CHAOS SYNCHRONIZATION AND CRYPTOGRAPHY FOR SECURE COMMUNICATIONS

FATIN NABILA BINTI ABD LATIFF

Universiti Malaya

FACULTY OF SCIENCE
UNIVERSITI MALAYA
KUALA LUMPUR

2021

CHAOS SYNCHRONIZATION AND CRYPTOGRAPHY FOR SECURE COMMUNICATIONS

FATIN NABILA BINTI ABD LATIFF

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

INSTITUTE OF MATHEMATICAL SCIENCES
FACULTY OF SCIENCE
UNIVERSITI MALAYA
KUALA LUMPUR

2021

Universiti Malaya

UNIVERSITI MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **FATIN NABILA BINTI ABD LATIFF**

Registration/Matric No.: **SHB160011 / 17019864/4**

Name of Degree: **DOCTOR OF PHILOSOPHY**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

CHAOS SYNCHRONIZATION AND CRYPTOGRAPHY FOR SECURE COMMUNICATIONS

Field of Study: **APPLIED MATHEMATICS, CRYPTOGRAPHY**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 25/7/2021

Subscribed and solemnly declared before,

Witness's Signature Date: 25/7/2021

Name:
Designation:

University of Malaya

CHAOS SYNCHRONIZATION AND CRYPTOGRAPHY FOR SECURE COMMUNICATIONS

ABSTRACT

Many Chaos-Based Cryptographic (CBC) methods, such as chaos-based secure communication, and chaos-based block/stream cipher, have been studied over the past decade. To the best of our knowledge, CBC is a new field of research in two areas, such as cryptography (computer and data security) and chaos (nonlinear dynamic system). For high security, encryption is one of the methods used to protect data against leakage. CBC describes chaos theory as a measure of communication techniques and computational algorithms to perform different cryptographic tasks in a cryptographic system in specific physical dynamic systems operating in chaotic systems. Chaos is an exciting phenomenon in various fields, such as physics, psychology, and biology in some systems. The theory of chaos provides the means to explain the phenomenon of chaos, control chaotic dynamic systems, and use the properties of chaos. In particular, the characteristics of chaos, such as robustness, merging property, sensitivity to initial conditions/parameter mismatches, the complexity of the structure and stochastic dynamics, which maps nicely with cryptographic requirements such as confusion, diffusion, complexity of the algorithm and deterministic pseudo-randomness, have been shown to be appropriate for the design of data protection means.

Besides, the probability of chaotic synchronization, where the Master System (MS) (transmitter) drives the Slave System (SS)(receiver) via its output signal, has made it likely that chaotic systems could be used to enforce protection in communication systems. Many techniques, such as chaotic shift key and Chaos Masking (CM), were suggested, but many attack methods later showed them insecurity. There are also different modifications to these

Universiti Malaya

methods in the literature to improve safety, but almost all suffer from the same disadvantage. The implementation of chaotic security systems, therefore, remains a challenge. This work introduces a Fractional-Order (FO), such as Fractional-Order Newton-Leipnik System (FONLS) and Fractional-Order Neural Networks (FONNs), which could improve the security of existing methods. The complexity of FO systems is due to the inclusion and derivation of non-integer orders being addressed. If these two chaotic signals of equal power are combined and then used to transmit message signals, it may be difficult for intruders to use conventional attack methods because the chaotic carrier signal has added complexity. Based on this, we analyzed various initial conditions within the same parameters and found the best FO minimum value of FONLS.

In this thesis, the second part of chaos-based secure communication is introducing a new encryption algorithm to improve the security of modern chaos-based communication systems. For secure communication that is reliable, secure, and has good performance, the focus is on developing Double Encryption System (DES). The combination of synchronization of chaos and symmetric encryption is called DES. In this thesis, theoretically and numerically, FONNs is formulated with multiple time delays and the stability of the chaotic systems and their safety are analyzed.

Keywords: Chaos synchronization, Cryptography, Symmetric encryption, Fractional-order, Secure communication.

Universiti Malaya

PENYEGERAKAN DAN KRIPTOGRAFI CHAOS UNTUK KOMUNIKASI SELAMAT

ABSTRAK

Banyak kaedah kaedah CBC, seperti komunikasi selamat berasaskan kaos, dan penyekat blok / aliran berasaskan kaos, telah dikaji selama satu dekad yang lalu. Sepengetahuan kami, CBC adalah bidang penyelidikan baru dalam dua bidang, seperti kriptografi (keselamatan komputer dan data) dan kaos (sistem dinamik bukan linier). Untuk keselamatan yang tinggi, enkripsi adalah salah satu kaedah yang digunakan untuk melindungi data daripada kebocoran. CBC menerangkan teori kaos sebagai ukuran teknik komunikasi dan algoritma komputasi untuk melakukan tugas kriptografi yang berbeza dalam sistem kriptografi dalam sistem dinamik fizikal tertentu yang beroperasi dalam sistem Kaos. Kaos adalah fenomena menarik dalam pelbagai bidang, seperti fizik, psikologi, dan biologi, dalam beberapa sistem. Teori kaos menyediakan cara untuk menjelaskan fenomena kaos, mengawal sistem dinamik kaos, dan menggunakan sifat-sifat kaos. Terutama, ciri-ciri kaos, seperti ergodisiti, penggabungan harta benda, kepekaan terhadap keadaan awal/ketidakcocokan parameter, kerumitan struktur dan dinamik stokastik, yang memetakan dengan baik dengan keperluan kriptografi seperti kekeliruan, penyebaran, kerumitan algoritma dan pseudo-randomness deterministik, telah terbukti sesuai untuk reka bentuk kaedah perlindungan data.

Selain itu, kebarangkalian kaos pensingkronian, di mana MS (pemancar) menggerakkan SS (penerima) melalui isyarat keluarannya, telah memungkinkan bahawa sistem kaos dapat digunakan untuk menegakkan perlindungan dalam sistem komunikasi. Banyak teknik, seperti shift yang kaos dan CM, dicadangkan, tetapi banyak kaedah serangan kemudian menunjukkan mereka tidak selamat. Terdapat juga modifikasi yang berbeza untuk kaedah ini dalam literatur untuk meningkatkan keselamatan, tetapi hampir semua

Universiti Malaya

mengalami kekurangan yang sama. Oleh itu, pelaksanaan sistem keselamatan yang kaos tetap menjadi cabaran. Karya ini memperkenalkan FO, seperti FONLS dan FONNs, yang dapat meningkatkan keselamatan kaedah yang ada. Kerumitan sistem FO disebabkan oleh pecahan tertib bukan nomber bulat yang ditangani. Sekiranya kedua-dua isyarat kaos dengan kekuatan yang sama digabungkan dan kemudian digunakan untuk menghantar isyarat mesej, mungkin sukar bagi penceroboh untuk menggunakan kaedah serangan konvensional kerana isyarat pembawa kaos telah menambahkan kerumitan. Berdasarkan ini, kami menganalisis pelbagai keadaan awal dalam parameter yang sama dan mendapati nilai minimum FO terbaik untuk FONLS.

Dalam tesis ini, bahagian kedua komunikasi selamat berasaskan kaos adalah memperkenalkan algoritma enkripsi baru untuk meningkatkan keselamatan sistem komunikasi berasaskan kaos moden. Untuk komunikasi selamat yang boleh dipercayai, aman, dan mempunyai prestasi yang baik, fokusnya adalah untuk mengembangkan DES. Gabungan kaos pensingkronian dan enkripsi simetri disebut DES. Dalam tesis ini, secara teoritis dan numerik, FONNs dirumuskan dengan dengan beberapa kelewatan masa dan kestabilan sistem kaos dan keselamatannya dianalisis.

Kata kunci: Kaos pensingkronian, kriptografi, kriptografi simetri, pecahan tertib, komunikasi selamat.

Universiti Malaya

ACKNOWLEDGEMENTS

First of all, Alhamdulillah, Praise to Allah for His Blessings in granting me to complete this studies. I would like to express my greatest gratitude to my supervisor Assoc. Prof. Dr. Wan Ainun Mior Othman for her precious guidance, encouragement and patience during my studies. Her precious ideas and advices were the great practical throughout the writing of this thesis. To Dr. Kumaresan Nallasamy, thanks for your guidance as my supervisor before leaving University of Malaya.

My deepest gratitude and appreciation to my father, Mr. Abd Latiff Alus and my mother, Mrs. Norita Osman for their endless love, prayers, patience, and encouragement. To my parents for all their love and inspiration in all that I do, and without their help, none of my accomplishments would be possible. I deeply thank my dear brothers Faris Najwan and Faris Naufal for their love and support. And finally, to Meow, a loyal friend who has always supported me.

My profound thanks to University of Malaya Faculty Research Grant (GPF, Project No.: GPF033B-2018) and Impact Oriented Interdisciplinary Research Grant (IIRG, Project No.: IIRG001C-2019), for their financial support to work as graduate research assistant (GRA).

I also would like to send my special thanks to all my friends for your supports and contribution of ideas in this studies.

Fatin Nabila Abd Latiff

January 2021

Universiti Malaya

TABLE OF CONTENTS

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

LIST OF FIGURES

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

Universiti Malaya

LIST OF TABLES

Universiti Malaya

LIST OF SYMBOLS AND ABBREVIATIONS

ACC : Active Control.

CapD : Caputo Derivativel.

CapFD : Caputo Fractional Derivative.

CBC : Chaos-Based Cryptographic.

CM : Chaos Masking.

DASS : Delayed Active Sliding Surface.

DES : Double Encryption System.

EDS : Error Dynamical System.

FLDM : Factional-Order Lyapunov Direct Method.

FO : Fractional-Order.

FONLS : Fractional-Order Newton-Leipnik System.

FONNs : Fractional-Order Neural Networks.

IO : Integer-Order.

IONNs : Integer-Order Neural Networks.

LDM : Lyapunov Direct Method.

LTF : Laplace Transformation.

MS : Master System.

MSSYS : Master-Slave System.

NLS : Newton-Leipnik System.

NNs : Neural Networks.

ODE : Ordinary Differential Equation.

PC : Pecora and Carroll.

PFONNs : Projective Fractional-Order Neural Networks.

RLFD : Riemann-Liouville Fractional Derivative.

Universiti Malaya

SMC : SLIDING MODE CONTROL.

SS : Slave System.

SWS : Switching Surface.

Universiti Malaya

LIST OF APPENDICES

Universiti Malaya

CHAPTER 1: INTRODUCTION

This chapter introduced some prior knowledge about chaos theory, synchronization and cryptography. The primary purpose was to show a close relationship between chaos theory and cryptography for secure communication. We also show how the appropriate combination of chaos theory and synchronization can lead to innovative chaos-based cryptography, that ensures a high level of communication security.

1.1 Chaos and Synchronization

In this section, the significant theories of chaos are described. It is concentrating on the characteristics that tend to be essential for its cryptographic implementation. The presentation indeed begins with the fundamental notion of chaotic systems and will guide to efficient implementation through non-linear dynamic systems. Therefore, this part will describe the significance of the relationship within chaos systems in cryptographic applications.

1.1.1 Chaos Theory

Chaos is the complex periodic time-evolution of a deterministic nonlinear system. With reference to chaos theory, it is the study of behavior of dynamical systems that are very sensitive to initial conditions. Chaos theory is a relatively new discipline, with boundless applications in all areas of science and technology. Started originally as field of study in mathematics (Kloeden & Mees, 1985; Ruelle, 2006; Sharkovskiĭ, 1995), chaos theory has also been encountered in a wide variety of fields including mechanics (Poole & Safko, 2001), biology (Mackey & Glass, 1977; Skinner, 1994), chemistry (Epstein, 1983; Kuramoto, 2003), electronics (Chua et al., 1993; Matsumoto, 1987), and optics (Gibbs et al., 1981; Ikeda & Matsumoto, 1987).

Universiti Malaya

Since these dynamic systems are based on deterministic models, their high sensitivity to initial conditions or control parameters makes them unpredictable for their solutions (E. N. Lorenz, 1995). In many natural phenomena, such as weather and astronomy (Hénon, 1976; Kolmogorov, 1941), the chaotic behaviour of such systems can be observed. In fact, Henry Poincare's early discovery of chaotic systems goes back to the 1880s in his attempt to demonstrate the solar system's stability through his work on the restricted three-body problem (Poincaré, 1890). Edward Lorenz's subsequent work in weather prediction in 1961 also contributed to the chaos theory (E. N. Lorenz, 1963).

The unpredictability caused by the extreme sensitivity to initial conditions and control parameters, otherwise known to the world as the 'butterfly-effect' (E. N. Lorenz, 1963), is one of the essential elements in chaotic dynamical systems. This idea means that even insignificant modifications in initial conditions or control parameters will result in dramatically different outputs with a nonlinear chaotic system. As time elapses, this allows the evolution of the nonlinear chaotic system completely 'unpredictable' (E. N. Lorenz, 1963; H.-W. Lorenz, 1993).

The ability to synchronise with each other under certain conditions is another crucial and relevant characteristic of chaotic systems. Since it is impossible to predict the long-term behaviour of chaotic dynamical systems, such a synchronization appears impossible. However, it has been shown that under some circumstances, two or more chaotic dynamic systems may undergo identical motion, which is coupled together and develop from different initial conditions (Pecora & Carroll, 1990, 1991).

The field of cryptography is one of the important applications of chaos. Cryptography deals with methods to secure the transmission of messages between two parties through the encryption of those messages. The close relationship between chaos and cryptography has been emphasised by several researchers, (Alvarez et al., 1999; Fridrich, 1998; Gotz et al.,

Universiti Malaya

1997; Kocarev et al., 1998). Even more remarkably, as Shannon pointed out in his classical paper: "Communication Theory of Secrecy Systems", (Shannon, 1949), the concept of using chaotic systems in cryptography predated the popularisation of the term "chaos", that successful mixing transformations in good secrecy systems are done by simple operations that are the centre of chaotic maps (Shujun, 2003). He originally invented two new terms in the same paper, which are considered the most basic principles of cryptographic algorithms: "confusion" and "diffusion". The combination of property and sensitive to initial conditions of chaos generators are mapped to the diffusion and confusion of cryptosystems. The tight relation between cryptography and chaos, consequently, resulted in another area of research known as chaotic cryptography and a great deal of work has been published (Antonik et al., 2018; Beth et al., 1994; Hasimoto-Beltrán, 2008; Kocarev, 2001; Matthews, 1989; Teh et al., 2020).

1.1.2 Chaotic Systems

When the state changes with time, the system is called a dynamic system or an oscillator. The system is called continuous systems; if the time is continuous, then the system's evolution is described mathematically by an Ordinary Differential Equation (ODE) and a set of initial conditions. One example of chaotic systems that researchers have studied a lot is the Lorenz system. The nonlinear differential equations of these systems are presented as:

$$\begin{aligned} \frac{dx}{dt} &= a(x_1(t) - x_2(t)) \\ \frac{dy}{dt} &= bx_1(t) - x_2(t) - x_1(t)x_3(t) \\ \frac{dz}{dt} &= x_1(t)x_2(t) - cx_3(t) \end{aligned} \tag{1.1}$$

Where the parameters $a = 10$, $b = 28$ and $c = \frac{8}{3}$ are given. There are two nonlinearities responsible for the chaotic behaviour of Lorenz's equations : the first one is the products

Universiti Malaya

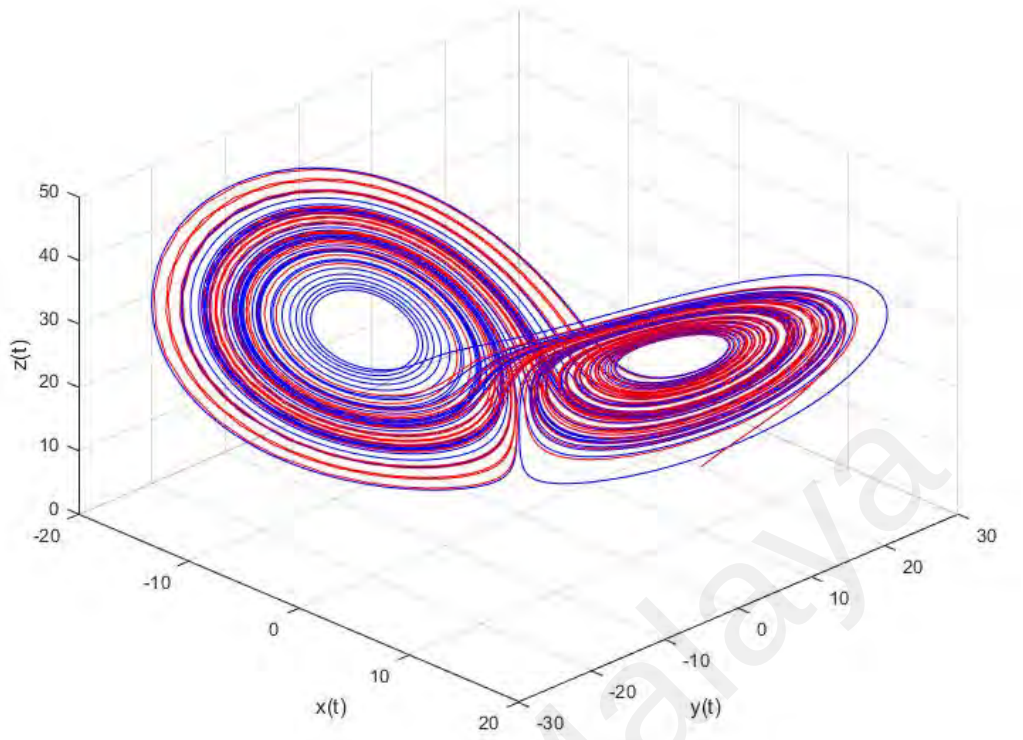


Figure 1.1: Lorenz's attractor.

$x_1(t)x_3(t)$ and another one is also the product $x_1(t)x_2(t)$ that are performed by two multipliers (E. N. Lorenz, 1963). The Lorenz's equations are simulated using the MATLAB and the characteristic of the Lorenz equations (1.1) that is called "butterfly wings" is shown in Figure 1.1.

1.1.3 Chaos Synchronization

The hallmark of chaos is its extreme sensitivity to perturbations. Two chaotic systems converge gradually in time, starting from very close initial conditions, contributing to drastically different trajectories. It was long thought that the synchronization of chaotic systems was counterintuitive or impractical, mainly because of the sensitivity to initial conditions that prevented the display of perfectly correlated time evolutions by two identical chaotic systems. However, thanks to pioneering work in 1983, the significance of chaos for applications changed massively, (V. Afraimovich et al., 1986; Fujisaka & Yamada,

Universiti Malaya

1983). Throughout this context, with their pioneering studies on chaos synchronization, the suggestion that two coupled chaotic systems can be synchronized came as a surprise to the nonlinear dynamics community and made it possible.

Followed by Pecora and Caroll's work, they succeeded in synchronizing two chaotic systems (Pecora & Carroll, 1990). The first implementation of chaos-based communications is demonstrated on the electronic circuits was demonstrated three years later by (Cuomo & Oppenheim, 1993). This proof clearly laid the groundwork for chaos-based communications. Until now, numerous forms of synchronization in chaotic systems have been acknowledged, leading to the development of encoding the message in any available mathematical method. Here, two systems are said to be coupled if they exchange partial information about their respective dynamical states. The phenomenon of synchronization of nonlinear oscillators is pervasive in nature and science.

Different forms of chaos synchronization exist, namely generalized synchronization (E. Afraimovich & Smirnov, 1987), complete synchronization (Pecora & Carroll, 1990; Zhan et al., 2003), partial synchronization (Maistrenko et al., 2000) and phase synchronization (Rosenblum et al., 1997) have been devoloped. After having reported many applications, particularly in mechanical systems (Blekhman et al., 1995), in control theory (Pogromsky & Nijmeijer, 2001) and telecommunications (Abel & Schwarz, 2002), this groundbreaking research has increased the interest in synchronization. Synchronization is an essential concept in chaos-based systems as well. The basic idea of secure chaos-based communication is to utilize a chaotic system's inherent complexity and provide security by making the transmitted message unrecognizable to possible eavesdroppers.

1.2 Cryptography

Cryptography is an art or science in which messages are hidden from the public. The message will be called plaintext or cleartext in cryptographic terminology. It is called

Universiti Malaya

encryption to encode the message content, which conceals its secret message from the public. The message that has been encrypted is called ciphertext. The process by which plaintext can be recovered from ciphertext is called decryption. Encryption and decryption occasionally the coding algorithm that uses a key and is such that decryption can be conducted only by knowing the exact key.

1.2.1 Cryptographical System

An operation of encryption and decryption technique is referred to as a cryptosystem. Some cryptographic methods rely on the algorithms' secrecy; these algorithms are mostly of historical interest and are not sufficient for actual requirements. All modern algorithms use a key; a message can only be decrypted when the key resembles the key's encryption. For decryption, the key used can be different from the key used for encryption, but they are the same for most algorithms. Key-based algorithms are available in two classes; asymmetric or public-key and symmetric or secret keys. The difference between the two is that symmetric encryption uses the same encryption's key and decryption's key, whereas asymmetric cryptographic algorithms uses different encryption's key and decryption's keys.

Suppose that a message is transmitted via a public channel, such as the Internet, from the transmitter to another receiver. For the transmission of a message to occur, the two parties, who are the sender and recipient, must collaborate. When it is desirable or appropriate to secure the message transmission from an attacker who may cause harmful effects to confidentiality or authenticity, security considerations come into play. There are various method can be used to secure the message, including the encryption or encryption-like transformation of the message, the most common approach used in the implementation. This methodology is used to protect from defensive and offensive deception. It refers to an essential discipline, called cryptography, which is defined as the science and art of

Universiti Malaya

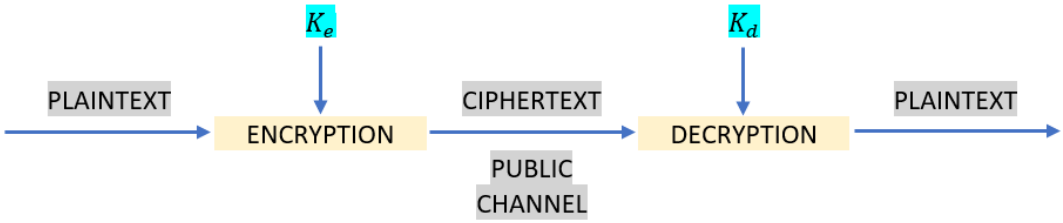


Figure 1.2: General cryptosystem

converting a legible message.

Figure 1.2 is an example of the most general form of a cryptosystem. Plaintext is denoted by P and ciphertext is denoted C, respectively. We may define the encryption procedure as $C = E_{k_s}(P)$, where the encryption key is K_e and the encryption function is $E(.)$. Similarly, the decryption procedure is $P = D_{K_d}(C)$, where the decryption key is K_d and the decryption function is $D(.)$.

1.2.2 Connection Between Chaos and Cryptography

The characteristic properties of chaos meet it effectively with cryptographic characteristics of uncertainty and propagation (Shannon, 1949). The elements in the chaotic attractor are given by periodic circles that produce similar statistical arrangements. Substitution-like procedures may use these arrangements to cover simple messages.

Then again, propagation is almost related to the capacity of chaotic processes to influence initial conditions and control parameters. Diffusion produces plenty of slide's impact, where a straightforward analysis in the cryptosystem's contribution gives a fully recognizable output. Meanwhile, a slight change to its initial conditions or control parameters, a chaotic system produces this behaviour. The use of these variables will generate the same slide effect as a contribution to the cryptosystem calculation. The similarity between the theory of dynamical systems and cryptography is easily illustrated

Universiti Malaya

Table 1.1: Analogy between chaos and cryptography properties

Chaos property	Cryptography property
System parameters	Key
Ergodicity	Confusion
Initial state	Plaintext
Final state	Ciphertext
Structure complexity	Algorithm complexity
Sensitivity to parameter/ initial conditions	Diffusion with a slight change in the secret key/plaintext
Mixing property	Diffusion with a small change in whole plaintext
Chaotic system: - infinite number of state -nonlinear transformation - infinite number of iterations	Pseudo-chaotic system: - finite number of state - nonlinear transformation - finite number of iterations

by Table 1.1. At the same time, the comparison between the two was made very clear in the review paper (Alvarez & Li, 2006):

- Periodicity, auto-similarity and mixing property in chaotic compare with the confusion in cryptography where the output of the system seems similar for any input.
- Sensitivity to control parameters and introductory conditions in chaotic relate to.
- Diffusion in cryptography where a very different output is generated by a slight difference in the input.
- Deterministic chaotic properties refer to deterministic pseudo-randomness, where pseudo-randomness is generated by a deterministic process.
- Chaotic complexity relates to the algorithmic complexity of cryptography, where extremely complex outputs are generated by a simple algorithm.

Universiti Malaya

1.3 Chaos Synchronization and Cryptography in Secure Communication

In recent years, a part of the scientific community has gained significant interest in the analysis of chaotic systems and their potential applications to cryptography. It is a contribution to future software cryptography in the transmission of real high-speed data. Three important features are needed for CBC in the communication architecture: (I) two identical chaotic systems, that is called MSSYS, (ii) the ability to synchronise MSSYS, and (iii) the process of encryption/decryption to protect and retrieve the message. The primary concept that makes CBC attractive is that chaotic signals have features required in cryptography. (Alvarez & Li, 2006; Takens, 1988).

In the Shanon paper on cryptography (Shannon, 1949), the close relationship between cryptography and chaos is given, and (Alvarez & Li, 2006) provides a more complex relationship between chaos and cryptography. Various methods exist in cryptography to explain the embedding of the message. CM, chaos-shift keying and chaos modulation are the most common ones. The message is added to the chaotic generator's output at the transmitter with chaotic masking (Kocarev et al., 1992). To secure the message at the receptor, one has to achieve synchronization, and the message signal is usually 20 to 30 dB weaker than the chaotic signal (Dedieu et al., 1993). The chaotic signal is subtracted by the receiver to recover the message. Several attacks have been built on this cryptosystem, making CM unsafe (Alvarez et al., 2005). Another cryptography method used for secure communication is symmetric encryption that yields new encryption algorithms called double encryption.

1.3.1 Chaos Masking

After demonstrating that the chaotic system has a synchronization property, this property can now discuss the masking technique when sending secret messages. Different methods have been suggested for the transmission of information signals using chaotic dynamics.

Universiti Malaya

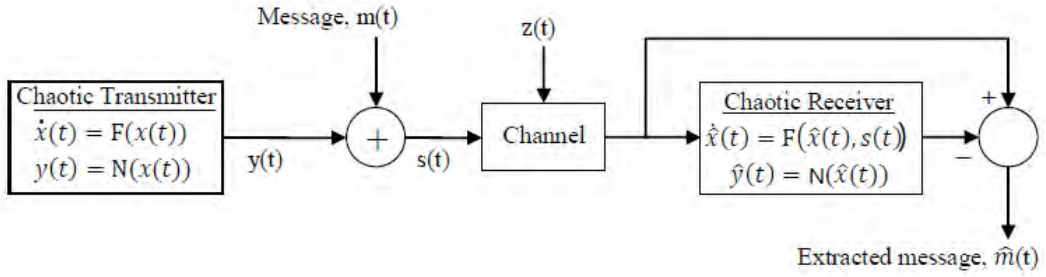


Figure 1.3: Chaotic communication scheme based on chaotic masking

The most used method for encoding a message is CM. The message is mixed after it leaves the circuit of the transmitter with the chaotic carrier. Thus, the message in the transmitter does not lead to the generation of the carrier. It is possible to do the masking in many ways, including adding the message to the chaotic carrier or modulating the chaotic carrier amplitude (Mirasso et al., 1996; Sanchez-Diaz et al., 1999). The amplitude of the message must be small enough in these schemes to allow high-quality synchronization and to conceal it.

This is among the earlier methods of using chaotic signals as defined in (Kocarev et al., 1992; Morgül & Feki, 1999) for the transmission of a message signal and is illustrated in Figure 1.3. In this CM scheme, a signal message is added to a chaotic system on the transmitter side before delivery. A chaotic synchronization is performed simultaneous, accepting the signal on the receiver team. The chaotic part is deducted from the received signal, thereby restoring the $m(t)$ original message signal. The transmitter is indicated by the following representation of state space as given by:

$$\begin{aligned} \dot{x} &= F(x(t)) \\ y(t) &= N(x(t)) \end{aligned} \tag{1.2}$$

The output signal $y(t)$, which is the transmitter state function $x(t)$, is added to $m(t)$ to

Universiti Malaya

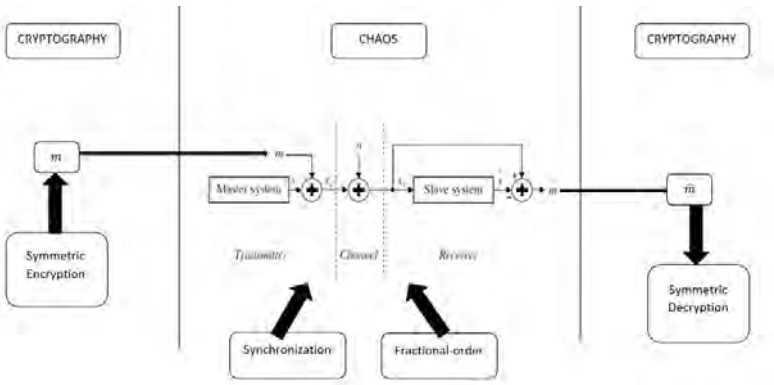


Figure 1.4: General Double Encryption

form the $s(t)$ transmitted signal given as follows:

$$s(t) = y(t) + m(t). \tag{1.3}$$

The general method of choosing $y(t)$ is to prefer one $x(t)$ parts. Nevertheless, in the general problem $N(x(t))$ can be any function of $x(t)$ as long as chaotic synchronization is possible at the receiver, by selecting the product signal. The receiver, which is run by $s(t)$, is defined by the state-space expression as follows:

$$\begin{aligned} \dot{\hat{x}} &= F(\hat{x}(t), s(t)) \\ y(t) &= N(x(t)) \end{aligned} \tag{1.4}$$

1.3.2 Double Encryption

Double encrption or multiple encryption is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm to increase the complexity of the cryptosystem, thereby providing greater security. Symmetric algorithm and the public key are first employed to encrypt the original message to produce the ciphertext, and the ciphertext is re-encrypted by using chaotic synchronization to achieve double encryption. This methodology is illustrated in Figure 1.4

Universiti Malaya

1.3.3 Security in Chaos-based Communications

The encryption efficiency of chaos-based communication systems relies on two key points: the carrier signal's unpredictability and the sensitivity of the synchronization to the parameter mismatch. Consequently, device cryptosystems' security is most likely the main weakness, as it involves many aspects. The insufficiency of only one can permanently disrupt the viability of the system. One of the strong requirements that any chaotic cryptosystem should meet is the efficient masking of the message within the chaotic carrier (Jacobo et al., 2010). This condition is generally fulfilled when a small amplitude message is protected within much greater chaotic perturbations with a large amplitude. Second, the system should be able to hide parameters that serve as physical keys for decryption. Third, the chaotic carrier should be complex enough to avoid its reconstruction using simple techniques such as return maps. For instance, some communication schemes using low-dimensional chaotic signals can be unmasked because of their narrow spectra. They can be reconstructed from the time series (Kulkarni & Amritkar, 2001; Short, 1994, 1996, 1997) or from the appropriate return maps (Pérez & Cerdeira, 1995; T. Yang et al., 1998; Zhou & Chen, 1997). Fourth, the space dimension parameter should be large enough to avoid being shattered by brute-force-attack or similar techniques.

Other exciting recommendations methods to quantify the cryptanalysis of chaotic encryption schemes and achieve a reasonable degree of security has been suggested in (Alvarez & Li, 2006; Tenny & Tsimring, 2004) . In our thesis, the CBC method will be introduced later, in Chapters 4 and 6.

1.4 Research Questions

Works of literature available on Integer-Order (IO) of chaos systems are abundant. On the other hand, the combination of IO and FO of chaos systems are still hardly available. Hence, such an investigation will be addressed in the present study as the following:

Universiti Malaya

1. How to find the minimum order of fractional-order with a different value of initial condition of a chaotic system in order for synchronization of chaotic systems occurs and combined with the cryptography for secure communication?.
2. How to find the best value of FO chaotic Neural Networks (NNs) that can provide synchronization with the IO chaotic NNs?.
3. How to perform DES that consists of chaotic NNs and symmetrical algorithms?.

These unattended issues are the concentrates and aim to accomplish in this study, and numerical simulations are performed to validate our finding.

1.5 Research Objectives

The main objective of this thesis is to investigate and study the application of chaos synchronization and cryptography. Eventually, a new algorithm is proposed along with the implementation of a chaos-based encryption system. The significant contributions to this thesis include:

1. To study the implementation of the chaos synchronization is being applied to cryptography with the specific chaotic interval which is $-2 < x, y, z < 1$.
2. To perform theoretical and numerical simulations of chaotic systems.
3. To observe the behavior of synchronization of IO chaotic NNs and FO chaotic NNs.
4. To develop an algorithm for encryption and decryption in chaos cryptography for secure communications.

1.6 Research Methodology

This research work must be carried on primarily by the succeeding steps:

1. Literature Review:

   A brief literature review is carried out under the following subtopics: chaos

Universiti Malaya

synchronization, cryptography, time delays and FO.

2. Problem formulation

   From the intensive review of the literature review, we formulate some problems based on our research study's previous research.

3. Defining the research objective

   Based on the problem mentioned above, we can answer the problems based on the research objective.

4. Proposed new cryptographic algorithm:

   The proposed method is used to construct a chaotic communication system consists of a transmitter MS and a receiver SS. The input message is masked to the chaotic system, then transmitted from the transmitter to the receiver. The results will show that the synchronization between the transmitter and the receiver can be achieved and the input message can be recovered entirely on the receiver side.

5. Numerical simulations and MATLAB:

   Chaotic systems cannot be solved analytically, and therefore the primary method of understanding them is through numerical calculations. We use MATLAB to run numerical simulations of chaos systems in order to study their system behaviour. Moreover, write multiple copies of the code's system and examine the errors in systems.

1.7 Scope of Research

The scope of this study is listed below:

1. The study explores the performance, behaviour, and mathematical representation of fractional-order chaos system between $0.95 \leq \alpha \leq 1$.
2. The study time-delay chaotic systems of NNs, which are a series of algorithms that

Universiti Malaya

mimic a human brain's operations to recognize relationships between vast amounts of data.

3. The study presents a design methodology to obtain double encryption systems for NNs based secure communications in multiple time-delay chaotic systems. Chaotic synchronization is combined with a symmetric algorithm to increase the cryptosystem's complexity, thereby providing greater security.

1.8 Thesis Outline

The organization of this thesis is as follows:

Chapter 1 briefly introduces the concept of chaos theory, chaos synchronization, cryptography and CBC. The research questions, research objectives, research methodology and scope for this research are also identified.

In **Chapter 2**, we discuss the current literature work on various problem analyses of different type of chaotic system based on our research problems.

In **Chapter 3**, we introduce the methodology used in this thesis, such as Lyapunov exponents and Laplace Transformation (LTF). Synchronization technique and time delay are also highlights, which appears in many areas of engineering and sciences. Such systems have achieved great success in developing secure chaos-based communications because of the large dimension of their attractor and strong entropy (apparent randomness).

Chapter 4 introduces the FO to increase the complexity of the transmitted chaos systems that will be used to masked the signal message called as Newton-Leipnik System (NLS). The chapter starts by describing the mathematics behind these systems and examines the shape of their attractors. Based on the theory of LTF, the conditions for achieving synchronization of fractional order systems are studied.

Universiti Malaya

The numerical results of performance with a different value of α is evaluated while the original message and recovered message are identified.

Chapter 5 introduces the synchronization of Integer-Order Neural Networks (IONNs) and FONNs. Then, the numerical example and simulation with a different value of α are evaluated to find the best value of α.

Chapter 6 introduces a new cryptographic algorithm called double encryption. We present a design methodology to obtain double encryption systems for NNs. The combination is between Projective Fractional-Order Neural Networks (PFONNs) and symmetric encryption. Then the numerical example and simulation of the synchronization are demonstrated in this chapter.

Chapter 7 presents some summaries and conclusions of our research problem and suggestion for future work.

The thesis ends with references, a list of publications, and an appendix arranges in that order. Appendix A contains published papers. Finally, Appendix B contains MATLAB codes for the algorithms used to study chaos systems in Chapter 4,5 and 6.

Universiti Malaya

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The chapter presents a discussion on previous literature with different current studies perspectives. This chapter is developed in two sections. Section 2.2 is about chaos based encryption with the subsection 2.2.1, focused on FONLS and chaos masking. While subsection 2.3.1 presents a discussion on IONNs and FONNs with time delays, then subsection 2.3.2 is focused on combination of FONNs with symmetric encryption.

2.2 Prior Research Works on Chaos Based Encryption

Chaos-based encryption has received more interest from researchers in many different fields since the late 1980s because chaotic systems and cryptosystems share many related properties. There has been extensive interest in synchronization in chaotic dynamic systems from many different research fields in recent years. The application is secure communication because chaos synchronization is a key technique for secret communication. The problems related to chaos synchronization have been broadly considered since early 1990 and contributed a high impact on science (Pecora & Carroll, 1990). Numerous effective methods for synchronising identical chaotic systems have been implemented following Pecora and Carroll, such as active control (Bai & Lonngren, 1997), adaptive control (Agiza & Matouk, 2006; Hegazi et al., 2002; Liao & Lin, 1999; Yassen, 2003), feedback synchronization (Matouk, 2008), lag synchronization (Taherion & Lai, 1999), and the approach of backstepping design (Matouk & Agiza, 2008).

Several encryption schemes based on chaos were proposed, and many of those schemes were later eradicated. Indeed without replacing the transmitter's chaotic dynamics, some chaotic encryption schemes were broken, such that without studying for the secret key used to encrypt the message. This form of attack is generally applicable if modifying the

Universiti Malaya

transmitted plaintext, the ciphertext change's statistical properties possible at the receiver, by selecting the product signal.

2.2.1 FONLS with Chaos Masking and Associated Problem

The masking of the message is done by (Colet & Roy, 1994; Cuomo et al., 1992, 1993) in chaotic communication systems by embedding the signal inside a chaotic carrier. The message recovery is based on the synchronization phenomenon, introduced by Ashwin (2003), enabling the receiver to replicate the chaotic part of the signal being transmitted. After synchronization occurs, by analyzing the input and output of the recipient, the decoding of the message is straightforward. In unpredictable communication systems, privacy arises from the fact that in order to recover the message, the eavesdropper must have the correct hardware and parameter settings. Argyris et al. (2005) has recently shown that chaos masking to be one of the applications of chaos-based cryptography. Nevertheless, the security of their systems yet a critical problem to be addressed.

Previously, researchers only interested in some unique chaotic systems of unknown parameters which is integer order without fractional-order. That is why the synchronization can be completed in a short time because of the simple structure of the chaotic systems. In this case, there is a limitation for the extendibility, portability and feasibility if we use these methods. It is only started in 1995 when chaos in a fractional-order was introduced (Hartley et al., 1995) while the first person who used FO in NLS is Sheu et al. (2008).

In this study, inspired by the earlier discussions, we introduce the combination of FONLS and CM since this research area is very limited. We showed that CM within the FONLS can be achieved and results on FONLS and CM are presented in Chapter 4.

Universiti Malaya

2.3 Synchronization Problem for Various Types of NNs with Time Delays

Previous literature on chaos-based cryptography in a secure communication system is able to deliver a higher degree of security. Note that it just provides the perfect situation for communication. Nevertheless, during transmitting message signals from the transmitter to the receiver, there is always a propagation time-delay for every real communication device. From the control theory, the time-delay will cause the communication system to be inaccurate and lead to synchronization failure. Analyzing the stability of a synchronized system with the time-delay is, therefore, a significant issue. Consequently, we will consider this real-world problem in the following section to investigate the stability of the proposed secure communication system that consists of a time delay.

Synchronization in NNs, such as Hopfield NNs, cellular NNs and bi-directional associative memory networks, has received much attention among scientists from different areas over the last few years (Cao et al., 2007; G. Chen & Dong, 1993; Cheng et al., 2006; C. Li et al., 2007; Q. Wang et al., 2008). To fully experience different kinds of complex networks' dynamical behaviours, an exciting and essential phenomenon to analyze is all dynamical nodes' synchrony. Synchronization is an essential movement in nature that has been studied for a great time after Christian Huygens discovered the synchronization of two pendulum clocks in 1665.

Time-delayed systems are found in almost every scientific field, including physics, biology, and chemistry (Erneux, 2009). For example, in (Mackey & Glass, 1977), they modelled the regulation of breathing rate and white blood cells' production as nonlinear time-delayed feedback processes. The dynamics of a time-delayed feedback system is affected not just by its present state but also by the past states. Such systems are mathematically described by delay-differential equations which, in principle, are infinite-dimensional because a continuous history function defined over at least one delay period is

Universiti Malaya

required to solve the equations.

However, resulting from the finite switching speed of the amplifiers or the finite speed of information processing time delays; such as discrete delays or the state derivative (neutral delays) were mostly experienced in system design (Fridman, 2006; Hale & Lunel, 1993; Karimi & Gao, 2008; Park & Won, 1999), which could be a source of oscillation, divergence and instability in NNs. Some other type of time-delays, namely time-delays distributed, has received increasing attention from researchers (Z. Wang et al., 2006). The primary factor is that a NNs is usually nonlinear, due to several parallel pathways of a variety of axon sizes and lengths. Continuously delays should be introduced in the modelling of the NNs, over a specific continuation of time. The different knowledge has less impact than the recent behaviour of the state (Y. Wang et al., 2006). Hence (He, Liu, Rees, & Wu, 2007; Karimi & Gao, 2009; Shen & Wang, 2007; Zhang & Wang, 2008) have gained an exceptional deal of research attention in the stability problems of NNs with mixed time delays.

Recently, appropriate conditions have been proposed for both delay independent and delay-dependent to verify the asymptotic or exponential stability of delayed NNs, see for example the references (He, Liu, & Rees, 2007; Mou et al., 2008; L. Wu et al., 2010; Y. Zhao et al., 2008); (C. Li et al., 2005; Zeng & Wang, 2006) and references therein.

In addition, several findings have been published on the issue of stability analysis for different distributed time-delays NNs, such as recurring NNs (Liang & Cao, 2007; Song et al., 2006) (Song et al., 2006), bi-directional associative memory networks (Liang & Cao, 2004), Hopfield NNs (H. Zhao, 2004b), cellular NNs, (H. Zhao, 2004a). It is noted that the references (Liu et al., 2008; Song & Wang, 2008; Z. Wang et al., 2006). have recently found both discrete and distributed time delays.

The synchronization problem for stochastic discrete-time MSSYS networks with time-

Universiti Malaya

varying delay in (Liang et al., 2008) was explored by using the Lyapunov functional approach combined with the stochastic analysis as well as the technique of feedback control. This method's benefit was that a less conservative condition was obtained depending on the lower and upper limits of the time-varying delay. Besides, the published findings show that, despite its functional significance, general results relating to exponential synchronization of MSSYS with mixed neutral, discrete and distributed delays and $H\infty$ performance criteria are few and constrained, mainly due to mathematical difficulties.

From the previous researches, synchronization of identical FONNs or non-identical FONNs exists without delay (Bao & Cao, 2015; Ding & Shen, 2016). In fact, there is always some noise and disruptions, which can affect performance and therefore disrupt the output of the synchronization. The synchronization of delayed FONNs is, therefore, essential to be studied.

2.3.1 IONNs and FONNs with Time Delays and Associated Problem

From the literature review, minimal studies on synchronization between a fractional-order and integer order system. To the author's best knowledge, only these papers (D. Chen et al., 2012; Feki & Gain, 2011; Keyong et al., 2019; Y.-P. Wu & Wang, 2013; L.-x. Yang et al., 2011; X. Yang et al., 2017) mention the combination of integer-order and fractional-order. Furthermore, the combination of fractional-order and integer-order in NNs has not yet been studied in depth. Thus, studies on FONNs and IONNs is presented in Chapter 5.

2.3.2 FONNs with Symmetric Encryption and Associated Problem

Existing cryptography originates in the work of Claude Shannon after World War II Shannon (1949). Shannon's ideas are based on substitution-permutation networks, which are at the heart of the Lucifer encryption algorithm designed by IBM in the late 1960s and early 1970s, (Pieprzyk et al., 2003).

Universiti Malaya

Chaotic system-generated signals are broadband, noise-like and have random-like statistical properties, despite being deterministic. This makes them a very efficient tool for implementing the principles of confusion and diffusion required by Shannon for cryptosystems (Massey, 1992; Shannon, 1949). The first proposals to this effect were made around 1990 (Habutsu et al., 1991; Matthews, 1989). In 1990 the episode of chaos synchronization (Pecora & Carroll, 1990) entered, a new technique for analogue communication (Kocarev et al., 1992) whose potential for cryptography was soon exploited (Cuomo et al., 1993). Since then, many schemes have been proposed to mask information using chaos properties, either based on discreet chaotic maps or synchronizing signals.

According to this issue, to enhance the cryptosystem's strength and provide greater security, we carry out double encryption that combines chaotic synchronization with a symmetric algorithm. A future explanation is in Chapter 6.

2.4 Time Domain for Chaos Stability in Fractional-Order Systems

In the last two decades, great efforts have been made to bring fractional-order systems into control theory. Podlubny found time domain analytical solutions of fractional differential equations (Podlubny, 1999), but it's hard to analyze because the expression with infinite terms does not converge in steady state (Hwang et al., 2002). Many authors have changed their minds to study time domain approximate expression and its efficient algorithms (Vinagre et al., 2000; Xue & Chen, 2002). Some results have been made in time domain analysis, but they are always complicated to realize because most studies have the configuration of the synchronization scheme determined through trial by error.

Nevertheless, in this study we investigates chaos in the fractional-order system from the time-domain point of view and illustrates one remarkable findings; chaos exists in the FONLS with order as low as 0.94, which represents the smallest value ever reported in literature for any chaotic system studied so far. For finding a more convenient method, we

Universiti Malaya

analyzed such systems properties in time domain and got the clear relationship of time properties between fractional-order systems and integer-order ones.

Universiti Malaya

CHAPTER 3: METHODOLOGY

3.1 Introduction

This chapter explains the methodology employed in this thesis. We describe the Lyapunov Direct Method (LDM) for the stability analysis of nonlinear systems. LDM is then used to develop a general approach in the design of synchronous chaotic systems. Also, we describe details of technique of chaos synchronization in cryptography.

3.2 Lyapunov Stability Analysis

In both system analysis and control design, the Lyapunov stability theory plays an important role. It provides an efficient means of analysing the stability of nonlinear differential equations where it is difficult to obtain the solutions to these equations. The basic approach of the stability analysis of Lyapunov is to find an energy-like scalar function, or so-called function of Lyapunov $V(t, x(t, x_0))$, and to examine its time derivative $\dot{V}(t, x(t; x_0))$ along the system's state trajectory $x(t, x_0)$. In Lyapunov stability analysis, there are two main approaches: the first method of Lyapunov, namely the indirect method of Lyapunov, can be applied to determine the local stability properties of the linearized system around the equilibrium point and its neighbourhood. Although the first method produces only local outcomes, it provides a fundamental design tool for linearized systems that achieve stability around the point of operation. The second method of Lyapunov, namely the LDM, is based on the notion of energy dissipation. The problem of stability is solved by using the $f(x(x_0, t_0), t)$ form instead of the system's explicit solution.

3.2.1 Lyapunov's Direct Method

Two important steps demonstrate asymptotic stability via the direct Lyapunov method. The first step is to find the Lyapunov function, and the second step is to show that the Lyapunov function's derivative is negative semi-definite. By definition, a Lyapunov

Universiti Malaya

function is a function which is positive definite except at the origin where it equals zero, and its derivative is negative semi-definite (Bacciotti & Rosier, 2006). $E(t,x)$ function is said to be a semidefinite positive for x if $E(t,0) = 0$, and $E(t,x) \geq 0$. If $-E(t,x)$ is semi-definite for x then $E(t,x)$ is semi-defined negative for x.

3.2.2 Construction of Lyapunov Direct Method with Time Delays (Razumikhin's Method)

One of the main impediments application of Lyapunov's method to physical system is the lack of formal procedures to construct the Lyapunov function differential equation describing the given physical system. A number of investigators have worked on involving some kind of general methods application to a certain class of problems. One of the most suitable method is by Razumikhin (1960). Consider the time-varying time-delay system, $\dot{x}(t) = f(t, x_t)$. The system is said to be globally uniformly asymptotically stable, if there exist a continuous function $V(t,x)t \in J_\tau, x \in R_n$, three K_∞-functions u, v, w and a continuous nondecreasing function $q(s) \geq s$ for $s \geq 0$, such that the following two conditions are met for all $t \in J$. (I) $u(|x|) \leq V(t,x) \leq v(|x|), x \in R^n$,. (II) $\dot{v}(t, x(t)) \leq -w(|x(t)|)$. (III) If $V(t+s, x(t+s)) \leq q(V(t, x(t))), \forall s \in [-\tau, 0]$. And in the Razumikhin stability theorem the time-derivative of the Razumikhin function $V(t, x(t))$ is also required to be negative definite under the Razumikhin's condition (III).

3.3 Synchronization of Chaotic System

The general synchronization method is to determine two or more identical chaotic systems and combine them to have the same chaotic behaviour. We define the overall combined framework as:

$$dx/dt = f(x) \tag{3.1}$$

$$dy/dt = f(x,y) \tag{3.2}$$

Universiti Malaya

where x and y are vectors of dimension n, and n is any integer, and $f : R_n \rightarrow R_n$ is a nonlinear vector field, then the two systems are said to be synchronized if the synchronization error signal $e(t)$,

$$e(t) = (y(t) - x(t)) \rightarrow 0 \ \ as \ \ \ t \rightarrow \infty \tag{3.3}$$

As to increase the complexity of the transmitter, one may use a FO chaotic system as transmitter. A chaotic FO dynamical equation produces a complex behavior which makes the masked signal more encrypted and consequently hard to decipher. The complexity of fractional-order systems is due to dealing with integration and derivation of non-integer orders.

3.4 Conclusion

In this chapter, we explained the LDM methodology used in this thesis. LDM is used for nonlinear systems stability analysis to develop a synchronous chaotic system. To explain the synchronization methods used in this study, numerical examples and simulation will provided to demonstrate the effectiveness of our derived theoritical results. Further information about how the technique is applied are explained in Chapters 4, 5, and 6.

Universiti Malaya

CHAPTER 4: SYNCHRONIZATION OF FONLS COMBINED WITH CHAOS MASKING WITH MINIMAL ORDER BY CONTROLLING THE INITIAL CONDITION FOR SECURE COMMUNICATION

4.1 Introduction

In this chapter, we studied two identical strange attractors of FONLS. Various initial conditions are numerically analyzed within the same parameter condition of FONLS. For the different initial conditions used in this analysis, the ranges are relatively wide, and the synchronization of two identical FONLS is studied in this chapter. An Active Control (ACC) is the method used for obtaining the synchronization within chaotic FONLS. Based on the theory of LTF, the conditions for obtaining synchronization of FO systems are investigated. In order to verify the synchronization process for efficiency and viability, numerical simulations are given, so the process's outcome is simultaneously verified with theoretical principles and computational methods. The earlier theory is also utilized to secure communications by employing the CM system.

4.2 The Model's System.

The NLS is characterized by the following differential equation

$$\begin{aligned} \dot{x} &= -ax + y + 10yz \\ \dot{y} &= -x - 0.4y + 5xz \\ \dot{z} &= bz - 5xy \end{aligned} \tag{4.1}$$

where a, b are unknown positive constant parameters while x, y and z are state variables. With the parameter's values $a = 0.4$ and $b = 0.175$, chaotic behaviour in NLS can occur.

The FONLS is a nonlinear system, and the stability of the nonlinear fractional system is very complex and differs from that of the linear fractional system. The significant difference is that steady states, equilibrium point and limit cycle need to be investigated for

Universiti Malaya

a nonlinear system. There are many definitions of stability and several equilibrium points for nonlinear systems, and Lyapunov formulated the primary idea (Lyapunov, 1992).

Theorem 4.2.1 *"According to stability theorem defined in (Tavazoei & Haeri, 2007a) the equilibrium points are asymptotically stable for* $\alpha_1 = \alpha_2 = ... = \alpha_n$ *if all the eigenvalues* e_i, $(i = 1, 2, \ldots, n)$ *of the Jacobian matrix* $J = \partial f/\partial x$, *where* $f = [f1, f2, \ldots, fn]^T$, *evaluated at the equilibrium* E^*, *satisfy the condition (Tavazoei & Haeri, 2007a, 2007b)"*

$$arg(eig(\mathbf{J}))| = |arg(\lambda_i)| > a\frac{\pi}{2}, \quad i = 1, 2, \ldots, n$$

Definition 4.2.1 *"Suppose that the unstable eigenvalues of scroll focus points are:* $\lambda_{1,2} = \gamma_{1,2} \pm \beta_{1,2}$. *The necessary condition to exhibit double-scroll attractor of system* $D^a x = f(x)$ *is the eigenvalues* $\lambda_{1,2}$ *remaining in the unstable region (Tavazoei & Haeri, 2008). The condition for commensurate derivatives order is"*

$$\alpha > \frac{2}{\pi} a\tan\left(\frac{|\beta_i|}{\gamma_i}\right), \qquad i = 1, 2.$$

For nonlinear systems, definition 4.2.1 is used to compute the least order for the system to generate chaos (Tavazoei & Haeri, 2007a). The system cannot be chaotic when negative result is obtained from the instability measure $\frac{\pi}{2m} - min(|arg(\lambda)|)$.

For the FONLS, the fractional is use instead of the integer-order derivative one. α_1, α_2, α_3 are derivatives orders of;

$$\begin{aligned} D_t^{\alpha_1} x_1(t) &= -ax_1(t) + y_1(t) + 10y_1(t)z_1(t) \\ D_t^{\alpha_2} y_1(t) &= -x_1(t) - 0.4y_1(t) + 5x_1(t)z_1(t) \\ D_t^{\alpha_3} z_1(t) &= bz_1(t) - 5x_1(t)y_1(t) \end{aligned}$$

where $0 < \alpha_1, \alpha_2, \alpha_3 \leq 1$.

Universiti Malaya

While for the case where $\alpha_1 = \alpha_2 = \alpha_3 \equiv a$, we called it as a commensurate order system and for the system to show better dynamic behaviour, the lowest total order was $\alpha_1 + \alpha_2 + \alpha_3 = 2.82$ (Sheu et al., 2008).

4.3 Synchronization of FONLS with Active Control

We will begin with the synchronization between two identical FONLS. We consider the MS (4.1) and the SS with $U = [U_a, U_b, U_c]^T$ as the controller function presented in the SS. The controller is introduced for synchronizing of two coupled identical FONLS with the same parameters a and b but with different initial conditions.

The two systems will be synchronized if the trajectory of MS follows the same path as the MS, that means

$$|x(t) - y(t)| \to c, \; t \to \infty.$$

If $c = 0$, then the synchronization is called complete synchronization.

The following are described as MS and SS

$$\begin{aligned} D_t^{\alpha_1} x_1(t) &= -ax_1(t) + y_1(t) + 10y_1(t)z_1(t) \\ D_t^{\alpha_2} y_1(t) &= -x_1(t) - 0.4y_1(t) + 5x_1(t)z_1(t) \\ D_t^{\alpha_3} z_1(t) &= bz_1(t) - 5x_1(t)y_1(t) \end{aligned} \tag{4.2}$$

$$\begin{aligned} D_t^{\alpha_1} x_2(t) &= -ax_2(t) + y_2(t) + 10y_2(t)z_2(t) + U_a(t) \\ D_t^{\alpha_2} y_2(t) &= -x_2(t) - 0.4y_2(t) + 5x_2(t)z_2(t) + U_b(t) \\ D_t^{\alpha_3} z_2(t) &= bz_2(t) - 5x_2(t)y_2(t) + U_c(t) \end{aligned} \tag{4.3}$$

Subtracting equation (4.2) from equation (4.3) will generate the error Error Dynamical

Universiti Malaya

System (EDS) as follows:

$$\begin{aligned} D_t^{\alpha_1} e_1(t) &= -ae_1(t) + e_2(t) + 10y_2(t)z_2(t) - 10y_1(t)z_{1(t)} + U_a(t) \\ D_t^{\alpha_2} e_2(t) &= -e_1(t) - 0.4e_2(t) + 5x_2(t)y_2(t) - 5x_1(t)y_1(t) + U_b(t) \\ D_t^{\alpha_3} e_3(t) &= be_3(t) - 5x_2(t)y_2(t) + 5x_1(t)y_1(t) + U_c(t), \end{aligned} \tag{4.4}$$

where $e_1 = x_2 - x_1$, $e_2 = y_2 - y_1$, $e_3 = z_2 - z_1$. We will re-write the control U by considering another control V suitable chosen that is a function of EDS e_1, e_2, e_3. We re-refine U as

$$\begin{aligned} U_a(t) &= -10y_2(t)z_2(t) + 10y_1(t)z_1(t) + V_a(t) \\ U_b(t) &= -5x_2(t)y_2(t) + 5x_1(t)y_1(t) + V_b(t) \\ U_c(t) &= 5x_2(t)y_2(t) - 5x_1(t)y_1(t) + V_c(t) \end{aligned} \tag{4.5}$$

substituting 4.5 in 4.4 we get

$$\begin{aligned} D_t^{\alpha_1} e_1(t) &= -ae_1(t) + e_2(t) + V_a(t) \\ D_t^{\alpha_2} e_2(t) &= -e_1(t) - 0.4e_2(t) + V_b(t) \\ D_t^{\alpha_3} e_3(t) &= be_3(t) + V_c(t) \end{aligned} \tag{4.6}$$

We proved that the two considered systems are globally synchronized, that means we must choose the ACC V such that the error converges to 0 when $t \rightarrow \infty$. We prefer V such that:

$$\begin{bmatrix} V_a \\ V_b \\ V_c \end{bmatrix} = A \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} \tag{4.7}$$

A is the $[3 \times 3]$ matrix selected to satisfy the condition of $|arg\,(\lambda i)| > \alpha\frac{\pi}{2}$, $i = 1, 2, 3$, for all the system (4.7)'s eigenvalues, λi.

Universiti Malaya

One choice of A is

$$A = \begin{bmatrix} -1+a & -1 & 0 \\ 1 & -0.6 & 0 \\ 0 & 0 & -1-b \end{bmatrix} \tag{4.8}$$

and the ACC are

$$\begin{aligned} V_a(t) &= (-1+a)\, e_1 - e_2 \\ V_b(t) &= e_1 - 0.6 e_2 \\ V_c(t) &= (-1-b)\, e_3 \end{aligned} \tag{4.9}$$

Then all three eigenvalues of the system (4.6) are -1. Therefore, the condition of Theorem 4.2.1 is satisfied for $\alpha > 2$. Since we consider only the values $\alpha \leq 1$, The error system (4.6) becomes

$$\begin{aligned} D_t^{\alpha_1} e_1(t) &= -\, e_1(t) \\ D_t^{\alpha_2} e_2(t) &= -\, e_2(t) \\ D_t^{\alpha_3} e_3(t) &= -\, e_3(t) \end{aligned} \tag{4.10}$$

Proposition 4.3.1 *The systems of fractional differential equation* (4.2) *and* (4.3) *will approach locally asymptotically stable for any initial condition and with the ACC* (4.9).

Proof Based on LTF, we multiplying LTF in both sides of equation (4.10), letting $\mathcal{L}\,(e_i\,(t)) = F_i\,(s)$, and utilizing $\mathcal{L}\,(D^{\alpha_i}\, e_i\,(t)) = s^{\alpha_i}\, F_i\,(s) - \; s^{\alpha_i - 1}\, F_i\,(0)$, where $i = 1, 2, 3$ and s is complex number frequency parameter, we obtain

$$\begin{aligned} s^{\alpha_1}\, F_1\,(s) - \; s^{\alpha_1 - 1}\, e_1\,(0) &= -\, F_1(s) \\ s^{\alpha_2}\, F_2\,(s) - \; s^{\alpha_2 - 1}\, e_2\,(0) &= -\, F_2(s) \\ s^{\alpha_3}\, F_3\,(s) - \; s^{\alpha_3 - 1}\, e_3\,(0) &= -\, F_3(s) \end{aligned} \tag{4.11}$$

Universiti Malaya

Equation (4.11) can be rewritten as follows;

$$\begin{aligned} F_1(s) &= \frac{s^{\alpha_1 - 1}\, e_1(0)}{s^{\alpha_1} + 1} \\ F_2(s) &= \frac{s^{\alpha_2 - 1}\, e_2(0)}{s^{\alpha_2} + 1} \\ F_3(s) &= \frac{s^{\alpha_3 - 1}\, e_3(0)}{s^{\alpha_3} + 1} \end{aligned} \tag{4.12}$$

By using the final-value theorem of the LTF, we have

$$\begin{aligned} \lim_{s \to 0} sF_1(s) &= \lim_{t \to \infty} e_1(t) = 0 \\ \lim_{s \to 0} sF_2(s) &= \lim_{t \to \infty} e_2(t) = 0 \\ \lim_{s \to 0} sF_3(s) &= \lim_{t \to \infty} e_3(t) = 0 \end{aligned} \tag{4.13}$$

Therefore, $e_1(t)$, $e_2(t)$ and $e_3(t)$ converge to zero, that is the system (4.2) and (4.3) are asymptotic synchronized for any initial condition with the ACC (4.9). This completes the proof.

4.4 Chaos Masking and FONLS in Secure Communications

CM has become one of the oldest known recommendations for chaotic communication techniques (Cuomo & Oppenheim, 1993; Kocarev et al., 1992; Oppenheim et al., 1992). The CM is based on the Pecora and Carroll (PC) synchronization ideology that consists of transmitting analogue signals. CM involving the transmission of the combination of the two signals. The process involved by adding the message signal m to a chaotic carrier signal x (Oppenheim et al., 1992).

The message signal $m(t) = 0.5\ sin(\pi)$ is added with the chaotic mask signal and gives the transmitted signal $s(t)$. We have to assume that the signal message of the message is weaker than chaotic signal, $c(t)$. We can assume that without knowing the exact $c(t)$, the message signal $m(t)$ can not be separated from $s(t)$ because the chaotic signal $c(t)$

Universiti Malaya

from FONLS is very complex and $m(t)$ is weaker than $c(t)$. To synchronize the chaotic systems, the received $r(t)$ signal is used on the receiver and transmitter. After the chaotic synchronization has been completed, the $c(t)$ and $m(t)$ signals can be retrieved at the receiver and are denoted by $\hat{c}(t)$ and $\hat{m}(t)$ respectively.

The selected MS are as follows.

$$\begin{aligned} D_t^{\alpha_1} x_1(t) &= -ax_1(t) + y_1(t) + 10y_1(t)z_1(t) + 0.5\sin(n\pi) \\ D_t^{\alpha_2} y_1(t) &= -x_1(t) - 0.4y_1(t) + 5x_1(t)z_1(t) \\ D_t^{\alpha_3} z_1(t) &= bz_1(t) - 5x_1(t)y_1(t) \end{aligned} \tag{4.14}$$

The EDS will be:

$$\begin{aligned} D_t^{\alpha_1} e_1(t) &= -ae_1(t) + e_2(t) + 10y_2(t)z_2(t) - 10y_1(t)z_1(t) - 0.5\,sin(n\pi) + U_a(t) \\ D_t^{\alpha_2} e_2(t) &= -e_1 - 0.4e_2(t) + 5x_2(t)y_2(t) - 5x_1(t)y_1(t) + U_b(t) \\ D_t^{\alpha_3} e_3(t) &= be_3(t) - 5x_2(t)y_2(t) + 5x_1(t)y_1(t) + U_c(t) \end{aligned} \tag{4.15}$$

where $e_1 = x_2 - x_1$, $e_2 = y_2 - y_1$, $e_3 = z_2 - z_1$. We will rewrite the control U by considering another control V suitable chosen that is a function of EDS e_1, e_2, e_3. We redefine U as

$$\begin{aligned} U_a(t) &= -10y_2(t)z_2(t) + 10y_1(t)z_1(t) + 0.5\,sin(n\pi)) + V_a(t) \\ U_b(t) &= -5x_2(t)y_2(t) + 5x_1(t)y_1(t) + V_b(t) \\ U_c(t) &= 5x_2(t)y_2(t) - 5x_1(t)y_1(t) + V_c(t) \end{aligned} \tag{4.16}$$

Universiti Malaya

substituting (4.16) in (4.15) we get

$$\begin{aligned} D_t^{\alpha_1} e_1(t) &= -ae_1(t) + e_2(t) + V_a(t) \\ D_t^{\alpha_2} e_2(t) &= -e_1(t) - 0.4e_2(t) + V_b(t) \\ D_t^{\alpha_3} e_3(t) &= be_3(t) + V_c(t) \end{aligned} \tag{4.17}$$

The same parameters are used for the CM of the FONLS with the initial condition $[-0.10, -0.10, -0.18]$, $[-0.20, -0.20, -0.18]$ and $\alpha = 0.95$.

Remark 4.4.1 *In Figure 4.28, an obvious difference between the message signal in Figure 4.28 and the chaotic carrier* (4.14) *can be studied. The transmitted signal is a signal which consists of the original message and the chaotic carrier. A small graph change was observed on the attractor caused by the embedding of the message min the attractor of FONLS. The Figure 4.31 illustrates the state trajectories for EDS* (4.15) *that converge with control input to zero.*

Remark 4.4.2 *The implementation of the FONLS MSSYS in the secure communication system based on CM is shown in theoretically and numerically. The capability to recover the transmitted signal message in Figure 4.30 is established under the condition of noiseless by processing the signal message* $0.5\ sin(n\pi)$ *through the system. By comparing the graphs, one can figure that the transmitted original signal message has been recovered with reasonable accuracy. We emphasized that our proposed technique could be applied with any synchronized chaotic system since it is universal. Our simulation and theoretical results were signifying that the proposed technique may be used in other applications. We also conclude that any reasonable control's input can be chosen to achieve synchronization, and we believed that the same results could be archived for anti-synchronization.*

Universiti Malaya

4.5 Numberical Examples and Simulations

The method of numerical simulation introduced here is the use of MATLAB tools and the graphical analysis displays the findings using this programme. We use two coupled systems, for example (4.2) as MS and (4.3) as a SS. Their chaotic behaviour already proven exist and the results are presented as a graphical display for parameters $(a,\ b) = (0.4, 0.175)$. In order to control the initial condition of the systems, we tested with different sets of initial conditions for MS and SS. The simulation results of chaotic behaviour are illustrated in Figures (4.1-4.3) with different values of α in which the control (4.9) are applied, respectively. In the simulation for $\alpha = 0.95$, the initial condition $[-0.10, -0.10, -0.18]$ and $[-0.20, -0.20, -0.18]$ are chosen for the systems (4.2) and (4.3), respectively. The simulation results are illustrated in Figures (4.8 - 4.10) which show the state trajectories of MS (4.2) and MS (4.3) with control input. Figure 4.11 represent the synchronization errors of MS and SS.

Remark 4.5.1 *From the simulation results, Figures (4.4 - 4.6) which show the state trajectories of MS* (4.2) *and MS* (4.3) *without control input and* $\alpha = 0.95$. *Figure 4.7 illustrates the state trajectories of error dynamical system* (4.6) *which are not converge to zero without control input.*

Remark 4.5.2 *From the simulation results Figures (4.1 and 4.2), it can be seen that when* $\alpha = 0.94$ *with control input, the state are not stable. As the value of* α *decrease, the dynamical systems are not stable, so the minimum value is* $\alpha = 0.95$. *And we can conclude that the best set of initial condition with the minimum order is the third set with* $\alpha = 0.95$ *because it takes the fastest time for the synchronization to archive.*

Remark 4.5.3 *Figures (4.12 - 4.17) represent the state trajectories of the dynamical systems with* $\alpha = 0.99$ *to* $\alpha = 0.94$ *in steps of* 0.005 *with initial condition,* $[0.19, 1.00, -0.18]$

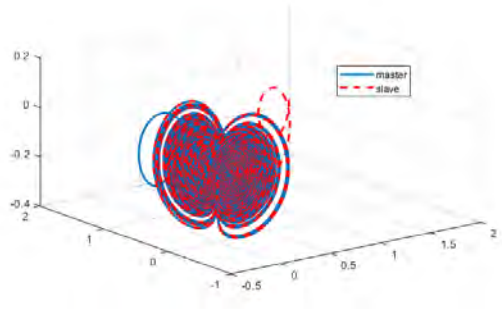
Universiti Malaya

Table 4.1: Synchronization error for different value of initial condition

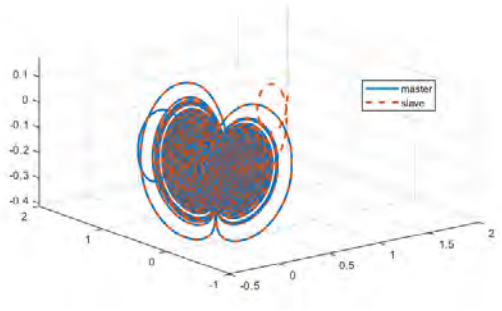
INITIAL CONDITION $(x_1(0), y_1(0), z_1(0)$ $(x_2(0), y_2(0), z_2(0)$	$[0.19, 1.00, -0.18]$ $[2.00, 2.00, -0.18]$	$[0.10, 0.10, 0.18]$ $[0.20, 0.20, 0.18]$	$[-0.10, -0.10, -0.18]$ $[-0.20, -0.20, -0.18]$
α=0.99	5.511	12.008	5.265
α=0.98	5.590	12.156	5.315
α=0.97	5.685	12.300	5.510
α=0.96	5.900	12.650	5.920
α=0.95	6.153	12.971	6.125
α=0.94	6.644 Not stable	Infeasible	6.315 Not stable
α=0.93	Infeasible	Infeasible	Infeasible

and $[2.00, 2.00, -0.18]$. *Figures (4.18 - 4.22) represent the state trajectories of the dynamical systems with* $\alpha = 0.99$ *to* $\alpha = 0.95$ *again in steps of* 0.005 *with initial condition,* $[0.10, 0.10, 0.18]$ *and* $[0.20, 0.20, 0.18]$. *Figures (4.23 - 4.27) represent the state trajectories of the dynamical systems with* $\alpha = 0.99$ *to* $\alpha = 0.94$ *again in steps of* 0.005 *with initial condition,* $[-0.10, -0.10, -0.18]$ *and* $[-0.20, -0.20, -0.18]$. *From Figures (4.12 - 4.27), we observe that the state trajectories of synchronization error of the dynamical system converge to zero. From this, we confirm that the dynamical behaviour of the system is very sensitive to the initial condition with the minimal value of* α. *Furthermore, the synchronization error of all set of initial condition converge to zero and one can easily show that the minimal value of* α *is* 0.95. *We obtain the time taken for syncronization to archive with different initial condition and* α *as listed in the Table 4.1.*

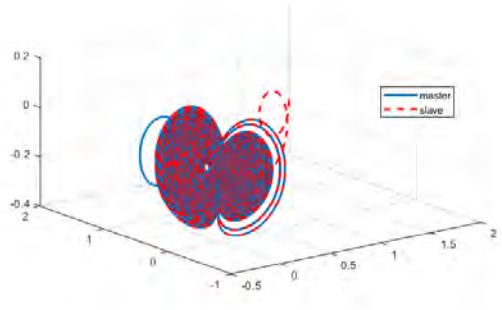
Universiti Malaya



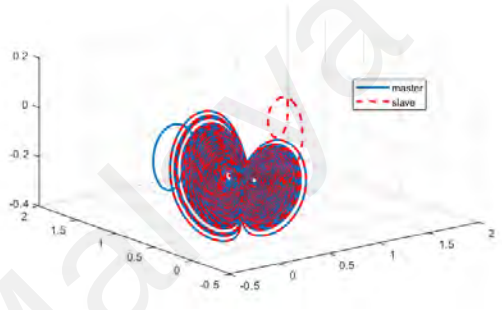
(a) $\alpha = 0.99$



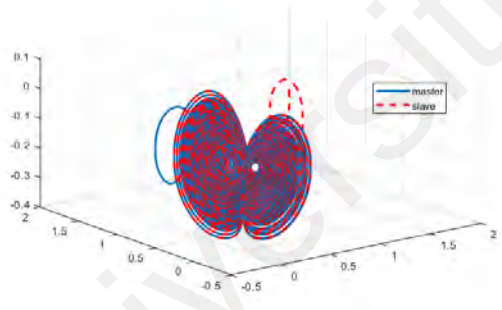
(b) $\alpha = 0.98$



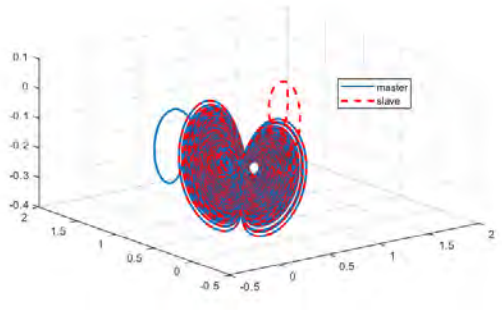
(c) $\alpha = 0.97$



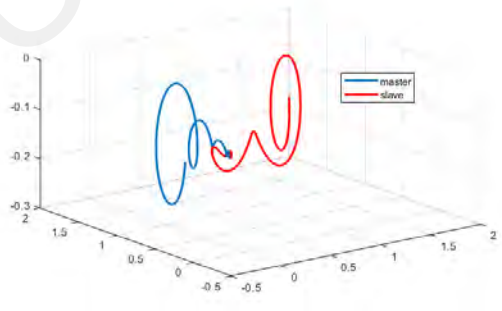
(d) $\alpha = 0.96$



(e) $\alpha = 0.95$



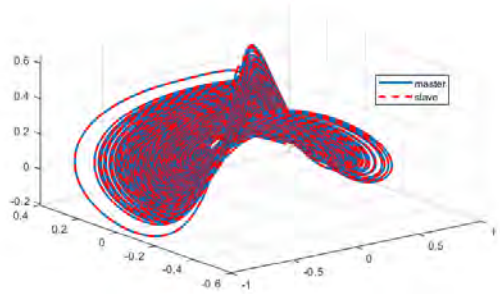
(f) $\alpha = 0.94$



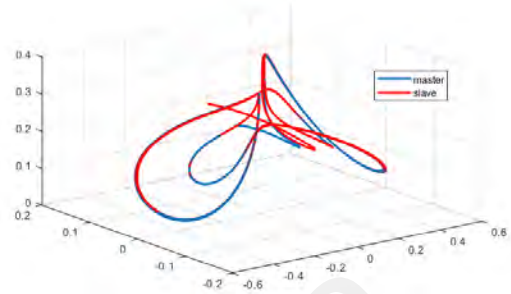
(g) $\alpha = 0.93$

Figure 4.1: Chaotic attractor of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9) **after the synchronization and with different values of** α**,** $\alpha = 0.93$ **to** $\alpha = 0.99$

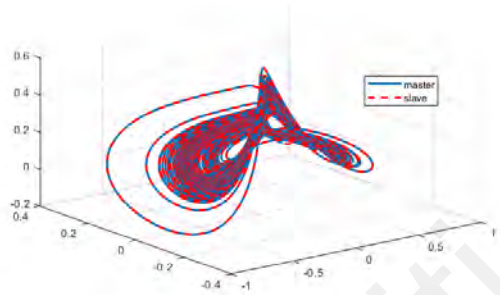
Universiti Malaya



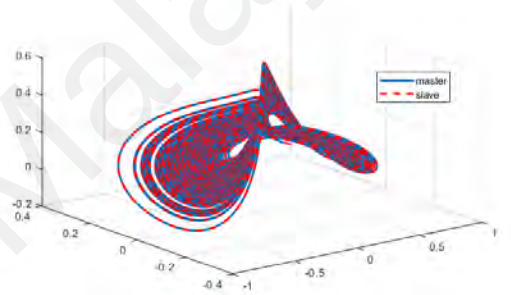
(a) $\alpha = 0.99$



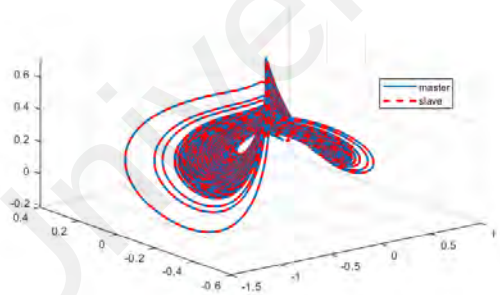
(b) $\alpha = 0.98$



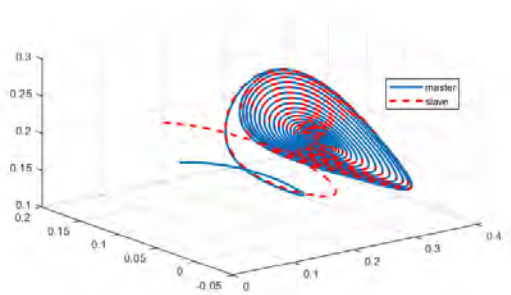
(c) $\alpha = 0.97$



(d) $\alpha = 0.96$



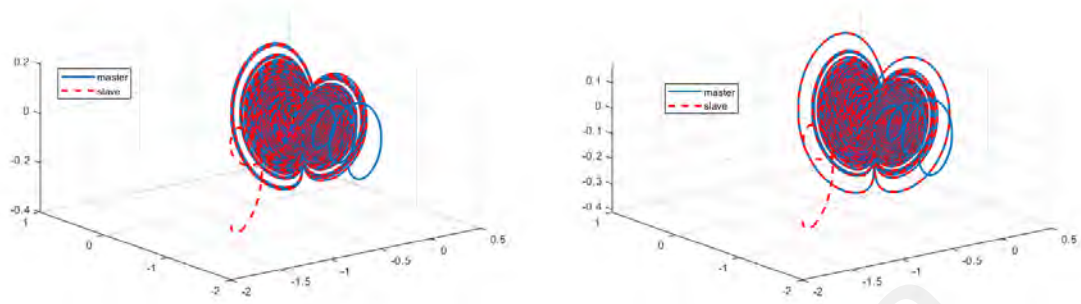
(e) $\alpha = 0.95$



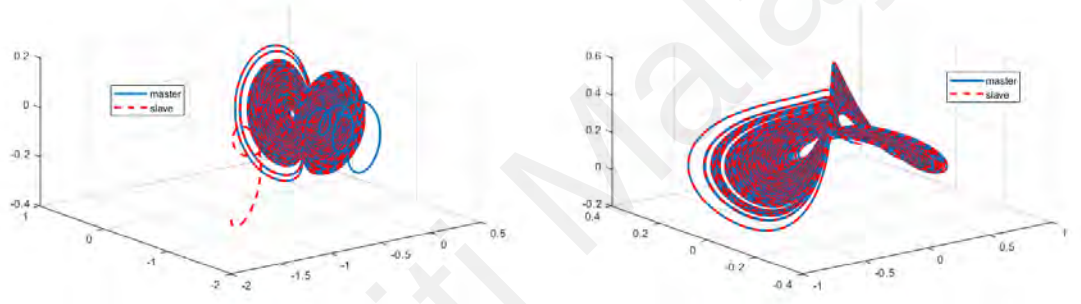
(f) $\alpha = 0.95$

Figure 4.2: Chaotic attractor of MS (4.2) **and SS** (4.3) **of initial condition** $[0.10, 0.10, 0.18]$ **and** $[0.20, 0.20, 0.18]$ **with control input** (4.9) **after the synchronization and with different values of** α

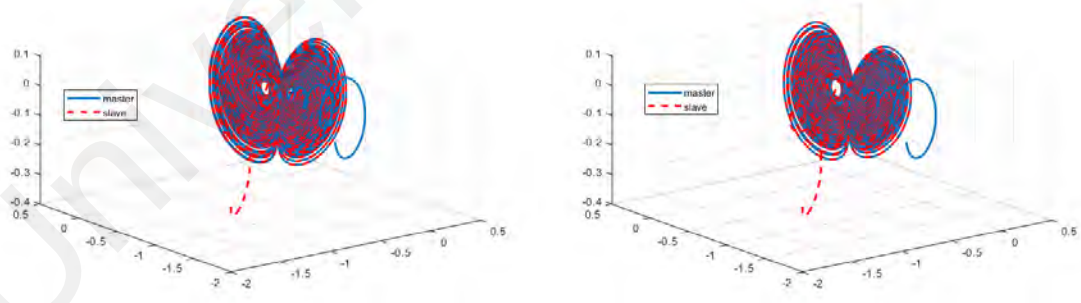
Universiti Malaya



(a) $\alpha = 0.99$ (b) $\alpha = 0.98$



(c) $\alpha = 0.97$ (d) $\alpha = 0.96$



(e) $\alpha = 0.95$ (f) $\alpha = 0.95$

Figure 4.3: Chaotic attractor of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **after the synchronization and with different values of** α

Universiti Malaya

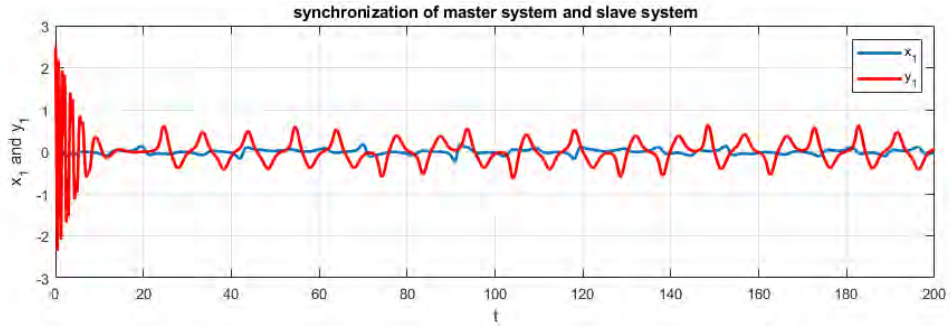


Figure 4.4: State trajectories of MS (4.2) **and SS** (4.3)**,** x_1 **and** y_1 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **without control input and** $\alpha = 0.95$

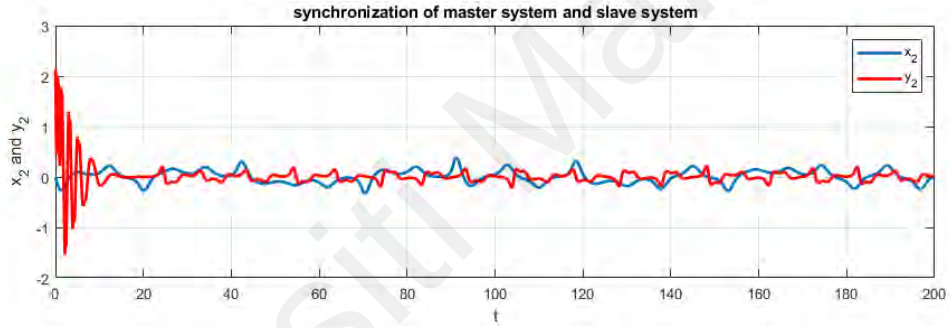


Figure 4.5: State trajectories of MS (4.2) **and SS** (4.3)**,** x_2 **and** y_2 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **without control input and** $\alpha = 0.95$

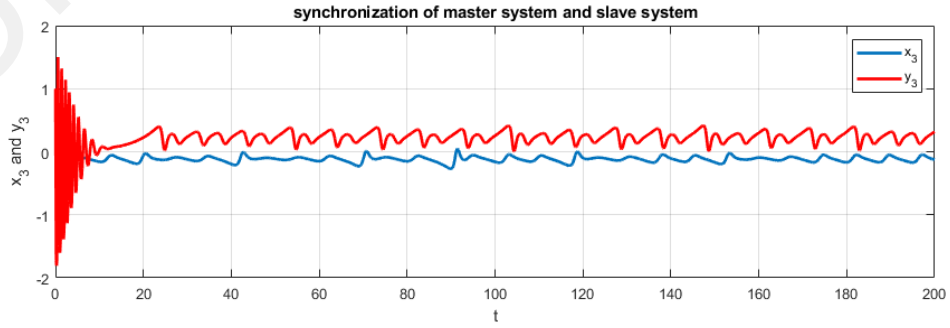


Figure 4.6: State trajectories of MS (4.2) **and SS** (4.3)**,** x_3 **and** y_3 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **without control input and** $\alpha = 0.95$

Universiti Malaya

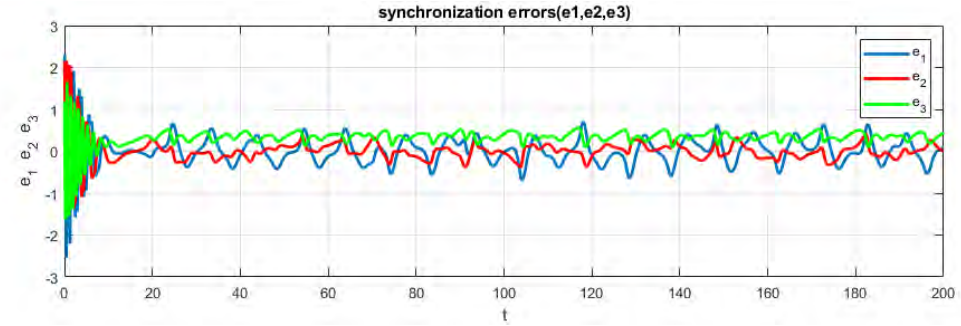


Figure 4.7: State trajectories of synchronization errors e_1, e_2, e_3 with initial condition $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **without control input and** $\alpha = 0.95$

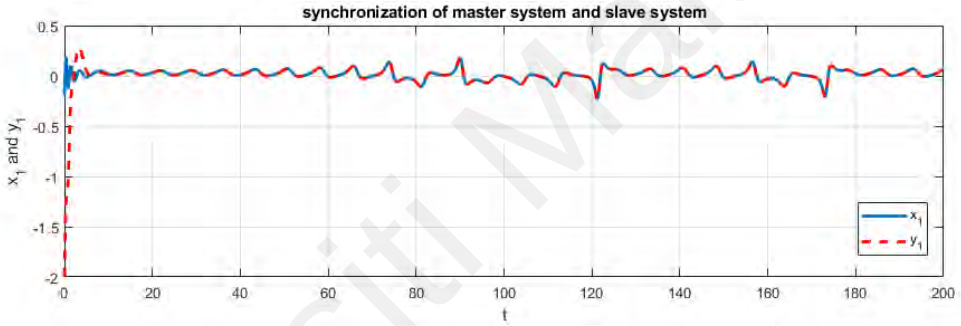


Figure 4.8: State trajectories of MS (4.2) **and SS** (4.3), x_1 **and** y_1 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **and** $\alpha = 0.95$

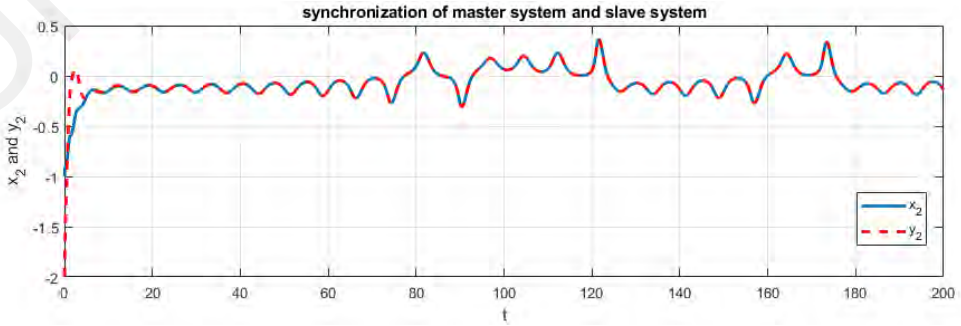


Figure 4.9: State trajectories of MS (4.2) **and SS** (4.3) **system,** x_2 **and** y_2 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **and** $\alpha = 0.95$

Universiti Malaya

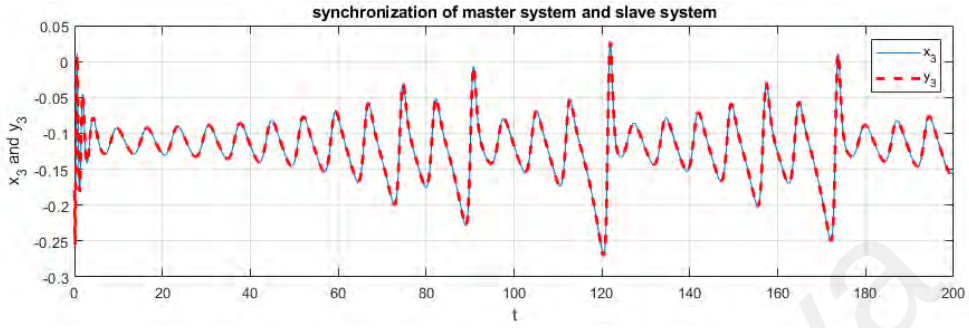


Figure 4.10: State trajectories of MS (4.2) **and SS** (4.3)**,** x_3 **and** y_3 **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **and** $\alpha = 0.95$

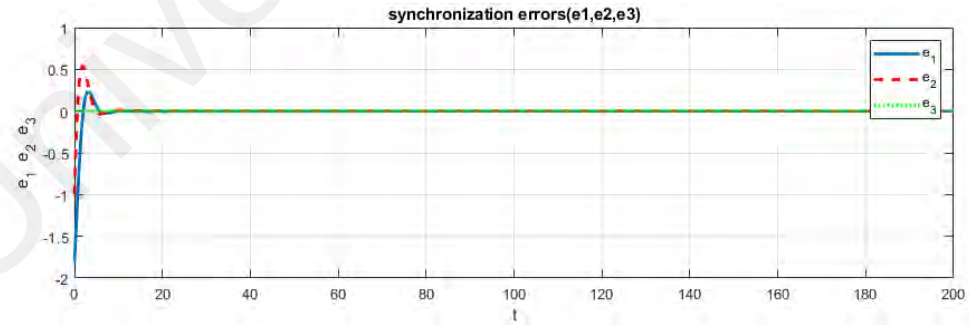


Figure 4.11: State trajectories of synchronization errors e_1**,** e_2**,** e_3 **with initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **and** $\alpha = 0.95$

Universiti Malaya

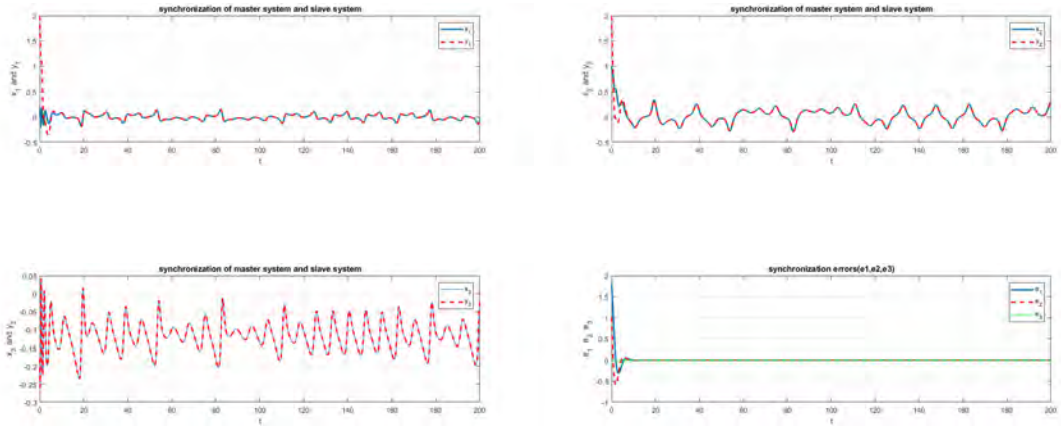


Figure 4.12: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.99$

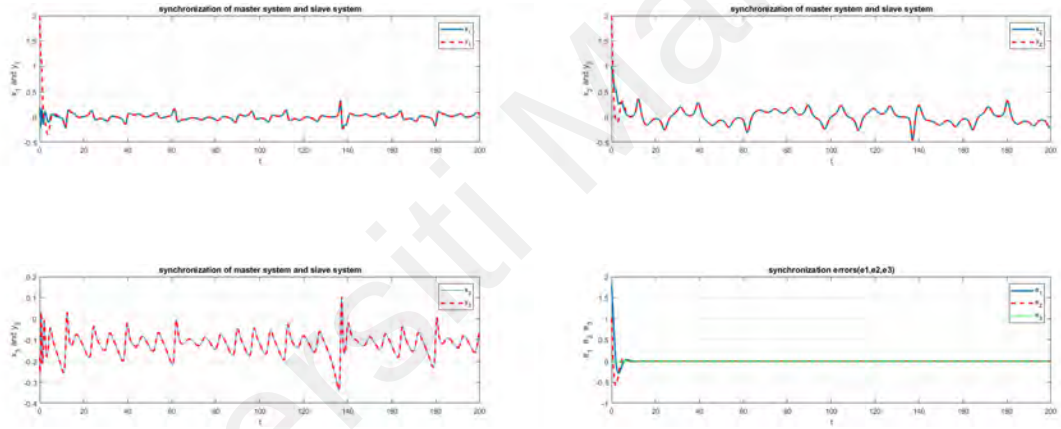


Figure 4.13: State trajectories of MS (4.2) **and SS**(4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.98$

Universiti Malaya

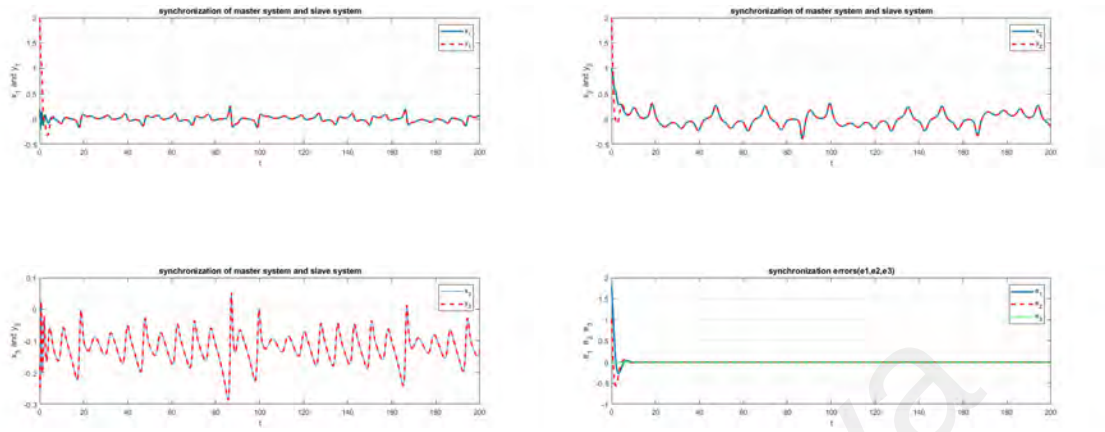


Figure 4.14: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.97$

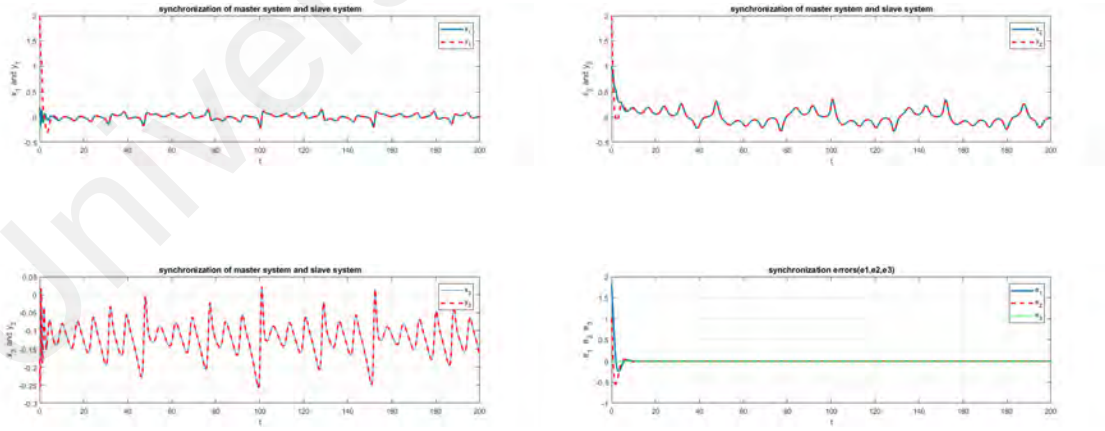


Figure 4.15: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.96$

Universiti Malaya

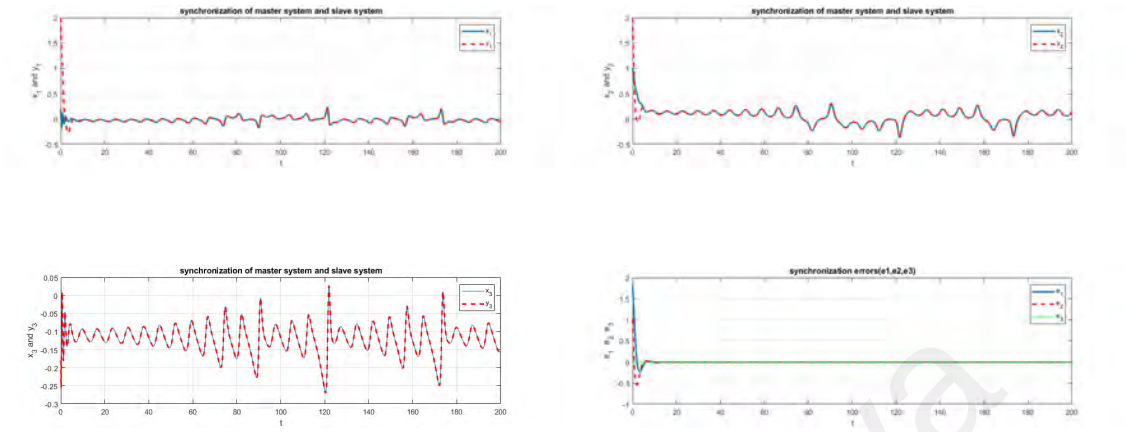


Figure 4.16: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.95$

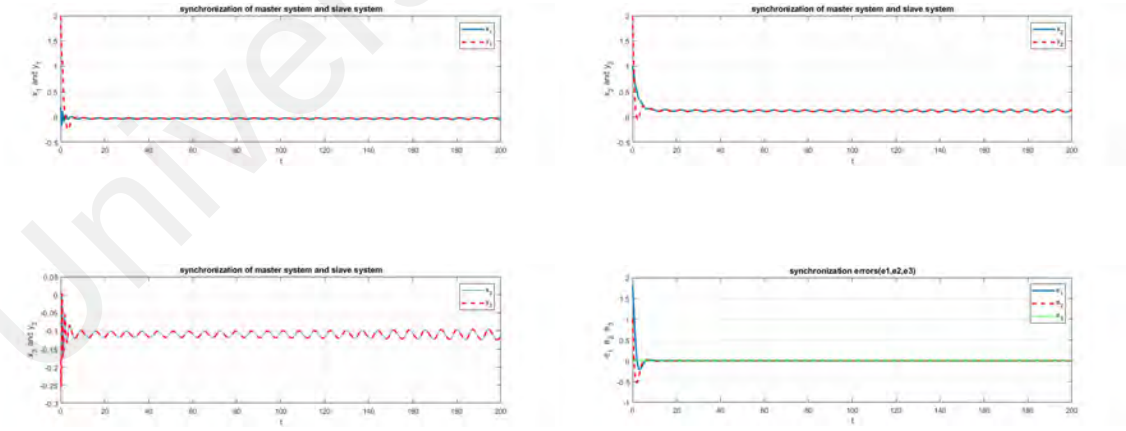


Figure 4.17: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.94$

Universiti Malaya

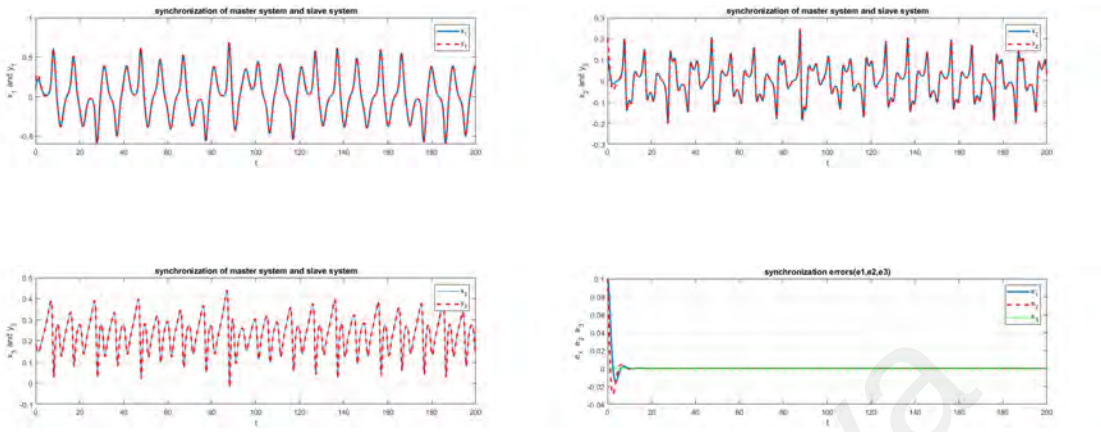


Figure 4.18: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.99$

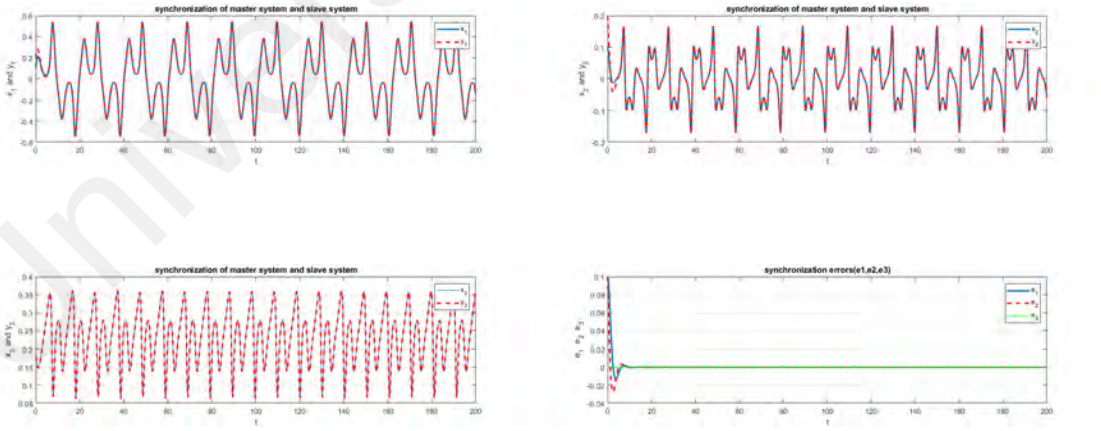


Figure 4.19: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.98$

Universiti Malaya

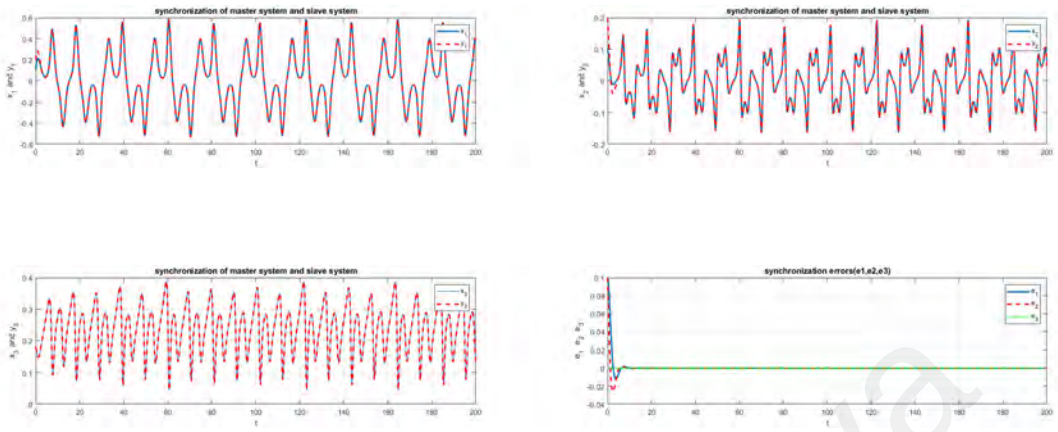


Figure 4.20: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.97$

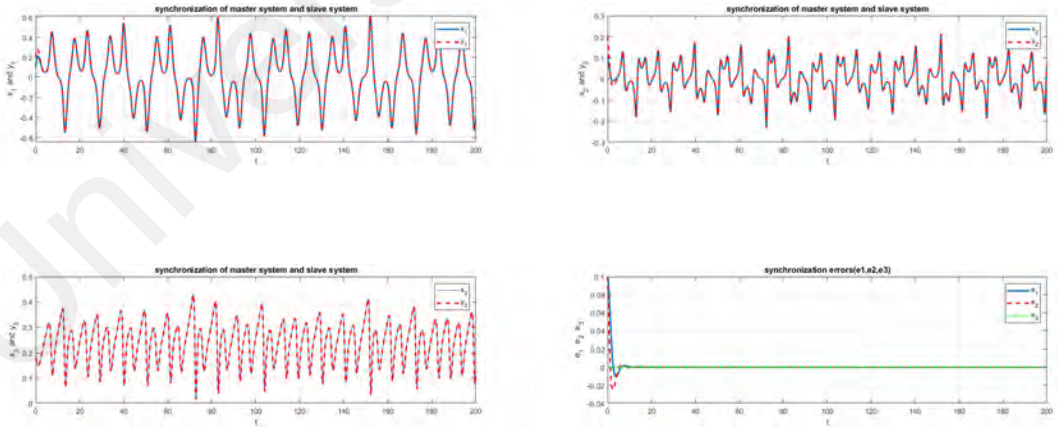


Figure 4.21: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.96$

Universiti Malaya

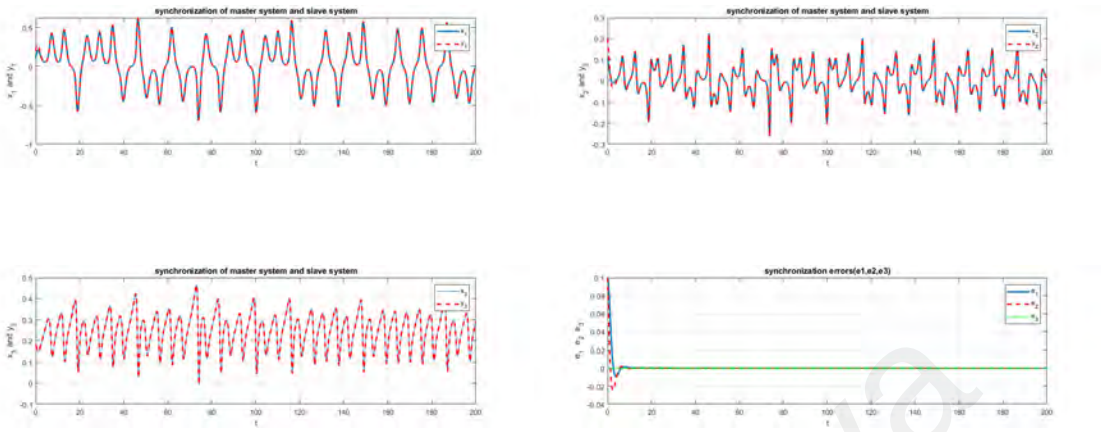


Figure 4.22: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[0.19, 1.00, -0.18]$ **and** $[2.00, 2.00, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.95$

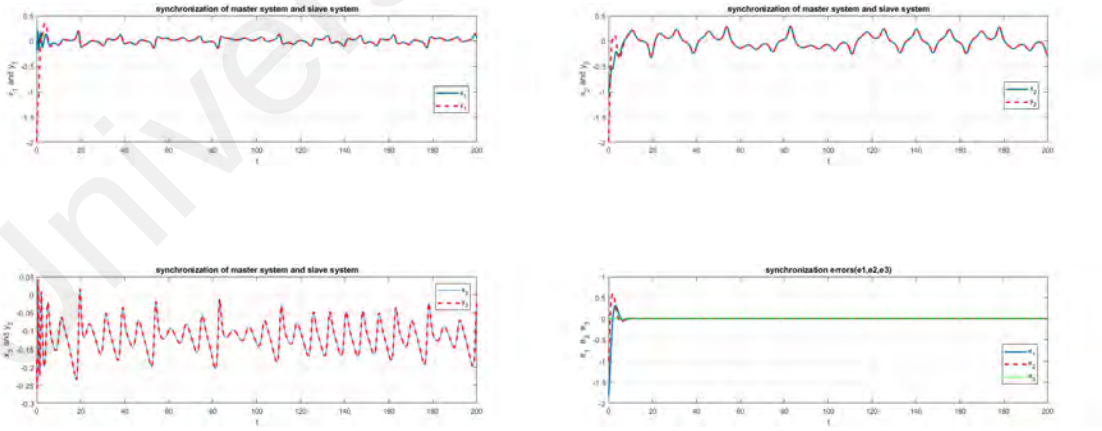


Figure 4.23: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.99$

Universiti Malaya

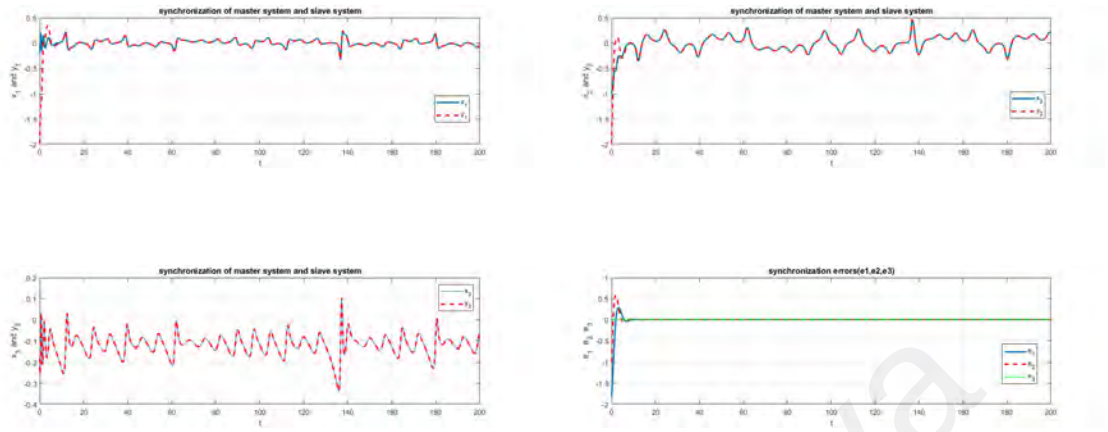


Figure 4.24: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.98$

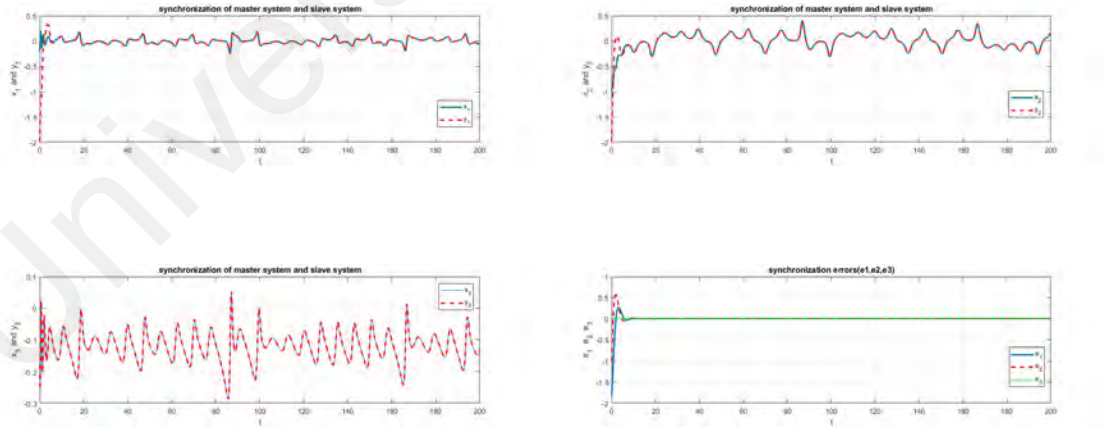


Figure 4.25: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.97$

Universiti Malaya

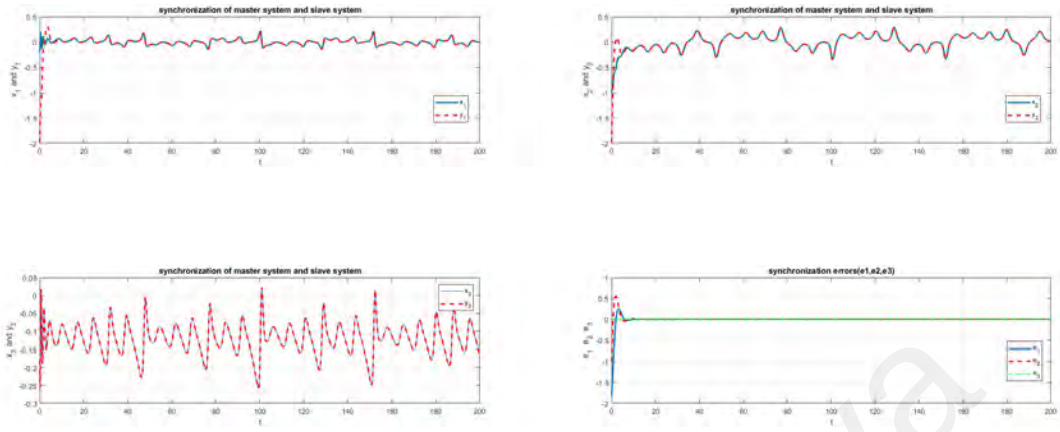


Figure 4.26: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.96$

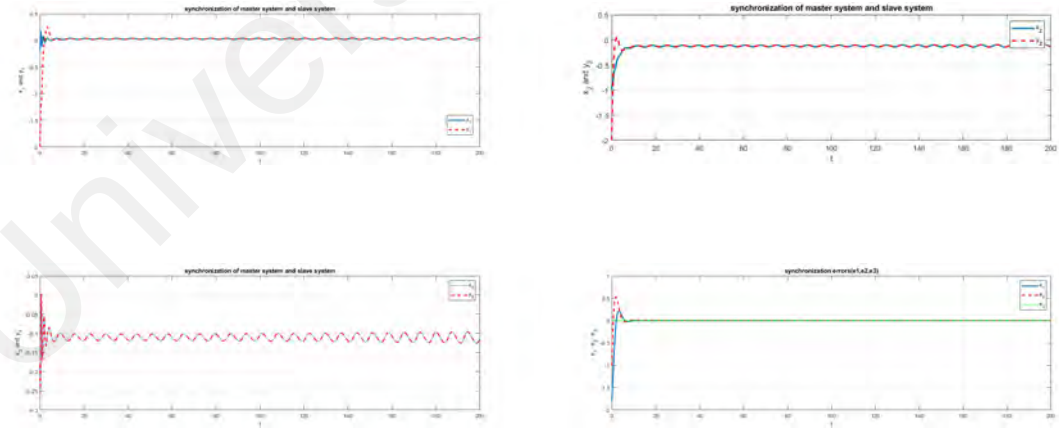


Figure 4.27: State trajectories of MS (4.2) **and SS** (4.3) **of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9)**, synchronization errors** e_1**,** e_2**,** e_3 **and** $\alpha = 0.94$

Universiti Malaya

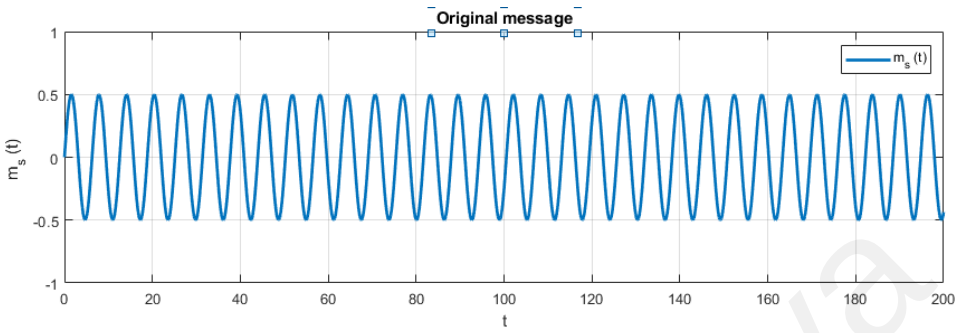


Figure 4.28: Original signal message $0.5sin(n\pi)$

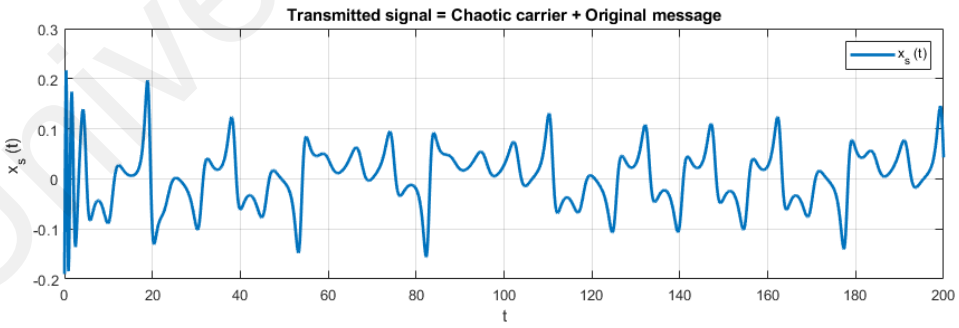


Figure 4.29: State trajectories of MS (4.14) **and SS** (4.3) **system masked with signal message, of initial condition** $[-0.10, -0.10, -0.18]$ **and** $[-0.20, -0.20, -0.18]$ **with control input** (4.9) **and** $\alpha = 0.95$

Universiti Malaya

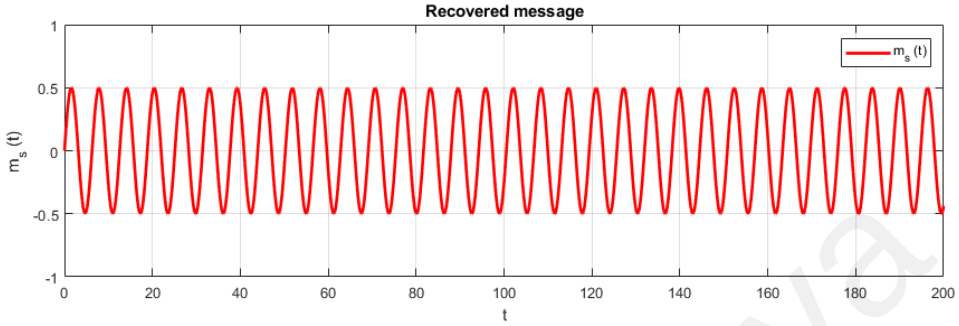


Figure 4.30: Recovered original signal message $0.5sin(n\pi)$

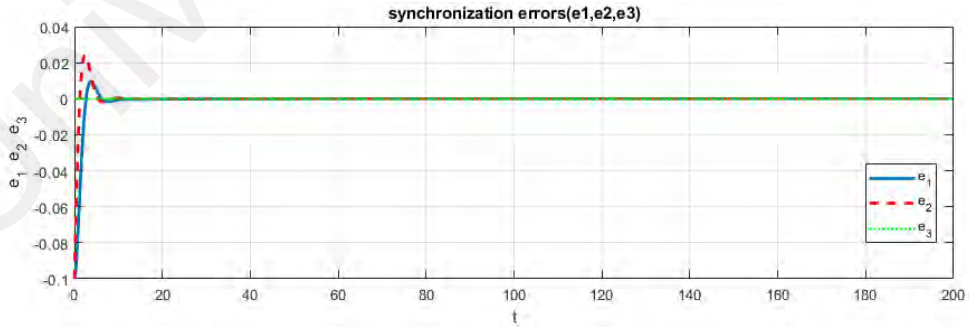


Figure 4.31: State trajectories of synchronization errors of masked signal message

Universiti Malaya

4.6 Conclusion

A comparative theoretical and experimental analysis of FONLS and CM has been performed in this chapter to explore the effects of various values of α on error synchronization. The experimental simulation results showed that $\alpha = 0.95$ is the minimum value for chaos to occur. In theoretical and numerical terms, the implementation of FONLS as MSSYS in a secure communication system based on CM is seen. The capability to recover the transmitted signal message is established under the noiseless condition by processing the signal message $0.5sin(n\pi)$ through the system. By comparing the graphs in Figure 4.28 and 4.30, one can determine that the initially transmitted signal message is recovered with appropriate precision.

Universiti Malaya

CHAPTER 5: SYNCHRONIZATION OF IONNS AND FONNS WITH TIME - DELAYS ACTIVE SMC

5.1 Introduction

In this chapter, we discussed about the problem of two chaotic NNs with different value of fractional-order. To resolve the synchronization's problem of IONNs and FONNs, an active SMC scheme is introduced. Factional-Order Lyapunov Direct Method (FLDM) is designed and is enforced to active SMC of the systems to keep the stability of the systems. To investigate the characteristics of IONNs and FONNs, we tend to enforce the method of numerical simulation by utilizing MATLAB programming to demonstrate the performance and efficiency of the results. Based on this study, the results show that the synchronization between integer-order and fractional-order will significantly occur once the recommended active SMC is introduced. This main result can provide a great advantage within the area of network security of secure communication by implementation of DES.

5.2 The Model's System.

The following is the master system of FONNs denoted by

$$D^{\alpha}\chi_i(t) = -q_i\chi_i(t) + \sum_{l=1}^{m}\sum_{a=1}^{c} u_{ikj} f_k(\chi_k(t)) + \sum_{l=1}^{m}\sum_{p=a}^{c} v_{ikj} f_k(\chi_k(t-\tau)) + \Gamma_i, \quad (5.1)$$

Or the vector form

$$D^{\alpha}\chi(t) = -Q\chi(t) + Uf(\chi(t)) + Vf(\chi(t-\tau)) + \Gamma, \quad (5.2)$$

Where D^{α} denotes as Caputo Fractional Derivative (CapFD) and $0 \leq \alpha \leq 1$. The state vector denoted by $\chi(t) \in R^n$ denotes $f(.)$ as the activation feature. While the constant matrices is represent by C, U and V, the external vector is indicated as Γ. The default state

Universiti Malaya

of (5.1) is expressed by:

$$\chi_i(r) = \varphi_i(r), \quad r \in [-\tau, 0], \quad i = 1, 2, \cdots, n \tag{5.3}$$

where $\varphi_i(r) \in C([-\tau, 0], R)$, and the norm, $||\varphi|| = \sup_{r\epsilon[-\tau,0]} \sum_{i=1}^{n} \varphi_i(r)$. The output of the system (5.2) is denoted by $(\mathfrak{Z}(t), \chi(t)) := \Xi_1\chi(t) + \Xi_2\chi(t-\tau)$, where $\Psi(\mathfrak{Z}(t), \chi(t)) \in R^m$ is the output state vector and $\Xi_1, \Xi_2 \in R^{m\times c}$ are the constant matrices. The equivalent system for slaves is defined as

$$D^{\alpha}\mathfrak{Z}(t) = -Ez(t) + Bg(\mathfrak{Z}(t)) + Tg(\mathfrak{Z}(t-\tau)) + J + \Theta(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t)), \tag{5.4}$$

Where $z(t) \in R^n$ denotes the state vector, while E, B and H are represented in the constant matrices. The SMC we want to build is portrayed as $\Theta(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t))$. The primary states of (5.4) are represented as

$$z_i(r) = \psi_i(r), \quad r \in [-\tau, 0], \quad i = 1, 2, \ldots, n,$$

where $||\psi|| = sup_{r\epsilon[-\tau,0]} \sum_{i=1}^{n} \psi_i(r)$.

Definition 5.2.1 *"(C. Li & Deng, 2007) The basis of the system* (5.1) *is unchanging if*

$$||\chi(t)|| = \left\{\Re(\chi(t_0))\, E_q(-\delta(t-t_0)^q)\right\}^{\sigma},\text{"} \tag{5.5}$$

Lemma 5.2.1 *(Stamova, 2014) Assume that the upper right-hand derivative of function v in Caputo's sense of order* $\alpha(0 < \alpha < 1)$ *with respect to time variable is such that for*

Universiti Malaya

$t \in [t_0, \infty)$, $\varphi \in PC[-\tau, 0], R^n]$, $\varsigma \in R$ *is a constant, and the following inequality*

$$D_+^{\alpha} v(t, \emptyset(t)) \leq \varsigma v(t, \emptyset(0)),$$

where t_0 *denotes the initial instant,* $q \in (0, 1)$, $\delta > 0$, $\sigma > 0$, $\Re(0) = 0$, $\Re(\chi) \geq 0$, *and* $\Re(\chi)$ *is locally Lipschiz on* $x \in R$ *with respect to Lipschitz constant* $\Re_0$.

Lemma 5.2.2 *"(C. Li & Deng, 2007) If* $f(t)$, $g(t) \in C^1[t_0, b]$, *then*

1. $D^{-\alpha} D^{-\beta} f(t) = D^{-\alpha-\beta} f(t)$, $\alpha, \beta \geq 0$;
2. $D^{\alpha} D^{-\alpha} f(t) = f(t)$, $\alpha \geq 0$;
3. $D^{-\alpha} D^{\alpha} f(t) = f(t) - \sum_{k=0}^{n-1} \frac{t^k}{k!} f^k(0)$, $\alpha \geq 0$.
4. $D^{\alpha}(v_1 f(t) + v_2 g(t)) = v_1 D^{\alpha} f(t) + v_2 D^{\alpha} g(t)$, v_1 *and* v_2 *are any constants.*
5. $D^{\alpha} c = 0$, c *is any constant."*

5.3 Synchronization of IONNs and FONNs with Active SMC

The method for the active SMC technique is implemented by combining SMC with ACC. Then we'll discuss the stability issue of the proposed system.

5.3.1 Method in Active SMC

A chaotic system by a nonlinear differential equation defined as follows:

$$\dot{\chi} = U_1 \chi + f_1(\chi), \tag{5.6}$$

Where the state vector is $\chi(t)$, the nonlinear function is $f_1(\chi)$, and U_1 represents a weight matrix of self-connection. The $\Theta(\chi(t))$ and $\Psi(\mathfrak{z}(t), \chi(t))$ controllers are substituted into

Universiti Malaya

SS (5.4) , such that:

$$D^{\alpha}{}_{\mathfrak{Z}}(t) = U_{2\mathfrak{Z}} + f_2(\mathfrak{Z}) + \Theta(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t)), \tag{5.7}$$

where $\mathfrak{Z}(t)$ is the state vector SS, U_2 represents the weight matrix of the self-connection, and $f_2(\mathfrak{Z})$ is the nonlinear function. The tracking controller is $\Phi(\chi(t)) + \Psi(z(t), \chi(t))$, and we define the tracking controller as:

$$\Theta(\chi(t)) = D^{\alpha}\chi(t) - f(\chi(t)) \tag{5.8}$$

The problem with the synchronization protocol is to construct a $\Theta(\chi(t))$ and $\Psi(\mathfrak{Z}(t), \chi(t))$ controller that synchronises both (5.1) and (5.4). The synchronization's EDS was expressed as follows:

$$\begin{aligned} D^{\alpha}\mathcal{E}(t) &= U_{2\mathfrak{Z}} + f_2(\mathfrak{Z}) - U_1 x + f_1(\chi) + \Theta(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t)) \\ &= U_2\mathcal{E} + F(\chi, \mathfrak{Z}) + \Theta(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t)) \end{aligned} \tag{5.9}$$

where

$$\mathcal{E}(t) = \mathfrak{Z}(t) - \chi(t)$$

$$F(\chi, \mathfrak{Z}) = f_2(\mathfrak{Z}) - f_1(\chi) + (U_2 - U_1)\chi$$

The purpose is to create the $\Theta(t) + \Psi(\mathfrak{Z}(t), \chi(t)$ controller in such a way that

$$\lim_{t\to\infty} ||\mathcal{E}(t)|| = 0$$

Following the design methodology of ACC by (D. Chen et al., 2012; Jia et al., 2018; Y. Li & Li, 2016), we used a control input of $\Theta(t) + \Psi(\mathfrak{Z}(t), \chi(t))$ to extract the nonlinear

Universiti Malaya

component of EDS. The following is the new input vector:

$$\Theta(t) + \Psi(\mathfrak{z}(t), \chi(t)) = H(t) - F(\chi, \mathfrak{z})$$

The (5.9) error system will then be rewritten as:

$$D^{\alpha}\mathcal{E}(t) = U_2\mathcal{E} + H(t) \tag{5.10}$$

Equation (5.10) is the newly described $H(t)$ control input of the EDS. There are numerous possibilities to choose from for the $H(t)$ control input. Finally, we choose the following law of SMC as:

$$H(t) = K\Theta(t) \tag{5.11}$$

Where a constant gain vector is $K = [k_1, k_2, k_3]^T$, and $\Theta(t)$ is the control input that meets the following condition:

$$\Theta(t) = \begin{cases} \Theta^{+}(t) & s(\mathcal{E}) \geq 0 \\ \Theta^{-}(t) & s(\mathcal{E}) < 0 \end{cases} \tag{5.12}$$

Then $s = s(\mathcal{E})$ is Switching Surface (SWS) where the error is displayed. The EDS is then defined as:

$$D^{\alpha}\mathcal{E} = U_2\mathcal{E} + K\Theta(t) \tag{5.13}$$

Then, based on the SMC principle, the suitable SMC will be drawn.

Universiti Malaya

5.3.2 Sliding Surface

The sliding surface is determined as

$$s\left(\mathcal{E}\right) = Q\mathcal{E}, \tag{5.14}$$

Where a constant vector is $Q = [q_1,\ q_2,\ q_3]$. We know that $\dot{s}\left(\mathcal{E}\right) = 0$ is an essential state to stay on SWS where the trajectory of the state is $s(\mathcal{E}) = 0$. So, another similar controller is generated, and there are two states must be followed by this controller which are:

$$\begin{aligned} s(\mathcal{E}) &= 0 \\ \dot{s}\left(\mathcal{E}\right) &= 0 \end{aligned} \tag{5.15}$$

We will obtain the following by using (5.13), (5.14) and (5.15):

$$\dot{s}\left(\mathcal{E}\right) = \frac{\partial s(\mathcal{E})}{\partial e}\dot{\mathcal{E}} = Q\left[U\mathcal{E} + K\Theta(t)\right] = 0 \tag{5.16}$$

by solving (5.16) for $\Theta(t)$ results in an identical control for $\Theta_{eq}(t)$ as follows:

$$\Theta_{eq}\left(t\right) = -(QK)^{-1}CU\mathcal{E}\left(t\right) \tag{5.17}$$

where the existence of $(QK)^{-1}$ is a necessary condition in the system. Substitution for $\Theta(t)$ in (5.13) from $\Theta_{eq}\left(t\right)$ of 5.12 will result the sliding mode state equation as follows:

$$D^{\alpha}\mathcal{E} = \left[I - K(QK)^{-1}C\right]U\mathcal{E} \tag{5.18}$$

Equation (5.18) is asymptotically stable if the system equation (5.13) has negative real parts for all eigenvalues.

Universiti Malaya

5.3.3 SMC

It is assumed that the constant plus proportional rate reaching law (5.16)-(5.18) is used. And we can choose the reaching law as:

$$\dot{s} = -q\ sgn(s) - rs, \tag{5.19}$$

where $sgn(.)$ is the sign function and the sliding condition is calculated by the r and q values, where $r > 0$ and $q > 0$, then the sliding mode motion occurred.

It is found, from (5.13) and (5.14), that;

$$\dot{s} = Q\left[U\mathcal{E} + K\Theta(t)\right], \tag{5.20}$$

Now, from (5.19) and (5.20), the control input is constructed as:

$$\Theta(t) = -(QK)^{-1}\left[Q(rI + U)\mathcal{E}(t) + q\ sgn(s)\right] \tag{5.21}$$

5.3.4 SMC with Time Delay

We let the MS as

$$D^{\alpha_0}\chi(t) = -Q\chi(t) + Uf(\chi(t)) + Vf(\chi(t-\tau)) + \Gamma$$

and, we rewrite equation (5.4) as

$$D^{\alpha}\mathfrak{Z}(t) = -Ez(t) + Bg(\mathfrak{Z}(t)) + Tg(\mathfrak{Z}(t-\tau)) + J + D^{\alpha_0}\chi(t) - f(\chi(t)) + \Psi(\mathfrak{Z}(t), \chi(t)) \tag{5.22}$$

where

$$f(\chi(t)) = -E\chi(t) + Bg(\chi(t)) + Tg(\chi(t-\tau)).$$

Universiti Malaya

Synchronization errors are denoted as $\mathcal{E}(t) = \mathfrak{z}(t) - \chi(t)$. The error is determined from the subtraction of the equation (5.2) and the equation (5.4). And from the calculation the derivative synchronization error is represented as:

$$D^{\alpha}\mathcal{E}(t) = -E(\mathfrak{z}(t) - \chi(t)) + Bg(\mathfrak{z}(t) - \chi(t)) + Tg(\mathfrak{z}(t-\tau) - \chi(t-\tau)) + D^{\alpha_0}\chi(t) + Q\chi(t) - Uf(\chi(t)) - Vf(\chi(t-\tau)) + (J-\Gamma) + \Psi(\mathfrak{z}(t), \chi(t)) \tag{5.23}$$

where $\Phi(\mathcal{E}(t)) := g(\mathfrak{z}(t)) - g(\chi(t))$, $\Phi(\mathcal{E}(t-\tau)) := g(\mathfrak{z}(t-\tau)) - g(\chi(t-\tau))$. By applying Lemma 5.2.2, we have

$$\begin{aligned}\mathcal{E}(t) =& \mathcal{E}(0) + D^{-\alpha}[-E\mathcal{E}(t) + B\Phi(\mathcal{E}(t)) + T\Phi(\mathcal{E}(t-\tau)) + D^{\alpha_0}\chi(t) + Q\chi(t) \\ & - Uf(\chi(t)) - Vf(\chi(t-\tau)) + (J-\Gamma) + \Psi(\mathfrak{z}(t), \chi(t))]\end{aligned} \tag{5.24}$$

Based on the (5.24) which is a synchronization error, the Delayed Active Sliding Surface (DASS) is represented as

$$\begin{aligned}s(t) =& \mathcal{E}(t) + D^{-\alpha}[\Pi(\Xi_1\mathcal{E}(t) + \Xi_2\mathcal{E}(t-\tau) - \Psi(\mathfrak{z}(t), \chi(t))] \\ & - D^{-\alpha}[-Q\mathcal{E}(t) + B\Phi(\mathcal{E}(t)) + T\Phi(\mathcal{E}(t-\tau))].\end{aligned} \tag{5.25}$$

where $\Pi \in R^{q\times m}$ is a gain matrix.

$$\begin{aligned}s(t) =& \mathcal{E}(0) + D^{-\alpha}[(Q - E + \Pi\Xi_1)\mathcal{E}(t) + \Xi_2\mathcal{E}(t-\tau) + D^{\alpha_0}\chi(t) + Q\chi(t) \\ & - Uf(\chi(t)) - Vf(\chi(t-\tau)) + (J-\Gamma) + \Psi(\mathfrak{z}(t), \chi(t))]\end{aligned} \tag{5.26}$$

Then, we calculate the derivative of equation (5.26) as follows:

$$D^{\alpha}s(t) = D^{\alpha}\mathcal{E}(0) + D^{\alpha}D^{-\alpha}[(Q - E + \Pi\Xi_1)\mathcal{E}(t) + \Xi_2\mathcal{E}(t-\tau) + D^{\alpha_0}\chi(t) + Q\chi(t) - Uf(\chi(t)) - Vf(\chi(t-\tau)) + (J-\Gamma) + \Psi(\mathfrak{z}(t), \chi(t))]$$

Universiti Malaya

$$=(Q - E + \Pi\Xi_1)\mathcal{E}(t) + \Xi_2\mathcal{E}(t-\tau) + D^{\alpha_0}\chi(t) + Q\chi(t) - Uf(\chi(t))$$

$$- Vf(\chi(t-\tau)) + (J - \Gamma) + \Psi(\mathfrak{Z}(t), \chi(t)). \tag{5.27}$$

The DASS theory and the derivative of delayed active SMC must satisfy the fact that $s(t) = 0$ and $\dot{s}(t) = 0$. Besides, we can gain $\dot{s}(t) = D^{\alpha}D^{-\alpha}s(t)$. by using Lemma 5.2.2. So, the equivalent of $\dot{s}(t) = 0$ is $D^{\alpha}s(t) = 0$. Thus, by statute, we can define delayed SMC as:

$$\Psi_1(\mathfrak{Z}(t), \chi(t)) = -(Q - E + \Pi\Xi_1)\mathcal{E}(t) - \Xi_2\mathcal{E}(t-\tau) - D^{\alpha_0}\chi(t) - Q\chi(t) + Uf(\chi(t))$$

$$+ Vf(\chi(t-)) - J + \Gamma \tag{5.28}$$

Equation (5.23) and equation (5.28) is solved and, then we defined error of delayed SMC as:

$$D^{\alpha}\mathcal{E}(t) = -(Q + \Pi\Xi_1)\mathcal{E}(t) - \Xi_2\mathcal{E}(t-\tau) + B\Phi(\mathcal{E}(t)) + T\Phi(\mathcal{E}(t-\tau)). \tag{5.29}$$

Therefore, we can assume that the equation (5.29) is the equilibrium point of $\mathcal{E} = 0$. An approaching law is defined from the theory of delayed SMC such that:

$$\Psi_2(\mathfrak{Z}(t), \chi(t)) = -K[sgn(s(t)] \tag{5.30}$$

where $s(t) = [\zeta_1(t), \zeta_2(t), \ldots, \zeta_n(t)]^T$ and the switching gain is $k > 0$. We express $sgn(\zeta_i(t))$ as follows:

Universiti Malaya

$$sgn(\zeta_i(t)) = \begin{cases} -1 & ,\zeta_i(t) < 0 \\ 0 & ,\zeta_i(t) = 0 \\ 1 & ,\zeta_i(tt) > 0 \end{cases}$$

Finally, delayed SMC of $\Psi(\mathfrak{Z}(t), \chi(t))$ is denoted by:

$$\begin{aligned} \Psi(\mathfrak{Z}(t), \chi(t)) &= \Psi_1(\mathfrak{Z}(t), \chi(t)) + \Psi_2(\mathfrak{Z}(t), \chi(t)) \\ &= -(Q - E + \Pi\Xi_1)\mathcal{E}(t) - \Xi_2\mathcal{E}(t-\tau) - D^{\alpha_0}\chi(t) - Q\chi(t) + Uf(\chi(t)) \\ &\quad + Vf(\chi(t-\tau)) - J + \Gamma - K[sgn(s(t)] \end{aligned} \tag{5.31}$$

There is a discontinuous function which is $sgn(\cdot)$ in the equation (5.31) that may initiate some dangerous noise. We will then replace the discontinuous function $sgn(\cdot)$ with the continuous function $tanh(\cdot)$ to avoid the risk. The modified equation (5.31) is then represented as:

$$\begin{aligned} \Psi(\mathfrak{Z}(t), \chi(t)) &= \Psi_1(\mathfrak{Z}(t), \chi(t)) + \Psi_2(\mathfrak{Z}(t), \chi(t)) \\ &= -(Q - E + \Pi\Xi_1)\mathcal{E}(t) - \Xi_2\mathcal{E}(t-\tau) - D^{\alpha_0}\chi(t) - Q\chi(t) + Uf(\chi(t)) \\ &\quad + Vf(\chi(t-\tau)) - J + \Gamma - K[tanh(s(t)] \end{aligned} \tag{5.32}$$

The law of exponential convergence is alternatively as follows:

$$\dot{s}(t) = -\varepsilon sgn(s(t)) - \omega s(t).$$

If we use a smaller value of ε and a larger value of ω, the method has the advantages of fast transition time.

Theorem 5.3.1 *"Suppose that the delayed sliding switching surface defined by* (5.25) *holds,*

Universiti Malaya

based on the delayed sliding mode control (5.31)*, the trajectories of the synchronization error* (5.21) *can be asymptotically reached against the delayed sliding switching surface* $s(t) = 0$*." (Stamova & Stamov, 2017)*

Proof. We define the quadratic function of Lyapunov as;

$$v(t) = \frac{1}{2}s(t)\dot{s}(t), \tag{5.33}$$

From the Lemma 5.2.1, by evaluating the CapFD of $v(t)$ relative to time t, along the equation (5.25) trajectories, one determines that;

$$\begin{aligned}
\dot{v}(t) =& s(t)\dot{s}(t) \\
=& s(t)[(Q - E + \Pi\Xi_1)\mathcal{E}(t) + \Pi\Xi_2\mathcal{E}(t-t) + D^{q_0}\chi(t) + Q\chi(t) - Uf(\chi(t)(t)) \\
& - Vf(\chi(t)(t-t)) + (J - \Gamma) + \Psi(\eth(t), \chi(t)(t))] \\
=& s(t)[-K[sgn(s(t)]] \\
=& -K \cdot |s(t)|,
\end{aligned} \tag{5.34}$$

The system must asymptotically converge to $s(t) = 0$ if $K > 0$. This implies that the equation (5.24) is globally reached on the delayed active SWS. This ensures the proof completed.

Theorem 5.3.2 *"Suppose that* (H) *holds. Assume that there exist positive constants* m_i *and li such that* $m_i = max\left\{\left|m_i^-\right|, \left|m_i^+\right|\right\}$ *,* $l_i = max\left\{\left|l_i^-\right|, \left|l_i^+\right|\right\}$ *, and constant matrices* Π*,* Ξ_1 *and* Ξ_2 *such that* $\Pi = (\pi_{jl})_{a\times m}$*,* $\Xi_1 = (\varphi_{li})_{m\times a}$*,* $\Xi_2 = (\vartheta_{li})_{m\times a}$ *and" (Stamova & Stamov, 2017).*

Universiti Malaya

$$\begin{cases} \gamma_1 := \min_{1\le i\le c}\left[q_i - \sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left(\left|\pi_{jl}\varphi_{li}\right|\right)\right) - \sum_{l=1}^{m}\sum_{a=1}^{c}\left(\left|b_{ji}\right| m_i\right)\right] > 0 \\ \gamma_2 := \max_{1\le i\le c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left(\left|\pi_{jl}\vartheta_{li}\right|\right)\right) + \sum_{l=1}^{m}\sum_{a=1}^{c}\left(\left|h_{ji}\right| l_i\right)\right] > 0 \\ \gamma_1 - \gamma_2 > 0 \end{cases} \tag{5.35}$$

The original equation (5.29) is then stable.

Proof. We therefore modified equation (5.28), delayed synchronization error system to:

$$\begin{aligned} D^{\alpha}\mathcal{E}(t) = &- q_i x_i(t) + \sum_{l=1}^{m}\sum_{a=1}^{c}\left[\pi_{jl}\varphi_{li}\right]\mathcal{E}_j(t) + \sum_{l=1}^{m}\sum_{a=1}^{c}\left[\pi_{jl}\vartheta_{li}\right]\mathcal{E}_j(t-\tau) \\ &+ \sum_{l=1}^{m}\sum_{a=1}^{c} b_{ipl}\Phi\mathcal{E}_j(t) + \sum_{l=1}^{m}\sum_{a=1}^{c} h_{ipl}\Phi\mathcal{E}_j(t-\tau) \end{aligned} \tag{5.36}$$

We defined the Lyapunov function candidate by

$$\begin{aligned} D^{\alpha}v(t,\mathcal{E}(t)) &= \sum_{i=1}^{c} D_{+}^{\alpha}\left|\mathcal{E}_i(t)\right| \\ &\le \sum_{i=1}^{c} sgn\left(\mathcal{E}_i(t)\right) D_{+}^{\alpha}\mathcal{E}_i(t) \\ &\le -\sum_{i=1}^{c} Q_i\left|\mathcal{E}_i(t)\right| + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\pi_{jl}\varphi_{li}\right)\left|\mathcal{E}_j(t)\right|\right] \\ &\quad + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\pi_{jl}\vartheta_{li}\right)\left|\mathcal{E}_j(t-\tau)\right|\right] + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|b_{ikl}\right|\right)m_j\left|\mathcal{E}_j(t)\right|\right] \\ &\quad + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|h_{ikl}\right|\right)l_j\left|\mathcal{E}_j(t-\tau)\right|\right] \\ &= -\sum_{i=1}^{c} Q_i\left|\mathcal{E}_i(t)\right| + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\pi_{jl}\varphi_{li}\right)\right]\left|\mathcal{E}_j(t)\right| \\ &\quad + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\pi_{jl}\vartheta_{li}\right)\right]\left|\mathcal{E}_j(t-\tau)\right| + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|b_{ipl}\right|\right)m_j\right]\left|\mathcal{E}_j(t)\right| \\ &\quad + \sum_{i=1}^{c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|h_{ipl}\right|\right)l_j\right]\left|\mathcal{E}_j(t-\tau)\right| \\ &= -\sum_{i=1}^{c}\left[Q_i - \sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|\pi_{jl}\varphi_{li}\right|\right) - \sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|b_{ipl}\right|\right)m_j\right]\left|\mathcal{E}_j(t)\right| \\ &\quad + \sum_{i=1}^{q}\left[C_i - \sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|\pi_{jl}\vartheta_{li}\right|\right) - \sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left|h_{ipl}\right|\right)l_j\right]\left|\mathcal{E}_j(t-\tau)\right| \end{aligned}$$

Universiti Malaya

$$
\begin{aligned}
&\leq \min_{1\leq i\leq c}\left[Q_i-\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left(\left|\pi_{jl}\varphi_{li}\right|\right)\right)-\sum_{l=1}^{m}\sum_{a=1}^{c}\left(\left|b_{ji}\right|m_i\right)\right]-\sum_{i=1}^{c}\left|\mathcal{E}_j\left(t\right)\right| \\
&\quad+\max_{1\leq i\leq c}\left[\sum_{l=1}^{m}\left(\sum_{a=1}^{c}\left(\left|\pi_{jl}\vartheta_{li}\right|\right)\right)+\sum_{l=1}^{m}\sum_{a=1}^{c}\left(\left|h_{ji}\right|l_i\right)\right]\sum_{i=1}^{c}\left|\mathcal{E}_j\left(t-\tau\right)\right| \\
&\leq \gamma_1 V\left(t,\mathcal{E}\left(t\right)\right)+\gamma_2\sup_{t-\tau\leq s\leq t}V\left(s,\mathcal{E}\left(s\right)\right) \qquad (5.37)
\end{aligned}
$$

As a consequence of any $\mathcal{E}_i(t)$ of error system (5.36) that satisfies the Razumikhin condition, one has;

$$
\sup_{t-\tau\leq s\leq t} v\left(s,\mathcal{E}\left(s\right)\right)\leq v\left(t,\mathcal{E}\left(t\right)\right) \qquad (5.38)
$$

Then, based on (5.37), (5.38) and Theorem 5.3.2, it is assumed that there is a constant $\delta > 0$, one has

$$
\begin{cases}
D_{+}^{\alpha}v\left(t,\mathcal{E}\left(t\right)\right)\leq-\left(\gamma_1-\gamma_2\right)v\left(t,\mathcal{E}\left(t\right)\right) \\
\gamma_1-\gamma_2\geq\delta
\end{cases} \qquad (5.39)
$$

and from (5.39), one observes that

$$
D_{+}^{\alpha}v\left(t,\mathcal{E}\left(t\right)\right)\leq\delta v\left(t,\mathcal{E}\left(t\right)\right) \qquad (5.40)
$$

Then from (5.40) and Lemma 5.2.1,

$$
v\left(t,\mathcal{E}\left(t\right)\right)\leq v\left(0\right)E_{\alpha}\left(-\delta t^{\alpha}\right) \qquad (5.41)
$$

So,

$$
\begin{aligned}
\left\|\mathcal{E}\left(t\right)\right\| &= \left\|\beth_i\left(t\right)-x\left(t\right)\right\| \\
&= \sum_{i=1}^{n}\left\|\beth_i\left(t\right)-x\left(t\right)\right\| \qquad (5.42) \\
&\leq \left\|\Psi_o-\emptyset_0\right\|E_{\alpha}\left(-\delta t^{\alpha}\right)
\end{aligned}
$$

It is noted that if $\mathcal{E}=0$ the stabilisation of the equilibrium point is stable. This is

Universiti Malaya

evidence that the equation (5.29) is stable as $\|\mathcal{E}(t)\| \rightarrow 0$ and$(t \rightarrow +\infty)$, the is stable. This summarises the proof. ■

5.4 Numberical Example and Simulations

In this section, the suggested idea with numerical examples is revealed to justify the proposed model's effectiveness. The Euler method was used in numerical simulations to solve the 0.005 time step size.

Case 1. Consider equation (5.2) as MS,and equation (5.4) as SS and controller equation (5.32) with the following parameters:

Where $\alpha = 0.98$, $\tau = 0.5$, $f(\chi(t)) = tanh(\chi(t))$, $g(\mathfrak{z}(t)) = tanh(\mathfrak{z}(t))$, $\Xi_1 = (0, 1, 0)$, $\Xi_2 = (0, 1, 0)$, $\Gamma = (0, 0, 0)^T$, $J = (0, 0, 0)^T$,

$$Q = \begin{bmatrix} -9.5 & 0 & 0 \\ 0 & -10.5 & 0 \\ 0 & 0 & -3.7 \end{bmatrix}, U = \begin{bmatrix} 2 & 0.5 & 5.5 \\ 0.5 & 0.5 & 5.1 \\ 0.5 & 1 & -5.5 \end{bmatrix}, V = \begin{bmatrix} 7 & 7 & 4.1 \\ 1 & 1 & 2.5 \\ 0.1 & -10.1 & 4.5 \end{bmatrix}$$

$$E = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -7.7 \end{bmatrix}, B = \begin{bmatrix} 0.01 & 0.3 & 7.5 \\ 0.01 & 0.5 & 7.5 \\ 0.01 & 3 & -5.5 \end{bmatrix}, T = \begin{bmatrix} 0.3 & 5.5 & 5.5 \\ 0.5 & 2.5 & 5.5 \\ 0.1 & -1.5 & 1.5 \end{bmatrix}$$

As we understand, the MS are in the IO form, so the α_0 value is 1. Using MATLAB tools, the numerical simulation technique is presented here and the graphical analysis displays the findings using this tools. To do so, IONNs controls equation (5.2) and FONNs controls equation (5.4). The initial state of (5.2) is displayed as $(\chi_1(0), \chi_2(0), \chi_3(0)) = (0.1, 0.3, -0.1)$, whereas the initial state of (5.4) is $(\mathfrak{z}_1(0), \mathfrak{z}_2(0), \mathfrak{z}_3(0)) = (0.1, 1.2, 0.1)$. The results of the simulation are shown in figures (5.7 - 5.9) showing the state trajectories of the control

Universiti Malaya

Table 5.1: Synchronization error for different value of fractional-order

	$\alpha = 0.99$	$\alpha = 0.98$	$\alpha = 0.97$	$\alpha = 0.96$	$\alpha = 0.95$
$\alpha_0 = 1$	Infeasible	159.785	160.335	160.260	162.155

input MSSYS.

The error dynamical system (5.29) is asymptotically synchronised by the theorem (5.3.2). The simulation results are displayed in Figures 5.11 and Figures 5.10 with and without control of the controller built in equation (5.32), respectively.

Case 2. Consider master system (5.2), slave system (5.4) and controller (5.32) with the same parameters in Case 1. For this case the SS are in the form of IO, so the value for α is 1 and the value of α for MS is in FO. From the Figure 5.20, one can seen that the error of synchronization not converge to zero, and we can conclude that Case 2 is not suitable.

Remark 5.4.1 *For the values of* α *such as* $\alpha = 0.98$, $\alpha = 0.97$, $\alpha = 0.96$ *and* $\alpha = 0.95$ *are chosen as the master system* (5.2). *We can seen that all the results are infeasible. Table 5.2.*

Universiti Malaya

Table 5.2: Synchronization error for fixed value of fractional-order

	$\alpha_0 = 0.99$	$\alpha_0 = 0.98$	$\alpha_0 = 0.97$	$\alpha_0 = 0.96$	$\alpha_0 = 0.95$
$\alpha = 1$	Infeasible	Infeasible	Infeasible	Infeasible	Infeasible

Remark 5.4.2 *Chaotic behaviour of the system* (5.2) *and* (5.4) *with control inputs and without control inputs illustrared in Figures 5.1 and 5.2 respectively. From the simulation results (Figures 5.12 - 5.14), it can be seen that when values of* α *decreases such as* $\alpha = 0.98$, $\alpha = 0.97$, $\alpha = 0.96$ *and* $\alpha = 0.95$ *with the control input, the time taken for synchronization error is increasing and it is globally asymptotically stable. From this, we confirm that the dynamical behaviour of the system is very sensitive to the values of* α*. Furthermore, the synchronization error of converge to zero and one can easily show that the* $\alpha = 0.98$ *is chosen. We obtain the time taken for synchronization to archive with different values of* α *as listed in the Table 5.1. The time segment of* $T = 200$ *for error synchronization are chosen. While Figure 5.25 illustrates the state trajectories of systems* (5.2), (5.4) *and synchronization error of* $\alpha = 0.99$ *which are not converge to zero with control input.*

Remark 5.4.3 *Chaotic behaviour of the system* (5.2) *without the synchronization illustrated in Figure 5.3*

Remark 5.4.4 *From the simulation results, Figures (5.4 - 5.6) which show the state trajectories of MS* (5.2) *and SS* (5.4) *without control input and* $\alpha = 0.98$*. Figure illustrates the state trajectories of error dynamical system which are not converge to zero without control input.*

5.5 Conclusion

In conclusion, it shown that the results obtained from the synchronization of IONNs and FONNs will give the fast convergence of synchronization error as the value of α approach

Universiti Malaya

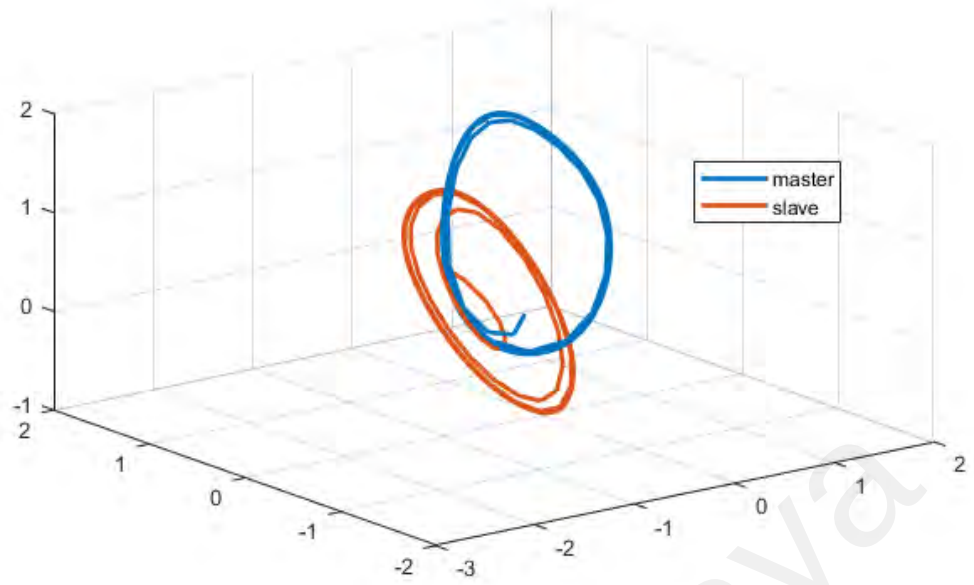


Figure 5.1: Chaotic attractor of MS (5.2) **and SS** (5.4) **without control inputs** (5.2) **after the synchronization and** $\alpha = 0.98$

to integer-order. We also conclude that in order for the synchronization of MSSYS to occurs, one have to confirm that the MS must in interger-order and SS in fractional-order. It is infeasible to get the error of synchronization converge to zero if the slave system in integer order. Our expected outcomes of this chapter can be approximately summed up as follows: Based on the Lyapunov direct method, the synchronization of FO and IO chaotic systems is discussed.

Based on this chapter, we will introduce a new concept that combines NNs synchronization with a symmetrical algorithm, and we call this combination double encryption, to enhance the level of security of chaos-based cryptography that will provide solid security. The concept is shown in the next chapter.

Universiti Malaya

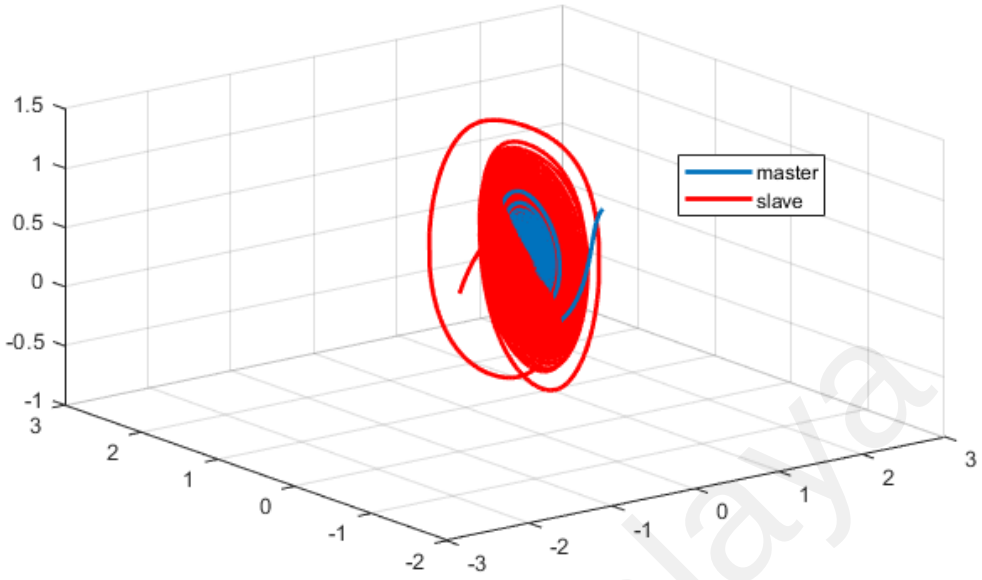


Figure 5.2: Chaotic attractor of MS (5.2) **and SS** (5.4) **with control inputs** (5.2) **after the synchronization and** $\alpha = 0.98$

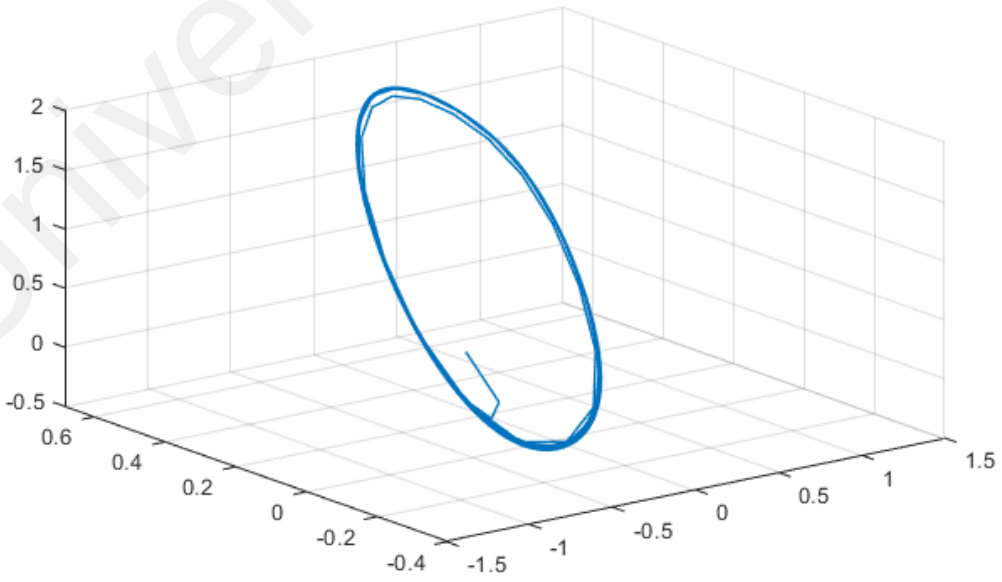


Figure 5.3: Chaotic attractor of MS (5.2) **without the synchronization**

Universiti Malaya

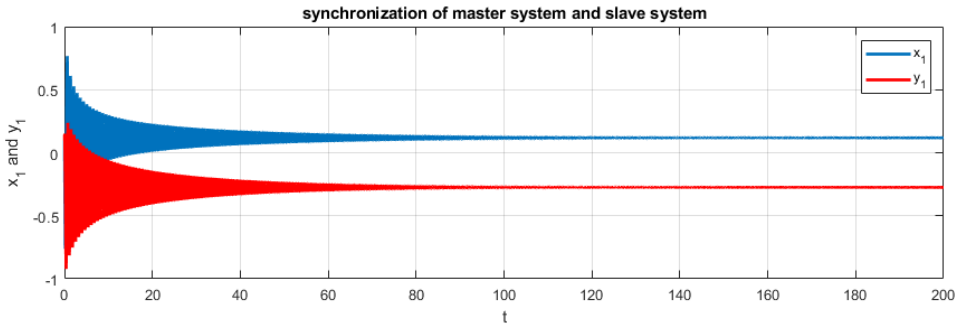


Figure 5.4: State trajectories of MSSYS χ_1, $\mathfrak{z}_1$ without control input and $\alpha = 0.98$

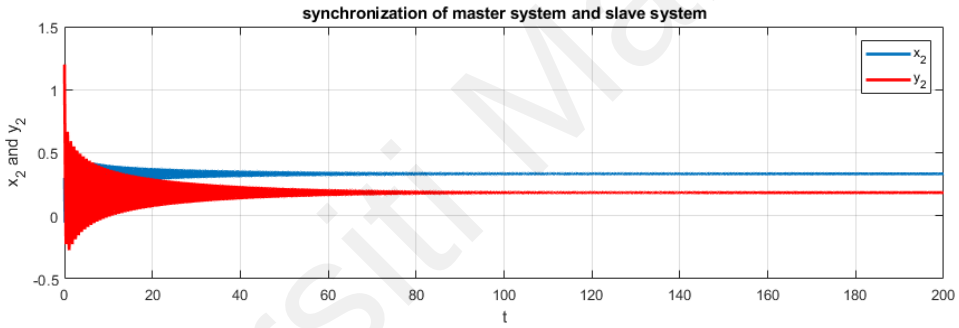


Figure 5.5: State trajectories of MSSYS χ_2, $\mathfrak{z}_2$ without control input and $\alpha = 0.98$

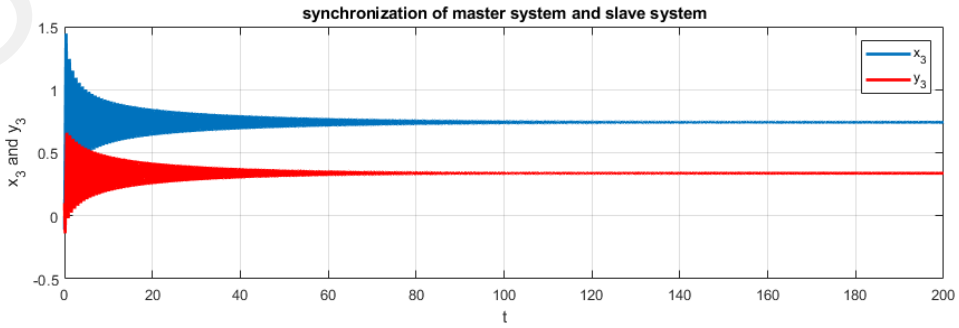


Figure 5.6: State trajectories of MSSYS χ_3, $\mathfrak{z}_3$ without control input and $\alpha = 0.98$

Universiti Malaya

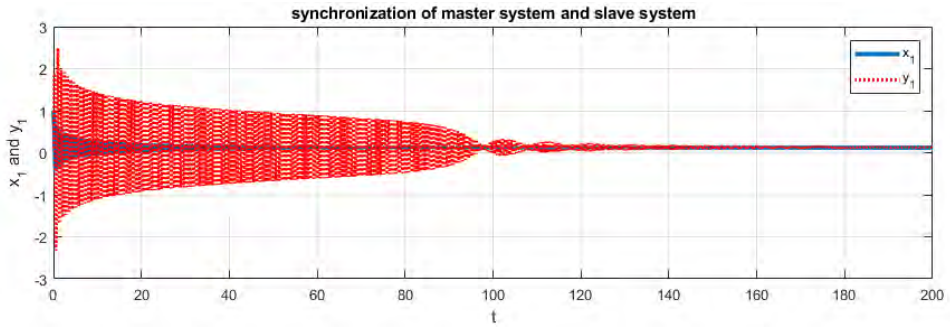


Figure 5.7: State trajectories of MSSYS χ_1, $\mathfrak{z}_1$ with control input and $\alpha = 0.98$

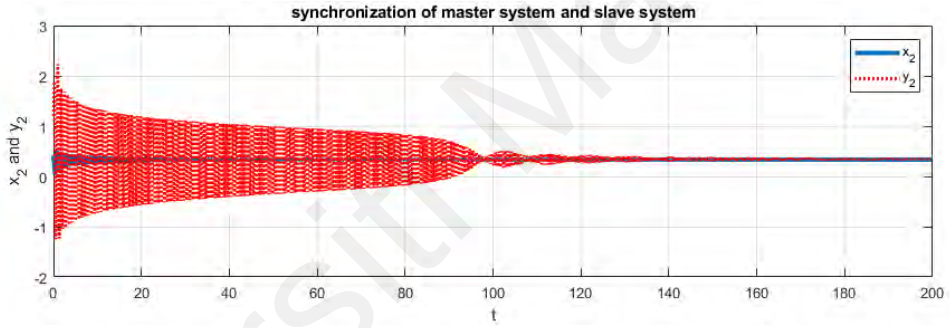


Figure 5.8: State trajectories of MSSYS χ_2, $\mathfrak{z}_2$ with control input and $\alpha = 0.98$

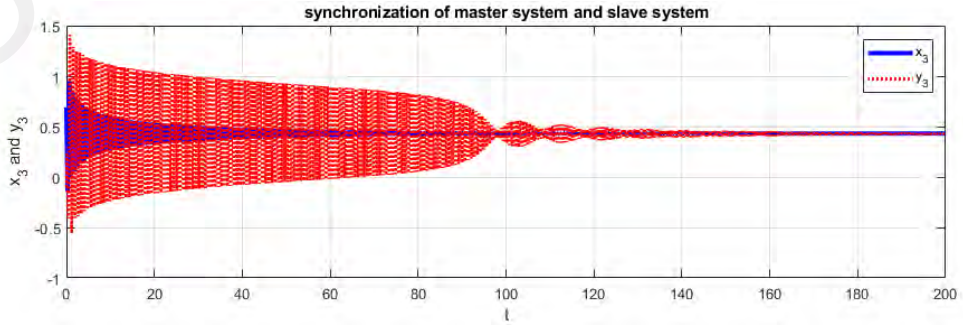


Figure 5.9: State trajectories of MSSYS χ_3, $\mathfrak{z}_3$ with control input and $\alpha = 0.98$

Universiti Malaya

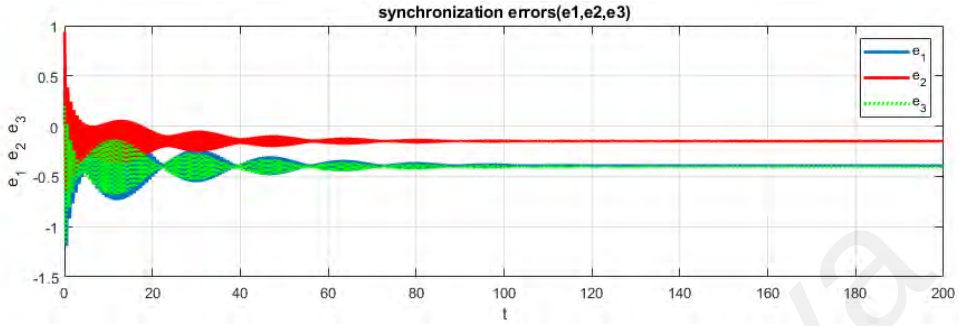


Figure 5.10: State trajectories of synchronization errors without control input and $\alpha = 0.98$

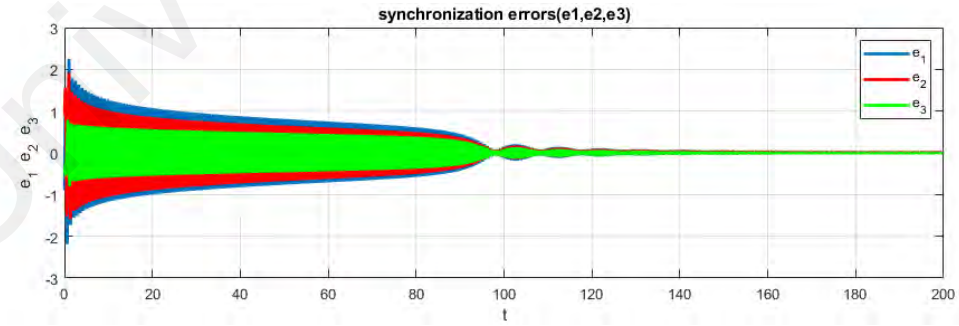
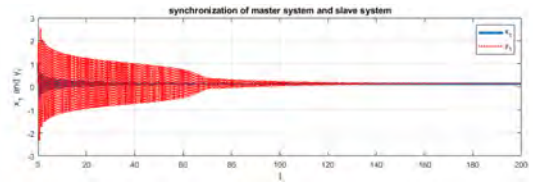
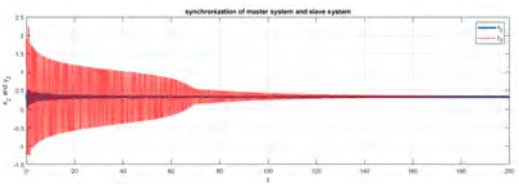


Figure 5.11: State trajectories of synchronization errors with control input and $\alpha = 0.98$

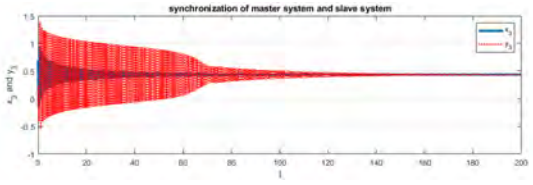
Universiti Malaya



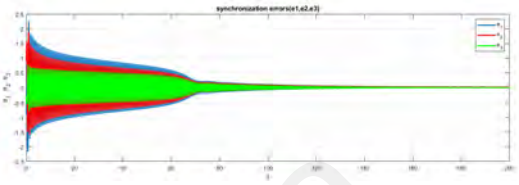
(a) χ_1 and $\mathfrak{z}_1$



(b) χ_2 and $\mathfrak{z}_2$

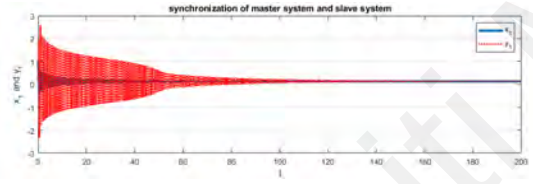


(c) χ_3 and $\mathfrak{z}_3$

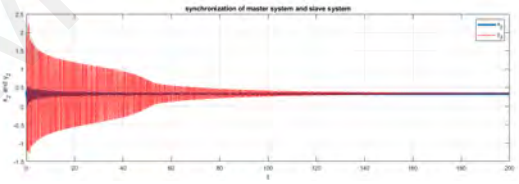


(d) synchronization errors e_1, e_2, e_3

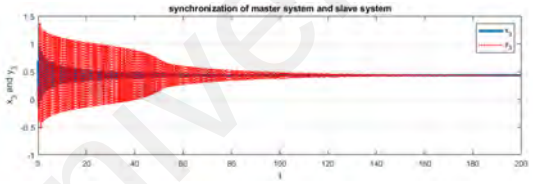
Figure 5.12: State trajectories of MSSYS χ_1, χ_2, χ_3, $\mathfrak{z}_1$, $\mathfrak{z}_2$, $\mathfrak{z}_3$ and synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ with control input and $\alpha = 0.97$



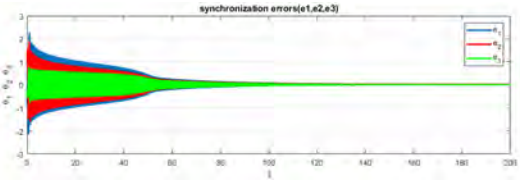
(a) χ_1 and $\mathfrak{z}_1$



(b) χ_2 and $\mathfrak{z}_2$



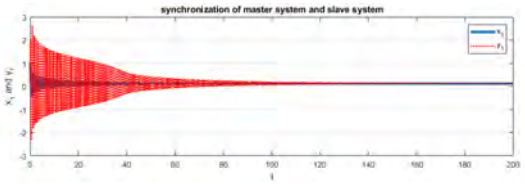
(c) χ_3 and $\mathfrak{z}_3$



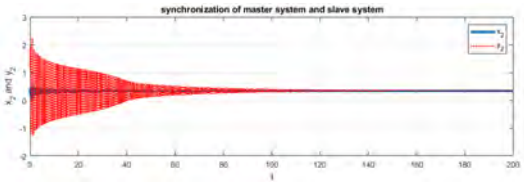
(d) synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$

Figure 5.13: State trajectories of MSSYS χ_1, χ_2, χ_3, $\mathfrak{z}_1$, $\mathfrak{z}_2$, $\mathfrak{z}_3$ and synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ with control input and $\alpha = 0.96$

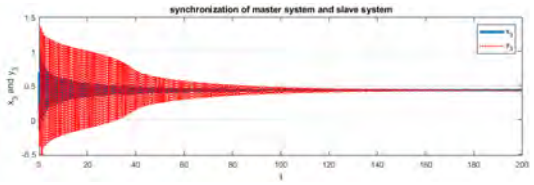
Universiti Malaya



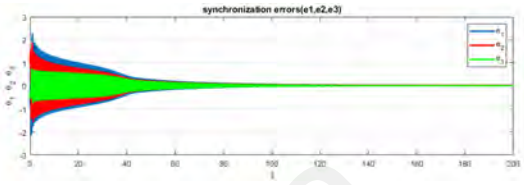
(a) χ_1 and $\mathfrak{z}_1$



(b) χ_2 and $\mathfrak{z}_2$



(c) χ_3 and $\mathfrak{z}_3$



(d) synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$

Figure 5.14: State trajectories of MSSYS χ_1, χ_2, χ_3, $\mathfrak{z}_1$, $\mathfrak{z}_2$, $\mathfrak{z}_3$ and synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ with control input and $\alpha = 0.95$

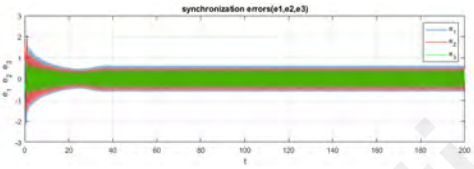


Figure 5.15: $\alpha = 0.99$

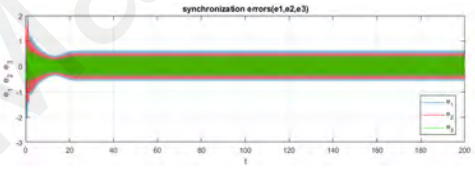


Figure 5.16: $\alpha = 0.98$

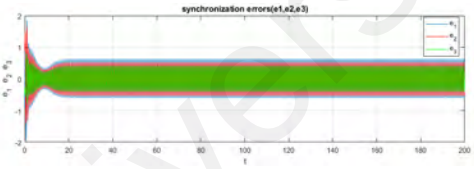


Figure 5.17: $\alpha = 0.97$

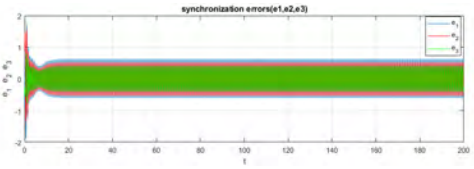


Figure 5.18: $\alpha = 0.96$

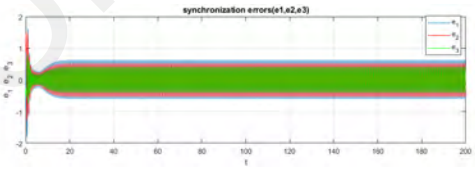


Figure 5.19: $\alpha = 0.95$

Figure 5.20: State trajectories of d synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ with control input and the SS (5.4) **of $\alpha = 1$, MS** (5.2) **with different values of α.**

Universiti Malaya

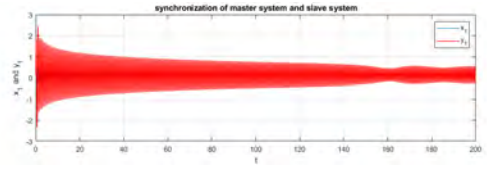


Figure 5.21: χ_1 **and** $\mathfrak{z}_1$

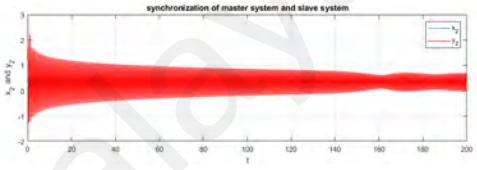


Figure 5.22: χ_2 **and** $\mathfrak{z}_2$

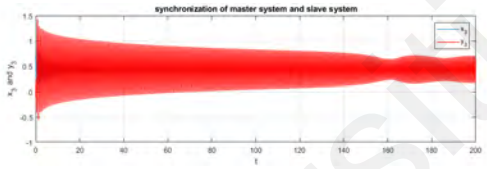


Figure 5.23: χ_3 **and** $\mathfrak{z}_3$

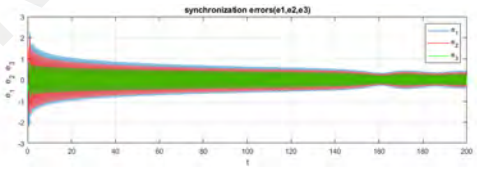


Figure 5.24: synchronization errors $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$

Figure 5.25: State trajectories of MSSYS χ_1, χ_2, χ_3, $\mathfrak{z}_1$, $\mathfrak{z}_2$, $\mathfrak{z}_3$ **and synchronization errors** $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ **with control input and** $\alpha = 0.99$**.**

Universiti Malaya

CHAPTER 6: SYNCHRONIZATION OF PFONNS COMBINED WITH SYMMETRIC ENCRYPTION FOR SECURE COMMUNICATION

6.1 Introduction

This chapter's main objective is to introduce a way to combine the synchronization of PFONNs with symmetric encryption to form a stable private communication system. PFONNs synchronization can be accomplished with different MSSYS initial conditions with the specified values of parameters. It should also be noted that with several time delays, the conventional Lyapunov functional method cannot be applied to FONNs, but FO Lyapunov functional method stability theorems are more applicable. This combination is called the third generation of chaotic secure communication proposed by (T. Yang et al., 1997). Their idea was to improve the degree of security to a higher level than the older generations. This generation has the highest security among the other generations of chaotic secure communication systems, and most secure communication has used this cryptosystem because of its advantages. They are its fast sending of the message and its easy execution (Ghosh et al., 2007). Another name for this combination is called double encryption. Here, the combination of the symmetric encryption technique and chaotic FO synchronization is used to enhance the degree of security.

There are four significant aspects to the key contributions of this chapter. First, to achieve the PFONNs, a new controller is designed. Second, two new synchronization conditions of PFONNs are proposed here, based on the time delays of linear FO calculus system's stability theorem. Third, double encryption is being created, combining symmetric encryption with PFONNs. Finally, our studies will achieve a significant enhancement compared to previous works and provide quit self-belief to say that the results found are far less conventional and more universal.

Universiti Malaya

6.2 The Model's System

Two definitions of the most common FO calculus derivatives used are mentioned in the literature: the Riemann-Liouville Fractional Derivative (RLFD) and the CapFD. In this work, the Caputo Derivativel (CapD) is implemented because it is possible to give its initial conditions in terms of IO derivatives, which is more practical in actual problems.

Definition 6.2.1 *"(Podlubny, 1998) The fractional derivative of Caputo of order α for a function u(t) is defined by:*

$$\mathcal{D}^{a}u\left(t\right)=\frac{1}{\Gamma(m-a)}\int_{0}^{t}\left(t-t\right)^{m-a-1}u^{(m)}\left(t\right)dt \tag{6.1}$$

where $t \geq t_0$, m is the integer, $m-1 < \alpha < m$, $\Gamma(\cdot)$ is the Gamma function, $\Gamma(s)=\int_0^{\infty}t^{s-1}e^{-t}\,dt$."

In this chapter, we consider the following NNs, which is called PFONNs considered as the MSS is denoted as

$$\mathcal{D}^{\alpha}x_i\left(t\right)=-c_i x_i\left(t\right)+\sum_{j=1}^{n}a_{ij}f_j\left(x_j\left(t\right)\right)+\sum_{j=1}^{n}g_{ij}f_j\left(x_j\left(t-t_i\right)\right)+\varphi_i \tag{6.2}$$

where $0 < \alpha < 1$, $i, j = 1, 2, \ldots, n$, n is the number of neurons in a NNs, $x_i(t)$ represents the ith neuron's pseudo state variable of the MS, $c_i > 0$ is the ith neuron's self-inhibition parameters. The external input of the ith neuron is $_j$, a_{ij} and g_{ij} denote the relation of the jth neuron with the ith neuron at time t and $t-t_j$, respectively, $t_j > 0$ is the delayed transmission, $f_j(x_j(t))$ and $f_j(x_j(t-t))$ denote the jth neuron's activation function output at time t and $t-t_j$, respectively. Equation 6.2 can be written in the vector form:

$$\mathcal{D}^{\alpha}x\left(t\right)=-CX\left(t\right)+Af_c\left(x\left(t\right)\right)+Gf_c\left(x(t-\tau_i)\right)+\varphi \tag{6.3}$$

Universiti Malaya

The corresponding SS is denoted as

$$\mathcal{D}^{\alpha} y_i(t) = -d_i y_i(t) + \sum_{j=1}^{n} b_{ij} g_j\left(y_j(t)\right) + \sum_{j=1}^{n} h_{ij} g_j\left(x_j(t-\tau_i)\right) + \mu_i + \nu_i(t) \qquad (6.4)$$

where $0 < \alpha < 1$, $i, j = 1, 2, \ldots, n$, n is the number of neuron in a NNs, $y_i(t)$ represents the ith neuron's pseudo state variable of the SS, $d_i > 0$ is the ith neuron's self-inhibition parameters. $_j$ represents the external input of the ith neuron, b_{ij} and h_{ij} denote the relation of the jth neuron with the ith neuron at time t and $t - t_j$, respectively, $t_j > 0$ is the delayed transmission, $g_j(x_j(t))$ and $g_j(x_j(t-t))$ denote the jth neuron's activation function output at time t and $t - t_j$, respectively. While $\nu_i(t)$ is an appropriate controller.

For simplification, in the next part, definition and lemmas are given.

Definition 6.2.2 *(Yu et al., 2014) If there exist a nonzero constant ρ, such that for any two solutions $x(t)$ and $y(t)$ of systems* (6.2) *and* (6.4) *with different initial values, one can get:*

$$\lim_{t \to +\infty} \| y(t) - \rho x(t) \| = 0 \qquad (6.5)$$

then the MS (6.2) and the SS (6.4) can achieve globally asymptotically in projective synchronization, where $\|\cdot\|$ represents the Euclidean norm of a vector.

Lemma 6.2.1 *(Aguila-Camacho et al., 2014) Suppose $x(t) \in R$ is a continuous differentiable vector-value function. Hence, for any time instant $t \geq t_0$, we have.*

$$D^{\alpha} x^T(t) x(t) \leq 2 x^T(t) D^{\alpha} x(t), \qquad (6.6)$$

where $0 < \alpha < 1$.

Universiti Malaya

6.3 Synchronization of PFONNs with Adaptive Control

Two identical PFONNs synchronization conditions are achieved in this section by designing a suitable controller. Defines the errors of synchronization as $\mathfrak{E}(t) = y_i(t) - \rho x_i(t)$, $(i = 1, 2, \ldots, n)$. Based on the MS (6.2) and SS (6.4), the control function $\nu_i(t)$, $(i = 1, 2, \ldots, n)$ can be selected as follows:

$$\begin{aligned}\nu_i(t) = &-\left[c_i + \left(\pi_{jl}\right)_{n\times m} \cdot (\omega_{li})_{m\times n} - d_i\right] \mathfrak{E}_j(t) - \left[\left(\pi_{jl}\right)_{n\times m} \cdot (\varepsilon_{li})_{m\times n}\right] \mathfrak{E}_j(t-\tau_i) \\ &- \rho(c_i - d_i) x_j(t) - \sum_{j=1}^{n} b_{ij} g_j\left[\rho x_j(t)\right] - \sum_{j=1}^{n} h_{ij} g_j\left[\rho x_j(t-\tau_i)\right] \\ &+ \rho \sum_{j=1}^{n} a_{ij} f_j\left[x_j(t)\right] + \rho \sum_{j=1}^{n} g_{ij} f_j\left[x_j(t)\right] - \rho\varphi_i + \mu_i\end{aligned} \tag{6.7}$$

where $i, j, n, m = 1, 2, \ldots, n$ and ρ is the projective coefficient.

From (6.2), (6.4) and (6.7), you can get the $\mathcal{D}^{\alpha}\mathfrak{E}(t)$ error system as follows:

$$\begin{aligned}\mathcal{D}^{\alpha}\mathfrak{E}(t) = &\, d_i e_i(t) + \sum_{j=1}^{n} b_{ij}\left[g_j\left(y_j(t)\right) - g_j\left(\rho x_j(t)\right)\right] \\ &+ \sum_{j=1}^{n} h_{ij}\left[g_j\left(y_j(t-\tau_i)\right) - g_j\left(\rho x_j(t-t)\right)\right] + \rho(c_i - d_i) x_j(t) \\ &+ \sum_{j=1}^{n} b_{ij}\left[g_j\left(x_j(t)\right)\right] + \sum_{j=1}^{n} h_{ij}\left[g_j\left(\rho x_j(t-\tau_i)\right)\right] \\ &- \rho \sum_{j=1}^{n} a_{ij}\left[f_j\left(x_j(t)\right)\right] - \rho \sum_{j=1}^{n} g_{ij}\left[f_j\left(x_j(t-\tau_i)\right)\right] \\ &- \rho\varphi_i + \mu_i + \nu_i(t)\end{aligned} \tag{6.8}$$

Now (6.7) and (6.8) are combined together and the error system of delayed SMC, $\mathcal{D}^{\alpha}\mathfrak{E}(t)$ can be defined by

$$\begin{aligned}\mathcal{D}^{\alpha}\mathfrak{E}(t) = &-\left[c_i + \left(\pi_{jl}\right)_{n\times m} \cdot (\omega_{li})_{m\times n}\right] \mathfrak{E}_i(t) - \left[\left(\pi_{jl}\right)_{n\times m} \cdot (\varepsilon_{li})_{m\times n}\right] \mathfrak{E}_j(t-\tau_i) \\ &+ \sum_{j=1}^{n} b_{ij}\left[g_j\left(y_j(t)\right) - g_j\left(\rho x_j(t)\right)\right] + \sum_{j=1}^{n} h_{ij}\left[g_j\left(y_j(t-\tau_i)\right) - g_j\left(\rho x_j(t-\tau_i)\right)\right]\end{aligned} \tag{6.9}$$

Universiti Malaya

Then, it follows from (6.9), that

$$\mathcal{D}^{\alpha}\mathfrak{E}(t) = -c_i e_i(t) - \left[\sum_{j=1}^{n}\sum_{l=1}^{m}(\pi_{jl})(\omega_{li})\right]\mathfrak{E}_i(t) - \left[\sum_{j=1}^{n}\sum_{l=1}^{m}(\pi_{jl})(\varepsilon_{li})\right]\mathfrak{E}_j(t-\tau_i) + \sum_{j=1}^{n} b_{ij}\left[g_j(y_j(t)) - g_j\left(\rho x_j(t)\right)\right] + \sum_{j=1}^{n} h_{ij}\left[g_j(y_j(t-\tau_i)) - g_j\left(\rho x_j(t-\tau_i)\right)\right] \tag{6.10}$$

Theorem 6.3.1 *" (Podlubny, 1998) Suppose that (H) holds. Assume that there exist positive constants m_i and l_i such that $m_i = max\left\{\left|m_i^-\right|, \left|m_i^+\right|\right\}$, $l_i = max\left\{\left|l_i^-\right|, \left|l_i^+\right|\right\}$, and constant matrices that $(\pi_{jl})_{n\times m}$, $(\omega_{li})_{m\times n}$, $(\varepsilon_{li})_{m\times n}$ and*

$$\begin{cases} \Psi_1 := \min_{1\le i\le n}\left[c_i - \sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|(\pi_{jl})(\omega_{li})\right|\right] - \sum_{j=1}^{n}\left|b_{ji}\right| m_i\right] > 0 \\ \Psi_2 := \max_{1\le i\le n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|(\pi_{jl})(\varepsilon_{li})\right|\right] + \sum_{j=1}^{n}\left|h_{ji}\right| l_i\right] > 0 \\ \Psi_1 - \Psi_2 > 0 \end{cases} \tag{6.11}$$

Then the equation (6.9) *is stable."*

Proof. According to (H) and theorem 6.3.1, we have

$$m_j^- \le \frac{g_j\left[y_j(t)\right] - g_j\left[\rho x_j(t)\right]}{\left(y_j(t)\right) - \left(\rho x_j(t)\right)} \le m_j^+$$

and

$$l_j^- \le \frac{g_j\left[y_j(t-t_i)\right] - g_j\left[\rho x_j(t-t_i)\right]}{\left(y_j(t-t_i)\right) - \left(\rho x_j(t-t_i)\right)} \le l_j^+$$

Next, we obtain that

$$\begin{cases} \left|g_j\left[y_j(t)\right] - g_j\left[\rho x_j(t)\right]\right| \le m_j\left|\left(y_j(t)\right) - \left(\rho x_j(t)\right)\right| \\ \left|g_j\left[y_j(t-\tau_i)\right] - g_j\left[\rho x_j(t-\tau_i)\right]\right| \le l_j\left|\left(y_j(t-\tau_i)\right) - \left(\rho x_j(t-\tau_i)\right)\right| \end{cases} \tag{6.12}$$

Universiti Malaya

Generate the following function of Lyapunov

$$V\left[\mathfrak{E}\left(t\right)\right]=\sum_{i=1}^{n}\left|\mathfrak{E}_{i}\left(t\right)\right| \tag{6.13}$$

Based on Lemma 6.2.1, By letting the upper right CapD $\mathcal{D}_{+}^{a}\left[\mathfrak{E}\left(t\right)\right]$ along the trajectories, equation (6.13) can be obtained as follows;

We defined the Lyapunov function candidate by

$$\begin{aligned}
\mathcal{D}_{+}^{a}\,V[\mathfrak{E}_{i}(t)] &= \sum_{i=1}^{n}\mathcal{D}_{+}^{a}\,|\mathfrak{E}_{i}(t)| \\
&\leq -\sum_{i=1}^{n} sgn[\mathfrak{E}_{i}(t)]\;D_{+}^{a}\mathfrak{E}_{i}(t) \\
&= -\sum_{i=1}^{n} sgn\,[\mathfrak{E}_{i}(t)]\left[\left[c_{i}+\sum_{j=1}^{n}\left[\sum_{l=1}^{m}(\pi_{jl})\,(\omega_{li})\right]\right]\mathfrak{E}_{j}(t)\right. \\
&\quad +\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}(\pi_{jl})\,(\varepsilon_{li})\right]\right]\mathfrak{E}_{j}(t-\tau_{i}) \\
&\quad +\sum_{j=1}^{n} b_{ij}\left[g_{j}\,(y_{j}(t))-g_{j}\,(\rho x_{j}(t))\right] \\
&\quad \left.+\sum_{j=1}^{n} h_{ij}\left[g_{j}(y_{j}\,(t-\tau_{i}))-g_{j}\,(\rho x_{j}(t-\tau_{i}))\right]\right] \\
&\leq -\sum_{i=1}^{n} c_{i}\,|\mathfrak{E}_{i}(t)|+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}|(\pi_{jl})\,(\omega_{li})|\right]|\,\mathfrak{E}_{j}(t)|\right] \\
&\quad +\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}|(\pi_{jl})\,(\varepsilon_{li})|\;|\mathfrak{E}_{j}(t-\tau_{i})|\right]\right] \\
&\quad +\sum_{i=1}^{n}\left[\sum_{j=1}^{n}|b_{ij}|\;m_{j}\;|(y_{j}(t))-(\rho x_{j}(t))|\right] \\
&\quad +\sum_{i=1}^{n}\left[\sum_{j=1}^{n}|h_{ij}|\;l_{j}|(y_{j}(t-\tau_{i}))-(\rho x_{j}(t-\tau_{i}))|\right] \\
&= -\sum_{i=1}^{n} c_{i}\,|\mathfrak{E}_{i}(t)|+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}|(\pi_{jl})\,(\omega_{li})|\right]\right]|\mathfrak{E}_{i}(t)| \\
&\quad +\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}|(\pi_{jl})\,(\varepsilon_{li})|\right]\right]|\mathfrak{E}_{j}(t-t_{i})|
\end{aligned}$$

University of Malaya

$$
\begin{aligned}
&+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left|b_{ij}\right|m_j\left|\left(y_j(t)\right)-\left(\rho x_j(t)\right)\right|\right]\\
&+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left|h_{ij}\right|l_j\left|\left(y_j(t-t_i)\right)-\left(\rho x_j(t-t_i)\right)\right|\right]\\
=&-\sum_{i=1}^{n}\left[c_i-\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|\left(\pi_{jl}\right)\left(\omega_{li}\right)\right|\right]\right]\right.\\
&\left.-\left[\sum_{j=1}^{n}\left|b_{ij}\right|m_j\left|\left(y_j(t)\right)-\left(\rho x_j(t)\right)\right|\right]\right]\left|\mathfrak{E}_i(t)\right|\\
&+\left[\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|\left(\pi_{jl}\right)\left(\varepsilon_{li}\right)\right|\right]\right]\right.\\
&\left.+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}\left|h_{ij}\right|l_j\left|\left(y_j(t-t_i)\right)-\left(\rho x_j(t-t_i)\right)\right|\right]\right]\left|\mathfrak{E}_j(t-t_i)\right|\\
\leq&\max_{1\leq i\leq n}\left[\sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|\left(\pi_{jl}\right)\left(\varepsilon_{li}\right)\right|\right]\sum_{j=1}^{n}\left|h_{ji}\right|l_i\right]\left|\mathfrak{E}_j(t-\tau_i)\right|\\
&-\min_{1\leq i\leq n}\left[c_i-\sum_{j=1}^{n}\left[\sum_{l=1}^{m}\left|\left(\pi_{jl}\right)\left(\varepsilon_{li}\right)\right|\right]-\sum_{j=1}^{n}\left|b_{ji}\right|m_i\right]\left|\mathfrak{E}_i(t)\right|\\
\leq&\Psi_1 V\left(\mathfrak{E}_i(t)\right)+\Psi_2\sup_{t-\tau_i\leq u\leq t}V\left(\mathfrak{E}_i(u)\right).
\end{aligned}
\tag{6.14}
$$

Note that

$$
\sup_{t-t_i\leq u\leq t}V\left(\mathfrak{E}_i(u)\right)\leq V\left(\mathfrak{E}_i(t)\right). \tag{6.15}
$$

Then, based on (6.14), (6.15) and Theorem 6.3.1, supposed that there is a constant $\Delta > 0$, one has

$$
\begin{cases}
\mathcal{D}_+^a V\left(\mathfrak{E}_i(t)\right)\leq-\left(\Psi_1-\Psi_2\right)V\left(\mathfrak{E}_i(t)\right)\\
\Psi_1-\Psi_2\geq\Delta
\end{cases}
\tag{6.16}
$$

We construct that (6.16) as;

$$
\mathcal{D}_+^{\alpha}V\left(\mathfrak{E}_i(t)\right)\leq\Delta V\left(\mathfrak{E}_i(t)\right). \tag{6.17}
$$

Universiti Malaya

So,

$$\begin{aligned} \|\mathfrak{E}_i(t)\| &= \left\| \left(y_j(t)\right) - \left(\rho x_j(t)\right) \right\| \\ &= \sum_{i=1}^{n} \left\| \left(y_j(t)\right) - \left(\rho x_j(t)\right) \right\| \end{aligned} \tag{6.18}$$

Finally, we can conclude that the error of delayed SMC (6.9) is stable as $\|\mathfrak{E}_i(t)\| \rightarrow 0$ as t approaches infinity.

This completes the proof. ■

Remark 6.3.1 *When $\rho = 1$, projective synchronization is standardized with multiple time delays for the complete synchronization of PFONNs.*

Remark 6.3.2 *When $\rho = -1$, the projective synchronization is standardized to the complete globally antisynchronized of PFONNs with multiple time delays.*

Remark 6.3.3 *The results obtained is extended from (Latiff et al., 2020) for nonidentical PFONNs with multiple time-delays. This disturbance should not be neglected since it generally occurs in such systems and can lower the efficiency of the system.*

6.4 Symmetric Encryption with NNs in Secure Communications

In this section, we will perform the encryption and decryption of a message. Symmetric encryption and the public key are first used an original message that is called as plaintext to generate the ciphertext, and the ciphertext is re-encrypted to achieve double encryption using synchronization. It consists of the encrypter (SS and encryption function) and the decrypter (MS and decryption function). We use (6.2) as MS and (6.4) as SS and we have shown that the DDMDEs (6.9) is $\|\mathfrak{E}_i(t)\| \rightarrow 0$, the synchronization is achieved. The sender uses PFONNs (6.2) and the receiver uses PFONNs (6.4) and they both choose for $x_4(t)$ and $y_4(t)$ as the public keys after a period of time, which is means that the synchronization between two PFONNs took place. Sender pick up the data from $x_4(t)$ to

Universiti Malaya

obtain the secret keys for encryption, while the receiver pick up data from $y_4(t)$ to obtain secret keys and decrypt the ciphertext.

The plaintext and ciphertext are represented by numbers, each letter from the alphabet is substituted by the corresponding numeral, which is associated with ASCII representation. The formula for encryption and decryption is given by:

$$\begin{aligned} c_i &= p_i + k_i \quad (mod 38), \\ p_i &= c_i - k_i \quad (mod 38), \end{aligned} \tag{6.19}$$

With k_i are the secret keys that mask the message. These secret keys are completely applied for once. The sender can randomly adjust the initial conditions of PFONNs (6.2) for the next time. This is because chaotic systems are actually sensitive to the initial state.

6.4.1 Proposed Algorithm

One may summarize the entire design technique as follows:

Problem: The problem is how to enforce double encryption through symmetric encryption and chaotic synchronization, provided the two NNs with different initial conditions and symmetric encryption/decryption schemes. Based on the following steps, we can overcome this problem:

Step 1: Both sender and receiver agree private keys are from the values of integers part of $10000x$ and $10000y$.

Step 2: Sender pick up the data from $x_4(t)$ to obtain the secret keys for encryption, while the receiver pick up data from $y_4(t)$ to obtain secret keys and decrypt the ciphertext.

Step 3: Input plaintext and the private keys to form an ciphertext by symmetric encryption function.

Universiti Malaya

Step 4: Construct the PFONNs of the MS (6.2) and the SS (6.4), respectively.

Step 5: Define the error of delayed SMC can then be obtained using MATLAB simulation.

Step 6: In order to get the encrypted signal, the ciphertext is then forwarded to the MS.

Step 7: Based on the encrypted signal, we can retrieve the ciphertext from the SS.

Step 8: The plaintext is obtained using private keys and the symmetric decryption scheme.

6.5 Numberical Example and Simulations

In this section, by using MATLAB tools, the numerical simulation method is presented here. The graphical analysis displays the findings using this program. The suggested definition with numerical examples is disclosed to validate the feasibility and efficacy of the results obtained by using four dimensional PFONNs with two time-delays as the MSSYS, described as follows:

We can answer the above problem based on the following steps.

Step 1: A message is converted from plaintext by an ASCII encoder, Table 6.1, the space between two words is assigned by 10.

Chaotic Synchronization + symmetric encryption = DES

Plaintext: NEURAL NETWORKS

Step 2: Both sender and receiver computes agree private keys are from the values of integers part of $10000x$ and $10000y$.

Step 3: Sender pick up the data from x_4 (t) to obtain the secret keys for encryption, while the receiver picks up data from $y_4(t)$ to obtain secret keys and decrypt the ciphertext.

Universiti Malaya

Table 6.1: ASCII Value

Unit Message	N	E	U	R	A	L	-	N	E	T	W	O	R	K	S
ASCII	78	69	85	82	65	76	10	78	69	84	87	79	82	75	83

Step 4: Since the PFONNs is with the time delay, to be secure they both agree to change values of τ_1 and τ_2 after every five unit of message. They increase the values of τ_1 and τ_2 by 0.1 and established the chaotic NNs for MS and SS (6.20)-(6.27).

Step 5: Define that synchronization errors can then be obtained which is at $160.245s$. Then the key is chosen as the time is above $160.245s$. The convergence in the finite time of state error is shown in Figure 6.13. It demonstrated that as the controller is triggered, all the systems converge to zero.

Step 6: Enter plaintext and the public key to construct a ciphertext by symmetric encryption function. The ciphertext is then forwarded to the MS to get the encrypted signal.

$c_i = p_i + k_i \pmod{38}$, Table 6.2

Ciphertext: 931322328182097371835161213

Step 7: We can retrieve the ciphertext from the SS based on the encrypted signal.

Step 8:The plaintext is recovered via symmetric decryption scheme and the private keys.

$p_i = c_i - k_i \pmod{38}$, Table 6.3

Ciphertext: 931322328182097371835161213

Message: NEURAL NETWORKS

Universiti Malaya

Established the PFONNs for MS and SS.

$$\mathcal{D}^a x_1(t) = -c_1\, x_1 + a_{11} f_1(x_1(t)) + a_{12}\, f_2(x_2(t)) + a_{13}\, f_3(x_3(t)) + a_{14}\, f_4(x_4(t)) + g_{11} f_1(x_1(t-\tau_1)) + g_{11} f_1(x_1(t-\tau_2)) + g_{12} f_2(x_2(t-t_1)) + g_{12} f_2(x_2(t-t_2)) + g_{13} f_3(x_3(t-\tau_1)) + g_{13} f_3(x_3(t-\tau_2)) + g_{14} f_4(x_4(t-\tau_1)) + g_{14} f_4(x_4(t-\tau_2)) + \varphi_1 \tag{6.20}$$

$$\mathcal{D}^a x_2(t) = -c_2\, x_2 + a_{21} f_1(x_2(t)) + a_{22}\, f_2(x_2(t)) + a_{23}\, f_3(x_3(t)) + a_{24}\, f_2(x_4(t)) + g_{21} f_1(x_1(t-\tau_1)) + g_{21} f_1(x_1(t-\tau_2)) + g_{22} f_2(x_2(t-\tau_1)) + g_{22} f_2(x_2(t-\tau_2)) + g_{23} f_3(x_3(t-\tau_1)) + g_{23} f_3(x_3(t-\tau_2)) + g_{24} f_4(x_4(t-\tau_1)) + g_{24} f_4(x_4(t-\tau_2)) + \varphi_2 \tag{6.21}$$

$$\mathcal{D}^a x_3(t) = -c_3\, x_3 + a_{31} f_1(x_1(t)) + a_{32}\, f_2(x_2(t)) + a_{33}\, f_3(x_3(t)) + a_{34}\, f_2(x_4(t)) + g_{31} f_1(x_1(t-\tau_1)) + g_{31} f_1(x_1(t-\tau_2)) + g_{32} f_2(x_2(t-\tau_1)) + g_{32} f_2(x_2(t-\tau_2)) + g_{33} f_3(x_3(t-\tau_1)) + g_{33} f_3(x_3(t-\tau_2)) + g_{34} f_4(x_4(t-\tau_1)) + g_{34} f_4(x_4(t-\tau_2)) + \varphi_3 \tag{6.22}$$

$$\mathcal{D}^a x_4(t) = -c_4\, x_4 + a_{41} f_1(x_1(t)) + a_{42}\, f_2(x_2(t)) + a_{43}\, f_3(x_3(t)) + a_{44}\, f_2(x_4(t)) + g_{41} f_1(x_1(t-\tau_1)) + g_{41} f_1(x_1(t-\tau_2)) + g_{42} f_2(x_2(t-\tau_1)) + g_{42} f_2(x_2(t-\tau_2)) + g_{43} f_3(x_3(t-\tau_1)) + g_{43} f_3(x_3(t-\tau_2)) + g_{44} f_4(x_4(t-\tau_1)) + g_{44} f_4(x_4(t-\tau_2)) + \varphi_4 \tag{6.23}$$

Universiti Malaya

And

$$\mathcal{D}^a y_1(t) = -d_1\, y_1 + b_{11} f_1(y_1(t)) + b_{12}\, f_2(y_2(t)) + b_{13}\, f_3(y_3(t)) + a_{14}\, f_4(y_4(t)) + h_{11} f_1(y_1(t-\tau_1)) + h_{11} f_1(y_1(t-\tau_2)) + h_{12} f_2(y_2(t-\tau_1)) + h_{12} f_2(y_2(t-\tau_2)) + h_{13} f_3(y_3(t-\tau_1)) + h_{13} f_3(y_3(t-\tau_2)) + h_{14} f_4(y_4(t-\tau_1)) + h_{14} f_4(y_4(t-\tau_2)) + \mu_1 + \nu_1(t) \tag{6.24}$$

$$\mathcal{D}^a y_2(t) = -d_2\, y_2 + b_{21} f_1(y_2(t)) + b_{22}\, f_2(y_2(t)) + b_{23}\, f_3(y_3(t)) + b_{24}\, f_4(y_4(t)) + h_{21} f_1(y_1(t-\tau_1)) + h_{21} f_1(y_1(t-\tau_2)) + h_{22} f_2(y_2(t-\tau_1)) + h_{22} f_2(y_2(t-\tau_2)) + h_{23} f_3(y_3(t-\tau_1)) + h_{23} f_3(y_3(t-\tau_2)) + h_{24} f_4(y_4(t-\tau_1)) + h_{24} f_4(y_4(t-\tau_2)) + \mu_2 + \nu_2(t) \tag{6.25}$$

$$\mathcal{D}^a y_3(t) = -d_3\, y_3 + b_{31} f_1(y_1(t)) + b_{32}\, f_2(y_2(t)) + b_{33}\, f_3(y_3(t)) + b_{34}\, f_4(y_4(t)) + h_{31} f_1(y_1(t-\tau_1)) + h_{31} f_1(y_1(t-\tau_2)) + h_{32} f_2(y_2(t-\tau_1)) + h_{32} f_2(y_2(t-\tau_2)) + h_{33} f_3(y_3(t-\tau_1)) + h_{33} f_3(y_3(t-\tau_2)) + h_{34} f_4(y_4(t-\tau_1)) + h_{34} f_4(y_4(t-\tau_2)) + \mu_3 + \nu_3(t) \tag{6.26}$$

$$\mathcal{D}^a y_4(t) = -d_4\, y_4 + b_{41} f_1(y_1(t)) + b_{42}\, f_2(y_2(t)) + b_{43}\, f_3(y_3(t)) + b_{44}\, f_4(y_4(t)) + h_{41} f_1(y_1(t-\tau_1)) + h_{41} f_1(y_1(t-\tau_2)) + h_{42} f_2(y_2(t-\tau_1)) + h_{42} f_2(y_2(t-\tau_2)) + h_{43} f_3(y_3(t-\tau_1)) + h_{43} f_3(y_3(t-\tau_2)) + h_{44} f_4(y_4(t-\tau_1)) + h_{44} f_4(y_4(t-\tau_2)) + \mu_4 + \nu_4(t) \tag{6.27}$$

with the following parameters $\alpha = 0.98$,$c_1 = c_4 = -9.5$, $c_2 = -10.5$, $c_3 = -3.7 a_{11} = 2.0$, $a_{12} = 0.5$, $a_{13} = 5.5$, $a_{14} = 2$, $a_{21} = 0.5$, $a_{22} = 0.5$, $a_{23} = 5.1$, $a_{24} = 0.5, a_{31} = 0.5$, $a_{32} = 1.0$, $a_{33} = -5.5$, $a_{34} = 5.1$, $a_{41} = 0.5$, $a_{42} = 1.0$, $a_{43} = -9.5$, $a_{44} = 0.5, g_{11} = 7$, $g_{12} = 7, g_{13} = 4.1, g_{14} = 7, g_{21} = 1, g_{22} = 1, g_{23} = 2.5, g_{24} = 1, g_{31} = 0.1, g_{32} =$

Universiti Malaya

Table 6.2: Encryption of Plaintext to Ciphertext

Time Lag τ_1	Time Lag τ_2	Time t	$x_4(t)$	Keys k	Plaintext P	Ciphertext $c_i = p_i + k_i(mod\ 38)$
1.0	1.5	200.0	0.24821..	24821	N	9
		201.0	0.49704..	49704	E	31
		202.0	0.18453..	18453	U	32
		203.0	0.47897..	47897	R	23
		204.0	0.21585..	21585	A	28
1.1	1.6	205.0	0.43376..	43376	L	18
		206.0	0.25698..	25698	-	20
		207.0	0.39907..	39907	N	9
		208.0	0.29312..	29312	E	7
		209.0	0.37003..	37003	T	37
1.2	1.7	210.0	0.31395..	31395	W	18
		211.0	0.35144..	35144	O	35
		212.0	0.32576..	32576	R	16
		213.0	0.34403..	34403	K	12
		214.0	0.33712..	33712	S	13

$-10.1, g_{33} = 4.5, g_{34} = 0.1,\ g_{41} = 7, g_{42} = 7, g_{43} = 4.1, g_{44} = 7, d_1 = d_4 = -1,\ d_2 = -3, d_3 = -7.7,\ b_{11} = 0.01,\ b_{12} = 0.3,\ b_{13} = 7.5,\ b_{14} = 0.01,\ b_{21} = 0.01,\ b_{22} = 7.5,\ b_{23} = 0.01,\ b_{24} = 0.01,\ b_{31} = 0.01,\ b_{32} = 3,\ b_{33} = -5.5,\ b_{34} = -5.5,\ b_{41} = 0.01,\ b_{42} = 3,\ b_{43} = 3,\ b_{44} = -5.5,\ h_{11} = 0.3,\ h_{12} = 5.5,\ h_{13} = 5.5, h_{14} = 0.3, h_{21} = 0.5, h_{22} = 7.5, h_{23} = 0.01, h_{24} = 0.5, h_{31} = 0.1, h_{32} = -1.5, h_{33} = 1.5, h_{34} = 0.1,\ h_{41} = 0.1,\ h_{42} = 5.5,\ h_{43} = 5.5,\ h_{44} = 0.1, t_1 = 1, t_2 = 1\ .\ 5\ ,\ f_1(x) = f_2(x) = tanh(x), \varphi_1 = \varphi_2 = \varphi_3 = \varphi_4 = 0,\ \mu_1 = \mu_2 = \mu_3 = \mu_4 = 0,\ \nu_1(t) = \nu_2(t) = \nu_3(t) = \nu_4(t) = 1,$

Based the above parameters, the system is shown in Figure 6.3.

Furthermore, the initial values of the MS and SS are assumed as $x_1(0) = 0.1,\ x_2(0) = 0.3,\ x_3(0) = -0.1,\ x_4(0) = 0.1, y_1(0) = 0.1,\ y_2(0) = 1.2,\ y_3(0) = 0.1,\ y_4(0) = 0.1.$

Remark 6.5.1 *Chaotic behaviour of the system* (6.20) - (6.23) *without the synchronization illustrated in Figure 6.1*

Remark 6.5.2 *From the simulation results, Figures (6.4 - 6.7) which show the state trajectories of MS* (6.20) - (6.23) *and MS* (6.24) - (6.27) *without control input and*

Universiti Malaya

Table 6.3: Decryption of Ciphertext to Plaintext

Time Lag τ_1	Time Lag τ_2	Time t	$y_4(t)$	Keys k	Ciphertext P	Plaintext $p_i = c_i - k_i \ (mod\ 38)$
1.0	1.5	200.0	0.24821..	24821	9	78 (N)
		201.0	0.49704..	49704	31	69 (E)
		202.0	0.18453..	18453	32	85 (U)
		203.0	0.47897..	47897	23	82 (R)
		204.0	0.21585..	21585	28	65 (A)
1.1	1.6	205.0	0.43376..	43376	18	76 (L)
		206.0	0.25698..	25698	20	10 (-)
		207.0	0.39907..	39907	9	78 (N)
		208.0	0.29312..	29312	7	69 (E)
		209.0	0.37003..	37003	37	84 (T)
1.2	1.7	210.0	0.31395..	31395	18	87 (W)
		211.0	0.35144..	35144	35	79 (O)
		212.0	0.32576..	32576	16	82 (R)
		213.0	0.34403..	34403	12	75 (K)
		214.0	0.33712..	33712	13	83 (S)

Table 6.4: Synchronization error for different value of fractional-order with time delay $\tau_1 = 1.00$ and $\tau_2 = 1.50$

	$\alpha = 0.99$	$\alpha = 0.98$	$\alpha = 0.97$	$\alpha = 0.96$	$\alpha = 0.95$	$\alpha = 0.94$
$\tau_1 = 1.00$ $\tau_2 = 1.50$	Infeasible	160.245	172.450	178.225	181.855	187.640

$\alpha = 0.98$. *Figure 6.12 illustrates the state trajectories of error dynamical system which are not converge to zero without control input.*

Remark 6.5.3 *From the simulation results (Figures 6.13 - 6.17), it can be seen that when values of* α *decreses such as* $\alpha = 0.98$, $\alpha = 0.97$, $\alpha = 0.96$, $\alpha = 0.95$ *and* $\alpha = 0.94$ *with the control input, the time taken for syncronization error is increasing and it is globally asymptotically stable. From this, we confirm that the dynamical behaviour of the system is very sensitive to the values of* α. *Furthermore, the synchronization error converge to zero and one can easily show that the* $\alpha = 0.98$ *is chosen. We obtain the time taken for syncronization to archive with different values of* α *as listed in the Table 6.4. The time segment of* $T = 200$ *for error synchronization are chosen. While Figure (6.18 - 6.22) illustrates the state trajectories of systems* (6.2), (6.4) *and synchronization error of*

Universiti Malaya

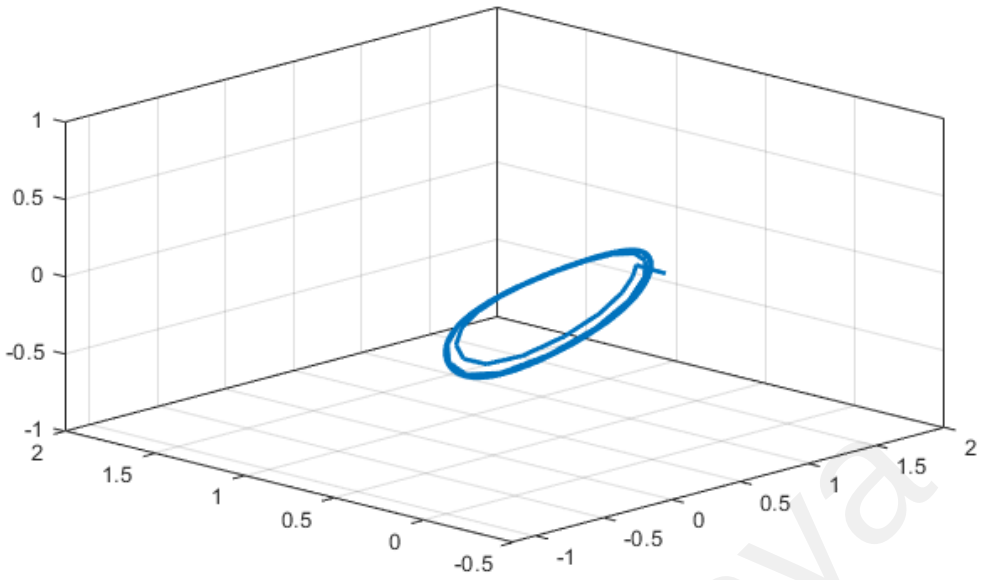


Figure 6.1: Chaotic attractor of MS (6.20)**,** (6.21)**,** (6.22) **and** (6.23) **with multiple delay without synchronization**

$\alpha = 0.99$ *which are not converge to zero with control input.*

Universiti Malaya

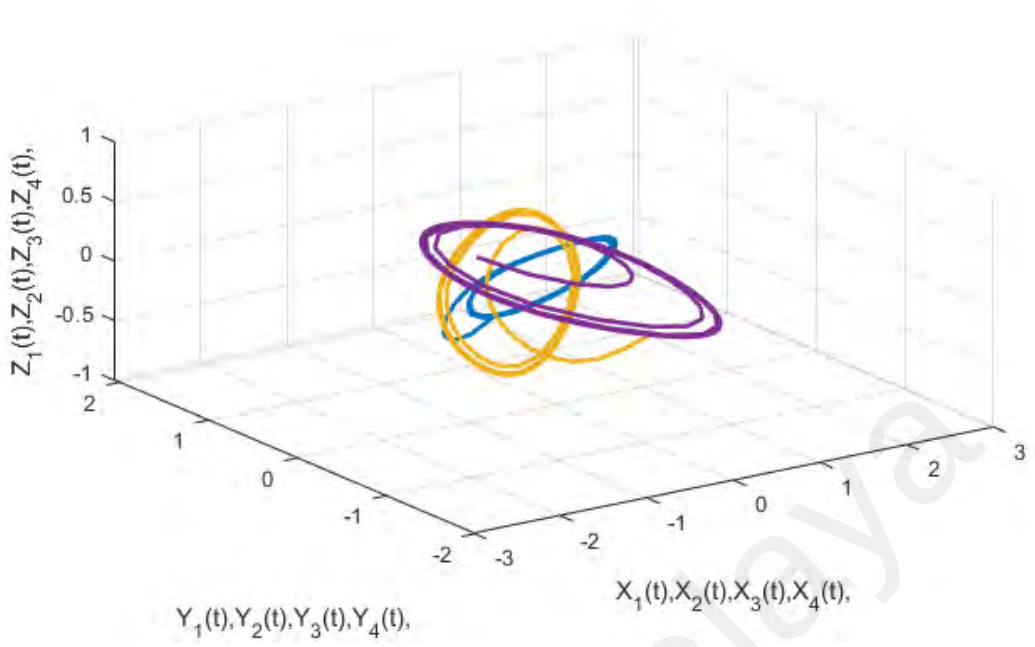


Figure 6.2: Chaotic attractor of MS (6.20)**,** (6.21)**,** (6.22)**,** (6.23) **and SS** (6.24)**,** (6.25)**,** (6.26)**,** (6.27) **with multiple delay without control inputs after synchronization and** $\alpha = 0.98$

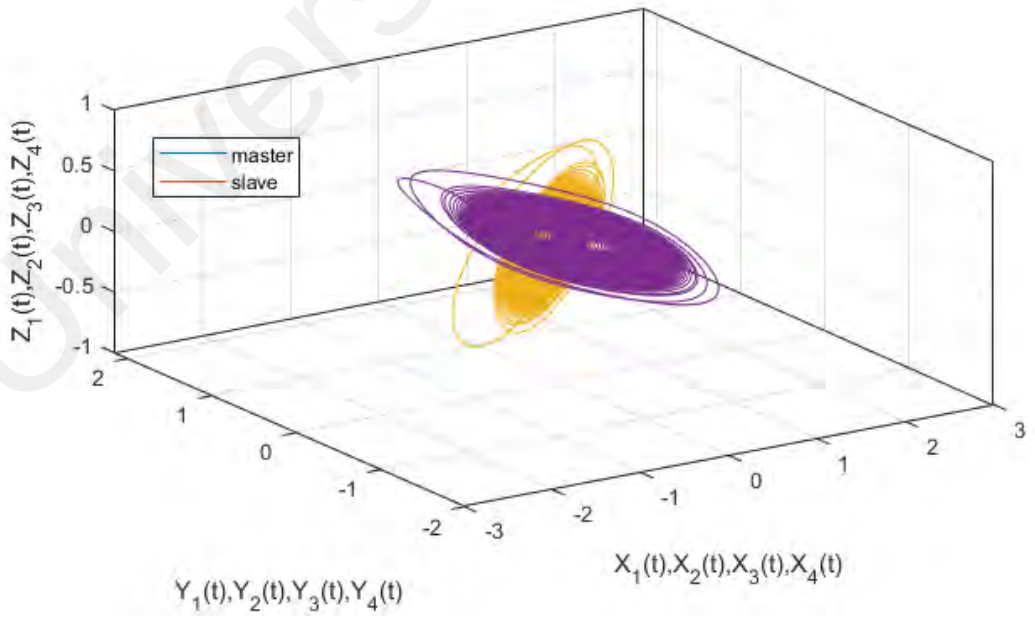


Figure 6.3: Chaotic attractor of MS (6.20)**,** (6.21)**,** (6.22)**,** (6.23) **and SS** (6.24)**,** (6.25)**,** (6.26)**,** (6.27) **with multiple delay with** (6.10) **control input after synchronization and** $\alpha = 0.98$

Universiti Malaya

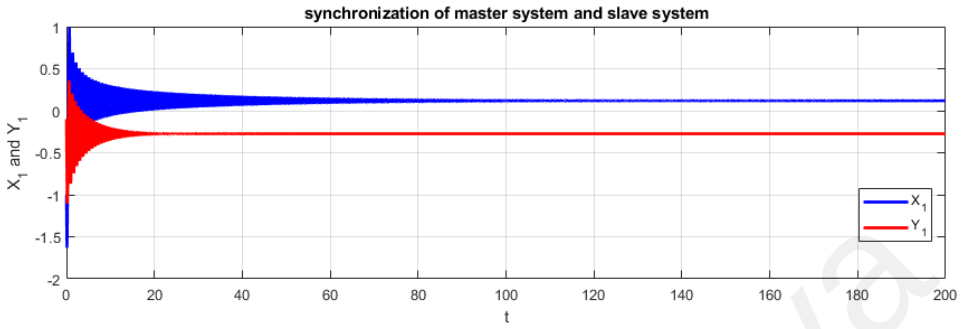


Figure 6.4: State trajectories of MS (6.20) **and SS** (6.24) **system** x_1**,** y_1 **with multiple delay without control input and** $\alpha = 0.98$

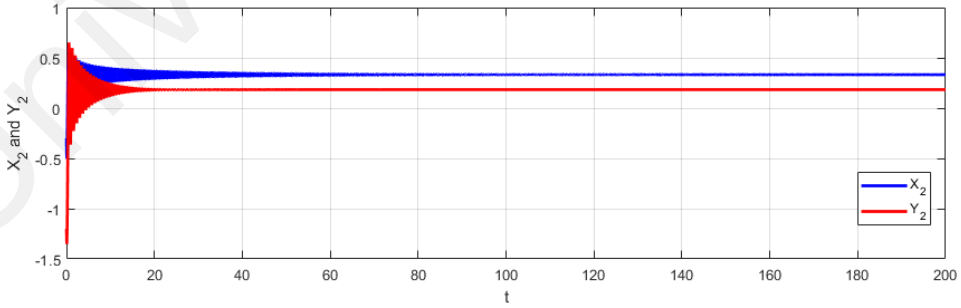


Figure 6.5: State trajectories of MS (6.21) **and SS** (6.25) **system** x_2**,** y_2 **with multiple delay without control input and** $\alpha = 0.98$

Universiti Malaya

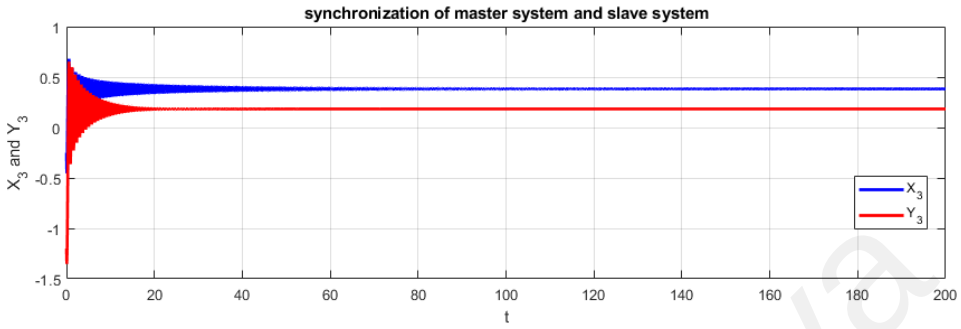


Figure 6.6: State trajectories of MS (6.22) **and SS** (6.26) **system** x_3**,** y_3 **with multiple delay without control input and** $\alpha = 0.98$

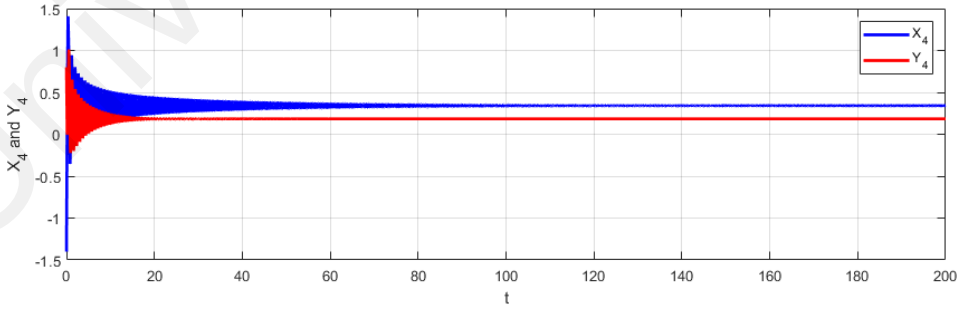


Figure 6.7: State trajectories of MS (6.23) **and SS** (6.27) **system** x_4**,** y_4 **with multiple delay without control input and** $\alpha = 0.98$

Universiti Malaya

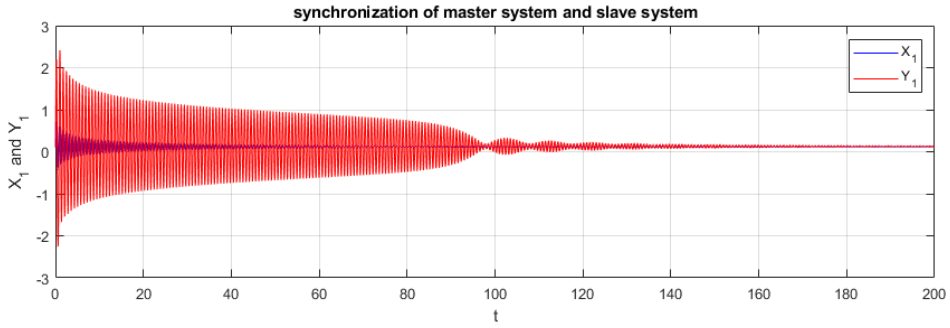


Figure 6.8: State trajectories of MS (6.20) **and SS** (6.24) **system** x_1, y_1 **with multiple delay with control input and** $\alpha = 0.98$

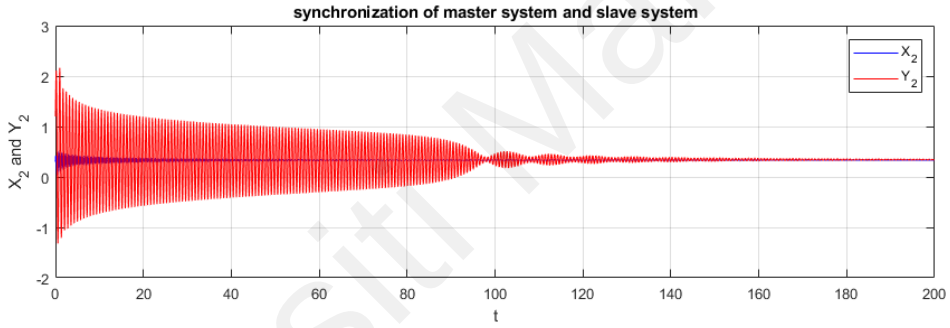


Figure 6.9: State trajectories of MS (6.21) **and SS** (6.25) **system** x_2, y_2 **with multiple delay with control input and** $\alpha = 0.98$

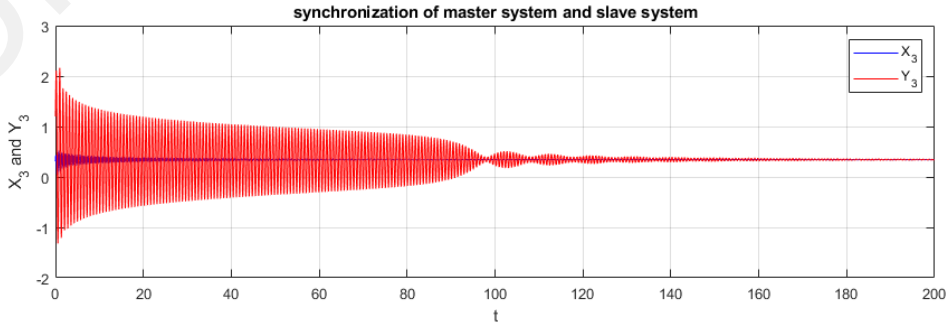


Figure 6.10: State trajectories of MS (6.22) **and SS** (6.26) **system** x_3, y_3 **with multiple delay with control input and** $\alpha = 0.98$

Universiti Malaya

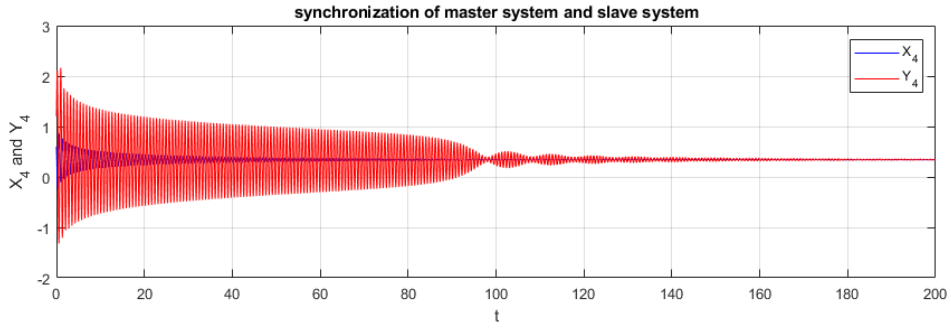


Figure 6.11: State trajectories of MS (6.23) **and SS** (6.27) **system** x_4**,** y_4 **with multiple delay with control input and** $\alpha = 0.98$

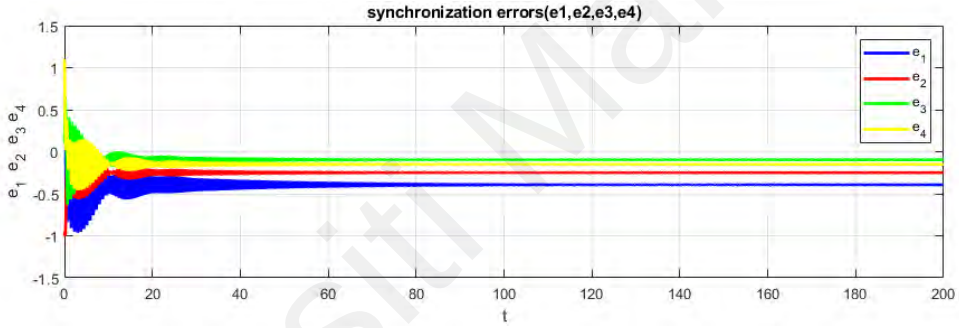


Figure 6.12: State trajectories of synchronization errors e_1, e_2, e_3, e_4 **with multiple delay without control input and** $\alpha = 0.98$

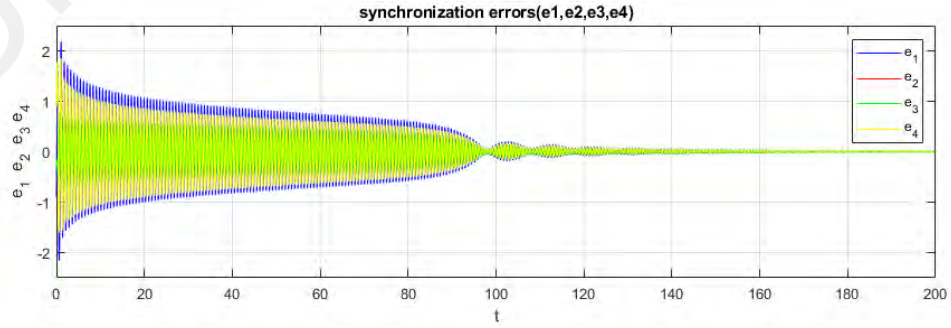
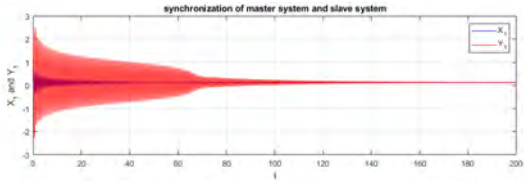
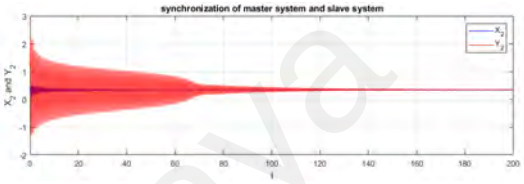


Figure 6.13: State trajectories of synchronization errors e_1, e_2, e_3, e_4 **with multiple delay with control input and** $\alpha = 0.98$

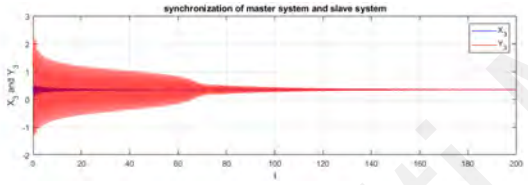
Universiti Malaya



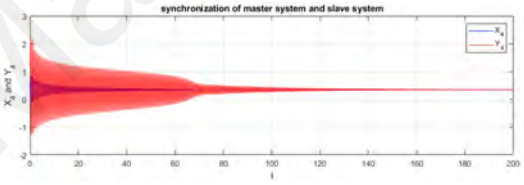
(a) x_1 and y_1



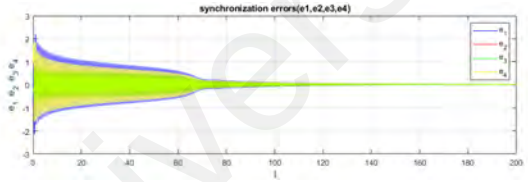
(b) x_2 and y_2



(c) x_3 and y_3



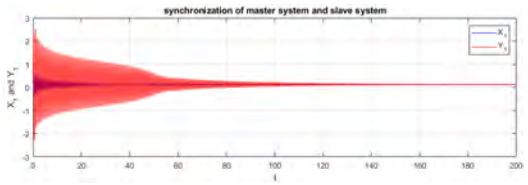
(d) x_4 and y_4



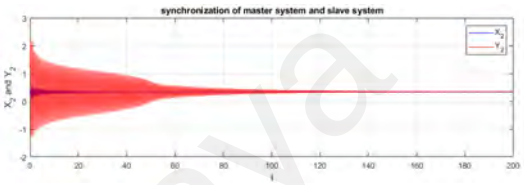
(e) synchronization errors e_1, e_2, e_3, e_4

Figure 6.14: State trajectories of MS (6.20)-(6.23) **and SS** (6.24)-(6.27) **systems with multiple delay with control input and** $\alpha = 0.97$

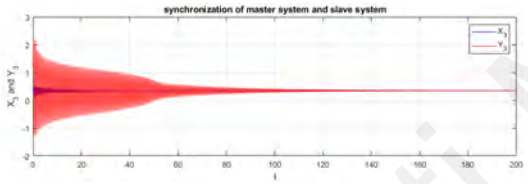
Universiti Malaya



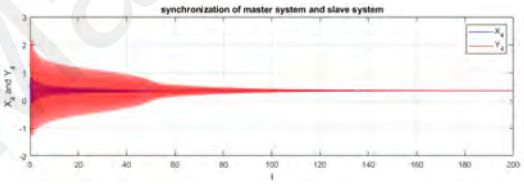
(a) x_1 and y_1



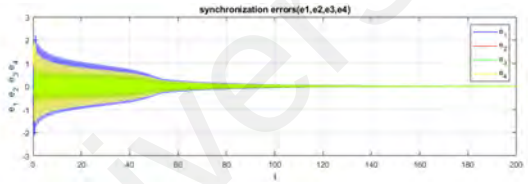
(b) x_2 and y_2



(c) x_3 and y_3



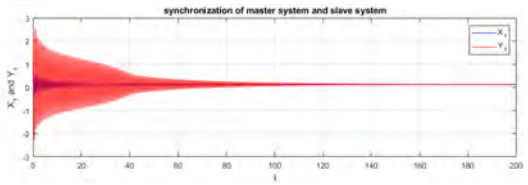
(d) x_4 and y_4



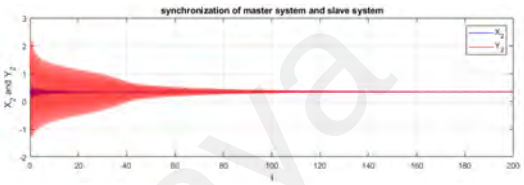
(e) synchronization errors e_1, e_2, e_3, e_4

Figure 6.15: State trajectories of MS (6.20)-(6.23) **and SS** (6.24)-(6.27) **systems with multiple delay with control input and** $\alpha = 0.96$

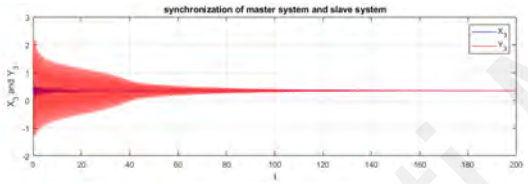
Universiti Malaya



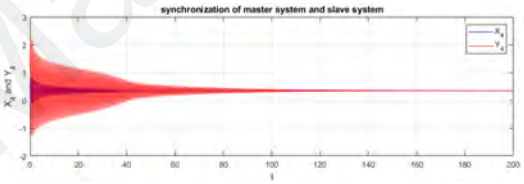
(a) x_1 and y_1



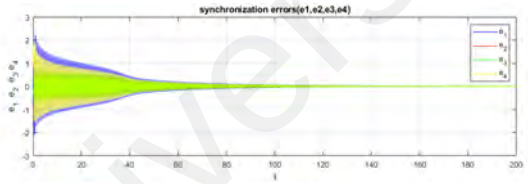
(b) x_2 and y_2



(c) x_3 and y_3



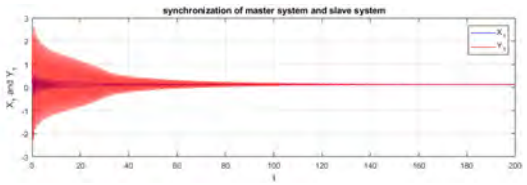
(d) x_4 and y_4



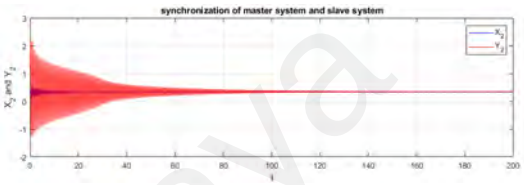
(e) synchronization errors e_1, e_2, e_3, e_4

Figure 6.16: State trajectories of MS (6.20)-(6.23) **and SS** (6.24)-(6.27) **systems with multiple delay with control input and** $\alpha = 0.95$

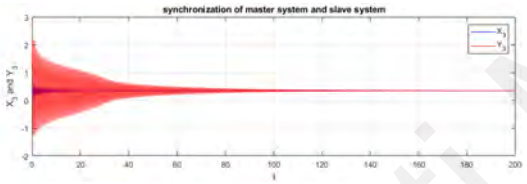
Universiti Malaya



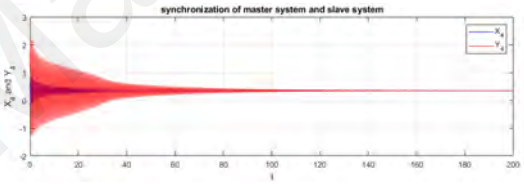
(a) x_1 and y_1



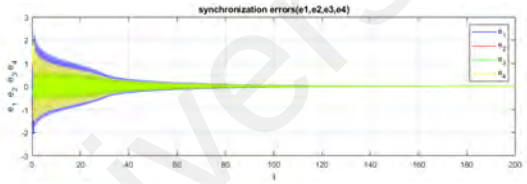
(b) x_2 and y_2



(c) x_3 and y_3



(d) x_4 and y_4



(e) synchronization errors e_1, e_2, e_3, e_4

Figure 6.17: State trajectories of MS (6.20)-(6.23) **and SS** (6.24)-(6.27) **systems with multiple delay with control input and** $\alpha = 0.94$

Universiti Malaya

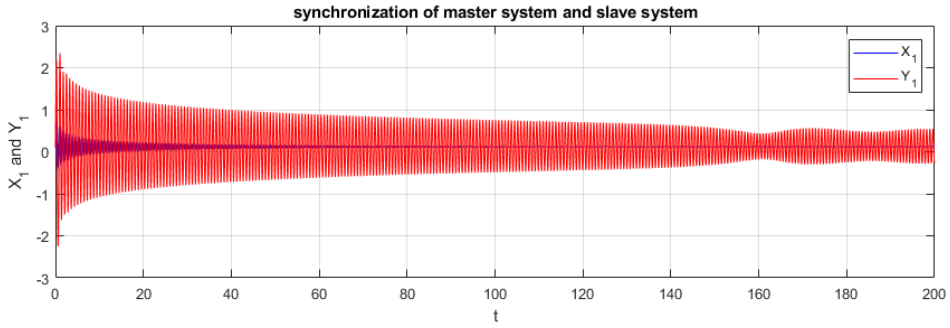


Figure 6.18: State trajectories of MS (6.20) **and SS** (6.24) **system** x_1, y_1 **with multiple delay with control input and** $\alpha = 0.99$

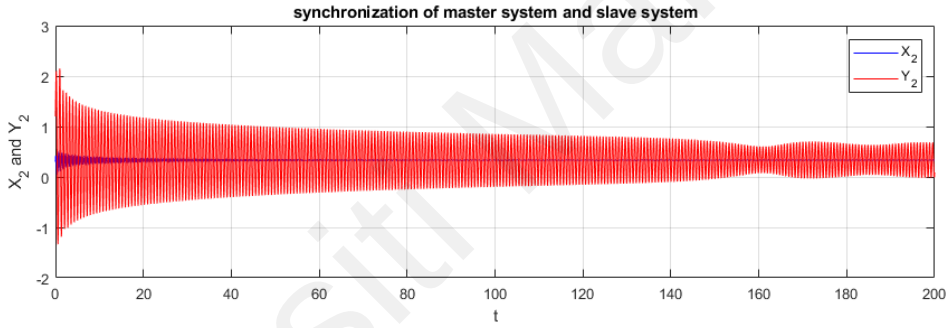


Figure 6.19: State trajectories of MS (6.21) **and SS** (6.25) **system** x_2, y_2 **with multiple delay with control input and** $\alpha = 0.99$

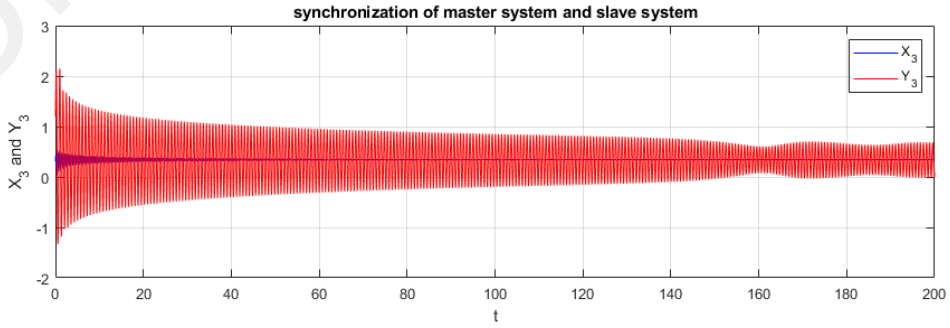


Figure 6.20: State trajectories of MS (6.22) **and SS** (6.26) **system** x_3, y_3 **with multiple delay with control input and** $\alpha = 0.99$

Universiti Malaya

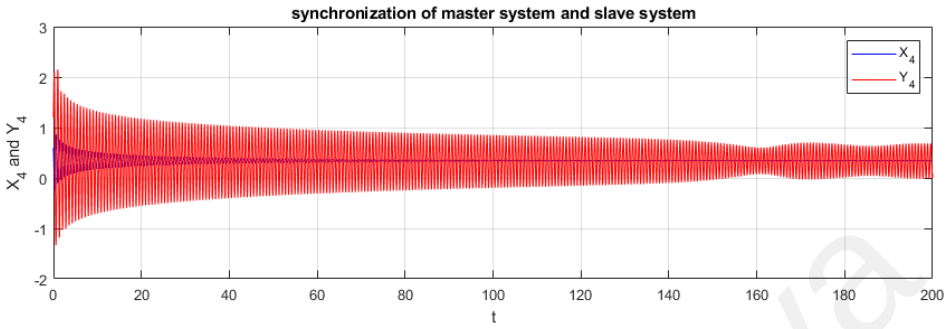


Figure 6.21: State trajectories of MS (6.23) **and SS** (6.27) **system** x_4**,** y_4 **with multiple delay with control input and** $\alpha = 0.99$

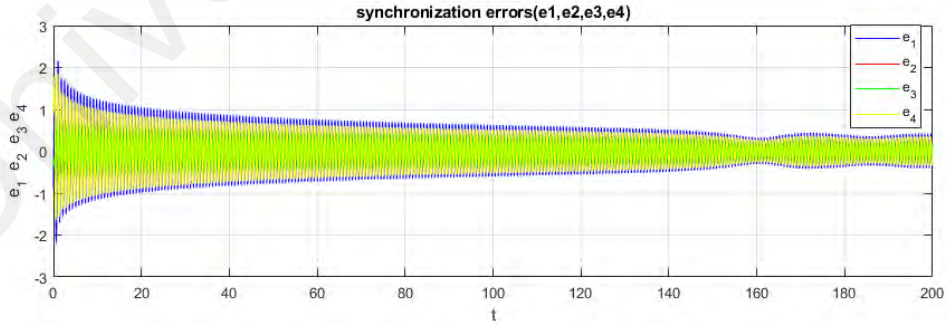


Figure 6.22: State trajectories of synchronization errors e_1, e_2, e_3, e_4 **with multiple delay with control input and** $\alpha = 0.99$ **not converge to zero**

Universiti Malaya

6.6 Conclusion

This chapter presents a design methodology to obtain double encryption systems for NNs based secure communications in multiple time-delay chaotic systems. Chaotic synchronization is combined with a symmetric algorithm to increase the cryptosystem's complexity, thereby providing greater security. The idea synchronization of chaotic NNs to secure communication system has been presented because the chaotic system will not produce the same results if the inputs keys are not the specified keys, so it is difficult to attack to have the plain text without knowing the secret keys. This chapter demonstrates the PFONNs can be easily controlled using techniques of active control. We showed that synchronization between the two PFONNs by using the controller that we proposed could be achieved. The synchronization is achieved as the convergence of synchronization errors infinite time has been ensured with the initial conditions for MS and SS are given as $x_1(0) = 0.1, x_2(0) = 0.3,\ x_3(0) = -0.1, x_4(0) = 0.1,\ y_1(0) = 0.1,\ y_2(0) = 1.2,\ y_3(0) = 0.1, y_4(0) = \ 0.1$.

From this, the keys are generated to be used in a cryptosystem. We can say that this cryptosystem is safe since we know that chaotic is very sensitive to the initial condition, and we use many algorithms to cipher the data as a secret key. These algorithms are based on the coding and decoding of alphabet algorithms that will transform the value to another value. The result data from generating key algorithm will be used in the encryption and decryption process and the generated chaotic NNs. This double encryption will give the proposed system efficiency and high security.

Universiti Malaya

CHAPTER 7: CONCLUSION

7.1 Summary

There are seven chapters in the thesis with Chapters 1, 2, 3 and 7 discussing the introduction, literature review, methodology and summary respectively. Chapters 4,5 and 6 have present the different FO of a chaos system and their implementation to secure communication.

Chapter 4 presents the chaos synchronization of FONLS aad technique for chaos masking. To regenerate a clean driving signal at the receiver and thus perfectly recover the message, chaos masking with a low-level message signal is applied to the synchronizing driving signal. Using the signal masking approach, synchronization in chaotic systems, such as FONLS, has been numerically found that synchronization errors always exist. Errors depend on the signal frequencies: messages with relatively higher frequencies lead to more precise retrieval, a low-frequency message could be completely distorted.

Chapter 5, we have analysed the synchronization of IONNs systems and FONNs systems. Based on the delayed active SMC, the theory of delayed active SMC, the FLDM is introduced to prove the synchronization efficiency. We have proved that the synchronization of IONNs systems and FONNs systems can occur when the proposed controller is activated the result showed that the state error is converged to zero.

Chapter 6, to maximize the effectiveness of secure communication that will provide greater security, we have developed double encryption that combines symmetric cryptographic algorithms symmetric encryption with neural network synchronization. It is well known that symmetric encryption is outstanding in speed and precision, but less effective. So, we combine both techniques where the secret keys are generated from the third part of the neural network system to increase effectiveness and security. The keys are used only

Universiti Malaya

once to encrypt and decrypt the message, and the results of performance efficiency are demonstrated in numerical simulation.

7.2 Conclusion

In this thesis, we have studied methodologies and applications of chaos synchronization. The chaos synchronization phenomena are observed through the theoretical analysis and numerical simulation, and their synchronization properties, such as robustness and initial condition sensitivity, are investigated. Robustness of synchronization is a significant factor concerned in the chaos-based cryptography. Numerical methods have been used in this thesis to test the initial condition sensitivity for different value of fractional-order chaotic systems.

Chapters 4, 5 and 6 solved the different type of chaos system which are FONLS and FONNs with the different values of initial condition for the chaos synchronization. Chapter 6 is the extended idea from Chapter 5 by introducing double encryption.

A few physical examples have illustrated in the implementation of this technique in the application section, besides we used MATLAB to depict the graph of solutions, which could be a very valuable and significant intuition. Based on the overall findings of this study, the following conclusions are drawn:

1. It was found that the minimal value of $\alpha = 0.95$ for FONLS is a better choice for obtaining chaotic synchronization. Throughout the MATLAB simulation of signal masking approach, it has been found that the quality of message recovery is related to the frequency of the message.
2. Synchronization of IONNs and FONNs will chose the best value of $\alpha = 0.98$. We also conclude that in order for the synchronization of MSSYS to occurs, one has to confirm that the MS must result in integer-order and SS in fractional order. It

Universiti Malaya

is infeasible to get synchronization to converge to zero if the slave system is in integer-order.

3. A new algorithm was proposed for secure communication by combining the chaos synchronization of PFONNs with symmetrical encryption. The result showed that the best value for synchronization occurs when $\alpha = 0.98$.

7.3 Future Work

Although extensive work has been done to implement chaotic signals for secure communication, it is imperative to provide a list of additional work needed to make the system more effective and efficient. The method that has been proposed in this study still may has more potential for further studies. Some of these possible studies are listed below:

1. The message signal used for transmission was a very low-frequency signal in most cases. Further investigation is necessary to modify the proposed method to be used to support higher bandwidth.
2. The method was mostly implemented using the identical FONNs. Therefore, to further the study, different values of fractional-order can also be carried out.
3. Instead of symmetric cryptography, asymmetric cryptography is implemented via chaos synchronization for secure communication.

Universiti Malaya

REFERENCES

Abel, A., & Schwarz, W. (2002). Chaos communications-principles, schemes, and system analysis. *Proceedings of the IEEE*, *90*(5), 691–710.

Afraimovich, E., & Smirnov, V. (1987). Polarization of a radio signal reflected from the subauroral ionosphere. *Geomagnetism and Aeronomy*, *27*, 835–837.

Afraimovich, V., Verichev, N., & Rabinovich, M. I. (1986). Stochastic synchronization of oscillation in dissipative systems. *Radiophysics and Quantum Electronics*, *29*(9), 795–803.

Agiza, H., & Matouk, A. (2006). Adaptive synchronization of chua's circuits with fully unknown parameters. *Chaos, Solitons & Fractals*, *28*(1), 219–227.

Aguila-Camacho, N., Duarte-Mermoud, M. A., & Gallegos, J. A. (2014). Lyapunov functions for fractional order systems. *Communications in Nonlinear Science and Numerical Simulation*, *19*(9), 2951–2957.

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

Alvarez, G., Li, S., Montoya, F., Pastor, G., & Romera, M. (2005). Breaking projective chaos synchronization secure communication using filtering and generalized synchronization. *Chaos, Solitons & Fractals*, *24*(3), 775–783.

Alvarez, G., Montoya, P., Pastor, G., & Romera, M. (1999). Chaotic cryptosystems. In *Proceedings IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology* (pp. 332–338).

Antonik, P., Gulina, M., Pauwels, J., & Massar, S. (2018). Using a reservoir computer to learn chaotic attractors, with applications to chaos synchronization and cryptography. *Physical Review E*, *98*(1), 012215.

Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., . . . Shore, K. A. (2005). Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature*, *438*(7066), 343–346.

Ashwin, P. (2003). Synchronization from chaos. *Nature*, *422*(6930), 384–385.

Bacciotti, A., & Rosier, L. (2006). *Liapunov functions and stability in control theory*. Springer Science & Business Media.

Bai, E.-W., & Lonngren, K. E. (1997). Synchronization of two systems using active control. *Chaos, Solitons & Fractals*, *8*(1), 51–58.

Bao, H.-B., & Cao, J.-D. (2015). Projective synchronization of fractional-order memristor-

Universiti Malaya

based neural networks. *Neural Networks*, *63*, 1–9.

Beth, T., Lazic, D. E., & Mathias, A. (1994). Cryptanalysis of cryptosystems based on remote chaos replication. In *Annual International Cryptology Conference* (pp. 318–331).

Blekhman, I., Landa, P. S., & Rosenblum, M. G. (1995). Synchronization and chaotization in interacting dynamical systems. *Applied Mechanics Reviews*, *48*, 733–752.

Cao, J., Wang, Z., & Sun, Y. (2007). Synchronization in an array of linearly stochastically coupled networks with time delays. *Physica A: Statistical Mechanics and its Applications*, *385*(2), 718–728.

Chen, D., Zhang, R., Sprott, J., Chen, H., & Ma, X. (2012). Synchronization between integer-order chaotic systems and a class of fractional-order chaotic systems via sliding mode control. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *22*(2), 023130.

Chen, G., & Dong, X. (1993). From chaos to order—perspectives and methodologies in controlling chaotic nonlinear dynamical systems. *International Journal of Bifurcation and Chaos*, *3*(06), 1363–1409.

Cheng, C.-J., Liao, T.-L., Yan, J.-J., & Hwang, C.-C. (2006). Exponential synchronization of a class of neural networks with time-varying delays. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *36*(1), 209–215.

Chua, L. O., Wu, C. W., Huang, A., & Zhong, G.-Q. (1993). A universal circuit for studying and generating chaos. i. routes to chaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *40*(10), 732–744.

Colet, P., & Roy, R. (1994). Digital communication with synchronized chaotic lasers. *Optics Letters*, *19*(24), 2056–2058.

Cuomo, K. M., & Oppenheim, A. V. (1993). Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, *71*(1), 65.

Cuomo, K. M., Oppenheim, A. V., & Isabelle, S. H. (1992). *Spread spectrum modulation and signal masking using synchronized chaotic systems*. Research Laboratory of Electronics, Massachusetts Institute of Technology.

Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). 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.

Dedieu, H., Kennedy, M. P., & Hasler, M. (1993). 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.

Universiti Malaya

Ding, Z., & Shen, Y. (2016). Projective synchronization of nonidentical fractional-order neural networks based on sliding mode controller. *Neural Networks*, *76*, 97–105.

Epstein, I. R. (1983). Oscillations and chaos in chemical systems. *Physica D: Nonlinear Phenomena*, *7*(1-3), 47–56.

Erneux, T. (2009). *Applied delay differential equations* (Vol. 3). Springer Science & Business Media.

Feki, M., & Gain, R. (2011). Synchronizing fractional order chaotic systems with an integer order observer. In *Eighth International Multi-Conference on Systems, Signals & Devices* (pp. 1–5).

Fridman, E. (2006). A new lyapunov technique for robust control of systems with uncertain non-small delays. *IMA Journal of Mathematical Control and Information*, *23*(2), 165–179.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, *8*(06), 1259–1284.

Fujisaka, H., & Yamada, T. (1983). Stability theory of synchronized motion in coupled-oscillator systems. *Progress of Theoretical Physics*, *69*(1), 32–47.

Ghosh, D., Banerjee, S., & Chowdhury, A. R. (2007). Synchronization between variable time-delayed systems and cryptography. *EPL (Europhysics Letters)*, *80*(3), 30006.

Gibbs, H. M., Hopf, F. A., Kaplan, D., & Shoemaker, R. L. (1981). Observation of chaos in optical bistability. *Physical Review Letters*, *46*(7), 474.

Gotz, M., Kelber, K., & Schwarz, W. (1997). Discrete-time chaotic encryption systems. i. statistical design approach. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *44*(10), 963–970.

Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1991). A secret key cryptosystem by iterating a chaotic map. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 127–140).

Hale, J. K., & Lunel, S. M. V. (1993). Near equilibrium and periodic orbits. In *Introduction to Functional Differential Equations* (pp. 302–330). Springer.

Hartley, T. T., Lorenzo, C. F., & Qammer, H. K. (1995). Chaos in a fractional order chua's system. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *42*(8), 485–490.

Hasimoto-Beltrán, R. (2008). High-performance multimedia encryption system based on chaos. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *18*(2), 023110.

He, Y., Liu, G., & Rees, D. (2007). New delay-dependent stability criteria for neural networks with time-varying delay. *IEEE Transactions on Neural Networks*, *18*(1),

Universiti Malaya

310–314.

He, Y., Liu, G.-P., Rees, D., & Wu, M. (2007). Stability analysis for neural networks with time-varying interval delay. *IEEE Transactions on Neural Networks*, *18*(6), 1850–1854.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, *50*(1), 69–77.

Hegazi, A., Agiza, H., & El-Dessoky, M. (2002). Adaptive synchronization for rössler and chua's circuit systems. *International Journal of Bifurcation and Chaos*, *12*(07), 1579–1597.

Hwang, C., Leu, J.-F., & Tsay, S.-Y. (2002). A note on time-domain simulation of feedback fractional-order systems. *IEEE Transactions on Automatic Control*, *47*(4), 625–631.

Ikeda, K., & Matsumoto, K. (1987). High-dimensional chaotic behavior in systems with time-delayed feedback. *Physica D: Nonlinear Phenomena*, *29*(1-2), 223–235.

Jacobo, A., Soriano, M. C., Mirasso, C. R., & Colet, P. (2010). Chaos-based optical communications: Encryption versus nonlinear filtering. *IEEE Journal of Quantum Electronics*, *46*(4), 499–505.

Jia, S., Hu, C., Yu, J., & Jiang, H. (2018). Asymptotical and adaptive synchronization of cohen–grossberg neural networks with heterogeneous proportional delays. *Neurocomputing*, *275*, 1449-1455.

Karimi, H. R., & Gao, H. (2008). Mixed h2/h_∞ output-feedback control of second-order neutral systems with time-varying state and input delays. *ISA Transactions*, *47*(3), 311–324.

Karimi, H. R., & Gao, H. (2009). New Delay-Dependent Exponential H_∞ Synchronization for Uncertain Neural Networks With Mixed Time Delays. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *40*(1), 173–185.

Keyong, S., Ruixuan, B., Wang, G., Qiutong, W., & Yi, Z. (2019). Passive synchronization control for integer-order chaotic systems and fractional-order chaotic systems. In *2019 Chinese Control Conference (CCC)* (pp. 1115–1119).

Kloeden, P. E., & Mees, A. I. (1985). Chaotic phenomena. *Bulletin of Mathematical Biology*, *47*(6), 697–738.

Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6–21.

Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O., & Parlitz, U. (1992). Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*, *2*(03), 709–713.

Universiti Malaya

Kocarev, L., Jakimoski, G., Stojanovski, T., & Parlitz, U. (1998). From chaotic maps to encryption schemes. In *Proceedings of the 1998 IEEE International Symposium on Circuits and Systems ISCAS* (Vol. 4, pp. 514–517).

Kolmogorov, A. N. (1941). The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, *30*, 301–305.

Kulkarni, D., & Amritkar, R. (2001). Decoding of signal from phase modulated unstable periodic orbit. *International Journal of Bifurcation and Chaos*, *11*(12), 3133–3136.

Kuramoto, Y. (2003). *Chemical oscillations, waves, and turbulence*. Courier Corporation.

Latiff, F. N. A., Othman, W. A. M., & Kumaresan, N. (2020). Synchronization of delayed integer order and delayed fractional order recurrent neural networks system with active sliding mode. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, *11*(12), 1–15.

Li, C., & Deng, W. (2007). Remarks on fractional derivatives. *Applied Mathematics and Computation*, *187*(2), 777-784.

Li, C., Liao, X., & Zhang, R. (2005). Delay-dependent exponential stability analysis of bi-directional associative memory neural networks with time delay: an LMI approach. *Chaos, Solitons & Fractals*, *24*(4), 1119–1134.

Li, C., Sun, W., & Kurths, J. (2007). Synchronization between two coupled complex networks. *Physical Review E*, *76*(4), 046204.

Li, Y., & Li, C. (2016). Complete synchronization of delayed chaotic neural networks by intermittent control with two switches in a control period. *Neurocomputing*, *173*, 1341-1347.

Liang, J., & Cao, J. (2004). Global asymptotic stability of bi-directional associative memory networks with distributed delays. *Applied Mathematics and Computation*, *152*(2), 415–424.

Liang, J., & Cao, J. (2007). Global output convergence of recurrent neural networks with distributed delays. *Nonlinear Analysis: Real World Applications*, *8*(1), 187–197.

Liang, J., Wang, Z., & Liu, X. (2008). Exponential synchronization of stochastic delayed discrete-time complex networks. *Nonlinear Dynamics*, *53*(1), 153–165.

Liao, T.-L., & Lin, S.-H. (1999). Adaptive control and synchronization of lorenz systems. *Journal of the Franklin Institute*, *336*(6), 925–937.

Liu, Y., Wang, Z., Liang, J., & Liu, X. (2008). Synchronization and state estimation for discrete-time complex networks with distributed delays. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *38*(5), 1314–1325.

Universiti Malaya

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of Atmospheric Sciences*, *20*(2), 130–141.

Lorenz, E. N. (1995). *The essence of chaos*. USA: Routledge.

Lorenz, H.-W. (1993). *Nonlinear dynamical economics and chaotic motion* (Vol. 334). Springer.

Lyapunov, A. M. (1992). The general problem of the stability of motion. *International Journal of Control*, *55*(3), 531–534.

Mackey, M. C., & Glass, L. (1977). Oscillation and chaos in physiological control systems. *Science*, *197*(4300), 287–289.

Maistrenko, Y., Popovych, O., & Hasler, M. (2000). On strong and weak chaotic partial synchronization. *International Journal of Bifurcation and Chaos*, *10*(01), 179–203.

Massey, D. (1992). Politics and space/time. *New Left Review*(196), 65.

Matouk, A. (2008). Dynamical analysis, feedback control and synchronization of liu dynamical system. *Nonlinear Analysis: Theory, Methods & Applications*, *69*(10), 3213–3224.

Matouk, A., & Agiza, H. (2008). Bifurcations, chaos and synchronization in advp circuit with parallel resistor. *Journal of Mathematical Analysis and Applications*, *341*(1), 259–269.

Matsumoto, T. (1987). Chaos in electronic circuits. *Proceedings of the IEEE*, *75*(8), 1033–1057.

Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, *13*(1), 29–42.

Mirasso, C. R., Colet, P., & García-Fernández, P. (1996). Synchronization of chaotic semiconductor lasers: Application to encoded communications. *IEEE Photonics Technology Letters*, *8*(2), 299–301.

Morgül, Ö., & Feki, M. (1999). A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, *251*(3), 169–176.

Mou, S., Gao, H., Qiang, W., & Chen, K. (2008). New delay-dependent exponential stability for neural networks with time delay. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *38*(2), 571–576.

Oppenheim, A. V., Wornell, G. W., Isabelle, S. H., & Cuomo, K. M. (1992). Signal processing in the context of chaotic signals. In *Proceedings ICASSP-92: 1992 IEEE International Conference on Acoustics, Speech, and Signal Processing* (Vol. 4, pp. 117–120).

Universiti Malaya

Park, J. H., & Won, S. (1999). Asymptotic stability of neutral systems with multiple delays. *Journal of Optimization Theory and Applications*, *103*(1), 183–200.

Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters*, *64*(8), 821.

Pecora, L. M., & Carroll, T. L. (1991). Driving systems with chaotic signals. *Physical Review A*, *44*(4), 2374.

Pérez, G., & Cerdeira, H. A. (1995). Extracting messages masked by chaos. *Physical Review Letters*, *74*(11), 1970.

Pieprzyk, J., Hardjono, T., & Seberry, J. (2003). Private-key cryptosystems. In *Fundamentals of Computer Security* (pp. 69–170). Springer.

Podlubny, I. (1998). *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*. Elsevier.

Podlubny, I. (1999). Fractional-order systems and pi/sup/spl lambda//d/sup/spl mu//-controllers. *IEEE Transactions on Automatic Control*, *44*(1), 208–214.

Pogromsky, A., & Nijmeijer, H. (2001). Cooperative oscillatory behavior of mutually coupled dynamical systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *48*(2), 152–162.

Poincaré, H. (1890). Sur le problème des trois corps et les équations de la dynamique. *Acta Mathematica*, *13*(1), A3–A270.

Poole, C. P., & Safko, J. L. (2001). *Classical mechanics*. Addison Wesley.

Razumikhin, B. (1960). Application of liapunov's method to problems in the stability of systems with a delay. *Automat. i Telemeh*, *21*, 740–749.

Rosenblum, M. G., Pikovsky, A. S., & Kurths, J. (1997). From phase to lag synchronization in coupled chaotic oscillators. *Physical Review Letters*, *78*(22), 4193.

Ruelle, D. (2006). What is a strange attractor. *Notices of the AMS*, *53*(7), 764–765.

Sanchez-Diaz, A., Mirasso, C. R., Colet, P., & Garcia-Fernandez, P. (1999). Encoded gbit/s digital communications with synchronized chaotic semiconductor lasers. *IEEE Journal of Quantum Electronics*, *35*(3), 292–297.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*(4), 656–715.

Sharkovskiĭ, A. (1995). Coexistence of cycles of a continuous map of the line into itself. *International Journal of Bifurcation and Chaos*, *5*(05), 1263–1273.

Universiti Malaya

Shen, Y., & Wang, J. (2007). Noise-induced stabilization of the recurrent neural networks with mixed time-varying delays and markovian-switching parameters. *IEEE Transactions on Neural Networks*, *18*(6), 1857–1862.

Sheu, L.-J., Chen, H.-K., Chen, J.-H., Tam, L.-M., Chen, W.-C., Lin, K.-T., & Kang, Y. (2008). Chaos in the newton–leipnik system with fractional order. *Chaos, Solitons & Fractals*, *36*(1), 98–103.

Short, K. M. (1994). Steps toward unmasking secure communications. *International Journal of Bifurcation and Chaos*, *4*(04), 959–977.

Short, K. M. (1996). Unmasking a modulated chaotic communications scheme. *International Journal of Bifurcation and Chaos*, *6*(02), 367–375.

Short, K. M. (1997). Signal extraction from chaotic communications. *International Journal of Bifurcation and Chaos*, *7*(07), 1579–1597.

Shujun, L. (2003). Analyses and new designs of digital chaotic ciphers. *School of Electronic and Information Engineering, Xi'an Jiaotong University*.

Skinner, J. E. (1994). Low-dimensional chaos in biological systems. *Bio/technology*, *12*(6), 596–600.

Song, Q., Cao, J., & Zhao, Z. (2006). Periodic solutions and its exponential stability of reaction–diffusion recurrent neural networks with continuously distributed delays. *Nonlinear analysis: Real World Applications*, *7*(1), 65–80.

Song, Q., & Wang, Z. (2008). Neural networks with discrete and distributed time-varying delays: a general stability analysis. *Chaos, Solitons & Fractals*, *37*(5), 1538–1547.

Stamova, I. (2014). Global mittag-leffler stability and synchronization of impulsive fractional-order neural networks with time-varying delays. *Nonlinear Dynamics*, *77*(4), 1251-1260.

Stamova, I., & Stamov, G. (2017). Mittag-leffler synchronization of fractional neural networks with time-varying delays and reaction–diffusion terms using impulsive and linear controllers. *Neural Networks*, *96*, 22-32.

Taherion, S., & Lai, Y.-C. (1999). Observability of lag synchronization of coupled chaotic oscillators. *Physical Review E*, *59*(6), R6247.

Takens, F. (1988). *An introduction to chaotic dynamical systems*. Springer.

Tavazoei, M. S., & Haeri, M. (2007a). A necessary condition for double scroll attractor existence in fractional-order systems. *Physics Letters A*, *367*(1-2), 102–113.

Tavazoei, M. S., & Haeri, M. (2007b). Unreliability of frequency-domain approximation in recognising chaos in fractional-order systems. *IET Signal Processing*, *1*(4), 171–181.

Universiti Malaya

Tavazoei, M. S., & Haeri, M. (2008). Limitations of frequency domain approximation for detecting chaos in fractional order systems. *Nonlinear Analysis: Theory, Methods & Applications*, *69*(4), 1299–1320.

Teh, J. S., Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, *50*, 102421.

Tenny, R., & Tsimring, L. S. (2004). Steps towards cryptanalysis of chaotic active/-passive decomposition encryption schemes using average dynamics estimation. *International Journal of Bifurcation and Chaos*, *14*(11), 3949–3968.

Vinagre, B., Podlubny, I., Hernandez, A., & Feliu, V. (2000). Some approximations of fractional order operators used in control theory and applications. *Fractional Calculus and Applied Analysis*, *3*(3), 231–248.

Wang, Q., Duan, Z., Perc, M., & Chen, G. (2008). Synchronization transitions on small-world neuronal networks: Effects of information transmission delay and rewiring probability. *EPL (Europhysics Letters)*, *83*(5), 50008.

Wang, Y., Zhang, J., Mori, S., & Nathans, J. (2006). Axonal growth and guidance defects in frizzled3 knock-out mice: a comparison of diffusion tensor magnetic resonance imaging, neurofilament staining, and genetically directed cell labeling. *Journal of Neuroscience*, *26*(2), 355–364.

Wang, Z., Shu, H., Liu, Y., Ho, D. W., & Liu, X. (2006). Robust stability analysis of generalized neural networks with discrete and distributed time delays. *Chaos, Solitons & Fractals*, *30*(4), 886–896.

Wu, L., Feng, Z., & Zheng, W. X. (2010). Exponential stability analysis for delayed neural networks with switching parameters: average dwell time approach. *IEEE Transactions on Neural Networks*, *21*(9), 1396–1407.

Wu, Y.-P., & Wang, G.-D. (2013). Synchronization between fractional-order and integer-order hyperchaotic systems via sliding mode controller. *Journal of Applied Mathematics*, *2013*.

Xue, D., & Chen, Y. (2002, Jun). A comparative introduction of four fractional order controllers. In *Proceedings of the 4th World Congress on Intelligent Control and Automation* (Vol. 4, pp. 3228–3235). IEEE. doi: 10.1109/WCICA.2002.1020131

Yang, L.-x., He, W.-s., & Liu, X.-j. (2011). Synchronization between a fractional-order system and an integer order system. *Computers & Mathematics with Applications*, *62*(12), 4708–4716.

Yang, T., Wu, C. W., & Chua, L. O. (1997). Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *44*(5), 469–472.

Universiti Malaya

Yang, T., Yang, L.-B., & Yang, C.-M. (1998). Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A*, *245*(6), 495–510.

Yang, X., Liu, H., & Li, S. (2017). Synchronization of fractional-order and integer-order chaotic (hyper-chaotic) systems with different dimensions. *Advances in Difference Equations*, *2017*(1), 1–16.

Yassen, M. (2003). Adaptive control and synchronization of a modified chua's circuit system. *Applied Mathematics and Computation*, *135*(1), 113–128.

Yu, J., Hu, C., Jiang, H., & Fan, X. (2014). Projective synchronization for fractional neural networks. *Neural Networks*, *49*, 87–95.

Zeng, Z., & Wang, J. (2006). Improved conditions for global exponential stability of recurrent neural networks with time-varying delays. *IEEE Transactions on Neural Networks*, *17*(3), 623–635.

Zhan, M., Wang, X., Gong, X., Wei, G., & Lai, C.-H. (2003). Complete synchronization and generalized synchronization of one-way coupled time-delay systems. *Physical Review E*, *68*(3), 036208.

Zhang, H., & Wang, Y. (2008). Stability analysis of markovian jumping stochastic cohen–grossberg neural networks with mixed time delays. *IEEE Transactions on Neural Networks*, *19*(2), 366–370.

Zhao, H. (2004a). Existence and global attractivity of almost periodic solution for cellular neural network with distributed delays. *Applied Mathematics and Computation*, *154*(3), 683–695.

Zhao, H. (2004b). Global asymptotic stability of hopfield neural network involving distributed delays. *Neural Networks*, *17*(1), 47–53.

Zhao, Y., Gao, H., & Mou, S. (2008). Asymptotic stability analysis of neural networks with successive time delay components. *Neurocomputing*, *71*(13-15), 2848–2856.

Zhou, C.-S., & Chen, T.-L. (1997). Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. *Physics Letters A*, *234*(6), 429–435.

Universiti Malaya