\begin{cases} x=\dot{f}(t,x) \\ Y=\mathrm{h(t)} \end{cases} \tag{9}$$

Où $x\in\mathbb{R}^n et$ h : $\mathbb{R}^n\longrightarrow\mathbb{R}^n$, x est le vecteur d'état et f est la fonction de sous –système.

Et un système esclave donné par :

$$\begin{cases} \hat{\dot{x}} = \hat{f}\ (t,\hat{x}\ ,\ y) \\ \hat{y} = \hat{h}(\hat{x}) \end{cases} \qquad (10)$$

Avec $\hat{x} \in \mathbb{R}^n et\ \hat{h} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$

Où $(\hat{x}, \hat{\dot{x}})$ sont les états des systèmes et (y; $\hat{y}$) sont les sorties.

Soit φ une fonction continue, qui décrit la relation entre le maître et l'esclave lors de la synchronisation

$\hat{y}=\varphi(y)$; $\varphi: \mathrm{R}^n \longrightarrow R^n$

La synchronisation est dite complète si :

$$\hat{x}(t) = x(t)$$

Ce qui implique que ; m = q etφ est une identitè [17].

Si$\hat{f} = f$, la relation devient une synchronisation complète identique.

Si $\hat{f} \neq f$ c'est une synchronisation complète non identique.

La synchronisation complète est donc une coïncidence complète entre les variables d'état des deux systèmes synchronisés .Les méthodes de synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques.

La majorité des concepts de synchronisation complète utilise un schéma de rétroaction et la synchronisation considérée comme étant bidirectionnelles, car les deux systèmes sont à la fois source et destination [17].

II.5 Synchronisation généralisée

La synchronisation généralisée est considérée comme une généralisation de la synchronisation complète pour synchroniser des systèmes chaotiques de modèles différents. Elle se manifeste par une relation fonctionnelle entre deux systèmes chaotiques couplés [18].

II.6 Synchronisation par contre-réaction (couplage diffusif)

Les recherches qui ont suivi celles de Pecora et Carroll ont montré que la synchronisation par remplacement complet n'était qu'un cas très particulier de la méthode que nous allons maintenant présenter dans ce paragraphe [18].

En général, on garde les mêmes notions pour le système chaotique étudié mais sans le diviser en sous-systèmes .Pour que la synchronisation ait lieu, on prend au moins un des signaux x_{ri} et on ajoute un facteur amortissant qui a pour valeurs différentes x_{ci}-x_{ri} au système de réponse On a alors [18] :

$$\dot{x}_c = \text{f}(x_c) \text{ et } \dot{x}_r = \text{f}(x_r) + \text{C e}(x_c - x_r) \tag{11}$$

Où « C » est le facteur de couplage et e est une fonction linéaire qui définit la combinaison linéaire des signaux qui seront utilisés pour l'amortissement. Similairement, on pose : $\varepsilon = x_r - x_c$

$$\text{Ou : } \dot{\varepsilon} = f(x_c) - f(x_r) - \text{C}e(x_c - x_r) \approx (j_f - C.e)\varepsilon \tag{12}$$

Pour avoir la stabilité asymptotique, on calcule les exposant de Lyapunov correspondants à l'équation vibrationnelle (j_f -C.e) en fonction de C et on choisit ce facteur de manière à avoir les exposants négatifs. Si le facteur de couplage positif tend vers l'infini alors on se retrouve dans le cas de la synchronisation par remplacement complet car la matrice « e » remplacera dans le f tout les « x_{ri} » par « x_{ci} » cependant, les exposants de Lyapunov des signaux utilisés ne seront pas forcément négatifs dans le cas limite.

La figure 22 montre le principe de cette méthode

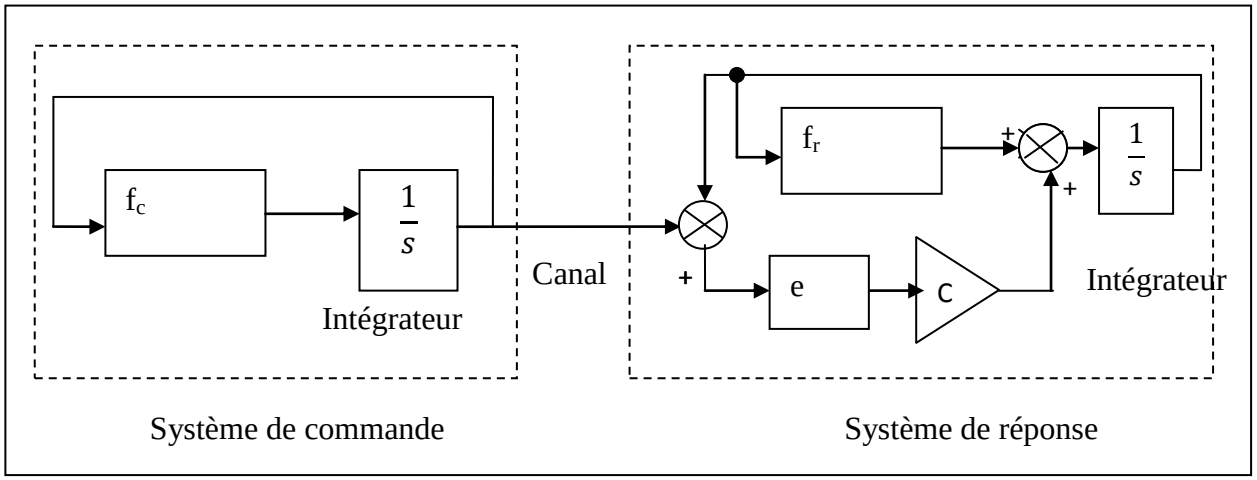


Figure (22) : *Synchronisation par contre-réaction*

Remarque : Le montage de synchronisation est unidirectionnel (composé d'un système maître qui commande un système esclave).On peut aussi réaliser des montages de synchronisation bidirectionnels à couplage en ajoutant $c`* \dot{e}(x_r\text{-}x_c)$ à l'équation différentielle du système f_c dans ce cas, le résultat est similaire mais il dépendra de deux variables [19].

Si on a $\dot{c}$= c et $\dot{e}$= e, alors les exposants de Lyapunov sont les mêmes que ceux du couplage unidirectionnel mais avec un facteur 2C [19].

II.7. Synchronisation impulsive

Dans un schéma de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation au niveau du récepteur. On propose la synchronisation impulsive et dans le but de réduire la redondance du signal transmis. La figure 23 illustre le principe de cette méthode [20].

Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système changent soudainement.

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

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

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquels un signal y(t)=C_x(t) est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état. [17].

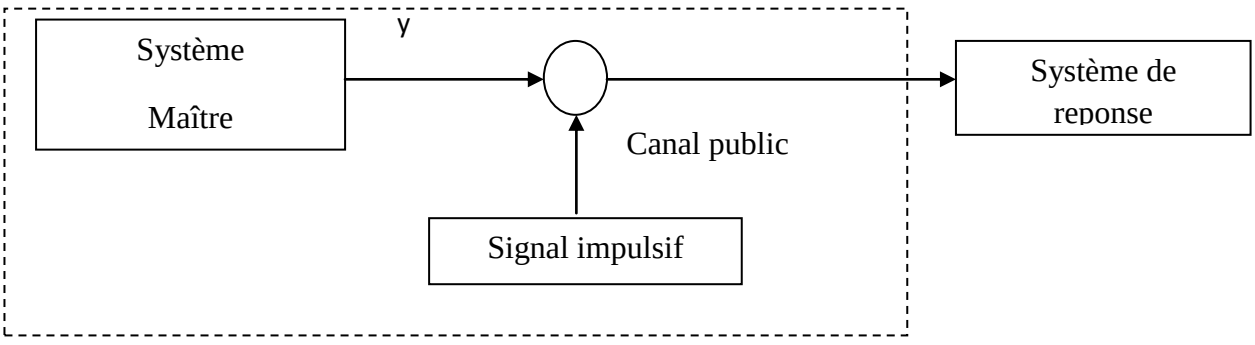


Figure (23) : *Synchronisation impulsive*

II.9 La synchronisation anticipée

Comme dans le cas de la synchronisation Lag, la relation entre les variables d'état des systèmes maitre et esclave est donnée par [20] :

$$\hat{x}(t) \approx x(t+\tau), \tau > 0 \tag{13}$$

II.10. La synchronisation de phase

Soient φ_1 et φ_2 les phases des systèmes, maitre et esclave respectivement. La synchronisation de phase est réalisée si pour deux nombres entiers m et n il existe un nombre positif très petit ε tel que [21] :

$$\left| m_{\varphi 1} \text{-} n_{\varphi 2} \right| < \varepsilon \tag{14}$$

Le phénomène de synchronisation de phase est totalement différent de ceux présentés précédemment .Généralement, lorsque la synchronisation chaotique est obtenue, les exposants de Lyapunov du système esclave sont tous négatifs. Cependant, dans le cas de la synchronisation de phase, les exposants de Lyapunov peuvent prendre des valeurs positives [21].

II.11 La synchronisation retardée

Dans cette synchronisation l'état du système esclave tend vers l'état décalé dans le temps du système maitre c'est-à-dire [22] :

$$\lim_{t\to\infty} \| \hat{x}_1(t) - x(t-\tau) \| = 0$$

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

$\hat{x}$ (t) est l'état du système récepteur et τ est un retard positif [22].

II.12 Synchronisation projective

Dans cette méthode, l'état du système réponse se synchronise avec un multiple de l'état du système maître se traduit par la relation suivante [21], [22].

$$\lim_{t\to\infty} \| \hat{x}(t) - ax(t-\tau) \| \tag{15}$$

Où « a » est le facteur d'échelle, $x(t)$ est l'état du système maître, et $\hat{x}(t)$ est l'état du système esclave et τ est un retard positif. Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur de très faible valeur.

II.13 Transmission basée sur la synchronisation des systèmes chaotiques

Dans cette partie du chapitre, on s'intéresse aux techniques de transmission sécurisée d'informations qui reposent sur le principe de synchronisation chaotique. Le point commun constaté dans la majorité des techniques développées dans la littérature est l'utilisation de la configuration maître-esclave pour laquelle on dispose d'un émetteur chaotique (système maître) qui génère un signal porteur du message transmis dans le canal de communication vers un système récepteur (système esclave) qui a pour objectif de se synchroniser avec le système maître dans l'objectif de restaurer le signal d'information[23],[24.]

Les signaux chaotiques peuvent être utilisés pour la transmission de l'information principalement dans deux objectifs : Le premier objectif est de protéger l'information transmise et dans ce cas, les applications réalisées sont en compétition avec les méthodes de cryptographie classiques. Un deuxième objectif est d'étaler le signal informationnel avec tous les avantages des techniques à étalement de spectre. Dans ce deuxième cas, les méthodes développées doivent être comparées aux systèmes classiques à étalement de spectre [24].

Si on regarde du point de vue de la structure d'un tel système de transmission, on peut définir deux approches. La première, représentée dans la figure 24 remplace le signal porteur sinusoïdal par un modulateur chaotique contrôle, d'une manière quelconque par le signal informationnel. Cette solution a l'avantage d'être très simple à implémenter, mais par contre nécessite un système chaotique avec des contraintes fortes sur les paramètres intrinsèques. En plus, celui-ci doit travailler à des hautes fréquences. En pratique, il est difficile de trouver des circuits permettant un tel fonctionnement. Pour le moment, cette solution est surtout considérée dans un cadre théorique [24].

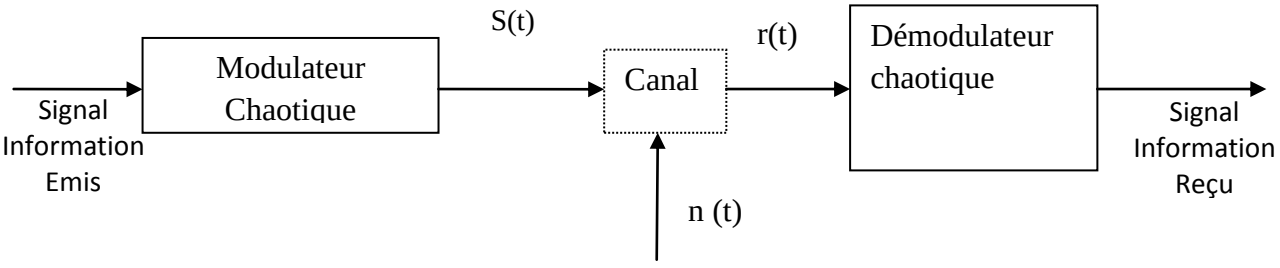


Figure (24): *Modulation directe du signal informationnel par porteuse chaotique haute fréquence.*

Une deuxième solution est de moduler le signal informationnel par un signal chaotique, et après d'appliquer une transposition en haute-fréquence, par l'intermédiaire d'une porteuse sinusoïdale [24]. Ce schéma est présenté dans la figure 25. Son avantage principal consiste en une simplification importante du modulateur chaotique [25].

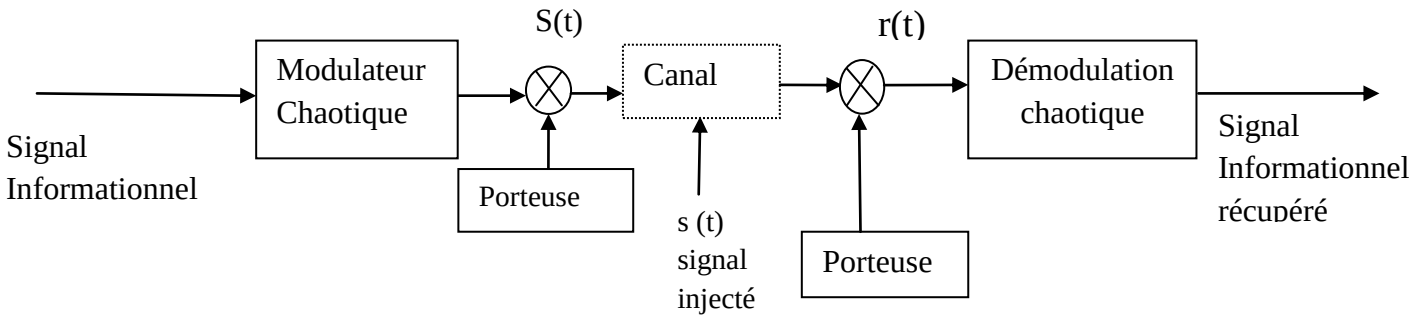


Figure (25) : *Modulation en bande du signal informationnel par le signal chaotique, combinée avec une mise sur porteuse classique*

Parmi les techniques de communications traditionnelles à base du chaos, on cite le masquage chaotique, la modulation paramétrique, la commutation chaotique, le cryptage par injection (inclusion), la transmission à deux voies et le cryptage combiné [25].

II.14 Définition de la cryptologie

La cryptologie (du grec (cryptos) : caché et (graphein) : écrire), est une science mathématique qui comporte deux branches : La cryptographie et la cryptanalyse [25].

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible : c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré.

Dans la cryptographie moderne, les transformations en question sont des chiffrements. Le décryptage est l'action consistant à retrouver le texte en clair sans connaître la clef de chiffrement [25].

Remarque :

Les termes "cryptage" et "crypter" sont des anglicismes, dérivés de l'anglais to encrypt, souvent employés à la place de chiffrement et chiffrer. Le "cryptage" pourrait être défini

comme l'inverse du décryptage, c'est-à-dire comme l'action consistant à obtenir un texte chiffré à partir d'un texte en clair sans connaître la clef [26].

II.15 Cryptographie par chaos

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée. En effet, un signal chaotique apparaît comme un « bruit» pseudo-aléatoire .Il peut être utilisé lors du cryptage de données, pour masquer les informations dans une transmission sécurisée ; il suffit de le «mélanger » de manière appropriée au message à envoyer confidentiellement [26].

II.16. Les méthodes de cryptage à base de systèmes chaotiques

Dans cette partie, nous développons six méthodes à base des systèmes chaotiques.

a. Cryptage par addition

Dans le cryptage additif, le message est tout simplement additionné au signal chaotique, et le signal résultant est envoyé au récepteur. En conséquence, après la synchronisation, le message confidentiel peut être récupéré par une simple opération de soustraction entre la sortie du récepteur et le signal émis sur le canal public [26].

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée pour des messages continus ou discrets. Dans les deux cas, il est impératif que l'amplitude du message original soit plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission [26].

Dans tout les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique [16]. Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit. Ce compromis va s'exprimer dans toutes les

techniques que nous présentons dans ce mémoire. La figure 26 montre en détails le principe de cryptage par addition [27].

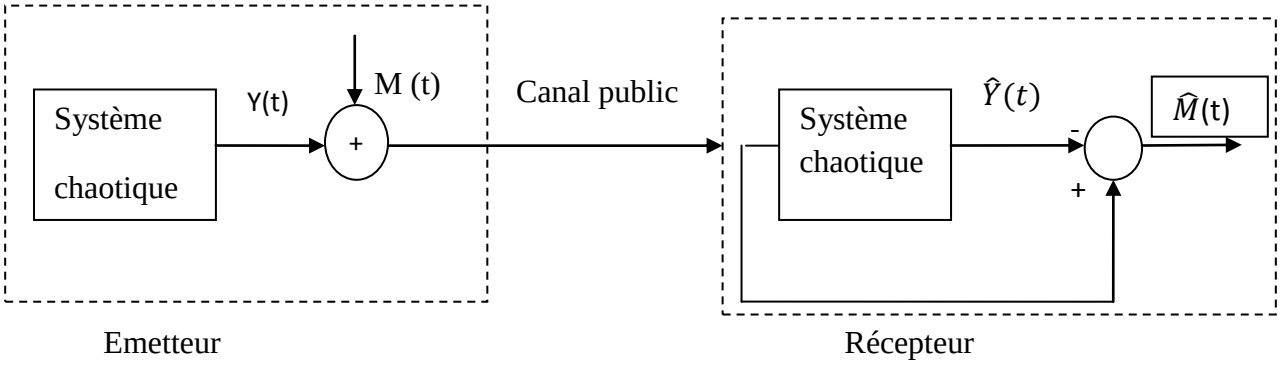


Figure (26)*: Principe du cryptage par addition.*

b.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 a entrées inconnues, soit sur l'inversion du système émetteur [27].

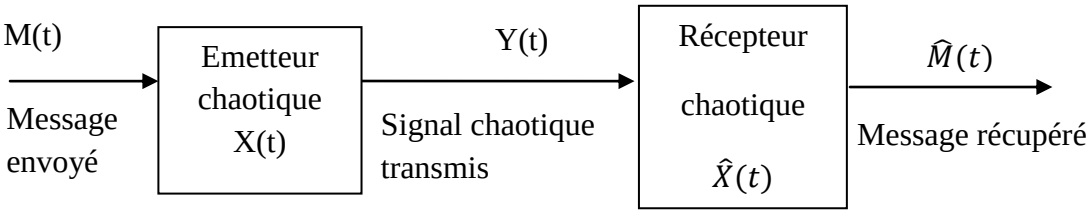


Figure (27) : *Cryptage par inclusion*

c.Cryptage par modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure 28 [28].

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre (s) impose à la trajectoire de changer continument 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 « classiques » [28].

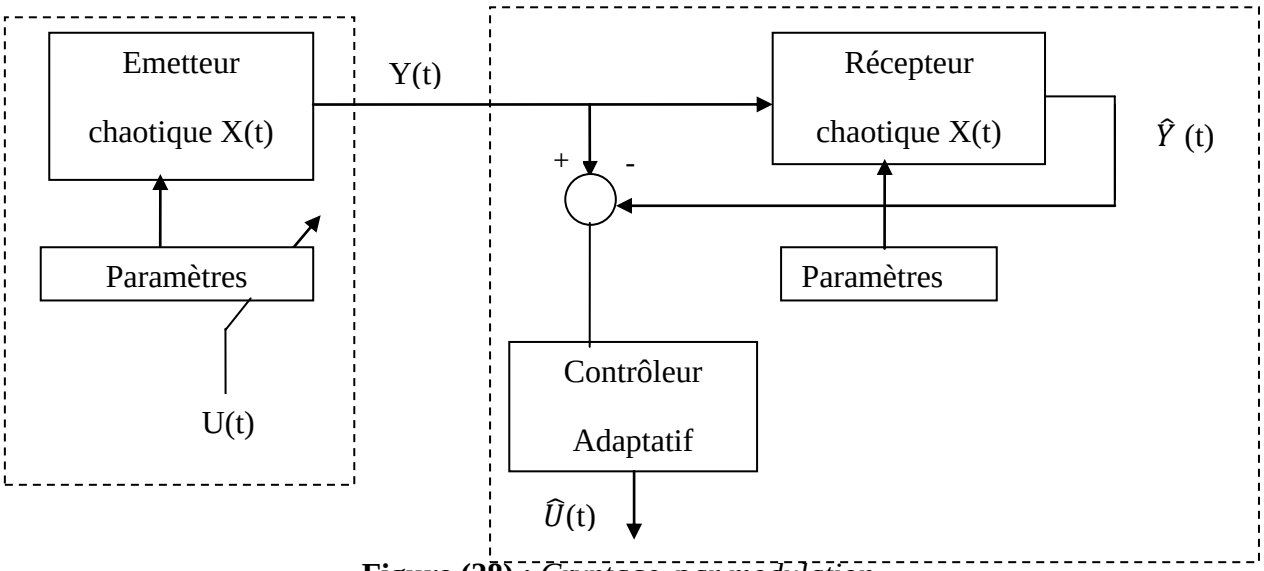
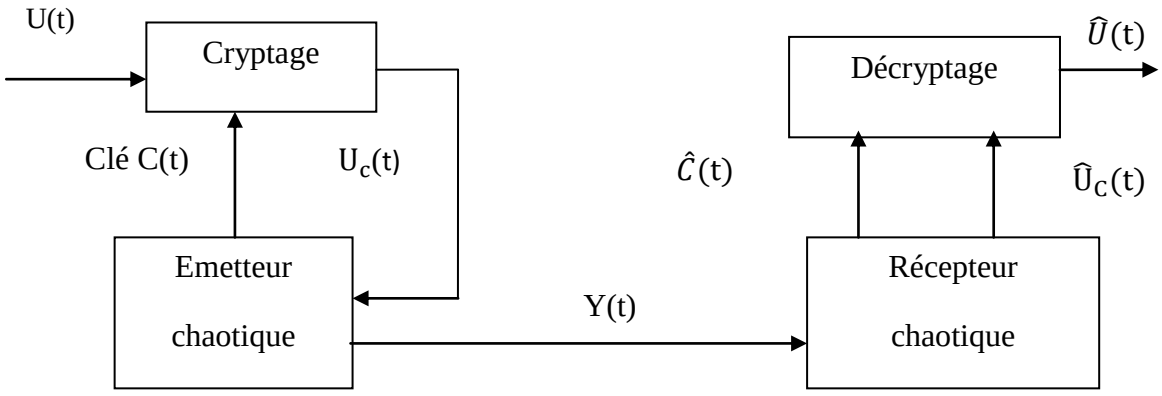


Figure (28) : *Cryptage par modulation*

d.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 établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message [16]. Le principe général de la méthode est illustré dans la Figure (29) [27].



Figure(29) *: Cryptage mixte*

e.Cryptage par commutation

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la figure 30 où une opération de commutation est employée selon la valeur du message binaire :

Si sa valeur est 0, alors le système chaotique 1est choisi et le signal de sortie est transmis, sinon c'est la sortie du système chaotique2 qui est transmise.

Dans ce sens, le message binaire commute avec l'émetteur entre deux attracteurs étranges correspondants aux deux systèmes chaotiques [28].

Du coté récepteur, il y a deux sous-systèmes chaotiques 3 et 4 qui correspondent respectivement à 1et 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, celon les erreurs de synchronisation (1,3) et (2,4), le signal pourra être récupéré avec succès. [7], [15].

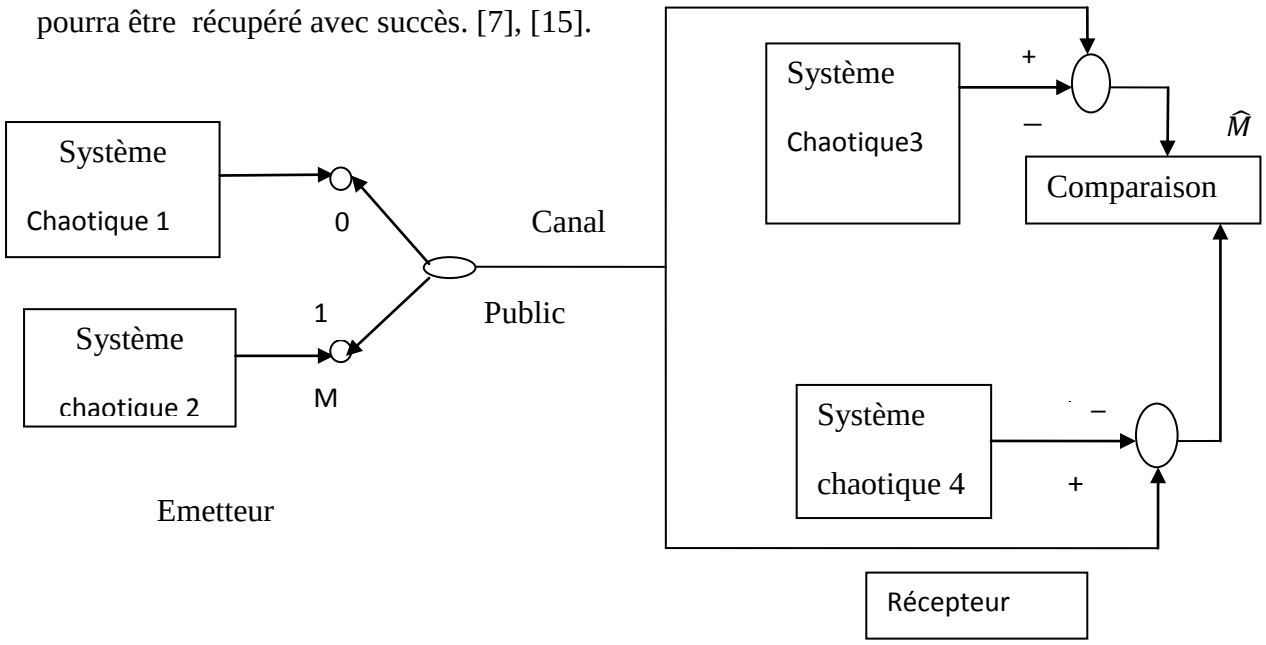


Figure (30) : *Cryptage par commutation*

f. Transmission par deux voies

Dans le schéma présenté dans la figure 31, l'émetteur envoie deux signaux au récepteur. Le premier (y_1) est une fonction à valeur réelles de l'état *(x)* du système émetteur chaotique,

son unique rôle 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 [29].

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 crypté par une fonction non linéaire de l'état *(x),* soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse [29].

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

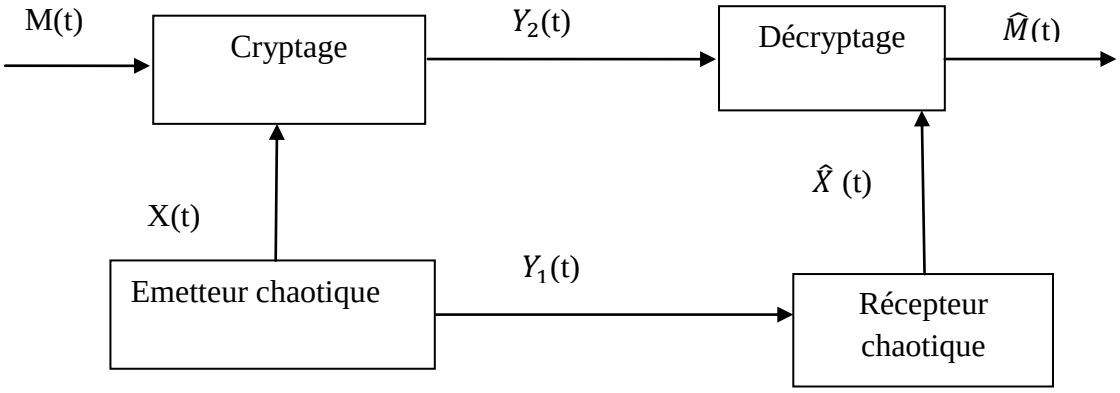


Figure (31) : *Méthode de transmission par deux voies*

II.17 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 crypto système en « cassant» la fonctions cryptographiques qui le composent.

La cryptographie et la cryptanalyse sont deux domaines d'étude évoluant constamment et en parallèle [18]. En effet, de nouveaux crypto-systèmes, 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 crypto systèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un crypto- système 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 [30].

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, information 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 [30].

A travers les années, de nombreuses attaques possibles contre les crypto- systèmes 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 [30].

Dans l'attaque active, 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 des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi, etc [30].

Dans les attaques passives, l'adversaire observe l'information qui transite sur le canal sans les modifier. Il cherche à récupérer des informations sur le crypto-système sans l'altérer, telles que le message, la clé secrète, etc. Dans ce cas, l'adversaire touche à la confidentialité des données [30].

Conclusion :

Ce chapitre a comme objectif de faire le lien entre les systèmes dynamiques chaotiques et le domaine des télécommunications .En première lieu, nous avons introduit les notions de synchronisation des systèmes chaotiques nous avons présenté les différentes méthodes de synchronisation puis nous nous sommes concentrés sur les techniques de transmission sécurisée d'information fondé sur le principe de synchronisation chaotique. En dernier lieu, nous nous sommes intéressés à la cryptanalyse et aux différentes techniques utilisées dans ce domaine.

Chapitre III

III.1 Introduction

Durant les dernières décennies, la synchronisation du chaos a attiré une attention considérable à cause de son application potentielle dans divers champs tels que les réactions chimiques, système biologiques et communication sécurisée. Plusieurs méthodes ont été proposées pour mieux l'exploiter, et envisager des perspectives d'application plus intéressantes.

Récemment une nouvelle méthode de commande est développée, il s'agit de la synchronisation impulsive. Cette technique assure la synchronisation des systèmes chaotiques en utilisant de simples impulsions, et elle est appliquée dans plusieurs systèmes de communication basée sur le chaos puisqu'elle garantit une bonne performance.

Dans notre travail, nous avons proposé et étudié un système de transmission basé sur le principe de la synchronisation impulsive.

Le système transmission est composé de deux blocs : Le premier est l'émetteur composé de deux systèmes chaotiques discrets : Le système de Lozi et le système de Hénon. Le deuxième bloc constitue le récepteur composé de deux types d'observateurs : L'observateur impulsif dont le rôle est de restaurer les états du système de Lozi et l'observateur étape par «étape ayant le rôle de reconstituer les états du système de Hénon. Le message à transmettre est d'abord crypté en utilisant un des état du système de Lozi avant d'être inclus dans le système de Hénon. La figure 32 illustre le schéma de transmission proposé.

Structure du schéma proposée

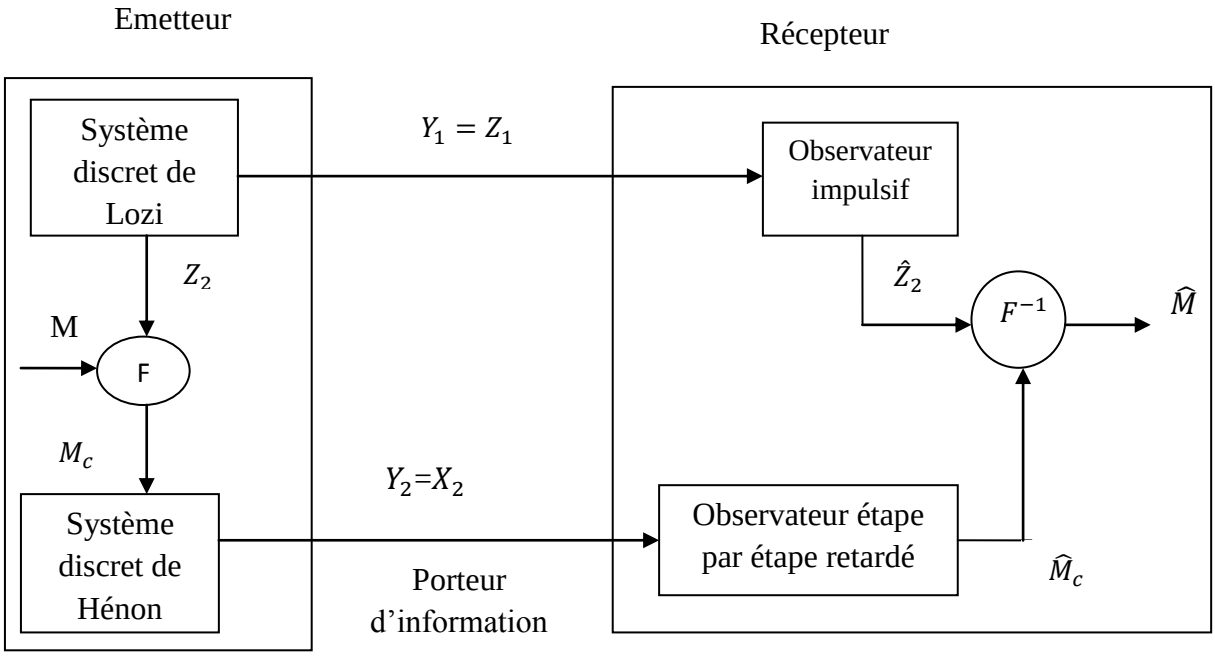


Figure (32): *La structure du schéma proposé.*

Dans la suite de ce chapitre, nous expliquons plus en détails le contenu et le rôle de chaque sous-bloc du schéma de transmission.

III.2 Etude de l'émetteur

Nous développons les deux systèmes chaotiques discrets constituant l'émetteur.

1. Présentation des équations de système Lozi :

Notre étude se porte sur le système discret de Lozi qui a deux dimensions, il est régi par le système d'équation suivant.

$$\begin{cases} Z_1\,(k+1) = 1 - a * \left| Z_1\,(k) \right| + b * Z_2\,(k). \\ Z_2(k+1) = Z_1(k). \qquad (1) \end{cases}$$

$$Y_1(k) = Z_1(k) o\grave{u} (Z_1, Z_2) \in$$

$$R^2\ est\ le\ vecteur\ d'état; Y_1(k) est la\ sortie\ du\ système.$$

2. Définition des paramètres

- a=1.7 et b=0.5 sont des constantes positifs.
- $Z_1(0)$= 0. 1 et $Z_2(0)$=0.2 sont les conditions initiales de l'équation (1) tel-que $Z_1(0)$ est utilisés pour synchronisation impulsive et $Z_2(0)$ est utilisé pour cryptage dans le système de Hénon.

Pour les valeurs a= 1.7, b= 0.5 le système présente un comportement chaotique, tel qu'il est illustré sur la figure 33.

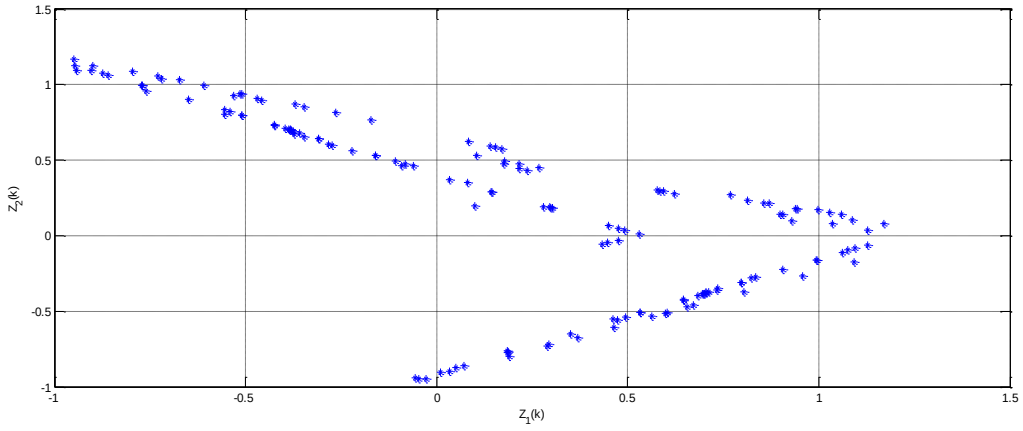


Figure (33) : *Attracteur étrange de Lozi*

3. Présentation des équations de Hénon :

On prend le système discret Hénon qui se présente sous la forme d'équations aux différences suivantes. [19]

$$\begin{cases} X_1(k+1) = a_h - X_1(k)2 + \mathrm{b_h X_2(k)} \\ X_2(k+1) = X_2(k) \\ Y_2(k) = X_2(k) \end{cases} \quad (2)$$

Où $(X, Y) \in R^2$ est le vecteur d'état, Y_2 est la sortie du système

Le système de Hénon que nous étudions a une dynamique chaotique, sa trajectoire dans le plan de phase est un attracteur étrange pour les paramètres a_h=1.4, b_h=0.3

On a $X_1(0) = 0.1\,, X_2(0) = 0.1$ sont des conditions initiales pour faire le calcule de la fonction de cryptage.

La figure 34 représente l'attracteur étrange du Hénon pour les valeurs$a_h et b_h$ fixés précédemment.

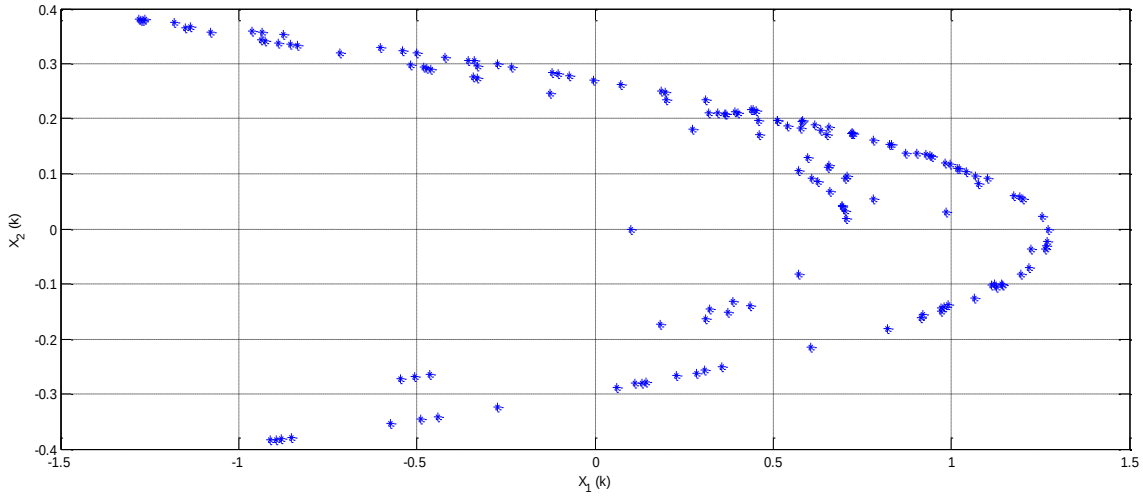


Figure (34) *: Attracteur étrange de Hénon*

4. La fonction de cryptage

La fonction de cryptage est définie par l'équation suivante :

$$M_{c=} \text{ F (M,}Z_2) = \text{g*M+c*}Z_2\text{-}dZ_2^2 \quad (3)$$

où g=0.0005, d=0.002 et c=0.001 sont des constantes et sont considérées comme des clés de cryptage additionnelles. M est le message binaire et M_C le message crypté inclus dans la dynamique du système discret de Hénon.

Le nouveau système de Hénon obtenu est alors :

$$\begin{cases} X_1(k+1) = a_h - X_1(k)2 + b_h X_2(k) + M_c \\ X_2(k+1) = X_1(k) \\ Y_2(k) = X_2(k) \end{cases} \quad (4)$$

III.3 Etude du récepteur

L'utilisation d'observation est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système dynamique est dit observable si on peut récupérer toutes grandeurs par une combinaison de mesures et de leurs dérivées. En 1997, Nijmeijer et Mareels [31]. Ont montré que la synchronisation unidirectionnelle de deux systèmes chaotiques peut être considérée comme un problème d'observateur non linéaire et par conséquent, les théories d'automatique peuvent être utilisés pour analyser ce phénomène [31].

- ✓ **Observateur impulsif**

On a le système suivant :

$$\begin{cases} \hat{Z}_1(k+1) = A * \hat{Z}(k) + \emptyset(\hat{Z}(k)) \quad k \neq k_i \\ \hat{Z}(k_i^+) = \hat{Z}(k_i) - B_{ki} * e(k_i) \quad k = k_i \ , i = 1,2,\dots \end{cases} \qquad (5)$$

Où $\hat{Z} = (\hat{Z}_1, \hat{Z}_2) \in R^2$ sont des états du système, le principe consiste à contraindre l'observateur à suivre l'évolution du système original a des instants (k_i). $B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$ est une matrice carre (2×2) diagonale, elle joue le rôle d'un facteur de correction à l'arrivée des impulsions.

On appelle $k_i^+ \ et \ k_i^-$ les instants juste après et juste avant l'arrivée des impulsions.

$e = Z - \hat{Z}$ Est l'erreur de synchronisation.

- $\emptyset(k_i) = \begin{pmatrix} 1 - a|Z_i| \\ 0 \end{pmatrix}$ et $A = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$ est la matrice d'état (2×2) avec des paramètres $a \ et \ b$ ont les même valeurs à savoir$a = 1.7$, b=0.5.

Le système d'erreur est donné comme suit [33] [34].

$$\begin{cases} e_{k+1} = Ae_k + \emptyset(Z_k) - \emptyset(\hat{Z}_k), k \neq k_i \\ \Delta e_k = e_{ki+} - e_{ki-} = B_{ki} e_{ki-} = B_{ki} e_k, k = k_i, i=1,2\dots \end{cases} \qquad (6)$$

La synchronisation impulsive entre les systèmes (1) et (5) dépend de la stabilité du système d'erreur (6).

- ✓ **Observateur retardé étape par étape**

La première étape consiste à appliquer un pas de retard sur la sortie et ainsi reconstruire le premier état du système de Hénon .Durant la seconde étape on applique deux pas de

retard sur la sortie et un pas de retard sur l'état venant d'être reconstruit afin de reconstruire le second état. L'application de retards est faite sur tous les états jusqu'à la dernière information contenant l'entrée du système de départ. Chaque état reconstruit à l'itération k contribue à la reconstruction du prochain état à l'itération $k+1$ [35], [36].

a. Reconstruction de l'état $\widehat{X}_1$

De la première équation du système (7), en appliquant un retard d'un pas, on déduit l'état $\hat{X}_1$comme suit :

$$\hat{X}_1(\text{k-1})={}^{Y_2(k)}/_{b_h}, \qquad (7)$$

Avec le paramètre de fonction Hénon b_h=0.3

b. Reconstruction de l'état $\widehat{M}_c$

Dans la seconde équation (8) du message crypté, en appliquant un retard de deux pas à la sortie, nous déduisons le message $\widehat{M}_c$ comme suit :

$$\widehat{M}_c(\text{k-2})= \hat{X}_1(\text{k-1}) \text{ -1+}a_h(\hat{X}_1\,(k-2)^2) \text{ –Y (k-2).} \qquad (8)$$

Avec le paramètre a_h=1.4.

La figure 35 illustre le signal du message crypté inclus dans le système de Hénon

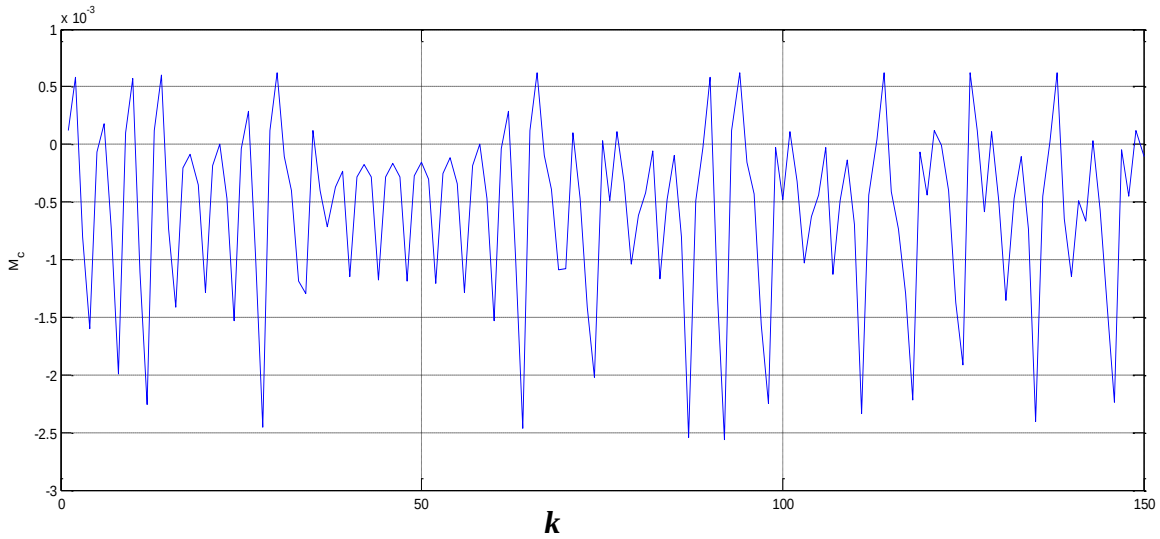


Figure (35) : *Message crypté*

c. Fonction de décryptage

L'équation suivante représente la fonction de décryptage qui est l'inverse de la fonction de cryptage F.

$$\widehat{M}(k) = F^{-1}\left(\widehat{M}_{c,}\hat{Z}_2\right) = \widehat{M}_c(k) - \hat{Z}_2(k) + d * (Z_2^2(k))/g. \qquad (9)$$

III.4 Canaux de transmission

Dont notre cas, nous avons deux canaux de transmission définis comme suit :

- ✓ **Canal 1 :** c'est le canal qui permet la transmission du signal de synchronisation impulsive Z_1.
- ✓ **Canal 2** : c'est le canal porteur de l'information X_2.

Conclusion

Dans ce chapitre nous avons défini l'ensemble des paramètres des fonctions permettant la synchronisation de deux blocs (émetteur, récepteur), ce que nous permet de restituer correctement le signal message envoyé. Dans le chapitre suivant nous donnerons les résultats de simulation obtenus et nous discuterons sur l'efficacité du schéma de transmission proposé.

Chapitre IV

IV.1 Introduction

Dans ce chapitre, nous allons procéder à la simulation de notre système sous Matlab. Nous considérons les paramètres suivants :

- La matrice carrée diagonale de correction $B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}, b_1 = b_2 = -0.95$ et les paramètres de l'observateur impulsif T si la période des impulsions=3s

- Les paramètres du système de Lozi $a = 1.7\ et\ b = 0.5\ , Z_1(0) = 0.1\ et\ Z_2(0) = 0.2$ et les paramètres du système de Hénon $a_h = 1.4\ et\ b_h = 0.3\ , X_1 = 0.1\ \ et X_2 = 0.1.$

IV.1. Résultats de synchronisation

Dans cette parties, nous donnons les résultats de synchronisions pour chaque système discret.

- **Synchronisation impulsive**

Reconstruction de l'état(Z_1 , $\widehat{Z}_1$)

La figure (36) montre le processus de reconstruction de l'état Z_1 du système de Lozi.

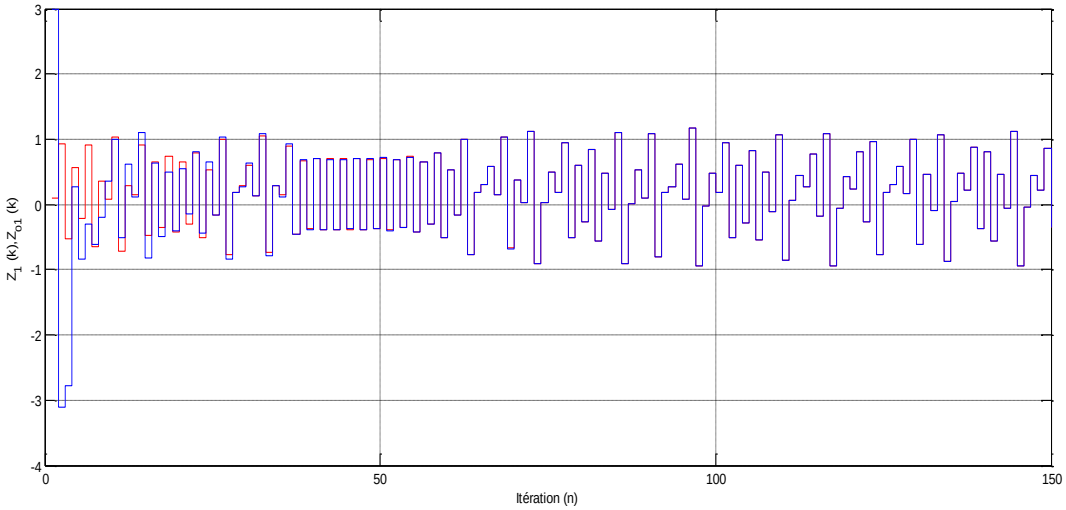
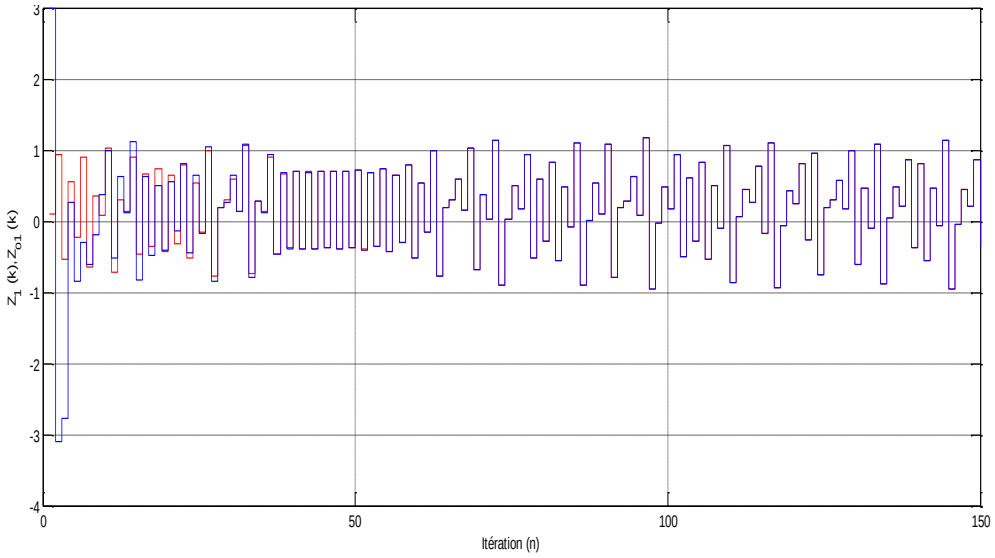


Figure (36): Les états *synchronisation*$Z_1 et\ \hat{Z}_1$.

- **Reconstruction de l'état Z_2**

La figure (37) montre le processus de reconstruction de l'état Z_2 du système de Lozi.



Figure(37) :*L'état de synchronisation de*Z_2.

Les figures (38) et (39) représentent les erreurs (e_1, e_2) de synchronisations impulsives.

- **Erreur de synchronisation $e_1 = Z_1 - \hat{Z}_1$.**

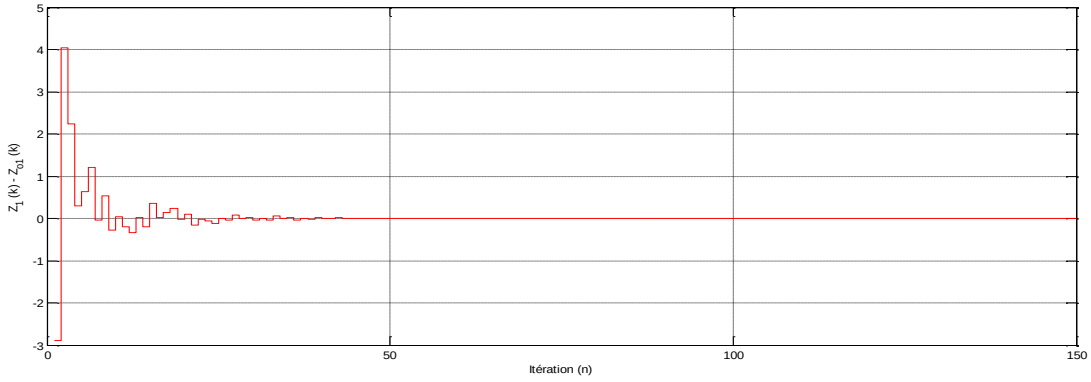


Figure (38) : *Erreur de synchronisation* $e_1 = Z_1 - \hat{Z}_1$

Remarque : $Z_{O1} = \hat{Z}_1, Z_{O2} = \hat{Z}_2$

$X_{o1} = \hat{X}_1$

- **Erreur de synchronisation $e_2 = Z_2 - \hat{Z}_2$**

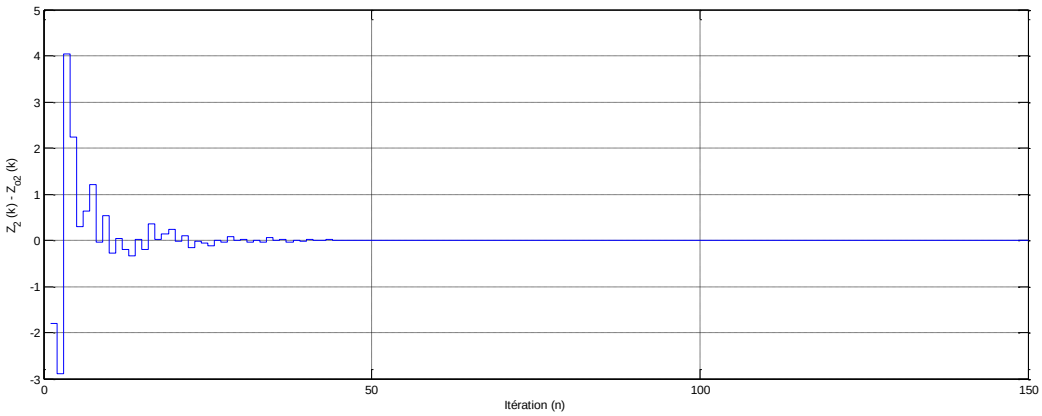
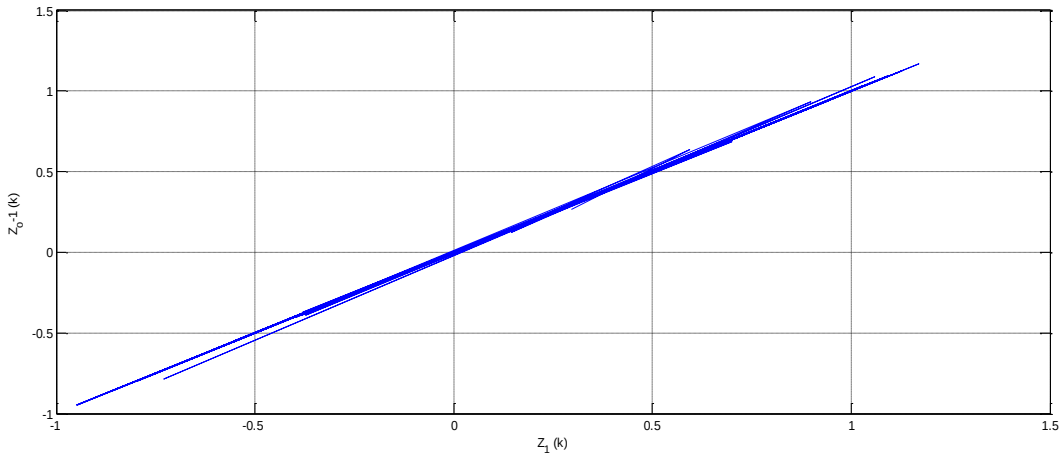


Figure (39) : *Erreur de synchronisation $e_2 = Z_2 - \hat{Z}_2$.*

A partir des figures (38) et (39), nous constatons la synchronisation impulsive a bien lieu après un court régime transitoire des 'états synchronisé Z_1 *et* $\hat{Z}_1$

- **Plan de phase de synchronisation $(Z_1, \hat{Z}_1)$**



Figure(40) : *Plan de phase de synchronisation $(Z_1, \hat{Z}_1)$.*

- La droite obtenue confirme l'établissement de la synchronisation impulsive.

Pour constater l'impotence du choix de la période des impulsions T. Nous avons augmenté cette dernière et observé, le comportement de l'observateur impulsive.

La figure (41) illustre l'effet d'augmentation de la période T

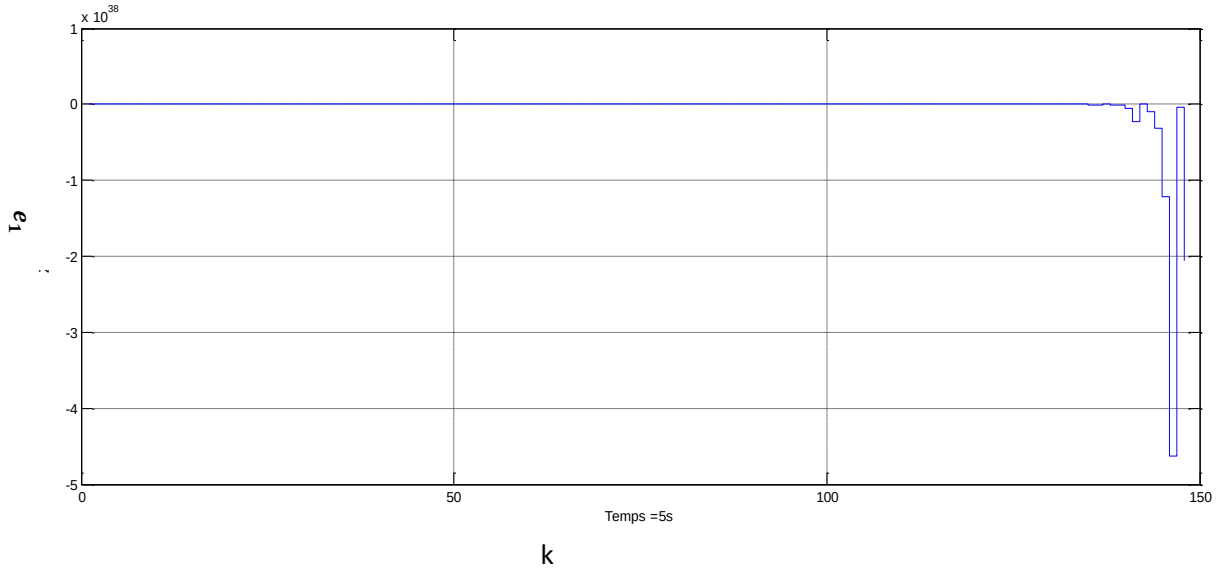


Figure (41) : Augmentation de la période des impulsions

Remarque : Nous remarquons que la période T des impulsions prend une valeur supérieure à 3, l'erreur de synchronisation diverge, autrement dit, la synchronisation impulsive n'a pas lieu.

- **Synchronisation étape par étape (X_1,$\hat{X}_1$)**

  La figure (42) représente l'état $\hat{X}_1$et son estimé $\hat{X}_1$. On remarque qu'il n'ya aucun régime transitoire et que la synchronisation est exacte.

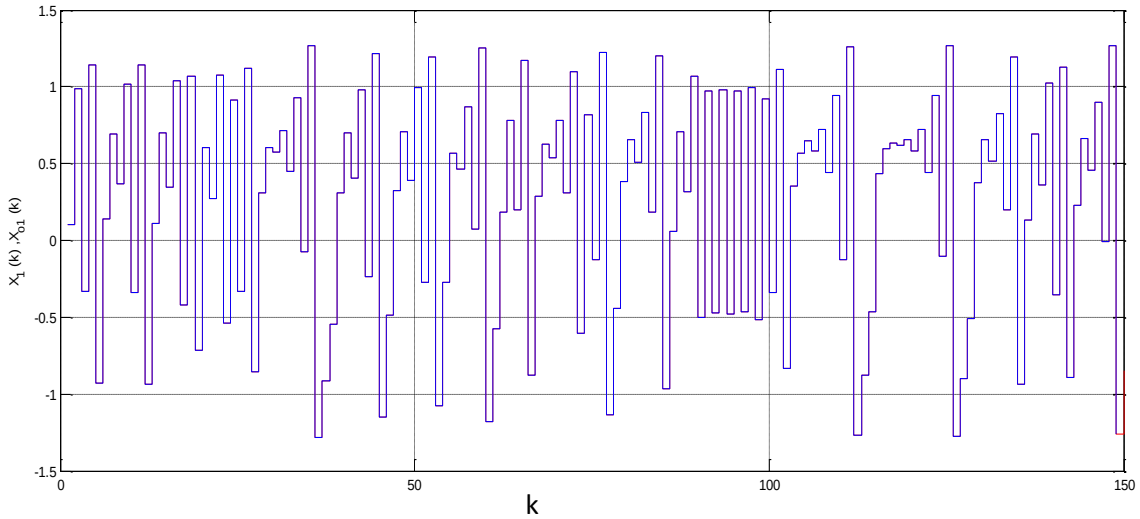


Figure (42) : Les états *synchronisés* $X_{1,}et\hat{X}_1$.

IV.2. Résultats de transmission

Nous avons pris comme exemple un signal triangulaire d'amplitude A=1 et de période $\Delta = 1s$, la figure 43 illustre le message crypté M_c et son estimé$\widehat{M}_c$ (M_{co}).

- **La transmission du message crypté(M_c,$\widehat{M}_c$).**

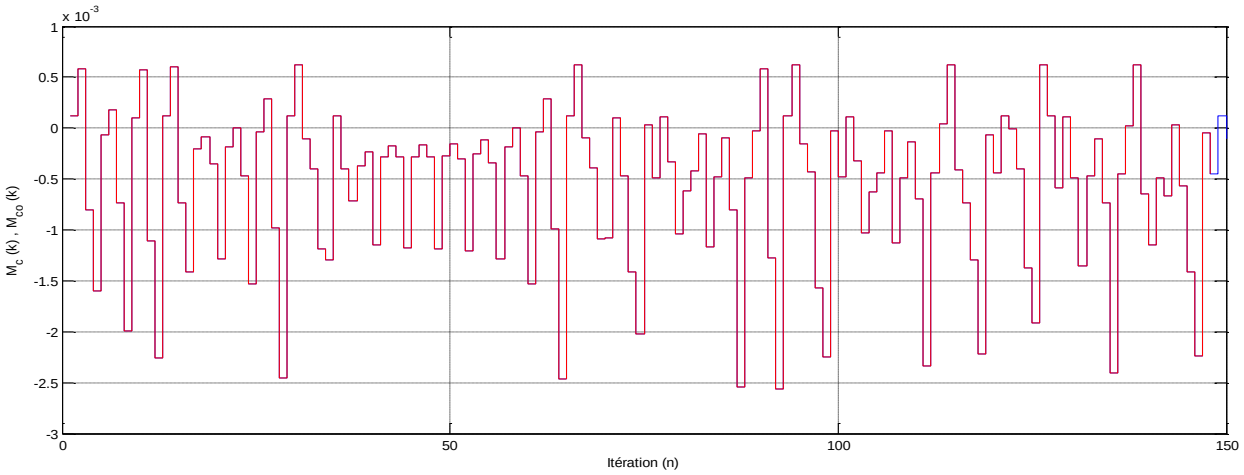


Figure (43) : *Transmission du message crypté M_c.*

- Nous remarquons que, comme pour les états $X_1 \; et \; \hat{X}_1$, la reconstruction du message M_c est parfaite.

- **Résultats de la transmission du message *M***

La figure (44) représente les résultats de la transmission du message$\widehat{M}$.

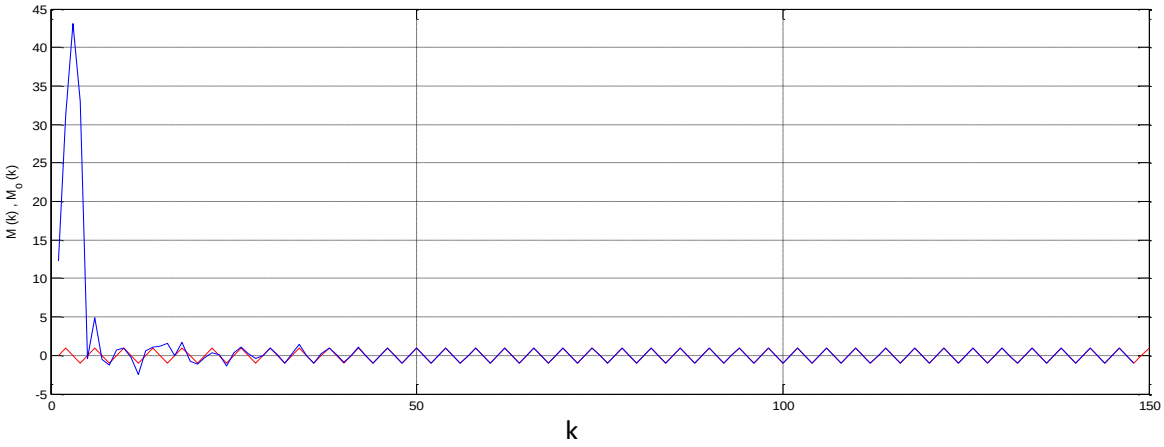
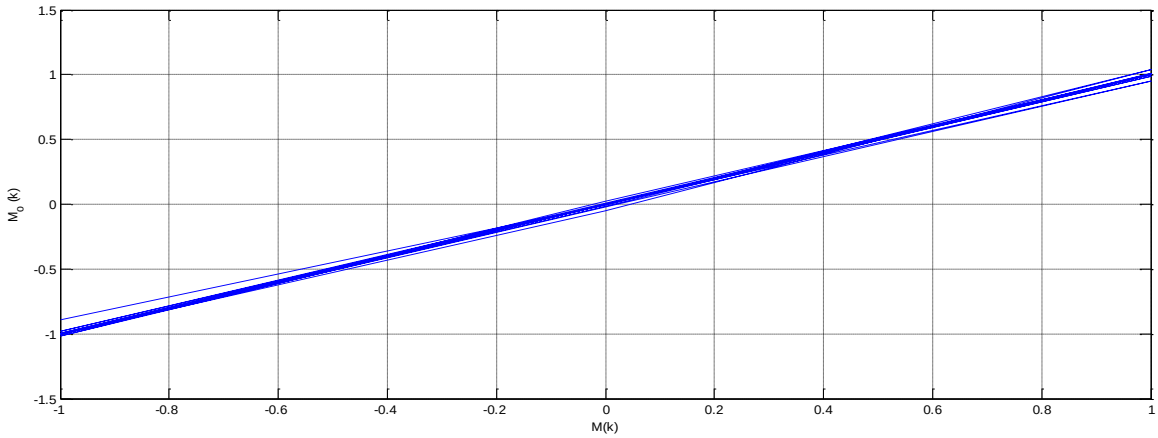


Figure (44) : *Le message décrypté $\widehat{M}$.*

A partir de la figure 44 précédent, nous pouvons affirmer que le message est bien récupéré au niveau du récepteur, et ce, après un court régime transitoire de même durée que celui constaté lors de la synchronisation impulsive.

- **Plan de phase du message décrypté.**

La figure (45) illustre le plan de phase des deux messages envoyéM et reçu $\widehat{M}$.

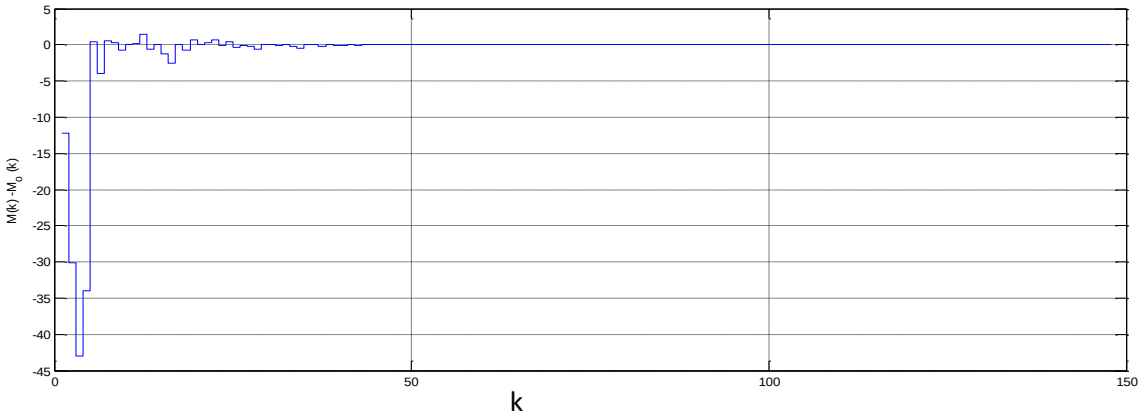


Figure(45) : *Plan de phase des messages*$M, \widehat{M}$.

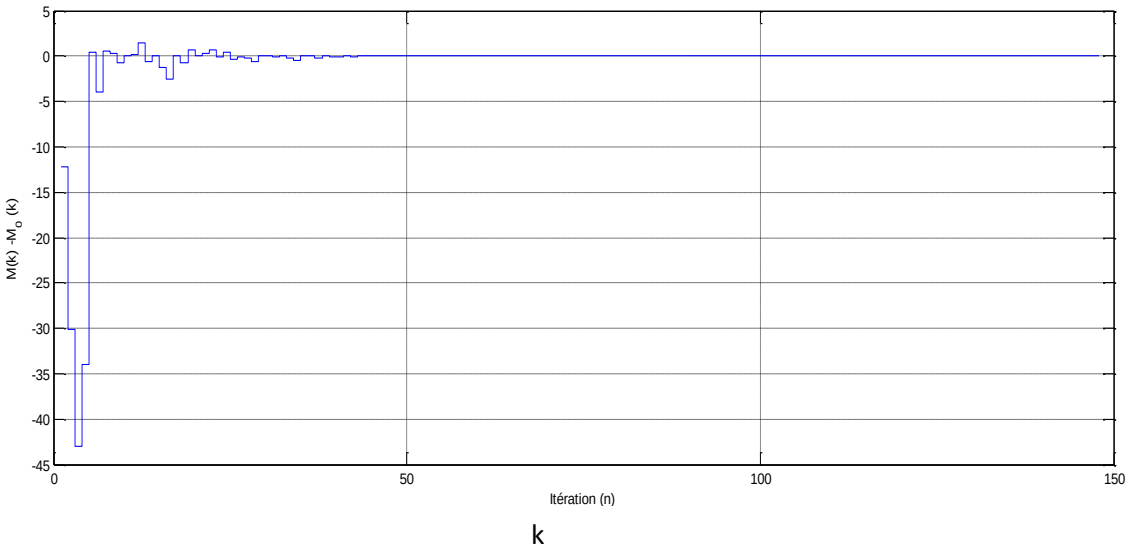
L droit obtenue confirme a qualité de transmission u message de transmission $e_M = (M - \widehat{M})$.

- **Erreur de message décrypté**

L'erreur s'annule après un court régime transitoire comme peut le voir sur la figure (46).



Figure(46) : *Erreur sur le message* $e_M = M - \widehat{M}$.



Figure(47) : *Erreur sur le message* $e_M = M - \widehat{M}$.

Conclusion :

Dans ce chapitre, nous avons présenté les résultats de simulations de notre dispositif de transmission. Ce dernier est composé de deux parties (un émetteur et un récepteur). La partie représentant l'émetteur est constituée du système de Lozi et du système de Hénon. La partie récepteur est constituée d'un observateur impulsif et observateur retardé étape par étape. Le choix de ce dernier est justifié par sa capacité à reconstruire les états de l'émetteur d'une manière exacte. Autrement dit, les erreurs de synchronisations entre les états de l'émetteur et ceux du récepteur s'annulent. Par conséquent, le message a été reconstruit au niveau du récepteur.

Conclusion générale :

Le travail que nous avons réalisé nous a permis de toucher a une partie de domaine de chaos. Pour ce faire, nous avons étudié et réalisé un système transmission de données sécurisé en utilisant le chaos. Nous avons présenté tous les points essentiels concernant ces systèmes, tel que les définitions et leur caractéristiques et au final nous avons conclu que malgré la complexité de ces systèmes leur étude et leur réalisation n'est pas impossible.

Dans le premier chapitre, nous avons définit les notions des systèmes chaotiques en abordant leurs propriétés les plus intéressantes. Nous l'avons clos en montrant les différents cas de transition vers le régime chaotique.

Dans le deuxième chapitre, nous avons cité les méthodes utilisées pour la synchronisation de ces systèmes chaotiques, et les différentes méthodes de transmission des données.

Dans le troisième chapitre, nous avons étudié le schéma proposé qui se compose de deux blocs. Le premier bloc est un émetteur composé des systèmes de Lozi et de Hénon, et le deuxième bloc est un récepteur (observateur impulsif et observateur étape par étape).

Dans le quatrième chapitre nous avons simulé ce système de transmission sur Matlab. Des résultats de simulation bien illustré les performances de la méthode proposé (A récupération de tous les états aussi que le message crypté au niveau de l'émetteur).

Afin d'améliorer notre travail nous envisageons de réalisé un système de transmission avec deux cartes programmables, par exemple les cartes Arduino Uno ou cartes Méga (l'une joue le rôle de l'émetteur et l'autre un récepteur).

Pour finir, on souhaite vivement que notre travail soit apprécié et fera objet d'une contribution aussi minime soit-elle dans le domaine de l'analyse et la synchronisation des systèmes chaotiques

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

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

[3]G. Kaddoum «Contributions à l'amélioration des systèmes de communication multi utilisateurs par Chaos : synchronisation et analyse des performances » thèses de Doctorat de l'Université de Toulouse, 2008.

[4] E. Goncalvès « introduction au système dynamiques et Chaos ». Cours de l'institut National Polytechnique de Grenoble, 2004.

[5]D.Viennot « Analyse Spectrale pour les systèmes dynamiques classiques ». Cours Master Physique & physique Numérique, Université de Franche-Comté.

[6] C.Morel « Analyse et contrôle de dynamiques Chaotiques, application à des circuits éléctroniques non-linéaires ». Thèse de Doctorat de l'école Doctorale d' Angers.2005.

[7] A. Ouastaloup, J. Sabatier, and P.Lanusse. « From fractal robustness to the crone control » fractional Calculus and Applied nalysis, 2, 1999.

[8] C. Ramus-Serment, X.Morceau, M.Nouillant, A.Oustaloup, and F. Levron. « Genéralised approach on fractional response of fractal networks », Chaos Solitions & Fractals, 2002.

[9] G.Zaibi « Sécurisation par dynamiques des réseaux locaux sans fil au niveau de la couche MAC », thèse de Doctorat de l'université de Toulouse, 2012.

[10] M. Inoue and H. Kamifukumoto « Scenarios Leading to Chaos in a Forced Lotka-Volterra Model », Progress of Theoretical Physics, Vol.71, No.5, May 1984.

[11] J. Malek « La Théorie du Chaos en Finance : une application économique », Mémoire de Licence, école de commerce Solvay, ULB, 1995.

[12] A.B. Zer & E. Akin « Tools For Dectecting Chaos", Institut des Sciences et Technologies, Université Sakarya, Jornal 9 Cilt, 1 Say1, Turquie, 2005.

M. Hénon & C. heils, « Yhe Applicability of the Third integral Of Motion : Some Numerical Experiments » The Astrophysical Journal, 69 (1994), 73 – 79.

[13] S. Penaud « Etude des Potentialités du Chaos pour les systèmes de Télécommunications, évaluation des performances de systèmes à accès Multiples à répartition par les Codes (CDMA) Utilisant des séquences d'étalement Chaotique » Thèse de Doctorat de l'Université de Limoges, 2001.

[14] L.M Pecora, T.L. Carroll « Synchronization in Chaotic systems », physical review letters, Vol 64 N° 8, 1990.

[15] I. Ameur « Synchronisation Chaotification et Hyperchaotification des systèmes non-linéaires : Méthodes et applications», thèse de Doctorat de l'Université Mentouri de Constantine, 2011.

[16] T. Hoet, B. Lorenz, S. Sahin « la cryptographie Chaotique », Mémoire de Licence IMACS INSA Toulouse, 2012.

[17] O. Magherbi « étude et réalisation d'un système sécurisé à base de système Chaotique » Mémoire de Magister en Automatique, Université Mouloud Mammeri Tizi-Ouzou, 2013.

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

[19] M. Hassler and T.Schnimming « communications using Chaos » Ins.Conf. On Signals and Electronic systems, 2001.

[20] M. Abramowitz, I.A. Stegun Handbook of mathermatical functions with Formulas, graphs and Mathematical tables », Dover Publications, Inc, New York, 1965.

[21] G.R.Coopper, R.W. Nettleton « asead spectrum Tecgnique For Gigh capacity mobile communications », IEEE Trans. Veh. Tech, Vol. VT 27, 1978.

[22] G.R. Cooper, R. W. Nettleton « Spectral efficiency in cellular Iand-mobile communications: a spread spectrum approach », final Report, TR- EE 78-44, Purdue University, West lafayette .Ind 1978.

[23] H. Nijmeijet and I.Mareels. « Synchronisation des systèmes Chaotiques par observateurs et applications à la transmission d'informations », Thèse de Doctorat de l'Université de Paris Sud 11.2012.

[24] H. Nijmeijet and I. Mareels. «An observer looks at synchronization» IEEE Trans. On Circ Syst.I: Fundamental Thery and Applications, 44(10): 882-890, 1997.

[25] H. Hamiche "Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Applications à la Transmission sécurisée de donnée » Thèse de Doctorat, Université Mouloud Mammeri de Tizi-Ouzou, 2011.

[26] K. Veselyand J.Podolsky, « Chaos in a modified Hénon- Heiles system describing geodesics in gravitation waves »

[27] M.Djemai, J-P Barbot and I. Belmouhoub, « Discrete-Time Normal From for Left Invertibilily problem », Eur, J.Control, Vol.15, p194-2014, 2009.

[28] I. Belmouhoub, M. Demai and J.P. Barbot, « Observability quadtatic normal Form for discrete-Time système », IEEE Transactions on Automatic control, vol 50, July 2005.

[29] M.Djemai, J-P Barbot and I. Belmouhoub, « Discrete-Time Normal From for Left Invertibilily problem », European Jornal of Control, Vol.15, p194-2014, 2009.

[30] L.M. Pecora and T.L. Caroll, « Synchronization in systems », Phys. Rev. Lett, Vol. 64, PP. 973977, 1992.

[31] L. Cong and W. Xiaofu, « Design and realization of an FPGA- based generator for chaotic frequency hopping sequences », IEEE Transactions on circuits and systems-I Fundamental theory and applications, vol. 48, pp. 521532, 2001.

[32] DataSheet ATMEGA 328.

[33] R.Mainieri, J.Rehacek $\ll Projective\ synchronzation\ in\ three-dimensional \gg$ Physical Review Letters, volume 82, N015, pp.3042-3045, 1999.

[34] P. Bergé<<L 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.Barbo, 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, Thése de doctorat, Université Pierre et Marie curie, Paris, France, 2007.

[38] ZHENG Yong-Ai, NIAN Yi-Bei, LIU Zeng-Rong. 2003 Chinese Physical Society and IOP Pubishing Ltd.

Sources internet:

http://just.loic.free.fr/index.php?page=alem.

http://fr.questmachine.org/wiki/la_th%C3%A9orie_du_chaos.

http://www.mathworks.com/matlabcentral/fileexcha,ge/233-let