People's Democratic Republic of Algeria
Ministry of Higher Education
and Scientific Research

Order number :.....
Series :.....

University Mohammed Seddik BENYAHIA - Jijel
Faculty of Science and Technology
Department of Automatic Control

THESIS

Submitted at
Department of Automatic Control
This thesis is submitted in fulfillment of the requirement for the degree
DOCTORAT 3th cycle (LMD)

By :

Mohammed Salah BOURIDAH

Theme :

Contribution to chaotic and fractional data cryptography

Defended on: 17/03/2022 in front of the examination committee:

Pr. Salim LABIOD	Mohammed Seddik Benyahia university, Jijel	President
Pr. Toufik BOUDEN	Mohammed Seddik Benyahia university, Jijel	Supervisor
Dr. Naamane BOUNAR	Mohammed Seddik Benyahia university, Jijel	Examiner
Dr. Ahsene BOUBAKIR	Mohammed Seddik Benyahia university, Jijel	Examiner
Pr. Abderrazak LACHOURI	20 août 1955 university, Skikda	Examiner
Pr. Messaoud RAMDANI	Badji Mokhtar university-Annaba	Examiner

This thesis was carried out within the non destructive testing laboratory (NDT) at Mohammed Seddik Benyahia university, Jijel.

Acknowledgement

Above all, I would like to thank Allah, the Almighty who gave me the strength, the will and the courage to accomplish this modest work.

First and foremost, I would like to express my sense of gratitude and indebtedness to my supervisor Mr. **Toufik BOUDEN**, professor at Mohammed Seddik Benyahia University in Jijel, for his inspiring guidance, encouragement and support during the completion of this work. I also thank him for his total availability and his objective advice, throughout these years. His timely help and painstaking efforts made it possible to present the work contained in this thesis. I consider myself fortunate to have worked under his quidance.

I am also most grateful to Mr. **Mustak Erhan Yalçin**, professor at Istanbul Technical University in Istanbul, Turkey who gave me the right ones advice and support during my internships in the Nonlinear Dynamics Systems Laboratory in Istanbul, Turkey.

I would like to express my deep gratitude to Mr. **Salim LABIOD**, professor at Mohammed Seddik Benyahia University in Jijel for for the honor that he give me by agreeing to chairing the jury for this thesis.

I address all my thanks to Mr. **Naamane BOUNAR**, associate professor at Mohammed Seddik Benyahia University in Jijel, as well as to Mr. **Ahsene BOUBAKIR**, associate professor at Mohammed Seddik Benyahia University in Jijel also to Mr.**Abderrazak LACHOURI**, professor at 20 août 1955 University in Skikda and to Mr.**Messaoud RAMDANI**,professor at Badji Mokhtar University in Annaba for the honor that they give me by agreeing to examine this thesis.

My gratitude goes to my parents for their unconditional dedication, who have always supported and pushed me to give the best of myself. My heartfelt thanks to the teachers of our university, to my colleagues and my friends.

Mohammed Salah BOURIDAH

DEDICATION

In the name of Allah the almighty, who is always by my side

I dedicate this modest work

To

My father allah yerhamo** and **my mother may allah keep her for us

May no dedication be able to express what I owe them, for their benevolence, their affection and their support, in testimony of my deep loves and great gratitude.

To

Souad, Souraya, Soumia, Bilal and Wissam

To

To my friends

To

All those who have helped me from far and near

MOHAMMED SALAH BOURIDAH

Contents

List of figures

List of tables

Glossary of abbreviations

AE	Average Energy.
BER	Bit Error Eate.
eXOR	Expanded XOR.
GVD	Gray Difference Degree.
Jac	Jacobian matrix.
LMI	Linear Matrix Inequality.
MKY	Meyer–Kalman–Yakubovich.
MSE	Mean Square Error.
NPCR	Number of Pixel Changing Rate.
PSNR	Peak Signal Noise Ratio.
SNR	Signal to Noise Ratio.
SPR	Strictly Positive Real.
UACI	Unified Averaged Changed Intensity.

Glossary of symbols

$\mathfrak{R}$	Set of real numbers.
$x(t),\ y(t)$	State vectors.
$u(t)$	Control input state.
$\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \kappa_6$	System parameters.
V(t)	Volume.
S(t)	Surface.
$\alpha,\ \beta,\ \theta$	Fractional order derivatives.
$\Gamma(\cdot)$	Euler's gamma function.
$\sigma(\cdot),\ \eta(\cdot)$	Lur'e system nonlinearity.
$\delta,\ \mu,\ \mu_1,\ \mu_2$	Positive numbers.
$\mathcal{L}$	Lyapunov function.
$\mathcal{H}$	Information entropy.
$A,\ B,\ H,\ K,\ F,\ C,\ R_{1,\ 2,\ 3},\ Q$	Matrices of appropriate dimensions.
$\mathcal{F}$	Transfer function.
$m(t)$	Plain message.
$\hat{m}(t)$	Recovered message.
γ	Set of encryption key.
τ	Time delay.

Contributions of the author

The results of this thesis have been partially participated in doctoral student's days and published as articles in the following international specialized confernces and journals:

Doctoral student's days

- M. S. Bouridah, T. Bouden & A. Boulkroune, (6 December 2017). "Contribution to chaotic data cryptography", *Doctoral student's days within Mohamed Seddik Benyahia university*, Jijel, Algeria.
- M. S. Bouridah, T. Bouden & A. Boulkroune, (16 December 2019). "Color image encryption based on fractional order chaotic systems", *Doctoral student's days within Mohamed Seddik Benyahia university*, Jijel, Algeria.

Conferences

- M. S. Bouridah, T. Bouden & A. Boulkroune, (29-31 October 2017). "Image secure transmission using chaotic synchronization", 5^{th} *International Conference on Electrical Engineering Conference, ICEE-B'17*, Boumerdes, Algeria.
- M. S. Bouridah, T. Bouden & A. Boulkroune, (11-12 December 2017). "Image Secure Transmission Using Lorenz and arneodo systems and chaotic synchronization", *International Conference on Automatic Control, Telecommunications and Signals, ICATS'17*, Annaba, Algeria.
- M. S. Bouridah, T. Bouden & A. Boulkroune, (10-11 December 2018). "Fractional Chaos Synchronization For Color Image Encryption", *Third International Conference on Technological Advances in Electrical Engineering, ICTAEE'18*, Skikda, Algeria.

Journals

- M. S. Bouridah, T. Bouden & M. E. Yalçin, (2020). "Chaos Synchronization of fractional order Lur'e Systems", *International Journal of Bifurcation and Chaos* **30**(14), 2050206.
- M. S. Bouridah, T. Bouden & M. E. Yalçin, (2021). "Delayed outputs fractional order hyperchaotic systems synchronization for images encryption", *Multimedia Tools and Applications* **80**, 14723—14752.

General introduction

With the fast evolution of communications in terms of the number of users and the nature of the information to be transmitted, securing the transmission channel becomes more and more necessary. For this, currently any high-performance telecommunications system requires a robust encryption system in order to protect itself against various possible attacks.

Cryptography is one of the most important tools for ensuring information security. It generally acknowledged as the best method of data protection against passive and active fraud. Cryptosystems seeks to transform a plain message into an encrypted one, which seems random. Cryptography is a scientific discipline in its own right, which is the study of methods of providing services of integrity, authenticity and confidentiality in information and transmission systems [Shannon (1948)]. There are three general classes of cryptographic algorithms, which are defined by the number or types of cryptographic keys that are used with each, symmetric-key (secret key) algorithms, asymmetric-key (public key) algorithms and Hash functions. Depending on the type of data, two types of cryptosystems are known, which are block cryptosystems and stream cryptosystems [Amigó (2009)]. A stream cryptosystem is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. The main alternative method to stream cryptosystem is in fact, the block cryptosystem, where a key and algorithm are applied to blocks of data rather than individual bits in a stream. A block cryptosystem is a method of encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm. The block cipher processes fixed-size blocks simultaneously, as opposed to a stream cryptosystem, which encrypts data one bit at a time. Most modern block ciphers are designed to encrypt data in fixed-size blocks of either 64 or 128 bits [Amigó (2009)].

Cryptanalysis is the science of studying attacks against cryptographic schemes. A fundamental assumption in cryptanalysis was flrst stated by Kerkhoff in the nineteenth century. It is usually referred to as Kerkhofi's Principle. It states that the adversary knows all the details of the cryptosystem, including algorithms and their implementations.

According to this principle, the security of a cryptosystem must be entirely based on the secret keys [Alvarez & Li (2006), Amigó (2009)]. Cryptography and cryptanalysis are often subsumed by the more general term cryptology.

However, the transmission systems based on the encryption methods mentioned above suffer from the low throughput problem caused by their slow execution of encryption algorithms. It's for this reason that new systems are being developed in order to overcome the overall effective transmission rate obstacle while maintaining the high level of security. two solutions are proposed, quantum cryptography and chaotic cryptography which the later is the intereste in the present work. Chaotic systems are governed by deterministic laws, but they are unpredictable in the long term. In 1963 Lorenz observed the phenomenon of chaos when he involved three differential equations to model any meteorological component [Lorenz (1963)]. A chaotic system can caracterized by one positive Lyapunov exponent, on the other hand a hyperchaotic system have more than one positve Lyapunov exponent, in fact higher dimensional chaotic systems with more one Lyapunov exponent clearly exhibit more complex dynamics [Wiggins (2003)].

The history of chaos based cryptography is more than two decades long. In 1998, Baptista proposed in his article a chaos based encryption scheme [Baptista (1998)]. This article was one of the first to present concrete and working cases of chaotic cryptography. Some rules have been suggested to achieve a reasonable degree of security [Alvarez & Li (2006)]. Methods to quantify the cryptanalysis of chaotic encryption schemes have been also proposed [Tenny *et al.* (2006)]. Therefore, the use of chaos in cryptography is of great interest to many areas, including military image databases, Internet banking operations and services, and the protection of transmission channels in order to preserve confidential data against attacks from enemies, spies, antagonists, etc. Moreover chaos based cryptography have advantages of a large space, simple implement, robustness and faster encryption over the traditional methods and we can be easily implement them by micro-processors or personal computers [Alvarez & Li (2006)].

During the last decades, the numerous studies carried out on that chaotic systems have shown, apart from their random behavior, attractive properties and that chaos appears as a promising solution to increase the performance of current transmission systems in terms of transmission speed and securing of information to be exchanged between two protagonists [Amigó (2009)]. Although this aperiodic behavior seems completely random, its evolution is perfectly deterministic, so that it can be reproduced identically at the receiver level. For a successful transmission, it is essential to ensure synchronization. Chaotic synchronization seeks to reproduce, at the the receiver level the chaotic signal

sent by the transmitter. Synchronization between the transmitter and the receiver systems is necessary to retrieve the information transmitted. Chaos based transmission systems can be classified into four categories: chaotic masking, chaotic parametric modulation, chaotic shift keying and chaotic inclusion method [Tenny *et al.* (2006)].

Since the early 1990, researchers have been able to prove that chaotic systems can be synchronized by various methods. Chaotic synchronization was firstly reported by Pecora and Carroll for two identical chaotic systems [Pecora & Carroll (1990)], where they proposed a technique that make possible to reconstruct the states of the transmitter from the signal transmitted by using analog circuits. Different approaches have been proposed to improve this method and reduce the error between the states of the transmitter and those restored at the receiver.

Moreover, transmission delay or propagation delay is a natural issue in exchange of signals and this cause poor performance and instability of the system, and fail of recovering the message. In 2000 [Chen & Liu (2000)] was the first report on propagation delay in master-slave configurations. The authors called this a phase sensitivity and the existence of it can destroy the synchronization. Therfore investigating time delay systems stability becomes an important subject [Yalçin *et al.* (2001)]. The propagation delay problem was reported and studied theoretically in [Chen *et al.* (2004), Liao & Chen (2003), Yalçin *et al.* (2001)]. There are two types of propagation delays, i.e. constant and time-varying propagation delay.

Recently, studying fractional order systems has become an active research area [Zhou *et al.* (2015)]. The fractional order models give more accuracy results than the corresponding integer order models. There are two main features of that claim, the fractional order parameter improves the system performance by increasing one degree of freedom, and the other one is related to fractional derivatives provides a valuable instrument for the description of memory and hereditary properties in various processes [Petráš (2011)]. Fractional integrals and derivatives also appears in theory of chaotic systems. One of the main objectives in the literature is found that chaotic behavior in fractional order systems [Zhu *et al.* (2009), Huang *et al.* (2012)]. The fractional derivatives have complex geometrical interpretation due of their nonlocal character and high nonlinearity, the power spectrum of fractional order chaotic systems fluctuates complexly increasing the chaoticity in frequency domain; and the computational complexity goal is also achieved. More specifically, the security in cryptosystems based on chaos can be increased using the derivative orders of fractional order chaotic systems as secret keys in addition to the system's parameters [Kiani *et al.* (2009)] so, the complexity of the verification of each key is strengthened causing the traditional cracking algorithms of chaotic masking to be

unusable. Therefore, new fractional chaotic systems are crucial to enhance the performance of several integer-order chaos-based applications. Recently, engineering applications using fractional order chaotic systems have been demonstrated, such as a digital cryptography approach, an image cryptosystem, a cipher and an authenticated encryption scheme [Bouridah *et al.* (2018), Bouridah *et al.* (2021)].

Thesis aims and scope

In this thesis, the mains objectives consists in providing tools for thesynchronization of chaotic and hyperchaotic systems and also for the design of new chaos based cryptograpy and transmission schemes. It addresses the challenges generated by the design of cryptographic systems using the intrinsic properties of chaotic systems, as well as the usual techniques of classical cryptography.

This thesis manuscript is organized as follows:

In **chapter 1**, we will recall some basic notions of the chaotic systems, fractional order systems as well as some synchronization methods. Moreover some definitions which essential in the design of new chaos based cryptograpy and transmission schemes, will be given.

Chapter 2, is devoted to the presentation two new theorems, which guarantee the synchronization of fractional order chaotic chaotic Lur'e systems. Lyapunov functions is chosen to derive the synchronization criterions. The derived criterions is a suffcient condition for the asymptotic stability of the error systems, formulated in the form of linear matrix inequalities. The controllers gain can be achieved by solving the LMI. A set of computer simulations will be carried out to illustrate and further validate the theoretical finding.

In **chapter 3**, we will addresses the synchronization problem of the master-slave type via a static error feedback. Sufficient conditions expressed by means of linear matrix inequality for the synchronization of fractional-order hyperchaotic systems with a known time delay between them is presented. The delay-dependent criterion is given based upon a Lyapunov function. Moreover, as an application a new chaos base cryptography scheme is presented. We considered two scenarios corresponding to the transmission channel, under occlusion attack and under noisse addition respectively. Results for the studied scenarios are presented and compared. The extensive simulation results will be given to prove the applicability and effectiveness of the proposed scheme.

Chapter 4 will investigate chaos based transmission scheme using an adaptive synchronization between fractional order chaotic systems. The encrypted signal will modulated into the transmitter. Then this encrypted signal will sented to the receiver end. By appropriately selecting a feedback gain, adaptative chaotic synchronization between the coupled transmitter and receiver will be achieved by solving LMI problems. Using Lyapunov stability theorem and LMI, sufficient conditions for indirect coupled synchronization between keystream generators will be obtained. Since synchronization is ensured, using an adaptive demodulator the encrypted signal will be recovered and decrypted by using the n-shift cipher algorithm. A set of numerical simulations will be given to illustrate the performances of the proposed scheme possessing.

Finally, we will close this manuscript with a general conclusion in which we return to what has been achieved along this thesis, and we will present the main results obtained and underline at the end of this conclusion the perspectives of this work, and which may be the subject of future work.

Chapter 1

State of the art of chaos, fractional order and cryptograpy

1.1 Introduction

Chaos is an interesting phenomenon often happens in some systems in various fields, as in biology [Degn *et al.* (2013)], medicine [Ditto (1996)], physics [Sciamanna & Shore (2015)] etc. Chaos is characterized by the way a dynamical system which does not repeat itself, even though the system is governed by deterministic equations [Strogatz (1994)]. Chaotic systems are highly sensitive to the choice of initial conditions. In other words systems in which the development of two very close starting points differs considerably over time. The era of chaos began in 1963 Edward Lorenz ocame up with a set of three differential equations popularly known as the Lorenz equation [Lorenz (1963)]. By studying the given model, Lorenz discovered a connection between chaotic systems and fractal structures [Lorenz (1963)]. He showed that despite seemingly random and unpredictable behavior, the system remains bounded in a certain area, which was later called a strange attractor [Strogatz (1994)].

Fractional calculus, are powerful mathematical tools that handle differentiation and integration of noninteger orders. In past decades, fractional order systems have represented an emerging area of research because of their capability to better exemplify real-world applications [Yan (2016)].

Currently chaos theory has emerged much more in electronics and more specifically in cryptography and secure transmissions.

This chapter is devoted to the presentation of chaos theory and the basic mathematical tools of integer and fractional order calculus, as well as some techniques and methods of chaos synchronization. The chapter ends with a part reserved for a generale view on chaos based cryptography and most popular chaos based transmission methods.

1.2 Chaos

Chaos does not mean absence of order, it is an interweaving of order and disorder. Chaos is a aperiodic long-term behaviour in a deterministic system that exhibits sensitive dependence on initial conditions [Strogatz (1994)]. From the definition chaos has three properties:

- Aperiodic long term behaviour.
- deterministic.
- Sensitive to initial conditions.

To explain these properties, we use the Lorenz system [Lorenz (1963)] given as:

$$\begin{cases} \dot{x}_1(t) = \kappa_1(x_2(t) - x_1(t)) \\ \dot{x}_2(t) = x_1(t)(\kappa_2 - x_3(t)) - x_2(t) \\ \dot{x}_3(t) = x_1(t)x_2(t) - \kappa_3 x_3(t) \end{cases} \tag{1.1}$$

where $\kappa_1 = 10$, $\kappa_2 = 28$ and $\kappa_3 = \frac{8}{3}$.

1.2.1 Aperiodic long term behaviour

This property means that the system trajectories do not settle down to any fixed points, periodic orbits or quasiperiodic orbits as $t \to \infty$. The profile of the output state variable x_1 is shown in figure (1.1), where it evolving with time aperiodically. To be sure that it indeed aperiodic, an autocorrelation function is carried out in figure (1.2).
One can see that at any time instant x_1 is not similar to itself. Therefore, it autocorrelation function only has a single spike at zero time shift. This clearly demonstrates that $x_1(t)$ is aperiodic in nature.

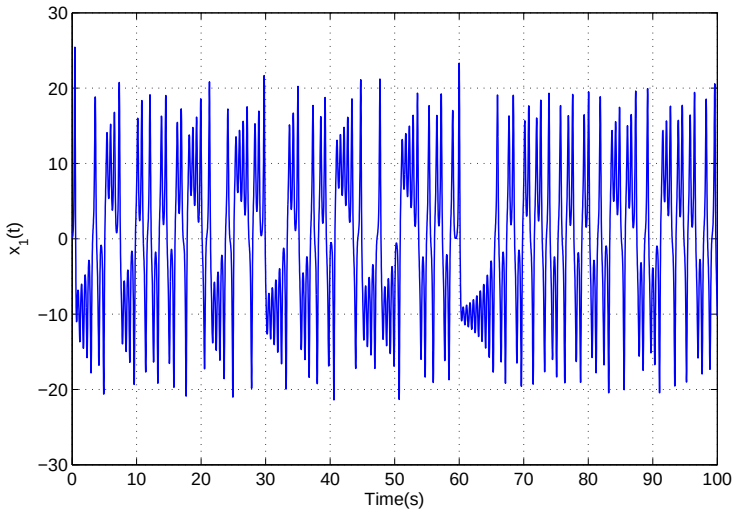


Figure 1.1 : The trajectory of the state variable $x_1(t)$.

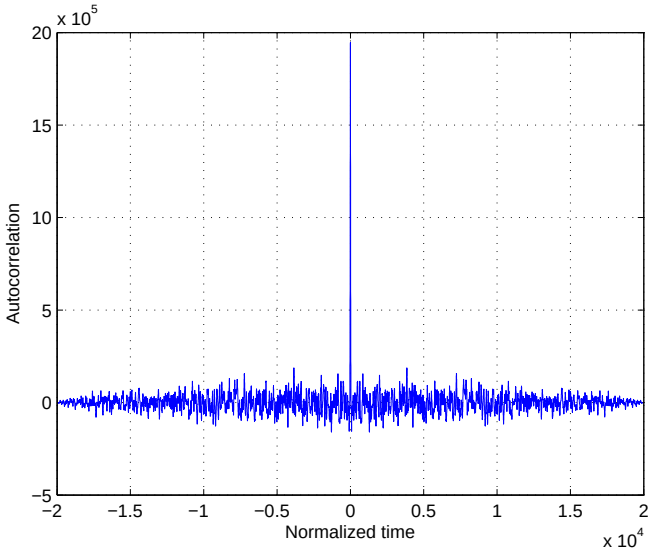


Figure 1.2 : The autocorrelation function of $x_1(t)$.

1.2.2 Deterministic

Determinism means that a behavior generated by one or more deterministic equations which do not involve any random parameter. We call a system is not random or do not have any stochastic input parameters deterministic system. In other words, the irregular behavior of the system arises from non linear dynamics and not from noisy driving forces. The past, present and future states of the system are governed by deterministic laws. This property can be seen by plotting the state variables $x_2(t)$ and $x_3(t)$ trajectories in figure (1.3). The figure show a demonstration on how a simple looking deterministic system could have extremely erratic dynamics where solutions oscillate irregularly, never exactly repeating but always remaining in a bounded region of phase space.

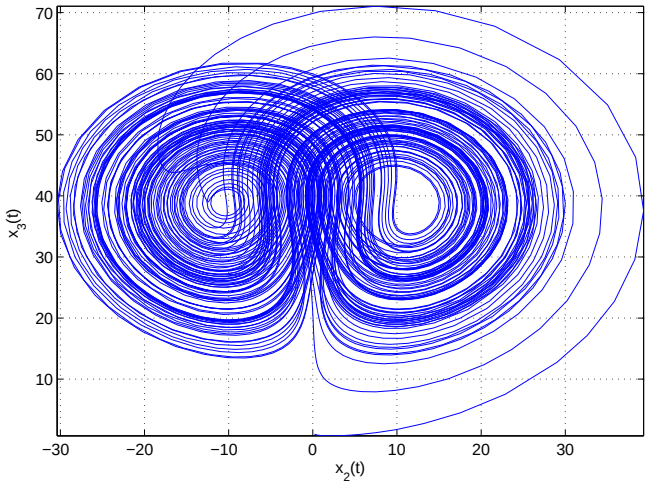


Figure 1.3 : The trajectory of the state variable $x_3(t)$ vs the trajectory of the state variable $x_2(t)$.

1.2.3 Sensitivity to initial conditions

This means that the trajectories even if they start from very close initial conditions will separate exponentially fast. In other words, the initially close trajectories in phase-space separate exponentially fast in time. This means a long term predictability becomes impossible. A simulation is performed where two identical Lorenz systems (x and y) are taken with same parameters but starting from different initial conditions. The difference in initial condition was chosen to be 10^{-6}. Figure (1.4) depicts the trajectories of the state variables $x_1(t)$ and $y_1(t)$, one can see that they quickly diverge from each other.

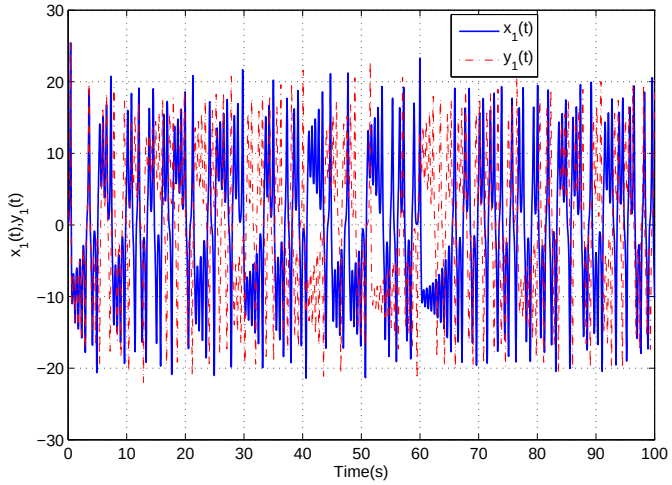


Figure 1.4 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$.

Figure (1.5) show a fast exponential divergence between the trajectories of the state variables $x_1(t)$ and $y_1(t)$. This means a long term prediction of chaotic systems is not possible since the slightest change in the initial condition will result in an exponential divergence.

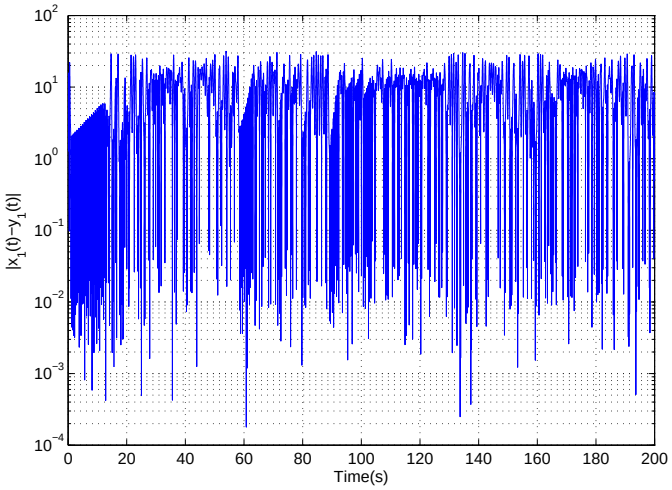


Figure 1.5 : The exponential divergence of the trajectories.

Remark 1.2.1. *Chaos exhibit also the sensitivity to parameters mismatches. To show this sensitivity, in the simutions the systems are taken starting with same initial condition but with nearly identical parameters values. For this, the difference in parameter* κ_1 *is taken to be* 10^{-15}*. Figure (1.6) depicts the trajectories of the state variables* $x_1(t)$ *and* $y_1(t)$*, which clearly shows they diverging from each other.*

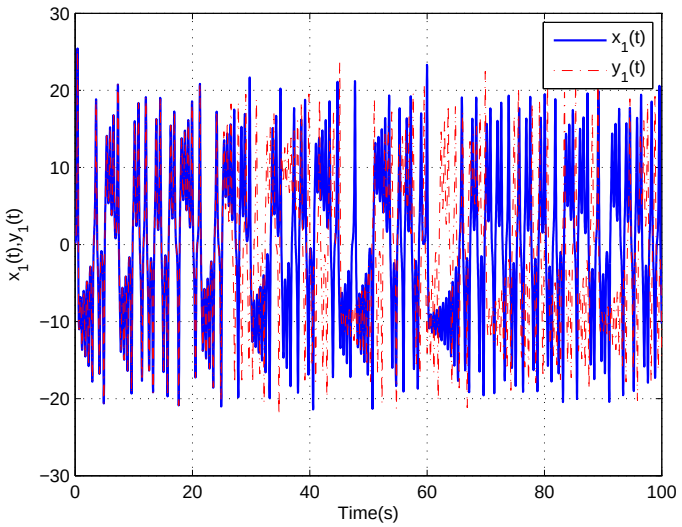


Figure 1.6 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ with parameters mismatches.

1.3 Route to chaos

The idea of chaos and how it occurs in a system can be visualized by means of a bifurcation diagram. A bifurcation diagram is a good way to highlight a signature of chaos [Kaplan & Glass (1995)]. The graph represent the behavior of a max value associated with each point of an attractor as a function of one of the parameters of the model where makes it possible to highlight two types of behavior. Either the attractor is represented by a finite number of points visited successively, which will correspond to a periodic behavior, or by a whole set of points distributed on the vertical corresponding to the value of the parameter considered, points visited irregularly, this which will lead to the conclusion that there is a chaotic attractor [Kaplan & Glass (1995)]. Let us take an example by using the Logistic equation [Baptista (1998)], given as:

$$x_{n+1} = rx_n(1 - x_n) \tag{1.2}$$

Figure (1.7), shows it bifurcation diagram, with initial condition is taking as $x(0) = 0.5$. One can seen that when r is between 0 and 1, the orbit converges to zero. When r is between 1 and 3, the trajectory converges to some fixed point. At point $r = 3$, the trajectory enter an attracting periodic orbit of period 2. As r increases the period

continues doubling with the bifurcation diagram splitting from period 2, 4, 8 onwards and with the trajectory being attracted to these periodic orbits. This will continues until $r > 3.58$, beyond which chaos become visible. It can be seen in figure (1.7) that for value of $r > 3.58$, the trajectory of x_n is not settling down to any fixed points or periodic orbits. However, the system is not chaotic for all values of r greater than 3.58. In figure (1.8) a zoom on the plot in figure (1.7), we observe what it called window, for example when $r \in [3.83,\ 3.88]$. In fact, between 3.58 and 4 there is a rich interleaving of chaos and order. A small change in r can make a stable system chaotic, and vice versa.

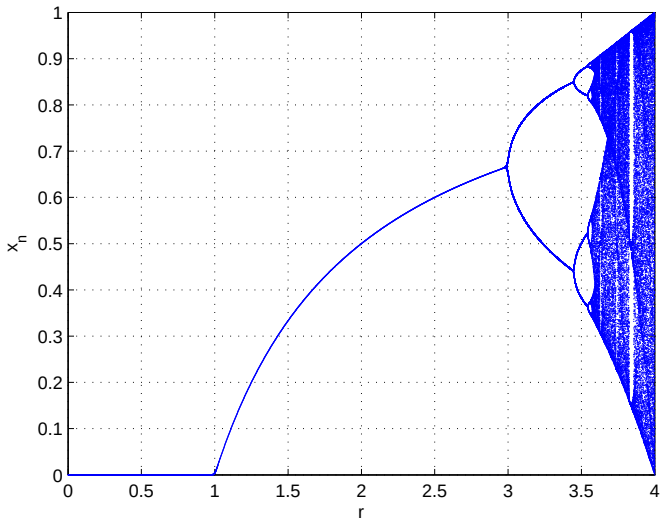


Figure 1.7 : Bifurcation diagram for the Logistic map.

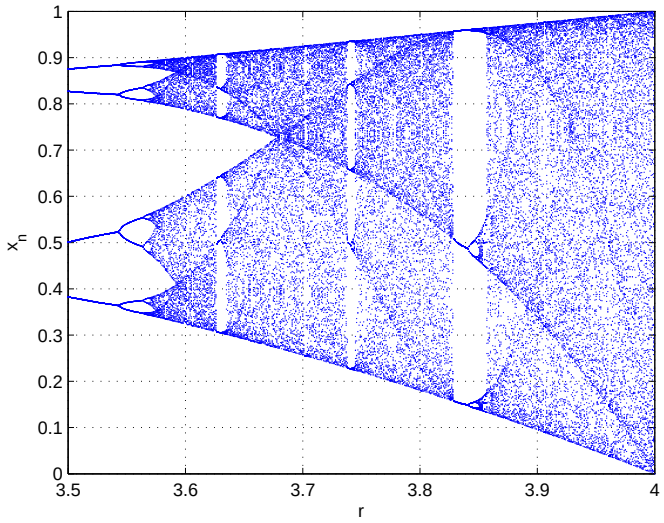


Figure 1.8 : Zoom of the bifurcation diagram for the Logistic map.

1.4 Lyapunov exponents

The Lyapunov exponents (LEs) measure the average rate of divergence or convergence of orbits starting from nearby initial points. Therefore, they can be used to analyze the stability of limits sets and to check sensitive dependence on initial conditions [Wiggins (2003)]. Geometrically, this results in the fact that if we choose a set of initial conditions located in an infinitely small sphere of $\delta(0)$ as its diameter in the basin of attraction of the dynamic system of dimension n, under the effect of dynamics this sphere will deform to transform into an ellipsoid. The i^{th} Lyapunov exponent is then defined as a function of the deformation undergone on the i^{th} direction as:

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} ln \frac{\delta_i(t)}{\delta_i(0)}, \ i \ = \ 1, \ldots, n \tag{1.3}$$

The signs of exponents provide a qualitative picture of the systems dynamics. A positive Lyapunov exponent may be taken as the defining signature of chaos. The existence of one positive exponent presents chaotic behavior. Howeover, more than one positive exponent presents what is called hyperchaos [Wiggins (2003)].
Figure (1.9), show the dynamic of Lyapunov exponents for the Lorenz system equation (1.1).

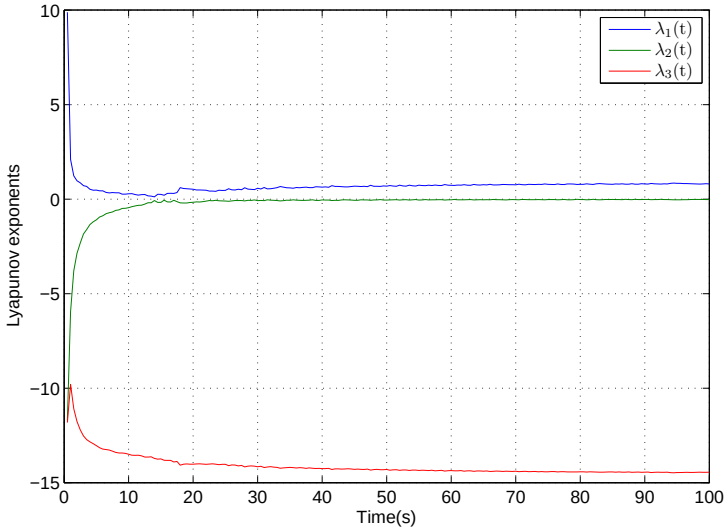


Figure 1.9 : Dynamics of the LEs for the Lorenz system.

Most dynamical systems have more than one Lyapunov exponent. If a system is defined in n-dimensions, then that system has n Lyapunov exponents, one for each of its dimensions. Combined, this set of exponents is referred to as the **Lyapunov spectrum**. The spectrum is typically ordered from largest exponent to smallest.

Definition 1.4.1. [Li & York (2004)] If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the Lyapunov exponents for a dynamical system in $\Re^n$, then the Lyapunov spectrum is the set $\{\lambda_1, \ \lambda_2, \ \cdots, \ \lambda_n\}$.

We can identify chaos with the following criterion:

$$\begin{cases} \lambda_1 > 0 \leftrightarrow & chaotic \\ \lambda_1 \leq 0 \leftrightarrow & nonchaotic \end{cases} \tag{1.4}$$

1.5 Dissipativity, fractals and attractors

These concepts are developed from the ground up. Firstly we define what a dissipative dynamical system is. Secondly we introduce fractal dimension used to identify fractal geometry and lastly we define what it means to be an attractor and in particular a strange attractor.

1.5.1 Dissipativity

Considering the following system as:

$$\dot{x} = f(x) \tag{1.5}$$

The dissipativeness of a dynamical system, meaning that an arbitrary volume element $V(t)$ enclosed by some surface $S(t)$ in phase space contracts. The surface S evolves by having each point on it follow an orbit generated by equation (1.5) into a new surface $S(t + dt)$, figure (1.10) shows a side view of the volume.

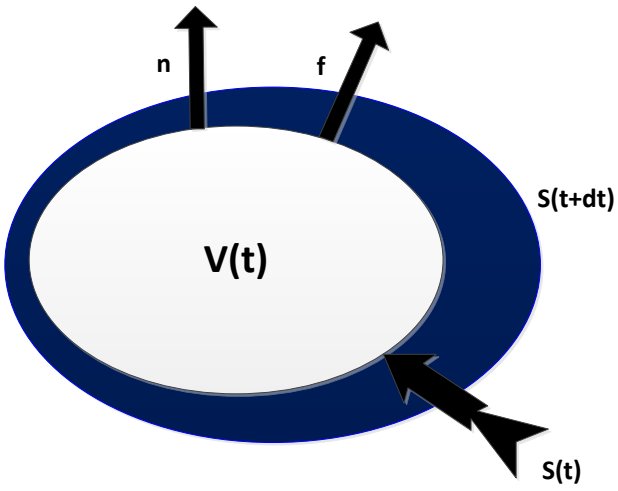


Figure 1.10 : Side view of the volume [Strogatz (1994)].

Let n denote the outward normal on S. Since f is the instantaneous velocity of the points, $f.n$ is the outward normal component of velocity. Therefore in time dt a patch of area dA sweeps out a volume $f.n\ dt\ dA$, as shown in figure (1.11).

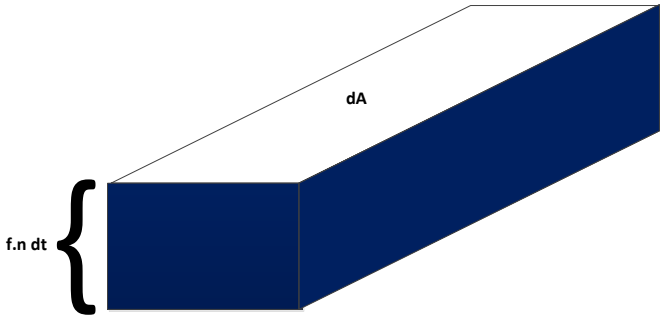


Figure 1.11 : A patch of area dA [Strogatz (1994)].

Hence $V(t+dt) = V(t)+$ (volume sweeps out by tiny patches of surface, integrated over all patches), so we obtain the following:

$$V(t+dt) = V(t) + \int_S (f.n\ dt)\, dA \tag{1.6}$$

Hence, we yields to:

$$\dot{V} = \frac{V(t+dt) - V(t)}{dt} = \int_S f.n\ dA \tag{1.7}$$

Theorem 1.5.1. *(Gauss–Ostrogradskii formula)[Weisstein (2002)] The total flux across the boundaries of a surface S, that in our case $\int_S (f.n\ dt) dA$, equal the total divergence of the vector field f inside the entire volume V enclosed by the surface $\int_\nu \nabla.f dV$.*

Finally, we rewrite the equation (1.7) using theorem (1.5.1) as:

$$\dot{V} = \int_V \nabla.f dV \tag{1.8}$$

1.5.1.1 Example

We take for example the Lorenz system in equation (1.1), for which one finds the following:

$$\begin{aligned} \nabla.f &= \frac{\partial}{\partial x_1}\left[\kappa_1 (x_2 - x_1)\right] + \frac{\partial}{\partial x_2}\left[x_1 (\kappa_2 - x_3) - x_2\right] + \frac{\partial}{\partial x_3}\left[x_1 x_2 - \kappa_3 x_3\right] = -\kappa_1 \\ & -1 - \kappa_3 < 0 \end{aligned} \tag{1.9}$$

Since the divergence is constant, thus the equation (1.8) reduce to:

$$\dot{V} = -\left(\kappa_1 + 1 + \kappa_3\right) V \tag{1.10}$$

which has solution as:

$$V(t) = V(0) e^{-(\kappa_1 + 1 + \kappa_3)t} \tag{1.11}$$

Thus, volumes in phase space shrink exponentially fast, hence if we start with a enormous solid blod of initial conditions, it eventually shirnk to a limiting set of zero volume. All trajectories starting in the blod end up somewhere in this limiting set, where it consists of a fixed points, a limit cycles, a torus attractor or a strange attractor.

1.5.2 Fractals

Simply put, a fractal is a geometric object that is selfsimilar on all scales. This somewhat vague description applies to a very wide variety of geometric objects found in both the abstract and natural worlds. Coastlines, mountains ranges and trees are some typical examples of natural objects with fractal properties [Li & York (2004)].
Just as some geometric objects can be 2-dimensional or 3-dimensional, there can also exist objects that have dimensions of $\frac{7}{4}$, $\frac{5}{3}$ or $\cdots$ [Crilly *et al.* (2012)].

Definition 1.5.1. [Crilly *et al.* (2012), Li & York (2004)] A set of points is said to be fractal if its dimension is non-integer.

There exist many different ways of estimating dimension, and each has its own advantages and disadvantages. One measurement that is found very often in introductory liturature on fractals is the Kaplan-Yorke dimension.

Definition 1.5.2. [Li & York (2004)] If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$ are the Lyapunov exponents for a dynamical system in $\Re^n$ and $j = n - 1$, then the Kaplan-Yorke dimension is given by:

$$D_{KY} = j + \frac{\lambda_1 + \lambda_2 + \cdots + \lambda_j}{|\lambda_{j+1}|} \tag{1.12}$$

1.5.2.1 Example

We take for example the Lorenz system in equation (1.1). By using equation (1.3), we find the Lyapunov spectrum is $\{\lambda_1 = 0.95,\ \lambda_2 = -0.02,\ \lambda_3 = -7.2\}$.
From the Lyapunov spectrum, we can easily compute the Kaplan-Yorke dimension as follow:

$$D_{KY} = 2 + \frac{0.95 - 0.02}{|-7.20|} = 2.13 \tag{1.13}$$

Notice that D_{KY} is a non integer. Thus, the attracting set has a fractal structure.

1.5.3 Attractors

An attractor is a region in the phase space to which all trajectories converge after a transition time. It is the long term behaviour of a dissipative dynamical system [Strogatz (1994)].
An attractor can be:

- Non strange: Those attractors are nonfractal, the behavior of which can be accurately predicted. There are three known types:
  - Fixed point.
  - Limit cycle.
  - Torus attractor.
- Strange nonchaotic: The attracting set of the attractor is fractal in nature.
- Strange chaotic: The name for the attractors that exhibit chaotic behavior and have fractal dimension.

Remark 1.5.1. *From definitions (1.4.1) and (1.5.1) the Lorenz system in equation (1.1) has a strange and chaotic attractor.*

1.6 Fundamentals in fractional calculus

Fractional calculus is a generalization of differentiation and integration of functions to non integer order. Different definitions of fractional order integration and differentiation have emerged during the development of fractional order calculus theory. Some of the definitions are directly extended from the conventional order calculus. The most commonly used definitions are presented in [Podlubny (1998)].

1.6.1 Definitions in fractional calculus

In this section, sevral approches to the generalization of the notion of differentiation and integration are considered. The subscripts a and t denote the two limits related to the fractional differentiation and fractional integration operations. Let us consider a continuous function $x = f(t)$.

1.6.1.1 Definition of Grünwald-Letnikov (G-L)

1.6.1.1.1 Grünwald-Letnikov fractional derivative

A generation of the backward difference by allowing the derivative order to be an arbitrary positive real was proposed by Günwald-Letnikov [Podlubny (1998)] as:

$$ {}_{a}^{GL}D_{t}^{\alpha} f(t) = \lim_{\substack{h\to 0 \\ nh=t-a}} \frac{1}{h^{\alpha}} \sum_{r=0}^{n} (-1)^{r} \begin{pmatrix} \alpha \\ \mathrm{r} \end{pmatrix} f(t-rh) = \lim_{\substack{h\to 0 \\ nh=t-a}} f_{h}^{\alpha}(t) \tag{1.14} $$

with:

$$\lim_{\substack{h\to 0\\ nh=t-a}} f_h^{\alpha}(t) = \sum_{k=0}^{m} \frac{f^{(k)}(a)(t-a)^{k-\alpha}}{\Gamma(1+k-\alpha)} + \frac{1}{\Gamma(1+m-\alpha)} \int_a^t (t-\tau)^{m-\alpha} f^{m+1}(\tau)\, d\tau \tag{1.15}$$

Binomial coefficients are defined as:

$$\begin{pmatrix} \alpha \\ \mathrm{r} \end{pmatrix} = \frac{\alpha\,(\alpha-1)\cdots(\alpha-r+1)}{r!} \tag{1.16}$$

$$\begin{pmatrix} \alpha \\ \mathrm{r} \end{pmatrix} = \begin{pmatrix} \alpha-1 \\ r \end{pmatrix} + \begin{pmatrix} \alpha-1 \\ r-1 \end{pmatrix} \tag{1.17}$$

In the case of negative value of α, we have:

$$\begin{pmatrix} -\alpha \\ r \end{pmatrix} = (-1)^r \begin{bmatrix} \alpha \\ r \end{bmatrix} \tag{1.18}$$

$$\begin{bmatrix} \alpha \\ \mathrm{r} \end{bmatrix} = \frac{\alpha\,(\alpha+1)\cdots(\alpha+r-1)}{r!} \tag{1.19}$$

1.6.1.1.2 Grünwald-Letnikov fractional integral

The GL α-order fractional integration of a function $f(x)$ is as follows [Podlubny (1998)]:

$${}_a^{GL}D_t^{-\alpha} f(t) = \lim_{\substack{h\to 0\\ nh=t-a}} h^{\alpha} \sum_{r=0}^{n} (1)^r \begin{bmatrix} \alpha \\ \mathrm{r} \end{bmatrix} f(t-rh) \tag{1.20}$$

1.6.1.2 Definition of Riemann-Liouville (R-L)

1.6.1.2.1 Riemann- Liouville fractional derivative

The R-L definition of the α-order fractional derivative $m \leq \alpha < m+1$ is defined as [Podlubny (1998)]:

$${}_a^{RL}D_t^{\alpha} f(t) = \left(\frac{d}{dt}\right)^{k+1} \int_a^t (t-\tau)^{m-\alpha} f(\tau)\, d\tau \tag{1.21}$$

where $\Gamma(\cdot)$ is the well-known Euler's gamma function described in appendix A.

1.6.1.2.2 Riemann-Liouville fractional integral

The R-L α-order fractional integration of a function $f(t)$ is as follows [Podlubny (1998)]:

$$ {}_{a}^{RL}D_{t}^{-\alpha} f\left(t\right) = \frac{1}{\Gamma(\alpha)} \int_{a}^{t} \left(t-\tau\right)^{\alpha-1} f\left(\tau\right) d\tau \tag{1.22} $$

Remark 1.6.1. *The Riemann-Liouville derivative exist and coincides with the Grünwald-Letnikov derivative if the function $f(t)$ is (n-1) continously differentiable in $[a,T]$ and that $f^{(n)}(t)$ is integrable in $[a,T]$ and $0 < m-1 \leq \alpha < m \geq n$, then for $a < t < T$ the following holds [Podlubny (1998)]:*

$$ {}_{a}^{GL}D_{t}^{-\alpha} f(t) = {}_{a}^{RL}D_{t}^{-\alpha} f\left(t\right) = \sum_{k=0}^{m-1} \frac{f^{(k)}(a)(t-a)^{k-\alpha}}{\Gamma(1+k-\alpha)} + \frac{1}{\Gamma(m-\alpha)} \int_{a}^{t} \frac{f^{m}\left(\tau\right) d\tau}{(t-\tau)}^{\alpha-m+1} \tag{1.23} $$

1.6.1.3 Definition of Caputo

Caputo introduced a new definition of α-order fractional derivative given by the following formula [Podlubny (1998)]:

$$ {}_{a}^{C}D_{t}^{\alpha} f\left(t\right) = \frac{1}{\Gamma\left(\alpha-m\right)} \int_{a}^{t} \frac{f^{(m)}(\tau) d\tau}{\left(t-\tau\right)^{\alpha+1-m}} \tag{1.24} $$

with $m-1 < \alpha < m$.

Remark 1.6.2. *The Caputo formula can be formulated according to the Riemann–Liouville formula as follows [Podlubny (1998)]:*

$$ {}_{a}^{RL}D_{t}^{\alpha} f\left(t\right) = {}_{a}^{C}D_{t}^{\rho} f\left(t\right) + \sum_{k=0}^{m-1} \frac{f^{(k)}(a)(t-a)^{k-\alpha}}{\Gamma\left(k-\alpha+1\right)} \tag{1.25} $$

Properties of fractional order integration and differerltiation are found in appendix A.

1.6.2 Stability and chaos in fractional order systems

Here, stability conditions for fractional order systems are discussed and then a necessary condition for chaos occurrence is given.

Consider the following system:

$$\begin{cases} D_t^\alpha x_1 = f_1(x_1,\ x_2,\ x_3) \\ D_t^\alpha x_2 = f_2(x_1,\ x_2,\ x_3) \\ D_t^\alpha x_3 = f_3(x_1,\ x_2,\ x_3) \end{cases} \tag{1.26}$$

Now we calculate the equilibrium points of the system in equation (1.26) by the following equations:

$$\begin{cases} D_t^\alpha x_1 = 0 \\ D_t^\alpha x_2 = 0 \\ D_t^\alpha x_3 = 0 \end{cases} \tag{1.27}$$

Thus, the jacobian matrix is:

$$Jac = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \frac{\partial f_1}{\partial x_3} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \frac{\partial f_2}{\partial x_3} \\ \frac{\partial f_3}{\partial x_1} & \frac{\partial f_3}{\partial x_2} & \frac{\partial f_3}{\partial x_3} \end{bmatrix} \tag{1.28}$$

Definition 1.6.1. [Tavazoei & Haeri (2007)] An equilibrium point ρ of the system equation (1.26) is called a saddle point of index 1 if the jacobian matrix at ρ has one eigenvalue with a non negative real part (unstable).

Definition 1.6.2. [Tavazoei & Haeri (2007)] An equilibrium point ρ of the system equation (1.26) is called a saddle point of index 2 if the Jacobian matrix at ρ has two unstable eigenvalue.

From the following theorem we can obtain the necessary condition for chaos occurrence.

Theorem 1.6.1. *[Matignon (1996)] Considering the following system as:*

$$D_t^\alpha x = Ax,\ x(0) = x_0 \tag{1.29}$$

where $0 < \alpha < 1$, $x \in \mathfrak{R}$ *and* $A \in \mathfrak{R}^{n\times n}$ *is asymptotically stable if and only if* $|arg(eig)A| > \alpha\frac{\pi}{2}$. *In this case, each component of the states decays towards* 0 *like* $t^{-\alpha}$. *Also, this system is stable if and only if* $|arg(eig)A| \geq \alpha\frac{\pi}{2}$ *and those critical eigenvalues that satisfy* $|arg(eig)A| = \alpha\frac{\pi}{2}$ *have geometric multiplicity one.*

We can use theorem (1.6.1) to analyze the stability of the system equation (1.26) in its equilibrium points. Let Λ_i are eigenvalues of the jacobian matrix equation (1.28) in a saddle points of index two. Therefore, instability region of these saddle points can be

determined by the following condition:

$$\alpha\frac{\pi}{2} \geq \min_i \{arg|\Lambda_i|\} \tag{1.30}$$

Since we can obtain the stability region of saddle points, hence the minimum value of α for the system equation (1.26) to remain chaotic can be obtained.

1.6.2.1 Example

Let the fractional order Genesio–Tesi system [Jun-Guo (2005)] given by:

$$\begin{cases} D_t^\alpha x_1 = x_2 \\ D_t^\alpha x_2 = x_3 \\ D_t^\alpha x_3 = -\kappa_1 x_1 - \kappa_2 x_2 - \kappa_3 x_3 + \kappa_4 x_1^2 \end{cases} \tag{1.31}$$

where $\kappa_1 = 6$, $\kappa_2 = 2.92$, $\kappa_3 = 1.2$, $\kappa_4 = 1$ and α is the fractional order derivative satisfying $0 < \alpha \leq 1$. To study the chaotic behavior of system equation (1.31) we consider the stability condition of the equilibrium points to obtain the necessary condition of chaos occurrence. The system has the following equilibrium points:

$$\begin{cases} \rho_1 = (0,\ 0,\ 0) \\ \rho_2 = (6,\ 0,\ 0) \end{cases} \tag{1.32}$$

Stability will be spotted by eigenvalues, which are determined through the evaluation of jacobian matrix at the equilibrium points:

$$Jac = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\kappa_1 + 2\kappa_4 x_1 & -\kappa_2 & -\kappa_3 \end{bmatrix} \tag{1.33}$$

Evaluation of jacobian matrix at the equilibrium points, yield the following eigenvalues:

$$\begin{cases} \Lambda_1 = -11.6354 \\ \Lambda_2 = -0.8177 + j6.880 \end{cases} \tag{1.34}$$

According to definitions (1.6.1) and (1.6.2) it can be concluded that Λ_1 is a saddle point of index 2 and Λ_2 is a saddle point of index 1. From theorem (1.6.1) we can get the following inequality in order to determine the stability condition:

$$arg\{0.220 \pm j1.8975\} > \alpha\frac{\pi}{2} \rightarrow \alpha < 0.9259 \tag{1.35}$$

Therefore, the necessary condition for appearance of chaos in fractional order Genesio–Tesi system is $\alpha \geq 0.9256$. Since the aforementioned condition is a necessary but not sufficient condition, it does not warrant chaos itself. In order to find the lowest order of system equation (1.31) to remain chaotic we investigate numerically the dynamics of this system where our results are validated by the existence of a positive Lyapunov exponent. Table (1.1) show that for $\alpha \geq 0.93$, the system has positive largest Lyapunov exponent which implies that the system is chaotic.

Table 1.1 : The largest Lyapunov exponent.

α	λ_{max}
0.90	-0.0153
0.91	-0.0071
0.92	-0.0005
0.93	0.0022
0.94	0.0031
0.95	0.0047
0.96	0.0020
0.97	0.0039

Remark 1.6.3. *A fractional order system it called commensurate system when it derivative orders are all equals ($\alpha_1 = \alpha_2 = \cdots = \alpha_n$). In the other case it called incommensurate system when it derivative orders are not equals ($\alpha_1 \neq \alpha_2 \neq \cdots \neq \alpha_n$) where n is the number of state variables [Tavazoei & Haeri (2008)].*

1.7 Chaos synchronization

Synchronization issue consists in designing a system (slave system) whose behavior mimics another one (master system). The latter drives the slave system via the transmitted signals. The synchronization occurs in a process where in two (or many) chaotic systems (either equivalent or inequivalent) have a common behavior due to diffusive and multiplicative couplings [Pecora & Carroll (1990)]. All the types of synchronization, are grouped together according to two coupling modes: unidirectional coupling and bidirectional coupling.

- Unidirectionnel synchronization: The synchronization is carried out in one direction only, i.e. the master system has an action on the slave system, but the opposite is false. This coupling is done using an element that works in only one direction.
- Bidirectional Synchronization: Unlike unidirectional synchronization, here the synchronization is done in two directions.

Let consider two chaotic systems as:

$$\dot{x}(t) = f(x(t)) \tag{1.36}$$

and

$$\dot{y}(t) = f(y(t)) \tag{1.37}$$

There are many types of synchronization being explained in the literatures. These different types can be grouped into the following categories:

- Complet synchronization [Pecora & Carroll (1990)]: The trajectories of the master and the slave systems converge to be exactly the same. This is the earliest and the simplest form of synchronization. This occurs in coupled identical systems and is also referred as a conventional synchronization or an identical synchronization, are said to obtain CS if :

  $$\lim_{t\to\infty} ||x(t) - y(t)|| = 0 \tag{1.38}$$

  for any combination of initial condition $x(0)$ and $y(0)$.
  The nature of the coupling can have two possibilities. When the evolution of one of the coupled system is unaffected by the coupling mechanism, then this is unidirectional coupling or a drive-response coupling. However, when both the systems are connected to each other such that the evolution of both affects each other, then this type of coupling is called bi-directional coupling mechanism. CS can be achieved by various types of schemes such the Pecora-Carroll method as explained above, the negative feedback, the sporadic driving, the active-passive decomposition, diffusive coupling/hybrid methods and observer based methods [Amritkar & Gupte (1993), Boccaletti *et al.* (2002), Pecora & Carroll (1990), Wang & Guan (2006)].

- Phase synchronization [Rosenblum *et al.* (1996)]: The slave system phase converges to the masters but their amplitude may not be the same, thus can be formed by a weak coupling and is mostly achieved in coupled non identical systems.

- Lag synchronization [Rosenblum *et al.* (1997)]: The output of the slave system and the master system lock their phase and amplitude with a presence of a time delay τ_{lag}. This is a special case of CS and phase synchronization.

- Projective synchronization [Mainieri & Rehacek (1999)]: This is a special case of GS where one-to-one mapping function is a simple linear function $\phi = ax$.

- Generalized synchronization (GS) [Boccaletti *et al.* (2002)]: The trajectories of the slave system to the master trajectories are one-to-one mapping of the function ϕ. GS is used for synchronization for completely different systems where the output of one system is the function of the output of another system. the Systems mention above are said to exhibit GS if:

  $$\lim_{t\to\infty} ||y(t) - \phi(x(t))|| = 0 \tag{1.39}$$

where the properties of the transformation ϕ are independent of the initial conditions $x(0)$ and $y(0)$. CS is a special case of GS where the mapping function ϕ is unity.

- Impulsive Synchronization [Yang (2004)]: In this case, the driving signal from master system is not sent continuously but sent as impulses determined by a fixed or time varying interval τ.
- Adaptive Synchronization [Yang *et al.* (2008)]: Here some adaptive methods are applied for synchronizing the master and slave systems.

1.8 Chaos based cryptography and transmission

1.8.1 Chaos based cryptography

During the 1980s, two new methods of cryptography emerged, quantum cryptography and chaos based cryptography. Quantum cryptography is based on the Heisenberg principle, according to which the measurement of a quantum system disturbs that system. It is then possible to transmit a key that being sure it has not been listened to, and then using it with regular encryption. As for chaos based cryptography, it is possible to encrypt and decrypt information in real time by drowning the message in the chaotic signal. For this, it uses the properties of chaotic dynamics which are noisy-looking temporal evolution and local determinism [Tenny *et al.* (2006)]. Additionally, chaotic dynamical systems have the advantage of providing qualitatively simple mechanisms to generate deterministic pseudo randomness [Zhen *et al.* (2014)]. We can classify cryptography according to several criteria [Amigó (2009)]. Depending on the type of key there is:

1. Symmetric cryptography: Symmetric cryptography is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process, however it suffers from the key management problem, when the number of users increases.
2. Asymmetric or public key cryptography: Asymmetric or public key cryptography has come to solve the problem of the keys distribution problem, but it has also the disadvantage of being much slower than secret key algorithms. In asymmetric algorithms, the encryption and decryption keys are distinct and cannot be inferred from each other and the decryption key cannot, be calculated from the encryption key.
3. Hash functions: A cryptographic hash function does not use keys for its basic operation. This function creates a small digest or “hash value” from often large amounts

of data through a one-way process. Hash functions are generally used to create the building blocks with which applications such as secure internet communication can be realized.

Depending on the type of data, two types of cryptosystems are known [Amigó (2009)]:

1. Block cryptosystems: A Block cryptosystems transform a relatively short string to a string of the same length under control of a secret key.

2. Stream cryptosystems: A stream (pseudo random number generator) cryptosystems is a deterministic method, usually described with a mapping, to produce from a small set of random numbers, called the seed, a larger set of random looking numbers called pseudo-random numbers. Stream cryptosystems processes the plain text bit by bit.

Remark 1.8.1. *Block and stream cryptosystems categorised as symmetric cryptography.*

1.8.2 Chaos based transmission

The past two decades have seen massive use of chaotic systems for encryption and chaos securing transmissions. These practices were made possible by the discovery of the synchronization of chaotic systems. Indeed, two completely isolated chaotic systems cannot synchronize, because of their sensitivity to errors, even very small. Then, some kind of coupling must be introduced between the systems to be synchronized. So, Pecora has proposed an example, where a chaotic system and a duplicate of part of the system are synchronized. Chaos based transmission is by mixing the information with a chaotic signal. The output of the transmitter is sent to the receiver, which has the role of extracting information from the received signal. chaos synchronization is required for successful message recovery [Cuomo *et al.* (1993)]. Since the early nineties, several methods for chaos synchronization between transmitters and receivers have been proposed [Cuomo *et al.* (1993), Dedieu *et al.* (1993), Pecora & Carroll (1990)], with applications to secure transmissions [Feldmann *et al.* (1996), Kwon *et al.* (2011), Smaoui *et al.* (2011)]. Chaos based transmission systems can be classified into four categories:

1. Chaotic masking [Cuomo *et al.* (1993)]: In this method, a message signal is added to the output of the chaotic transmitter system. A chaotic synchronization is performed and the chaotic signal is subtracted from the received signal at the receiver side, thus obtain the message signal.

2. Chaotic parametric modulation [Feldmann *et al.* (1996)]: The message signal is used to modulate the transmitter parameters such that its trajectories keep changing in a

chaotic attractors. At the receiver side, chaos synchronization is performed along with some adaptive tuning, thus recovering the message signal.

3. Chaotic shift keying [Dedieu *et al.* (1993)]: Chaotic shift keying basically a special case of the parametric modulation technique devise to transmit digital message securely.

4. Chaotic inclusion method [L'Hernault *et al.* (2008)]: In this method, instead of modulate the chaotic parameter, the message signal is used to change the chaotic attractor directly in the phase space. The message is included at one of states (or more) of the chaotic transmitter. Once the synchronization is achieved, the message is recovered by some inverse operation.

1.9 Conclusion

In this chapter we have first approached the different definitions of chaos, with its main characteristics. Secondly, we recalled the functions useful in fractional order calculus, as well as the different definitions of integration and fractional order derivation. We also discussed the tools necessary for the chaos synchronization. Finally, we highlighted the most popular chaos based cryptography and transmission techniques.

Chapter 2

Chaos synchronization of fractional order Lur'e systems

2.1 Introduction

We consider Lur'e systems which consist of a linear dynamical system, feedback interconnected to a static nonlinearity that satisfies a sector condition. Some fractional order systems of common interest can be presented in the Lur'e form [Huang *et al.* (2012)]. In the last few years, one unified approach for chaos synchronization is to reformulate the problem as a Lur'e system and then discuss the absolute stability of its error dynamics [Suykens & Vandewalle (1996), Yalçin *et al.* (2001)]. Various schemes have been proposed and studied, such as state delayed feedback control [Yalçin *et al.* (2001)] and dynamic output feedback with time delay [Huang & Cao (2006)]. The authors in [Suykens & Vandewalle (1996)] present a synchronization scheme with a linear state feedback control technique where the glaobal asymptotic stability citerion is derived from a Lur'e Postnikov Lyapunov function. In [Yalçin *et al.* (2001)], a synchronization scheme of Lur'e systems using delayed state feedback control is proposed and the effect of delay are analyzed. However, these results and criterions could not be extended to the fractional order case due of well known Leibniz rules does not hold for fractional derivatives [Duarte-Mermoud *et al.* (2015), Podlubny (1998)]. Recently, the synchronization problem between integer order chaotic system and fractional order chaotic system, or between fractional order chaotic systems with different fractional derivative orders, began to attract the attention among researchers [Bouridah *et al.* (2020), Odibat (2010)]. Compared with the conventional chaos synchronization research, the synchronization scheme between chaotic systems with non identical derivative orders has some advantages. One of them is that the fractional orders of the states to be synchronized in the slave fractional order chaotic system are freed from the fixed orders of the corresponding states in master

system, which can provide more flexible mechanism in the selections of the master and slave systems. In addition, the fractional derivatives are variable parameters, which can be used as secret keys if this synchronization scheme is adopted in digital communications. On the other hand, it is worthy noticing that the propagation delay may exist in master-slave configurations and will destroy the synchronization. Since Chen and Liu [Chen & Liu (2000)] introduced the delay of the chaotic synchronization and showed that the delay may break the synchronization, especially many research efforts have been focused on the effect of the propagation delay for the chaotic synchronization. The authors in [Yalçin *et al.* (2001)] conducted the first research considering the effect of time delay in chaotic synchronization of Lur'e system and presented sufficient conditions for stability. Liao and Chen [Liao & Chen (2003)] proposed a synchronization scheme for Lur'e systems with time delay using a feedback controller. After the research of Liao and Chen, various synchronization schemes for the chaotic Lur'e systems with time delay were presented in [Chen *et al.* (2004), Liao & Chen (2003), Yalçin *et al.* (2001)]. In those synchronization schemes, a delayed state feedback controller was designed and its gain matrix was derived from a sufficient condition for stability of error dynamics between a master system and a slave system. Motived by the above discussion, in this chapter, sufficient criterions for the synchronization of fractional order Lur'e systems and the synchronization of fractional order Lur'e systems with different fractional derivatives and time delay respectively are proposed.

2.2 Master-slave synchronization scheme of fractional order Lur'e type systems

Based on some fractional calculus essential concepts and the theorem related to the fractional extension of Lyapunov direct method, we presente in this section a synchronization scheme of fractional order Lur'e systems. A quadratic Lyapunov function is chosen to derive the synchronization criterion. The derived criterion is a sufficient condition for the asymptotic stability of the error system, formulated in the form of matrix inequalities. The controller gain can be achieved by solving a linear matrix inequality. Main contributions of this scheme are as follows:

- The absolute stability is explored, to derive a sufficient condition for synchronize fractional order Lur'e systems.
- The efficiency and validity of this the proposed criterion is tested, in an appropriate numerical simulation framework, both on fractional order chaotic systems and cellular neural networks in the Lur'e form.

- It can be used to synchronizing fractional order chaotic and hyperchaotic systems.
- Our obteined results can not only applied to fractional order Lur'e systems, in partice we can easily realize the synchronization of integer order Lur'e systems based on our criterion.

2.2.1 Chaos synchronization

2.2.1.1 Problem formulation

The main objective of this scheme is to synchronize the master system $\mathcal{M}$ and the slave system $\mathcal{S}$. Figure (2.1) presents the proposed synchronization scheme.

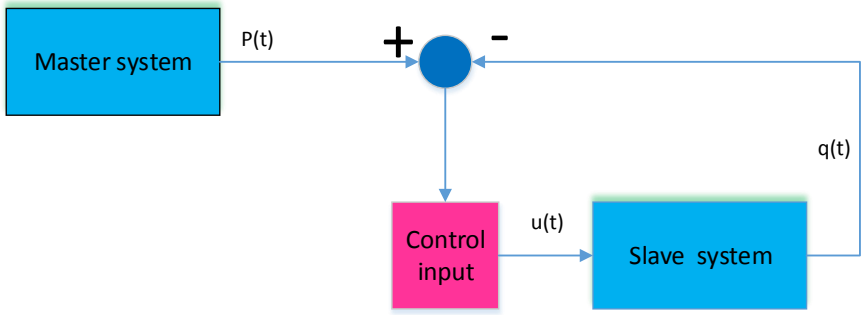


Figure 2.1 : Synchronization scheme.

Consider the following master–slave synchronization scheme as:

$$\begin{aligned}
\mathcal{M}: &\begin{cases} D_t^\alpha x(t) &= Ax(t) + B\sigma(Cx(t)) \\ p(t) &= Hx(t) \end{cases} \\
\mathcal{S}: &\begin{cases} D_t^\alpha y(t) &= Ay(t) + B\sigma(Cy(t)) + u(t) \\ q(t) &= Hy(t) \end{cases} \\
\mathcal{C}: &\quad \{u(t) = F(p(t) - q(t))
\end{aligned} \tag{2.1}$$

The state vectors of the master and slave systems are $x \in \Re^n$ and $y \in \Re^n$, respectively. The matrices $A \in \Re^{n\times n}$, $B \in \Re^{n\times n_h}$, $C \in \Re^{n_h\times n}$ and $H \in \Re^{n\times n}$ are known real constant matrices. $p(t) \in \Re^m$ and $q(t) \in \Re^m$ are the outputs of the master and the slave systems, respectively. $\sigma(\cdot) : \Re^{n_h} \to \Re^{n_h}$ satisfies a sector condition [Khalil (1993), Suykens & Vandewalle (1996), Yalçin *et al.* (2001)]. The master system and also the slave system is represented with a fractional order linear dynamical system interconnected with feedback to a static nonlinearity $\sigma(\cdot)$ which satisfies a sector condition and belongs to

sector $[0, \mathcal{K}]$. This is in fact describes a Lur'e system which is a classical structure in control theory when $\alpha = 1$. Therefore, the master and the slave systems are named as fractional order Lur'e system.
In this section D_t^α stands for Caputo derivative, and for simplicity we note $\eta(Ce(t); y) = \eta(Ce; y) = \eta$.

Remark 2.2.1. *Our obteined results can not only applied to fractional order Lur'e systems. In practice we can easily realize a synchronization between integer order Lur'e systems based on our criterion.*

The main objective of this scheme is to synchronize the master system $\mathcal{M}$ and the slave system $\mathcal{S}$ by applying a linear state error feedback to the slave system with control signal $u(t) \in \mathfrak{R}^n$ with feedback matrix $F \in \mathfrak{R}^{n\times n}$. Defining the synchronization error as $e(t) = x(t) - y(t)$, the error dynamic can be obtained as:

$$\mathcal{E}: \ \{D_t^\alpha e(t) = (A - FH)e(t) + B\eta(Ce; y) \tag{2.2}$$

where $\eta(Ce; y) = \sigma(Ce + Cy) - \sigma(Cy)$. The nonlinearity $\sigma(\cdot)$ belongs to sector $[0, \mathcal{K}]$ and the nonlinearity $\eta(Ce; y)$ satisfies the following:

$$0 \leq \frac{\eta(c_i^T e; y)}{c_i^T e} = \frac{\sigma_i(c_i^T e + c_i^T y) - (\sigma_i(c_i^T y)}{c_i^T e} \leq K, \quad \forall e, y \tag{2.3}$$

where c_i^T denote the i^{th} row vector of C and $c_i^T e \neq 0$ [Suykens & Vandewalle (1996)]. Hence, the error system $\mathcal{E}$ is also given in the structure of fractional order Lur'e type system and its nonlinearity $\eta(Ce; y)$ belongs to sector $[0, \mathcal{K}]$.

Lemma 2.2.1. [Chen *et al.* (2012)].
If the nonlinearity $\eta(Ce; y)$ belongs to sector $[0, \mathcal{K}]$, the following inequality holds:

$$||\eta(Ce; y)|| \leq d||e|| \tag{2.4}$$

where $d = \mathcal{K}\sqrt{\sum_{i=1}^m ||c_i^T c_i||}$.

Lemma 2.2.2. [Duarte-Mermoud *et al.* (2015)]. Let $x(t) \in \mathfrak{R}^n$, be a vector of differentiable function. Then for any time instant $t \geq t_0$, the following relationships holds:

$$D_t^\alpha x^T(t)Px(t) \leq 2x^T(t)PD_t^\alpha x(t), \qquad 0 < \alpha \leq 1 \tag{2.5}$$

where $P \in \mathfrak{R}^{n\times n}$ is a constant, square, symmetric and positive definite matrix.

Lemma 2.2.3. [Chen & Zhang (2007)]. Let s and q be real vectors of appropriate dimensions. For any positive scalar μ, we have:

$$2s^T q \leq \mu s^T s + \frac{1}{\mu} q^T q. \tag{2.6}$$

Lemma 2.2.4. [Duarte-Mermoud *et al.* (2015)]. Let $x = 0$ be an equilibrium point for the following fractional order nonlinear system:

$$D_t^\alpha x(t) = f(t, x) \tag{2.7}$$

and $\mathcal{L}(t)$ be a Lyapunov function, and let class-k functions $\gamma_i \ \ (i = 1, 2, 3)$ such that:

$$\begin{aligned} &(a) \quad \gamma_1 ||x|| \leq \mathcal{L}(t, x) \leq \gamma_2 ||x|| \\ &(b) \quad D_t^\alpha \mathcal{L}(t, x) \leq -\gamma_3 ||x|| \end{aligned} \tag{2.8}$$

where $1 \geq \alpha > 0$. Then, the equilibrium point $x = 0$ is asymptotically stable.

The stability of the error system $\mathcal{E}$ given in equation (2.2) is explored in order to obtain a synchronization criterion.

Theorem 2.2.1. *Suppose $\sigma(\cdot)$ belongs to sector $[0, \mathcal{K}]$ and there exists matrix $0 < P = P^T \in \mathfrak{R}^{n \times n}$, a matrix F with appropriate dimensions, $0 < \mu \in \mathfrak{R}$ and*

$$\mathfrak{M} = \left[-PA + XH - \frac{\mu}{2} I_n - \frac{d^2 \phi_{max} \left(PBB^T P \right)}{2\mu} I_n \right] > 0 \tag{2.9}$$

where $F = P^{-1}X$,I_n is the $n \times n$ identity matrix, ϕ_{max} is the maximum eigenvalue function, then the master–slave system equation (2.1) globally and asymptotically synchronized.

Proof. We consider the following quadratic and positive definite Lyapunov function, as:

$$\mathcal{L}(t) \ = \ \frac{1}{2} \left[e(t)^T P e(t) \right], \quad P = P^T > 0 \tag{2.10}$$

Taking the fractional derivative of the Lyapunov function, one obtains:

$$D_t^\alpha \mathcal{L}(t) \ = \ \frac{1}{2} \left[D_t^\alpha [e(t)^T P e(t)] \right] \tag{2.11}$$

By using the lemma (2.2.2), we can yields:

$$D_t^\alpha \mathcal{L}(t) \leq e^T P \ D_t^\alpha e(t) \tag{2.12}$$

Substituting equation (2.2) in equation (2.12), we obtain:

$$D_t^{\alpha}\mathcal{L}(t) \leq e(t)^T P\left[(A-FH)e(t)+B\eta\right] \tag{2.13}$$

By using lemmas (2.2.1) and (2.2.3), we get:

$$\begin{aligned} e(t)^T PB\eta &\leq \frac{\mu}{2}e(t)^T e(t)+\frac{1}{2\mu}\eta^T PBB^T\eta \leq \frac{\mu}{2}||e(t)||^2+\frac{1}{2\mu}||B^T P\eta||^2 \\ &\leq \frac{\mu}{2}||e(t)||^2+\frac{d^2}{2\mu}||B^T Pe(t)||^2 \leq \frac{\mu}{2}||e(t)||^2+\frac{d^2\phi_{max}\left(PBB^T P\right)}{2\mu} \\ &\quad ||e(t)||^2 \end{aligned} \tag{2.14}$$

where $\phi_{max}\left(PBB^T P\right)$ is the maximum eigenvalue of $PBB^T P$.

Substituting $e(t)^T PB\eta$ back into equation (2.13), one obtain:

$$D_t^{\alpha}\mathcal{L}(t) \leq -e(t)^T\left[-P(A-FH)-\frac{\mu}{2}I_n-\frac{d^2\phi_{max}\left(PBB^T P\right)}{2\mu}I_n\right]e(t) \tag{2.15}$$

We can conclude that:

$$D_t^{\alpha}\mathcal{L}(t) \leq -e^T(t)\mathfrak{M}e(t) \tag{2.16}$$

where:

$$\mathfrak{M}=\left[-PA+XH-\frac{\mu}{2}I_n-\frac{d^2\phi_{max}\left(PBB^T P\right)}{2\mu}I_n\right]>0 \tag{2.17}$$

with $F=P^{-1}X$. Therefore, if there is a positive symmetric matrix P, a positive scalar μ and a matrix F with appropriate dimensions that the condition of equation (2.17) is met, then $D_t^{\alpha}\mathcal{L}(t)\leq 0$ is guaranteed. Then according to lemma (2.2.4), we can conclude that the origin of the equation (2.2) is asymptotically stable. This completes the proof. □

2.2.1.2 Numerical examples

2.2.1.2.1 Fractional order Chua's circuit

To verify the effectiveness of the proposed synchronization scheme, we considere the fractional order Chua's circuit [Zhu *et al.* (2009)], as follows:

$$\begin{cases} D_t^{\alpha}x_1(t)=a(x_2(t)-x_1-h(x_1(t))) \\ D_t^{\alpha}x_2(t)=x_1(t)-x_2(t)+x_3(t) \\ D_t^{\alpha}x_3(t)=-bx_2(t) \end{cases} \tag{2.18}$$

with nonlinear characteristic $h(x_1(t)) = m_1 x_1 + \frac{1}{2}(m_0 - m_1)(|x_1(t)+1| - |x_1(t)-1|)$ and parameters $m_0 = -1.27, m_1 = -0.68, a = 10, b = 14.87$. The system can be represented in Lur'e form by:

$$A = \begin{bmatrix} -a(1+m_1) & a & 0 \\ 1 & -1 & 1 \\ 0 & -b & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} -a(m_0 - m_1); 0; 0 \end{bmatrix},$$

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

and $\sigma(Cx(t)) = \frac{1}{2}(|x_1(t)+1| - |x_1(t)-1|)$, that belongs to sector $[0, 1]$ (*i.e.* $\mathcal{K} = 1$). The system in equation (2.18) has a chaotic attractor when the fractional derivatives are set as : $\alpha \geq 0.94$ [Zhu *et al.* (2009)]. The initial conditions are selected as $x(0) = \begin{bmatrix} 0.6,\ 0.1,\ -0.6 \end{bmatrix}^T$ and $y(0) = \begin{bmatrix} 2,\ 1,\ -1.8 \end{bmatrix}^T$. Figures (2.2) and (2.3) shows the chaotic attractor of the master and the slave systems, respectively. The MATLAB LMI toolbox is used to solve the following LMI optimization problem:

$$\underset{P,\ X,\ \mu}{min}\ \Lambda(-\mathfrak{M}) \quad \text{subject to } P = P^T > 0, \mu > 0.$$

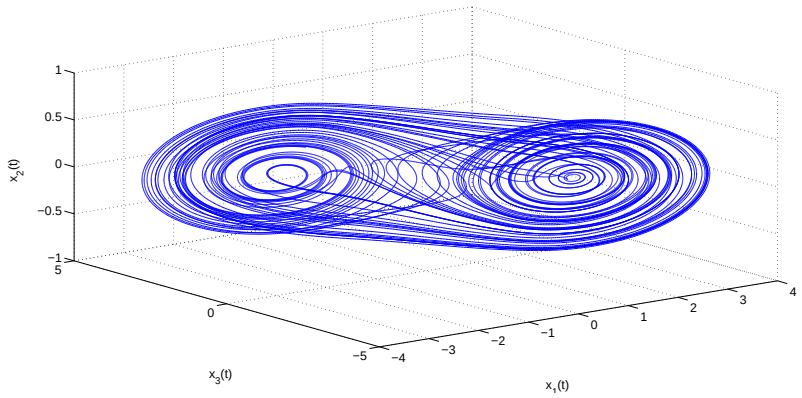


Figure 2.2 : Three-dimensional view on the double scroll attractor for the master system in fractional order Chua's circuit.

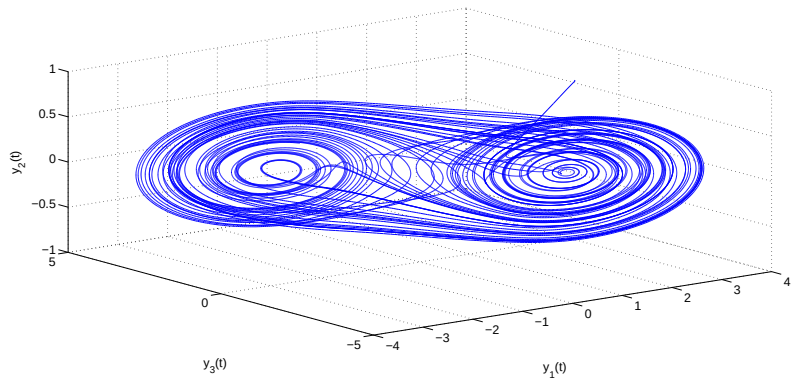


Figure 2.3 : Three-dimensional view on the double scroll attractor for the slave system in fractional order Chua's circuit.

We choose $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, The matrices P, X and F and the scalare μ are found with $d = 1$ as:

$$P = 10^{-13} \times \begin{bmatrix} 0.1416 & 0 & 0 \\ 0 & 0.1416 & 0 \\ 0 & 0 & 0.1416 \end{bmatrix},$$

$$X = 10^{-12} \times \begin{bmatrix} 0.3885 & -0.0306 & 0.0031 \\ 0.0026 & 0.3053 & -0.0289 \\ 0.0423 & -0.0284 & 0.2849 \end{bmatrix},$$

$$F = \begin{bmatrix} 27.4413 & -0.1594 & 0.2160 \\ 0.1823 & 21.5608 & -2.0389 \\ 2.9862 & -0.0074 & 20.1183 \end{bmatrix},$$

$\mu = 10^{-13} \times 3.1149$.

Moreover, one can easily found that:

$$\mathfrak{M} = 10^{-12} \times \begin{bmatrix} 0.0141 & -0.1722 & 0.0031 \\ -0.0116 & 0.0413 & -0.0430 \\ 0.0423 & 0.1821 & 0.0067 \end{bmatrix},$$

is a positive definite matrix. The synchronization errors between the master and the slave systems are shown in figure (2.4). It shows that the synchronization errors, converges to zero asymptotically. The trajectories of the state variables of the master and the slave systems are depicted in figures (2.6), (2.8) and (2.10). It can be seen that the state trajectories of the slave track those of the master.

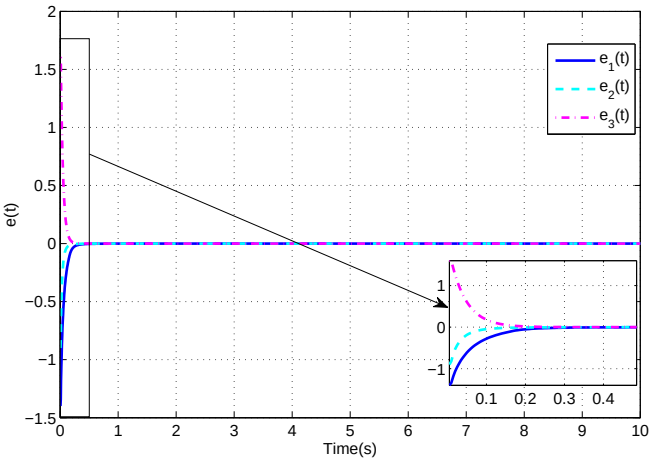


Figure 2.4 : The trajectories of the synchronization errors of fractional order Chua's circuit.

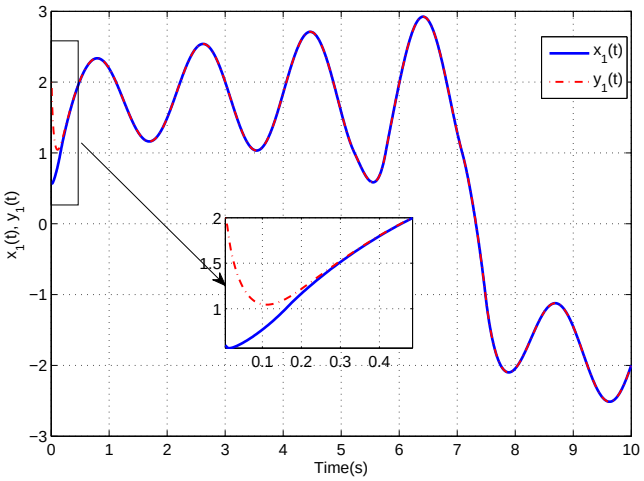


Figure 2.5 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order Chua's circuit.

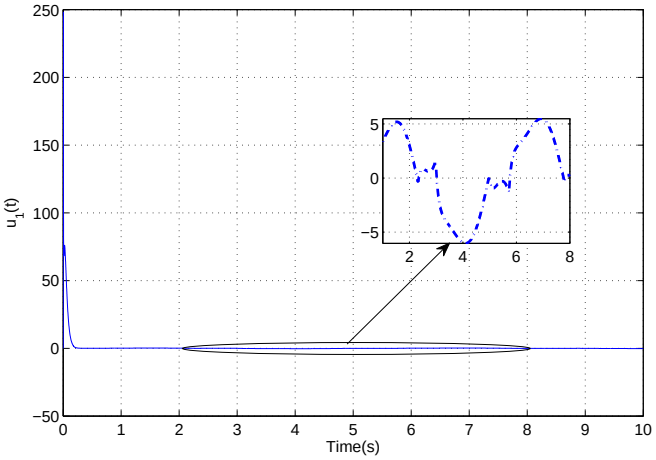


Figure 2.6 : The trajectory of the control input $u_1(t)$ in fractional order Chua's circuit.

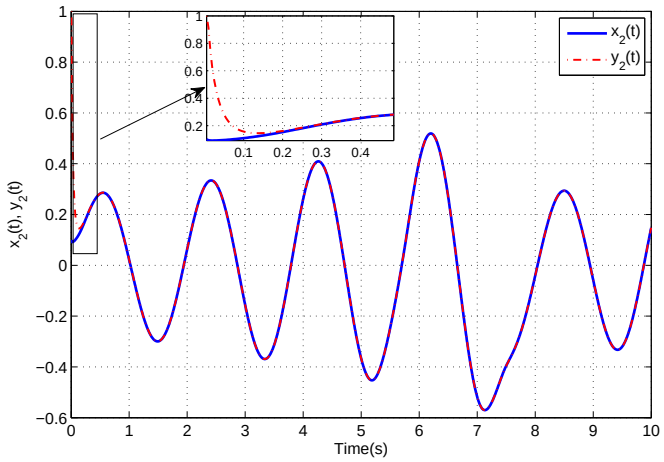


Figure 2.7 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order Chua's circuit.

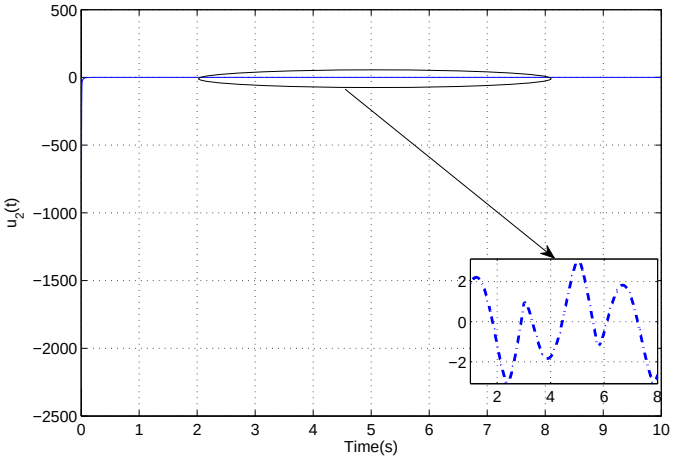


Figure 2.8 : The trajectory of the control input $u_2(t)$ in fractional order Chua's circuit.

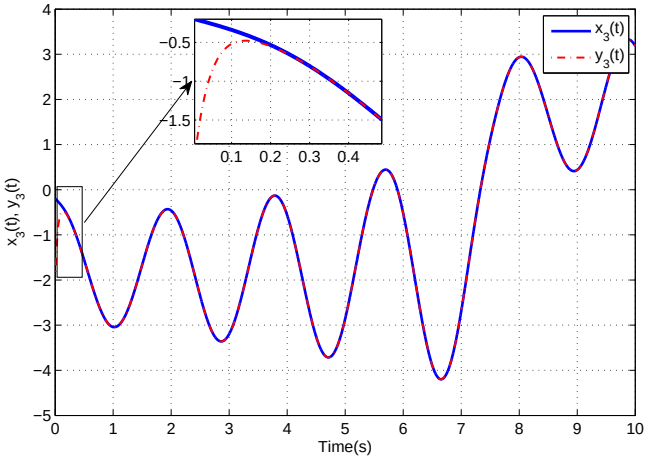


Figure 2.9 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order Chua's circuit.

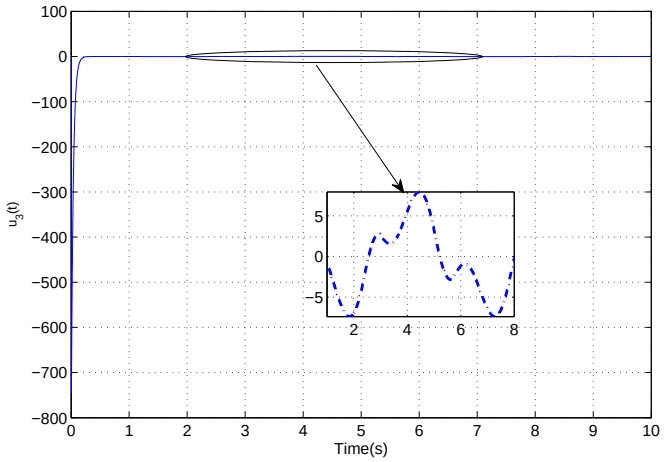


Figure 2.10 : The trajectory of the control input $u_3(t)$ in fractional order Chua's circuit.

2.2.1.2.2 Fractional order four-cell CNN

Now, let us consider the following fractional order four-cell CNN [Huang *et al.* (2012)]:

$$\begin{cases} D_t^\alpha x_1(t) = -x_3(t) - x_4(t) \\ D_t^\alpha x_2(t) = 2x_2(t) + x_3(t) \\ D_t^\alpha x_3(t) = 14x_1(t) - 14x_2(t) \\ D_t^\alpha x_4(t) = 100(x_1(t) - x_4(t) + h(x_4(t))) \end{cases} \tag{2.19}$$

with nonlinear characteristic $h(x_4(t)) = (|x_4(t)+0.8| - |x_4(t)-0.8| + |x_4(t)-0.4| - |x_4(t)+0.4|)$. The system can be represented in Lur'e form [Suykens *et al.* (1997)] by:

$$A = \begin{bmatrix} 0 & 0 & -1 & -1 \\ 0 & 2 & 1 & 0 \\ 14 & -14 & 0 & 0 \\ 100 & 0 & 0 & -100 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 200 & -200 \end{bmatrix},$$

$$C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and $\sigma(Cx(t)) = \begin{bmatrix} \sigma_1(C_1x(t)) \\ \sigma_2(C_2x(t)) \end{bmatrix}$ with $\sigma_1(C_1x(t)) = \frac{1}{2}(|x_4(t)+0.8| - |x_4(t)-0.8|)$ and $\sigma_2(C_2x(t)) = \frac{1}{2}(|x_4(t)+0.4| - |x_4(t)-0.4|)$, that belongs to sector $[0,1]$ (*i.e.* $\mathcal{K} = 1$)[Suykens *et al.* (1997)].

The system in equation (2.19) has a chaotic attractor when the fractional derivatives are set as : $\alpha \geq 0.97$ [Huang *et al.* (2012)]. The initial conditions are selected as

$x(0) = \left[\ 0.3,\ 0.3,\ -0.2,\ 0.2\ \right]^T$ and $y(0) = \left[\ 0.5,\ 0.9,\ -0.7,\ 0.9\ \right]^T$. Figures (2.11) and (2.12) show the chaotic attractor of the master and the slave systems, respectively. The same LMI optimization process has been applied as for fractional order Chua's circuit.

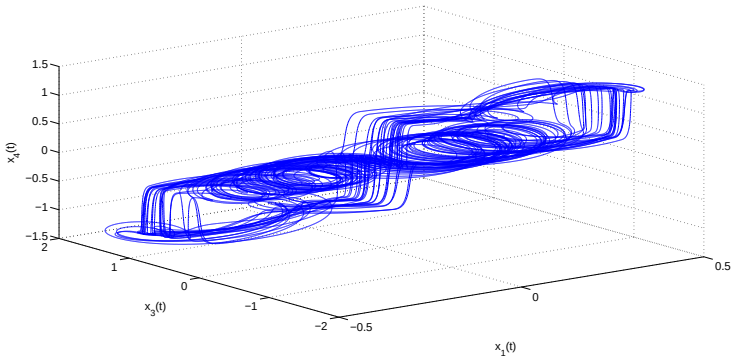


Figure 2.11 : Three-dimensional view on the double scroll attractor for the master system in fractional order four-cell CNN.

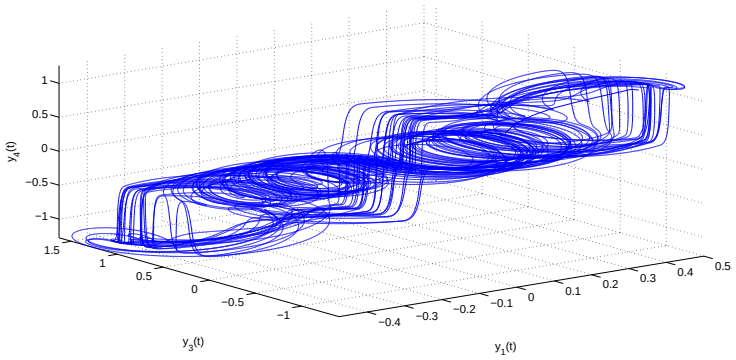


Figure 2.12 : Three-dimensional view on the double scroll attractor for the master system in fractional order four-cell CNN.

We choose $H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, the matrices P , X and F and the scalare μ are found using MATLAB LMI optimization toolbox with $d = 1$ as:

$$P = 10^{-14} \times \begin{bmatrix} 0.2031 & 0 & 0 & 0 \\ 0 & 0.2031 & 0 & 0 \\ 0 & 0 & 0.2031 & 0 \\ 0 & 0 & 0 & 0.2031 \end{bmatrix},$$

$$X = 10^{-12} \times \begin{bmatrix} 0.4602 & -0.0204 & 0.0585 & 0.1036 \\ 0.0019 & 0.5488 & 0.0404 & 0.0207 \\ 0.0001 & 0.0000 & 0.6089 & 0.0007 \\ 0.0008 & 0.0785 & 0.1937 & 0.4805 \end{bmatrix},$$

$$F = \begin{bmatrix} 226.6389 & -10.0470 & 28.8303 & 51.0000 \\ 0.9318 & 270.2337 & 19.8900 & 10.1949 \\ 0.0459 & 0.0000 & 299.8749 & 0.3570 \\ 0.4080 & 38.6529 & 95.3700 & 236.6298 \end{bmatrix},$$

$\mu = 10^{-13} \times 5.7412$.

Moreover, one can easily found that:

$$\mathfrak{M} = 10^{-12} \times \begin{bmatrix} -0.1141 & -0.0204 & 0.0606 & 0.1056 \\ 0.0019 & -0.0297 & 0.0384 & 0.0207 \\ -0.0283 & 0.0284 & 0.0346 & 0.0007 \\ -0.2022 & 0.0785 & 0.1937 & 0.1092 \end{bmatrix},$$

is a positive definite matrix. Figure (2.13) shows that the synchronization errors, converges to zero asymptotically. the trajectories of the state variables of the master and the slave systems are depicted in figures (2.15), (2.17), (2.19) and (2.21). One can easily see that the slave system is driven to asymptotically follow the chaotic dynamics of the master one, and the controller inputs perform well.

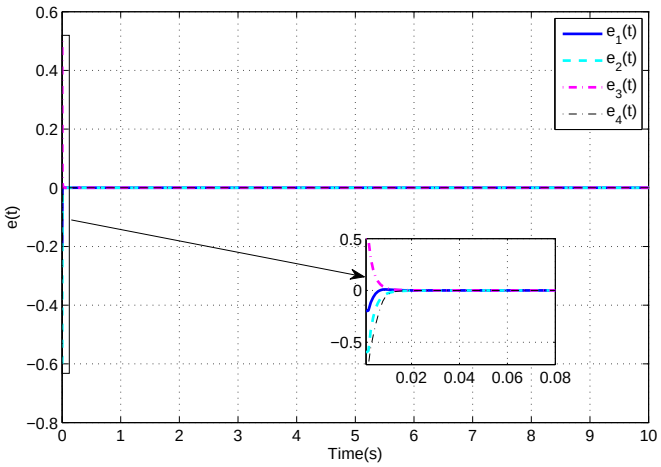


Figure 2.13 : The trajectories of the synchronization errors of fractional order four-cell CNN.

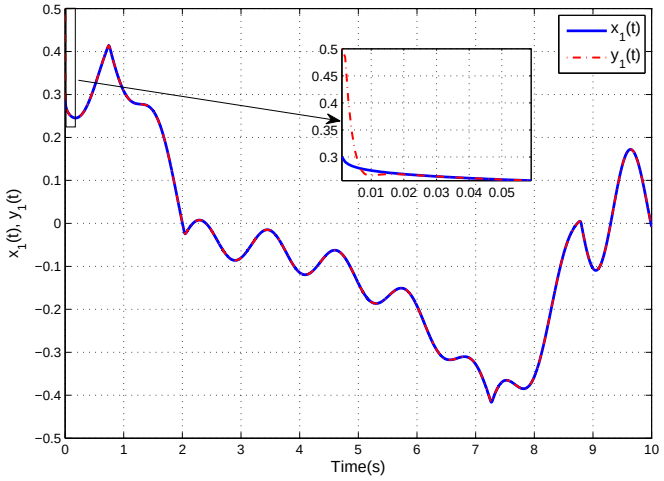


Figure 2.14 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order four cell CNN.

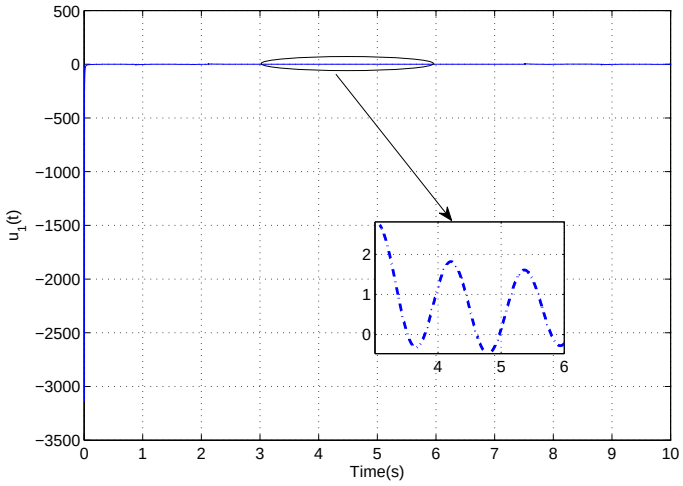


Figure 2.15 : The trajectory of the control input $u_1(t)$ in fractional order four cell CNN.

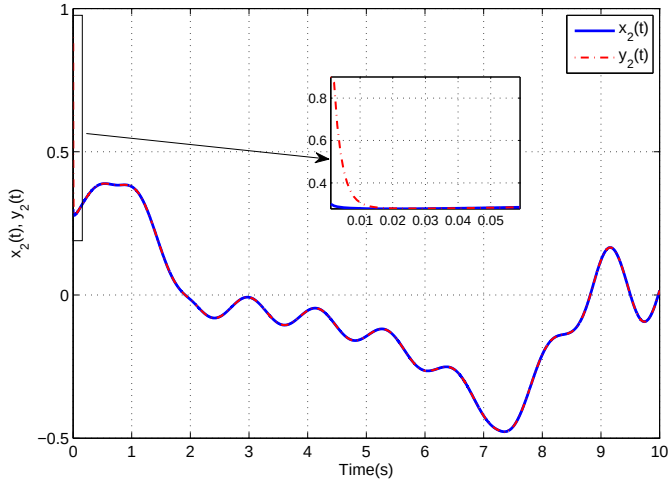


Figure 2.16 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order four cell CNN.

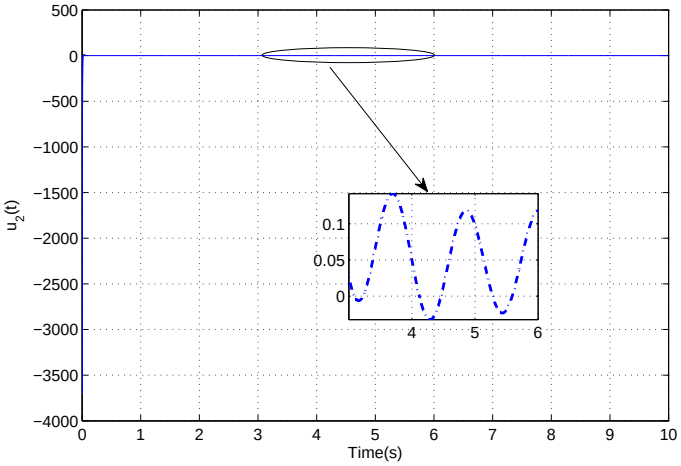


Figure 2.17 : The trajectories of the state variables $u_2(t)$ in fractional order four cell CNN.

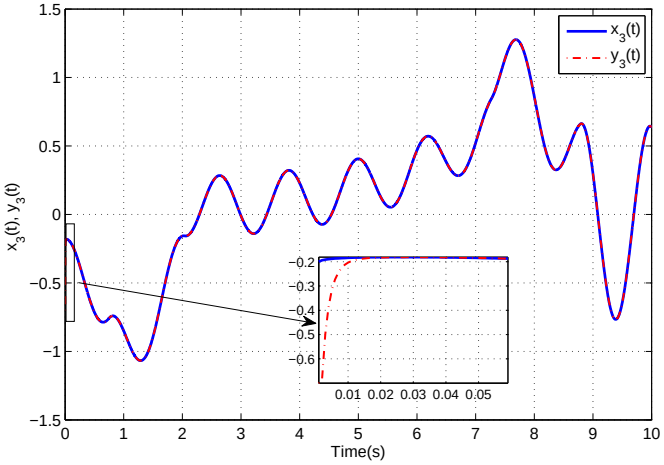


Figure 2.18 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order four cell CNN.

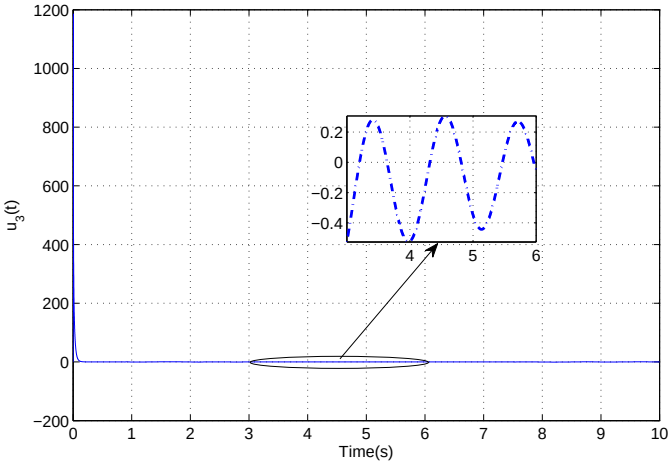


Figure 2.19 : The trajectory of the control input $u_3(t)$ in fractional order four cell CNN.

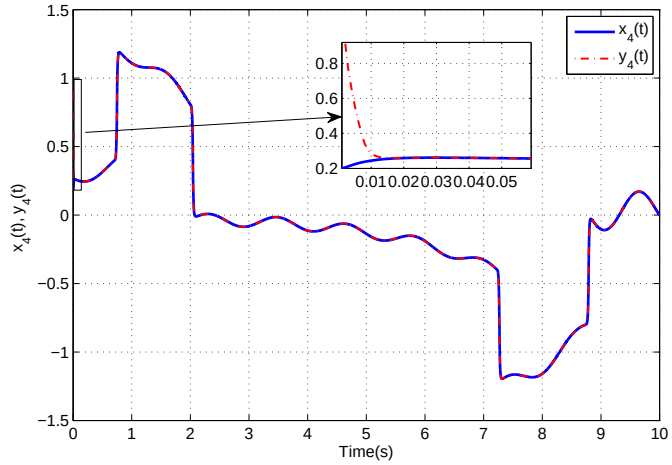


Figure 2.20 : The trajectories of the state variables $x_4(t)$ and $y_4(t)$ in fractional order four cell CNN.

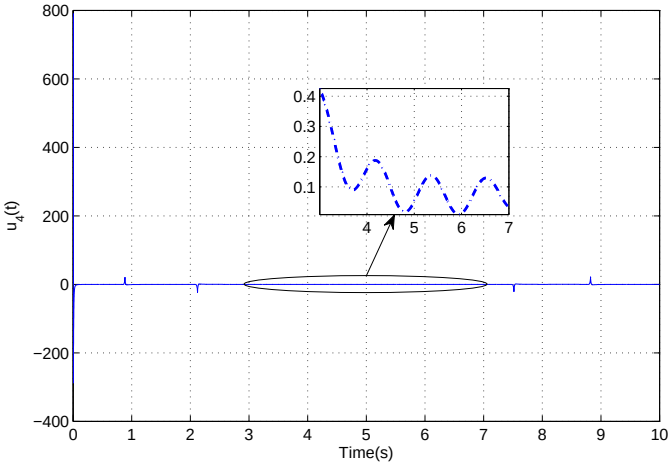


Figure 2.21 : The trajectories of the state variables $u_4(t)$ in fractional order four cell CNN.

2.2.2 Discusion

A master-slave synchronization scheme for fractional order Lur'e systems is considered in this section. A sufficient condition for the asymptotic stability of the error system was given and successfully applied to fractional order Chua's circuits and fractional order four-cell CNN's. Numerical simulations confirm the theoretical results and they prove the effectiveness of the proposed scheme. It worth saying that the proposed scheme is also validated to be applied on other circuits of fractional order Lur'e systems.

2.3 Master-slave synchronization of fractional order Lur'e systems with different derivatives and time delay

In this section, we addresses the synchronization problem between two non-identical chaotic fractional order Lur'e systems with a time delay between them (i.e. with a delayed feedback controller). Based on an Lyapunov function we derive the synchronization criterion, witch is a suffcient condition for the asymptotic stability of the error system. The designed controller ensures the synchronization. Numerical simulations are performed to show the performance of the proposed scheme. Our Main contributions of this scheme are as follows:

- The master and the slave systems, considered here, are assumed to be with non-identical fractional derivatives.
- The sysnchronization between commensurate and incommensurate fractional order Lur'e can be achieved.
- We take in consideration the propagation time-delay in the master-slave configuration.

2.3.1 Chaos synchronization

2.3.1.1 Probleme formulation

The main objective of this scheme is to synchronize the master system $\mathcal{M}$ and the slave system $\mathcal{S}$. Consider the following master–slave synchronization scheme as:

$$\begin{aligned}
\mathcal{M}: &\begin{cases} D_t^{\alpha} x(t) &= Ax(t) + B\sigma(Cx(t)) \\ p(t) &= Hx(t) \end{cases} \\
\mathcal{S}: &\begin{cases} D_t^{\beta} y(t) &= Ay(t) + B\sigma(Cy(t)) + u(t) \\ q(t) &= Hy(t) \end{cases} \\
\mathcal{C}: &\quad \Big\{ u(t) = D_t^{\beta} x(t) - D_t^{\alpha} y(t) - D_t^{\beta} e(t) + F(p(t-\tau) - q(t-\tau))
\end{aligned} \tag{2.20}$$

The state vectors of the master and slave systems are $x \in \mathfrak{R}^n$ and $y \in \mathfrak{R}^n$, respectively. The matrices $A \in \mathfrak{R}^{n\times n}$, $B \in \mathfrak{R}^{n\times n_h}$, $C \in \mathfrak{R}^{n_h\times n}$ and $H \in \mathfrak{R}^{n\times n}$ are known real constant matrices. $p(t) \in \mathfrak{R}^m$ and $q(t) \in \mathfrak{R}^m$ are the outputs of the master and the slave systems, respectively. $u(t) \in \mathfrak{R}^n$ is the control signal with feedback matrix $F \in \mathfrak{R}^{n\times n}$. $\sigma(\cdot) : \mathfrak{R}^{n_h} \to \mathfrak{R}^{n_h}$ satisfies a sector condition [Khalil (1993), Suykens & Vandewalle (1996), Yalçin *et al.* (2001)]. The following assumption will be useful to derive our main result:

Assumption 2.3.1. *We assume the following equality:*

$$D_t^{\beta} y(t) \;= D_t^{\alpha} D_t^{-\theta} y(t) = D_t^{\alpha-\theta} y(t) \tag{2.21}$$

where according to the property in equation (A.12), if $\alpha \geq \theta \geq 0$ then the relationship in equation (2.21) holds.

In this section D_t^{α}, D_t^{β} and D_t^{θ} stands for Rieman-Liouville derivatives, and for simplicity we note $\eta(Ce(t); y) = \eta(Ce; y) = \eta$.
Defining the synchronization error as $e(t) = x(t) - y(t)$.
Now, one introduces a new error variable $\hat{e}$ such that:

$$\hat{e}(t) = x(t) - D_t^{-\theta} y(t) \tag{2.22}$$

Using equation (2.20), the fractional derivative of equation (2.22) is as follows:

$$D_t^{\alpha} \hat{e}(t) = Ae(t) + B\eta(Ce; y) - FHe(t-\tau) - D_t^{\beta} x(t) + D_t^{\alpha} y(t) + D_t^{\beta} e(t) \tag{2.23}$$

where $e(t) = x(t) - y(t)$. Replicing equation (2.22) in equation (2.23) we have:

$$D_t^{\alpha}(y(t)+e(t)) - D_t^{\alpha}D_t^{-\theta}(x(t)-e(t)) = \quad Ae(t) + B\eta(Ce(t);y) - FHe(t-\tau) - D_t^{\beta}x(t) + D_t^{\beta}e(t) + D_t^{\alpha}y(t) \tag{2.24}$$

Using the properties (A.12), we yield to:

$$D_t^{\alpha}e(t) + D_t^{\alpha}y(t) - D_t^{\beta}x(t) + D_t^{\beta}e(t) = \quad Ae(t) + B\eta(Ce;y) - FHe(t-\tau) - D_t^{\beta}x(t) + D_t^{\beta}e(t) + D_t^{\alpha}y(t) \tag{2.25}$$

Thus, the error dynamic can be obtained as:

$$\mathcal{E}: \ \{D_t^{\alpha}e(t) = Ae(t) - FHe(t-\tau) + B\eta \tag{2.26}$$

The nonlinearity $\sigma(\cdot)$ belongs to sector $[0, \mathcal{K}]$ and the nonlinearity $\eta(Ce;y)$ satisfies equation (2.3). Hence, the error system $\mathcal{E}$ is also given in the structure of fractional order Lur'e type system and its nonlinearity $\eta(Ce;y)$ belongs to sector $[0, \mathcal{K}]$.

Lemma 2.3.1. (Barbalat's lemma)[Khalil (1993)] Assume that $f(t)$ is a function of time and has a limit when $t \to \infty$, if $\dot{f}(t)$is uniformly continuous ($\ddot{f}(t)$is bounded), then $\dot{f}(t) \to 0$ as $t \to \infty$.

Lemma 2.3.2. [Li *et al.* (2016)]. Let $x(t) \in \mathfrak{R}^n$, be a continuous and differentiable function. If the derivative of $x(t)$ is integrable, then the following inequalies holds:

$$D_t^{\alpha}x^T(t)Px(t) \leq 2x^T(t)PD_t^{\alpha}x(t), \qquad 0 < \alpha \leq 1 \tag{2.27}$$

where $P \in \mathfrak{R}^{n\times n}$ is a constant, square, symmetric and positive definite matrix.

Lemma 2.3.3. [Zhang *et al.* (2018)]
For any positive definite matrix $Q > 0$, a scalar $\tau > 0$, vector function, $f(.) : [0, \tau] \to \mathfrak{R}^n$ such that the integrations concerned are well defined, the following inequality holds :

$$\left(\int_0^{\tau} f(s)ds\right)^T Q \left(\int_0^{\tau} f(s)ds\right) \leq \tau \left(\int_0^{\tau} f^T(s)Qf(s)ds\right) \tag{2.28}$$

The stability of the error system $\mathcal{E}$ given in equation (2.26) is explored in order to obtain a synchronization criterion.

Theorem 2.3.1. *for a given $\tau > 0$ and suppose $\sigma(\cdot)$ belongs to sector $[0, \mathcal{K}]$, the error system described as equation (2.26) is asymptoticly stable if there exists the matrices*

$P = P^T > 0$, $R = R^T > 0$, $Q = Q^T > 0$ a matrix F with appropriate dimensions and constant positive scalars μ_1 and μ_2 there is a solution of the following optimization problem:

$$\begin{aligned}
&\underset{P,\ X,\ R,\ \mu_{j=1,\ 2}}{min} \\
&Z = \\
&\begin{bmatrix} 2PA + \mu_1 I + \frac{d^2\phi_{max}\left(PBB^TP\right)}{\mu_1} I - \mu_2 I + \tau Q + R & 0 & 0 \\ 0 & -\frac{\phi_{max}\left(XHH^TX^T\right)}{\mu_2} I - R & 0 \\ 0 & 0 & \frac{-1}{\tau} Q \end{bmatrix} \\
&< 0
\end{aligned} \tag{2.29}$$

where $F = P^{-1}X$, I is the $n \times n$ identity matrix and ϕ_{max} is the maximum eigenvalue function. then the master–slave system equation (2.20) globally and asymptotically synchronized.

Proof. Let us construct a Lyapunov function as:

$$\begin{aligned}
\mathcal{L}(t) = \quad & D_t^{-(1-\alpha)} \left[e^T(t)Pe(t)\right] + \int_{-\tau}^{0} \int_{t+s}^{t} e^T(\psi)Qe(\psi)d\psi ds + \int_{t-\tau}^{t} e(\Theta)^T Re(\Theta) \\
& d\Theta
\end{aligned} \tag{2.30}$$

where the function is reduced to the classical Lyapunov-Krasovskii function when $\alpha = 1$ (see property in equation (A.9)), and the term $D_t^{-(1-\alpha)}[e^T(t)Pe(t)]$ is constructed as a Rieman-Liouville fractional integral when $1 > \alpha > 0$, thus according to equation (1.22) and integral property the positive defitiveness for the function is guaranted.

An application of property in equation (A.16), we get the time derivative of equation (2.30) as:

$$\begin{aligned}
\dot{\mathcal{L}}(t) = \quad & D_t^{\alpha}[e(t)^T Pe(t)] + \tau e^T(t)Qe(t) - \int_{t-\tau}^{t} e^T(\Theta)Qe(\Theta) + e^T(t)Re(t) - \\
& e^T(t-\tau)Re(t-\tau)
\end{aligned} \tag{2.31}$$

Using the lemma (2.3.3) ylieds to:

$$\left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right]^T Q \left[\int_{t-\tau}^{t} e(\Theta)d\sigma\right] \leq \tau \int_{t-\tau}^{t} e(\Theta)^T Qe(\Theta)d\Theta \tag{2.32}$$

thus, we have:

$$\dot{\mathcal{L}}(t) \leq \quad D_t^{\alpha}[e(t)^T P e(t)] + \tau e^T(t) Q e(t) - \frac{1}{\tau}\left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right]^T Q \left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right] + e^T(t) \\ Re(t) - e^T(t-\tau) Re(t-\tau) \tag{2.33}$$

Using lemma (2.3.2) and substituting equation (2.26) into equation (2.33) ylieds to:

$$\dot{\mathcal{L}}(t) \leq \quad 2e^T(t) P\left[Ae(t) - FHe(t-\tau) + B\eta\right] + \tau e^T(t) Q e(t) - \frac{1}{\tau}\left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right]^T \\ Q\left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right] + e^T(t) Re(t) - e^T(t-\tau) Re(t-\tau) \tag{2.34}$$

By using lemmas (2.2.1) and (2.2.3), we get:

$$\begin{aligned} 2e(t)^T PB\eta \quad &\leq \quad \frac{\mu_1}{1} e(t)^T e(t) + \frac{1}{\mu_1} \eta^T PBB^T \eta \leq \mu_1 ||e(t)||^2 + \frac{1}{\mu_1} ||B^T P\eta||^2 \\ &\leq \quad \mu ||e(t)||^2 + \frac{d^2}{\mu_1} ||B^T Pe(t)||^2 \leq \mu_1 ||e(t)||^2 + \frac{d^2 \phi_{max}\left(PBB^T P\right)}{\mu_1} \\ &\quad ||e(t)||^2 \end{aligned} \tag{2.35}$$

and

$$\begin{aligned} 2e^T(t) PFHe(t-\tau) \quad &\leq \mu_2 ||e(t)||^2 + \frac{1}{\mu_2} ||H^T F^T Pe^T(t-\tau)||^2 \leq \mu_2 ||e^T(t)||^2 + \\ &\quad \frac{\phi_{max}\left(PFHH^T F^T P\right)}{\mu_2} ||e(t-\tau)||^2 \end{aligned} \tag{2.36}$$

where $\phi_{max}(\cdot)$ represnt the maximum eigenvalue of a matrix.

Replicing all we ylieds to:

$$\dot{\mathcal{L}}(t) \leq \quad e^T(t)\left[2PA + \mu_1 + \frac{d^2 \phi_{max}\left(PBB^T P\right)}{\mu_1} - \mu_2 + \tau Q + R\right] - e^T(t-\tau) \\ - \left[\frac{\phi_{max}\left(PFH^T HF^T P\right)}{\mu_2} + R\right] e(t-\tau) - \frac{1}{\tau}\left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right]^T Q \\ \left[\int_{t-\tau}^{t} e(\Theta) d\Theta\right] \tag{2.37}$$

We can conclude that:

$$\dot{L}(t) \leq \xi(t)^T \mathfrak{M} \xi(t) < 0 \tag{2.38}$$

where $\xi(t) = [e(t); e(t-\tau); \int_{t-\tau}^{t} e(\Theta)d\Theta]$ and $\mathfrak{M} =$

$$\begin{bmatrix} 2PA + \mu_1 I + \frac{d^2\phi_{max}(PBB^TP)}{\mu_1} I - \mu_2 I + \tau Q + R & 0 & 0 \\ 0 & -\frac{\phi_{max}(XHH^TX^T)}{\mu_2} I - R & 0 \\ 0 & 0 & \frac{-1}{\tau} Q \end{bmatrix}$$

with $X = PF$. Then if $\mathfrak{M} < 0$, then $\dot{\mathcal{L}}(t) \leq 0$. To derive asymptotical stability we use lemma (2.3.1). Form $\dot{\mathcal{L}}(t) < 0$ it obtain that $\mathcal{L}(t) < \mathcal{L}(0)$. To verify the boudennes of $\ddot{\mathcal{L}}(t)$, it needs to show that $\xi(t) \in \ell_2$. Note that $\mathcal{L}$ is a non-increasing and positive definite function then:

$$-\int_0^t \dot{\mathcal{L}}(t) = \mathcal{L}(0) - \mathcal{L}(t) < \infty \tag{2.39}$$

$$\begin{aligned} &-\int_0^t \dot{\mathcal{L}}(t)d\tau < \infty \\ &\Rightarrow \int_0^t [\Lambda_{min}(-\mathfrak{M})||\xi(t)||^2]d\tau < \infty \\ &\Rightarrow \sqrt{\int_0^t [\Lambda_{min}(-\mathfrak{M})||\xi(t)||^2]d\tau} < \infty \\ &\Rightarrow \sqrt{\int_0^t ||\xi(t)||^2 d\tau} < \infty \end{aligned} \tag{2.40}$$

where $\Lambda_{min}(-\mathfrak{M})$ represent the minimum eigenvalues of $-\mathfrak{M}$. From equation (3.16), it is concluded that $\xi(t) \in \ell_2$. Then it is derived that $\lim_{t\to\infty} \dot{\mathcal{L}}(t) = 0$, the asymptotic stability is concluded. This completes the proof. □

2.3.1.2 Numerical examples

2.3.1.2.1 Fractional order Chua's circuit

To verify the effectiveness of the proposed synchronization scheme, we considere the fractional order Chua's circuit in equation (2.18). We set the fractional derivatives for the slave system as : $\beta \geq 0.94$ and for the master system as $\alpha = 1$. The initial conditions are selected as $x(0) = \begin{bmatrix} 0.6,\ 0.1,\ -0.6 \end{bmatrix}^T$ and $y(0) = \begin{bmatrix} 2,\ 1,\ -1.8 \end{bmatrix}^T$.

We choose $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, The matrices $P,\ R,\ X$ and Q and the scalares $\mu_{i=1,\ 2}$ are found such that $d = 1$ and $\tau = 0.18$ as:

$$P = 10^7 \times \begin{bmatrix} 2.1777 & -0.6045 & -0.0807 \\ -0.6045 & 0.4997 & 0.6894 \\ -0.0807 & 0.6894 & 1.5642 \end{bmatrix},$$

$$X = 10^8 \times \begin{bmatrix} 4.5810 & 0 & 0 \\ 0 & 4.5810 & 0 \\ 0 & 0 & 4.5810 \end{bmatrix},$$

$$F = \begin{bmatrix} 92.7720 & 232.1013 & -90.6030 \\ 232.1013 & 950.3051 & -372.6875 \\ -90.6030 & -372.6875 & 194.7487 \end{bmatrix},$$

$$R = 10^8 \times \begin{bmatrix} 2.9753 & -0.8866 & -1.2930 \\ -0.8866 & 0.9465 & 0.4386 \\ -1.2930 & 0.4386 & 2.3170 \end{bmatrix},$$

$$Q = 10^8 \times \begin{bmatrix} 3.6542 & -0.1669 & -0.2358 \\ -0.1669 & 3.2825 & 0.0774 \\ -0.2358 & 0.0774 & 3.5368 \end{bmatrix},$$

$\mu_1 = 10^5 \times 6.6724,$

$\mu_2 = 10^8 \times 1.4873.$

Moreover, one can easily find that $\mathfrak{M}$ is a negative definite matrix. The synchronization errors between the master and the slave systems. The synchronization errors between the master and the slave systems are shown in figure (2.22). It shows that the synchronization errors, converges to zero asymptotically. The trajectories of the state variables of the master and the slave systems are depicted in figures (2.24), (2.26) and (2.28). It can be seen that the state trajectories of the slave track those of the master.

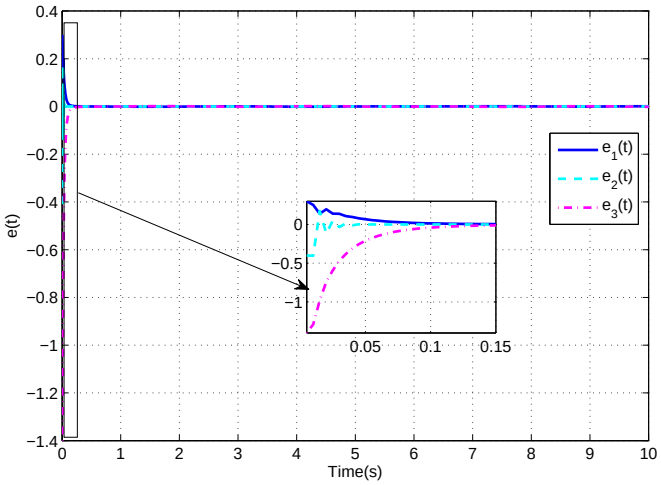


Figure 2.22 : The trajectories of the synchronization errors of fractional order Chua's circuit.

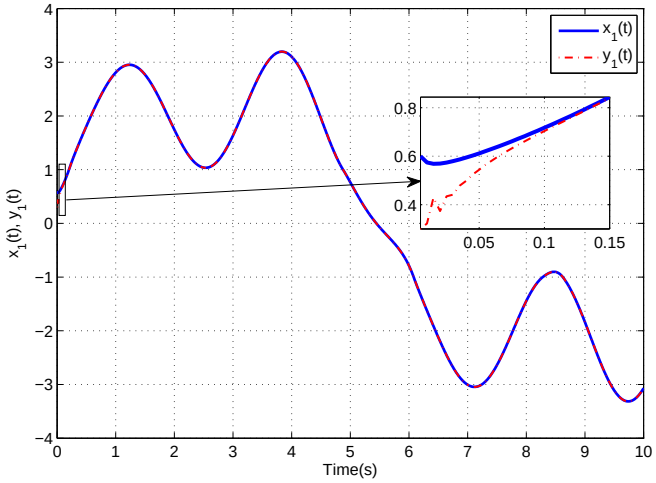


Figure 2.23 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order Chua's circuit.

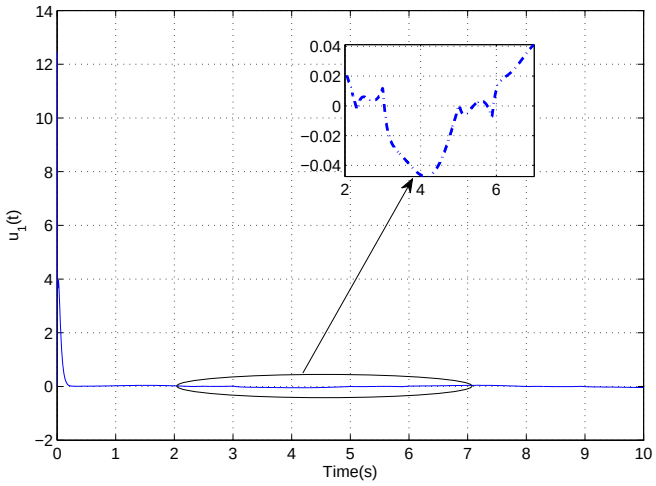


Figure 2.24 : The trajectory of the control input $u_1(t)$ in fractional order Chua's circuit.

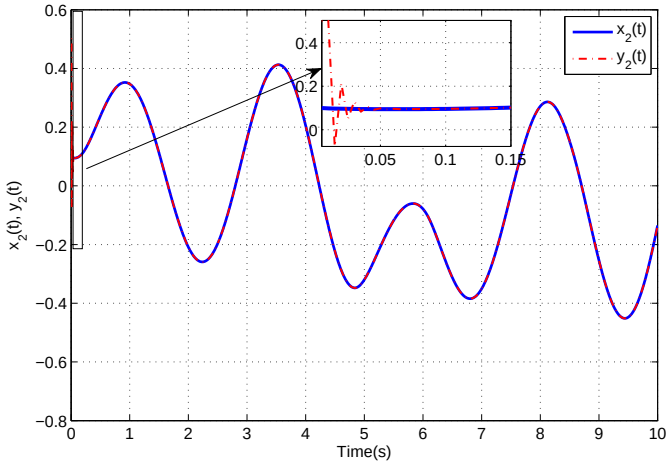


Figure 2.25 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order Chua's circuit.

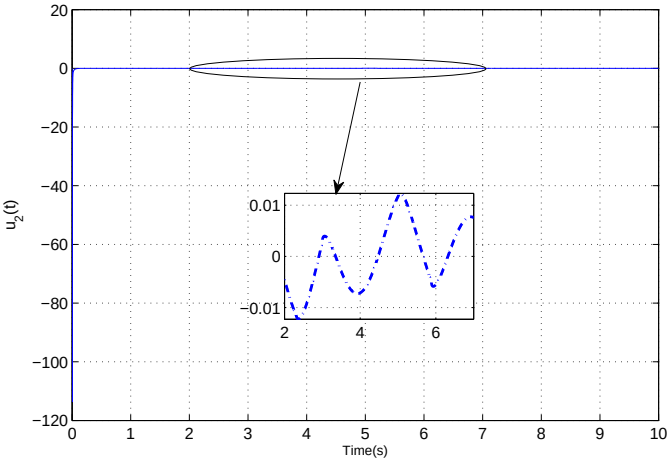


Figure 2.26 : The trajectory of the control input $u_2(t)$ in fractional order Chua's circuit.

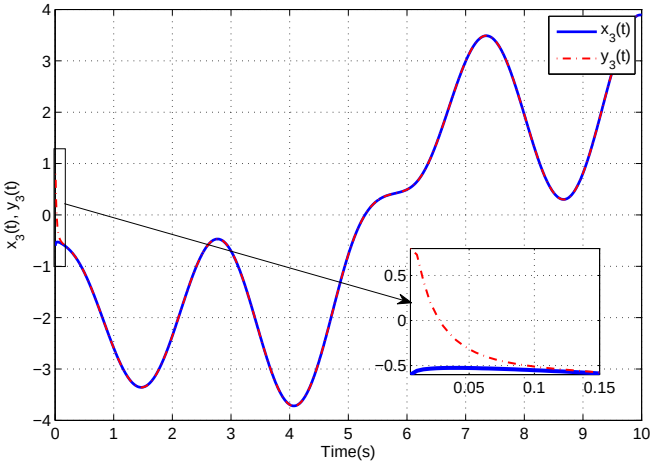


Figure 2.27 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order Chua's circuit.

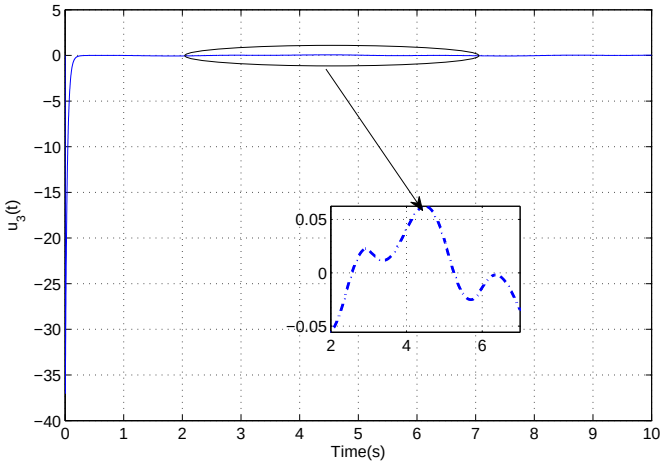


Figure 2.28 : The trajectory of the control input $u_3(t)$ in fractional order Chua's circuit.

2.3.1.2.2 Fractional order four-cell CNN

Let consider the fractional order four-cell CNN in equation (2.19) as the master system. We set the fractional derivatives as: $\alpha = 1$ and for the slave system $\beta \geq 0.97$. The initial conditions are selected as $x(0) = \begin{bmatrix} 0.3,\ 0.3,\ -0.2,\ 0.2 \end{bmatrix}^T$ and $y(0) = \begin{bmatrix} 0.5,\ 0.9,\ -0.7,\ 0.9 \end{bmatrix}^T$. We choose $H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, The matrices $P,\ R,\ X$ and Q and the scalares $\mu_{i=1,\ 2}$ are found such that $d = 1$ and $\tau = 0.63$ as:

$$P = 10^4 \times \begin{bmatrix} 0.2491 & 0.0394 & -0.4092 & 0.0567 \\ 0.0394 & 0.1552 & 0.0756 & 0.0200 \\ -0.4092 & 0.0756 & 1.1450 & -0.2157 \\ 0.0567 & 0.0200 & -0.2157 & 4.3106 \end{bmatrix},$$

$$X = 10^8 \times \begin{bmatrix} 4.9354 & 0 & 0 & 0 \\ 0 & 4.9354 & 0 & 0 \\ 0 & 0 & 4.9354 & 0 \\ 0 & 0 & 0 & 4.9354 \end{bmatrix},$$

$$R = 10^3 \times \begin{bmatrix} 5.1364 & 0.1087 & -0.1980 & 0.2568 \\ 0.1087 & 3.7535 & 0.0735 & -0.0599 \\ -0.1980 & 0.0735 & 5.6397 & 0.0180 \\ 0.2568 & -0.0599 & 0.0180 & 6.0337 \end{bmatrix},$$

$$Q = 10^4 \times \begin{bmatrix} 1.1850 & 0.0213 & -0.0347 & 0.0325 \\ 0.0213 & 0.9394 & 0.0157 & -0.0089 \\ -0.0347 & 0.0157 & 1.2657 & 0.0030 \\ 0.0325 & -0.0089 & 0.0030 & 1.3240 \end{bmatrix},$$

$\mu_1 = 10^3 \times 3.0958,$
$\mu_2 = 10^4 \times 5.7757.$
Thus:

$$F = \begin{bmatrix} 426.0734 & -85.1316 & 36.5653 & -265.2476 \\ -85.1316 & 219.1817 & -31.1993 & -3.8509 \\ 36.5653 & -31.1993 & 44.4060 & -6.3407 \\ -265.2476 & -3.8509 & -6.3407 & 279.2396 \end{bmatrix}.$$

Moreover, one can easily find that $\mathfrak{M}$ is a negative definite matrix. Figure (2.29) shows that the synchronization errors, converges to zero asymptotically. the trajectories of the state variables of the master and the slave systems are depicted in figures (2.31), (2.33), (2.35) and (2.37). One can easily see that the slave system is driven to asymptotically follow the chaotic dynamics of the master one.

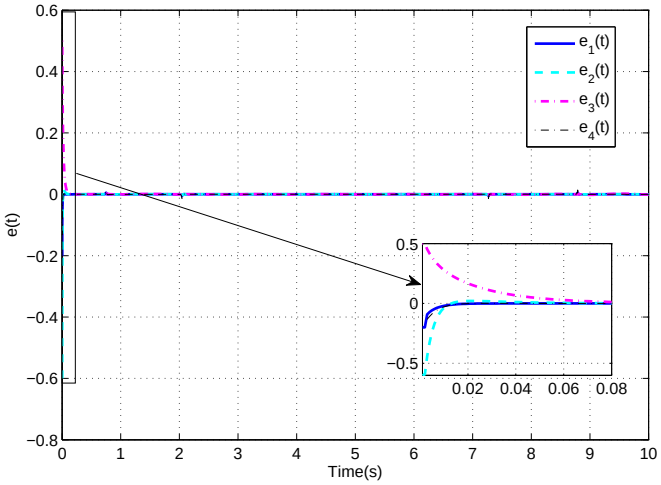


Figure 2.29 : The trajectories of the synchronization errors of fractional order four-cell CNN.

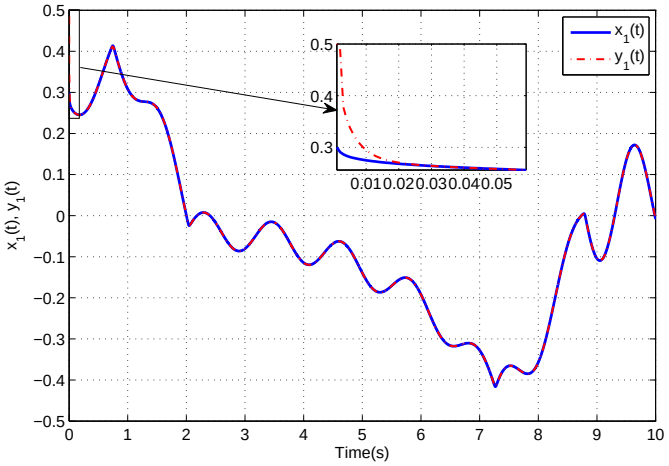


Figure 2.30 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order four cell CNN.

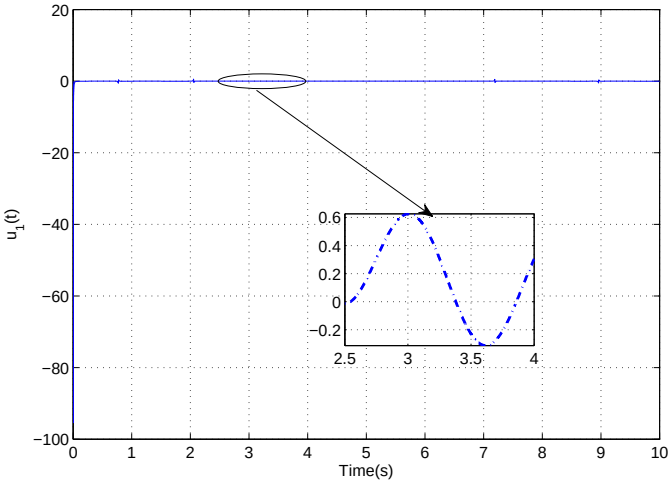


Figure 2.31 : The trajectory of the control input $u_1(t)$ in fractional order four cell CNN.

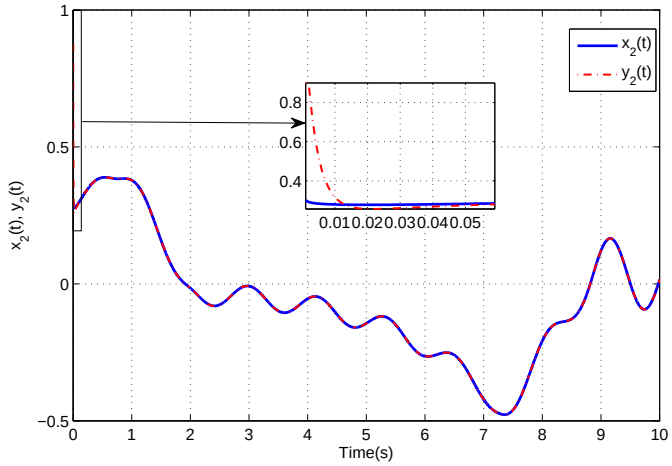


Figure 2.32 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order four cell CNN.

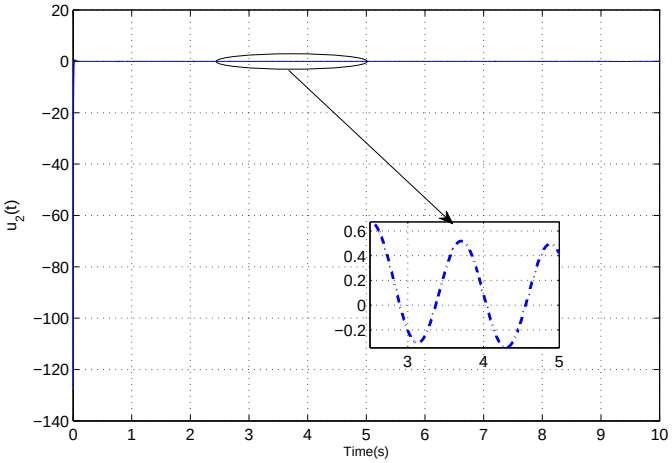


Figure 2.33 : The trajectory of the control input $u_2(t)$ in fractional order four cell CNN.

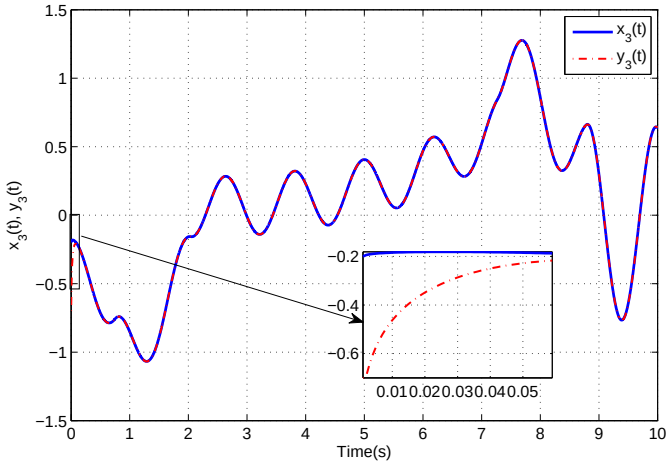


Figure 2.34 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order four cell CNN.

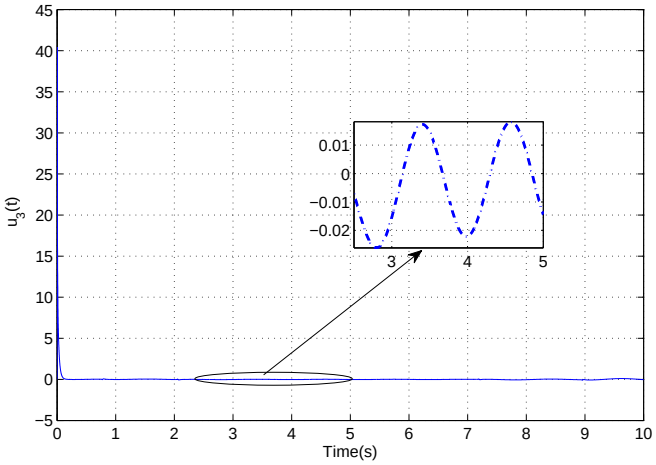


Figure 2.35 : The trajectory of the control input $u_3(t)$ in fractional order four cell CNN.

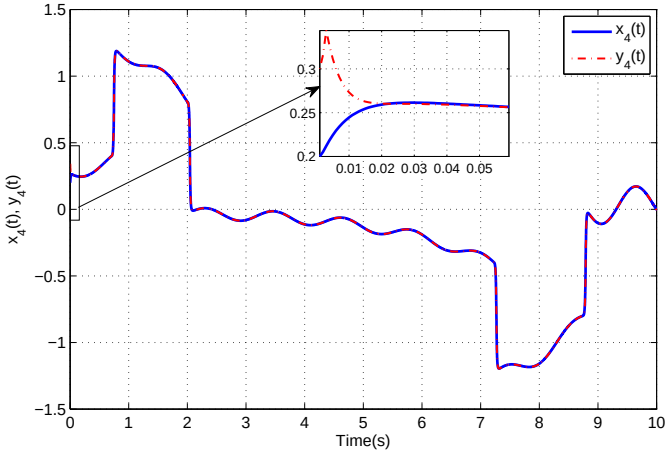


Figure 2.36 : The trajectories of the state variables $x_4(t)$ and $y_4(t)$ in fractional order four cell CNN.

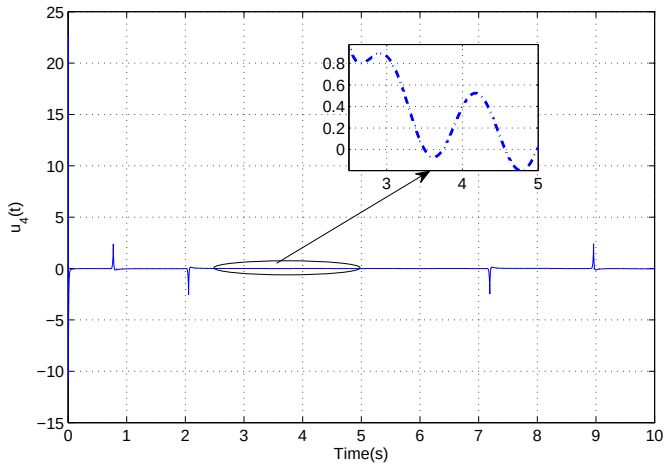


Figure 2.37 : The trajectory of the control input $u_4(t)$ in fractional order four cell CNN.

2.3.2 Discusion

In this section, we have proposed a synchronization scheme for fractional order Lur'e systems with no identical fractional derivatives and a time delay between them. The sufficient condition is attained for the asymptotic stability of the error system using the Lyapunov stability theory and some essantial concepts of fractional order calculus, where it formulated as an LMI problem. Numerical simulations have demonstrated the feasibility and effectiveness of the proposed scheme.

2.4 Conclusion

This chapter prensent two new theorems which guarantees the synchronization of chaotic fractional order chaotic Lur'e systems. The first one is for the synchronization between two identical fractional order chaotic Lur'e systems. The seconde theorem is for the synchronization between two fractional order chaotic Lur'e systems with different fractional derivatives and time delay. Numerical simulations have demonstrated the feasibility and effectiveness of the proposed schemes.

Chapter 3

Chaos synchronization: Application to chaos based image cryptography

3.1 Introduction

In chaos base image cryptography, cryptosystems completely transform the plain image into a randomly arranged pixels, forming a disorganized encrypted image. There are two kinds of cryptosystems, block and stream [Wu *et al.* (2015), Wang & Zhang (2015)]. Generally, the stream cryptosystems are much faster than the block cryptosystems, they generates a sequence of bits as a key, and the encryption is accomplished by combining it with the plain image. A lot of image cryptosystems have been developed up to now such as in [Diaconu *et al.* (2014), Rehman *et al.* (2018), Rehman & Liao (2019), Zhang *et al.* (2017)]. By DNA sequences operation, the authors in [Zhang *et al.* (2017)] shuffled the pixels value of the plain image, and by using the generated sequences from a fractional order hyperchaotic system a pemutation operation on the pixels position is performed. In [Rehman *et al.* (2018)], a cryptosystem is presented, which a SHA-2 function is used to generate the initial conditions for the chaotic systems, after a DNA exclusive-OR is perform for pixel substitution. A cryptosystem based on fractional order chaotic systems has a higher security level, in addition has an improvement on the encryption key space [Kiani *et al.* (2009)]. More recently, images cryptosystems built from fractional order chaotic systems have been proposed such as in [Bouridah *et al.* (2018), Bouridah *et al.* (2021), Wu *et al.* (2015)]. As of late, the exploration of the synchronization of fractional order chaotic systems have attracted the attention of researchers worldwide to design more committed images cryptosystems [Bouridah *et al.* (2018), Bouridah *et al.* (2021)]. In [Bouridah *et al.* (2018)], a synchronization problem via a fractional sliding mode control was investigated. Then, as an application an image cryptosystem was presented. Howeover, the existance of propagation

delay in the master-slave configuration, may jeopardize the stability of the system. Motivated by the above discussions, this chapter presente a synchronization scheme between two identical fractional order hyperchaotic systems via a static error feedback with a known time delay existing in the master-slave configuration. In an application point of view, the synchronized systems are applied in a new chaos base stream cryptosystem for images. In the confusion (scrambling) stage, two permutations processes are designed to break inter intra correlation of the plain image. The first is done by cyclic shift operations and according to the selected chaotic sequences indexes we perform the other one. In the diffusion stage, we performs the XOR and expanded XOR operations for each components of the scrambled image, to obtain the encrypted image. Compared with the existing works in the literature, the principal contributions of this study can be summarized as:

- Propagation time-delay has been considered.
- The derived criterion is a sufficient condition for the stability of the error dynamics between the master and the slave systems.
- A new chaos base stream cryptosystem.

3.2 Chaos synchronization

3.2.1 Problem formulation

The main objective of this scheme is to synchronize the master system $\mathcal{M}$ and the slave system $\mathcal{S}$. Figure (3.1) presents the proposed synchronization scheme.

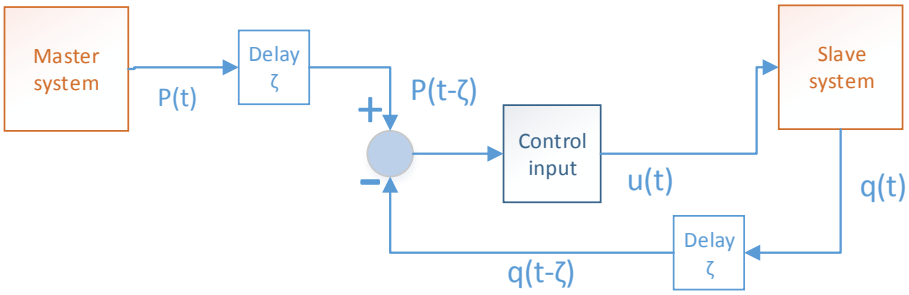


Figure 3.1 : Synchronization scheme.

Consider the following master-–slave synchronization scheme with a time delay τ:

$$\begin{aligned}
\mathcal{M}: & \begin{cases} D_t^\alpha x(t) &= Ax(t) + Bf(x(t)) \\ p(t) &= Cx(t) \end{cases} \\
\mathcal{S}: & \begin{cases} D_t^\alpha y(t) &= Ay(t) + Bf(y(t)) + u(t) \\ q(t) &= Cy(t) \end{cases} \\
\mathcal{C}: & \quad \{u(t) = F(p(t-\tau) - q(t-\tau)).
\end{aligned} \tag{3.1}$$

The state vectors of the master and slave systems are $x \in \Re^n$ and $y \in \Re^n$, respectively. The matrices $A \in \Re^{n\times n}$, $B \in \Re^{n\times n_h}$, $C \in \Re^{n_h\times n}$ and $F \in \Re^{l\times n}$ are known real constant matrices. $f(x(t))$ is a smooth bounded function of times. $p(t) \in \Re^m$ and $q(t) \in \Re^m$ are the outputs of the master and the slave systems, respectively. The main objective of this scheme is to synchronize the master system $\mathcal{M}$ and the slave system $\mathcal{S}$ by applying a linear state error feedback to the slave system with control signal $u(t) \in \Re^n$ with feedback matrix $F \in \Re^{l\times n}$.
In this chapter D_t^α stands for Rieman-Liouville derivative.
Defining the synchronization error as $e(t) = x(t) - y(t)$, the error dynamic can be obtained as:

$$\mathcal{E}: \ \{D_t^\alpha e(t) = Ae(t) + B(f(x(t)) - f(y(t))) - FCe(t-\tau) \tag{3.2}$$

Assumption 3.2.2. *Since $f(x(t))$ is smooth functions, they should be Lipschitz in x, y respectively. In other words, one has:*

$$||f(x(t)) - f(y(t))|| \leq l_e||x(t) - y(t)||, \quad \forall x(t), y(t) \in \Re^n \tag{3.3}$$

where l_e is an appropriate positive constants.

The stability of the error system $\mathcal{E}$ given in equation (3.2) is explored in order to obtain a synchronization criterion.

Theorem 3.2.1. *For a given $\tau > 0$ and $l_e > 0$, the error system described as equation (3.2) is asymptoticly stable if there exists the matrices $P = P^T > 0$, $R_1 = R_1^T > 0$, $R_2 = R_2^T > 0$ and $R_3 = R_3^T > 0$, a matrix F with appropriate dimensions and constant*

positive scalars μ_1 and μ_2 there is a solution of the following optimization problem:

$$\begin{aligned} &\underset{P,\ X,\ R_{i=1,2,3},\ \mu_{j=1,\ 2}}{min} \\ &Z = \\ &\begin{bmatrix} \Omega & I & R_3 \\ I & -\frac{\phi_{max}\left(XCC^TX^T\right)}{\mu_2}I - R_1 & -R_3 \\ R_3 & -R_3 & \frac{-1}{\tau}R_2 \end{bmatrix} < 0 \end{aligned} \tag{3.4}$$

with $\Omega = 2XC + \frac{l_e^2\phi_{max}\left(PBB^TP\right)}{\mu_1}I + \mu_1 I - \mu_2 I + R_1 + \tau R_2$, $F = P^{-1}X$ and I is the $n \times n$ identity matrix and ϕ_{max} is the maximum eigenvalue function.

Proof. Let us construct a Lyapunov function as:

$$\begin{aligned} \mathcal{L}(t) = \quad & D_t^{-(1-\alpha)}\left[e^T(t)Pe(t)\right] + \int_{-\tau}^{0} e^T(t)(t+\Theta)R_1e(t+\Theta)d\Theta + \int_{t-\tau}^{t}\int_{t+\Theta}^{t} e(\psi)^TR_2 \\ & e(\psi)d\psi d\Theta + \left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right]^T R_3\left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right], \quad 1 \geq \alpha > 0 \end{aligned} \tag{3.5}$$

where the function is reduced to the classical Lyapunov-Krasovskii function when $\alpha = 1$ (see property in equation (A.9)), and the term $D_t^{-(1-\alpha)}[e^T(t)Pe(t)]$ is constructed as a Rieman-Liouville fractional integral when $1 > \alpha > 0$, thus according to equation (1.22) and integral property the positive defitiveness for the function is guaranted.

An application of property in equation (A.16), we get the time derivative of equation (3.5) as:

$$\begin{aligned} \dot{\mathcal{L}}(t) = \quad & D_t^{\alpha}[e(t)^TPe(t)] + e^T(t)R_1e(t) - e^T(t-\tau)R_1e(t-\tau) + \tau e^T(t)R_2e(t) - \\ & \int_{-\tau}^{0} e^T(t)(t+\Theta)R_2e(\Theta)d\Theta + [e(t) - e(t-\tau)]^T R_3\left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right] \\ & + \left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right]^T R_3\left[e(t) - e(t-\tau)\right] \end{aligned} \tag{3.6}$$

Applying lemma (2.3.2) to the right side of equation (3.6) results to:

$$\begin{aligned} \dot{\mathcal{L}}(t) \leq \quad & 2e^TPD_t^{\alpha}e(t) + e^T(t)R_1e(t) - e^T(t-\tau)R_1e(t-\tau) + \tau e^T(t)R_2e(t) - \\ & \int_{-\tau}^{0} e^T(t+\Theta)R_2e(t+\Theta)d\Theta + [e(t) - e(t-\tau)]^T R_3\left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right] \\ & + \left[\int_{-\tau}^{0} e(t+\Theta)d\Theta\right]^T R_3\left[e(t) - e(t-\tau)\right] \end{aligned} \tag{3.7}$$

Substituting equation (3.2) in equation (3.7) yields to:

$$\begin{aligned}\dot{\mathcal{L}}(t) \quad &\leq e^T(t)[2PA]e(t) + 2e^T PB(f(x(t)) - f(y(t))) - 2e^T(t)PFCe(t-\tau) \\ &+e^T(t)R_1e(t) - e^T(t-\tau)R_1e(t-\tau) + \tau e^T(t)R_2e(t) - \int_{t-\tau}^{t} e^T(\sigma)R_2e(\sigma) \\ &d\Theta + [e(t) - e(t-\tau)]^T R_3 \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right] + \left[\int_{t-\tau}^{t} e(\Theta)d\right]^T R_3[e(t) - \\ &e(t-\tau)] \end{aligned} \tag{3.8}$$

In view of the assumption (3.2.2) and lemma (2.2.3), we obtain:

$$\begin{aligned}2e^T(t)PB(f(x(t)) - f(y(t))) \leq \quad &\mu_1||e(t)||^2 + \frac{l_e^2}{\mu_1}||BPe(t)||^2 \leq \mu_1||e(t)||^2 \\ &+\frac{l_e^2\phi_{max}(PBB^TP)}{\mu_1}||e(t)||^2 \end{aligned} \tag{3.9}$$

and

$$\begin{aligned}2e^T(t)PFCe(t-\tau) \quad &\leq \mu_2||e(t)||^2 + \frac{1}{\mu_2}||C^TF^TPe^T(t-\tau)||^2 \leq \mu_2||e^T(t)||^2 + \\ &\frac{\phi_{max}\left(PFCC^TF^TP\right)}{\mu_2}||e(t-\tau)||^2 \end{aligned} \tag{3.10}$$

where $\phi_{max}(\cdot)$ represnt the maximum eigenvalue of a matrix.

By using the lemma (2.3.3) we obtain:

$$\left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right]^T R_2 \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right] \leq \tau \int_{t-\tau}^{t} e^T(\Theta)R_2 \int_{t-\tau}^{t} e(\sigma)d\sigma \tag{3.11}$$

and

$$\int_{t-\tau}^{t} e^T(\Theta)R_2 \int_{t-\tau}^{t} e(\Theta)d\Theta \geq \frac{1}{\tau}\left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right]^T R_2 \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right] \tag{3.12}$$

Thus, we have:

$$\begin{aligned}\dot{\mathcal{L}}(t) \leq \quad &e^T(t)2PAe(t) + \frac{l_e^2\phi_{max}\left(PBB^TP\right)}{\mu_1}||e(t)||^2 + \mu_1||e(t)||^2 - \mu_2 \\ &||e(t)||^2 - \frac{\phi_{max}\left(PFCC^TF^TP\right)}{\mu_2}||e^T(t-\tau)||^2 + e^T(t)R_1e(t) - e^T(t-\tau)R_1 \\ &e(t-\tau) + \tau e^T(t)R_2e(t)\frac{-1}{\tau}\left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right]^T R_2 \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right] \\ &+ [e(t) - e(t-\tau)]^T R_3 \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right] + \left[\int_{t-\tau}^{t} e(\Theta)d\Theta\right]^T \\ &R_3[e(t) - e(t-\tau)] \end{aligned} \tag{3.13}$$

Therefore:

$$\dot{\mathcal{L}}(t) \leq \xi(t)^T \mathfrak{M} \xi(t) < 0 \tag{3.14}$$

where $\xi(t) = [e(t); e(t-\tau); \int_{t-\tau}^{t} e(\Theta)d\Theta]$ and $\mathfrak{M} =$

$$\begin{bmatrix} 2PA + \frac{l_e^2 \phi_{max}(PBB^T P)}{\mu_1} I + \mu_1 I - \mu_2 I + R_1 + \tau R_2 & I & R_3 \\ I & -\frac{\phi_{max}(XCC^T X^T)}{\mu_2} I - R_1 & -R_3 \\ R_3 & -R_3 & \frac{-1}{\tau} R_2 \end{bmatrix}$$

with $X = PF$. Then if $\mathfrak{M} < 0$, then $\dot{\mathcal{L}}(t) \leq 0$. To derive asymptotical stability we use the lemma (2.3.1). Form $\dot{\mathcal{L}}(t) < 0$ it is obtain that $\mathcal{L}(t) < \mathcal{L}(0)$. To verify the boudennes of $\ddot{\mathcal{L}}(t)$, it needs to show that $\xi(t) \in \ell_2$. Note that $\mathcal{L}$ is a non-increasing and positive definite function then:

$$-\int_0^t \dot{\mathcal{L}}(t) = \mathcal{L}(0) - \mathcal{L}(t) < \infty \tag{3.15}$$

$$\begin{aligned} & -\int_0^t \dot{\mathcal{L}}(t)d\tau < \infty \\ & \Rightarrow \int_0^t [\Lambda_{min}(-\mathfrak{M})||\xi(t)||^2]d\tau < \infty \\ & \Rightarrow \sqrt{\int_0^t [\Lambda_{min}(-\mathfrak{M})||\xi(t)||^2]d\tau} < \infty \\ & \Rightarrow \sqrt{\int_0^t ||\xi(t)||^2 d\tau} < \infty \end{aligned} \tag{3.16}$$

where $\Lambda_{min}(-\mathfrak{M})$ represent the minimum eigenvalues of $-\mathfrak{M}$. From equation (3.16), it is concluded that $\xi(t) \in \ell_2$. Then it is derived that:

$$\lim_{t \to \infty} \dot{\mathcal{L}}(t) = 0 \tag{3.17}$$

the asymptotic stability is concluded. This completes the proof. □

Remark 3.2.1. *The matrix inequalites equation (3.4) include information on the delay. Therefore this result is a delay–dependent criterion.*

3.2.2 Numerical example

In this subsection, we will numerically verify the effectiveness of the proposed synchronization scheme on the fractional order commensurate hyper-chaotic Liu system [Qiang *et al.* (2013)].

The master system is given by:

$$\begin{cases} D_t^{\alpha_1} x_1(t) = \kappa_1(x_2(t) - x_1(t)) + x_4(t) \\ D_t^{\alpha_2} x_2(t) = \kappa_2 x_1(t) - x_1(t)x_3(t) + \kappa_3 x_4(t) \\ D_t^{\alpha_3} x_3(t) = 4x_1^2(t) - \kappa_4 x_3(t) - x_4(t) \\ D_t^{\alpha_4} x_4(t) = -x_4(t) - \kappa_5 x_2(t) \end{cases} \tag{3.18}$$

where $\kappa_1 = 10$, $\kappa_2 = 40$, $\kappa_3 = 0.5$, $\kappa_4 = 2.5$ and $\kappa_5 = 10/15$.

Thus the systems matrices in equation (4.1) are:

$$A = \begin{bmatrix} -\eta_1 & \kappa_1 & 0 & 1 \\ \kappa_2 & 0 & 0 & \kappa_3 \\ 0 & 0 & \kappa_4 & -1 \\ 0 & -\kappa_5 & 0 & -1 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$f(x(t)) = \begin{bmatrix} -x_1(t)x_3(t) \\ 4x_1^2(t) \end{bmatrix}.$$

Initial conditions are selected as: $x(0) = [2,\ -1,\ 0.8,\ 0.8]^T$ and $y(0) = [5,\ 3,\ 2,\ \ 1]^T$ respectively. We choose $C = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$. The matrices P, X and $R_{i=1,2,3}$ and the scalares $\mu_{j=1,\ 2}$ are found using MATLAB LMI optimization toolbox with $l_e = 5$ and $\tau = 0.163$ as:

$$R_1 = 10^{-4} \times \begin{bmatrix} 0.6403 & -0.1115 & -0.0701 & -0.0761 \\ -0.1115 & 0.7144 & -0.0725 & -0.1025 \\ -0.0701 & -0.0725 & 0.6827 & -0.1333 \\ -0.0761 & -0.1025 & -0.1333 & 0.6584 \end{bmatrix},$$

$$R_2 = 10^{-3} \times \begin{bmatrix} 0.1486 & -0.0018 & -0.0025 & -0.0031 \\ -0.0018 & 0.1484 & -0.0024 & -0.0022 \\ -0.0025 & -0.0024 & 0.1486 & -0.0021 \\ -0.0031 & -0.0022 & -0.0021 & 0.1479 \end{bmatrix},$$

$$R_3 = 10^{-4} \times \begin{bmatrix} 0.6832 & -0.0746 & -0.0463 & -0.0475 \\ -0.0746 & 0.7393 & -0.0454 & -0.0691 \\ -0.0463 & -0.0454 & 0.7153 & -0.0891 \\ -0.0475 & -0.0691 & -0.0891 & 0.6959 \end{bmatrix},$$

$\mu_1 = 10^{-5} \times\ 2.1032,$

$\mu_2 = 10^{-6} \times\ 5.0017,$

$$X = 10^{-4} \times \begin{bmatrix} -0.1535 \\ 0.2944 \\ -0.0626 \\ 0.0719 \end{bmatrix},$$

$$P = 10^{-5} \times \begin{bmatrix} 0.1144 & -0.0344 & 0.0014 & 0.0047 \\ -0.0344 & 0.1035 & -0.0020 & -0.0096 \\ 0.0014 & -0.0020 & 0.0935 & 0.0010 \\ 0.0047 & -0.0096 & 0.0010 & 0.0919 \end{bmatrix},$$

$$F = \begin{bmatrix} -5.5159 \\ 27.5302 \\ -6.1322 \\ 11.0624 \end{bmatrix}.$$

Note that, one can easily find that $\mathfrak{M}$ is a negative definite matrix. The fractional orders $\alpha_{i(i=1,\ 2,\ 3,\ 4)}$ are also set to 0.9 to ensure the existence of chaos [Qiang *et al.* (2013)]. Figures (3.3)-(3.9) show the trajectories of the state variables of the master and slave systems. The synchronization errors are revealed in figure (3.10). As expected, one can observe that the trajectories of the slave system track those of the master, and the synchronization errors tend to zero.

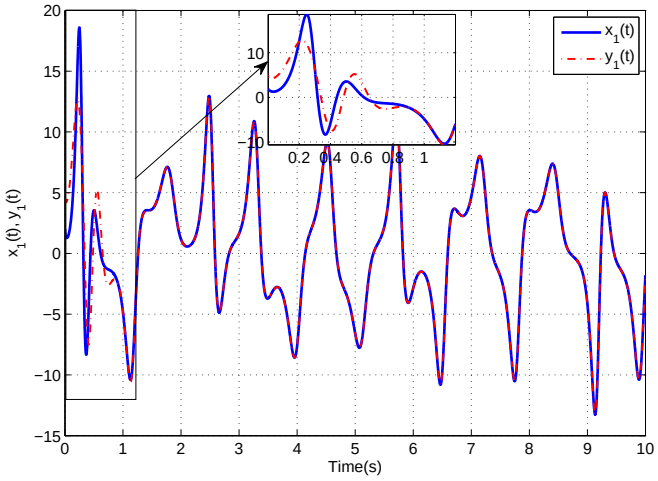


Figure 3.2 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order hyper chaotic Liu system.

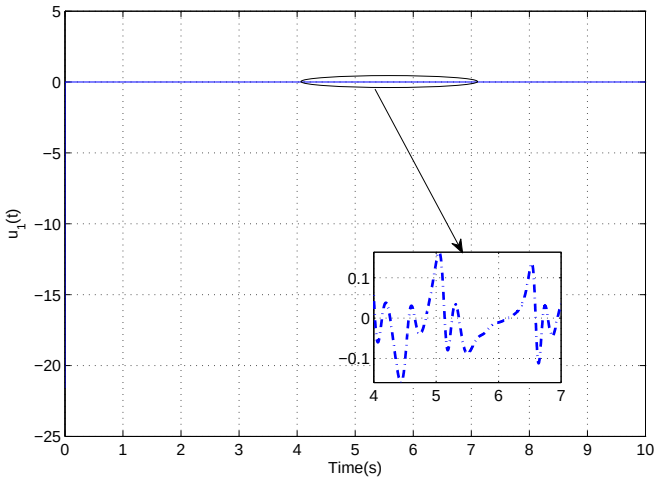


Figure 3.3 : The trajectory of the control input $u_1(t)$ in fractional order hyper chaotic Liu system.

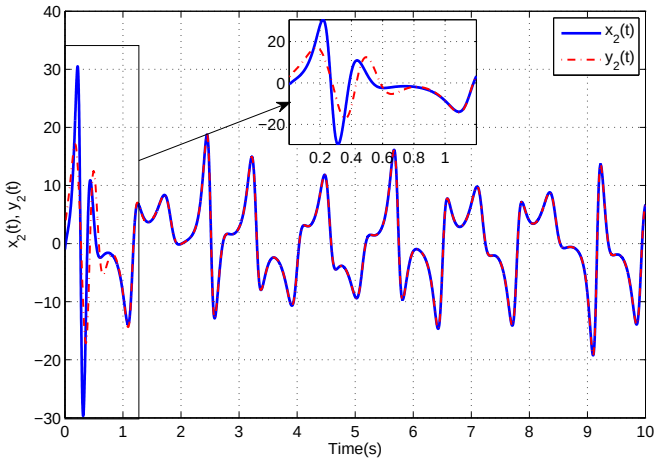


Figure 3.4 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order hyper chaotic Liu system.

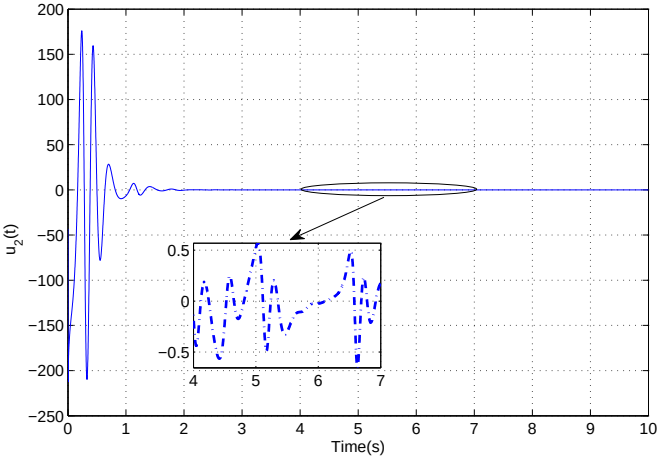


Figure 3.5 : The trajectory of the control input $u_2(t)$ in fractional order hyper chaotic Liu system.

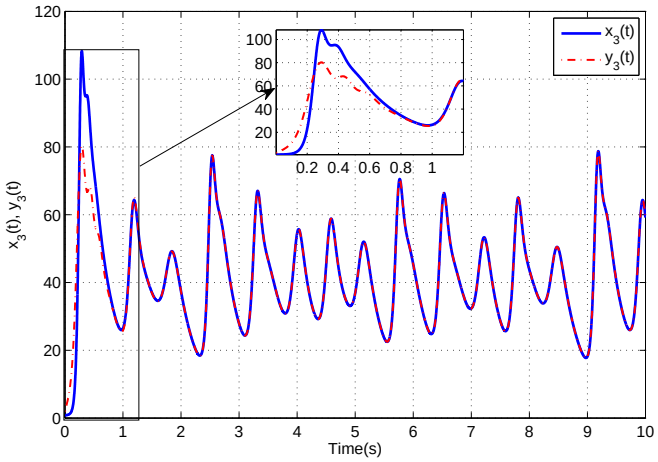


Figure 3.6 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order hyper chaotic Liu system.

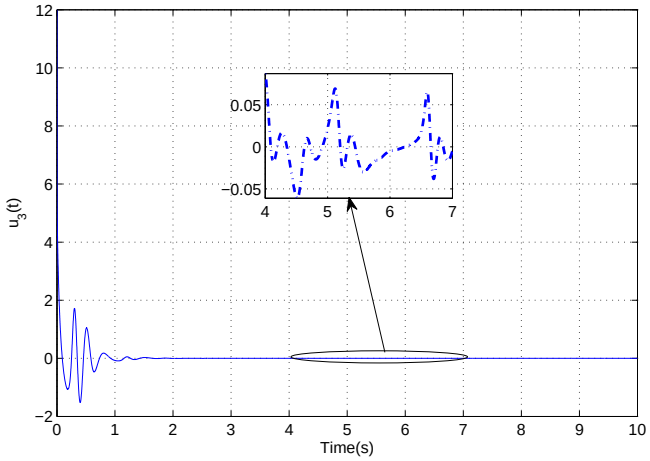


Figure 3.7 : The trajectory of the control input $u_3(t)$ in fractional order hyper chaotic Liu system.

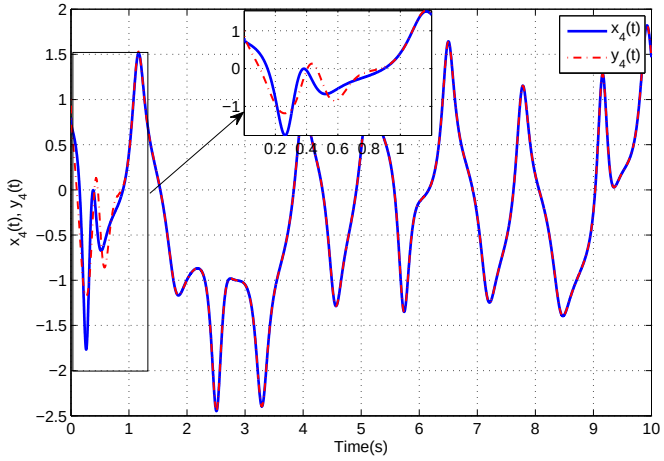


Figure 3.8 : The trajectories of the state variables $x_4(t)$ and $y_4(t)$ in fractional order hyper chaotic Liu system.

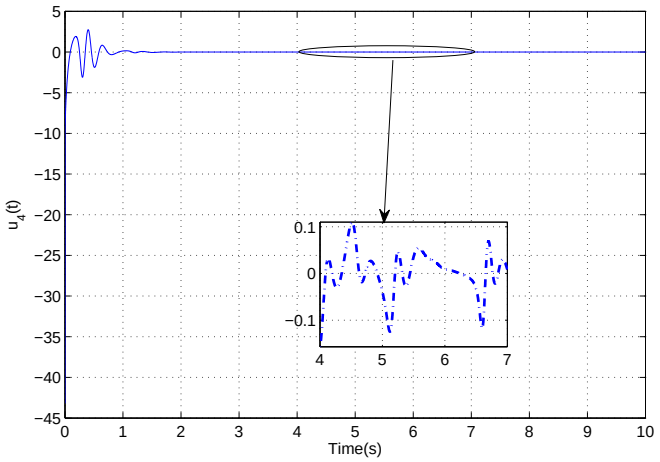


Figure 3.9 : The trajectory of the control input $u_4(t)$ in fractional order hyper chaotic Liu system.

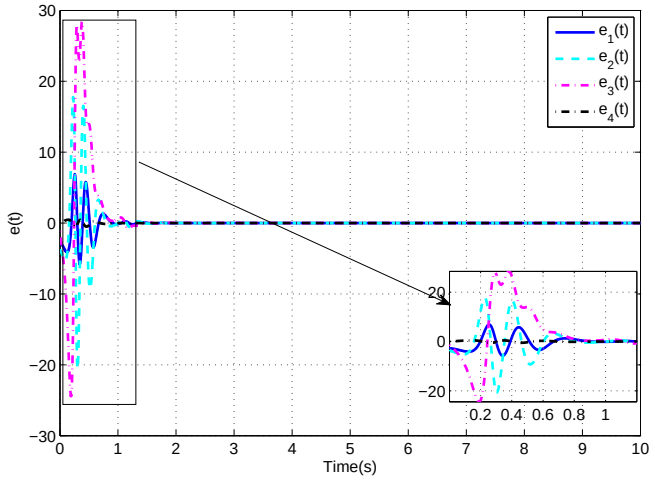


Figure 3.10 : The trajectories of the synchronization errors of fractional order hyper chaotic Liu system.

3.3 Image cryptosystem

Definition 3.3.1. (improved expanded XOR operation)
The improved expanded XOR operation [Wang & Zhang (2015)] introduce an enhancement on the overall security level of the proposed scheme. For two inputs $r1 = \sum_{i=0}^{7} r1_i$ and $r2 = \sum_{i=0}^{8} r2_i$, the operator can be described as:

$$eXOR(r1, r2) = \sum_{i=0}^{7} not(r1_i \oplus r2_i \oplus r2_{i+1} \times 2^i) \tag{3.19}$$

where $not(r1)$ flips a single bit $r1$. The operator has the following property: if $eXOR(r_1, r_2) = t$, then $eXOR(t, r2) = r1$. This property can be deduced from table (3.1) as,

Table 3.1 : The result of $not(r1_i \oplus r2_i \oplus r2_{i+2})$

$r1_i$	$r2_i r2_{i+2}$			
	00	01	10	11
0	1	0	0	1
1	0	1	1	0

3.3.1 The proposed cryptosystem

3.3.1.1 Generating and selecting the chaotic sequences

Due that the synchronization between the master and the slave systems, need some time to occur (see figure (3.10)). Equation (4.1) is iterated $T_S + 8MN$ time to generate the chaotic sequences after we discard the first T_S elements to avoid initial synchronization errors.

3.3.1.2 Generation of the scrambling and diffusion sequences

In this stage we generate $\mathfrak{S}_1$, $\mathfrak{S}_2$ and $Ind.x_i$ where they used as scrambling sequences and D_{f_i} as diffusion sequences. The following described the generation process.

3.3.1.2.1 Scrambling sequences

1. Sort the first MN elements of the selected chaotic sequences $x_{1,2,3}$ in ascendant order according to the following equation:

$$[Val.x_i(K)\ , Ind.x_i(K)] = sort(x_i(K)), \quad i = 1, 2, 3, \quad K = 1, 2, \ldots, MN \tag{3.20}$$

   where $Val.x_i$, $Ind.x_i$ are arrays with size $1 \times MN$ which contains the values and the indexs position respectively.

2. Produce three others arrays x'_i with size $1 \times 8MN$ by the following formula:

$$x'_i = mod([(\lceil |x_i| \rceil - |x_i|) \times 10^8], 256), \quad i = 1, 2, 3 \tag{3.21}$$

   where $|\cdot|$ denote the absolute value, $mod(\cdot)$ refer to the module operation and $\lceil a \rceil$ refers to get the smallest integer greater than or equal to a.

3. Combien all there arrays x'_i into an array $\mathfrak{S}$ with the size $1 \times 24MN$ as:

$$\mathfrak{S} = cat(x'_1, x'_2, x'_3) \tag{3.22}$$

then get two new arrays $\mathfrak{S}_1$ and $\mathfrak{S}_2$ with the length M and $24N$ respectively, using equation (3.23) shown as follows:

$$\begin{aligned}\mathfrak{S}_1 &= [\mathfrak{S}(1), \mathfrak{S}(2), \ldots, \mathfrak{S}(M)] \\ \mathfrak{S}_2 &= [\mathfrak{S}(M+1), \mathfrak{S}(M+2), \ldots, \mathfrak{S}(24N)]\end{aligned} \tag{3.23}$$

3.3.1.2.2 Diffusion sequences

1. The arrays $Val.x_i$ are processed using equation (3.24) as follow:

$$Val.x_i = mod([(\lceil |Val.x_i| \rceil - |Val.x_i|) \times 10^8], 256) \tag{3.24}$$

then transform them to binary matrices BV_i with the size of $M \times 8N$ and combine them into a $M \times 24N$ matrix T_V by the following:

$$T_V = cat(BV_1,\ BV_2,\ BV_3) \tag{3.25}$$

2. Rows circular shift. The rows shift result T'_V is obtained by moving the row rw of T_V by the step number $\mathfrak{S}_1(rw)$ and $rw = 1, 2, \ldots, M$.

3. Process the matrix T'_V by a circular column shift operation where the column col of T'_V is moved by the step number $\mathfrak{S}2(col)$ and $col = 1, 2, \ldots, 24N$ resulting T''_V.

4. Convert the binary values of T''_V into decimal base resulting a matrix with size $M \times 3N$ then split it into three sub–matrices $T_{sub_{i=1,2,3}}$ with size $M \times N$ and after combine the elements of each sub-matrix $T_{sub_{i=1,2,3}}$ into an array $D_{f_{i=1,2,3}}$ with size $1 \times MN$ respectively.

5. Substitute the elements of each array D_{f_i} using the XOR operation as follows:

$$D_{f_i} = D_{f_i} \oplus Val.x_i \tag{3.26}$$

where the $\oplus$ denotes the XOR operation.

3.3.1.3 Image scrambling

The proposed scrambling of the plain image is performed by the following steps:

1. Decompose the RGB image $\mathbb{P}$ into $\mathbb{P}_\mathbb{R}$, $\mathbb{P}_\mathbb{G}$, $\mathbb{P}_\mathbb{B}$ components, then transform them into binary matrices $\mathbb{R}$, $\mathbb{G}$ and $\mathbb{B}$ with the size of $M \times 8N$ and combine them into a $M \times 24N$ matrix T_E as:

$$T_E = cat(\mathbb{R},\ \mathbb{G},\ \mathbb{B}) \tag{3.27}$$

2. Rows circular shift. The rows shift result T'_E is obtained by following rules: the row rw of T_E is moved by step number $\mathfrak{S}_1(rw)$.

3. Process the matrix T'_E by a circular column shift operation, where the column col of T'_E is moved by step number $\mathfrak{S}_2(col)$ resulting T''_E.

4. Convert the binary values of T''_E into decimal base resulting a matrix with size $M \times 3N$, then split it into three sub–matrices of size $M \times N$ after combining the elements of each sub–matrices into 1-dimensional arrays $I_{D_{i=1,\ 2,\ 3}}$ with size $1 \times MN$ then rearrange the elements of each I_{D_i} according to $Ind.x_i$ respectively to get the scrambled image as shown in the following equation:

$$I_{D_i}(K) = I_{D_i}(Ind.x_i(K)), \quad K = 1,\ 2,\ \ldots,\ MN \tag{3.28}$$

3.3.1.4 Image diffusion

In this stage we proceed as follow:

1. Diffuse the elements of each array I_{D_i} as follow:

$$I_{E_i} = I_{D_i} \oplus D_{f_i} \tag{3.29}$$

2. Use the XOR and expanded XOR operations to perform another substitution by the following equation:

$$\begin{aligned} I_{E_i}(K) = \quad & eXOR((I_{E_i}(K), (mod(((4 \times x_i(K) - 2 \times x_{i+1}(K)) \times 10^8), 256)))) \oplus \\ & (mod((x_{i+1}(K) \times 10^8), 256)), \quad i = 1, 2, 3, \quad K = 1, 2, \ldots, MN \end{aligned} \tag{3.30}$$

3. Convert the arrays I_{E_i} into matrices with size $M \times N$ which are separately the red, green and blue components of the final encrypted image.

3.3.2 Decryption process

The decryption is done by a inverse of encryption process, using the synchronized sequences $y_{j(j=1,2,3,\ldots,n)}$.

3.3.3 Numerical simulation and cryptanalysis

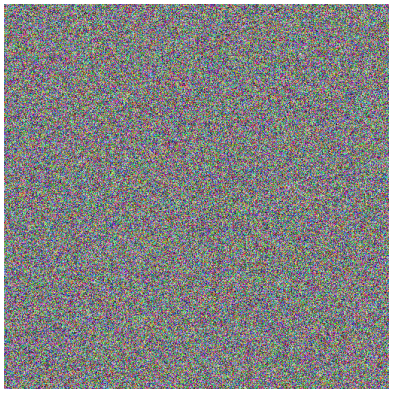
In the simulations the fractional order hyperchaotic Liu system is used. The cryptosystem is applied on sevral different images named Lena, Panda, Vegetables, Baboon, Peppers,

Girl, Black and also images from USC-SIPI database set. The plain images are shown in figures (3.11(a)-(c)) while corresponding encrypted and decrypted images are shown in figures (3.11(d)-(i)), respectively.

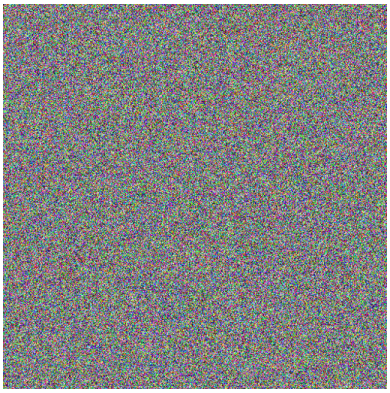
(a) Plain image of Lena.

(b) Plain image of Vegetables.

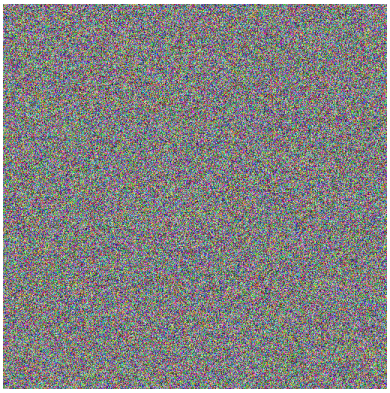
(c) Plain image of Panda.



(d) Encrypted-image of Lena.



(e) Encrypted image of Vegetables.



(f) Encrypted image of Panda.

(g) Decrypted image of Lena.

(h) Decrypted image of Vegetables.

(i) Decrypted image of Panda.

Figure 3.11 : Encryption and decryption output.

The following evaluation parameters, are taken into consideration to test the performance of the proposed cryptosystem.

3.3.3.1 Key space

A good cryptosystem, should have a large enough key space to resist an exhaustive. Here, the fractionbal derivatives $\alpha_i (i = 1 : 4)$ and the parameters $\kappa_i (i = 1 : 5)$ are used as the secret key, therefore, the secret key-set is as $(\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$, where each key independent of others. In the simulations (repeated over 100 times) we find that the precision of each secret key is approximately 10^{-15} (see remark (1.2.1)), then the key space size is about 10^{135}, so it can resist brute force attacks and in comparison with the references given in table (3.2) it larger than [Enayatifar *et al.* (2015), Gan *et al.* (2019), Pak & Huang (2017), Rehman *et al.* (2018), Wei *et al.* (2012)].

Table 3.2 : Comparison of key space.

Cryptosystem	Key space
Proposed	10^{135}
[Enayatifar *et al.* (2015)]	10^{70}
[Gan *et al.* (2019)]	$10^{95.75}$
[Pak & Huang (2017)]	$10^{41.54}$
[Rehman *et al.* (2018)]	10^{94}
[Wei *et al.* (2012)]	10^{70}

3.3.3.2 Differential analysis

It is well known that a good algorithm can also withstand a brutal differential attack. To test it resistance, two known tests known as Number of Pixel Changing Rate (NPCR) and Unified Averaged Changed Intensity (UACI) which introduce by [Wu *et al.* (2011)] to investigate a cryptosystem against differential attacks. The NPCR test is given by equation (3.31) and the UACI by equation (3.32) as follow:

$$NPCR(\mathsf{en}_1, \mathsf{en}_2) = \left[\sum_{i=0}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{M \times N}\right] \times 100\% \tag{3.31}$$

$$UACI(\mathsf{e}_1, \mathsf{en}_2) = \left[\sum_{i=0}^{M}\sum_{j=1}^{N}\frac{|\mathsf{en}_1(i,j) - \mathsf{en}_2(i,j)|}{L \times M \times N}\right] \times 100\% \tag{3.32}$$

where en_1 and en_2 are two encrypted images generated from inputs which differ in one-bit only. M, N represent the height and width of the encrypted images and L denotes the largest intensity allowed in the image for any pixel respectively. $D(i,j)$ is defined like follows:

$$D(i,j) = \begin{cases} 1 & if \quad \mathsf{en}_1(i,j) \neq \mathsf{en}_2(i,j) \\ 0 & else \end{cases} \tag{3.33}$$

The theoretical values of UACI score is 0.36, and the closer the NPCR score is to 1, the more sensitive the encryption scheme is to the plain image, and the better the scheme resists differential attack [Wu *et al.* (2011)]. The NPCR and UACI scores for Lena, Panda,

Vegetables and Peppers encrypted images are listed in table (3.3). The NPCR and UACI scores are compared to [Firdous *et al.* (2019), Rehman *et al.* (2018)].

Table 3.3 : Average NPCR and UACI scores of plain image sensitivity.

Cryptosystem	Image	NPCR			UACI		
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	99.5944	99.6372	99.6131	33.1148	33.6548	33.2761
	Vegetables	99.6304	99.5964	99.6058	33.5753	33.1670	33.4792
	Panda	99.6498	99.6135	99.6449	33.1694	33.3718	33.5097
	Peppers	99.6261	99.6051	99.6032	33.2897	33.9634	33.7678
[Firdous *et al.* (2019)]	Lena	99.5895	99.6170	99.6582	33.4558	33.4901	33.4438
[Rehman *et al.* (2018)]	Lena	99.6078	99.6088	99.6081	33.4291	33.4252	33.4219
	Vegetables	99.6193	99.6090	99.6102	33.5106	33.5011	33.5096
	Panda	99.6084	99.6087	99.6099	33.5030	33.4973	33.4920
	Peppers	99.6081	99.6096	99.6143	33.4256	33.4255	33.4217

3.3.3.3 Key sensitivity analysis

An efficient cryptosystem should have a sensitivity to its secret key-set. In anthoer word a very small change in the secret key-set will cause a significant change in the decrypted image. To analyze the sensitivity of the secret key-set we do a litlle modification in initial one (i.e $\gamma_0 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$) we obtaine the other secret key-sets as the following:

$\gamma_1 = (\kappa_1 + 10^{-15},\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_2 = (\kappa_1,\ \kappa_2 + 10^{-15},\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_3 = (\kappa_1,\ \kappa_2,\ \kappa_3 + 10^{-15},\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_4 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4 + 10^{-15},\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_5 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5 + 10^{-15},\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_6 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1 + 10^{-15},\ \alpha_2,\ \alpha_3,\ \alpha_4)$,
$\gamma_7 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2 + 10^{-15},\ \alpha_3,\ \alpha_4)$,
$\gamma_8 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3 + 10^{-15},\ \alpha_4)$,
$\gamma_9 = (\kappa_1,\ \kappa_2,\ \kappa_3,\ \kappa_4,\ \kappa_5,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4 + 10^{-15})$.

Using the secret key-sets, the rate of difference is calculated for Lena, Vegetables and Panda and shown in table (3.4). The results of key sensitivity are compared to [Rehman *et al.* (2018)] and the proposed cryptosystem has clear advantage over it.

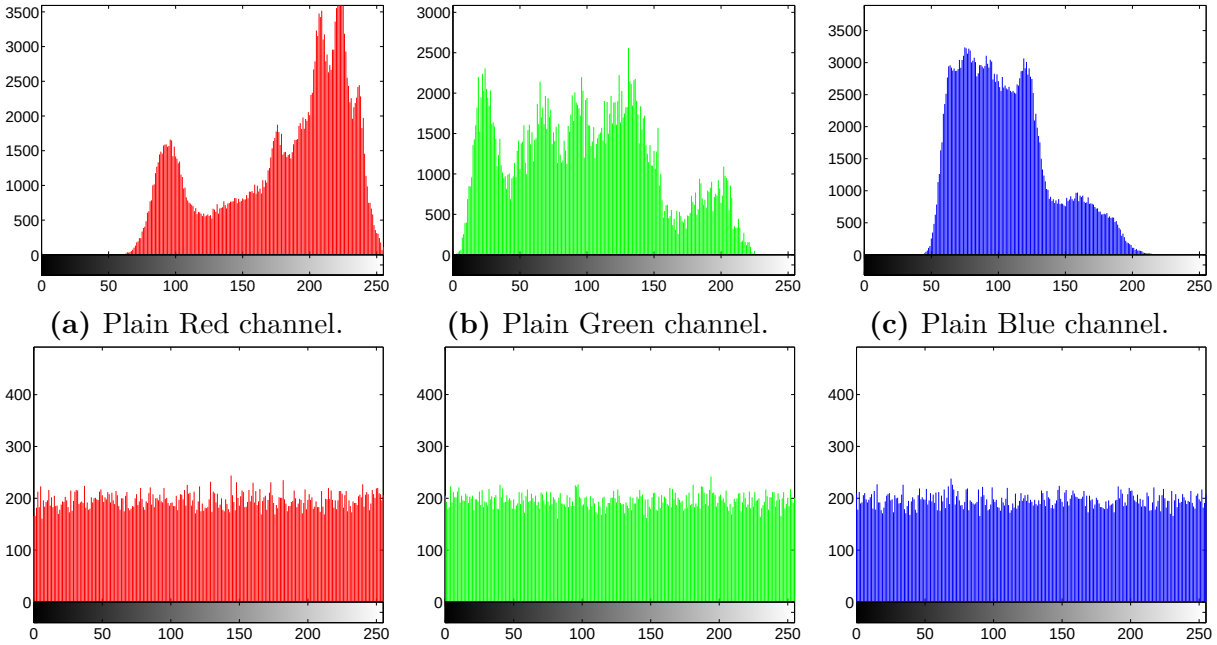
Table 3.4 : NPCR scores between two encrypted images using slightly different key.

γ	Proposed			[Rehman *et al.* (2018)]		
	Lena	Vegetables	Panda	Lena	Vegetables	Panda
γ_1	99.6063	99.6172	99.6039	99.5992	99.5982	99.5972
γ_2	99.6016	99.6150	99.6106	99.6114	99.5600	99.6037
γ_3	99.5973	99.6088	99.6101	99.5936	99.6277	99.5931
γ_4	99.6099	99.6121	99.6097	99.6033	99.6205	99.5956
γ_5	99.6031	99.6129	99.6122	99.6302	99.6388	99.6047
γ_6	99.6381	99.6176	99.6186	99.6104	99.6109	99.5952
γ_7	99.6160	99.6080	99.6127	99.5972	99.6164	99.6104
γ_8	99.6165	99.6133	99.6033	99.6063	99.6216	99.6205
γ_9	99.6084	99.6032	99.6154	99.6145	99.6022	99.6287
Average	99.6108	99.6120	99.6107	99.6073	99.6106	99.6056
Average all	99.6111			99.6079		

3.3.3.4 Statistical analysis

1. Histogram and uniformity analysis

   The image histogram reflects the distribution of the pixels value. A strong cryptosystem should mask the perceptual meaning of the plain image and flatten its histogram (i.e., become near uniform distribution) [Zhou *et al.* (2015)]. The histograms before and after encryption are shown in figure (3.12) for the test image Lena. It clear that the encrypted image histograms are sufficiently uniform.



(a) Plain Red channel. **(b)** Plain Green channel. **(c)** Plain Blue channel.

(d) Encrypted Red channel. **(e)** Encrypted Green channel. **(f)** Encrypted Blue channel.

Figure 3.12 : Histograms of Lena.

According to the quantitative analysis method, to measure the uniformity of an encrypted image we compute the variance of it histograms [Rehman *et al.* (2018)]. The lower the variance value indicate a higher uniformity of the encrypted image The variance can be calculated as:

$$var = \frac{1}{256^2}\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{1}{2}(z_i - z_j)^2 \tag{3.34}$$

where z_i and z_j are the frequencies at i^{th} and j^{th} gray levels respectively.
In table (3.5), the variances of histograms of encrypted images, for each secret key-set are provided.

Table 3.5 : Images histogram variation under different keys.

γ	Proposed				[Rehman *et al.* (2018)]	[Wu *et al.* (2015)]
	Lena	Vegetables	Panda	Average	Average	Average
γ_1	312.90	391.87	350.45	343.56	5461.83	5473.17
γ_2	252.92	339.34	596.68	350.33	5652.87	5465.89
γ_3	213.61	346.54	567.17	375.78	5456.66	5458.30
γ_4	209.79	350.44	538.54	366.26	5468.17	5458.30
γ_5	308.34	417.63	496.06	407.34	5459.97	5458.39
γ_6	248.31	270.54	533.89	350.91	5475.67	5465.78
γ_7	233.58	322.18	490.68	348.81	5456.58	5466.23
γ_8	294.25	316.61	592.30	401.05	5470.56	5468.31
γ_9	243.98	356.64	440.92	347.18	5472.24	5458.88

In order to further examen the influence of the modification of the secret set-keys on the uniformity of the encrypted images, we compute the percentage of the variance differences between two encrypted images obtained separately by the initial secret key-set γ_0 and the secret key-sets $\gamma_i (i = 1, 2, ..., 9)$. The percentage can be computed by equation (3.35) as:

$$\mathcal{P}(var)_{\gamma_i} = \frac{|var_{\gamma_i} - var_{\gamma_0}|}{var_{\gamma_0}} \tag{3.35}$$

where $\mathcal{P}(var)_{\gamma_i}$ is the percentage of variance difference when only one key is changed, var_{γ_0} and var_{γ_i} represent the histogram variances of the encrypted image by the secret key-set γ_0 and $\gamma_{i=1,2,...,9}$ respectively. The results are listed in table (3.5). The percentage of average variance difference scores by the proposed cryptosystem listed in table (3.6) are better than [Wu *et al.* (2015)] and comparable to [Rehman *et al.* (2018)].

Table 3.6 : Percentage of variance difference.

γ	Proposed				[Rehman *et al.* (2018)]	[Wu *et al.* (2015)]
	Lena	Vegetables	Panda	Average	Average	Average
γ_1	0.52	0.17	0.21	0.30	0.10	0.16
γ_2	0.23	0.30	0.19	0.24	0.30	0.14
γ_3	0.32	0.12	0.05	0.16	0.30	0.26
γ_4	0.33	0.11	0.10	0.18	0.23	0.12
γ_5	0.50	0.25	0.17	0.31	0.22	0.18
γ_6	0.21	0.31	0.11	0.20	0.26	0.16
γ_7	0.25	0.18	0.18	0.20	0.22	0.17
γ_8	0.43	0.19	0.29	0.30	0.20	0.15
γ_9	0.22	0.09	0.22	0.19	0.15	0.18

2. Correlation of two adjacent pixels

   It well known that in an image there is strong interconnected relationship between a adjacent pixels in the horizontal, vertical and diagonal directions, so it is very important for a good encryption process to not preserve those relationships or at least weaken them, to get the ability to face on statistical attacks [Bluman (1998)]. Those relationships are elaborated in figure (3.13(a)-(c)) for plain Lena image figure (3.11(a)) and figures (3.13(d)-(f)) for the corresponding encrypted figure (3.11(d)). In the simulations, we select randomly 3000 pairs of adjacent pixels to measure the correlation coefficients for figures (3.11(a)) and (3.11(d)) in the three directions using equation (3.36) [Bluman (1998)] as:

$$\rho_{\mathfrak{gr}_1,\mathfrak{gr}_2} = \frac{|(cov(\mathfrak{gr}_1,\mathfrak{gr}_2))|}{\sqrt{D(\mathfrak{gr}_1)D(\mathfrak{gr}_2)}} \tag{3.36}$$

   where the covariance $coL(\mathfrak{gr}_1,\mathfrak{gr}_2)$ is obtainted by:

$$cov(\mathfrak{gr}_1,\mathfrak{gr}_2) = \frac{1}{L}\sum_{i=1}^{L}(\mathfrak{gr}_{1_i} - E(\mathfrak{gr}_1))(\mathfrak{gr}_{2_i} - E(\mathfrak{gr}_2)) \tag{3.37}$$

   the variance value $D(\mathfrak{gr}_1)$ is obtainted by:

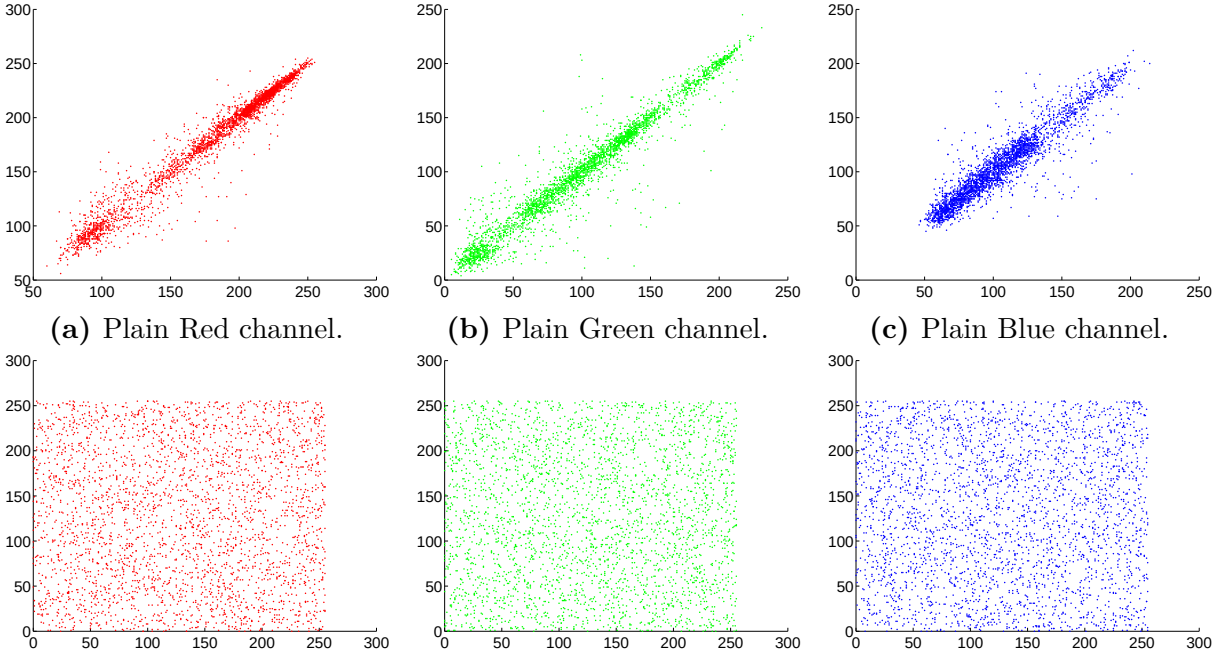
$$D(\mathfrak{gr}_1) = \frac{1}{L}\sum_{i=1}^{L}(\mathfrak{gr}_{1_i} - E(\mathfrak{gr}_1))^2 \tag{3.38}$$

   the mean value $E(\mathfrak{gr}_1)$ is obtainted by:

$$E(\mathfrak{gr}_1) = \frac{1}{L}\sum_{i=1}^{L}\mathfrak{gr}_{1_i} \tag{3.39}$$

   and $\mathfrak{gr}_1$, $\mathfrak{gr}_2$ are the gray values of two adjacent pixels and L is the number of samples taken, (in this case $L = 3000$). The results are listed in table (3.7), and

it clear that our cryptosystem has a low correlation as compared with the plain image (i. e. no information leakage from the encrypted images when statistical attacks happen). One can easily see that the results are comparable to the results in [Firdous *et al.* (2019), Rehman *et al.* (2018)].



(a) Plain Red channel. **(b)** Plain Green channel. **(c)** Plain Blue channel.

(d) Encrypted Red channel. **(e)** Encrypted Green channel. **(f)** Encrypted Blue channel.

Figure 3.13 : Correlation of adjacent pixels of Lena.

Table 3.7 : Correlation comparison.

Cryptosystem	Channel	Direction		
		Horizontal	Vertical	Diagonal
Proposed	Red	1×10^{-5}	-0.0276	0.0041
	Green	-4×10^{-4}	-0.0029	0.0022
	Blue	-5×10^{-6}	-0.0128	0.0039
[Firdous *et al.* (2019)]	Red	0.0105	-0.0391	0.0028
	Green	0.0073	0.0114	-0.0081
	Blue	-0.0134	-0.0312	-0.0184
[Rehman *et al.* (2018)]	Red	-0.0073	0.0010	-0.0013
	Green	0.0011	-0.0020	0.0078
	Blue	-0.0061	0.0058	-0.0003

3.3.3.5 Evaluating the pixels randomness

It is observed from figures (3.11(d)-(f)) that the encrypted images appear to be noise and similar to random images, so the proposed cryptosystem sucessfully masked the perceptual semantic of the plain images. we use the information entropy metric and the Chi-Square test to evaluate this randomness.

1. Information entropy

   The information entropy is evaluated to analyze the spreading of the gray scales of the image, in other words to measure the randomness of the image. The ideal entropy score of encrypted message is 8 in higher the value higher will be the uniform distribution [Wu *et al.* (2013)]. Mathematically, we can represent the entropy $\mathcal{H}$ for a data source $\mathfrak{gr}$ is characterized as:

$$\mathcal{H}(\mathfrak{gr}) = -\sum_{i=0}^{K-1} Pr(\mathfrak{gr}_i) log_2 Pr(\mathfrak{gr}_i) \tag{3.40}$$

   where $Pr(\mathfrak{gr}_i)$ and K are the probability and the total number of the gray value $\mathfrak{gr}_i$, respectivly. We have calculated the information entropy using equation (3.40) by using our cryptosystem and some other in [Firdous *et al.* (2019), Rehman *et al.* (2018), Rehman & Liao (2019)]. The information entropy results are given in table (3.8). It's well shown that the information entropy values obtained by our proposed cryptosystem is far better than [Rehman *et al.* (2018), Rehman & Liao (2019)] and comparable to [Firdous *et al.* (2019)].

Table 3.8 : Comparison of the information entropy.

Cryptosystem	Image	Plain image			Encrypted image		
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	7.2531	7.5940	6.9684	7.9993	7.9993	7.9993
	Vegetables	7.8832	7.8169	7.3828	7.9993	7.9993	7.9993
	Panda	7.7074	7.5693	7.7376	7.9992	7.9993	7.9993
	Peppers	7.3301	7.4963	7.0583	7.9992	7.9993	7.9993
	Baboon	6.9294	6.3175	7.2895	7.9993	7.9993	7.9993
[Firdous *et al.* (2019)]	Lena	-	-	-	7.9993	7.9992	7.9992
	Baboon	-	-	-	7.9993	7.9993	7.9993
[Rehman *et al.* (2018)]	Lena	7.2417	7.5767	6.9170	7.9966	7.9972	7.9967
	Vegetables	7.8277	7.8245	7.3598	7.9848	7.9846	7.9835
	Panda	7.7335	7.6452	7.7969	7.9903	7.9902	7.9903
	Peppers	7.3388	7.4962	7.0583	7.9910	7.9918	7.9905
[Rehman & Liao (2019)]	Lena	7.2417	7.5767	6.9170	7.9973	7.9965	7.9969
	Vegtbls	7.8277	7.8245	7.3598	7.9962	7.9955	7.9956
	Panda	7.7335	7.6452	7.7969	7.9950	7.9951	7.9946
	Peppers	7.3388	7.4962	7.0583	7.9965	7.9963	7.9970

2. The Chi-Square test

   The variance of an histogram is the output which represents the variation in the frequency of gray levels and the Chi-square score is a measurement of how expectations are compare with the output. The low scores of Chi-square demonstrate that we have a better randomness in the encrypted image [Ravichandran *et al.* (2017)]. The

Equation for Chi-Square test can be defined as follow:

$$\mathfrak{X}^2 = \sum_{i=0}^{255} \frac{(z_i - kk/256)^2}{kk/256} \tag{3.41}$$

where z_i is the number of pixels at i^{th} gray level and $kk/256$ is the expected frequency at i^{th} gray level. The scores of the Chi-square test for three different images are listed in table (3.9) and compared with [Firdous *et al.* (2019), Rehman *et al.* (2018)]. From the table, the results are comparable to [Firdous *et al.* (2019)], and better than [Rehman *et al.* (2018)].

Table 3.9 : Chi-square comparison.

Cryptosystem	Image	$\mathfrak{X}^2$		
		Red	Green	Blue
Proposed	Lena	264.6602	276.7544	251.8287
	Girl	236.3116	279.1655	281.6753
	Black	249.0969	260.0598	256.5356
[Firdous *et al.* (2019)]	Lena	284.7163	247.3794	235.1047
	Girl	232.6460	248.1597	254.8251
	Black	261.3726	259.5290	258.0384
[Rehman *et al.* (2018)]	Lena	363.0897	389.5104	327.8953
	Girl	1297.5838	1266.1413	1174.2451

3.3.3.6 Pixel modification based measurements

1. The Mean Square Error

   An encrypted image should not be equivalent to the plain image due to the application of the encryption procedure, which surely adds some noise to the actual digital content. We compute the Mean Square Error (MSE) between the plain and encrypted images to analyze the level of enciphering [Wang & Bovik (2006)]. Mathematically, MSE is defined as:

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(\mathsf{en}(i,j) - I(i,j)\right)^2}{MN} \tag{3.42}$$

   where en and I represent the encrypted and the plain images respectively. M and N indicate the width and the height of the test image, respectively. A larger value of the MSE enhances the security. Table (3.10) provides a comparison of the MSE scores of our proposed cryptosystem with the one in [Diaconu *et al.* (2014)]. The table shows that our proposed cryptosystem has clear advantage.

Table 3.10 : MSE comparison.

Cryptosystem	Lena			Baboon		
	Red	Green	Blue	Red	Green	Blue
Proposed	8868.4058	9320.8270	10453.2134	8590.3324	7852.9975	9861.7785
[Diaconu *et al.* (2014)]	3708.1469	3076.1575	3009.0649	2108.4576	1814.0706	2380.6572

2. The Peak Signal Noise Ratio

   PSNR metric is a ratio between the plain and the encrypted images. It employed as a security evaluation parameter when the plain and the encrypted images are taken as a signal and a noise respectivtly. A higher value of PSNR declare that the encrypted image is close to the plain image which is of course not desirable in any encryption procedure [Wang & Bovik (2006)]. Mathematically, PSNR can be written as:

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{3.43}$$

   The lower PSNR value provide an evidence that a plain image is significantly different from its corresponding encrypted and also become very difficult to retrieve it. The result for PSNR metric is listed in table (3.11). As compared with the other cryptosystems in [Firdous *et al.* (2019), Rehman *et al.* (2018), Rehman & Liao (2019)], the effectiveness of the proposed cryptosystem is evident by lower values of PSNR.

Table 3.11 : PSNR comparison.

Cryptosystem	Lena			Baboon		
	Red	Green	Blue	Red	Green	Blue
Proposed	7.85	7.61	6.76	8.61	7.01	8.40
[Firdous *et al.* (2019)]	7.87	8.50	9.64	8.94	9.49	8.58
[Rehman *et al.* (2018)]	7.86	8.57	9.67	8.93	9.50	8.56
[Rehman & Liao (2019)]	7.85	8.59	9.64	8.90	9.50	8.57

3. The gray difference degree (GVD)

   The gray difference degree is another measure of pixel modification by comparing the plain and the encrypted image. The GVD score approaches to 1 indicates that the two images are completely different [Davis (2011)]. The GVD, can be computed by using equation (3.44) as:

$$GVD(\mathfrak{gr}_1, \mathfrak{gr}_2) = \frac{AN'[GN(\mathfrak{gr}_1, \mathfrak{gr}_2)] - AN[GN(\mathfrak{gr}_1, \mathfrak{gr}_2)]}{AN'[GN(\mathfrak{gr}_1, \mathfrak{gr}_2)] + AN[GN(\mathfrak{gr}_1, \mathfrak{gr}_2)]} \tag{3.44}$$

   where:

$$GN(\mathfrak{gr}_1, \mathfrak{gr}_2) = \frac{\sum[I(\mathfrak{gr}_1 - \mathfrak{gr}_2) - I(\mathfrak{gr}'_1, \mathfrak{gr}'_2)]^2}{4} \tag{3.45}$$

   with the pair $(\mathfrak{gr}'_1, \mathfrak{gr}'_2)$ comes in fourth cases like $(\mathfrak{gr}'_1, \mathfrak{gr}'_2) = \begin{cases} (\mathfrak{gr}_1 - 1, \mathfrak{gr}_2) \\ (\mathfrak{gr}_1, \mathfrak{gr}_2 - 1) \\ (\mathfrak{gr}_1 + 1, \mathfrak{gr}_2) \\ (\mathfrak{gr}_1, \mathfrak{gr}_2 + 1) \end{cases}$.

   $I(\mathfrak{gr}_1, \mathfrak{gr}_2)$ and $I(\mathfrak{gr}'_1, \mathfrak{gr}'_2)$ represents the gray score at position $(\mathfrak{gr}_1, \mathfrak{gr}_2)$ and $(\mathfrak{gr}'_1, \mathfrak{gr}'_2)$ respectively.

   and

$$AN[GN(\mathfrak{gr}_1, \mathfrak{gr}_2)] = \frac{\sum_{N=2}^{M-1}\sum_{M=2}^{N-1} GN(\mathfrak{gr}_1, y)}{(M-2)(N-2)} \tag{3.46}$$

with AN and AN' are the Average Neighborhood gray value before and after the encrypting respectively. Table (3.12) contains the GVD values of images from USC-SIPI database set. Further we compute the GVD score of Lena and Baboon images as shown in table (3.13). The listed results are comparable to [Firdous *et al.* (2019), Rehman *et al.* (2018)].

Table 3.12 : GVD scores of images from USC-SIPI database.

Image	Proposed			[Rehman *et al.* (2018)]		
	Red	Green	Blue	Red	Green	Blue
4.1.01	0.976	0.978	0.975	0.977	0.979	0.975
4.1.02	0.979	0.981	0.981	0.978	0.979	0.979
4.1.03	0.976	0.978	0.979	0.978	0.976	0.977
4.1.04	0.985	0.982	0.985	0.979	0.975	0.980
4.1.05	0.979	0.964	0.967	0.982	0.966	0.969
4.1.06	0.943	0.910	0.932	0.943	0.912	0.934
4.1.07	0.990	0.987	0.988	0.989	0.983	0.992
4.1.08	0.985	0.980	0.981	0.985	0.973	0.983
4.2.01	0.996	0.991	0.991	0.989	0.968	0.977
4.2.03	0.878	0.860	0.859	0.936	0.906	0.903
4.2.05	0.979	0.975	0.978	0.954	0.939	0.976
4.2.06	0.971	0.953	0.948	0.971	0.958	0.924
4.2.07	0.976	0.972	0.974	0.976	0.948	0.974
House	0.964	0.963	0.965	0.943	0.938	0.942
Average	0.968	0.962	0.965	0.970	0.957	0.963
Average all	0.965			0.963		

Table 3.13 : GVD comparison.

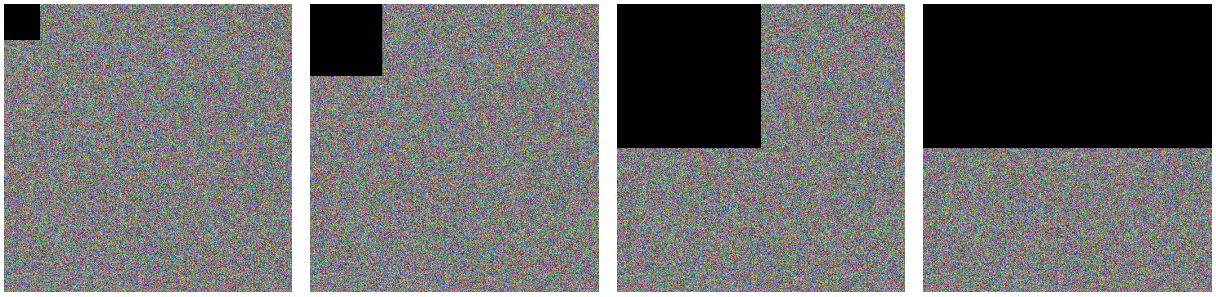
Image	Proposed			[Firdous *et al.* (2019)]			[Rehman *et al.* (2018)]		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	0.9864	0.9885	0.9886	0.9865	0.9854	0.9867	0.9953	0.9891	0.9877
Baboon	0.9785	0.9810	0.9898	0.9868	0.9875	0.9829	0.9650	0.9693	0.9540
Average	0.9825	0.9850	0.9892	0.9867	0.9864	0.9848	0.9801	0.9792	0.9710
Average all	0.9856			0.9860			0.9770		

3.3.3.7 Robustness analysis

In the real issue, the errors often occur in the data while being transmitted by a physical communication system. A unimportant change in the encrypted image may cause a strong distortion in the decryption procedure which results in failure to recover the plain image such that one can loses the plain image completely. A decent cryptosystem should be designed in a way that it does not have domino effect in the decryption procedure. To illustrat the performance of our cryptosystem in those situations, we applied it to the following scenarios:

- Attack in the transmission channel, where we applied occlusion attack to the encrypted images.
- Noise in the transmission channel, in this scenario we add noise to the encrypted images.

1. Occlusion attack scenario
   In the communications channels, lossing some parts of the transmitted (i. e. the encrypted) image can occur, so in this section we test our proposed cryptosystem to show it reaction under an occlusion attack. To show the strength of proposed cryptosystem we remove 1/16, 1/8, 1/4 and 1/2 part respectively of the encrypted image in figure (3.11(d)) is removed as shown in figures (3.14(a)-(d)) and resultant the decrypted images in figures (3.14(e)-(h)).



(a) 1/16 of encrypted Lena. **(b)** 1/8 of encrypted Lena. **(c)** 1/4 of encrypted Lena. **(d)** 1/2 of encrypted Lena.

(e) Decrypted image of (a). **(f)** Decrypted image of (b). **(g)** Decrypted image of (c). **(h)** Decrypted image of (d).

Figure 3.14 : Test of occlusion attack.

The PSNR, NPCR and UCI scores are listed for the lossy decrypted images in table (3.14). The scores are far better than [Rehman *et al.* (2018), Rehman & Liao (2019)].

Table 3.14 : PSNR, NPCR and UACI between plain and decrypted image under different clipping size.

Cryptosystem	Clipping size	Scores		
		PSNR	NPCR	UACI
Proposed	1/16	31.5154	0.3803	0.1119
	1/8	25.4857	1.5523	0.4795
	1/4	19.4787	6.2277	1.8931
	1/2	13.4436	24.8197	7.0959
[Rehman *et al.* (2018)]	1/16	20.5755	6.2312	1.7060
	1/8	17.5727	12.4569	3.8502
	1/4	14.5911	24.9108	7.6825
	1/2	11.5804	49.8112	15.0037
[Rehman & Liao (2019)]	1/16	20.7135	6.2317	1.8709
	1/8	17.7001	12.4213	3.7845
	1/4	14.7211	24.9004	7.5223
	1/2	11.7071	49.8135	15.1348

2. Noise addition scenario

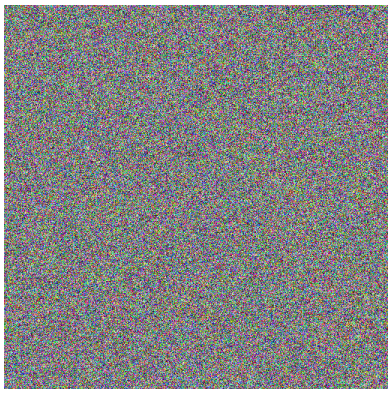
   In order to show the robustness of our proposed cryptosystem on a noisy envirement, we take for example figure (3.11(f)) and we contaminaed it by the Salt & Pepper noise where the noise density is 0.005, 0.05 and 0.5 which resulting the images in figures (3.15(a)-(c)), with their corresponding decrypted images are displayed in figures (3.15(d)-(f)). With a similar way, the Gaussian noise with a zero mean and a noise variances of 0.002, 0.05 and 0.3 is add to figure (3.11(f)) resultant the images shown in figure (3.16(a)-(c)) and the corresponding decrypted images are displayed in figure (3.16(d)-(f)). The scores of NPCR, UACI and PSNR are computed and compared with [Rehman *et al.* (2018), Rehman & Liao (2019), Wu *et al.* (2015)] in tables (3.15) and (3.16). It clear that the obtained scores by using our propsed cryptosystem are far better than the others cryptosystems.

Table 3.15 : Comparison of Salt & Pepper noise robustness.

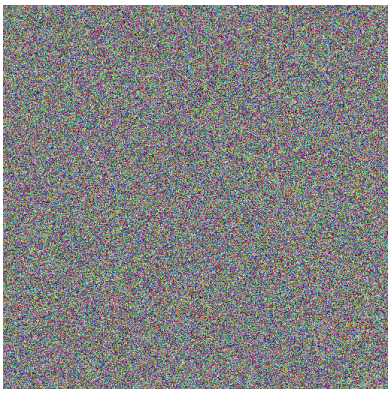
Cryptosystem	Test	Density		
		0.005	0.05	0.5
Proposed	PSNR	31.2433	21.3224	11.3258
	NPCR	0.4883	5.0161	49.8182
	UACI	0.1627	1.6167	15.9819
[Rehman *et al.* (2018)]	PSNR	30.8746	20.7749	10.7973
	NPCR	4.9687	4.9544	49.7898
	UACI	1.5299	1.6801	16.8714
[Rehman & Liao (2019)]	PSNR	30.9406	20.8718	10.8938
[Wu *et al.* (2015)]	PSNR	30.5055	20.7361	10.7593

Table 3.16 : Comparison of Gaussian noise robustness.

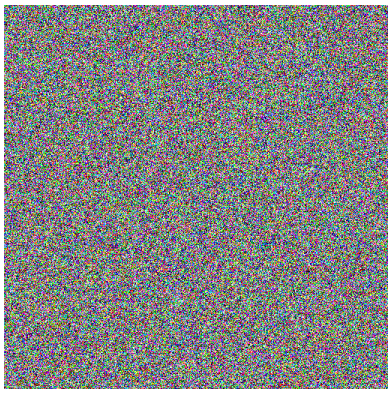
Cryptosystem	Test	Variance		
		0, 0.002	0, 0.05	0, 0.3
Proposed	PSNR	16.8478	11.5359	9.6040
	NPCR	64.0608	65.9392	66.2140
	UACI	5.2099	12.8488	17.3394
[Rehman *et al.* (2018)]	PSNR	16.1519	10.8171	9.5722
	NPCR	96.1743	98.9512	99.3285
	UACI	8.8256	20.9620	26.2130
[Rehman & Liao (2019)]	PSNR	15.1541	10.0792	8.8382
[Wu *et al.* (2015)]	PSNR	16.3605	10.9838	9.1990



(a) Encrypted with density 0.005.



(b) Encrypted with density 0.05.



(c) Encrypted with density 0.5.

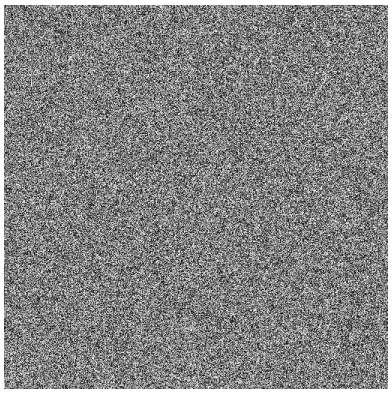
(d) Decrypted Panda image from (a).

(e) Decrypted Panda image from (b).

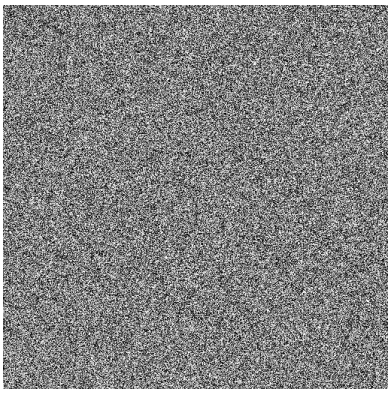
(f) Decrypted Panda image from (c).

Figure 3.15 : Test of Salt & Pepper noise.

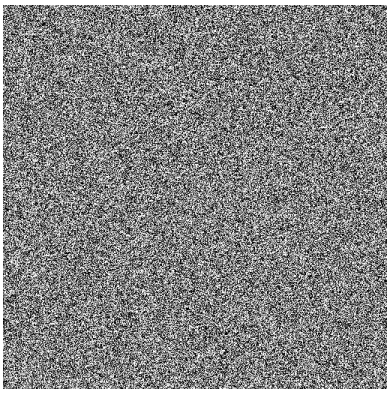
To further investigate the robustness to resist the transmission noise, In a similarty, we perform on figure (3.11(e)) the same scenario as for figure (3.11(f)), the only difference in this case we change the noise parameters, where the densities of Salt & Pepper noise is choosen as 0.01, 0.05, 0.1 and 0.25, and the variances of the Gaussian noise is set as 0.0001, 0.0003 and 0.0005. The results are shown in tables (3.17) and (3.18) which clearly shows that the proposed cryptosystem has better results than [Chai *et al.* (2017), Kulsoom *et al.* (2016), Rehman *et al.* (2018)].



(a) Encrypted with variance 0.005.



(b) Encrypted with variance 0.05.



(c) Encrypted with variance 0.5.

(d) Decrypted Panda image from (a).

(e) Decrypted Panda image from (b).

(f) Decrypted Panda image from (c).

Figure 3.16 : Test of Gaussian noise.

Table 3.17 : Comparison of Salt & Pepper noise robustness.

Cryptosystem	Test	Density			
		0.01	0.05	0.1	0.25
Proposed	PSNR	38.1723	28.3143	21.3222	14.3476
	NPCR	0.1076	0.9726	5.0187	24.8343
	UACI	0.0003	0.3144	1.6187	7.9938
[Kulsoom *et al.* (2016)]	NPCR	25.6199	32.3309	28.7823	32.3357
	UACI	0.3033	2.9426	1.4048	2.9432
[Rehman *et al.* (2018)]	PSNR	28.5722	19.8898	20.7754	14.5109
	NPCR	0.9922	92.3276	4.9533	25.1391
	UACI	0.3047	4.9975	1.6838	7.7347

Table 3.18 : Comparison of Gaussian noise robustness.

Cryptosystem	Test	Variance		
		0, 0.0001	0, 0.0003	0, 0.0005
Proposed	PSNR	23.0860	20.7191	19.5909
	NPCR	56.0293	60.4372	61.7786
	UACI	1.7293	2.6475	3.2007
[Chai *et al.* (2017)]	PSNR	29.0343	28.4843	28.3235
	NPCR	87.7093	93.3500	94.9966
	UACI	17.3511	20.3160	21.5733
[Rehman *et al.* (2018)]	PSNR	22.1317	19.8808	18.8853
	NPCR	86.9097	92.3272	94.0958
	UACI	3.3572	4.9537	5.9804

3.4 Conclusion

In this chapter, a master-slave synchronization scheme using a static error feedback for fractional order hyperchaotic systems have been studied for a known time delay existing in the master-slave configuration. The delay-dependent criterion been given based upon a Lyapunov function and formulated as an LMI problem. The criterion have been applied to fractional order hyperchaotic Liu systems. The simulation results show that the proposed synchronization scheme gives good performance in the presence of time delay in the outputs of the systems. Further, wé have implemented the synchronized systems into a new image stream cryptosystem. Several performance tests are done such as key space and key sensitivity analysis, pixels randomness valuation and pixel modification based measurement and a comparison with other cryptosystems show that the proposed cryptosystem is stronger than the usual cryptosystem due to the hardness of an additional securities derived from the fractional derivativess and has a good security performence.

Chapter 4

Adaptive chaos synchronization: Application to chaos based transmission

4.1 Introduction

Chaos based transmission schemes, as originally conceived, use synchronization of chaotic oscillators as a backbone. It means that, under certain circumstances, the complex and highly sensitive nonlinear dynamics of coupled chaotic oscillators can synchronize, and such synchronous state can be exploited in several different manners to allow communication [Tenny *et al.* (2006)]. In order to improve the degree of security to a much higher level, classical encryption techniques and chaotic synchronization are usually combined [Amigó (2009)]. Since the early nineties, several methods for chaotic synchronization of the transmitter and receiver with applications to secure analog communications have been proposed [Abd *et al.* (2017), Kharel *et al.* (2012), Kwon *et al.* (2011), Smaoui *et al.* (2011), Zhou *et al.* (2021)]. In [Kharel *et al.* (2012)], the authors proposed a chaotic secure transmission scheme based on indirect coupled synchronization scheme. The chaotic transmitter is first used to generate two output signals. The first output signal is used for modulation purposes, while the second output signal is used to drive the chaotic keystream generator, and whose structure is different from the transmitter. Then, the output of the keystream generator is used as a key to encrypt the plain message. The resulting encrypted signal is masked using the first output signal from the transmitter. At the receiver end, the chaotic observer allows obtaining an estimate of the transmitted output signal by synchronization. Consequently, the plain message can be recovered by using the decryption rule. Recently, using linear matrix inequalities (LMIs), sufficient conditions for secure transmission schemes on the n-shift cipher and public key have been obtained in

[Kwon *et al.* (2011)] using a delayed feedback controller technique. Unfortunately, the use of fractional order chaotic systems ha not previously considered in all mentioned schemes. Motivated by above citeed works, this chapter focuses on investigating chaos based analog transmission scheme using an adaptive synchronization between fractional order chaotic systems. The proposed approach is given as follows. Firstly, the encrypted signal by keystream generator is modulated into the transmitter. By appropriately selecting A feedback gain, adaptative chaotic synchronization between the coupled transmitter and receiver is achieved by solving LMI problems. After, by using a Lyapunov stability theorem and LMI, sufficient conditions for indirect coupled synchronization between keystream generators are achieved. Since synchronization is ensured, using an adaptive demodulator the encrypted signal is recovered, then we decrypt it by using the n-shift cipher algorithm and the keystream generator at the receiver side. All involved numerical simulations verify the effectiveness of the proposed scheme possessing remarkable stability to noise. As it would be shown below, our scheme demonstrates the great resistance to noise in comparison with other schemes found in the literature In order to make clear our contribution, let us point out the main differences with respect to the above citeed works:

- Using fractional derivatives in a new chaos based transmission scheme.
- Better resistance to noise.

The structure of the proposed chaos based transmission scheme is shown in figure (4.1).

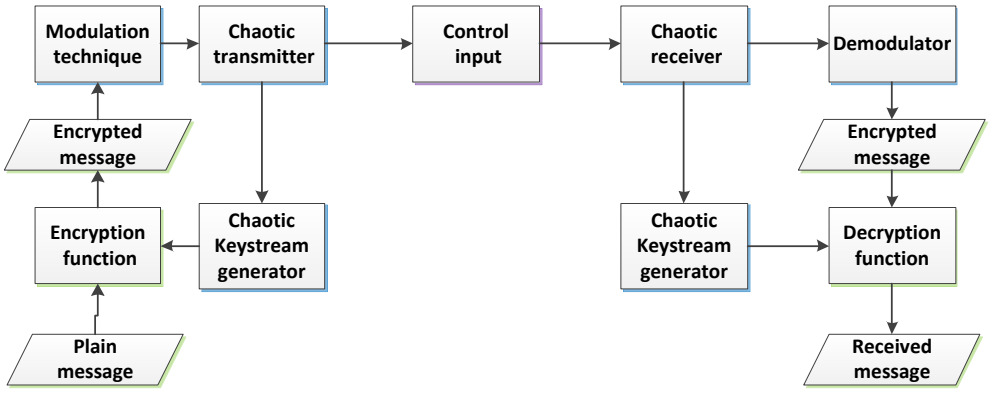


Figure 4.1 : Proposed chaos based transmission scheme.

4.2 Chaos synchronization

4.2.1 Problem formulation

The chaos based transmission scheme using fractional order chaotic systems is considered as follows:

$$
\begin{aligned}
\mathcal{TR}: \quad & \begin{cases} D_t^\alpha x(t) &= A_1 x(t) + f(x(t)) + B\varphi(t) g_1(x(t)) \\ p(t) &= Cx(t) \end{cases} \\
\mathcal{RC}: \quad & \begin{cases} D_t^\alpha y(t) &= A_1 y(t) + f(y(t)) + B\hat{\varphi}(t) g_1(y(t)) + u(t) \\ q(t) &= Cy(t) \end{cases} \\
\mathcal{C}: \quad & \{u(t) = F(p(t) - q(t)). \\
\mathcal{ST}_\mathcal{M}: \quad & \begin{cases} D_t^\alpha \hat{x}(t) &= A_2 \hat{x}(t) + g_2(x(t)) \\ k_1(t) &= \hat{x}_1(t) \end{cases} \\
\mathcal{ST}_\mathcal{S}: \quad & \begin{cases} D_t^\alpha \hat{y}(t) &= A_2 \hat{y}(t) + g_2(y(t)) \\ k_2(t) &= \hat{y}_1(t) \end{cases}
\end{aligned} \tag{4.1}
$$

where $A_1,\ A_2 \in \mathfrak{R}^{n\times n}$, $B \in \mathfrak{R}^{n\times n_m}$, $C \in \mathfrak{R}^{m_n \times n}$ and $F \in \mathfrak{R}^{n\times n_m}$ are constant matrices. $x(t)$, $y(t)$, $\hat{x}(t)$ and $\hat{y}(t)$ are the state vectors of the transmitter ($\mathcal{TR}$), receiver($\mathcal{RC}$), keystream ($\mathcal{ST}_\mathcal{M}$) and keystream ($\mathcal{ST}_\mathcal{S}$) systems respectively. The output of subsystems are $p(t)$, $q(t)$, $k_1(t)$ and $k_2(t) \in \mathfrak{R}^{m_n}$ respectively. $f(\cdot)$, $g_1(\cdot)$ and $g_2(\cdot)$ are smooth bounded functions of times. $\varphi(t)$ is the output of an encryption function that encrypt the plain message $m(t)$ where it updated as:

$$
D_t^\alpha \hat{\varphi}(t) = \delta \left(e^T(t) C^T \right) g_1(y(t)) \tag{4.2}
$$

In this chapter D_t^α stands for Rieman-Liouville derivative.
Defining the synchronization error between $\mathcal{TR}$ and $\mathcal{RC}$ as $e(t) = x(t) - y(t)$, thus one can yields to:

$$
\begin{aligned}
D_t^\alpha e(t) = \quad & (A_1 - FC)e(t) + (f(x(t)) - f(y(t))) + B\left[(\varphi(t) - \hat{\varphi}(t))\, g_1(y(t)) + \right. \\
& \left. \varphi(t)\, (g_1(x(t)) - g_1(y(t))) \right]
\end{aligned} \tag{4.3}
$$

Defining the synchronization error between $\mathcal{ST}_\mathcal{M}$ and $\mathcal{ST}_\mathcal{S}$ as $e_{\mathcal{STR}}(t) = \hat{x}(t) - \hat{y}(t)$, then

the error dynamics is given by:

$$D_t^{\alpha} e_{\mathcal{STR}}(t) = \quad A_2 e_{\mathcal{STR}}(t) + g_2(x(t)) - g_2(y(t)) \tag{4.4}$$

The following mild assumptions are required.

Assumption 4.2.1. *Since $f(x(t))$, $g_1(x(t))$ and $g_2(x(t))$ are smooth functions, they should be Lipschitz in x, y respectively. In other words, one has:*

$$||f(x(t)) - f(y(t))|| \leq l_e ||x(t) - y(t)||, \ \forall x, \ y \in \Re^n \tag{4.5}$$

$$||g_1(x(t)) - g_1(y(t))|| \leq l_g ||x(t) - y(t)||, \ \forall x, \ y \in \Re^n \tag{4.6}$$

$$||g_2(x(t)) - g_2(y(t))|| \leq l_\varphi ||x(t) - y(t)||, \ \forall x, \ y \in \Re^n \tag{4.7}$$

where l_e, l_g and l_φ are appropriate positive constants.

Assumption 4.2.2. *The matrix $(A_1 - FC)$ is Hurwitz (i. e. so all signals in the closed loop system are bounded).*

Assumption 4.2.3. *The parameter $\varphi(t)$ fulfill the following boundedness property:*

$$||\varphi(t)|| \leq \varphi_c \tag{4.8}$$

where φ_c is a given positive constant.

Assumption 4.2.4. *There is a constant vector F, such that:*

$$\mathcal{F}(\epsilon) = C(\epsilon I - (A_1 - FC))^{-1} B \tag{4.9}$$

is a strictly positive real transfer function(SPR), where ϵ is the Laplace variable.

Remark 4.2.1. *According to the MKY Lemma [Marino & Tomei (1995)], the strict positive realness of $\mathcal{F}(\epsilon)$ equation (4.9) assures the existence of a symmetric and positive matrices $P_1 = P_1^T$, $Q = Q^T > 0$ which satisfies:*

$$(A_1 - FC)^T P_1 + P_1 (A_1 - FC) = -Q \tag{4.10}$$

$$B^T P_1 = C \tag{4.11}$$

Note that the equality in equation (4.11) implies that the span of rows of $B^T P_1$ belongs to the span of rows of C.

Definition 4.2.1. The transmitter ($\mathcal{TR}$) and receiver($\mathcal{RC}$) systems are said to be asymptotically synchronized if and only if the error dynamical system in equation (4.3) is globally asymptotically stable for the equilibrium point $e(t) = 0$. That is, $e(t) \to 0$ as $t \to \infty$.

Theorem 4.2.1. *Let P_1 and Q be positive symmetric matrices, a matrix F with appropriate dimension and two positive constants l_e and l_g. Then there is a positive constant μ_1 in wich satisfie the sufficient condition for asymptotic stability of error system in equation (4.3) given by the following matrix inequalities: $\min_{\mu_1}$, subject to :*

$$(A_1 - FC)^T P_1 + P_1(A_1 - FC) + Q < 0 \tag{4.12}$$

$$\mathcal{M}_1 = \left[-Q - (A_1 - FC)^T P_1 + l_e \phi_{max}(P_1) I + \left(\frac{(\varphi_c^2 + l_g^2)\phi_{max}(P_1 B B^T P_1)}{2\mu_1} I + \frac{\mu_1}{2} I\right)\right] < 0 \tag{4.13}$$

Proof. Consider the following Lyapunov function:

$$\mathcal{L}(t) = D_t^{-(1-\alpha)} \left(\frac{1}{2}\left(e^T(t) P_1 e(t)\right) + \frac{1}{2\delta}\left(\varphi(t) - \hat{\varphi}(t)\right)^2\right) \tag{4.14}$$

where the function is reduced to the classical Lyapunov function when $\alpha = 1$ (see property in equation (A.9)), and it constructed as a Rieman-Liouville fractional integral when $1 > \alpha > 0$, so with δ is positive constant, thus according to equation (1.22) the positive defitiveness for the function is guaranted.

An application of property in equation (A.16) and lemma (2.3.2), we get the time derivative of equation (4.14) as:

$$\dot{\mathcal{L}}_1(t) \leq e^T(t) P_1 D_t^{\alpha} e(t) - \frac{1}{\delta}\left(\varphi(t) - \hat{\varphi}(t)\right) D_t^{\alpha} \hat{\varphi}(t) \tag{4.15}$$

Inserting the error dynamics from equation (4.3), thus we have:

$$\begin{aligned} \dot{\mathcal{L}}_1(t) \leq \quad & e^T(t) P_1 \left((A_1 - FC)e(t) + \left(f(x(t)) - f(y(t))\right) + B\left[\left(\varphi(t) - \hat{\varphi}(t)\right) g_1(y(t))\right.\right. \\ & \left.\left. + \varphi(t)\left(g_1(x(t)) - g_1(y(t))\right)\right]\right) - \frac{1}{\delta}\left(\varphi(t) - \hat{\varphi}(t)\right) D_t^{\alpha} \hat{\varphi}(t) \end{aligned} \tag{4.16}$$

By adding and subtracting likewise terms, we obtain the following:

$$\begin{aligned} \dot{\mathcal{L}}_1(t) \leq \quad & e^T(t) \Big((P_1(A_1 - FC) + (A_1 - FC)^T P_1)e(t) + \left(f(x(t)) - f(y(t))\right) + B\left[(\varphi(t) - \right. \\ & \left.\hat{\varphi}(t)\right) g_1(y(t)) + \varphi(t)\left(g_1(x(t)) - g_1(y(t))\right)\right] - \frac{1}{\delta}\left(\varphi(t) - \hat{\varphi}(t)\right) D_t^{\alpha} \hat{\varphi}(t) \\ & - (A_1 - FC)^T P_1 e(t) \end{aligned} \tag{4.17}$$

In the light of the assumption (4.2.1) and lemma (2.2.3), we can get:

$$e(t)^T P_1 B\left(\varphi(t)(g_1(x(t)-g_1(y(t))\right) \leq \quad \varphi_c||B^T P_1 e(t)||l_p||e(t)|| \leq \frac{\varphi_c^2+l_g^2}{2\mu}||B^T P_1 e(t)||^2 + \frac{\mu_1}{2}||e(t)||^2 \leq \left(\frac{\left(\varphi_c^2+l_g^2\right)\phi_{max}\left(P_1 B B^T P_1\right)}{2\mu_1}+\frac{\mu_1}{2}\right) ||e(t)||^2 \tag{4.18}$$

and

$$e(t)^T(f(x(t)-f(y(t)) \leq l_e \phi_{max}(P_1)||e(t)||^2 \tag{4.19}$$

On the basics of the assumption (4.2.2), we yields to:

$$\dot{\mathcal{L}}_1(t) \leq e(t)^T\left[-Q-(A_1-FC)^T P_1+\left(\frac{\left(\varphi_c^2+l_g^2\right)\phi_{max}\left(P_1 B B^T P_1\right)}{2\mu_1}+\frac{\mu_1}{2}+l_e\phi_{max}(P_1)\right) I_n\right] + e(t)^T B P_1(\varphi(t)-\hat{\varphi}(t))g_1(y(t)))] - \frac{1}{\delta}(\varphi-\hat{\varphi})D_t^{\alpha}\hat{\varphi} \tag{4.20}$$

Using equation (4.11), and $\hat{\varphi}(t)$ is updated according to equation (4.2), hence:

$$\dot{\mathcal{L}}_1(t) \leq e(t)^T\left[-Q-(A_1-FC)^T P_1+\left(\frac{\left(\varphi_c^2+l_g^2\right)\phi_{max}\left(P_1 B B^T P_1\right)}{2\mu_1}+\frac{\mu_1}{2}+l_e\phi_{max}(P_1)\right) I_n\right] e(t) \tag{4.21}$$

Therefore:

$$\dot{\mathcal{L}}_1(t) \leq e(t)^T \mathfrak{M}_1 e(t) < 0 \tag{4.22}$$

with:

$$\mathfrak{M}_1 = \left[-Q-(A_1-FC)^T P_1+\left(\frac{\left(\varphi_c^2+l_g^2\right)\phi_{max}\left(P_1 B B^T P_1\right)}{2\mu_1}+\frac{\mu_1}{2}+l_e\phi_{max}(P_1)\right) I_n\right] \tag{4.23}$$

Then if $\mathfrak{M}_1 < 0$, then $\dot{\mathcal{L}}_1(t) \leq 0$. To derive asymptotical stability we use the lemma (2.3.1). Form $\dot{\mathcal{L}}_1(t) < 0$ it is obtain that $\mathcal{L}_2(t) < \mathcal{L}_1(0)$. To verify the boudennes of $\ddot{\mathcal{L}}_1(t)$, it needs to show that $e(t) \in \ell_2$. Note that $\mathcal{L}_1$ is a non-increasing and positive definite function then:

$$-\int_0^t \dot{\mathcal{L}}_1(t) = \mathcal{L}_1(0) - \mathcal{L}_1(t) < \infty \tag{4.24}$$

$$
\begin{aligned}
&-\int_0^t \dot{\mathcal{L}}_1(t)d\tau < \infty \\
&\Rightarrow \int_0^t [\Lambda_{min}(-\mathfrak{M}_1)||e(t)||^2]d\tau < \infty \\
&\Rightarrow \sqrt{\int_0^t [\Lambda_{min}(-\mathfrak{M}_1)||e(t)||^2]d\tau} < \infty \\
&\Rightarrow \sqrt{\int_0^t ||e(t)||^2 d\tau} < \infty
\end{aligned} \tag{4.25}
$$

where $\Lambda_{min}(-\mathfrak{M}_1)$ represent the minimum eigenvalues of $-\mathfrak{M}_1$. From equation (4.25), it is concluded that $e(t) \in \ell_2$. Then it is derived that:

$$\lim_{t\to\infty} \dot{\mathcal{L}}_1(t) = 0 \tag{4.26}$$

the asymptotic stability is concluded. This completes the proof. □

Theorem 4.2.2. *Assume that equation (4.22) is satisfied. Let P_2 be a positive symmetric matrix and two positive constants l_φ and μ_2 then a sufficient condition for asymptotic stability of error system equation (4.4) is given by the following matrix inequalities:*

$$\mathfrak{M}_2 = \begin{bmatrix} P_2 A_2 + \frac{\mu_2}{2} I_n & 0 \\ 0 & \frac{l_\varphi}{2\mu_2}\phi_{max}(P_2) I_n \end{bmatrix} < 0 \tag{4.27}$$

Proof. Given a Lyapunov function candidate as:

$$\mathcal{L}_2(t) = D_t^{-(1-\alpha)} \left(\frac{1}{2} \left(e_{\mathcal{STR}}^T(t) P_2 e_{\mathcal{STR}}(t) \right) \right) \tag{4.28}$$

where the function is reduced to the classical Lyapunov function when $\alpha = 1$ (see property in equation (A.9)), and it constructed as a Rieman-Liouville fractional integral when $1 > \alpha > 0$, thus according to equation (1.22) the positive defitiveness for the function is guaranted.

An application of property in equation (A.16) and lemma (2.3.2), we get the time derivative of equation (4.28) as:

$$\dot{\mathcal{L}}_2(t) \leq e_{\mathcal{STR}}^T(t) P_2 D_t^\alpha e_{\mathcal{STR}}(t) \tag{4.29}$$

Inserting the error dynamics from equation (4.4), we can get:

$$\dot{\mathcal{L}}_2(t) \leq e_{\mathcal{STR}}^T(t) P_2 \left[A_2 e_{\mathcal{STR}}(t) + g_2(x(t) - g_2(y(t)] \right. \tag{4.30}$$

Using the assumption (4.2.1) and lemma (2.2.3), we can get:

$$e_{\mathcal{STR}}(t)^T P_2(g_2(x(t)) - g_2(y(t))) \leq \frac{\mu_2}{2}||e_{\mathcal{STR}}(t)||^2 + \frac{l_\varphi}{2\mu_2}\phi_{max}(P_2)||e(t)||^2 \tag{4.31}$$

Thus, we have:

$$\dot{\mathcal{L}}_2(t) \leq \quad e^T_{\mathcal{STR}}(t)P_2A_2e_{\mathcal{STR}}(t) + \frac{\mu_2}{2}||e_{\mathcal{STR}}(t)||^2 + \frac{l_\varphi}{2\mu_2}\phi_{max}(P_2)||e(t)||^2 \tag{4.32}$$

Therefore:

$$\dot{\mathcal{L}}_2(t) \leq \xi(t)^T\mathfrak{M}_2\xi(t) < 0 \tag{4.33}$$

where $\xi(t) = [e_{\mathcal{STR}}(t); e(t)]$ and $\mathfrak{M}_2 =$

$$\begin{bmatrix} P_2A_2 + \frac{\mu_2}{2}I_n & 0 \\ 0 & \frac{l_\varphi}{2\mu_2}\phi_{max}(P_2)I_n \end{bmatrix}$$

Then if $\mathfrak{M}_2 < 0$, then $\dot{\mathcal{L}}_2(t) \leq 0$. To derive asymptotical stability we use the lemma (2.3.1). Form $\dot{\mathcal{L}}_2(t) < 0$ it is obtain that $\mathcal{L}_2(t) < \mathcal{L}_2(0)$. To verify the boudennes of $\ddot{\mathcal{L}}_2(t)$, it needs to show that $\xi(t) \in \ell_2$. Note that $\mathcal{L}_2$ is a non-increasing and positive definite function then:

$$-\int_0^t \dot{\mathcal{L}}_2(t) = \mathcal{L}_2(0) - \mathcal{L}_2(t) < \infty \tag{4.34}$$

$$\begin{aligned} &-\int_0^t \dot{\mathcal{L}}_2(t)d\tau < \infty \\ &\Rightarrow \int_0^t [\Lambda_{min}(-\mathfrak{M}_2)||\xi(t)||^2]d\tau < \infty \\ &\Rightarrow \sqrt{\int_0^t [\Lambda_{min}(-\mathfrak{M}_2)||\xi(t)||^2]d\tau} < \infty \\ &\Rightarrow \sqrt{\int_0^t ||\xi(t)||^2 d\tau} < \infty \end{aligned} \tag{4.35}$$

where $\Lambda_{min}(-\mathfrak{M}_2)$ represent the minimum eigenvalues of $-\mathfrak{M}_2$. From equation (4.35), it is concluded that $\xi(t) \in \ell_2$. Then it is derived that:

$$\lim_{t\to\infty} \dot{\mathcal{L}}_2(t) = 0 \tag{4.36}$$

the asymptotic stability is concluded. This completes the proof. □

Remark 4.2.2. *The fact that the matrix $A_1 - FC$ is Hurwitz, allows us to conclude about the stability of the scheme. However, if the matrix $A_1 - FC$ has eigenvalues with positive real parts, then consequently the stability can't be proved using this methodology and the Lyapunov function in equation (4.14).*

4.2.2 Numerical example

To verify the theoretical results, we carry out numerical simulations, where the fractional order Lorenz system [Grigorenko & Grigorenko (2003)] is used as the transmitter and receiver, whereas transmitting and receiving keystream generators are chosen to be the fractional order Chua system as described equation (2.18).
Consider the following representation of the fractional order Lorenz system:

$$\begin{cases} D_t^\alpha x_1(t) = \kappa_1(x_2(t) - x_1(t)) \\ D_t^\alpha x_2(t) = x_1(t)(\kappa_2 - x_3(t)) - x_2(t) \\ D_t^\alpha x_3(t) = x_1(t)x_2(t) - \kappa_3 x_3(t) \end{cases} \tag{4.37}$$

where:$\kappa_1 = 10$, $\kappa_2 = 28$, $\kappa_3 = \frac{8}{3}$ and we set $\alpha = 0.995$ to ensure the existence of chaos [Grigorenko & Grigorenko (2003)]. An encrypted message is added in the right-hand side of equation (4.37). The transmitter is described as follows:

$$\begin{cases} D_t^\alpha x_1(t) = \kappa_1(x_2(t) - x_1(t)) + \varphi(t)g(x_1(t)) \\ D_t^\alpha x_2(t) = x_1(t)(\kappa_2 - x_3(t)) - x_2(t) \\ D_t^\alpha x_3(t) = x_1(t)x_2(t) - \kappa_3 x_3(t) \end{cases} \tag{4.38}$$

and the receiver as:

$$\begin{cases} D_t^\alpha y_1(t) = \kappa_1(y_2(t) - y_1(t)) + \hat{\varphi}(t)g(y_1(t)) + u_1(t) \\ D_t^\alpha y_2(t) = y_1(t)(\kappa_2 - y_3(t)) - y_2(t) + u_2(t) \\ D_t^\alpha y_3(t) = y_1(t)y_2(t) - \kappa_3 y_3(t) + u_3(t) \end{cases} \tag{4.39}$$

Moreover, by introducing $p(t) = x_1(t)$, equation (4.38) can be rewritten in a compact form as follows:

$$\begin{aligned} D_t^\alpha x(t) = & \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -\frac{8}{3} \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ -x_1(t)x_3(t) \\ x_1(t)x_2(t) \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \varphi(t)g_1(x_1(t)) = \\ & A_1 x(t) + f(x(t)) + B\varphi(t)g_1(x_1(t)) \end{aligned} \tag{4.40}$$

with $p(t) = x_1(t) = [1\ 0\ 0] \times x(t) = C \times x(t)$ and $g_1(x_1(t)) = |x_1(t) + 1| - |x_1(t) - 1|$. It can be easily verified that (A_1, B) is a controllable pair and (C, A_1) is an observable pair. The vector $F = \begin{bmatrix} 0 \\ 38 \\ 0 \end{bmatrix}$ can be found so that the eigenvalues of matrix $A_1 - FC$ are

$-2.6667, -5.5000 + 8.9303i$ and $-5.5000 - 8.9303i$ and so that the transfer function:

$$\mathcal{F}(\epsilon) = \frac{\epsilon^2 + 3.667\epsilon + 902.7}{\epsilon^3 + 13.67\epsilon^2 + 1039\epsilon + 9293} \tag{4.41}$$

is strictly positive real, hence the assumptions (4.2.2) and (4.2.4) are satisfied. Moreover, the following symmetric and positive-definite matrices $Q = \begin{bmatrix} 20 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5.3 \end{bmatrix}$ and $P_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and the two positive constants $l_e = 10$ and $l_g = 4$ are choosing to satisfie the LMIs in equations (4.12) and (4.13). After solving the LMIs, the corresponding solution is: $\mu_1 = 6.3301 \times 10^{-13}$.

One can verifie that $B^T P_1 = C$. Moreover, one can easily found that:

$$\mathfrak{M}_1 = \begin{bmatrix} -30.0000 & -10.0000 & 0 \\ 10.0000 & -3.0000 & 0 \\ 0 & 0 & -7.9667 \end{bmatrix}.$$

Further, we verify the synchronization between the keystreams. The positive constant $l_\varphi = 0.5$ is choosing to satisfie the LMI in equation (4.27). After solving the LMI we find:

$$P_2 = 10^4 \times \begin{bmatrix} 0.3168 & 0.1086 & -0.5052 \\ 0.1086 & 0.0699 & -0.0208 \\ -0.5052 & -0.0208 & 1.5156 \end{bmatrix},$$

$\mu_2 = 3.7834 \times 10^{-13}$.

Moreover, one can easily found that $\mathfrak{M}_2$ is negative definite matrix.

4.3 Encryption and decryption

4.3.1 Proposed scheme

The encryption process consists of the n-shift cipher algorithm [Yang *et al.* (1997)] given as:

$$\varphi(t) = \mathcal{G}\left(\cdots \mathcal{G}\left(\mathcal{G}\left(m(t), k_1(t)\right), k_1(t)\right), \cdots, k_1(t)\right) \tag{4.42}$$

where $\mathcal{G}\left(m(t), k_1(t)\right)$ is given by:

$$\mathcal{G}\left(m(t), k_1(t)\right) = \begin{cases} m(t) + k_1(t) + 2l & -2l \leq m(t) + k_1(t) < -l \\ m(t) + k_1(t) & -l \leq m(t) + k_1(t) < l \\ m(t) + k_1(t) - 2l & l < m(t) + k_1(t) \leq 2l \end{cases} \tag{4.43}$$

with l being an encryption parameter which is chosen such that $m(t)$ and $k(t)$ lie within the interval $[-l, l]$.

4.3.2 Decryption

From the received signal $\hat{\varphi}(t)$ and decryption key signal $\mathcal{ST}_{\mathcal{S}}$, the recovered signal $\hat{m}(t)$ can be obtained by the decryption function as follows:

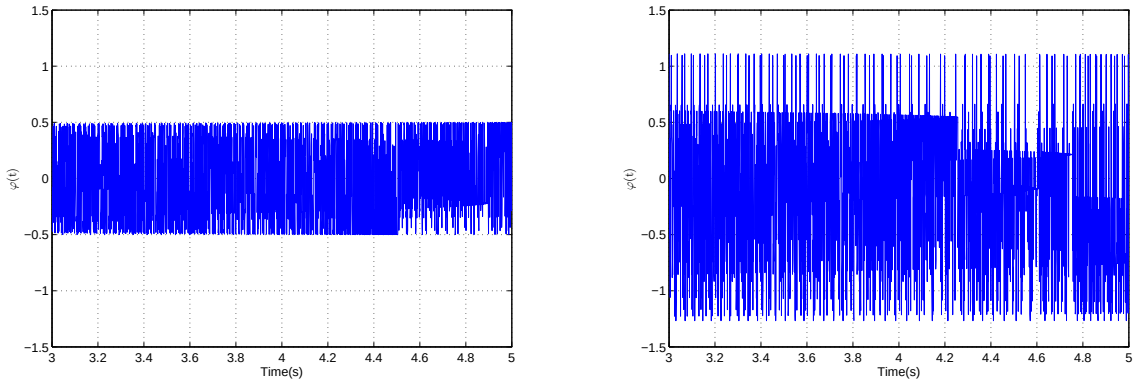
$$\hat{m}(t) = \mathcal{G}\left(\cdots \mathcal{G}\left(\mathcal{G}\left(\hat{\varphi}(t), -k_2(t)\right), -k_2(t)\right), \cdots, -k_2(t)\right) \tag{4.44}$$

4.4 Numerical simulations and performances analysis

Let us transmit two plain messages $m(t) = 0.7\left(1 + sin\left(0.1t\right)\right) cos\left(t\right)$ and $m(t) = 0.5sin\left(2t\right)$. Initial conditions of the keystreams are chosen as $\hat{x}(0) = [0.6,\ -0.1,\ -0.6]^T$ and $\hat{y}(0) = [-2,\ 2,\ 3.8]^T$, respectively. Taking $n = 5$ in equation (4.42), the following encryption is done:

$$\varphi(t) = \mathcal{G}\left(\mathcal{G}\left(\mathcal{G}\left(\mathcal{G}\left(m(t), \hat{x}_1(t)\right), \hat{x}_1(t)\right), \hat{x}_1(t)\right), \hat{x}_1(t)\right), \hat{x}_1(t)\right) \tag{4.45}$$

Choosing the parameter $l = 1.5$ since $||m(t)|| \leq 1.5$ ($||m(t)|| \leq 0.5$) The encrypted messages by equation (4.45) are plotted against time, as given figure (4.2).



(a) Encrypted message of the plain message $m(t) = 0.5sin\left(2t\right)$.

(b) Encrypted message of the plain message $m(t) = 0.7\left(1 + sin\left(0.1t\right)\right) cos\left(t\right)$.

Figure 4.2 : Encrypted messages.

Now the encrypted messages has been transmitted. Initial conditions of the transmitter and receiver systems are $x(0) = [1.8,\ 1.48,\ 1.94]^T$ and $y(0) = [1.9,\ 1.7,\ 1.5]^T$, respectively. The chaotic attractor formed at the transmitter is plotted in figure (4.3).

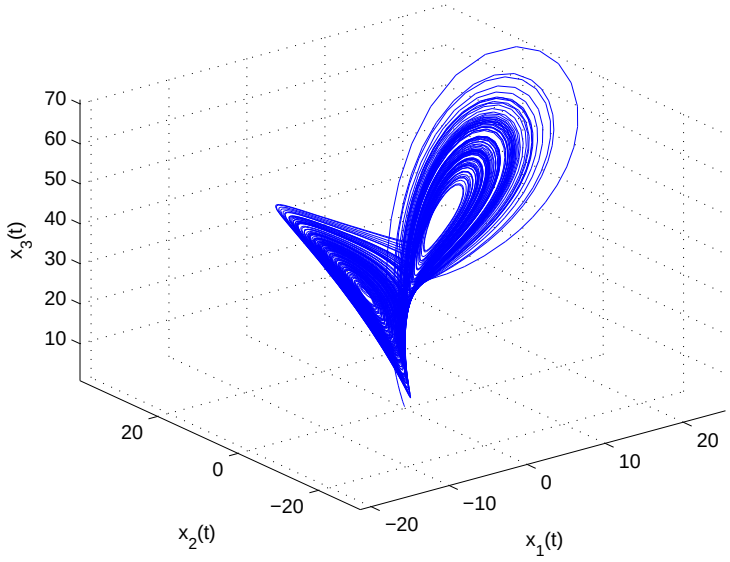


Figure 4.3 : Chaotic attractor of the Lorenz system when φ(t) is modulated.

The synchronization errors between the transmitter and the receiver are depicted in figure (4.4). One can see that the synchronization errors converge to zero, which indicates that the chaos synchronization is indeed realized. The time responses of the state variables of the transmitter and the receiver systems are depicted in figures (4.5), (4.7) and (4.9). It can be seen that the trajectories of the state variables of the receiver track those of the transmitter. The resultant error between the keystreams is given in figure (4.11). The trajectories of the state variables of $\mathcal{ST}_{\mathcal{M}}$ and $\mathcal{ST}_{\mathcal{S}}$ systems are depicted in figures (4.12), (4.13) and (4.14). It is clear that the synchronization is realized.

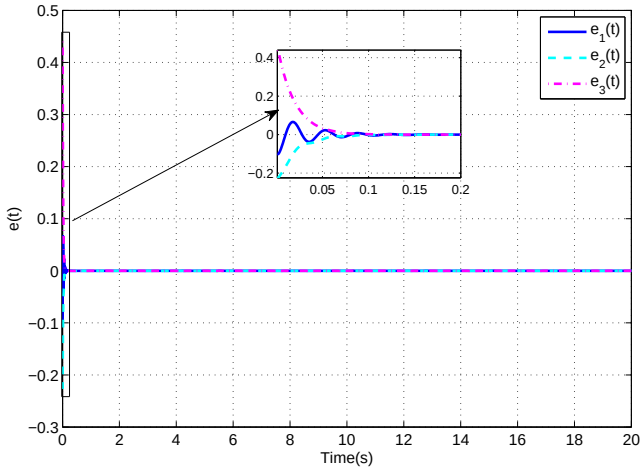


Figure 4.4 : The trajectories of the synchronization errors between transmitter and receiver.

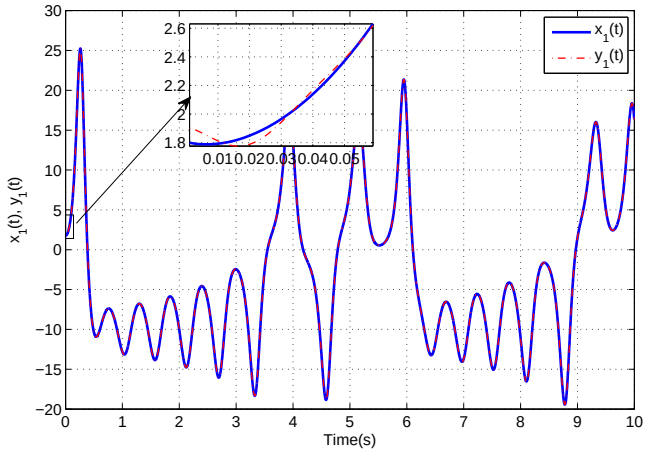


Figure 4.5 : The trajectories of the state variables $x_1(t)$ and $y_1(t)$ in fractional order Lorenz system.

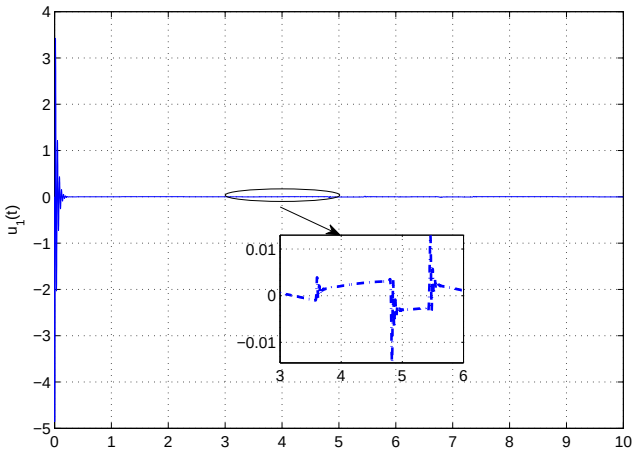


Figure 4.6 : The trajectory of the control input $u_1(t)$ in fractional order Lorenz system.

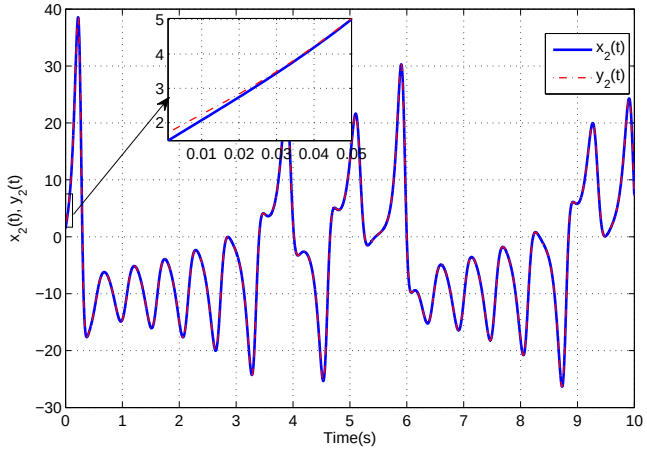


Figure 4.7 : The trajectories of the state variables $x_2(t)$ and $y_2(t)$ in fractional order Lorenz system.

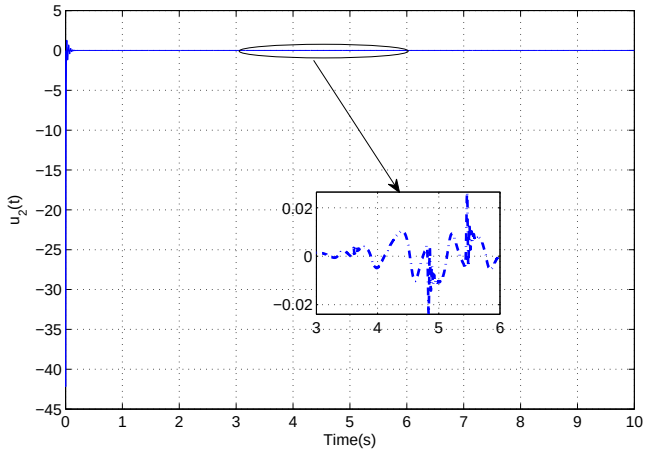


Figure 4.8 : The trajectory of the control input $u_2(t)$ in fractional order Lorenz system.

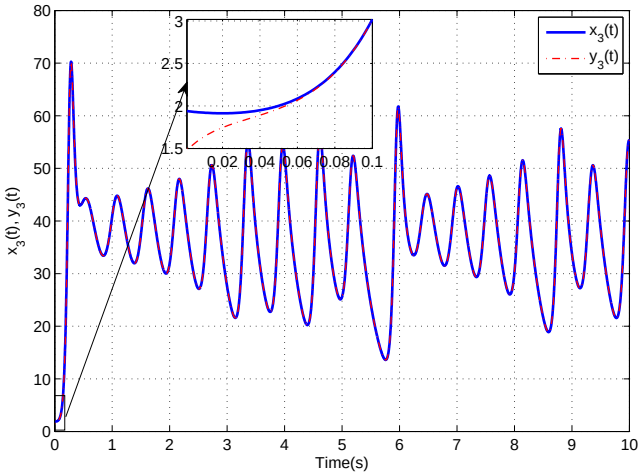


Figure 4.9 : The trajectories of the state variables $x_3(t)$ and $y_3(t)$ in fractional order Lorenz system.

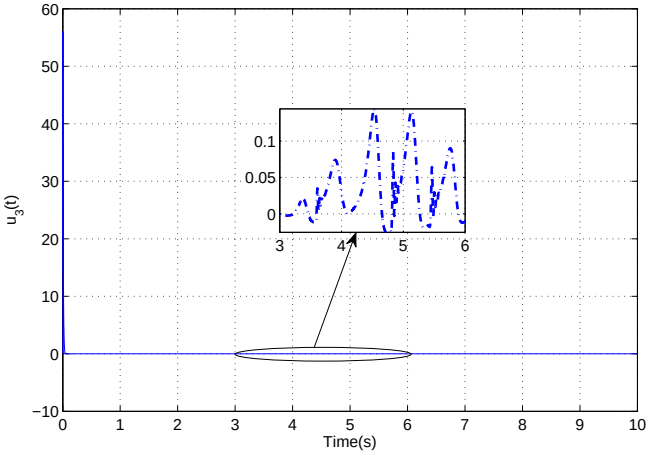


Figure 4.10 : The trajectory of the control input $u_3(t)$ in fractional order Lorenz system.

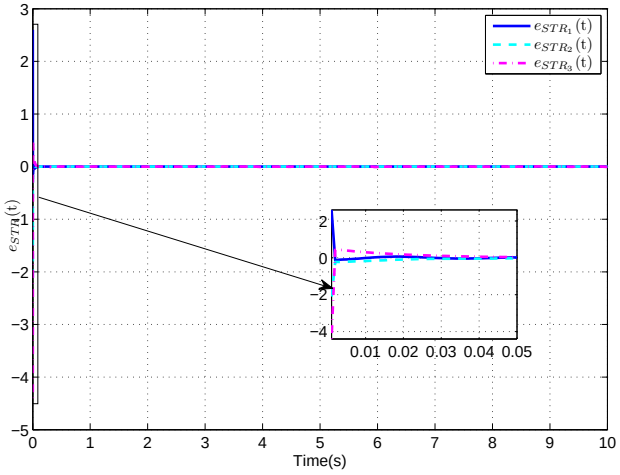


Figure 4.11 : The trajectories of the synchronization errors between keystream generators.

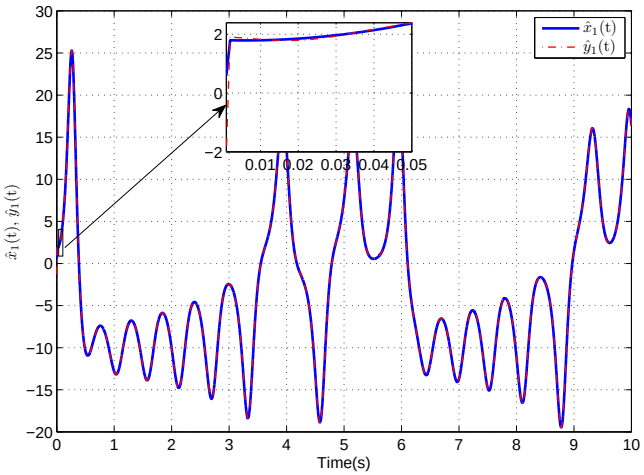


Figure 4.12 : The trajectories of the state variables $\hat{x}_1(t)$ and $\hat{y}_1(t)$ in fractional order Chua's circuit.

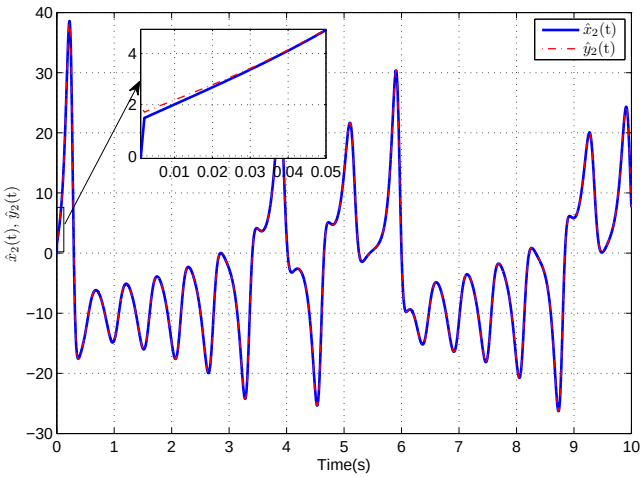


Figure 4.13 : The trajectories of the state variables $\hat{x}_2(t)$ and $\hat{y}_2(t)$ in fractional order Chua's circuit.

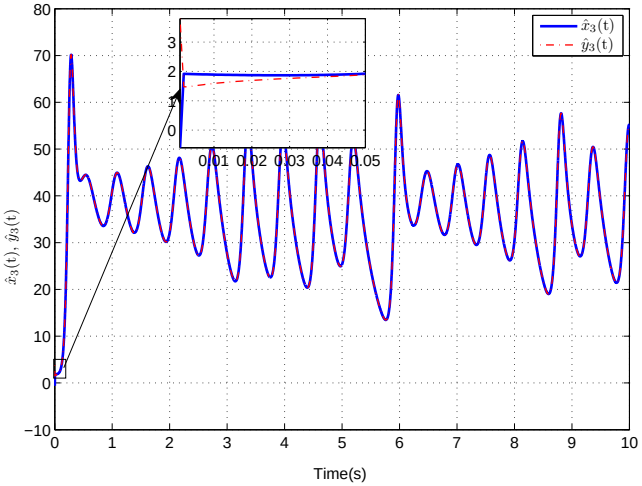
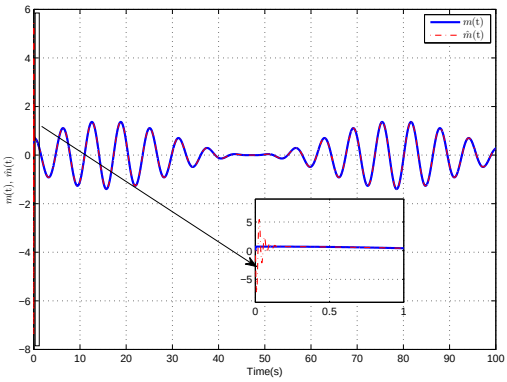
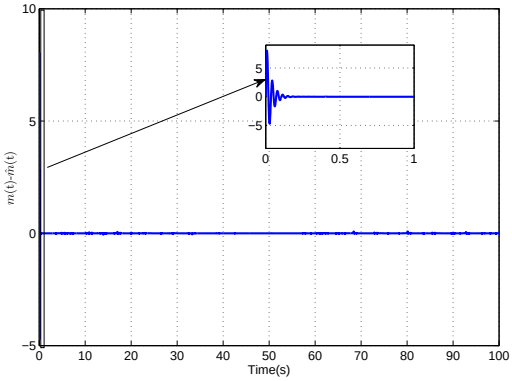


Figure 4.14 : The trajectories of the state variables $\hat{x}_3(t)$ and $\hat{y}_3(t)$ in fractional order Chua's circuit.

Now to recover the messages we use equations (4.2) and (4.44). Figures (4.15) and (4.16) show simulations results. We can clearly see that recovery of plain message using the proposed scheme is achieved quickly.

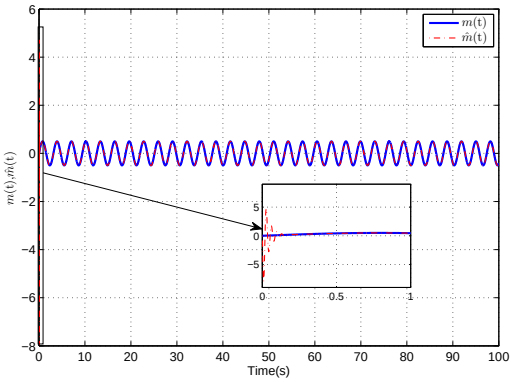


(a) The plain message $m(t)$ and the recovered message $\hat{m}(t)$.

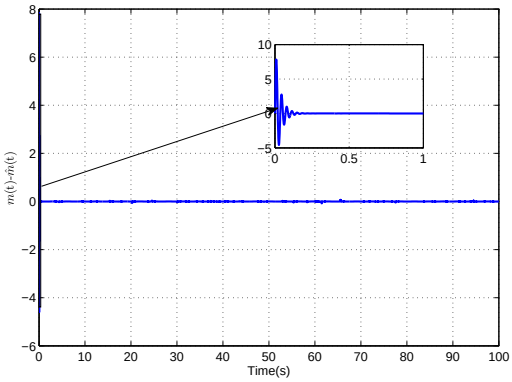


(b) The error between the plain message $m(t)$ and the recovered messages $\hat{m}(t)$.

Figure 4.15 : Behavior of the transmission when $m(t) = 0.7\,(1 + sin\,(0.1t))\,cos\,(t)$.



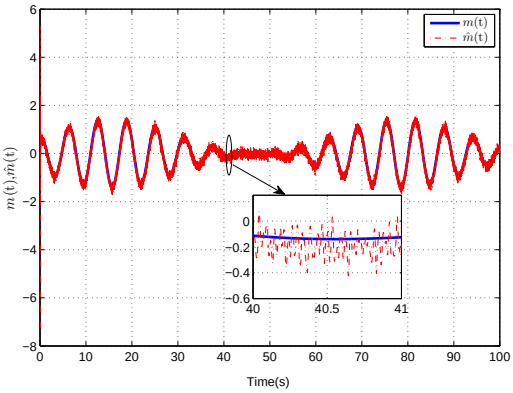
(a) The plain message $m(t)$ and the recovered message $\hat{m}(t)$.



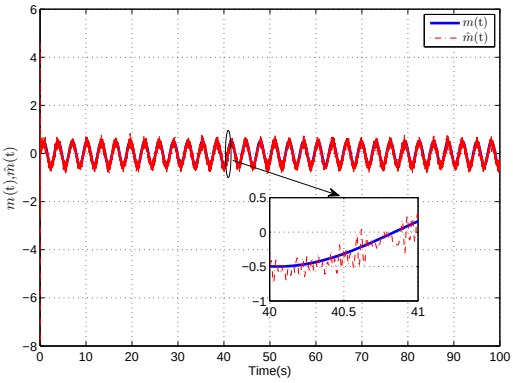
(b) The error between the plain message $m(t)$ and the recovered message $\hat{m}(t)$.

Figure 4.16 : Behavior of the transmission when $m(t) = 0.5sin\,(2t)$.

The stability of communication schemes to noise is one of the most important features of secure communication scheme. To verify the robustness in presence of noise, White Gaussian Noise (WGN) is added at the transmitter side. Figures (4.17(a)) and (4.17(b)) show simulations results. We can clearly see that recovery of plain message using the proposed secure communication scheme is achieved quickly, in the presence of the channel noise.



(a) Behavior of the transmission in presence of WGN when $m(t) = 0.7\,(1 + sin\,(0.1t))\,cos\,(t)$.



(b) Behavior of the transmission in presence of WGN when $m(t) = 0.5sin\,(2t)$.

Figure 4.17 : Behavior of the transmission in presence of WGN.

In order to measure the efficiency of the proposed scheme in the presence of noise the following evaluation parameters, are taken into consideration.

4.4.1 The average energy (AE)

For digital secure transmission schemes such characteristics is an average energy of chaotic radio pulse per transmitted information bit E_b related to the noise spectral density N_0, up to which the secure transmission scheme remains efficient [Sklar (2001)]. The average

energy (AE) is given by:

$$AE = \frac{E_b}{N_0}\,[dB] \tag{4.46}$$

where the energy per bit E_b is described by:

$$E_b = P_{signal} \times T \tag{4.47}$$

where P_{signal} and T are the power of transmitted signal without noise and the time spent for transmission of one bit of information respectively.
The noise spectral density N_0 is defined as:

$$N_0 = P_{noise}/\Delta \tag{4.48}$$

where P_{noise} is the power of noise in the communication channel and Δ is the bandwidth of the channel. In the simulations the channel bandwidth has been chosen to be $\Delta = 0.2$. To compare the effectiveness of our communication scheme in the presence of noise with the several other ones we have estimated the value of AE, up to which secure communication scheme remains efficient, for our scheme and a series of another schemes proposed in earlier publications [Abd *et al.* (2017), Smaoui *et al.* (2011), Zhou *et al.* (2021)]. The AE values are shown in table (4.1). From the table, one can observe that our proposed scheme shows a remarkable robustness against additive noise even if the noise intensity considerably exceeds the transmitting signal one.

Table 4.1 : Average energy comparison.

Scheme	AE (dB)
Proposed	73.4670
[Abd *et al.* (2017)]	55.2481
[Smaoui *et al.* (2011)]	38.2957
[Zhou *et al.* (2021)]	31.8784

4.4.2 Performance in terms of BER

The BER between the transmitted message and the received message is calculated by the following equation:

$$BER = \frac{Number\ of\ erroneous\ bits}{Total\ number\ of\ bits} \times 100\% \tag{4.49}$$

In figure (4.18), we numerically evaluate the performance of the mentioned schemes in terms of BER as a function of average energy. The white noise power spectral density in the channel is N0/2. As expected, it is clear that the proposed scheme is the one that has the best performance among them. This is so basically because the energy per symbol is

kept constant in this scheme.

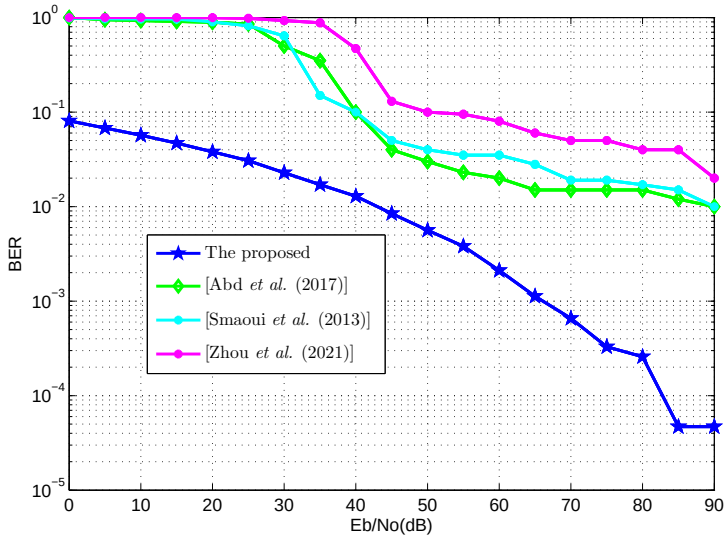


Figure 4.18 : BER performance.

4.5 Conclusion

In this chapter, we have proposed a new chaos based transmission scheme based on adptative and indirect coupled synchronization schemes between fractional order chaotic systems. The plain message have been encrypted by a keystream generatorr and modulated in the transmitter parameters. An adaptive controller is constructed so that the transmitter and the receiver systems are to be synchronized. By appropriately selecting feedback gain vector such that the strictly positive real condition is satisfied. Sufficient conditions for indirect coupled synchronization between keystream generators have been achieved. Since synchronization was ensured, using an adaptive demodulator the encrypted signal is recovered and decrypted. Compared to some secure transmission schemes, this proposed scheme provides a higher level of security, maintains the recovery of the plain message, and shows robustness against additive noise. Numerical simulations are consistent with the theoretical results.

General conclusion

In this research work, we have looked at the problem of chaos synchronization, and we have arrived at the main contributions:

- Design a chaotic and fractional order synchronization schemes.
- The development of a new chaos based cryptography and transmission schemes.

In this thesis, we have presented two new theorems, which guarantee the synchronization of fractional order chaotic chaotic Lur'e systems. the Lyapunov functions were chosen to derive the synchronization criterions. The derived criterions are a suffcient condition for the asymptotic stability of the error systems, formulated in the form of linear matrix inequalities. The controllers gain have been achieved by solving the LMI. The validity of these proposed synchronization schemes has been confirmed via some numerical simulations. This is all part of our **first contribution**.

The **second contribution** of our work, deals about a synchronization scheme of the master-slave type with a known time delay via a static error feedback. Where a sufficient conditions were expressed by means of linear matrix inequality and the delay-dependent criterion was given based upon a Lyapunov function. The **third contribution** was a simple application of this second one to a new chaos cryptosystem. Where we have considered two scenarios corresponding to the transmission channel, under occlusion attack and under noise addition respectively. Some simulations experiments have been carried out to assess the performanace of the proposed contributions.

In the **fourth contribution**, a new chaos based transmission scheme using an adaptive synchronization between fractional order chaotic systems has been investigated. In the design process, the encrypted message have been modulated into the transmitter. By appropriately selecting a feedback gain, adaptative chaotic synchronization between the coupled transmitter and receiver was achieved by solving LMI problems. After the synchronization was achieved, using Lyapunov stability theorem and an LMI, sufficient conditions for indirect coupled synchronization between keystream generators have been achieved.

Finally, by using an adaptive demodulator the encrypted message was recovered and we have decrypt it by using the n-shift cipher algorithm. A set of numerical simulations have illustrated the performances of the proposed scheme.

In **perspective** of our doctoral research work, we will focus on:

- The practical realization of the proposed chaos based cryptography and transmission schemes with performance improvement.
- The design of a synchronization scheme between fractional order chaotic Lur'e systems with multiple random delays and parameters uncertainty and parameters mismatch.
- We plan also to propose a T.S fuzzy and H_∞ synchronization scheme for fractional order chaotic systems subject to input constraints.

Appendix A

Useful functions and properties in fractional calculus

A.1 Useful functions

A.1.1 The Gamma function

The Euler's gamma function, $\Gamma(Z)$, is one of the basic functions of the fractional order calculus. It can generalize the fractional $n!$ and allows n to take also non-integer and even complex values. That is why it is usually treated as the factorial of non-integer numbers [Artin (1964)]. It's integrad form can be written as:

$$\Gamma\left(\mathrm{Z}\right) = \int_0^{+\infty} e^{-t} t^{z-1} dt, \;\; Z > 0 \tag{A.1}$$

where $\Gamma(1) = 1$, $\Gamma(0) = +\infty$.
Two main properties characterize the Gamma function:

1. An integration by part of its formula leads to a recurrence relation given as follows:

$$\Gamma\left(\mathrm{Z}+1\right) = \mathrm{Z}\Gamma\left(\mathrm{Z}\right) \tag{A.2}$$

2. This function is generalization of a factorial in the following form:

$$\Gamma\left(\mathrm{Z}\right) = (\mathrm{Z}-1)! \tag{A.3}$$

A.1.2 The Mittag-Leffler function

The Mittag-Leffler function plays a generalization the exponential function in the whole calculus. Its formula was introduced by G.M. Mittag-Leffler [Mittag-Leffler (1903)] wich plays an essential role in the solution of fractional order differential equations. It expressed by the following function:

$$\mathrm{E}_{\alpha}\left(\mathrm{Z}\right)=\sum_{k=0}^{\infty}\frac{\mathrm{Z}^{k}}{\Gamma\left(\alpha k+1\right)},\ \left(\alpha>0\right) \tag{A.4}$$

A new two-parameter formula defined by the following [Gorenflo *et al.* (1998)]:

$$\mathrm{E}_{\alpha,\beta}\left(\mathrm{Z}\right)=\sum_{k=0}^{\infty}\frac{\mathrm{Z}^{k}}{\Gamma\left(\alpha k+\beta\right)},\ \left(\alpha>0,\ \beta>0\right) \tag{A.5}$$

A.2 Useful properties

According to [Podlubny (1998)], Here some main properties of fractional order integration and differentiation. Let $f(t)$ and $g(t)$ be n continuous functions for $t\geq a$, $\mu_1,\mu_2\in\mathfrak{R}$ and $1\geq\alpha>0$, $1\geq\beta>0$.

A.2.1 Grünwald-Letnikov

The Grünwald-Letnikov fractional differentiation operator is a linear, hence:

$${}_{a}^{GL}D_{t}^{\alpha}\left(\mu_1 f(t)+\mu_2 g(t)\right)=\mu_1\,{}_{a}^{GL}D_{t}^{\alpha}f(t)+\mu_2\,{}_{a}^{GL}D_{t}^{\alpha}g(t) \tag{A.6}$$

The Grünwald-Letnikov fractional differentiation operators are commute, thus:

$${}_{a}^{GL}D_{t}^{\alpha}\left({}_{a}^{GL}D_{t}^{\beta}f(t)\right)={}_{a}^{GL}D_{t}^{\alpha+\beta}f(t) \tag{A.7}$$

A.2.2 Riemann-Liouville

Under certain reasonable asumptions, we have:

$$\lim_{\alpha\to 0}\,{}_{a}^{RL}D_{t}^{-\alpha}f(t)=f(t) \tag{A.8}$$

so we can put:

$${}_{a}^{RL}D_{t}^{0}f(t)=f(t) \tag{A.9}$$

The integration of arbitrary real order have the following property:

$$ {}_{a}^{RL}D_{t}^{-\alpha}\left({}_{a}^{RL}D_{t}^{-\beta}f(t)\right) = {}_{a}^{RL}D_{t}^{-\alpha-\beta}f(t) \tag{A.10} $$

The Riemann- Liouville fractional differentiation operator is a left inverse to the Riemann-Liouville fractional integration operator, which means that:

$$ {}_{a}^{RL}D_{t}^{\alpha}\left({}_{a}^{RL}D_{t}^{-\alpha}f(t)\right) = f(t) \tag{A.11} $$

The aboved mentioned property is a particular case of the more general property:

$$ {}_{a}^{RL}D_{t}^{\alpha}\left({}_{a}^{RL}D_{t}^{-\beta}f(t)\right) = {}_{a}^{RL}D_{t}^{\alpha-\beta}f(t) \tag{A.12} $$

with $\alpha \geq \beta \geq 0$, for that the derivative ${}_{a}^{RL}D_{t}^{\alpha-\beta}f(t)$ exists.
If the fractional derivative of the function $f(t)$ is integrable, then:

$$ {}_{a}^{RL}D_{t}^{-\alpha}\left({}_{a}^{RL}D_{t}^{\alpha}f(t)\right) = f(t) - \sum_{j=1}^{k}\left[{}_{a}^{RL}D_{t}^{\alpha-j}f(t)\right]_{t=a}\frac{(t-a)^{\alpha-j}}{\Gamma(\alpha-j+1)} \tag{A.13} $$

The Riemann- Liouville fractional differentiation operator is a linear, such that:

$$ {}_{a}^{RL}D_{t}^{\alpha}\left(\mu_1 f(t) + \mu_2 g(t)\right) = \mu_1 {}_{a}^{RL}D_{t}^{\alpha}f(t) + \mu_2 {}_{a}^{RL}D_{t}^{\alpha}g(t) \tag{A.14} $$

The Riemann- Liouville fractional differentiation operators do not commute, that means:

$$ {}_{a}^{RL}D_{t}^{\alpha}\left({}_{a}^{RL}D_{t}^{\beta}f(t)\right) = {}_{a}^{RL}D_{t}^{\alpha+\beta}f(t) - \sum_{j=1}^{m}\left[{}_{a}^{RL}D_{t}^{\beta-j}f(t)\right]_{t=a}\frac{(t-a)^{-\alpha-j}}{\Gamma(1-\alpha-j)} \tag{A.15} $$

Remark A.2.1. *If the conditions in remark (1.6.1) are satisfied, then if for a given function $f(t)$ having integrable derivative the Riemann-Liouville (Grünwald-Letnikov) derivative ${}_{a}^{RL}D_{t}^{\alpha}f(t)$ exist and is integrable. Then, for every $0 < \beta < \alpha$ the derivative ${}_{a}^{RL}D_{t}^{\beta}f(t)$ also exist and integrable. Hence, if we denote $g(t) = {}_{a}^{RL}D_{t}^{-(1-\alpha)}f(t)$, then we can write:*

$$ {}_{a}^{RL}D_{t}^{\alpha}f(t) = \frac{d}{dt}\left({}_{a}^{RL}D_{t}^{-(1-\alpha)}f(t)\right) = \dot{g}(t) \tag{A.16} $$

Noting that $\dot{g}(t)$ is integrable and taking into account the formula in equation (1.23) and the inequality $0 < 1 + \beta - \alpha < 1$, we conclude that the derivative ${}_{a}^{RL}D_{t}^{1+\beta-\alpha}g(t)$ exist and integrable. Then using the property in equation (A.12), we obtain:

$$ {}_{a}^{RL}D_{t}^{1+\beta-\alpha}g(t) = {}_{a}^{RL}D_{t}^{1+\beta-\alpha}\left({}_{a}^{RL}D_{t}^{-(1-\alpha)}f(t)\right) = {}_{a}^{RL}D_{t}^{(\alpha)}f(t) \tag{A.17} $$

A.2.3 Caputo

The Caputo fractional derivative operator is a linear, such that:

$$ {}_a^C D_t^\alpha \left(\mu_1 f(t) + \mu_2 g(t)\right) = \mu_1 {}_a^C D_t^\alpha f(t) + \mu_2 {}_a^C D_t^\alpha g(t) \tag{A.18} $$

The Caputo fractional differentiation operators are commute, hence:

$$ {}_a^C D_t^\alpha \left({}_a^C D_t^\beta f(t)\right) = {}_a^C D_t^{\alpha+\beta} f(t) \tag{A.19} $$

Remark A.2.2. *The Leibniz rule for the fractional differentiation is the following. If $f(\tau)$ is continuous in $[t, a]$ and $g(\tau)$ has $n+1$ continuous derivatives in $[t, a]$, then the fractional derivative of the product $f(t)g(t)$ is given by:*

$$ \begin{aligned} {}_a D_t^\alpha \left(f(t)g(t)\right) = \quad & \sum_{k=0}^{n} \left(\begin{array}{c} \alpha \\ k \end{array} \right) f^{(k)}(t) {}_a D_t^{\alpha-k} g(t) - \frac{1}{n!\Gamma(-\alpha)} \int_a^t (t-\tau)^{-\alpha-1} g(\tau) \\ & d\tau \int_\tau^t f^{(n+1)}(\zeta) (\tau - \zeta)^n \, d\zeta \end{aligned} \tag{A.20} $$

where $n \geq \alpha + 1$ and ${}_a D_t^\alpha$ denotes any operator of the fractional differentiation considered in this thesis.

Appendix B

Linear Matrix inequalities (LMI)

B.1 Definition

LMIs are matrix inequalities which are linear or affine in a set of matrix variables. They are essentially convex constraints and therefore many optimization problems with convex objective functions and LMI constraints can easily be solved efficiently using many existing software. This method has been very popular among control engineers in recent years. This is because a wide variety of control problems can be formulated as LMI problems. An LMI in the variable $x \in \mathcal{R}^n$ has the form:

$$F(x) = A_0 + \sum_{i=1}^{n} A_i x_i > 0 \tag{B.1}$$

where $x \in \Re^n$ is the vector of decision variables and $A_0,\ A_1,\ \cdots,\ A_n \in \Re^{m \times n}$ are symmetric matrices.

B.2 Tricks used in LMIs

Although many problems in control can be formulated as LMI problems, some of these problems result in nonlinear matrix inequalities. There are certain tricks which can be used to transform these nonlinear inequalities into suitable LMI forms.

B.2.1 Change of variables

By defining new variables, it is sometimes possible to linearize nonlinear matrix inequalities [Scherer (2000)]. We take for example, a synthesis of state feedback controller. The objective is to determine a matrix $G \in \mathcal{R}^{m \times n}$ such that all the eigenvalues of the matrix

$A + BG \in \mathfrak{R}^{n\times n}$ lie in the open left-half of the complex plane. Using Lyapunov theory, it can be shown that this is equivalent to find a matrix G and a positive definite matrix $P \in \mathfrak{R}^{n\times n}$ such that the following inequality holds:

$$P\left(A + BG\right) + \left(A + BG\right)^T P < 0 \tag{B.2}$$

Note that the terms with products of G and P are nonlinear or bilinear. Let us multiply either side of the above equation by $Q = P^{-1}$. This gives:

$$QA^T + AQ + QG^T B + BGQ < 0 \tag{B.3}$$

But it is still nonlinear. Let us define a second new variable $L = GQ$. This gives:

$$QA^T + AQ + L^T B^T + BL < 0 \tag{B.4}$$

After solving this LMI, the feedback matrix G and Lyapunov variable P can be recovered from $G = LQ^{-1}$ and $P = Q^{-1}$. This shows that by making a change of variables, we can obtain an LMI from a nonlinear matrix inequality.

B.2.2 Schur's complement

Schur's complement used in transforming nonlinear inequalities of convex type into LMI [Boyd *et al.* (1994)]. Let $Q\left(x\right) = Q(x)^T \in R^{n\times n}$, $R\left(x\right) = R(x)^T \in R^{n\times m}$ and $S\left(x\right) \in R^{n\times p}$ matrices refined in x, the following inequalities are equivalent:

$$\begin{cases} R\left(x\right) < 0 \\ Q\left(x\right) - S\left(x\right) R(x)^{-1} S(x)^T < 0 \end{cases} \tag{B.5}$$

where is equivalent to:

$$\begin{bmatrix} Q\left(x\right) & S\left(x\right) \\ S(x)^T & R\left(x\right) \end{bmatrix} < 0 \tag{B.6}$$

B.3 Types of LMI problems

There are three main classes of optimization problems with constraints that can be expressed using LMI [Boyd *et al.* (1994)].

B.3.1 Feasibility issue

The feasibility problem is to find any feasible solutions for an optimization problem without regard to the objective value. It about finding a vector $x \in C \subset \mathcal{R}^n$ such as $F(x) < 0$. The problem is feasible if $C \neq 0$, there exists a nonempty set of satisfying the inequality $F(x) < 0$.

B.3.2 Linear goal minimization problem

Here, we try to minimize a linear objective under LMI constraints:

$$\begin{aligned} &\min C^T x \\ &x \in R^m / F(x) < 0 \end{aligned} \tag{B.7}$$

where C^T is a known row vector.

B.3.3 Eigenvalue Problem

This is to minimize the largest eigenvalue of a symmetric matrix under an LMI type constraint:

$$\begin{aligned} &\min \lambda \\ &\begin{cases} \lambda I - A(x) < 0 \\ B(x) < 0 \end{cases} \end{aligned} \tag{B.8}$$

where the matrices $A(x)$, $B(x)$ are symmetric and linear.

B.3.4 Generalized eigenvalue problem

In this case, the objective is to minimize the largest generalized eigenvalue of a pair of matrices, linearly dependent on the variable x under LMIs conditions. This challenge is expressed as follows:

$$\begin{aligned} &\min \lambda \\ &\begin{cases} \lambda B(x) - A(x) < 0 \\ B(x) > 0, A(x) < 0 \end{cases} \end{aligned} \tag{B.9}$$

References

[Abd *et al.* (2017)] M. H. Abd, F. R. Tahir, G. A. Al-Suhail & V. T. Pham, "An adaptive observer synchronization using chaotic time-delay system for secure communication", *Nonlinear Dynamics* **90**(4), 2583–2598.

[Alvarez & Li (2006)] G. Alvarez & S. Li, "Some basic Cryptographic requirements for chaos-based cryptosystems", *International Journal of Bifurcation and Chaos* **16**(08), 2129–2151.

[Amigó (2009)] J. M. Amigó, *Chaos-based cryptography. In L. Kocarev, Z. Galias & S. Lian, (eds), Intelligent computing based on Chaos. Studies in Computational Intelligence* **184**, Springer, ISBN:978-3-540-95971-7.

[Amritkar & Gupte (1993)] R. E. Amritkar & N. Gupte, "Synchronization of chaotic orbits: The effect of a finite time step", *Physical Review E* **47**(6), 3889–3895.

[Artin (1964)] E. Artin, *The gamma function*, Courier Dover Publications, ISBN:978-0486789781.

[Baptista (1998)] M. S. Baptista, "Cryptography with chaos", *Physics Letters A* **240**(1-2), 50–54.

[Bluman (1998)] A. G. Bluman, *Elementary Statistics*, McGraw-Hill, ISBN:978-1259755330.

[Boccaletti *et al.* (2002)] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares & C. S. Zhou, "The synchronization of chaotic systems", *Physics reports* **366**(1-2), 1–101.

[Bouridah *et al.* (2018)] M. S. Bouridah, T. Bouden & A. Boulkroune, "Fractional chaos synchronization for color image encryption", *Proc. Third International Conference on Technological Advances in Electrical Engineering*, pp. 1–8.

[Bouridah *et al.* (2020)] M. S. Bouridah, T. Bouden & M. E. Yalçin, "Chaos Synchronization of fractional order Lur'e Systems", *International Journal of Bifurcation and Chaos* **30**(14), 2050206.

[Bouridah *et al.* (2021)] M. S. Bouridah, T. Bouden & M. E. Yalçin, "Delayed outputs fractional order hyperchaotic systems synchronization for images encryption", *Multimedia Tools and Applications* **80**(10), 14723–14752.

[Boyd *et al.* (1994)] S. Boyd, L. El-Ghaoui, E. Feron & V. Balakrishnan, *Linear matrix inequalities in system and control theory*, Society for industrial and applied mathematics, ISBN:0-89871-334-X.

[Chai *et al.* (2017)] X. Chai, Y. Chen & L.Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations", *Optics and Lasers in engineering* **88**, 197–213.

[Chen & Liu (2000)] H. F. Chen & J. M. Liu, "Open-loop chaotic synchronization of injection-locked semiconductor lasers with Gigahertz range modulation", *IEEE journal of quantum electronics* **36**(1),27–34.

[Chen & Zhang (2007)] F. Chen & W. Zhang, "LMI criterion for robust chaos synchronization of a class of chaotic systems", *Nonlinear Analysis: Theory, Methods & Applications* **67**(12), 3384–3393.

[Chen *et al.* (2004)] C. Chen, G. Feng & X. Guan, "Robust synchronization of chaotic Lur'e systems via delayed feedback control", *Physics Letters A* **321**(5-6), 344–354.

[Chen *et al.* (2012)] W. H. Chen, Z. Wang & X. Lu, "On sampled-data control for master-slave synchronization of chaotic Lur'e systems", *IEEE Transactions on Circuits and Systems II: Express Briefs* **59**(8), 1–5.

[Crilly *et al.* (2012)] A. J. Crilly, R. Earnshaw & H. Jones, *Fractals and chaos*, Springer Science & Business Media, ISBN:978-1-4612-7770-5.

[Cuomo *et al.* (1993)] K. M. Cuomo, A. V. Oppenheim & S. H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications", *IEEE Transactions on circuits and systems II: Analog and digital signal processing* **40**(10), 626–633.

[Davis (2011)] R. Davis, *International Assessment of Research and Development in Catalysis by Nanostructured Materials*, World Scientific, ISBN:978-1-84816-690-5.

[Dasgupta *et al.* (2015)] T. Dasgupta, P. Paral & S. Bhattacharya, "Fractional order sliding mode control based chaos synchronization and secure communication", *Proc. International Conference on Computer Communication and Informatics*, pp. 1–6.

[Dedieu *et al.* (1993)] H. Dedieu, M. P. Kennedy, & M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's

circuits", *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing* **40**(10), 634–642.

[Degn *et al.* (2013)] H. Degn, A. V. Holden & L. F. Olsen, *Chaos in biological systems*, Springer Science & Business Media, ISBN: 978-1-4757-9633-9.

[Ditto (1996)] W. L. Ditto, "Applications of chaos in biology and medicine", *Proc. AIP Conference*, pp. 175–201.

[Delavari & Mohadeszadeh (2016)] H. Delavari & M. Mohadeszadeh, "Robust finite-time synchronization of non-identical fractional order hyperchaotic systems and its application in secure communication", *IEEE/CAA Journal of Automatica Sinica* **6**(1), 228–235.

[Diaconu *et al.* (2014)] A. V. Diaconu, A. Costea & M. A. Costea, "Color Image Scrambling Technique Based on Transposition of Pixels between RGB Channels Using Knight's Moving Rules and Digital Chaotic Map", *Mathematical Problems in Engineering* **2014**, 1–15.

[Duarte-Mermoud *et al.* (2015)] M. A. Duarte-Mermoud, N. Aguila-Camacho & J. A. Gallegos, "Using general quadratic Lyapunov function to prove Lyapunov uniform stability for fractional order systems", *Commun Nonlinear Sci Numer Simul* **22**(1-3), 650–659.

[Enayatifar *et al.* (2015)] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee & I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata", *Optics and Lasers in Engineering* **71**, 33–41.

[Feldmann *et al.* (1996)] U. Feldmann, M. Hasler & W. Schwarz, "Communication by chaotic signals :the inverse system approach", *International Journal of Circuit Theory and Applications* **24**, 551–579.

[Firdous *et al.* (2019)] A. Firdous, A. Ur-Rehman & M. M. Saad Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2", *Multimed Tools Appl 78*(17), 24809–248352.

[Kharel *et al.* (2012)] R. Kharel, K. Busawon, Z. Ghassemlooy, Secure communication based on indirect coupled synchronization", *Proc. International Conference on Systems*, pp. 184–189.

[Gan *et al.* (2019)] Z. Gan, X. Chai, D. Han & T. Y. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation", *Neural Comput & Applic* **31**(11), 7111–7130.

[Gorenflo *et al.* (1998)] R. Gorenflo, A. A. Kilbas & S. V. Rogosin, "On the generalized Mittag-Leffler type functions", *Integral Transforms and Special Functions* **7**(3-4), 215–224.

[Grigorenko & Grigorenko (2003)] I. Grigorenko & E. Grigorenko, "Chaotic dynamics of the fractional Lorenz system", *Physical review letters* **91**(3), 34–101.

[Huang & Cao (2006)] X. Huang & J. Cao, "Synchronization criterion for Lur'e systems by dynamic output feedback with time-delay", *International Journal of Bifurcation and Chaos* **16**(8), 2293–2307.

[Huang *et al.* (2012)] X. Huang, Z. Zhao, Z. Wang & Y. Li, "Chaos and hyperchaos in fractional order cellular neural networks", *Neurocomputing* **94**, 13–21.

[Jun-Guo (2005)] L. Jun-Guo, "Chaotic dynamics and synchronization of fractional-order Genesio–Tesi systems", *Chinese Physics* **14**(8), 1517.

[Kaplan & Glass (1995)] D. Kaplan & L. Glass, *Finite-difference equations: understanding nonlinear dynamics* **19**, Springer Science & Business Media, ISBN:978-1-4612-0823-5.

[Khalil (1993)] H. K. Khalil, *Nonlinear Systems*, Patience Hall, ISBN: 978-0130673893.

[Kiani *et al.* (2009)] B. A. Kiani, K. Fallahi, N. Pariz & H. Leung, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter", *Communications in Nonlinear Science and Numerical Simulation* **14**(3), 863–879.

[Kilbas *et al.* (2006)] A. Kilbas, H. Srivastava & J. Trujillo, *Theory and applications of fractional differential equations*, Elsevier, ISBN: 9780444518323.

[Kocarev (2001)] L. Kocarev, "Chaos-based cryptography: a brief overview", *IEEE Circuits and Systems Magazine* **1**(13), 6–21.

[Kulsoom *et al.* (2016)] A. Kulsoom, D. Xiao, A. Ur-Rehman & S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules", *Multimed. Tools Appl* **75**(1), 1–23.

[Kwon *et al.* (2011)] O. M. Kwon, J. H. Park & S. M. Lee, "Secure communication based on chaotic synchronization via interval time-varying delay feedback control", *Nonlinear Dynamics* **63**(1), 239–252.

[L'Hernault *et al.* (2008)] M. L'Hernault, J.-P. Barbot & A. Ouslimani, "Feasibility of analog realization of a Sliding-Mode Observer: Application to Data Transmission", *IEEE Transactions on Circuits and Systems I: Regular Papers* **55**(2), 614–624.

[Li & York (2004)] T. Y. Li & J. A. York, *Period Three Implies Chaos. In B. R. Hunt, T. Y. Li, J. A. Kennedy & H. E. Nusse, (eds), The Theory of Chaotic Attractors*, Springer, ISBN:978-1-4419-2330-1.

[Li *et al.* (2016)] S. Li, X. Zhou, X. Li & W. Jiang, "Asymptotical stability of Riemann–Liouville fractional nonlinear systems", *Nonlinear Dynamics* **86**(1), 65–71.

[Liang *et al.* (2015)] S. Liang, R. Wu & L. Chen, "Comparison principles and stability of nonlinear fractional order cellular neural networks with multiple time delays", *Neurocomputing* **168**, 618–625.

[Liao & Chen (2003)] X. Liao & G. Chen, "Chaos synchronization of general Lur'e systems via time-delay feedback control", *International Journal of Bifurcation and Chaos* **13**(1), 207–213.

[Lorenz (1963)] E. N. Lorenz, "Deterministic non periodic flow", *Journal of atmospheric sciences* **20**(2), 130–141.

[Mainieri & Rehacek (1999)] R. Mainieri & J. Rehacek, "Projective synchronization in three-dimensional chaotic systems", *Physical Review Letters* **82**(15), 3042-–3045.

[Matignon (1996)] D. Matignon, "Stability results for fractional differential equations with applications to control processing", *Proc. Computational Engineering in Systems and Application Multiconference*, pp. 963–968.

[Menezes *et al.* (1996)] A. J. Menezes, S. A. Vanstone & P. C. V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, ISBN: 0-8493-8523-7.

[Mittag-Leffler (1903)] G. M. Mittag-Leffler, "Sur la nouvelle fonction $E\alpha(x)$", *CR Acad. Sci* **137**(2), 554–558.

[Marino & Tomei (1995)] R. Marino & P. Tomei, *Nonlinear control design-–geometric, adaptive, robust*, Prentice-Hall, ISBN:978-0133426359.

[Odibat (2010)] Z. M. Odibat, "Adaptive feedback control and synchronization of non-identical chaotic fractional order systems", *Nonlinear Dynamics* **60**(4), 479–487.

[Pak & Huang (2017)] C. Pak & L. Huang, "A new color image encryption using combination of the 1D chaotic map", *Signal Processing* **138**, 129–137.

[Pecora & Carroll (1990)] L. M. Pecora & T. L. Carroll, "Synchronization in chaotic systems", *Physical review letters* **64**(8), 821–824.

[Petráš (2011)] I. Petráš, *Fractional-Order Nonlinear Systems Modeling, Analysis and Simulation*, Springer Science & Business Media, ISBN:978-3-642-18100-9.

[Podlubny (1998)] I. Podlubny, *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*, Academic Press, ISBN:0-12-558840-2.

[Polizzi (2013)] G. Polizzi, "Philosophical aspects of the work of Poincaré", *Lettera Matematica* **1**(1-2), 55–67.

[Qiang *et al.* (2013)] H. Qiang, L. Chong-Xin, S. Lei & Z. Da-Rui, "A fractional order hyperchaotic system derived from a Liu system and its circuit realization", *Chinese Physics B* **22**(2), 020502.

[Ravichandran *et al.* (2017)] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan & R. Amirtharajan, "DNA chaos blend to secure medical privacy", *IEEE transactions on nanobioscience* **16**(8), 850–858.

[Rehman & Liao (2019)] A. Ur-Rehman & X. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos DNA and SHA-2", *Multimedia Tools & Applications* **78**(2), 2105–2133.

[Rehman *et al.* (2018)] A. Ur-Rehman, X. Liao, R. Ashraf, S. Ullah, H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2", *Optik* **159**, 348–367.

[Rosenblum *et al.* (1996)] M. G. Rosenblum, A. S. Pikovsky & J. Kurths, "Phase synchronization of chaotic oscillators", *Physical review letters* **76**(11), 1804–1807.

[Rosenblum *et al.* (1997)] M. G. Rosenblum, A. S. Pikovsky & J. Kurths, "From Phase to Lag Synchronization in Coupled Chaotic Oscillators", *Physical review letters* **78**(22), 4193–4196.

[Scherer (2000)] C. W. Scherer, "An efficient solution to multi-objective control problems with LMI objectives", *Systems & control letters* **40**(1), 43–57.

[Sciamanna & Shore (2015)] M. Sciamanna & K. A. Shore, "Physics and applications of laser diode chaos", *Nature photonics* **9**(3), 151–162.

[Shannon (1948)] C. E. A. Shannon, "A mathematical theory of communication", *The Bell system technical journal* **27**(4), 379–423.

[Sklar (2001)] B. Sklar, *Digital Communications: Fundamentals and Applications*, Prentice Hall PTR, ISBN:978-0134724058.

[Smaoui *et al.* (2011)] N. Smaoui, A. Karouma & M. Zribi, "Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems", *Commun Nonlinear Sci Numer Simul* **16**(8), 3279–3293.

[Souaia *et al.* (2017)] M. A. Souaia, H. Trabelsi & K. B. Saad, "Synchronization of the Liu chaotic system and its application in secure communication", *Proc. International Conference on Control, Automation and Diagnosis*, pp. 434–438.

[Strogatz (1994)] S. H. Strogatz, *Dynamics and Chaos, with applications to physics, biology, chemistry, and engineering*, Nonlinear Perseus, ISBN:978-0738204536.

[Suykens & Vandewalle (1996)] J. A. K. Suykens & J. Vandewalle, "Master-slave synchronization of Lur'e systems", *International Journal of Bifurcation and Chaos* **7**(3), 665–669.

[Suykens *et al.* (1997)] J. A. K. Suykens, A. Huang & L. O. Chua, "A family of n-scroll attractors from a generalized Chua's circuit", *Int. J. Electron. Commun* **51**(3), 131–138.

[Tavazoei & Haeri (2007)] M. S. Tavazoei & M. Haeri, "A necessary condition for double scroll attractor existence in fractional order systems", *Physics Letters A* **367**(1-2),102–113.

[Tavazoei & Haeri (2008)] M. S. Tavazoei & M. Haeri, "Chaotic attractors in incommensurate fractional order systems", *Physica D: Nonlinear Phenomena* **237**(20), 2628–2637.

[Tenny *et al.* (2006)] R. Tenny, L. S. Tsimring, H. D. Abarbanel & L. E. Larson, *Security of Chaos-Based Communication and Encryption. In L. E. Larson, L. S. Tsimring & J. M. Liu, (eds), Digital Communications Using Chaos and Nonlinear Dynamics*, Springer, ISBN:978-0-387-29787-3.

[Wang & Bovik (2006)] Z. Wang & A. C. Bovik, *Modern Image Quality Assessment*, Morgan & Claypool, ISBN:9781598290233.

[Wang & Guan (2006)] Y. W. Wang & Z. H. Guan, "Generalized synchronization of continuous chaotic system", *Chaos Solitons & Fractals* **27**(1), 97–101.

[Wang & Song (2009)] X. Y. Wang & J. M. Song, "Synchronization of the fractional order hyperchaos Lorenz systems with activation feedback control", *Commun. Nonlinear Sci. Numer. Simul.* **14**(8), 3351–3357.

[Wang & Zhang (2015)] X. Wang & H. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos", *Optics Communications* **342**, 51–60.

[Wei *et al.* (2012)] X. Wei, L. Guo, Q. Zhang, J. Zhang & S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", *Journal of Systems and Software* **85**(2), 290–299.

[Weisstein (2002)] E. W. Weisstein, *CRC concise encyclopedia of mathematics*, Chapman & Hall/CRC press, ISBN:978-0849319464.

[Wiggins (2003)] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, Springer Nature, ISBN:978-0-387-00177-7.

[Wu *et al.* (2011)] Y. Wu, J. P. Noonan & S. Agaian, "NPCR and UACI randomness tests for image encryption", *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications* **1**(2), 31–38.

[Wu *et al.* (2013)] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan & P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness", *Information Sciences* **222**, 323–342.

[Wu *et al.* (2015)] X. Wu, H. Kan & J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps", *Applied Soft Computing* **37**, 24–39.

[Wu *et al.* (2015)] X. Wu, Y. Li & J. Kurths, "A new color image encryption scheme using cml and a fractional order chaotic system", *PloS one* **10**(3), e0119660.

[Yalçin *et al.* (2001)] M. E. Yalçin, J. A. K. Suykens & J. Vandewalle, "Master-slave synchronization of Lur'e systems with time-delay," *International Journal of Bifurcation and Chaos* **11**(6), 1707–1722.

[Yang *et al.* (1997)] T. Yang, C.W. Wu & L. O. Chua, "Cryptography based on chaotic systems", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **44**(5), 469–472.

[Yan (2016)] Y. Yan, "Synchronization for a class of uncertain fractional order chaotic systems with unknown parameters using a robust adaptive sliding mode controller", *Mathematical Problems in Engineering* **2016**, 220–226.

[Yang (2004)] T. Yang, "A survey of chaotic secure communication systems", *International Journal of Computational Cognition* **2**(2), 81–130.

[Yang *et al.* (2008)] X. Liang, J. Zhang & X. Xia, "Adaptive Synchronization for Generalized Lorenz Systems", *IEEE Transactions on Automatic Control* **53**(7), 1740–1746.

[Zhang *et al.* (2017)] L.M. Zhang, K.H. Sun, W.H. Liu & S. B. He, "A novel color image encryption scheme using fractional order hyperchaotic system and DNA sequence operations", *Chinese Physics B* **26**(10), 100504.

[Zhang *et al.* (2018)] H. Zhang, R. Ye, S. Liu, J. Cao, A. Alsaedi & X. Li, "LMI-based approach to stability analysis for fractional order neural networks with discrete and distributed delays", *International Journal of Systems Science* **49**(3), 537–545.

[Zhang *et al.* (2019)] W. Zhang, J. Cao, R. Wu, F. E. Alsaedi & A. Alsaedi, "Lag projective synchronization of fractional-order delayed chaotic systems", *Journal of the Franklin Institute* **356**(3), 1522–1534.

[Zhen *et al.* (2014)] P. Zhen, G. Zhao, L. Min, & X. Li, "A survey of chaos-based cryptography", *Proc. 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 237–244.

[Zhou & Kuang (2010)] P. Zhou & F. Kuang, "Synchronization between fractional-order chaotic system and chaotic system of integer orders", *Acta Physica Sinica* (**59**(10), 6851–6858.

[Zhou *et al.* (2015)] Y. Zhou, C. Ionescu & J. A. Tenreiro-Machado, "Fractional dynamics and its applications", *Nonlinear Dynamics* **80**(4), 1661–1664.

[Zhou *et al.* (2016)] N. Zhou, S. Pan, S. Cheng & Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing", *Optics & Laser Technology* **82**, 121–133.

[Zhou *et al.* (2021)] L. Zhou, F. Tan, X. Li & L. Zhou, "A fixed-time synchronization-based secure communication scheme for two-layer hybrid coupled networks", *Neurocomputing* **433**, 131–141.

[Zhu *et al.* (2009)] H. Zhu, S. Zhou & J. Zhang, "Chaos and synchronization of the fractional order Chua's system", *Chaos, Solitons & Fractals* **39**(4), 1595–1603.

ملخص: شهدت بداية القرن الواحد و العشرين تطور هائل و سريع لتكنولوجيات الاتصال و الوسائط المتعددة، حيث أصبح من الممكن نقل المعلومات الرقمية بأشكال مختلفة، و بالإمكان تبادل المعلومات و حتى القيام بعمليات تداول تجارية عبر الإنترنيت بكل سهولة و يسر. و بقدر ايجابيات الإنترنيت في حياتنا اليومية غير ان لها مساوئ تنطوي ايضا على مخاطر منها: سرقة المعلومات و قرصنتها خاصة تلك المرتبطة بقطاعات حساسة و جد استراتيجية مثل القرارات السياسية، المعلومات المتعلقة بالأمن القومي، الإستقرار الاجتماعي و النظام التجاري والتي من الممكن استعمالها بشكل غير قانوني. و لان الانظمة الفوضوية المنظمة تتميز بخاصية العشوائية و عدم القدرة على التنبؤ بالإضافة الي الحساسية المفرطة للشروط الأولية هدا الأمر يجعلها مثالية لتشفير البيانات و حمايتها. و من خلال هده الأطروحة تم التركيز على هدفين رئيسيين يتمثل الأول في تصميم أنظمة التزامن الفوضوي المنظم و الكسري جديدة. تطوير انظمة تشفير و إتصال جديدة ترتكز على الفوضى المنظمة هو الهدف الثاني لهده الرسالة.

كلمات مفتاحية: التشفير، أنظمة الاتصال، التزامن، الفوضى المنظمة، الحساب الكسري.

Abstract: With the rapid development of network technology and multimedia, digital information can be transported in different form conveniently. People can exchange information and trade online easily. The internet does not just bring convenience to people's lives but also involves risks. Some sensitive information can be stolen and even distributed illegally. It is linked to political, diplomatic and military life, economic, social and commercial security. Since chaos has good cryptography properties such as randomness, aperiodicity, extremely sensitive to initial conditions and parameters, forcing the robustness of data cryptography. This thesis revolves around two main objectives. The first is to design chaotic and fractional order synchronization systems. The development of new chaos based cryptography and transmission schemes is the second objective of this thesis.

Key words: Cryptography, transmission, synchronization, chaotic, fractional order calculus.

Résumé: Avec le développement rapide de la technologie de réseau et de multimédia, l'information numérique peut être transportée sous différentes formes commodément. Les gens peuvent échanger des informations et commercer en ligne facilement. Internet n'apporte pas seulement de la commodité à la vie des gens mais comporte aussi des risques. Certaines informations sensibles peuvent être volées et même diffusées illégalement. Il est lié à la vie politique, diplomatique, militaire, sécurité économique, sociale et commerciale. Puisque le chaos possède de très bonnes propriétés pour la cryptographie comme l'aléatoire, l'apériodicité, sensibilité aux conditions et paramètres initiaux, forçant la robustesse de la cryptographie de données. Cette thèse s'articule autour de deux objectifs principaux. Le premier consiste à concevoir des systèmes de synchronisation chaotique et d'ordre fractionnaire. le développement de nouveaux schémas de cryptographie et de transmission basée sur le chaos est le deuxième objectif de cette thèse.

Mots clés: Cryptographie, transmission, synchronisation, chaotique, calcul d'ordre fractionnaire.