Sur la synchronisation et le cryptage de systèmes chaotiques à temps discret utilisant les techniques d'agrégation et la représentation en flèche des matrices

Rania Linda Filali

N° d'ordre : 220

ÉCOLE CENTRALE DE LILLE
UNIVERSITÉ DE TUNIS EL MANAR
ECOLE NATIONALE D'INGENIEURS DE TUNIS

THÈSE

présentée en vue d'obtenir le grade de

DOCTEUR

en Automatique, Génie Informatique, Traitement du Signal et Image

par

Rania Linda FILALI

Ingénieur Enit en Génie Électrique

Doctorat délivré conjointement par l'École Centrale de Lille
et l'École Nationale d'Ingénieurs de Tunis

Sur la synchronisation et le cryptage de systèmes chaotiques à temps discret utilisant les techniques d'agrégation et la représentation en flèche des matrices

soutenue le 04 juin 2013 devant le Jury d'Examen composé de :

Président	Noureddine ELLOUZE	Professeur, ENIT
Rapporteur	Abdellah EL MOUDNI	Professeur, UTBM
Rapporteur	Safya BELGHITH	Professeur, ENIT
Examinateur	José RAGOT	Professeur, INPL-ENSG
Directeur de Thèse	Mohamed BENREJEB	Professeur, ENIT
Directeur de Thèse	Pierre BORNE	Professeur,EC-Lille

Thèse préparée dans le Laboratoire LAGIS (EC-Lille) et dans le Laboratoire Automatique (LARA, ENIT)
Ecole Doctorale SPI 072 (Lille I, Lille III, Artois, ULCO, UVHC, EC Lille)

PRES Université Lille Nord-de-France

Dédicaces

A mon père Taieb et à ma mère Nadia, *pour leur amour infini, leurs sacrifices et leurs encouragements continus. Qu'ils trouvent ici l'expression de mon grand amour et mes sentiments les plus sincères. Je leur dédie cette réussite et ce travail.*

A mon mari Mehdi, *pour son encouragement et son soutien permanent. Je lui dois tout et aucun mot ne peut témoigner l'étendue des sentiments que j'éprouve à son égard.*

A mon frère Rayen et à ma soeur Cyrine*, à qui je dédie ce travail en signe de la profonde et indéfectible affection que je leur porte et leur adresse tous mes voeux de réussite et de succès.*

Mes pensées vont également ***à feue ma grand-mère Liliane*** *qui me manque et qui a toujours cru en moi,* ***à feux mes grands parents Slaheddine Bey, Abdelkader et Khadija Filali****. Je dédie ce travail aux familles Filali et Housseini pour leur soutien et leur présence sans bornes.*

J'adresse toute ma gratitude à mes beaux parents ***Khaled et Mounira Dami*** *pour leur gentillesse et leur soutien, ainsi qu'à mes amis proches pour leur soutien constant.*

Avant-propos

Le travail, que je présente dans ce mémoire de Thèse de Doctorat, a été effectué au Laboratoire de Recherche en Automatique (LARA) de l'Ecole Nationale d'Ingénieurs de Tunis (ENIT) et au Laboratoire d'Automatique, Génie Informatique et Signal (LAGIS) de l'Ecole Centrale de Lille (EC-Lille).

Je tiens, tout d'abord, à exprimer mon profond respect et ma parfaite reconnaissance pour le grand honneur que m'a fait Monsieur Noureddine ELLOUZE, Professeur du Laboratoire de Recherche Traitement du Signal, de Traitement d'Images et Reconnaissance de Formes de l'ENIT, en acceptant de présider mon Jury d'Examen.

Je souhaite aussi exprimer ma gratitude, ma plus grande reconnaissance et mon profond respect à Monsieur Pierre BORNE, Professeur à l'EC-Lille et à Monsieur Mohamed BENREJEB, Professeur à l'ENIT et Directeur du Laboratoire de Recherche en Automatique qui ont co-dirigé mes travaux de recherche et qui m'ont apporté leur soutien, leurs judicieux conseils, leur grande disponibilité, leur apport scientifique indéniable et la qualité exceptionnelle de leur encadrement, tout au long de l'élaboration de ma thèse. J'ai profité de leur approche rigoureuse, de leurs précieux et nombreux conseils et de leurs qualités humaines.

Je suis très honoré que Monsieur Abdellah EL MOUDNI, Professeur du Laboratoire Systèmes et Transport de l'Université de Technologie de Belfort-Montbéliard, que je remercie vivement, ait accepté de rapporter sur mes travaux.

J'exprime ma très vive reconnaissance et toute ma gratitude à Madame Safya BELGHITH, Professeur à l'ENIT à qui j'adresse mes sincères remerciements pour avoir bien voulu accepter de rapporter sur mon travail et participer au Jury de ma thèse.

Je suis heureuse d'exprimer ma profonde gratitude à Monsieur José RAGOT, Professeur à l'Institut National Polytechnique de Lorraine et Directeur du Laboratoire d'Automatique et de Recherche Appliquée de L'Ecole Nationale Supérieure de Géologie de Nancy, pour avoir accepté de participer à mon Jury de thèse et évaluer mes travaux.

J'adresse ma plus profonde gratitude envers les membres du Laboratoire LARA Automatique de l'ENIT et ceux du Laboratoire LAGIS de l'EC-Lille pour leur accueil chaleureux et leur disponibilité qui m'ont permis de profiter d'un environnement agréable qui a facilité le bon déroulement et la finalisation de cette thèse.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Dans les dernières décennies, le domaine de l'informatique s'est fortement développé influençant ainsi toutes les branches des sciences modernes. Les automaticiens se sont donc intéressés à développer des méthodes donnant la possibilité de profiter des moyens puissants fournis par l'informatique. En conséquence, la commande numérique s'est répandue ces dernières années avec le développement des méthodes d'analyse et de synthèse pour les systèmes non linéaires à temps discret.
Ces méthodes posent souvent des problèmes aussi bien au niveau de la détermination d'un modèle que du choix des méthodes d'étude.
Pour les systèmes de grande dimension, la modélisation passe souvent par une phase de décomposition en sous-systèmes, qui, si elle est adoptée, peut ramener l'étude du processus complexe à l'étude plus simple de ces sous-systèmes. Il s'avère donc intéressant de chercher à mettre la matrice caractéristique du système étudié sous une forme adéquate aux méthodes d'études retenues. Le cas de la mise sous forme en flèche de ces matrices a, dans ce sens, déjà conduit à des résultats intéressants et importants.
C'est dans ce contexte que nous avons mené les travaux présentés qui concernent essentiellement l'étude de la stabilité et de la stabilisation des systèmes dynamiques non linéaires échantillonnés, qui, par la suite, sont adaptées à la résolution du problème de la synchronisation d'une classe de systèmes non linéaires au comportement très complexe qui sont les systèmes chaotiques à temps discret. Parmi les applications de la technique de synchronisation, nous trouvons les systèmes de transmission sécurisée de l'information exploitant les propriétés fondamentales des systèmes chaotiques.
La nouvelle approche est donc la détermination de lois de commande stabilisantes pour des fins de synchronisation, par réaction d'état ou de sortie, conférant au processus étudié la structure hiérarchisée à deux niveaux, et ce dans le cas discret.
Le présent mémoire est structuré en trois chapitres.
Après une introduction générale, mettant en relief l'objectif du présent travail, le premier chapitre de ce mémoire est consacré à la présentation de bases théoriques sur les

différentes classes de systèmes dynamiques échantillonnés non linéaires et plus précisément les systèmes chaotiques. Nous y présentons les propriétés importantes des systèmes chaotiques ainsi que l'étude et la synthèse de leur comportement. Ceci nécessite une étude à l'aide des outils de la dynamique non linéaire. Nous avons introduit aussi quelques propriétés importantes des matrices de formes en flèche ainsi que les notions utilisées et les principales méthodes d'étude de la stabilité des systèmes échantillonnés de grande dimension.

Dans le deuxième chapitre, l'élaboration de nouvelles conditions suffisantes de stabilisabilité de systèmes non linéaires discrets est envisagée sur la base de la description des systèmes par des matrices caractéristiques de forme en flèche et de l'utilisation d'une méthode d'étude de stabilité bien appropriée. Les critères élaborés, soit pour l'analyse de la stabilité soit pour la synthèse d'une loi de commande stabilisante par retour d'état ou de sortie, sont ensuite exploités, avec succès, pour la formulation de nouvelles conditions suffisantes de vérification des propriétés de synchronisation, d'anti-synchronisation ou de synchronisation hybride de systèmes chaotiques discrets. Ces propriétés sont d'un grand intérêt pour garantir une transmission sécurisée.

Les travaux effectués dans le troisième chapitre consistent, dans un premier temps, à étudier des systèmes de communication dont le cryptage des données repose sur les propriétés du chaos. Pour ces systèmes de cryptographie, il a été démontré que la synchronisation du point de vue de la théorie du contrôle est un problème de conception d'observateurs. Ainsi, un observateur, qui repose sur la description des systèmes par des matrices caractéristiques de forme en flèche, est élaboré en vue d'obtenir des conditions de synchronisation. Ces conditions ont montré leur efficacité dans les systèmes de communication choisis pour la phase de décryptage et la récupération de l'information. Dans un second temps, les travaux effectués consistent à tester la robustesse de l'observateur proposé à l'effet du bruit dans le canal de transmission.

Chapitre 1

Généralités sur l'analyse de systèmes discrets non linéaires

1.1 Introduction

Dans ce chapitre, nous commençons par introduire des notions relatives à la description des systèmes non linéaires échantillonnés et aux différentes représentations matricielles de tels systèmes. Ensuite, nous présentons un cas particulier de systèmes non linéaires : les systèmes chaotiques ainsi que certains outils d'analyse de tels systèmes. Des notions sur la stabilité et des méthodes générales d'étude de cette propriété sont ensuite considérées. Nous donnons, aussi, un bref aperçu sur la synchronisation à base d'observateurs et de retour d'état et sa liaison avec les méthodes générales d'étude de la stabilité. Nous finissons ce chapitre en posant le problème de la relation entre la synchronisation et les principes de la cryptographie par chaos.

1.2 Description des systèmes dynamiques étudiés

1.2.1 Notion de modèle

Un processus est un système dynamique susceptible d'évoluer en fonction d'une variable indépendante appelée temps [Borne *et al.*, 1992, Belghith, 1997]. Un processus est caractérisé par :

– des entrées de commande, qui sont des grandeurs physiques externes sur lesquelles il est possible d'agir et dont la variation contribue à l'évolution du comportement du système ;

- des entrées de perturbation sur lesquelles il n'est pas possible d'agir par l'utilisateur et qui agissent également sur le processus ;
- une ou plusieurs grandeurs de sortie, mesurables et plus ou moins détectables, qui constituent le résultat du processus des sorties ;
- des variables d'état, variables internes du système, dont l'action sur l'environnement n'est pas nécessairement directement perceptible, mais dont l'évolution régit celle du processus étudié.

1.2.2 Les systèmes dynamiques

Les systèmes dynamiques se différencient par la nature des signaux intervenant dans leur description. Ces types de systèmes sont classés en deux catégories : les systèmes dynamiques à temps discret et les systèmes dynamiques à temps continu.
Dans la suite, nous nommerons $x \in R^n$ le vecteur état et $u \in R^m$ le vecteur de commande.

1.2.2.1 Les systèmes à temps continu

Un système continu est celui dans lequel les signaux sont définis par rapport à une variable temps t continue. Ce système est décrit par un système d'équations différentielles de la forme :

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

$G : R^n \times R^m \times R^+ \rightarrow R^n$ caractérise la dynamique du système continu. t représente le temps $\in R^+$. A chaque couple choisi $(x(t_0)\,;\, t_0)$ et pour une commande $u(t)$ donnée, on peut associer une solution unique du système définie par l'équation (1.1) . L'evolution de l'état du système, en fonction du temps t, s'appelle la trajectoire.

1.2.2.2 Les systèmes à temps discret

Un système discret est celui dans lequel les signaux sont définis à des intervalles de temps discrets, pouvant être périodiques ou non. Ce type de système d'ordre n est représenté, dans le cas périodique, par l'équation d'état suivante :

$$x(k+1) = f(x(k), u(k), k) \tag{1.2}$$

où $f : R^n \times R^m \times N \rightarrow R^n$ est une fonction qui définit la dynamique du système discret et l'instant kT représente l'instant d'échantillonnage, T étant la période d'échantillonnage. Les systèmes que nous nous proposons d'étudier, dans la suite du mémoire, sont les

systèmes discrets. Un processus échantillonné est essentiellement caractérisé par un transfert de l'information à des instants discrets du temps. Si t_k désigne l'instant du $k^{\text{ème}}$ échantillonnage, l'état du système à $t = t_k$ peut être représenté par un vecteur $x_k = x(t_k) = x(kT)$, avec $x_k \in R^n$ et de composantes $x_i\,(k)$ $i = 1, 2, \ldots, n$.

1.3 Représentation des systèmes non linéaires à temps discret

Il est souvent nécessaire d'établir un modèle des processus étudiés. Modéliser le processus consiste, généralement, à établir un modèle mathématique qui correspond en fait à une approximation de la réalité du processus [EL-Moudni, 1985].
Le modèle mathématique doit satisfaire un compromis entre la complexité et la simplicité. Le modèle doit être suffisamment précis pour traduire fidèlement le comportement du processus. Il doit être, de plus, suffisamment simple pour qu'il puisse être mis en oeuvre avec les outils mathématiques disponibles d'analyse et de synthèse. Les modèles mathématiques, correspondant aux systèmes étudiés, sont en général des modèles d'état, des équations récurrentes, ou des fonctions de transfert, lorsqu'en particulier le processus est linéaire. Nous nous intéressons, dans ce mémoire, à deux catégories de modèles mathématiques récurrents, les équations scalaires et les représentations d'état.

1.3.1 Représentation scalaire

L'application des lois de la physique régissant l'évolution d'un processus non perturbé conduit, généralement dans le cas discret, à une équation récurrente de la forme :

$$h(y\,(k)\,, y\,(k+1)\,, ..., y(k+n), u\,(k)\,, u\,(k+1)\,, ..., u(k+m), k) = 0 \qquad (1.3)$$

Cette équation exprime directement la relation entre l'entrée $u\,(k)$ et la sortie $y\,(k)$, h étant une fonction non linéaire, et $m < n$.

1.3.2 Représentations vectorielles

Les systèmes étudiés, décrivant les modèles de systèmes physiques, sont supposés être régis par un ensemble d'équations récurrentes du premier ordre de la forme :

– d'une équation d'état :

$$x_i(k+1) = f_i(x_1(k), x_2(k), ..., x_n(k), u_1(k), u_2(k), ...u_m(k), k) \ \forall i = 1, \ldots, n \tag{1.4}$$

– d'une équation de sortie :

$$y_i(k) = g_i(x_1(k), x_2(k), ..., x_n(k), u_1(k), u_2(k), ...u_m(k), k) \ \forall i = 1, \ldots, l \tag{1.5}$$

expressions dans lesquelles f_i $(i = 1, 2, ..., n)$ et g_i $(i = 1, 2, ..., l)$ désignent des fonctions non linéaires des variables $x_j(k)$ $(j = 1, 2, ..., n)$ et $u_l(k)$ $(l = 1, 2, ..., m)$, $x_j(k) \in \mathbb{R}$ et $u_l(k) \in \mathbb{R}$. En notation vectorielle, ce modèle mathématique d'un système physique peut s'écrire comme suit :

– équation d'état :

$$x(k+1) = f(x(k), u(k), k) \tag{1.6}$$

– équation de sortie :

$$y(k) = g(x(k), u(k), k) \tag{1.7}$$

où $x(k)$, $y(k)$ et $u(k)$ représentent respectivement le vecteur d'état,
$x(k) = [x_1(k) \ x_2(k) \ ... \ x_n(k)]^T$, $x(k) \in \mathbb{R}^n$,
$y(k)$ le vecteur de sortie $y(k) = [y_1(k) \ y_2(k) \ ... \ y_l(k)]^T$, $y(k) \in \mathbb{R}^l$
et $u(k)$ le vecteur de commande $u(k) = [u_1(k) \ u_2(k) \ ... \ u_m(k)]^T$, $u(k) \in \mathbb{R}^m$.
Pour une large classe de processus, il est possible, en particulier pour les systèmes non linéaires, de représenter les systèmes comme suit :

$$x_i(k+1) = \sum_{j=1}^{n} a_{ij}(x(k), k) x_j(k) + \sum_{j=1}^{m} b_{ij}(x(k), k) u_j(k), \ i = 1, 2, \ldots, n \tag{1.8}$$

et :

$$y_i(k) = \sum_{j=1}^{n} c_{ij}(x(k), k) x_j(k) + \sum_{j=1}^{m} d_{ij}(x(k), k) u_j(k), \ i = 1, 2, \ldots, l \tag{1.9}$$

ou encore sous la forme matricielle :

$$\begin{aligned} x(k+1) &= A(x(k), k) x(k) + B(x(k), k) u(k) \\ y(k) &= C(x(k), k) x(k) + D(x(k), k) u(k) \end{aligned} \tag{1.10}$$

avec :

– $A(.)$: matrice carrée de dimension $n \times n$ et d'éléments a_{ij}, $\forall i, j = 1, 2, \ldots, n$,
– $B(.)$: matrice de dimension $n \times m$ et d'éléments b_{ij}, $\forall i = 1, 2, \ldots, n$, $\forall j = 1, 2, \ldots, m$,
– $C(.)$: matrice de dimension $l \times n$ et d'éléments c_{ij}, $\forall i = 1, 2, \ldots, l$, $\forall j = 1, 2, \ldots, n$,

– $D(.)$: matrice de dimension $l \times m$ et d'éléments d_{ij}, $\forall i = 1, 2, \ldots, l$, $\forall j = 1, 2, \ldots, m$,

Les éléments de ces matrices peuvent être linéaires ou non linéaires. Une représentation graphique de tels systèmes est donnée dans la figure.1.1

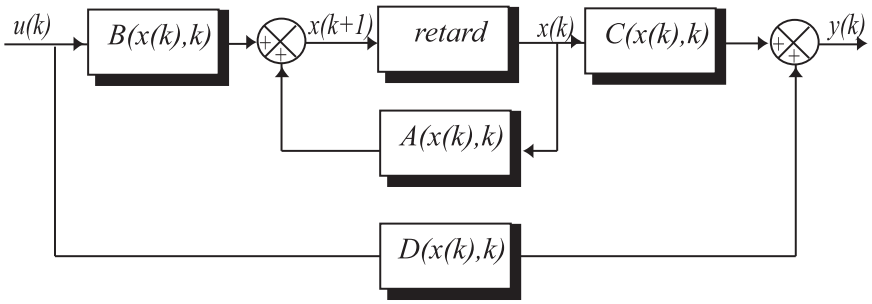


FIGURE 1.1 – Représentation d'état d'un système dynamique non linéaire.

1.3.2.1 Formes canoniques des matrices

Le choix des composantes du vecteur état peut être dicté par des considérations physiques ou mathématiques de façon à obtenir une matrice permettant une analyse performante des propriétés des systèmes (stabilité, commandabilité et observabilité). Un certain nombre de représentations, appelées formes canoniques, peut être rencontré dans la littérature ; on peut citer, les formes Compagnon et Frobénius, lorsque le polynôme caractéristique est connu, diagonale ou de Jordan, lorsque les modes peuvent être déterminés aisément [Rosenbroch et Storey, 1970] et en flèche [Benrejeb, 1980] lorsque les formes diagonales ou de Jordan ne sont pas réalisables sur le corps des réels.

– Matrice de forme Compagnon

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & & & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{bmatrix} \tag{1.11}$$

– Matrice de forme Frobénius

$$A = \begin{bmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix} \tag{1.12}$$

– Matrice de forme diagonale

$$A = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{bmatrix} \tag{1.13}$$

– Matrice de forme de Jordan avec v valeurs propres simples ou multiples distinctes

$$A = \begin{bmatrix} \lambda_1 & 1 & 0 & \dots & 0 & & & & & & & & \\ 0 & \lambda_1 & \ddots & \ddots & \vdots & & & & & & & & \\ \vdots & \ddots & \lambda_1 & 1 & 0 & & & & & & 0 & & \\ 0 & \dots & 0 & \lambda_1 & 1 & & & & & & & & \\ 0 & \dots & \dots & 0 & \lambda_1 & & & & & & & & \\ & & & & & \ddots & \ddots & & & & & & \\ & & & & & & \lambda_i & 1 & & & & & \\ & & & & & & & \ddots & & & & & \\ & & & & & & & & \lambda_v & 1 & 0 & \dots & 0 \\ & & & & & & & & 0 & \lambda_v & \ddots & \ddots & \vdots \\ & & 0 & & & & & & \vdots & \ddots & \lambda_v & 1 & 0 \\ & & & & & & & & 0 & \dots & 0 & \lambda_v & 1 \\ & & & & & & & & 0 & \dots & \dots & 0 & \lambda_v \end{bmatrix} \tag{1.14}$$

1.3.2.2 Formes en flèche de Benrejeb

a. Différents types de formes en flèche

La mise sous forme en flèche des matrices caractéristiques des systèmes correspond à une structure hiérarchisée à deux niveaux dépendant d'un certain nombre de paramètres pouvant être choisis arbitrairement et constitue, ainsi, un outil mathématique

pouvant faciliter le conditionnement de la représentation par rapport à la méthode d'étude choisie pour le système [Benrejeb, 1980].

Formes en Flèche Mince (FFM) :

La matrice caractéristique A est dite de forme en flèche mince notée A_{FFM}, si les éléments pouvant être non nuls sont répartis sur la diagonale principale, la dernière ligne et la dernière colonne de A.

– Forme en flèche mince de type I

$$A_{FFM} = \begin{bmatrix} a_{11} & & & a_{1n} \\ & \ddots & & \vdots \\ & & a_{n-1n-1} & a_{n-1n} \\ a_{n1} & \cdots & a_{nn-1} & a_{nn} \end{bmatrix} \tag{1.15}$$

– Forme en flèche mince de type II

Celle-ci peut être obtenue aisément à partir de la forme en flèche de type I :

$$A_{FFM} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \\ \vdots & & \ddots & \\ a_{n1} & & & a_{nn} \end{bmatrix} \tag{1.16}$$

Forme en Flèche Mince Généralisée (FFMG) :

Les matrices sont dites de forme en flèche mince généralisée, notées A_{FFMG}, d'ordre r, lorsque les éléments, pouvant être non nuls, sont isolés sur la diagonale principale, sur les $(n-r+1)$ dernières lignes et sur les $(n-r+1)$ dernières colonnes de telles matrices :

$$A_{FFMG} = \begin{bmatrix} a_{1,1} & & & & a_{1,r} & \cdots & & a_{1,n} \\ & \ddots & & & \vdots & & & \vdots \\ & & a_{r-1,r-1} & & a_{r-1,r} & \cdots & & a_{r-1,n} \\ a_{r,1} & \cdots & a_{r,r-1} & & a_{r,r} & \cdots & & a_{r,n} \\ \vdots & & \vdots & & \vdots & \ddots & & \vdots \\ a_{n1} & \cdots & & a_{n,r-1} & a_{n,r} & \cdots & & a_{n,n} \end{bmatrix} \tag{1.17}$$

Forme en Flèche Epaisse d'ordre r (FFE) :

La généralisation de la FFM peut être considérée lorsque les éléments pouvant

être non nuls sont isolés dans les blocs diagonaux, les dernières lignes et les dernières colonnes de la matrice considérée comme suit :

$$A_{FFE} = \begin{bmatrix} A_{11} & & & A_{1r} \\ & A_{22} & & A_{2r} \\ & & \ddots & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rr} \end{bmatrix} \tag{1.18}$$

b. Les systèmes dynamiques hiérarchisés - Interprétation structurelle

La caractérisation d'un système dynamique, en régime libre, par une matrice en flèche mince telle que, par exemple, la forme (1.15) permet la détermination d'une structure hiérarchisée à deux niveaux comme le montre la figure 1.2, associée à cette description [Benrejeb, 1980].

Le premier niveau étant composé de sous-systèmes S_i $\forall i = 1, 2, ..., n-1$, du premier ordre et dont les modes sont définis par les a_{ii} ; et le deuxième niveau est le sous-système S_n appelé dans ce cas coordonnateur, de mode instantané a_{nn}.

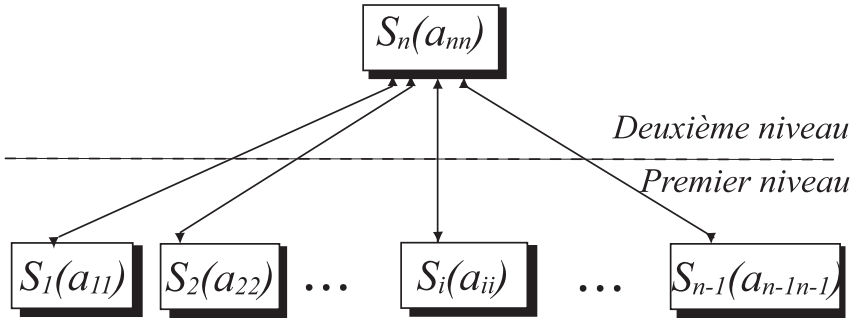


FIGURE 1.2 – Structure hiérarchisée à deux niveaux associée à une matrice caractéristique instantanée en flèche mince.

c. Opérations sur les matrices de forme en flèche

Calcul du déterminant d'une matrice en flèche mince : Le déterminant de la matrice A_{FFM} en flèche mince [Benrejeb, 1980], définie par (1.19), est égal à :

$$\det(A_{FFM}) = (a_{nn} - \sum_{i=1}^{n-1} \frac{a_{ni}a_{in}}{a_{ii}}) \prod_{i=1}^{n-1} a_{ii} \tag{1.19}$$

Calcul de l'inverse d'une matrice en flèche mince : Si a_{ij} est l'élément de la ième ligne et de la jème colonne de la matrice A_{FFM} [Benrejeb, 1980], définie

par (1.19), les éléments de la matrice A_{FFM}^{-1}, notés a_{ij}^{*}, peuvent être exprimés par :

$$a_{nn}^{*} = \left(a_{nn} - \sum_{i=1}^{n-1} a_{ni} a_{in} a_{ii}^{-1} \right)^{-1} \tag{1.20}$$

$$a_{ij}^{*} = a_{ii}^{-1} a_{in} a_{nn}^{*} a_{nj} a_{jj}^{-1} \ \forall i, j = 1, \ldots, n-1, \ i \neq j \tag{1.21}$$

$$a_{nj}^{*} = -a_{nn}^{*} a_{nj} a_{jj}^{-1} \ \forall j = 1, \ldots, n-1 \tag{1.22}$$

$$a_{in}^{*} = -a_{ii}^{-1} a_{in} a_{nn}^{*} \ \forall i = 1, \cdots, n-1 \tag{1.23}$$

$$a_{ii}^{*} = a_{ii}^{-1} (1 + a_{in} a_{nn}^{*} a_{ni} a_{ii}^{-1}) \ \forall i = 1, \ldots, n-1 \tag{1.24}$$

Remarque 1.1. *L'inverse explicite d'une matrice en forme en flèche mince* (1.19) *peut être exploîté pour déterminer, d'une manière également explicite, les matrices caractéristiques de la représentation d'état discrète (respectivement continue) à partir de la représentation d'état continue (respectivement discrète), et ceci en utilisant, par exemple, la transformation homographique [Soudani, 1997].*

d. Passage aux matrices de forme en flèche mince de Benrejeb

– Cas d'une matrice initiale de forme Compagnon

Considérons le système non linéaire (S) dont l'évolution est régie, en régime libre, par la représentation d'état suivante :

$$x(k+1) = A(x(k), k)\, x(k) \tag{1.25}$$

la matrice $A(x(k), k)$ étant de forme Compagnon (1.26) et $a_i(x(k), k), \forall i = 1, \ldots, n-1$ des éléments pouvant être non linéaires :

$$A(x(k), k) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & & & 0 & 1 \\ -a_0(.) & -a_1(.) & \cdots & -a_{n-2}(.) & -a_{n-1}(.) \end{bmatrix} \tag{1.26}$$

Considérons le changement de variables de matrice de passage P définie par (1.27), [Benrejeb, 1980] :

$$x(k) = P z(k) \tag{1.27}$$

telle que :

$$P = \begin{bmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & 0 \\ (\alpha_1)^2 & (\alpha_2)^2 & \dots & (\alpha_{n-1})^2 & \vdots \\ \vdots & \vdots & & \vdots & 0 \\ (\alpha_1)^{n-1} & (\alpha_2)^{n-1} & \dots & (\alpha_{n-1})^{n-1} & 1 \end{bmatrix} \tag{1.28}$$

et :

$$\alpha_i \neq 0, \alpha_i \neq \alpha_j \; \forall i \neq j \tag{1.29}$$

Il conduit à la nouvelle matrice caractéristique de forme en flèche mince de Benrejeb A_{FFM} comme suit :

$$A_{FFM}\left(x\left(k\right),k\right) = \begin{bmatrix} \alpha_1 & & & \beta_1 \\ & \ddots & & \vdots \\ & & \alpha_{n-1} & \beta_{n-1} \\ \gamma_1\left(x\left(k\right),k\right) & \dots & \gamma_{n-1}\left(x\left(k\right),k\right) & \gamma_n\left(x\left(k\right),k\right) \end{bmatrix} \tag{1.30}$$

avec :

$$\beta_i = \prod_{\substack{j=1 \\ i \neq j}}^{n-1} \left(\alpha_i - \alpha_j\right)^{-1} \; \forall i = 1, \dots, n-1 \tag{1.31}$$

$$\gamma_i(., \alpha_i) = -P_A(., \alpha_i) \; \forall i = 1, 2, \dots, n-1 \tag{1.32}$$

$$\gamma_n(., \sum_{i=1}^{n-1} \alpha_i) = \gamma_n(.) = -a_{n-1}(.) - \sum_{i=1}^{n-1} \alpha_i \tag{1.33}$$

dans laquelle les paramètres α_{ii}, $\forall i = 1, \dots, n-1$, peuvent être choisis arbitrairement non nuls, satisfaisant toutefois les conditions (1.29) et le polynôme $P_A\left(., \lambda\right)$ est défini par :

$$P_A(., \lambda) = \lambda^n + \sum_{i=0}^{n-1} a_i(.)\lambda^i \tag{1.34}$$

– Cas d'une matrice initiale de forme quelconque : Considérons les systèmes discrets linéaires monovariables représentés dans l'espace d'état par :

$$x\left(k+1\right) = Ax\left(k\right) + Bu\left(k\right) \tag{1.35}$$

où A et B sont deux matrices à paramètres constants de formes quelconques constituant une paire commandable.

Soit $P_A(\lambda)$ le polynôme caractéristique de la matrice A, comme suit :

$$P_A(\lambda) = \lambda^n + \sum_{i=0}^{n-1} a_i \lambda^i \tag{1.36}$$

Le passage de la représentation d'état d'une forme quelconque de la matrice caractéristique à la forme en flèche mince de Benrejeb, peut être formulé par le théorème suivant [Gasmi, 2001].

Théorème 1.1. *Le changement de base H, tel que* $x(k) = Hz(k)$*, et*

$$H = \begin{bmatrix} H^1 & H^2 & \dots & H^n \end{bmatrix} \tag{1.37}$$

avec :

$$\begin{cases} H^i = \left(A^{n-1} + \sum_{k=1}^{n-1} \mu_{ki} A^{k-1} \right) B \ \forall i = 1, \dots, n-1 \\ H^n = B \end{cases} \tag{1.38}$$

et :

$$\mu_{ki} = a_k + \alpha_{ii}^{n-k} + \sum_{j=1}^{n-k-1} a_{k+j} \alpha_{ii}^{j} \quad \forall i, k = 1, \dots, n-1 \tag{1.39}$$

où les paramètres α_{ii}*,* $\forall i = 1, \dots, n-1$*, sont des paramètres choisis arbitrairement distincts et non nuls, permettant ainsi de décrire le processus* (1.35) *par l'équation d'état :*

$$z(k+1) = A_f z(k) + Gu(k) \tag{1.40}$$

où $A_f(.)$ *est une matrice caractéristique de forme en flèche mince de Benrejeb avec les notations* (1.30) , (1.31), (1.32), (1.33) *et G est un vecteur colonne, décrit comme suit :*

$$G = \begin{bmatrix} 0 & \dots & 0 & 1 \end{bmatrix}^T \tag{1.41}$$

1.3.3 Cas d'inaccessibilité de variables d'état - Observateurs d'état

Étant donné que les variables mesurées directement ne peuvent généralement couvrir la totalité des grandeurs susceptibles de décrire le comportement du procédé, à savoir les états, il est souvent recommandé de reconstituer l'information non mesurée directement à partir de celle disponible ; c'est dans ce cadre que nous avons eu recours à la conception d'observateurs.

1.3.3.1 Observabilité des systèmes non linéaires à temps discret

Un observateur est un système dynamique qui permet de reconstruire les variables d'état non mesurées dans le cas d'une insuffisance de capteurs physiques capables de les mesurer (figure 1.3).

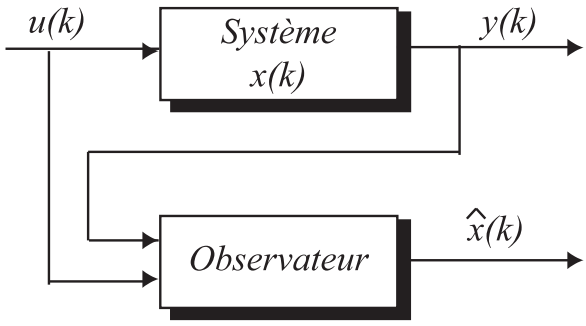


FIGURE 1.3 – Principe d'un observateur

A partir d'une commande, notée $u(k)$, l'observateur permet de faire correspondre les sorties mesurées du système, $y(k)$, et les prédictions du modèle $\hat{y}(k)$. L'observateur fournit $\hat{x}(k)$ l'estimation de l'état réel $x(k)$ du système.
Le problème de synthèse d'observateurs peut être présenté comme suit.
Soit le système non linéaire représenté dans l'espace d'état par :

$$\begin{cases} x(k+1) = f(x(k), u(k)) \\ y(k) = g(x(k), u(k)) \end{cases} \tag{1.42}$$

$x(k) \in R^n$ étant le vecteur d'état, $u(k) \in R^m$ le vecteur d'entrée, $y(k) \in R^l$ le vecteur de sortie, et $x(0) = x_0$ le vecteur conditions initiales.

Définition 1.1. *(Observateur).*
Afin de construire l'estimation des états du vecteur $x(k)$, on est amené à effectuer un choix judicieux des fonctions Φ et Ψ, telles que le système dynamique, représenté par :

$$\begin{cases} z(k+1) = \Phi(z(k), u(k), y(k)) \\ \hat{x}(k)(k) = \Psi(z(k), u(k), y(k)) \end{cases} \tag{1.43}$$

avec $z(k) \in R^q$, $q \leq n$, $z(0) = z_0$ les conditions initiales, $u(k)$ et $y(k)$ les entrées de ce système, $\hat{x}(k) \in R^n$ la sortie qui est l'état estimé, vérifie les deux hypothèses suivantes [Besançon, 2007] :

- *si $\hat{x}(k_0) = x(k_0)$, alors on a : $\hat{x}(k) = x(k)$, $k \geq k_0$*

– *sinon l'erreur d'estimation* $e(k)$, $e(k) = \hat{x}(k) - x(k)$, *tend asymptotiquement vers zéro,*

alors le système (1.43) est un observateur du système (1.42), d'ordre plein si $q = n$ et d'ordre réduit si $q < n$

Pour étudier la convergence de l'observateur d'un système, des outils concernant la stabilité des systèmes dynamiques discrets sont utilisés. Ces outils sont détaillés ultérieurement dans ce mémoire.

Il existe des techniques d'estimation non linéaires qui ont été mises en oeuvre dans la littérature [Besançon, 2007, Primbs, 1996]. On envisage de détailler l'observateur de Luenberger qu'on utilisera ultérieurement dans le prochain chapitre.

1.3.3.2 Différents types d'observateurs

Observateur de Luenberger [Luenberger, 1971] La théorie de l'observation de Luenberger repose essentiellement sur des techniques de placement de pôles.

Soit le système linéaire représenté dans l'espace d'état par :

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + D\omega(k) \\ y(k) = Cx(k) + v(k) \end{cases} \tag{1.44}$$

avec $x(k) \in R^n$, $u(k) \in R^m$, $y(k) \in R^p$. $\omega(k) \in R^r$ et $v(k) \in R^p$ sont deux bruits blancs gaussiens d'espérances nulles, de covariances respectives Q et R. Ces bruits sont supposés non corrélés. Les matrices du système sont de dimensions appropriées et les conditions initiales définies par $x(0) = x_0$.

Dans le cas déterministe (les bruits $\omega(k)$ et $v(k)$ sont nuls), Luenberger propose l'observateur suivant pour le système (1.44) :

$$\hat{x}(k+1) = A\hat{x}(k) + Bu(k) + L(y(k) - C\hat{x}(k)) \tag{1.45}$$

La dynamique de l'erreur d'estimation $e(k)$, $e(k) = \hat{x}(k) - x(k)$, est représentée par :

$$e(k+1) = (A - LC)e(k) \tag{1.46}$$

Un choix convenable du gain L de l'observateur, basé sur des techniques de stabilisation que nous détaillerons ultérieurement, permet d'assurer, la convergence de $\hat{x}(k)$ vers l'état $x(k)$, si les valeurs propres de la matrice $(A - LC)$ sont à l'intérieur du cercle unité.

Pour la conception d'observateurs des systèmes non linéaires, il faut noter qu'il n'existe pas une technique de conception commune pour tous les types de systèmes. Ainsi, il existe plusieurs approches pour la conception des observateurs des systèmes non linéaires. Certaines d'entre elles ont essayé d'appliquer directement la théorie des observateurs linéaires. De ce fait, la plupart des techniques élaborées dans la littérature s'inspirent des approches de synthèse d'observateurs linéaires en les généralisant au cas non linéaire. En effet, dans de nombreuses références, la structure des observateurs non linéaires proposés est basée sur celle de l'observateur de Luenberger, auquel on associe des hypothèses supplémentaires telles que la condition de Lipschitz et cela pour faire face aux termes non linéaires [Primbs, 1996].

1.4 Cas des systèmes chaotiques

1.4.1 Espaces de phases de systèmes chaotiques et hyperchaotiques

L'espace des phases décrit l'évolution de l'état des variables dynamiques indépendantes du système, en faisant abstraction du temps. Les variables utilisées pour le tracé du diagramme des phases doivent représenter chacune un degré de liberté du système. La figure obtenue en traçant la trajectoire dynamique dans cet espace, après suppression des transitoires, représente l'attracteur du système. L'attracteur associé à un régime de point fixe stable est un point. Lorsque le système évolue vers un régime périodique, la forme de l'attracteur change et devient une courbe fermée. A un régime chaotique correspond un attracteur avec une forme caractéristique dans l'espace des phases.

Cas de l'attracteur chaotique de Ikeda : L'attracteur bidimensionnel chaotique Ikeda [Ikeda, 1979], considéré en optique par le médecin Ikeda, est donné par la représentation d'état suivante :

$$\begin{cases} x_1(k+1) = 1 + u\left(x_1(k)\cos(\theta(k)) - x_2(k)\sin(\theta(k))\right) \\ x_2(k+1) = u\left(x_1(k)\sin(\theta(k)) + x_2(k)\cos(\theta(k))\right) \\ \theta(k) = 0.4 - \frac{6}{1+x_1^2(k)+x_2^2(k)} \end{cases} \tag{1.47}$$

La figure 1.4 présente un comportement chaotique de cet attracteur pour $u = 0.9$ et pour l'état initial (0.1,0.1).

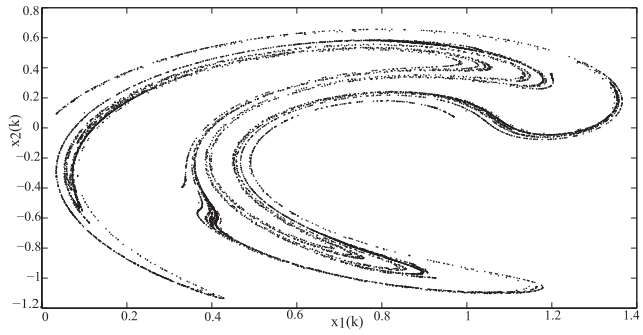


FIGURE 1.4 – Attracteur de Ikeda de dimension 2

Cas de l'attracteur chaotique de Hénon : L'attracteur de Hénon est un système dynamique à temps discret de dimension 2 [Hénon, 1976] dont la représentation d'état est la suivante :

$$\begin{cases} x_1(k+1) = a - x_1^2(k) + bx_2(k) \\ x_2(k+1) = x_1(k) \end{cases} \tag{1.48}$$

Pour les valeurs $a = 1.4$ et $b = 0.3$, cet attracteur présente un comportement chaotique.

La figure 1.5 présente un comportement chaotique de cet attracteur pour l'état initial (1,0.1).

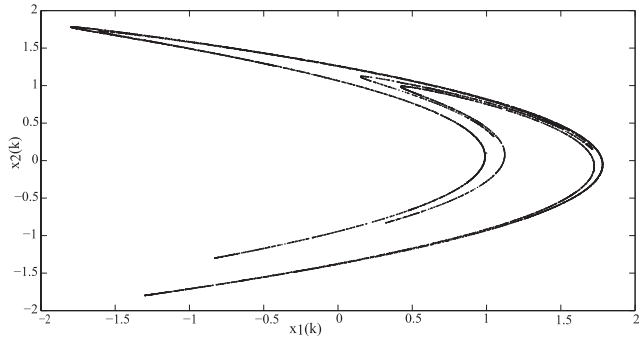


FIGURE 1.5 – Attracteur de Hénon de dimension 2

Cas de l'attracteur chaotique de Lozi : L'attracteur de Lozi [Peitgen *et al.*, 2004], de dimension 2, admet la représentation d'état suivante :

$$\begin{cases} x_1(k+1) = -a|x_1(k)| + x_2(k) + 1 \\ x_2(k+1) = bx_1(k) \end{cases} \tag{1.49}$$

avec : $a = 1.7$ et $b = 0.5$. La figure. 1.6 présente son comportement chaotique pour l'état initial (1,0.1).

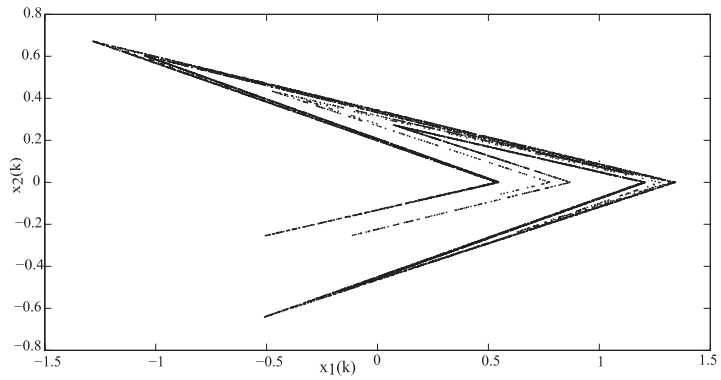


FIGURE 1.6 – Attracteur de Lozi de dimension 2

Cas de l'attracteur hyperchaotique généralisé de Hénon (Baier-Klein) : Il est représenté par [Grassi et Miller, 2002, Baier et Klein, 1990] :

$$\begin{cases} x_1(k+1) = b - x_2^2(k) - a.x_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \tag{1.50}$$

avec : $a = 0.1$ et $b = 1.76$.

La figure 1.50 montre un attracteur hyperchaotique dans un espace tridimensionnel, pour 10 000 itérations avec les valeurs initiales $x(0) = (1, 0.1, 0)$.

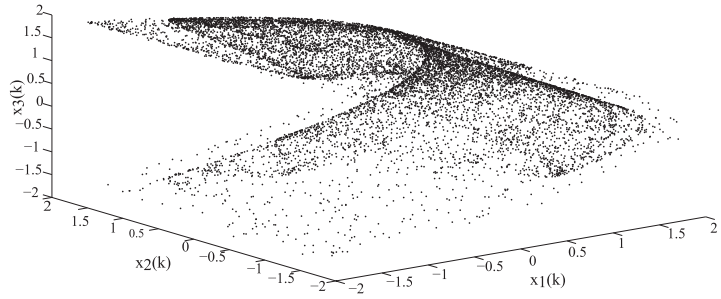


FIGURE 1.7 – Attracteur hyperchaotique de Hénon (Baier-Klein)

Cas de l'attracteur hyperchaotique de Hénon (Hitzl-Zele) : cet attracteur découvert par Hitzl et Zele [Y.J. Xue, 2003, Hitzl et Zele, 1985] est décrit comme :

$$\begin{cases} x_1(k+1) = -b_1 x_2(k) \\ x_2(k+1) = 1 + x_3(k) - a_1 x_2^2(k) \\ x_3(k+1) = b_1 x_2(k) + x_1(k) \end{cases} \tag{1.51}$$

avec : $a_1 = 1.07$ et $b_1 = 0.3$.

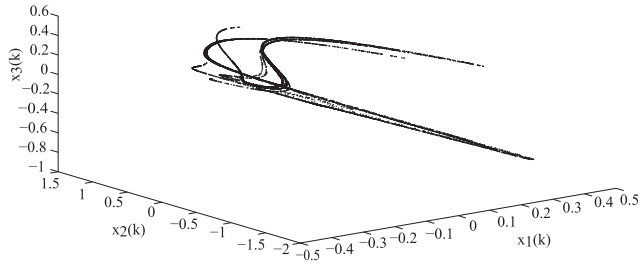


FIGURE 1.8 – Attracteur hyperchaotique de Hénon (Hitzl-Zele)

La figure 1.8 montre un attracteur hyperchaotique dans un espace tridimensionnel, pour 10 000 itérations avec les valeurs initiales $x(0) = (0.2, 0.7, 0.06)$.

Cas de l'attracteur hyperchaotique de Rössler : Il est représenté par :

$$\begin{cases} x_1(k+1) = \alpha x_1(k)(1 - x_1(k)) - \beta(x_3(k) + \gamma)(1 - 2x_2(k)) \\ x_2(k+1) = \delta x_2(k)(1 - x_2(k)) + \zeta x_3(k) \\ x_3(k+1) = \eta((x_3(k) + \gamma)(1 - 2x_2(k)) - 1)(1 - \theta x_1(k)) \end{cases} \tag{1.52}$$

avec $\alpha = 3.8, \beta = 0.05, \gamma = 0.35, \delta = 3.78, \zeta = 0.2, \eta = 0.1$ et $\theta = 1.9$.
L'attracteur Rössler présente une dynamique hyperchaotique. La figure 1.9 montre un attracteur hyperchaotique dans un espace tridimensionnel, pour 10000 itérations et pour $x(0) = (0.1, 0.2, -0.1)$.

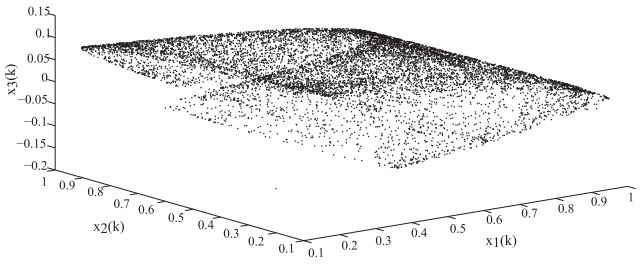


FIGURE 1.9 – Attracteur de Rössler

1.4.2 Définitions du chaos

Une dynamique non linéaire stationnaire correspondant à un système peut être représentée sous la forme suivante :

$$x\left(k+1\right)=f\left(x\left(k\right)\right) \tag{1.53}$$

$x(0)$ étant l'instant initial, $x\left(k\right)\in R^{n}$ le vecteur d'état et n correspondant à la dimension du système. Celui-ci est dit stationnaire quand l'instant discret k n'apparaît pas explicitement dans l'équation (1.53).

A partir de la condition initiale $x(0)$, la solution de (1.53) est une séquence de points appelée espaces de phase, ou orbite. L'évolution temporelle de l'état est complètement déterminée à partir de l'état initial $x(0)$ et de la dynamique du système. La séquence, ainsi itérée peut atteindre des états stationnaires qui peuvent coexister ; les plus répandus sont :

- l'état stationnaire : appelé aussi point d'équilibre ou point fixe tel que :
  $x\left(k+1\right)=x\left(k\right)=x^{*}$
- l'orbite périodique : correspondant à des cycles d'ordre fini K^{0} et obéissant à :
  $x\left(k+K^{0}\right)=x\left(k\right)$ et $x\left(k+K'^{0}\right)\neq x\left(k\right)$, $\forall\ k$, pour $K'^{0}<K^{0}$
- l'orbite chaotique : pouvant être considérée comme une trajectoire de période infinie obéissant donc à :
  $x\left(k+K^{0}\right)\neq x\left(k\right)\ \forall K^{0}$ et $x\left(k\right)$ borné.

Cette relation n'est pas suffisante pour définir formellement le chaos. Dans ce qui suit, une définition stricte du chaos est donnée.

Soit $(I\in R,l)$ désignant un espace métrique compact (l est une distance) et soit f la fonction continue non linéaire définissant l'attracteur :

$$f:I\rightarrow I\quad x\left(k+1\right)=f\left(x\left(k\right)\right),\ x\left(0\right)\in I \tag{1.54}$$

Avant de donner la définition du chaos, due à R.L. Devaney [Devaney, 1989], quelques définitions de base sont nécessaires.

Définition 1.2. *f est dite avoir la propriété de sensibilité aux conditions initiales s'il existe $\delta > 0$ tel que, pour tout $x(0) \in I$ et tout $\varepsilon > 0$, il existe un point $y(0) \in I$ et un entier $j \geq 0$ satisfaisant :*

$$l(x(0), y(0)) > \varepsilon \Rightarrow d\left(f^{(j)}(x(0)), f^{(j)}(y(0))\right) > \delta \tag{1.55}$$

où l représente la distance et $f^{(j)}$ la j ème itération de f.

Définition 1.3. *f est dite topologiquement transitive, si U et V étant deux ensembles non vides ouverts dans I, il existe $x(0) \in U$ et un indice $j \in Z^+$, tel que pour $f^{(j)}(x(0)) \in V$ ou, de façon équivalente, il existe un indice $j \in Z^+$, telle que $f^{(j)}(U) \cap V \neq \emptyset$.*

On est maintenant en position d'énoncer la définition d'un système chaotique, au sens de Devaney.

Définition 1.4. *Une fonction continue $f : I \to I$ est dite constituée une dynamique chaotique si :*

- *f est sensible aux conditions initiales ;*
- *f est topologiquement transitive ;*
- *l'ensemble des points périodiques de f est dense dans I.*

Pour déterminer la sensibilité aux conditions initiales d'un système dynamique, on peut avoir recours à la notion d'exposants de Lyapunov, introduite dans les parties qui suivent.

1.4.3 Caractérisation du chaos

La théorie du chaos traîte des systèmes dynamiques déterministes qui présentent un phénomène fondamental d'instabilité appelé «sensibilité aux conditions initiales» ; cela les rend non prédictibles en pratique sur le «long» terme. Le chaos est défini généralement comme un comportement semblant aléatoire (ou imprévisible) d'un système dynamique défini par des équations déterministes. Un système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état $x(k) \in R^n$, $x(k) = \{x_i(k) \in R\}$, $i = 1, \ldots, n$, n étant la dimension de ce vecteur. On appelle vecteur état d'un système l'ensemble des variables qui, étant connues à l'instant initial, permettent de décrire l'évolution de ce système dans le temps. Le processus évolue de manière déterministe si ses états futurs sont caractérisés par la connaissance de ses états présents et passés. La loi d'évolution

dans le temps de ce système dynamique est généralement désignée par "dynamique". La notion de déterminisme provient aussi du fait que le système est caractérisé par son état initial et sa dynamique.

1.4.3.1 Spectre et autocorrélation

Le comportement des systèmes dynamiques non linéaires étudiés évolue en fonction de paramètres de bifurcation. Pour caractériser le comportement chaotique, il est nécessaire de chercher le spectre et la fonction d'autocorrélation.
En ce qui concerne le calcul du spectre du signal, il s'agit de l'extraction des composantes fréquentielles d'un signal, par utilisation de la transformée de Fourier de ce signal.

$$S(k) = \sum_{n=0}^{N-1} s(n)\, e^{-2i\pi k \frac{n}{N}} \quad pour\ 0 \leq k \leq N \tag{1.56}$$

En ce qui concerne la fonction d'autocorrélation, elle est définie par :

$$R(j) = \sum_{n} (x(n) - m)(x(n-j) - m) \tag{1.57}$$

m étant la valeur moyenne de $x(n)$.
Cette fonction mesure la ressemblance de la variable x, noté $x(n)$ à un instant donné nT, avec sa valeur à un instant antérieur $(n-j)T$. En faisant varier progressivement l'intervalle j, on construit la fonction $R(j)$ qui traduit le taux de similitude du signal avec lui-même quand le temps s'écoule. Si $x(n)$ est constante, périodique ou quasi-periodique, $R(j)$ ne tendra pas vers zéro quand j tendra vers l'infini ; car, dans ce cas, le spectre de Fourier est formé de raies distinctes. Les signaux périodiques (ou quasi-périodiques) gardent donc leur similitude interne quand le temps s'écoule. Le comportement du système est prédictible puisque sa connaissance, pendant un laps de temps suffisant, permet de savoir, par simple comparaison, ce qu'il sera à tout instant ultérieur. Par contre, dans un régime chaotique, $R(j)$ tend vers zéro quand j augmente.
La figure 1.10 présente les trois fonctions d'autocorrélation des trois variables d'état du système (1.10) pour 10000 itérations. L'état initial choisi pour chaque simulation est $x(0) = (1, 0.1, 0)$. D'après cette figure, nous pouvons conclure que les signaux chaotiques présentent une ressemblance à du bruit. En effet, la fonction d'autocorrélation d'un bruit blanc est un pic de Dirac, ce que nous avons retrouvé sur la figure 1.10 où nous apercevons l'allure de ce type de pic. Cependant, nous ne pouvons certainement pas conclure qu'un signal chaotique est un bruit blanc.

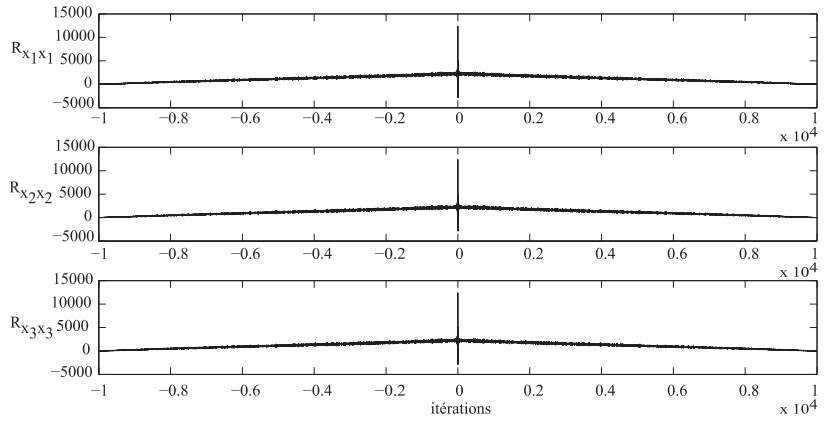


FIGURE 1.10 – Fonctions d'autocorrélation des trois états du système de Hénon généralisé (Baier-Klein)

1.4.3.2 Diagrammes de bifurcation

La transition vers le chaos peut être expliquée à l'aide d'un diagramme appelée "diagramme de bifurcation".
Prenons l'exemple de la récurrence de Hénon 2D, dont la représentation d'état est donnée par (1.48) et dont le diagramme de bifurcation est présenté dans la figure 1.11, le paramètre a étant variable.

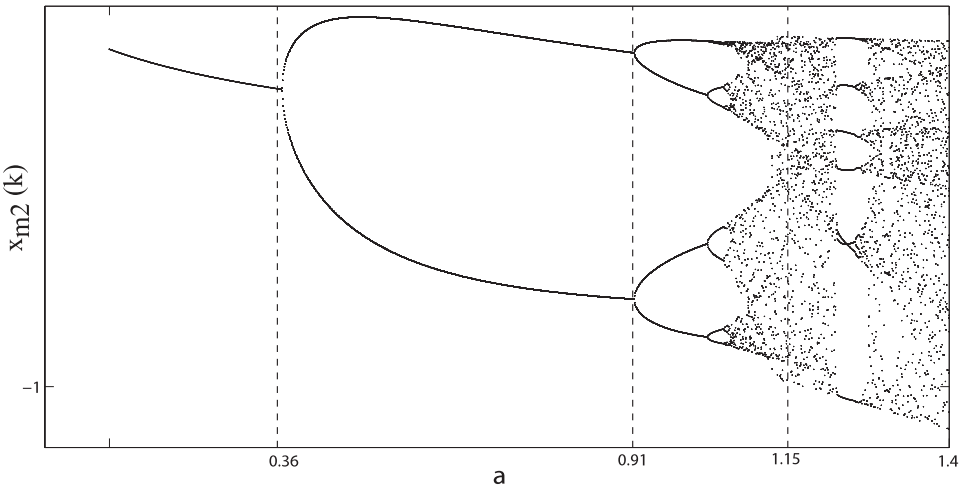


FIGURE 1.11 – Diagramme de bifurcation de l'attracteur de Hénon de dimension 2

- Pour : $0 < a < 0.36$, le système possède un point fixe stable ;
- Pour : $0.36 < a < 0.91$, le point fixe se déstabilise et un cycle d'ordre 2 stable apparaît ;

– Pour : $0.91 < a < 1.15$, le cycle d'ordre 2 se déstabilise et un cycle d'ordre 4 stable apparaît.

On peut noter sur la figure (1.12) relative à (1.50) que le comportement est plus complexe que le comportement chaotique de la figure (1.11). En effet, le système de Hénon (Baier-Klein) de dimension 3 présente un comportement hyperchaotique favorisant la complexité observée dans les deux figures.

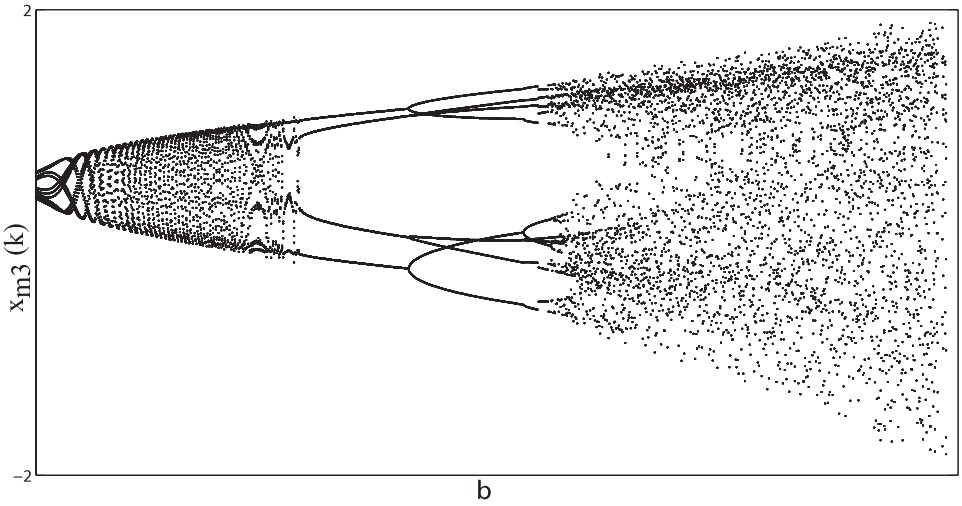


FIGURE 1.12 – Diagramme de bifurcation de l'attracteur de Hénon (Baier-Klein) de dimension 3

1.4.3.3 Exposants de Lyapunov

Les exposants de Lyapunov sont des coefficients qui permettent de mesurer la sensibilité aux conditions initiales d'une série temporelle. C'est le taux de divergence entre deux trajectoires distinctes qui ont commencé à partir de deux conditions initiales très proches. Cette propriété de sensibilité aux états initiaux garantit la propriété de diffusion, très importante dans les systèmes de sécurité de l'information.

Le calcul des exposants de Lyapunov utilise un système efficace basé sur la méthode QR [Bremena *et al.*, 1997].

Soit le système non linéaire dynamique à temps discret suivant :

$$x(k+1) = f(x(k)) \tag{1.58}$$

avec : $x(k) \in R^n$. Nous supposons que la trajectoire émanant d'un état initial $x(0)$ atteint un attracteur. $x(k)$ est ainsi bornée à l'intérieur de l'attracteur.

Considérons le cas d'un système de dimension 1.
Nous choisissons deux conditions initiales très proches, notées $x(0)$ et $x'(0)$, et nous regardons comment se comportent les trajectoires qui en sont issues. En supposant que les deux trajectoires $x(k)$ et $x'(k)$ s'écartent, en moyenne, à un rythme exponentiel, après k itérations, il vient :

$$|x'(k) - x(k)| = |x'(0) - x(0)| e^{k\lambda} \tag{1.59}$$

λ indique le taux de divergence par itération des deux trajectoires dont l'expression est la suivante :

$$\lambda = \frac{1}{k} \ln \left| \frac{x'(k) - x(k)}{x'(0) - x(0)} \right| \tag{1.60}$$

Pour $x(0)$ et $x'(0)$ proches, si le module de la différence $\varepsilon = |x'(0) - x(0)|$ a tendance à converger vers zéro, on obtient :

$$\lambda_L = \lim_{k\to\infty} \lim_{\varepsilon\to 0} \frac{1}{k} \ln \left| \frac{x'(k) - x(k)}{x'(0) - x(0)} \right| \tag{1.61}$$

Cela donne :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\varepsilon\to 0} \ln \left| \frac{x'(k) - x(k)}{x'(k-1) - x(k-1)} . \frac{x'(k-1) - x(k-1)}{x'(k-2) - x(k-2)} \cdots \frac{x'(1) - x(1)}{x'(0) - x(0)} \right| \tag{1.62}$$

et :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\varepsilon\to 0} \sum_{i=0}^{k-1} \ln \left| \frac{x'(i+1) - x(i+1)}{x'(i) - x(i)} \right| = \lim_{k\to\infty} \frac{1}{k} \lim_{\varepsilon\to 0} \sum_{i=0}^{k-1} \ln \left| \frac{f(x'(i)) - f(x(i))}{x'(i) - x(i)} \right| \tag{1.63}$$

Finalement, on a :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\varepsilon\to 0} \sum_{i=0}^{k-1} \ln \left| \frac{df(x(i))}{dx(i)} \right| \tag{1.64}$$

λ_L, appelé exposant de Lyapunov, mesure le taux moyen de divergence de deux trajectoires distinctes, à partir de deux conditions initiales très proches.
Pour le cas d'un système de dimension $n > 1$, le système possède n exposants de Lyapunov $\lambda_L^{(j)}$ $(j = 1, \ldots, n)$. Chacun d'entre eux mesure le taux de divergence, suivant un des axes de l'espace de phase.
Pour le calcul de l'exposant de Lyapunov, nous partons d'un point initial $x(0) \in R^n$, pour caractériser le comportement infinitésimal autour du point $x(k)$ par la première matrice dérivée $Df(x(i))$:

$$Df(x(i)) = \begin{bmatrix} \frac{\partial f_1 x(i)}{\partial x_1(i)} & \cdots & \frac{\partial f_1 x(i)}{\partial x_n(i)} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_n x(i)}{\partial x_1(i)} & \cdots & \frac{\partial f_n x(i)}{\partial x_n(i)} \end{bmatrix} \tag{1.65}$$

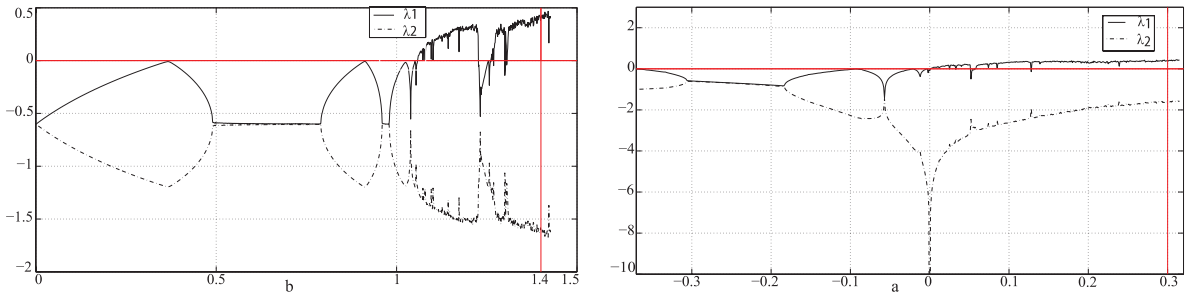
Notons $J_k = Df\left(x\left(k-1\right)\right)\cdots Df\left(x\left(0\right)\right)$, avec : $J_0 = Df\left(x\left(0\right)\right)$.
L'exposant de Lyapunov est calculé par l'expression suivante :

$$\lambda_{Li} = \lim_{k\to\infty} \frac{1}{k} \ln\left|\lambda_i\left(J_k \ldots J_1\right)\right|, \ \forall i = 1, \ldots, n \tag{1.66}$$

En analysant l'exposant de Lyapunov d'un système non linéaire, nous pouvons conclure sur le type du comportement dynamique d'un système, c'est-à-dire nous pouvons indiquer s'il s'agit d'un comportement hyperchaotique, chaotique ou d'un régime périodique [Parker et Chua, 1989] :

- dans le cas où on a : $\lambda_n \leq \ldots \leq \lambda_1 < 0$: il existe des points d'équilibre asymptotiquement stables,
- dans le cas où on a : $\lambda_1 = 0, \lambda_n \leq \ldots \leq \lambda_2 < 0$, l'attracteur est un cycle limite asymptotiquement stable,
- dans le cas où on a : $\lambda_1 = \ldots \lambda_2 = 0, \lambda_n \leq \ldots \leq \lambda_3 < 0$, l'attracteur est un tore de dimension 2, c'est-à-dire quasi-périodique (2 fréquences),
- dans le cas où on a : $\lambda_1 = \ldots \lambda_k = 0, \lambda_n \leq \ldots \leq \lambda_{k+1} < 0$, l'attracteur est un tore de dimension k, c'est-à-dire quasi-périodique (k fréquences),
- dans le cas où on a : $\lambda_1 > 0, \sum_i \lambda_i < 0$, l'attracteur est chaotique,
- dans le cas où on a : $\lambda_1 > \ldots \lambda_k > 0, \sum_i \lambda_i < 0$, l'attracteur est hyperchaotique.

Lorsque l'exposant de Lyapunov est positif, les trajectoires sont divergentes et de ce fait le système est chaotique. Sur les figures (1.13) et (1.15), nous pouvons observer les variations des exposants de Lyapunov des systèmes de Hénon d'ordre 2 et d'ordre 3, selon les paramètres a variable et b fixe (dans les figures (1.13) et (1.15) (i)) et selon b variable et a fixe (dans les figures (1.13) et (1.15) (ii)). Ces figures, nous permettent de savoir s'il s'agit d'un comportement hyperchaotique, chaotique ou d'un régime périodique. Les figures (1.14) et (1.16) présentent les évolutions temporelles des exposants de Lyapunov. Ainsi, dans la figure (1.14), nous notons une valeur négative et une positive qui caractérisent un comportement chaotique. Par contre, dans la figure (1.16), on trouve deux valeurs positives de l'exposant de Lyapunov qui caractérisent le comportement hyperchaotique.



(i) $0 < b < 1.5$, avec $a = 0.3$ (ii) $-0.37 < a < 0.32$, avec $b = 1.4$

FIGURE 1.13 – Evolutions des exposants de Lyapunov pour l'exemple de l'attracteur de Hénon d'ordre 2

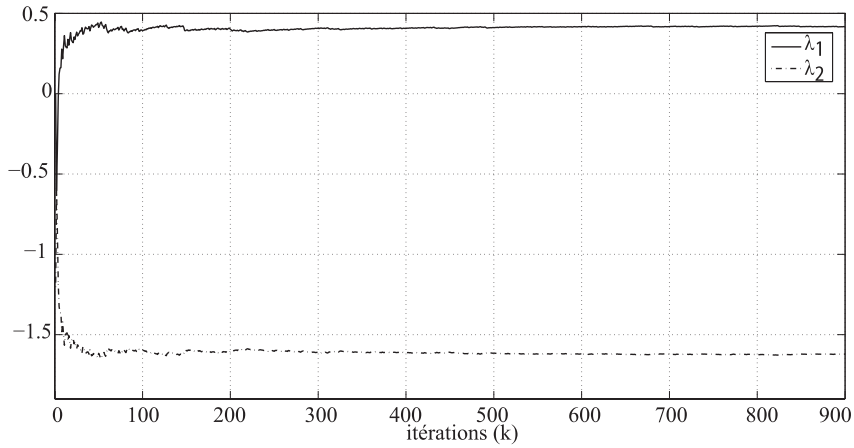
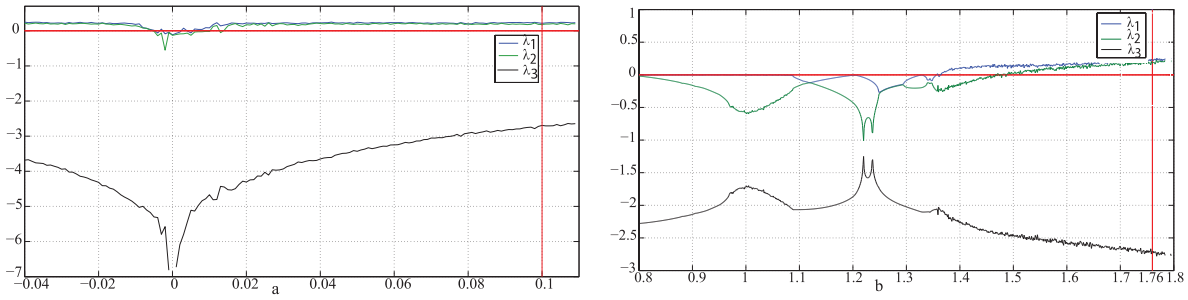


FIGURE 1.14 – Evolutions des exposants de Lyapunov pour l'exemple de l'attracteur de Hénon d'ordre 2 ($\lambda_1 = 0.4238$ et $\lambda_2 = -1.6277$)



(i) $-0.04 < a < 0.11$, avec $b = 1.76$ (ii) $0.8 < b < 1.8$, avec $a = 0.1$

FIGURE 1.15 – Evolutions des exposants de Lyapunov pour l'exemple de l'attracteur de Hénon (Baier-Klein) d'ordre 3

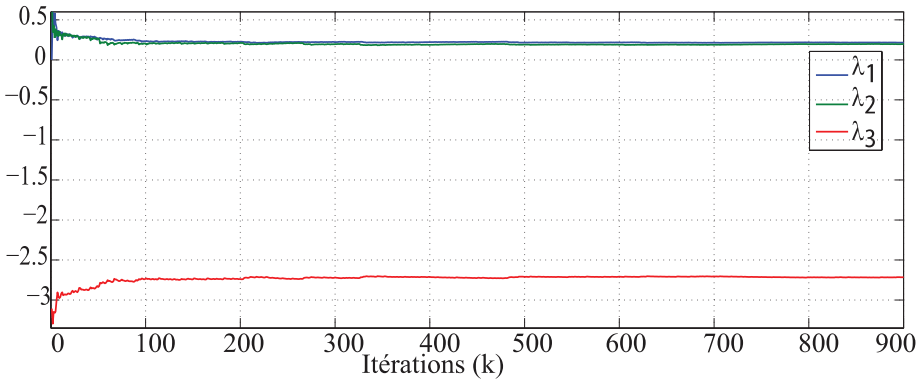


FIGURE 1.16 – Evolutions des exposants de Lyapunov pour l'exemple de l'attracteur de Hénon d'ordre 3 (Baier-Klein) ($\lambda_1 = 0.2223$, $\lambda_2 = 0.1918$ et $\lambda_3 = -2.7166$)

La figure 1.16 montre le signe des exposants de Lyapunov correspondants à $b = 1.76$ et $a = 0.1$; de ces exposants, nous pouvons conclure qu'il existe une région très étroite qui exhibe un comportement hyperchaotique du modèle de Hénon généralisé (Baier-Klein) d'ordre 3.
Afin d'améliorer la sécurité, la synchronisation des systèmes de grande dimension ayant plusieurs exposants de Lyapunov positifs (systèmes hyperchaotiques) est préférable à l'utilisation de certaines applications utilisant des systèmes chaotiques. En effet, les systèmes hyperchaotiques sont largement utilisés pour la cryptographie et la sécurité de l'information, en raison de la présence de plus d'un exposant de Lyapunov ; ce qui améliore nettement la sécurité des systèmes de communication, en générant des dynamiques plus complexes. Il est à noter que la sensibilité aux états initiaux garantit la propriété de diffusion [Belkhouche et Gokcen, 2009].

1.5 Synchronisation et stabilité des systèmes chaotiques

1.5.1 Introduction

La synchronisation constitue une phase primordiale dans les schémas de communication. Nous allons présenter dans cette section, tout d'abord, des techniques de stabilité et de stabilisation qui sont utilisées ultérieurement pour résoudre le problème de synchronisation. Puis, dans un deuxième temps, nous appliquons ces techniques au problème de synchronisation du type maître-esclave.

1.5.2 Stabilité des systèmes dynamiques non linéaires à temps discret

1.5.2.1 Introduction

La stabilité constitue une notion fondamentale dans l'analyse du comportement dynamique d'un système non linéaire échantillonné. Elle consiste à étudier, en particulier, l'influence de certaines perturbations sur la trajectoire d'un processus. Dans le cas d'un système non linéaire, les méthodes usuelles utilisées pour les systèmes linéaires par applications de la linéarisation, se sont révélées généralement insuffisantes. En effet, la linéarisation est une méthode d'approximation qui n'est valide que localement autour du point de fonctionnement concerné. Elle ne peut pas être utilisée pour étudier un comportement global ou fortement non linéaire. Dans la suite, diverses définitions et divers concepts relatifs à la stabilité des systèmes non linéaires échantillonnés sont présentés.

1.5.2.2 Stabilité - Définitions

Il existe diverses définitions de la stabilité [Matrozov, 1962, Gentina *et al.*, 1972, Grujic *et al.*, 1978, Borne, 1976, Amri *et al.*, 2010, Braiek *et al.*, 1995], dont seulement les plus utilisées sont présentées dans cette section.
Soit le système dynamique non linéaire (1.6) dont la réponse est telle que :

$$x\left(k\right) = x(k, k_0, x(k_0)) \tag{1.67}$$

pour des conditions initiales définies par :

$$x(k_0) = x(0) \tag{1.68}$$

Soit x_e une position d'équilibre ; on a :

$$f(x_e) = x_e \tag{1.69}$$

Définition 1.5. ***Stabilité au sens de Lyapunov***
Le système décrit par (1.6) *est dit stable au sens de Lyapunov par rapport à l'équilibre* x_e*, si, pour des conditions initiales* $x(k_0)$ *suffisamment proches de l'équilibre* x_e*, la trajectoire reste dans la boule de centre* x_e *et de rayon* ε *arbitraire, soit :*

$$\exists \delta \; si \;\; \|x(k_0) - x_e\| < \delta \;\; alors \;\; \|x(k, k_0, x(k_0)) - x_e\| < \varepsilon, \;\; \forall k \geqslant k_0 \tag{1.70}$$

Définition 1.6. ***Attractivité***

L'équilibre x_e est attractif lorsqu'il y a convergence de l'état x vers l'état x_e au bout d'un temps infini, les conditions initiales $x(k_0)$ étant bornées, soit :
$\forall k_0 \in \mathbb{N};\ \exists \delta_0(k_0),$ *tel que* :

$$si\ \ \|x(k_0) - x_e\| < \delta_0(k_0)\ alors\ \lim_{k\to\infty} x(k, k_0, x(k_0)) = x_e \tag{1.71}$$

Lorsque $\delta_0(k_0) = +\infty$, on dit que l'équilibre x_e est globalement attractif.

Définition 1.7. ***Stabilité asymptotique***

L'équilibre x_e est dit asymptotiquement (respectivement globalement asymptotiquement) stable lorsqu'il est à la fois stable au sens de Lyapunov et attractif (respectivement globalement attractif). Les trajectoires $x(k, k_0, x(k_0))$ restent alors arbitrairement bornées pour des conditions initiales suffisamment faibles.

1.5.2.3 Méthodes d'étude de la stabilité des systèmes discrets non linéaires

a. Méthodes de Lyapunov

Les définitions proposées par Lyapunov concernant la stabilité ont été formulées pour des systèmes à temps discret. On distingue deux méthodes de Lyapunov [Borne *et al.*, 1993, Byrnes et Ghosh, 1993, Abderrahman et Mohammed, 1996].

Première méthode de Lyapunov : On considère le cas où le système non linéaire décrit par (1.6) admet, au voisinage de $x_e = 0$, un développement limité de la forme :

$$x\,(k+1) = Ax\,(k) + r(\|x\|) \tag{1.72}$$

dans lequel la matrice A est constante et :

$$\lim_{x\to 0} \frac{\|r(\|x\|)\|}{\|x\|} = 0 \tag{1.73}$$

Le système linéaire décrit par la relation :

$$z(k+1) = Az\,(k) \tag{1.74}$$

peut être considéré comme la linéarisation de (1.10) autour $x_e = 0$. Il permet de statuer, localement, sur la stabilité du système non linéaire au point $x_e = 0$:

– si toutes les valeurs propres de A sont de modules strictement inférieurs à l'unité, alors l'état d'équilibre $x_e = 0$ du système non linéaire est asymptotiquement stable ;

– si la matrice A admet au moins une valeur propre de module strictement supérieur à l'unité, alors l'état d'équilibre $x_e = 0$ est instable ;
– si certaines valeurs propres de la matrice A sont sur le cercle de rayon unité et les autres à l'intérieur, on ne peut pas conclure quant à la stabilité locale de l'état d'équilibre $x_e = 0$ du système non linéaire considéré.

Deuxième méthode de Lyapunov : La deuxième méthode de Lyapunov permet l'analyse de la stabilité directement à partir des équations décrivant les processus et ne nécessite pas la détermination explicite de leurs solutions [Borne *et al.*, 1993].

Nous introduisons une fonction continue $v(x(k))$, dite de Lyapunov, $R^n \rightarrow R^+$ et vérifiant :

- $v(x(k))$ définie positive, c'est-à-dire $v(x(k)) > 0, \forall (x(k)) \neq 0, v(0) = 0$;
- les courbes $v(x(k)) = constante$, appelées équipotentielles de Lyapunov, définissent des domaines connexes emboîtés :

$$\begin{aligned} &D_i = \{x(k) \in R^n,\ v(x(k)) \leq c_i\}, \\ &c_1 < c_2\ alors\ D_1 \subset D_2 \end{aligned} \tag{1.75}$$

Il est à noter que $v(x(k))$ est non bornée en rayon, si on a : $\lim_{\|x(k)\| \rightarrow +\infty} v(x(k)) = +\infty$

Le principe de la deuxième méthode consiste à remplacer l'étude de convergence de $x(k, k_0, x(k_0))$ vers $x_e = 0$ par celle de $v(x(k)) = v(x(k, k_0, x(k_0)))$. En effet, si $\Delta v(k)$ est définie négative pour tout k et pour tout $x(k)$ au voisinage de $x_e = 0$ tels que :

$$\begin{aligned} \forall x(k) \neq 0\ \Delta v(x(k)) &= v(x(k+1)) - v(x(k)) \\ &= v(f(x(k))) - v(x(k)) < 0,\ \Delta v(0) = 0 \end{aligned} \tag{1.76}$$

nous pouvons alors conclure à la stabilité de cet état d'équilibre.

Etude de la stabilité par utilisation de la fonction de Lyapunov quadratique Une fonction de Lyapunov quadratique est de la forme générale suivante :

$$v(x(k)) = x(k)^T P x(k) \tag{1.77}$$

P est une matrice symétrique définie positive et peut, souvent, conduire à une condition suffisante de stabilité.

Théorème 1.2. *Le système défini par l'équation d'état :*

$$x\left(k+1\right)=A(k,x\left(k\right))x\left(k\right) \tag{1.78}$$

est asymptotiquement stable si $\exists P>0$*, telle que :*

$$A^{T}\left(x\left(k\right),k\right)PA\left(x\left(k\right),k\right)-P<0\ \forall k,\ \forall x\left(k\right) \tag{1.79}$$

Démonstration. Soit le système défini par (1.78) ; on a :
$\Delta v\left(k\right)=v(x\left(k+1\right))-v(x\left(k\right))=x\left(k+1\right)^{T}Px\left(k+1\right)-x\left(k\right)^{T}Px\left(k\right)$
On obtient :
$\Delta v\left(k\right)=x\left(k\right)^{T}A^{T}\left(x\left(k\right),k\right)PA\left(x\left(k\right),k\right)x\left(k\right)-x\left(k\right)^{T}Px\left(k\right)$
$\Delta v\left(k\right)=x\left(k\right)^{T}\left(A^{T}\left(x\left(k\right),k\right)PA\left(x\left(k\right),k\right)-P\right)x\left(k\right)$
Une condition suffisante de stabilité est donc que la condition (1.79) soit vérifiée. □

b. Utilisation des techniques d'agrégation pour l'étude de la stabilité
Dans cette section, nous allons considérer les méthodes d'agrégation qui consistent à substituer au modèle initial un modèle de taille égale ou inférieure à l'ordre du système permettant de conclure à la stabilité du système initial.
L'objectif est que ce modèle soit un modèle de comparaison, pouvant être du premier ordre, et que l'étude de sa stabilité implique celle du système initial. Bellman [Bellman, 1962], Matrozov [Matrozov, 1962] et Borne [Grujic *et al.*, 1979, Richard *et al.*, 1988, Borne *et al.*, 1972, Borne, 1976] ont proposé une extension qui consiste à choisir, pour le système global, une fonction de Lyapunov vectorielle, afin de déterminer un système de comparaison, d'ordre supérieur, décrit dans l'espace d'état.

c. Notion de norme vectorielle [Borne *et al.*, 1972, Borne *et al.*, 1972, Borne, 1976, Gentina *et al.*, 1976, Borne, 1987, Gruyitch *et al.*, 2004, Borne et Benrejeb, 2008, Borne et Benrejeb, 2012]
Considérons l'espace vectoriel $\mathbb{R}^{n}$ et les sous-espaces $\mathbb{R}^{n_i}$, $\forall i=1,2,\ldots,r$, tels que :

$$n=n_1+n_2+\ldots+n_r \tag{1.80}$$

$$x\left(k\right)=\left[\begin{array}{cccc} x_1^{T}\left(k\right) & x_2^{T}\left(k\right) & \ldots & x_r^{T}\left(k\right)\end{array}\right]^{T} \tag{1.81}$$

avec : $x\left(k\right)\in\mathbb{R}^{n}$ et $x_i\left(k\right)\in\mathbb{R}^{n_i}$.
On définit la norme vectorielle $p(.)$ sur $\mathbb{R}^{n}$ par :

$$p(x\left(k\right))=\left[\begin{array}{cccc} p_1(x_1\left(k\right)) & p_2(x_2\left(k\right)) & \ldots & p_r(x_r\left(k\right))\end{array}\right]^{T} \tag{1.82}$$

telle que $p_i(.)$ soit une norme scalaire définie sur R^{n_i} et $p(x(k))$ satisfaisant les conditions suivantes :

(a) $p(x(k)) > 0, \forall x(k) \neq 0 \in \mathbb{R}^n$

(b) $p(x(k)) = 0 \Leftrightarrow x(k) = 0$

(c) $p(x(k) + y(k)) \leqslant p(x(k)) + p(y(k)), \forall x(k), y(k) \in \mathbb{R}^n$

(d) $p(\lambda x(k)) = |\lambda| p(x(k)), \forall \lambda \in \mathbb{R}, \forall x(k) \in \mathbb{R}^n$

d. Système majorant [Borne *et al.*, 1972] : Soit un système dynamique échantillonné non linéaire décrit par l'équation d'état (1.78). La matrice $M(x(k))$ du système discret (1.83), de dimension $r \times r$, définit un système majorant relatif à la norme vectorielle $p(x(k)) \in \mathbb{R}^r_+$ si et seulement si l'inégalité :

$$p(x(k+1)) \leqslant M(k, x(k)) p(x(k)) \ \forall k, x(k) \in \mathbb{Z} \times \mathbb{R}^n \tag{1.83}$$

est vérifiée le long des trajectoires de (1.78) pour chaque composante de $p(x(k+1))$

e. Lemmes de comparaison [Borne *et al.*, 1972, Borne *et al.*, 2003, Gruyitch *et al.*, 2004, Gruyitch *et al.*, 2004, Borne et Benrejeb, 2008, Borne et Benrejeb, 2012] : Pour le système (1.78), Borne et Gentina ont démontré un lemme de comparaison correspondant à une généralisation du lemme de comparaison de Wazewski.

Lemme de comparaison

Soit $p(x(k))$ une norme vectorielle de taille r . Si la matrice $M(k, x(k))$, de dimension $r \times r$, associée au système discret (1.78) est à éléments non négatifs, et telle que l'inégalité (1.83) soit vérifiée, le système :

$$z(k+1) = M(k, x(k)) z(k), \ \forall k \in \mathbb{Z}_d \text{ et } \forall x_k \in \chi \tag{1.84}$$

avec :

$$z(k_0) \geqslant p(x(k_0)) \tag{1.85}$$

est un système de comparaison de (1.78) et l'inégalité suivante :

$$z(k) \geqslant p(x(k)) \ \forall k > k_0 \tag{1.86}$$

est vérifiée.

Si le système en z (1.84) est asymptotiquement stable, il en est, donc, de même du système en x (1.78).

f. Cas d'un système majorant linéaire

Considérons le système de vecteur d'état $x(k) \in R^n$ dont l'évolution est régie par la relation suivante :

$$x\left(k+1\right) = f\left(x\left(k\right)\right) \tag{1.87}$$

Pour certains systèmes, il est possible de formuler $f\left(x\left(k\right)\right)$ comme suit :

$$f\left(x\left(k\right)\right) = F^*\left(x\left(k\right)\right) x\left(k\right) \tag{1.88}$$

$F^*\left(x\left(k\right)\right)$ étant une matrice $n \times n$ dont les éléments sont bornés en module ou encore :

$$F^*\left(x\left(k\right)\right) \in \left[F_1, F_2\right] \subset R^{n\times n} \tag{1.89}$$

F_1 et F_2 étant deux matrices à éléments constants.

Lemme 1.1. ***Enoncé de la conjecture du linéaire d'Aizerman*** *[Grujic et al., 1978] Soit le processus dont l'évolution est décrite par l'équation d'état :*

$$x\left(k+1\right) = Ax\left(k\right) \tag{1.90}$$

$x\left(k\right) \in R^n$ étant le vecteur d'état et A une matrice $n \times n$ à éléments constants. Si A est stable quelque soit la valeur de $A \in \left[F_1, F_2\right]$, alors il est possible de conclure à la stabilité asymptotique de l'état d'équilibre $x(0)$ pour le système dont la relation est représentée par (1.87).

– Lemme de Kotelyanski : Si le système dont l'évolution est régie par l'équation définie par (1.90), $A = \{a_{ij}\}$ étant une matrice $n \times n$ à éléments constants et indépendants du temps. L'application des conditions de Hurwitz sur les paramètres du polynôme caractéristique de la matrice caractéristique A, défini par :

$$\det\left(\lambda I - A\right) = 0 \tag{1.91}$$

implique que les valeurs propres de la matrice A sont de modules inférieurs à l'unité.

Il est à noter que les travaux de Kotelyanski ont mis en évidence un lemme particulier dans le cadre de l'étude de la stabilité des systèmes lorsque la matrice A est à éléments positifs.

Lemme 1.2. ***Enoncé du lemme de Kotelyanski*** *Les valeurs propres de la matrice A, d'éléments positifs, sont de modules inférieurs à un nombre réel μ, si et seulement si tous les mineurs principaux de la matrice $M = \mu I_{n\times n} - A$ sont positifs, $I_{n\times n}$ étant la matrice identité.*

g. Critère pratique de stabilité de Borne et Gentina, [Borne, 1976, Gentina *et al.*, 1972]. Soit le système échantillonné non linéaire défini dans l'espace d'état par (1.78). Soit le système de comparaison de matrice caractéristique $M_k(A(x(k),k))$ relatif à la norme vectorielle $p(z(k)) = [|z_1(k)| \dots |z_n(k)|]^T$, $z(k) = [z_1(k) \ \dots \ z_n(k)]^T$, telle que :

$$M_k(A(x(k),k)) = \left\{ a^*_{ij}(.) = |a_{ij}(.)| \ \ \forall i,j = 1,...,n \right\} \tag{1.92}$$

Si les termes non constants sont isolés dans une seule ligne ou une seule colonne de la matrice $M_k(A(x(k),k))$, la stabilité asymptotique est assurée si tous les mineurs principaux successifs de la matrice $(I - M_k(A(x(k),k)))$ sont positifs. ou encore si les conditions suivantes sont vérifiées :

$$\begin{array}{l} 1 - a^*_{11} > 0, \begin{vmatrix} 1-a^*_{11} & -a^*_{12} \\ -a^*_{21} & 1-a^*_{22} \end{vmatrix} > 0, \dots, \\ \begin{vmatrix} 1-a^*_{11} & -a^*_{12} & \dots & -a^*_{1n} \\ -a^*_{21} & 1-a^*_{22} & \dots & -a^*_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ -a^*_{n1} & -a^*_{n2} & \dots & 1-a^*_{nn} \end{vmatrix} > 0 \ \ \forall \, (k, x(k)) \in Z \times R^n \end{array} \tag{1.93}$$

1.5.2.4 Stabilisation

Au cours des quatre dernières décennies, la stabilisation des systèmes dynamiques non linéaires, a attiré l'attention de plusieurs chercheurs [Brockett, 1983, P.Kokotovic et Arcak, 2001, Nijmeijer et der Schaft, 1990, Borne *et al.*, 1996, Benrejeb, 2010].
Pour le système non linéaire discret suivant :

$$x(k+1) = f(x(k), u(k)) \tag{1.94}$$

$x(k) \in R^n$ et $u(k) \in R^m$, le problème de sa stabilisation revient à construire une loi commande $u(k)$ par retour d'état ou de sortie telle que sa position d'équilibre $x_e = 0$ soit asymptotiquement stable.
Plusieurs méthodes ont été développées pour résoudre le problème de stabilisation dans le cas des systèmes non linéaires continus et discrets [Aeyels, 1985, Byrnes et Lin, 1993, Lin, 1996, J. Mohseni et Olejniczak, 1998, Nijmeijer, 1987, Qian et Lin, 2001].
Parmi les méthodes d'étude envisageables dans le cas de systèmes discrets, permettant de trouver une solution à la stabilisation, nous proposons dans le cadre de nos travaux de recherche d'utiliser les approches basées sur des techniques d'agrégation [Borne, 1976,

Borne *et al.*, 1996] associées à une représentation matricielle bien définie, conduisant à des conditions suffisantes de stabilisation de mise en oeuvre aisée.

1.5.3 Synchronisation de systèmes chaotiques à temps discret couplés

La synchronisation des systèmes chaotiques a fait l'objet de nombreux travaux de recherche. L'un des premiers travaux proposant cette approche a été réalisé en 1990, par les chercheurs Pecora et Carroll, qui ont montré [Pecora et Carroll, 1990] que deux systèmes chaotiques peuvent se synchroniser sous certaines conditions. Ainsi la synchronisation de deux systèmes chaotiques à temps discret permet de forcer deux systèmes chaotiques discrets, caractérisés par un comportement imprévisible à long terme, à suivre la même trajectoire.
On dit alors qu'un système esclave :

$$x_s(k+1) = f_s(x_s(k)),\ x_s(k) \in R^n \tag{1.95}$$

se synchronise avec le système maître suivant :

$$x_m(k+1) = f_m(x_m(k)),\ x_m(k) \in R^n \tag{1.96}$$

pour toutes conditions initiales $(x_m(0), x_s(0))$. Il s'avère donc important de vérifier la convergence de l'écart des évolutions du comportement des systèmes maître et esclave. Pour y arriver, une solution est de mettre en oeuvre une condition de stabilité pour le système écart permettant d'obtenir une condition d'unicité de la réponse. Lorsque ces méthodes ne sont pas efficaces, il est souvent intéressant d'opter pour une technique forçant les propriétés de synchronisation. Parmi les nouvelles techniques envisageables dans le cadre du discret, nous proposons dans nos travaux d'utiliser les méthodes de commande par retour d'état et de sortie (observateur) et particulièrement les méthodes de stabilisation, introduites dans le paragraphe précédent, permettant ainsi de garantir les performances souhaitées pour l'écart des signaux.
Cette capacité de synchronisation, dérivant de la théorie de la commande, a ouvert la voie à de nombreuses applications parmi lesquelles nous avons retenu les systèmes de communications sécurisées.

1.6 Synchronisation et cryptage de systèmes chaotiques. Position du problème

Ces dernières années, une nouvelle classe de méthodes, utilisant la dynamique chaotique pour la transmission sécurisée de l'information, a été considérée comme solution très prometteuse pour augmenter les performances des systèmes actuels de transmission. Les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée et qui possèdent une infinité de trajectoires non périodiques denses. Le comportement aléatoire et la sensibilité aux conditions initiales et aux réglages des paramètres permet à des systèmes chaotiques de remplir les propriétés requises pour les schémas de chiffrement telles que les propriétés de confusion et diffusion de Shannon [Shannon, 1949], usuellement rencontrées en cryptographie standard [Barthélemy *et al.*, 2005]. Ces propriétés permettent, théoriquement, de générer un nombre infini de signaux chaotiques non corrélés d'un même système en utilisant différentes valeurs initiales ou en effectuant une petite variation de ses paramètres.
Le tableau (1.1) montre l'analogie entre les systèmes cryptographiques et les systèmes chaotiques [Alvarez et Li, 2006].

TABLE 1.1 – Analogie entre les systèmes cryptographiques et les systèmes chaotiques

Propriétés cryptographiques	**Propriétés chaotiques**
Diffusion avec une légère modification dans le texte clair ou la clé secrète	Sensibilité aux conditions initiales et aux paramètres du système
Confusion : complexité de la relation entre la clé secrète ou le texte chiffré	Ergodicité : caractéristiques macroscopiques de l'attracteur étrange
Déterminisme des générateurs pseudo-aléatoires	Déterminisme des systèmes chaotiques
Complexité des algorithmes de cryptage	Comportements complexes
Clé secrète	Paramètres de bifurcation comme clés secrètes

Le principe des schémas de chiffrement par chaos consiste à mélanger une information $m(k) \in R$ issue d'un émetteur avec un système chaotique de vecteur d'état $x_m(k)$ de dimension n. Seule une partie du vecteur d'état $x_m(k)$, notée $y_m(k)$, est transmise à

travers le canal public. La sortie $y_m(k)$ est généralement de faible dimension et doit être unidimensionnelle dans le cas idéal (de dimension 1), l'émetteur étant de vecteur d'état notée $x_s(k)$. Pour la plupart des cryptosystèmes basés sur le chaos, la récupération du message $m(k)$ est basée sur la synchronisation des deux systèmes chaotiques maître et esclave respectivement dans la partie émettrice et réceptrice.
Ainsi, il faut préciser qu'a priori la synchronisation entre deux systèmes dynamiques chaotiques est primordiale à la récupération de l'information transmise. Dans la suite de ce travail, nous proposons une solution de synchronisation basée sur le retour d'état et sur les observateurs, susceptibles d'offrir effectivement les meilleures performances possibles [Perez et Cerdeira, 1995, Short, 1994, Pecora et Carroll, 1990, Guojie *et al.*, 2003].

1.7 Conclusion

Dans ce chapitre, nous avons présenté des généralités sur les systèmes discrets et plus précisément les systèmes chaotiques, fait un tour d'horizon des techniques d'étude de la stabilité et introduit le problème de stabilisation et ses applications à la synchronisation. Dans la suite, nous allons nous intéresser aux systèmes non linéaires chaotiques à temps discret.
Les résultats énoncés sur la stabilité sont appliqués, dans le chapitre 2, pour proposer une nouvelle approche de stabilisation pour les systèmes non linéaires discrets ainsi qu'une nouvelle approche de synchronisation de deux systèmes chaotiques discrets identiques et non identiques par retour d'état et par observateurs.

Chapitre 2

Méthodes de synchronisation proposées pour les systèmes hyperchaotiques à temps discret

2.1 Introduction

Après avoir présenté, au chapitre précédent, des généralités sur l'analyse des systèmes discrets non linéaires, plus précisément les systèmes chaotiques et des approches d'étude de la stabilisation et de la synthèse d'observateurs, nous nous intéressons, dans ce chapitre, à l'étude de différents schémas de synchronisation à partir de nouvelles approches proposées basées sur les techniques de stabilisation utilisant les techniques d'aggrégation. La phase de synchronisation se décompose en trois étapes principales, à savoir : le choix du système maître, la conception du système esclave et l'analyse de la synchronisation. Nous envisageons, dans ce chapitre, d'élaborer deux approches pour résoudre le problème de synchronisation de deux systèmes chaotiques identiques et différents. La première approche repose sur la synthèse d'une commande stabilisante par retour d'état et la deuxième est basée sur la synthèse d'un observateur. Les résultats de ces deux approches permettent d'énoncer des conditions suffisantes de synchronisation basées sur l'utilisation du critère pratique de Borne et Gentina pour l'étude de la stabilité et de matrices sous forme en flèche de Benrejeb pour la description des systèmes étudiés. Différents schémas de synchronisation proposés sont testés par simulation.

2.2 Sur les techniques de synchronisation

Dans cette section, nous proposons de nouvelles commandes par retour d'état et de sortie permettant la détermination de nouvelles conditions suffisantes de stabilisabilité asymptotique de systèmes dynamiques discrets non linéaires. Dans cette optique, nous présentons, aussi, des résultats de la stabilisation appliqués à la synchronisation.

2.2.1 Types de synchronisation

Dans la suite, nous introduisons différents types de synchronisation, à savoir la synchronisation complète, généralisée, de phase, retardée ou projective.

2.2.1.1 Synchronisation complète

On dit qu'il se produit une synchronisation complète, lorsque les variables d'état $x_s(k)$ du système chaotique (ou hyperchaotique) esclave convergent asymptotiquement vers les variables d'état $x_m(k)$ du système chaotique (ou hyperchaotique) maître [Pecora et Carroll, 1990, Boccaletti *et al.*, 2002].
Considèrons les deux systèmes dynamiques (2.1) et (2.2) suivants :

$$x_m(k+1) = f_m(x_m(k)) \tag{2.1}$$

$$x_s(k+1) = f_s(x_s(k)) \tag{2.2}$$

Ils sont identiquement synchronisés, lorsque, quelles que soient leurs conditions initiales, on a :

$$\lim_{k\to+\infty} \|x_m(k) - x_s(k)\| = 0, \quad \forall x_s(0),\ x_m(0) \tag{2.3}$$

2.2.1.2 Synchronisation généralisée

Considérons les systèmes (2.1) et (2.2). S'il existe une transformation M, $R^n \to R^n$, telle que toutes les trajectoires des systèmes maître et esclave, avec les conditions initiales $x_s(0)$ et $x_m(0)$, vérifient :

$$\exists M \quad \lim_{k\to+\infty} \|x_s(k) - M(x_m(k))\| = 0 \quad \forall x_s(0),\ \forall x_m(0) \tag{2.4}$$

alors les systèmes (2.1) et (2.2) se synchronisent au sens généralisé [Rulkov *et al.*, 1995]. Il est à noter que la fonction M doit être inversible, afin que $M^{-1}x_s(k)$ puisse fournir une estimation de l'état de $x_m(k)$. L'inconvénient de cette technique est qu'elle présente

un défaut pour certaines techniques de communication qui utilisent l'état du système émetteur pour décrypter le message transmis.

2.2.1.3 Synchronisation de phases

Pour étudier la synchronisation de phases entre deux systèmes chaotiques (ou hyperchaotiques) continus couplés [Chen *et al.*, 2003], on doit d'abord calculer les phases des oscillateurs en utilisant l'approche analytique [Rosenblum *et al.*, 1996]. Un signal analytique $\psi(t)$ est une fonction complexe définie par :

$$\psi(t) = s(t) + j\tilde{s}(t) = A(t)\, e^{j\phi(t)} \tag{2.5}$$

où $\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$:

$$\tilde{s}(t) = \frac{1}{\pi} VP \int_{-\infty}^{+\infty} \frac{s(\tau)}{t-\tau} d\tau \tag{2.6}$$

V.P. étant la valeur principale de Cauchy de l'intégrale. On vérifie, ensuite, que la condition suivante :

$$|n\phi_1 - m\phi_2| < c \tag{2.7}$$

est satisfaite, avec : $m, n \in \mathrm{N}$, c une constante positive et ϕ la phase de $\psi(t)$.

2.2.1.4 Synchronisation retardée

On dit qu'on a une synchronization retardée si les variables d'état $x_s(k)$ du système chaotique (ou hyperchaotique) esclave convergent vers les variables d'état $x_m(k)$ décalées dans le temps du système chaotique (ou hyperchaotique) maître, comme l'indique la relation ci-dessous [Li *et al.*, 1986] :

$$\lim_{k \to +\infty} \|x_s(k) - x_m(k-\tau)\| = 0 \quad \forall x(0) \tag{2.8}$$

2.2.1.5 Synchronisation projective

On dit qu'on a une synchronisation projective [Mainieri et Rehacek, 1999], si les variables d'état du système chaotique (ou hyperchaotique) esclave se synchronisent avec une constante multiple de l'état du système chaotique (ou hyperchaotique) maître, tels que :

$$\exists\, \alpha_i \;\; et \;\; \tau \;\; tels\ que \;\; \lim_{k \to +\infty} \|x_{si}(k) - \alpha_i x_{mi}(k-\tau)\| = 0 \;\; \forall x_s(0) \;\; x_m(0)\,, \; \forall i = 1, \cdots, n \tag{2.9}$$

Ce type de synchronisation permet de synchroniser, à un facteur près, les variables d'état des systèmes chaotiques (ou hyperchaotiques) couplés. Le cas où tous les α_i sont égaux à 1 représente un cas de synchronisation complète. Le cas où tous les α_i sont égaux à -1 est un cas d'anti-synchronisation et la synchronisation hybride correspond au cas où quelques variables d'état atteignent la synchronisation et d'autres atteignent l'anti-synchronisation, simultanément.

2.3 Nouvelles méthodes de stabilisation proposées pour les systèmes discrets non linéaires par la mise sous forme en flèche de la matrice caractéristique instantanée du système bouclé

2.3.1 Stabilisation des systèmes continus non linéaires - Idée de base

En se référant aux travaux réalisés dans le cadre de l'analyse et la synthèse de systèmes dynamiques continus non linéaires, la méthode proposée est basée sur la détermination systématique de conditions suffisantes de stabilité et de stabilisation asymptotiques qui tiennent compte de la mise sous forme en flèche mince de la matrice caractéristique du système bouclé ; ce qui permet d'obtenir des formulations de lois de commande stabilisante par retour d'état ou par retour de sortie, de mises en oeuvre aisées [Benrejeb et Hammami, 2008, Benrejeb, 2010, Hammami *et al.*, 2010c].

2.3.2 Cas de lois de commande par réaction d'état de systèmes discrets

2.3.2.1 Approche de stabilisation des systèmes étudiés

Considérons le système discret décrit par l'équation d'état suivante :

$$x(k+1) = A(x(k), k)x(k) + B(x(k), k)u(k) \tag{2.10}$$

où $x(k)$ représente le vecteur d'état de dimension n à l'instant kT, $u(k)$ le vecteur des entrées de commande de dimension m, $A(x(k), k) = \{a_{ij}(x(k), k)\}$ une matrice $n \times$

n et $B(x(k),k)$ une matrice $n \times m$, $B(x(k),k) = \{b_{ij}(x(k),k)\}$, T étant la période d'échantillonnage.
La loi de commande stabilisante par retour d'état de la forme :

$$u(k) = -K(x(k),k)x(k) \tag{2.11}$$

conduit au système bouclé décrit par :

$$x(k+1) = A_f(x(k),k)x(k) \tag{2.12}$$

$$A_f(x(k),k) = A(x(k),k) - B(x(k),k)K(x(k),k) \tag{2.13}$$

$K(x(k),k)$ étant la matrice gain de dimension $m \times n$, $K(x(k),k) = \{k_{ij}(x(k),k)\}$.
Les éléments des matrices $A(.)$, $B(.)$ et $K(.)$ peuvent être non linéaires.
Lorsqu'il est possible de trouver une matrice gain $K(x(k),k)$ qui permet d'obtenir une matrice $A_f(x(k),k)$ de forme en flèche mince de type 1 ou 2, $A_f(x(k),k) = \left\{a_{f_{ij}}(x(k),k)\right\}$, on a :

- Pour le cas de la forme en flèche de type 1

$$\begin{cases} x_i(k+1) = a_{f_{ii}}(x(k),k)x_i(k) + a_{f_{in}}(x(k),k)x_n(k) \ \ \forall\, i = 1,2,\ldots,n-1 \\ x_n(k+1) = \sum_{i=1}^{n} a_{f_{ni}}(x(k),k)x_i(k) \end{cases} \tag{2.14}$$

- Pour le cas de la forme en flèche de type 2

$$\begin{cases} x_1(k+1) = \sum_{i=1}^{n} a_{f_{1i}}(x(k),k)x_i(k) \\ x_i(k+1) = a_{f_{ii}}(x(k),k)x_i(k) + a_{f_{i1}}(x(k),k)x_n(k) \ \ \forall\, i = 2,\ldots,n \end{cases} \tag{2.15}$$

Le polynôme caractéristique instantané de cette matrice, noté $P_{A_f}(\lambda, x(k), k)$, est défini par :

$$P_{A_f}(\lambda, x(k), k) = \det\left(\lambda I - A_f(x(k),k)\right) \tag{2.16}$$

Comme montré dans [Borne, 1976, Benrejeb *et al.*, 2008, Benrejeb et Gasmi, 2001a, Benrejeb et Abdelkrim, 2003, Benrejeb *et al.*, 2005, Borne et Benrejeb, 1977, Benrejeb, 2010], l'étude de la stabilité à partir d'une telle matrice peut être rendue aisée, par application du critère pratique de Borne et Gentina [Borne *et al.*, 1976, Gentina *et al.*, 1972] lorsque les non linéarités sont isolées dans une seule rangée.
En effet, le choix d'un système de comparaison de matrice caractéristique $M_k\left(A_f(x(k),k)\right)$,

relativement à la norme vectorielle $p(z(k)) = \left[\begin{array}{ccc} |z_1(k)| & \dots & |z_n(k)| \end{array} \right]^T$,
$z(k) = \left[\begin{array}{ccc} z_1(k) & \dots & z_n(k) \end{array} \right]^T$, telle que :

$$m_{k_{ij}}(x(k), k) = \left| a_{f_{ij}}(x(k), k) \right| \forall i, j = 1, \dots, n \tag{2.17}$$

conduit, lorsque les non linéarités sont isolées dans une seule rangée, aux conditions suffisantes de stabilisation suivantes :

$$(I - M_k(A_f(x(k), k))) \begin{pmatrix} 1 & 2 & \dots & h \\ 1 & 2 & \dots & h \end{pmatrix} > 0 \ \ \forall h = 1, 2, \dots, n \tag{2.18}$$

Pour une matrice $A_f(x(k), k)$ de forme en flèche mince, les conditions précédentes peuvent être réécrites simplement d'une manière analytique [Benrejeb, 1980, Benrejeb, 2010].

2.3.2.2 Conditions de stabilisabilité par retour d'état des systèmes discrets

Théorème 2.1. *Le processus défini par* (2.10) *est stabilisable par la loi de commande définie par* (2.11)*, si le système corrigé* (2.13) *de matrice caractéristique instantanée* $A_f(x(k), k)$*, telle que :*
Pour la forme en flèche mince type 1 :

i. les éléments non constants de la matrice $A_f(.)$ *sont isolés dans une seule rangée ;*

ii. les éléments diagonaux, $a_{f_{ii}}(.)$*, de la matrice* $A_f(.)$ *sont tels que :*

$$1 - |a_{f_{ii}}(x(k), k)| > 0 \ \forall i = 1, 2, \dots, n-1 \tag{2.19}$$

iii. il existe $\varepsilon > 0$*, tel que :*

$$(1 - |a_{f_{nn}}(x(k), k)|) - \sum_{i=1}^{n-1} \left(|a_{f_{in}}(x(k), k) a_{f_{ni}}(x(k), k)| \left(1 - |a_{fii}(x(k), k)|\right)^{-1} \right) \geq \varepsilon \tag{2.20}$$

Pour la forme en flèche mince type 2 :

i. les éléments non constants de la matrice $A_f(.)$ *sont isolés dans une seule rangée ;*

ii. les éléments diagonaux, $a_{f_{ii}}(.)$*, de la matrice* $A_f(.)$ *sont tels que :*

$$1 - |a_{f_{ii}}(x(k), k)| > 0 \ \forall i = 2, \dots, n \tag{2.21}$$

iii. il existe $\varepsilon > 0$*, tel que :*

$$(1 - |a_{f_{11}}(x(k), k)|) - \sum_{i=2}^{n} \left(|a_{f_{i1}}(x(k), k) a_{f_{1i}}(x(k), k)| \left(1 - |a_{fii}(x(k), k)|\right)^{-1} \right) \geq \varepsilon \tag{2.22}$$

Dans tout le mémoire, nous utiliserons l'une ou l'autre des formulations des conditions de stabilité par retour d'état de Borne et Gentina

Démonstration. Considérons le système majorant $M_k\left(A_f(x\left(k\right),k)\right)$, relatif à la norme vectorielle $p(z\left(k\right))$ précédente, obtenu à partir de (2.17) :

$$z\left(k+1\right) = M_k\left(A_f(x\left(k\right),k)\right) z\left(k\right) \tag{2.23}$$

Le système (2.10) est stabilisable par (2.11), si la matrice $M_k\left(A_f(x\left(k\right),k)\right)$ est une M-matrice [Robert, 1964], de forme en flèche à éléments constants ou encore si les éléments non constants sont isolés dans une seule rangée, par application du critère pratique de Borne et Gentina [Borne *et al.*, 1976, Gentina *et al.*, 1972], on a :

– Pour la forme en flèche de type 1

$$\begin{cases} 1 - |a_{f_{ii}}(x\left(k\right),k)| > 0 \; \forall i = 1,2,\ldots,n-1 \\ \det\left(I - M_k\left(A_f(x\left(k\right),k)\right)\right) > 0 \end{cases} \tag{2.24}$$

– Pour la forme en flèche de type 2

$$\begin{cases} 1 - |a_{f_{ii}}(x\left(k\right),k)| > 0 \; \forall i = 2,\ldots,n \\ \det\left(I - M_k\left(A_f(x\left(k\right),k)\right)\right) > 0 \end{cases} \tag{2.25}$$

Pour les deux cas le développement du premier membre de la dernière inégalité du système d'inéquations :

– Pour la forme en fèche de type 1

$$\begin{aligned} &\det\left(I - M_k\left(A_f(x\left(k\right),k)\right)\right) = \\ &\left(1 - |a_{f_{nn}}(x\left(k\right),k)| - \sum_{i=1}^{n-1}\left(\begin{array}{l} |a_{f_{in}}(x\left(k\right),k)a_{f_{ni}}(x\left(k\right),k)| \\ \times\left(1 - |a_{f_{ii}}(x\left(k\right),k)|\right)^{-1} \end{array}\right)\right) \times \left(\prod_{j=1}^{n-1}\left(1 - |a_{f_{ii}}(x\left(k\right),k)|\right)\right) \end{aligned} \tag{2.26}$$

– Pour la forme en flèche de type 2

$$\begin{aligned} &\det\left(I - M_k\left(A_f(x\left(k\right),k)\right)\right) = \\ &\left(1 - |a_{f_{11}}(x\left(k\right),k)| - \sum_{i=2}^{n}\left(\begin{array}{l} |a_{f_{i1}}(x\left(k\right),k)a_{f_{1i}}(x\left(k\right),k)| \\ \times\left(1 - |a_{f_{ii}}(x\left(k\right),k)|\right)^{-1} \end{array}\right)\right) \times \left(\prod_{j=2}^{n}\left(1 - |a_{f_{ii}}(x\left(k\right),k)|\right)\right) \end{aligned} \tag{2.27}$$

achève aisément la démonstration du théorème. □

Corollaire 2.1. *Le processus défini par* (2.10) *est stabilisable par la commande définie par* (2.11)*, si le système corrigé* (2.14) *de matrice caractéristique instantanée* $A_f(x\left(k\right),k)$*, de forme en flèche mince de type 1, telle que :*

i. *les éléments non constants sont isolés dans une seule rangée ;*

ii. *les éléments* $a_{f_{ii}}(.)$, *de la matrice* $A_f(.)$ *sont tels que :*
$1 - |a_{f_{ii}}(x(k), k)| > 0,\ \forall i = 1, 2, \ldots, n-1$;

iii.

$$a_{f_{in}}(x(k), k) a_{f_{ni}}(x(k), k) \geq 0,\ \forall i = 1, \ldots, n-1 \tag{2.28}$$

iv. *il existe* $\varepsilon > 0$ *tel que le polynôme caractéristique instantané* $P_{A_f}(\lambda, x(k), k)$ *est strictement positif pour* $\lambda = 1$ *ou encore :*

$$P_{A_f}(\lambda, x(k), k)\,|_{\lambda=1} \geq \varepsilon \tag{2.29}$$

Démonstration. La démonstration du corollaire 2.1 se déduit de celle du théorème 2.1 par la prise en considération de la nouvelle hypothèse *(iii)* de ce corollaire, qui permet d'assurer l'identité de la matrice $A_f(x(k), k)$ et de sa majorante $M_k(A_f(x(k), k))$; ce cas spécifique constitue un cas de vérification de la conjecture du linéaire d'Aizerman [Grujic, 1978, Benrejeb, 2010]. □

2.3.2.3 Résultats principaux obtenus dans le cas du retour d'état

Nous envisageons, dans cette partie, la détermination d'une structure de compensateur de la forme (2.11), destinée à la stabilisation d'un processus dynamique discret non linéaire (2.10), tout en imposant à la matrice caractéristique du système bouclé la forme en flèche mince de type 1. La matrice caractéristique instantanée du système bouclé peut être mise sous forme en flèche mince de type 1 [Benrejeb *et al.*, 1982], s'il existe des gains $k_{ij}(.)$ vérifiant les égalités suivantes :

$$a_{ij}(.) - \sum_{l=1}^{m} b_{il}(.) k_{lj}(.) = 0 \quad \forall i, j = 1, \ldots, n-1 \text{ pour } i \neq j \tag{2.30}$$

Dans ce cas, les $(m \times n)$ paramètres de correction $k_{lj}(.),\ \forall j = 1, \ldots, n$ *et* $\forall l = 1, \ldots, m$, vérifiant $(n-1)(n-2)$ équations, sont à déterminer. Une condition nécessaire d'existence d'une telle solution est que le nombre d'équations à résoudre soit inférieur ou égal au nombre d'inconnues à déterminer, soit :

$$mn \geq (n-1)(n-2) \tag{2.31}$$

Théorème 2.2. *Le processus défini par* (2.10) *est stabilisable par la commande définie par* (2.11), *si le système corrigé* (2.14) *de matrice caractéristique instantanée* $A_f(x(k), k)$, *telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. les éléments diagonaux sont tels que :

$$1 - \left| a_{ii}(.) - \sum_{e=1}^{m} b_{ie}(.) k_{em}(.) \right| \geq \varepsilon \tag{2.32}$$

iii. il existe $k_{ij}(.)$ *solutions du système* (2.30) $\forall i = 1, 2, \ldots, m \;\; \forall j = 1, 2, \ldots, n-1$

iv. il existe $\varepsilon > 0$*, tel que :*

$$1 - \left| a_{nn}(.) - \sum_{l=1}^{m} b_{nl}(.) k_{\ln}(.) \right| - \sum_{i=1}^{n-1} \left(\begin{array}{l} \left| \left(a_{in}(.) - \sum_{l=1}^{m} b_{il}(.) k_{\ln}(.) \right) \right. \\ \left. \times \left(a_{ni}(.) - \sum_{l=1}^{m} b_{nl}(.) k_{li}(.) \right) \right| \\ \times \left(1 - \left| a_{ii}(.) - \sum_{l=1}^{m} b_{il}(.) k_{li}(.) \right| \right)^{-1} \end{array} \right) \geq \varepsilon \tag{2.33}$$

condition pouvant être réécrite sous la forme condensée suivante :

$$\left(1 - \left|a_{f_{nn}}(x(k), k)\right|\right) - \sum_{i=1}^{n-1} \left(\left|a_{f_{in}}(x(k), k) a_{f_{ni}}(x(k), k)\right| \left(1 - \left|a_{ii}(x(k), k)\right|\right)^{-1} \right) \geq \varepsilon \tag{2.34}$$

Démonstration. La démonstration du théorème 2.2 est similaire à celle du théorème 2.1 ; en effet, les conditions (2.32) et (2.34) sont obtenues à partir des conditions (2.19) et (2.20), en remplaçant les éléments $a_{f_{ij}}(.)$ par leurs expressions en fonction des éléments des matrices $A(.)$, $B(.)$ et $K(.)$. □

Corollaire 2.2. *Le processus défini par* (2.10)*, est stabilisable par la commande définie par* (2.11) *si la matrice caractéristique instantanée* $A_f(x(k), k)$*, définie par* (2.14)*, est telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. les éléments diagonaux sont tels que :

$$-1 < a_{ii}(.) - \sum_{l=1}^{m} b_{il}(.) k_{li}(.) < 1 \;\forall i = 1, 2, \ldots, n-1 \tag{2.35}$$

iii. il existe $k_{ij}(.)$ *solutions du système* (2.30) $\forall i = 1, 2, \ldots, m \;\forall j = 1, 2, \ldots, n-1$

iv.

$$\left(a_{in}(.) - \sum_{l=1}^{m} b_{il}(.) k_{\ln}(.) \right) \left(a_{ni}(.) - \sum_{l=1}^{m} b_{nl}(.) k_{li}(.) \right) \geq 0, \;\forall i = 1, \ldots, n-1 \tag{2.36}$$

v. il existe $\varepsilon > 0$ *tel que le polynôme caractéristique instantané* $P_{A_f}(\lambda, x(k), k)$ *de* $A_f(.)$, *vérifie la condition suivante :*

$$P_{A_f}(1, .) \geq \varepsilon \tag{2.37}$$

Démonstration. La démonstration du corollaire 2.2 se déduit de celle du théorème 2.2, en explicitant les éléments de la matrice caractérisant le système dynamique discret non linéaire corrigé, et en tenant compte de l'hypothèse *(iv)* qui se traduit par : $M_k(A_f(.)) \equiv A_f(.)$ et en remarquant que :

$$\det(I - M_k(A_f(.))) = P_{A_f}(1, .) \tag{2.38}$$

Ce qui achève la démonstration du corollaire 2.2. □

2.3.3 Cas de lois de commande par réaction de sortie de systèmes discrets

2.3.3.1 Description des systèmes étudiés

Dans cette partie, il s'agit d'adapter les conditions de stabilisation, précédemment établies, dans le cas d'une commande par retour de sortie.
Considérons le système discret décrit par l'équation d'état suivante :

$$\begin{cases} x(k+1) = A(x(k)\,k)\,x(k) + B(x(k)\,k)\,u(k) \\ y(k) = C(x(k)\,k)\,x(k) \end{cases} \tag{2.39}$$

où, à l'instant kT, $x(k)$ représente le vecteur état de dimension n, $u(k)$ le vecteur des entrées de commande de dimension m, $A(x(k), k) = \{a_{ij}(x(k), k)\}$ une matrice $n \times n$, $B(x(k), k)$ une matrice $n \times m$, $B(x(k), k) = \{b_{ij}(x(k), k)\}$, $C(x(k), k) = \{c_{ij}(x(k), k)\}$ une matrice $l \times n$, T étant la période d'échantillonnage et $y(k)$ le vecteur de sortie de dimension l.
La loi de commande stabilisante par retour de sortie est de la forme :

$$u(k) = -K(x(k), k)y(k) \tag{2.40}$$

telle que $K(x(k), k) = \{k_{ij}(x(k), k)\}$ est une matrice de dimension $m \times l$ à déterminer.
Il vient le système bouclé décrit par :

$$x(k+1) = A_f(x(k), k)x(k) \tag{2.41}$$

avec :

$$A_f(x(k),k) = A(x(k),k) - B(x(k),k)K(x(k),k)C(x(k),k) \tag{2.42}$$

Les éléments des matrices $A(.)$, $B(.)$, $C(.)$ et $K(.)$ peuvent être non linéaires.

2.3.3.2 Conditions de stabilisabilité par retour de sortie des systèmes discrets

Nous envisageons, dans cette partie, la détermination d'une structure de compensateur par retour de sortie de la forme (2.40), destinée à la stabilisation d'un processus dynamique discret non linéaire (2.39), tout en imposant à la matrice caractéristique du système bouclé la forme en flèche mince de type 1. Pour être mise sous cette forme, la condition suivante doit être vérifiée :

$$a_{ij}(.) - \sum_{s=1}^{l}\left(\sum_{r=1}^{m} b_{ir}(.)\,k_{rs}(.)\right)c_{sj}(.) = 0 \quad \forall i,j = 1,\ldots,n-1 \quad i \neq j \tag{2.43}$$

Dans ce cas, les $(m \times l)$ paramètres de correction $k_{ij}(.)$, $\forall\, i = 1,\ldots,m$ et $\forall\, j = 1,\ldots,l$, vérifiant $(n-1)(n-2)$ équations, sont à déterminer. Une condition nécessaire d'existence d'une telle solution est que le nombre d'équations à résoudre soit inférieur ou égal au nombre d'inconnues à déterminer, soit :

$$ml \geq (n-1)(n-2) \tag{2.44}$$

Théorème 2.3. *Le processus défini par* (2.39)*, est stabilisable par la commande définie par* (2.40)*, si la matrice caractéristique instantanée* $A_f(x(k),k)$*, du système corrigé définie par* (2.42)*, peut être mise sous la forme en flèche mince de type* (2.14) *et est telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. il existe $k_{ij}(.)$ *solutions du système d'équations (2.43)* $\forall i = 1,2,\ldots,m\ \forall j = 1,2,\ldots,l$ *;*

iii. les éléments diagonaux sont tels que :

$$1 - \left| a_{ii}(.) - \sum_{s=1}^{l}\left(\sum_{r=1}^{m} b_{ir}(.)\,k_{rs}(.)\right)c_{si}(.) \right| > 0 \ \forall i = 1,2,\ldots,n-1 \tag{2.45}$$

iv. il existe $\varepsilon > 0$, tel que :

$$\left(\begin{array}{l} 1 - \left| a_{nn}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{nr}(.) k_{rs}(.) \right) c_{sn}(.) \right| \\ - \sum\limits_{i=1}^{n-1} \left(\begin{array}{l} \left| \begin{array}{l} \left(a_{in}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{ir}(.) k_{rs}(.) \right) c_{sn}(.) \right) \\ \times \left(a_{ni}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{nr}(.) k_{rs}(.) \right) c_{si}(.) \right) \end{array} \right| \\ \times \left(1 - \left| a_{ii}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{ir}(.) k_{rs}(.) \right) c_{si}(.) \right| \right)^{-1} \end{array} \right) \end{array} \right) \geq \varepsilon \quad (2.46)$$

Dans tout le mémoire, nous utiliserons l'une ou l'autre des formulations des conditions de stabilité par retour de sortie de Borne et Gentina

Démonstration. La démonstration du théorème 2.3 est similaire à celle du théorème 2.1 ; En effet, les conditions (2.45) et (2.46) sont obtenues à partir des conditions (2.19) et (2.20), en remplaçant les éléments $a_{f_{ij}}(.)$ par leurs expressions en fonction des éléments des matrices $A(.)$, $B(.)$ $C(.)$ et $K(.)$. □

Corollaire 2.3. *Le processus défini par* (2.39) *est stabilisable par la commande définie par* (2.40)*, si la matrice caractéristique instantanée $A_f(x(k), k)$ du système corrigé, définie par* (2.42)*, est en flèche mince telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. il existe $k_{ij}(.)$ solutions du système d'équations (2.43) $\forall i = 1, 2, \ldots, m$ $\forall j = 1, 2, \ldots, l$ *;*

iii. les éléments diagonaux sont tels que :

$$-1 < a_{ii}(.) - \sum_{s=1}^{l} \left(\sum_{r=1}^{m} b_{ir}(.) k_{rs}(.) \right) c_{si}(.) < 1 \ \forall i = 1, 2, \ldots, n-1 \quad (2.47)$$

iv.

$$\begin{array}{l} \left(a_{in}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{ir}(.) k_{rs}(.) \right) c_{sn}(.) \right) \\ \times \left(a_{ni}(.) - \sum\limits_{s=1}^{l} \left(\sum\limits_{r=1}^{m} b_{nr}(.) k_{rs}(.) \right) c_{si}(.) \right) \geq 0, \ \forall i = 1, \ldots, n-1 \end{array} \quad (2.48)$$

v. il existe $\varepsilon > 0$, tel que le polynôme caractéristique instantané $P_{A_f}(\lambda, x(k), k)$ de $A_f(.)$, vérifie la condition suivante :

$$P_{A_f}(1, .) \geq \varepsilon \quad (2.49)$$

Ce corollaire constitue un cas de vérification de la conjecture du linéaire d'Aizerman.

2.3.4 Conclusion

La méthode de stabilisation proposée, dans cette section, exploite avec succès les conditions suffisantes de stabilité utilisant les normes vectorielles présentées dans le premier chapitre. Cette méthode est basée sur le choix d'une représentation par la mise sous forme en flèche mince de la matrice caractéristique instantanée du processus bouclé dans l'espace d'état, associé au choix des paramètres de la loi de commande stabilisante. L'application de cette méthode, à des fins de synchronisation des systèmes hyperchaotiques discrets, est envisagée dans la partie suivante.

2.4 Application à la synchronisation des systèmes chaotiques discrets par retour d'état

2.4.1 Idée de base

Après la présentation de l'approche de stabilisation proposée, utilisant le critère pratique de Borne et Gentina pour l'étude de la stabilité et la mise sous forme en flèche, nous abordons, dans cette partie, la notion de synchronisation. Jusqu'en 1990, l'apparition de phénomènes chaotiques dans l'évolution de systèmes dynamiques était indésirable, car ce phénomène était incontrôlable. La théorie du contrôle du chaos formulée dans [Ott *et al.*, 1990], puis les articles de [Pecora et Carroll, 1990, Carroll et Pecora, 1991] ont ouvert la voie à une recherche fructueuse sur les applications du chaos. Les techniques de synchronisation utilisées sont basées sur les techniques d'estimation d'état. Dans la suite de ce chapitre, l'idée consiste à appliquer les approches de stabilisation par retour d'état d'une part et par retour de sortie d'autre part, développées dans la partie précédente, pour la résolution du problème de synchronisation des systèmes maître / esclave considérés.

2.4.2 Conditions de synchronisation par couplage unidirectionnel utilisant la commande par retour d'état proposée

2.4.2.1 Cas de la synchronisation de deux systèmes hyperchaotiques de Hénon (Baier-Klein)

Les systèmes hyperchaotiques de Hénon considérés sont introduits dans [Baier et Klein, 1990, Grassi et Miller, 2002].

A un système de Hénon généralisé, considéré en tant que système maître et décrit par :

$$\begin{cases} x_{m1}(k+1) = \mu - x_{m2}^2(k) - bx_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \end{cases} \tag{2.50}$$

est associé un système identique du type esclave, défini par :

$$\begin{cases} x_{s1}(k+1) = \mu - x_{s2}^2(k) - bx_{s3}(k) + u_1(k) \\ x_{s2}(k+1) = x_{s1}(k) + u_2(k) \\ x_{s3}(k+1) = x_{s2}(k) + u_3(k) \end{cases} \tag{2.51}$$

$x_m(k) = [x_{m1}(k)\, x_{m2}(k)\, x_{m3}(k)]^T$ représente le vecteur d'état du système maître, $x_s(k) = [x_{s1}(k)\ \ x_{s2}(k)\ \ x_{s3}(k)]^T$ celui du système esclave et $u(k) = [u_1(k)\ \ u_2(k)\ \ u_3(k)]^T$ la commande active à déterminer pour assurer la synchronisation complète, l'anti-synchronisation ou la synchronisation hybride des deux systèmes.

L'attracteur hyperchaotique (2.50) est caractérisé par : $b = 0.1$ et $\mu = 1.76$, avec les états initiaux $x_m(0) = (1, 0.1, 0)$ [Baier et Klein, 1990, Grassi et Miller, 2002].

Considérons les écarts dynamiques sur les variables d'état entre les deux systèmes hyperchaotiques, définis par :

$$e_i(k) = x_{si}(k) - x_{mi}(k),\ \forall i = 1, 2, 3 \tag{2.52}$$

Il vient la représentation du système écart :

$$\begin{cases} e_1(k+1) = -(x_{s2}(k) + x_{m2}(k))e_2(k) - 0.1e_3(k) + u_1(k) \\ e_2(k+1) = e_1(k) + u_2(k) \\ e_3(k+1) = e_2(k) + u_3(k) \end{cases} \tag{2.53}$$

ou encore matriciellement :

$$e(k+1) = A_s(x(k))\, e(k) + Bu(k) \tag{2.54}$$

$$u(k) = -K(x(k), k)\, e(k) \tag{2.55}$$

avec :

$$A_s(x(k)) = \begin{bmatrix} 0 & -(x_{s2}(k) + x_{m2}(k)) & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.56}$$

et :

$$B = I_{3\times 3} \tag{2.57}$$

La figure 2.4.1 présente les évolutions des écarts dynamiques entre les systèmes (2.50) et (2.51) lorsque la commande par retour d'état n'est pas activée avec les états initiaux $x_s(0) = (-0.5, 0, 0.3)$. Il est clair que l'erreur évolue chaotiquement avec le temps.

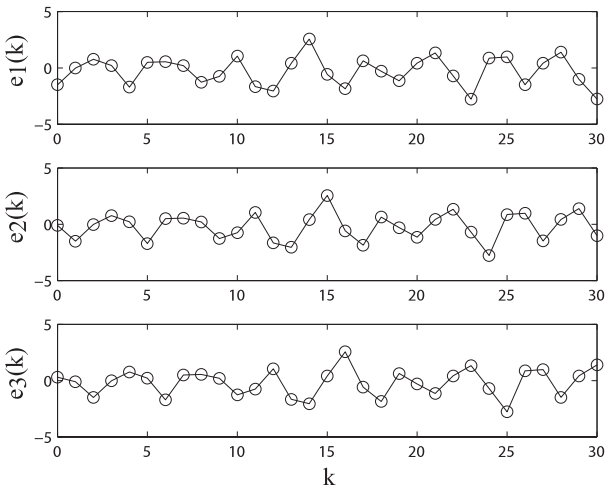


FIGURE 2.4.1 – Dynamiques des erreurs pour les systèmes du troisième ordre de Hénon généralisés lorsque le contrôle est désactivé

Du point de vue théorique, la synchronisation de système (2.53) est équivalente à la stabilisation du système (2.54) selon la loi de commande de rétroaction $u(k)$.
Pour atteindre cet objectif, nous allons considérer $u(k)$ et déterminer les gains $k_{ij}(.)$ de la loi de commande (2.55) :

$$K(x(k)) = \begin{bmatrix} k_{11}(x(k)) & k_{12}(x(k)) & k_{13}(x(k)) \\ k_{21}(x(k)) & k_{22}(x(k)) & k_{23}(x(k)) \\ k_{31}(x(k)) & k_{32}(x(k)) & k_{33}(x(k)) \end{bmatrix} \tag{2.58}$$

L'équation aux erreurs devient :

$$e(k+1) = A_{sc}(x(k))e(k) \tag{2.59}$$

avec :

$$A_{sc}(x(k)) = A_s(x(k)) - BK(x(k)) \tag{2.60}$$

$A_{sc}(x(k))$ peut être réécrite sous la forme :

$$A_{sc}(x(k)) = \begin{bmatrix} -k_{11}(x(k)) & -(x_{s2}(k) + x_{m2}(k)) - k_{12}(x(k)) & -0.1 - k_{13}(x(k)) \\ 1 - k_{21}(x(k)) & -k_{22}(x(k)) & -k_{23}(x(k)) \\ -k_{31}(x(k)) & 1 - k_{32}(x(k)) & -k_{33}(x(k)) \end{bmatrix} \tag{2.61}$$

Le choix des paramètres du système de commande k_{23} et k_{32} constants, tels que :

$$\begin{cases} 1 - k_{32} = 0 \\ k_{23} = 0 \end{cases} \tag{2.62}$$

permet la mise de la matrice caractéristique $A_{sf}(x(k))$ sous forme en flèche de Benrejeb :

$$A_{sf}(x(k)) = \begin{bmatrix} -k_{11}(x(k)) & -(x_{s2}(k) + x_{m2}(k)) - k_{12}(x(k)) & -0.1 - k_{13}(x(k)) \\ 1 - k_{21}(x(k)) & -k_{22}(x(k)) & 0 \\ -k_{31}(x(k)) & 0 & -k_{33}(x(k)) \end{bmatrix} \tag{2.63}$$

Le système caractérisé par (2.63) est asymptotiquement stable, si les gains de contrôle $k_{ij}(x(k))$, $i, j = 1, 2, 3$, sont choisis de telle sorte que les contraintes suivantes soient satisfaites :

i. les éléments non linéaires de la matrice $A_{sf}(x(k))$ sont isolés dans une rangée ;

ii. les éléments diagonaux de la matrice $A_{sf}(x(k)$ sont, tels que :

$$\begin{cases} 1 - |k_{33}(x(k))| > 0 \\ 1 - |k_{22}(x(k))| > 0 \end{cases} \tag{2.64}$$

iii. il existe $\varepsilon > 0$, tel que :

$$\begin{cases} 1 - |k_{11}(x(k))| - \frac{|k_{31}(x(k))(0.1 + k_{13}(x(k)))|}{1 - |k_{33}(x(k))|} \\ - \frac{|(k_{12}(x(k)) + x_{s2}(k) + x_{m2}(k))(1 - k_{21}(x(k)))|}{1 - |k_{22}(x(k))|} \end{cases} \geq \varepsilon \tag{2.65}$$

Pour satisfaire les contraintes (2.64) et (2.65), les paramètres de correction $k_{ij}(x(k)), \forall i, j = 1, 2, 3$ peuvent être choisis, tels que :

$$K(x(k)) = \begin{bmatrix} 0.05 & 0.5 - x_{s2}(k) - x_{m2}(k) & 0.1 \\ 0.5 & 0.5 & 0 \\ 0.2 & 1 & 0.8 \end{bmatrix} \tag{2.66}$$

impliquant ainsi que le système (2.50) va globalement se synchroniser avec le système (2.51).

La figure 2.4.1 a montré les écarts dynamiques dans le cas où la commande des deux systèmes chaotiques (2.50) et (2.51) couplés n'est pas activée. Les figures 2.4.2 et 2.4.3, montrent, respectivement, les évolutions des variables d'état des systèmes maître et esclave et des différents états du système écart, résultant du couplage de (2.50) avec (2.51), après

l'activation du signal de commande, permettant la synchronisation de ces deux systèmes. Ces résultats illustrent, ainsi, l'efficacité de l'approche de commande proposée. La figure 2.4.3 montre que $e_1(k)$ converge vers zéro après 4 itérations et $e_2(k)$ *et* $e_3(k)$ après 5 itérations.

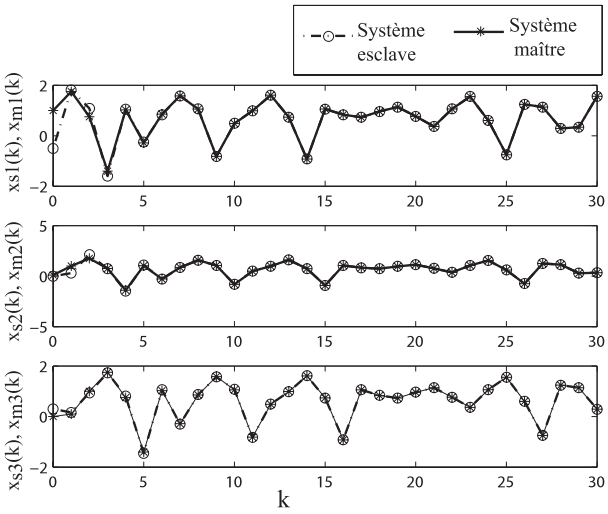


FIGURE 2.4.2 – Réponses temporelles du système hyperchaotique maître ($*$) et du système hyperchaotique esclave ($\ominus$)

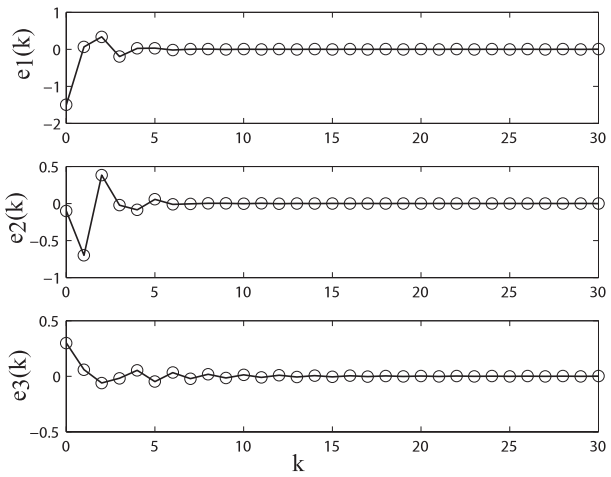


FIGURE 2.4.3 – Dynamiques de l'erreur de deux systèmes hyperchaotiques de troisième ordre de type Hénon généralisé lorsque la commande est active.

2.4.2.2 Cas de l'anti-synchronisation de deux systèmes hyperchaotiques de Hénon

Dans cette section, l'objectif est de concevoir une structure de commande par retour d'état de telle sorte que le système de Hénon généralisé du troisième ordre (2.51) soit anti-synchronisé avec celui (2.50), c'est-à-dire, de permettre la convergence de la somme des signaux oscillants vers zéro, lorsque $k \to +\infty$.
Prenons, dans le cas présent, le vecteur d'erreur suivant :

$$e\left(k+1\right) = x_{si}\left(k\right) + x_{mi}\left(k\right),\ \forall i = 1,2,3 \tag{2.67}$$

Il vient les équations régissant le comportement du système écart entre ces deux systèmes (2.50) et (2.51) :

$$\begin{cases} e_1\left(k+1\right) = -x_{m2}^2\left(k\right) - x_{s2}^2\left(k\right) - 0.1e_3\left(k\right) + 3.52 + u_1\left(k\right) \\ e_2\left(k+1\right) = e_1\left(k\right) + u_2\left(k\right) \\ e_3\left(k+1\right) = e_2\left(k\right) + u_3\left(k\right) \end{cases} \tag{2.68}$$

Les équations précédentes (2.68) peuvent être réécrites sous la description matricielle suivante :

$$e\left(k+1\right) = A_{As}(x\left(k\right))e\left(k\right) + Bu\left(k\right) + C_{As}(x\left(k\right)) \tag{2.69}$$

avec :

$$A_{As}(x\left(k\right)) = \begin{bmatrix} 0 & x_{s2}\left(k\right) - x_{m2}\left(k\right)) & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.70}$$

$$C_{As}(x\left(k\right)) = \begin{bmatrix} 3.52 - 2x_{s2}^2\left(k\right) \\ 0 \\ 0 \end{bmatrix} \tag{2.71}$$

et : $B = I_{3\times 3}$.
La figure 2.4.4 montre les écarts dynamiques dans le cas où la commande des deux systèmes hyperchaotiques (2.50) et (2.51) n'est pas activée. Il est évident que l'erreur évolue chaotiquement avec le temps.

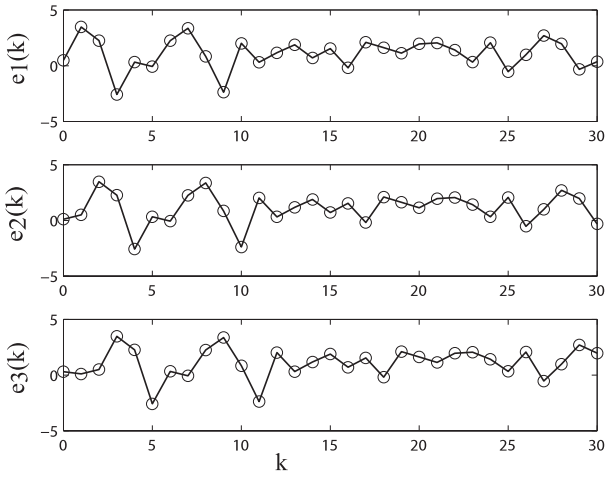


FIGURE 2.4.4 – Dynamiques de l'erreur de deux systèmes couplés de Hénon lorsque la commande est désactivée.

Pour obtenir la propriété d'anti-synchronisation entre les systèmes identiques de Hénon généralisé de troisième ordre (2.50) et (2.51) et en se référant à l'hypothèse mentionnée dans le théorème énoncé dans la section précédente, on va déterminer une loi de commande, par retour d'état et par compensation du terme complémentaire $C_{As}(x(k))$ figurant dans la description (2.69), de la forme :

$$u_i(k) = -f_i(x(k)) - \sum_{j=1}^{3} k_{ij}(x(k))\, e_j(k)\,,\ \forall i = 1,2,3 \tag{2.72}$$

$$u(k) = -\begin{bmatrix} 3.52 - 2x_{s2}^2(k) \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} k_{11}(x(k)) & k_{12}(x(k)) & k_{13}(x(k)) \\ k_{21}(x(k)) & k_{22}(x(k)) & k_{23}(x(k)) \\ k_{31}(x(k)) & k_{32}(x(k)) & k_{33}(x(k)) \end{bmatrix} e(k) \tag{2.73}$$

La loi de commande par retour d'état permet de décrire le système erreur (2.69) comme suit :

$$e(k+1) = A_{Asc}(x(k))e(k) \tag{2.74}$$

avec :

$$A_{Asc}(x(k)) = A_{As}(x(k)) - BK(x(k)) \tag{2.75}$$

$A_{Asc}(x(k))$ peut être réécrite sous la forme suivante :

$$A_{Asc}(x(k)) = \begin{bmatrix} -k_{11}(x(k)) & x_{s2}(k) - x_{m2}(k) - k_{12}(x(k)) & -0.1 - k_{13}(x(k)) \\ 1 - k_{21}(x(k)) & -k_{22}(x(k)) & -k_{23}(x(k)) \\ -k_{31}(x(k)) & 1 - k_{32}(x(k)) & -k_{33}(x(k)) \end{bmatrix} \tag{2.76}$$

En procédant comme précédemment, afin de caractériser le système en boucle fermée par une matrice de forme en flèche mince, les paramètres de correction k_{23} et k_{32} doivent être choisis selon les relations (2.62).
Ensuite, les paramètres de la chaîne de correction restants $k_{ij}(x(k)), \forall i,j = 1,2,3, (i,j) \neq (2,3)\ (i,j) \neq (3,2)$, peuvent être choisis de telle sorte que les contraintes (2.64) et (2.65) du théorème soient satisfaites, soit :

$$K(x(k)) = \begin{bmatrix} 0.05 & 0.5 - x_{m2}(k) + x_{s2}(k) & 0.1 \\ 0.5 & 0.5 & 0 \\ 0.2 & 1 & 0.8 \end{bmatrix} \tag{2.77}$$

Le système (2.74) converge ainsi vers zéro et l'anti-synchronisation des systèmes (2.50) et (2.51) est assurée, comme le montre les figures 2.4.5, 2.4.6 et 2.4.7.

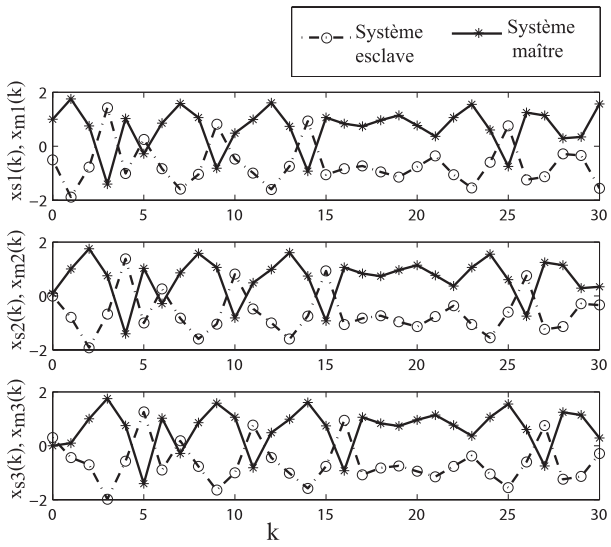


FIGURE 2.4.5 – Evolutions temporelles des variables d'état des deux systèmes identiques de Hénon généralisés de types maître $*$ et esclave $\ominus$, après l'activation des signaux de commande.

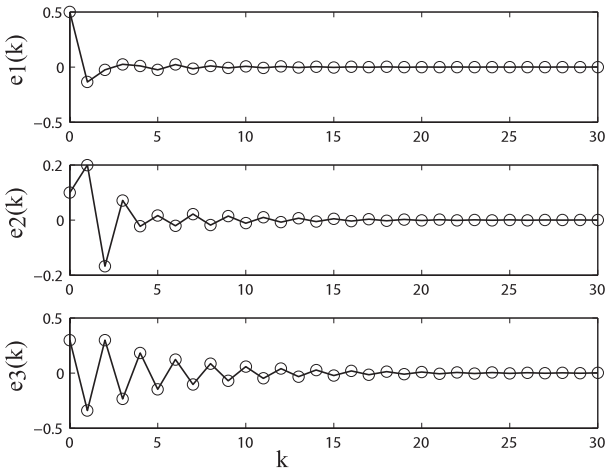


FIGURE 2.4.6 – Dynamiques de l'erreur des deux systèmes couplés de troisième ordre Hénon généralisé après activation de la commande.

La mise en oeuvre de la commande caractérisée par (2.73) et (2.77) a abouti aux résultats de la figure 2.4.6 qui met en exergue, en particulier, la convergence vers zéro du système erreur suite à l'application de la commande proposée. On peut observer que $e_1(k)$, $e_2(k)$ *et* $e_3(k)$ convergent vers zéro respectivement en 2, 4 et 11 itérations. La figure 2.4.5 montre trois trajectoires évoluant, dans des directions opposées.

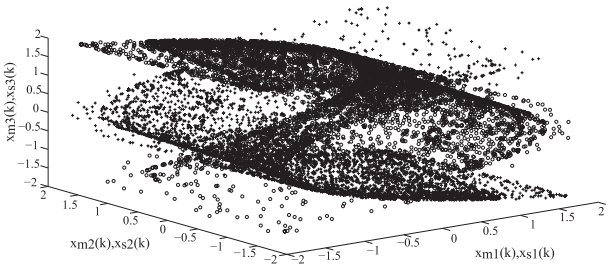


FIGURE 2.4.7 – Attracteur du système hyperchaotique maître (o) et du système hyperchaotique esclave ($+$).

La figure 2.4.7 représente la projection des attracteurs sur le plan de dimension 3, $x_{mi}(k)$ et $x_{si}(k)$, $\forall\, i = 1, 2, 3$. Nous pouvons conclure que les vecteurs d'état des systèmes maître et esclave évoluent dans des directions opposées.

2.4.2.3 Cas de la synchronisation hybride de deux systèmes hyperchaotiques de Hénon (Baier-Klein)

Dans cette section, nous nous concentrons sur le problème du processus de synchronisation hybride de deux systèmes hyperchaotiques identiques généralisés de Hénon.
Le vecteur d'erreur défini par :

$$\begin{cases} e_1(k+1) = x_{s1}(k) - x_{m1}(k) \\ e_2(k+1) = x_{s2}(k) + x_{m2}(k) \\ e_3(k+1) = x_{s3}(k) - x_{m3}(k) \end{cases} \tag{2.78}$$

conduit au système d'erreur suivant :

$$\begin{cases} e_1(k+1) = (x_{m2}(k) - x_{s2}(k))e_2(k) - 0.1e_3(k) + u_1(k) \\ e_2(k+1) = e_1(k) + 2x_{m1}(k) + u_2(k) \\ e_3(k+1) = e_2(k) - 2x_{m2}(k) + u_3(k) \end{cases} \tag{2.79}$$

Celui-ci peut être réécrit sous la forme matricielle suivante :

$$e(k+1) = A_{Hs}(x(k))e(k) + Bu(k) + C_{Hs}(x(k)) \tag{2.80}$$

avec :

$$A_{Hs}(x(k)) = \begin{bmatrix} 0 & x_{m2}(k) - x_{s2}(k) & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.81}$$

$$C_{Hs}(x(k)) = \begin{bmatrix} 0 \\ 2x_{m1}(k) \\ -2x_{m2}(k) \end{bmatrix} \tag{2.82}$$

et : $B = I_{3\times 3}$.
La figure 2.4.8 montre les dynamiques du système erreur lorsque la commande est désactivée. On peut conclure que ce système évolue chaotiquement avec le temps.

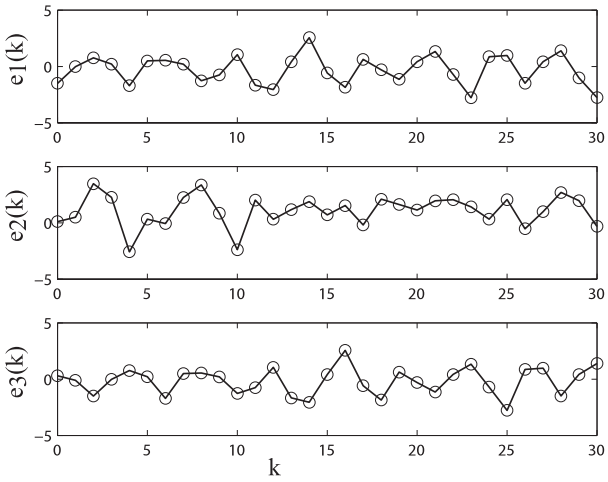


FIGURE 2.4.8 – Dynamiques de l'erreur de deux systèmes de troisième ordre Hénon généralisé lorsque la commande est désactivée.

Comme précédemment, nous cherchons une loi de commande stabilisante de la forme suivante :

$$u_i(k) = -f_i'(x(k)) - \sum_{j=1}^{3} k_{ij}(x(k))e_j(k),\ \forall i = 1,2,3 \tag{2.83}$$

$$u(k) = -\begin{bmatrix} 0 \\ 2x_{m1}(k) \\ -2x_{m2}(k) \end{bmatrix} - \begin{bmatrix} k_{11}(x(k)) & k_{12}(x(k)) & k_{13}(x(k)) \\ k_{21}(x(k)) & k_{22}(x(k)) & k_{23}(x(k)) \\ k_{31}(x(k)) & k_{32}(x(k)) & k_{33}(x(k)) \end{bmatrix} e(k) \tag{2.84}$$

Il vient le système erreur dans l'espace d'état suivant :

$$e(k+1) = A_{Hsc}(x(k))e(k) \tag{2.85}$$

avec :

$$A_{Hsc}(x(k)) = A_{Hs}(x(k)) - BK(x(k)) \tag{2.86}$$

$A_{Hsc}(x(k))$ peut être réécrite comme suit :

$$A_{Hsc}(x(k)) = \begin{bmatrix} -k_{11}(x(k)) & x_{m2}(k) - x_{s2}(k) - k_{12}(x(k)) & -0.1 - k_{13}(x(k)) \\ 1 - k_{21}(x(k)) & -k_{22}(x(k)) & -k_{23}(x(k)) \\ -k_{31}(x(k)) & 1 - k_{32}(x(k)) & -k_{33}(x(k)) \end{bmatrix} \tag{2.87}$$

Si ces lois de rétroaction stabilisent le système (2.79), $e_1(k)$, $e_2(k)$ et $e_3(k)$ convergeront vers zéro quand $k \to +\infty$, impliquant ainsi la synchronisation hybride des deux systèmes identiques (2.50) et (2.51) de Hénon.

Pour atteindre cet objectif, la matrice des gains $k_{ij}(x(k))$, $\forall i,j = 1,2,3$, relative à la description du système sous forme en flèche mince et la vérification des inégalités (2.64) et (2.65) du théorème énoncé dans la section précédente pour l'étude de la stabilité :

$$K(x(k)) = \begin{bmatrix} 0.05 & 0.5 + x_{m2}(k) - x_{s2}(k) & 0.1 \\ 0.5 & 0.5 & 0 \\ 0.2 & 1 & 0.8 \end{bmatrix} \tag{2.88}$$

garantit la synchronisation hybride des deux systèmes du troisième ordre de Hénon (Baier-Klein) couplés étudiés comme le montre les figures 2.4.9 et 2.4.10.

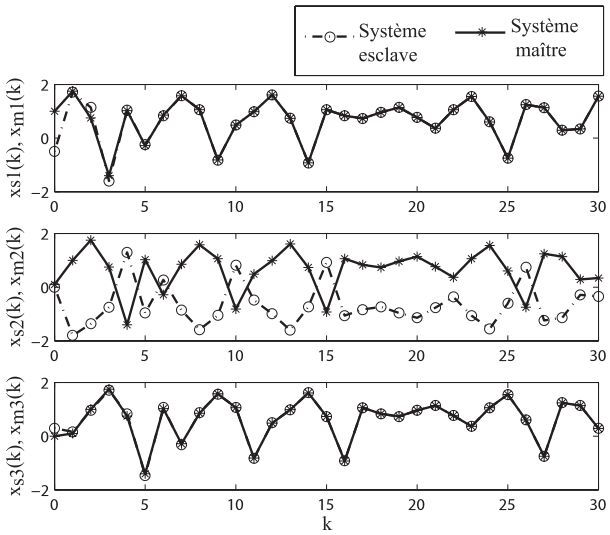


FIGURE 2.4.9 – Réponses temporelles des variables d'état des systèmes hyperchaotiques maître $*$ et esclave $\ominus$.

On peut conclure, d'après la figure 2.4.10 que $e_1(k)$, $e_2(k)$ et $e_3(k)$ convergent vers zéro respectivement après 4, 6 et 5 itérations.

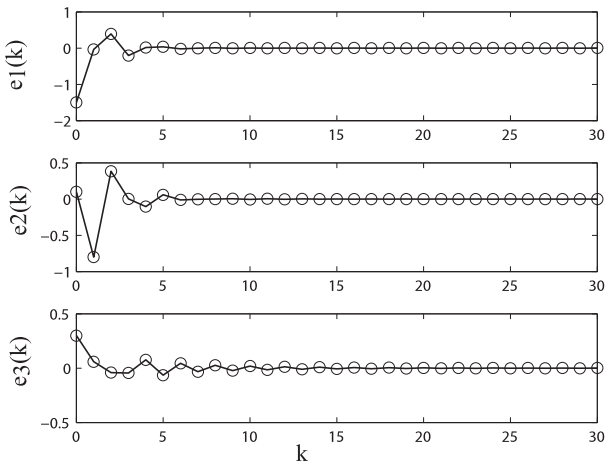


FIGURE 2.4.10 – Dynamiques de l'erreur résultant du couplage de deux systèmes hyperchaotiques de type Hénon généralisé lorsque la commande est activée

2.4.3 Synchronisation maître-esclave de systèmes chaotiques proposés non identiques

2.4.3.1 Mise en situation

Dans cette partie, il est envisagé de déterminer une commande afin d'accomplir la synchronisation de deux systèmes non identiques de types maître et esclave.
On considère, comme précédemment, un système hyperchaotique de dimension n considéré en tant que système maître décrit comme suit :

$$x_m(k+1) = Ax_m(k) + E + f(x_m(k)) \tag{2.89}$$

E étant un vecteur constant.
On associe au système maître un système non identique du type esclave défini par :

$$x_s(k+1) = A_1 x_s(k) + E_1 + f_1(x_s(k)) + Bu(k) \tag{2.90}$$

avec : $x_m(k) = \left[\begin{array}{ccc} x_{m1}(k) & \ldots & x_{mn}(k) \end{array} \right]^T \in R^n$, $x_s(k) = \left[\begin{array}{ccc} x_{s1}(k) & \ldots & x_{sn}(k) \end{array} \right]^T \in R^n$ et E_1 un vecteur constant.
Soit B la matrice identité :

$$B = I_{n\times n} \tag{2.91}$$

$A = \{a_{ij}\}$ et $A_1 = \{a_{1_{ij}}\}$ des matrices à éléments constants, $f(x_m(k))$ et $f_1(x_s(k))$ deux vecteurs à éléments non linéaires. La commande active $u(k)$ est à déterminer pour assurer

la synchronisation des deux systèmes non identiques (2.89) et (2.90).
Les écarts des variables d'état, définis par :

$$e(k) = x_s(k) - x_m(k) \tag{2.92}$$

conduit au système écart suivant :

$$e(k+1) = A_1 x_s(k) - A x_m(k) + f_1(x_s(k)) - f(x_m(k)) + E_1 - E + Bu(k) \tag{2.93}$$

La structure de la loi de commande $u(k)$, retenue dans le cas présent, par retour d'état et par compensation du terme complémentaire, est formulée comme suit :

$$u(k) = (A - A_1) x_s(k) + f(x_s(k)) - f_1(x_s(k)) - E_1 + E - K(.)e(k) \tag{2.94}$$

$K(.) = \{k_{ij}(.)\} \in R^{n \times n}$ étant des gains inconnus à déterminer pour assurer la synchronisation.
L'introduction de la commande par retour d'état (2.94) dans le système (2.93) conduisent à la nouvelle représentation du système erreur comme suit :

$$e(k+1) = Ae(k) + f(x_s(k)) - f(x_m(k)) - BK(.)e(k) \tag{2.95}$$

On peut noter que le choix du retour d'état $u(k)$ définie en (2.94), réduit l'étude de la synchronisation de deux systèmes hyperchaotiques non identiques à celle de deux systèmes hyperchaotiques identiques.
Pour plusieurs systèmes chaotiques, le vecteur écart suivant : $f(x_s(k)) - f(x_m(k))$ peut être factorisé comme suit, [Jiang *et al.*, 2003] :

$$f(x_s(k)) - f(x_m(k)) = Q(x_m(k), x_s(k)) e(k) \tag{2.96}$$

où $Q(x_s(k), x_m(k))$ est une matrice bornée dont les éléments dépendent des composantes des vecteurs d'état $x_m(k)$ et $x_s(k)$.
Le système peut être, dans ce cas, réécrit comme suit :

$$e(k+1) = A_f(x_m(k), x_s(k)) e(k) \tag{2.97}$$

avec :

$$A_f(x_m(k), x_s(k)) = (A + Q(x_s(k), x_m(k)) - BK(.)) \tag{2.98}$$

Le système erreur, décrit par (2.95) est stabilisé par le choix judicieux de la loi de commande définie par (2.94), si la matrice $A_f(x_m(k), x_s(k))$, définie par (2.98), est en forme

en flèche. Pour atteindre cet objectif, le théorème établi suivant, est basé sur l'utilisation du critère de Borne et Gentina [Borne *et al.*, 1972, Borne *et al.*, 1976, Borne, 1987, Gentina *et al.*, 1972], associé à la représentation en flèche de Benrejeb de la matrice $A_f(.) = \{a_{a_{ij}}(.)\} = (A + Q(x_s(k), x_m(k)) - BK(.))$ [Benrejeb et Borne, 1978, Benrejeb *et al.*, 1982, Benrejeb et Hammami, 2008, Borne *et al.*, 2007, Borne et Benrejeb, 2008], donnant ainsi des conditions suffisantes de la synchronisation du système esclave (2.89) avec le système maître (2.90) [Benrejeb, 2010, Benrejeb et Hammami, 2008].

Théorème 2.4. *Le processus erreur défini par* (2.95) *converge vers zéro, si la matrice caractéristique instantanée* $A_f(.)$ *du système corrigé, définie par* (2.98)*, de forme en flèche mince de type 2 comme définie par* (2.15)*, est telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. les éléments diagonaux $a_{f_{ii}}(.)$*, de la matrice* $A_f(.)$*, sont tels que :*

$$1 - |a_{f_{ii}}(.)| > 0, \ \forall i = 2, \ldots, n \tag{2.99}$$

iii. il existe $\varepsilon > 0$*, tel que :*

$$1 - |a_{f_{11}}(.)| - \sum_{i=2}^{n} \left(\begin{array}{l} |a_{f_{i1}}(.)\, a_{f_{1i}}(.)| \\ \times (1 - |a_{f_{ii}}(.)|)^{-1} \end{array} \right) \geq \varepsilon \tag{2.100}$$

Démonstration. La démonstration du théorème 2.4 est similaire à celle du théorème 2.1, □

2.4.3.2 Cas de la synchronisation du système de Hénon (Hitzl-Zele) couplé avec le système de Hénon (Baier-Klein)

On considère le système hyperchaotique de type Baier-Klein de troisième ordre (aussi appelé système de Hénon généralisé) [Baier et Klein, 1990, Miller et Grassi, 2001] décrit comme suit :

$$\begin{cases} x_{m1}(k+1) = b - x_{m2}^2(k) - a.x_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \end{cases} \tag{2.101}$$

$a = 0.1$ et $b = 1.76$.

Dans l'espace d'état, (2.101) peut être réécrite comme suit :

$$x_m(k+1) = Ax_m(k) + f(x_m(k)) + E \tag{2.102}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.103}$$

$$f\left(x_m\left(k\right)\right) = \begin{bmatrix} -x_{m2}^2\left(k\right) & 0 & 0 \end{bmatrix}^T \tag{2.104}$$

et :

$$E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T \tag{2.105}$$

On considère, maintenant le système hyperchaotique d'ordre 3D Hénon (Hitzl-Zele) [Y.J. Xue, 2003, Hitzl et Zele, 1985] :

$$\begin{cases} x_{s1}\left(k+1\right) = -b_1 x_{s2}\left(k\right) + u_1\left(k\right) \\ x_{s2}\left(k+1\right) = 1 + x_{s3}\left(k\right) - a_1 x_{s2}^2\left(k\right) + u_2\left(k\right) \\ x_{s3}\left(k+1\right) = b_1 x_{s2}\left(k\right) + x_{s1}\left(k\right) + u_3\left(k\right) \end{cases} \tag{2.106}$$

$a_1 = 1.07$ et $b_1 = 0.3$, pouvant être représenté par :

$$x_s\left(k+1\right) = A_1 x_s\left(k\right) + f_1\left(x_s\left(k\right)\right) + E_1 + Bu\left(k\right) \tag{2.107}$$

avec :

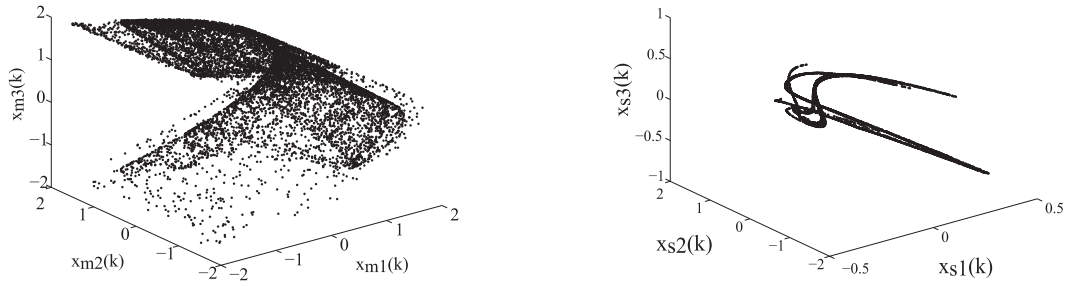
$$A_1(x_s\left(k\right)) = \begin{bmatrix} 0 & -0.3 & 0 \\ 0 & 0 & 1 \\ 1 & 0.3 & 0 \end{bmatrix} \tag{2.108}$$

$$f_1\left(x_s\left(k\right)\right) = \begin{bmatrix} 0 & -1.07x_{s2}^2\left(k\right) & 0 \end{bmatrix}^T \tag{2.109}$$

et :

$$E_1 = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T \tag{2.110}$$

Dans la figure (2.4.11), les évolutions des deux systèmes considérés sont présentées.



(i) Attracteur de type Hénon (Baier-Klein) (ii) Attracteur de type Hénon (Hitzl-Zele)

FIGURE 2.4.11 – Attracteurs des systèmes de troisième ordre de Hénon (Baier-Klein) et Hénon (Hitzl-Zele)

Considérons le système erreur entre le système maître (2.101) et le système esclave (2.106) décrit par :

$$e_i(k) = x_{si}(k) - x_{mi}(k),\ \forall i = 1, 2, 3 \tag{2.111}$$

La figure 2.4.12 présente les évolutions des variables du système erreur, entre (2.101) et (2.106), lorsque la commande est désactivée. Cette figure montre que ce système présente un comportement chaotique.

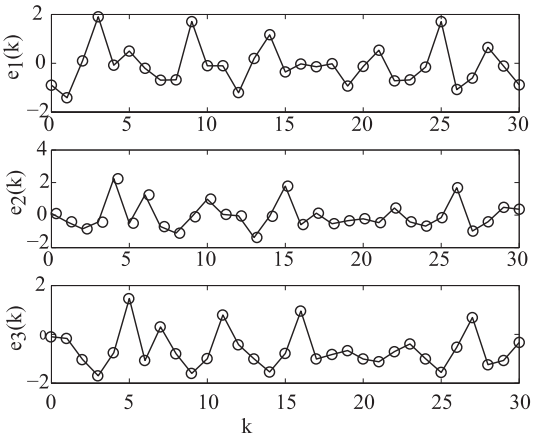


FIGURE 2.4.12 – Dynamiques de l'erreur des systèmes de Hénon (Baier-Klein) et de Hénon (Hitzl-Zele) en l'absence de commande

En appliquant (2.94), la loi de commande $u(k)$ peut être réécrite comme suit :

$$\begin{cases} u_1(k) = 0.3x_{s2}(k) - 0.1x_{s3}(k) + 1.76 - x_{s2}^2(k) - \sum_{j=1}^{3} k_{1j}e_j(k) \\ u_2(k) = x_{s1}(k) - x_{s3}(k) - 1 + 1.07x_{s2}^- \sum_{j=1}^{3} k_{2j}e_j(k) \\ u_3(k) = -x_{s1}(k) + 0.7x_{s2}(k) - \sum_{j=1}^{3} k_{3j}e_j(k) \end{cases} \tag{2.112}$$

Par ce choix de $u(k)$, il vient la possibilité de ramener l'étude de la synchronisation de deux systèmes non identiques de type Hénon (Baier-Klein) et Hénon (Hitzl-Zele) à l'étude de la synchronisation de deux systèmes hyperchaotiques identiques de type Hénon (Baier-Klein).

Dans l'espace d'état, l'erreur peut être reformulée comme suit :

$$e(k+1) = (A + Q(x_m(k), x_s(k)) - BK)\, e(k) \tag{2.113}$$

avec :

$$Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -(x_{s2}(k) + x_{m2}(k)) & -0.1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.114}$$

$$B = I_{3\times 3} \tag{2.115}$$

et :

$$K(.) = \{k_{ij}(.)\} \tag{2.116}$$

Soit la matrice $A_f(.)$:

$$A_f(x(k)) = A + Q(x_m(k), x_s(k)) - BK \tag{2.117}$$

qui peut être ainsi réécrite comme suit :

$$A_f(.) = \begin{bmatrix} -k_{11}(.) & -(k_{12}(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 - k_{13}(.) \\ 1 - k_{21}(.) & -k_{22}(.) & -k_{23}(.) \\ -k_{31}(.) & 1 - k_{32}(.) & -k_{33}(.) \end{bmatrix} \tag{2.118}$$

Le choix des paramètres de correction k_{23} et k_{32} correspondant à :

$$\begin{cases} 1 - k_{32} = 0 \\ k_{23} = 0 \end{cases} \tag{2.119}$$

permet de forcer la matrice caractéristique $A_a(x(k))$ à être sous forme en flèche de Benrejeb, comme suit :

$$A_f(.) = \begin{bmatrix} -k_{11}(.) & -(k_{12}(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 - k_{13}(.) \\ 1 - k_{21}(.) & -k_{22}(.) & 0 \\ -k_{31}(.) & 0 & -k_{33}(.) \end{bmatrix} \tag{2.120}$$

Le système caractérisé par (2.113) est asymptotiquement stable, si les gains $k_{ij}(x(k))$, $i, j = 1, 2, 3$, sont choisis, tels que les contraintes suivantes soient vérifiées :

i. les éléments non linéaires de la matrice caractéristique $A_a(x(k))$ sont isolés dans une seule rangée ;

ii. les éléments diagonaux de la matrice caractéristique $A_a(x(k))$ sont tels que :

$$\begin{cases} 1 - |k_{33}(x(k))| > 0 \\ 1 - |k_{22}(x(k))| > 0 \end{cases} \tag{2.121}$$

iii. Il existe $\varepsilon > 0$, tels que :

$$\begin{cases} 1 - |k_{11}(x(k))| - \frac{|k_{31}(x(k))(0.1+k_{13}(x(k)))|}{1-|k_{33}(x(k))|} \\ -\frac{|(k_{12}(x(k))+x_{s2}(k)+x_{m2}(k))(1-k_{21}(x(k)))|}{1-|k_{22}(x(k))|} \geq \varepsilon \end{cases} \tag{2.122}$$

Ainsi, les gains instantanés $k_{ij}(x(k))$, $\forall i, j = 1, 2, 3$, satisfaisant les inégalités (2.121) et (2.122), tels que :

$$K(x(k)) = \begin{bmatrix} 0.005 & 0.5 - x_{m2}(k) - x_{s2}(k) & 0.1 \\ 0.9 & 0.3 & 0 \\ 0.2 & 1 & 0.8 \end{bmatrix} \tag{2.123}$$

garantissent la synchronisation entre les deux systèmes (2.101) et (2.106), comme le montre les figures 2.4.13 et 2.4.14.

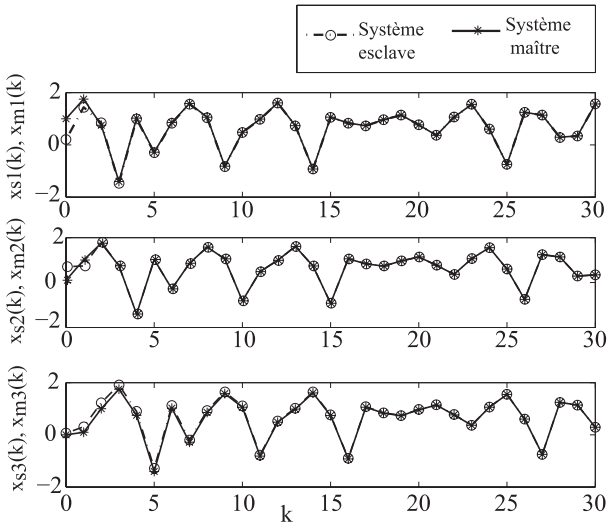


FIGURE 2.4.13 – Evolutions temporelles des variables d'état du système maître (Baier-Klein map) $*$ et du système esclave (Hitzl-Zele map)$\ominus$.

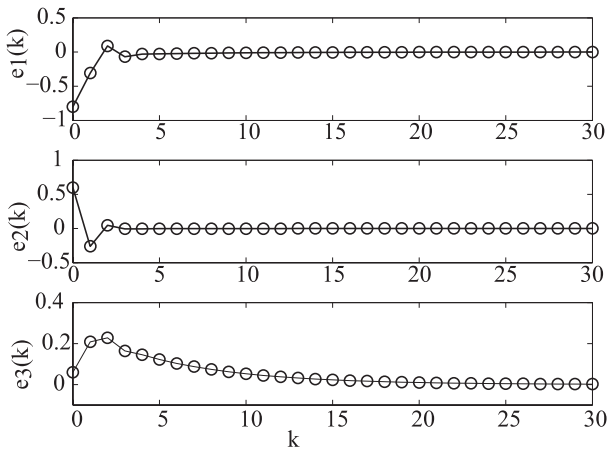
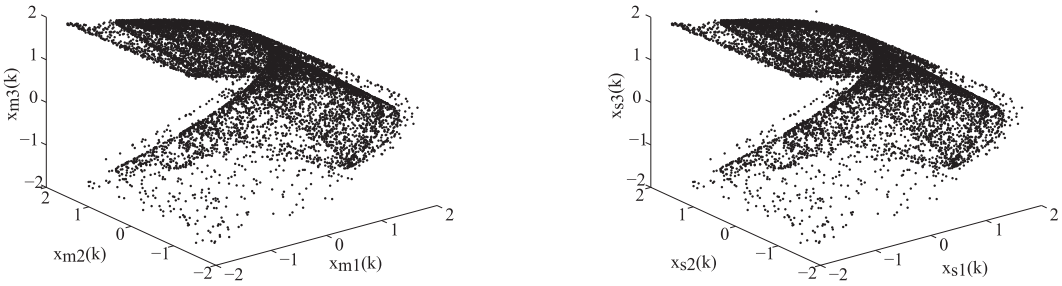


FIGURE 2.4.14 – Dynamiques de l'erreur de deux systèmes hyperchaotiques différents lorsque la commande est activée.

La figure 2.4.15 présente les attracteurs correspondants aux systèmes maître et esclave pour les instants initiaux $x_m(0) = (1, 0.1, 0)$ et $x_s(0) = (0.2, 0.7, 0.06)$, lorsque la commande est activée. Nous pouvons conclure que la commande proposée a conduit à des résultats satisfaisants à savoir la synchronisation des systèmes maître et esclave.



(i) Attracteur du système maître (ii) Attracteur du système esclave

FIGURE 2.4.15 – Attracteurs hyperchaotiques des systèmes maître et esclave

2.4.3.3 Cas de la synchronisation du système de Rössler couplé avec le système de Hénon (Baier-Klein map)

Considérons le système de troisième ordre Baier-Klein [Baier et Klein, 1990, Miller et Grassi, 2001] décrit comme suit :

$$\begin{cases} x_{m1}(k+1) = b - x_{m2}^2(k) - a.x_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \end{cases} \tag{2.124}$$

$a = 0.1$ et $b = 1.76$, qui présente un comportement hyperchaotique comme le montre la figure 2.4.16.
Matriciellement, le système est décrit comme suit :

$$x_m(k+1) = Ax_m(k) + f(x_m(k)) + E \tag{2.125}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.126}$$

$$f(x_m(k)) = \begin{bmatrix} -x_{m2}^2(k) & 0 & 0 \end{bmatrix}^T \tag{2.127}$$

et :

$$E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T \tag{2.128}$$

Considérons, maintenant, le système de troisième ordre de Rössler comme système esclave :

$$\begin{cases} x_{s1}(k+1) = \alpha x_{s1}(k)(1 - x_{s1}(k)) - \beta(x_{s3}(k) + \gamma)(1 - 2x_{s2}(k)) \\ x_{s2}(k+1) = \delta x_{s2}(k)(1 - x_{s2}(k)) + \zeta x_{s3}(k) \\ x_{s3}(k+1) = \eta((x_{s3}(k) + \gamma)(1 - 2x_{s2}(k)) - 1)(1 - \theta x_{s1}(k)) \end{cases} \tag{2.129}$$

$\alpha = 3.8, \beta = 0.05, \gamma = 0.35, \delta = 3.78, \zeta = 0.2, \eta = 0.1, \theta = 1.9$ décrit dans l'espace d'état comme suit :

$$x_s(k+1) = A_1 x_s(k) + f_1(x_s(k)) + E_1 \tag{2.130}$$

avec :

$$A_1 = \begin{bmatrix} 3.8 & 0.035 & -0.05 \\ 0 & 3.78 & 0.2 \\ 0.1235 & -0.07 & 0.1 \end{bmatrix} \tag{2.131}$$

$$E_1 = \begin{bmatrix} -0.0175 & 0 & -0.065 \end{bmatrix}^T \tag{2.132}$$

et :

$$f_1(x_s(k)) = [f_{1_1} \quad f_{1_2} \quad f_{1_3}]^T \tag{2.133}$$

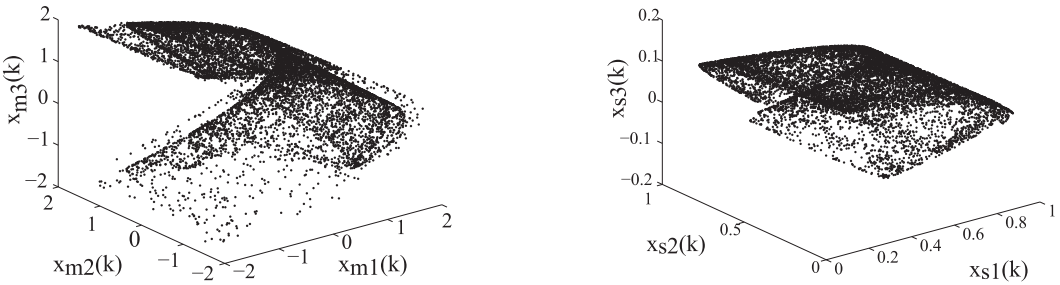
On a :

$f_{1_1} = -3.8x_{s1}^2(k) + 0.1x_{s2}(k)x_{s3}(k)$

$f_{1_2} = -3.78x_{s2}^2(k)$

$f_{1_3} = -0.19(1 - 2x_{s2}(k))x_{s3}(k)x_{s1}(k) + 0.133x_{s2}(k).x_{s1}(k) + 0.2x_{s3}(k).x_{s2}(k)$

La figure (2.4.16) montre que l'attracteur du système maître de Henon (Baier-Klein) et l'attracteur de Rössler esclave ne sont pas synchronisés.



(i) Attracteur de Hénon de type (Baier-Klein) (ii) Attracteur de type Rössler

FIGURE 2.4.16 – Attracteurs hyperchaotiques de troisième ordre de types Baier-Klein et Rössler

L'erreur de synchronisation entre les systèmes (2.101) et (2.106) a la forme suivante :

$$e_i(k) = x_{si}(k) - x_{mi}(k),\ \forall i = 1,2,3 \tag{2.134}$$

En substituant les équations (2.126), (2.128), (2.127), (2.131), (2.132) et (2.133) dans (2.94), $u(k)$ peut être formulée par les relations suivantes :

$$\begin{cases} u_1(k) = -3.8x_{s1}(k)(1 - x_{s1}(k)) - (x_{s2}(k) + 0.035)x_{s2}(k) \\ \qquad - (0.1 - 0.05(1 - 2x_{s2}(k)))x_{s3}(k) + 1.7775 - \sum_{j=1}^{3} k_{1j}e_j(k) \\ u_2(k) = x_{s1}(k) - (3.78(1 - x_{s2}(k)))x_{s2}(k) - 0.2x_{s3}(k) - \sum_{j=1}^{3} k_{2j}e_j(k) \\ u_3(k) = 0.19((x_{s3}(k) + 0.35)(1 - 2x_{s2}(k)) - 1)x_{s1}(k) \\ \qquad +1.07x_{s2}(k) - 0.1(1 - 2x_{s2}(k))x_{s3}(k) + 0.065 - \sum_{j=1}^{3} k_{3j}e_j(k) \end{cases} \tag{2.135}$$

Le choix de $u(k)$ telle que (2.135), réduit l'étude de la synchronisation de systèmes non identiques (les systèmes 3D de type Baier-Klein et 3D de Rössler) à celle de l'étude de la synchronisation de systèmes identiques, à savoir l'étude de la synchronisation de deux systèmes hyperchaotiques Baier-Klein.
La figure 2.4.17 représente les variables d'état du système erreur entre les systèmes (2.124) et (2.129) lorsque la commande est désactivée.

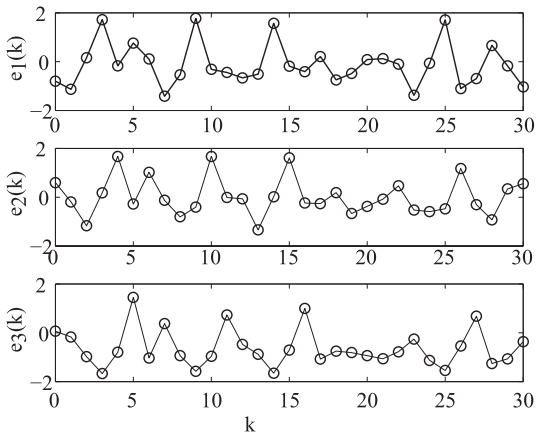


FIGURE 2.4.17 – Dynamiques de l'erreur entre les systèmes hyperchaotiques Rössler et Baier-Klein avec la commande désactivée.

L'erreur de synchronization peut être décrite, dans l'espace d'état, comme suit :

$$e(k+1) = (A + Q(x_m(k), x_s(k)) - BK)e(k) \tag{2.136}$$

telle que :

$$A_f(x(k)) = (A + Q(x_m(k), x_s(k)) - BK) \tag{2.137}$$

avec : A, $Q(x_m(k), x_s(k))$, B et $K(.)$ satisfaisant respectivement (2.126), (2.114), (2.115) et (2.116).
$A_f(x(k))$ peut être alors, réécrite comme suit :

$$A_f(.) = \begin{bmatrix} -k_{11}(.) & -(k_{12}(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 - k_{13}(.) \\ 1 - k_{21}(.) & -k_{22}(.) & 0 \\ -k_{31}(.) & 0 & -k_{33}(.) \end{bmatrix} \tag{2.138}$$

On opère, comme précédemment ; $K(.)$ est choisie comme (2.123), de telle façon que les gains garantissent la synchronisation, entre les systèmes (2.124) et (2.129), comme le montre la figure. 2.4.18. Les dynamiques du système erreur entre les systèmes maître et esclave sont présentées figure. 2.4.19.

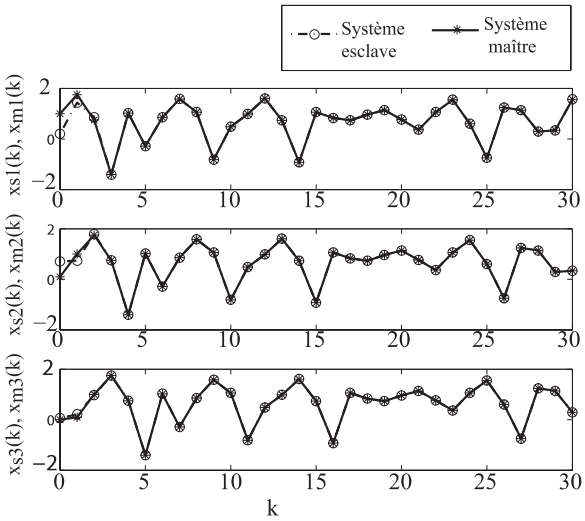


FIGURE 2.4.18 – Evolutions temporelles des variables d'état du système maître (Baier-Klein) $*$ et du système esclave (Rössler) $\circ$.

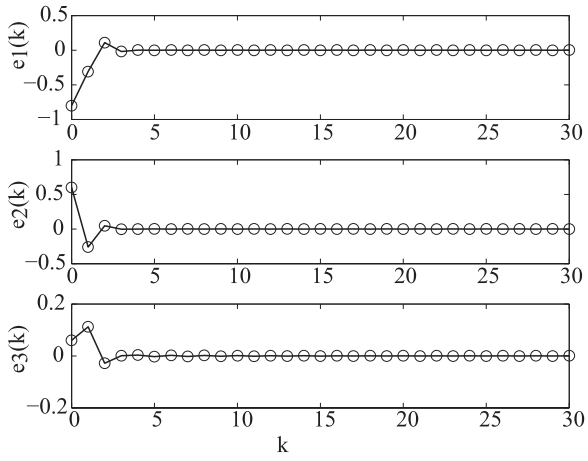
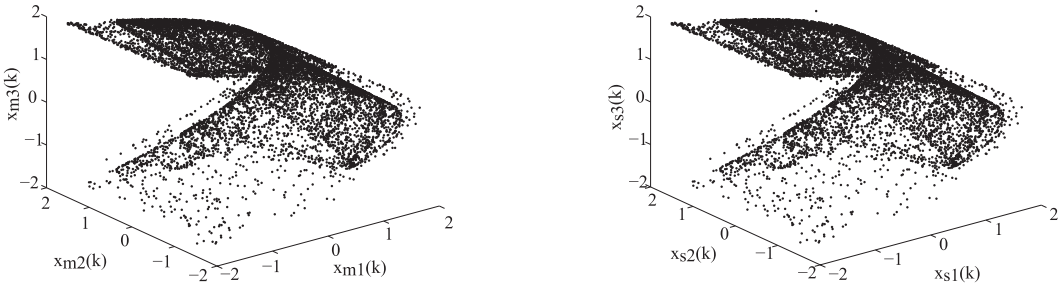


FIGURE 2.4.19 – Dynamiques de l'erreur de deux systèmes non identiques lorsque la commande par retour d'état est activée.

Des figures 2.4.15 et 2.4.20, nous pouvons conclure que la synchronisation entre deux systèmes hyperchaotiques à temps discret est assurée par la loi de commande proposée. On note que le système Hénon (Hitzl-Zele) est forcé de suivre l'évolution du système Hénon (Baier-Klein) ; il en est de même pour le système hyperchaotique de Rössler qui, à son tour, est amené à suivre le comportement du système (Baier-Klein).



(i) Attracteur du système maître (ii) Attracteur du système esclave

FIGURE 2.4.20 – Attracteurs hyperchaotiques des systèmes maître et esclave une fois la loi de commande activée.

2.5 Application à la synchronisation des systèmes chaotiques à temps discret avec un observateur

Le problème de la synchronisation peut être formulé comme un problème d'observation. En effet, on n'a pas toujours accès à toutes les variables d'état du système maître, surtout dans le cas d'une synchronisation utilisée dans les techniques de communication. Ces techniques de communication, utilisant l'approche de synchronisation, font l'objet du chapitre suivant. Nous supposons que nous n'avons accès qu'à la sortie du système maître. Le système esclave est à synchroniser avec la dynamique du système maître en n'ayant donc connaissance que de sa sortie. Il s'agit d'un problème de synthèse d'observateur [Morgül et Solak, 1996, Nijmeijer et Mareels., 1997, Millerioux, 1997, Cherrier *et al.*, 2006, Cherrier *et al.*, 2005, H.Dimassi *et al.*, 2010, H.Dimassi *et al.*, 2011].

2.5.1 Conditions de synchronisation par couplage unidirectionnel utilisant l'observateur de Luenberger. Idée de base

Cette partie a pour but de construire et de synthétiser un observateur pour une classe de systèmes non linéaires satisfaisant les systèmes de type Lur'e Postnikov.
Pour cela, on considère le système maître suivant :

$$\begin{cases} x_m(k+1) = Ax_m(k) + f(x_m(k)) \\ y_m(k) = Cx_m(k) \end{cases} \tag{2.139}$$

avec : $y_m(k) \in R^l$,
Pour le système esclave, nous choisissons la forme standard d'un observateur non linéaire correspondant au système (2.140) :

$$x_s(k+1) = Ax_s(k) + f(x_s(k)) + L(y_m(k) - Cx_s(k)) \tag{2.140}$$

$x_m(k) \in R^n$, $x_s(k) \in R^n$ étant des variables d'état respectives des systèmes maître et esclave, $A \in R^{n\times n}$ une matrice constante et $f(x(k))$ une fonction non linéaire à temps discret.
Pour la classe des systèmes étudiés, nous considérons que nous avons la condition de factorisation suivante :

$$f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))(x_m(k) - x_s(k)) \tag{2.141}$$

avec : $Q(.) = \{q_{ij}(.)\}$. Il vient alors le vecteur erreur $e(k+1) = x_s(k+1) - x_m(k+1)$. D'après (2.139) et (2.140), il vient la nouvelle formulation de l'erreur :

$$e(k+1) = (A - LC)\, e(k) + f(x_m(k)) - f(x_s(k)) \tag{2.142}$$

qui peut être reformulée comme suit, en utilisant (2.141) :

$$e(k+1) = (A - LC + Q(x_m(k), x_s(k)))\, e(k) \tag{2.143}$$

avec :

$$A_f(x_m(k), x_s(k)) = (A - LC + Q(x_m(k), x_s(k))) \tag{2.144}$$

Remarque 2.1. *La plupart des systèmes chaotiques, y compris les systèmes non linéaires de type Lur'e Postnikov et les systèmes non linéaires Lipschitz, peuvent être décrits par* (2.139) *et* (2.141). *Dans la section suivante, un exemple de système satisfaisant* (2.139) *va être utilisé dans le but de synthétiser un observateur afin d'obtenir la synchronisation de deux systèmes hyperchaotiques couplés [Jiang et al., 2003].*

Pour que le système (2.139) tende vers zéro quand $k \to +\infty$, une solution est d'appliquer le critère pratique de stabilité de Borne et Gentina [Gentina *et al.*, 1972, Borne *et al.*, 1976] au système écart (2.143) pour l'étude de la stabilité associée à la représentation en flèche mince de la matrice caractéristique.

Théorème 2.5. *Le processus défini par* (2.143) *est stabilisable par la commande définie par l'observateur* (2.140), *si la matrice caractéristique* $A_f(x(k), k) = \{a_{f_{ij}}(.)\}$ (2.144) *est sous forme en flèche mince de type 2* (2.15), *avec* $a_{f_{ij}}(.) = q_{ij}(.) + a_{ij} + \left(\sum_{r=1}^{l} l_{ir}(.)\, c_{rj}(.)\right)$ $\forall i, j = 1, \ldots, n-1$, *et est telle que :*

i. les éléments non linéaires sont isolés dans une seule rangée de la matrice caractéristique instantanée $A_f(.)$;

ii. les éléments diagonaux, $a_{f_{ii}}(.)$, *de la matrice caractéristique* $A_f(.)$ *sont, tels que :*

$$1 - |a_{f_{ii}}(.)| > 0,\ \forall i = 2, \ldots, n \tag{2.145}$$

iii. il existe $\varepsilon > 0$, *tel que :*

$$1 - |a_{f_{11}}(.)| - \sum_{i=2}^{n} \left(\begin{array}{l} |a_{f_{i1}}(.)\, a_{f_{1i}}(.)| \\ \times (1 - |a_{f_{ii}}(.)|)^{-1} \end{array} \right) \geq \varepsilon \tag{2.146}$$

2.5.2 Cas de la synchronisation de deux systèmes hyperchaotiques de Hénon (Baier-Klein)

Dans cette partie, l'objectif est de synchroniser deux systèmes identiques à travers un observateur d'ordre plein de Luenberger. Le système maître discret considéré est le système hyperchaotqiue de Hénon (Baier-Klein).
Soit le système maître représenté par :

$$\begin{cases} x_{m1}(k+1) = 1.76 - x_{m2}^2(k) - 0.1x_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \\ y_{m1}(k) = c_{11}(.)\, x_{m1}(k) + c_{12}(.)\, x_{m2}(k) + c_{13}(.)\, x_{m3}(k) \\ y_{m2}(k) = c_{12}(.)\, x_{m1}(k) + c_{22}(.)\, x_{m2}(k) + c_{23}(.)\, x_{m3}(k) \end{cases} \tag{2.147}$$

que nous associons au système esclave suivant :

$$\begin{cases} x_{s1}(k+1) = 1.76 - x_{s2}^2(k) - 0.1x_{s3}(k) + l_{11}(y_{m1}(k) - y_{s1}(k)) + l_{12}(y_{m2}(k) - y_{s2}(k)) \\ x_{s2}(k+1) = x_{s1}(k) + l_{21}(y_{m1}(k) - y_{s1}(k)) + l_{22}(y_{m2}(k) - y_{s2}(k)) \\ x_{s3}(k+1) = x_{s2}(k) + l_{31}(y_{m1}(k) - y_{s1}(k)) + l_{32}(y_{m2}(k) - y_{s2}(k)) \\ y_{s1}(k) = c_{11}(.)\, x_{s1}(k) + c_{12}(.)\, x_{s2}(k) + c_{13}(.)\, x_{s3}(k) \\ y_{s2}(k) = c_{12}(.)\, x_{s1}(k) + c_{22}(.)\, x_{s2}(k) + c_{23}(.)\, x_{s3}(k) \end{cases} \tag{2.148}$$

Remarque 2.2. ***Propriété de bornitude*** *Pour le système hyperchaotique de Hénon (Baier-Klein) [Grassi et Miller, 2002, Baier et Klein, 1990] et pour les conditions initiales $x_m(0) = (1, 0.1, 0)$, on peut comme le montre la figure 1.8 conclure que les variables d'état $x_{mi}(k)$ sont bornées [Fradkov et Pogromsky, 1998] : $|x_{mi}| < 2\ \forall i = 1, 2, 3$.*

– La description du système maître peut être reformulée dans l'espace d'état par [Baier et Klein, 1990, Grassi et Miller, 2002] :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E \\ y_m(k) &= Cx_m(k) \end{aligned} \tag{2.149}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.150}$$

$$f(x_m(k)) = [-x_{m2}^2(k) \quad 0 \quad 0]^T \tag{2.151}$$

et :

$$E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T \tag{2.152}$$

– le système esclave est considéré être formulé comme suit :

$$\begin{aligned} x_s(k+1) &= Ax_s(k) + f(x_s(k)) + E + L(y_m(k) - y_s(k)) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{2.153}$$

avec :

$$L = \begin{bmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \\ l_{31} & l_{32} \end{bmatrix} \tag{2.154}$$

$$C = \begin{bmatrix} c_{11} & c_{12} & 1 \\ 0 & 0 & 1 \end{bmatrix} \tag{2.155}$$

les l_{ij} étant les gains de l'observateur, et le vecteur non linéaire est formulé comme suit :

$$f(x_s(k)) = [-x_{s2}^2(k) \quad 0 \quad 0]^T \tag{2.156}$$

Soit le système erreur $e(k)$, entre les systèmes (2.147) et (2.148), suivant :

$$e_i(k) = x_{mi}(k) - x_{si}(k), \ \forall i = 1, 2, 3 \tag{2.157}$$

Pour ce type de système, l'expression $f(x_m(k)) - f(x_s(k))$ peut être factorisée telle que : $f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))\, e(k)$, avec :

$$Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -x_{m2}(k) - x_{s2}(k) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.158}$$

D'après (2.144), il vient la matrice suivante pour le système erreur :

$$A_c(x_m(k), x_s(k)) = \begin{bmatrix} -(c_{11}l_{11}) & -(x_{m2}(k) + x_{s2}(k)) - (c_{12}l_{11}) & -0.1 - (l_{11} + l_{12}) \\ 1 - (c_{11}l_{21}) & -(c_{12}l_{21}) & -(l_{21} + l_{22}) \\ -(c_{11}l_{31}) & 1 - (c_{12}l_{31}) & -(l_{31} + l_{32}) \end{bmatrix} \tag{2.159}$$

En utilisant la norme vectorielle : $p(z(k)) = \begin{bmatrix} |z_1(k)| & \dots & |z_n(k)| \end{bmatrix}^T$, $z(k) = \begin{bmatrix} z_1(k) & \dots & z_n(k) \end{bmatrix}^T$, il vient la matrice majorante $M_k(A_c(x_m(k), x_s(k)))$ d'éléments $m_{ij}(.)$ définis par :

$$m_{k_{ij}}(x(k), k) = \left| a_{f_{ij}}(x(k), k) \right| \forall i, j = 1, \dots, n \tag{2.160}$$

On a :

$$M_k\left(A_c\left(x_m\left(k\right),x_s\left(k\right)\right)\right)=\begin{bmatrix}|c_{11}l_{11}| & |x_{m2}\left(k\right)+x_{s2}\left(k\right)+c_{12}l_{11}| & |0.1+(l_{11}+l_{12})|\\ |1-c_{11}l_{21}| & |c_{12}l_{21}| & |l_{21}+l_{22}|\\ |c_{11}l_{31}| & |1-c_{12}l_{31}| & |l_{31}+l_{32}|\end{bmatrix} \tag{2.161}$$

Le choix des paramètres constants l_{21}, l_{21}, l_{31} et c_{12} vérifient les relations suivantes :

$$\begin{cases} l_{21}+l_{22}=0\\ (1-c_{12}l_{31}=0)\end{cases} \quad ou\ encore\ :\ \begin{cases} l_{21}=-l_{22}\\ l_{31}=\frac{1}{c_{12}}\end{cases} \tag{2.162}$$

force la matrice caractéristique (2.161) à être une matrice de forme en flèche, comme suit :

$$M\left(A_f\left(x_m\left(k\right),x_s\left(k\right)\right)\right)=\begin{bmatrix}|c_{11}l_{11}| & |x_{m2}\left(k\right)+x_{s2}\left(k\right)+c_{12}l_{11}| & |0.1+(l_{11}+l_{12})|\\ |1-c_{11}l_{21}| & |c_{12}l_{21}| & 0\\ \left|\frac{c_{11}}{c_{12}}\right| & 0 & \left|\frac{1}{c_{12}}+l_{32}\right|\end{bmatrix} \tag{2.163}$$

Comme il est noté dans la Remarque 1, les variables d'état du maître et de l'esclave sont bornées telles que : $\mid x_{m2} \mid< 2$ et $\mid x_{s2} \mid< 2$; il vient :
$\mid x_{m2}+x_{s2}+l_{21}c_{11} \mid< 4+ \mid l_1c_2 \mid$
En utilisant le théorème précédent, les conditions de synchronisation (2.145) and (2.146) deviennent :

i.

$$\begin{cases} 1-\left|\frac{1}{c_{12}}+l_{32}\right|>0\\ 1-|c_{12}l_{21}|>0\end{cases} \tag{2.164}$$

ii.

$$1-|c_{11}l_{11}|-\frac{|x_{m2}\left(k\right)+x_{s2}\left(k\right)+c_{12}l_{11}|\,|1-c_{11}l_{21}|}{1-|c_{12}l_{21}|}-\frac{\left|\frac{c_{11}}{c_{12}}\right|\,|0.1+(l_{11}+l_{12})|}{1-\left|\frac{1}{c_{12}}+l_{32}\right|}>0 \tag{2.165}$$

En utilisant la propriété de bornitude, l'équation (2.165) devient :

$$1-|c_{11}l_{11}|-\frac{(4+|c_{12}l_{11}|)\,|1-c_{11}l_{21}|}{1-|c_{12}l_{21}|}-\frac{\left|\frac{c_{11}}{c_{12}}\right|\,|0.1+(l_{11}+l_{12})|}{1-\left|\frac{1}{c_{12}}+l_{32}\right|}>0 \tag{2.166}$$

d'où nos choix possibles de L et C suivants :

$$L = \begin{bmatrix} -0.20 & -0.1 \\ 0.55 & -0.55 \\ \frac{1}{0.9} & -1 \end{bmatrix} \tag{2.167}$$

$$C = \begin{bmatrix} 1.73 & 0.9 & 1 \\ 0 & 0 & 1 \end{bmatrix} \tag{2.168}$$

Les états initiaux des systèmes maître et esclave sont
$(x_m(0), x_s(0)) = ((1, 0.1, 0), (-0.5, 0, 0.3))$. La figure. 2.5.21 et figure. 2.5.22 illustrent l'efficacité de la méthode proposée, compte tenu qu'en particulier $e_1(k)$, $e_2(k)$ et $e_3(k)$ convergent vers zéro.

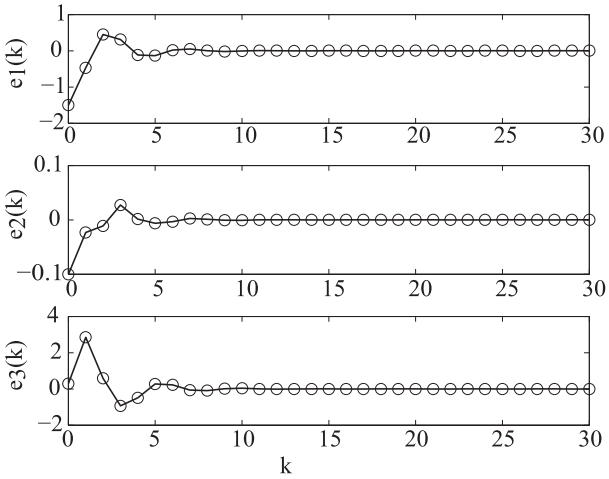


FIGURE 2.5.21 – Dynamiques de l'erreur du système de troisième ordre Hénon généralisé lorsque la commande est activée.

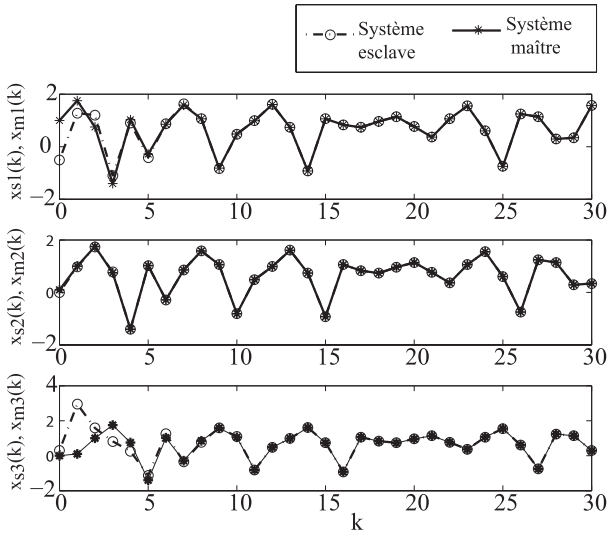


FIGURE 2.5.22 – Réponses temporelles des variables d'état des systèmes maître et esclave.

2.6 Conclusion

Dans ce chapitre, nous avons proposé plusieurs schémas de synchronisation. Le choix des systèmes maîtres s'est fixé sur une structure particulière de systèmes hyperchaotiques, structure qui a été exploitée pour concevoir le système esclave correspondant, sous la forme de retour d'état et d'observateurs. Des conditions suffisantes de synchronisation ont été établies, principalement, en utilisant le critère pratique de Borne et Gentina pour l'étude de la stabilité et la représentation en flèche de Benrejeb pour la description des systèmes étudiés. La première approche de synchronisation, basée sur le contrôle par retour d'état, nécessite la mesure de toutes les variables d'état du système. Lorsque des informations partielles sur ces variables sont disponibles, c'est à dire que seulement les variables de la sortie du système maître sont transmises au système esclave, l'approche de la synchronisation par observateur s'est avéré nécessaire. On peut noter, toutefois, que les conditions suffisantes, établies dans ce chapitre et vérifiées dans ce cas grace à l'estimation de l'état des systèmes chaotiques choisis comme système maître, sont performantes. Cette capacité de synchronisation va être appliquée aux systèmes de communication et testée en présence de bruit, dans le chapitre suivant.

Chapitre 3

Approches de synchronisation proposées pour le cryptage chaotique à temps discret

3.1 Introduction

Dans ce chapitre, nous nous intéressons à la reconstruction d'entrées inconnues qui seront désignées, par la suite, par le terme ″signal d'informations″. En ce qui concerne le contexte des communications sécurisées, nous avons opté pour l'application des techniques de synchronisation qui ont été détaillées au chapitre précédent. Dans un premier temps, nous présentons les systèmes de communication sécurisée utilisant les systèmes chaotiques exploitant la synchronisation à base d'observateurs. Dans un deuxième temps, nous proposons un examen des avantages et des inconvénients de ces systèmes. Nous retiendrons deux types de systèmes de communication dont l'efficacité est testée, ci-après, sur des simulations variées. A la fin de ce chapitre, nous étudions l'impact de la présence de bruits de transmission sur la restauration des messages.

3.2 Méthode proposée - Idée de base

La découverte réalisée par Pecora et Carroll en 1990 [Pecora et Carroll, 1990] a ouvert la voie à de nombreuses applications, telles que l'utilisation du chaos dans des systèmes de communication. En effet, ils ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser, s'ils sont couplés

sous certaines conditions. Le développement des systèmes de communication utilisant le chaos a été surtout utilisé pour des systèmes analogiques, visant le cryptage et la reconstruction simultanés d'un signal d'informations ; ce n'est pas encore le cas pour les systèmes digitaux.

3.3 Cryptage usuel et chiffrement basés sur le chaos

3.3.1 Cryptage standard

La cryptographie standard consiste en l'étude de techniques mathématiques liées à la sécurité de l'information qui consiste en l'élaboration de techniques de cryptage et décryptage. L'opération de cryptage consiste à transformer un message d'informations afin d'empêcher à un intrus de récupérer l'information alors que le décryptage est un procédé inverse dont l'unique objectif est de récupérer l'information côté récepteur. Un cryptosystème est l'ensemble de cryptage et de décryptage. Parmi une grande variété de mécanismes de cryptage, nous distinguons les deux algorithmes principaux : le cryptage à clé publique et le cryptage à clé secrète.

3.3.1.1 Cryptage à clé publique ou asymétrique

Le chiffrement à clé publique, ou chiffrement asymétrique, a été proposé par Diffie et Hellman en 1976. Dans une telle technique, la clé de cryptage est différente de celle utilisée pour le décryptage. Quiconque peut utiliser la clé de cryptage, ou clé publique, pour crypter un message. Cependant, seul, celui qui a accès à la clé de décryptage ou clé privée, peut déchiffrer le message crypté. Prenons l'exemple suivant : soit un émetteur 1 et un récepteur 1 qui veulent communiquer de façon sécurisée. Le récepteur 1 choisit une paire de clés de cryptage et de décryptage K_c et K_d. Ce récepteur 1 envoie la clé publique K_c à l'émetteur 1 à travers un canal qui n'est pas forcément sécurisé. En ayant cette clé, l'émetteur 1 transforme le message d'informations $m\,(k)$ en un message crypté grâce à l'équation $V\,(k) = v_c(K_c, m\,(k))$ et envoie ce message ainsi crypté au côté récepteur. De son côté, le récepteur 1 récupère l'information $m_r\,(k)$ via l'algorithme de décryptage et la clé privée connue uniquement par ce récepteur tel que : $m_r\,(k) = v_d(K_d, V\,(k))$.

3.3.1.2 Cryptage symétrique

Contrairement au cryptage à clé asymétrique ou publique, cette technique est aussi apellée cryptage à clé secrète. Généralement les clés de cryptage et de décryptage sont identiques. L'émetteur et le récepteur doivent se mettre d'accord sur une clé gardée secrète, car la sécurité d'une telle technique repose sur cette clé.

3.3.2 Cryptage basé sur le chaos

Le principe d'un système de communication, utilisant le chaos, se base sur le fait de mélanger l'information, notée $m(k)$, avec un système chaotique dans la partie émettrice, décrite généralement par une représentation d'état de vecteur état $x_m(k)$. L'émetteur génère un signal de sortie $y_m(k)$ qui est transmis au récepteur par l'intermédiaire d'un canal. Le rôle du récepteur consiste à extraire l'information originale du signal à partir du signal reçu $y_m(k)$. La récupération de l'information est basée sur le concept de synchronisation des variables d'état du système maître $x_m(k)$ avec celles du système esclave $x_s(k)$, de telle sorte que l'on ait la relation : $\lim_{k\to+\infty} \|x_m(k) - x_s(k)\| = 0, \quad \forall x_s(0), \ x_m(0)$. Différents schémas d'injection de l'information dans un système chaotique sont proposés dans ce chapitre. On peut citer le masquage additif [Cuomo *et al.*, 1993], la modulation chaotique [Dedieu *et al.*, 1993a], la modulation paramétrique [Parlitz *et al.*, 1992], l'approche par inclusion [Millerioux et Daafouz., 2004], l'approche par cryptage mixte [Yang et Chua, 1997] et l'approche utilisant deux voies de transmission [Millérioux et Mira, 1998].

3.3.2.1 Masquage par addition

Le principe de ce masquage additif [Cuomo *et al.*, 1993, Morgül et Feki, 1999] consiste à effectuer une addition entre le signal de sortie chaotique de l'émetteur, noté $y_m(k)$, et l'information originale $m(k)$.
Considérons les représentations suivantes du système maître correspondant à l'émetteur :

$$\begin{cases} x_m(k+1) = f(x_m(k)) \\ y_m(k) = h(x_m(k)) + m(k) \end{cases} \tag{3.1}$$

et du système esclave correspondant au récepteur :

$$\begin{cases} x_s(k+1) = f(x_s(k)) \\ y_s(k) = h(x_s(k)) \end{cases} \tag{3.2}$$

où $x_m(k) \in R^n$ est le vecteur d'état de l'émetteur, $x_s(k) \in R^n$ celui du récepteur, $y_m(k)$ et $y_s(k)$ représentant respectivement la sortie de l'émetteur et celle du récepteur, généralement choisies appartenant à R et $m(k) \in R$ l'information à sécuriser. Cette technique est illustrée dans la figure (3.3.1).

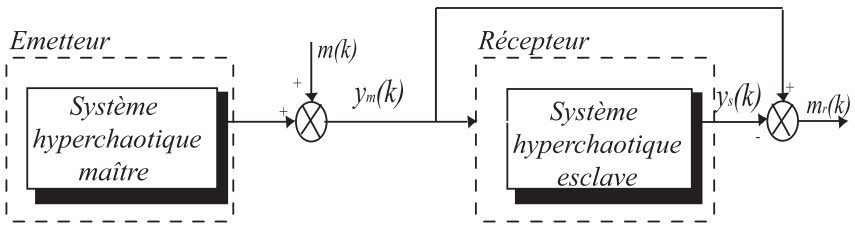


FIGURE 3.3.1 – Masquage additif.

La récupération de l'information exige la synchronisation du système maître et du système esclave correspondant respectivement à l'émetteur et au récepteur. Ainsi, l'information peut être reconstruite en soustrayant la sortie du récepteur à celle de l'émetteur, comme suit :

$$m_r(k) = y_m(k) - y_s(k) \tag{3.3}$$

Le principal avantage de la méthode du masquage additif réside dans la simplicité du cryptage. Il est impératif que l'amplitude de l'information originale soit significativement plus petite que celle du signal chaotique, afin de ne pas perturber l'établissement de la synchronisation au niveau du récepteur et d'assurer la confidentialité de la transmission.

3.3.2.2 Modulation chaotique

Cette technique [Dedieu *et al.*, 1993a], appelée aussi cryptage par commutation, est utilisée pour le cas de signaux numériques. Dans cette technique de communication, l'information est utilisée pour commuter entre deux attracteurs chaotiques de même structure et de paramètres différents. En effet, du côté émetteur, elle consiste à faire correspondre, à chaque symbole $m(k) = m^i$ de l'information appartenant à un ensemble fini $\{m(1), \ldots, m(N)\}$, un signal $y_m^i(k)$ issu d'un système chaotique décrit par :

$$\begin{cases} x_m^i(k+1) = f_\theta^{i(m(k))}(x_m(k)) \\ y_m^i(k) = h_\theta^{i(m(k))}(x_m(k)) \end{cases} \tag{3.4}$$

$i \in \{1, \ldots, N\}$, où $x_m(k) \in R^n$ est le vecteur d'état et $y_m^i(k) \in R$ la sortie côté émetteur. Le cas le plus simple correspond à un message binaire à transmettre. Ainsi, l'émetteur (3.4)

est constitué de deux systèmes chaotiques correspondant respectivement à l'information $m^1 = 0$ et à l'information $m^2 = 1$. La figure (3.3.2) illustre ce principe.

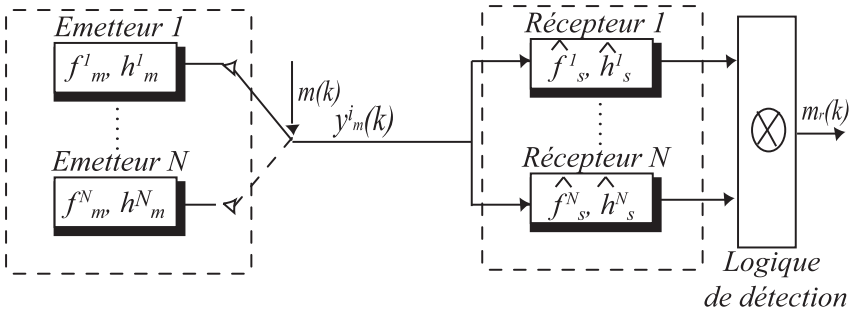


FIGURE 3.3.2 – Modulation chaotique

A la réception, le signal reçu est utilisé pour produire un système chaotique identique à celui de l'émetteur. Ainsi, le récepteur doit être composé, à son tour, du même nombre de systèmes que l'émetteur et est décrit par :

$$\begin{cases} x_s(k+1) = \hat{f}_{\hat{\theta}}^{i(m(k))}(x_s(k)) \\ y_s^{i(m(k))}(k) = \hat{h}_{\hat{\theta}}^{i(m(k))}(x_s(k)) \end{cases} \tag{3.5}$$

Côté émetteur, on a un seul signal $y_m^i(k)$ qui peut être la sortie de l'émetteur 1 ou celle de l'émetteur 2 selon le message $m(k)$ qui prend la valeur 1 ou 0 ; par contre, côté récepteur, on a deux sorties à savoir $y_s^1(k)$ et $y_s^1(k)$. Cette méthode a l'avantage d'être robuste au bruit de transmission. En effet, au niveau du récepteur, on détermine la valeur exacte du message :

- soit en évaluant l'erreur de synchronisation au niveau des deux copies ;
- soit par corrélation entre le signal $y_m^i(k)$ reçu et les signaux $y_s^1(k)$ et $y_s^2(k)$.

Dans le premier cas, si l'information $m(k)$ prend la valeur 0 correspondant à l'émetteur 1, alors le récepteur 1 se synchronise et le récepteur 2 ne se synchronise pas. De ce fait, l'erreur de synchronisation $e_1(k) = y_s^1(k) - y_m(k)$ va tendre vers 0, tandis que l'erreur $e_2(k) = y_s^2(k) - y_m(k)$ sera d'amplitude non nulle. Le processus est symétrique lorsque l'information prend la valeur 1.

Dans le deuxième cas, il s'agit de déterminer le système chaotique généré par les deux émetteurs qui "ressemble" le plus au signal reçu. La corrélation minimise certainement l'influence du bruit sur l'erreur de synchronisation. Cependant, le taux de transmission du cryptage par commutation est assez bas. En effet, un signal binaire contient moins d'informations qu'un signal analogique, et le temps nécessaire à l'établissement de la synchronisation est perdu à chaque fois que le message change de valeur. Il est à noter aussi,

que la sécurité n'est plus garantie si les deux ensembles de paramètres, correspondant à l'émetteur 1 et l'émetteur 2, sont trop différents. Il résulte de cette différence qu'on peut constater les changements de système chaotique émetteur au niveau du signal transmis.

3.3.2.3 Modulation paramétrique

La modulation paramétrique est une technique qui permet de moduler un ou plusieurs paramètres du système chaotique par l'information à transmettre $m(k)$ [Yang et Chua, 1996]. Ainsi, il en résulte une multiplication entre le (les) paramètre(s) du système chaotique et l'information. Le cas le plus simple correspond à deux informations binaires [Parlitz *et al.*, 1992, Cruz et Nijmeijer, 2000], "1" et "0", codées chacune par des systèmes chaotiques différents.
L'émetteur est décrit par :

$$\begin{cases} x_m(k+1) = f(x_m(k), \theta(k)) \\ y_m(k) = h(x_m(k)) \end{cases} \tag{3.6}$$

Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma synoptique de la technique de modulation paramétrique est présenté à la figure (3.3.3).

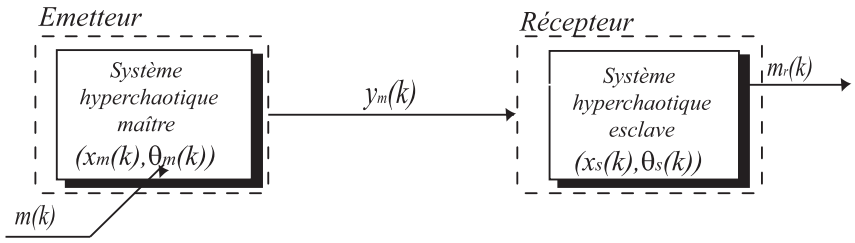


FIGURE 3.3.3 – Modulation paramétrique

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur. Il résulte de cette différence que le signal transmis sera plus complexe qu'un autre signal chaotique. Cependant, il faut attacher de l'importance à la façon d'insérer l'information, plus précisément, à la fonction de modulation des paramètres qui ne doit en aucun cas supprimer le caractère chaotique du signal transmis au côté récepteur.

3.3.2.4 Chiffrement par inclusion

Cette technique de chiffrement consiste à injecter le signal information dans un système chaotique jouant le rôle d'émetteur, qui admet la représentation d'état suivante :

$$\begin{cases} x_m(k+1) = f_\theta(x_m(k), m(k)) \\ y_m(k) = h_\theta(x_m(k), m(k)) \end{cases} \tag{3.7}$$

où $x_m(k) \in R^n$ représente le vecteur d'état du système maître, $y_m(k) \in R$ la sortie, $m(k) \in R$ l'information à masquer, $\theta = \begin{bmatrix} \theta_1 & \dots & \theta_l \end{bmatrix} \in R^l$ le vecteur des paramètres constants du système chaotique.
Le récepteur a pour représentation d'état :

$$\begin{cases} x_s(k+1) = \hat{f}_{\hat{\theta}}(x_s(k), y_m(k)) \\ m_r(k) = d(x_s(k), y_m(k)) \end{cases} \tag{3.8}$$

$m_r(k)$ étant le message récupéré dans le côté récepteur. La restauration de l'information se fait par deux techniques, reposant :

- soit sur les observateurs à entrées inconnues ;
- soit sur l'inversion du système émetteur.

Observateurs à entrées inconnues [Millerioux et Daafouz., 2004] L'objectif est de reconstruire l'état $x_m(k)$ du système maître et également l'entrée inconnue $m(k)$ représentant l'information. Différentes techniques de synthèse d'observateurs à entrées inconnues peuvent être utilisées à des fins de décryptage. Le schéma de la figure (3.3.4) illustre une technique de cryptage par inclusion utilisant les observateurs à entrées inconnues.

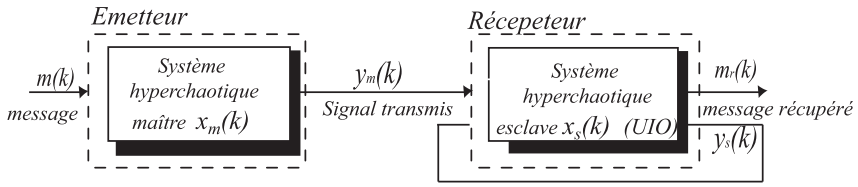


FIGURE 3.3.4 – Cryptage par inclusion utilisant la technique de récupération d'informations par observateurs à entrées inconnues (UIO, Unknown Input Observer)

Décryptage par inversion [Feldmann *et al.*, 1996] Le récepteur du schéma de communication est conçu en inversant le modèle de l'émetteur.

Définition 3.1. ***Système inversé***

Considérons deux systèmes, Γ_1 *et* Γ_2*. On peut dire que le système* Γ_2 *est un système inverse de* Γ_1 *si les conditions suivantes sont satisfaites :*

i. les ensembles Ω_1 *et* Ω_2 *des entrées admissibles, respectivement, de* Γ_1 *et* Γ_2 *coincident avec l'ensemble des sorties de* Γ_2 *et* Γ_1 *;*

ii. pour tout signal $m(k) \in \Omega_1$ *et toute condition initiale du système* Γ_1*, il existe une condition initiale du système* Γ_2*, telle que pour tout* $k > 0$*,* $m_r(k) = m(k)$ *;*

iii. la condition précédente (ii) est satisfaite si les rôles de Γ_1 *et* Γ_2 *sont inversés.*

La figure (3.3.5) illustre le principe général de l'approche de cryptage par inclusion utilisant la technique de récupération de l'information par inversion telle que :

$$\begin{aligned} y_m(k) &= h_\theta(x_m(k), m(k)) \\ m_r(k) &= h_\theta^{-1}(x_s(k), y_m(k)) \end{aligned} \tag{3.9}$$

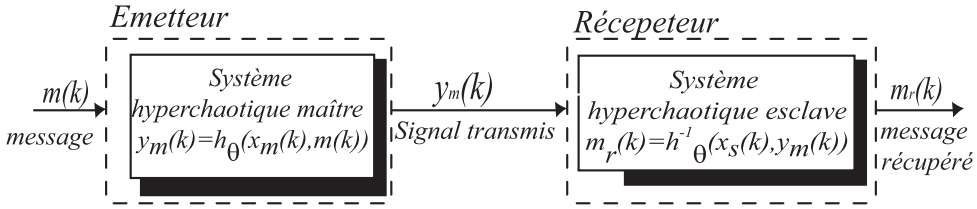


FIGURE 3.3.5 – Cryptage par inclusion utilisant la technique de récupération d'informations par inversion.

3.3.2.5 Cryptage mixte

Yang a proposé une nouvelle technique de sécurisation de l'information qui regroupe les principes de la cryptographie standard et la synchronisation de systèmes chaotiques [Yang et Chua, 1997, Yang, 2004]. Dans la partie émettrice, le message $m(k) \in R$ contenant l'information est crypté via une clé secrète $K_c(k)$. Cette clé est le résultat d'une combinaison des variables d'état du système chaotique ou hyperchaotique maître. Le signal ainsi crypté $V(k)$ est injecté dans la dynamique chaotique du système maître, le rendant plus complexe. Seule la sortie $y_m(k) \in R$ du système maître est transmise. Dans la partie

réceptrice, la clé secrète $K_d(k)$ peut alors être reconstruite en utilisant les techniques de synchronisation étudiées dans le chapitre précédent. Cette clé peut finalement décoder le message.
Le principe général de cette technique de sécurisation de l'information est illustré par la figure (3.3.6). Grâce à la complexité du processus de cryptage, cette nouvelle génération de cryptosystèmes s'est révélée jusqu'ici plus robuste aux attaques classiques.

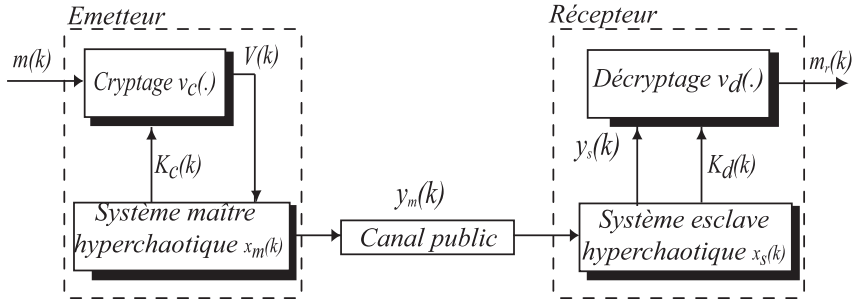


FIGURE 3.3.6 – Cryptage mixte

3.3.2.6 Cryptage à deux voies de transmission

Dans la technique de cryptage à deux voies de transmission, l'émetteur envoie deux signaux au récepteur à travers deux voies de transmission : la première voie est utilisée pour transmettre le signal de sortie $y_m(k)$ d'un système hyperchaotique maître dont l'unique objectif est de permettre la synchronisation du récepteur. La deuxième voie est utilisée pour transmettre un signal $V(k)$ généré par l'émetteur permettant, lorsque la synchronisation est établie, de transmettre l'information. Ce signal est le résultat d'une fonction de cryptage v_c entre le message $m(k)$ contenant l'information et la clé secrète chaotique $K_c(k)$, telle que : $V(k) = v_c(K_c(k), m(k))$. L'ensemble des équations régissant l'émetteur est :

$$\begin{cases} x_m(k+1) = f_\theta(x_m(k)) \\ y_m(k) = h_\theta(x_m(k)) \\ V(k) = v_c(K_c(k), m(k)) \end{cases} \tag{3.10}$$

et celui du récepteur est :

$$\begin{cases} x_s(k+1) = f_{s\theta}(x_s(k)) \\ y_s(k) = h_{s\theta}(x_s(k)) \\ m_r(k) = v_d(K_d(k), V(k)) \end{cases} \tag{3.11}$$

A la réception, le signal chaotique $y_m(k)$ étant une information sans perturbation extérieure, une synchronisation parfaite est achevée entre les systèmes couplés (3.10) et (3.11) permetant de récupérer l'information. La fonction de décodage v_d est définie par :

$$m_r(k) = v_d(K_d(k), V(k)) = m(k) \quad lorsque \quad x_s(k) = x_m(k) \tag{3.12}$$

Cette technique est illustrée dans la figure (3.3.7).

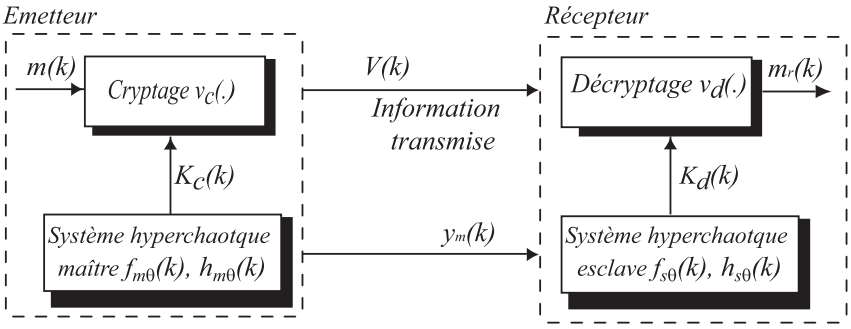


FIGURE 3.3.7 – Cryptage à deux voies de transmission

Cette technique a été proposée dans les articles [Millérioux et Mira, 1998, Jiang, 2002]. Elle présente l'avantage que le signal $y_m(k)$ ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. Le second signal $V(k)$ contient l'information qui peut être, soit cryptée par une fonction non linéaire en fonction des variables d'état du système maître comme proposé dans la référence [Millérioux et Mira, 1998, Jiang, 2002], soit simplement par un masquage utilisant un signal chaotique maître généré par l'émetteur servant de porteuse. Il est à noter que les deux phases, de synchronisation et de cryptage, étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation.

3.3.2.7 Choix de la méthode de transmission : Avantages et inconvénients des méthodes existantes

L'examen des différentes techniques de sécurisation de l'information, exposées dans les sections précédentes, a contribué à l'élimination de certaines techniques qui présentent des défaillances.

- Tout d'abord, nous avons écarté le principe du masquage additif pour plusieurs raisons. En effet, le message est additionné au signal chaotique, empêchant ainsi d'avoir une synchronisation parfaite. Plus précisément, au niveau du récepteur, le message apparaît comme une perturbation, même si on admet des messages d'informations ayant une amplitude très faible devant celle du système chaotique considéré. Par ailleurs, il est à noter qu'au niveau spectral, le message contenant l'information doit être caché dans la partie basses fréquences du spectre du système chaotique. La largeur de la densité spectrale varie selon le système chaotique, limitant ainsi le choix de messages pouvant être transmis.
- Nous avons également écarté la technique de cryptage par modulation chaotique pour deux raisons. D'une part, cette technique est propre aux messages d'informations prenant un nombre fini de valeurs, alors que nous voulons transmettre des messages à valeurs réelles. D'autre part, le signal transmis est composé de séquences générées alternativement par les différents systèmes chaotiques constituant l'émetteur. Côté émetteur, à chaque changement de système chaotique, la synchronisation est rompue. Il faut, donc, que le récepteur se synchronise de nouveau. Ainsi, le temps nécessaire à la transmission du message d'informations est plus long que pour la technique précédente, vu qu'à chaque fois que la valeur du message d'informations change, il faut ajouter le temps nécessaire à l'établissement d'une nouvelle synchronisation.
- Les techniques de cryptage par modulation paramétrique présentent des défauts au niveau de la sécurité de transmission. En effet, vu que ces dernières exploitent la signature intrinsèque de chaque attracteur chaotique, l'injection du message d'informations dans la dynamique chaotique de l'émetteur provoque une petite distorsion dans l'espace des phases du système chaotique original, tel qu'il est montré dans [Short, 1996]. Or, cet espace des phases peut être reproduit, par des techniques de reconstruction. Deux autres possibilités pour reconstituer l'information, à partir du message transmis par l'émetteur, sont développées dans [Yang *et al.*, 1998, Alvarez *et al.*, 2004]. Ces attaques, menant à la restauration du message secret par un intrus, concernent aussi le cryptage par inclusion.

Après avoir écarté les techniques de cryptage chaotique précédentes et en se référant à la liste des schémas décrits dans les sections précédentes, il ne reste que les techniques de cryptage mixte et celles reposant sur une transmission à deux voies. Nous avons ainsi décidé de choisir les méthodes qui combinent à la fois la technique de cryptographie standard et la synchronisation du chaos afin d'améliorer le degré de sécurité. Dans la suite du chapitre, nous nous proposons de tester les deux techniques de sécurisation en utilisant les méthodes de synchronisation proposées dans le cas d'entrées inconnues.

3.4 Cryptage à deux voies de transmission basé sur la méthode de synchronisation proposée et la mise en oeuvre d'observateurs

3.4.1 Préliminaires et formulation du problème de synchronisation dans le cas de cryptage à deux voies de transmission

Afin de renforcer la sécurité des cryptosystèmes, dans les articles [Millérioux et Mira, 1998, Jiang, 2002] l'accent est mis sur la nécessité de séparer totalement les étapes de cryptage et de synchronisation, d'où l'intérêt de la technique de cryptage à deux voies de transmission. Cette technique de cryptage s'est avérée être satisfaisante sur plusieurs plans. Le premier signal, permettant à l'observateur d'estimer l'état de l'émetteur et d'obtenir une synchronisation des deux systèmes couplés, est transmis indépendamment du message et ne contient, donc, aucune information sur le message. Ainsi, aucune perturbation ne pourrait gêner la synchronisation. En admettant que les conditions de synchronisation détaillées au chapitre précédent soient vérifiées, le système hyperchaotique esclave du côté récepteur peut se synchroniser avec le système hyperchaotique maître du côté émetteur sans rupture ni perte de qualité, et ce contrairement aux techniques de cryptage par commutation. On peut alors noter que l'estimation d'état au niveau du récepteur est optimale du point de vue qualité, car il n'y a pas de perte de synchronisation et du point de vue rapidité, étant donné que seul le signal chaotique est transmis. Ces deux qualités nous paraissent primordiales pour un cryptosystème performant. Ensuite, le principe de cryptage à deux voies sépare complètement les phases de synchronisation et de transmission de l'information. La reconstruction des entrées inconnues, c'est à dire la reconstitution de l'information, repose sur une estimation de l'état de l'émetteur quasi

parfaite, et la synchronisation se fait indépendamment du cryptage. La transmission des deux signaux est réalisée sur deux canaux, pas nécessairement en même temps et sans interaction entre les deux signaux, ce qui représente un gage de sécurité supplémentaire. Dans l'hypothèse de conditions de transmission parfaites, l'efficacité de ce principe de transmission est testée, dans la suite du chapitre, sur des simulations variées, à savoir la transmission d'un signal quelconque, d'une image puis d'un texte.

3.4.2 Application à la sécurité de l'information

L'approche de synchronisation proposée dans le chapitre précédent, est utilisée pour la mise en oeuvre du système de cryptage à deux voies de transmission [Filali *et al.*, 2012b]. Le schéma de communication est illustré dans la figure 3.4.8. Ce système de chiffrement qui utilise deux canaux de transmission est adopté dans le but de synchronisation plus rapide et plus sécurisée [Jiang, 2002]. Les systèmes maître et esclave chaotiques sont utilisés, respectivement, comme clé de cryptage et de décryptage. Une fois, la synchronisation obtenue entre (3.10) et (3.11) en utilisant des conditions appropriées pour la synchronisation basée sur l'utilisation du critère pratique de Borne et Gentina associé à la forme de matrice en flèche de Benrejeb, le message peut être facilement décrypté du côté du récepteur.

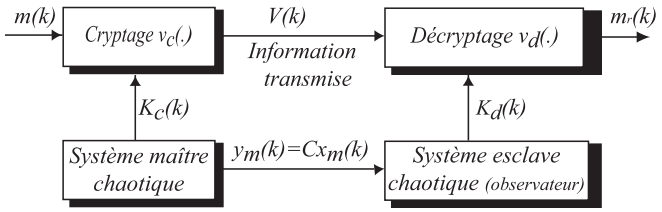


FIGURE 3.4.8 – Cryptage à deux voies de transmission

Le cryptage $v_c(.)$ utilisé est l'algorithme de chiffrement par décalage de n, "n-shift cipher algorithm" [Kharel *et al.*, 2009, Kharel *et al.*, 2010, Jiang, 2002] :

$$v_c(m(k), K_c(k)) = f_1(\ldots f_1(f_1(f_1(m(k), K_c(k))), K_c(k)), \ldots, K_c(k)) \tag{3.13}$$

$f_1(.)$ étant une fonction non-linéaire définie par :

$$f_1(m(k), K_c(k))) = \begin{cases} s(k) + 2h, pour \ : \ -2h \leq s(k) \leq -h \\ s(k), pour \ : \ -h < s(k) < h \\ s(k)) - 2h, pour \ : \ h \leq s(k) \leq 2h \end{cases} \tag{3.14}$$

où :
$s(k) = m(k) + K_c(k)$.
h est un paramètre de cryptage qui est choisi de telle sorte que $m(k)$ et $K_c(k)$ se situent dans l'intervalle $[-h, h]$.
$m(k)$ peut être récupéré à l'aide d'une règle de décryptage donnée par :

$$\begin{aligned} m_r(k) &= v_d(V(k), K_d(k)) \\ &= f_1(\ldots f_1(f_1(f_1(V(k), -K_d(k)), -K_d(k)), -K_d(k)), \ldots, -K_d(k)) \end{aligned} \tag{3.15}$$

$m_r(k)$ est le signal crypté récupéré, $v_d(.)$ la fonction de déchiffrement et $K_d(k)$ récupéré dans le circuit récepteur ayant approximativement la valeur de $K_c(k)$.
Si les systèmes hyperchaotiques dans le récepteur et l'émetteur sont synchronisés, le récepteur peut, ainsi, trouver la même valeur pour $K_d(k)$, que la valeur $K_c(k)$ dans l'émetteur. L'objectif, est de synchroniser (3.10) et (3.11) et, en même temps, de synthétiser un observateur de Luenberger discret de gain $L(.)$, tel que l'ensemble du système soit asymptotiquement stable, en utilisant le critère de Borne et Gentina associé à la mise sous forme en flèche de la matrice caractéristique instantanée du système écart.

3.4.3 Cas de clés identiques utilisant deux systèmes de Hénon généralisés

3.4.3.1 Synchronisation de deux systèmes hyperchaotiques identiques basée sur la commande par observateur et utilisant un signal scalaire. Position du problème

Considérons les systèmes hyperchaotiques discrets maître et esclave d'ordre n de type Lur'e.
Le système maître est modélisé comme suit :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) \\ y_m(k) &= Cx_m(k) \end{aligned} \tag{3.16}$$

kT est le temps discret, $x_m \in R^n$ et $y_m \in R$ sont respectivement le vecteur d'état et la sortie du système maître. A est une $(n \times n)$ matrice constante, C une $(1 \times n)$ matrice constante et $f(x(k))$ un vecteur non linéaire. Le système esclave est décrit comme un observateur non-linéaire suivant :

$$\begin{aligned} x_s(k+1) &= Ax_s(k) + f(x_s(k)) + Bu(k) \\ y_s(k) &= Cx_s(k) \\ B &= I_{n\times n} \end{aligned} \tag{3.17}$$

où la loi :

$$u(k) = -L(.)(y_s(k) - y_m(k)) \tag{3.18}$$

joue le rôle de la rétroaction de sortie.
$x_s \in R^n$ et $y_s \in R$ sont, respectivement, le vecteur d'état et la sortie du système esclave et $L(x_m(k), x_s(k))$ le vecteur gain de l'observateur de Luenberger [Liao et Huang, 1999] :

$$L(.) = [l_1(.) \ \ldots \ l_n(.)]^T, \ l_i \in R, \ i = 1, 2, \ \ldots \ , n \tag{3.19}$$

permettant de satisfaire la synchronisation maître/esclave [Pecora et Carroll, 1990,Carroll et Pecora, 1991] c'est-à-dire,

$$\lim_{k\to+\infty} \|x_{mi}(k) - x_{si}(k)\| = 0, \ i = 1, 2, 3 \tag{3.20}$$

Le vecteur d'erreur de synchronisation est défini par : $e(k) = x_m(k) - x_s(k)$. Utilisant (3.10) et (3.11), sa dynamique est exprimée par :

$$\begin{aligned} e(k+1) &= Ae(k) + Bu(k) + f(x_m(k)) - f(x_s(k)) \\ &= (A - BL(.)C)e(k) + f(x_m(k)) - f(x_s(k)) \\ &= (A - L(.)C)e(k) + f(x_m(k)) - f(x_s(k)) \end{aligned} \tag{3.21}$$

Considérons que la fonction $f(.)$ est telle que :

$$f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))e(k) \tag{3.22}$$

Le système d'erreur peut être réécrit sous la forme :

$$e(k+1) = A_f(x_m(k), x_s(k))e(k) \tag{3.23}$$

avec :

$$A_f(x_m(k), x_s(k)) = A - BL(.)C + Q(x_m(k), x_s(k)) \tag{3.24}$$

Le théorème suivant, basé sur l'utilisation du critère pratique de Borne et Gentina [Borne *et al.*, 1972, Borne *et al.*, 1976, Borne, 1987, Gentina *et al.*, 1972, Gentina *et al.*, 1972] associé à la mise sous forme canonique particulière : matrice de forme en flèche de Benrejeb $A_f(.) = \{a_{a_{ij}}(.)\}$ [Benrejeb et Borne, 1978, Benrejeb *et al.*, 1982, Borne et Benrejeb, 2008, Benrejeb, 2010], donne des conditions suffisantes de synchronisation complète du système esclave (3.11) avec le système maître (3.10).

Théorème 3.1. *L'erreur de synchronisation, décrite par* (3.23) *converge vers zéro, si la matrice* $A_f(.)$*, définie par* (3.24) *du système corrigé de la forme* (2.15)*, est sous la forme en flèche de type 2 telle que :*

i. les éléments non linéaires de la matrice caractéristique $A_f(.)$ *sont isolés dans une rangée ;*

ii. les éléments diagonaux, $a_{f_{ii}}(.)$*, de la matrice caractéristique* $A_f(.)$ *sont tels que :*

$$1 - |a_{f_{ii}}(.)| > 0, \ \forall i = 2, \ldots, n \tag{3.25}$$

iii. il existe $\varepsilon > 0$*, de telle sorte que :*

$$1 - |a_{f_{11}}(.)| - \sum_{i=2}^{n} \left(\begin{array}{l} |a_{f_{i1}}(.)\, a_{f_{1i}}(.)| \\ \times \left(1 - |a_{f_{ii}}(.)|\right)^{-1} \end{array} \right) > \varepsilon \tag{3.26}$$

Démonstration. La démonstration du théorème 3.1 est similaire à celle du théorème 2.1, □

3.4.3.2 Cas de clés identiques utilisant deux systèmes hyperchaotiques de Hénon

Dans cette section, les performances de l'approche de synchronisation proposée sont illustrées pour la technique de transmission à deux canaux de transmission, en utilisant le système hyperchaotique d'ordre 3 de Hénon généralisé en tant que clé de l'émetteur et du récepteur [Baier et Klein, 1990, Miller et Grassi, 2001, Grassi et Miller, 2002, Li *et al.*, 2009] :

- le système maître défini par :

$$\begin{cases} x_{m1}(k+1) = 1.76 - x_{m2}^2(k) - 0.1.x_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \\ y_m(k) = x_{m2}(k) \\ K_c(k) = \sqrt{|x_{m1}(k) + x_{m2}(k) + x_{m3}(k)|} \\ V(k) = v_c(m(k), K_c(k)) \end{cases} \tag{3.27}$$

La fonction de cryptage v_c est définie par (3.13), où par le système hyperchaotique d'ordre 3 de Hénon généralisé, défini, pour le côté émetteur, dans l'espace d'état, par :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) \\ y_m(k) &= Cx_m(k) \end{aligned} \tag{3.28}$$

- le système esclave est défini par :

$$\begin{cases} x_{s1}(k+1) = 1.76 - x_{s2}^2(k) - 0.1x_{s3}(k) + l_1(.)\varepsilon(k) \\ x_{s2}(k+1) = x_{s1}(k) + l_2(.)\varepsilon(k) \\ x_{s3}(k+1) = x_{s2}(k) + l_3(.)\varepsilon(k) \\ y_s(k) = x_{s2}(k) \\ K_d(k) = \sqrt{|x_{s1}(k) + x_{s2}(k) + x_{s3}(k)|} \\ m_r(k) = v_d(V(k), K_d(k)) \end{cases} \tag{3.29}$$

avec : $\varepsilon(k) = y_m(k) - y_s(k)$ et v_d la fonction de décryptage définie par (3.15), où le système hyperchaotique d'ordre 3 de Hénon généralisé est défini, pour le côté récepteur, dans l'espace d'état, par :

$$\begin{aligned} x_s(k+1) &= Ax_s(k) + f(x_s(k)) + Bu(k) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{3.30}$$

$x_m(k) = [x_{m1}(k)\ \ x_{m2}(k)\ \ x_{m3}(k)]^T$ est le vecteur d'état du système maître,
$x_s(k) = [x_{s1}(k)\ \ x_{s2}(k)\ \ x_{s3}(k)]^T$ celui du système esclave, et où la loi de rétroaction de sortie $u(k)$ introduite dans (3.18) étant définie de telle sorte que :

$$L(.) = [l_1(.)\, l_2(.)\, l_3(.)]^T \tag{3.31}$$

Le vecteur C est choisi comme suit :

$$C = [0 \quad 1 \quad 0] \tag{3.32}$$

A peut être écrite comme suit :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{3.33}$$

et :

$$B = I_{3\times 3} \tag{3.34}$$

$$f(x(k)) = [-x_2^2(k) \quad 0 \quad 0]^T \tag{3.35}$$

Considérons les composantes de l'erreur de synchronisation $e_i(k)$, entre les systèmes (3.28) et (3.30) :

$$e_i(k) = x_{mi}(k) - x_{si}(k), \ \forall i = 1, 2, 3 \tag{3.36}$$

Il vient :

$$e(k+1) = A_f(x_m(k), x_s(k))e(k) \tag{3.37}$$

avec :
$A_f(x_m(k), x_s(k)) = A - BL(.)C + Q(x_m(k), x_s(k))$
et :

$$Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -x_{m2}(k) - x_{s2}(k) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{3.38}$$

On a alors :

$$A_f(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -x_{m2}(k) - x_{s2}(k) - l_1(.) & -0.1 \\ 1 & -l_2(.) & 0 \\ 0 & 1 - l_3 & 0 \end{bmatrix} \tag{3.39}$$

et :

$$I - M(A_f(x_m(k), x_s(k))) = \begin{bmatrix} 1 & -|-x_{m2}(k) - x_{s2}(k) - l_1(.)| & -0.1 \\ -1 & 1 - |l_2(.)| & 0 \\ 0 & -|1 - l_3| & 1 \end{bmatrix} \tag{3.40}$$

$M(A_f(.))$ étant la majorante de $A_f(.)$ relativement à la norme vectorielle $p(z(k))$ précédente, obtenu à partir de (2.17).
Le paramètre de correction l_3, choisi constant comme suit :

$$l_3 = 1 \tag{3.41}$$

rend la matrice $A_f(x_m(k), x_s(k))$ sous forme en flèche mince de Benrejeb. Il vient :

$$I - M(A_f(x_m(k), x_s(k))) = \begin{bmatrix} 1 & -|-x_{m2}(k) - x_{s2}(k) - l_1(.)| & -0.1 \\ -1 & 1 - |l_2(.)| & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3.42}$$

La synchronisation est obtenue lorsque les conditions de stabilisation (3.25) et (3.26) du théorème énoncé dans la section précédente :

$$\begin{cases} 1 - |l_2(.)| > 0, \\ 1 - \frac{|x_{m2}(k)+x_{s2}(k)+l_1(.)|}{1-|l_2(.)|} > 0 \end{cases} \tag{3.43}$$

sont satisfaites.
Ensuite, les gains instantanés $l_1(.)$ et $l_2(.)$, satisfaisant les inégalités (3.43), tels que :

$$L(x_m(k), x_s(k)) = [0.25 - x_{m2}(k) - x_{s2}(k) \quad 0.5 \quad 1]^T \tag{3.44}$$

garantissent la synchronisation entre le système maître et le système esclave de Hénon généralisé, ayant ainsi la synchronisation entre les clés secrètes $K_c(k)$ et $K_d(k)$ et on a enfin la reconstruction du message d'informations $m_r(k) = m(k)$, après un certain nombre d'itérations.
Les simulations, effectuées en utilisant Matlab/Simulink, ont conduit aux résultats présentés ci-dessous qui illustrent bien la synchronisation dans le cas discret. Ils résultent de l'utilisation du critère pratique de Borne et Gentina associée à la mise de la matrice caractéristique sous forme en flèche mince de Benrejeb et de son application à la technique de cryptage à deux canaux de communication.
Les résultats de la simulation relatifs à la transmission du message d'informations $m(k)$ et l'extraction du message récupéré $m_r(k)$, à travers du cryptosystème proposé, sont indiqués dans la figure 3.4.9. Il est à noter que $m_r(k)$ est exactement égal à $m(k)$ à partir de l'étape $k = 54$ Tableau (3.1). Le signal crypté est présenté dans la figure 3.4.10, les clés de l'émetteur et du récepteur, dans la figure 3.4.11, le cryptage h étant pris égal à 2, et n' égal à 4.

La figure 3.4.12 présente les dynamiques des erreurs de synchronisation ; en effet, on peut observer que $e_1(k)$, $e_2(k)$ et $e_3(k)$ convergent vers zéro après quelques itérations. Enfin, la figure. 3.4.13 indique que les variables d'état du vecteur du système esclave atteignent la synchronisation avec celles du système maître, à partir de différentes conditions initiales telles que $(x_m(0), x_s(0)) = ((1, 0.1, 0), (-0.5, 0, 0.3))$.

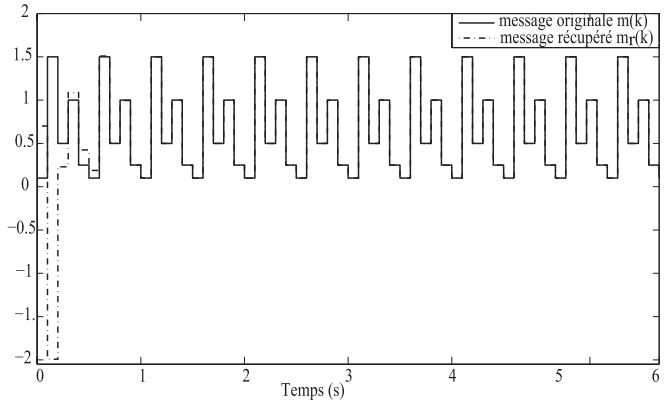


FIGURE 3.4.9 – Message d'informations original $m(k)$ (—) et message récupéré $m_r(k)$ $(- \cdot -)$

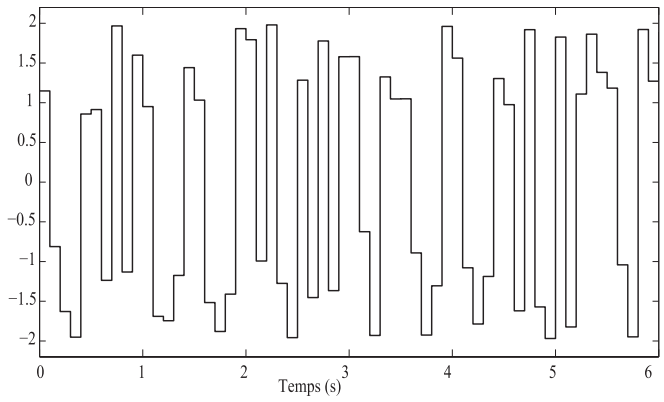


FIGURE 3.4.10 – Message crypté $V(k)$

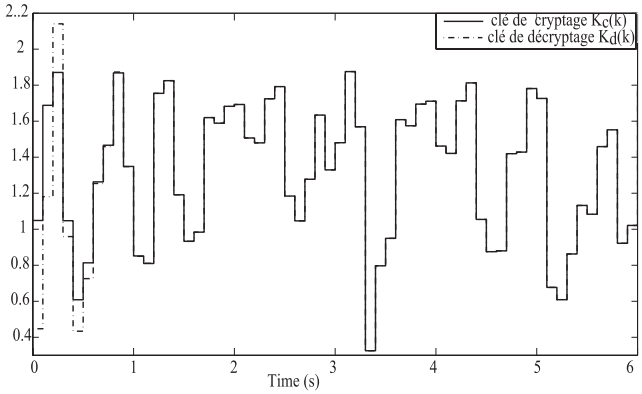


FIGURE 3.4.11 – Clé secrète de cryptage $K_c(k)$ (—) et clé secrète de déryptage $K_d(k)$ $(- \cdot -)$

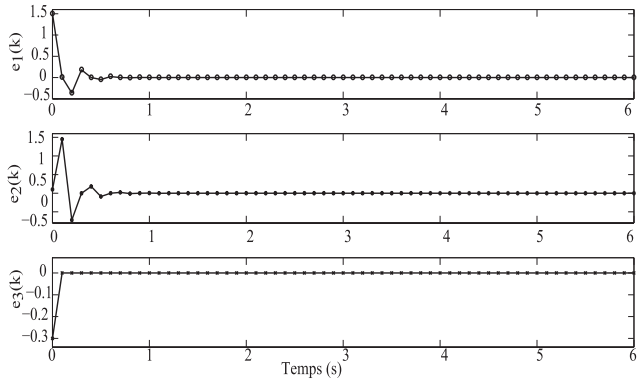


FIGURE 3.4.12 – Dynamiques des variables du vecteur erreur

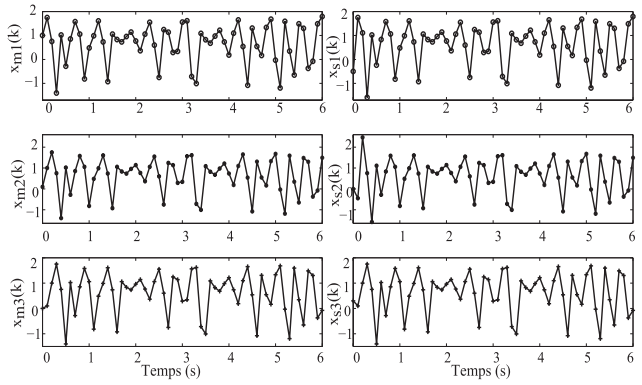


FIGURE 3.4.13 – Réponses temporelles des variables d'état des systèmes maître et esclave

TABLE 3.1 – $m(k)$ et $m_r(k)$ en fonction de k

$m(k)$	k	$m_r(k)$	k	$m_r(k)$	k	$m_r(k)$
0.10	1	1,59602244367011	21	0,0999987802622770	41	0,100000000000905
1.50	2	-1,99290687948836	22	1,50000022467681	42	1,49999999999931
0.25	3	0,230151230526206	23	0,500000234409508	43	0,500000000000094
1.00	4	1,08845003732530	24	0,999999850353680	44	1,00000000000009
0.50	5	0,424542463707385	25	0,250000023616540	45	0,249999999999883
0.10	6	0,0120990296191550	26	0,100000036618606	46	0,100000000000023
1.50	7	1,50881421709450	27	1,49999996917314	47	1,50000000000002
0.50	8	0,507771216233836	28	0,500000004140873	48	0,499999999999989
0.10	9	0,995478901334732	29	1,00000000331680	49	1.000000000000001
0.25	10	0,251028416208063	30	0,249999996966815	50	0.250000000000001
0.10	11	0,101670417411753	31	0,100000000446618	51	0.099999999999999
1.50	12	1,49869518534731	32	1,50000000036122	52	1.500000000000000
0.50	13	0,500098783301088	33	0,499999999678753	53	0.500000000000001
1.00	14	1,00009731510352	34	1,00000000025408	***54***	***1.000000000000000***
0.25	15	0,249889103943457	35	0,250000000106292	55	0,250000000000000
0.10	16	0,100023228288427	36	0,0999999999336394	56	0,100000000000000
1.50	17	1,50002256567954	37	1,50000000000642	57	1,50000000000000
0.50	19	1,00000170423726	38	0,500000000006724	58	0,500000000000000
1.00	18	0,499989803687935	39	0,999999999995353	59	0,100000000000000
0.25	20	0,250001649073327	40	0,250000000000755	60	0.250000000000000

3.4.3.3 Mise en oeuvre dans le cas de la transmission d'une image

L'image originale, prise dans ce chapitre, est la photographie de Lena, couramment utilisée en traitement d'images. Elle est présentée dans la figure 3.4.14.

FIGURE 3.4.14 – Photographie de Lena

Cette image en couleur, est définie par trois matrices, chacune code l'intensité d'une couleur de base à savoir rouge, vert et bleu. A partir de cette image, on génère un signal à une dimension : les lignes de la première matrice sont concaténées pour former un seul

vecteur. De manière analogue, on effectue le même principe avec la deuxième matrice qui prolonge ce vecteur, puis on termine avec la troisième matrice. Les images, cryptée et reconstruite, sont consignées respectivement dans les figures 3.5.27i (i) 3.5.27i (ii).
On définit la clé de cryptage et décryptage comme suit :

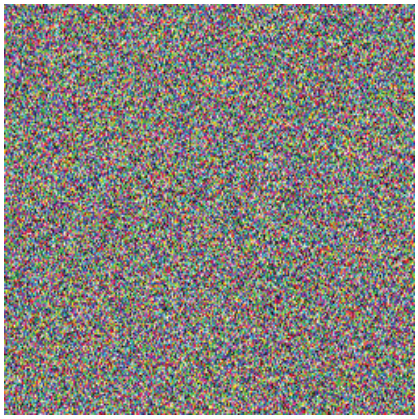
$$K_c(k) = \left(A\sqrt{\left(x_{m1}^4(k) + x_{m2}^4(k) + x_{m3}^4(k)\right)} \right) \bmod (256) \tag{3.45}$$

$$K_d(k) = \left(A\sqrt{\left(x_{s1}^4(k) + x_{s2}^4(k) + x_{s3}^4(k)\right)} \right) \bmod (256) \tag{3.46}$$

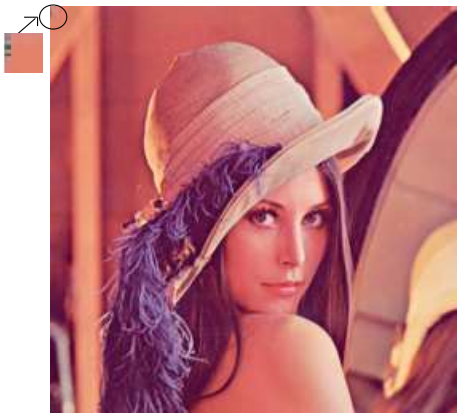
et les fonctions de cryptage et décryptage comme suit :

$$V(k) = m(k) \oplus K_c(k) \tag{3.47}$$

$$m_r(k) = V(k) \oplus K_d(k) \tag{3.48}$$



(i) Image transmise



(ii) Image reconstruite

FIGURE 3.4.15 – Reconstruction de l'image de Lena dans le cryptage à deux voies de transmission.

Pour $A = 100$ et les conditions initiales $x_m = (1, 0.1, 0)$ et $x_s = (-0.5, 0, 0.3)$, on constate que les premiers points, à gauche et en haut, de l'image reconstruite (figure 3.5.27i (ii)) présentent des erreurs.

3.4.3.4 Mise en oeuvre dans le cas de la transmission d'une partie d'un texte

Les paramètres de simulation, précédemment indiqués dans le paragraphe (3.4.4.2), sont conservés. Le texte à transmettre est reproduit dans la figure 3.4.16 (a). A l'aide du code ASCII, on génère un vecteur dont les composantes sont des entiers compris entre 0 et

255. On applique le processus de cryptage et on obtient le texte crypté de la figure 3.4.16 (b) ; on applique ensuite le processus inverse en utilisant de nouveau le code ASCII et on obtient le texte décrypté tel qu'on le voit dans la figure 3.4.16 (c). On peut ajouter un texte vide d'une certaine longueur à déterminer pour pallier aux erreurs et obtenir une reconstitution parfaite.

(a)
Stabilization conditions are proposed for hyperchaotic discrete-time systems synchronization. They are based on the use of an observer and of the aggregation techniques.
(b)
76&□Ê²é~zmí{:u øóé□ÜÃà□y,□Ú´êò□ □s×Ìô^Ð×¤BUZµ¢ÎÜ,"HK@!□qfÊâóþ□6¬□□Eì?□°ý ;ÆØãj}f□ç°¥ëÑ:;g }□□M□Ûé;~è$4□úh'%:n⊠@pôÛ ì'xwÜ□g⊠9R ð¶×á□Z]þ¯Ä□R□⊠□Áf□ð/ÙÇ°⊠ìÑ ·ûyââ ⊠
(c)
,P□ [□}dthnn#conditions are proposed for hyperchaotic discrete-time systems synchronization. They are based on the use of an observer and of the aggregation techniques.

FIGURE 3.4.16 – (a) : Texte original, (b) : Texte correspondant au signal transmis, (c) : Texte décrypté

3.4.4 Cas de clés non identiques utilisant un système de Hénon généralisé couplé avec le système de Hénon

3.4.4.1 Synchronisation de clés hyperchaotiques non identiques. Position du problème

Dans cette partie, il est envisagé de déterminer une commande par retour de sortie afin d'accomplir la synchronisation de deux systèmes non identiques de types maître et esclave. Commençons, tout d'abord, par l'élaboration de conditions de synchronisation, ensuite nous testons les conditions élaborées pour un exemple de systèmes chaotiques en utilisant la technique de cryptage utilisant deux voies de transmission.
On considère, comme précédemment, un système hyperchaotique de dimension n considéré en tant que système maître décrit comme suit :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E \\ y_m(k) &= Cx_m(k) \end{aligned} \tag{3.49}$$

On associe à ce système maître un système non identique, du type esclave, défini par :

$$\begin{aligned} x_s(k+1) &= A_1 x_s(k) + f_1(x_s(k)) + E_1 + Bu(k) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{3.50}$$

avec : $x_m(k) = \left[\begin{array}{ccc} x_{m1}(k) & \dots & x_{mn}(k) \end{array}\right]^T \in R^n$, $x_s(k) = \left[\begin{array}{ccc} x_{s1}(k) & \dots & x_{sn}(k) \end{array}\right]^T \in R^n$,

E et E_1 représentant, respectivement, des vecteurs constants des systèmes (3.49) et (3.50), et :

$$B = I_{n\times n} \tag{3.51}$$

$A = \{a_{ij}\}$ et $A_1 = \{a_{1_{ij}}\}$ sont des matrices constantes et $f(x_m(k))$ et $f_1(x_m(k))$ des vecteurs non linéaires. La commande active $u(k)$ est à déterminer pour assurer la synchronisation de ces deux systèmes non identiques.
Les écarts dynamiques sur les variables d'état, peuvent être définis par :

$$e(k) = x_s(k) - x_m(k) \tag{3.52}$$

Il vient le système écart correspondant :

$$e(k+1) = A_1 x_s(k) + f_1(x_s(k)) - Ax_m(k) + f(x_m(k)) + E_1 - E + Bu(k) \tag{3.53}$$

La structure de la loi de commande $u(k)$, retenue dans le cas présent, est, d'une part, par retour de sortie vu que dans le cas de la sécurité de transmission, on n'a connaissance que de la sortie de l'émetteur et, d'autre part, par compensation du terme complémentaire représentée comme suit :

$$u(k) = (A - A_1) x_s(k) + f(x_s(k)) - f_1(x_s(k)) - E_1 + E + L(y_m(k) - y_s(k)) \tag{3.54}$$

$L(.) = \{l_i(.)\} \in R^n$ étant des gains d'observateur inconnus à déterminer pour assurer la synchronisation.
La substitution de la commande par retour d'état (3.54) dans le système (3.53) conduit à la nouvelle représentation du système erreur comme suit :

$$e(k+1) = Ax_s(k) + f(x_s(k)) - Ax_m(k) - f(x_m(k)) - BL(.)C(.)e(k) \tag{3.55}$$

On peut noter que le choix du retour de sortie $u(k)$, comme (3.54), ramène l'étude de la synchronisation de deux systèmes hyperchaotiques non identiques à celle de deux systèmes hyperchaotiques identiques.
Pour plusieurs systèmes chaotiques, l'écart $f(x_s(k)) - f(x_m(k))$ peut être factorisé comme suit [Jiang *et al.*, 2003] :

$$f(x_s(k)) - f(x_m(k)) = Q(x_m(k), x_s(k))e(k) \tag{3.56}$$

où $Q(x_s(k), x_m(k))$ est une matrice bornée dont les éléments dépendent des vecteurs d'état $x_m(k)$ et $x_s(k)$.
Le système peut être alors réécrit comme suit :

$$e(k+1) = A_f(x_m(k), x_s(k))e(k) \tag{3.57}$$

avec :

$$A_f\left(x_m\left(k\right), x_s\left(k\right)\right) = \left(A + Q\left(x_s\left(k\right), x_m\left(k\right)\right) - BL\left(.\right)C\left(.\right)\right) \tag{3.58}$$

Le système erreur, décrit par (3.55) est stabilisé par le choix judicieux du retour de sortie défini par (3.54), si la matrice $A_f\left(x_m\left(k\right), x_s\left(k\right)\right)$, définie par (3.58), est de forme en flèche telle que sa représentation est de la forme (2.15). Pour atteindre cet objectif, le théorème suivant peut être établi, basé sur l'utilisation du critère de Borne et Gentina [Borne *et al.*, 1972, Borne *et al.*, 1976, Borne, 1987, Gentina *et al.*, 1972], associé à la représentation en flèche de la matrice $A_f\left(.\right) = \left\{a_{f_{ij}}\left(.\right)\right\} = \left(A + Q(x_s\left(k\right), x_m\left(k\right)) - BK\left(.\right)\right)$ [Benrejeb et Borne, 1978, Benrejeb *et al.*, 1982, Benrejeb et Hammami, 2008, Borne *et al.*, 2007, Borne et Benrejeb, 2008], donnant ainsi des conditions suffisantes de synchronisation du système esclave (2.89) avec le système maître (2.90) [Benrejeb, 2010].

Théorème 3.2. *Le processus erreur défini par* (3.55) *converge vers zéro, si la matrice caractéristique instantanée* $A_f(.)$ *du système corrigé* (2.15)*, est en forme en flèche mince de type 2, telle que :*

i. les éléments non constants sont isolés dans une seule rangée ;

ii. les éléments diagonaux $a_{f_{ii}}(.)$*, de la matrice* $A_f(.)$*, sont tels que :*

$$1 - |a_{f_{ii}}(.)| > 0,\ \forall i = 2, \ldots, n \tag{3.59}$$

iii. il existe $\varepsilon > 0$ *tel que :*

$$1 - |a_{f_{11}}\left(.\right)| - \sum_{i=2}^{n} \left(\begin{array}{l} |a_{f_{i1}}\left(.\right) a_{f_{1i}}\left(.\right)| \\ \times \left(1 - |a_{f_{ii}}\left(.\right)|\right)^{-1} \end{array} \right) > \varepsilon \tag{3.60}$$

Démonstration. La démonstration du théorème 3.2 est similaire à celle du théorème 2.1. □

3.4.4.2 Cas de synchronisation de la clé de 3D Hénon (Hitzl-Zele) couplée avec la clé de Hénon généralisée (Baier-Klein)

On considère le système hyperchaotique de type Baier-Klein de troisième ordre (aussi appelé système de Hénon généralisé) [Baier et Klein, 1990, Miller et Grassi, 2001] qui peut

être décrit comme suit :

$$\begin{cases} x_{m1}(k+1) = 0.1 - x_{m2}^2(k) - 1.76.x_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \\ y_m(k) = c_1 x_{m1}(k) + c_2 x_{m2}(k) + c_3 x_{m3}(k) \\ K_c(k) = \sqrt{|x_{m1}(k) + x_{m2}(k) + x_{m3}(k)|} \\ V(k) = v_c(m(k), K_c(k)) \end{cases} \tag{3.61}$$

Dans l'espace d'état, (3.61) peut être réécrite comme suit :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E \\ y_m(k) &= Cx_m(k) \end{aligned} \tag{3.62}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{3.63}$$

$$f(x_m(k)) = \begin{bmatrix} -x_{m2}^2(k) & 0 & 0 \end{bmatrix}^T \tag{3.64}$$

et :

$$E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T \tag{3.65}$$

Considérons le système hyperchaotique d'ordre 3 Hénon (Hitzl-Zele) [Y.J. Xue, 2003, Hitzl et Zele, 1985] :

$$\begin{cases} x_{s1}(k+1) = -0.3x_{s2}(k) + u_1(k) \\ x_{s2}(k+1) = 1 + x_{s3}(k) - 1.07x_{s2}^2(k) + u_2(k) \\ x_{s3}(k+1) = 0.3x_{s2}(k) + x_{s1}(k) + u_3(k) \\ y_s(k) = c_1 x_{s1}(k) + c_2 x_{s2}(k) + c_3 x_{s3}(k) \\ K_d(k) = \sqrt{|x_{s1}(k) + x_{s2}(k) + x_{s3}(k)|} \\ m_r(k) = v_d(V(k), K_d(k)) \end{cases} \tag{3.66}$$

Dans l'espace d'état, celui-ci peut être représenté par :

$$\begin{aligned} x_s(k+1) &= A_1 x_s(k) + f_1(x_s(k)) + E_1 + Bu(k) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{3.67}$$

avec :

$$A_1(x_s(k)) = \begin{bmatrix} 0 & -0.3 & 0 \\ 0 & 0 & 1 \\ 1 & 0.3 & 0 \end{bmatrix} \tag{3.68}$$

$$f_1(x_s(k)) = \begin{bmatrix} 0 & -1.07x_{s2}^2(k) & 0 \end{bmatrix}^T \tag{3.69}$$

et :

$$E_1 = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T \tag{3.70}$$

Comme il a été déjà montré dans le chapitre 2, la figure. 2.4.11 illustre bien la différence des deux attracteurs chaotiques de types Hénon (Hitzl-Zele) et Hénon généralisé (Baier-Klein). En outre, la figure. 2.4.12 représente bien les évolutions des variables du système erreur entre (3.61) et (3.66) lorsque la commande par retour de sortie est désactivée. Cette dernière ne tendant pas vers zéro, on n'a pas de synchronisation des systèmes couplés.
Considérons les composants du vecteur état du système erreur du système maître (3.61) et du système esclave (3.66), définies par :

$$e_i(k) = x_{si}(k) - x_{mi}(k), \ \forall i = 1, 2, 3 \tag{3.71}$$

En appliquant (3.54), $u(k)$ peut être réécrite comme suit :

$$\begin{cases} u_1(k) = 0.3x_{s2}(k) - 0.1x_{s3}(k) + 1.76 - x_{s2}^2(k) - \sum_{j=1}^{3} l_1 c_j e_j(k) \\ u_2(k) = x_{s1}(k) - x_{s3}(k) - 1 + 1.07x_{s2}^2 - \sum_{j=1}^{3} l_2 c_j e_j(k) \\ u_3(k) = -x_{s1}(k) + 0.7x_{s2}(k) - \sum_{j=1}^{3} l_3 c_j e_j(k) \end{cases} \tag{3.72}$$

Par le choix (3.72) de $u(k)$, il vient la possibilité de transformer l'étude de la synchronisation de deux systèmes non identiques de types Baier-Klein et Hénon en l'étude de la synchronisation de deux systèmes hyperchaotiques identiques de type Baier-Klein.
Dans l'espace d'état, l'erreur peut être reformulée comme suit :

$$e(k+1) = (A + Q(x_m(k), x_s(k)) - BLC)\, e(k) \tag{3.73}$$

telle que :

$$A_f(x(k)) = (A + Q(x_m(k), x_s(k)) - BLC) \tag{3.74}$$

avec :

$$Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -(x_{s2}(k) + x_{m2}(k)) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{3.75}$$

$$B = I_{3\times 3} \tag{3.76}$$

$$C = \begin{bmatrix} c_1 & c_2 & c_3 \end{bmatrix} \tag{3.77}$$

et :

$$L = \begin{bmatrix} l_1 & l_2 & l_3 \end{bmatrix}^T \tag{3.78}$$

Alors, $A_f(x(k))$ peut être réecrite comme suit :

$$A_f(.) = \begin{bmatrix} -l_1(.)c_1(.) & -(l_1(.)c_2(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 - l_1(.)c_3(.) \\ 1 - l_2(.)c_1(.) & -l_2(.)c_2(.) & -l_2(.)c_3(.) \\ -l_3(.)c_1(.) & 1 - l_3(.)c_2(.) & -l_3(.)c_3(.) \end{bmatrix} \tag{3.79}$$

Le choix des paramètres de correction c_3 et l_3 tels que :

$$\begin{cases} l_2 c_3 = 0 \\ 1 - l_3 c_2 = 0 \end{cases} \tag{3.80}$$

permet de forcer la matrice caractéristique $A_f(x(k))$ à être sous la forme en flèche de Benrejeb de type 2 :

$$A_f(.) = \begin{bmatrix} -l_1(.)c_1(.) & -(l_1(.)c_2(.) + x_{m2}(k) + x_{s2}(k)) & -0.1 \\ 1 - l_2(.)c_1(.) & -l_2(.)c_2(.) & 0 \\ -l_3(.)c_1(.) & 0 & 0 \end{bmatrix} \tag{3.81}$$

Le système caractérisé par (3.74) est asymptotiquement stable, si les gains l_i et c_j, $i, j = 1, 2, 3$, sont choisis, tels que les contraintes suivantes soient vérifiées :

i. les éléments non linéaires de la matrice caractéristique $A_f(x(k))$ sont isolés dans une seule rangée ;

ii. les éléments diagonaux de la matrice caractéristique $A_f(x(k))$ sont, tels que :

$$1 - |l_2 c_2| > 0 \tag{3.82}$$

iii. il existe $\varepsilon > 0$ tel que :

$$1 - |l_1 c_1| - \frac{(x_{m2}(k) + x_{s2}(k) + |l_1 c_2|)(|1 - l_2 c_1|)}{1 - |l_2 c_2|} - \frac{0.1 c_1}{c_2} \geq \varepsilon \tag{3.83}$$

Remarque 3.1. ***Propriété de bornitude***

Le système hyperchaotique x_m *de* (2.147) *est globalement, uniformément borné. En effet, plusieurs systèmes physiques tels que les oscillateurs et plus particulièrement les systèmes chaotiques vérifient cette propriété.*
Soit $\omega_i > 0$, $\forall i = \{1, \ldots, n\}$. *On définit le compact* $\Omega \subset R^n$
$\Omega := \{x \in R^n : |x_i(k) \leq \omega_i|\}$. *La propriété de bornitude [Eckmann et Ruelle, 1985] des systèmes* (2.101) *et* (2.106) *nous permet d'effectuer la transformation suivante :*
$|x_{mi}| < 2$ *et* $|x_{si}| < 2$. *Ainsi, on a :*
$| x_{m2} + x_{s2} + l_1 c_2 | < 4 + | l_1 c_2 |$

En substituant les équations (3.80) dans la condition (3.83), cette dernière peut être réecrite comme suit :

$$1 - |l_1 c_1| - \frac{(4 + |l_1 c_2|)(|1 - l_2 c_1|)}{1 - |l_2 c_2|} - \left|\frac{0.1 c_1}{c_2}\right| > 0 \tag{3.84}$$

Ainsi, les gains instantanés $l_i(.)$ et $c_j(.)$, $\forall i, j = 1, 2, 3$, satisfaisant les inégalités (3.82), (3.83) et (3.84) choisis, tels que :

$$C = [1.73 \quad 0.91 \quad 0] \tag{3.85}$$

$$L = [-0.20 \quad 0.55 \quad 1.10]^T \tag{3.86}$$

garantissent la synchronisation entre les deux systèmes (3.61) et (3.66), comme le montre les figures 3.4.18, 3.4.19 et 3.4.20 dans la transmission du message $m(k)$ consigné dans la figure 3.4.17, la période d'échantillonnage T étant prise égale à $0.1s$

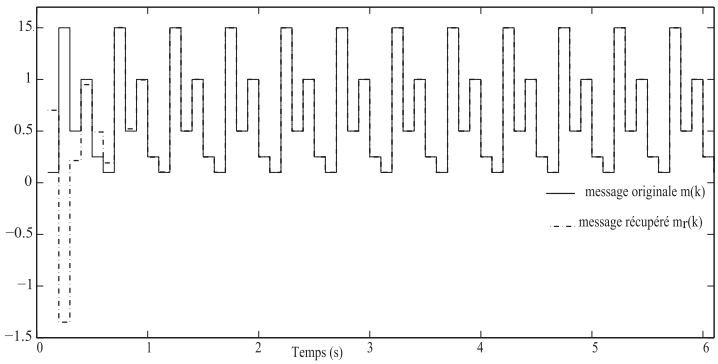


FIGURE 3.4.17 – Message d'informations original $m(k)$ et message récupéré $m_r(k)$

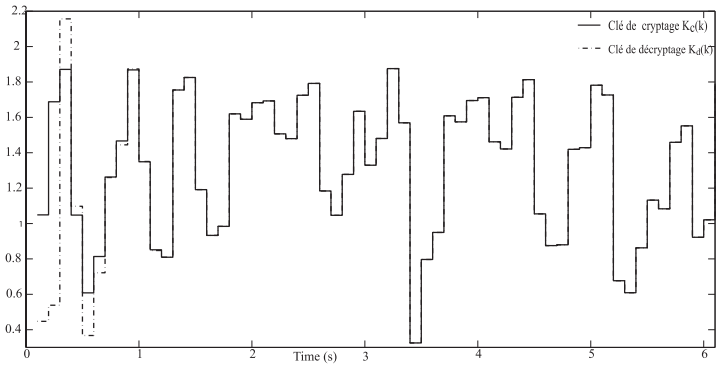


FIGURE 3.4.18 – Clé de cryptage $K_c(k)$ (—) et clé de décryptage $K_d(k)(- \cdot -)$

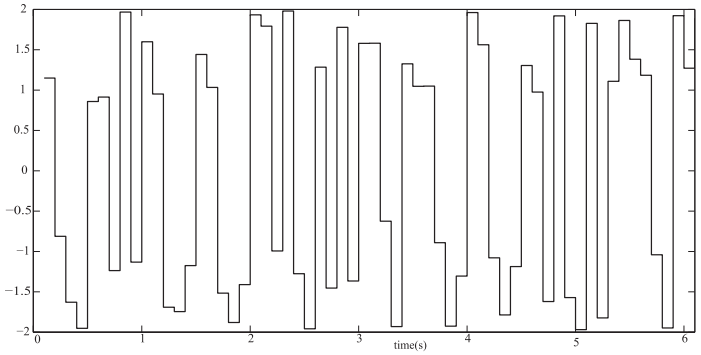


FIGURE 3.4.19 – Message crypté

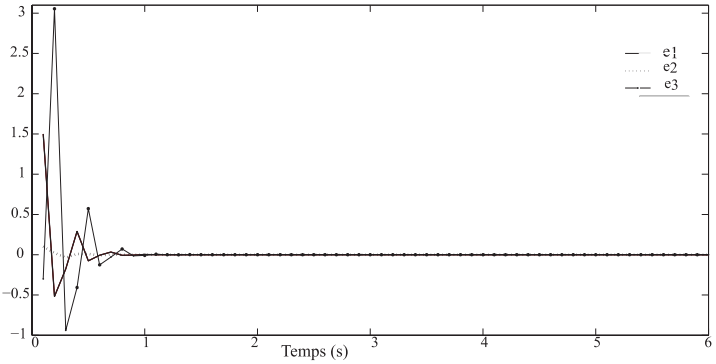


FIGURE 3.4.20 – Dynamiques des variables d'état du système erreur

3.5 Cryptage mixte basé sur la méthode de synchronisation proposée et la mise en oeuvre d'observateurs

3.5.1 Préliminaires et formulation du problème de synchronisation dans le cas du cryptage mixte proposé

Dans cette section, une technique de communication à base de systèmes hyperchaotiques discrets sécurisés, appelée cryptosystème hyperchaotique, (figure 3.5.21), est présentée en utilisant une combinaison, à la fois, de la technique de cryptographie standard et la synchronisation du chaos à base d'observateurs [Grassi et Mascolo, 1997]. La synchronisation hyperchaotique maître/esclave est basée sur un observateur linéaire, comme le montre la figure 3.5.21, permettant au récepteur hyperchaotique de récupérer le message d'informations.

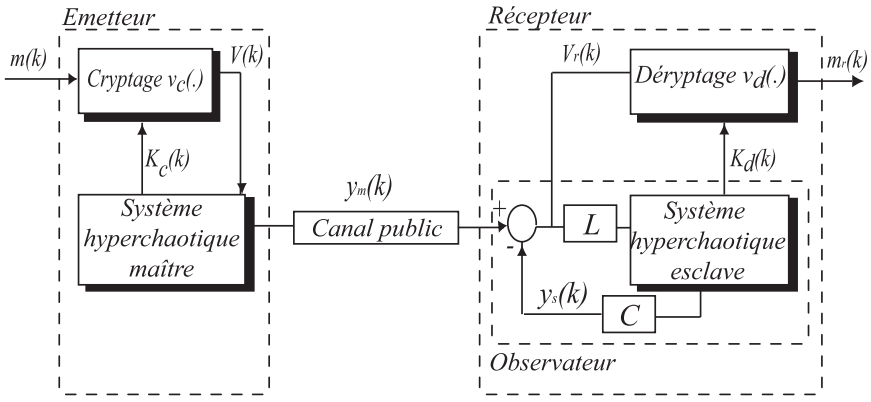


FIGURE 3.5.21 – Cryptosystème basé sur l'utilisation de la synchronisation chaotique à base d'observateurs

Le système proposé comprend deux blocs, de cryptage et de décryptage, qui contiennent, respectivement, un système hyperchaotique maître et un système hyperchaotique esclave.

– Le système maître est décrit, dans l'espace d'état, par :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + \alpha NV(k) \\ y_m(k) &= Cx_m(k) + \alpha V(k) \end{aligned} \tag{3.87}$$

$x_m(k)$ étant le vecteur d'état, à l'instant kT, T la période d'échantillonnage, $x_m \in R^n$,

$A = \{a_{ij}\}$ une matrice constante $(n \times n)$, $C = [c_1 \ldots c_n]$ un vecteur de dimension $(1 \times n)$ à déterminer afin de satisfaire la synchronisation maître/esclave. $N = [n_1 \ \ldots \ n_n]^T$ un vecteur constant caractérisant la manière d'injection du message crypté à $V(k)$ avec le signal hyperchaotique $x_m(k)$, α un facteur d'échelle choisi pour que l'expression, $\alpha NV(k)$ appartienne à une gamme compatible avec le respect du minimum et du maximum des variables d'état du système maître et ainsi de préserver le comportement du signal hyperchaotique $V(k)$ [Millerioux et Daafouz., 2003] et $f(x_m(k))$ une fonction vectorielle nonlinéaire de $x_m(k)$.

Le système hyperchaotique maître considéré (3.87) génère le signal de sortie $y_m(k)$ et la clé de cryptage $K(k)$ utilisée n' fois comme un flux de clés pour chiffrer le message d'informations $m(k)$ avec un algorithme de chiffrement $v_c(.)$, nommé "n-shift cipher algorithm" [Fallahi *et al.*, 2008], tels que :

$$\begin{aligned} V(k) &= v_c(m(k), K_c(k)) \\ &= \underbrace{f_1(\ldots f_1(f_1}_{n'}(m(k), \underbrace{K_c(k)), K_c(k)), \ldots, K_c(k))}_{n'} \end{aligned} \tag{3.88}$$

avec :

$$K_c(k) = \sqrt{|x_{m1}(k) + x_{m2}(k) + \ldots + x_{mn}(k)|} \tag{3.89}$$

les $x_{mi}(k)$, $\forall i = 1, \ldots, n$ sont les composants de vecteur x_m.

$f_1(.)$ est une fonction non linéaire définie, dans ce cas, par :

$$f_1(m(k), K_c(k)) = \begin{cases} m(k) + K_c(k) + 2h, \ pour \ : \ -2h \leq m(k) + K_c(k) \leq -h \\ m(k) + K_c(k), \ pour \ : \ -h < m(k) + K_c(k) < h \\ m(k) + K_c(k) - 2h, \ pour \ : \ h \leq m(k) + K_c(k) \leq 2h \end{cases} \tag{3.90}$$

h est un paramètre de cryptage choisi de telle sorte que le message transmis $m(k)$ et la clé $K_c(k)$ se situent dans l'intervalle $[-h, h]$.

Le signal de sortie $y_m \in R$, est envoyé par la voie publique au côté récepteur.

– Le système hyperchaotique esclave, est décrit par :

$$\begin{aligned} x_s(k+1) &= Ax_s(k) + f(x_s(k)) + Bu(k) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{3.91}$$

avec : $B = I_{n \times n}$; tel que $u(k)$ est définie par :

$$u(k) = LV_r(k) \tag{3.92}$$

qui joue le rôle d'une loi de commande par retour de sortie du système d'erreur de la synchronisation :

$$V_r(k) = y_m(k) - y_s(k) \tag{3.93}$$

et agit comme un observateur de type Luenberger à entrées inconnues. En effet, les observateurs à entrées inconnues ont été développés afin d'estimer l'état d'un système en dépit des entrées inconnues non mesurables. Ces dernières apparaissent dans les processus physiques sous la forme d'erreurs de modélisation, d'incertitudes, de défauts, de perturbations, etc.

Cet observateur, de vecteur de gain $L = [l_1 \ \ldots \ l_n]^T$ générant un signal de sortie $y_s(k)$ et la clé $K_d(k)$, est utilisé pour décrypter $V_r(k)$ et ainsi récupérer le message d'informations utilisant l'algorithme de décryptage $v_d(.)$, comme suit :

$$\begin{aligned} m_r(k) &= v_d\left(\alpha^{-1}V_r(k), -K_d(k)\right) = en\left(\alpha^{-1}V_r(k), -K_d(k)\right) \\ &= \underbrace{f_1(\ldots f_1(f_1}_{n'}\left(\alpha^{-1}V_r(k), \underbrace{-K_d(k)), -K_d(k)), \ldots, -K_d(k))}_{n'} \end{aligned} \tag{3.94}$$

avec :

$$K_d(k) = \sqrt{|x_{s1}(k) + x_{s2}(k) + \ldots + x_{sn}(k)|} \tag{3.95}$$

$x_s \in R^n$ et $y_s \in R$ sont respectivement le vecteur d'état et la sortie du système esclave et les $x_{si}(k)$, $\forall i = 1 \ldots n$ sont les composants du vecteur x_s.

Tenant compte du fait que la trajectoire chaotique reste confinée dans un espace délimité [Eckmann et Ruelle, 1985], le problème considéré dans cette section est de concevoir un observateur de Luenberger à entrées inconnues tel que la synchronisation maître et esclave soit satisfaite ; dans ce cas, elle est notée en anglais "Input Independence global synchronization IIGS". Il est a noter qu'il faut faire un choix approprié des gains (n_i, l_i, c_i) pour $i = 1, \ldots, n$, tels que :

$$\lim_{k \to +\infty} \|x_{mi}(k) - x_{si}(k)\| = 0, \ i = 1, 2, \ \ldots \ , n \tag{3.96}$$

Dans la suite, la conception d'un observateur de Luenberger est proposée pour synchroniser (3.87) et (3.91).

En considérant le vecteur d'erreur de synchronisation $e(k)$

$$e(k) = x_m(k) - x_s(k) \tag{3.97}$$

le système erreur entre (3.87) et (3.91) est décrit par :

$$\begin{aligned} e(k+1) = Ae(k) + f(x_m(k)) - f(x_s(k)) + N\alpha V(k) \\ -BL(Cx_m(k) + \alpha V(k) - Cx_s(k)) \end{aligned} \tag{3.98}$$

ou encore par :

$$e(k+1) = (A - BLC)e(k) + \alpha V(k)(N - BL) + f(x_m(k)) - f(x_s(k)) \tag{3.99}$$

Propriété 3.1. *Il est à noter, qu'une condition sur les matrices N et L doit être vérifiée afin d'aboutir à une convergence à entrée indépendante (IIGS). l'approche proposée est de concevoir un système maître/esclave tel que $x_s(k)$ converge vers $x_m(k)$, pour toute valeur de $V(k)$ et pour toutes valeurs initiales $x_s(0)$ et $x_m(0)$, soit :*

$$\lim_{k\to+\infty} \|x_m(k) - x_s(k)\| = 0, \quad \forall(x_s(0), x_m(0)), \quad \forall V(k) \tag{3.100}$$

Lorsque (3.100) *est satisfaite, la convergence est à entrée indépendante.*
Ainsi le système erreur de synchronisation (3.99) *converge vers zéro si*

- *$f(x_m(k)) - f(x_s(k))$ peut être factorisée comme suit [Jiang et al., 2003] :*

$$f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))e(k) \tag{3.101}$$

  $Q(.)$ étant une matrice $(n \times n)$ dépendant de $x_m(k)$ et $x_s(k)$, $Q(.) = \{q_{ij}(.)\}$.
- *N=BL*
- *$(A - BLC + Q(.))$ est stable.*

Dans ce cas, la description du système erreur peut être réécrite sous la forme :

$$e(k+1) = A_f(x_m(k), x_s(k))e(k) \tag{3.102}$$

avec :

$$A_f(x_m(k), x_s(k)) = A - BLC + Q(x_m(k), x_s(k)) \tag{3.103}$$

et : $B = I_{n\times n}$
Les éléments de la matrice $A_f(.) = \{a_{f_{ij}}(.)\}$ étant définis par $a_{f_{ij}}(.) = a_{ij} + q_{ij}(.) + l_i c_j \quad \forall i, j = 1, \ldots, n$
Du point de vue de la théorie du contrôle, la synchronisation des systèmes (3.87) et (3.91) équivaut à la stabilisation du système (3.102) par une rétroaction de loi de commande $u(k)$ comme (3.92).

Pour atteindre cet objectif, nous concevons des conditions garantissant la stabilité asymptotique du système d'erreur (3.102).
Le système majorant $M(A_f(x_m(k), x_s(k)))$, associé à la norme vectorielle suivante [Borne, 1987] :

$$p(z(k)) = [|z_1(k)| \ \dots \ |z_n(k)|]^T \tag{3.104}$$

$z(k) = [z_1(k) \ \dots \ z_n(k)]^T$, est décrit par :

$$z(k+1) = M(A_f(x_m(k), x_s(k)))z(k) \tag{3.105}$$

avec : $M(A_f(x_m(k), x_s(k))) = \{m_{f_{ij}}(.)\}$, $m_{f_{ij}}(.) = |a_{f_{ij}}(.)| \ \forall i, j = 1, \dots, n$.
Les signaux chaotiques sont des signaux bornés délimités d'une façon déterministe [Eckmann et Ruelle, 1985]. Exploitant cette propriété, la matrice $M(A_f(x_m(k), x_s(k)))$ peut être majorée par une $n \times n$ matrice $M_1 = \left\{m^1_{f_{ij}}\right\} \forall i, j = 1, \dots, n$, dont tous les éléments sont constants, positifs et indépendants des variables d'état $x_m(k)$ et $x_s(k)$, des systèmes maître et esclave tels que les inégalités :

$$p(z(k+1)) \leqslant M(A_f(x_m(k), x_s(k)))\, p(z(k)) \leqslant M_1 p(z(k)) \tag{3.106}$$

soient satisfaites.
Le système (3.102) est, alors, stabilisable par (3.92), si la matrice $(I - M_1)$ est une M-matrice, c'est à dire :

$$(I - M_1)\begin{pmatrix} 1 & 2 & \dots & i \\ 1 & 2 & \dots & i \end{pmatrix} > 0 \ \forall i = 1, \dots, n \tag{3.107}$$

Le choix de la forme en flèche mince pour la matrice instantanée rend les conditions de stabilité suffisantes facile à tester. Ainsi, nous allons concevoir la loi de commande $u(k)$, de sorte que la valeur instantanée de la matrice caractéristique majorante du système en boucle fermée M_1 soit de forme en flèche de type 2, comme indiqué dans les références suivantes [Benrejeb et Borne, 1978, Benrejeb *et al.*, 1982, El-Kamel *et al.*, 1999, Benrejeb et Gasmi, 2001b, Benrejeb *et al.*, 2006, Borne *et al.*, 2007, Borne et Benrejeb, 2008, Benrejeb et Hammami, 2008, Benrejeb, 2010] :

$$\begin{cases} e_1(k+1) = \displaystyle\sum_{i=1}^{n-1} m^1_{f_{1i}} e_i(k) + m^1_{f_{1n}} e_n(k) \\ e_i(k+1) = m^1_{f_{ii}} e_i(k) + m^1_{f_{i1}} e_n(k) \quad i = 2, \dots, n \end{cases} \tag{3.108}$$

Le théorème suivant, basé sur l'utilisation du lemme de Kotelyanski [Gentina *et al.*, 1972] associé à la forme canonique spécifique de forme en flèche de Benrejeb M_1 [Benrejeb et Borne, 1978, Benrejeb *et al.*, 1982, El-Kamel *et al.*, 1999, Benrejeb et Gasmi, 2001b, Benrejeb *et al.*, 2006, Borne *et al.*, 2007, Borne et Benrejeb, 2008], donne des conditions suffisantes de synchronisation du système esclave (3.91) avec le système maître (3.87) [Benrejeb et Hammami, 2008, Benrejeb, 2010, Filali *et al.*, 2012a].

Théorème 3.3. *Le vecteur erreur de synchronisation* (3.97) *converge vers zéro, et si le système* (3.102) *est stabilisable par la loi de commande définie par* (3.92) *, si pour le système corrigé* (3.108)*, la matrice* M_1 *sous forme en flèche mince de type 2, et telle que :*

i. Les éléments diagonaux, $m^1_{f_{ii}}$*, de la matrice constante* M_1 *sont tels que :*

$$1 - m^1_{f_{ii}} > 0,\ \forall i = 2, \ldots, n \tag{3.109}$$

ii. Il existe, $\varepsilon > 0$ *tel que :*

$$\Delta = 1 - m^1_{f_{11}} - \sum_{i=2}^{n} \left(m^1_{f_{i1}} m^1_{f_{1i}} \left(1 - m^1_{f_{ii}}\right)^{-1} \right) > \varepsilon \tag{3.110}$$

Démonstration. Le système erreur, décrit par (3.97) , est stabilisable par la commande par retour de sortie (3.92), si nous faisons un choix approprié des gains de l'observateur L tel que la matrice $(I - M_1)$ soit une M - matrice [Robert, 1964], c'est-à-dire :

$$\begin{cases} 1 - m^1_{f_{ii}} > 0,\ \forall i = 2, \ldots, n \\ det(I - M_1) > \varepsilon \end{cases} \tag{3.111}$$

Le calcul du premier membre de la dernière inégalité conduit à l'expression suivante :

$$\det\left(I - M_1\right) = \Delta \prod_{j=2}^{n} \left(1 - m^1_{f_{jj}}\right) \tag{3.112}$$

et permet d'achever facilement la preuve du théorème. □

3.5.2 Cas de clés identiques utilisant deux systèmes hyperchaotiques de Hénon

Dans cette partie, le système hyperchaotique discret choisi est le système de Hénon généralisé (Baier-Klein) décrit par :

$$\begin{cases} x_{m1}(k+1) = \mu - x_{m2}^2(k) - bx_{m3}(k) \\ x_{m2}(k+1) = x_{m1}(k) \\ x_{m3}(k+1) = x_{m2}(k) \end{cases} \tag{3.113}$$

Remarque 3.2. *L'attracteur hyperchaotique du système* (3.113) *caractérisé par :* $b = 0.1$ *et* $\mu = 1.76$*, avec les conditions initiales* $x_m(0) = (1, 0.1, 0)$ *[Grassi et Miller, 2002] montre, dans la figure* 3.5.22*, que les variables d'état* $x_{mi}(k)$ *sont bornées [Eckmann et Ruelle, 1985] :* $|x_{mi}| < 2 \; \forall i = 1, 2, 3$

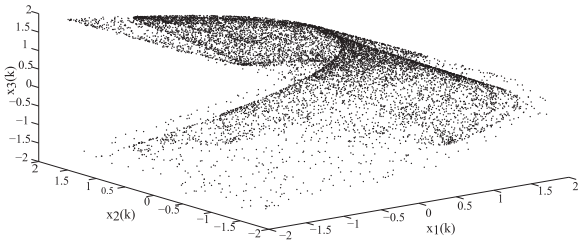


FIGURE 3.5.22 – L'attracteur hyperchaotique de Hénon généralisé d'ordre 3.

Considérons les systèmes hyperchaotiques maître et esclave de Hénon suivants [Baier et Klein, 1990, Grassi et Miller, 2002] :

– le système maître :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + \alpha NV(k) \\ y_m(k) &= Cx_m(k) + \alpha V(k) \end{aligned} \tag{3.114}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{3.115}$$

et :

$$f(x_m(k)) = [-x_{m2}^2(k) \quad 0 \quad 0]^T \tag{3.116}$$

– le système esclave :

$$\begin{aligned} x_s(k+1) &= Ax_s(k) + f(x_s(k)) + L(y_m(k) - y_s(k)) \\ y_s(k) &= Cx_s(k) \end{aligned} \tag{3.117}$$

$L = [l_1\ l_2\ l_3]^T$, ou les l_i sont les gains de l'observateur, et :

$$f(x_s(k)) = [-x_{s2}^2(k) \quad 0 \quad 0]^T \tag{3.118}$$

Considérons l'erreur de synchronisation $e(k)$, entre les systèmes (3.114) et (3.117) :

$$e_i(k) = x_{mi}(k) - x_{si}(k),\ \forall i = 1, 2, 3 \tag{3.119}$$

Considérant que l'expression de : $f(x_m(k)) - f(x_s(k))$ peut être facilement factorisée pour le système hyperchaotique de Hénon généralisé, telle que :
$f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))\, e(k)$

$$Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -x_{m2}(k) - x_{s2}(k) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{3.120}$$

la matrice définie par (3.103) du système erreur devient :

$$A_f(x_m(k), x_s(k)) = \begin{bmatrix} -l_1c_1 & -x_{m2}(k) - x_{s2}(k) - l_1c_2 & -0.1 - l_1c_3 \\ 1 - l_2c_1 & -l_2c_2 & -l_2c_3 \\ -l_3c_1 & 1 - l_3c_2 & -l_3c_3 \end{bmatrix} \tag{3.121}$$

Par l'utilisation de la norme vectorielle (3.104), le système majorant est caractérisé par la matrice $M(A_f(x_m(k), x_s(k)))$ suivante :

$$M(A_f(x_m(k), x_s(k))) = \begin{bmatrix} |l_1c_1| & |-x_{m2}(k) - x_{s2}(k) - l_1c_2| & |-0.1 - l_1c_3| \\ |1 - l_2c_1| & |l_2c_2| & |l_2c_3| \\ |l_3c_1| & |1 - l_3c_2| & |l_3c_3| \end{bmatrix} \tag{3.122}$$

Comme il est noté dans la Remarque 3.1, les variables d'état des systèmes maître et esclave sont bornées comme le montre l'inégalité suivante : $|\ x_{m2}\ | < 2$ et $|\ x_{s2}\ | < 2$; ainsi nous avons :

$| x_{m2} + x_{s2} + l_1 c_2 | < 4 + | l_1 c_2 |$

Il s'agit d'un nouveau système majorant caractérisé par la matrice constante M_1 définie par :

$$M_1 = \begin{bmatrix} |l_1 c_1| & 4 + |l_1 c_2| & | - 0.1 - l_1 c_3| \\ |1 - l_2 c_1| & |l_2 c_2| & |l_2 c_3| \\ |l_3 c_1| & |1 - l_3 c_2| & |l_3 c_3| \end{bmatrix} \tag{3.123}$$

Le choix suivant des paramètres constants l_2, l_3, c_2 et c_3 :

$$\begin{cases} l_2 c_3 = 0 \\ 1 - l_3 c_2 = 0 \end{cases} \textit{ ou encore } : \begin{cases} c_3 = 0 \\ l_3 = \frac{1}{c_2} \end{cases} \tag{3.124}$$

rend la matrice (3.123) de forme en flèche mince.

En utilisant le théorème 3.2, les conditions (3.109) et (3.110) deviennent :

$$\begin{cases} 1 - |l_3 c_3| > 0 \\ 1 - |l_2 c_2| > 0 \\ 1 - |l_1 c_1| - \dfrac{(4 + |l_1 c_2|)\,(|1 - l_2 c_1|)}{1 - |l_2 c_2|} - \dfrac{|l_3 c_1|\,|-0.1 - l_1 c_3|}{1 - |l_3 c_3|} \geq \varepsilon > 0 \end{cases} \tag{3.125}$$

ou encore en utilisant (3.124) :

$$\begin{cases} 1 - |l_2 c_2| > 0 \\ 1 - |l_1 c_1| - \dfrac{(4 + |l_1 c_2|)\,(|1 - l_2 c_1|)}{1 - |l_2 c_2|} - \left|\dfrac{0.1 c_1}{c_2}\right| \geq \varepsilon > 0 \end{cases} \tag{3.126}$$

Parmi les gains possibles des matrices L et C, nous avons choisi les valeurs suivantes :

$$C = [1.73 \quad 0.91 \quad 0] \tag{3.127}$$

$$L = [-0.20 \quad 0.55 \quad 1.10]^T \tag{3.128}$$

qui sont utilisées dans la prochaine section, pour tester le schéma de communication choisi. Afin de montrer l'efficacité de la méthode proposée pour la conception de l'observateur à entrées inconnues, différentes simulations numériques sont présentées dans cette section. Dans ce qui suit, la synchronisation des systèmes maître / esclave de type Hénon, basée sur les techniques d'agrégation, est appliquée en utilisant les gains L et C donnés en (3.128) et (3.127) pour les conditions initiales du système maître (3.114) et esclave (3.117) : $(x_m(0), x_s(0)) = ((1, 0.1, 0), (-0.5, 0, 0.3))$ et pour une période d'échantillonnage T égale à $0.1s$.

Les figures 3.5.23 et 3.5.24 illustrent bien l'efficacité de la méthode proposée qui repose sur l'utilisation des techniques d'agrégation associées à la matrice de forme en flèche de Benrejeb pour la description du système ; on peut observer que $e_1(k)$, $e_2(k)$ et $e_3(k)$ convergent vers zéro respectivement après 6, 7 et 7 itérations.

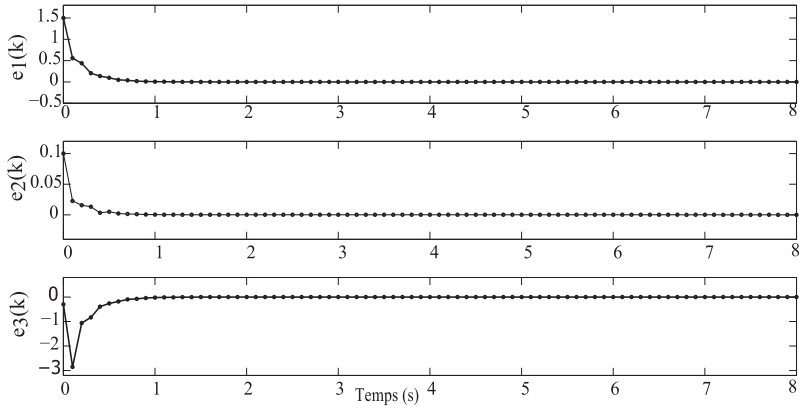


FIGURE 3.5.23 – Dynamiques de l'erreur du système de troisième ordre de Hénon généralisé lorsque la commande est activée.

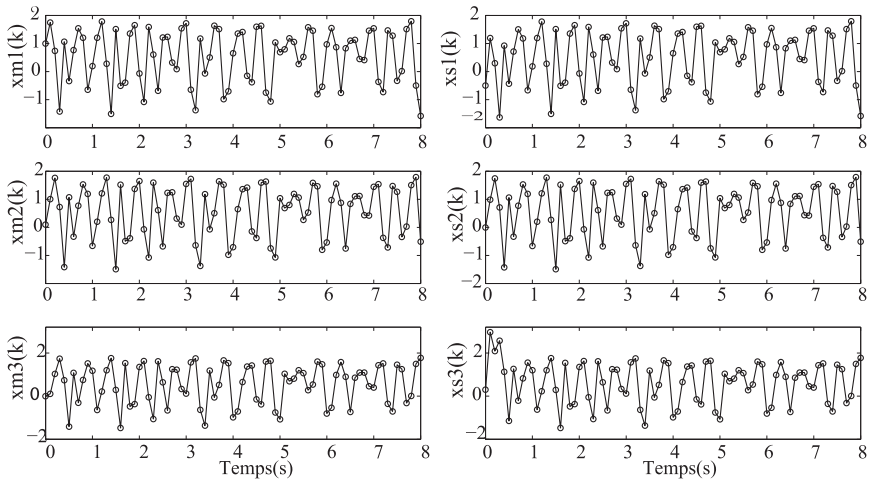


FIGURE 3.5.24 – Evolutions temporelles des variables d'état des systèmes maître et esclave lorsque la commande est activée

Pour les paramètres de chiffrement $h = 2$, $\alpha = 0.01$, $n = 5$ et la période d'échantillonnage $T = 0.1s$, le signal hyperchaotique de l'émetteur incluant le message d'informations $m(k)$, tels que $m(k) = sin(0.1k)$, est envoyé au récepteur et le signal $m_r(k)$ est récupéré approximativement par l'observateur proposé comme le montre les figures 3.5.25(a) et 3.5.25(b). $y_m(k)$, qui est envoyé dans le canal public entre l'émetteur et le récepteur, est indiqué

dans la figure. 3.5.25(e) et les clés de cryptage et décryptage, respectivement dans les figures 3.5.25(c) et 3.5.25(d).

On peut observer que, lorsque les systèmes maître et esclave sont synchronisés c'est à dire $x_s(k) \to x_m(k)$, il s'ensuit $K_d(k) \to K_c(k)$, $V_r(k) \to V(k)$ lorsque $k \to +\infty$,

Pour éviter la déformation de la récupération du message $m_r(k)$, en régime transitoire, la solution serait d'envoyer le message $m(k)$ avec un certain retard à calculer. Le système de transmission sécurisée aussi décrit est testé sur deux types de messages, à savoir une image, et un texte.

Prenons, maintenant, le message d'informations, précédemment utilisé dans le cas du cryptage utilisant deux voix de transmission.

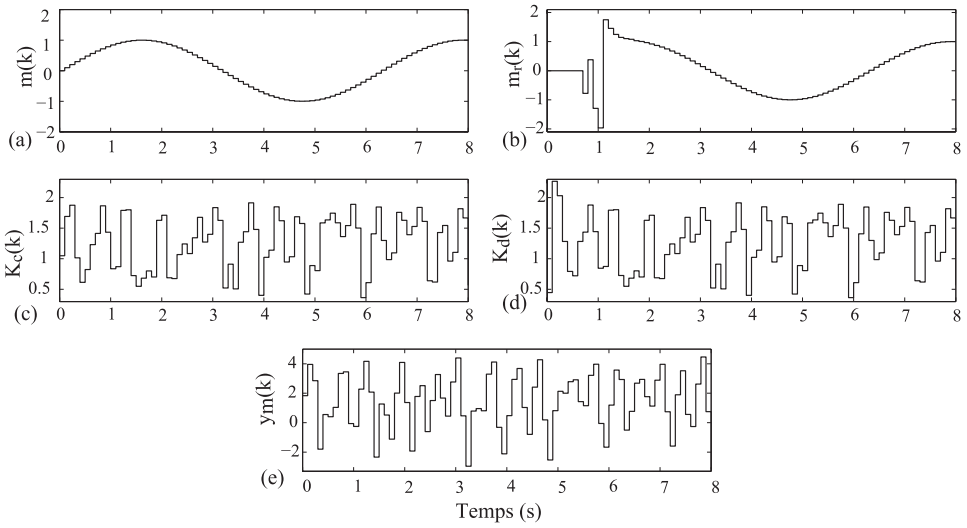


FIGURE 3.5.25 – Exemple d'un système de cryptage chaotique utilisant le système de troisième ordre de Hénon généralisé. Cas d'un message de type sinusoïde

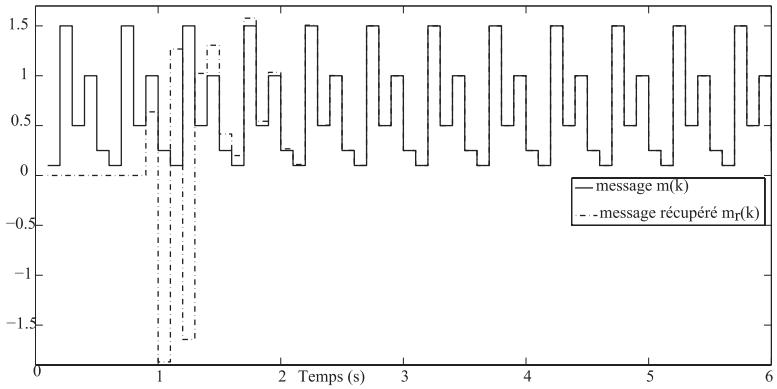


FIGURE 3.5.26 – Message original $m(k)$ (—) et message récupéré $m_r(k)(- \cdot -)$

En comparant les figures (3.5.26) et (3.4.9), nous pouvons conclure que le système de cryptage utilisant deux voies de transmission réalise une synchronisation plus rapide que le cryptage mixte tel qu'il est dit dans [Jiang, 2002]. Cependant, le cryptage à deux voies de transmission utilise deux canaux de transmission au lieu de un.

3.5.2.1 Mise en oeuvre dans le cas de la transmission d'une image

L'image originale, prise dans cette étude, est la photographie de Lena déjà présentée dans la figure 3.4.14. A partir de cette image, définie par une matrice, on génère un signal à une dimension. les images cryptées et reconstruites sont présentées respectivement dans les figures 3.5.27 (a) et (b). Les clés de cryptage et décryptage sont définies par

$$K_c(k) = \left(A\sqrt{\left(x_{m1}^4(k) + x_{m2}^4(k) + x_{m3}^4(k)\right)} \right) \bmod (256) \tag{3.129}$$

$$K_d(k) = \left(A\sqrt{\left(x_{s1}^4(k) + x_{s2}^4(k) + x_{s3}^4(k)\right)} \right) \bmod (256) \tag{3.130}$$

et les fonctions de cryptage et décryptage par :

$$V(k) = m(k) \oplus K_c(k) \tag{3.131}$$

$$m_r(k) = V(k) \oplus K_d(k) \tag{3.132}$$

(i) Image transmise (ii) Image reconstruite

FIGURE 3.5.27 – Reconstruction de l'image de Lena dans le cryptage mixte

D'après la figure 3.5.27 (ii) les premiers points à gauche, en haut de l'image reconstruite présentent des erreurs.
Il est à noter qu'on a eu recours à ajouter un facteur d'échelle afin que le signal reste dans

la plage $\alpha = 10^{-5}$ afin de préserver le comportement chaotique de la clé de cryptage et de décryptage la constante A de la clé de cryptage étant prise égale à 100.

3.5.2.2 Mise en oeuvre dans le cas de la transmission d'un texte

Les paramètres de simulation, précédemment indiqués, sont conservés. Le texte à transmettre est consigné dans la figure 3.5.28 (a). A l'aide du code ASCII, on génère un vecteur dont les composantes sont des entiers compris entre 0 et 255. On applique le processus de cryptage et on obtient le texte crypté comme le montre la figure 3.5.28 (b) ; en appliquant le processus inverse en utilisant de nouveau le code ASCII, on obtient le texte décrypté tel qu'on le voit dans la figure 3.5.28 (c). On peut ajouter un texte vide au début d'une longueur à déterminer pour obtenir une reconstitution du texte parfaite.

(a)
Stabilization conditions are proposed for hyperchaotic discrete-time systems synchronization. They are based on the use of an observer and of the aggregation techniques.
(b)
(c)
Stabilization conditions are proposed for hyperchaotic discrete-time systems synchronization. They are based on the use of an observer and of the aggregation techniques.

FIGURE 3.5.28 – (a) : Texte original, (b) : Texte correspondant au signal transmis, (c) : Texte décrypté

3.5.3 Cas de clés non identiques utilisant un système de Rössler couplé avec le système de Hénon généralisé

Dans cette partie, on va appliquer la synchronisation de deux systèmes non identiques à base d'observateurs, les systèmes hyperchaotiques discrets choisis étant :

– le système de Hénon généralisé considéré comme système maître, qui est considéré décrit par [Baier et Klein, 1990, Grassi et Miller, 2002] :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E + \alpha NV(k) \\ y_m(k) &= Cx_m(k) + \alpha V(k) \end{aligned} \tag{3.133}$$

avec :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{3.134}$$

$$E = \begin{bmatrix} 1.76 & 0 & 0 \end{bmatrix}^T \tag{3.135}$$

et :

$$f(x_m(k)) = [-x_{m2}^2(k) \quad 0 \quad 0]^T \tag{3.136}$$

– le système de Rössler considéré comme système esclave décrit par [Baier et Klein, 1990, Grassi et Miller, 2002] :

$$\begin{aligned} x_s(k+1) &= A_1 x_s(k) + f_1(x_s(k)) + E_1 + u(k) \\ y_s(k) &= C x_s(k) \end{aligned} \tag{3.137}$$

tel que :

$$u(k) = (A(x_s(k)) - A_1(x_s(k)))\, x_s(k) - E_1 + E + L(y_m(k) - y_s(k)) \tag{3.138}$$

$L = [l_1\ l_2\ l_3]^T$ et les l_i étant les gains de l'observateur de Luenberger,
avec :

$$A_1 = \begin{bmatrix} 3.8 & 0.035 & -0.05 \\ 0 & 3.78 & 0.2 \\ 0.1235 & -0.07 & 0.1 \end{bmatrix} \tag{3.139}$$

et :

$$E_1 = \begin{bmatrix} -0.0175 & 0 & -0.065 \end{bmatrix}^T \tag{3.140}$$

$$f_1(x_s(k)) = [f_{1_1} \quad f_{1_2} \quad f_{1_3}]^T \tag{3.141}$$

et :
$f_{1_1} = -3.8x_{s1}^2(k) + 0.1x_{s2}(k)\, x_{s3}(k)$
$f_{1_2} = -3.78x_{s2}^2(k)$
$f_{1_3} = -0.19(1 - 2x_{s2}(k))\, x_{s3}(k)\, .x_{s1}(k) + 0.133x_{s2}(k)\, .x_{s1}(k) + 0.2x_{s3}(k)\, .x_{s2}(k)$
Considérons l'erreur de synchronisation $e(k)$, entre les systèmes (3.133) et (3.137) :

$$e_i(k) = x_{mi}(k) - x_{si}(k),\ \forall i = 1, 2, 3 \tag{3.142}$$

Avec le choix de $u(k)$ défini en (3.138), on obtient :

$$\begin{cases} u_1(k) = -3.8x_{s1}(k)(1 - x_{s1}(k)) - (x_{s2}(k) + 0.035)\, x_{s2}(k) \\ \qquad - (0.1 - 0.05(1 - 2x_{s2}(k)))\, x_{s3}(k) + 1.7775 + l_1(y_m(k) - y_s(k)) \\ u_2(k) = x_{s1}(k) - (3.78(1 - x_{s2}(k)))\, x_{s2}(k) - 0.2x_{s3}(k) + l_2(y_m(k) - y_s(k)) \\ u_3(k) = 0.19((x_{s3}(k) + 0.35)(1 - 2x_{s2}(k)) - 1)\, x_{s1}(k) \\ \qquad +1.07x_{s2}(k) - 0.1(1 - 2x_{s2}(k))\, x_{s3}(k) + 0.065 + l_3(y_m(k) - y_s(k)) \end{cases} \tag{3.143}$$

Nous ramènons ici aussi l'étude de la synchronisation des systèmes non identiques Rössler et Hénon généralisé à l'étude de synchronisation de deux systèmes de Hénon généralisé (Baier-Klein).
Pour $B = I_{3\times 3}$, considérons vient le système erreur suivant :

$$e(k+1) = (A - BL(.)C(.) + Q(.))e(k) \tag{3.144}$$

lorsque $f(x_m(k)) - f(x_s(k))$ est factorisée comme c'est le cas pour certains cas de systèmes hyperchaotiques tels que les systèmes de troisième ordre Hénon généralisé (Baier-Klein), tell que :
$f(x_m(k)) - f(x_s(k)) = Q(x_m(k), x_s(k))e(k)$

$$avec : Q(x_m(k), x_s(k)) = \begin{bmatrix} 0 & -x_{m2}(k) - x_{s2}(k) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{3.145}$$

Il vient la matrice suivante (3.103) du système erreur :

$$A_f(x_m(k), x_s(k)) = \begin{bmatrix} -l_1c_1 & -x_{m2}(k) - x_{s2}(k) - l_1c_2 & -0.1 - l_1c_3 \\ 1 - l_2c_1 & -l_2c_2 & -l_2c_3 \\ -l_3c_1 & 1 - l_3c_2 & -l_3c_3 \end{bmatrix} \tag{3.146}$$

dont l'étude de stabilisation a été déjà faite dans la section précédente dans laquelle les valeurs des gains choisis pour L et C sont :

$$C = [1.73 \quad 0.91 \quad 0] \tag{3.147}$$

$$L = [-0.20 \quad 0.55 \quad 1.10]^T \tag{3.148}$$

D'après la figure (3.5.29), nous pouvons conclure à la synchronisation maître esclave dans le cas de synchronisation de deux systèmes non identiques utilisés dans le cryptage mixte.

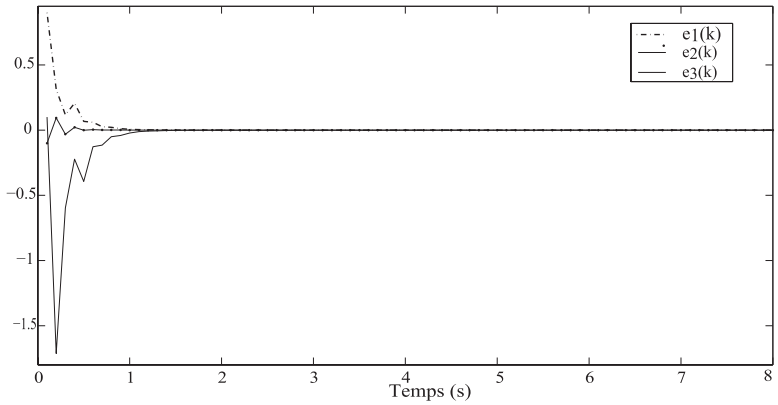


FIGURE 3.5.29 – Dynamiques de l'erreur du système de troisième ordre de Hénon généralisé lorsque la commande est activée.

Les figures 3.5.29 et 3.5.30 montre qu'il y a synchronisation du système maître / esclave. Ainsi la clé de cryptage est égale à la clé de décryptage après quelques itérations. Comme le montre la figure 3.5.31, pour des clés de cryptage et décryptage générées par des signaux hyperchaotiques différents, le message d'informations récupéré est identique au message original au bout d'un certains temps.

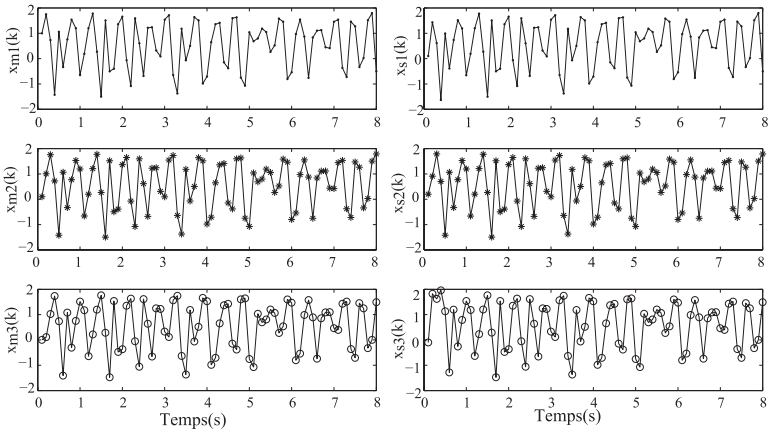


FIGURE 3.5.30 – Evolutions temporelles des variables d'état des systèmes maître et esclave lorsque la commande est activée

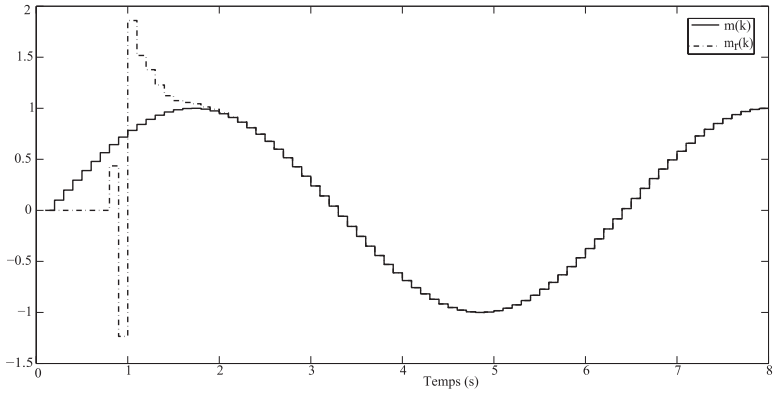


FIGURE 3.5.31 – Message d'informations original $m(k)$ (—) et message récupéré $m_r(k)(--)$

3.6 Cas de la robustesse du système au bruit du canal de transmission

3.6.1 Position du problème

La robustesse au bruit est un critère à prendre en compte dans les systèmes de communication sécurisés. Il s'agit ainsi de reconstruire l'état du système esclave malgré la présence de bruits. La synchronisation de l'observateur ne peut donc pas se faire de façon parfaite. Plusieurs approches ont été proposées pour étudier la robustesse au bruit, telles que la commande H_∞ [Suykens *et al.*, 1997]. Notre travail, consiste donc à trouver un gain de l'observateur et un gain d'un vecteur de sortie garantissant une borne supérieure sur l'erreur d'estimation relativement faible en utilisant la technique des normes vectorielles [Borne *et al.*, 2007, Borne *et al.*, 2013]. Pour cela, nous allons considérer un système de cryptage utilisant deux voies de transmission (3.4.8) utilisant des systèmes hyperchaotiques identiques.
Prenons le cas du système maître décrit dans l'espace d'état par :

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + E \\ y_m(k) &= Cx_m(k) + n(k) \end{aligned} \tag{3.149}$$

$x_m(k) \in R^n$, $y_m(k) \in R$ représentent respectivement, le vecteur d'état et le vecteur de sortie du système maître et $n(k) \in R$ est un bruit à énergie bornée.
Comme on l'a déjà mentionné, $f(x_m(k))$ est une fonction non linéaire discrète factorisable

telle que :

$$f\left(x_m\left(k\right)\right) - f\left(x_s\left(k\right)\right) = Q\left(x_m\left(k\right), x_s\left(k\right)\right)\left(x_m\left(k\right) - x_s\left(k\right)\right) \tag{3.150}$$

$Q\left(x_m\left(k\right), x_s\left(k\right)\right)$ étant une matrice bornée dépendant des variables $x_m\left(k\right)$ et $x_s\left(k\right)$. Avec la synthèse d'un observateur comme décrit précédemment, le système esclave peut être construit comme suit :

$$\begin{aligned} x_s\left(k+1\right) &= Ax_s\left(k\right) + f\left(x_s\left(k\right)\right) + E + Bu\left(k\right) \\ y_s\left(k\right) &= Cx_s\left(k\right) \end{aligned} \tag{3.151}$$

$B = I_{n\times n}$, pour la loi de commande suivante :

$$u\left(k\right) = -L(.)(y_s\left(k\right) - y_m\left(k\right)) \tag{3.152}$$

joue le rôle d'une rétroaction de sortie, $L = [l_1, l_2, \ldots, l_n]^T$ étant le gain de l'observateur à déterminer.
Le vecteur erreur :

$$e\left(k\right) = x_m\left(k\right) - x_s\left(k\right) \tag{3.153}$$

a son évolution décrite par l'équation :

$$\begin{aligned} e\left(k+1\right) &= Ae\left(k\right) + Bu\left(k\right) + f\left(x_m\left(k\right)\right) - f\left(x_s\left(k\right)\right) \\ &= \left(A - BL\left(.\right)C\right)e\left(k\right) + f\left(x_m\left(k\right)\right) - f\left(x_s\left(k\right)\right) - BLn\left(k\right) \\ &= \left(A - L\left(.\right)C\right)e\left(k\right) + f\left(x_m\left(k\right)\right) - f\left(x_s\left(k\right)\right) - Ln\left(k\right) \end{aligned} \tag{3.154}$$

ou encore par :

$$e\left(k+1\right) = \left(A - BLC + Q\left(x_m\left(k\right), x_s\left(k\right)\right)\right)e\left(k\right) - Ln\left(k\right) \tag{3.155}$$

$$e\left(k+1\right) = A_f\left(x_m\left(k\right), x_s\left(k\right)\right)e\left(k\right) - Ln\left(k\right) \tag{3.156}$$

Dans ce qui suit, nous allons considérer la dynamique du système (3.156) directement. Si ce système est stable, cela signifie que le système esclave est synchronisé avec le système maître.
Notons que le signal bruit $n\left(k\right)$ est un bruit à énergie bornée, tels que $\left|n\left(k\right)\right| \leq n_{max}$, n_{max} étant positif. Nous supposons ainsi :

si $n\left(k\right) = 0$, le système erreur (3.156) est asymptotiquement stable, si la matrice $A_f\left(x_m\left(k\right), x_s\left(k\right)\right)$, est sous forme en flèche mince et ainsi les gains L et C doivent être choisis tels que les conditions i) et ii) du Théorème 3.3. soient satisfaites.

si $n(k) \neq 0$ afin de pouvoir minimiser l'effet du bruit, l'amélioration des propriétés de stabilité est requise. Ainsi dans cette section, l'étude de la robustesse de l'approche de synchronisation proposée par rapport au bruit, est basée sur l'étude de stabilité des systèmes non linéaires par le calcul des systèmes majorants.

Dans le cas où le système de comparaison est de la forme (3.106) il vient :

$$z(k+1) = M_1 z(k) + N \tag{3.157}$$

N étant un vecteur constant positif tel que $N = [|l_1 n_{\max} n_{max}|, |l_2 n_{\max}|, \ldots, |l_n n_{\max}|]^T$ et $M_1 = \left\{m^1_{f_{ij}}\right\} \forall i,j = 1,\ldots,n$, une matrice constante majorante de la matrice $M(A_f(x_m(k), x_s(k))) = \left\{m_{f_{ij}}(.)\right\}$ telle que $m_{f_{ij}}(.) = \left|a_{f_{ij}}(.)\right| \ \forall i,j = 1,\ldots,n$.

Si $I - M_1$ est une M-matrice, le système en (z) atteint ainsi son régime permanent ; il vient dans e cas :

$$\lim_{k\to\infty} z(k) = cste \tag{3.158}$$

et :

$$z(k) = M_1(k) z(k) + N \tag{3.159}$$

Ainsi, on a :

$$z(k) \to (I - M_1)^{-1} N \quad quand \quad k \to +\infty \tag{3.160}$$

Le problème de minimisation de bruit à résoudre peut donc s'énoncer de la manière suivante : trouver un gain L de l'observateur (3.151) et trouver un gain C du vecteur de sortie afin de minimiser $\|(I - M_1)^{-1} N\|$ tout en satisfaisant les conditions (i) et (ii) du théorème 3.3 pour que la matrice M_1 soit stable. Nous proposons une solution à ce problème sous la forme de la propriété suivante.

Propriété 3.2. *S'il existe un gain L, et C tels :*

- *M_1 est stable en utilisant le théorème 3.3*
- $\min\limits_{L,C} \|(I - M_1)^{-1} N\|$

$\left\|(I - M)^{-1} N\right\| \leq \left\|(I - M)^{-1}\right\| . \|N\|$, *il suffit, que les modules des valeurs propres de M_1, qui sont dans le disque unité, soient les plus faibles possibles. Le problème devient un problème de placement de pôles.*

3.6.2 Cas d'un cryptage utilisant deux voies de transmission utilisant deux clés identiques de Hénon

Dans le cas de deux systèmes hyperchaotiques de type Hénon généralisé (Baier-Klein), les systèmes (3.149) (3.151), sont caractérisés par :

$$A = \begin{bmatrix} 0 & 0 & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{3.161}$$

et :

$$f(x_m(k)) = [-x_{m2}^2(k) \quad 0 \quad 0]^T \tag{3.162}$$

$$f(x_s(k)) = [-x_{s2}^2(k) \quad 0 \quad 0]^T \tag{3.163}$$

$L = [l_1\ l_2\ l_3]^T$, gain de l'observateur et $n(k)$ bruit à énergie bornée de variance donnée et de moyenne nulle, figures 3.6.32 et 3.6.34

Le problème revient à minimiser $\|(I - M_1)^{-1}N\|$ c'est-à-dire à choisir les valeurs propres de M_1 les plus faibles possibles, pour la matrice majorante M_1 établie précédemment dans (3.123) :

$$M_1 = \begin{bmatrix} |l_1c_1| & 4 + |l_1c_2| & |-0.1 - l_1c_3| \\ |1 - l_2c_1| & |l_2c_2| & |l_2c_3| \\ |l_3c_1| & |1 - l_3c_2| & |l_3c_3| \end{bmatrix} \tag{3.164}$$

Nous choisissons les gains l_3 et c_3 comme suit :

$$\begin{aligned} l_3 &= \tfrac{1}{c_2} \\ c_3 &= 0 \end{aligned} \tag{3.165}$$

Ce qui rend la matrice (3.164) de forme en flèche mince.

En utilisant le théorème 3.3, les conditions (3.109) et (3.110) deviennent :

$$\begin{cases} 1 - |l_2c_2| > 0 \\ 1 - |l_1c_1| - \dfrac{(4 + |l_1c_2|)(|1 - l_2c_1|)}{1 - |l_2c_2|} - \left|\dfrac{0.1c_1}{c_2}\right| > 0 \end{cases} \tag{3.166}$$

Afin de minimiser l'effet du bruit, notre objectif consiste à minimiser les modules des valeurs propres de M_1 Tableau (3.2) de façon à ce que les contraintes (3.166) soient vérifiées. Dans le Tableau (3.2), nous proposons de comparer deux commandes 1 et 2 avec différentes valeurs de L et C.

TABLE 3.2 – Minimisation des valeurs propres de M_1

	valeurs propres de M_1	L	C
1	$\lambda_1 = 0.4253$, $\lambda_2 = 0.0428$ et $\lambda_3 = -0.0266$	L=[0.0001 0.4724 0.4921]	C=[2.1348 2.0321 0]
2	$\lambda_1 = -0.4264$, $\lambda_2 = 0.9997$ et $\lambda_3 = 0.2483$	L=[-0.15009 0.6080 1.0850]	C=[1.7407 0.9217 0]

D'après les figures. 3.6.33 et 3.6.35, nous pouvons conclure, que les messages récupérés dans les figures 3.6.33 et 3.6.35.(i) présentent moins de distorsion et de débordement que les messages dans les figures 3.6.33 et 3.6.35.(ii). Cela montre bien qu'en dépit de l'obtention de la stabilité, le fait de minimiser les modules des valeurs propres de la matrice M_1 permet de réduire l'effet du bruit. Nous pouvons aussi conclure que, plus ce rapport SNR est grand, moins le bruit perturbe le signal original.

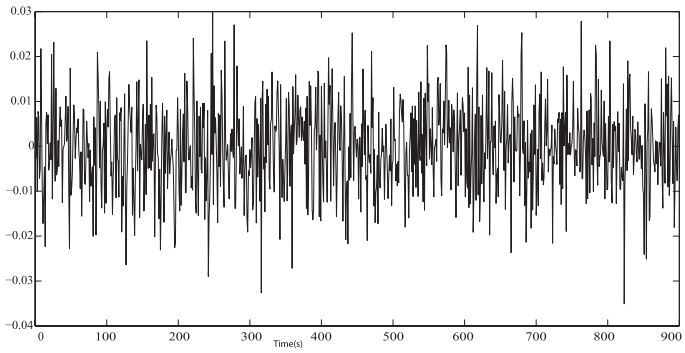


FIGURE 3.6.32 – Bruit gaussian de variance = 0.0001.

(i) Photo récupérée de Lena relative à la commande 1

(ii) Photo récupérée de Lena relative à la commande 2

FIGURE 3.6.33 – Transmission à deux voies de transmission dans le cas d'un bruit additif de variance = 0.0001 et $SNR = 46dB$

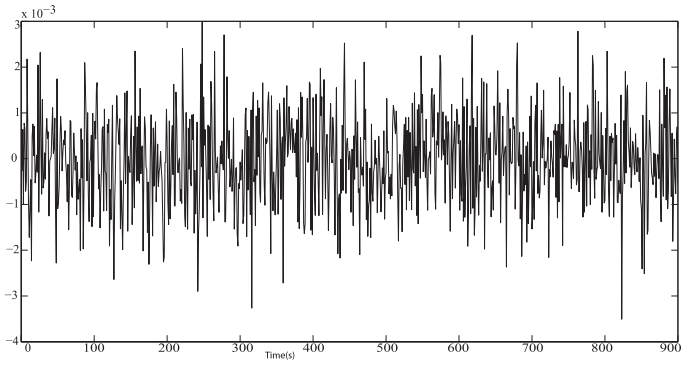


FIGURE 3.6.34 – Bruit gaussian de variance = 0.000001.

(i) Photo récupéré de Lena relative à la commande 1

(ii) Photo récupéré de Lena relative à la commande 2

FIGURE 3.6.35 – Transmission à deux voies de transmission de variance = 0.000001 et $SNR = 66dB$

3.7 Quelques points de sécurité. Analyse de la sécurité : confusion et diffusion

Les systèmes de communication proposés aux paragraphes précédents comportent deux étapes distinctes, à savoir une étape de synchronisation et une étape de transmission de l'information. Il reste maintenant à examiner le point de vue de la sécurité du processus de synchronisation. En effet, ce choix repose sur le choix de l'émetteur chaotique. Il consiste à choisir comme émetteur un système comportant un retard ou un système hyperchaotique, cette dernière solution étant celle que nous avons retenue.
Il est à signaler que les techniques de cryptaanalyse dans les systèmes de communica-

tions chaotiques choisis ne sont pas considérées dans ce manuscrit. Nous n'allons étudier que quelques points de sécurité du processus de transmission de données proposé. Cette analyse reposera sur l'analyse des propriétés de confusion et diffusion qui permettent de quantifier la sécurité de la clé.
En 1949, Shannon a identifié des propriétés fondamentales de confusion et diffusion, que doit posséder tout cryptosystème fiable [Shannon, 1949].

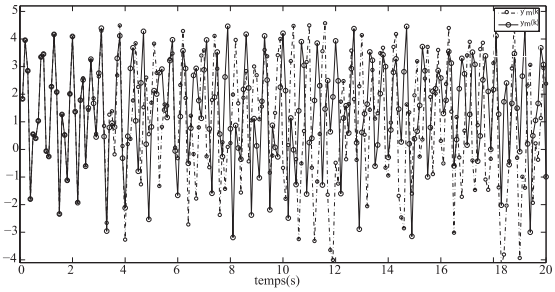
- L'objectif de la confusion est de masquer toute relation existante entre le message clair à transmettre, le message crypté et la clé de cryptage.
- L'objectif de la diffusion est de répartir les effets conjugués du message clair à transmettre et de la clé de cryptage sur la plus grande longueur possible de message crypté.

Nous nous proposons dans cette section, de tester la sécurité, c'est-à-dire confusion et diffusion de notre cryptosystème.

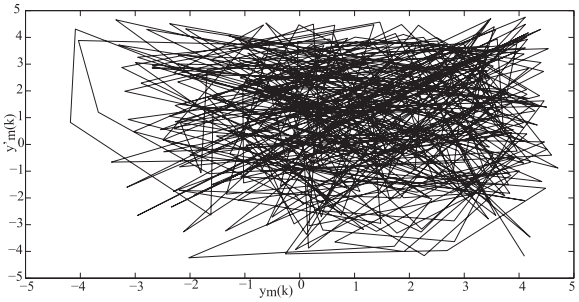
3.7.1 Propriété de diffusion

Dans cette partie, nous nous proposons de montrer que les cryptosystèmes à savoir (cryptosystème mixte ou cryptosystème utilisant deux voies de transmission) que nous proposons possèdent la propriété de diffusion. Cette propriété s'énonce comme suit : deux clés aussi proches que possible dans l'espace des clés, ou deux messages d'informations clairs très peu différents produisent des signaux cryptés complètement différents. Nous allons par la suite, réaliser une simulation où on transmet deux fois le même message, dans un système de communication sécurisé qui réalise le cryptage grâce à deux clés très peu différentes. La première clé $b = 1.76$ correspond au signal crypté $y_m(k)$ et $V(k)$ dans le cas respectivement, de cryptage mixte et de cryptage à deux voies de transmission, et la seconde clé $b = 1,7601$ au signal crypté $y'_m(k)$ et $V'(k)$ dans les cas respectives, de cryptage mixte et de cryptage à deux voies de transmission. Les figures 3.7.36(i) et 3.7.37(i) représentent, respectivement, les deux signaux cryptés $y_m(k)$ et $y'_m(k)$ et les deux signaux cryptés $V(k)$ et $V'(k)$. Puis on trace, le premier signal envoyé en fonction du second. Les figures 3.7.36(ii) et 3.7.37(ii) montrent la courbe ainsi générée. Opérant avec le même message d'informations, les signaux cryptés générés avec deux clés très peu différentes (l'écart étant de 10^{-4}) sont complètement différents. Cette différence est due à la sensibilité de la clé. En effet, en effectuant la simulation précédente avec des conditions initiales identiques pour la transmission du message d'informations, on obtient des figures analogues aux figures 3.7.36(i), 3.7.36(ii), 3.7.37(i) et 3.7.37(ii). Il est à noter aussi, que la propriété de diffusion se confirme également à l'aide de deux messages très peu

différents. Dans ce cas, la diffusion s'appuie sur la sensibilité aux conditions initiales. Plus exactement, si on préserve les mêmes conditions initiales et deux messages très proches, les signaux cryptés sont très proches.

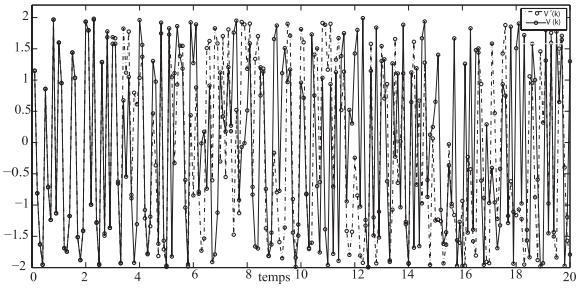


(i) Signaux cryptés correspondant à des clés différentes de 10^{-4}

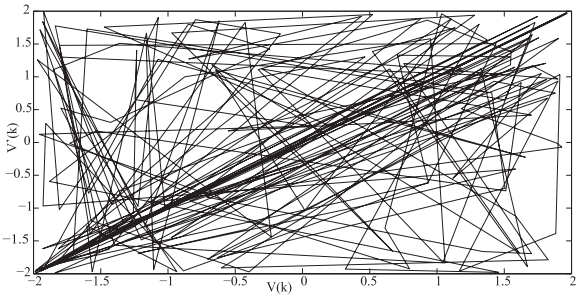


(ii) $y'_m(k)$ en fonction de $y_m(k)$

FIGURE 3.7.36 – Test de diffusion pour le cas d'un cryptage mixte



(i) Signaux cryptés correspondant à des clés différentes de 10^{-4}



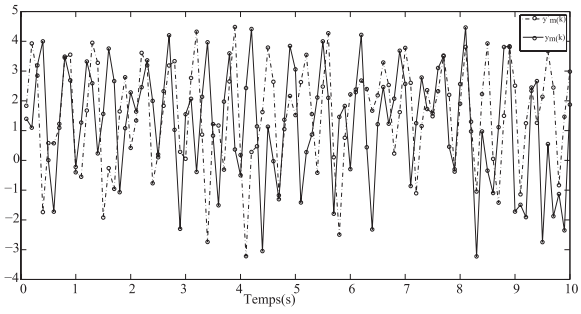
(ii) $V'(k)$ en fonction de $V(k)$

FIGURE 3.7.37 – Test de diffusion pour le cas d'un cryptage utilisant deux canaux de transmission

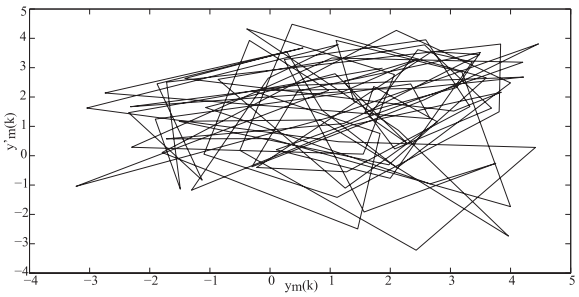
3.7.2 Propriété de confusion

Dans cette section, nous nous proposons de montrer que les cryptosystèmes proposés (cryptage mixte, cryptage à deux voies de transmission) possèdent la propriété de confusion. Ainsi, nous effectuons une simulation semblable à la précédente : le même message est communiqué deux fois au récepteur, mais sans changer la clé entre les deux transmissions. Les figures 3.7.38 et 3.7.39 donnent une confirmation que les deux signaux cryptés avec la même clé de cryptage, correspondant au même message d'informations clair, sont

remarquablement différents. En effet, à chaque transmission du message d'informations, l'état des variables d'états de l'émetteur (correspondant à l'état initial pour la transmission d'informations en cours) change. Cela montre que la méthode de transmission d'informations choisie utilise au mieux l'extrême sensibilité aux conditions initiales des systèmes hyperchaotiques. Il faut noter que le principe de cryptage seul ne peut pas satisfaire la propriété de confusion, si l'état initial de l'émetteur ne varie pas à chaque transmission de message. En effet, l'émetteur étant un système déterministe, le même état initial entraîne la même trajectoire. Ainsi, si on transmet un message deux fois, avec le même état initial du côté de l'émetteur, le signal crypté demeurera le même. Si on considère plusieurs transmissions d'un même message d'informations transmit transmit $m(k)$, dès lors que les instants où le message d'informations transmis est noyé par la porteuse hyperchaotique, et sont différents, alors les deux signaux cryptés correspondants sont différents. Cette propriété résulte de la sensibilité aux conditions initiales exhibée par les systèmes hyperchaotiques. Cependant, du côté du récepteur autorisé, quelque soit le message crypté correspondant à $m(k)$, la restauration produit le même résultat $m_r(k)$. Il est à souligner que pour un message d'informations donné, il existe éventuellement une infinité de messages cryptés, qui correspondent tous au même message décrypté.

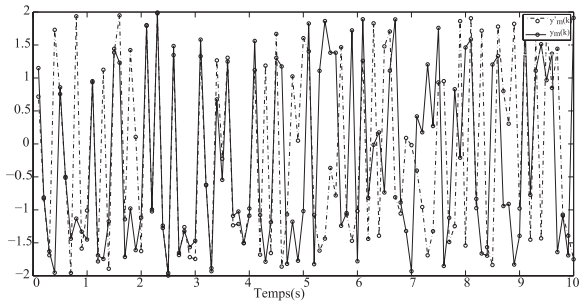


(i) Signaux cryptés correspondant au même message clair

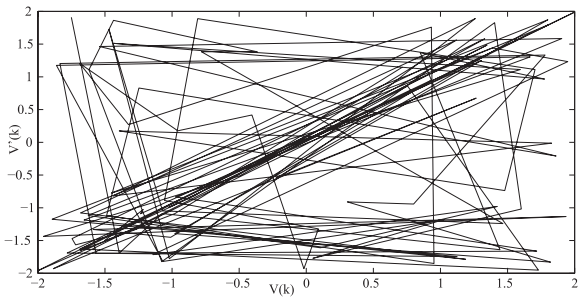


(ii) $y'_m(k)$ en fonction de $y_m(k)$

FIGURE 3.7.38 – Test de confusion pour le cas d'un cryptage mixte



(i) Signaux cryptés correspondant au même message clair



(ii) $V'(k)$ en fonction de $V(k)$

FIGURE 3.7.39 – Test de confusion pour le cas d'un cryptage utilisant deux canaux de transmission

3.8 Conclusion

Dans ce dernier chapitre, nous avons présenté une application importante de la synchronisation à base d'observateurs qui permet la communication sécurisée de l'information. La problématique est celle de la restauration d'entrées inconnues à savoir le signal d'informations. Après un tour d'horizon de diverses techniques de communication exploîtant les systèmes chaotiques, présents dans la littérature, nous avons retenu deux principes de transmission à savoir la technique de cryptage utilisant deux voies de transmission et le cryptage mixte. Ces techniques permettent notamment d'exploîter les schémas de synchronisation à base d'observateurs, proposés dans le chapitre précédent, qui sont basés sur l'utilisation des techniques d'aggrégation et la mise sous forme en flèche de la matrice du système erreur. Sous l'hypothèse de conditions parfaites, c'est-à-dire, en ne considérant ni le bruit, ni le retard dans la transmission, l'efficacité des techniques de synchronisation proposées dans le cadre des deux techniques de transmission utilisées, a été testée sur différents types de messages, à savoir un signal quelconque une, image et un texte. Dans les trois cas, la restauration de l'entrée inconnue se révèle excellente. Dans un deuxième temps, nous avons envisagé le cas où le cryptosystème proposé est perturbé par la présence d'un bruit de transmission. L'observateur proposé dans ce chapitre permet, par un choix convenable des gains, d'atténuer l'influence d'un bruit additif sur le signal transmis sur l'erreur de synchronisation. Finalement, nous avons vérifié que le cryptosystème proposé possède les propriétés de confusion et de diffusion.

Conclusion générale

Le développement de nouvelles conditions suffisantes de stabilisation asymptotique des systèmes dynamiques complexes discrets et leur application à la résolution du problème de synchronisation de systèmes chaotiques et à la sécurisation de l'information à base de chaos, constitue la principale contribution de nos travaux de recherche, consignés dans ce mémoire.

L'élaboration de ces conditions de synchronisation est basée sur l'utilisation des normes vectorielles et des techniques d'agrégation et réside dans le choix d'une représentation matricielle bien adaptée ; il s'agit de la forme en flèche mince des matrices qui caractérisent, à chaque instant, les systèmes complexes hiérarchisés à deux niveaux. Ainsi, la synthèse de lois de commande, par retour d'état et par retour de sortie, conduit à des résultats satisfaisants et de mises en oeuvre aisées, notamment pour la vérification de différentes propriétés de synchronisation.

Dans le cas de l'inaccessibilité des variables d'état, des schémas de synchronisation à base d'observateurs basés sur l'utilisation de techniques d'agrégation et de mise en forme en flèche des matrices ont été élaborés. Cette approche a conduit à des résultats satisfaisants. Nous avons ainsi établi des conditions de stabilisation permettant la détermination des gains de l'observateur choisi de façon à assurer la synchronisation.

Par la suite, les conditions de synchronisation chaotique établies, utilisant la synthèse d'observateurs, ont été appliquées dans le cas de deux techniques de cryptage, la première étant la technique de cryptage utilisant deux voies de transmission et la seconde étant le cryptage mixte. Ces conditions se sont avérées performantes dans le cadre de la sécurisation de l'information. En effet, nous avons pu récupérer plusieurs types d'informations a savoir un signal quelconque, une image et un texte. Des conditions de synthèse du gain de l'observateur, tenant compte de la robustesse au bruit, ont été aussi établies et testées avec succés.

Il est intéressant de mener, en perspectives, une expérimentation numérique (DSP ou FPGA) des cryptosystèmes chaotiques étudiés et d'y tester les commandes élaborées ; ce

qui constituerait un développement complémentaire intéressant de cette thèse. En outre, les résultats présentés dans ce mémoire peuvent être étendus à un problème général d'estimation d'état en présence d'un éventuel retard de transmission variable ou inconnu. Finalement, pour compléter la présentation de ces techniques de cryptage, nous projetons d'aborder et de tester la question de la sécurité de la transmission d'informations relative au cryptanalyse.

Bibliographie

[Abderrahman et Mohammed, 1996] Abderrahman, I. et Mohammed, B. (1996). Stability of discrete time systems : New criteria and application to control problems. *Rapport de Recherche, INRIA*. 46

[Aeyels, 1985] Aeyels, A. (1985). Stabilization by smooth feedback of the angular velocity of a rigid body. *Syst. Control Lett.*, 6(1):59–63. 51

[Alvarez et Li, 2006] Alvarez, G. et Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcation Chaos Appl. Sci. Eng*, 16(8):2129–2151. 53

[Alvarez *et al.*, 2004] Alvarez, G., Montoya, F., Romera, M. et Pastor, G. (2004). Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons and Fractals*, 21(4):783–787. 109

[Amri *et al.*, 2010] Amri, I., Soudani, D. et Benrejeb, M. (2010). Delay dependent robust exponential stability criterion for perturbed and uncertain neutral systems with time varying delays. *Studies in Informatics and Control*, 19(2):135–0. 45

[Babtista, 1998] Babtista, S. (1998). Cryptography with chaos. *Physical Letters A*, 240(1-2):50–54.

[Baier et Klein, 1990] Baier, G. et Klein, M. (1990). Maximum hyperchaos in generalized Hénon circuit. *Phys. Lett. A.*, 151(67):281–284. 34, 67, 68, 81, 87, 94, 114, 124, 136, 142, 143

[Barthélemy *et al.*, 2005] Barthélemy, P., Rolland, R. et Véron., P. (2005). Cryptographie. *Hermès Science*. 53

[Belghith, 1997] Belghith, S. (1997). *Méthodes algébriques et numériques pour l'étude de comportements complexes de systèmes non linéaires*. Thése de Doctorat ès Sciences Physiques, Faculté des Sciences de Tunis. 19

[Belkhouche et Gokcen, 2009] Belkhouche, F. et Gokcen, I. (2009). Digital image encoding using hyperchaos. *In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pages 1349 – 1352, San Antonio. 44

[Bellman, 1962] Bellman, R. (1962). Vector Lyapunov functions. *J. SIAM Control, Ser. A*, 1. 48

[Benrejeb, 1976] Benrejeb, M. (1976). *Sur la synchronisation des systèmes continus non linéaires en régime forcé.* Thése Docteur Ingénieur, Université des Sciences et Techniques de Lille.

[Benrejeb, 1980] Benrejeb, M. (1980). *Sur l'analyse et la synthèse de processus complexes hiérarchisés. Application aux systèmes singulièrement perturbés.* Thése de Doctorat ès Sciences Physiques, Université des Sciences et Techniques de Lille. 23, 25, 26, 27, 60

[Benrejeb, 2010] Benrejeb, M. (July 2010). Stability study of two level hierarchical nonlinear systems Plenary lecture. *In* 12^{th} *International Federation of Automatic Control Large Scale Systems Symposium : Theory and Applications, IFAC, LSS*, Lille. 51, 58, 59, 60, 62, 81, 114, 124, 134, 135

[Benrejeb et Abdelkrim, 2003] Benrejeb, M. et Abdelkrim, M. N. (2003). On order reduction and stabilization of tsk nonlinear fuzzy models by using arrow form matrix systems. *Analysis Modeling Simulation*, 73(7):977–991. 59

[Benrejeb et Borne, 1978] Benrejeb, M. et Borne, P. (1978). On an algebraic stability criterion for non linear process interpretation in the frequency domain. *In Proceedings of the International Symposium, Advances in MEasurement and Control, MECO, Acta Press*, pages 678–682, Athens. 81, 114, 124, 134, 135

[Benrejeb *et al.*, 1982] Benrejeb, M., Borne, P. et Laurent, F. (1982). Sur une application de la représentation en flèche à l´analyse des processus. *RAIRO Aut./Sys. Analysis and COntrol*, 16(2):133–146. 62, 81, 114, 124, 134, 135

[Benrejeb et Gasmi, 2001a] Benrejeb, M. et Gasmi, M. (2001a). On the use of an arrow form matrix for modeling and stability analysis of singularly perturbed nonlinear systems. *Systems Analysis Modeling Simulation*, 40(4):509–0. 59

[Benrejeb et Gasmi, 2001b] Benrejeb, M. et Gasmi, M. (2001b). On the use of an arrow form matrix for modelling and stability analysis of singularly perturbed nonlinear systems. *Systems Analysis Modelling Simulation*, 40:209–225. 134, 135

[Benrejeb *et al.*, 2005] Benrejeb, M., Gasmi, M. et Borne, P. (2005). New stability conditions for ts fuzzy continuous nonlinear models. *Nonlin. Dynam. and Syst. Theory*, 5(4):369–379. 59

[Benrejeb et Hammami, 2008] Benrejeb, M. et Hammami, S. (Octobre 2008). New approach of stabilization of nonlinear continuous monovariable processes characterized by an arrow form matrix. *In First International Conference on, Systems ENgineering Design and Applications, SENDA*, Monastir. 58, 81, 124, 134, 135

[Benrejeb *et al.*, 2008] Benrejeb, M., Sakly, A., Othman, K. B. et Borne, P. (2008). Choice of conjunctive operator of tsk fuzzy systems and stability domain study. *Mathematics and Computers in Simulation*, 76(5):410–421. 59

[Benrejeb *et al.*, 2006] Benrejeb, M., Soudani, D., Sakly, A. et Borne, P. (2006). New discrete Tanaka Sugeno Kang Fuzzy Systems characterization and Stability Domain. *International Journal of Computers, Communications & Control*, I(4):9–19. 134, 135

[Besançon, 2007] Besançon, G. (2007). *Nonlinear Observers and Applications*. Springer Verlag, New York. 30, 31

[Bitsoris, 1983] Bitsoris, G. (1983). Stability analysis of nonlinear dynamical systems. *Int. J. of Control*, 38(3):699–711.

[Boccaletti *et al.*, 2002] Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. et Zhou, C. (2002). The synchronization of chaotic systems. *Physics Reports*, 366. 56

[Borne, 1976] Borne, P. (1976). *Contribution à l'étude des systèmes discrets non linéaires de grande dimension. Application aux systèmes interconnectés.* Thése de Doctorat ès Sciences Physiques, Université des Sciences et Techniques de Lille. 45, 48, 51, 59

[Borne, 1987] Borne, P. (1987). *Non linear systems stability : Vector norm approach.* Systems and Control Encyclopedia, Pergamon Press. 48, 81, 114, 124, 134

[Borne et Benrejeb, 1977] Borne, P. et Benrejeb, M. (1977). On the stability of a class of interconnected systems. *In Application to the forced Working conditions 4th IFAC Symposium MTS*, Fredericton, Canada. 59

[Borne et Benrejeb, 2008] Borne, P. et Benrejeb, M. (2008). On the representation and the stability study of large scale systems. *International Journal of Computers Communications and Control*, 3(5):55–66. 48, 49, 81, 114, 124, 134, 135

[Borne et Benrejeb, 2012] Borne, P. et Benrejeb, M. (Avril 2012). Stability study of complex systems using vector norms. *In conférence plénière, CESA 2012*, Santiago du Chili. 48, 49

[Borne *et al.*, 2003] Borne, P., Dambrine, M., Perruquetti, W. et Richard, J.-P. (2003). *Vector Lyapunov functions : nonlinear, time-varying, ordinary and functional differential equations.* Advances in Stability Theory, Ed. A.A. Martynyuk, Taylor & Francis, London. 49

[Borne *et al.*, 1992] Borne, P., Dauphin-Tanguy, G., Richard, J. P., Rotella, F. et Zambettakis, I. (1992). Modélisation et identification des processuss. *Tome I, Ed. Technip Paris.* 19

[Borne *et al.*, 1993] Borne, P., Dauphin-Tanguy, G., Richard, J. P., Rotella, F. et Zambettakis, I. (1993). *Analyse et Régulation des Processus Industriels, Tome 2 - Régulation Numérique.* Editions Technip, Paris. 46, 47

[Borne *et al.*, 1976] Borne, P., Gentina, J.-C. et Laurent, F. (1976). Stability study of large scale non linear discrete systems by use of vector norms. *In IFAC Symposium on Symposium on Large Scale Systems Theoryand Applications*, pages 187–193, Udine. 59, 61, 81, 93, 114, 124

[Borne *et al.*, 1972] Borne, P., Gentina, J.-C. et Laurent, F. (Mai 1972). Sur la stabilité des systèmes échantillonnés non linéaires. *RAIRO Revue Jaune, AFCET*, (J2):96–105. 48, 49, 81, 114, 124

[Borne *et al.*, 2013] Borne, P., Popescu, D., Filip, F. et Stefanoiu, D. (2013). *Optimization in Engineering Sciences. Exact methods.* Wiley. 146

[Borne *et al.*, 1996] Borne, P., Richard, J. P. et Radhy, N. E. (1996). *Stability, stabilization, regulation using vector norms.* Nonlinear Systems, Vol. 2, Stability and Stabilization, Chapter 2. 51

[Borne *et al.*, 2007] Borne, P., Vanheeghe, P. et Duflos, E. (2007). *Automatisation des processus dans l´espace d´état.* Ed. Technip, Paris. 81, 124, 134, 135, 146

[Braiek *et al.*, 1995] Braiek, E. B., Rotella, F. et Benrejeb, M. (1995). Algebraic criteria for global stability analysis of non-linear systems. *Systems Analysis Modeling Simulation*, 17(3):211–227. 45

[Bremena *et al.*, 1997] Bremena, H. F. V., Udwadia, F. E. et Proskurowski, W. (1997). An efficient QR based method for the computation of Lyapunov exponents. *Physica D : Nonlinear Phenomena*, 101(1-2):1–16. 40

[Brockett, 1983] Brockett, R. W. (1983). Asymptotic stability and feedback stabilization. *Differential geometric control theory*, 27. 51

[Byrnes et Lin, 1993] Byrnes, C. et Lin, W. (1993). On discrete-time nonlinear control. *In 32th IEEE Conf. Decision Control*, pages 2990–2996, Antonio, Texas. 51

[Byrnes et Ghosh, 1993] Byrnes, I. et Ghosh, B. (1993). Stabilization of discrete time non linear systems by smooth feedback. *Systems & Control Letters*, 21. 46

[Carroll et Pecora, 1991] Carroll, T. L. et Pecora, L. M. (1991). Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems*, 38(4):453–456. 67, 113

[Chen *et al.*, 2003] Chen, J., Wong, K. et Cheng, L. (2003). A secure communication scheme based on the phase synchronization of chaotic systems. *Chaos*, 13(2):508–514. 57

[Cherrier *et al.*, 2005] Cherrier, E., Boutayeb, M. et Ragot, J. (2005). Observers based synchronization and input recovery for a class of chaotic models. *In 44nd IEEE Conference on Decision and Control and European Control Conference*, Seville. 92

[Cherrier *et al.*, 2006] Cherrier, E., Boutayeb, M. et Ragot, J. (2006). Observers based synchronization and input recovery for a class of nonlinear systems. *IEEE Transactions on Circuits and Systems I*, 53(9):1977–1988. 92

[Cruz et Nijmeijer, 2000] Cruz, C. et Nijmeijer, H. (2000). Synchronization through filtering. *International Journal of Bifurcation and Chaos*, 110(4):763–775. 104

[Cuomo *et al.*, 1993] Cuomo, K. M., Oppenheim, A. et Strogatz, S. H. (1993). Robustness and signal recovery in a synchronized chaotic system. *International Journal of Bifurcation and chaos*, 3(6):1629–1638. 101

[Cuomo et Oppenheim, 1993] Cuomo, K. M. et Oppenheim, A. V. (1993). Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.*, 71(1):65–68.

[Dedieu *et al.*, 1993a] Dedieu, H., Kennedy, M. P. et Hasler, M. (1993a). Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronization Chua's circuits. *IEEE Trans. on Circuit Syst. II : Anal. Digit. sign. Process*, 40. 101, 102

[Dedieu *et al.*, 1993b] Dedieu, H., Kennedy, M. P. et Hasler, M. (1993b). Chaos shift keying : modulation and demodulation of a chaotic carrier using selfsynchronizing Chua's circuit. *IEEE Transactions on Circuits and Systems II : Analog and Digital Signal Processing*, 40(10):634–642.

[Devaney, 1989] Devaney, R. L. (1989). An introduction to chaotic dynamical systems. *In Addison-Wesley*, Redwood City, CA. 37

[Eckmann et Ruelle, 1985] Eckmann, J. et Ruelle, D. (1985). Ergodic theory of chaos and strange attractors. *Reviews of Modern Physics*, 57(3):617–656. 128, 132, 134, 136

[El-Kamel *et al.*, 1999] El-Kamel, A., Borne, P., Ksouri-Lahmari, M. et Benrejeb, M. (1999). On the stability of nonlinear multimodel systems. *SACTA*, 2(1-2):40–52. 134, 135

[EL-Moudni, 1985] EL-Moudni, A. (1985). *Contribution à la modélisation et à l'analyse des systèmes discrets à échelles de temps multiples. Application à la commande optimale.* Thèse de Doctorat ès Sciences Physiques, Université des Sciences et Techniques de Lille. 21

[Fallahi *et al.*, 2008] Fallahi, K., Raoufi, R. et Khoshbin, H. (2008). An application of Chen system for secure chaotic communication based on extended kalman filter and multi-shift cipher algorithm. *Commun Nonlinear Sci Numer Simulat*, 13(4):763–781. 131

[Feki, 2003] Feki, M. (2003). An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons and Fractals*, 18(1):141–148.

[Feki *et al.*, 2003] Feki, M., Robert, B., Gelle, G. et Colas, M. (2003). Secure digital communication using discrete-time chaos synchronization. *Chaos, Solitons and Fractals*, 18(4):881–890.

[Feldmann *et al.*, 1996] Feldmann, U., Hasler, M. et Schwarz, W. (1996). Communication by chaotic signals : The inverse system approach. *International Journal of Circuit Theory and Applications*, 24(5):551–579. 105

[Filali *et al.*, 2012a] Filali, R., Hammami, S., Benrejeb, M. et Borne, P. (2012a). On synchronization, anti-synchronization and hybrid synchronization of 3D discrete generalized Hénon map. *Nonlinear Dynamics and Systems Theory*, 12(1):81–95. 135

[Filali *et al.*, 2012b] Filali, R., Hammami, S., Benrejeb, M. et Borne, P. (2012b). Synchronization of discrete-time hyperchaotic maps based on aggregation technique for encryption. *In 9th International Multi-Conference on Systems, Signals and Devices (SSD)*, pages 1–6, Chemnitz, Germany. 111

[Fradkov et Pogromsky, 1998] Fradkov, A. et Pogromsky, A. Y. (1998). Introduction to control of oscillations and chaos. *In World Scientific*, Singapore. 94

[Gasmi, 2001] Gasmi, M. (2001). *Contribution à la modélisation et à l'étude de la stabilité des systèmes continus complexes de grande dimension. Cas des systèmes singulièrement perturbés et des systèmes dynamiques à commande floue de type TSK.* Thése de Doctorat ès Sciences Physiques, Ecole Nationale d'Ingénieurs de Tunis, Tunis. 29

[Gentina *et al.*, 1972] Gentina, J.-C., Borne, P. et Laurent, F. (August, 1972). Stabilité des systèmes continus non linéaires de grande dimension. *RAIRO Revue Jaune, AFCET*, (J3):69–77. 45, 51, 59, 61, 81, 93, 114, 124, 135

[Gentina *et al.*, 1976] Gentina, J.-C., Grujic, L. T. et Borne, P. (1976). General aggregation of large scale systems by vector lyapunov functions and vector norms. *International Journal of Control*, 24(4):529–550. 48

[Ghosha *et al.*, 2010] Ghosha, D., Sahab, P. et Chowdhury, A. R. (2010). Linear observer based projective synchronization in delay Roossler system. *Commun Nonlinear Sci Numer Simulat*, 15(6):1640–1647.

[Grassi et Mascolo, 1997] Grassi, G. et Mascolo, S. (1997). Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44(10):1011–1014. 130

[Grassi et Mascolo, 1999a] Grassi, G. et Mascolo, S. (1999a). Synchronizing hyperchaotic systems by observer design. *IEEE Transactions on Circuits and Systems II : Analog and Digital Signal Processing*, 46(4):478–483.

[Grassi et Mascolo, 1999b] Grassi, G. et Mascolo, S. (1999b). A system theory approach for designing cryptosystems based on hyperchaos. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 46(9):1135–1138.

[Grassi et Miller, 2002] Grassi, G. et Miller, D. A. (2002). Theory and experimental realization of observer-based discrete-time hyperchaos synchronization. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 49(3):373–378. 34, 67, 68, 94, 114, 136, 142, 143

[Grujic, 1978] Grujic, L. T. (1978). Solutions for the Lur'e Postnikov and Aizerman problems. *Int. J. Syst. Sc.*, 9(12):1359–1372. 62

[Grujic *et al.*, 1979] Grujic, L. T., Borne, P. et Gentina, J.-C. (1979). Matrix approaches to the absolute stability of time-varying Lur'e Postnikov systems. *International Journal of Control*, 30(6):967–980. 48

[Grujic *et al.*, 1978] Grujic, L. T., Gentina, J.-C., Borne, P., Burgat, C. et Bernussou, J. (1978). Sur la stabilité des systèmes de grandes dimension, fonction de lyapunov vectorielles. *RAIRO Automatique*, 12(4):319–348. 45, 50

[Gruyitch *et al.*, 2004] Gruyitch, L. T., Richard, J., Borne, P. et Gentina, J. (2004). *Stability Domains*. Champan and Hall. 48, 49

[Guojie *et al.*, 2003] Guojie, H., Zhengjin, F. et Ruiling, M. (2003). Chosen ciphertext attack on chaos communication based on chaotic synchronization. *IEEE Trans Circuits and Systems*, 50(2):275–279. 54

[Hammami *et al.*, 2009a] Hammami, S., Ben-Saad, K. et Benrejeb, M. (2009a). On the synchronization of identical and non-identical 4-D chaotic systems using arrow form matrix. *Chaos, Solitons and Fractals*, 42(1):101–112.

[Hammami *et al.*, 2009b] Hammami, S., Benrejeb, M. et Borne, P. (2009b). New nonlinear output feedback controller for stabilizing the Colpitts oscillator. *International Journal on Sciences and Techniques of Automatic control and computer engineering, IJ-STA*, 3(2):996–1011.

[Hammami *et al.*, 2010a] Hammami, S., Benrejeb, M. et Borne, P. (2010a). On nonlinear continuous systems stabilization using arrow form matrices. *International REview of Automatic COntrol, IREACO*, 3(2):106–114.

[Hammami *et al.*, 2010b] Hammami, S., Benrejeb, M., Feki, M. et Borne, P. (2010b). Feedback control design for Rossler and Chen chaotic systems anti-synchronization. *Phys. Lett. A*, 374(28):2835–2840.

[Hammami *et al.*, 2010c] Hammami, S., Filali, R. et Benrejeb, M. (2010c). Nouvelles conditions suffisantes de stabilisabilité de processus échantillonnés non linéaires. *Revue e-STA*, 7(1):17–22. 58

[Hasler, 1998] Hasler, M. (1998). Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, 8(4):1357–1368.

[H.Dimassi *et al.*, 2010] H.Dimassi, A.Loria et Belghith, S. (2010). A robust adaptive observer for nonlinear systems with unknown inputs and disturbance. *In 49th. IEEE Conf. Decision Control*, pages 2602–2607, US. 92

[H.Dimassi *et al.*, 2011] H.Dimassi, A.Loria et Belghith, S. (2011). Sliding-mode observer for nonlinear systems with unknown inputs and noisy measurements. *In the 18th IFAC World Congress*, volume 18, pages 1–6, Milan. 92

[Hénon, 1976] Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, 50(1):96–77. 33

[Hitzl et Zele, 1985] Hitzl, D. L. et Zele, F. (1985). An exploration of the Hénon quadratic map. *Physica D*, 14. 35, 82, 125

[Hyun *et al.*, 2006] Hyun, C.-H., Kim, J.-H., Kim, E. et Park, M. (2006). Adaptive fuzzy observer based synchronization design and secure communications of chaotic systems. *Chaos, Solitons and Fractals*, 27(4):930–940.

[Ikeda, 1979] Ikeda, K. (1979). Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Opt. Commun*, 30. 32

[Isidori, 1995] Isidori, A. (1995). Nonlinear control system (3rd Ed). *Springer*.

[Itoh et Murakami, 1995] Itoh, M. et Murakami, H. (1995). New communication systems via chaotic synchronizations and modulation. *IEICE Transactions on Fundamentals*, E78(A3):285–290.

[J. Mohseni et Olejniczak, 1998] J. Mohseni, E. Y. et Olejniczak, K. (1998). State-dependent LMI control of discrete-time nonlinear systems. *In 37th IEEE Conf. Decision Control*, pages 4626–4627, San Diego, CA. 51

[Jiang et Tang, 2002] Jiang, G.-P. et Tang, W. K.-S. (2002). A global synchronization criterion for coupled chaotic system via unidirectional linear error feedback approach. *International Journal of Bifurcation and Chaos*, 12(10):2239–2253.

[Jiang *et al.*, 2003] Jiang, G.-P., Tang, W. K.-S. et Chen, G. (2003). A simple global synchronization criterion for coupled chaotic systems. *Chaos, Solitons and Fractals*, 15(5):925–935. 80, 93, 123, 133

[Jiang, 2002] Jiang, Z.-P. (2002). A note on chaotic secure communication systems. *IEEE Trans. on Circuits. Syst. I : Fundamental Theo. Appl*, 49(1):92–96. 108, 110, 111, 141

[Kharel *et al.*, 2009] Kharel, R., Busawon, K. et Ghassemlooy, Z. (2009). Indirect coupled oscillators for keystream generation in secure chaotic communication. *In 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference*, pages 4099–4104, Shanghai. 111

[Kharel *et al.*, 2010] Kharel, R., Busawon, K. et Ghassemlooy, Z. (2010). Secure digital communication using discrete-time chaotic systems via indirect coupling synchronization. *In Proceedings of the American Control Conference (ACC)*, pages 1791–1796, Newcastle upon Tyne. 111

[Li *et al.*, 1986] Li, C., Liao, X. et Wong, K.-W. (1986). Chaotic lag synchronization of coupled time-delayed systems and its application in secure communication. *Systems and Control Letters*, 7(3-4):133–142. 57

[Li *et al.*, 2009] Li, E., Li, G., Wen, G. et Wang, H. (2009). Hopf bifurcation of the third-order hénon system based on an explicit criterion. *Nonlinear Analysis : Theory, Methods & Applications*, 70(9):3227–3235. 114

[Lian et Liu, 2000] Lian, K.-Y. et Liu, P. (2000). Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. *IEEE Trans. on Circuits and Syst. I : Fundamental Theo. Appl*, 47(9):1418–1424.

[Liao et Huang, 1999] Liao, T. L. et Huang, N. S. (1999). An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Transactions on Circuits and Systems-I : Fundamental Theory And Applications*, 49(9):1144–1150. 113

[Liao et Tsai, 2000] Liao, T.-L. et Tsai, S.-H. (2000). Adaptive synchronization of chaotic systems and its application to secure communication. *Chaos, Solitons and Fractals*, 11(9):1387–1396.

[Lin, 1996] Lin, W. (1996). Further results in global stabilization of discrete nonlinear systems. *Syst. Control Lett.*, 29(1):51–59. 51

[Luenberger, 1971] Luenberger, D. G. (1971). An introduction to observers. *IEEE Transactions on Automatic Control*, 16(6):596–602. 31

[Mainieri et Rehacek, 1999] Mainieri, R. et Rehacek, J. (1999). Projective synchronization in three-dimensional chaotic systems. *Physical Review Letters*, 82(15):3042–3045. 57

[Maizières et Laurent, 1967] Maizières, C. et Laurent, F. (1967). Sur un modèle mathématique pour l'étude du circuit ferrorésonnant série. Application à la détermination d'une condition suffisante de non démultiplication de fréquence. *In CRAS, Série B, T. 265,*, pages 801 – 803, Paris.

[Matrozov, 1962] Matrozov, V. M. (1962). On the theory of stability of motion. *Prikl. Mat. Mekhan*, 26. 45, 48

[Miller et Grassi, 2001] Miller, D. A. et Grassi, G. (August, 2001). A discrete generalized hyperchaotic Hénon map circuit. *In Proceedings of the 44th IEEE Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 328–331, Dayton, Ohio. 81, 87, 114, 124

[Millerioux, 1997] Millerioux, G. (1997). Chaotic synchronization conditions based on control theory for systems described by discrete piecewise linear. *International Journal of Bifurcation and Chaos*, 7(7):1635–1649. 92

[Millerioux et Daafouz., 2003] Millerioux, G. et Daafouz., J. (2003). An observer-based approach for input-independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. on Circuits. Syst. I : Fundamental Theo. Appl*, 50(10): 1270–1279. 131

[Millerioux et Daafouz., 2004] Millerioux, G. et Daafouz., J. (2004). Unknown input observers for message embedded chaos synchronization of discrete-time systems. *International Journal of Bifurcation and Chaos*, 14(4):1357–1368. 101, 105

[Millérioux et Mira, 1998] Millérioux, G. et Mira, C. (1998). Coding scheme based on chaos synchronization from noninvertible maps. *International Journal of Bifurcation and Chaos*, 8(10):2019–2029. 101, 108, 110

[Morgül et Feki, 1999] Morgül, O. et Feki, M. (1999). A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, 251(3):169–176. 101

[Morgül et Solak, 1996] Morgül, O. et Solak, E. (1996). Observer based synchronization of chaotic systems. *Physical Review E*, 54(5):4803–4811. 92

[Nijmeijer, 1987] Nijmeijer, H. (1987). Local (dynamic) input-output decoupling of discrete-time nonlinear systems. *IMA J. Math. Control and Info*, 4(3):237–250. 51

[Nijmeijer et der Schaft, 1990] Nijmeijer, H. et der Schaft, A. J. V. (1990). *nonlinear dynamical control systems*. Springer, New York. 51

[Nijmeijer et Mareels., 1997] Nijmeijer, H. et Mareels., I. (1997). An observer looks at synchronization. *IEEE Transactions on Circuits and Systems*, I(44):882–890. 92

[Ott *et al.*, 1990] Ott, E., Grebogi, C. et Yorke, J. (1990). Controlling chaos. *Physical Review Letters*, 64(11):1196–1199. 67

[Parker et Chua, 1989] Parker, T. S. et Chua, L. O. (1989). *Practical Numerical Algorithms for Chaotic Systems*. Springer-Verlag, New York. 42

[Parlitz *et al.*, 1992] Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. et Shang, A. (1992). Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, 2(4):973–977. 101, 104

[Pecora et Carroll, 1990] Pecora, L. M. et Carroll, T. L. (1990). Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824. 52, 54, 56, 67, 99, 113

[Peitgen *et al.*, 2004] Peitgen, H. O., Jürgens, H. et Saupe, D. (2004). *Chaos and Fractals : New Frontiers of Science*. Springer, New York. 33

[Perez et Cerdeira, 1995] Perez, G. et Cerdeira, H. (1995). Extracting messages masked by chaos. *Physical Review Letters*, 74(11):1970–1973. 54

[P.Kokotovic et Arcak, 2001] P.Kokotovic et Arcak, M. (2001). constructive nonlinear control : a historical perspective. *Automatica*, 37(5):637–662. 51

[Primbs, 1996] Primbs, J. (1996). Survey of nonlinear observer design techniques. 31, 32

[Qian et Lin, 2001] Qian, C. et Lin, W. (2001). A continuous feedback approach to global strong stabilization of nonlinear systems. *IEEE Trans. Automat. Contr.*, 46(7):1061–1079. 51

[Richard *et al.*, 1988] Richard, J. P., Borne, P. et Gentina, J. (1988). Estimation of stability domains by use of vector norms. *Tinformation and Decision Technologiess, Nord - Holland*, 14:241–251. 48

[Robert, 1964] Robert, F. (1964). Normes vectorielles de vecteurs et de matrices. *RFTI Chiffres*, 17(4):261–299. 61, 135

[Rosenblum *et al.*, 1996] Rosenblum, M., Pikovsky, A. et Kurths, J. (1996). Phase synchronization of chaotic oscillators. *Physical Review Letters*, 76(11):1804–1807. 57

[Rosenbroch et Storey, 1970] Rosenbroch, H. H. et Storey, C. (1970). *Mathematics of Dynamical Systems*. Editions Nelson. 23

[Rulkov *et al.*, 1995] Rulkov, N. F., Sushchik, M. M., Tsimring, L. S. et Abarbanel, H. D. I. (1995). Generalized synchronization of chaos in directionally coupled chaotic systems. *Physical Review E*, 51(2):980–994. 56

[Shannon, 1949] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28:656–715. 53, 152

[Short, 1994] Short, K. (1994). Steps toward unmasking secure communication. *International Journal of Bifurcation and Chaos*, 4(4):959–977. 54

[Short, 1996] Short, K. (1996). Unmasking a modulated chaotic communications scheme. *International Journal of Bifurcation and Chaos*, 6(2):367–375. 109

[Soudani, 1997] Soudani, D. (1997). *Sur la détermination explicite de solutions à des problèmes d'analyse et de synthèse de systèmes singulièrement perturbés*. Thèse de Doctorat, Ecole Nationale d'Ingénieurs de Tunis, Tunis. 27

[Suykens *et al.*, 1997] Suykens, J. A. K., Curran, P. F., Vandewalle, J. P. et Chua, L. O. (1997). Robust nonlinear h_∞ synchronization of chaotic Lur'e systems. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 44(10): 891–904. 146

[Vidyasagar, 1993] Vidyasagar, M. (1993). Non linear systems analysis. *In Centre for A.I. and Robotics, Second Edition*, Prentice Hall, India.

[Wu et Chua, 1993a] Wu, C. et Chua, L. O. (1993a). A simple way to synchronize chaotic systems with application to secure systems. *International Journal of Bifurcation and Chaos*, 3(6):1619–1627.

[Wu et Chua, 1993b] Wu, C. W. et Chua, L. O. (1993b). A simple way to synchronize chaotic systems with applications to secure communication systems. *International Journal of Bifurcation and Chaos*, 3(6):1619–1627.

[Yang, 2004] Yang, T. (2004). A survey of chaotic secure communication systems. *Int. J. of Computational Cognition*. 106

[Yang et Chua, 1996] Yang, T. et Chua, L. (1996). Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I*, 43(9):817–819. 104

[Yang et Chua, 1997] Yang, T. et Chua, L. (1997). Impulsive stabilization for cotrol and synchronization of chaotic systems : Theory and application to secure communications. *IEEE Transactions on Circuits and Systems I*, 44(10):976–988. 101, 106

[Yang *et al.*, 1998] Yang, T., Yang, L.-B. et Yang, C.-M. (1998). Cryptanalysing chaotic secure communications using return maps. *Physics Letters A*, 245(6):495–510. 109

[Yang et Chenb, 2002] Yang, X.-S. et Chenb, G. (2002). Some observer-based criteria for discrete-time generalized chaos synchronization. *Chaos, Solitons and Fractals*, 13(6): 1303–1308.

[Y.J. Xue, 2003] Y.J. Xue, S. Y. (2003). Synchronization of generalized Hénon map by using adaptive fuzzy controller. *Chaos Solitons Fractals*, 17(4):717–722. 35, 82, 125

[Zhu, 2009] Zhu, F. (2009). Observer-based synchronization of uncertain chaotic system and its application to secure communications. *Chaos, Solitons and Fractals*, 40(5):2384–2391.

Titre en français Sur la synchronisation et le cryptage de systèmes chaotiques à temps discret utilisant les techniques d'agrégation et la représentation en flèche des matrices

Résumé en français L'objectif de cette thèse concerne le développement d'une méthode de synthèse de commande par retour d'état puis par observateurs à base de conditions de synthèse non contraignantes dans le cas de systèmes non linéaires à temps discret. Celle-ci met en exergue l'importance du choix de la description des systèmes sur l'étendue des résultats pouvant être obtenus lorsque la méthode d'étude de la stabilité est fixée. Ainsi, l'utilisation des normes vectorielles comme fonction d'agrégation et du critère pratique de Borne et Gentina pour l'étude de la stabilité, associée à la description des systèmes par des matrices caractéristiques de forme en flèche de Benrejeb, a conduit à l'élaboration de nouvelles conditions suffisantes de stabilisation de systèmes dynamiques discrets non linéaires, formulées en théorèmes et corollaires. Les résultats ainsi obtenus sont ensuite exploités, avec succès, pour la formulation de nouvelles conditions suffisantes de vérification des propriétés de synchronisation pour les systèmes hyperchaotiques à temps discrets. Le cas de synthèse d'observateurs est considéré et validé dans deux types de transmission chaotique.

Mots-clefs Systèmes discrets non linéaires ; Techniques d'agrégation ; Normes vectorielles ; Formes en flèche des matrices ; Stabilisation ; Systèmes chaotiques ; Cryptage ; Observateur

Titre en anglais On synchronization and encryption of discrete-time chaotic systems using aggregation techniques and arrow form matrices

Résumé en anglais The objective of this thesis concerns the development of a method for synthesizing control state feedback and observers by offering soft synthesis conditions for nonlinear discrete-time systems. It highlight the importance of choosing the systems description of the scope of what can be achieved when the stability study method is fixed. The use of vector norms as an aggregation function and the practical Borne-Gentina criterion for stability study, associated to Benrejeb arrow form matrix for system discription, leads to the development of new stabilization sufficient conditions of nonlinear discrete dynamical systems, formulated as theorems and corollaries. These results are then used, with success, for the formulation of new sufficient conditions for checking properties of synchronization for hyperchaotics discrete-time systems. The synthesis of observer then considered and is validated for two types of chaotic transmission.

Keywords Non linear discret time systems ; Aggregation technique ; Vector norms ; Arrow form matrix ; Stabilization ; Chaotic systems ; Cryptography ; Observer