2006

Observer-based chaos synchronization for secure communications

Sun, Shuwen

Observer-based Chaos Synchronization for Secure Communications

by

Shuwen Sun

Under the Supervision of Dr. Abdelhamid Tayebi

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

Master of Science
in Control Engineering

Lakehead University, Thunder Bay, Ontario, Canada

July 2006

Your file Votre référence
ISBN: 978-0-494-21541-8
Our file Notre référence
ISBN: 978-0-494-21541-8

Abstract

Chaos, with reference to chaos theory, refers to an apparent lack of order in a system that, nevertheless, obeys particular laws or rules. The chaotic signals generated by chaotic systems have some properties such as randomness, complexity and sensitive dependence on initial conditions, which make them particularly suitable for secure communications. Since the 1990s, the problem of secure communication, based on chaos synchronization, has been thoroughly investigated and many methods, for instance, robust and adaptive control approaches, have been proposed to realize the chaos synchronization. However, from systems theory perspective, it may seem obvious that many robust and adaptive control methods could be considered for possible attacks against secure communication.

In this thesis, we introduce the concept of secure chaos synchronization from the control theoretic view point. A new secure communication system, based on the chaos synchronization, is proposed and its security is analyzed, both theoretically and numerically.

Acknowledgements

I would like to express my sincere appreciation to my advisor, Dr. Abdelhamid Tayebi, for his guidance and support during the years of my graduate studies. He has been of inestimable help in formulating my understanding of control theory.

I also want to thank all the professors and graduate students of the faculty of Engineering of Lakehed University for their kind help to my thesis.

Finally, I would like to thank my family and my wife Zhuoli for their endless love and support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Nonlinear systems, which have attracted heightened interest and refreshed vigor since the last decades, have always played a crucial role in the study of natural phenomena. The interest in nonlinear system research is mainly boosted by the discovery of chaos. One of the basic principles of science, concerning deterministic systems, is that the behaviour of these systems can be predicted. The discovery of chaos phenomena, however, has proven that this point of view may not be true all the time.

Chaos, with reference to chaos theory, is a relatively new discipline, with boundless applications in all areas of science and technology such as: mathematics, physics, biology, chemistry as well as engineering. Chaos describes a specific range of irregular behaviour of what we consider to be simple, well-behaved systems. The type of behaviour, that in the last few decades has come to be called "chaotic" (Li and Yorke 1975), looks erratic and almost random, which is quite similar to the behaviour of a system strongly influenced by the outside, random noise. Nevertheless, chaotic systems, defined as dynamical systems having such random-like behaviour, are sometimes very simple systems, almost free of noise. In fact, these systems are essentially deterministic; that is, given the initial condition and the equations describing a system, the future behaviour of the system can be predicted for all time.

One of the most essential elements in chaotic dynamical systems is the unpredictability, which is caused by the extreme sensitivity to initial conditions and control parameters, otherwise known to the world as the "butterfly-effect" (Lorenz 1963). This concept means that with a nonlinear chaotic system, even infinitesimal changes in initial conditions or control parameters will result in dramatically different output of that system. This makes the evolution of the nonlinear chaotic system become entirely "unpredictable" as time elapses (Lorenz 1963; Lorenz 1993).

Another salient feature about chaotic systems is their ability to synchronize with each other under some certain conditions. Since the long-term behaviour of chaotic dynamical systems is impossible to predict, such a synchronization seems impossible. However, it has been proved that under certain circumstances two or more chaotic dynamical systems, which are coupled together and evolving from different initial conditions, can undergo identical motion (Pecora and Carroll 1990; Pecora and Carroll 1991).

1.1 Motivation

Currently, along with the rapid advancement of information technology, computers have become major components of information technology for a variety of applications, such as communications, electronic mail, on-line business and others. Moreover, the Internet and communication systems have become another important component of information technology to provide connectivity at global and local scales, for the sharing of various information and data. This leads to an explosive increase in transmission of messages containing the useful information through different ways. It is no surprise then, in such transmission, implementing and maintaining security and privacy is a prerequisite to protect the information as well as the systems involved in the transmission. Cryptography becomes necessary when higher security and privacy are specially required, especially when the message is transmitted over any untrusted medium, which includes any network, particularly, the Internet. The main objective of cryptography is to develop a cryptosystem, which keeps the transmission information secret and tamper-proof; protects information from unauthorized parties; prevents fraud; and ensures personal privacy. Therefore, in light of their important role, cryptosystems have become an indispensable part of modern information technology.

Chaotic systems have several interesting features such as the ergodicity, randomness, nonperiodicity and sensitive dependence on initial conditions (Lasota and Mackey 1997; Hilborn 1994), which make them very attractive to the cryptographist. In fact, some researchers have pointed out that such significant properties can be connected with several cryptographic primitive characters such as "diffusion" and "confusion" required by modern cryptography (Fridrich 1998; Kocarev *et al.* 1998; Álvarez *et al.* 1999). Interestingly, the idea of using chaos in cryptography is not novel and can be traced back to Shannon's classic paper titled "Communication Theory of Secrecy Systems" published in 1949 (Shannon 1949). Of course, he could not use the term chaos; he just mentioned that the good mixing transformations, used in a good secrecy system, depend on their arguments in a "sensitive" way. The good mixing transformations can be considered as chaotic maps or equations bounded in limited phase space with positive Lyapunov exponents. In fact, from an algorithmic point of view, any good cryptosystem can be regarded as a chaotic or pseudo-chaotic system (Chirkikov and Vivaldi 1999), since perfect cryptographic properties are ensured by pseudo-random disorder, generated from deterministic encryption operations, which is just like chaos generated from chaotic dynamical systems (Brown and Chua 1996). In (Götz *et al.* 1997), it has been shown that some conventional cryptosystems can present chaotic behaviour. This definitely reveals that there exists a tight relationship between chaos and cryptography, so it is a natural idea to use chaos and chaotic systems to enrich the design of new chaos-based cryptosystems.

In the last few decades, the construction of chaos-based cryptosystems has attracted a great deal of attention, and plenty of chaotic cryptosystems have been developed, among which two main design paradigms for two different purposes can be found in the literature: the discrete-time chaotic cryptosystem and the continuous-time chaotic cryptosystem.

Discrete-time chaotic cryptosystems, as the name suggest, is used to encrypt the digital information by employing discrete-time chaotic dynamical systems. In this application, discrete-time chaotic systems are usually used as the pseudo-random bit generators, which serve as a one-time pad for encrypting the information. The use of discrete-time chaotic systems for the encryption purpose has been done for the first time by Matthews (Matthews 1989). In his approach, a one-dimensional chaotic map, exhibiting chaotic behaviour for a range of initial conditions and control parameters, has been utilized to generate a sequence of pseudo-random numbers in order to encrypt and decrypt the message. Shortly thereafter, in 1990, a cryptosystem based on a piecewise linear chaotic Tent map was developed by Habutsu with his colleague (Habutsu *et al.* 1991), where the parameter of the Tent map was used as a secret key, and the encryption and decryption were achieved by performing the inverse and forward iterations of the chaotic Tent map, respectively. A great number of other discrete chaotic cryptographic algorithms have also been proposed in the recent years; see (Li *et al.* 2001), and (Masuda and Aihara 2002), for a more comprehensive description of the discrete-time chaotic cryptosystems.

Continuous-time chaotic cryptosystems, on the other hand, aim mainly to use continuous-time chaotic dynamical systems to generate the broadband, nonperiodic and noise-like chaotic signals for secure communications, where message signals, usually continuous signals, are hidden into the chaotic signal at the transmitter side, and recovered at the receiver side through the chaos synchronization technique.

The idea of utilizing synchronous chaotic systems for secure communications was first discovered by Pecora and Carroll (Pecora and Carroll 1990). They reported that certain chaotic systems can be decomposed into two subsystems: a drive subsystem and a stable response subsystem that synchronize when they are coupled with a common drive signal. After that, vast amounts of research of chaos synchronization and its application to secure communications have been presented in the literature. Adhering to the Pecora-Carroll drive-response concept, several chaotic secure communication systems have been successfully established (Chua *et al.* 1992; Oppenheim *et al.* 1992; Ogorzalek 1993; Halle *et al.* 1993). Furthermore, based on Lyapunov stability criterion, linear or nonlinear state feedback is another useful way to achieve synchronization of two isolated chaotic systems for secure communication applications (Wu and Chua 1994). More recently, some traditional problems in systems and control theory have been linked to chaos synchronization (Morgül and Solak 1996; Nijmeijer and Mareels 1997; Morgül 1999). This treatment opens another world of the synchronization problem for chaotic secure communication purpose. For example, a nonlinear state observer design approach is developed to solve the chaotic synchronization problem of a class of chaotic systems in (Grassi and Mascolo 1997; Liao and Huang 1999; Alvarez-Ramirez *et al.* 2002). Moreover, in (Liao and Lin, 1999; Fradkov *et al.* 1999; Lian *et al.* 2002), the adaptive observer design method is presented to design the receiver system for a secure communication system to deal with the problem of synchronizing two chaotic systems with mismatching parameters, since the adaptive mechanism can compensate for the effects of those parametric uncertainties.

Following these approaches, the proposed chaotic secure communication methods may be classified as: chaotic masking, chaotic modulation and chaotic switching. In the first case, the private message signal is just added to the chaotic carrier signal (Pecora and Carroll 1991; Cuomo and Oppenheim 1993; Lian *et al.* 2002). In the second case, not only is the message signal added to the chaotic carrier signal, but also the states of the chaotic generator are modulated by the message signal through an invertible procedure; thus, the generated chaotic signal inherently contains the information of the message signal (Halle *et al.* 1993; Liao and Huang 1999; Boutayeb *et al.* 2002). In the third case, chaotic switching is based on the requirement of two distinct chaotic systems for bits "1" and "0". The transmission signal is obtained by switching between these two chaotic systems according to either a bit "1" or "0" of the message signal being transmitted (Cuomo and Oppenheim 1993; Kolumbán *et al.* 1997; Murali *et al.* 2001). Clearly, the two former approaches are designed for transmitting analog signals, while the latter is designed for transmitting digital signals.

Although being demonstrated successfully in computer simulations and hardware implementation, the preliminary application of chaotic systems for the secure communications has a low level of security because an intruder can extract the hidden message signal from the transmission signal by using different unmasking techniques (Short 1996). To overcome the problem of unmasking the message signal from the chaotic transmission signal, several different approaches have been recently introduced to improve the security of the chaotic cryptosystem. For instance, a more advanced encryption scheme of using multiple chaotic signals is developed in (Yang *et al.* 1997), and in (Grassi and Mascolo 1999; Murali *et al.* 2001), the authors presented an idea of achieving secure transmission of the message signal by considering the fact that encrypting the chaotic signal is as important as encrypting the message signal. Therefore, for this purpose, the conventional cryptographic method and chaos synchronization are combined together for the design of a chaotic cryptosystem, which can offer higher security and privacy for the users.

Nevertheless, since all these chaotic secure communication systems, mentioned above, are based on the synchronization properties of simple chaotic systems, the key issue for these approaches is the security of the synchronization. This means the synchronization of chaotic systems should play a crucial role in preventing the private message from being read by any intruder during the transmission procedure. Unfortunately this problem did not get the deserved consideration when synchronization-based secure communication schemes were proposed in the past. For example, in (Suykens *et al.* 1999; Li and Shi 2003), some researchers have proposed the robust synchronization and adaptive synchronization theory to deal with the parameter mismatch or unknown parameter problems. As we know, the value of parameters of the chaotic system is usually considered as the secret "Key" for the synchronization between the transmitter and the receiver. These robust and adaptive approaches, however, give a possibility to measure the "Key". This means that by using the robust and adaptive techniques, an intruder can design a receiver system, which can synchronize with the transmitter system without the precise knowledge of the "key". Therefore, from the viewpoint of systems theory, many adaptive or robust control methods may be considered for possible attacks against secure communications and encryption schemes. In light of this, the concept of secure synchronization with respect to adaptive and robust control methods has been introduced in (Čelikovský and Chen 2005).

1.2 Thesis Objective

Inspired by the earlier works of other researchers, in this thesis, we further study the behaviour of chaotic dynamical systems and its application in modern cryptography. The primary objective of this thesis is to develop a chaotic secure communication scheme based on the synchronization of two continuous-time chaotic dynamical systems, which can provide higher security level for the transmission of various kind of messages. Moreover, since the signal propagation delay is unavoidable for any real communication system, the second objective is to verify the validity of the developed communication system with an unknown propagation time-delay involved during the transmission of message signals. In order to fulfill these objectives, we first analyze the security of several synchronization approaches for certain chaotic systems proposed in the literature, from the control theory viewpoint, since chaos synchronization is the basis of the design of secure communication systems. As we know, due to the fact that chaotic systems are very sensitive to initial conditions and control parameters, a very general way used in almost all the chaotic secure communication schemes is to set the values of system parameters as the secret "Key", which means that only the transmitter and the receiver in a communication system using the exact same "Key" can realize the synchronization. Some synchronization methods, however, have been proposed without this consideration, implying that even with a different "Key" the synchronization can still be achieved. This means that the security requirement for these synchronization methods is not satisfied.

Since the security property is the most important aspect of chaos synchronization, the concept of secure synchronization of synchronized chaotic systems, from the control theory point of view, is then presented in detail in order to lay a sound foundation for the later development of the secure communication scheme. Also, based on the generalized Lorenz system, a new chaotic secure communication scheme, which combines the secure synchronization scheme with the conventional cryptographic technique, is developed in this thesis. The analysis of its security is performed from both the control theory viewpoint and the cryptographical viewpoint to verify that the proposed secure communication system can offer a higher security and privacy for the transmission of messages. Finally, the stability of the proposed secure communication system with the time-delay problem is discussed, since the propagation time-delay during the transmission procedure is always exist for any real communication systems.

1.3 Thesis Structure

This research was multidisciplinary and involved several different fields of research: nonlinear dynamics, chaos theory, communications, cryptography and control theory. The first portion of this dissertation provides a comprehensive overview of those fields of research. The second portion provides a detailed description of our research contribution: Designing a new secure communication system based on the secure synchronization scheme.

In Chapter 2, we present a comprehensive overview of chaos and chaotic systems by describing the definition, classification and characteristics of chaos and chaotic systems. Particularly, a class of chaotic systems named generalized Lorenz system is also introduced in this chapter.

Chapter 3 focuses on representing the relationship between chaotic systems with the modern cryptography. Some basic principles of cryptography are introduced, and two different kinds of chaotic cryptosystems are presented.

Chapter 4 is devoted to introducing the methodology of chaos synchronization. There are two major schemes for coupling and synchronizing identical chaotic systems that are investigated in detail, especially the one approached from the control theory point of view, namely, the observer-based synchronization. Further, the application of chaos synchronization for secure communication is discussed, and some examples are provided.

In Chapter 5, attention is turned to designing a new secure communication system on the basis of secure synchronization of chaotic systems. First, a scheme of chaotic secure synchronization using the generalized Lorenz system family as the platform is presented. Then, a new secure communication system is developed and its security is discussed. Furthermore, the validity of the secure communication system is analyzed by taking into account the propagation time-delay problem.

Finally, conclusions are summarized in Chapter 6, where the future work is also mentioned.

Chapter 2

Chaos and Chaotic Systems

As one of the greatest accomplishment in human's history, the differential calculus and the laws of motion discovered by Newton, in the 17th century, gave rise to the deterministic view of nature and then led to a great optimism about our ability to predict the behaviour of dynamical systems. Subsequent generations of scientists believed that the nature of dynamical systems was expected to be completely determined dependent upon the nature of the forces acting on them and upon their initial states.

According to the Newtonian laws of physics, it was assumed that, if the initial condition for any dynamical system could be measured precisely, the behaviour of the dynamical system could be predicted accurately, and that the more accurate the measurements of initial conditions were, the more precise would be the resulting predictions. However, in the early 20th century, Poincaré, a great French mathematician, discovered that in some astronomical systems, there were an unpredictability for the system evolution, which meant that even a small error in the measurement of initial conditions would make the prediction about the system future condition impossible. In fact, this unpredictability is so called "chaos" now. Even though Poincaré could not use the unburned term "chaos" to describe the unpredictability at that time, he did prove mathematically that, even if the measurement could be made much more precise, the unpredictability for outcomes did not shrink along with the inaccuracy of measurement, but remained huge (Poincaré 1892-1899).

Half a century later, Edward Lorenz, a meteorologist at MIT, worked on a project to simulate weather patterns on a computer. He accidentally found the surprising phenomenon that, with some certain parameters, the deterministic system described by ordinary differential equations that he used to theoretically model the motion of atmospheric air flow became unpredictable (Lorenz 1963). This has become known as the phenomenon of chaos. After repeated experimentation, Lorenz revealed the underlying mechanism of chaos: simply formulated systems with only a few variables can display highly complicated behaviour that is unpredictable. This started a new age for humanity's understanding of nature and triggered enthusiasm in the study of chaos phenomenon.

2.1 Examples of Chaos Phenomenon

Humanity's understanding for the natural and social phenomenon originally stems from some particular things or events, and the discovery of chaos is no exception. In this section, we shall briefly introduce the chaos phenomenon through two representative examples of chaotic systems.

2.1.1 The Logistic Map

The first example of chaotic systems is a very simple mathematical model from ecology named the *logistic map*, also called the *logistic equation*, which is often used to describe the growth of biological population. Due to its mathematical simplicity, the simple model continues to be a useful tool for new ideas in chaos study.

The equation of logistic map is given by:

$$x_{n+1} = \mu x_n(1 - x_n) = f(x_n), \qquad n = 1, 2, ... \tag{2.1}$$

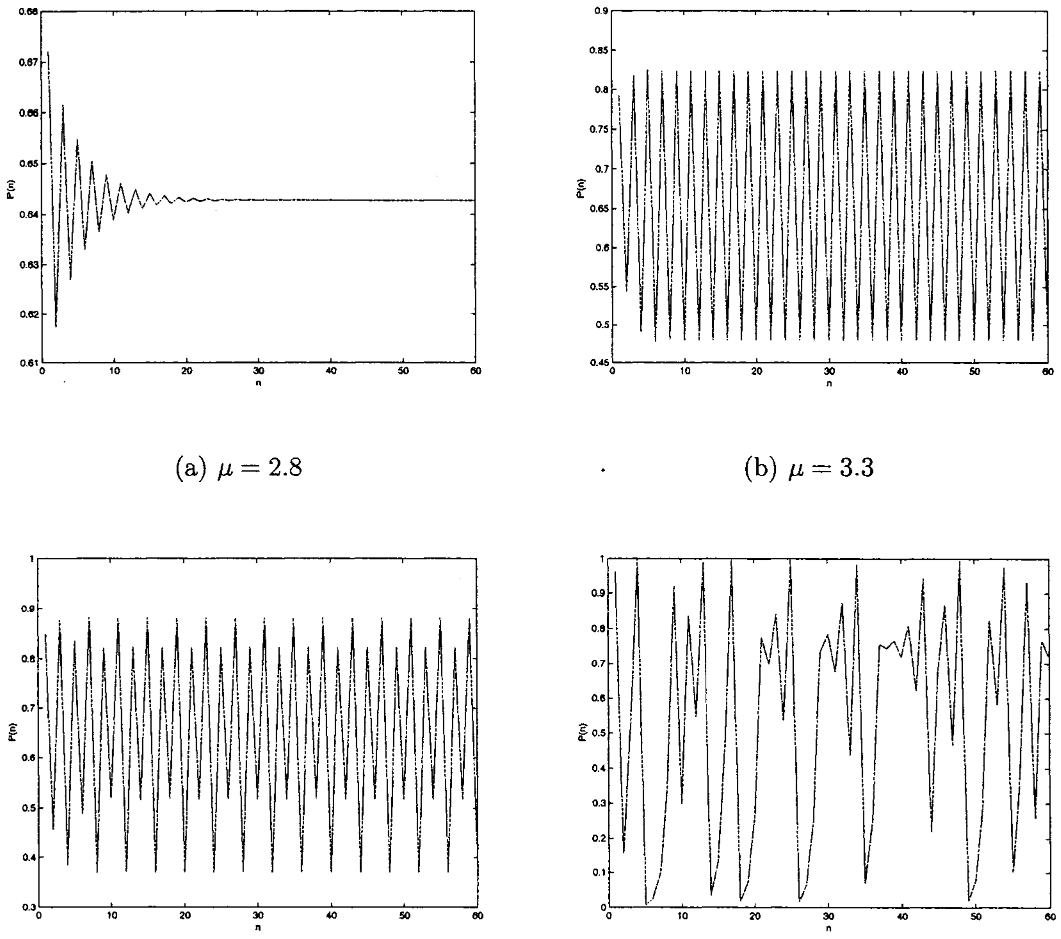
where, μ is a constant depending on the conditions of the ecological environment, and x_n represents the population of a species reproducing in a controlled environment at generation n. To keep the number manageable, we let x_n represent the percentage of some *a priori* upper bound for the population, so $0 \leq x_n \leq 1$ (Kapitaniak 2000). Given this equation with some initial population x_0, it would seem straightforward to predict the behaviour of x_n. As we shall see, however, this is far from the case for certain values of the constant μ. For different values of the parameter μ, the dynamical analysis of the model of the logistic equation can be carried out as follows:

1.) For $0 < \mu \leq 1$, the dynamical characteristics of the logistic equation is very simple, and $x = 0$ is the only equilibrium or fixed point in the range of x, which means that the population of the species decreases and dies.

2.) For $1 < \mu < 3$, there are two equilibrium points for the dynamical system of the logistic equation that are $x = 0$ and $x = 1 - \frac{1}{\mu}$, and the equilibrium point of $x = 0$ becomes a "repelling fixed point" since trajectories that start near $x = 0$ move away from that value. This implies that the population increases for a few generations, then becomes stable, as Figure 2.1(a) shows.

3.) For $3 \leq \mu \leq 4$, the logistic equation presents a complex dynamical behaviour that the values of x oscillate back and forth between two values, and then four, then eight, then sixteen, etc, as shown in Figure 2.1(b,c). Finally, it turns into never settling down to a periodic cycle — instead the long term behaviour is aperiodic, that is *chaos*, as shown in Figure 2.1(d).

It is noticeable that the system has a periodic behaviour with $\mu = 3.3$, shown in Figure 2.1(b), and then as the value of the parameter μ changes to $\mu = 3.53$, this periodicity becomes twice that of the behaviour with $\mu = 3.3$, as shown in Figure 2.1(c). This phenomenon refers to the *period-doubling bifurcation*, which is one of the most primary routers to chaos (Reichl 1992).



(a) $\mu = 2.8$

(b) $\mu = 3.3$

(c) $\mu = 3.53$

(d) $\mu = 4.0$

Figure 2.1: Logistic map with different parameters

2.1.2 The Lorenz Equations

Our second example of chaotic systems is the highly simplified model of a convecting fluid, originally introduced by E. Lorenz in 1963 (Lorenz 1963). In this paradigmic model, what Lorenz set out to demonstrate was that even a very simple system may have an unusual and unpredictable behaviour. The Lorenz system can be expressed by the following three coupled differential equations:

$$\left\{\begin{array}{lcl} \frac{dx}{dt} & = & -\sigma(x-y) \\ \frac{dy}{dt} & = & -xz+\rho x-y \\ \frac{dz}{dt} & = & xy-\beta z \end{array}\right. \tag{2.2}$$

where state variables x, y, z are related to the physical properties of a convecting fluid, and σ is called the Prandtl number, which is usually set as a value of 10. The parameter β relates to the size of the area represented by this convecting fluid model and it was set to $\beta = \frac{8}{3}$. Finally, ρ, called the Rayleigh number, is the adjustable control parameter.

This model, also called the *Lorenz system*, although based on what appears to be a very simple set of differential equations, exhibits very complex behaviour with certain parameters. In the following part we shall explain why this simple dynamical system may present an unusual chaotic behavior.

From the equation (2.2), it can be shown that the equilibrium or fixed points of the Lorenz system satisfy the following condition:

$$\left\{\begin{array}{l} x = y \\ x(\rho-1-z) = 0 \\ x = \pm\sqrt{\beta z} = \pm\sqrt{\beta(\rho-1)} \end{array}\right. \tag{2.3}$$

Notice that, when $\rho < 1$, there is only one fixed point: $O(0,0,0)$. When $\rho > 1$, there are three distinct fixed points, given by:

$$\left\{\begin{array}{l} O(0,0,0) \\ P^{+}(\sqrt{\beta(\rho-1)}, \sqrt{\beta(\rho-1)}, \rho-1) \\ P^{-}(-\sqrt{\beta(\rho-1)}, -\sqrt{\beta(\rho-1)}, \rho-1) \end{array}\right. \tag{2.4}$$

For the fixed point: $O(0,0,0)$, it is easy to obtain the Jacobi matrix evaluated a this point, which is given by:

$$A = \begin{bmatrix} -\sigma & \sigma & 0 \\ \rho & -1 & 0 \\ 0 & 0 & -\beta \end{bmatrix}, \tag{2.5}$$

and the eigenvalue equation

$$(\beta + \lambda)((\sigma + \lambda)(1 + \lambda) - \rho\sigma) = 0, \tag{2.6}$$

with the eigenvalues, given by:

$$\begin{aligned} \lambda_1 &= -\beta \\ \lambda_{2,3} &= 0.5(-(\sigma + 1) \pm \sqrt{(\sigma + 1)^2 - 4\sigma(1 - \rho)}). \end{aligned} \tag{2.7}$$

Clearly, $\lambda_{1,2,3} < 0$ with $\rho < 1$, which means that the fixed point $O(0,0,0)$ is a stable point, as shown in Figure 2.2(a). When $\rho > 1$, from the equation (2.7), it can be concluded that $\lambda_2 > 0$, while $\lambda_3 < 0$, implying that the fixed point $O(0,0,0)$ becomes the saddle point[1].

For the fixed points P^+ and P^-, the Jacobi matrix can be expressed as follows:

$$A = \begin{bmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & -\sqrt{\beta(\rho - 1)} \\ \sqrt{\beta(\rho - 1)} & \sqrt{\beta(\rho - 1)} & -\beta \end{bmatrix}. \tag{2.8}$$

The corresponding eigenvalue equation is given by:

$$\lambda^3 + (\sigma + \beta + 1)\lambda^2 + \beta(\sigma + \rho)\lambda + 2\beta\sigma(\rho - 1) = 0. \tag{2.9}$$

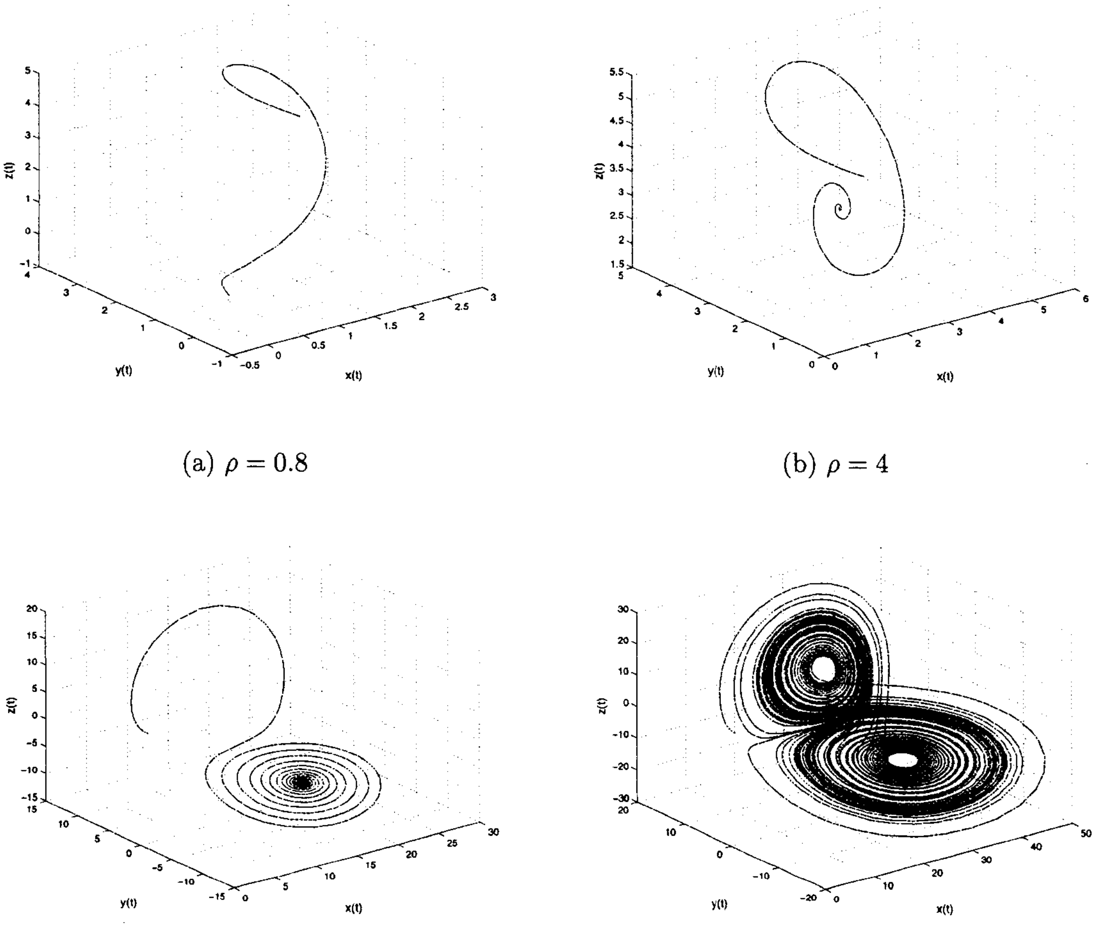
Now, we set a value of parameter ρ as

$$\rho_h = \frac{\sigma(\sigma + \beta + 3)}{\sigma - \beta - 1}. \tag{2.10}$$

For example, if we take the values of parameters as Lorenz did, *i.e.*, $\sigma = 10$ and $\beta = \frac{8}{3}$, then $\rho_h = 24.74$. It can be seen that if the parameter ρ can be chosen such

[1] Saddle point is the fixed point that attract trajectories on one side but repel them on the other.

that $\rho < \rho_h$, the equation (2.9) has three real negative eigenvalues or one real negative eigenvalue and two complex conjugate eigenvalues with the negative real part. This means that P^+ and P^- become attracting fixed points, implying that the trajectories are attracted to one or the other of the two fixed points, as Figure 2.2(b-c) show. On the other hand, if the parameter ρ is chosen as $\rho > \rho_h$, the equation (2.9) has one real negative eigenvalue and two complex conjugate eigenvalues with the positive real part, which means that the fixed points P^+ and P^- become the saddle points, which leads to the chaotic behavior, as shown in Figure 2.2(d).



(a) $\rho = 0.8$

(b) $\rho = 4$

(c) $\rho = 22$

(d) $\rho = 28$

Figure 2.2: Behavior of the Lorenz system with different value of parameters

2.2 Chaos

Through the examples illustrated above we have a vivid comprehension for the chaos phenomenon. Chaos represents a kind of very complex dynamical behaviour more complicated than the familiar steady state or cyclic patterns occuring in a fairly simple system without any external noise and perturbation. Before engaging in more serious discussion about the applications of chaos and chaotic systems, it is necessary to study them theoretically.

2.2.1 What Is Chaos?

There is not yet a unified, universally accepted, rigorous definition of chaos in the current scientific literature; nevertheless, it can be depicted in several different but closely related ways.

Sensitive dependence on initial conditions, which is also named the "Butterfly Effect" (Lorenz 1993), would be considered as the essence of chaos by many scientists. It is believed that the term "chaos" first appeared in the famous paper "Period Three Implies Chaos" published by T. Li and J.A. Yorke to refer to a kind of unusual, and irregular movement, presented by some dynamical systems (Li and Yorke 1975). In 1986, at a conference on mathematical chaos held by the Royal Society in London, mathematicians were asked to define "chaos" that had become the buzzword for their hot research area. After much deliberation, chaos is formally defined as ***the stochastic behaviour occurring in a deterministic system*** (Stewart 1990).

2.2.2 Classification of Chaos

Based on the type of dynamical systems, the chaos phenomenon can be classified into two different categories: continuous-time chaos and discrete-time chaos.

Continuous-Time Chaos

Continuous-time chaos is the erratic and irregular behaviour presented by continuous chaotic systems, for example, the Lorenz system. A very common representation of these systems is that of a system of n-simultaneous first order ordinary differential equations (ODE's) given by the following equation:

$$\frac{dx}{dt} = f(x, t), \tag{2.11}$$

where $x(t) \in \mathbb{R}^n$ are the state variables of the system, and $0 \leq t < \infty$.

Generally, the bounded steady-state behaviour of the continuous-time chaotic systems is not an equilibrium point, not periodic and not quasi-periodic. The limiting trajectories of these systems are attracted to a region in state space which forms a set having fractional dimension and zero volume, which means that these sets are not simple geometrical objects like a circle or a torus. Since the trajectories, in this limiting set, are locally unstable, yet remain bounded within some region of the system's state space, these sets are termed *strange attractor* or *chaotic attractor* (Hilborn 1994).

Clearly, the Lorenz system, introduced above, is a continuous-time chaotic system, and other typical examples of the continuous time chaotic systems are:

The Chua's oscillator, given by

$$\left\{\begin{array}{rcl} \frac{dx}{dt} & = & \alpha(y - x - f(x)) \\ \frac{dy}{dt} & = & x - y + z \\ \frac{dz}{dt} & = & -\beta y - \gamma z, \end{array}\right. \tag{2.12}$$

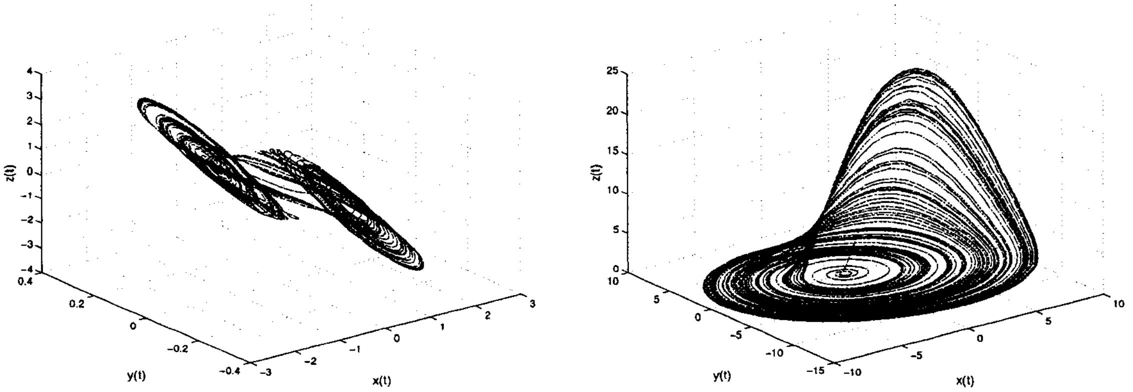
where $f(x) = bx + \frac{1}{2}(a-b)(\mid x+1 \mid - \mid x-1 \mid)$ with $a < b < 0$, and α, β and γ are positive constants.

The Rössler system, given by

$$\left\{\begin{array}{rcl} \frac{dx}{dt} & = & ax + y \\ \frac{dy}{dt} & = & -x - z \\ \frac{dz}{dt} & = & b - cz + yz, \end{array}\right. \tag{2.13}$$

where a, b and c are positive constants.

The trajectories of these two chaotic systems, as shown in Figure 2.3, lie inside bounded but locally unstable regions with wells being the strange attractors mentioned earlier.



(a) Trajectory of Chua's system

(b) Trajectory of Rössler system

Figure 2.3: The chaotic behaviour of the Chua's system and the Rössler system

Discrete-Time Chaos

Now, for discrete-time chaotic systems, similar features that we have seen for the case of continuous-time chaotic systems can also be found, although they follow different formulation. This formulation is expressed by a map f from a set S onto itself, that is,

$$x_{n+1} = f(x_n, \alpha), \quad n = 0, 1, 2, ..., \tag{2.14}$$

where $x_n = \begin{bmatrix} x_{n1} & x_{n2} & \dots & x_{nm} \end{bmatrix}^T$ are the state variables and $\alpha = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_p \end{bmatrix}^T$ are parameters of the system. Generally, the trajectories of the dynamical variables x_n is computed by iterating it; *i.e.*, given an initial value x_0, we can compute x_1 and then using x_1 compute x_2, and so on (Lakshmanan and Rajasekar 2003). Similar to the continuous-time case, the trajectories of discrete chaotic systems are never attracted into an equilibrium point or become periodic but they are aperiodic and random-like, that is, chaotic. The example of the logistic map discussed at the beginning of this chapter is a discrete-time chaotic system.

2.2.3 Characteristics of Chaotic Systems

We now take up briefly the problem of characterizing the chaos phenomenon presented by dynamical systems. Although chaos and chaotic systems have been discovered and extensively studied for fewer than forty years, and the complete knowledge of this very unusual phenomenon has not been obtained yet, there are still three fundamental features that can be used to identify whether or not we face a chaotic system.

(1) Combination of stochasticity and determinism.

Chaotic systems present an internal stochasticity which make the systems locally unstable; namely, the movement of chaotic systems appears irregular, seemingly random and its long-term behaviour can not be predicted. The internal stochasticity is used mainly to distinguish it from the external stochasticity, which is the random motion caused by external random excitation. Usually, a system is considered to be stochastic if some state of the system can appear or disappear, under certain conditions. The internal stochasticity is the stochastic character produced spontaneously by a completely deterministic system under certain system parameter conditions (Chen and Leung 1998).

Thus, although chaos has the internal stochasticity, it should be clear that chaos is not a completely random phenomenon. The chaotic behaviour arises in very simple systems which are essentially deterministic, implying that from moment to moment the system is evolving in a deterministic way, that is, the current state of a system depends upon the previous state in a rigidly determined way. This is in contrast to a random system such as the game of playing dice, where the present state has no causal connection to the previous one (Rasband 1990).

(2) Sensitivity to initial conditions.

What is closely related to the internal stochasticity is the property that chaotic systems are sensitively dependent on initial conditions. For regular dynamical systems, a small variation in initial conditions, caused by intrinsic and external noise perturbation, will result in a small change of the system state. In other words, the evolution of a dynamical system, exhibiting a regular behaviour for two specifications of initial states, that are initially very close together, is always similar and even identic. This makes it possible to predict the future state of that regular system.

On the contrary, for a chaotic system, due to the intrinsic property of internal stochasticity in the system, even the smallest change in initial conditions will lead trajectories diverging from each other exponentially. Such a property is often called the sensitivity to initial conditions.

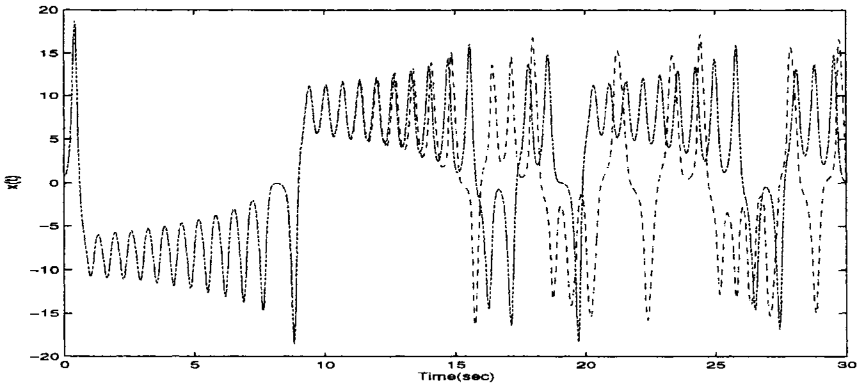


Figure 2.4: Two trajectories started with the initial state $x_0 = 1$ (the broken line) and $x'_0 = 1.001$ (the solid line)

Here, we take the Lorenz system, referring to equation (2.2), as an instance to demonstrate this very important property for chaotic systems. We run the equation with two nearby initial conditions for the same value of parameters that make the Lorenz system behave chaotically, and study the difference between the two resultant solutions of the state variable x. Figure 2.4 shows the trajectories for two initial conditions with $\sigma = 10, \beta = \frac{8}{3}$ and $\rho = 28$. One orbit (the broken line) starts from $x_0 = 1$, and another one (the solid line) starts from $x_0 = 1.001$. As we see, in the beginning, the trajectories overlap, but later, they separate quite a bit, displaying the divergence of nearby trajectories.

Since there is always some imprecision in specifying initial conditions in any real experiment, it can be noticed that the actual future behaviour of a chaotic system is in fact unpredictable. This essential feature of chaotic systems was once vividly referred to the "Butterfly effect" by Lorenz. He stated that, owing to the sensibility of the system to the initial conditions, only a little flap of the butterfly's wings can make the meteorologist unable to predict the weather in a month.

(3) Nonlinearity.

For a linear differential equation, given definite initial conditions would yield a determined solution. This implies that linear systems can not have a chaotic behaviour; therefore, it can be pointed out that chaos only appears in non-linear systems. Certainly, nonlinearity is only a necessary condition but not sufficient for the appearance of chaos, that is, chaotic behaviour must come via non-linear systems but nonlinearity does not necessarily imply chaotic behaviour.

2.2.4 Lyapunov Exponents

As we have seen deterministic chaos is associated with random-like behaviour arising from the sensitivity to initial conditions. Thus, we would like to have some specific quantitative measures in order to recognize chaos and sort out true chaotic behaviour from just noisy behaviour or erratic behaviour due to the complexity. Indeed, there are many such quantitative measures available in the literature for this purpose and the most prominent of them is the *Lyapunov exponents* (Eckmann and Ruelle 1985).

For a chaotic system, the Lyapunov exponents measure essentially the aver-

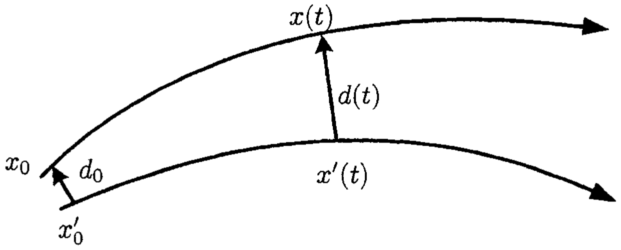


Figure 2.5: Trajectories starting from two nearby points

age divergence rate of nearby trajectories in the phase space. Suppose $x(t)$ is the trajectory of the following nonlinear dynamical system:

$$\dot{x} = f(x), \quad x \in \mathbb{R}^n \tag{2.15}$$

We consider two trajectories $x(t)$ and $x'(t)$, shown in Figure 2.5, in a n-dimensional space starting from two nearby points x_0 and x'_0. Let $d(t) = x(t) - x'(t)$ represents the measure of the distance between the two trajectories $x(t)$ and $x'(t)$. We can find that the change of the distance between the two orbits can be expressed by

$$d(t) \approx d_0 e^{\lambda_i t}, \quad i = 1, 2, ..., n. \tag{2.16}$$

where λ_i are called the Lyapunov exponents. If there exists one positive Lyapunov exponent, the distance between the two trajectories, that is $d(t)$, changes exponentially fast, implying sensitive dependence on initial conditions; therefore, the motion is said to be chaotic. Consequently, finding a single positive Lyapunov exponent is sufficient to confirm the existence of chaos. When more than one of the Lyapunov exponents are positive, then the motion is referred to as *hyperchaos* (Wolf *et al.* 1985).

We often consider computing the largest Lyapunov exponent for a dynamical system, measuring the maximal average rate of separation of nearby states. A simple procedure has been developed by Benettin *et al.*, which estimates the largest Lyapunov exponent directly from the equations governing the system (Benettin *et al.* 1976). In (Wolf *et al.* 1985), the authors generalized Benettin's method to time series data, known as Wolf's method. Although Wolf's paper only discussed the computation of non-negative Lyapunov exponents, it can be used effectively to compute the largest Lyapunov exponent of a chaotic system.

2.3 Generalized Lorenz System

For later convenience, we now introduce a general class of continuous-time chaotic systems, which is called the generalized Lorenz system.

As described above, the original Lorenz system (2.2) was discovered about 40 years ago, which has played a very important role in the study of chaos theory. After that, some other similar chaotic systems have been discovered one after another, such as the Chen system (Chen and Ueta 1999; Ueta and Chen 2000) and the Lü system (Lü and Chen 2002), which are described by (2.17) and (2.18), respectively, as follows

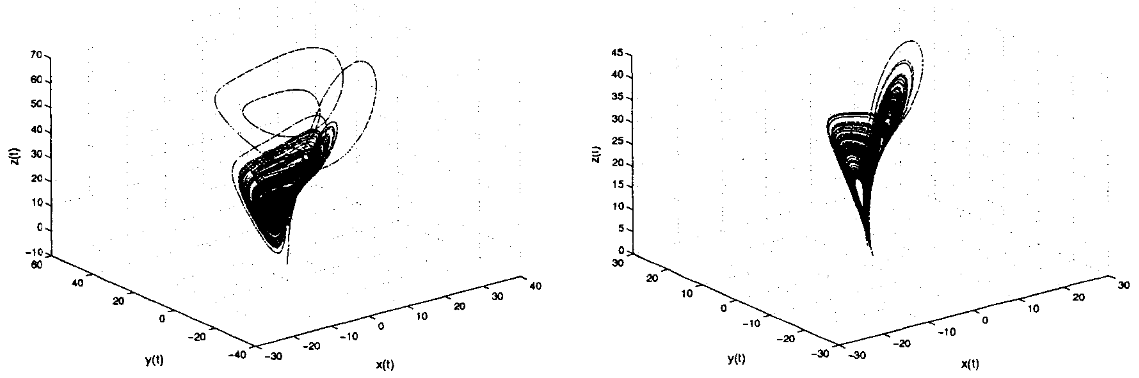
$$\left\{\begin{array}{rcl} \frac{dx}{dt} & = & -\sigma(x-y) \\ \frac{dy}{dt} & = & (\rho-\sigma)x - xz + \rho y \\ \frac{dz}{dt} & = & xy - \beta z \end{array}\right. \tag{2.17}$$

$$\left\{\begin{array}{rcl} \frac{dx}{dt} & = & -\sigma(x-y) \\ \frac{dy}{dt} & = & -xz + \rho y \\ \frac{dz}{dt} & = & xy - \beta z. \end{array}\right. \tag{2.18}$$

With the appropriately chosen parameters system (2.17) and (2.18) can present a very complex behaviour, that is chaotic, as shown in Figure 2.6(a) and Figure 2.6(b).

As a matter of fact, it was pointed out that, according to the system structures, all chaotic systems, mentioned above, can be classified into a very large and general class of relevant chaotic systems, named the *generalized Lorenz system* (GLS) (Čelikovský and Chen 2002), which can be expressed by the following definition.

Definition 2.3.1. *The following general class of three-dimensional nonlinear systems*



(a) Trajectory of Chen system

(b) Trajectory of Lü system

Figure 2.6: The chaotic behaviour of the Chen system and the Lü system

of ordinary differential equations is called a generalized Lorenz system (GLS):

$$\begin{aligned} \dot{x} &= Ax + (Cx)Bx, \\ A = \begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}, \quad B &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \quad \textit{and } C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \end{aligned} \tag{2.19}$$

where $x = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^T$. *The generalized Lorenz system is said to be nontrivial if it has at least one solution that goes neither to a constant nor to infinity nor to a limit cycle.*

In order to render the system (2.19) exhibit chaotic behaviour, the matrix A has to be chosen in such a way that the following inequality must be satisfied:

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0, \tag{2.20}$$

where $\lambda_{1-3} \in \mathbb{R}$ are the eigenvalues of the matrix A (Wiggins 1988). Since this is the only requirement, the generalized Lorenz system (2.19) represents a quite general class of three-dimensional autonomous systems.

Moreover, in the work of (Čelikovský and Chen 2002), the authors found that there exists a nonsingular linear transformation of coordinates, by which the system

(2.19) can be transformed into a form, called the *generalized Lorenz canonical form.* This generalized Lorenz canonical form can be given as the following definition.

Definition 2.3.2. *The following general class of three-dimensional nonlinear system of ordinary differential equations is called a generalized Lorenz canonical form (GLCF):*

$$\begin{aligned} \dot{z} &= Az + (Cz)Bz, \\ A = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}, B &= \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \kappa & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix} \end{aligned} \tag{2.21}$$

where $z = \begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix}^T$ *and* $\kappa \in (-1, \infty)$.

Notice that there is only one scalar real parameter κ in GLCF, which plays a subtle tuning role for the chaotic behaviour of the system. Further study of GLCF reveals that it represents a family of chaotic systems with only one parameter κ. When $-1 < \kappa < 0$, it represents the Chen system and when $\kappa = 0$, it represents the Lü system, while it represents the Lorenz system in the case of $0 < \kappa < \infty$.

Chapter 3

Chaos and Cryptography

Chaos theory, which has brought to our attention a surprising fact that simple dynamical systems are able to exhibit a very complex and unpredictable behaviour, consistently plays an active role in modern cryptography. It is the every special characteristic of random-like behaviour and extreme sensitivity to initial conditions and parameter settings, presented by chaotic systems, that attract people to use chaos as the basis for developing the new cryptosystem, since these properties seem perfectly satisfying the classic Shannon requirements of confusion and diffusion (Shannon 1949). In an ideal cryptosystem, the confusion property decreases the correlativity between the original message and the encrypted message, while the diffusion property guarantees that the data at some coordinates in the input message block is relocated to other coordinates in the output message block (Schneier 1996). In other words, we can say that diffusion changes the position of data in a message, while the data itself is modified during the confusion process. Furthermore, the fast encryption rate and the ease of implementing chaotic systems into both hardware and software also make the application of chaotic dynamics in cryptography particularly attractive.

It is worth to notice that a deep relation between chaos and cryptography has not been established yet. An important difference between chaos and cryptography lies on the fact that systems used in chaos are defined only on real numbers, while cryptography deals with systems defined on finite number of integers (Gickenheimer and Holmes 1983; Schneier 1996). Nevertheless, it is believed that these two disciplines can benefit from each other. Thus, for example, as we show in this chapter, new cryptographic algorithms can be derived from chaotic systems. On the other hand, chaos theory may also benefit from cryptography: new methods and techniques for chaos analysis may be developed from cryptography.

3.1 Basic Principles of Cryptography

Suppose a message is to be transferred from one party (*transmitter*) to another (*receiver*) across some sort of public channel, for instance, the Internet. The two parties, the transmitter and receiver, must cooperate for the transmission of a message to occur. Security aspects come into play when it is desirable or necessary to protect the message transmission from an intruder who may present a threat to confidentiality or authenticity. There are various techniques that can be used to provide the protection for the message, among which the most common method used in practice is the encryption or encryption-like transformation of the message. This technique refers to a very important discipline, called *cryptography*, which is defined to be the science and art of converting a legible message, for the protection against passive and active fraud. An overview of recent developments in the design of conventional cryptographic algorithms is given in (Preneel *et al.* 1998).

In the domain of cryptography, a encryption system is also called a *cipher*, or a *cryptosystem*. The message before being encrypted in any way is called the *plaintext*, and the encrypted message is called the *ciphertext*. The process of disguising a message in such a way as to hide its substance is *encryption*. Similarly, the *decryption* is the process of turning the ciphertext back into the plaintext. The operation of encryption or decryption depends on two components: the *cryptographic algorithm* and the *key*. The cryptographic algorithm is the mathematical function used to encrypt and decrypt the message and the key is a piece of information that controls the operation of the cryptographic algorithm to produce a unique result for a particular user. In key-based cryptosystem, the key is required for both the encryption and decryption processes; the key specifies the particular transformation of the plaintext into the ciphertext, or vice versa, during the process of decryption. Therefore, only if the key being used for decryption matches that being used for encryption procedure, the encrypted message can be decrypted correctly. By following Kerckhoffs's principle, the security of a cryptosystem should only rely on the "key", since adversaries can only recover the plaintext from the observed ciphertext when they get the correct key, and the longer the key, the more time and computing power it takes to crack the cryptographical scheme. It should be emphasized here, that the whole idea behind cryptography is not to make the cryptographical methods crack-proof, but to make breaking it more costly than the value of the message being protected (Schneier 1996).

The most general form of a cryptosystem can be illustrated as Figure 3.1. Denote the plaintext and the ciphertext by P and C, respectively. The encryption procedure can be described as $C = E_{K_e}(P)$, where K_e is the encryption key and $E(\cdot)$ is the encryption function. Analogously, the decryption procedure is $P = D_{K_d}(C)$, where K_d is the decryption key and $D(\cdot)$ is the decryption function.

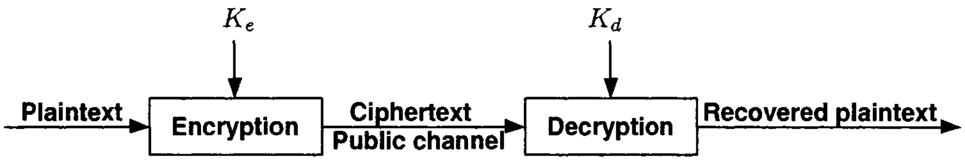


Figure 3.1: The general cryptosystem

3.2 Conventional and Chaotic Cryptography

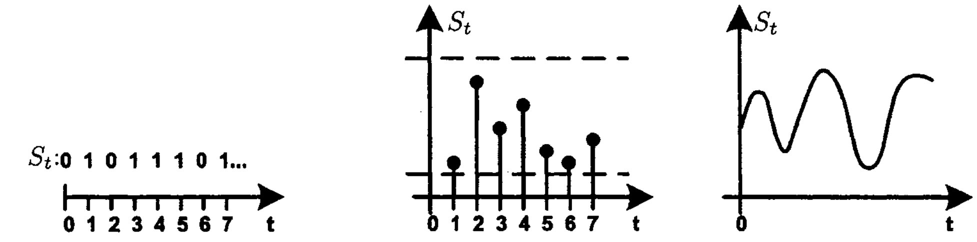
It is clear from the above demonstration that the complexity and the secrecy of the key, used for encryption-decryption purposes, play a major role in the security of the desired cryptosystem. It is used as the tool to complement the security-related transformation in encrypting messages, thereby, it has to be generated as randomly as possible. In other words, the key generators must be able to be operated in the unpredictably random way in order to add more uncertainty into the cryptosystem, making it less vulnerable.

Due to the importance of randomness in cryptography, recently the use of chaos for data encryption has received much more consideration, since chaotic signals are broadband, noise-like and difficult to predict. In fact, chaotic systems are very sensitive to the changes in initial conditions and parameters, which make them behave in an unpredictable pattern. This would be considered a good source of randomness needed for a good cryptosystem. For this reason, in the last ten years many cryptographical approaches based on chaos phenomenon have been proposed and a relatively new branch of modern cryptography has been developed, that is, the *chaotic cryptography* in contrast to the *conventional cryptography.*

When it comes to conventional cryptography, cryptosystems operate on discrete values and in discrete time. In fact, since its ancient beginnings, cryptosystems have been almost exclusively applied to the discrete-value message. These systems range from the so called Caesar cipher, to the well known Vigenère Cipher, up to the modern encryption algorithms, like data encryption standard (DES) or the asymmetrical algorithm by Rivest, Shamir and Adelman (RSA) (Schneier 1996). On the other hand, for chaotic cryptography, the continuous-value message and the usage of continuous-value systems, which may operate in continuous or discrete time, become the crucial points in it. To emphasize its difference to conventional cryptography, we shall use the term continuous-value cryptography synonymously with chaotic encryption or chaotic cryptography. In our understanding, it is just a necessity to utilize nonlinearities and to force the system dynamics into a chaotic operation to fulfill basic cryptographical requirements in the continuous-value case (Dachselt and Schwarz 2001).

Hence, the most important difference between conventional and chaotic cryptosystems is the domain of the involved elementary signals, which is called the *symbol level*, describing the smallest pieces of which the stream of information is composed.

Since conventional cryptosystems operate on discrete signals, the plaintext, the ciphertext and the key are elements of finite sets no matter whether these are bits, integer numbers or some kind of metasymbols. Usually, the symbol level of conventional cryptosystems is binary. On the contrary, in discrete-time continuous-value cryptosystems plaintexts, ciphertexts and keys are in general real values, so the symbol level is the real axis or an interval of it. The case of continuous-time continuous-value cryptosystems is even more complicated. The whole plaintext and ciphertext time functions are usually considered as elements of the symbol level, because there is no strict mathematical method that can be used to break this information down into smaller units. Figure 3.2 illustrates the comparison of symbol level domains for conventional and chaotic cryptosystems.



Discrete-time
Discrete-value
Conventional cryptosystems

Discrete-time Continuous-time
Continuous-value
Chaotic cryptosystems

Figure 3.2: Different classes of encryption systems

3.3 Chaotic Cryptosystems

In chaotic cryptography, chaotic systems are utilized in two major different ways for encrypting two different types of message data. The early attempts of using chaos in cryptography were in the conventional way, namely, in discrete-value and discrete-time implementation, and was for encrypting the digital message (Matthews 1989; Habutsu *et al.* 1991; Li *et al.* 2001). In these applications, chaotic systems, usually discrete-time chaotic systems, were used as a pseudo-random number generator for the encryption purpose. Since this kind of cryptosystem uses chaotic systems instead of the conventional way to generate pseudo-random numbers, it is also called the *chaos-based cipher.* The other approach of chaotic cryptosystems is based on the synchronization of continuous-time chaotic systems, and is generally designed for secure communications where, usually, the analog signals, for instance voice signals, are encrypted and transfered within a given network, thereby called *chaotic secure communications.*

3.3.1 Chaos-Based Cipher

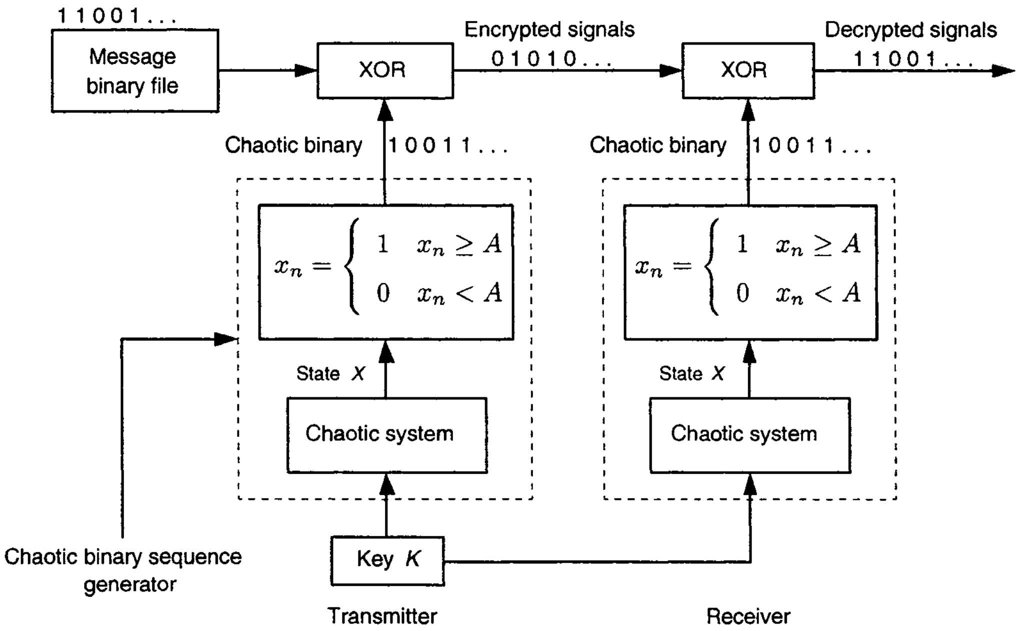


Figure 3.3: Schematic diagram of the chaos-based cipher

For the chaos-based cipher, Figure 3.3 shows its schematic diagram. Without loss of generality, we assume that the message transmitted from the transmitter is a binary file consisting of a chain of 0's and 1's. Before the transmission of the binary message takes place, the transmitter and the receiver have previously agreed to use the same n-dimensional discrete chaotic dynamical algorithm governed by equation (2.14) for the encryption and decryption purpose.

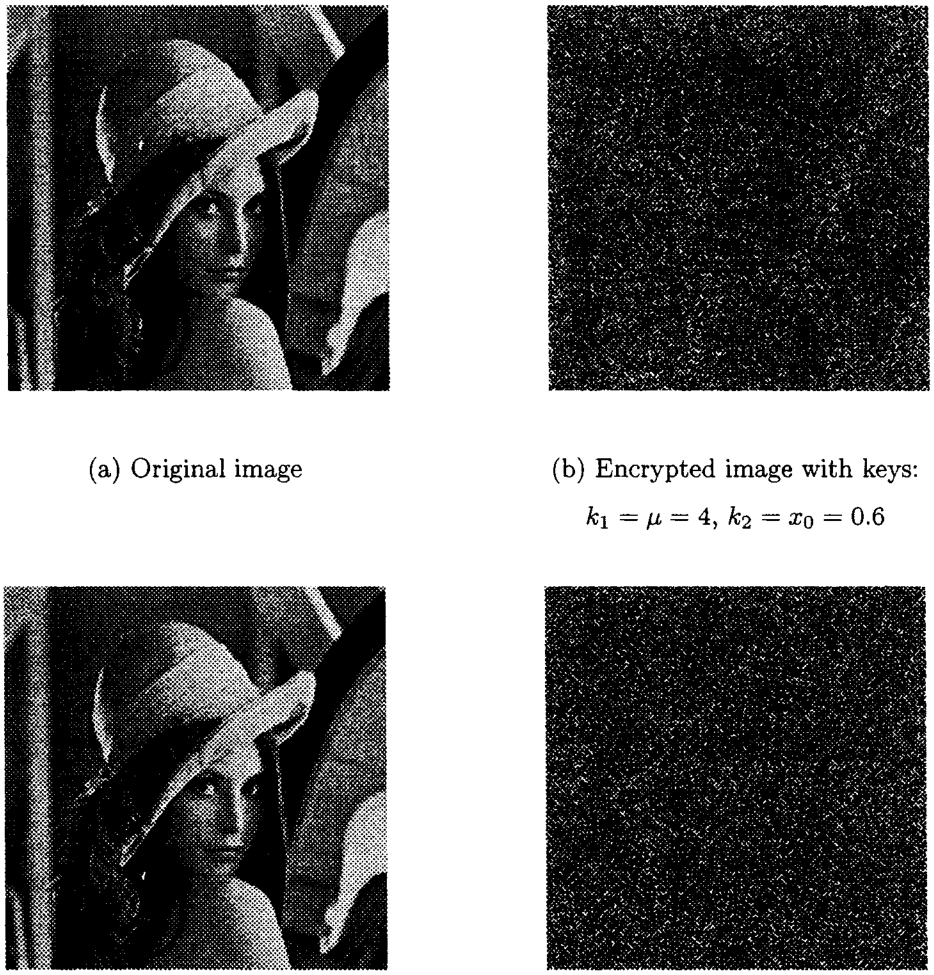
The encryption procedure can be expressed as this. As the first step, the transmitter searches for a sequence of the original message of a fixed size specified by a parameter. Then the chaotic dynamics is turned on with arbitrary initial conditions and/or parameters, set by the key K to generate the same size sequence of real numbers by iterating it. After that, a threshold A is chosen for the real number sequence to construct the chaotic binary sequence by this convention: if $x_n \geq A$ it is set as 1, and if $x < A$ it is set as 0. Once the chaotic binary sequence is generated, the XOR operation can be applied to the message binary file and the chaotic binary sequence, and then we get the encrypted binary sequence. The same process is carried on for remaining parts of the original message and, finally, the ciphertext would be obtained.

In order to decrypt the ciphertext and retrieve the original message data again, the procedure described above is simply repeated at the receiver side. Since we use the key K to set the initial conditions and parameters, upon which the chaotic dynamical system is extremely dependent in the sense that two arbitrarily close initial values will result in totally different systems states, this means that even the slightest difference of the key K will make the generated chaotic binary sequence completely unuseful. In other words, it can be said that only with the precise knowledge of the key K one can recover the ciphertext successfully.

Here, we give an example to demonstrate the implementation of the chaos-based cipher. In this example, we use the logistic equation (2.1) as the chaotic binary sequence generator to design a chaos-based cipher, and then use it to encrypt and decrypt an image file. Moreover, in this example, we use two sets of keys, k_1 is for the parameter $\mu = 4$ and k_2 is the initial value of $x_0 = 0.6$. Figure 3.4 illustrates the results of encrypting and decrypting an image file.

3.3.2 Chaotic Secure Communications

The approach of chaotic secure communications, referring to dealing with continuous value information by using continuous-time chaotic systems, for instance, the



(a) Original image

(b) Encrypted image with keys: $k_1 = \mu = 4$, $k_2 = x_0 = 0.6$

(c) Decrypted image with correct keys: $k_1 = \mu = 4$, $k_2 = x_0 = 0.6$

(d) Decrypted image with partial wrong keys: $k_1 = \mu = 4.001$, $k_2 = x_0 = 0.6$

Figure 3.4: Example of encrypting and decrypting an image file with a chaos-based cipher

Lorenz equation (2.2), was mainly promoted by the pioneering work of Pecora and Carroll. In (Pecora and Carroll 1990; Pecora and Carroll 1991), the authors proposed to use stable subsystems of given chaotic systems to construct unidirectionally coupled synchronization systems[1]. Moreover, Pecora and Carroll noticed that by adding a continuous message signal with a small amplitude to the chaotic signal, the synchronization of two chaotic systems can still be obtained, if they have the exact same parameters in the system equations, which can be considered as the private *key* for this secure communication system. Thereafter, the idea of using two synchronous chaotic systems, for secure communications, has received a great deal of interest, and several secure communication methods, such as: the chaotic masking, chaotic modulation and chaotic switching have been successfully developed based on the realization of synchronization of two chaotic systems.

In conventional communication systems, the signal carriers are usually the periodic sinusoidal signals because they can increase the bandwidth efficiency for communication systems. However, the transmitted power of the sinusoidal signals is concentrated within a narrow band, which leads to a high power spectral density. As a result, some unwanted problems may occur. For example, the synchronization between the transmitter and receiver may be destroyed due to high attenuation over a narrow frequency band; the interference among users on the system may be exacerbated; the possibilities of intercepting the message may increase. On the contrary, chaotic signals are usually broadband and noise-like, which are suitable to be used to design a secure communication system, for the secure transmission of analog and digital message signals (Chen and Dong 1998).

The common feature of most existing chaotic secure communication algorithms is that a scalar chaotic signal is used for transmitting message signals. Usually, the most general form of the communication system requires two components, each of which consists of a chaotic system, identical in most cases. One of these two components is called the transmitter and the other one is called the receiver, as Figure 3.5

[1] More detail will be discussed in Chapter 4.

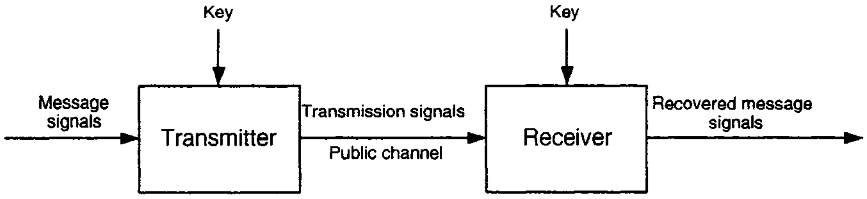


Figure 3.5: The chaotic secure communication system

shows. The basic idea of this kind of chaotic cryptosystems is to use, at the transmitter side, a chaotic system to generate the broadband noise-like chaotic carrier signal with the cryptographic key. By a proper modulation and encryption operation, the private message signal is hidden in the chaotic carrier signal and becomes an unintelligible signal, which is then transmitted over the public channel to the receiver. At the receiver, the chaotic carrier signal is regenerated by the synchronous chaotic system, so that by combining it with the received signal, through the inverse modulation and encryption operation, the original message signal can be extracted. The peculiarity of the chaotic secure communication lies in the message signal extraction process, which is based on synchronization phenomena between the transmitter and the receiver. This phenomena is required for successful message recovery, since only the completely synchronized receiver is capable of reconstructing the chaotic carrier signal. Due to the properties of great sensitivity to initial conditions and parameter settings of chaotic systems, it is believed that the chaotic receiver will only synchronize with the transmitter, if it has exactly the same parameter settings with the transmitter. Thus, these parameter settings can be considered as the secrete "Key" for a chaotic secure communication system (Dachselt and Schwarz 2001).

Since the synchronization of chaotic systems plays a central role in the recovering process of the private message signal for this kind of chaotic cryptosystems, here, we only introduce it briefly, and we shall describe it thoroughly in the next chapter, after introducing the concept of chaos synchronization.

Chapter 4

Chaos Synchronization

Synchronization, which usually refers to the coherence of different processes due to a coupling or to a forcing, is the basic phenomenon appearing in wide range of real systems, such as in biology, neural networks, physiological process, and so on. Although this phenomenon appears to be quite regular, when applied to periodic oscillations, the thought that two systems, each running chaotically, could synchronize with each other sounds quite inconceivable. Indeed, there is an essential difference between the synchronization of periodic oscillations and synchronization of chaotic systems. In the former case the oscillations do not have intrinsic instability and stochasticity which are common features of chaotic systems, whereas, in systems oscillating chaotically, it has been seen that infinitesimally nearby initial conditions trigger quite distinct evolutions. As a result, chaotic systems intrinsically defy synchronization, because even two identical systems, starting from slightly different initial conditions, would evolve in time in an unsynchronized manner. Considering this, it would seem rather pointless to attempt to synchronize chaotic systems in any sense (Chen and Dong 1998).

It was only until 1990, Pecora and Carroll discovered that a particular class of chaotic systems possesses a self-synchronization property, which means that by arranging these chaotic systems in a specific way, the identical chaotic behaviour could be achieved for these chaotic systems even if they were isolated, implying that it is possible to design a synchronizing system driven by chaotic signals (Pecora and Carroll 1990; Pecora and Carroll 1991). This striking discovery has attracted considerable interest among researchers from various disciplines. The motivation of the investigations has come from potential applications of this phenomenon to secure communications, model verification of nonlinear dynamics and many other areas.

Up to now, there are several different categories of chaos synchronization. Most frequently, chaos synchronization is studied where a complete system consists of unidirectionally coupled *identical* subsystems, as described by Pecora and Carroll. In this case, the synchronization appears as an actual equality of the corresponding state variables of the coupled systems as they evolve over time. In other words, it implies that all state trajectories of the synchronized chaotic systems asymptotically converge to each other in the course of the time. We refer to this type of synchronization as *identical synchronization* or *complete synchronization.* Another situation is when coupled chaotic systems are *not* identical. This kind of problems has been reported by Rulkov and his colleagues in (Rulkov *et al.* 1995) where two unidirectionally coupled chaotic systems are called synchronized if a static functional relation exists between the states of both systems. This kind of synchronization is usually termed as *generalized synchronization.*

In this chapter, we shall focus on the realization of the identical synchronization of chaotic systems and its application to secure communications.

4.1 Synchronization of Chaotic Systems

Considering the complex behaviour of chaotic dynamical systems, it is interesting to wonder whether we can find some mechanisms for externally influencing the functioning of chaotic systems and, on the other hand, how we can possibly utilize the amazing ability for performing other useful tasks such as signal processing. These questions and many more may be answered through investigating the concept of chaos synchronization. Therefore, we shall study the synchronization problem of two chaotic systems using different approaches that have been proposed so far in the literature. Each method will be investigated thoroughly and an example will be provided for each one of them.

The first thing to be highlighted is that the most common process, leading to synchronized states of chaotic systems, refers to the so-called drive-response coupling configuration, consisting of two chaotic dynamical systems, one of which generates driving signals, so it is called the *drive system* (or the *driving system*), and the other is driven by these signals and then it is called the *response system* (or the *driven system*). This implies that one chaotic system evolves freely and drives the evolution of the other. As a result, the response system is slaved to follow the dynamics of the drive system, which, instead, purely acts as an external but chaotic forcing for the response system. Based on this situation the definition of synchronization can be introduced in the general sense as follows:

Definition 4.1.1. *Given a drive system of variables $x(t)$, with dynamics governed by a continuous-time nonlinear dynamical system, given by equation (2.11), and an identical response system of variables $\hat{x}(t)$, it is said that there is synchronization if*

$$\lim_{t\to\infty} \| x(t) - \hat{x}(t) \| = 0. \tag{4.1}$$

Notice that it is clear from this definition that the synchronization of two dynamical systems means that trajectories of one of the two systems will converge to the same values of the other one and will remain in step for the future time. This makes the synchronization appear to be structurally stable.

4.1.1 Pecora-Carroll's Approach

Consider the n-dimensional autonomous dynamical system, whose temporal evolution is governed by equation (2.11). We suppose that the system can be arbitrarily divided into three components:

$$\dot{u} = f(u, v) \tag{4.2a}$$

$$\dot{v} = g(u, v) \tag{4.2b}$$

$$\dot{w} = h(u, w) \tag{4.2c}$$

where $u = (u_1, u_2, ..., u_m)^T$, $v = (v_1, v_2, ..., v_k)^T$, $w = (w_1, w_2, ..., w_l)^T$, and $n = m+k+l$. The first two components (4.2a) and (4.2b) represent the *drive subsystem*, whereas the last equation (4.2c) represents the response component which is then called the *response subsystem.* We now create a new subsystem with variables w' identical to the response subsystem of equation (4.2c), given by

$$\dot{w}' = h(u, w') \tag{4.3}$$

where $u(t)$ is the driving signal.

For the system described by equations (4.2), the chaos synchronization can be expressed as this: giving the same chaotic driving signal $u(t)$ for the response subsystem (4.2c) and its replica (4.3), at the moment $t = t_0$, generally $e(t_0)$ is not equal to zero, where $e(t)$ is the synchronization error defined by $e(t) = \| w(t) - w'(t) \|$. But as the time approaches to infinity, it yields that $\lim_{t\to\infty} \| e(t) \| = 0$. This means that the trajectories of two systems, starting from different initial conditions, will converge under the action of the chaotic driving signal.

The key problem is how to guarantee that, for a fixed set of drive initial conditions, wherever $w'(t)$ starts, it would always converge to the trajectory of the subsystem (4.2c), that is $w(t)$, and at each point of time always be at the same predictable place on that trajectory. This leads to the linear variational expansion for the response subsystem, given by

$$\dot{e} = h(u, w') - h(u, w) = J_w h(u, w)e + \mathcal{O}(w, u) \tag{4.4}$$

where $J_w h$ is the Jacobian matrix of the w subsystem vector field with respect to the variable w only, and $\mathcal{O}(w)$ represents the higher-order terms. In the limit of small e, the behaviour of equation (4.4) depends on the Lyapunov exponents of the response subsystem w for the particular driving signal $u(t)$, which are called *conditional Lyapunov exponents.* In (Pecora and Carroll 1990; Pecora and Carroll 1991), it has been shown that the necessary and sufficient condition for the trivial solution of equation (4.4) to be asymptotically stable is that all of conditional Lyapunov exponents[1] are negative. Such a condition can be met if $u(t)$ is a synchronizing signal. However, given a chaotic system , not all possible options of the driving signal lead to a synchronized state, as we shall show momentarily.

Let us describe this procedure using an example of the Lorenz system introduced in the former chapter. Its dimensionless equation is given by

$$\begin{aligned} \dot{x} &= -\sigma(x-y) \\ \dot{y} &= -xz+\rho x - y \\ \dot{z} &= xy - \beta z, \end{aligned} \tag{4.5}$$

and it can be decomposed into three different response subsystems considering the state x, y and z as the driving signal, respectively, described as follows:

(1) x-drive response subsystem

$$\begin{aligned} \dot{y}' &= -xz'+\rho x - y' \\ \dot{z}' &= xy' - \beta z' \end{aligned} \tag{4.6}$$

(2) y-drive response subsystem

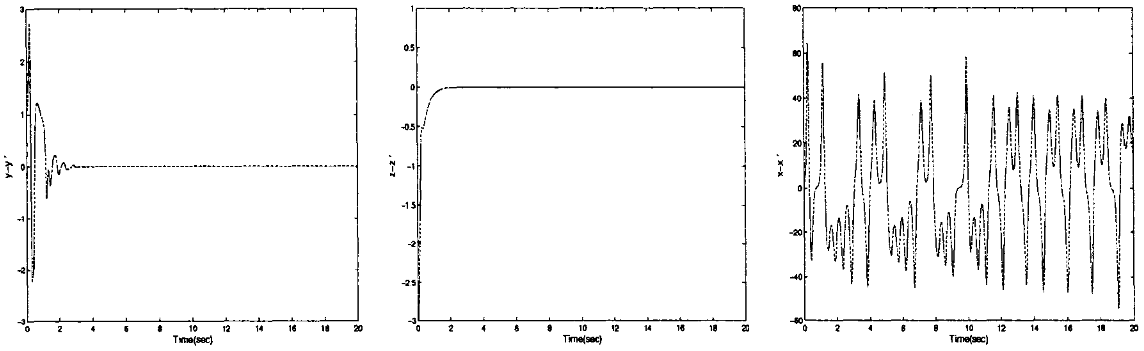
$$\begin{aligned} \dot{x}' &= -\sigma(x'-y) \\ \dot{z}' &= x'y - \beta z' \end{aligned} \tag{4.7}$$

(3) z-drive response subsystem

$$\begin{aligned} \dot{x}' &= -\sigma(x'-y') \\ \dot{y}' &= -x'z+\rho x' - y' \end{aligned} \tag{4.8}$$

[1] For the method to calculate Lyapunov exponents, refer to (Eckmann and Ruelle 1985).

Notice that the dynamics of all of the response subsystems given above is independent of the original Lorenz system; therefore, the original Lorenz system (4.5) is considered as the drive system and its decomposed subsystems (4.6), (4.7) and (4.8) are regarded as the response system. It can be shown that for $\sigma = 10$, $\beta = \frac{8}{3}$ and $\rho = 60$ giving rise to a chaotic dynamics drive and response systems can be synchronized only for the $x-$ and $y-$drive response systems, as shown in Figure 4.1(a,b), since conditional Lyapunov exponents are ($\lambda_1 = -1.81$, $\lambda_2 = -1.86$), ($\lambda_1 = -2.67$, $\lambda_2 = -10$) and ($\lambda_1 = 0.011$, $\lambda_2 = -11.01$) respectively for $x-$, $y-$ and $z-$drive response systems. This means that due to the slightly positive conditional Lyapunov exponent for the z-drive response system, its trajectory will not converge to that of the drive system even though there is a driving signal acting on it. Figure 4.1(c) demonstrates this result.



(a) x-drive

(b) y-drive

(c) z-drive

Figure 4.1: Results of chaos synchronization from P-C approach

Thus, these two $x-$ and $y-$drive response subsystems can converge to the corresponding components of the original Lorenz system respectively. Notice that, these two subsystems can be combined together to construct a full-dimensional response system, which is structurally similar to the drive system (4.5) (Cuomo and Oppenheim 1993). For example, if we consider the state x of the system (4.5) as the driving signal, the full-dimensional dynamics of the response system can be given by:

$$\begin{aligned} \dot{x}' &= -\sigma(x' - y') \\ \dot{y}' &= -xz' + \rho x - y' \\ \dot{z}' &= xy' - \beta z' \end{aligned} \tag{4.9}$$

In this case, it can be shown straightforwardly that the synchronization is a global property of the nonlinear error dynamics between the system (4.5) and (4.9) with the parameter $\sigma, \beta > 0$. First, let us define the synchronization error dynamics $e = (e_1, e_2, e_3)^T$ as

$$\begin{aligned} \dot{e}_1 &= \dot{x} - \dot{x}' &= -\sigma(e_1 - e_2) \\ \dot{e}_2 &= \dot{y} - \dot{y}' &= -e_2 - xe_3 \\ \dot{e}_3 &= \dot{z} - \dot{z}' &= xe_2 - \beta e_3. \end{aligned} \tag{4.10}$$

Then we consider the Lyapunov function as

$$V = \frac{1}{2}(\frac{1}{\sigma}e_1^2 + e_2^2 + e_3^2) \tag{4.11}$$

where σ is a positive constant. Taking the time derivative of V along trajectories of the resulting error dynamical system (4.10) leads to

$$\begin{aligned} \dot{V} &= \frac{1}{\sigma}e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 \\ &= -(e_1 - \frac{1}{2}e_2)^2 - \frac{3}{4}e_2^2 - \beta e_3^2. \end{aligned} \tag{4.12}$$

Therefore, it follows that $\dot{V} < 0$ for $\beta > 0$. According to the Lyapunov stability theory, it implies that the error dynamics converge to zero exponentially fast, that is

$$\lim_{t \to \infty} e(t) = 0. \tag{4.13}$$

Figure 4.2 shows the synchronization between the drive system (4.5) and the full-dimensional response system (4.9).

4.1.2 Observer-based Synchronization

Notice that once the chaotic drive system is given, the above drive-response method does not give a systematic procedure to determine the response system and

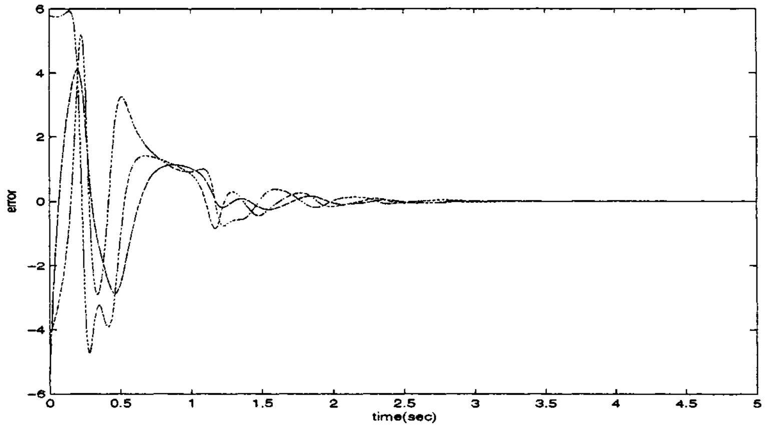


Figure 4.2: The components of the synchronization error for the drive system (4.5) and the full-dimensional response system (4.9)

the driving signal. Hence, it depends on the choice of the drive system and could not be easily generalized to an arbitrary chaotic drive system. This leaves some ambiguity as to what the actual response system should be, given a drive system. A natural attempt would be to consider the drive system as transmitting a driving signal to the response system and the response system is requested to recover the full state trajectory of the drive system. This problem is intimately related to the observer problem in control theory. Naturally, many efforts have been made to show that the synchronization problem of chaotic systems could be solved through the observer design approach, which has been then called *observer-based synchronization.* In this approach, for the given drive system, the response system could be chosen in the observer form, which is a copy of the drive system modified with a term depending on the difference between the received signal and its prediction. This additional term is used to attenuate the difference between the state of the designed drive system and the state of the observer system. Then under some relatively mild conditions, local or global synchronization of drive and observer systems can be guaranteed. Hence, this synchronization scheme offers a systematic procedure, independent of the choice of the drive system.

The observer-based synchronization method was proposed in (Grassi and Mascolo

1997; Liao and Huang 1999; Alvarez-Ramirez *et al.* 2002) and first motivated by the work in (Peng *et al.* 1996). Compared with Pecora-Carroll's method, this approach does not require the computation of the conditional Lyapunov exponents or the initial conditions belonging to the same basin of attraction. Moreover, it guarantees synchronization of a wide class of chaotic systems, via a scalar synchronizing signal only. In order to illustrate how this method works, we shall consider synchronizing two identical n-dimensional chaotic systems through the observer design technique.

Consider the general nonlinear chaotic system (2.11) having the form given by

$$\begin{aligned} \dot{x} &= Ax + f(x,y) \\ y &= C^T x \end{aligned} \tag{4.14}$$

where $x \in \mathbb{R}^n$ is the state, and $y \in \mathbb{R}$ is the output signal used as the synchronizing signal for the observer. The matrix $A \in \mathbb{R}^{n \times n}$ and $C \in \mathbb{R}^n$ are constants. Notice that in this case the noise description is not taken into account so this differential equation is deterministic. Moreover, $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is assumed to be a real analytic vector field and satisfy the global Lipschitz condition in x, *i.e.,* there exists a positive constant, called the Lipschitz constant, γ, such that

$$\| f(x,y) - f(\hat{x},y) \| \leq \gamma \| x - \hat{x} \| \tag{4.15}$$

for all x, $\hat{x} \in \mathbb{R}^n$ and for all $y \in \mathbb{R}$. By following the method proposed by Rachavan and Hedrick (Raghavan and Hedrick 1994), the observer design can be described as follows. We assume that the linear part of equation (4.14) is observable, *i.e.,* the pair $(A,\ C^T)$ is observable in the sense that the rank of the observability matrix

$$O = \begin{pmatrix} C^T \\ C^T A \\ \vdots \\ C^T A^{n-1} \end{pmatrix} \in \mathbb{R}^{n \times n} \tag{4.16}$$

is equal to n.

So now we can construct an observer for the system (4.14) in the following form:

$$\dot{\hat{x}} = A\hat{x} + f(\hat{x},y) + L(y - C^T\hat{x}) \tag{4.17}$$

where $\hat{x} \in \mathbb{R}^n$ represents the dynamic estimate of the state x and $f(\hat{x}, y)$ represents the estimated vector of $f(x, y)$ based on the estimated $\hat{x}$. $L \in \mathbb{R}^n$ is the observer gain vector chosen in such a way that $(A - LC^T)$ is an exponentially stable matrix which is always possible since the pair $(A,\ C^T)$ is observable (Ogata 2002). Then for any symmetric and positive definite matrix $Q \in \mathbb{R}^{n \times n}$ there exists a symmetric and positive definite matrix $P \in \mathbb{R}^{n \times n}$ such that the following well-known Lyapunov matrix equation is satisfied:

$$(A - LC^T)^T P + P(A - LC^T) = -Q \tag{4.18}$$

Let us now define the error for the state estimate as $e = x - \hat{x}$ and by using (4.14) and (4.17) we obtain the following error dynamics:

$$\dot{e} = (A - LC^T)e + f(x, y) - f(\hat{x}, y) \tag{4.19}$$

By considering the positive definite Lyapunov function $V(e) = e^T Pe$, it has been shown that if

$$\gamma < \frac{\lambda_{min}(Q)}{2\lambda_{max}(P)} \tag{4.20}$$

where the matrices P and Q are positive definite satisfying equation (4.18) and $\lambda_{min}(Q)$, $\lambda_{max}(P)$ denote the minimum and maximum eigenvalues of the matrices P and Q, respectively. Then

$$\lim_{t \longrightarrow \infty} e(t) = 0, \tag{4.21}$$

implying that the designed observer (4.17) yields asymptotically stable estimates for the system (4.14) (Thau 1973).

To demonstrate the above observer design method for synchronization, we shall take a numerical example employing the Rössler system given by equation (2.13), which can be written in the form of system (4.14), with $a = 0.2, b = 0.2$ and $c = 5$ exhibiting the chaotic behaviour, as follows:

$$
\begin{aligned}
\dot{x} &= Ax + f(x,y) \\
&= \begin{bmatrix} -0.2 & 0 & 0 \\ -1 & 0 & -1 \\ 0 & 0 & -5 \end{bmatrix} x + \begin{bmatrix} y \\ 0 \\ 0.2 + x_3 y \end{bmatrix} \\
y &= C^T x = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} x = x_2
\end{aligned}
\tag{4.22}
$$

where $x = \begin{bmatrix} x_1, x_2, x_3 \end{bmatrix}^T$ and y is the synchronizing signal. Notice that, since the pair $(A,\ C^T)$ for the system (4.22) is observable, it can be concluded, by applying the above discussion, that there exists a gain vector L, such that a response system designed through the observer design approach can synchronize with the drive system for any initial state. The observer-based response system designed in the form of system (4.17) is given as follows:

$$
\begin{aligned}
\dot{\hat{x}} &= A\hat{x} + f(\hat{x},y) + L(y - C^T\hat{x}) \\
&= \begin{bmatrix} -0.2 & 0 & 0 \\ -1 & 0 & -1 \\ 0 & 0 & -5 \end{bmatrix} \hat{x} + \begin{bmatrix} y \\ 0 \\ 0.2 + \hat{x}_3 y \end{bmatrix} + L(y - C^T\hat{x})
\end{aligned}
\tag{4.23}
$$

If the observer gain is chosen as $L = \begin{bmatrix} -2.1323 & 2.2 & -2.3077 \end{bmatrix}^T$, it makes the matrix $(A - LC^T)$ stable with the eigenvalues of -1, -2 and -4. Thus the error dynamics can be driven to zero as shown in Figure 4.3.

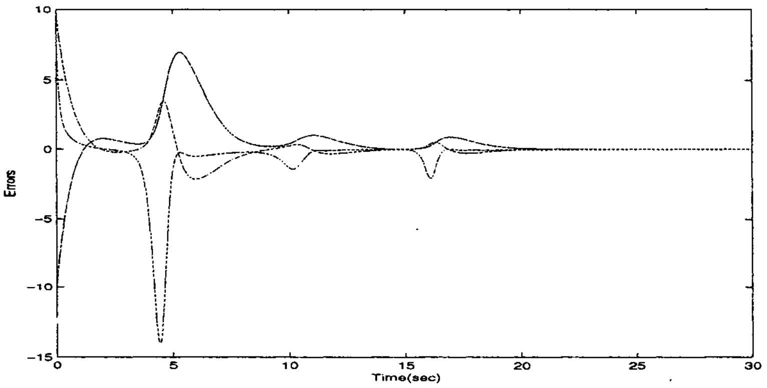


Figure 4.3: The components of the synchronization error for system (4.22) and (4.23)

Brunowsky Canonical Form

We now consider a special case of chaos synchronization on the basis of the observer design technique, where a particular way can be used to determine the observer gain vector L for the synchronization of two chaotic systems (4.14) and (4.17).

Suppose that there exists a linear change of coordinates $z = Ox$ by which the chaotic drive system (4.14) can be transformed into the following so-called *Brunowsky canonical form* (Ciccarella *et al.* 1993), given by

$$\begin{aligned} \dot{z} &= \bar{A}z + \bar{B}\phi(z,y) \\ y &= \bar{C}z \end{aligned} \tag{4.24}$$

with

$$\bar{A} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \bar{C} = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix}$$

It can be proven that, since the nonlinearity $f(x,y)$ in the systems (4.14) is globally Lipschitz in x, $\phi(z,y)$ in (4.24) is also globally Lipschitz in z (i.e. $\| \phi(z,y) - \phi(\hat{z},y) \| \leq \gamma_z \| z - \hat{z} \|$). Then, the corresponding observer system can be depicted as follows

$$\begin{aligned} \dot{\hat{z}} &= \bar{A}\hat{z} + \bar{B}\phi(\hat{z},y) + \bar{L}(y - \hat{y}) \\ \hat{y} &= \bar{C}\hat{z} \end{aligned} \tag{4.25}$$

where $\bar{L} = OL$ is the transformation of the observer gain vector L. We further consider that $\bar{L}$ depends on a positve parameter θ, and it is in the following form

$$\bar{L}(\theta) = \begin{bmatrix} \alpha_1\theta \\ \alpha_2\theta^2 \\ \vdots \\ \alpha_n\theta^n \end{bmatrix} \tag{4.26}$$

where $\alpha_{1,2,\ldots,n}$ are some constants appropriately chosen in such a way to make the polynomial $H(\lambda) = \lambda^n + \alpha_1 \lambda^{n-1} + \cdots + \alpha_n$ Hurwitz.

We now introduce the θ-scaled synchronization error:

$$e = \Lambda(z - \hat{z}) \tag{4.27}$$

where $\Lambda = diag(\theta^{n-1}, \theta^{n-2}, \ldots, 1)$.

Based on the equations of (4.24)–(4.27), we can obtain the following error dynamics:

$$\dot{e} = \theta(\bar{A} - \bar{L}(1)\bar{C})e + \Lambda \bar{B}(\phi(z, y) - \phi(\hat{z}, y)). \tag{4.28}$$

It can easily be shown that, with the appropriately chosen $\bar{L}(\theta)$ in the form (4.26), the matrix $(\bar{A} - \bar{L}(1)\bar{C})$ is stable so that there is a symmetric and positive definite matrix P satisfying equation (4.18) with $Q = I$.

Now, we choose the Lyapunov function as $V = e^T P e$, and then the time derivative of V along the trajectories of system (4.28) is

$$\begin{aligned} \dot{V} &= -\theta \parallel e \parallel^2 + 2e^T P(\Lambda \bar{B}(\phi(z, y) - \phi(\hat{z}, y)) \\ &\leq -\theta \parallel e \parallel^2 + 2 \parallel e^T P(\Lambda \bar{B}(\phi(z, y) - \phi(\hat{z}, y)) \parallel \\ &\leq -\theta \parallel e \parallel^2 + 2 \parallel e \parallel \parallel P \parallel \parallel \Lambda \bar{B} \parallel \parallel \phi(z, y) - \phi(\hat{z}, y) \parallel \\ &\leq -\theta \parallel e \parallel^2 + 2\gamma_z \lambda_{max}(P)|b_0| \parallel z - \hat{z} \parallel \parallel e \parallel \\ &\leq -\theta \parallel e \parallel^2 + 2\gamma_z \lambda_{max}(P)|b_0| \|\Lambda^{-1}\| \parallel e \parallel^2 \\ &\leq -(\theta - 2\gamma_z \lambda_{max}(P)|b_0| \|\Lambda^{-1}\|) \parallel e \parallel^2 . \end{aligned} \tag{4.29}$$

where $|b_0| = \|\Lambda B\|$ is a positive nonzero constant and the γ_z is the Lipschitz constant. Clearly, the following inequality holds for all of $\theta \geq 1$:

$$\dot{V} \leq -(\theta - 2\gamma_z \lambda_{max}(P)|b_0|) \parallel e \parallel^2 . \tag{4.30}$$

Once the parameter θ is chosen appropriately such that $\theta > max\,\{1,\ 2\gamma_z \lambda_{max}(P)|b_0|\}$, we can conclude that $\dot{V} < 0$, which implies that, from standard Lyapunov arguments, the given chaotic drive system (4.14) and the designed observer (4.17) can be synchronized, if the observer gain vector L is chosen as

$$L(\theta) = O^{-1}\bar{L}(\theta), \theta > max\,\{1,\ 2\gamma_z \lambda_{max}(P)|b_0|\} . \tag{4.31}$$

This method of designing the observer gain vector L provides a simple way to adjust the convergence rate of the synchronization errors by an appropriate choice of the parameter θ. In fact, since $V(t) \leq V(0)\text{exp}^{-(\theta - 2\gamma_z \lambda_{max}(P)|b_0|)}$, the larger the value of θ, the faster the convergence of the trajectories of the drive and the observer system.

In order to illustrate the method discussed above, we still take the Rössler system as an example to construct a synchronization system, so the linear change of coordinates can be chosen as:

$$z = Ox, \; O = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ a^2 - 1 & a & -1 \end{bmatrix}. \tag{4.32}$$

With the same parameters as used in the previous example, the Rössler system (4.22) can be transformed into the form of system (4.24), given by:

$$\begin{aligned} \dot{z} &= \bar{A}z + \bar{B}\phi(z) \\ &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} z + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \phi(z) \\ y &= \bar{C}z = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} z \end{aligned} \tag{4.33}$$

where $\phi(z) = -5z_1 - 4.8z_3 - 0.2z_1^2 - 0.2z_2^2 + 0.96z_1z_2 - 0.2z_1z_3 + z_2z_3 - 0.2$. If $\bar{L}$ is chosen as $\bar{L}(\theta) = \begin{bmatrix} 3\theta & 3\theta^2 & \theta^3 \end{bmatrix}^T$ such that the eigenvalues of the matrix $(\bar{A} - \bar{L}(1)\bar{C})$ are all located at -1, then, according to equation (4.31), the observer gain matrix $L(\theta)$ can be obtained by:

$$L(\theta) = O^{-1}\bar{L} = \begin{bmatrix} -2.8845\theta^2 - 0.1923\theta^3 \\ 3\theta \\ -0.1155\theta^2 + 0.1923\theta^3 \end{bmatrix}. \tag{4.34}$$

Figure 4.4 and 4.5 present the synchronization errors for $\theta = 3$ and $\theta = 10$, with the corresponding $L = \begin{bmatrix} -31.1526 & 9.0000 & 4.1526 \end{bmatrix}^T$ and $L = \begin{bmatrix} -480.75 & 30.00 & 180.75 \end{bmatrix}^T$

respectively. As the figures show, the trajectories of the systems (4.14) and (4.17) converges to zero exponentially, and the larger the value of θ, the faster the convergence rate.

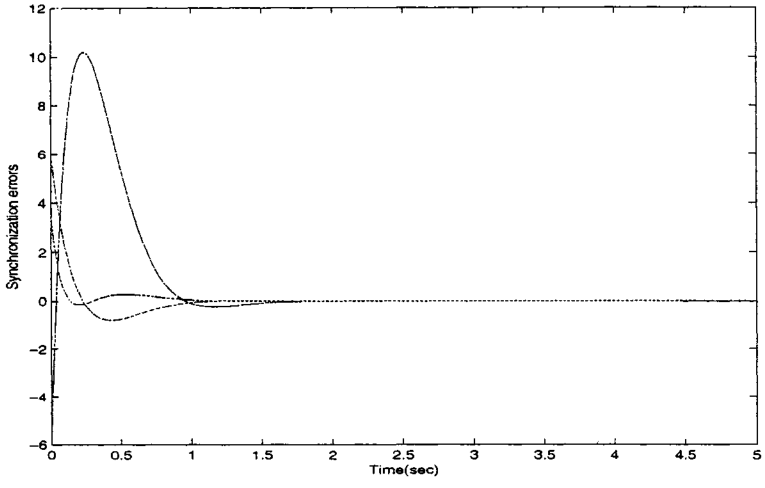


Figure 4.4: Synchronization errors of systems (4.14) and (4.17) for $\theta = 3$

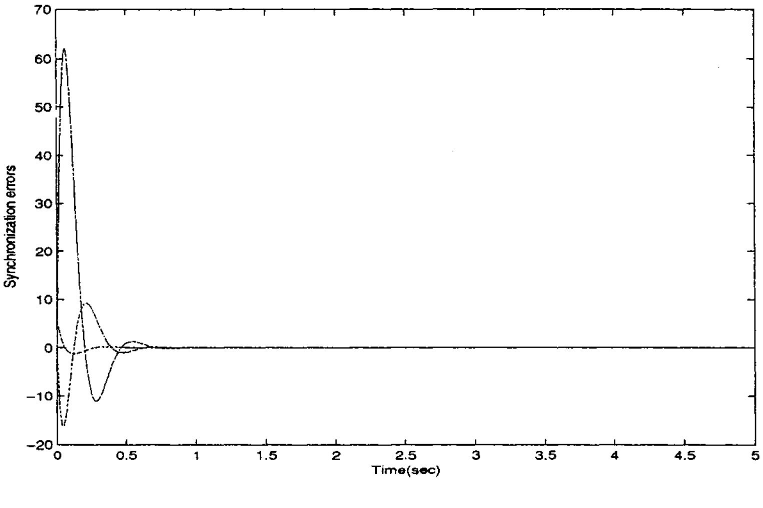


Figure 4.5: Synchronization errors of systems (4.14) and (4.17) for $\theta = 10$

4.2 Application in Secure Communications

As briefly introduced in the previous chapter, the problem of synchronizing two chaotic systems has been throughly studied recently, mainly because of its potential application to designing new chaotic cryptosystems for secure communications. For this application, on the transmitter side, the chaotic system with some preset parameters, as the *key*, is used to encrypt the private message signal, which is then transmitted through the public channel. The other chaotic system, on the receiver side, is used to retrieve the encrypted message signal via the synchronization of these two chaotic systems. Since chaotic systems are sensitively dependent on their initial conditions and parameters, it is believed that only the person, who knows exactly the key used in the transmitter, can design a synchronous receiver system to recover the message signal. Obviously, in the drive-response setup described above, the drive system can be considered as the transmitter and the response system can be regarded as the receiver, as illustrated in Figure 3.5.

Several methods concerning this matter have been proposed in the literature. We shall discuss three different approaches called chaotic masking, chaotic modulation and chaotic switching in the followings.

4.2.1 Chaotic Masking

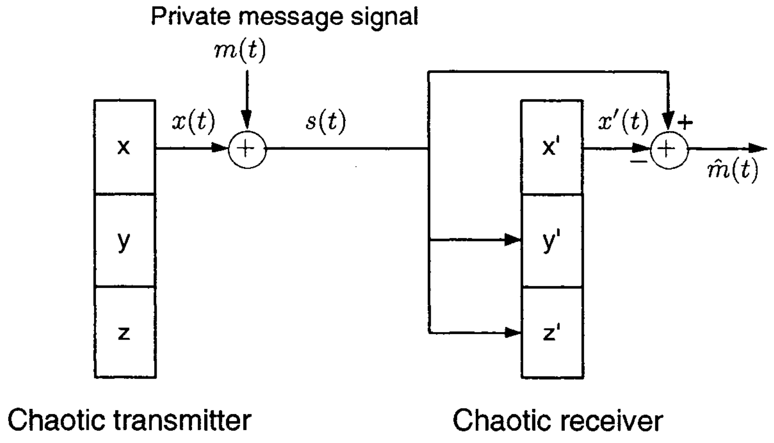


Figure 4.6: Chaotic signal masking cryptosystem

The most direct approach to communicating with a chaotic signal is called chaotic masking, which was proposed in (Pecora and Carroll 1990; Cuomo and Oppenheim 1993). The basic idea that underlines this method is that the private message signal $m(t)$ to be transmitted is added directly to the noise-like masking signal at the transmitter-end for the encryption purpose, then the overall signal is transmitted to the receiver over the public channel. At the receiver-end, the masking is removed via the synchronization of transmitter and receiver systems. This process is done by using the transmission signal as the driving signal to reconstruct the noise-like masking signal at the receiver system, and subtracting it from the received signal which finally recovers the message signal $m(t)$ (refer to Figure 4.6). In order for this scheme to work properly, the original message signal has to be sufficiently small with respect to the chaotic masking signal, so that it can be considered as a small perturbation in the transmission signal. Since it is found experimentally that the ability to synchronize is robust, *i.e.,* is not highly sensitive to perturbations in the transmission signal, implying that the synchronization can be done with the masked signal (Pecora and Carroll 1991).

By following the example of synchronization of Lorenz system in Section 4.1.1, we design a chaos masking secure communication system consisting of the transmitter the same as system (4.5) and the receiver similar to the system (4.9), with $x(t)$ replaced by $s(t)$ as a driving signal. Although there are many possible variations, we consider a transmission signal of the form $s(t) = x(t) + m(t)$ where we assume that the power level of the message signal $m(t)$ is significantly lower than that of the chaotic masking signal $x(t)$, so that the synchronization between the transmitter and receiver can be guaranteed. As Figure 4.6 illustrates, once the receiver is synchronized with the transmitter by the driving signal $s(t)$, then the masking signal $x(t)$ can be reconstructed, that is, $x(t) = x'(t)$. Consequently, the original information signal $m(t)$ can be finally recovered as $\hat{m}(t) = s(t) - x'(t) \rightarrow m(t)$, with $x(t) \rightarrow x'(t)$ as $t \rightarrow \infty$.

The performance of this secure communication system is demonstrated in Figure 4.7 with a segment of a sound signal: "The good boy." being transmitted through it.

The figure shows the original sound signal $m(t)$ and the recovered sound signal $\hat{m}(t)$. Clearly, the sound signal was recovered and was of reasonable quality in informal listening tests.

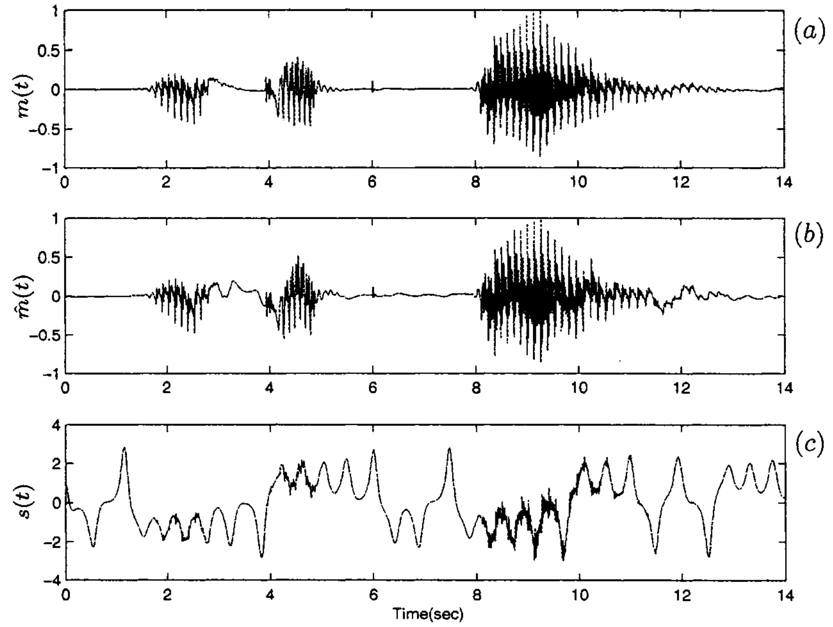


Figure 4.7: Sound signal encryption and recovery with chaotic masking method: (a) original sound signal; (b) recovered sound signal; (c) transmission signal

4.2.2 Chaotic Modulation

The method of chaotic modulation proposed in (Wu and Chua 1993) and (Liao and Huang 1999) resembles the above approach, but adds more complexity and security to the transmission of the message signal. The suggested idea is that, at the transmitter, the original message signal is not only modulated with the chaotic signal by some specified operation, but also injected into the chaotic system. This means that the message signal can modify states of the transmitter system through an invertible procedure; thus, the generated chaotic signal inherently contains the information of the message signal. The receiver synchronizes with the transmitter via reconstruction of its state using the transmission signal. The message signal is recovered by applying the inverse modulation operation to the reconstructed state and the received signal. The main idea of this method is sketched in Figure 4.8.

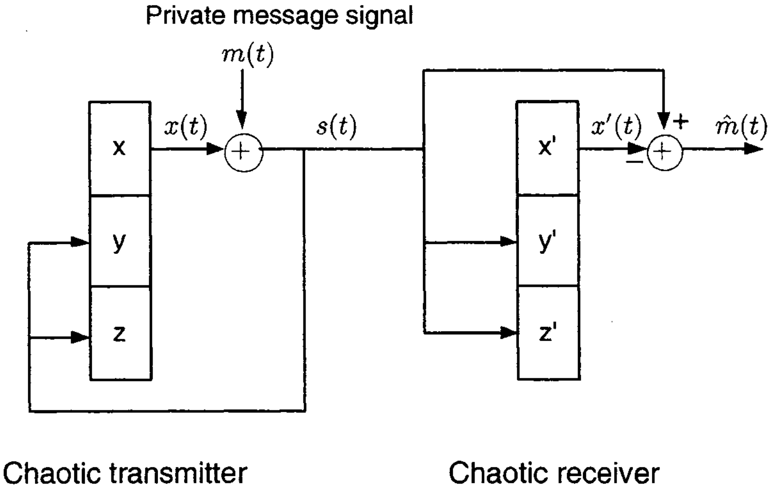


Figure 4.8: Chaotic signal modulation cryptosystem

We shall describe this method using the Lorenz system again, and consider a simple way to modulate the message signal $m(t)$ with the chaotic signal $x(t)$, that is, $s(t) = m(t) + x(t)$. This addition is then transmitted to the receiver; meanwhile it is also fed back into the transmitter system. Then, the transmitter for this scheme is given as follows:

$$\begin{aligned} \dot{x} &= -\sigma(x-y) \\ \dot{y} &= -(x+m(t))z + \rho(x+m(t)) - y \\ \dot{z} &= (x+m(t))y - \beta z. \end{aligned} \tag{4.35}$$

Now consider the transmission signal as $s(t) = x(t) + m(t)$, the receiver can be designed as:

$$\begin{aligned} \dot{\hat{x}} &= -\sigma(\hat{x}-\hat{y}) \\ \dot{\hat{y}} &= -(x+m(t))\hat{z} + \rho(x+m(t)) - \hat{y} \\ \dot{\hat{z}} &= (x+m(t))\hat{y} - \beta\hat{z}. \end{aligned} \tag{4.36}$$

For this chaotic modulation cryptosystem, it can be proven that the transmitter (4.35) can synchronize with the receiver (4.36), with the parameters $\sigma = 16$, $\beta = 4$ and

$\rho = 44.8$ (Wu and Chua 1993). Hence the original message signal can be retrieved by an inverse modulation operation, that is, $\hat{m}(t) = s(t) - \hat{x}(t) \to m(t)$, with $x(t) \to \hat{x}(t)$ as $t \to \infty$. Figure 4.9 shows the results of transmitting a continuous-time message signal by using the chaotic modulation method.

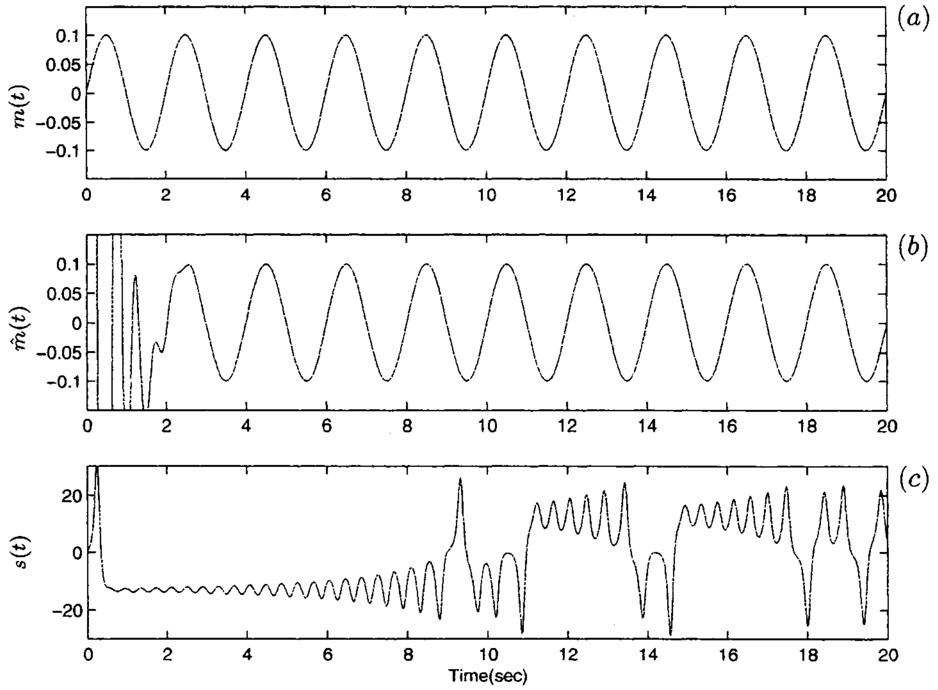


Figure 4.9: Transmission of message signals with the chaotic modulation method: (a) original message signal; (b) recovered message signal; (c) transmission signal

4.2.3 Chaotic Switching

In the method of chaotic masking and chaotic modulation, a continuous-time message signal was encrypted by a noise-like chaotic signal. Now, we present a quite similar cryptosystem, introduced in (Parlitz *et al.* 1992), to safely transmit and receive a discrete-valued message signal, which is usually binary. The essence of this method is that two sets of parameter values are predefined at the transmitter system, while only one set of parameter values, which is the same as one of those two sets used in the transmitter, is preset at the receiver system. Then the transmitter switches parameters, so that they change to one of two predefined sets of values depending on whether a "1" or a "0" is being transmitted. At the receiver, one set of values will lead to a perfect synchronization, while another one will produce a synchronization error between the received driving signal and the receiver's generated chaotic signal. By low pass filtering the synchronization error signal and applying a threshold test to the low pass filtered signal, the binary message signal can be retrieved successfully (Cuomo and Oppenheim 1993). This process is shown in Figure 4.10.

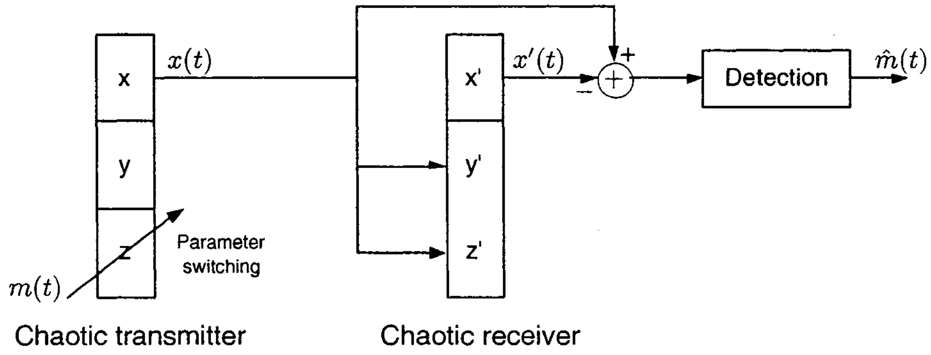


Figure 4.10: Chaotic signal switching system

To illustrate the performance of this scheme, we take a square wave as the binary message signal shown in Figure 4.11(a), which produces a variation in the parameter β of the transmitter, given by system (4.5), with zero-bit and one-bit parameters corresponding to $\beta(0) = 4$ and $\beta(1) = 4.4$, respectively, while, at the receiver system which is also given by system (4.5), the value of the parameter β is kept as $\beta = 4$ for all the time. Figure 4.11(b) shows the synchronization error signal. It is obvious that the parameter switching produces significant synchronization error during a "1" transmission and a very small error during a "0" transmission. Figure 4.11(c) shows the synchronization error signal filtered by a low-pass filter, designed as:

$$H(z) = \frac{10^{-8}(0.1216 + 0.3648z_1 + 0.3648z_2 + 0.1216z_3)}{1 - 2.9957z_1 + 2.9915z_2 - 0.9957z_3}. \tag{4.37}$$

Figure 4.11(d) shows that the square-wave can be finally recovered by applying a threshold test[2] to the filtered synchronization error signal.

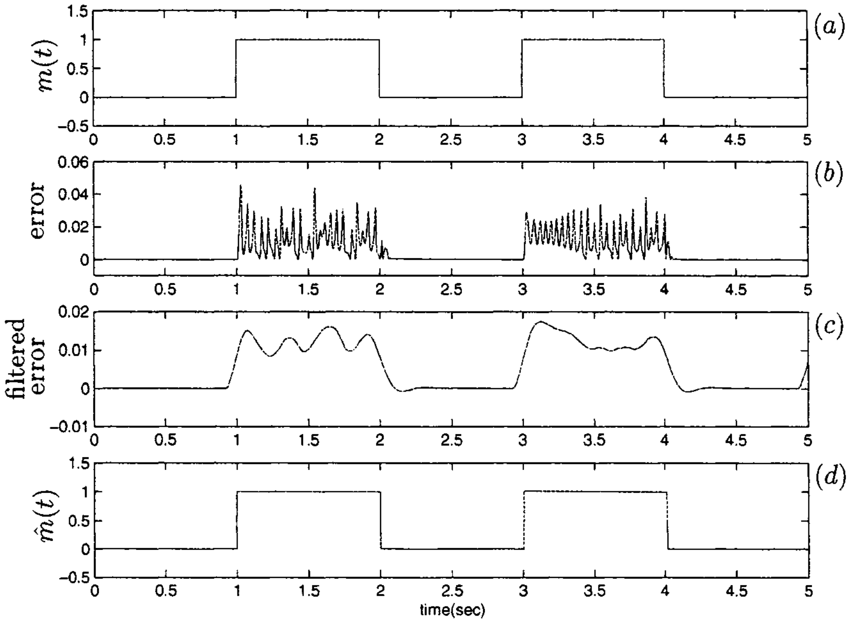


Figure 4.11: Discrete signal encryption and recovery with chaotic switching method: (a) digital information signal; (b)synchronization error power; (c) low pass filtered signal; (d) recovered digital signal.

[2] In this case, we set the threshold value as 0.008. For all the value of filtered synchronization error signal lesser than the threshold value, it is set as 0, otherwise it is set as 1.

Chapter 5

New Secure Communication System

Achieving easy recovery by the receiver but difficult detection by any third party of a message signal is always the most important issue in secure communications. As seen from the applications of chaos synchronization to secure communications discussed in the former chapter, the message signal is first modulated by a chaotic carrier signal for the encryption purpose and then transmitted to the receiver, while the receiver has to recover the message signal from the incoming transmission signal, via the synchronization of the transmitter and the receiver system. Since haotic systems are extremely dependent on their initial conditions and parameter settings, the asymptotic synchronization of the transmitter and the receiver is inevitable for the scheme, which not only guarantees a message signal being successfully recovered by the receiver, but also prevents it from being read during the transmission process by any unauthorized party. This means that the most important aspect of chaos synchronization is its security.

Commonly, in order to achieve the synchronization, some typical ways such as the drive-response mechanism, observer-based approach, etc., which have been discussed in detail in the former chapter are usually utilized. However, for several of these methods, the security of the synchronization is quite questionable as discussed in the following section. This chapter formalizes the concept of secure synchronization of chaotic systems and discusses an approach to achieve the secure synchronization of chaotic systems. A new secure communication system, based on the secure synchronization, is also developed and investigated.

5.1 Secure Synchronization

Generally, in applications of chaos synchronization to secure communications, the parameter settings of the drive system are considered as the secret "key" for the encryption of message signals, and it is believed that without precise knowledge of this secret "key", used in the drive system, it is very difficult to design a corresponding response system synchronized with the drive system to decrypt the encrypted message signals. However, from a control theory viewpoint, the problem of having unknown parameters in the system model can be solved by using certain techniques such as the adaptive control or robust control. For example, an adaptive observer usually includes an estimation subsystem for the unknown parameters, and, by using some adaptation algorithms, the unknown parameters can be estimated accurately. This means that the adaptive or robust control method may be considered for possible attacks against secure communication and encryption schemes. By using these techniques, an intruder might design a false receiver synchronized with the transmitter to recover the message signals without knowing the secrete "key". This problem, however, was mostly neglected when chaotic secure communication schemes were developed in the past. To demonstrate this problem, we shall introduce an adaptive synchronization scheme originally studied in (Fradkov *et al.* 1999) and (Liao and Tsai 2000), which employs the adaptive control technique for the synchronization of chaotic systems with unknown parameters, so that it is not suitable for the application to secure communications.

5.1.1 Example of Insecure Synchronization

Consider the following nonlinear chaotic system with the unknown constant parameters μ

$$\begin{aligned} \dot{x} &= Ax + B\mu^T\phi(y) \\ y &= C^Tx \end{aligned} \tag{5.1}$$

where $x \in \mathbb{R}^n$ is the state, and $y \in \mathbb{R}$ is the scalar output signal used as the synchronizing signal for the observer. The matrix $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times l}$and $C \in \mathbb{R}^n$ are constants. Moreover, $\phi(x)$ is $(l \times k)$ matrix with uniformly Lipschitz entries, $\mu \in \mathbb{R}^k$ is the constant parameter vector which may be unknown as the secret key.

Assume that the pair $(C^T,\ A)$ is observable. Then, on the basis of state observer design approach discussed before, an adaptive-observer-based synchronization system corresponding to the drive system (5.1) can be designed as follows:

$$\dot{\hat{x}} = A\hat{x} + B\hat{\mu}^T\phi(y) + L(y - C^T\hat{x}) \tag{5.2}$$

where y is the received transmission signal and $L \in \mathbb{R}^n$ is the observer gain vector which is chosen fittingly such that $(A - LC^T)$ is an exponentially stable matrix, which is possible since the pair $(C^T,\ A)$ is assumed to be observable. Moreover, $\hat{\mu} \in \mathbb{R}^k$ represents the adjustable parameters used to estimate the unknown parameters in the drive system, which are updated according to the following adaptation algorithm:

$$\dot{\hat{\mu}} = \phi(y)(y - \hat{y}). \tag{5.3}$$

Furthermore, we assume that there exists a strictly positive real (SPR) transfer function, $W(s) = C^T(sI - (A - LC^T))^{-1}B$, with an appropriately chosen L. In light of the well-known Kalman-Yakubovich Lemma (Ioannou and Sun 1996), this strict positive realness of $W(s)$ guarantees that there exist symmetric and positive matrices P and Q satisfying the following equations

$$\begin{aligned} &(A - LC^T)^TP + P(A - LC^T) = -Q \\ &PB = C. \end{aligned} \tag{5.4}$$

Then, we have the following proposition:

Proposition 5.1.1 (Liao and Tsai 2000). . *For the given drive system (5.1), the designed adaptive-observer-based response system (5.2) associated with the adaptation algorithm (5.3) can globally asymptotically synchronize with the drive system, i.e.,* $\|x(t) - \hat{x}(t)\| \to 0$ *as* $t \to 0$ *for all initial conditions.*

Proof. First of all, we define the state error for the system (5.1) and (5.2) as $e = x - \hat{x}$, and then, under the adaptation algorithm (5.3), the resulting error dynamics can be characterized as follows:

$$\dot{e} = (A - LC^T)e + B(\mu - \hat{\mu})^T \phi(y). \tag{5.5}$$

We now choose the Lyapunov function as

$$V = e^T P e + (\mu - \hat{\mu})^T (\mu - \hat{\mu}). \tag{5.6}$$

Taking the time derivative of V along the trajectories of the resulting error dynamical system (5.5) leads to

$$\begin{aligned}
\dot{V} &= \dot{e}^T P e + e^T P \dot{e} + 2(\mu - \hat{\mu})^T(-\dot{\hat{\mu}}) \\
&= ((A - LC^T)e + B(\mu - \hat{\mu})^T \phi(y))^T P e \\
&\quad + e^T P((A - LC^T)e + B(\mu - \hat{\mu})^T \phi(y)) + 2(\mu - \hat{\mu})^T(-\phi(y)C^T e) \\
&= e^T (A - LC^T)^T P e + \phi(y)^T (\mu - \hat{\mu}) B^T P e \\
&\quad + e^T P((A - LC^T)e + e^T P B(\mu - \hat{\mu})\phi(y)) - 2(\mu - \hat{\mu})^T \phi(y) C^T e \\
&= e^T((A - LC^T)^T P + P(A - LC^T))e + \phi(y)^T(\mu - \hat{\mu}) B^T P e \\
&\quad + e^T P B(\mu - \hat{\mu})\phi(y) - 2(\mu - \hat{\mu})^T \phi(y) T C^T e.
\end{aligned} \tag{5.7}$$

By using equation (5.4), it yields

$$\dot{V} = -e^T Q e. \tag{5.8}$$

Since V is a positive and decrescent function and $\dot{V}$ is negative semidefinite, by following the LaSalle Principle (Khalil 2002), we can conclude that $e(t) \to 0$ as

$t \to \infty$, which means that the designed adaptive-observer-based receiver (5.2) can synchronize with the given drive system (5.1).

■

Consider as an example of chaotic synchronization system where both drive and response systems are the well-known Chua's chaotic system. The drive system in dimensionless form is given by (2.12) and it can be written in the form (5.1) as follows:

$$\begin{aligned} \dot{x} &= Ax + B\mu^T\phi(y) \\ &= \begin{bmatrix} -10 & 10 & 0 \\ 1 & -1 & 1 \\ 0 & -15 & 0 \end{bmatrix} x + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} (-10by - 5(a-b)(\mid y+1 \mid - \mid y-1 \mid)) \\ y &= C^T x = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x = x_1 \end{aligned} \tag{5.9}$$

where $\phi(y) = \begin{bmatrix} y & \mid y+1 \mid - \mid y-1 \mid \end{bmatrix}$, and $\mu^T = \begin{bmatrix} \mu_1 & \mu_2 \end{bmatrix} = \begin{bmatrix} -10b & -5(a-b) \end{bmatrix}$ which is assumed to be *a priori* unknown motivating the use of an adaptation for the response system design. It can be easily verified that the pair $(C^T\ A)$ is observable, which means that the response system can be designed according to the above results, modeled as

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + B\hat{\mu}^T\phi(y) + L(y-\hat{y}) \\ &= \begin{bmatrix} -10 & 10 & 0 \\ 1 & -1 & 1 \\ 0 & -15 & 0 \end{bmatrix} x + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} (\hat{\mu}_1 y + \hat{\mu}_2(\mid y+1 \mid - \mid y-1 \mid)) + L(y-\hat{y}) \\ \hat{y} &= C^T\hat{x} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \hat{x} = \hat{x}_1 \end{aligned} \tag{5.10}$$

where $\hat{\mu}^T = \begin{bmatrix} \hat{\mu}_1 & \hat{\mu}_2 \end{bmatrix}$ represent the adjustable parameters used to estimate unknown parameters μ_1 and μ_2, which are updated according to the adaptation algorithm (5.3), that is,

$$\begin{aligned} \dot{\hat{\mu}}_1 &= (y-\hat{y})y \\ \dot{\hat{\mu}}_2 &= (y-\hat{y})(\mid y+1 \mid - \mid y-1 \mid). \end{aligned} \tag{5.11}$$

It can be found that, if L is chosen as $L = \begin{bmatrix}-8.9615 & 1.6921 & 0.5769\end{bmatrix}^T$ so that the matrix $(A - LC^T)$ is stable with the eigenvalues -0.9737 and $-0.5324 \pm j4.6518$, then we can get the strict positive real transfer function

$$W(s) = C^T(sI - (A - LC^T))^{-1}B = \frac{s^2 + s + 15}{s^3 + 2.0385s^2 + 22.9595s + 21.3461}. \tag{5.12}$$

This means that the following symmetric and positive-definite matrices

$$P = \begin{bmatrix} 0.5107 & 0.2553 & 0.0046 \\ 0.2553 & 7.5173 & -0.2977 \\ -0.0046 & -0.2977 & 0.5256 \end{bmatrix}, Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{5.13}$$

can be obtained according to equation (5.4).

Moreover, in the numerical simulation, the values of system's parameter, the secret "Key", are chosen as $a = -1.28$ and $b = -0.69$, implying that $\mu_1 = 6.9$ and $\mu_2 = 2.95$. Figure 5.1 demonstrates that the state of the designed adaptive observer (5.10) can converge to that of the given drive system (5.9), although some of system's parameters are unknown for the observer system. Figure 5.2 shows the unknown parameters μ_1 and μ_2, and the estimated parameters $\hat{\mu}_1$ and $\hat{\mu}_2$, respectively. Clearly, in this approach, although some parameters of the drive system are unknown, they can still be estimated by this adaptive-observer-based approach. Consequently, it is not secure to be used in secure communications applications.

5.1.2 Concept of Secure Synchronization

Certainly it is undesirable if a synchronization scheme, which might be used for secure communications, is known to be vulnerable to simple attacks. In view of this, here we present the concept of secure synchronization, with respect to adaptive and robust control schemes (Čelikovský and Chen 2005). We begin with re-defining the definition of the synchronization of chaotic systems, formulated in control theoretic terms.

Consider the nonlinear chaotic system (2.11) with a parameter vector μ, which

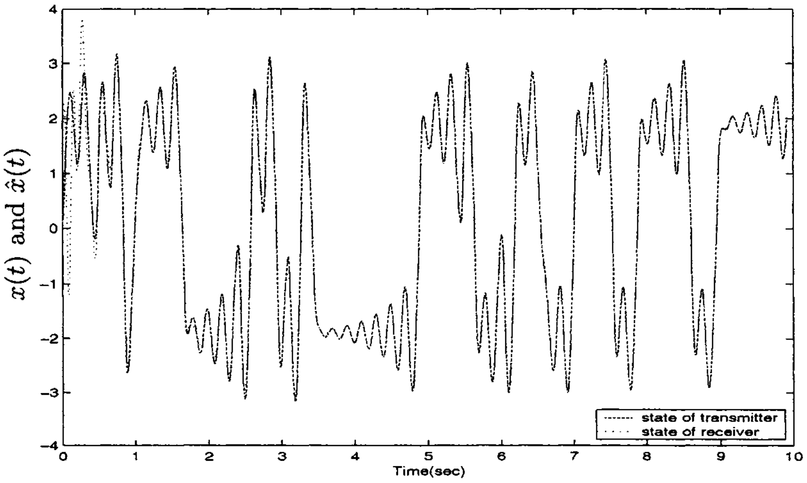


Figure 5.1: Adaptive-observer-based synchronization

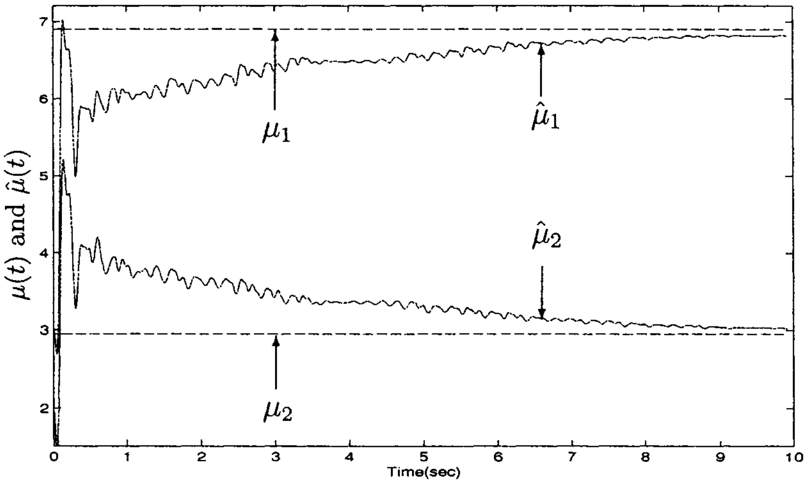


Figure 5.2: The unknown parameters and the estimated parameters

is re-written as follows:

$$\dot{x} = f(x, t, \mu), \tag{5.14}$$

where $x \in \mathbb{R}^n$ and $\mu \in \mathbb{R}^m$.

Definition 5.1.1. *System (5.14) is said to achieve a synchronization of a solution $x(t), t \geq t_0$, if there exists an auxiliary output, $y = y(x) \in \mathbb{R}^p, p < n$, such that with this output the system (5.14) has the following smooth asymptotic observer for the solution $x(t), t \geq t_0$:*

$$\dot{\hat{x}} = f(\hat{x}, t, \mu) + \varphi(y(x), y(\hat{x}), \hat{x}, \mu), \tag{5.15}$$

where $x, \hat{x} \in \mathbb{R}^n$ and $\mu \in \mathbb{R}^m$.

Definition 5.1.2. *The synchronization is said to be* ***antiadaptive secure*** *with respect to the parameter μ, if there does not exist any adaptive observer of the form (5.15) with $\mu = \hat{\mu}$, $\hat{\mu} \in \mathbb{R}^m$, which can be obtained from the following adaptation algorithm:*

$$\dot{\hat{\mu}} = \psi(\hat{\mu}, y(x), y(\hat{x}), \hat{x}, t). \tag{5.16}$$

Definition 5.1.3. *The synchronization is said to be* ***antirobust secure*** *with respect to the parameter μ, if there exists a positive constant K such that for any $\bar{\mu}$, $\tilde{\mu}$ from a given compact set and for any solution of the system (5.14) with $\mu = \bar{\mu}$ and the observer (5.15) with $\mu = \tilde{\mu}$, it holds that*

$$\lim_{t \to \infty} \|x(t) - \hat{x}(t)\| \geq K(\bar{\mu} - \tilde{\mu}). \tag{5.17}$$

Then the **secure synchronization** is defined as the one that is both antiadaptive secure and antirobust secure.

Obviously, for any synchronization scheme, the antiadaptive secure implies that, if the parameter μ is considered as the secret key, there should be no way that an intruder could obtain it by using the adaptive-observer design technique. Moreover, the antirobust secure means that, for any synchronization method employing an estimated key parameter, a big enough inaccuracy of the parameters estimation should cause big enough synchronization error. Therefore, both antiadaptive and antirobust security properties of the synchronization scheme are crucial for resisting potential attacks, since they guarantee that only the person who knows exactly the secret key can design an observer to construct the synchronization system.

Notice that although the secure synchronization is defined very broadly and therefore it seems difficult to verify, the intention here is to underline the fact that, the synchronization of chaotic systems for secure communications should offer a higher level of security to prevent the secure communication system from being vulnerable to simple attacks. Based on this consideration, the adaptive-observer-based approach to synchronize the well-known Chua's system with some unknown parameters presented by Proposition 5.1.1 is not antiadaptive secure. In fact, it has been shown that the unknown key parameters used in the drive system were estimated successfully by this adaptive-observer approach (see Figure 5.2). Moreover, the case of synchronization problem of a typical class of chaotic systems having the so-called Brunowsky canonical form, which is discussed in Section 4.1.2, can be considered as the one which is *not* antirobust secure. The reason is given by the following Proposition.

Proposition 5.1.2 (Alvarez-Ramirez *et al.* 2002). *Suppose that system (5.14) and its synchronizing output $y(x)$ have the form*

$$\begin{aligned} \dot{x} &= Ax + Bf(x,\mu) \\ y &= Cx \end{aligned} \tag{5.18}$$

with

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix}$$

where $f(x,\mu)$ is Lipschitz in x, x is bounded, and μ stays within a compact set. Then the system (5.18) allows synchronization that is not antirobust secure. Namely, the *system*

$$\dot{\hat{x}} = A\hat{x} + Bf(\hat{x}, \hat{\mu}) + \hat{L}(y - C\hat{x}) \tag{5.19}$$

where $\hat{\mu}$ is some nominal value of the unknown parameter μ and $\hat{L} = \begin{bmatrix} \theta & \theta^2 & \dots & \theta^n \end{bmatrix}^T$, has the property that for any positive constant ε, there exists a $\theta(\varepsilon) > 0$, such that $\lim_{t\to\infty} ||x(t) - \hat{x}(t)|| \to 0$.

Proof. Consider the θ-scaled synchronization error for the systems (5.18) and (5.19) as $e = \Lambda(x - \hat{x})$, where $\Lambda = diag(\theta^{n-1}, \theta^{n-2}, ..., 1)$, and then the resulting synchronization error dynamics can be characterized as follows:

$$\begin{aligned} \dot{e} &= \theta F(1)e + \begin{bmatrix} 0 & \dots & \rho(t) \end{bmatrix}^T \\ F(\theta) &= \begin{bmatrix} -\theta & 1 & 0 & \dots & 0 & 0 \\ -\theta^2 & 0 & 1 & 0 & \dots & 0 \\ -\theta^3 & 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & 0 \\ -\theta^{n-1} & 0 & 0 & \dots & 0 & 1 \\ -\theta^n & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \end{aligned} \tag{5.20}$$

where $\rho(t) = f(\hat{x}, \hat{\mu}) - f(x, \mu)$ is a certain bounded function, since $f(x, \mu)$ is Lipschitz, implying that $||\rho(t)|| \leq \alpha||x - \hat{x}||$, $\alpha > 0$ for all $t \geq 0$. It is easy to verify that the matrix $F(1)$ is Hurwitz. This means that there exists a symmetric positive definite matrix P such that the equation

$$F(1)^T P + P^T F(1) = -I \tag{5.21}$$

is satisfied.

We now choose the Lyapunov function as $V = e^T P e$, and then the time derivative of V along the solution of (5.20) is given by

$$\begin{aligned} \dot{V} &= -\theta||e||^2 + 2\begin{bmatrix} 0 & \dots & \rho(t) \end{bmatrix} Pe \\ &\leq -\theta||e||^2 + 2\alpha||x - \hat{x}||||P||||e|| \\ &\leq -\theta||e||^2 + 2\alpha||P||||e||^2 \\ &\leq (-\theta + 2\alpha||P||)||e||^2. \end{aligned} \tag{5.22}$$

From equation (5.22), it can be seen that for any positive constant α, a positive constant θ can be found such that $\dot{V} < 0$, which implies that

$$\lim_{t\to\infty} \|x(t) - \hat{x}(t)\| \to 0. \tag{5.23}$$

■

From Proposition 5.1.2, it is obvious that this synchronization approach has the robustness property, which means that it is not highly sensitive to the mismatch of parameters used in the drive and response systems. This is against the definition of secure synchronization presented above; therefore, it should not be used for secure communications. So, based on the above analysis, we may state that a secure synchronization scheme should not be based on typical drive-response techniques and should not use well-classified chaotic systems. On the contrary, a good candidate might be a system that admits an observer, but at the same time has some important components that are detectable but not observable.

5.1.3 Secure Synchronization Scheme

The generalized Lorenz system (GLS) and its transformation form, the so-called generalized Lorenz canonical form, have been introduced in Chapter 2. Since it represents a very general class of chaotic systems with only one parameter, we shall use it to design a synchronization system based on the concept of secure synchronization.

Now, by letting

$$\eta = \begin{bmatrix} z_1 - z_2 \\ \lambda_1 z_2 - \lambda_2 z_1 \\ z_3 - \dfrac{(\kappa+1)(z_1 - z_2)^2}{2(\lambda_1 - \lambda_2)} \end{bmatrix}, \tag{5.24}$$

where $\eta = \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 \end{bmatrix}^T$, the system (2.21) can be transformed into the following observer canonical form (Čelikovský and Chen 2005):

$$\dot{\eta} = A\eta + F(\eta, y) \tag{5.25}$$

where $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$ and $F(\eta, y) = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - 0.5(\kappa+1)(\eta_1)^3 \\ K(\kappa)(\eta_1)^2 \end{bmatrix}$
with $K(\kappa) = \dfrac{\lambda_3(\kappa+1) - 2\kappa\lambda_2 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}$.

The reason to transform the system (2.21) into the form (5.25), here, is to remove the cross term $z_2(z_1 - z_2)$ in the system (2.21); meanwhile to keep the term $K(\kappa)\eta_1^2$ in the system (5.25), which depends only on the component $\eta_1 = z_1 - z_2$. This property is crucial for the synchronization scheme design to be presented later on.

We now consider the system (5.25) with its bounded trajectory $\eta(t)$, $t \geq t_0$ as the drive system and the first state η_1 is chosen as the driving signal to drive a response system in order to achieve the synchronization. Then the drive system can be expressed as follows

$$\begin{aligned} \dot{\eta} &= A\eta + F(\eta, y) \\ y &= C^T\eta \end{aligned} \tag{5.26}$$

where $C^T = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$. Notice that, for the drive system (5.26), the pair $(C^T,\ A)$ is not observable but detectable, which implies the possibility to design a response system as an observer to synchronize the system (5.26). Now we consider the following system as the response one:

$$\begin{aligned} \dot{\hat{\eta}} &= A\hat{\eta} + F(\hat{\eta}, y) + L(\hat{\eta}_1 - \eta_1') \\ &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1' \\ -\lambda_1\lambda_2\eta_1' - (\lambda_1 - \lambda_2)\eta_1'\hat{\eta}_3 - 0.5(\kappa+1)(\eta_1')^3 \\ K(\kappa)(\eta_1')^2 \end{bmatrix} + \begin{bmatrix} l_1 \\ l_2 \\ 0 \end{bmatrix} (\hat{\eta}_1 - \eta_1') \end{aligned} \tag{5.27}$$

where $\hat{\eta} = \begin{bmatrix} \hat{\eta}_1 & \hat{\eta}_2 & \hat{\eta}_3 \end{bmatrix}^T$, and $L = \begin{bmatrix} l_1 & l_2 & 0 \end{bmatrix}^T$ with $l_{1,2} < 0$. In addition, η_1' is the input driving signal, which may be biased by the noise during the propagation procedure. Thus, by assuming $\|\eta_1(t) - \eta_1'(t)\| \leq \varepsilon$, where ε is a small positive constant, the following theorem can be obtained.

Theorem 5.1.1 (Čelikovský and Chen 2005). *Consider a drive system given by (5.26) and an observer-based response system given by (5.27). It holds exponentially* *in time that*

$$\lim_{t\to\infty} \|\eta(t) - \hat{\eta}(t))\| \leq D\varepsilon \tag{5.28}$$

where D is some positive constant. Particularly, if $\eta_1 = \eta_1'$, the response system (5.27) globally asymptotically synchronizes the drive system (5.26), i.e.,

$$\lim_{t\to\infty} \|\eta(t) - \hat{\eta}(t))\| = 0 \tag{5.29}$$

Proof. By allowing the state error $\tilde{\eta} = \begin{bmatrix}\tilde{\eta}_1 & \tilde{\eta}_2 & \tilde{\eta}_3\end{bmatrix}^T = \eta - \hat{\eta}$, the error dynamics can be written as follows:

$$\begin{aligned}
\dot{\tilde{\eta}}_1 &= \dot{\eta}_1 - \dot{\hat{\eta}}_1 \\
&= (\lambda_1 + \lambda_2)\eta_1 + \eta_2 - l_1\hat{\eta}_1 - \hat{\eta}_2 - (\lambda_1 + \lambda_2 - l_1)\eta_1' \\
&= l_1(\eta_1 - \hat{\eta}_1) + \eta_2 - \hat{\eta}_2 + (\lambda_1 + \lambda_2 - l_1)(\eta_1 - \eta_1') \\
&= l_1\tilde{\eta}_1 + \tilde{\eta}_2 + (\lambda_1 + \lambda_2 - l_1)(\eta_1 - \eta_1')
\end{aligned} \tag{5.30}$$

$$\begin{aligned}
\dot{\tilde{\eta}}_2 &= \dot{\eta}_2 - \dot{\hat{\eta}}_2 \\
&= -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - 0.5(\kappa + 1)\eta_1^3 \\
&\quad -l_2\hat{\eta}_1 + (\lambda_1\lambda_2 + l_2)\eta_1' + (\lambda_1 - \lambda_2)\eta_1'\hat{\eta}_3 + 0.5(\kappa + 1)(\eta_1')^3 \\
&= l_2(\eta_1 - \hat{\eta}_1) - (\lambda_1 - \lambda_2)\eta_1'(\eta_3 - \hat{\eta}_3) \\
&\quad +(-\lambda_1\lambda_2 - l_2 - (\lambda_1 - \lambda_2)\eta_3 - 0.5(\kappa + 1)(\eta_1^2 + \eta_1^2(\eta_1')^2 + (\eta_1')^2))(\eta_1 - \eta_1') \\
&= l_2\tilde{\eta}_1 + \phi(t)\tilde{\eta}_3 + \varphi(t)(\eta_1 - \eta_1')
\end{aligned} \tag{5.31}$$

where $\phi(t) = -(\lambda_1 - \lambda_2)\eta_1'$ and $\varphi(t) = (-\lambda_1\lambda_2 - l_2 - (\lambda_1 - \lambda_2)\eta_3 - 0.5(\kappa + 1)(\eta_1^2 + \eta_1^2(\eta_1')^2 + (\eta_1')^2))$. Since trajectories $\eta(t)$ are bounded, $\phi(t)$ and $\varphi(t)$ are bounded functions.

$$\begin{aligned}
\dot{\tilde{\eta}}_3 &= \dot{\eta}_3 - \dot{\hat{\eta}}_3 \\
&= \lambda_3(\eta_3 - \hat{\eta}_3) + K(\kappa)(\eta_1^2 - (\eta_1')^2) \\
&= \lambda_3\tilde{\eta}_3 + K(\kappa)(\eta_1 + \eta_1')(\eta_1 - \eta_1') \\
&= \lambda_3\tilde{\eta}_3 + \psi(t)(\eta_1 - \eta_1')
\end{aligned} \tag{5.32}$$

where $\psi(t) = K(\kappa)(\eta_1 + \eta_1')$ is also a bounded function.

Obviously, by solving equation (5.32), it is easy show that

$$\tilde{\eta}_3(t) = e^{\lambda_3 t}\tilde{\eta}_3(0) + e^{\lambda_3 t}\int_0^t e^{-\lambda_3 \tau}\psi(\tau)(\eta_1(\tau) - \eta_1'(\tau))d\tau. \tag{5.33}$$

Assume $\|\psi(t)\| \le d_1$, $d_1 > 0$. Then we can get

$$\begin{aligned}
\|\tilde{\eta}_3(t)\| &= \|e^{\lambda_3 t}\tilde{\eta}_3(0) + e^{\lambda_3 t}\int_0^t e^{-\lambda_3 \tau}\psi(\tau)(\eta_1(\tau) - \eta_1'(\tau))d\tau \,\| \\
&= e^{\lambda_3 t}\|\tilde{\eta}_3(0)\| + e^{\lambda_3 t}\int_0^t e^{-\lambda_3 \tau}\|\psi(\tau)\|\|(\eta_1(\tau) - \eta_1'(\tau))\|d\tau \\
&\le e^{\lambda_3 t}\|\tilde{\eta}_3(0)\| + d_1\varepsilon\, e^{\lambda_3 t}\int_0^t e^{-\lambda_3 \tau}d\tau \\
&\le e^{\lambda_3 t}\|\tilde{\eta}_3(0)\| + d_1\varepsilon\, e^{\lambda_3 t}(-\tfrac{1}{\lambda_3})(e^{-\lambda_3 t} - 1) \\
&\le e^{\lambda_3 t}\|\tilde{\eta}_3(0)\| - \tfrac{d_1\varepsilon}{\lambda_3} + \tfrac{d_1\varepsilon}{\lambda_3}e^{\lambda_3 t}.
\end{aligned} \tag{5.34}$$

Clearly, since $\lambda_3 < 0$, $d_1 > 0$ and $\varepsilon > 0$ we can obtain

$$\lim_{t\to\infty}\|\tilde{\eta}_3(t)\| \le e^{\lambda_3 t}\|\tilde{\eta}_3(0)\| - \frac{d_1\varepsilon}{\lambda_3} + \frac{d_1\varepsilon}{\lambda_3}e^{\lambda_3 t} \le -\frac{d_1\varepsilon}{\lambda_3} \le D_1\varepsilon \tag{5.35}$$

where $D_1 = -\frac{d_1}{\lambda_3}$ is a positive constant.

Now, by defining $\bar{\eta} = \begin{bmatrix}\tilde{\eta}_1 & \tilde{\eta}_2\end{bmatrix}^T$, and according to equation (5.30) and (5.31), we can have

$$\begin{aligned}
\dot{\bar{\eta}} &= \begin{bmatrix}\dot{\tilde{\eta}}_1 \\ \dot{\tilde{\eta}}_2\end{bmatrix} \\
&= \begin{bmatrix} l_1 & 1 \\ l_2 & 0\end{bmatrix}\bar{\eta} + \begin{bmatrix}0 \\ \phi(t)\end{bmatrix}\tilde{\eta}_3 + \begin{bmatrix}\lambda_3 + \lambda_2 - l_1 \\ \varphi(t)\end{bmatrix}(\eta_1 - \eta_1') \\
&= S\bar{\eta} + \tilde{\phi}(t)\tilde{\eta}_3 + \tilde{\varphi}(t)(\eta_1 - \eta_1').
\end{aligned} \tag{5.36}$$

where $S = \begin{bmatrix} l_1 & 1 \\ l_2 & 0\end{bmatrix}$, $\tilde{\phi}(t) = \begin{bmatrix}0 \\ \phi(t)\end{bmatrix}$ and $\tilde{\varphi}(t) = \begin{bmatrix}\lambda_1 + \lambda_2 - l_1 \\ \varphi(t)\end{bmatrix}$. Obviously, S is a Hurwitz matrix, and $\tilde{\phi}(t)$ and $\tilde{\varphi}(t)$ are also bounded functions.

Therefore, by solving (5.36), we can have:

$$\begin{aligned}
\bar{\eta}(t) &= e^{St}\bar{\eta}(0) + e^{St}\int_0^t e^{-S\tau}\tilde{\phi}(\tau)\tilde{\eta}_3(\tau)d\tau \\
&\quad + e^{St}\int_0^t e^{-S\tau}\tilde{\varphi}(\tau)(\eta_1(\tau) - \eta_1'(\tau))d\tau.
\end{aligned} \tag{5.37}$$

Similarly, assume $\|\tilde{\phi}(t)\| \leq d_2$ and $\|\tilde{\varphi}\| \leq d_3$, where d_2, d_3 are positive constants. Then we can get:

$$\begin{aligned} \|\bar{\eta}(t)\| &= \|e^{St}\|\|\bar{\eta}(0)\| + \|e^{St}\| \int_0^t \| e^{-S\tau}\|\|\tilde{\phi}(\tau)\|\|\tilde{\eta}_3(\tau)\|d\tau \\ &\quad + \|e^{St}\| \int_0^t \| e^{-S\tau}\|\|\tilde{\varphi}(\tau)\|\|(\eta_1(\tau) - \eta_1'(\tau))\|d\tau \\ &\leq \|e^{St}\|\|\bar{\eta}(0)\| + d_2 \| e^{St}\| \int_0^t \| e^{-S\tau}\|\|\tilde{\eta}_3(\tau)\|d\tau \\ &\quad + d_3\varepsilon \| e^{St}\| \int_0^t \| e^{-S\tau}\|d\tau \end{aligned} \tag{5.38}$$

Since the matrix S is Hurwitz, there exist two positive constants $m \geq 1$ and $\alpha > 0$ such that $\|e^{St}\| \leq me^{-\alpha t}$ for all $t \geq 0$. Thus, the following inequality:

$$\|\bar{\eta}(t)\| \leq m\,e^{-\alpha t}\|\bar{\eta}(0)\| + d_2 m \int_0^t e^{-\alpha(t-\tau)}\|\tilde{\eta}_3(\tau)\|d\tau + d_3\varepsilon m \int_0^t e^{-\alpha(t-\tau)}d\tau \tag{5.39}$$

is satisfied for all $t \geq 0$.

Notice that, based on equation (5.33) and (5.35), the second part of the right hand side of (5.39) can be written as

$$\begin{aligned} & d_2 m\, e^{-\alpha t} \int_0^t e^{\alpha\tau}\|\tilde{\eta}_3(\tau)\|d\tau \\ \leq\ & d_2 m\, e^{-\alpha t} \int_0^t e^{\alpha\tau}(e^{\lambda_3\tau}\|\tilde{\eta}_3(0)\| + D_1\varepsilon - D_1\varepsilon\, e^{\lambda_3\tau})d\tau \\ \leq\ & d_2 m\, e^{-\alpha t} \int_0^t (e^{(\alpha+\lambda_3)\tau}\|\tilde{\eta}_3(0)\| + D_1\varepsilon\, e^{\alpha\tau} - D_1\varepsilon\, e^{(\alpha+\lambda_3)\tau})d\tau \\ \leq\ & d_2 m\, e^{-\alpha t}(\frac{\|\tilde{\eta}_3(0)\|}{\alpha+\lambda_3}(e^{(\alpha+\lambda_3)t}-1) + \frac{D_1\varepsilon}{\alpha}(e^{\alpha t}-1) - \frac{D_1\varepsilon}{\alpha+\lambda_3}(e^{(\alpha+\lambda_3)t}-1)) \\ \leq\ & \frac{d_2 m \| \tilde{\eta}_3(0)\|}{\alpha+\lambda_3}e^{\lambda_3 t} - \frac{d_2 m \| \tilde{\eta}_3(0)\|}{\alpha+\lambda_3}e^{-\alpha t} + \frac{d_2 m D_1\varepsilon}{\alpha} - \frac{d_2 m D_1\varepsilon}{\alpha}e^{-\alpha t} \\ & -\frac{d_2 m D_1\varepsilon}{\alpha+\lambda_3}e^{\lambda_3 t} + \frac{d_2 m D_1\varepsilon}{\alpha+\lambda_3}e^{-\alpha t}. \end{aligned} \tag{5.40}$$

Clearly, with $\lambda_3 < 0$ and $\alpha > 0$, and as $t \rightarrow \infty$, the following inequality can be obtained

$$d_2 m\, e^{-\alpha t} \int_0^t e^{\alpha\tau}\|\tilde{\eta}_3(\tau)\|d\tau \leq \frac{d_2 m D_1\varepsilon}{\alpha}. \tag{5.41}$$

Similarly, we can get the solution for the third part of the right hand side of (5.39), given by

$$d_3\varepsilon m \int_0^t e^{-\alpha(t-\tau)}d\tau = \frac{d_3\varepsilon m}{\alpha} - \frac{d_3\varepsilon m}{\alpha}e^{-\alpha t}. \tag{5.42}$$

Obviously, $d_3\varepsilon m \int_0^t e^{-\alpha(t-\tau)}d\tau$ tends to $\frac{d_3\varepsilon m}{\alpha}$ as $t \rightarrow \infty$.

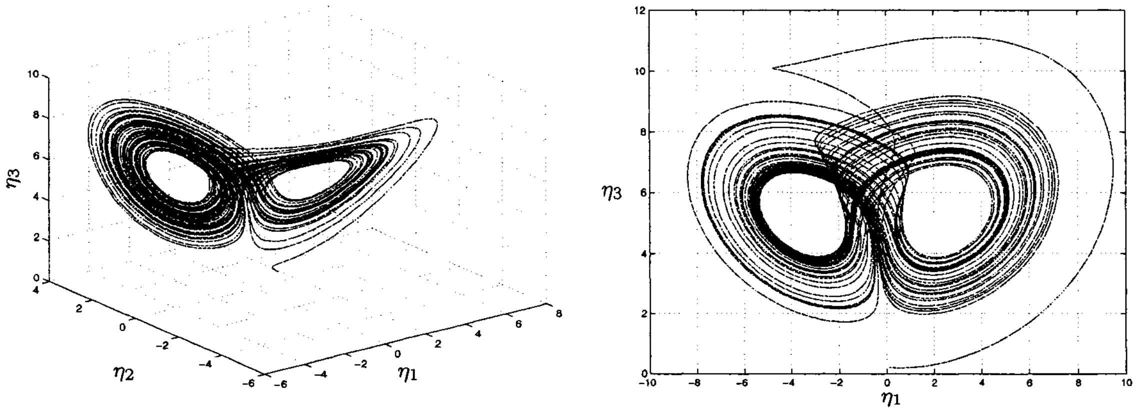
Based on equations (5.39)–(5.42), we can finally get:

$$\lim_{t\rightarrow\infty} \|\bar{\eta}(t)\| \leq \frac{d_2 m D_1\varepsilon}{\alpha} + \frac{d_3\varepsilon m}{\alpha} \leq D_2\varepsilon \tag{5.43}$$

where $D_2 = \frac{d_2 m D_1 + d_3 m}{\alpha}$ is a positive constant.

This completes the proof. ■

In the following numerical simulation, $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -2$, $\kappa = 0$, $l_1 = -8$ and $l_2 = -12$ was chosen to construct the secure synchronization system, while the initial error between the drive system (5.26) and the observer-based system (5.27) was set quite large. In addition, we only considered the case of $\eta_1(t) \equiv \eta_1'(t)$, that means there was no noise or bias involved in the driving signal η_1. Figure 5.3 shows the chaotic behaviour of the drive system (5.26) in three-dimension and in η_1-η_3 plane. Figure 5.4 demonstrates that the synchronization errors of the system (5.26) and (5.27) can converge to zero exponentially.



(a) The oscillator in three dimension

(b) The oscillator in η_1-η_3 plane

Figure 5.3: Chaotic behaviour of the drive system (5.26)

We now analyze the security property of the synchronization scheme. First of all, we only consider the parameter κ in the drive system (5.26) as the secret key. According to the definition of secure synchronization, it is supposed that with a mismatched key parameter κ used in the "fake" response system, it is very difficult for an intruder to achieve the synchronization. This refers to the property of antirobust secure. The effect of a mismatch in the key parameter κ is given in the following

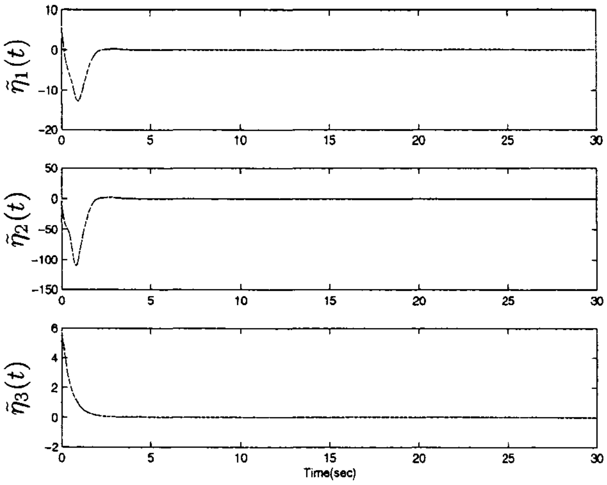


Figure 5.4: Synchronization of the drive system and the observer-based response system

proposition.

Proposition 5.1.3 (Čelikovský and Chen 2005). *Consider the drive system a key parameter $\kappa = \kappa_d$, and the observer-based response system with an unbiased input, i.e., $\eta_1' = \eta_1$ and a mismatched key parameter $\kappa = \kappa_r$. Then for sufficiently small $|\kappa_d - \kappa_r|$, we have*

$$\lim_{t\to\infty} \|\eta_i(t) - \hat{\eta}_i(t))\| \leq D_i(l_1, l_2)|\kappa_d - \kappa_r| \tag{5.44}$$

where, for $i = 1, 2$, $D_i(l_1, l_2) > 0$ are some parameters converging to zero under the condition $l_1 \pm \sqrt{l_1^2 + 4l_2} \to -\infty$, while $D_3(l_1, l_2) > 0$ is the parameter which does not depend on $l_{1,2}$.

Proof. Defining the state error $\tilde{\eta} = \begin{bmatrix}\tilde{\eta}_1 & \tilde{\eta}_2 & \tilde{\eta}_3\end{bmatrix}^T = \eta - \hat{\eta}$, the error dynamics can be written as follows:

$$\dot{\tilde{\eta}}_1 = l_1\tilde{\eta}_1 + \tilde{\eta}_2 \tag{5.45}$$

$$\dot{\tilde{\eta}}_2 = l_2\tilde{\eta}_1 - (\lambda_1 - \lambda_2)\eta_1\tilde{\eta}_3 + 0.5(\kappa_r - \kappa_d)\eta_1^3 \tag{5.46}$$

$$\begin{aligned}\dot{\tilde{\eta}}_3 &= \lambda_3\tilde{\eta}_3 + K(\kappa_d - \kappa_r)\eta_1^2 \\ &= \lambda_3\tilde{\eta}_3 + K(\kappa_d - \kappa_r)\psi(t)\end{aligned} \tag{5.47}$$

where $\psi(t) = \eta_1^2(t)$ is obviously a bounded function.

Analogous to the previous proof procedure, solving equation (5.47) yields

$$\tilde{\eta}_3(t) = e^{\lambda_3 t}\tilde{\eta}_3(0) + K(\kappa_d - \kappa_r)e^{\lambda_3 t}\int_0^t e^{-\lambda_3 \tau}\psi(\tau)d\tau. \tag{5.48}$$

And finally we can end up with

$$\lim_{t\to\infty} \|\tilde{\eta}_3(t)\| \leq D_3|K(\kappa_d - \kappa_r)| \tag{5.49}$$

where D_3 is a positive constant depending on the parameter λ_3.

Similarly, by defining $\tilde{\eta} = \begin{bmatrix}\tilde{\eta}_1 & \tilde{\eta}_2\end{bmatrix}^T$, and according to equation (5.45) and (5.46), we can have

$$\begin{aligned}\dot{\tilde{\eta}} &= \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}\tilde{\eta} + \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1 \end{bmatrix}\tilde{\eta}_3 + (\kappa_d - \kappa_r)\begin{bmatrix} 0 \\ 0.5\eta_1^3 \end{bmatrix} \\ &= S\tilde{\eta} + \phi(t)\tilde{\eta}_3 + (\kappa_d - \kappa_r)\varphi(t)\end{aligned} \tag{5.50}$$

where $S = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}$, $\phi(t) = \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1 \end{bmatrix}$ and $\varphi(t) = \begin{bmatrix} 0 \\ 0.5\eta_1^3 \end{bmatrix}$. Obviously, S is a Hurwitz matrix, implying that there exists two positive constants $m \geq 1$ and $\alpha > 0$ such that $\|e^{St}\| \leq m\, e^{-\alpha t}$ for all $t \geq 0$. Moreover, $\phi(t)$ and $\varphi(t)$ are bounded functions, i.e., $\|\phi(t)\| \leq a_1$ and $\|\varphi(t)\| \leq a_2$ with $a_1 > 0$, $a_2 > 0$.

Therefore, by solving (5.50), we can have:

$$\begin{aligned}\|\tilde{\eta}(t)\| &= \|e^{St}\|\|\tilde{\eta}(0)\| + \|e^{St}\| \textstyle\int_0^t \|\, e^{-S\tau}\|\|\phi(\tau)\|\|\tilde{\eta}_3(\tau)\|d\tau \\ &\quad +|\kappa_d - \kappa_r|\|e^{St}\| \textstyle\int_0^t \|\, e^{-S\tau}\|\|\varphi(\tau)\|d\tau \\ &\leq \|e^{St}\|\|\tilde{\eta}(0)\| + a_1\|e^{St}\| \textstyle\int_0^t \|e^{-S\tau}\|\|\tilde{\eta}_3(\tau)\|d\tau \\ &\quad +a_2|\kappa_d - \kappa_r|\|e^{St}\| \textstyle\int_0^t \|e^{-S\tau}\|d\tau) \\ &\leq m\, e^{-\alpha t}\|\tilde{\eta}(0)\| + a_1 m \textstyle\int_0^t e^{-\alpha(t-\tau)}\|\tilde{\eta}_3(\tau)\|d\tau \\ &\quad +a_2 m|\kappa_d - \kappa_r| \textstyle\int_0^t e^{-\alpha(t-\tau)}d\tau\end{aligned} \tag{5.51}$$

Based on equation (5.49) and (5.51), we can finally get:

$$\lim_{t\to\infty} \|\tilde{\eta}(t)\| \leq \frac{m}{\alpha}(\frac{-D_3 a_1}{\lambda_3} + a_2 m)|\kappa_d - \kappa_r| \leq D|\kappa_d - \kappa_r| \tag{5.52}$$

where $D = \frac{m}{\alpha}(\frac{-D_3a_1}{\lambda_3} + a_2m)$, whose value is dependent on the matrix S. Since $S = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}$, it can be proved that, if $l_1 \pm \sqrt{l_1^2 + 4l_2} \to -\infty$ then

$$\lim_{t \to \infty} \|\bar{\eta}(t)\| = 0. \tag{5.53}$$

■

Through the above mathematical analysis, it is clear that, due to the special structure of the system used for the secure synchronization purpose, the third state is detectable but not observable, which leads to the third component of the error dynamics to be independent of the gains l_1 and l_2. This means that $D_{1,2}$ can be made sufficiently small by choosing a large observer gain, l_1 and l_2, thereby making the first two components of synchronization errors converge to a sufficiently small value. However, the third component of the error dynamics only dependents on the mismatch of the parameter, which implies that the synchronization errors will stay large if there exists a mismatch of the parameter. Hence, using a mismatched "Key", κ , in a "fake" synchronization system may lead to a signal which is qualitatively similar to the correct one, but it will not help much the intruder to recover the hidden message signal by using this fake synchronization system. Therefore, the antirobust secure can be realized. On the other hand, the adaptive-observer-based scheme presented in Proposition 5.1.1 can not be used for this case, because, by considering $C^T = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$ in system (5.26) and equation (5.4) with P being nonsingular, it leads to the rank of B to be equal to one. This means that it is not possible to design an adaptive-observer to estimate the values of the key parameter κ in the given drive system (5.26). Moreover, it is noticeable that there is a singularity for $\eta_1 = 0$ which can prevent the observer canonical form (5.26) from being further transformed into an observability form, where the latter enables the use of Proposition 5.1.1 or Proposition 5.1.2 with B having rank equal to one. So, clearly, the antiadaptive secure property can also be obtained for this approach.

Figure 5.5 shows the simulation result of synchronizing the systems (5.26) and

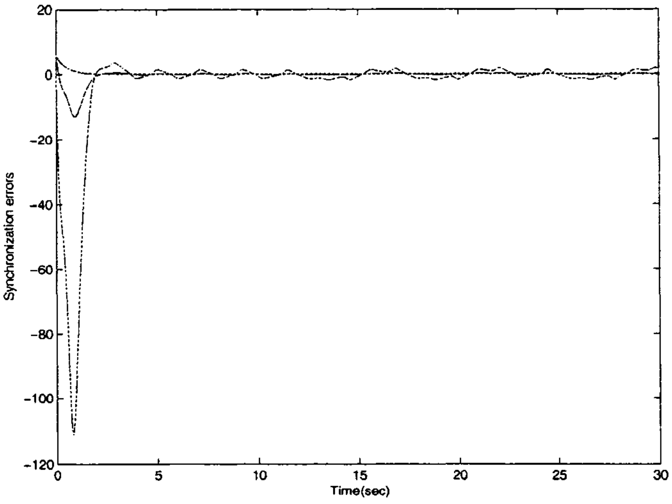


Figure 5.5: "Fake" synchronization of the system (5.26) and (5.27) with unmatched key parameter κ

(5.27), by using a slightly different parameter κ, namely, $\kappa_d = 0$ in the drive system (5.26) and $\kappa_d = 0.01$ in the response system (5.27). Other data are the same as those used in the previous simulations. As the figure shows, even a slight difference in the value of the parameter κ can cause a big synchronization error.

5.2 A New Secure Communication System

In previous sections, we discussed some insecure synchronization schemes, which make secure communication systems based on these synchronization schemes can not be applied to transmitting message signals that request a high level of security. The synchronization scheme based on the generalized Lorenz system discussed in Section 5.1.3 has antiadaptive secure and antirobust secure properties, which means that we can design a new secure communication system based on this synchronization scheme to offer high security and privacy for the transmission of messages.

In the following, the observer-based secure synchronization scheme, illustrated above, is applied to designing a new chaotic secure communication system. Since the security property is the most crucial aspect for secure communication systems, we shall construct the cryptosystem based on the chaotic modulation method which has been discussed in detail in Chapter 4.

5.2.1 System Structure

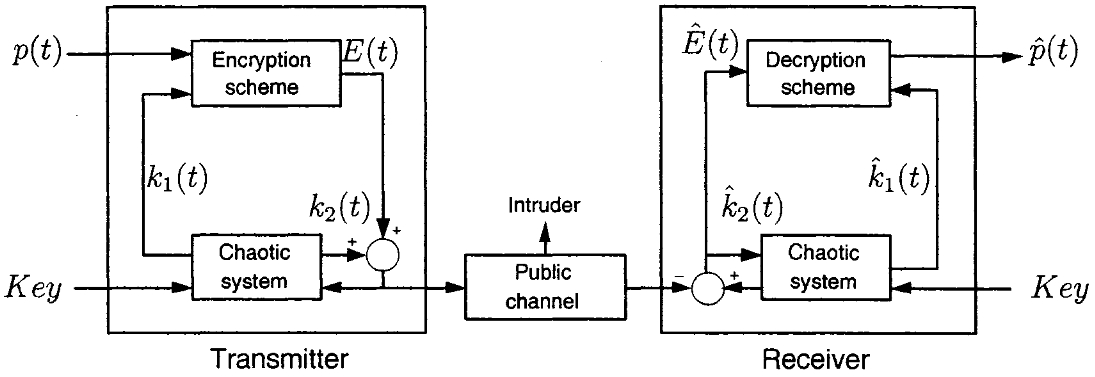


Figure 5.6: Block diagram of the chaotic secure communication system

Figure 5.6 shows the block diagram of the proposed cryptosystem, consisting of an encrypter module (Transmitter), a public communication channel and a decrypter module (Receiver). As the figure shows, the transmitter system consists of a chaotic system and an encryption scheme. The secret "Key", shown in Figure 5.6 is used to set the values of parameters of the chaotic system, namely, $Key \equiv \{\kappa, \lambda_1, \lambda_2, \lambda_3\}$. The chaotic system is used to generate two key signals, $k_1(t)$ and $k_2(t)$. The first key signal, $k_1(t)$, is one state variable of the chaotic system, which should be utilized by the encryption scheme to pre-encrypt the message signal $p(t)$. Then, the pre-encrypted signal, $E(t)$, is added to the second key signal, $k_2(t)$, which is another state variable of the chaotic system, for the further encryption. The sum is then transmitted to the receiver system through the public channel; meanwhile, it is also fed back to the chaotic system at the transmitter end. For the receiver system, same as the transmitter counterpart, it also consists of a chaotic system and a decryption scheme. By using exactly the same "Key" for the chaotic system parameters,

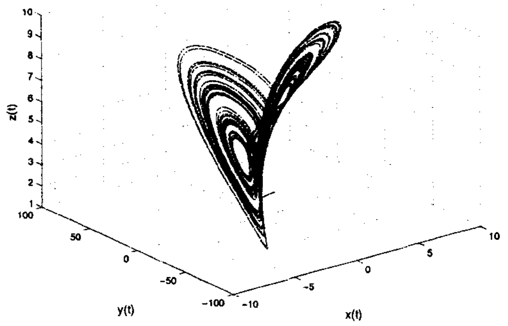


Figure 5.7: Chaotic behaviour of system (5.54).

the synchronization between the transmitter and the receiver can be achieved. Thus, two key signals, $\hat{k}_1(t)$ and $\hat{k}_2(t)$, precisely the same as those used by the transmitter system can be reconstructed, using a synchronization scheme. Hence, the decryption scheme can be employed to finally recover the message signal $p(t)$.

The chaotic system used in the transmitter is described by equation (5.26) with a slight modification[1] and represented as follows:

$$\begin{aligned} \dot{\eta} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta + \begin{bmatrix} (\lambda_1+\lambda_2)y(t) \\ -\lambda_1\lambda_2 y(t) - (\lambda_1-\lambda_2)\eta_3 y(t) - 0.5(\kappa+1)(y(t))^3 \\ K(\kappa)(y(t))^2 \end{bmatrix} + LE(t) \\ y &= \eta_1 + E(t) \end{aligned} \tag{5.54}$$

where $E(t) \in \mathbb{R}$ is the pre-encrypted signal outputted from the encryption scheme and $L = \begin{bmatrix} L_1 & L_2 & 0 \end{bmatrix}^T$ is a gain vector. Moreover, we consider $\eta_1(t)$ as the key signal, $k_2(t)$. Then, the sum of $k_2(t)$ and the pre-encrypted signal $E(t)$, namely, $y(t) \in \mathbb{R}$, is considered as the chaotic transmission signal, which drives the chaotic system at the

[1] Here, in order to design the receiver system properly, we modify the system (5.26) by adding the term $LE(t)$. Moreover, with an appropriately chosen parameters, the ratio of the value of the modification part, $LE(t)$, to the value of state variables can be made quite small, for instance, 0.001. Hence, we would consider it as a kind of external noise, which would not influence dynamical properties of the system, implying that system (5.54) can still present a chaotic behavior, as shown in Figure 5.7.

receiver end. For the encryption scheme, since the third component of state variables of the chaotic system, η_3, is only detectable but unobservable, we consider it as the other key signal, $k_1(t)$. This should further increase the security level of the proposed cryptosystem. Then, the message signal can be pre-encrypted by means of an n-shift cipher introduced in (Yang *et al.* 1997), which can be depicted as:

$$E(t) = \underbrace{f(\dots f(f}_{n}(p(t), \underbrace{k_1(t)), k_1(t)), \dots, k_1(t))}_{n} \tag{5.55}$$

where f is a nonlinear function given by:

$$f(x,k) = \begin{cases} (x+k)+2h, & -2h \le (x+k) \le -h \\ (x+k), & -h \le (x+k) \le h \\ (x+k)-2h, & h \le (x+k) \le 2h \end{cases} \tag{5.56}$$

where h is some constant parameter chosen in such a way that $x(t)$ and $k(t)$ lie within $(-h, h)$. This function is shown in Figure (5.8).

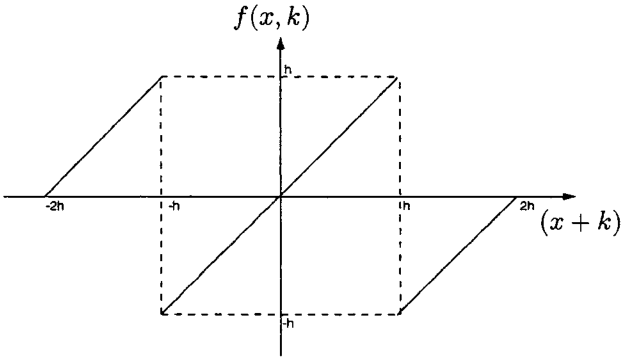


Figure 5.8: Nonlinear function used in continuous shift cipher

In the n-shift cipher, the key signal $k_1(t)$ is used n times to encrypt the message signal. Since the pre-encrypted signal is a function of $p(t)$ and $k_1(t)$, and since the pre-encrypted signal is then further modulated with another set of key signals, that is $k_2(t)$, it hides both the dynamical and the statistical characteristics of both $p(t)$ and $k_1(t)$.

Similarly, the synchronizing chaotic system at the receiver end can be constructed as follows:

$$\dot{\hat{\eta}} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} (\lambda_1 + \lambda_2)y(t) \\ -\lambda_1\lambda_2 y(t) - (\lambda_1 - \lambda_2)\hat{\eta}_3 y(t) - 0.5(\kappa + 1)(y(t))^3 \\ K(\kappa)(y(t))^2 \end{bmatrix} + L(y(t) - \hat{\eta}_1) \tag{5.57}$$

where y is the received signal and L is the gain vector the same as that used in the transmitter system.

Then, it is believed that the synchronization can only be achieved with the use of the same "Key" at both transmitter and receiver sides. Hence, the key signals can be re-generated, namely, $\hat{k}_1(t) \to k_1(t)$ and $\hat{k}_2(t) \to k_2(t)$ as t tends to infinity. Finally, the corresponding decryption scheme can be expressed as follows:

$$\hat{p}(t) = \underbrace{f(\ldots f(f}_{n}(\hat{E}(t), \underbrace{-\hat{k}_1(t)), -\hat{k}_1(t)), \ldots, -\hat{k}_1(t))}_{n} \tag{5.58}$$

where $\hat{E}(t) = y(t) - \hat{k}_1(t)$.

Then we have the following theorem:

Theorem 5.2.1. *Suppose a message signal, $p(t)$, is transmitted through a communication system consisting of a transmitter system with the chaotic system (5.54) and the encryption scheme (5.55), and a receiver system with the chaotic system (5.57) and the encryption scheme (5.58). Using the same "Key" in both transmitter and receiver system a global synchronization between the transmitter and the receiver system can be achieved and the message signal, $p(t)$, can be completely recovered at the receiver side.*

Proof. Defining the synchronization error $\tilde{\eta}(t) = \eta(t) - \hat{\eta}(t)$, where $\tilde{\eta} = \begin{bmatrix} \tilde{\eta}_1 & \tilde{\eta}_2 & \tilde{\eta}_3 \end{bmatrix}^T$, yields

$$\begin{aligned}\dot{\tilde{\eta}}_1(t) &= \dot{\eta}_1(t) - \dot{\hat{\eta}}_1(t)\\ &= \eta_2(t) + (\lambda_1+\lambda_2)(\eta_1(t)+E(t)) + L_1E(t)\\ &\quad -\hat{\eta}_2(t) - (\lambda_1+\lambda_2)(\eta_1(t)+E(t)) - L_1(\eta_1(t)+E(t)-\hat{\eta}_1(t))\\ &= -L_1(\eta_1(t)-\hat{\eta}_1(t)) + \eta_2(t) - \hat{\eta}_2(t)\\ &= -L_1\tilde{\eta}_1(t) + \tilde{\eta}_2(t)\end{aligned} \tag{5.59}$$

$$\begin{aligned}\dot{\tilde{\eta}}_2(t) &= \dot{\eta}_2(t) - \dot{\hat{\eta}}_2(t)\\ &= (-\lambda_1\lambda_2 - (\lambda_1-\lambda_2)\eta_3(t))(\eta_1(t)+E(t))\\ &\quad -0.5(\kappa+1)(\eta_1(t)+E(t))^3 + L_2E(t)\\ &\quad -(-\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\hat{\eta}_3(t))(\eta_1(t)+E(t))\\ &\quad +0.5(\kappa+1)(\eta_1(t)+E(t))^3 - L_2(\eta_1(t)+E(t)-\hat{\eta}_1(t))\\ &= -(\lambda_1-\lambda_2)(\eta_1(t)+E(t))\tilde{\eta}_3(t) - L_2\tilde{\eta}_1(t)\\ &= -L_2\tilde{\eta}_1(t) + (\lambda_1-\lambda_2)(\eta_1(t)+E(t))\tilde{\eta}_3(t)\end{aligned} \tag{5.60}$$

$$\begin{aligned}\dot{\tilde{\eta}}_3(t) &= \dot{\eta}_3(t) - \dot{\hat{\eta}}_3(t)\\ &= \lambda_3\eta_3(t) + K(\kappa)(\eta_1(t)+E(t))^2 - \lambda_3\hat{\eta}_3(t) - K(\kappa)(\eta_1(t)+E(t))^2\\ &= \lambda_3\tilde{\eta}_3(t)\end{aligned} \tag{5.61}$$

Obviously, by considering the inequality (2.20), the following equation is satisfied

$$\lim_{t\to\infty} \|\tilde{\eta}_3(t)\| = 0. \tag{5.62}$$

Further defining $\tilde{\eta}(t) = \begin{bmatrix}\tilde{\eta}_1(t) & \tilde{\eta}_2(t)\end{bmatrix}^T$, we can have:

$$\begin{aligned}\dot{\tilde{\eta}}(t) &= \begin{bmatrix}\dot{\tilde{\eta}}_1(t)\\ \dot{\tilde{\eta}}_2(t)\end{bmatrix}\\ &= \begin{bmatrix}-L_1 & 1\\ -L_2 & 0\end{bmatrix}\tilde{\eta}(t) + \begin{bmatrix}0\\ (\lambda_1-\lambda_2)(\eta_1(t)+E(t))\end{bmatrix}\tilde{\eta}_3(t)\\ &= S\tilde{\eta}(t) + \phi(t)\tilde{\eta}_3(t)\end{aligned} \tag{5.63}$$

where $S = \begin{bmatrix}-L_1 & 1\\ -L_2 & 0\end{bmatrix}$ and $\phi(t) = \begin{bmatrix}0\\ (\lambda_1-\lambda_2)(\eta_1(t)+E(t))\end{bmatrix}$ is a bounded function.

Since $\phi(t)$ and $\tilde{\eta}(t)$ ar $\lfloor(\lambda_1 - \lambda_2)(\eta_1(t) + E(t))\rfloor$

(t) are bounded, then if $L_{1,2}$ could be chosen in such a way that

S is a Hurwitz matrix, the synchronization error will converge to zero exponentially.

Once the synchronization between the transmitter and the receiver is achieved, the chaotic system in the receiver system can generate key signals the same as that used at the transmitter system, *i.e.*, $\lim_{t\to\infty} \hat{k}_1(t) \to k_1(t)$ and $\lim_{t\to\infty} \hat{k}_2(t) \to k_2(t)$. This means that $\lim_{t\to\infty} \hat{E}(t) = y(t) - \hat{k}_2(t) = E(t) + k_2(t) - \hat{k}_2(t) \to E(t)$, and then the decryption scheme (5.58) can be rewritten as:

$$\hat{p}(t) = \underbrace{f(\ldots f(f}_{n}(E(t), \underbrace{-k_1(t)), -k_1(t)), \ldots, -k_1(t))}_{n}. \tag{5.64}$$

Clearly, system (5.64) is the inverse procedure of the encryption scheme (5.55), which implies that the information signal can be finally retrieved.

■

5.2.2 Simulation Results

To explore the performance of the secure communication system proposed herein, two sets of numerical simulations have been performed for the different message signals.

Simulation I

In the first set of simulations, the message signal is considered as a sinusoidal function $p(t) = \sin(0.05\pi t)$, and the gain vector L is chosen as $L = \begin{bmatrix} 5 & 8 & 0 \end{bmatrix}^T$, implying that the matrix S in (5.63) is Hurwitz. For the encryption and decryption purpose, $h = 10$ and $n = 30$ are chosen for the n-shift cipher (5.55) and (5.58). First of all, we use the same "Key" for both of the transmitter and receiver system, namely, all the parameter settings of chaotic system in the transmitter and the receiver are the same.

Figure 5.9 shows the chaotic transmission signal transmitted over the public channel to the receiver system, and Figure 5.10 shows the synchronization error dy-

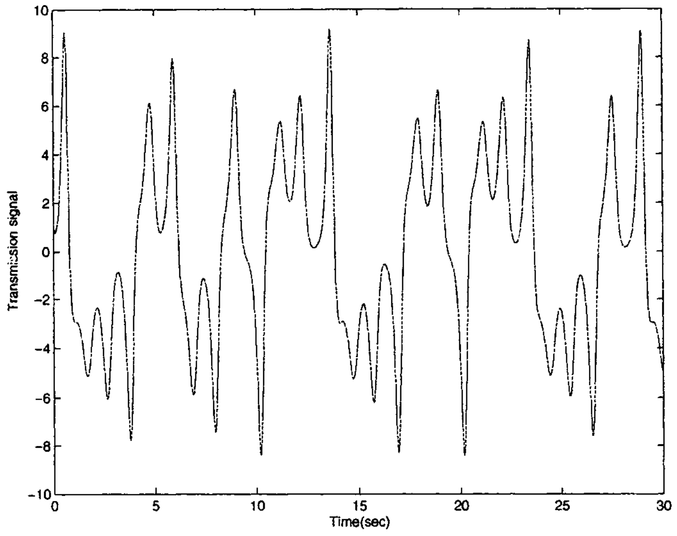


Figure 5.9: The transmission signal

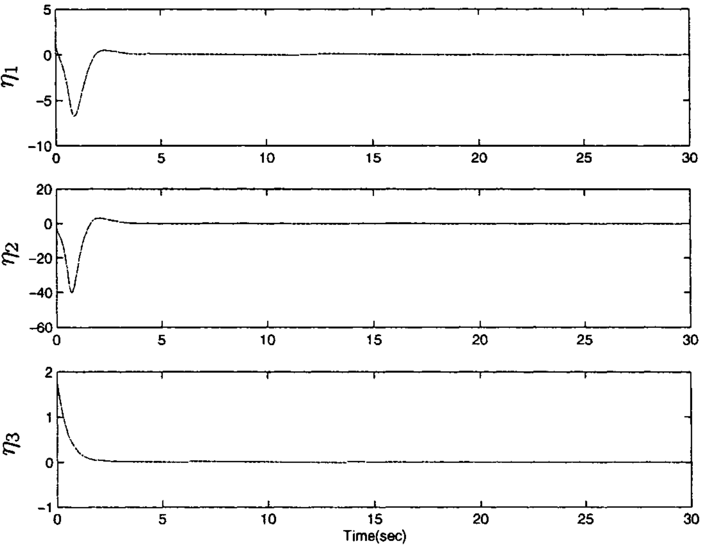


Figure 5.10: Synchronization errors

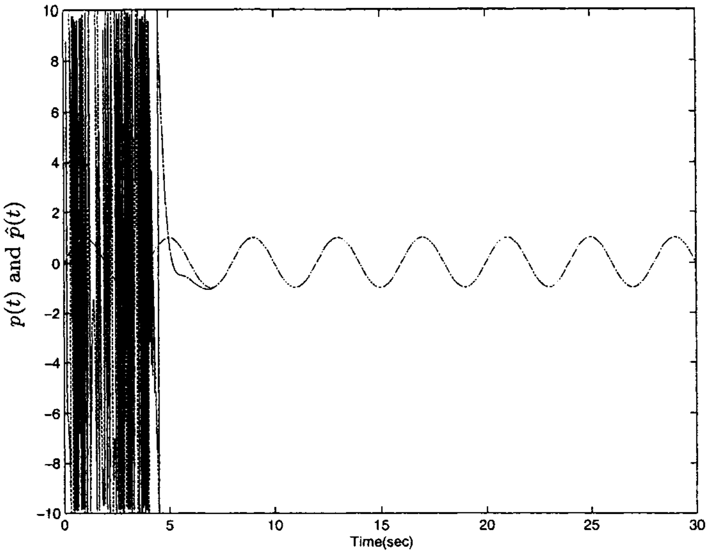


Figure 5.11: The original information signal and the recovered signal

namics of the proposed communication system. Figure 5.11 shows the original plain signal $p(t)$ and the retrieved signal $\hat{p}(t)$. Obviously, as the figure shows, after the synchronization phase, namely, once the synchronization of the transmitter and the receiver is achieved, the original message signal $p(t)$ is recovered successfully.

The following figures show the effect of a mismatch in the "Key" for the proposed secure communication system. Figure 5.12 shows that even with a slightly different parameter settings, (for instance, $\kappa_d = 0$ and $\kappa_r = 0.001$, where κ_d and κ_r are the parameter κ used in the transmitter and the receiver respectively, and other parameter settings are same), the synchronization error between the transmitter and the receiver is non-decayable. This means that the synchronization of the communication system, with the unmatched parameter, used in this simulation, can not be obtained. Therefore, the message signal can not be recovered at all, as shown in Figure 5.13.

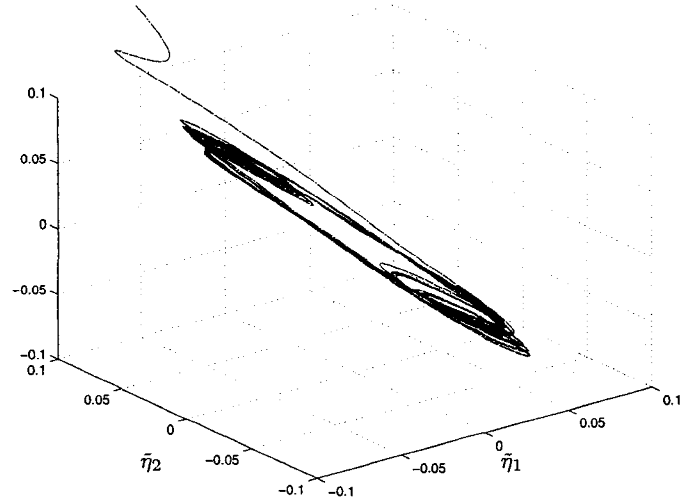


Figure 5.12: The behaviour of nondecaying errors of the "fake" synchronization with $\kappa_d = 0$ and $\kappa_r = 0.001$.

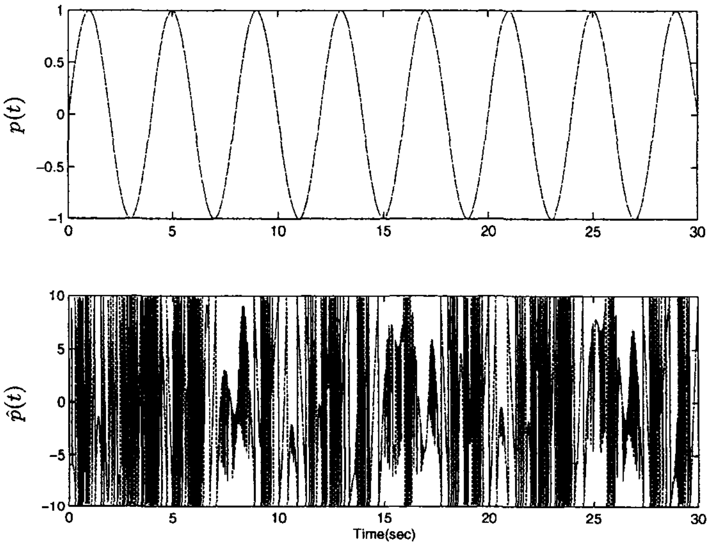


Figure 5.13: The original message signal and the wrongly recovered signal with the unmatched Key

Simulation II

In the second set of simulations, we choose a piece of sound signal, that is "This is the automatic control laboratory at the Lakehead University.", as the message signal to be transmitted through the proposed secure communication system. Similarly, we first use the same "Key" for the transmitter and the receiver. Figure 5.14 shows the simulation results; (a) represents the wave form of the original sound signal; (b) represents the wave form of the recovered sound signal and (c) represents the transmitted signal. Clearly, with the same "Key" used in the system, the original sound signal can be successfully retrieved at the receiver end. However, as Figure 5.15 shows, with the wrong "Key" used at the receiver side, it was not possible to achieve the synchronization, and therefore the original sound signal could not be recovered.

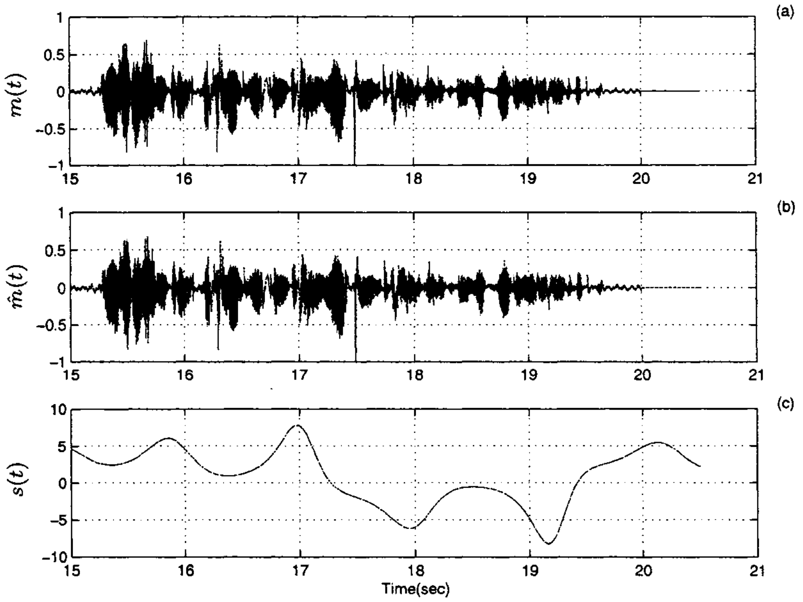


Figure 5.14: Simulation results for transmitting the sound signal with the same "Key" in transmitter and receiver systems

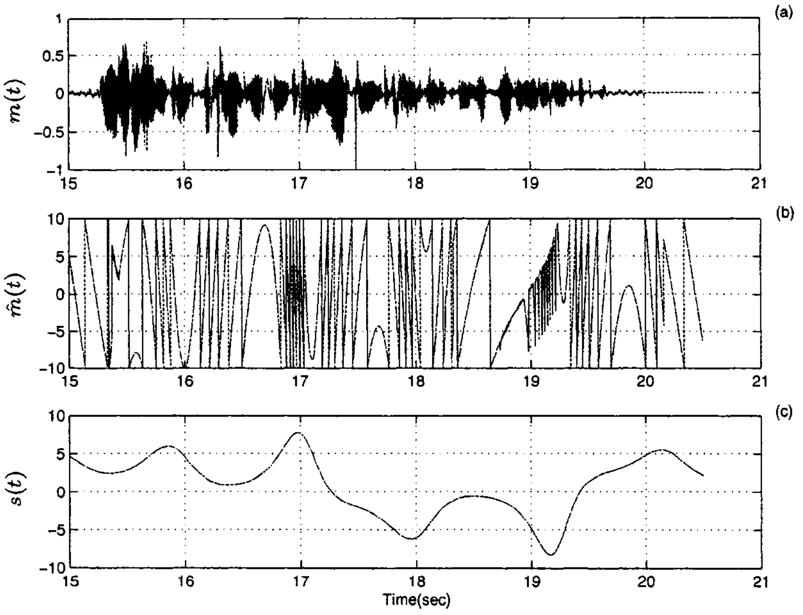


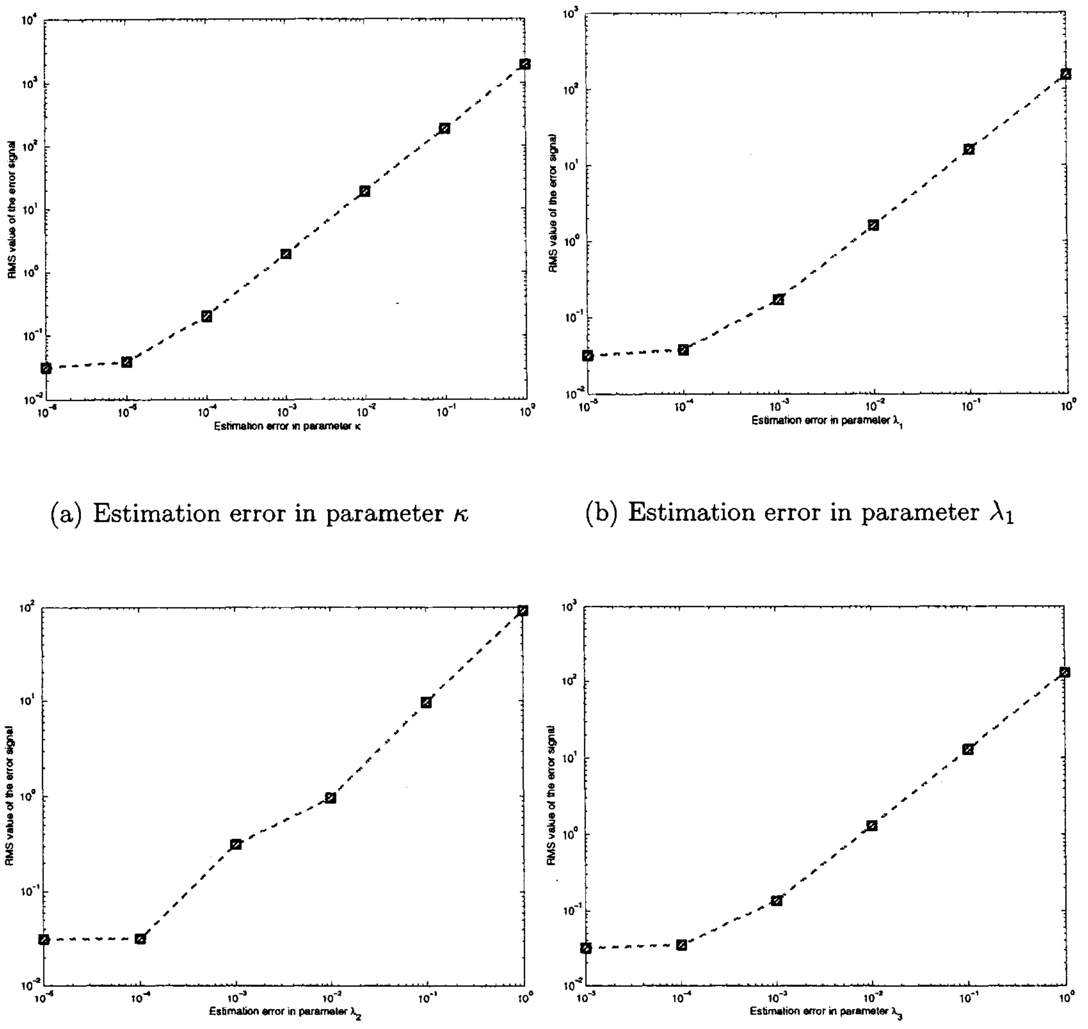
Figure 5.15: Simulation results for transmitting the sound signal with the unmatched "Key" in transmitter and receiver systems

5.2.3 System Security Analysis

For any secure communication scheme, a very important issue is whether or not it is actually secure. From the cryptographical viewpoint, according to (Schneier 1996), the security of a cryptosystem is a function of two things: the strength of the algorithm and the length of the key. In the previous section, we already analyzed the security property of the chaos synchronization scheme in secure communication systems, from the control theory point of view. Since the proposed secure communication system uses the chaos synchronization scheme, which has both antiadaptive secure and antirobust secure properties, thereby it can prevent the system from being vulnerable to some potential attacks. This means that the algorithm used in the proposed secure communication system is safe enough. We now turn our attention to analyzing another security property of the proposed secure communication system, namely the length of the key.

It is quite clear from the description and numerical simulation above that the security of the proposed communication system is entirely dependent on the secrecy of the parameter settings of the chaotic system, which are set by the secret "Key", *i.e.*, $Key \equiv \{\kappa, \lambda_1, \lambda_2, \lambda_3\}$. Hence, some very practical questions to ask are: how accurately must the values of parameters in the "Key" be known for an intruder to recover the encrypted message signal? Is there enough Keys to prevent the system from being attacked by a brute-force attack? To answer these questions, we simulated the proposed secure communication scheme by employing a wrong "Key" in the receiver system with random errors in the estimation of parameter settings. In these simulations, the message signal is still chosen as a sinusoidal function, *i.e.*, $p(t) = \sin(0.05\pi t)$, implying that the RMS norm value of the message signal is about 0.5. Figure 5.16 shows the effect of the estimation error in system parameters on the recovery of the encrypted message signal. As Figure 5.16(a) shows, the estimation error of parameter κ as little as 10^{-6} still produces a relatively large decryption error. Similarly, Figure 5.16(b-d) indicate that the estimation error of parameter λ_{1-3} as little as 10^{-5} still causes a relatively large decryption error. This means that, from the cryptographical view of point, the size of the key space of the proposed secure communication system will not be less than $10^6 \times 10^5 \times 10^5 \times 10^5 = 10^{21} \approx 2^{69}$ (Schneier 1996).

Assuming a brute-force search of every possible key is the most efficient method of breaking the secure communication system, then according to Table 5.1, which summarizes how long it would take to recover the encrypted message signal with the given key space, based on the fact that the key search machine tests 100 million keys per second, the length of the key for the proposed secure communication system is cryptographically large, implying that the proposed communication system is quite safe against a brute-force attack. Therefore, based on the analysis above, it is very clear that the proposed secure communication scheme can offer relatively high level of security for the transmission of message signals.



(a) Estimation error in parameter κ

(b) Estimation error in parameter λ_1

(c) Estimation error in parameter λ_2

(d) Estimation error in parameter λ_3

Figure 5.16: The dependence of the recovered signal power on a fixed error in parameters κ, λ_{1-3}, respectively

Key size	2^{40}	2^{56}	2^{64}	2^{69}
Required time	3.1 hours	347.5 days	5,849.4 years	317,100 years

Table 5.1: Brute-force key search times for various key sizes

5.3 Secure Communication System with the Time-Delay

In the former section, we proposed a new secure communication system, which has been proven to be able to offer a higher security level. Notice that, it only presents the ideal communication situation. However, for any real communication system, there always exists a propagation time-delay during the procedure of transmitting message signals from the transmitter to the receiver and, from the control theory point of view, the time-delay may cause the communication system to be unstable (Kamen 1982). For instance, the work by (Chen and Liu 2000) showed that the existence of a time-delay in the synchronous system may result in the loss of synchronization, thus, analyzing the stability of a synchronized system with the time-delay is a quite important subject. Therefore, in the following section we shall take into account this practical problem to analyze the stability of the proposed secure communication system in the presence of a time-delay.

Generally speaking, in a real communication system with the propagation time-delay involved, forcing the receiver system to synchronize with the transmitter system at exactly the same time seems unreasonable. Thus, in the following part, the synchronization of the transmitter and the receiver for a communication system with an unknown constant time-delay is re-defined as follows:

Definition 5.3.1 (Jiang *et al.* 2004). *The state of the receiver system at time t asymptotically synchronizes with the transmitter system at time $t - \tau_d$, if*

$$\lim_{t \to \infty} \parallel x(t - \tau_d) - \hat{x}(t) \parallel = 0,$$

where τ_d is the unknown constant time-delay, and $x(t)$ and $\hat{x}(t)$ are the state of transmitter and receiver system, respectively.

In light of this, the stability analysis for the proposed secure communication system with the time-delay involved can be carried on as follows. We suppose that there is an unknown constant propagation time-delay[2], τ_d, for the transmission of message signals from the transmitter to the receiver. This means that, at time $t - \tau_d$, the transmission signal is transmitted from the transmitter, and the delayed transmission signal will be received by the receiver at time t. Then the chaotic system (5.54) at the transmitter side can be re-expressed as follows:

$$\begin{aligned}
\dot{\eta}(t-\tau_d) &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta(t-\tau_d) + LE(t-\tau_d) \\
&\quad + \begin{bmatrix} (\lambda_1+\lambda_2)y(t-\tau_d) \\ -\lambda_1\lambda_2 y(t-\tau_d) - (\lambda_1-\lambda_2)\eta_3 y(t-\tau_d) - 0.5(\kappa+1)(y(t-\tau_d))^3 \\ K(\kappa)(y(t-\tau_d))^2 \end{bmatrix} \\
y(t-\tau_d) &= \eta_1(t-\tau_d) + E(t-\tau_d)
\end{aligned} \tag{5.65}$$

where L is the observer gain vector and $E(t - \tau_d)$ is the output of the encryption scheme. For the sake of brevity, here, we use a simple encryption scheme instead of function (5.55), which is given by:

$$E(t) = a_1\eta_3(t) + a_2 p(t), \tag{5.66}$$

where $p(t)$ is the message signal, and $0 < a_{1,2} < 1$ are some constant which should be chosen in such a way to make the chaos to signal ratio as high as possible.

For the chaotic system at the receiver side, since there is an unknown but constant time-delay, τ_d, for the transmission procedure, it will be driven by the delayed signal $y(t-\tau_d)$ for the synchronization purpose, so the system (5.57) can be re-expressed as

[2] Here, the assumption of a constant time-delay is based on the consideration that all the values of the transmission signal received by the receiver are unchanged but only delayed by a certain time.

follows:

$$\begin{aligned}
\dot{\hat{\eta}}(t) &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta}(t) + L(y(t-\tau_d) - \hat{y}(t)) \\
&\quad + \begin{bmatrix} (\lambda_1+\lambda_2)y(t-\tau_d) \\ -(\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\hat{\eta}_3(t))y(t-\tau_d) - 0.5(\kappa+1)(y(t-\tau_d))^3 \\ K(\kappa)(y(t-\tau_d))^2 \end{bmatrix} \qquad (5.67) \\
\hat{y}(t) &= \hat{\eta}_1(t)
\end{aligned}$$

where $y(t-\tau_d)$ is the received signal and L is the gain vector the same as that used in the transmitter system.

If system (5.65) can synchronize with system (5.67), *i.e.*, $\lim_{t\to\infty} \| x(t-\tau_d) - \hat{x}(t) \| = 0$, it can be obtained that $\hat{\eta}_1(t) \to \eta_1(t-\tau_d)$ and $\hat{\eta}_3(t) \to \eta_3(t-\tau_d)$. Then, the corresponding decryption scheme can be chosen as follows:

$$\hat{p}(t) = \frac{1}{a_2}(y(t-\tau_d) - \hat{y}(t) - a_1\hat{\eta}_3(t)) \qquad (5.68)$$

where $k_{1,2}$ are same as that in the encryption scheme, and $\hat{p}(t)$ is the retrieved message signal, which is the same as the original message signal but delayed by τ_d.

We now prove that, by appropriately choosing the observer gain vector L, system (5.67) can synchronize with (5.65), as described by the following theorem.

Theorem 5.3.1. *Suppose a message signal, $p(t)$, is transmitted through a secure communication system consisting of a transmitter system with the chaotic system (5.65) and the encryption scheme (5.66), and a receiver system with the chaotic system (5.67) and the decryption scheme (5.68). Further, consider that there is an unknown but constant propagation time-delay, τ_d, involved during the transmission procedure. By using the same "Key" in both the transmitter and the receiver system, the synchronization of the transmitter and the receiver can be achieved, and the message signal, $p(t)$, can be completely recovered at the receiver side, but only delayed by time τ_d.*

Proof. Defining the synchronization error $\tilde{\eta}(t) = \eta(t-\tau_d) - \hat{\eta}(t)$, where $\tilde{\eta} = \begin{bmatrix} \tilde{\eta}_1 & \tilde{\eta}_2 & \tilde{\eta}_3 \end{bmatrix}^T$, yields

$$\begin{aligned}
\dot{\tilde{\eta}}_1(t) &= \dot{\eta}_1(t-\tau_d) - \dot{\hat{\eta}}_1(t) \\
&= \eta_2(t-\tau_d) + (\lambda_1+\lambda_2)(\eta_1(t-\tau_d) + E(t-\tau_d)) + L_1 E(t-\tau_d) \\
&\quad -\hat{\eta}_2(t) - (\lambda_1+\lambda_2)(\eta_1(t-\tau_d) + E(t-\tau_d)) \\
&\quad -L_1(\eta_1(t-\tau_d) + E(t-\tau_d) - \hat{\eta}_1(t)) \\
&= -L_1(\eta_1(t-\tau_d) - \hat{\eta}_1(t)) + \eta_2(t-\tau_d) - \hat{\eta}_2(t) \\
&= -L_1\tilde{\eta}_1(t) + \tilde{\eta}_2(t)
\end{aligned} \tag{5.69}$$

$$\begin{aligned}
\dot{\tilde{\eta}}_2(t) &= \dot{\eta}_2(t-\tau_d) - \dot{\hat{\eta}}_2(t) \\
&= (-\lambda_1\lambda_2 - (\lambda_1-\lambda_2)\eta_3(t-\tau_d))(\eta_1(t-\tau_d) + E(t-\tau_d)) \\
&\quad -0.5(\kappa+1)(\eta_1(t-\tau_d) + E(t-\tau_d))^3 + L_2 E(t-\tau_d) \\
&\quad -(-\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\hat{\eta}_3(t))(\eta_1(t-\tau_d) + E(t-\tau_d)) \\
&\quad +0.5(\kappa+1)(\eta_1(t-\tau_d) + E(t-\tau_d))^3 - L_2(\eta_1(t-\tau_d) + E(t-\tau_d) - \hat{\eta}_1(t)) \\
&= -(\lambda_1-\lambda_2)(\eta_1(t-\tau_d) + E(t-\tau_d))\tilde{\eta}_3(t) - L_2\tilde{\eta}_1(t) \\
&= -L_2\tilde{\eta}_1(t) + (\lambda_1-\lambda_2)(\eta_1(t-\tau_d) + E(t-\tau_d))\tilde{\eta}_3(t)
\end{aligned} \tag{5.70}$$

$$\begin{aligned}
\dot{\tilde{\eta}}_3(t) &= \dot{\eta}_3(t-\tau_d) - \dot{\hat{\eta}}_3(t) \\
&= \lambda_3\eta_3(t-\tau_d) + K(\kappa)(\eta_1(t-\tau_d) + E(t-\tau_d))^2 \\
&\quad -\lambda_3\hat{\eta}_3(t) - K(\kappa)(\eta_1(t-\tau_d) + E(t-\tau_d))^2 \\
&= \lambda_3\tilde{\eta}_3(t)
\end{aligned} \tag{5.71}$$

Obviously, by considering the inequality (2.20), the following equation is satisfied

$$\lim_{t\to\infty} \|\tilde{\eta}_3(t)\| = 0. \tag{5.72}$$

Further defining $\tilde{\eta}(t) = \begin{bmatrix}\tilde{\eta}_1(t) & \tilde{\eta}_2(t)\end{bmatrix}^T$, we have:

$$\begin{aligned}
\dot{\tilde{\eta}}(t) &= \begin{bmatrix}\dot{\tilde{\eta}}_1(t)\\ \dot{\tilde{\eta}}_2(t)\end{bmatrix}\\
&= \begin{bmatrix}-L_1 & 1\\ -L_2 & 0\end{bmatrix}\tilde{\eta}(t) + \begin{bmatrix}0\\ (\lambda_1-\lambda_2)(\eta_1(t-\tau_d)+E(t-\tau_d))\end{bmatrix}\tilde{\eta}_3(t)\\
&= S\tilde{\eta}(t) + \phi(t)\tilde{\eta}_3(t)
\end{aligned}\tag{5.73}$$

where $S = \begin{bmatrix}-L_1 & 1\\ -L_2 & 0\end{bmatrix}$ and $\phi(t) = \begin{bmatrix}0\\ (\lambda_1-\lambda_2)(\eta_1(t-\tau_d)+E(t-\tau_d))\end{bmatrix}$ is a bounded function.

Since $\phi(t)$ and $\tilde{\eta}(t)$ are bounded, then if $L_{1,2}$ could be chosen in such a way that S is a Hurwitz matrix, the synchronization error will converge to zero exponentially. Thus, it can be obtained that $\hat{\eta}_1(t) \rightarrow \eta_1(t-\tau_d)$ and $\hat{\eta}_3(t) \rightarrow \eta_3(t-\tau_d)$ as t tends to infinity. Then, the message signal, $p(t)$, can be recovered as follows:

$$\begin{aligned}
\hat{p}(t) &= \tfrac{1}{a_2}(y(t-\tau_d) - \hat{y}(t) - a_1\hat{\eta}_3(t))\\
&= \tfrac{1}{a_2}(\eta_1(t-\tau_d) + a_1\eta_3(t-\tau_d) + a_2p(t-\tau_d) - \hat{\eta}_1(t) - a_1\hat{\eta}_3(t))\\
&\rightarrow p(t-\tau_d)
\end{aligned}\tag{5.74}$$

■

5.3.1 Simulation Results

Similar to the former section, to demonstrate the performance of the secure communication system with an unknown time-delay involved during the transmission procedure, two sets of numerical simulations have been performed for the different type of files.

Simulation I

In the first set of simulations, the message signal is still considered as a sinusoidal function $p(t) = \sin(0.05\pi t)$, and the gain vector L is chosen as $L = \begin{bmatrix}5 & 8 & 0\end{bmatrix}^T$, implying that the matrix S in (5.73) is Hurwitz. For the encryption and decryption purpose, $a_1 = 0.001$ and $a_2 = 0.01$ are chosen for function (5.66) and (5.68). Similarly, we first use the same "Key" for both of the transmitter and receiver system.

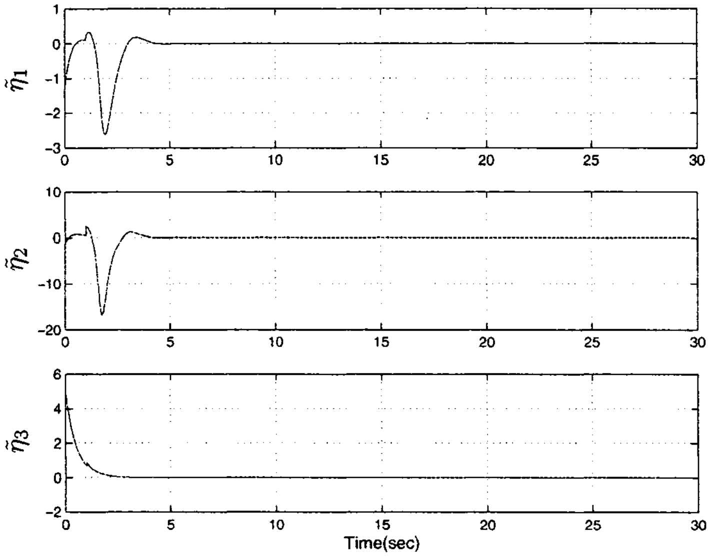


Figure 5.17: Synchronization errors of the secure communication system with the time-delay.

Figure 5.17 shows the synchronization error dynamics of the proposed cryptosystem with an unknown propagation time-delay. As the figure shows, even though there exists an unknown time-delay between the transmitter and the receiver for the proposed secure communication, the synchronization can still be achieved. Figure 5.18 shows the original message signal $p(t)$ and the retrieved signal $\hat{p}(t)$. Obviously, as the figure shows, once the synchronization of transmitter and receiver systems is achieved, the original message signal $p(t)$ is recovered successfully but only delayed by τ_d.

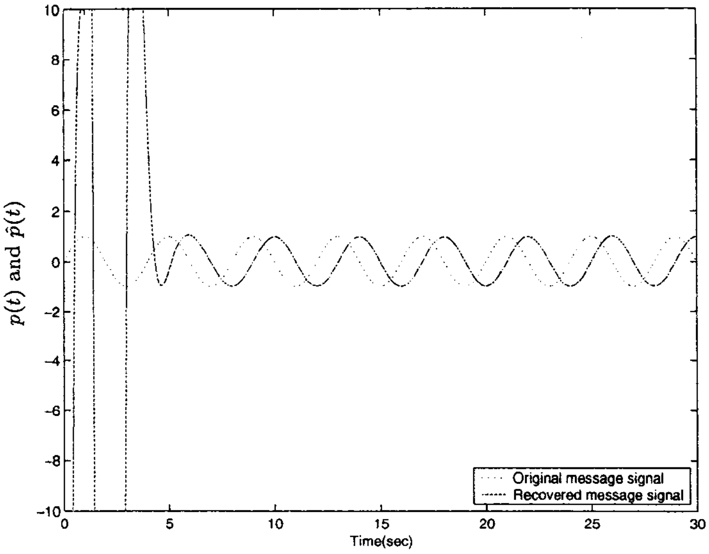


Figure 5.18: The original message signal and the recovered signal

The following figures show the effect of a mismatch in the "Key" for the secure communication system with an unknown time-delay. Figure 5.19 shows that, similar to the pervious delay-free case, even with a slightly different parameter settings, ($\kappa_d = 0$ and $\kappa_r = 0.001$ and other parameters are same), the synchronization error between the transmitter and the receiver is non-decayable. This means that the synchronization of the communication system, with the unmatched parameter, used in this simulation, can not be obtained. Therefore, the message signal can not be recovered at all, as shown in Figure 5.20.

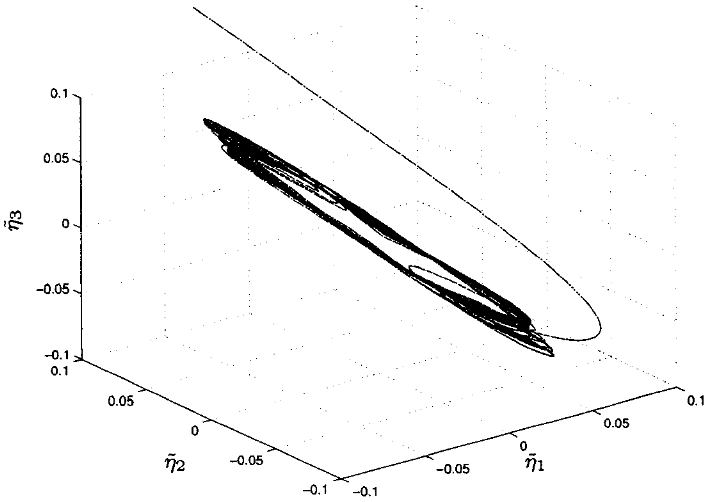


Figure 5.19: The behaviour of nondecaying errors of the "fake" synchronization with $\kappa_d = 0$ and $\kappa_r = 0.001$.

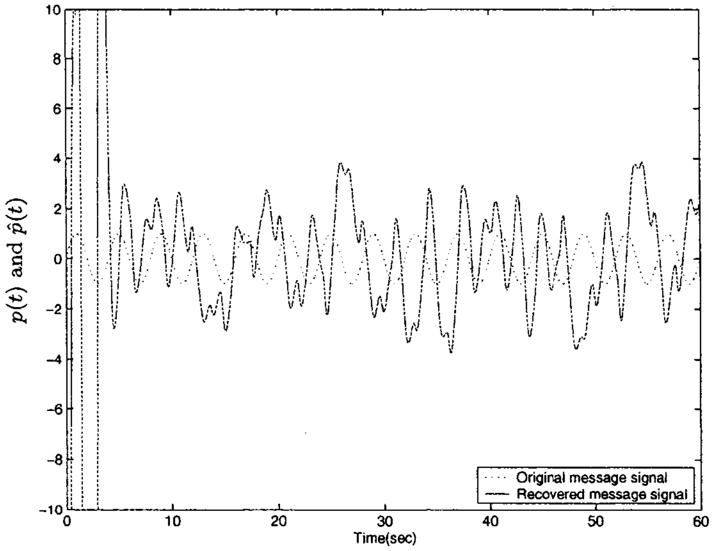


Figure 5.20: The original message signal and the wrongly recovered signal with the unmatched key parameter

Simulation II

In the second set of simulations, still, the sound signal:"This is the automatic control laboratory at the Lakehead University.", was chosen as the message signal to be transmitted through the secure communication system with an unknown time-delay. Similarly, we first use the same "Key" for the transmitter and the receiver. Figure 5.21 shows the simulation results; (a) represents the wave form of the original sound signal; (b) represents the wave form of the recovered sound signal and (c) represents the transmitted signal. Clearly, with the same "Key" used in the system, the original sound signal can be successfully retrieved at the receiver end, although there is an unknown time-delay in the proposed secure communication system. However, as Figure 5.22 shows, with the wrong "Key" used at the receiver side, it was not possible to achieve the synchronization, and therefore the original sound signal could not be recovered.

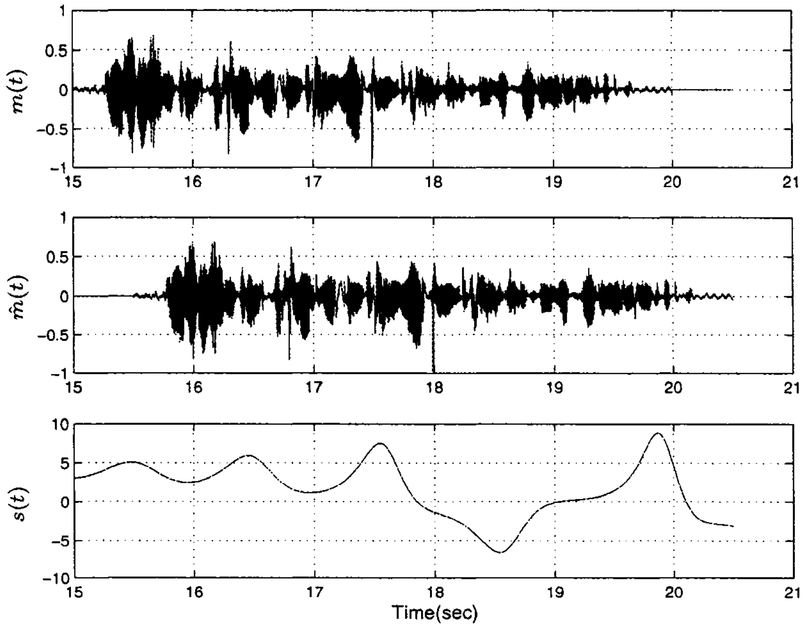


Figure 5.21: Simulation results for transmitting the sound signal with the same "Key" in transmitter and receiver systems

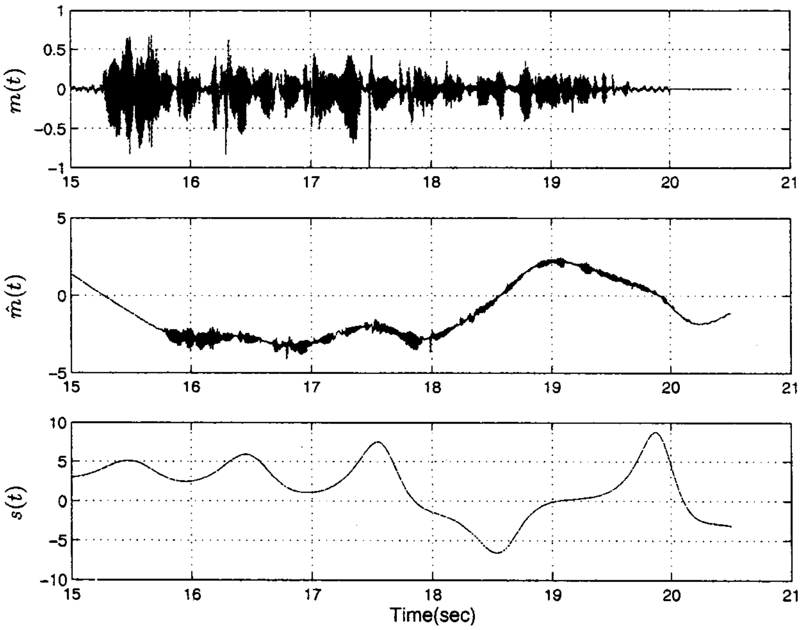


Figure 5.22: Simulation results for transmitting the sound signal with the unmatched "Key" in transmitter and receiver systems

Chapter 6

Conclusion

The interest in chaos synchronization has been boosted mainly by its potential application in the design of new chaotic cryptosystems for secure communications. In fact, the history of chaotic secure communications is short and its future is uncertain due to its problematic security. Plenty of attempts were made only to find that it was not difficult for an intruder to be able to extract the message signal from the chaotic transmission signal. The concept of secure synchronization, having the properties of antiadaptive and antirobust secure, has been discussed in this thesis, since, from the viewpoint of systems theory, adaptive and robust control methods can provide very powerful tools for the intruder to break the security of the communication system. Then, based on this consideration, a secure synchronization scheme has been discussed, using the generalized Lorenz system family as the platform. Due to the fact that this scheme has detectable but unobservable states, it excludes the possibility of using some straightforward adaptive and/or robust attacks.

The application of this synchronization scheme to secure communication has been also discussed in this thesis. A new secure communication system, combining the secure synchronization scheme with a conventional cryptographic technique, has been proposed to provide a desired security level. It has been proven that, since the proposed system has the antiadaptive secure and antirobust secure properties, the system's parameters, which are considered as the secret "Key" for this secure communication system, play a crucial role in the encryption and decryption of the private message signals being transmitted through the secure communication system. If an intruder tries to build a fake receiver to synchronize with the transmitter with a guessed "Key", a large enough error in guessing the "Key" leads to a large error in reconstructing the signals of the same magnitude, and this error cannot be suppressed even by choosing very high control gains. Therefore, it is very difficult for an intruder to guess the "Key", leading to the recovery of the transmitted message. Hence, a higher security level can be guaranteed.

Although the mathematical analysis and numerical simulation have shown that the proposed secure communication system can exclude a great deal of possible cryptosystem breaking schemes, thereby providing us with a very promising way for transmitting private messages safely, the system's security still needs to be further analyzed from the cryptographical viewpoint. Hence, the future work concerning a comprehensive and careful evaluation for the cryptographical properties of the proposed secure communication system may be carried out. Moreover, a further analysis of more sophisticated attacks, such as the known plaintext attack and ciphertext-only attack on the designed communication, is another aspect of the future work. Since attacks considered in this thesis mostly refer to the system control techniques, the capability of the designed communication system to withstand other more sophisticated attacks should be carried out to check the real security. This should provide us with a cryptographic view for the security of this designed cryptosystem.

Bibliography

Agiza H.N. and M.T. Yassen, 2001. Synchronization of Rossler and Chen Chaotic Dynamical Systems Using Active Control. *Physical Lett A*, Vol. 278, pp. 191-197.

Álvarez G., F. Monotoya, G. Pastor, and M. Romera, 1999. Chaotic Cryptosystems. *In IEEE 33rd Annual International Carnahan Conference on Security Technology*, pp. 332-338.

Alvarez-Ramirez J., H. Puebla, and I. Cervantes, 2002. Stability of Observer-Based Chaotic Communications for a Class of Lur'e System. *International Journal of Bifurcation and Chaos*, Vol. 7, pp. 1605-1618.

Bai E. and K.E. Lonngrn, 1999. Synchronization and control of chaotic systems. *Chaos, Solitons and Fractals*, Vol. 9, pp. 1571-1575.

Bai E. and K.E. Lonngrn, 2000. Sequential Synchronization of Two Lorenz Systems Using Active Control. *Chaos, Solitons and Fractals*, Vol. 11, pp. 1041-1044.

Benettin G., L. Galgani, and J.M. Strelcyn, 1976. Kolmogorov Entropy and Numerical Experiment. *Physical Review A* Vol. 14, pp. 2338-2345.

Boutayeb M., M. Darouach and H. Rafaralahy, 2002. Generalized State-Space Observers for Chaotic Synchronization and Secure Communication. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 49, pp. 345-349.

Brown R. and L.O. Chua, 1996. Clarifying Chaos: Examples and Counterexamples. *International Journal of Bifurcation and Chaos*, Vol. 6, pp. 219-249.

Čelikovský S and G. Chen, 2002. On a Generalized Lorenz Canonical Form of Chaotic Systems. *International Journal of Bifurcation and Chaos*, Vol. 12, pp. 1789-1812.

Čelikovský S. and G. Chen, 2005. Secure Synchronization of a Class of Chaotic Systems From a Nonlinear Observer Approach. *IEEE Transactions on Automatic Control*, Vol. 50, pp. 76-82.

Chen G. and T. Ueta, 1999. Yet Another Chaotic Attractor. *International Journal of Bifurcation and Chaos*, Vol. 9, pp. 1465-1466.

Chen G. and X. Dong, 1998. From Chaos to Order: Perspectives, Methodologies and Applications. Singapore: World Scientific.

Chen H. and J. Liu, 2000. Open-Loop Chaotic Synchronization of Injection-Locked Semiconductor Lasers with Gigahertz Range Modulation. *IEEE Journal of Quantum Electronics*, Vol. 36, pp. 27-34.

Chen Y. and A.Y.T. Leung, 1998. Bifurcation and Chaos in Engineering. Springer.

Chirkikov B.V. and F. Vivaldi, 1999. An Algorithmic View of Pseudochaos. *Physica D: Nonlinear Phenomena*, Vol. 129, pp. 223-235.

Chua L.0., L.j. Kocarev, K. Eckert and M. Itoh, 1992. Experimental Chaos Synchronization in Chua's Circuit. *International Journal of Bifurcation and Chaos*, Vol. 2, pp. 705-708.

Ciccarella G. , M.D. Mora, and A. Germani, 1993. A Luenberger-like Observer for Nonlinear Systems. *International Journal of Control*, Vol. 57, pp. 537-556.

Cuomo K.M. and A.V. Oppenheim, 1993. Chaotic Signals and Systems for Communications. *IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 3, pp. 137-140.

Cuomo K.M. and A.V. Oppenheim, 1993. Circuit Implementation of Synchronized Chaos with Applications to Communications. *Physical Review Letters*, Vol. 71, pp. 65-68.

Cuomo K.M. and A.V. Oppenheim, 1993. Synchronization of Lorenz-Based Chaotic

Circuit with Applications to Communications. *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, Vol. 40, pp. 626-633.

Dachselt F. and W. Schwarz, 2001. Chaos and Cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48, pp. 1498-1509.

Duan C.K., Yang S.S., 1997. Synchronizing Hyperchaos with a Scalar Signal by Parameter Controlling. *Physical Lett A*, Vol. 229, pp. 151-155.

Eckmann J.P. and D. Ruelle, 1985. Ergodic Theory of Chaos and Strange Attractors. *Reviews of Modern Physics*, Vol. 57, pp. 617-656.

Fradkov A.L., H. Nijmeijer, and A.Y. Pogromsky, 1999. Adaptive observer based synhronization *Controlling Chaos and Bifurcations in Engineering Systems*, G. Chen, Ed. Boca Raton, FL: CRC., pp. 417C435.

Frey D.R., 1993. Chaotic Digital Encoding: an Approach to Secure Communication. *IEEE Transactions on Circuits and Systems II*, Vol. 40, pp. 660-666.

Fridrich J., 1998. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, Vol. 8, pp. 1259-1284.

Gickenheimer J. and P. Holmes, 1983. Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields. Springer, Berlin.

Gonzales O., G. Han, J. Gyvez and E. Sanchez-Sinencio, 2000. Lorenz-based Chaotic Cryptosystem: A Monolithic Implementation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 47, pp. 1243-1247.

Götz M., K. Kelber and W. Schwarz, 1997. Discrete-Time Chaotic Encryption Systems — Part I: Statistical Design Approach. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44, pp. 963-970.

Grassi G. and S. Mascolo, 1997. Non-Linear Observer Design to Synchronize Hyperchaotic Systems via a Scalar Signal. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44(10), pp. 1011-1014.

Grassi G. and S. Mascolo, 1999. A System Theory Approach for Designing Cryptosystems Based on Hyperchaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 46(9), pp. 1135-1138.

Grassi G. and S. Mascolo, 1999. Synchronizing Hyperchaotic Systems by Observer Design. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 46(4), pp. 487-483.

Grebogi C., Y.C. Lai, and S. Hayes, 1997. Control and Applications of Chaos. *International Journal of Bifurcation and Chaos*, Vol. 7, pp. 2175-2197.

Habutsu H., Y. Nishio, I. Sasase and S. Mori, 1991. A Secret Key Cryptosystem by Iterating a Chaotic Map. *Advances in Cryptology - Proceedings of EuroCrypt'91*, Vol. 547, pp. 127-140.

Halle K.S., C.W. Wu, M. Itoh and L.O. Chua, 1993. Spread Spectrum Communication Through Modulation of Chaos. *International Journal of Bifurcation and Chaos*, Vol. 3, pp. 469-477.

Hilborn R.C., 1994. Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers. Oxford University Press.

Ioannou P. and J. Sun, 1996. Robust Adaptive Control. Englewood Cliffs, NJ: Prentice-Hall.

Jiang G.P., W.X. Zheng and G. Chen, 2004. Global Chaos Synchronization with Channel Time-Delay. *Chaos, Solitons and Fractals*, Vol. 20, pp. 267-275.

Kamen E.W., 1982. Linear Systems with Commensurate Time Delays: Stability and Stabilization Independent of Delay. *IEEE Transction on Automatic Control.*, Vol. 27, pp. 367-375.

Kapitaniak T., 2000. Chaos for Engineers: Theory, Applications, and Control. New York: Springer-Verlag.

Kelber K., T. Falk, M. Götz, W. Schwarz, and T. Kilias, 1996. Discrete-Time Chaotic Coders for Information Encryption—Part 2: Continuous- and Discrete-Value Realization. *In Proceedings Workshop Nonlinear Dynamics of Electronic Systems*, pp. 27-32.

Khalil H.K., 2002. Nonlinear Systems, 3rd ed. London, U.K.: Prentice-Hall.

Kocarev L., K.S. Halle, L.O. Chua, and U. Parlitz, 1992. Experimental Demonstration of Secure Communication via Chaotic Synchronization. *International Journal of Bifurcation and Chaos*, Vol. 2, No.3, pp. 709–713.

Kocarev L. and U. Parlitz, 1995. General Approach for Chaotic Synchronization with Applications to Communication. *Physical Review Letters*, Vol. 74, pp. 5028-5050.

Kocarev L., G. Jakimoski, T. Stojanovski, and U. Parlitz, 1998. From Chaotic Maps to Encryption Schemes. *In Proceedings IEEE International Symposium Circuits and Systems*, Vol. 4, pp. 514-517.

Kolumbán G, M.P. Kennedy, L.O. Chua, 1997. The Role of Synchronization in Digital Communication Using Chaos. Part 1: Fundamentals of Digital Communications. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44, pp. 927-936.

Kotulski Z. and J. Szczepanski, 1997. Discrete chaotic cryptography. *Annalen der Physik*, Vol. 6, pp. 381-394.

Lai Y.C. and C. Grebogi, 1993. Synchronization of Chaotic Trajectories Using Control. *Physical Review E*, Vol. 47, pp. 2357-2360.

Lakshmanan M. and S. Rajasekar, 2003. Nonlinear Dynamics: Integrability, Chaos and Patterns. Springer-Verlag, New York.

Lasota A. and M.C. Mackey, 1997. Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics. Second Edition, Springer-Verlag, New York.

Li S., X. Mou and Y. Cai, 2001. Pseudo-random Bit Generator Based on Couple Chaotic Systems and its Application in Stream-Ciphers Cryptography. *Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science*, Vol. 2247, pp. 316-329.

Li T.Y. and J.A. Yorke, 1975. Period Three Implies Chaos. *American Mathematical Monthly*, Vol. 82, pp. 985-992.

Li Z. and S. Shi, 2003. Robust Adaptive Synchronization of Rossler and Chen Chaotic Systems via Slide Technique. *Physics Letters A*, Vol. 311, pp. 389-395.

Lian K.Y. and P. Liu, 2000. Synchronization with Message Embedded for Generalized Lorenz Chaotic Circuits and Its Error Analysis. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 47, pp. 1418-1424.

Lian K.Y., P. Liu, T.S. Chiang, 2002. Adaptive Synchronization Design for Chaotic Systems via a Scalar Driving Signal. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 49, pp. 17-27.

Liao T.L. and N.S. Huang, 1999. An Observer-Based Approach for Chaotic Synchronization with Application to Secure Communications. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 46, pp. 1144-1150.

Liao T.L. and S.H. Lin, 1999. Adaptive control and synchronization of Lorenz systems. *Journal of The Franklin Institution*, Vol. 336, pp. 925-937.

Liao T. and S. Tsai, 2000. Adaptive Synchronization of Chaotic System and its Application to Secure Communications. *Chaos, Solitons and Fractals*, Vol. 11, pp. 1387-1396.

Lorenz E., 1963. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, Vol. 20, pp. 130-141.

Lorenz E., 1963. The Predictability of Hydrodynamic Flow. *Transactions of the New York Academy of Sciences. Series II*, Vol. 25, pp. 409-432.

Lorenz E., 1993. The Essence of Chaos. University of Washington Press.

Lü J. and G. Chen, 2002. A New Chaotic Attractor Coined. *International Journal of Bifurcation and Chaos*, Vol. 12, pp. 659-661.

Masuda N. and K. Aihara, 2002. Cryptosystems with Discretized Chaotic Maps. *IEEE*

Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 49, pp. 28-40.

Matthews R.A.J., 1989. On the Derivation of a “chaotic” Encryption Algorithm. *Cryptologia XIII*, Vol. 1, pp. 29-42.

Morgül O. and E. Solak, 1996. Observer Based Synchronization of Chaotic Systems. *Physical Review E*, Vol. 54, pp. 4803-4811.

Morgül O., 1999. Necessary Condition for Observer-Based Chaos Synchronization. *Physical Review Letters*, Vol. 82, pp. 77-80.

Murali K., 2000. Heterogeneous Chaotic Systems Based Cryptography. *Physics Letters A*, Vol. 272, pp. 184-192.

Murali K., H. Yu, V. Varadan, H. Leung, 2001. Secure Communication Using a Chaos Based Signal Encryption Scheme. *IEEE Transactions on Consumer Electronics*, Vol. 47, pp. 709-714.

Nijmeijer H., 2001. A Dynamical Control View on Synchronization. *Physica D: Nonlinear Phenomena*, Vol. 154, pp. 219-228.

Nijmeijer H. and I.M.Y. Mareels, 1997. An Observer Looks at Synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44, pp. 882-890.

Ogata K., 2002. Modern Control Engineering. 4th Edition, Prentice Hall, Upper Saddle River, N.J, USA.

Ogorzalek M.J., 1993. Taming Chaos-Part I: Synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 40, pp. 693-699.

Oppenheim A.V., G.W. Wornell, S.H. Isabelle and K.M. Cuomo, 1992. Signal Processing in the Context of Chaotic Signals. *In Proceedings IEEE ICASSP*, Vol. 4, pp. 117-120.

Parlitz U., L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, 1992. Transmission of

Digital Signals by Chaotic Synchronization. *International Journal of Bifurcation and Chaos*, Vol. 2, No. 4, pp. 973-977.

Pecora L.M. and T.L. Carroll, 1990. Synchronization in Chaotic Systems. *Physical Review Letters*, Vol. 64, pp. 821-824.

Pecora L.M. and T.L. Carroll, 1991. Driving Systems with Chaotic Signals. *Physical Review A*, Vol. 44, pp. 2374-2383.

Peng J. H., E. J. Ding, M. Ding and W. Yang, 1996. Synchronizing Hyperchaos with Scalar Transmitted Signal. *Physical Review Letters*, Vol. 76(6), pp. 904-907.

Poincaré J.H., 1892-1899. New Methods of Celestial Mechanics.

Preneel B., V. Rijmen, and A. Bosselears, 1998. Recent Developments in the Design of Conventional Cryptographic Algorithms. *Lecture Notes in Computer Science*, Vol. 1582, pp. 105-130.

Raghavan S. and J.K. Hedrick, 1994. Observer Design for a Class of Nonlinear Systems. *International Journal of Control*, Vol. 59, No. 2, pp. 515-528.

Rasband S.N., 1990. Chaotic Dynamics of Nonlinear Systems. Wiley, New York.

Reichl L.E., 1992. The Transition to Chaos. Springer Verlag, New York.

Rulkov N.F., M.M. Sushchik and L.S. Tsimring, 1995. Generalized Synchronization of Chaos in Directionally Coupled Chaotic Systems. *Physical Review E*, Vol. 51, pp. 980-994.

Schneier B., 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley and Sons, Inc., New York, second edition.

Shannon C.E., 1949. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, Vol. 28, pp. 656-715.

Short K., 1996. Unmasking a Modulated Chaotic Communication Scheme. *International Journal of Bifurcation and Chaos*, Vol. 6, pp. 367-375.

Stewart I., 1990. Does God Play Dice? - The Mathematics of Chaos. Blackwell Publishers, Oxford, UK.

Suykens J.A.K., P.F. Curran and L.O. Chua, 1999. Robust Synthesis for Master-Slave Synchronization of Lur'e Systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 46, pp. 841-850.

Thau F.E., 1973. Observing the State of Non-linear Dynamic Systems. *International Journal of Control*, Vol. 17, No. 3, pp. 471-479.

Ueta T and G. Chen, 2000. Bifurcation Analysis of Chen's Attractor. *International Journal of Bifurcation and Chaos*, Vol. 10, pp. 1917-1931.

Wiggins S., 1988. Global Bifurcation and Chaos: Analytical Methods. New York: Springer-Verlag.

Wolf A., J.B. Swift, H.L. Swinney and J.A. Vastano, 1985. Determining Lyapunov Exponents from a Time Series. *Physica D: Nonlinear Phenomena*, Vol. 16, pp. 285-317.

Wu C.W. and L.O. Chua., 1993. A simple way to synchronize chaotic systems with applications to secure communication systems. *International Journal of Bifurcation and Chaos*, Vol. 3, pp. 1619-1627.

Wu C.W. and L.0. Chua, 1994. A Unified Framework for Synchronization and Control of Dynamical Systems. *International Journal of Bifurcation and Chaos*, Vol. 4, pp. 979-998.

Yang T., C.W. Wu, and L.O. Chua, 1997. Cryptography Based on Chaotic Systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44, pp. 469-472.

Yassen M.T., 2003. Adaptive Control and Synchronization of a Modified Chua's Circuit System. *Applied Mathematics and Computation*, Vol. 135, pp. 113-128.