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

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

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

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**

Spécialité : **Commande des Systèmes**

Présenté par

Nouara MEZAR
Siham SEBTI

Mémoire dirigé par **Redouane KARA**

Thème

Etude d'un système de transmission de données robuste à base de la synchronisation impulsive chaotique

Mémoire soutenu publiquement le 24/09/ 2017 devant le jury composé de :

M Ahmed MAIDI
Professeur, UMMTO, Président

M Redouane KARA
Professeur, UMMTO, Encadreur

M Hamid HAMICHE
MCB, UMMTO, Examinateur

Remerciements

Nous adressons en premier lieu notre reconnaissance à notre ***DIEU*** *tout puissant, de nous donner la santé et la volonté d'entamer et terminer ce mémoire.*

Nous adressons le grand remerciement à notre promoteur ***Mr KARA*** *pour nous avoir honorées de diriger ce travail.*

Nous sommes conscientes de l'honneur que nous a fait le membre du jury d'avoir accepté d'examiner notre travail.

Nos remerciements s'adressent également à tous nos professeurs pour leur générosité et la grande patience dont ils ont su faire, en particulier ***Mlle MEGHERBI*** *.*

Nous exprimons nos profonds remerciements à l'encontre de nos parents qui nous ont enseigné la patience, la politesse, le sacrifice et qui ont été là pour nous.

On n'oublie pas de dire merci à toutes les personnes et tous nos amis qui ont contribué de près et de loin à l'enrichissement de notre travail et notre épanouissement intellectuel.

Dédicaces

Je dédie ce modeste travail :

*A ma très chère **maman**, puis à **maman**, puis à **maman**, puis à mon cher **père**. Aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.*

*Je t'aime **maman** merci*

*A ma chère grand-mère **ZEDJIGA**. A la mémoire de mon regretté défunt grand père **MOHAMMED**.*

*A mon frère adoré **WALID** que j'aime énormément*

*A l'homme de ma vie **FARID** qui m'a soutenue tout au long de ce projet, celui que je ne cesserai jamais d'aimer.*

*A mes chers **beaux-parents** que j'aime*

*A mes **beaux-frères** et **belles-sœurs***

*A mes chères tentes **ROZA** et **MALIKA** et leurs enfants*

*A toute ma famille et mes amis(es) **DOUDA, DAHBIA, DJOUDJOU, LAKY, LITY ..., HOCINE.K, AMINE.N** qui nous ont beaucoup aidées.*

*A mon binôme **NOUNA** et sa famille*

*Sans oublier bien sûr mes bien-aimées **ASMA, CELINE, FATI** et mon petit prince **AMIR***

Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

SIHAM. S

Dédicaces

Je dédie ce modeste travail :

*A **mes parents**, aucun hommage ne pourrait être à la hauteur de Lamour dont ils ne cessent de me combler. J'espère que je serai à la hauteur des valeurs que vous avez semées en moi. Que dieu vous procure bonne santé et longue vie.*

*A ma sœur adorée **Kenza**.*

*A mes chers frères **YACINE** et **ACHOUR**.*

*A toute ma grande famille, ma **grand-mère** en particulier.*

*A mon fiancé **AMIR** qui m'a soutenu tout au long de ce travail.*

*A mes **beaux-parents**.*

*A mes meilleurs amies **DIHIA** et **LYDIA***

*A mon binôme **SIHAM** et sa famille.*

*A tous mes amis (es) et camarade ... **AMINE.N, REZKI.O, NESSRINE.M, HOUSSINE.K.** Et à tous ceux qui ont contribué de près et de loin, je leur serais reconnaissante.*

NOUNA.M

Sommaire

Chapitre I

Chapitre II

Chapitre III

Liste des figures

Liste des figures

Liste des tableaux

Liste des tableaux

Introduction générale

Protéger des informations particulières a toujours été un des intérêts principaux de l'Homme. On a ainsi cherché à établir des techniques dites « cryptage » afin de rendre ces informations incompréhensibles à ceux qui n'ont pas accès à une « clé » secrète.

Depuis quelques années, des chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données, en particulier
Pour transmettre des quantités importantes d'informations sécurisées. L'intérêt d'utiliser des Signaux chaotiques réside dans deux propriétés du chaos [1]. Un signal chaotique est un signal à large spectre d'une part, il permet de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ [2].
Ce type de communication on essaye de mettre certains concepts de la théorie du chaos à la disposition du chiffrement, en particulier les attracteurs de Hénon et Lozi seront cryptés pour valider le chiffrement.

La transmission chaotique est un mode de communication à clé secrète, la connaissance de cette clé est nécessaire du coté de l'émetteur ainsi que du coté du récepteur pour le chiffrement et le déchiffrement du message, on doit disposer au niveau du récepteur d'un signal identique [2]. Cela veut dire que deux signaux chaotiques seront dit synchronisés s'ils sont asymptotiquement identiques.

Ce travail consiste à réaliser un système de transmission sécurisée à base du chaos, en utilisant deux systèmes, Hénon et Lozi, une partie sera consacrée pour la synchronisation à base d'un observateur impulsif et l'autre partie pour le chiffrement des données en employant le cryptage pas addition. En premier lieu nous allons faire une simulation sous Matlab puis nous essayerons de réaliser le système de transmission et de cryptage.

Ce travail est composé de trois chapitres :

Dans le premier chapitre nous allons présenter quelques définitions et propriétés des systèmes dynamiques non linéaires et les notions de base des systèmes chaotiques.

Dans le deuxième chapitre nous allons citer les différentes méthodes de synchronisation les plus usées et aussi les techniques de cryptage et de décryptage.

Dans le troisième chapitre , nous proposons une méthode de synchronisation à base d'un observateur Impulsif qui est la synchronisation impulsive et la technique de cryptage par addition qu'on a utilisé pour sécuriser le message, et leur application sur les deux systèmes Hénon et lozi.

Chapitre I:

Généralités sur les systèmes chaotiques

I.1 Introduction

Le mathématicien Henri Poincaré qui, dés la fin du XVIIIe siècle, a mis en évidence l'imprévisibilité d'un système de trois corps en interaction (système solaire) qui est a l'origine de la théorie du chaos.

Le terme "chaos'' définit un état particulier d'un système dont le comportement ne se prédit pas. Il est dû au fait qu'ils sont très sensibles aux conditions initiales (comme les erreurs arrondies dans les calcules numériques), entraînant des résultats totalement différents pour de tels système, rendant en générale toute prédiction impossible à long terme [2].

Eduard Lorenz, un mathématicien du MIT (Massachusetts Institute of technology) est le père officiel de la théorie du chaos. Il a simplifié les équations composant les modèles extrêmement compliqués qui décrivent l'atmosphère afin de mettre en évidence la sensibilité aux conditions initiales.

Actuellement cette théorie est utilisée dans de très nombreux domaines : la météorologie, la sociologie, la physique, l'informatique, l'ingénierie, l'économie et la biologie…etc.

- Historique du chaos

Le tableau suivant retrace les moments forts de l'évolution de la théorie du chaos.

1890	Henri Poincaré gagne le premier prix du roi Oscar II, étant le plus proche à résoudre le problème de n-corps des orbites des corps célestes. Il a découvert que l'orbite de trois corps célestes agissant l'un sur l'autre peut engendrer un comportement instable et imprévisible. c'est ici que le chaos est né
1963	Edward Lorenz découvre qu'un simple ensemble de trois équations non linéaires peut donner lieu à des trajectoires complètement chaotiques. Ainsi, il a mis en évidence un des premiers exemples du chaos déterministe.
1975	Le terme « chaos » a été introduit pour la première fois par tien-Yien Li et James A.Yorke
1978	Mitchell Feigenbaum introduit un nombre universel associé au chaos

1990	-Edward Ott, James A.Yorke et Celso Grebogi, introduisent la notion du contrôle de chaos. -Picora et Carroll : synchronisation des systèmes chaotiques

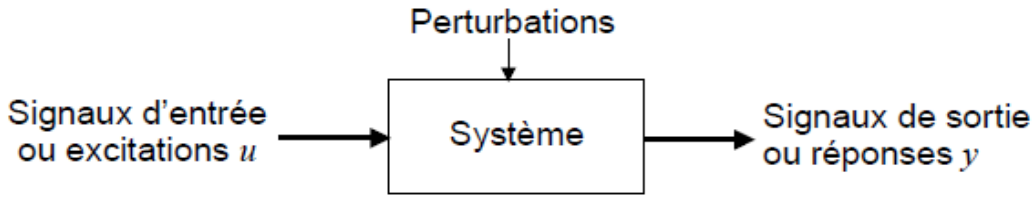
Tableau (1.1) : Historique du chaos

I.2 Définitions

I.2.1 Définition d'un système

Un système est un ensemble d'objets interagissant entre eux pour réaliser une fonction donnée. Il est connecté à son monde extérieure à travers :

- **Ses entrées**
  - **Signaux d'excitation :** actions envoyées au système.
  - **Perturbations:** qui sont en générale imprévisibles.
- **Ses sorties :** réponse du système aux signaux d'entrée [4].



Figure(I.1) : Schéma d'un système soumis à une perturbation.

I.2.2 Système non-linéaire

Un système dynamique peut être représenté par un ensemble de variables, qui évoluent dans le temps. Ces variables peuvent être destinées pour l'étude des fonctions d'état d'un phénomène ou d'un objet quelconque.

Un système est non linéaire s'il ne vérifie pas le principe de superposition. Les conditions de proportionnalité et d'additivité ne s'appliquent plus aux systèmes non linéaires.

I.2.3 Systèmes dynamiques

Mathématiquement un système dynamique est représenté par un ensemble de variables, qui évoluent au cours du temps. Il peut avoir une composante discrète ou continue.

On appelle système en temps continu tout système modélisé mathématiquement par un système d'équations différentielles, alors qu'en temps discret on parle d'équations aux différences finies.

Les systèmes dynamiques sont classés en deux catégories :

- **En temps continu**

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

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

- **En temps discret**

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

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

Où : $\mathbb{R}^n \rightarrow \mathbb{R}^n \times \mathbb{Z}^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système en temps discret

I.2.4 Système déterministe

On dit d'un système qu'il est déterministe si en connaissant l'état du système à un instant donné, on est, en mesure de prévoir son état à un instant ultérieur. Autrement dit un système est déterministe lorsque il est possible de calculer son évolution au cours du temps.

Dans un système dynamique, des conditions initiales identiques conduisent à des évolutions identiques [5].

I.2.5 Déterminisme et imprévisibilité

Chaque condition initiale détermine entièrement l'évolution future car il n'y a pas de hasard; le système est déterministe. Cependant, deux conditions initiales très proches peuvent avoir des évolutions complètement différentes.

L'évolution du système devient alors imprévisible car une petite erreur de mesure ou un simple arrondi conduit à des résultats complètement faux au bout d'un certain temps. C'est le chaos déterministe.

A long terme, on ne peut pas savoir approximativement, quelle sera la valeur d'un système chaotique, par contre, on peut étudier le système d'un point de vue statique [6].

I.2.6 Le principe de causalité

Les signaux temporels possèdent une propriété essentielle sur laquelle nous aurons l'occasion de revenir à maintes reprises: un effet ne pouvant survenir qu'après la cause qu'il lui a donné naissance, la réponse temporelle d'un système ne peut en aucun cas précéder la sollicitation qui en est la cause. Il s'agit du principe de causalité [9].

I.2.7 Espace de phase

Il s'agit d'un espace de dimensions 2 ou 3 dans lequel chaque coordonnée est une variable d'état du système considéré. Il permet d'obtenir toutes les composantes d'un système dynamique en une seule image [9].

I.2.8 attracteurs étranges

Un attracteur est la synthèse graphique d'un objet géométrique vers lequel tendent toutes les trajectoires de l'espace. L'attracteur traduit fidèlement les mouvements d'un objet c'est-à-dire sa vitesse et sa position et il caractérise l'évolution d'un système dynamique à long terme.

Il en existe quatre types distincts :

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

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

I.3 Le chaos

Il existe plusieurs définitions possibles du chaos. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant aussi le chaos.

Le chaos est un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Il est caractérisé par une évolution qui semble aléatoire et une extrême sensibilité aux conditions initiales, ce qui le rend imprédictible à long terme [7].

I.4 Propriétés des systèmes chaotiques

I.4.1 Sensibilité aux conditions initiales

La notion de **'**sensibilité aux conditions initiales**'** est l'une des propriétés essentielle du chaos. la plupart des systèmes chaotiques exhibent la sensibilité aux conditions initiales, pour deux conditions très voisines initialement; les deux trajectoires correspondantes à ces données initiales divergent exponentiellement, pour suite les deux trajectoires sont incomparables [6].

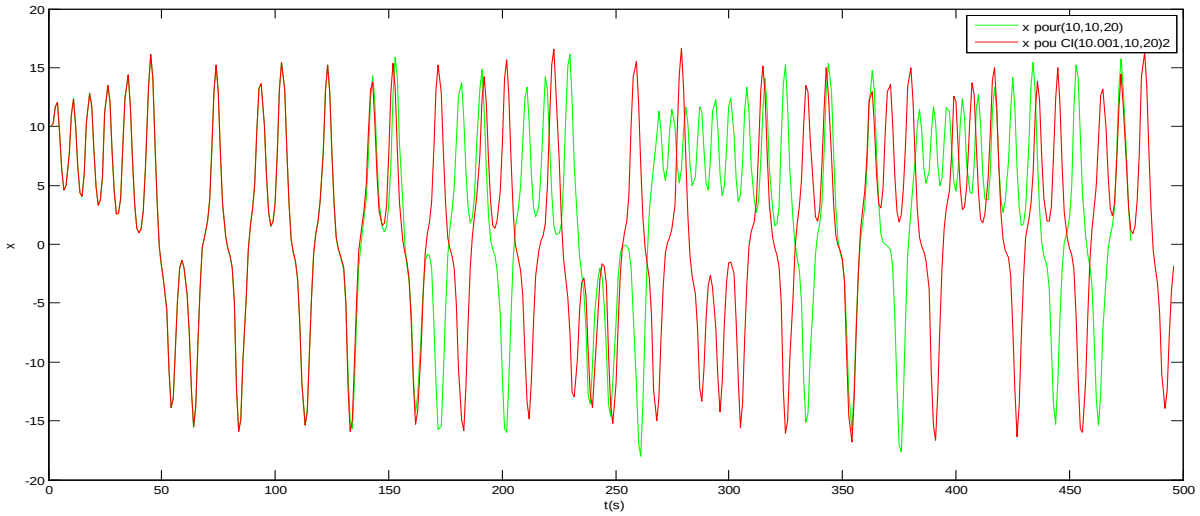
Pour illustrer cette propriété, on prend comme exemple le système de Lorenz

$$\begin{cases} \dot{x} = ay - ax \\ \dot{y} = -xz + by - y \\ \dot{z} = xy - cz \end{cases} \qquad (\mathbf{I.3})$$

Pour deux conditions initiales très proches :

$(x_0,\ y_0, z_0)$ = (10; 10; 20) et $(x_0^{'}, y_0^{'}, z_0^{'}) = (10.001 ; 10 ; 20)$

La simulation sur Matlab a donné les trajectoires de la figure suivante

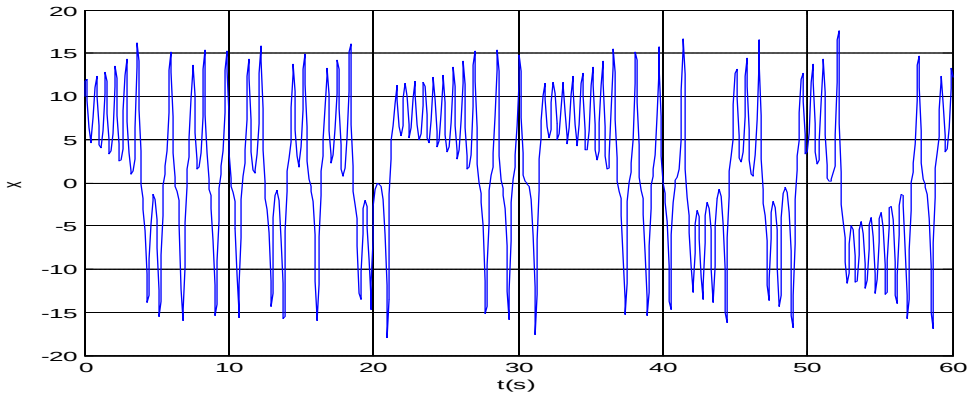


Figure(I.2) : Evolution dans le temps pour deux conditions initiales très proche pour l'état x(t) du système de Lorenz

I.4.2 Aspect aléatoire

La courbe précédente **Figure(I.1)** illustre la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur cette dernière. En effet, un système chaotiques évolue d'une manière qui semble aléatoire et son évolution est complexe, non périodique et non prédictible [9].

La figure (I.2) illustre l'aspect aléatoire des états du système **(I.3).**



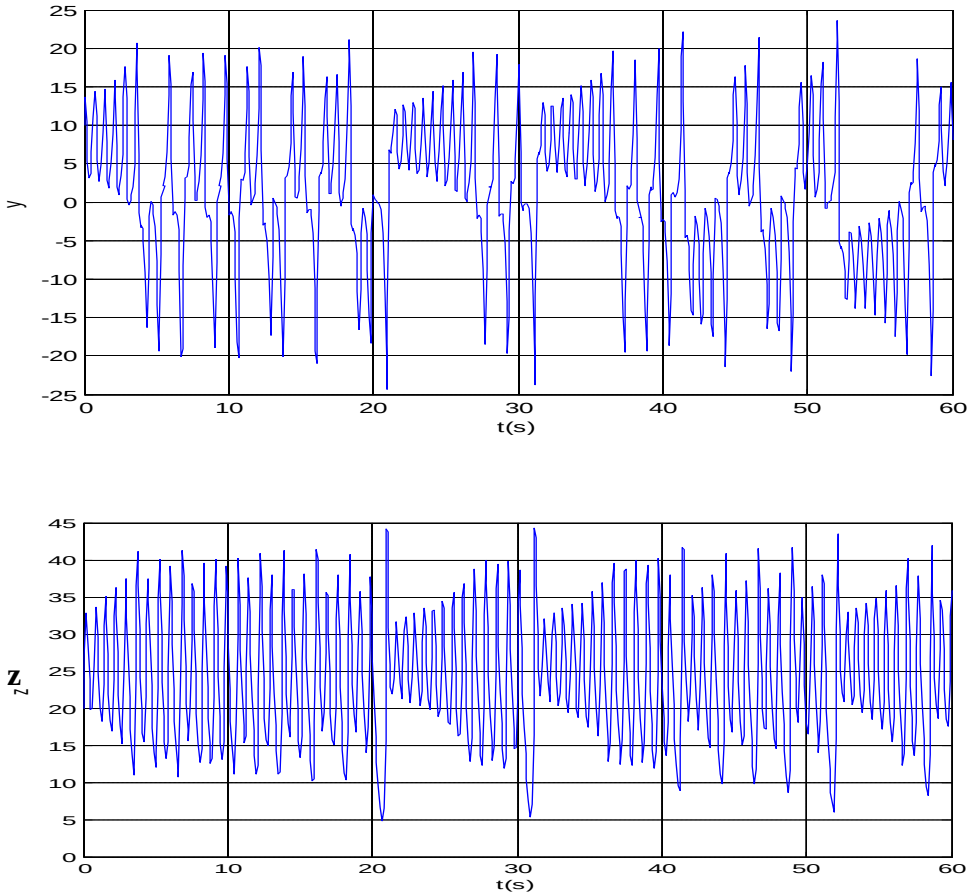


Figure (I.3) : Aspect aléatoire du système de Lorenz

I.4.3 Attracteur étrange

Une des découvertes les plus spectaculaires des dernières années a été celle des attracteurs étranges, ces objets géométriques issus de l'évolution des systèmes chaotiques. Dans le plan, ils sont formés d'une suite infinie de points x_0, x_1, x_2, $x_3 \ldots x_n$ qui dépendent de x_0 la valeur initiale. Au fur et à mesure que le nombre de points augmente, une image se forme dans le plan et devient de plus en plus net. Cette image n'est pas une courbe ni une surface, c'est en fait un objet intermédiaire constitué d'un ensemble dense de points. L'objet est qualifié d'étrange en raison de sa nature fractale [21].

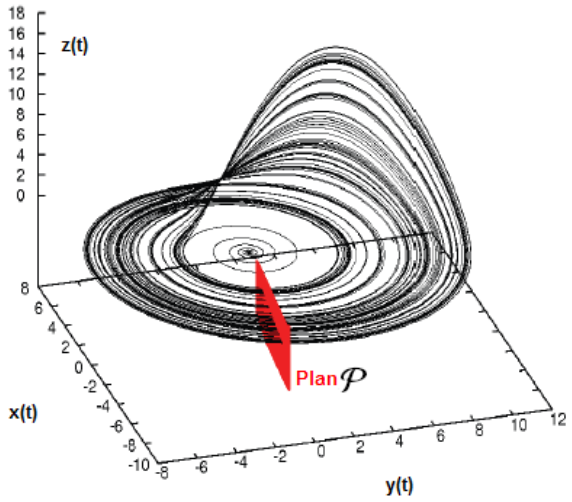
I.4.4 Section de Poincaré

Henri Poincaré a apporté une contribution très utile pour l'étude des systèmes chaotiques. Parmi ces contributions on trouve les sections de Poincaré.

Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases, afin d'étudier les interactions de cette trajectoire, par exemple en dimension 3 on passe d'un système à temps continu à un système a temps discret. Les mathématiciens ont bien sûr démontré que les propriétés du système sont conservées après la réalisation d'une section de Poincaré [9].

La section de Poincaré la plus naïve est de couper la trajectoire dans l'espace de phase pour un plan (en dimension trois) ou par une droite (en dimension deux).

Exemple : Coupe de Poincaré en dimension trois sur l'attracteur de Rössler.



Figure(I.4) : Coupe de Poincaré en dimension trois sur l'attracteur de Rössler.

I.4.5 Exposant de Lyapunov

Les exposants de Lyapunov sont des coefficients qui permettent de mesurer la sensibilité aux conditions initiales d'une série temporelle. Par définition, un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoire de l'espace de phase.

Le calcul des exposants de Lyapunov se fait par l'équation suivante :

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} ln\left|\acute{f}(x_{i-1})\right| \qquad (\mathbf{I.4})$$

L'approximation du chaos exige que les exposants de Lyapunov doivent remplir trois conditions.

- Au moins l'un deux est positif pour expliquer la divergence des trajectoires.
- Au moins l'un deux est négatif pour justifier le remplier des trajectoires.
- La somme de tous les exposants est négative pour expliquer qu'un système chaotique est dissipatif c'est-à- dire qu'il perd de l'énergie [10].

Etat	Attracteur	Dimension	Exposant de Lyapunov
Point d'équilibre	Point	0	$\lambda_n \le .... \le \lambda_1 \le 0$
Périodique	Cercle	1	$\lambda_1 = 0$ $\lambda_n \le .... \le \lambda_2 \le 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \le .... \le \lambda_3 \le 0$
Période d'ordre k	K-Tore	K	$\lambda_1 = ... = \lambda_k = 0$ $\lambda_n \le .... \le \lambda_{k+1} \le 0$
Chaotique	Attracteur chaotique	Non entière	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyper chaotique	Attracteur chaotique	Non entière	$\lambda_1 > 0$ $\lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tableau (1.2) : Exposants de Lyapunov et dimensions.

I.4.6 Dimension de Lyapunov

Paramètre permettant de mesurer la dimension du chaos. Suivant le type de chaos généré, la dimension de Lyapunov est plus ou moins grande pour des systèmes non retardés (dimension finie) tels que les systèmes de Lorenz ou Rössler, la dimension de Lyapunov est au maximum égale au nombre de variables du système (dimension faible), alors que pour les systèmes à retard (dimension infinie) la dimension de Lyapunov tend vers de grandes valeurs. Plus la dimension est grande, plus la complexité du chaos est élevée [14].

Classons les exposants de Lyapunov $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_j$.

La dimension de Lyapunov D_l est définie par :

$$D_j = j + \frac{\sum_{i=1}^{j} \lambda_i}{\lambda_{j+1}} \qquad \textbf{(I.5)}$$

Où j est le plus grand entier qui satisfait

$$\lambda_1 + \lambda_2 + \lambda_3 + \ \ldots\ldots\ldots + \lambda_j \geq 0$$

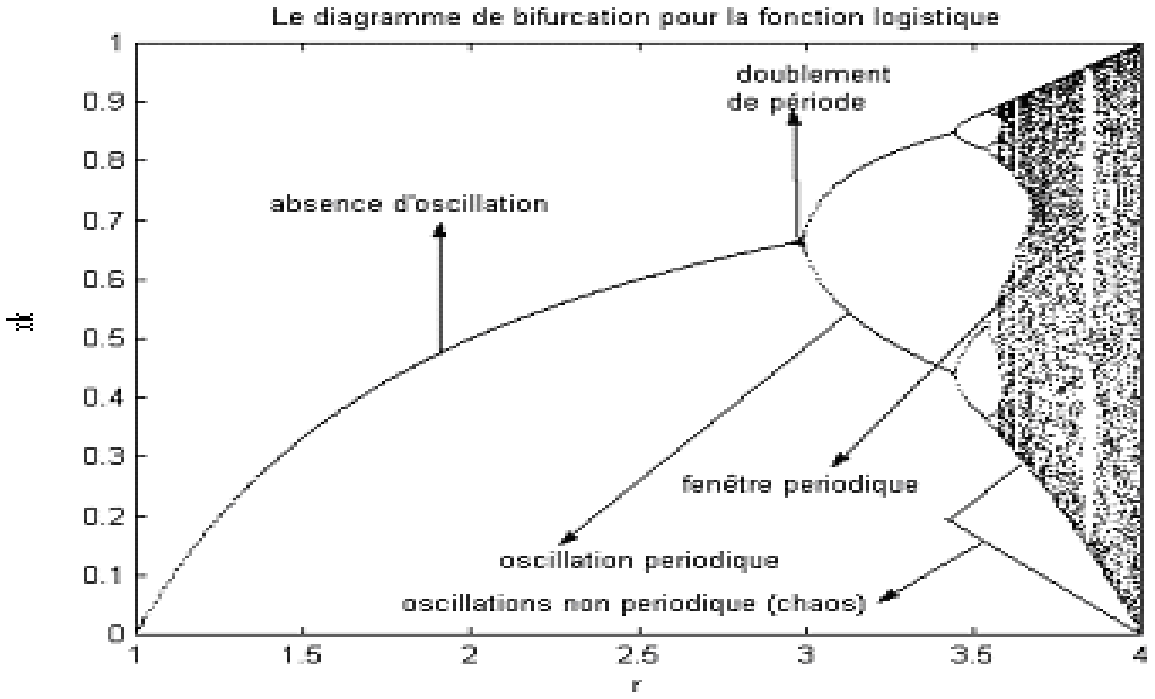
I.4.7 Bifurcation

Les systèmes que nous considérons sont en général fonctions des paramètres de contrôle. Un point de bifurcation est un point de l'espace de contrôle où le portrait de phase du système Change de façon quantitative mais ne modifie pas le comportement (état stationnaire) du système.

Le diagramme de bifurcation est un tracé repérant la nature des différentes solutions du système et leur stabilité lorsqu'un paramètre varie.

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

$$f : [0\ ,1] \rightarrow [0\ ,\ 1] \quad x_{k+1} = f(x_k) = \mathrm{r}x_k - \mathrm{r}x_k^2 \qquad \textbf{(I.6)}$$



Figure(I.5) : Diagramme de bifurcation de la fonction logistique.

I.4.8 Les routes vers le chaos

On ne sait pas à l'heure actuelle sous quelles conditions un système devient chaotique. Cependant il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Supposons que la dynamique étudiée dépende d'un paramètre de Contrôle. Lorsqu'on varie ce paramètre, le système peut passer d'un état stationnaire à un état périodique, puis au-delà d'un certain seuil, suivre un scénario de transition et devenir chaotique [10].

Nous allons en exposer brièvement trois types d'évolution possibles.

1. Le doublement de période :

Ce scénario de transition vers le chaos est sans doute le plus connu. Par augmentation d'un paramètre, la fréquence double, puis est multipliée par 4, par 8, par 16..etc.

Le doublement étant de plus en plus rapproché.

On tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie, c'est à ce moment que le système devient chaotique [10].

2. Intermittence :

Ce deuxième scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.

Le système conserve pendant ce mouvement un régime pratiquement quasi-périodique et il se stabilise brutalement pour donner lieu à un comportement chaotique [4].

3. Quasi-périodique

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

I.5 Exemples de systèmes chaotiques

Dans cette partie, nous exposons les exemples les plus étudié des systèmes chaotiques.

I.5.1 Systèmes à temps continu

Les systèmes considérés sont :

I.5.1.1 Système de Lorenz

Le système de Lorenz est un exemple célèbre des systèmes différentiels au comportement chaotique, pour certaines valeurs des paramètres.

Ce système est défini par les équations suivantes [9].

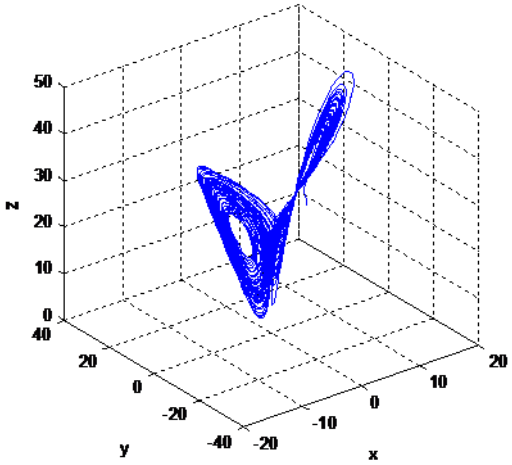
$$\begin{cases} \dot{x} = ay - ax \\ \dot{y} = -xz + by - y \\ \dot{z} = xy - cz \end{cases} \qquad (\mathbf{I.7})$$

Avec : (x, y, z) le vecteur d'état

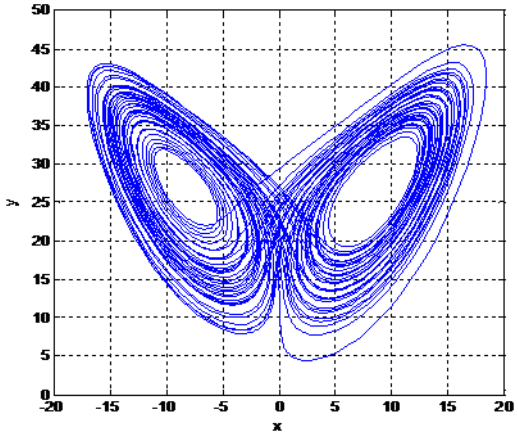
a=10, b=28, c=8/3

b : est un paramètre de contrôle

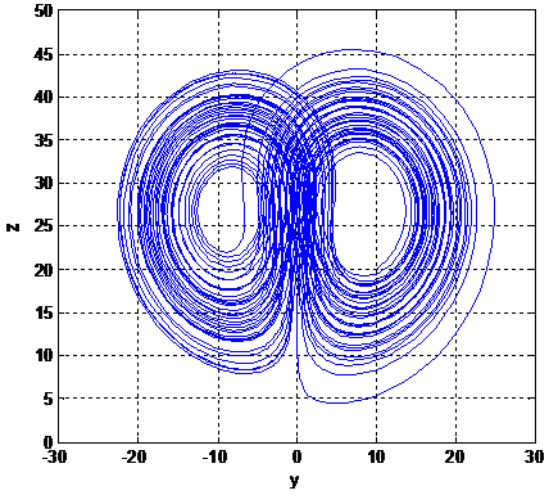
La figure ci-dessous illustre l'attracteur de Lorenz et est obtenu à partir des valeurs numériques suivantes (a=10; b=28; c=8/3) et (x(0)=10.001, y(0)=10, z(0)=20).



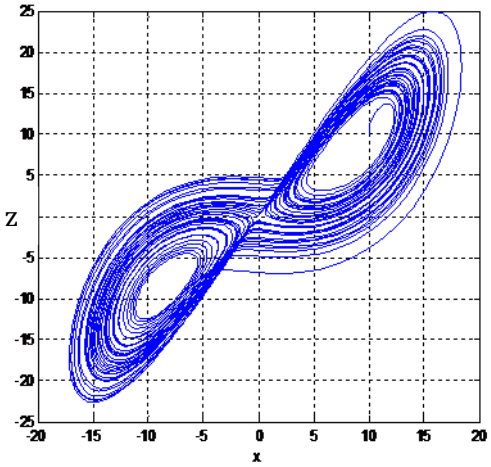
Attracteur en 3 dimensions (x, y, z)



Attracteur en 2 dimensions (x, y)



Attracteur en 2 dimensions (y, z)



Attracteur en 2 dimensions (x, z)

Figure (I.6) : Evolution de l'attracteur de Lorenz en 2 et 3 dimensions.

I.5.1.2 Système de Rössler

Le système de Rössler proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides, Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à

la suite des travaux en cinétique chimique. Ce système est défini par les équations suivantes [10].

$$\begin{cases} \dot{x}(t) = -y - z \\ \dot{y}(t) = x + ay \\ \dot{z}(t) = b - cz + xy \end{cases} \quad \textbf{(I.8)}$$

Avec : a, b, c des constantes

Pour une simulation numérique, nous proposons :

(a=0.398; b=2 ;c=4)

Nous obtenons l'attracteur de Rössler dans la figure ci-dessous

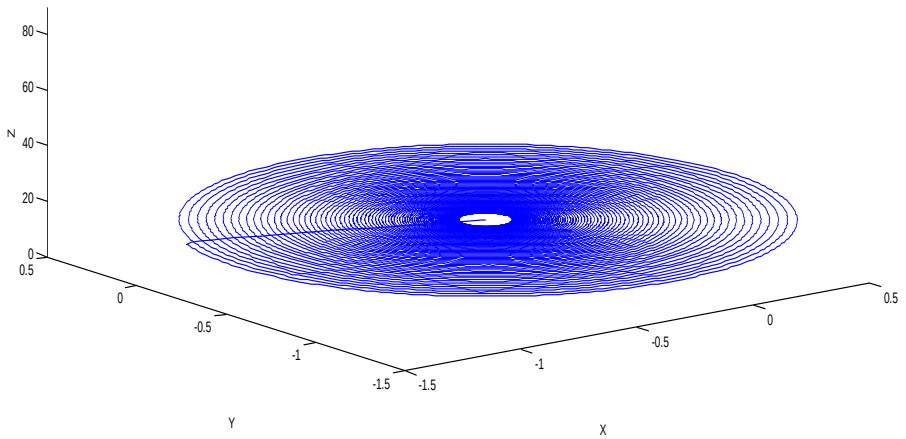


Figure (I.7) : Attracteur étrange de Rössler**.**

I.5.2 Systèmes a temps discret

I.5.2.1 Système de Hénon

Le système de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. L'attracteur est défini par le système d'équations suivant, où **a** et **b** sont des constantes [13].

$$\begin{cases} x_{k+1} = a - x_k^2 + b y_k \\ y_{k+1} = x_k \end{cases} \qquad \textbf{(I.9)}$$

Avec : k est le nombre d'itérations.

a=1.4 ; b=0.3 et(x(0)=1, y(0))=1, Le portrait de phase (l'attracteur) du système est représenté par la **Figure (I.7)** ainsi que les **Figures (I.8) (I.9)** qui montrent la trajectoire de x, y en discret.

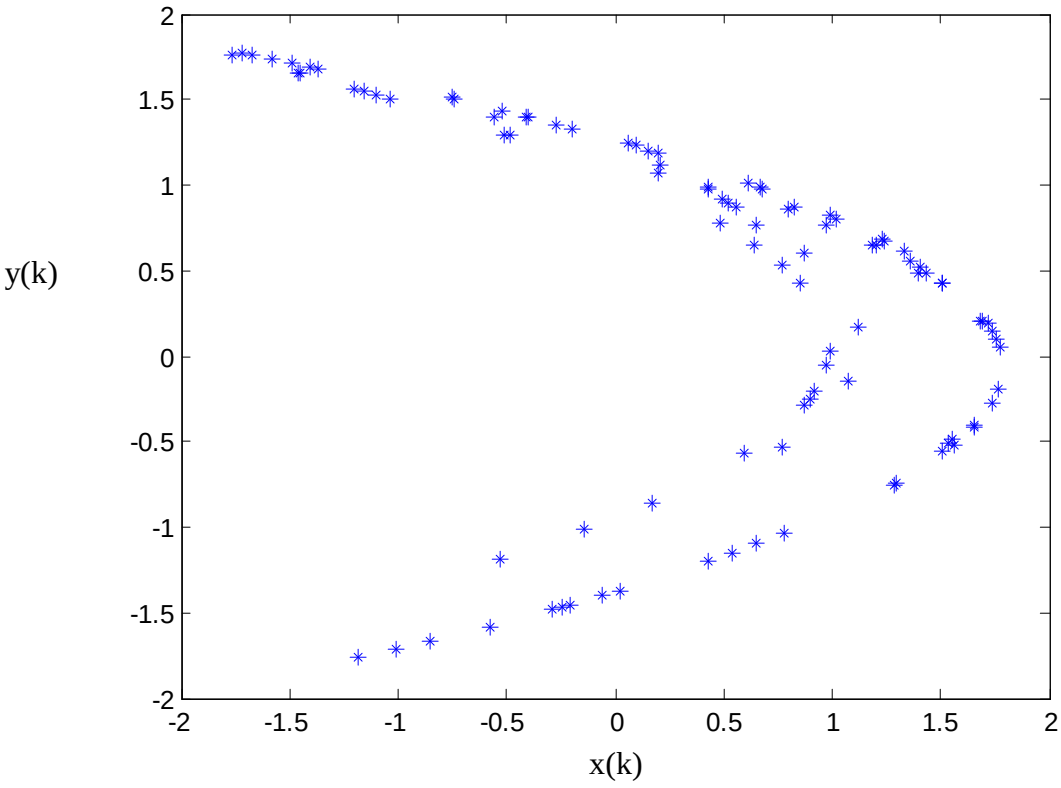


Figure (I.8) : Attracteur étrange de Hénon

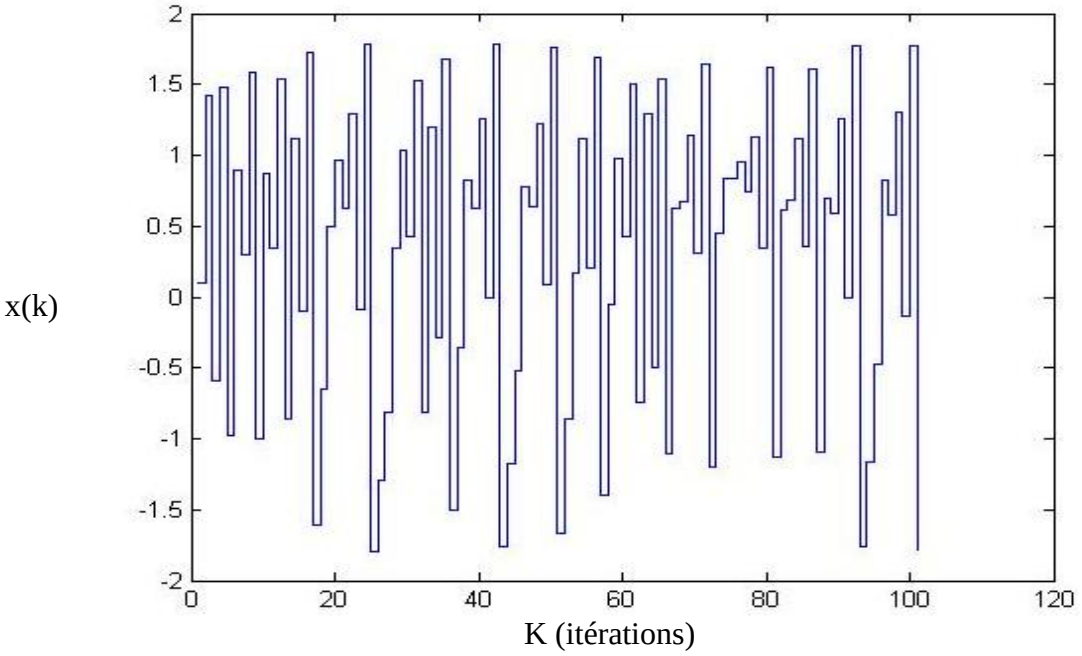


Figure (I.9) : Evolution aléatoire de x(k) du système de Hénon

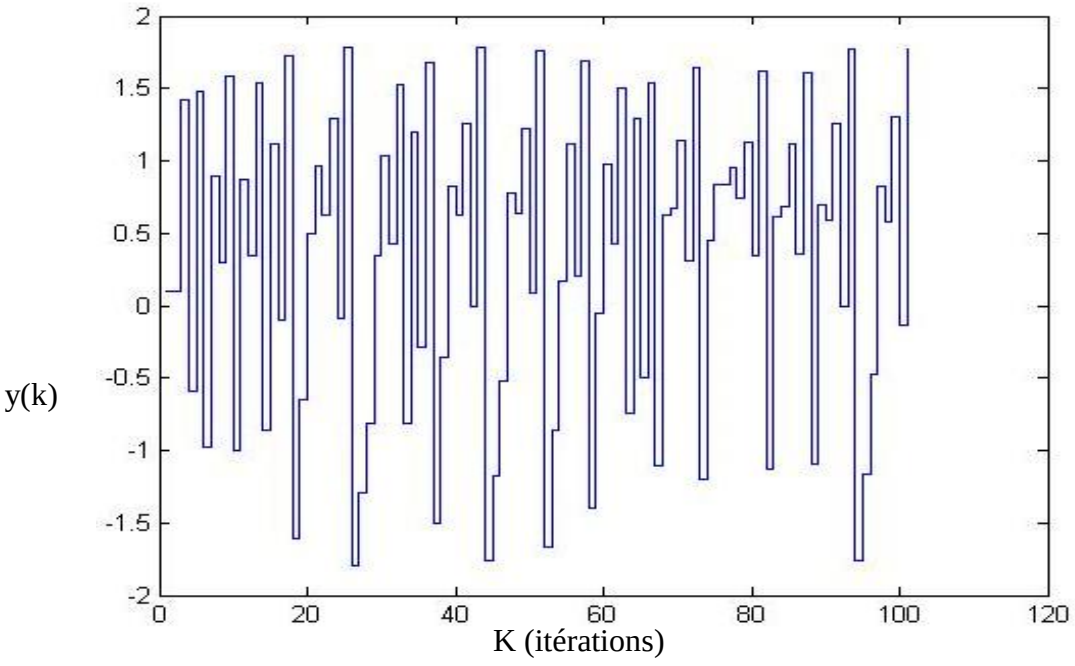


Figure (I.10) : Evolution aléatoire de y(k) du système de Hénon.

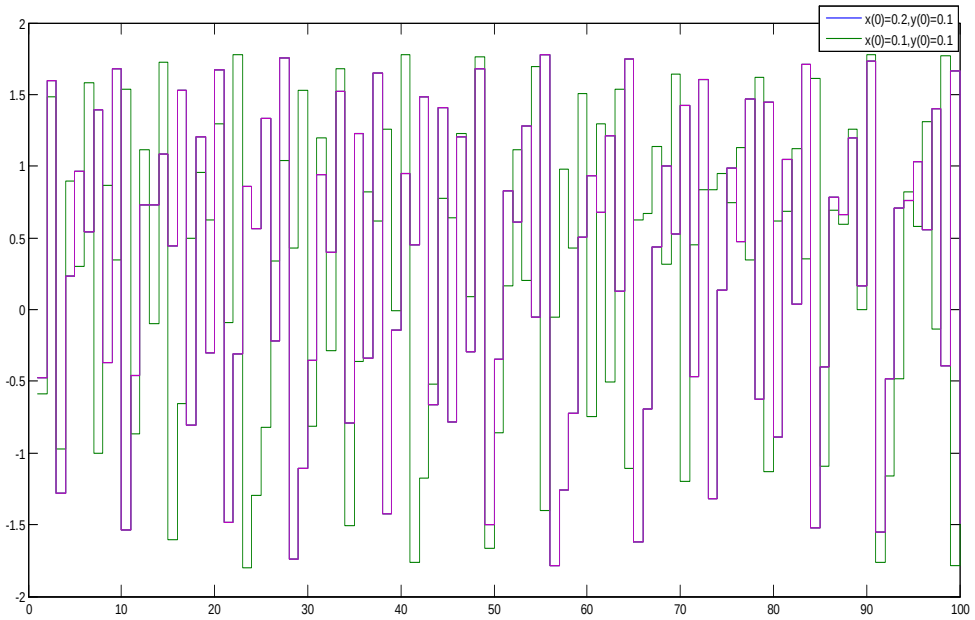


Figure (I.11) : Illustration de la sensibilité aux conditions initiales du système de Hénon.

I.6 Conclusion

Dans ce chapitre nous avons présenté les notions de base des systèmes chaotiques. Nous avons ainsi introduit quelques exemples des systèmes chaotiques très connus, comme le système de Lorenz et de Rössler. Par la suite nous avons discuté les propriétés importantes qui caractérisent le chaos telle que : La sensibilité aux conditions initiales, L'attracteur étrange, les exposants de Lyapunov…etc.

Le prochain chapitre sera consacré à la synchronisation du chaos et son application dans la transmission cryptée d'informations.

Chapitre II:

Transmission sécurisée à bas du chaos

II.1 Introduction

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des transferts de données. Il est donc nécessaire de développer un outil efficace de protection des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences [9].

1990, Picora et Carroll présentent une démonstration théorique et expérimentale de la possibilité de synchroniser deux systèmes chaotiques. Ici, la synchronisation signifie que deux systèmes chaotiques ayant la même structure avec des conditions initiales différentes sont amenés à reproduire le même signal chaotique.

De nombreux travaux utilisant le chaos ont été présentés ces dernières années dans le contexte des télécommunications. En effet, leurs caractéristiques, sensibilités aux conditions initiales, aspects aléatoires et spectres continus large bande, sont bien adaptées aux transmissions sécurisées.

Ce chapitre est organisé de la manière suivante ; dans la première partie du chapitre nous présenterons le concept de la synchronisation du chaos, dans la deuxième partie nous exposerons les principales méthodes utilisant des Systèmes chaotiques pour la communication.

II.2 Synchronisation des systèmes chaotiques

II.2.1 Définition

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre. Ce concept repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable.

Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante, Si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme

"Couplage'', les deux systèmes finiront par céder la place à un comportement commun, ils finiront par se synchroniser [12].

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

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

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

Les deux systèmes sont synchronisés si :

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

Avec :

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

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

II.2.2 Méthodes de synchronisation

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

II.2.2.1 Synchronisation par bouclage

La méthode de synchronisation par bouclage illustrée à la figure(II.1) utilise l'erreur entre les deux systèmes afin de corriger le comportement du récepteur et ainsi obtenir la synchronisation.

Supposons que l'émetteur s'écrit comme suit :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \quad \textbf{(II.3)}$$

Et que le récepteur peut être décrit comme suit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad \textbf{(II.4)}$$

Avec g une fonction de l'erreur entre y et $\hat{y}$

Cette fonction est choisie pour garantir la synchronisation entre l'émetteur et le récepteur.

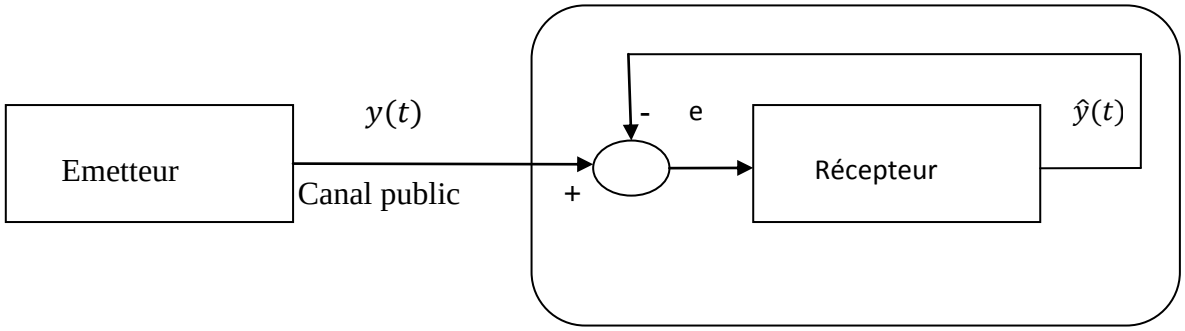


Figure (II.1) : Synchronisation par bouclage

II.2.2.2 Synchronisation identique ou approche de Pecora et Carroll

Pour illustrer la méthode de synchronisation par couplage entre deux systèmes Chaotiques, on a choisi de présenter la synchronisation identique proposée par Picora et Carroll [21].

L'idée consiste à diviser le système d'origine en deux sous-systèmes, l'un maître et l'autre esclave de telle sorte que les variables dynamiques de départ soient reparties de part et d'autre de chacun des sous-systèmes. Il s'agit ensuite de reproduire les sous systèmes à l'identique et de les mettre en cascade. Le signal issu du signal de départ (système maître) sert à piloter (synchroniser) le premier des deux systèmes dupliqués mis en cascade, qui lui-même permet de synchroniser le second sous-système dupliqué [3].

Considérons un système dynamique autonome, en temps continu de dimension *n* représenté par la relation suivante :

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

Où $x = [x_1, x_2, \ldots\ldots\ldots\ldots x_n]^T$ est le vecteur d'état.

.Par la suite on divise le système initial en deux sous-systèmes {S1, S2}.

$$\begin{cases} S_1 = \dot{x}^{\{1\}} = f^{\{1\}}(x^{\{1\}}(t), x^{\{2\}}) \\ S_2 = \dot{x}^{\{2\}} = f_2(x^{\{1\}}(t), x^{\{2\}}) \end{cases} \qquad \textbf{(II .6)}$$

On considère maintenant un sous-système S(21) caractérisé par une dynamique identique que S_2 dont l'entrée est x_1.

$$S(21) = \hat{\dot{x}}^{\{2\}} = f^{\{2\}}(x^{\{1\}},\ \hat{x}^{\{2\}}) \qquad \textbf{(II.7)}$$

On peut dire que ce sous-système réplique S(21) est un candidat susceptible de se synchroniser avec la dynamique complète initiale.

Pour que cette proposition soit vraie et que le sous système S(21) soit stable, il faut que l'ensemble des coefficients de Lyapunov de ce sous-système soient négatifs.

Dans la **figure (II.2)**, on représente graphiquement le processus de décomposition en sous-système.

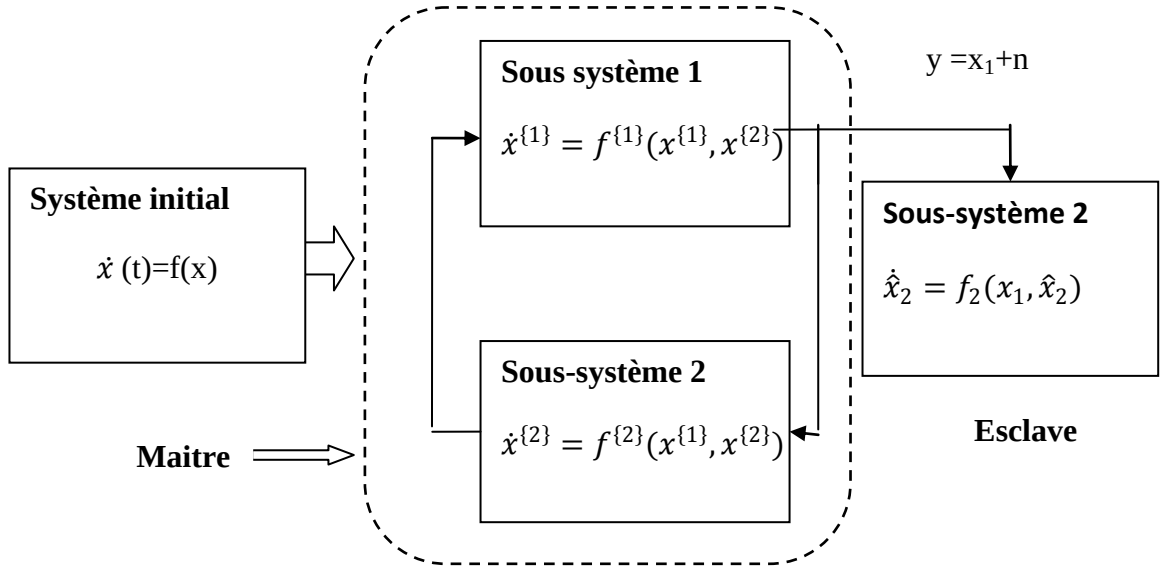
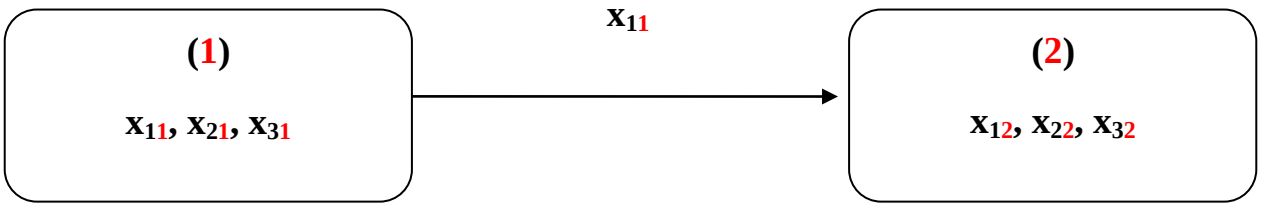


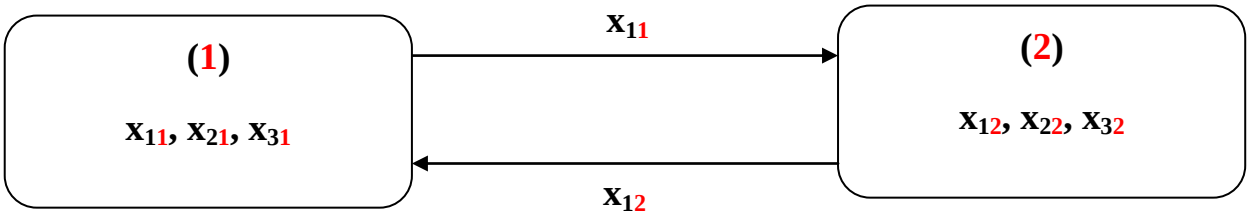
Figure (II.2) : Synchronisation maitre-esclave en utilisant la décomposition en sous-système

II.2.2.3 Synchronisation par couplage

Il est possible de coupler deux systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel). Dans le cas d'une synchronisation unidirectionnelle, le couplage entre les deux systèmes chaotique est réalisé à l'aide d'un élément fonctionnant dans un seul sens. Par contre, dans le cas de la synchronisation bidirectionnelle, le couplage est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, les deux types de couplages peuvent être appliqués pour des systèmes non identiques [3].



a : Couplage unidirectionnel



b : Couplage bidirectionnel

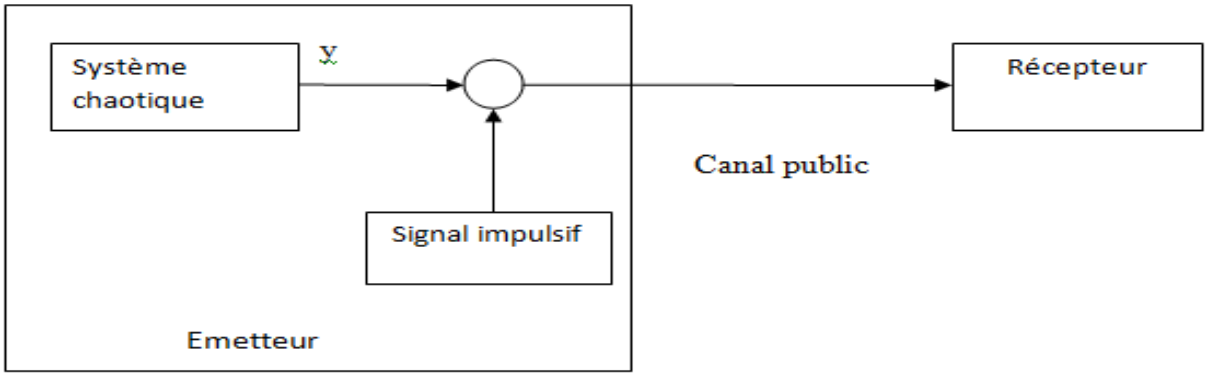
Figure (II.3) : Synchronisation par couplage

II.2.2.4 Synchronisation impulsive

Lorsque deux systèmes communiquent usuellement, le premier système dynamique (émetteur) transmis un état afin de pouvoir réaliser une synchronisation avec le second (récepteur).

La synchronisation impulsive à été proposée, **Figure (II.4),** Afin de réduire la redondance du signal transmis (rapport signal/bruit). Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système subit des changements soudains.

On considère le signal maitre défini par $\dot{x} = f(x(t))$, et on définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal y(t) est envoyé par le système maitre au système esclave, un changement dont les variables d'état subissent un saut et un changement d'état [20].



Figure(II.4) : Principe de la synchronisation impulsive

Cette technique assure la synchronisation de systèmes chaotiques en utilisant de simples impulsions, elle est appliquée dans plusieurs systèmes de communication basés sur le chaos puisqu'elle garantit une bonne performance pour la condition de synchronisation.

Cette méthode serra mieux développé et discuté par la suite pour être appliquée à la réalisation d'un système de transmission sécurisée.

II.2.2.5 Synchronisation généralisée

En générale**,** c'est quand il existe une différence entre les systèmes couplés c'est-à-dire quand on trouve un obstacle pour une réalisation pratique d'un sous système esclave purement identique à un autre sous système issu d'une décomposition d'un système maître.

La méthode généralisée est proposée afin de s'affranchir de cet obstacle, qui est une généralisation du concept de la synchronisation identique [19].

En conséquence les possibilités d'appliquer la synchronisation généralisée, peuvent être plus larges que la synchronisation identique, on dit que deux systèmes se synchronisent, au sens généralisé s'il existe une matrice M telle que :

$$\lim_{t\to\infty} \left\| \hat{x}(t) - Mx(t) \right\| = 0 \qquad \textbf{(II.8)}$$

Avec :

$x(t)$ **:** l'état du système émetteur

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

Séparément des conditions initiales, si M est inversible, alors $M^{-1}(\hat{x})$ fournit une estimation de l'état de x du système émetteur.

Dans le cas contraire, il serait impossible de fournir une estimation de l'état x du système récepteur, ceci présente alors un inconvénient majeur pour les techniques de communications utilisant l'état pour décrypter le message transmis.

II.2.2.6 Synchronisation retardée

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

$$\lim_{t\to\infty} \|\hat{x}(t) - x(t-\tau)\| = 0 \qquad \textbf{(II.9)}$$

Où x(t) est l'état du système maître, $\hat{x}$(t) est l'état du système récepteur et τ est un retard positif. Cette approche est utilisée pour les systèmes linéaires [5].

II.2.2.7 Synchronisation à l'aide d'observateur

La synchronisation peut être réalisée à l'aide d'un observateur

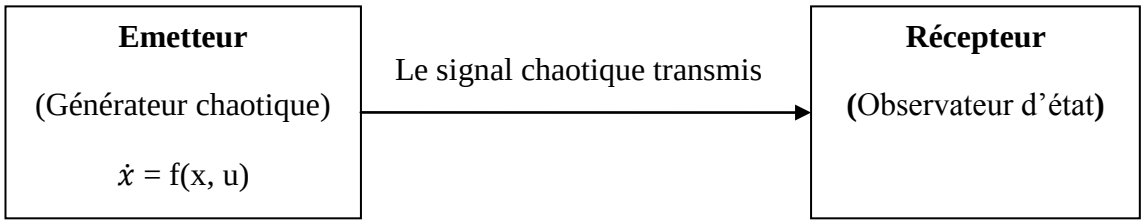


Figure (II.5) : Principe de la synchronisation à base d'observateur

Un système dynamique est dit observable si on peut récupérer toutes les grandeurs par une combinaison de mesures de ses sorties et leurs dérivées.

Si un changement quelconque est détecté dans le système [22], à partir des mesures qui sont disponibles, on dit que le système est observable.

La figure suivante montre le principe d'observateur.

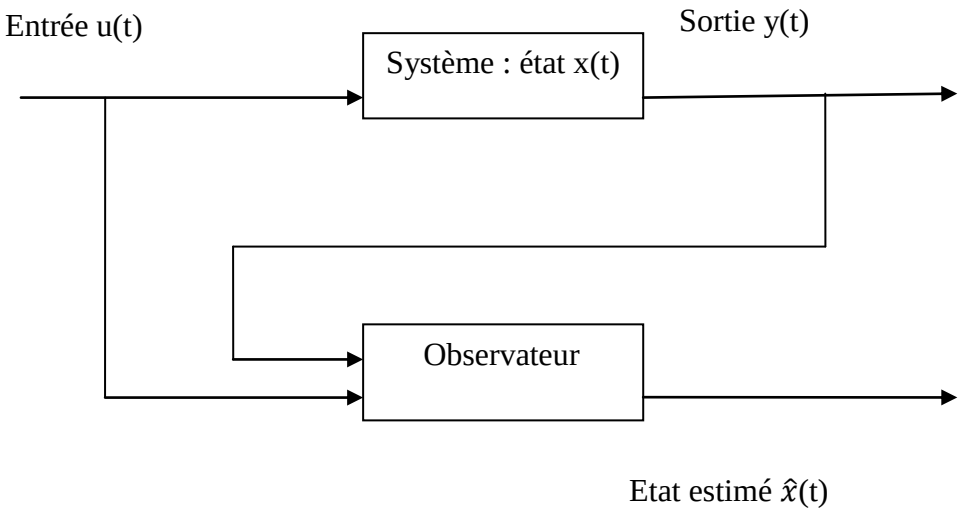


Figure (II.6) : Principe de l'observateur

Le problème de conception d'un système non linéaire donné est posé comme suit :

$|x(t) - \hat{x}(t)| \rightarrow 0$ quand $t \rightarrow \infty$ **(II.10)**

Où x(t) est l'état du système et $\hat{x}(t)$ l'état estimé.

A. Observabilité des systèmes non linéaires

A.1 Cas continu

Considérons le système non linéaire donné par la forme suivante.

$$\begin{cases} \dot{x}(t) = f(x) + g(x)u(t) \\ y(t) = h(x) \end{cases} \quad \textbf{(II.11)}$$

$x \in \mathbb{R}^n$ et $y \in \mathbb{R}^p$ représentent respectivement l'état de la sortie du système, f et h sont des vecteurs de dimensions appropriées.

- **Condition du rang d'observabilité**

Considérons le système **(II.11)**, on dit que la paire (f, h) est observable au sens du rang si la condition donnée par l'équation **(II.12)** est satisfaite. Il faut donc définir la dérivée de Lie, qui est une notion largement utilisée dans l'étude de l'observabilité des systèmes non linéaires.

$$rang(O) = Rang \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} = n \quad \textbf{(II.12)}$$

Où

$$O = Rang \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} \quad \textbf{(II.13)}$$

$L_f h$ Désigne la dérivée de Lie de h dans la direction de f

L'écriture de $dL_f^k h$ est donnée par le Co-vecteur

$$dL_f^k h = \left(\frac{\sigma L_f^k h}{\sigma x_1}, \frac{\sigma L_f^k h}{\sigma x_2}, \dots\dots\dots, \frac{\sigma L_f^k h}{\sigma x_n}\right) \quad \textbf{(II.14)}$$

A.2 Cas discret

Soit le système linéaire à temps discret donné par la forme suivante

$$\begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k = h(x_k) \end{cases} \quad \textbf{(II.15)}$$

Où $x_k \in \mathbb{R}^n, y_k \in \mathbb{R}^p$ et $u_k = (u_{1k}, u_{2k}, \dots\dots\dots, u_{mk})^T \in \mathbb{R}^m$.

Le système **(II.15)** est observable si :

Dim ($doh(x_0)$)= n

Avec n dimensions du système

- **Condition du rang d'observabilité**

Le système **(II.15)** est dit observable au sens du rang en $x_0 \in \mathbb{R}^n$ si span { dh, $d(foh)$, ... $d(f^{n-1}oh)$ } est de le rang n.

Exemple :

Observateur impulsif

Considérons le système suivant :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1, x_2, t) \\ \dot{x}_2(t) = f_2(x_1, x_2, t) \\ y(t_k) = x_1(t_k) \end{cases} \quad \textbf{(II.16)}$$

Avec : $x_1(t) \in \mathbb{R}^p, x_2(t) \in \mathbb{R}^{n-p}$ sont les états du système et $y(t_k) \in \mathbb{R}^p$ est le vecteur de sortie.

$$\begin{cases} \dot{\hat{x}}_1(t) = f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{\hat{x}}_2(t) = f_2(\hat{x}_1, \hat{x}_2, t) \\ \hat{y}_1(t_k^+) = x_1(t_k) \end{cases} \quad \textbf{(II.17)}$$

A partir des systèmes (II.16) et (II.17), on obtient le système d'erreur d'observation suivant :

$$\begin{cases} \dot{e}_1(t) = f_1(x_1, x_2, t) - f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{e}_2(t) = f_2(x_1, x_2, t) - f_2(\hat{x}_1, \hat{x}_2, t) \\ e_1(t_k^+) = 0 \end{cases} \quad \textbf{(II.18)}$$

B. Observabilité des systèmes linéaires

Une solution simple au problème de l'estimation de l'état des systèmes linéaires a été proposée par Luenberger dans le cadre déterministe.

Dans ce cas, On considère le modèle dynamique du système linéaire défini par :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Lw(t) \\ y(t) = Cx(t) + V(t) \end{cases} \quad (\textbf{II. 19})$$

Où $x(t) \in \mathbb{R}^n$, $\cup\ u(t) \subseteq \mathbb{R}^m$, $y(t) \in \mathbb{R}^p$,et $V(t) \in \mathbb{R}^r$, les matrices du système sont de dimensions appropriées.

Exemple :

Observateur de Luenberger

La théorie de l'observation du Luenberger repose essentiellement sur des techniques de placement de pôles on se place dans le cas déterministe, où les bruits w et v sont nuls.

Luenberger a proposé l'observateur suivant pour le système **(II.20)**.

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + k\,(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \quad \textbf{(II.20)}$$

Où $\hat{x}$(t) est l'estimé de x(t), $\hat{y}$(t) est l'estimé de y(t), la dynamique de l'erreur d'estimation e(t) = x(t) - $\hat{x}$(t) est représentée par l'expression :

$$\dot{e}(t)= (A-KC)\, e(t) \qquad \textbf{(II.21)}$$

L'évolution de l'état est corrigée grâce au modèle en fonction de l'écart entre la sortie mesurée et la sortie reconstruite par l'observateur $(y(t) - \hat{y}(t))$.

En utilisant une technique de placement de pôles, il suffit alors de choisir le gain k de l'observateur de telle sorte que la valeur propre de la matrice A-KC soit dans le demi-plan complexe gauche [17].

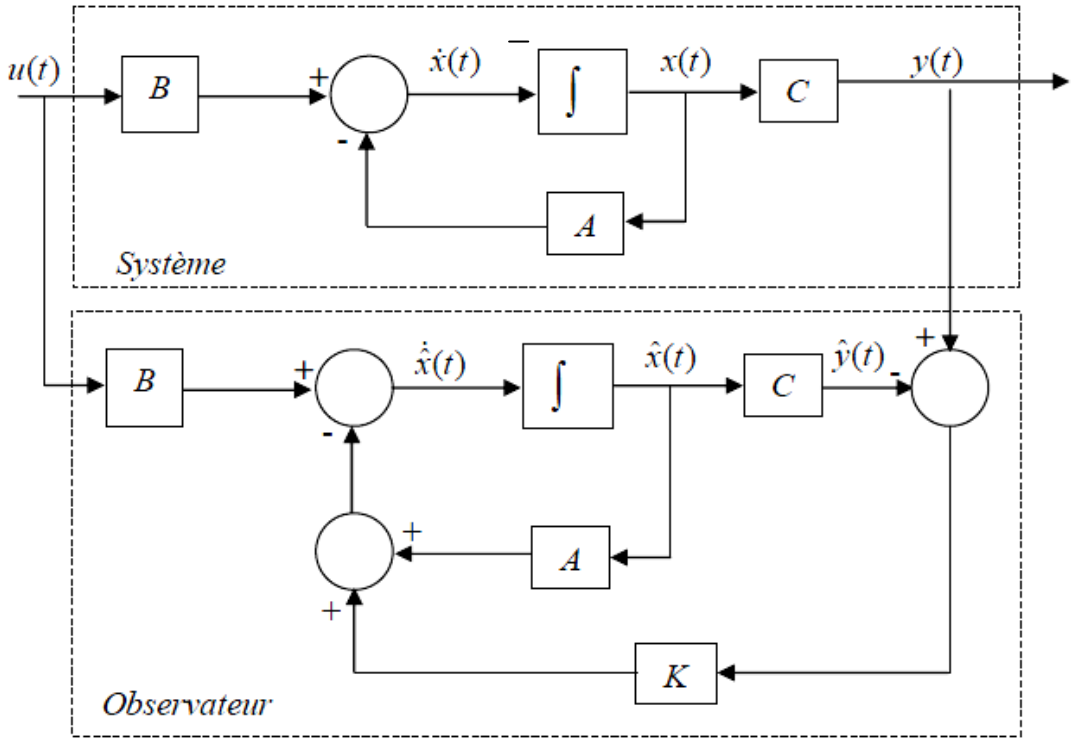


Figure (II.7) : Schéma structurel de l'observateur de Luenberger

II.3 Le chaos dans la transmission sécurisée :

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

Le principe de la cryptographie chaotique consiste à protéger le message en le transformant d'une manière à le rendre incompréhensible. Ce processus est appelé ‘‘chiffrement’’ ou ‘‘cryptage’’. Par ailleurs, le destinataire doit engager un processus appelé ‘‘déchiffrement’’ ou ‘‘décryptage’’ afin de reconstruire le message chiffré. Pour cela, des algorithmes sont utilisés, qui sont en effet des fonctions m

athématiques destinées au chiffrement et au déchiffrement du message. Et pour transmettre le message d'une manière sûre, un élément ‘‘clé’’ de cryptage est introduit, qui est utilisée par l'expéditeur et le destinataire. On distingue deux types de clés : clé ‘‘secrète’’ et clé ‘‘publique’’.

La cryptanalyse est l'étude des procédés cryptographiques dans le but de déterminer les éventuelles faiblesses des systèmes cryptographiques en étudiant les probabilités de succès des attaques, son principal objectif est de décrypter les textes chiffrés pour les rendre clairs [12].

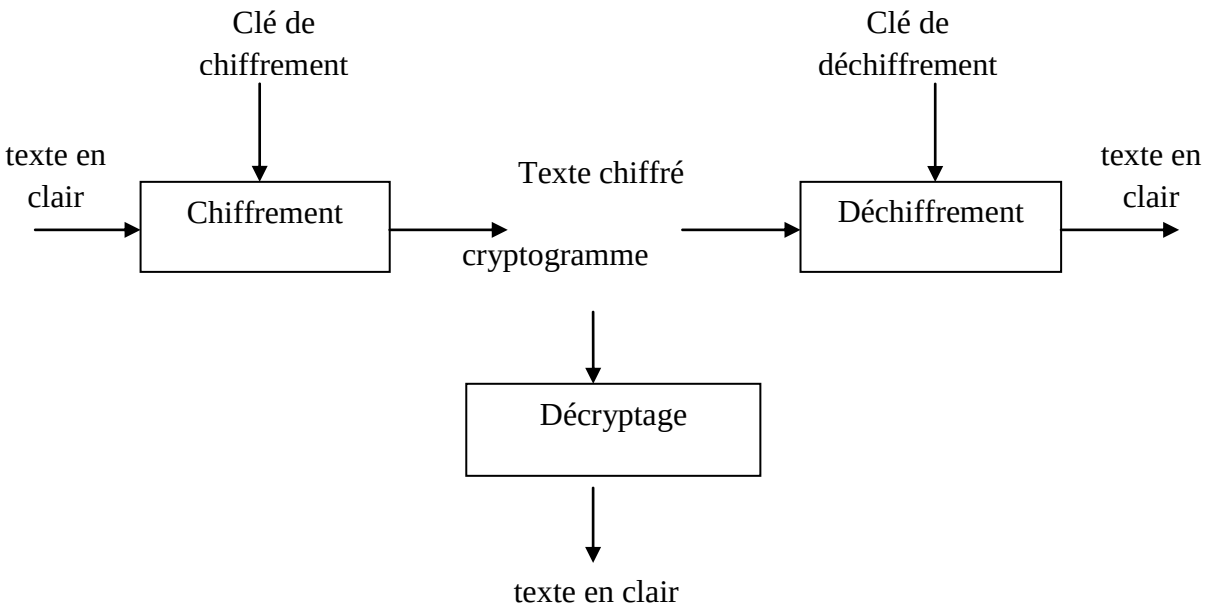


Figure (II.8) : Fondement de la transmission sécurisée à base du chaos

II.4 Méthodes de cryptage

La cryptographie par chaos, quant à elle, a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage. Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information [2].

Il existe plusieurs méthodes de cryptage, parmi ces dernières on peut citer :

II.4.1 Cryptage par addition :

Cette technique est considérée comme la première proposition d'utiliser le chaos pour sécuriser la communication [9]. L'émetteur est un système chaotique autonome dont le message m(t) est ajouté au signal y(t). La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal publique. Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction.

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

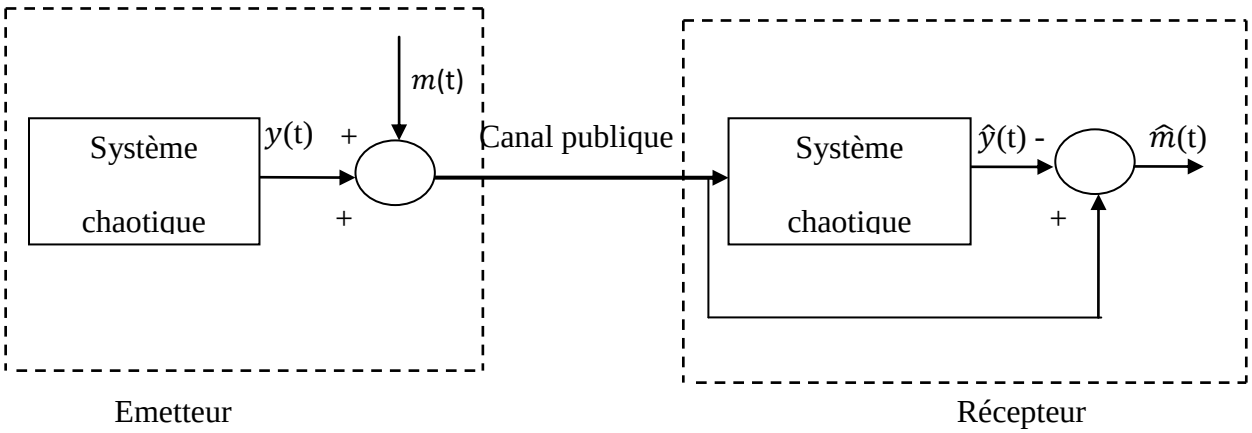


Figure (II.9) : Méthode de cryptage par addition

II.4.2 Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du coté de l'émetteur. Dans ce cas, la restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur [18].

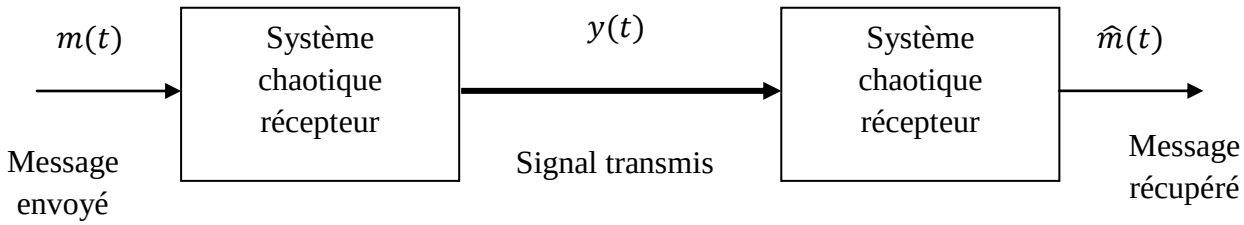


Figure (II.10) : Cryptage par inclusion

II.4.3 Cryptage par commutation

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la figure **(II.8)** ou une opération de commutation est employée selon la valeur du message binaire :

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

Du coté récepteur, il y'a deux sous-systèmes chaotiques 3 et 4 qui correspondent respectivement à 1 et 2. Supposons que le canal soit parfait, et que le signale transmis est 0 alors le sous-système 3 se synchronisera avec le système chaotique 1, mais le sous-système 4 ne pourra pas être synchronisé, selon les erreurs de synchronisation (1,3) et (2, 4), le signal ne pourra pas être synchronisé [12][16].

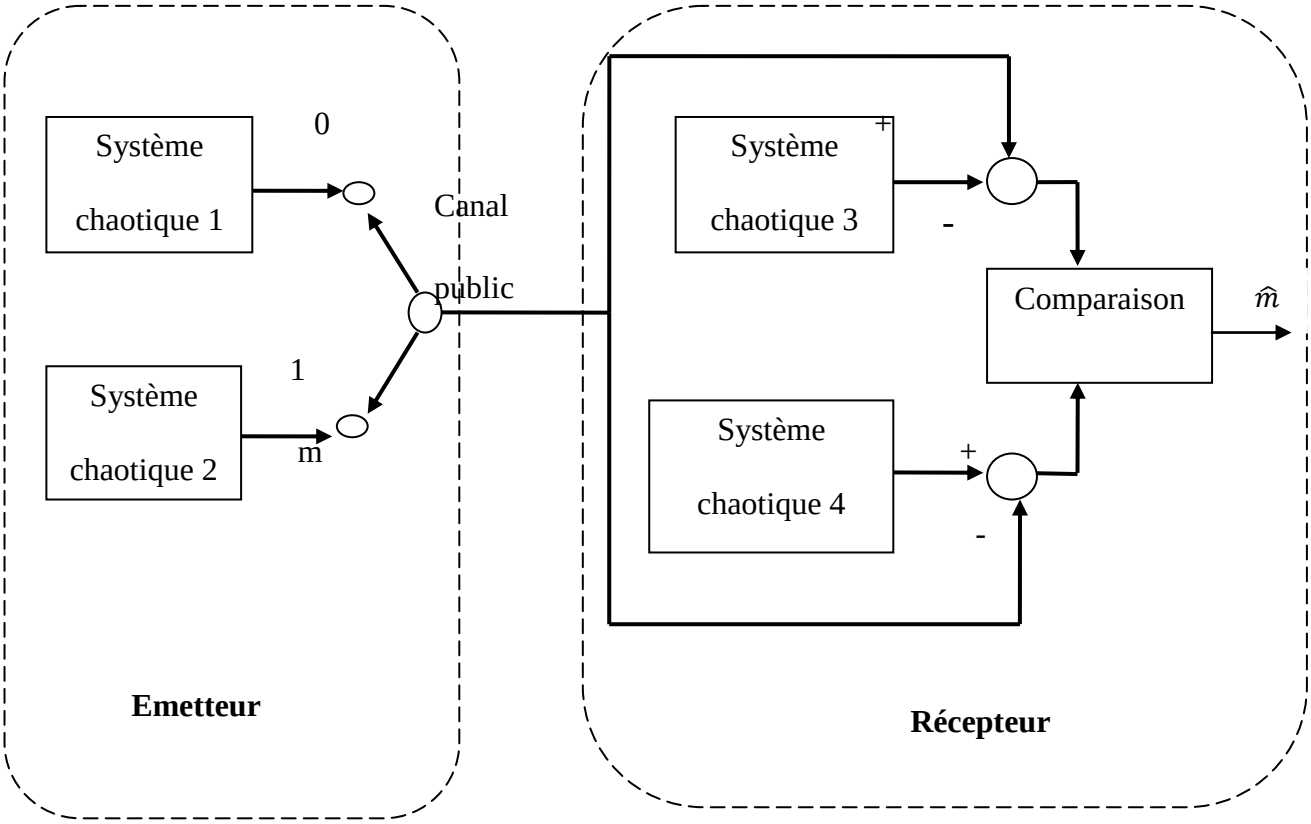


Figure (II.11) : Cryptage par commutation

II.4.4 Transmission à deux voies

Dans le schéma présenté dans **la Figure (II.12),** l'émetteur envoie deux signaux au récepteur. Le premier (y_1) est une fonction à valeurs réelles de l'état (x) du système émetteur chaotique, dont l'unique but est de permettre la synchronisation du récepteur. Le second (y_2) envoyé éventuellement sur un autre canal est un signal chaotique qui contient l'information à transmettre.

Parmi les avantages de cette méthode, on peut souligner d'une part que le signal (y_1) ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre coté, le second signal (y_2) contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état (x), soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse [8].

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

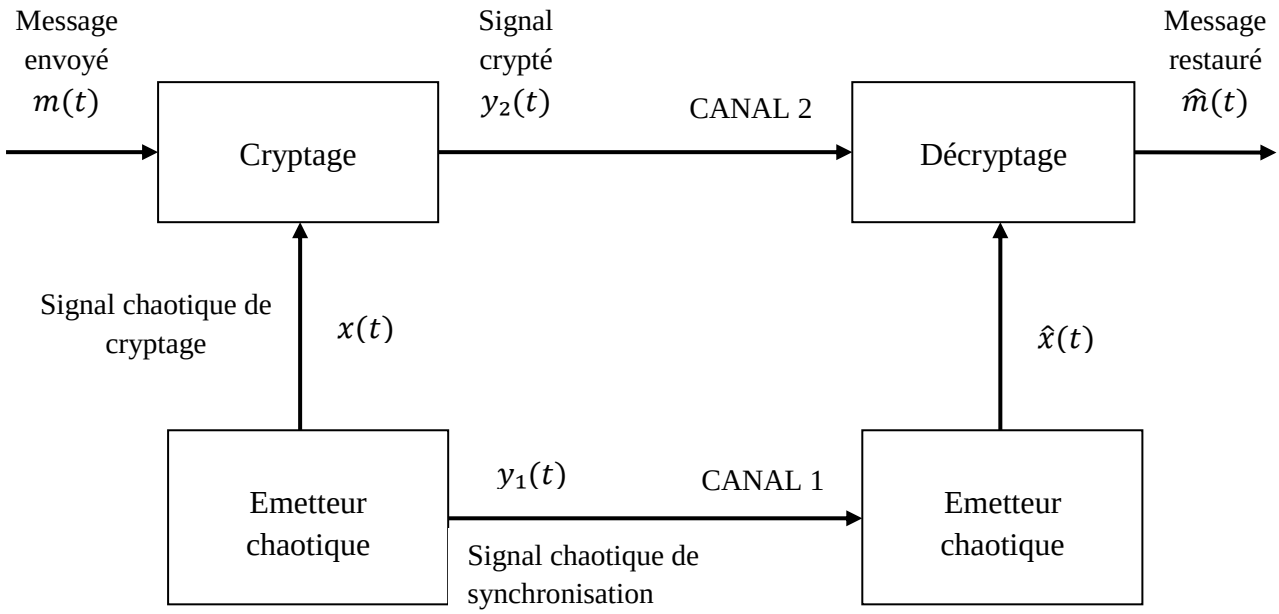


Figure (II.12) : Méthode de transmission à deux voies

II.5 Les objectifs des crypto-systèmes

Le crypto système assure et garantit : la confidentialité, l'authenticité, l'intégrité et la non-répudiation.

· La confidentialité signe qu'une personne non autorisée n'ait pas accès aux informations.

· L'authenticité fait référence pour la validation de la source du message pour assurer quel expéditeur est correctement identité.

· L'intégrité fournit l'assurance que le message n'a pas été modifié pendant la transmission, accidentellement ou intentionnellement.

· La non-répudiation signe qu'un expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

II.6 Conclusion

Dans ce chapitre, nous venons de voire le principe de la synchronisation chaotique. Ainsi que les différentes méthodes utilisées.

La synchronisation des systèmes chaotiques nous donne accès à la réalisation des différents systèmes permettant d'effectuer une transmission sécurisée d'information. Cette dernière est assurée par diverses méthodes de cryptages exploitant le chaos, à savoir le cryptage par addition, par inclusion, par commutation et nous avons fini par les techniques de transmission à deux voies en présentant leurs avantages et leurs inconvénients.

Chapitre III:

Synchronisation des deux systèmes chaotiques Hénon et Lozi

III. Introduction

Le phénomène de synchronisation se manifeste lorsque deux systèmes dynamiques évoluent d'une manière identique en fonction du temps.

Pour la synchronisation de deux systèmes (émetteur et récepteur), on injecte un signal carré généré par l'émetteur et envoyé sous forme d'impulsions au récepteur afin que ce dernier se synchronise avec l'émetteur, ce qui est réalisé par la synthèse d'un observateur.

Dans ce chapitre, nous proposons une méthode de synchronisation à base d'un observateur Impulsif en utilisant la technique de cryptage par addition pour sécuriser le message. Ceci sera appliqué aux systèmes de Hénon et de Lozi.

On va additionner un signal carré à une des variables du système émetteur qui sera transmis dans le canal de communication vers le récepteur afin qu'il se synchronise avec le système maître (émetteur) et à la fin récupérer le signal d'information. Par la suite on ferra une comparaison des résultats de simulation des deux systèmes (Hénon et Lozi) obtenu à partir de Matlab/Simulink.

III.2 Synchronisation et application à la transmission sécurisée

Plusieurs méthodes ont été proposées pour la synchronisation et la communication sécurisée.

Le masquage chaotique est la technique la plus élémentaire pour sécuriser l'information.

La **Figure(III.1)** illustre le principe de base de cette technique.

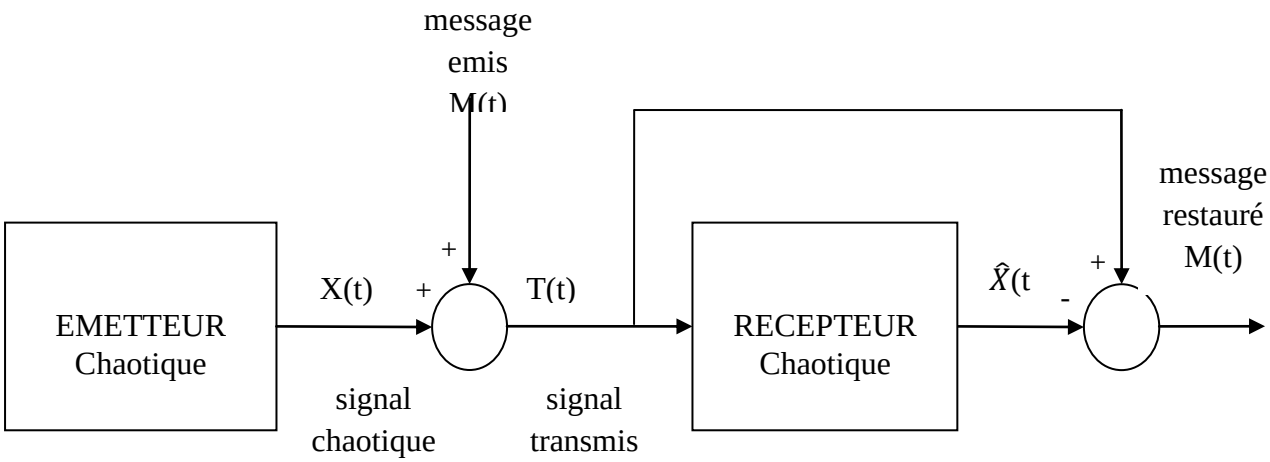


Figure (III.1) : Schéma présentatif de la technique de masquage chaotique

Le système de transmission proposé est constitué de deux bloques :

III.2.1 Bloc émetteur

Ce bloc contient un oscillateur chaotique, un signal en temps discret et un module de cryptage en utilisant la méthode de cryptage par addition pour masquer le signal choisi.

III.2.2 Bloc récepteur

Ce bloc contient un observateur impulsif pour estimer les états du système et un bloc de décryptage qui consiste en un soustracteur.

Dans notre cas nous avons utilisé deux exemples de systèmes chaotiques.

Exemple 1 : Synchronisation impulsive à base du système de Hénon

Considérons le système suivant

$$\begin{cases} x_1(k+1) = a - x_1^2(k) + bx_2(k) \\ x_2(k+1) = x_1(k) \\ y(k) = x_1(k) \end{cases} \qquad (\mathbf{III.1})$$

a et b sont les paramètres du système. Dans le but d'obtenir un comportement chaotique, ils sont choisis comme suit : a=1.4 ; b=0.3.

La **Figure (III.2)** montre l'attracteur chaotique obtenu en considérant les paramètres ci-dessus.

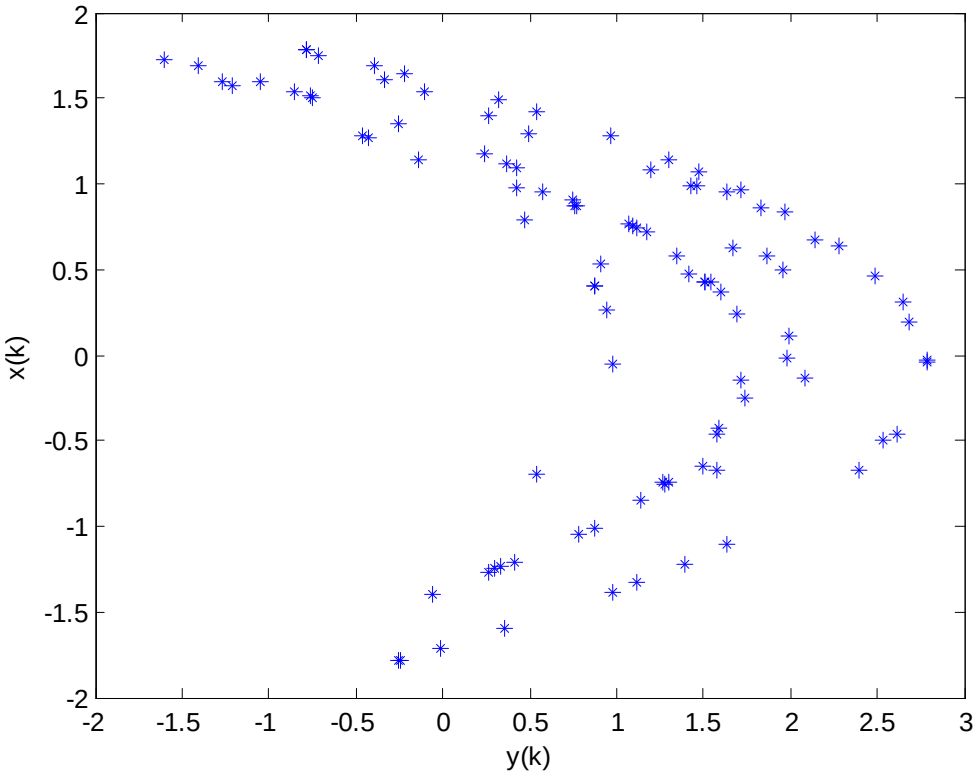


Figure (III.2) : Attracteur étrange de Hénon.

III.2.3 Observateur impulsif

Le rôle de l'observateur impulsif est d'estimer les états d'un autre système en le synchronisant à des instants discrets. Ces derniers représentent, en effet, les moments d'arrivée des impulsions.$\hat{x}_1^2$

L'observateur impulsif du système **(III.1)** est défini par les équations suivantes :

$$\begin{cases} \hat{x}_1(k+1) = a - \hat{x}_1^2(k) + b\hat{x}_2(k) & k \neq t_k \\ \hat{x}_2(k+1) = \hat{x}_1(k) & k \neq t_k \\ \hat{x}_1(t_k^+) = x_1(t_k) & k = t_k \end{cases} \quad (\mathbf{III.2})$$

t_k ensemble d'instants discrets indiquant les moments d'arrivée des impulsions

$$tel\ que\ 0 < t_1 < t_2 < \cdots < t_i < t_{i+1} < \cdots$$
$$et\ i \in \mathbb{Z}$$

A partir des systèmes **(III.1)** et **(III.2)** on obtient le système d'erreur d'observation :

$$\begin{cases} e(k+1) = -\left(x_1^2(k) - \hat{x}_1^2(k) \right) + b(x_2(k) - \hat{x}_2) \\ e(k+1) = x_2(k) - \hat{x}_2(k) \\ e(t_k^+) = 0 \end{cases} \quad (\mathbf{III.3})$$

Exemple 2 : Synchronisation impulsive à base du système de Lozi

Soit le modèle chaotique donné par les équations suivantes :

$$\begin{cases} x_1(k+1) = 1 - a|x_1(k)| + bx_2(k) \\ x_2(k+1) = x_1(k) \\ y(k) = x_1(k) \end{cases} \quad (\mathbf{III.4})$$

Avec : k est le nombre d'itérations.

a=1.7 ; b=0.5.

La **Figure (III.3)** montre la trajectoire de x et y en discret

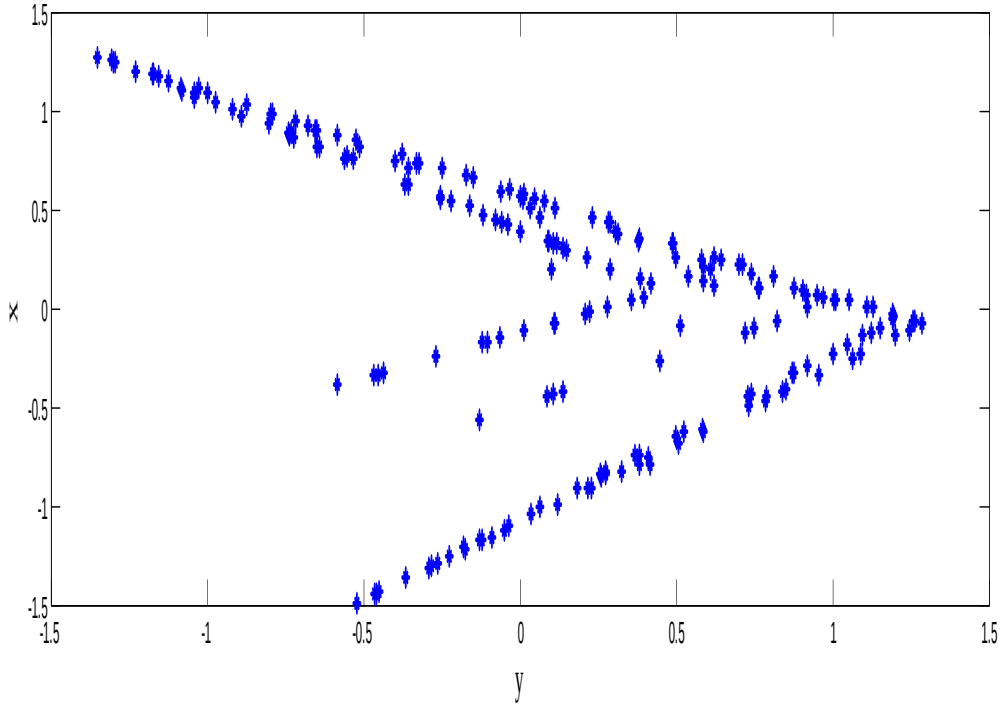


Figure (III.3) : Attracteur étrange de lozi

III.2.4 Observateur impulsif

Le modèle d'observateur impulsif pour le système de lozi **(III.4)** est représenté par :

$$\begin{cases} \hat{x}_1(k+1) = 1 - a|\hat{x}_1(k)| + b\hat{x}_2(k) \\ \hat{x}_2(k+1) = \hat{x}_1(k) \\ \hat{x}_1(t_k^+) = x_1(t_k) \qquad\qquad k = t_k \end{cases} \qquad (\mathbf{III.5})$$

$$t_k \ ensemble\ discret\ des\ instants\ de\ temps\ tel\ que\ 0 < t_1 < t_2 < \cdots < t_i < t_{i+1} < \cdots$$

$$et\ i \in \mathbb{Z}$$

A partir des systèmes $(\mathbf{III.4})$ et $(\mathbf{III.5})$ on obtient le système d'erreur d'observation suivant :

$$\begin{cases} e_1(k+1) = -a(x_1(k) - \hat{x}_1(k) + b(x_2(k) - \hat{x}_2(k)) \\ e_2(k+1) = x_2(k) - \hat{x}_2(k) \\ e(t_k^+) = 0 \end{cases} \qquad (\mathbf{III.6})$$

III.2.5 Résultat de simulation pour le système de Hénon

Nous allons présenter les résultats de simulation obtenus sous Matlab/Simulink.

Pour obtenir le régime chaotique, les paramètres du système sont fixés comme suit :

a=1.4, b=0.3, les conditions initiales (x(0), y(0)) = (0, 0) au niveau de l'émetteur et (x(0), y(0)) = (0,1) au niveau du récepteur, la période des impulsions de synchronisation est de T=3.

- **Reconstruction des états : $\hat{x}$(k)= x'(k), $\hat{y}$(k)= y'(k)**

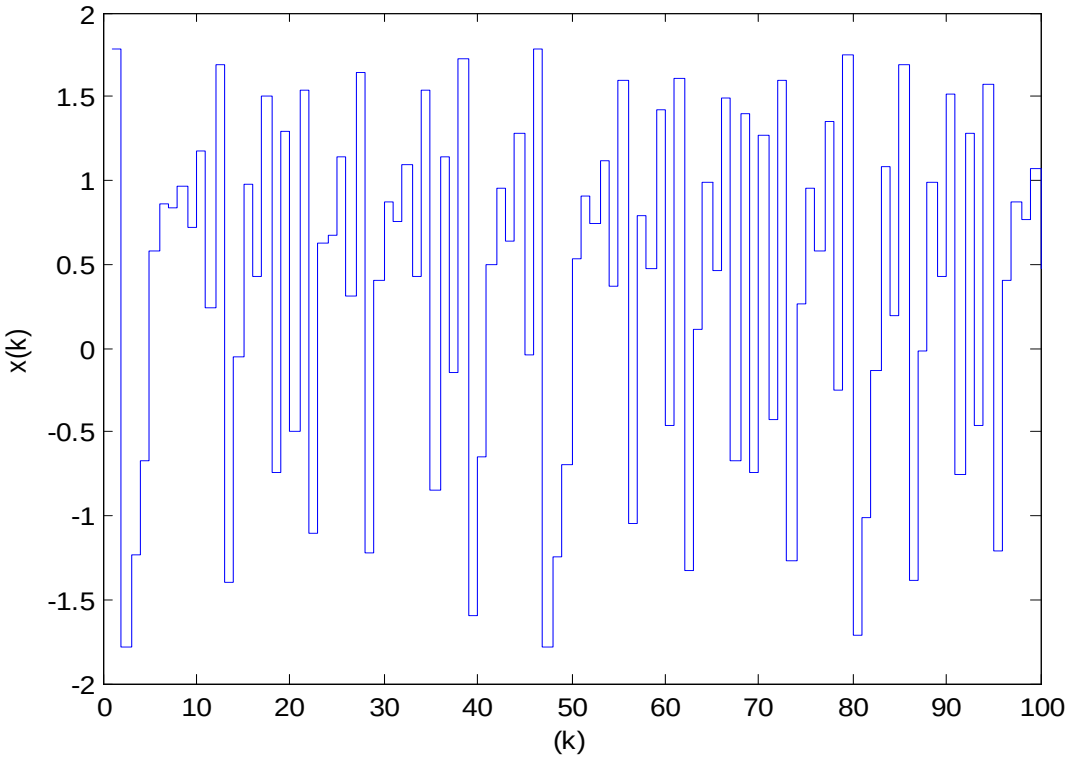


Figure (III.4) : Résultat de simulation de l'état x(k) du système de Hénon

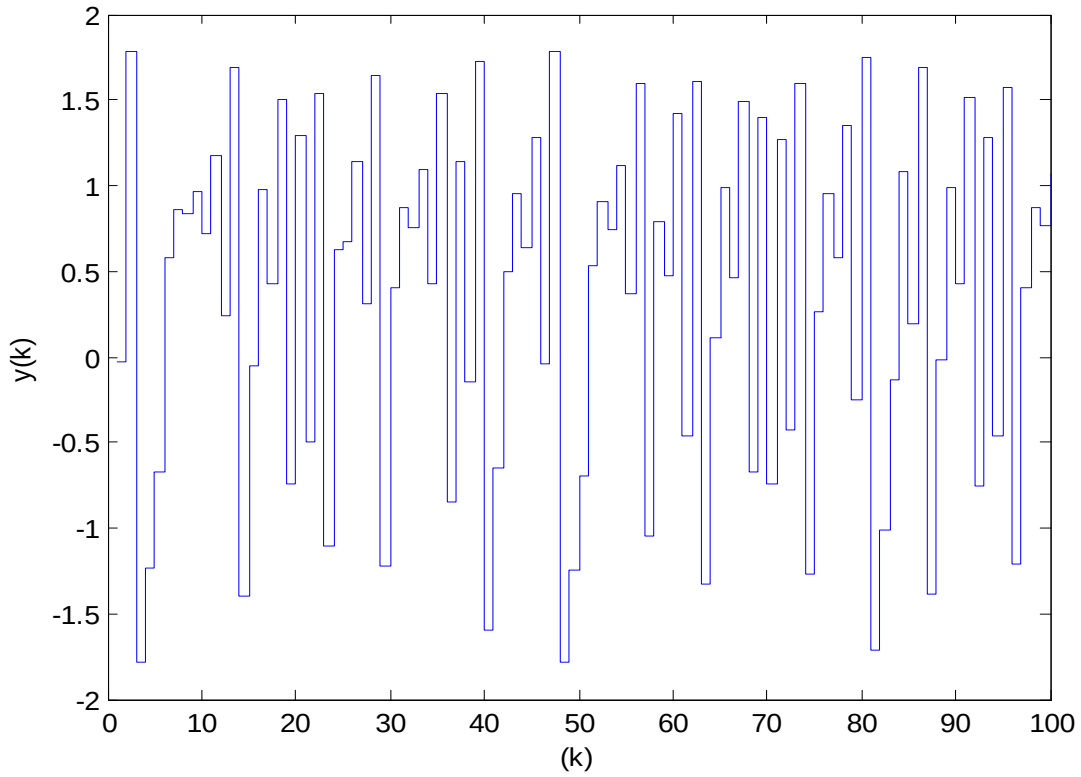


Figure (III.5) : Résultat de simulation de l'état y(k) du système de Hénon

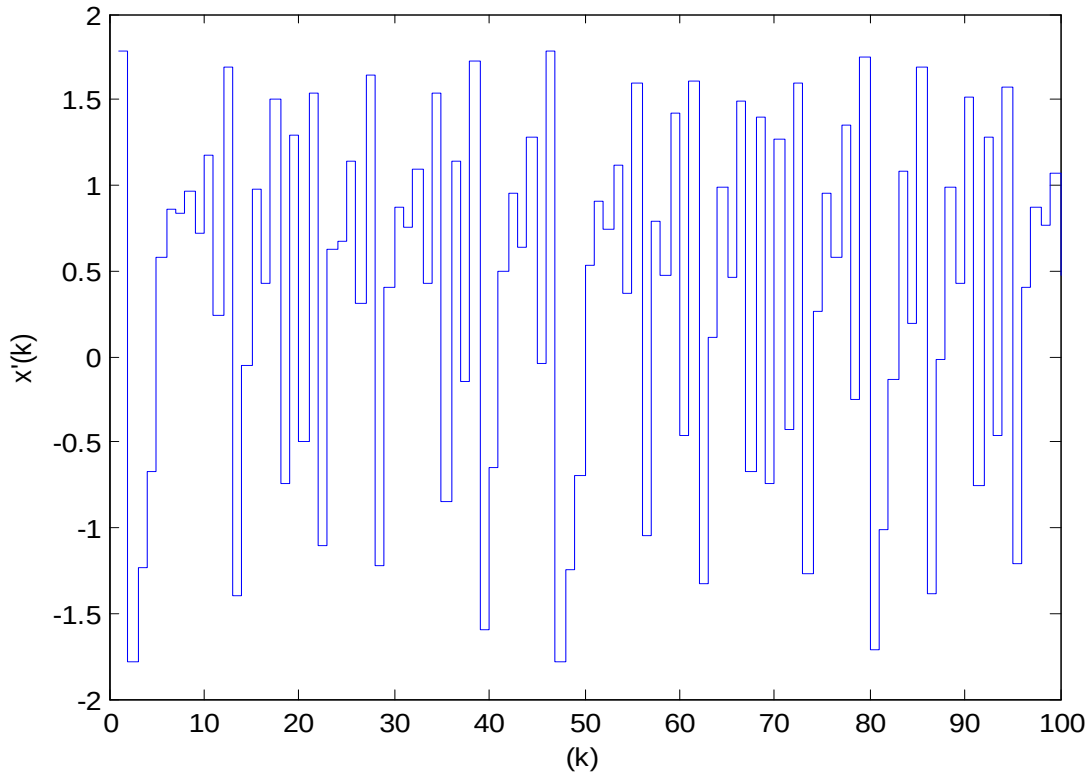


Figure (III.6) : Résultat de simulation de l'état $\hat{x}$(k) du système de Hénon

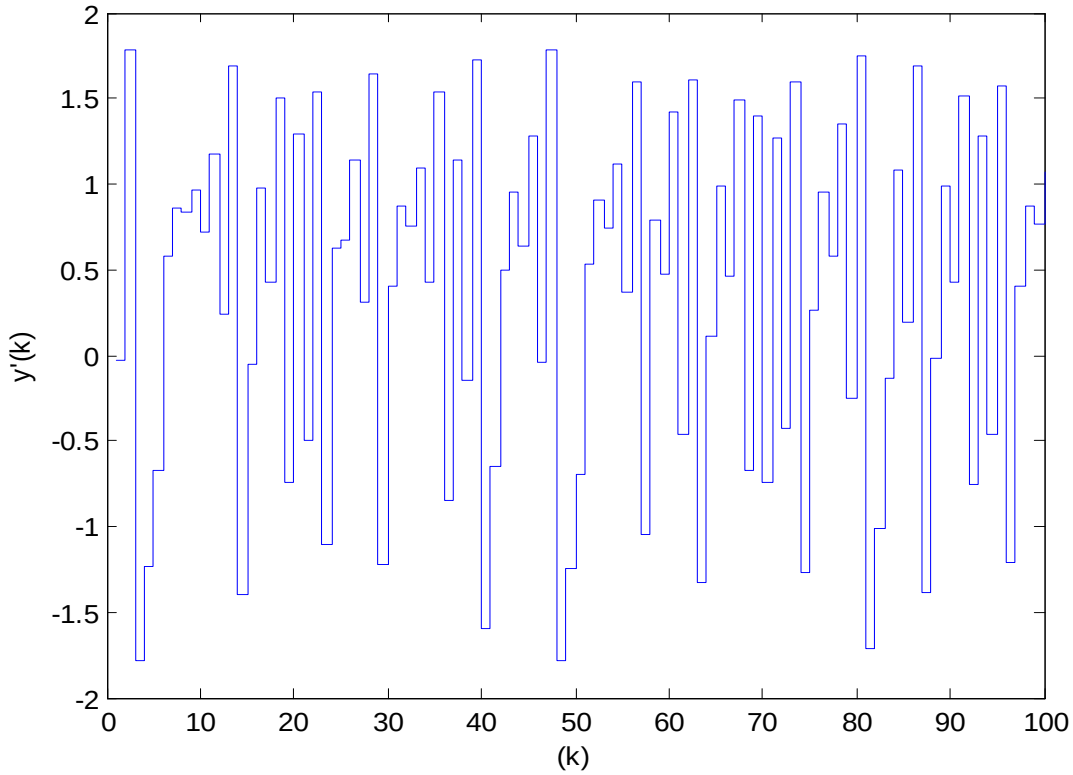


Figure (III.7) : Résultat de simulation de l'état $\hat{y}$(k) du système de Hénon

Nous remarquons dans ces résultats la présence d'oscillation irrégulière et apériodique ce qui explique que les signaux x(k), $\hat{x}$(k) et y(k) et $\hat{y}$(k) suivent un comportement chaotique.

III.2.6 Résultats de simulation pour le système de Lozi

Nous allons présenter les résultats de simulation obtenus sous Matlab/Simulink pour ce système.

Pour obtenir le régime chaotique les paramètres du système sont fixés comme suit :

a=1.7, b=0.5 les conditions initiales (x(0), y(0)) = (0, 0) au niveau de l'émetteur et, (x(0), y(0)) = (0,1) au niveau du récepteur, la période des impulsions de synchronisation est de T=0.05

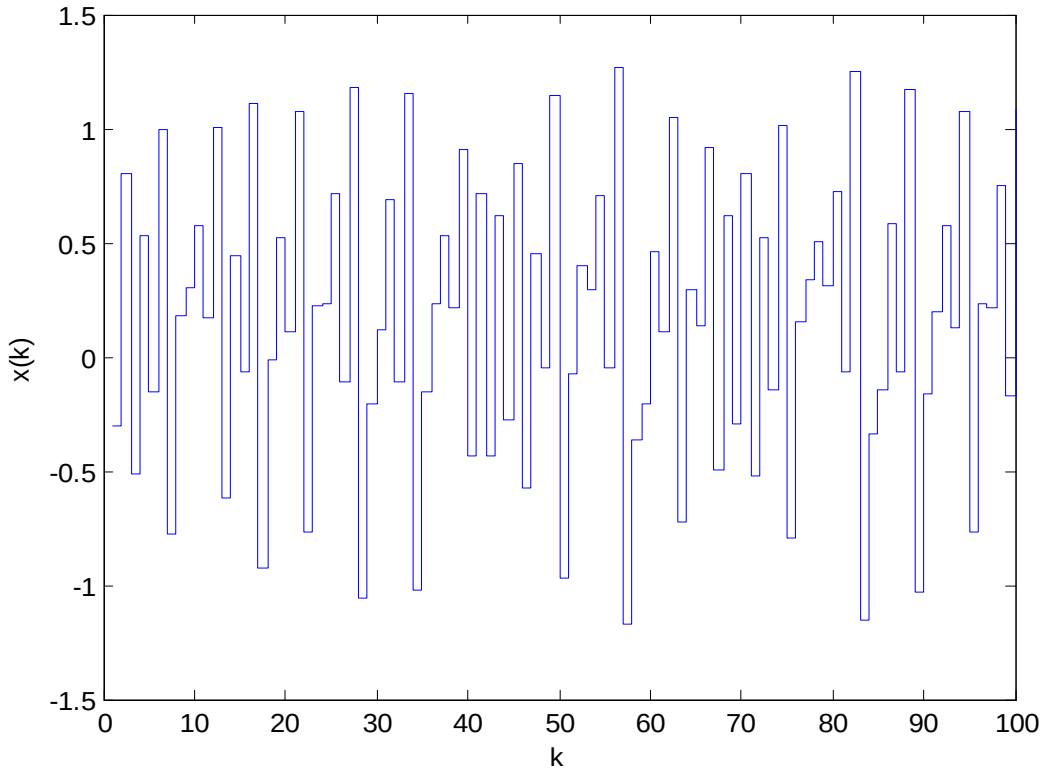


Figure (III.8) : Résultat de simulation de l'état x(k) du système de Lozi

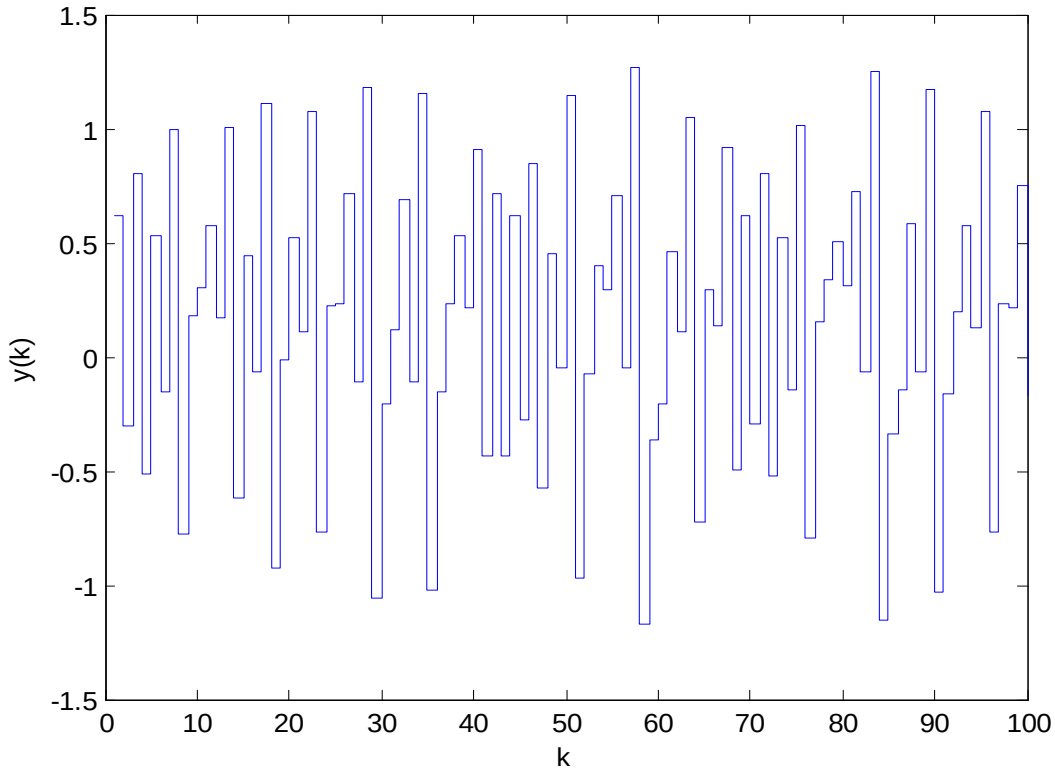


Figure (III.9) : Résultat de simulation de l'état y(k) du système de Lozi

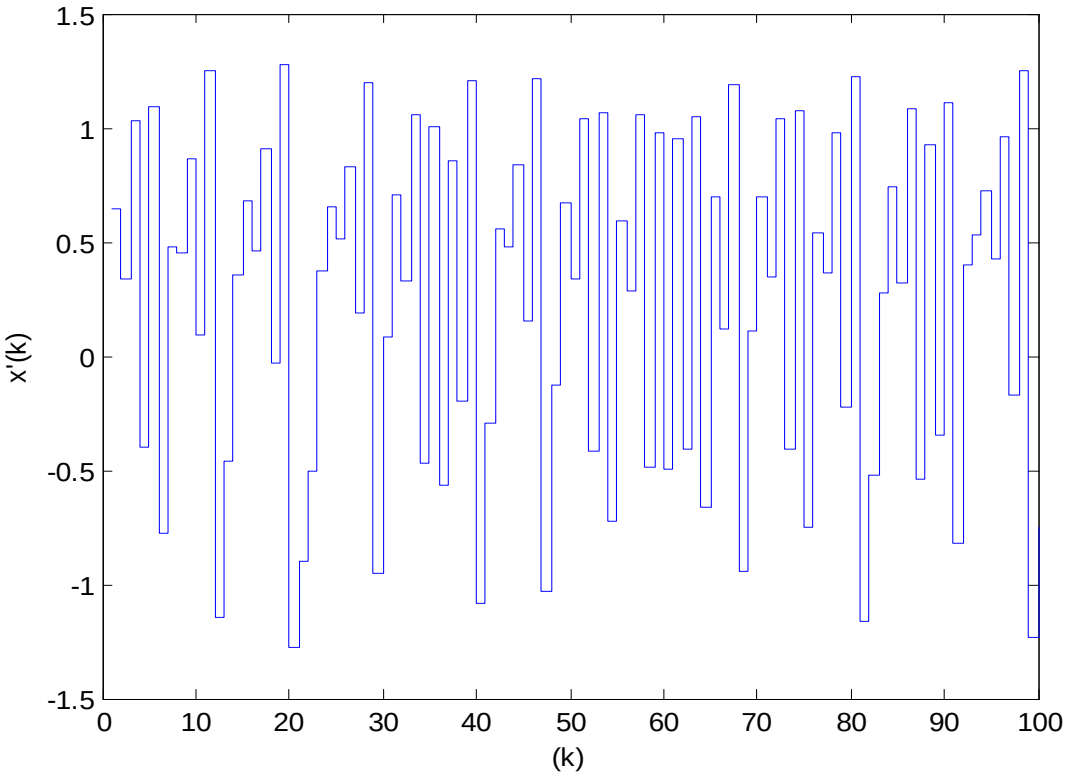


Figure (III.10) : Résultat de simulation de l'état $\hat{x}$(k) du système de Lozi

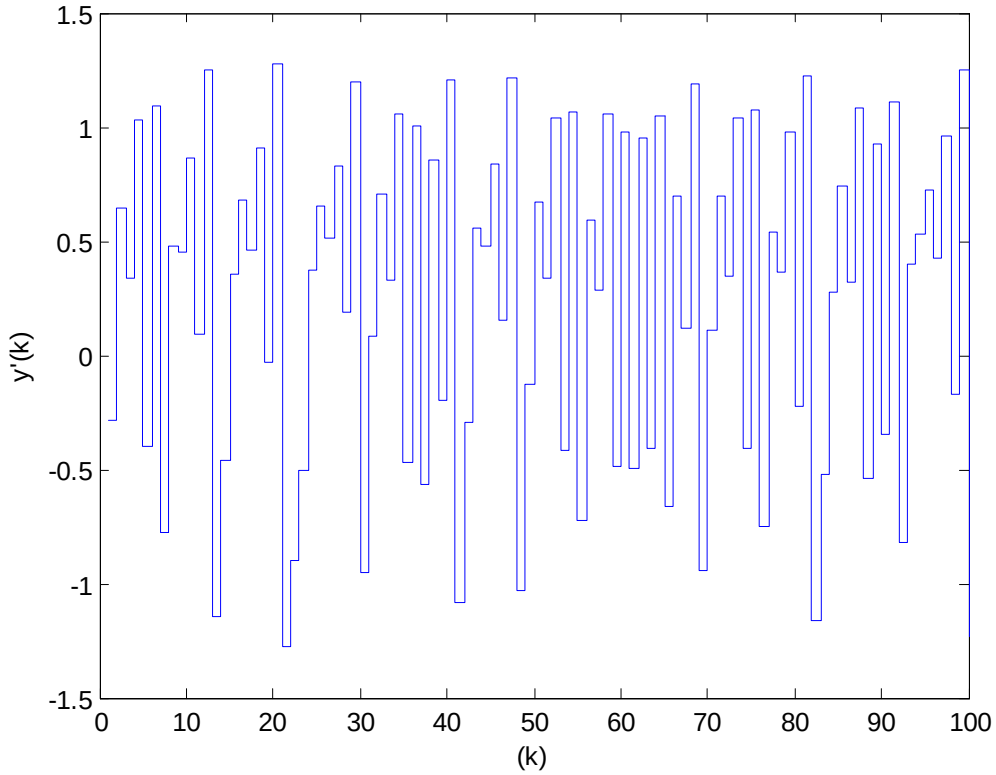
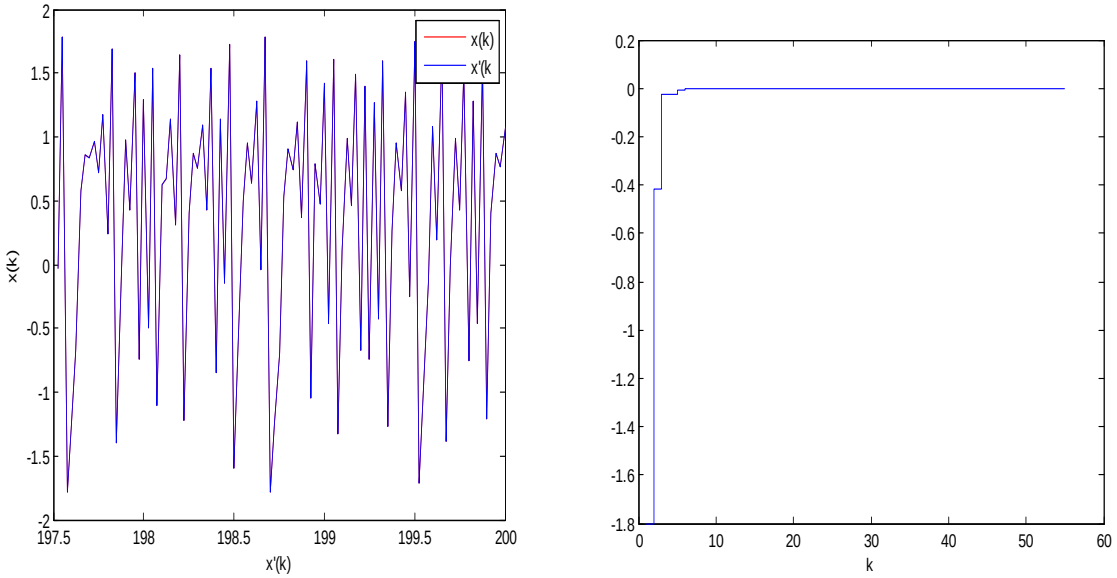


Figure (III.11) : Résultat de simulation de l'état $\hat{y}$(k) du système de Lozi

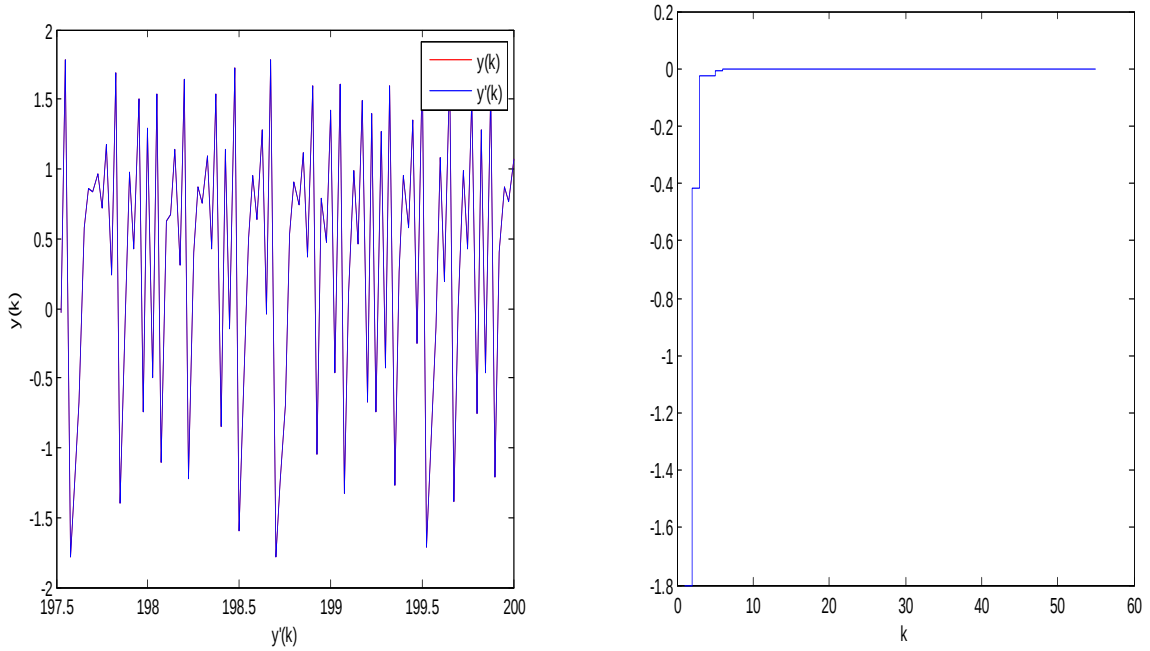
III.2.7 Résultats de synchronisation pour le système de Hénon

Ici nous présentons les résultats de synchronisation obtenus sous Matlab/Simulink pour le système de Hénon, la synchronisation se fait au niveau de l'état y et le masquage se fait par l'addition du message m à x de l'oscillateur au niveau de l'émetteur. La **Figure(III.12)** montre les résultats de synchronisation des états x(k) et $\hat{x}$(k) et ceux de y(k) et $\hat{y}$(k) sont montrés sur la **Figure (III.13).**



a: Etats x (k)et $\hat{x}$ (k) b : Erreur de synchronisation e_1=x-$\hat{x}$

Figure (III.12) : résultats de synchronisation des états x(k) et $\hat{x}$(k)



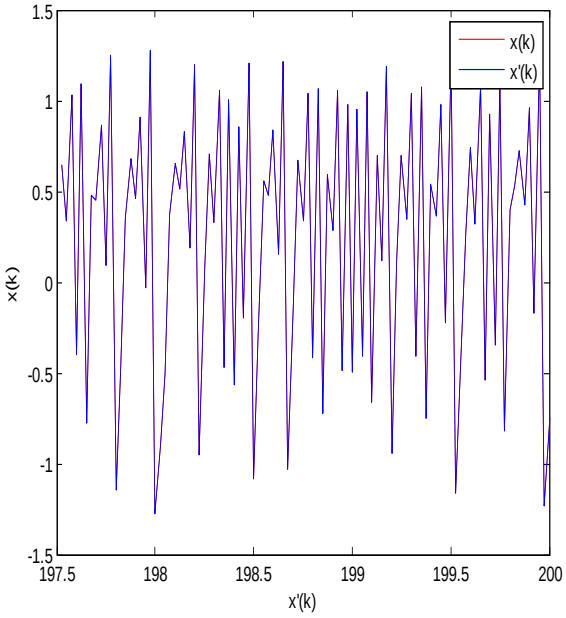
a: Etats y(k) et $\hat{y}$ (k) b : Erreur de synchronisation e_2=y -$\hat{y}$

Figure (III.13) : Résultats de synchronisation y -$\hat{y}$.

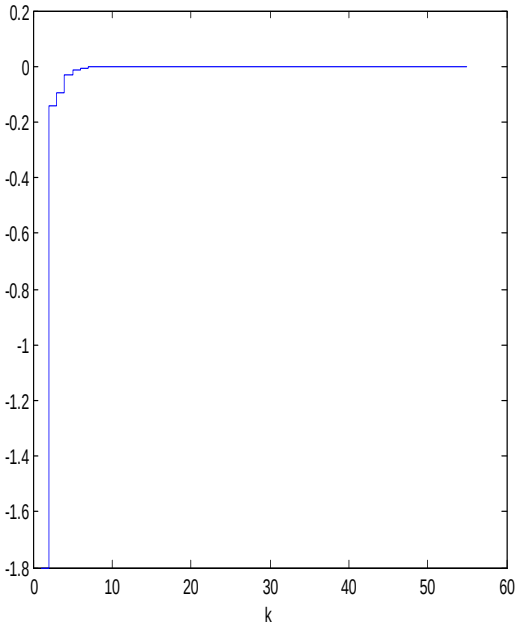
III.2.8 Résultats de synchronisation pour le système de Lozi

Dans ce cas nous allons présenter les résultats de synchronisation obtenus sous Matlab/Simulink pour le système de Lozi.

La synchronisation se fait au niveau de l'état y et le masquage se fait par l'addition du message m à x de l'oscillateur au niveau de l'émetteur, la **Figure (III.14)** montre les résultats de synchronisation des états x et $\hat{x}$ et ceux de y et $\hat{y}$ sont montré sur la **Figure (III.15)**.



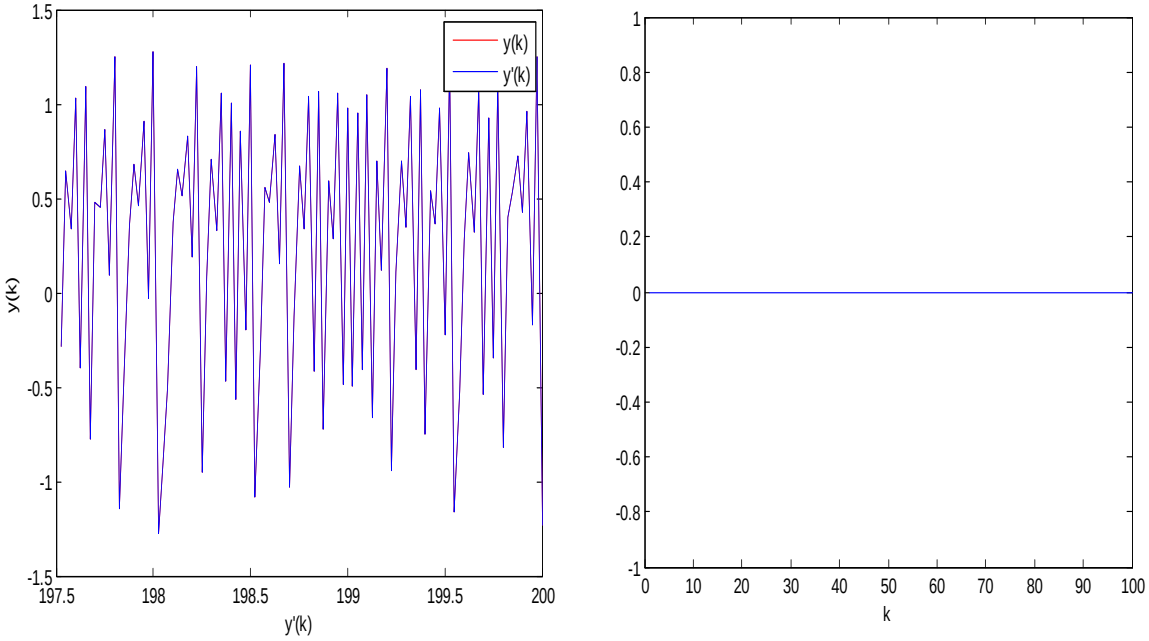
a : Etats x(k) et $\hat{x}$(k)



b : Erreur de synchronisation e_1=x-$\hat{x}$

Figure (III.14) : Erreur de synchronisation x(k) - $\hat{x}$(k).

D'après la **Figure (III.14)** on constate que l'erreur entre x(k) et $\hat{x}$(k) égale à zéro, ce qui explique que les deux systèmes sont parfaitement synchronisés.



a : Etats y(k) et $\hat{y}$(k) **b :** Erreur de synchronisation e_2=y -$\hat{y}$

Figure (III.15) : Erreur de synchronisation y(k) -$\hat{y}$(k)

D'après la **Figure (III.15)** on constate que l'erreur entre y(k) et $\hat{y}$(k) égale à zéro, ce qui explique que les deux systèmes sont parfaitement synchronisés.

.

III.2.9 Résultats de transmission pour les deux systèmes de Hénon

Le message à envoyer dans notre cas est un signal carré d'amplitude 1 et de période 0.5.

Comme nous l'avons cité auparavant, la méthode de cryptage utilisée consiste à additionner le message original à l'un des états du système chaotique.

Dans notre cas nous avons choisi d'additionner un message à l'état x du système de Hénon. La **Figure (III.16)** illustre l'allure du message original, le message crypté est donné par la **Figure (III.17)**.

Le message est décrypté au niveau du récepteur grâce au bloc de décryptage qui consiste en un soustracteur. En effet une fois l'estimé de l'état y à savoir $\hat{y}$ est obtenue, il suffit de le soustraire au message crypté envoyé par le canal de transmission.

La courbe du message récupéré est illustrée par la **Figure (III.18)**.

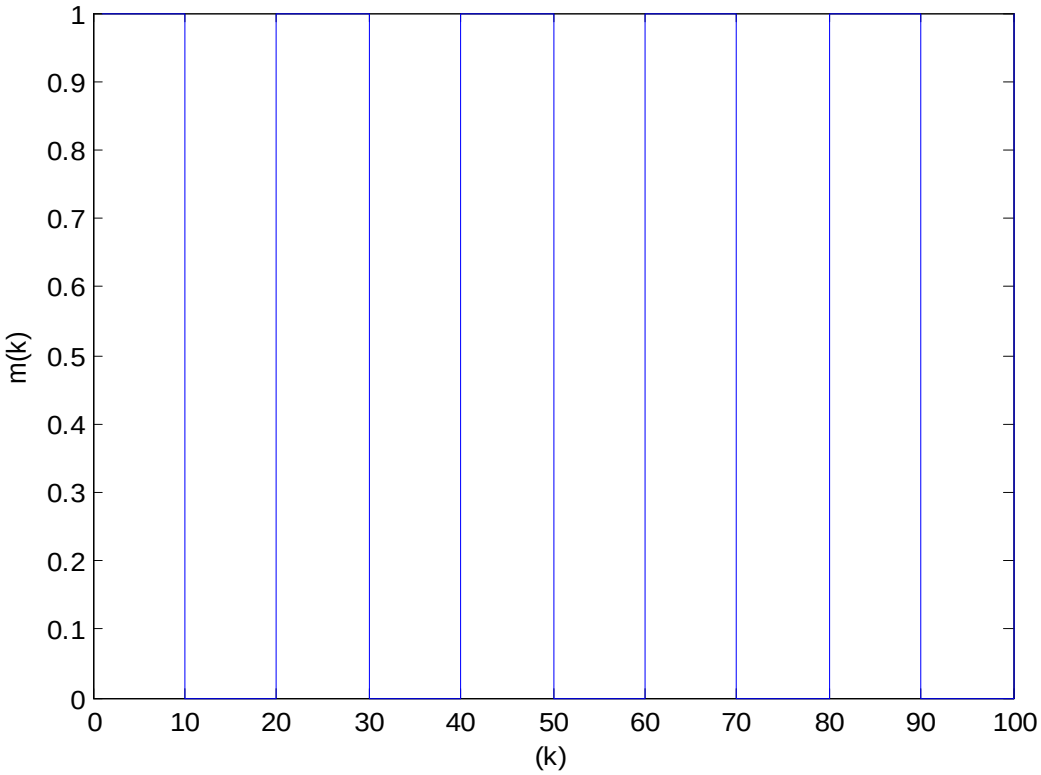


Figure (III.16) : Message original

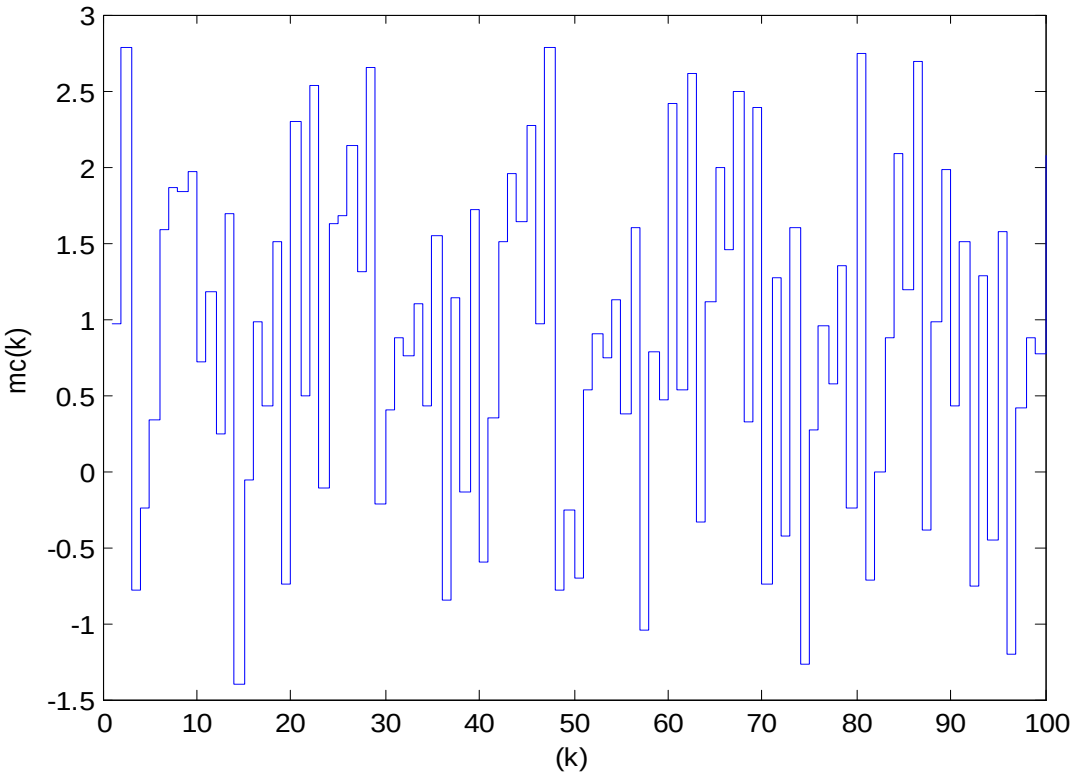


Figure (III.17) : Message crypté.

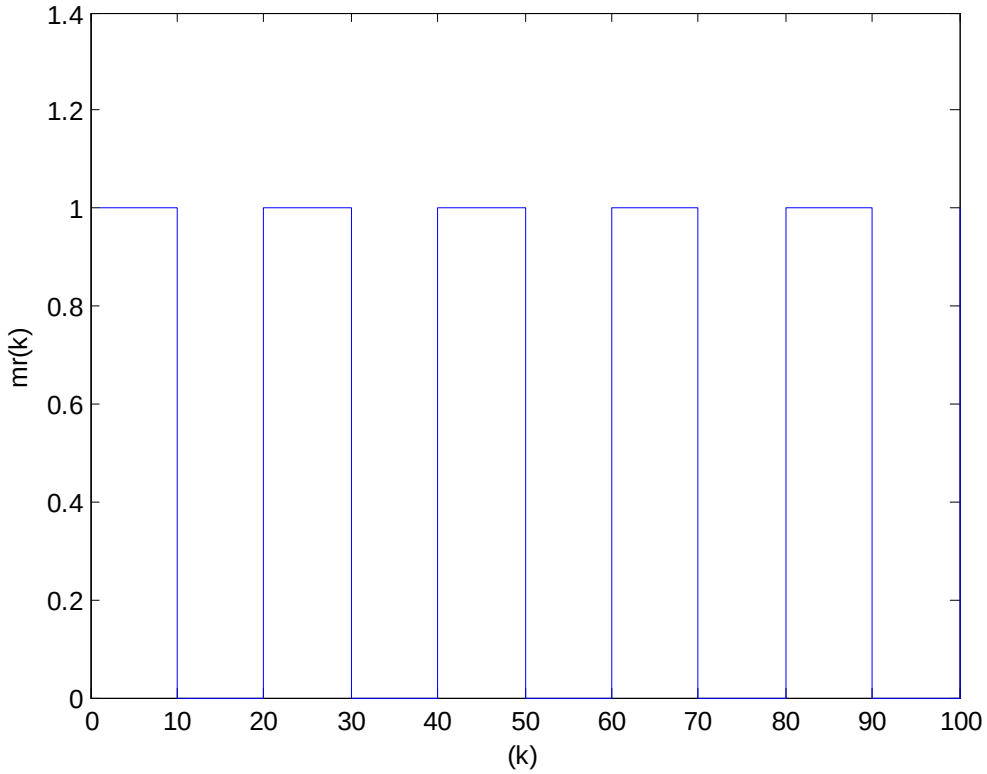


Figure (III.18) : Message récupéré

Une fois la synchronisation des états sont assurées, en observant les résultats obtenus, nous déduisons que le message est bien noyé dans le signal chaotique et que le message envoyé a été récupéré. Ce qui montre l'efficacité de la méthode de synchronisation impulsive

III.2.10 Résultats de transmission pour le système de Lozi

Nous utilisons le même message appliqué pour le système de Hénon et qui est illustré par la **Figure (III.19).**

Les **Figures (III.20)** et **(III.21)** montrent, respectivement le message crypté et envoyé par le canal de transmission et le message récupéré.

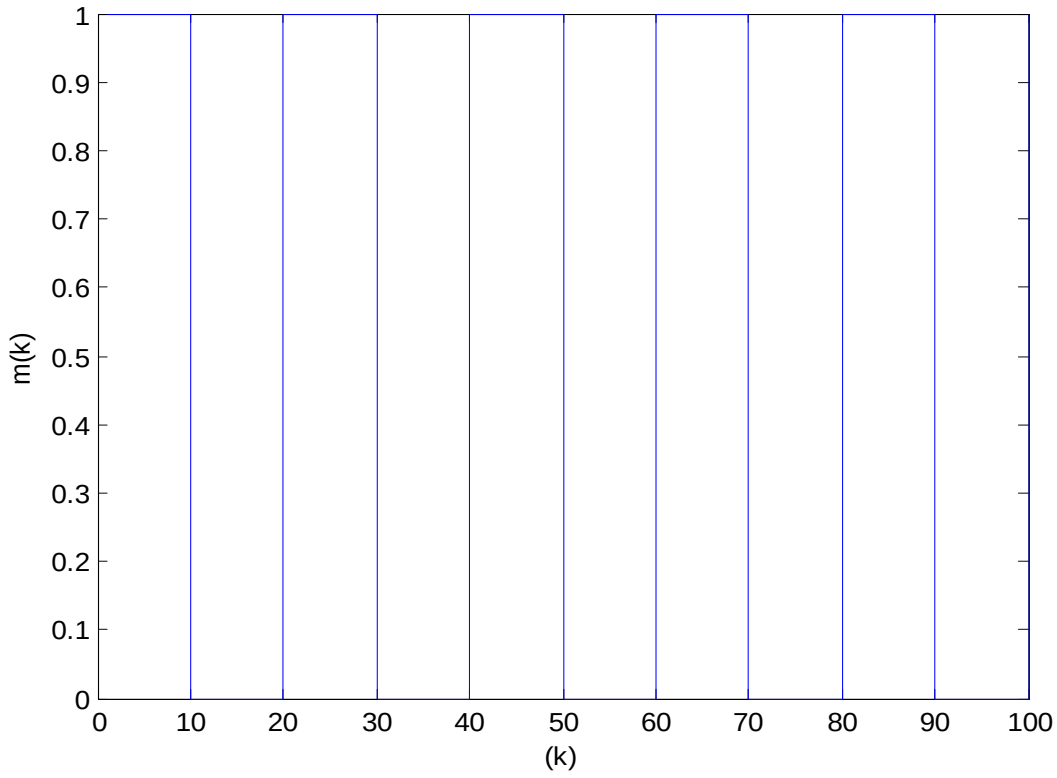


Figure (III.19) : Message original

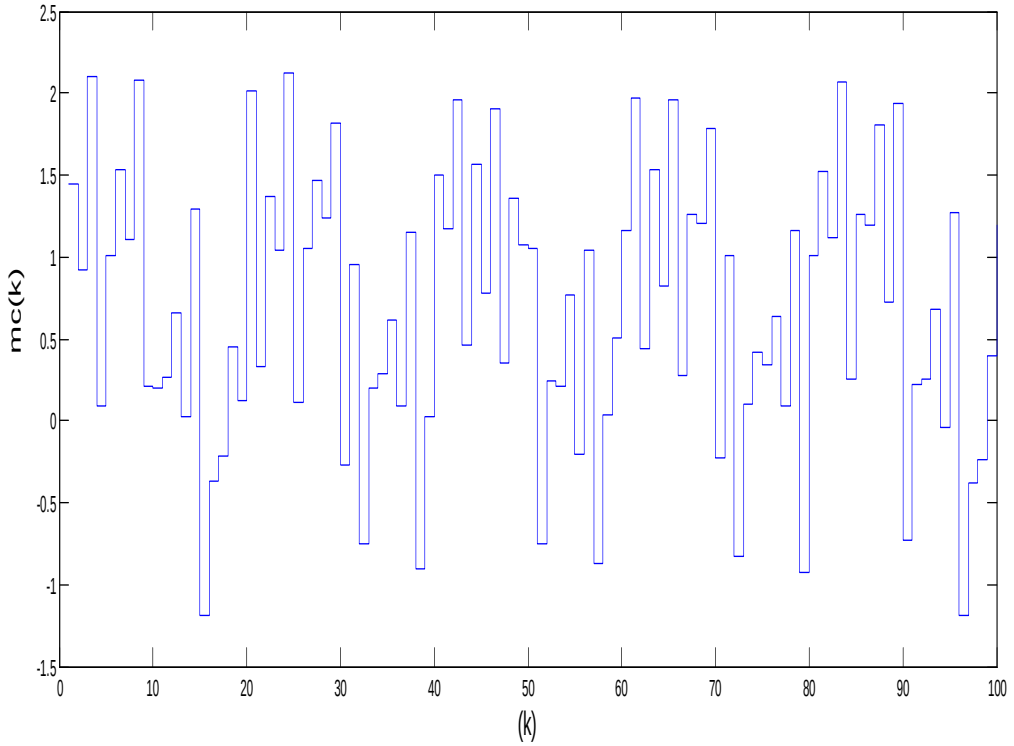


Figure (III.20) : Message crypté

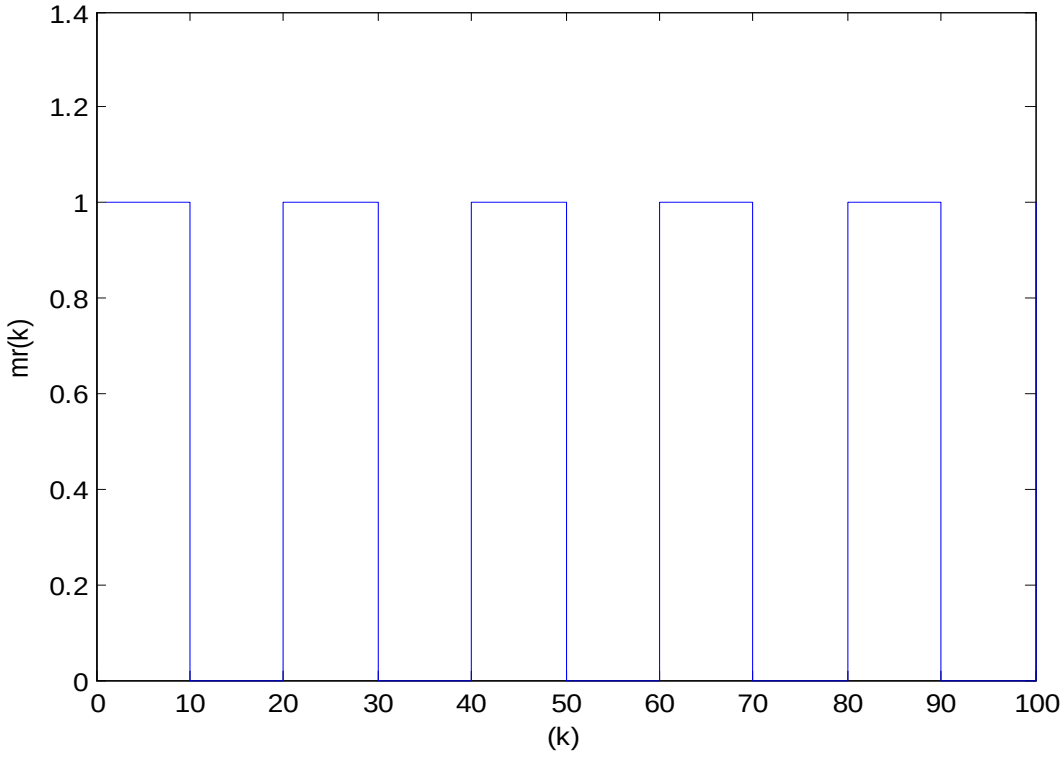


Figure (III.21) : Message récupéré

Remarque :

A partir des résultats obtenus pour les deux exemples d'application (systèmes de Hénon et Lozi) nous pouvons confirmer que le message est bien récupéré au niveau du récepteur pour les deux cas. Ceci implique l'efficacité de la méthode de synchronisation impulsive pour les deux systèmes.

III.2.10 Conclusion

Dans ce chapitre, nous avons réussi à synchroniser deux systèmes chaotiques de Hénon et Lozi, des résultats de simulations sont donnés pour illustrer l'efficacité de la méthode de synchronisation impulsive ceci a permis la récupération des messages en utilisant la méthode de cryptage par addition qui consiste à additionner le message original à l'un des états du système chaotique généré par l'émetteur, la récupération du message se fait au niveau du récepteur par soustraction du message crypté envoyé pas le canal de transmission et celui reconstruit par l'observateur impulsif.

En observant le résultat obtenu nous pouvons conclure que la méthode de synchronisation impulsive est efficace pour les deux systèmes.

Conclusion générale

Conclusion générale

Dans ce mémoire nous avons étudié et tester par simulation un système de transmission sécurisé de données basé sur les systèmes chaotiques et la synchronisation impulsive. Plus précisément nous avons utilisé les systèmes de Hénon et Lozi pour générer le chaos.

Nous avons dans un premier temps introduit les systèmes et leurs propriétés. Les propriétés de base à savoir : la sensibilité aux conditions initiales et variation paramétriques, le diagramme de bifurcation, l'aspect aléatoire ont été discutées et testées sur des systèmes chaotiques célèbres.

Dans le deuxième chapitre du mémoire, nous avons introduit le concept de la synchronisation des systèmes chaotiques et les méthodes utilisées dans la littérature. Par la suite nous avons introduit les notions de cryptage et de décryptage et les différentes méthodes utilisées.

Dans le troisième chapitre, nous avons proposé une méthode de synchronisation impulsive. C'est une approche qui utilise des impulsions qui permettent de synchroniser les états de deux systèmes chaotiques. Nous avons également utilisé le cryptage par additions pour masquer le message à transmettre. Le schéma est appliqué sur les deux systèmes Hénon et Lozi.

Des résultats de simulation sont donnés pour illustrer l'efficacité de la méthode de synchronisation impulsive et a permis la récupération du message transmis.

Bibliographie

[1] H.Thomas, L.Baptistd, S.Serdar, «La cryptographie chaotique»

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

[3] O.Megherbi « Etude et réalisation d'un système sécuriser a base de systèmes chaotiques, mémoire de magister, 2013.

[4] B.chauaib, «Photonique et réseaux optiques telecomunication »mémoire de master télécommunication, université de Tlemcen, 2014

[5] http://just.loic.free.fr/index.php?pas=hist.

[6] Eric Goncalves da Silva « Introduction aux systèmes dynamiques et chaos », Institut national polytechnique de Grenoble.

[7] Z.Elhadj « Etude de quelque types de systèmes chaotiques, généralisation d'un modèle issu du model de Chen », thèse de doctorat, université de Mentouri, Constantine

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

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

[10] T.Hamzia, « Système dynamique et chaos 'application à l'optimisation à l'aide d'algorithme chaotique' », thèse de doctorat, université de Mentouri, Constantine, 2007.

[11] H.Hamiche, « Inversion a gauche des systèmes dynamique hybrides chaotiques. Application à la transmission sécurisée de données », thèse de doctorat, université de mouloud Mammeri de Tizi-Ouzou, 2011.

[12] A.Zemouche, « Sur l'observation de l'état des systèmes dynamiques non linéaires », thèse de doctorat, université louis pasteur-Strasbourg I, France ,2007.

[13] I.Ameur « control, chaotification et hyperchaotification des systèmes dynamique », mémoire de magister, université de Mentouri de Constantin, 2007.

[14] LI.T-Y: E stimates of intermetency, spectra and blow.up in developed terbulance, comm., on pure and, math.4 (1981), 853 the evolution of a turbulent vorter, comm. Math .phys. the évolution procaccia, I 83 (1982) 517

[15] N.Slimani Boukhalfa, « système d'observateur non linéaires : application au diagnostic de défauts», Mémoire de magister, université de mouloud Mammeri de tizi-ouzou.

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

[17] S.Boccaletti, J.Kurth, G.Osipov, D.L.Valladarses, C.S; Zhou « the synchronisation of chaotic systems ».''Physics Repots, 2002:1-101.

[18] Gang ZHENG. «Formes Normales d'observabilité Paramétrées par les sorties : application au cryptage par synchronisation de systèmes chaotique»..Thèse de doctorat L'université de Cergy-Pontoise(2006).

[19] Mihai Bogdan Luca. « Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information ». Thèse doctorat 2006.

[20] J.Daafouz and G.Milleriaux, «Poly- quadratic stability and global chaos synchronization of discrcret time hybrid systems, special Issue of Mathematics and computers in simulation, vol.58.pp. 295.307, 20[1] H.Thomas, L.Baptistd, S.Serdar, «La cryptographie chaotique»

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