Chaos synchronisation, control and its application in digital communications

Chee, Chin Yi

2005

Chee, C. Y. (2005). Chaos synchronisation, control and its application in digital communications. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/6439>

<https://doi.org/10.32657/10356/6439>

Nanyang Technological University

Downloaded on 26 Apr 2023 13:24:01 SGT

**CHAOS SYNCHRONISATION, CONTROL AND ITS APPLICATION
IN DIGITAL COMMUNICATIONS**

CHEE CHIN YI

SCHOOL OF MECHANICAL AND AEROSPACE ENGINEERING

**A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Doctor of Philosophy**

2005

Acknowledgements

Above all, it is my greatest pleasure to give thanks and praises to God, my strong foundation, for He bestows wisdom upon me and in Him I find rest for my soul.

Thanks be to God.

It is my pleasure to acknowledge Prof Xu Daolin for his many brilliant ideas imparted to me and his patience in looking through my work. His support and knowledge are instrumental to the accomplishment of this thesis.

I would like to express my utmost gratefulness to my parents for providing and taking care of me all these years. Their contributions to my work here begin long before it started.

Last but not least, I would like to thank Dr Wen Guilin and Ms Lu Fangfang for their fruitful discussions with me and all research students and technicians for the help and joy they brought to me during my stay in the Mechanics of Machines Laboratory.

Chin Yi Chee
20 Dec 2004

CHAOS SYNCHRONISATION, CONTROL AND ITS APPLICATION IN DIGITAL COMMUNICATIONS

BY CHEE CHIN YI
*School of Mechanical and Production Engineering
Nanyang Technological University
Singapore*

CONTENTS

Abstract	I
List of Figures	II
Objectives and organisation of the thesis	IV
 Part I Background	
 Chapter 1 Introduction	1
1.1 Introduction to deterministic chaos	1
1.1.1 Chaotic motion	4
1.1.2 The butterfly effect	5
1.1.3 Poincaré section and chaotic attractor	7
1.2 Measuring chaos, Lyapunov exponent	12
1.3 Coupled systems and chaos synchronisation	14
1.3.1 Coupled systems	16
1.3.2 Chaos synchronisation – identical, phase and generalised synchronisation	17
 Chapter 2 Chaos-based communication techniques	22
2.1 Continuous-time chaotic encryption	25
2.1.1 Chaotic shift keying	26
2.1.2 Chaotic masking	29
2.1.3 Chaotic modulation	31
2.2 Discrete-time chaotic encryption	32
2.3 Chaos-based cryptanalysis	35

2.4	Chaos-based digital communication for spread spectrum applications	40
2.5	Shortcomings of the existing chaos-based communication techniques	46
 Part II Theoretical basis – stability criteria & control of projective synchronisation and pseudo-random switching key		
Chapter 3	Projective synchronisation in coupled systems and its stability criteria	51
3.1	Phenomenon of projective synchronisation	52
3.2	Stability criterion of projective synchronisation in three-dimensional continuous-time systems	57
3.3	Stability criteria of projective synchronisation in continuous-time systems of any dimension	59
3.4	Stability criterion of projective synchronisation in discrete-time systems	65
Chapter 4	Control of projective synchronisation	71
4.1	Manipulating the ultimate state of projective synchronisation in continuous-time systems	72
4.2	Manipulating the ultimate state of projective synchronisation in discrete-time systems	79
4.3	Manipulating the ultimate state of projective synchronisation in nonpartially linear chaotic systems	91
4.4	Control for full-state projective synchronisation in continuous-time systems	95
Chapter 5	Pseudo-random switching keys	100
5.1	Introduction	100
5.2	Design of pseudo-random switching keys	102
5.3	Time series analysis for secure communication	105
5.4	Higher order pseudo-random switching keys	114
5.5	Synchronisation of pseudo-random switching keys	117

Part III Applications

Chapter 6	Transmission of M-ary digital signals using controlled projective synchronisation	121
6.1	Introduction	121
6.2	Mechanism of digital communication system based on controlled projective synchronisation	123
6.3	Numerical experiments	127
Chapter 7	Secure digital communication using controlled projective synchronisation	134
7.1	Introduction	134
7.2	A scheme for secure communication	137
7.3	Security analysis	144
Chapter 8	Chaotic encryption using discrete-time synchronous chaos with pseudo-random switching keys	151
8.1	Introduction	151
8.2	Basic concept of the cryptosystem	153
8.3	Mechanism of the cryptosystem	156
8.4	Security analysis	162
Chapter 9	Conclusions	169
8.1	Introduction	169
8.2	Basic concept	171
References		173
Appendix A	Construction of controlled projective synchronisation based communication systems in Simulink®	186
A.1	Individual building blocks	186
A.1.1	Simulink blocks	186
A.1.2	Communication Blocksets	189
A.1.3	DSP Blocksets	190
A.2	Communication system and subsystems	192
A.2.1	Communication system	192

A.2.2	Transmitter end subsystem	193
A.2.3	Signal generator	194
A.2.4	Control vector and control function subsystems	195
A.2.5	Transmitter end system inputs subsystem	196
A.2.6	Modulator subsystem	197
A.2.7	Receiver end subsystem	198
A.2.8	Demodulator subsystem	199

Abstract

This thesis studies the phenomenon and applications of cooperative behaviour exhibited by coupled chaotic systems. This form of cooperative behaviour is known as chaos synchronisation. The systematic study of chaos synchronisation here contributes to the formulation of chaos theory where the theoretical basis spans between applied mathematics and physical sciences.

The new findings in coupled chaotic systems reported in this thesis provide important solutions to some of the existing fundamental problems in chaos theory. This led us to novel discoveries that could be useful in many fields of science and technology, with special focus on cryptography and digital communication.

The two main findings introduced in this thesis include controlled projective synchronisation and pseudo-random switching key. In controlled projective synchronisation, a newly derived control function allows us to manipulate the scaling feature of the coupled system. In terms of applications, this discovery shifted chaos-based digital communication to a truly M-ary transmission where each digital symbol can now consists of more than one bit which allows faster transmission rate and lower bit error ratio. In another finding, it is observed that identical synchronisation of chaos is still achievable in coupled chaotic system even with the sub-systems having different initial parameters that switch values within a chosen set in a discontinuous, rapid and random-like manner, refers to as pseudo-random switching keys. This observation opposes to the earlier belief that identical synchronisation can only be realised with identical and fixed system parameters. Incorporating pseudo-random switching keys into cryptography leads to the development of two highly secure cryptosystems.

List of Figures

Fig. 1.1	Time series solutions of the three variables used to describe the Rossler system.	5
Fig. 1.2	Discrete-time evolution of two waveforms generated using Logistic equation with an initial difference of 0.1%.	7
Fig. 1.3	Time series solutions of the Duffing system.	9
Fig. 1.4	Ueda's chaotic attractor.	10
Fig. 1.5	Time series solutions and attractor of the Lorenz system.	12
Fig. 1.6	The sketch shows the change in distance between two nearby orbits used to define the largest Lyapunov exponent.	14
Fig. 1.7	Time evolutions of the drive and response systems of the coupled Lorenz system.	19
Fig. 2.1	Circuitry of Lorenz system.	24
Fig. 2.2	Schematic of a basic chaotic shift keying communication system setup.	27
Fig. 2.3	Demonstration on secure digital communication using chaotic shift keying based on coupled Lorenz system.	29
Fig. 2.4	Schematic of a basic chaotic masking communication system setup.	30
Fig. 2.5	Schematic of a basic chaotic modulation communication system setup.	31
Fig. 2.6	A graphical representation of the Baptista-type cryptosystem.	33
Fig. 2.7	An illustration on the generation of pseudo-random bits sequence.	34
Fig. 2.8	Demonstration on using the construction of attractor from return map to uncover digital information encrypted by chaotic shift keying.	40
Fig. 2.9	Demonstration on M-ary frequency shift keying technique (MFSK) where digital information is modulated onto waveforms of four different frequencies.	43
Fig. 3.1	Time evolutions of the drive and response systems of the coupled Chen system.	55
Fig. 3.2	Synchronised chaotic attractors of the coupled system (3.41).	70
Fig. 3.3	Variation of coupled system (3.41).	70
Fig. 4.1	Demonstration on controlled projective synchronisation in continuous-time systems.	78
Fig. 4.2	Demonstration on controlled projective synchronisation in discrete-time systems.	87
Fig. 4.3	Effectiveness of controlled projective synchronisation in discrete-time systems.	90
Fig. 4.4	Demonstration on controlled projective synchronisation in nonpartially linear systems.	95
Fig. 4.5	Demonstration on full-state controlled projective synchronisation.	99

Fig. 5.1	Illustration of Rossler system (5.2) with PRSK	104
Fig. 5.2	Return maps constructed from time series generated by Lorenz system with and without PRSK.	106
Fig. 5.3	Measurements of local prediction error.	108
Fig. 5.4	Measurements of global prediction error.	111
Fig. 5.5	Demonstration on the effectiveness of PRSK in masking statistical properties along an intercepted information carrier signal.	114
Fig. 5.6	A chaotic attractor used as reference to trigger changes in the values of PRSK.	116
Fig. 5.7	Time evolution of x_1 from the Lorenz system with PRSK	117
Fig. 5.8	Demonstration on the robustness of synchronisation with initial mismatch of PRSK.	120
Fig. 6.1	Schematic of a controlled projective synchronisation digital communication scheme based on coupled Lorenz system.	126
Fig. 6.2	Decoding process at the receiver end with symbol duration of 5 time-units.	129
Fig. 6.3	Sample transmitted signal, $z_x(t)$, of 5 time-units.	129
Fig. 6.4	The BER performance results for binary symbols transmission.	131
Fig. 6.5	The BER performance results for M-ary symbols transmission.	132
Fig. 6.6	Digital images transmitted using controlled projective synchronisation over AWGN channel.	133
Fig. 7.1	Schematic of controlled projective synchronisation secure digital communication scheme based on system (7.3).	141
Fig. 7.2	Demonstration of a chaotic encryption scheme based on projective synchronisation with a pseudo-random switching key incorporated.	144
Fig. 7.3	Security analysis on chaotic shift keying scheme under attack from characteristic cryptanalysis that measures the synchronisation error.	147
Fig. 7.4	Security analysis on projective synchronisation based scheme under attack from characteristic cryptanalysis that measures the synchronisation error.	150
Fig. 8.1	Encryption process of the encrypter with Hénon map as the underlying chaotic system.	157
Fig. 8.2	Demonstration on the dynamical behaviour of PRSK.	160
Fig. 8.3	Set-up of the cryptosystem using three PCs used to test encryption and decryption processes.	162
Fig. 8.4	The original plaintext that is to be encrypted and the plaintext retrieved with 47% bit error ratio.	164
Fig. 8.5	The variation of the ciphertext, $u_{(k)} = x_{1,(k)}$ of a portion of the plaintext.	165
Fig. 8.6	Return maps constructed using a variable from Hénon map.	167

Objectives and organisation of the thesis

This thesis has two objectives. The first objective aims to contribute to the theoretical formulation of chaos theory in the area of coupled systems and chaos synchronisation. This would be achieved by deriving new theoretical findings analytically from mathematical proofs, which will be provided in this thesis. On top of the criteria for sound mathematical foundation, the thesis will undertake in new research directions that will lead to useful engineering and scientific applications. The second objective aims to solve some of the existing problems and develop new applications in chaos communication by utilising the new theoretical findings obtained under the first objective. These existing problems include low transmission rate and high bit error ratio in chaos-based digital communication and various security flaws in chaotic secure communication.

The thesis has nine chapters organised into three parts, namely the background, the derivations of the theoretical findings and the presentation of the newly developed applications.

In Part I, chapter 1 and 2 provide the background information necessary for subsequent discussions in this research topic. Chapter 1 gives the definition of chaos and describes the fundamental properties of chaotic dynamics and the dynamical behaviour of coupled systems and chaos synchronisation. Chapter 2 uses the background information to introduce the fundamental principles and mechanism of existing chaotic encryption and digital communication techniques.

The shortcomings and flaws of these existing techniques are highlighted in this chapter.

Part II fulfils the first objective of the thesis with chapters 3, 4 and 5 presenting new theoretical findings resulted from the works of this thesis. Chapters 3 and 4 provide insights into a recently observed cooperative behaviour of coupled chaotic system known as projective synchronisation, which opened up the possibility of solving some of the existing problems in chaos communications. Chapter 3 introduces this phenomenon and presents the derivations of the stability criteria for its occurrence under different conditions. Chapter 4 presents control algorithms that can be used to direct the ultimate state of projective synchronisation to any desired state. Chapter 5 introduces another new chaos synchronisation phenomenon refers to as the pseudo-random switching keys. It is observed that identical synchronisation can be achieved between two chaotic systems with the system parameters switching rapidly and randomly in a discontinuous manner within a chosen set of values. This opposes to the earlier belief that system parameters must be fixed to achieve chaos synchronisation. This observation leads to the development of two highly secure chaos-based cryptosystems that will be introduced in part III of the thesis.

Part III fulfils the second objective of the thesis where three applications in chaos communication are developed using the results obtained in part II. These applications that serve different purposes in chaos communication are introduced in four chapters from chapter 6 to 8.

The conclusion is given in chapter 9.

Chapter 1

Introduction

Twentieth-century science will be remembered for three things: relativity, quantum mechanics and chaos. Like the first two revolutions, chaos cuts away at the tenets of Newton's physics. Relativity eliminated the Newtonian illusion of absolute space and time; quantum theory eliminated the Newtonian dream of a controllable measurement process; and chaos eliminates the Laplacian fantasy of deterministic predictability. In this chapter the basic concept of chaos and the three key components that are essential for subsequent discussion in this research topic will be introduced. The key components that will be introduced in section 1.1 to 1.3 include the fundamental properties of chaos, the Lyapunov exponent used to measure chaos and coupled systems with the associated synchronous behaviour.

1.1 Introduction to Deterministic Chaos

Deterministic chaos, often simply referred to as chaos, is an interesting nonlinear phenomenon that exhibits contradicting characteristics, which is random in behaviour and yet deterministic in nature. This form of random behaviour referred to as chaotic dynamics, is governed by a deterministic law that differentiates itself from random noise. The formulation of Chaos Theory and the realisation of the distinction between chaotic dynamic and random noise thus enables us to explain in explicit mathematical terms the occurrence of various

prediction errors that arise due to over simplified description of nonlinear systems by linear models.

The growing understanding of nonlinear dynamics and chaos has since superseded the concept of describing our dynamical world based purely on linear modelling. This change that is taking place is gradual but certain. A growing number of articles in the literature have reported observation of chaotic behaviour in various systems and disciplines of science such as ecological systems [Blasius, 1999], solar system [Malhotra 2001], microscopic dynamical systems [Gaspard et al., 1998], electronic circuits [Chen & Ueta, 2002], cardiology [Poon & Merrill, 1997], neuroscience [Rabinovich & Abarbanel, 1998] and meteorology [Lorenz 1963; Shao, 2002]. Similarly in art [Boon et al., 1990; Boon & Decroly, 1995] and social sciences [Neuringer & Voss, 1993; Trippi, 1995; Smithson, 1997; Tomochi & Kono, 1998] the presence of chaotic behaviour has also been observed and reported.

Over the years the application of chaos has transformed itself from a cheap chat-up line for researchers to amuse friends and strangers to one that results in important and useful developments. For example in spread spectrum communication, chaos-based techniques with the inherent wideband characteristic offer the cheaper and more efficient alternative to the conventional techniques that require extra circuitry for spreading and de-spreading processes [Kennedy et al., 1998]. In cardiology, findings suggest that chaos is prevalent in healthy heart. Detecting a decrease in chaos may be indicative of congestive heart failure, which is a clinical condition associated with a high risk of sudden death [Poon & Merrill, 1997]. In astronautics, the idea of nonlinear dynamics and chaos provides a mean

to understand the global structure of all possible solutions to the relevant equations of the spacecraft trajectories. The geometry of these solutions can be used to guide a spacecraft to its destination with minimum fuel, which enables us to undertake missions that were previously deemed impossible [Howell, *et al.*, 1997]. Other chaos-based applications that relate closely to our daily uses include our household appliances such as washing machines, air-conditioners and microwave ovens. LG Electronics developed washing machines that incorporated chaotic motion in the washing process to produce cleaner and less tangled clothes. The same company also designed air-conditioner louvers with chaotic features to produce "natural breeze" for a more comfortable airflow. Panasonic developed microwave ovens with a "chaos defrost" setting. This setting uses a simple chaotic system to generate an irregular heating sequence, which can reduce the time required to defrost food by up to 50% [Kouda *et al.* 2001]. Furthermore in art and social sciences, chaotic mapping provides a new technique for musicians to generate musical variations of an original work [Dabby, 1996] and also a new prospective for political theorists to describe and control arms races [Behrens *et al.*, 1997; Tomochi & Kono, 1998].

Although the study of chaos has since shifted from a curious phenomenon to one with practical significant and applications [Stark & Hardy, 2003] with a number of notable articles in the literature [Moon, 1992; Gleick, 1998; Thompson & Stewart, 2002] written on this subject, there is still no existence of an accepted definition for chaos. However, chaotic dynamics can be described by three significant properties, namely randomlike behaviour, sensitive dependence on initial conditions and the deterministic nature of the system. These properties will be introduced in the following three sub-sections.

1.1.1 Chaotic Motion

The first property of chaos describes chaotic motion as a dynamic motion that resembles random noise. Given that any physical system that behaves non-periodically would be difficult to predict if not unpredictable, it is therefore this property of chaos that makes it desirable for applications in cryptography

Here the seemingly randomlike behaviour of chaos that results in unpredictability of the future dynamics is illustrated using the Rossler system. The Rossler system is credited to Otto Rossler and is the result from the work in chemical kinetics [Rossler, 1976]. The system is described by three nonlinear differential equations given as

$$\begin{aligned}\dot{x}_1 &= -x_2 - x_3, \\ \dot{x}_2 &= x_1 + \mu_1 x_2, \\ \dot{x}_3 &= \mu_2 - x_3(\mu_3 - x_1).\end{aligned}\tag{1.1}$$

The parameter set is chosen as $\boldsymbol{\mu} = [\mu_1, \mu_2, \mu_3] = [0.2, 0.2, 5.7]$, which leads to chaotic dynamics. The time series of the three variables x_1, x_2 and x_3 is shown in Fig.1.1.1. The time series shows that chaotic dynamics has an irregular appearance, which persists as long as time integration is carried out. Although the recurrent nature is evidence by the fact that certain patterns in the waveform repeat themselves at irregular intervals, there is never an exact repetition in a fix time interval and the motion is truly nonperiodic. The randomness in chaos is due to instability being found at every point of the dynamical system such that the time evolution never settles down to a fixed pattern where a solution resides.

Fig.1.1. Time series solutions of the three variables used to describe the Rossler system (1.1), with initial condition $[x_1, x_2, x_3] = [1, 1, 1]$.

1.1.2 The Butterfly Effect

The second property of chaos describes the extreme sensitivity of chaotic systems to the initial conditions. In fact, the word *chaos* is coined by [Li & Yorke, 1975] to refer to the mathematical problem in Chaos Theory that described a time evolution with sensitive dependence on initial conditions. This concept states that two identical dynamical systems that are started off together with an extremely small difference in initial conditions may have their time series diverged at some point, even though each maps out the same attractor in the phase space. This effect is known as the butterfly effect, which is first observed by Lorenz [Lorenz, 1963] in his work in meteorology. It describes the sensitive dependence on initial conditions where a small difference in the initial conditions can drastically change

the long-term behaviour of a system. Such a small amount of difference in a measurement may come from experimental noise, background noise, or an inaccuracy of the equipments. Ian Stewart in his book [Stewart, 2002] described this extremely small difference in initial condition to the flapping of the single butterfly's wing. He wrote: *"The flapping of a single butterfly's wing today produces a tiny change in the state of the atmosphere. Over a period of time, what the atmosphere actually does diverges from what it would have done. So, in a month's time, a tornado that would have devastated the Indonesian coast doesn't happen. Or maybe one that wasn't going to happen does."* This remark is derived from a report given by Edward Lorenz in 1972 entitled "Predictability: Does the Flap of a Butterfly's Wings in Brazil set off a Tornado in Texas?" see reference [Lorenz, 1993].

The butterfly effect is not limited only to atmospheric study. The sensitive dependency of chaos to initial conditions is found in all nonlinear systems. As an example, we introduce the Logistic equation, which is a simple one-dimensional map given as

$$L_{(k+1)} = rL_{(k)}(1 - L_{(k)}) . \quad (1.2)$$

Eq. (1.2) is proposed by Robert May [May 1976], an Australian mathematician engrossed in biology, to describe changes in population L from year k to the next year $k + 1$. The coefficient $0 < r \leq 4$ represents a combined rate for reproduction and starvation with chaotic behaviour observed for $3.56 < r \leq 4$. In this example as well as in the remaining part of the thesis, the subscript k in bracket is used to denote the number of iterations in map.

To illustrate the butterfly effect, the parameter r is chosen to be 3.8 and two initial conditions with only 0.1% difference is chosen as $L_{(0)}=0.04$ and $L_{(0)}=0.04004$ to produce two discrete-time evolutions shown in Fig.1.2. From Fig.1.2, it can be observed that all correlation between the two waveforms disappeared after the fifteenth iteration ($k > 15$) and thus demonstrated the sensitive dependency of chaos to initial conditions.

Fig.1.2. Discrete-time evolution of two waveforms generated using Logistic equation (1.2) with an initial difference of 0.1%.

1.1.3 Poincaré Section and the Chaotic Attractor

The third property of chaos describes the deterministic nature of chaotic dynamics. Chaotic systems are in fact deterministic. As such, the randomness observed in chaotic dynamics cannot be attributed to statistical fluctuations but is the result of an underlying rule that can be expressed in explicit mathematical

terms. Here we use the **Poincaré** section and the strange attractor to demonstrate the claim of an underlying determinism hidden under the disguise of irregularities.

Before carrying out the demonstration, let us first introduce the Duffing equation, which is one of the classical oscillators published by Duffing in 1918. This equation is expressed as,

$$\ddot{x} + \mu_1 \dot{x} + \mu_2 x^3 = F \cos t. \quad (1.3)$$

Eq. (1.3) can also be transformed and modelled as a set of differential equations given by,

$$\begin{aligned} \dot{x}_1 &= x_2, \\ \dot{x}_2 &= -\mu_1 x_2 - \mu_2 x_1^3 + F \cos t, \end{aligned} \quad (1.4)$$

where $x_1 = x$ and $x_2 = \dot{x}$.

In mechanical engineering, system (1.4), which is referred to as the Duffing system here, might, for example, be used to model the motion of a sinusoidally forced structure undergoing large elastic deflections. Here μ_1 and μ_2 are real constants and F is the forcing amplitude. We chose $\mu_1 = 0.05$, $\mu_2 = 1$ and $F = 7.5$ to produce chaotic response in system (1.4). The time series solution of x_1 and x_2 versus t obtained by integration of system (1.4) is presented in Fig.1.3 (a) and (b) respectively.

The observation of the randomlike dynamical behaviour shown in Fig.1.3 may cast doubt on whether a well-defined rule expressible in mathematical terms does exist. However, if the time evolutions indeed obey a governing rule, the underlying order can be uncovered in the midst of the randomness by a technique

known as the Poincaré mapping. In carrying out the technique, an arbitrary initial start off point, $t = T_s$, along the time axis

Fig.1.3. Time series solutions (a) x_1 versus t and (b) x_2 versus t of Duffing system (1.4).

is first chosen and the two points (x_1, x_2) corresponding to the chosen time instant is noted down. The process is carried on by continuously marking the time series solutions at times that are integer multiples of the forcing period 2π starting from T_s . In doing so, a sequence of corresponding pair of points at time instant $t = T_s + n2\pi$, $n = 0, 1, 2, \dots$ is accumulated. Subsequently by plotting these accumulated points on the (x_1, x_2) plane, known as the Poincaré section, a well-organised graphical pattern with distinct features is revealed as shown in Fig.1.4. Furthermore, it is observed that as the formation of the graphical pattern stabilises, all successive points taken at $t = T_s + n2\pi$ from the time series solutions wander

erratically within the structure of the formed pattern. A graphical pattern constructed from chaotic waveforms is known as the chaotic attractor, which is also referred to as the strange attractor.

Fig.1.4. Ueda's chaotic attractor named after the Japanese applied dynamicist who studied the steady-state chaotic behaviour of Duffing's equation (1.3). The chaotic attractor is formed using 3×10^5 integrated points.

The topological properties of the chaotic attractor formed with fixed system parameters are unique and independent of the initial conditions and the chosen T_s . In another words, as long as the system parameters remain the same an absolutely identical chaotic attractor is formed each time, even with a different set of initial conditions and any arbitrary chosen T_s . The revelation of a chaotic attractor within the irregular waveforms thus clearly demonstrates the presence of order within chaos and hence differentiates chaotic dynamics from random noise.

The Poincaré mapping is not the only technique to reveal the presence of a chaotic attractor. In fact, in the case of an autonomous chaotic system, any two variables can be used to plot a chaotic attractor. The Lorenz system (1.5) is used here for the illustration.

$$\begin{aligned}\dot{x}_1 &= \mu_1(x_2 - x_1), \\ \dot{x}_2 &= (\mu_2 - x_3)x_1 - x_2, \\ \dot{x}_3 &= x_1x_2 - \mu_3x_3.\end{aligned}\tag{1.5}$$

The Lorenz system (1.5) was proposed by Edward Lorenz as a simple model for thermally induced fluid convection [Lorenz 1963] and it is an excellent example of irregular behaviour that arises from the nonlinear relation within the system rather than from the driving forces. Here the parameter set is chosen as $\mu = [\mu_1, \mu_2, \mu_3] = [60, 10, 2]$. Fig.1.5 (a-c) show the time series solutions of the three variables of system (1.5). The time evolutions appear to be randomlike but when reproduced on a 3-D plot as shown in Fig.1.5 (d), it revealed a well-defined and distinct chaotic attractor that always remain bounded within an invisible boundary. Similar to the previous example, the statistical and topological properties of the chaotic attractor remain consistent and independent with respect to the initial conditions provided that the system parameters remain fixed.

The deterministic nature of chaos resulting from the underlying governing rule is an important property of chaos. A useful result of this property is the observation of chaos synchronisation, which leads to application in chaos-based communication, cryptography and cryptanalysis.

Fig.1.5. (a-c) Time series solutions of the Lorenz system (1.5). (d) The 3-D plot of the Lorenz attractor.

1.2 Measuring chaos, Lyapunov exponent

In the previous section, chaos is qualified using three properties. Although it has become clear that a chaotic system may be perfectly deterministic in principle but with its future time evolution being completely unpredictable in practice, it will be interesting to have a gauge to quantify chaos. In another word, given a chaotic system, it is natural to find out how chaotic or unpredictable is the generated dynamics.

To measure chaos, this section introduces the Lyapunov exponent, which is conceptually the most basic indicator of deterministic chaos that measures the exponential rate of divergence or convergence of nearby trajectories. Given any dynamical process, the Lyapunov exponent describes how the initial lengths, areas and volumes of the system change over time in phase space. For a chaotic system, two trajectories that have a small difference in initial conditions will diverge

exponentially from each other over a short period of time. Let Δx_0 be the initial distance between the starting points at time t_0 . As the trajectories of the continuous-time system evolve over a short period of time the distance between them will be

$$\Delta x(t) = \Delta x_0 C^{\lambda t}. \quad (1.6)$$

λ is used to denote Lyapunov exponent and C is the base of a logarithm, which can be taken as any real positive number greater than 1.

In a bounded system, the exponential divergence of chaotic orbits is confined locally since $\Delta x(t)$ cannot tend to infinity as $t \rightarrow \infty$. The numerical calculation of Lyapunov exponents begins with identifying a reference trajectory called fiduciary [Wolf *et al.*, 1985] and a point on a nearby trajectory. $\Delta x(t)/\Delta x_0$ is measured as time is run forward until $\Delta x(t)$ becomes too large such that the growth departs from exponential behaviour. Another nearby trajectory is then identified with respect to the fiduciary and Δx_0 is redefined, see Fig. 1.6. Thus, the Lyapunov exponent is the measure of this divergence of orbits by averaging the exponential growth at many such points along a trajectory shown in Fig. 1.6. The Lyapunov exponent is expressible as,

$$\lambda = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \frac{|\Delta x(x_0, t)|}{|\Delta x_0|}. \quad (1.7)$$

By inspecting equation (1.7), we can see that negative Lyapunov exponents, $\lambda < 0$ is the characteristic of dissipative or non-conservative systems. It implies the presence of a fixed point or a periodic attractor, which is asymptotically stable. If $\lambda = 0$ then the system is neutrally stable, such systems are conservative and in a

steady state mode. Orbit that is unstable and chaotic has positive λ . Nearby points will diverge irrespective how close they are initially. These points are classified as unstable.

Fig.1.6. The sketch shows the change in distance between two nearby orbits used to define the largest Lyapunov exponent. Figure largely adopted from [Moon, 1992].

1.3 Coupled systems and chaos synchronisation

The various forms of cooperative behaviours resulting from coupling two chaotic systems are collectively known as chaos synchronisation. Chaos synchronisation can be considered a property of chaotic dynamics. The history of synchronisation goes back to the 17th century when the famous Dutch scientist Christian Huygens reported his observation of synchronisation of two pendulum clocks. A concise description of early history of synchronisation is presented under the introduction in the paper by [Pikovsky *et al.*, 2000]. Chaos synchronisation is first considered by Fujisake and Yamada in the 1980's and later popularised in

early 1990 by [Pecora & Carroll, 1990]. Co-operative behaviour of chaotic dynamical system, in particular, the phenomenon of synchronisation has attracted much attention since then, due to its applicability in neural networks [Sompolinsky et al., 1991], biological systems [Strogatz et al., 1992], secure communication [Hayes et al., 1993; Carroll et al., 1996], and system identification [Parlitz et al., 1996]. More recently, chaotic synchronisation has found its applicability in human heartbeat regulation [Schafer et al., 1998] and ecological systems [San Roman et al., 1998; Blasius et al., 1999]. The systematic study in this area has classified different forms of synchronous behaviour found in coupled systems as identical, phase, generalised and projective synchronisation.

Chaos synchronisation is by far one of the most important and useful results of chaos. Although chaos synchronisation is observed in both the discrete-time systems as well as the continuous-time systems, which are modelled using difference equations and differential equations respectively, this thesis chooses to use continuous-time system for introducing this phenomenon. In order to describe the occurrence of chaos synchronisation, it is essential to introduce the coupled chaotic systems under the simple coupling mode, which will be discussed in section 1.3.1.

1.3.1 Coupled systems

A coupled system consists of two subsystems with one subsystem driving the other subsystem through coupling by using common variables. To illustrate this

description mathematically, consider an autonomous n -dimensional chaotic system expressed using differential equations given as

$$\dot{\mathbf{w}} = f(\mathbf{w}). \quad (1.8)$$

with $\mathbf{w} = [w_1, w_2, \dots, w_p]^T$. If system (1.8) is divided into two parts such that

$\mathbf{w} = [\mathbf{u}, \mathbf{v}]$ where $\mathbf{u} = [w_1, w_2, \dots, w_n]^T$, $\mathbf{v} = [w_{n+1}, w_{n+2}, \dots, w_p]^T$ then an equivalent expression for system (1.8) can be given as

$$\begin{aligned} \dot{\mathbf{u}} &= g(\mathbf{u}, \mathbf{v}), \\ \dot{\mathbf{v}} &= h(\mathbf{u}, \mathbf{v}). \end{aligned} \quad (1.9)$$

Next create a new system that is identical to system (1.9) and express it by

$$\begin{aligned} \dot{\mathbf{u}}' &= g(\mathbf{u}', \mathbf{v}'), \\ \dot{\mathbf{v}}' &= h(\mathbf{u}', \mathbf{v}'). \end{aligned} \quad (1.10)$$

To couple the two systems such that system (1.9) drives system (1.10), we chose $\mathbf{v}$ from system (1.9) as the coupling variables and substitute the vector into the first equation of system (1.10). The mathematical expression for the coupled system is therefore given as

$$\begin{aligned} \dot{\mathbf{u}} &= g(\mathbf{u}, \mathbf{v}), & \dot{\mathbf{u}}' &= g(\mathbf{u}', \mathbf{v}), \\ \dot{\mathbf{v}} &= h(\mathbf{u}, \mathbf{v}), & \dot{\mathbf{v}}' &= h(\mathbf{u}', \mathbf{v}'). \end{aligned} \quad (1.11)$$

From the coupled system (1.11), it can be observed that through the coupling, subsystem (1.10) now becomes dependent on the subsystem (1.9). Hence subsystem (1.9) is referred to as the drive or master system and subsystem (1.10) is referred to as the response or slave system. The vector $\mathbf{v}$, which consists of only a single variable in most cases is commonly referred to as the drive variable or the coupling variable.

The mathematical model of the simple coupled system shown in (1.11) is under *unidirectional* coupling where the master system drives the slave system. However if on top of the unidirectional coupling shown in (1.11), the vector $\mathbf{v}'$ from the first equation of the slave system in (1.11) also replaces $\mathbf{v}$ in the first equation of the master system then a simple coupled system is obtained under *bi-directional* coupling. In this thesis, the study of coupled chaotic systems will be in the context of unidirectional coupling. This is because unidirectional coupling is closely related to the applications in communication and cryptography, which are the focus applications in this thesis.

1.3.2 Chaos synchronisation – identical, phase and generalised synchronisation

We wish to stress that although the two identical systems may be coupled through common variables, the occurrence of chaotic synchronisation is not always guaranteed. The realisation of chaos synchronisation and the type of cooperative behaviour that will be exhibited between the two systems depends on the fulfilment of certain conditions and stability criteria. Chaos synchronisation is categorised into four different type of cooperative behaviour, namely identical synchronisation, phase synchronisation, generalised synchronisation and projective synchronisation. The first three types of synchronous behaviour will be briefly introduced in this section. Detail investigation and report on projective synchronisation is carried out under Part II, chapters 3 and 4.

Identical Synchronisation

Identical synchronisation is the first chaotic synchronous behaviour discovered, which was popularised by [Pecora & Carroll, 1990]. Their work on identical synchronisation brought about an era of active research in chaos synchronisation due to the possible applications in secure and spread spectrum communication techniques with simple and cheap software and hardware implementation [Kocarev *et al.*, 1992; Parlitz *et al.*, 1992; Cuomo & Oppenheim, 1993]. In identical synchronisation, the trajectories of the subsystems, i.e. $[\mathbf{u}, \mathbf{v}]$ and $[\mathbf{u}', \mathbf{v}']$, converge to the same values and remain in step as time persists. The criterion for the occurrence of identical synchronisation derived by [Pecora & Carroll, 1990] requires that all the Lyapunov exponents of $\mathbf{u}'(t)$ under coupling to be negative. Later on, it was pointed out that since the Lyapunov exponents of $\mathbf{u}'(t)$ are not simply a subset that belongs to the exponents of the composite system $[\mathbf{u}, \mathbf{v}, \mathbf{u}', \mathbf{v}']$ but rather it is dependable on $\mathbf{v}(t)$, hence a more precise term to be used is given as conditional Lyapunov exponents [Pecora & Carroll, 1991].

As an example consider two Lorenz systems in the coupled form given as

$$\left. \begin{aligned} \dot{x}_1 &= \mu_1(x_2 - x_1) \\ \dot{x}_2 &= (\mu_2 - x_3)x_1 - x_2 \\ \dot{x}_3 &= x_1x_2 - \mu_3x_3 \end{aligned} \right\} \text{Drive System,} \quad (1.12)$$

$$\left. \begin{aligned} \dot{y}_1 &= \mu_1(y_2 - y_1) \\ \dot{y}_2 &= (\mu_2 - y_3)x_1 - y_2 \\ \dot{y}_3 &= x_1y_2 - \mu_3y_3 \end{aligned} \right\} \text{Response System.}$$

Here $\mathbf{u} = [x_2, x_3]$, $\mathbf{u}' = [y_2, y_3]$ and the coupling variable $\mathbf{v} = [x_1]$. The coupled Lorenz system (1.12) fulfils the general model given in system (1.11). The parameter set is assigned as $\boldsymbol{\mu} = [\mu_1, \mu_2, \mu_3] = [60, 10, 8/3]$. Fig.1.7 shows the time evolution of the drive and response systems represented using the solid and dashed lines respectively. The time evolutions of the two subsystems under coupling start off with a large difference in initial conditions. Instead of diverging quickly, the two systems quickly synchronise with each other. The conditional Lyapunov exponent of y_2 and y_3 are measured to be $\lambda_2 = -1.81$ and $\lambda_3 = -1.86$.

Fig.1.7. Time evolutions of the drive and response systems of coupled Lorenz system (1.12) represented by solid and dashed lines respectively. Under the effect of coupling, the time evolutions of the response system quickly converges to that of the drive system. The conditional Lyapunov exponents of y_2 and y_3 are measured to be $\lambda_2 = -1.81$ and $\lambda_3 = -1.86$.

Phase Synchronisation

Phase synchronisation is realised in weakly coupled self-sustained systems [Rosenblum et al., 1996; Pikosky *et al.*, 2000]. This phenomenon is a characteristic feature of autonomous continuous-time systems and cannot be realised in periodically forced models [Rosenblum *et al.*, 1996] and so far no one has shown or proved that phase synchronisation could happen to discrete system. In phase synchronisation the two subsystems oscillate in phase through phase locking while there may be no relevant relationship in amplitude. In general, if the phase difference ϕ of the two subsystems has a bounded value, such that $\phi < \text{constant}$ then phase synchronisation can be considered taking place. Phase synchronisation found its application mostly in the study of life sciences and ecology. It has been discovered to be a key feature in the dynamics of human cardio-respiratory system [Schafer *et al.*, 1998], magnetoencephalographic activity of patients with Parkinson's disease [Tass *et al.*, 1998] and extended ecological system [Blasius, 1999]. More recently, the application of phase synchronisation has been extended to secure communication [Chen *et al.*, 2003].

Generalised Synchronisation

Generalised synchronisation categorises cooperative behaviour between two non-identical subsystems, $f(\mathbf{x}) \neq g(\mathbf{y})$, [Rulkov et al., 1995; Kocarev & Parlitz, 1996]. In this case, a response system, which is not a replica of the drive system, may not identically synchronise with the drive system but may achieve generalised

synchronisation instead. In generalised synchronisation the vector $\mathbf{x}(t)$ relates to the vector $\mathbf{y}(t)$ through a function ψ . Hence, generalised synchronisation occurs when $\mathbf{x}(t) = \psi(\mathbf{y}(t))$. To detect generalised synchronisation, a numerical method called the mutual false nearest neighbour [Rulkov et al., 1995] was proposed for detecting the presence of the function ψ and thereby distinguishing between synchronised and unsynchronised behaviour of coupled chaotic systems. The stability criterion for the occurrence of generalised synchronisation is that the phenomenon occurs if and only if all conditional Lyapunov exponent of $\mathbf{y}(t)$ are negative [Kocarev & Parlitz, 1996]. Applications of generalised synchronisation lie in the area of spatiotemporal chaos commonly found in fluid and chemical reactions that are modelled by extended coupled systems [Parmananda, 1997].

Chapter 2

Chaos-based communication techniques

The ability to design synchronous chaotic systems may open up interesting opportunities for applications of chaos to communication. Pecora and Carroll first proposed this idea in their work in chaos synchronisation [Pecora & Carroll, 1990]. This idea was demonstrated later on to be viable using a simple circuit implementation shown in Fig. 2.1, [Cuomo & Oppenheim, 1993]. The possibility of utilising chaos for communication soon leads to extensive research in chaos-based communication techniques. This interest that is generated among physicists, mathematicians and engineers arises due to the prospective of utilising the randomlike behaviour and the sensitivity to initial conditions of chaos to encrypt information for secure communication. These characteristics of chaos fulfil the classic Shannon requirements of confusion and diffusion [Shannon, 1949] for cryptography without the operation of large and complex algorithms found in conventional cryptosystems such as the *Data Encryption Standard* and *Advanced Encryption Standard*. Besides providing secure communication, the inherent wideband characteristic of chaos could also be used for spread spectrum applications to provide robust wideband communication.

The interest in utilising chaos for communication is further driven and supported by two other advantages of chaos-based communication techniques over conventional communication techniques.

Firstly, the self-synchronising and the inherent wideband characteristic of chaos allows the three stages in a conventional communication system, which include information encryption, carrier signal generation and frequency spreading to be combined into a single process without the necessity of extra circuitry. In another words, in a chaos-based communication system, the process of carrier signal generation will also provide information encryption and frequency spreading at the same time, using only a simple circuit such as the one shown in Fig. 2.1. Hence a chaos-based communication system offers the simpler and cheaper alternative by eliminating the use of complex circuits for encryption and frequency spreading found in the conventional communication system.

Fig. 2.1. Circuitry of Lorenz system (1.5) with system parameters assigned as $[\sigma, \mu, \rho] = [16, 45.6, 4]$. The components have the values given as [Resistors(k Ω): $R_1, R_2, R_3, R_4, R_6, R_7, R_{13}, R_{14}, R_{16}, R_{17}, R_{19} = 100$; $R_5, R_{10} = 49.9$; $R_8 = 200$; $R_9, R_{12} = 10$; $R_{11} = 63.4$; $R_{15} = 40.2$; $R_{18} = 66.5$; $R_{20} = 158$. Capacitors (pF): $C_1, C_2, C_3 = 500$. Op-Amps (1-8): LF353. Multipliers: AD632AD]. The diagram and information are taken from Physical Review Letters Vol. 71, pp.66, Fig.1, [Cuomo & Oppenheim, 1993].

Secondly, chaos-based digital communication systems offer a potentially simple solution for robust wideband communications. Many modern communications applications such as mobile or indoor radio are susceptible to multipath propagation effects arising from interaction between signals travelling along different propagation paths. By contrast, with a conventional digital communication system, where the digital symbols are mapped to a finite set of periodic waveform segments for transmission, every transmitted symbol in a chaos-based digital communication system is mapped to a different aperiodic waveform segment. As a result, the cross correlation between segments of a chaotic

Chapter 2 Chaos-based communication techniques

waveform are lower than between segments of periodic waveforms. Hence theoretically, chaos-based communication system ought to offer better performance under multipath propagation conditions.

Chaos-based communication techniques are primarily employed in secure communication and spread spectrum applications. Ironically, chaos theory is also used to develop cryptanalysis techniques to analyse and decipher the chaos-based secure communication schemes. The communication and cryptanalysis techniques will be introduced in this chapter using four sections. Section 2.1 and 2.2 introduce the approaches applied to secure information by using continuous-time and discrete-time signals respectively. Section 2.3 describes the fundamental routes of attack make use in cryptanalysis and some of the more efficient and powerful developed techniques. Section 2.4 introduces chaos-based digital communication techniques used for spread spectrum applications. Section 2.5 provides a short conclusion on the shortcomings of the existing chaos-based communication techniques.

2.1 Continuous-time chaotic encryption

Continuous-time chaotic encryption techniques are employed for transmission over noisy channels such as in radio transmission. These techniques utilise chaos synchronisation in the process. Continuous-time chaotic encryption can be broadly categorised into three approaches. They include chaotic shift keying [Parlitz *et al.*, 1992; Cuomo & Oppenheim, 1993], chaotic masking [Kocarev *et al.*, 1992; Cuomo & Oppenheim, 1993] and chaotic modulation [Halle *et al.*, 1993]. These papers

quoted here are the original schemes that were used to propose the three encryption approaches for the first time. Beside these schemes, there are a number of other schemes that are built around these original ideas to improve on the security and the transmission efficiency.

2.1.1 Chaotic shift keying

Chaotic shift keying [Parlitz *et al.*, 1992] has developed to transmit digital information. The communication setup shown in Fig. 2.2 consists of two identical chaotic systems with one system (*drive system*) at the transmitter end driving the other system (*response system*) at the receiver end using a state variable, $s = x_i \in \mathbf{x}$, of the drive system. In Fig. 2.2, $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and $\mathbf{y} = [y_1, y_2, \dots, y_n]^T$ are the corresponding vectors at the transmitter and receiver ends respectively. When a variable x_i from $\mathbf{x}$ is chosen to be the carrier signal, the corresponding variable y_i from $\mathbf{y}$ will be used for comparison, where $i = 1, 2, \dots, n$. The digital information $b(t)$, is a binary sequence, which has a value of either 0 or 1. To transmit digital information, the coupling variable s is produced at the drive system by slightly shifting a value of the parameter set $\boldsymbol{\mu}_x$ according to the binary sequence. In doing so, the drive system is essentially using two sets of parameters to generate s such that $\boldsymbol{\mu}_x = \boldsymbol{\mu}_0$ if $b(t) = 0$ and $\boldsymbol{\mu}_x = \boldsymbol{\mu}_1$ if $b(t) = 1$. At the receiver end, the response system has a fixed parameter set assigned as $\boldsymbol{\mu}_1$ throughout the transmission process. Assuming that the coupled system, which consists of drive and response systems, satisfies the criteria for identical synchronisation, then a bit of 1 is

received when synchronisation between y_i and $s = x_i$ is detected for a symbol duration, T_s . Otherwise a bit of 0 is received.

Fig. 2.2. Schematic of a basic chaotic shift keying communication system setup.

In secure communication, the parameter sets μ_0 and μ_1 is set as the secret keys. The aim is to defy an unauthorised receiver who has the knowledge of the response system but not the secret key to detect synchronisation from the coupling of his or her response system with the intercepted information carrier signal $s(t)$. As a result, the unauthorised receiver could not retrieve the transmitted information and hence secure communication is provided.

Fig. 2.3 shows a demonstration on secure digital communication using chaotic shift keying. The coupled system is constructed using the Lorenz system, given as

$$\begin{aligned}
& \left. \begin{aligned} \dot{x}_1 &= \mu_{x,1}(x_2 - x_1) \\ \dot{x}_2 &= (\mu_{x,2} - x_3)x_1 - x_2 \\ \dot{x}_3 &= x_1x_2 - \mu_{x,3}x_3 \end{aligned} \right\} \text{Drive System} \\
& \left. \begin{aligned} \dot{y}_1 &= \mu_{y,1}(y_2 - y_1) \\ \dot{y}_2 &= (\mu_{y,2} - y_3)s - y_2 \\ \dot{y}_3 &= sy_2 - \mu_{y,3}y_3 \end{aligned} \right\} \text{Response System}
\end{aligned} \tag{2.1}$$

The drive system variable $x_1(t)$ is used as the information carrier signal, $s(t) = x_1(t)$. The parameter set of the drive system is assigned as $\mu_x = [\mu_{x,1}, \mu_{x,2}, \mu_{x,3}] = [60.5, 10, 2]$ when $b(t) = 0$ and $[60, 10, 2]$ when $b(t) = 1$. For the response system, the parameter set is fixed at $\mu_y = [\mu_{y,1}, \mu_{y,2}, \mu_{y,3}] = [60, 10, 2]$.

Fig. 2.3(a) shows a sequence of binary information to be transmitted with alternate bits 0 and 1. The symbol duration T_s is set as 10 time-units as indicated in Fig. 2.3(a). The transmitted information carrier signal is shown in Fig. 2.3(b). From the figure, this signal does not leak any information to an unauthorised receiver who may intercept it intentionally or unintentionally. Only an authorised receiver with the secret key can retrieve the information by computing the synchronisation error, $E(t) = s(t) - y_1(t)$. According to the assignment of the parameter sets, bit 1 is received when identical synchronisation between the drive and response systems is detected for symbol duration T_s , indicated by $\lim_{t \rightarrow T_s} E(t) = 0$. Otherwise, bit 0 is received with $\lim_{t \rightarrow T_s} E(t) \neq 0$. Fig. 2.3(c) shows the computed $E(t)$ at the receiver end that corresponds to the digital information given in Fig. 2.3(a).

Fig. 2.3. Demonstration of secure digital communication using chaotic shift keying based on coupled Lorenz system (2.1). (a) A sequence of binary information to be transmitted with alternate bit 0 and 1. Symbol duration $T_s = 10$ time-units. (b) The transmitted information carrier signal $s(t) = x_1(t)$. (c) Synchronisation error, $E(t) = s(t) - y_1(t)$.

According to the assignment of the parameter sets, bit 0 is received when $\lim_{t \rightarrow T_s} E(t) \neq 0$, otherwise bit 1 is received when $\lim_{t \rightarrow T_s} E(t) = 0$.

2.1.2 Chaotic masking

Chaotic masking [Kocarev *et al.*, 1992] was initially developed to transmit analogue information but it has the capability of transmitting digital information as well. The communication setup is shown in Fig. 2.4. Two identical systems are used, with the drive system at the transmitter end and the response system at the receiver end. In chaotic masking schemes, a piece of analogue information with small amplitude, $a(t)$ is encrypted by adding it directly to a generated chaotic

Chapter 2 Chaos-based communication techniques

signal, x_i , from the drive system. The transmitted signal denoted by s_a is therefore the sum of two signals given as $s_a = x_i + a$. At the receiver end, s_a is used to couple the response system to achieve identical synchronisation, which could be expressed as $\lim_{t \rightarrow \infty} (x_i - y_i) = 0$. The information can then be recovered by computing $s_a(t) - y_i(t) = a(t)$. For chaotic masking to be functioning properly such that the encrypted analogue information could be recovered through a synchronisation process, the amplitude of $a(t)$ must be much smaller than $x_i(t)$, which is usually in the region of 1:400.

Chaotic masking can be employed to transmit digital information. This is carried out by converting a binary sequence into a continuous-time waveform of rectangular pulses similar to the one shown in Fig. 2.3(a). However, due to the requirement that the amplitude of $a(t)$ must be small, which resulted in poor bit error ratio (BER) performance, chaotic masking is usually not preferred over chaotic shift keying for transmitting digital information.

Fig. 2.4. Schematic of a basic chaotic masking communication system setup.

2.1.3 Chaotic modulation

Chaotic modulation is essentially similar to chaotic masking. The approach is to transmit analogue information and have the capability to transmit digital information. The communication setup is shown in Fig. 2.5. In chaotic modulation schemes, an analogue signal $a(t)$ of small amplitude is encrypted by adding it to a chaotic signal x_i from the drive system, which produces the transmitted signal, given as $s_a(t) = x_i(t) + a(t)$. Chaotic modulation differentiates itself from chaotic masking by feeding the transmitted signal $s_a(t)$ back into the drive system and at the same time transmitting the signal to the receiver end. Therefore, unlike chaotic shift keying and chaotic masking, f is also a function of $s_a(t)$, which produces $x_i(t)$ with a more complex dynamics. This creates difficulties in identifying the system parameters from the intercepted information carrier signal. The information can be extracted at the receiver end through a reverting process in synchronisation.

Fig. 2.5. Schematic of a basic chaotic modulation communication system setup.

2.2 Discrete-time chaotic encryption

Discrete-time chaotic encryption employs non-synchronous encryption techniques that use discrete-time systems to encrypt digital information before transmission in a computer communication network. These techniques serve a different purpose from continuous-time encryption techniques, which are used for transmission over noisy channels such as in radio transmission. Two different forms for discrete-time chaotic encryption are the Baptista-type cryptosystems [Baptista, 1998; Wong *et al.*, 2001; Wong *et al.*, 2003] and the Alvarez-type cryptosystems [Alvarez *et al.*, 1999; Li *et al.*, 2001]. Although security flaws and functional drawbacks [Alvarez *et al.*, 2001; Wong *et al.*, 2001] are identified in the original Baptista and Alvarez cryptosystems [Baptista, 1998, Alvarez *et al.*, 1999] but the modified versions [Wong *et al.*, 2001; Wong *et al.*, 2003, Li *et al.*, 2001, Li *et al.*, 2004] have been shown to provide sufficient security against cryptanalysis and improved efficiency.

In the Baptista-type cryptosystems, two identical discrete-time chaotic systems are used, with one at the transmitter and the other at the receiver end. The chaotic attractor bounded between $X_{\max}$ and $X_{\min}$ is divided into S levels of size $\varepsilon = (X_{\max} - X_{\min})/S$ each. Each level is associated with a unique plaintext as shown in Fig. 2.6. The ciphertext is the number of iterations made by the discrete chaotic system from a specified set of initial conditions to the level representing the plaintext. Therefore, in Baptista-type cryptosystems, the parameter set and the chosen initial conditions form the secret keys. To retrieve the plaintext, the receiver needs to carry out the same number of iterations as indicated by the ciphertext

using an identical discrete-time chaotic system from the specified initial conditions.

The plaintext is taken as the level at which the iteration stops according to Fig. 2.6.

Fig. 2.6. A graphical representation of how a chaotic attractor is divided into S levels of size $\epsilon = (X_{max} - X_{min})/S$ each. The space bounded between X_{min} and X_{max} is some portion (or the whole) of the attractor. Each level has an alphabet associated to it. The diagram is taken from Physics Letters A Vol. 240, pp.51, Fig. 1, [Baptista, 1998].

In the Alvarez-type cryptosystems, a discrete-time chaotic system is iterated from a specified set of initial conditions to produce a discrete waveform that oscillates about a threshold value to generate a pseudo-random binary bit sequence as shown in Fig. 2.7. In the figure, the chaotic discrete-time waveform oscillates about a threshold value equal to 0.6, which generates a bit 0 if $X_{(k)} > 0.6$ and a bit 1 if $X_{(k)} \leq 0.6$. From this illustration shown in Fig. 2.7, a pseudo-random bits sequence for $k = 30 \dots 40$ is generated as 0001011010. Assume that the first block of plaintext to be encrypted is given as 0110, which consists of four bits $b_1 = 4$ as shown in Fig. 2.7. Then if this block of plaintext occurs for the first time along the

pseudo-random bit sequence that begins at $k = 35$, then the ciphertext (b_1, c_1) will be (4,35).

Fig. 2.7. An illustration of the generation of a pseudo-random bits sequence. The solid line represents a chaotic discrete-time evolution. The dashed line marked out the threshold value that is equal to 0.6, which generates a bit 0 if $X_{(k)} > 0.6$ and a bit 1 if $X_{(k)} \leq 0.6$. The pseudo-random bits sequence is 00001011010 for $k = 30 \dots 40$.

The secret keys in an Alvarez-type cryptosystem consist of the parameter set, the chosen initial conditions and the threshold value. An intruder without the secret keys will not be able to produce an identical pseudo-random bits sequence as a result of the randomlike and sensitivity to initial condition of chaos. To retrieve the plain-text, the receiver generates an identical pseudo-random bits sequence using

the secret keys and an identical chaotic discrete-time system. The plain-text is the block along the pseudo-random bits sequence that corresponds to the given ciphertext (b_i, c_i) .

2.3 Chaos-based cryptanalysis

Chaos-based cryptanalysis techniques reviewed here have been developed to breakdown the security of continuous-time chaotic encryption. The aim is to uncover the encrypted information without prior knowledge of the secret keys. Chaos-based cryptanalysis techniques can be broadly grouped into two categories, namely identification cryptanalysis and characteristic cryptanalysis.

Identification cryptanalysis is based on reconstruction techniques developed to extract analogue information signals encrypted by either chaotic masking scheme [Kocarev *et al.*, 1992] or a chaotic modulation scheme [Halle *et al.*, 1993]. In order to extract the information signal masked by these schemes, the existing identification cryptanalysis techniques must ultimately undertake either one of the two fundamental routes of attack, depending on whether the intruder knows the underlying equations of the chaotic system or not. (I) If the intruder knows the dynamical form of the chaotic system but does not know the parameter set, which are the secret keys, then the cryptanalysis techniques will be based on parameters identification [Stojanovski *et al.*, 1996; Bezruchko *et al.*, 2001; Ponomarenko & Prokhorov, 2002]. (II) If both the dynamical form and parameter set of the chaotic system are unknown to the intruder, then the cryptanalysis techniques will be based

Chapter 2 Chaos-based communication techniques

on approximating the future time series either using a global [Short & Parker, 1998] or local [Zhou & Lai, 1999; Huang et al., 2001] prediction model.

Identification cryptanalysis

Identification cryptanalysis techniques generally involve very complex functions that are numerically intensive. Here a brief description of the general framework of the two fundamental routes of attack is given. A more in depth discussion will be carried out in conjunction with the introduction of pseudo-random switching key in chapter 5.

There are two fundamental routes of attack used by identification cryptanalysis techniques. The first type aims to identify or estimate the parameter set if the dynamical form of the chaotic system is known. The second type aims to predict the future dynamics of the information carrier signal either by local or global modelling, if the dynamical form of the chaotic system is unknown.

Techniques used to identify or estimate the parameters of chaotic system are dependent of the realisation of identical synchronisation. The intercepted signal $s(t) = x_i(t)$ from the transmitter end is used to couple a chaotic system $\mathbf{F}(\mathbf{y}_a, \boldsymbol{\mu}_a, s)$ that has a same dynamical form as the drive system $\mathbf{F}(\mathbf{x}, \boldsymbol{\mu}_x)$ used by the transmitter. Here $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and $\mathbf{y}_a = [y_{a,1}, y_{a,2}, \dots, y_{a,n}]^T$ are the state vectors and $\boldsymbol{\mu}_x$ and $\boldsymbol{\mu}_a(t)$ are the parameter sets, $\boldsymbol{\mu}_a(0) \neq \boldsymbol{\mu}_x$. The objective is to identify the parameter set of the drive system, $\boldsymbol{\mu}_x$, through the process of achieving identical synchronisation by using the coupled system, $\mathbf{F}(\mathbf{x}, \boldsymbol{\mu}_x), \mathbf{F}(\mathbf{y}_a, \boldsymbol{\mu}_a, s)$ such

Chapter 2 Chaos-based communication techniques

that as $\lim_{t \rightarrow \infty} \mathbf{y}(t) = \mathbf{x}(t)$, $\lim_{\mathbf{y} \rightarrow \mathbf{x}} \mu_a(t) = \mu_x$. This process can be carried out using a minimisation method [Parlitz et al., 1996], an autosynchronisation method [Parlitz, 1996], a random optimisation method [Sakaguchi, 2002] or a parameter adaptive method [Tao et al., 2004].

In local modelling [Farmer & Sidorowich, 1987; Short & Parker, 1998], nearby points of a trajectory in an embedding space is used to predict short-term dynamics in the future. In global modelling, the future dynamics of a time series is predicted by using a generalised mathematical model, which may be a polynomial or other basis functions. Hence with the aid from either local or global modelling to predict future time evolution, the encrypted information can be uncovered by subtracting the intercepted transmitted signal with the predicted time series.

Characteristic cryptanalysis

Characteristic cryptanalysis techniques are statistical properties analysis techniques developed to uncover digital information encrypted by chaotic shift keying [Parlitz et al., 1992]. In a chaotic shift keying scheme, a binary sequence is encrypted by shifting the parameter set between two sets of values according to bit 0 and 1. As a result, two symbol durations over the time series will exhibit two distinctive sets of statistical properties if they correspond to different digital symbols, i.e. 0 and 1. This is regardless of the proximity of the chosen parameter sets. Characteristic cryptanalysis techniques therefore aim to detect changes in statistical properties over the time series of the intercepted signal. These techniques include constructing attractors from return maps [Pérez & Cerdeira, 1995; Yang et

al., 1998a1, using a spectrogram [Yang et al., 1998b1, measuring the errors from generalised synchronisation transformations [Yang et al., 1998c] and measuring the weighted density of localised dynamics about a test trajectory [Storm & Freeman, 2002]. Here we point out a third fundamental route of attack used in chaos-based cryptanalysis. (III) If the digital information is encrypted using chaotic key shifting, then the chaos-based cryptanalysis carried out will focus on detecting changes between two distinct sets of statistical properties over the time series of the intercepted information carrier signal.

Fig. 2.8 shows a demonstration of using the return map technique [Pérez & Cerdeira, 1995] to uncover digital information encrypted by chaotic shift keying. The drive system employed is the Lorenz system (2.1) with parameter sets assigned as $[\mu_{x,1}, \mu_{x,2}, \mu_{x,3}] = [65, 10, 2]$ for $b(t) = 0$ and $[60, 10, 2]$ for $b(t) = 1$. The construction of an attractor from the return map is the first characteristic cryptanalysis technique developed to uncover digital information encrypted by chaotic shift keying. Although this technique is not the most effective among the others that follow, it is so far the simplest in term of computation.

To begin with, the maxima X_n and minima Y_n indicated by dots along the intercepted information carrier signal as shown in Fig. 2.8(a) are collected. If the signal is generated from a Lorenz system with a fixed system parameter set, then an attractor that consists of three solid lines will surface when sufficient points are plotted on a (A_n, B_n) plot as shown in Fig. 2.8(b). The variable A_n is the n th average of X_n and Y_n expressed as $A_n = (X_n + Y_n)/2$ and the variable B_n is the n th difference between X_n and Y_n expressed as $B_n = X_n - Y_n$. The formation of

Chapter 2 Chaos-based communication techniques

these three solid lines that surface from the computation of the maxima and minima of the Lorenz waveform is independent of the initial conditions. However the exact positioning of this attractor is influence by the chosen parameter set. This means that any alteration of the parameter setting will cause the attractor to shift to a new position while remaining in the same formation. Hence, if the signal is generated from the Lorenz system that switched between two sets of parameters, then the lines will appeared to be split as shown in Fig. 2.8(c). This is in fact due to the presence of two attractors being embedded along the same continuous waveform during different time interval. Once it is realised that the switching between two parallel segments of the attractor will also mean switching between the two parameter sets, an intruder could start classifying the points according to which branch of the attractor they fall in and uncover the digital information.

Fig 2.8 Demonstration of using the construction of attractor from return map to uncover digital information encrypted by chaotic shift keying. (a) A Lorenz waveform with the maxima X_n and the minima Y_n indicated by dots. (b) An attractor constructed from return map based on a fixed parameter set. The variables $A_n = (X_n + Y_n)/2$ and $B_n = X_n - Y_n$. (c) An attractor constructed from return map based on a two parameter sets.

2.4 Chaos-based digital communication for spread spectrum applications

Spread spectrum techniques were initially developed to apply in military communication systems [Scholtz, 1982]. A communication system is defined as a spread spectrum system if the transmitted signal occupies a bandwidth much in excess of the minimum bandwidth necessary to send the information. During the

Chapter 2 Chaos-based communication techniques

Second World War, research in spread spectrum techniques was motivated primarily by the desire to achieve highly jam-resistant communication systems. As a result of this research, there emerged an assortment of other applications in areas such as energy density reduction, high-resolution ranging and multiple accesses.

Given that the aim of spread spectrum techniques is to spread the bandwidth of the transmitted signal to a much wider range in excess of minimum required, the inherent wideband characteristic of chaos provides a good basis for employing it for the development of spread spectrum applications. In order to facilitate further discussion on chaos-based digital communication for spread spectrum applications, it is necessary to provide a brief introduction to the fundamental techniques used in conventional digital communication systems.

In conventional digital communication techniques, bandpass modulation is the process by which digital information are transformed into a sinusoidal waveform for transmission. Since a sinusoid has three features, namely amplitude, phase and frequency, bandpass modulation can be defined as the process by which one of these features or the combination of them is varied in accordance with the digital information to be transmitted.

Below the frequency shift keying technique where digital information is modulated onto waveforms of different frequency is used to provide a general illustration on the conventional digital communication techniques, see Fig.2.9. Consider the general form of the carrier wave given as $s(t) = A(t)\cos[\omega_0 t + \phi(t)]$.

In frequency shift keying, the amplitude $A(t)$ and the phase $\phi(t)$ can be fixed at 1 and 0 respectively for all t . For transmission, the frequency ω_0 in radians per

time-unit shifts to M different values according to the digital information signal. Assuming that digital symbols, which consist of two bits each and $K = 2$, are to be transmitted for each symbol duration T_s , then this will require four different combinations of digital symbol, $M = 2^K = 4$, to be employed in forming the digital information signal. The four digital symbols required are given as 00, 01, 10 and 11 as shown in Fig. 2.9(a). Hence, in the modulation process, the digital symbols are modulated onto waveforms of four different frequencies as shown in Fig. 2.9(b). Gray coding is used to assign digital symbols to frequencies as shown in Table 2.1. In Gray coding each increment in frequency has the corresponding digital symbol having only one bit difference from the previous symbol to minimise the bit error ratio (BER) at the receiver end. BER is defined as the number of bits decoded wrongly over the total number of bits transmitted. Lastly, in digital communication, when $K \geq 2$, it is termed as M -ary transmission and when $K = 1$, it is termed as binary transmission.

Digital Symbol	00	01	11	10
Frequency ω_0	2π	4π	6π	8π

Table 2.1

Fig 2.9. Demonstration on M-ary frequency shift keying technique where digital information is modulated onto waveforms of four different frequencies. Here $M = 4$. (a) Digital information in decimal value. (b) The transmitted signal corresponding to the information signal in (a).

For spread spectrum applications, the bandwidth of the transmitted signal is spread to a wider range of frequencies by using a pseudo-random code [Scholtz, 1982; Sklar 2002]. This approach suffers from two major disadvantages: (i) the code used for de-spreading at the receiver end must synchronise perfectly with the code applied at the transmitter for spreading; (ii) the spreading and de-spreading processes require extra circuitry that prevent the cost and power consumption of spread spectrum systems falling below a certain limit.

Chaotic signal with the self-synchronising capability and the inherent wideband characteristic may thus be a solution to the disadvantages of conventional digital communication systems. Chaotic shift keying [Parlitz *et al.*, 1992] used for secure communication may be considered as the first chaos-based digital communication

technique, which could be employed for spread spectrum applications. However, this technique that relies on the observation of synchronisation to differentiate between bit 0 and 1 may suffer from poor bit error ratio (BER) performances when transmitting under noisy environment. This is because perfect identical synchronisation may not be realisable once the transmitted signal is corrupted by channel noise. Difficulties thus arise at the receiver end in differentiating between synchronous and non-synchronous behaviour, which greatly degrade the BER performances of chaotic shift keying for practical applications in noisy environment [Kolumbán *et al.*, 1996a].

In order to apply chaotic signals for spread spectrum applications under noisy environment, a technique known as differential chaos shift keying (DCSK) [Kolumbán *et al.*, 1996b] is first proposed. This technique does not require synchronisation to receive digital information. DCSK was developed without the objective to provide secure communication. The basic idea of DCSK is that every digital bit to be transmitted is represented by two chaotic sample functions. The first sample function serves as a reference while the second one carries the information. Bit 1 is sent by transmitting a reference signal from a chaotic system twice, while for bit 0, the reference signal is transmitted followed by an inverted copy of the same signal. The two sample functions are correlated at the receiver end to retrieve the digital information. A positive autocorrelation indicates that bit 1 has been received while a negative autocorrelation indicates that bit 0 has been received.

From the basic idea of DCSK, two other chaos-based digital communication techniques were developed to improve on the BER performances. These techniques

Chapter 2 Chaos-based communication techniques

are frequency modulation – differential chaos shift keying (FM-DCSK) [Kolumbán *et al.*, 1998] and symbol dynamics – differential chaos shift keying (SD-DCSK) [Maggio & Galias, 2002]. Although these techniques [Kolumbán *et al.*, 1998; Maggio & Galias, 2002] manage to improve on the BER performances of DCSK, this also resulted in higher system complexity, which causes lower transmission efficiency. A comparison between these two techniques shows that SD-DCSK has better BER performances than FM-DCSK [Kolumbiin *et al.*, 1998; Maggio & Galias, 2002].

Ergodic chaotic parameter modulation (ECPM) [Leung *et al.*, 2002] is another chaos-based technique developed to transmit digital information for spread spectrum applications. ECPM achieved comparable BER performances as SD-DCSK using a simpler communication system. The ergodic theorem employs in ECPM states that for a waveform generated from a chaotic system with fixed parameter set, the limit $\lim_{N \rightarrow \infty} (1/N) \sum_{\tau=1}^N x_{\tau}$ exists with x_{τ} being the values sampled at regular time interval along the chaotic waveforms and $\tau = 1, 2, \dots, N$. In certain chaotic systems such as the Chebyshev map, this limit may have a monotonic relationship with the parameter set [Leung *et al.*, 2002]. The ergodic properties of chaotic waveform exploited by ECPM is in fact similar in principle to statistical properties mentioned in section 2.3. The functioning of ECPM is therefore similar to chaotic shift keying where two different sets of parameters are used to represent bit 0 and 1. However unlike chaotic shift keying, ECPM does not required synchronisation at the receiver end to retrieve the information. Instead

ECPM retrieves the digital information by measuring the ergodic properties of the received information carrier signal to differentiate between bit 0 and bit 1.

Besides DCSK, FM-DCSK, SD-DCSK and ECPM, there is a number of other chaos-based digital communication techniques developed. These four techniques are introduced here due to their robustness under noisy environment for practical application and their superior BER performances among the others. A description and evaluation of all developed techniques can be found in [Lau & Tse, 2003].

2.5 Shortcomings of the existing chaos-based communication techniques

The utilisation of chaos in communication may provide advantages that could not be achieved under the conventional communication techniques. It is due to the possibility of using these advantages that chaos communication existed. However, chaos-based communication has its shortcomings. This section will discuss the shortcomings of chaos-based communication techniques.

To begin with, let us recall that chaos communication at the very beginning stage was proposed based on two clear-cut advantages over conventional communication techniques. Firstly, it is self-synchronising characteristic and secondly, is the inherent wideband characteristics. These advantages offer us the simpler and cheaper alternative to conventional techniques in terms of software and hardware implementation. Therefore the cost and complexity factors must always be two of the main considerations when developing chaos-based communication systems.

Continuous-time chaotic encryption

Presently, continuous-time chaotic encryption is no longer effective in two senses, security-wise and cost-wise. Security-wise, it is known that chaos exhibits contradicting dynamics that is random in behaviour and yet deterministic in nature. Realising the distinction between the behaviour and the nature of chaos plays an important role in secure communication using continuous-time encryption. In continuous-time encryption, the random behaviour of the chaotic waveform is employed to hide information directly onto it. On the other hand, the deterministic nature is exploited by cryptanalysis techniques to uncover the information. As it is the nature rather than the behaviour that determines the fundamental of the system, it may therefore be concluded that the basis used to formulate continuous-time encryption may never be as strong as the basis used to formulate the cryptanalysis techniques. Hence presently we are witnessing many encryption techniques being broken shortly after being published.

Cost-wise, although it is suggested that security may be enhanced by using higher dimensional chaos [Peng et al., 1996] this may inevitably result in higher system complexity and cost, which is against the basic advantage of chaos communication stated above. Furthermore higher dimensional chaos may not provide the necessary security [Short & Parker, 1998].

To solve this problem, this thesis derived a simple technique to diffuse out the deterministic nature of chaos. This technique known as the pseudo-random switching keys (PRSK) [Xu & Chee, 2003] will be introduced in Chapter 5. In the process of deriving PRSK, this thesis discovered a new chaos synchronisation

Chapter 2 Chaos-based communication techniques

phenomenon whereby identical synchronisation is achieved between two chaotic subsystems with the system parameters switching rapidly and randomly in a discontinuous manner within a chosen set of values. This opposes the earlier belief that the system parameters must be fixed to achieve chaos synchronisation. This new observation will be introduced in chapter 5 [Chee *et al.*, 2004].

Discrete-time chaotic encryption

Discrete-time chaotic encryption [Baptista, 1998; Wong *et al.*, 2001; Wong *et al.*, 2003; Alvarez *et al.*, 1999; Li *et al.*, 2001] suffers from a major drawback. The Baptista-type and Alvarez-type cryptosystems usually require about 800 to 1000 iterations to encrypt a small block of digital information, which cannot consist of more than eight bits for practical application. This causes the cryptographic schemes to be too slow for transmitting large multimedia files through the Internet.

In this thesis, a cryptosystem that uses synchronous discrete-time chaos is developed. This cryptosystem requires only a single iteration of the chaotic system to encrypt a block of digital information of up to 52 bits. This is in contrast with the Baptista-type and Alvarez-type cryptosystems that require 800 to 1000 iterations to encrypt eight or fewer bits. Furthermore the developed cryptosystem in this thesis is able to generate ciphertext with storage size that is smaller than the inputted information.

Chaos-based digital communication for spread spectrum applications

Chaos-based techniques face major challenges from conventional techniques in terms of BER performances and transmission rates. So far, among the proposed

Chapter 2 Chaos-based communication techniques

chaos-based communication techniques, SD-DCSK [Maggio & Galias, 2002] and ECSK [Leung *et al.*, 2002] exhibit some of the best BER performances. However when BER performances are compared over additive white gaussian noise (AWGN) channel, SD-DCSK and ECPM are still inferior to conventional techniques such as phase shift keying (PSK) [Sklar, 2002] and frequency shift keying [Sklar, 2002]. This means that no chaos-based techniques have shown better BER performances than the conventional techniques. The relatively poor BER performances of chaos-based communication schemes may be due to the non-perfect orthogonality of the chaotic carrier signals in a typical chaos-based communication system.

Furthermore, the basic idea used for developing chaos-based techniques [Kolumbán *et al.*, 1996b; Kolumbán *et al.*, 1998; Maggio & Galias, 2002] allows only binary transmission where 1 bit of information is transmitted for each symbol duration. This reduces the efficiency of chaos-based techniques in terms of transmission rates. Although chaos-based M-ary transmission techniques have been proposed [Kolumbán *et al.*, 1997; Galias & Maggio, 2001], these techniques have extremely poor BER performances that makes them unsuitable for practical usage and the complexity of the systems increases with bits per symbol.

The poor BER performances exhibited by chaos-based communication techniques are not due to the chaotic signal being vulnerable to noise contamination. Rather, BER has a direct linkage to the encoding and decoding techniques used. Similarly, the ability to conduct *M*-ary transmission also depends on these techniques.

Chapter 2 Chaos-based communication techniques

This thesis recognised that projective synchronisation of chaos could be utilised to overcome the challenges from conventional techniques. To overcome these challenges and contribute to the theoretical formulation of chaos theory, this thesis develops a new control algorithm for projective synchronisation [Xu & Chee, 2002], which will be described in chapter 4. In chapter 6, a chaos-based digital communication system [Chee & Xu, 2004] is developed to transmit digital information using this control algorithm. This is the first chaos-based system to achieve better BER performances over conventional techniques in single-user environment. Furthermore, the developed system allows M-ary transmission without increase in system complexity.

Chapter 3

Projective synchronisation in coupled systems and its stability criteria

Projective synchronisation is one of the four main types of the chaos synchronisation phenomenon. In projective synchronisation, the corresponding state variables of two systems coupled by a common variable synchronised up to a similar proportional relationship and remain in phase. This phenomenon is first observed in the mid-1990s [Gonzalez-Miranda, 1996, 1998]. However, projective synchronisation is only named and qualitatively studied towards the end of the last century by [Mainieri & Rehacek, 1999]. This interesting behaviour remained as a phenomenon to be grasped. The occurrence criteria and the ultimate state of projective synchronisation remain unknown and unpredictable.

Beyond these works [Gonzalez-Miranda, 1996, 1998; Mainieri & Rehacek, 1999], further investigations in projective synchronisation in the areas of finding the stability criteria and developing control theories to manipulate the ultimate behaviour have been carried out within Nanyang Technological University. The systematic study carried out changed this incomprehensive phenomenon into a well-understood behaviour by a series of papers, [Xu, 2001; Li & Xu, 2001; Xu *et al.*, 2001; Xu & Li, 2002; Xu *et al.*, 2002; Xu & Chee, 2002; Xu *et al.*, 2004].

Chapter 4 will introduce the control algorithms developed to direct the ultimate state of projective synchronisation. Secondly, this thesis recognised that projective

Chapter 3 Projective synchronisation and its stability criteria

synchronisation could be used to solve some of the existing shortcomings of chaos-based communication. In this thesis the theoretical knowledge of projective synchronisation presented in chapter 3 and 4 is employed effectively to overcome these shortcomings.

Chapter 3 and 4 provide a complete insight to the theoretical basis of projective synchronisation. The derivations of the theories may be mathematically intensive but the end results are nevertheless simple and yet comprehensive.

3.1 Phenomenon of projective synchronisation

Projective synchronisation is the result of coupling two identical partially linear systems with a variable that relates nonlinearly with other variables. With respect to system (1.9), given as $\dot{\mathbf{u}} = \mathbf{g}(\mathbf{u}, \mathbf{v})$, $\dot{\mathbf{v}} = \mathbf{h}(\mathbf{u}, \mathbf{v})$, a system is partially linear if the state vector $\mathbf{u}$ in the first equation varies proportionally with its time derivative

$$\dot{\mathbf{u}} \text{ through the Jacobian matrix } \mathbf{M}(\mathbf{v}) = \begin{bmatrix} \frac{dg_1}{dx_1} & \dots & \frac{dg_1}{dx_n} \\ \vdots & & \vdots \\ \frac{dg_n}{dx_1} & \dots & \frac{dg_n}{dx_n} \end{bmatrix} - \begin{bmatrix} m_{11} & \dots & m_{1n} \\ \vdots & . & \vdots \\ m_{n1} & \dots & m_{nn} \end{bmatrix} \text{ where}$$

$\mathbf{M}(\mathbf{v}) \in \mathbb{R}^{n \times n}$ and the state vector $\mathbf{v} = [z_x]$ relates nonlinearly to the state vector $\mathbf{u}$.

Here the abbreviation $\mathbf{M}$ will be used interchangeably with $\mathbf{M}(\mathbf{v})$ for simplicity. In the study of projective synchronisation, the symbol z is commonly used to denote the nonlinear state variable. Hence if we replace $\mathbf{u}$ by $\mathbf{x}$ for the drive system and $\mathbf{u}'$

by y for the response system, a coupled partially linear system can be expressed in term of Jacobian matrix $\mathbf{M}(z_x)$ as

$$\begin{aligned}\dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x}, & \dot{\mathbf{y}} &= \mathbf{M}(z_x) \cdot \mathbf{y}, \\ \dot{z}_x &= h(\mathbf{x}, z_x), & \dot{z}_y &= h(\mathbf{y}, z_y).\end{aligned}\tag{3.1}$$

Chaotic systems that are partially linear include the Lorenz system [Lorenz, 1963], the disk dynamo system [Bullard, 1978], the Chen system [Chen & Ueta, 1999] and the Lü system [Lü & Chen, 2002].

In the coupled system (3.1), the drive system evolves independently, while the response system is driven by z_x that is governed by the drive system. Once the Jacobian $\mathbf{M}(z_x)$ satisfies the stability criteria [Xu *et al.*, 2002], all corresponding states of $\mathbf{x}$ and $\mathbf{y}$ synchronised up to a common scaling factor α . This proportional relationship between the drive and response states is expressed as $\lim_{t \rightarrow \infty} \|\alpha \mathbf{x} - \mathbf{y}\| = \mathbf{0}$ where the scaling factor α is defined by the limit of the state ratio

$$\alpha = \lim_{t \rightarrow \infty} \alpha(t) = \lim_{t \rightarrow \infty} \|\mathbf{y}\| / \|\mathbf{x}\|.\tag{3.2}$$

Here $\|\bullet\|$ denotes 1-norm of a vector.

As a consequent of the proportional relationship between $\mathbf{x}$ and $\mathbf{y}$ that arises, the nonlinear state variables z_x and z_y will also exhibit the projective synchronous behaviour given as $z_y / z_x = \alpha_z = \alpha^b$, where b is a real number upon the nonlinear system used. The scaling factors depend on the initial condition and chaotic variables of the underlying system [Xu, 2001]. Ultimately, the final state of projective synchronisation is hardly predictable.

Chapter 3 Projective synchronisation and its stability criteria

Projective synchronisation could occur in two ways. When projective synchronisation takes place with positive scaling factor, the state vectors of the drive and response systems evolve in the same quadrant in any instants of time evolution, that is to say the phase angle between the two state vectors in the phase space is zero. On the other hand, when projective synchronisation takes place with negative scaling factor, the state vectors of the drive and response systems evolve in the opposite quadrant in any instants of time evolution with a phase angle of π between the two state vectors in the phase space [Xu, 2001]. The proportionality in projective synchronisation allows us to duplicate a chaotic system with desired scales with the preservation of topological characteristics of the original systems.

To demonstrate projective synchronisation, consider the Chen system (3.3),

$$\begin{aligned}\dot{x}_1 &= \mu_1(x_2 - x_1), \\ \dot{x}_2 &= (\mu_2 - \mu_1 - z_x)x_1 - \mu_2 x_2, \\ \dot{z}_x &= x_1 x_2 - \mu_3 z_x.\end{aligned}\tag{3.3}$$

The Chen system (3.3) in the coupled form expressed in term of Jacobian matrix $\mathbf{M}(z_x)$ is given as

$$\begin{aligned}\dot{\mathbf{x}} &= \begin{bmatrix} -\mu_1 & \mu_1 \\ \mu_2 - \mu_1 - z_x & \mu_2 \end{bmatrix} \mathbf{x} \\ \dot{z}_x &= x_1 x_2 - \mu_3 z_x \end{aligned} \left\{ \text{Drive System}, \right. \\ \dot{\mathbf{y}} &= \begin{bmatrix} -\mu_1 & \mu_1 \\ \mu_2 - \mu_1 - z_x & \mu_2 \end{bmatrix} \mathbf{y} \\ \dot{z}_y &= y_1 y_2 - \mu_3 z_y \end{aligned} \left\{ \text{Response System.} \right. \tag{3.4}$$

Here the state vectors $\mathbf{x} = [x_1, x_2]^T$, $\mathbf{y} = [y_1, y_2]^T$, $\mathbf{v} = [z_x]$ and $\mathbf{v}' = [z_y]$. The parameter set is taken as $\boldsymbol{\mu} = [\mu_1, \mu_2, \mu_3] = [35, 28, 3]$. The drive system governs the

Chapter3 Projective synchronisation and its stability criteria

variable $z_x(t)$, which evolves independently of the response system. The coupled Chen system (3.4) is in fact a partially linear system coupled by the nonlinear state variable $z_x(t)$. Hence the occurrence of projective synchronisation between $\mathbf{x}=[x_1, x_2]^T$ and $\mathbf{y}=[y_1, y_2]^T$ should be expected. Fig. 3.1(a) and (c) show the time evolutions of the variables from the state vectors $\mathbf{x}$ and $\mathbf{y}$, represented using the solid and dashed lines respectively. From the figure, it is shown that the corresponding variables from the two state vectors synchronised up to a common scaling factor α indicated by $\alpha = \lim_{t \rightarrow \infty} \alpha_i(t) = \lim_{t \rightarrow \infty} [y_i(t)/x_i(t)] = 2.34$ in Fig. 3.1(b) and (d) with $i = 1, 2$.

Fig. 3.1. (a) and (c) show the time evolutions of the drive and response systems of the coupled Chen system (3.4) represented by solid and dashed lines respectively. The corresponding variables synchronised proportionally under the coupling effect of the variable $z_x(t)$. (b) and (d) indicate this proportional relationship by the scaling factor $\alpha = \lim_{t \rightarrow \infty} \alpha_i(t) = \lim_{t \rightarrow \infty} [y_i(t)/x_i(t)] = 2.34$, with $i = 1, 2$.

Chapter 3 Projective synchronisation and its stability criteria

To explain the occurrence of projection synchronisation [Mainieri & Rehacek, 1999], consider a three-dimensional (3-D) partially linear drive system (x_1, x_2, z_x) in polar coordinates

$$\left(\dot{r}_x, \dot{\theta}_x, \dot{z}_x \right) = \left(\frac{1}{r_x} (x_1 \dot{x}_1 + x_2 \dot{x}_2), \frac{\dot{x}_1 x_2 - \dot{x}_2 x_1}{x_1^2 + x_2^2}, \dot{z}_x \right) \quad (3.5)$$

where, $r_x = (x_1^2 + x_2^2)^{1/2}$ and $\tan \theta_x = x_1/x_2$.

The response system is also expressed in the same way. The time evolution of the polar angle θ is given as

$$\dot{\theta} = G(\theta, z) = m_{21} \cos^2 \theta - m_{12} \sin^2 \theta - (m_{11} - m_{22}) \cos \theta \sin \theta. \quad (3.6)$$

Eq. (3.6) holds for both the drive and response systems. Based on Eq. (3.6), the angular difference between the drive and response system evolves according to

$$\dot{\omega} = \dot{\theta}_x - \dot{\theta}_y = -\sin(\theta_x - \theta_y) \left[\cos(\theta_x + \theta_y)(m_{12} + m_{21}) + \sin(\theta_x + \theta_y)(m_{11} - m_{22}) \right]. \quad (3.7)$$

Due to ergodicity, Eq. (3.7) will at one point become small. At that instant, the angular difference can be approximately expressed by using

$$\dot{\omega} = G(\theta_x, z_x) - G(\theta_y, z_x) = G'(\theta_x, z_x) + O(\omega). \quad (3.8)$$

Notice that Eq. (3.8) is an ordinary differential equation. The general solution for such equation will be given as

$$\omega(t) = \omega(0) \exp \left(\int_0^t G'[\theta_x(\zeta)] d\zeta \right). \quad (3.9)$$

From Eq. (3.9), given sufficient large t , the vectors of the drive and response systems will oscillate in phase if

$$\int_0^t G'[\theta_x(\zeta)] d\zeta < 0. \quad (3.10)$$

Chapter 3 Projective synchronisation and its stability criteria

When inequality (3.10) is satisfied, phase synchronisation occurs between the vectors. This is one of the two characteristics observed in projective synchronisation. In order for the cooperative behaviour to be classified as projective synchronisation, the time evolution of the ratio of the radii given in Eq. (3.11) must be evaluated.

$$\begin{aligned} \frac{d}{dt} \frac{r_y}{r_x} &= \frac{r_y}{r_x} \left(\frac{\dot{r}_y}{r_y} - \frac{\dot{r}_x}{r_x} \right) \\ &= \frac{r_y}{r_x} \left[(m_{11} - m_{22}) \sin(\theta_x + \theta_y) \sin(\theta_x - \theta_y) \right. \\ &\quad \left. - (m_{12} + m_{21}) \cos(\theta_x + \theta_y) \sin(\theta_x - \theta_y) \right] \end{aligned} \quad (3.11)$$

Eq. (3.11) is a function of $\dot{r}/r$, which is dependent on the polar angle. Therefore, once inequality (3.10) is satisfied such that

$$\lim_{t \rightarrow \infty} \sin(\theta_x - \theta_y) = 0. \quad (3.12)$$

then

$$|\alpha| = \lim_{t \rightarrow \infty} r_y / r_x. \quad (3.13)$$

which is similar to $\alpha = \lim_{t \rightarrow \infty} \alpha(t) = \lim_{t \rightarrow \infty} \|\mathbf{y}\| / \|\mathbf{x}\|$ given in (3.2). The concurrent occurrence of the limits (3.12) and (3.13) indicates the realisation of projective synchronisation.

3.2 Stability criterion of projective synchronisation in three-dimensional continuous-time systems

In section 3.1, the occurrence of projective synchronisation is explained but the condition under which projective synchronisation will occur remained unknown. In

Chapter 3 Projective synchronisation and its stability criteria

this section the derivation for the stability criterion of projective synchronisation in 3-D continuous-time systems will be provided. The stability criterion of projective synchronisation was first reported in 3-D systems [Li & Xu, 2001] by studying the Lorenz and disk dynamo systems. In the report, it was revealed that projective synchronisation occurs in 3-D systems with Jacobian matrix that has negative trace.

Eq. (3.11) indicates that the time derivative of the ratio of the radii is a function of $\dot{r}/r$ that is purely dependent on the polar angles. To derive the stability criterion for the occurrence of projective synchronisation in 3-D systems, let us first multiply Eq. (3.12) by $-r_x r_y$ on both sides, which give

$$\lim_{t \rightarrow \infty} \left[-r_x r_y \sin(\theta_x - \theta_y) \right] = 0. \quad (3.14)$$

Eq. (3.14) is equivalent to the condition defined by Eq. (3.12) and can be converted to Cartesian coordinates given as

$$\lim_{t \rightarrow \infty} [x_1 y_2 - x_2 y_1] = 0. \quad (3.15)$$

Eq. (3.15) is useful in deriving the stability criterion.

Next the error dynamics given as $e(t) = x_1 y_2 - x_2 y_1$ is constructed. The idea is that if the error dynamics tend to zero then the limit (3.13) will exist and leads to projective synchronisation, i.e. $\lim_{t \rightarrow \infty} \|\alpha \mathbf{x} - \mathbf{y}\| = \mathbf{0}$. This allows the identification of the parameter set that leads the error dynamics to converge to zero, i.e. $\lim_{t \rightarrow \infty} e(t) = 0$.

In what follows, Lyapunov function is applied to derive the global stability criterion for projective synchronisation under any initial condition. Consider a Lyapunov function in the form

$$V(e) = e^2/2. \quad (3.16)$$

According to the Lyapunov stability theory, if function (3.16) satisfies the first condition: $V(e) > 0$ when $e \neq 0$, $V(e) = 0$ when $e = 0$ and the second condition: $\dot{V}(e) < 0$ when $e \neq 0$, $\dot{V}(e) = 0$ when $e = 0$, then the error $e(t)$ will asymptotically tends to zero leading to $\lim_{t \rightarrow \infty} [x_1 y_2 - x_2 y_1] = 0$. Based on the employed Lyapunov function, the first condition is unconditionally satisfied. To identify the setting at which the second condition will be satisfied, the time variation of the Lyapunov function given in Eq. (3.17) must be investigated.

$$\begin{aligned} \dot{V} &= e \dot{e} \\ &= e [m_{11} (x_1 y_2 - x_2 y_1) + m_{22} (x_1 y_2 - x_2 y_1)] \\ &= (m_{11} + m_{22}) e^2. \end{aligned} \quad (3.17)$$

From Eq. (3.17), it becomes obvious that if $m_{11} + m_{22}$, which is trace of the Jacobian matrix, is less than zero, the second condition will be satisfied. This will lead to the realisation of projective synchronisation. Therefore, the stability criterion for the occurrence of projective synchronisation in 3-D systems is given as $m_{11} + m_{22} < 0$.

3.3 Stability criteria of projective synchronisation in continuous-time systems of any dimension

The stability criterion of projective synchronisation in 3-D continuous-time systems laid the foundation for deriving the stability criteria of higher dimensional systems. A general condition for the occurrence of projective synchronisation in any dimension is viewed as important and essential to the theoretical basis of

Chapter 3 Projective synchronisation and its stability criteria

projective synchronisation and its applications. In this section the derivation for the stability criteria of projective synchronisation in continuous-time systems of arbitrary dimension [Xu *et al.*, 2002] will be provided. The derivation will show that for any bounded Jacobian matrix M , projective synchronisation occurs when all the Lyapunov exponents are nonpositive. Furthermore, two special cases are investigated here, namely systems with Jacobian matrix M that is symmetric with $m_{ik} = m_{ki}$ and systems with Jacobian matrix M that is skew-symmetric with $m_{ik} = -m_{ki}$.

To begin the derivation, let the proportional relationship of the drive and response system under projective synchronisation be stated as

$$\lim_{t \rightarrow \infty} \|\alpha \mathbf{x} - \mathbf{y}\| = 0. \quad (3.18)$$

The state vectors are given as $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and $\mathbf{y} = [y_1, y_2, \dots, y_n]^T$. The variable $\alpha(t)$ is referred to as the scaling factor that converges to a constant value at the limit. This constant value that defines the proportional relation between $\mathbf{x}$ and $\mathbf{y}$ at the limit can be expressed by

$$\alpha \mathbf{x} = \mathbf{y}. \quad (3.19)$$

Eq.(3.19) indicates that when projective synchronisation occurs, all the corresponding state variables of the drive and response systems synchronised up to a common scaling factor.

Here the Lyapunov stability theory is employed to derive stability criteria that are globally stable. To construct a Lyapunov function, the error vector $\mathbf{e}_i$ must first be defined. This error vector must tend to zero for projective synchronisation to

$$V(e) = e^2/2. \quad (3.16)$$

According to the Lyapunov stability theory, if function (3.16) satisfies the first condition: $V(e) > 0$ when $e \neq 0$, $V(e) = 0$ when $e = 0$ and the second condition: $\dot{V}(e) < 0$ when $e \neq 0$, $\dot{V}(e) = 0$ when $e = 0$, then the error $e(t)$ will asymptotically tends to zero leading to $\lim_{t \rightarrow \infty} [x_1 y_2 - x_2 y_1] = 0$. Based on the employed Lyapunov function, the first condition is unconditionally satisfied. To identify the setting at which the second condition will be satisfied, the time variation of the Lyapunov function given in Eq. (3.17) must be investigated.

$$\begin{aligned} \dot{V} &= e\dot{e} \\ &= e[m_{11}(x_1 y_2 - x_2 y_1) + m_{22}(x_1 y_2 - x_2 y_1)] \\ &= (m_{11} + m_{22})e^2. \end{aligned} \quad (3.17)$$

From Eq. (3.17), it becomes obvious that if $m_{11} + m_{22}$, which is trace of the Jacobian matrix, is less than zero, the second condition will be satisfied. This will lead to the realisation of projective synchronisation. Therefore, the stability criterion for the occurrence of projective synchronisation in 3-D systems is given as $q1 + m2 < 0$.

3.3 Stability criteria of projective synchronisation in continuous-time systems of any dimension

The stability criterion of projective synchronisation in 3-D continuous-time systems laid the foundation for deriving the stability criteria of higher dimensional systems. A general condition for the occurrence of projective synchronisation in any dimension is viewed as important and essential to the theoretical basis of

Chapter 3 Projective synchronisation and its stability criteria

Let $\mathbf{m}_i$ represents the i th row of $\mathbf{M}$. By Substituting $\dot{x}_i = \mathbf{m}_i \mathbf{x}$ and $\dot{y}_i = \mathbf{m}_i \mathbf{y}$ into Eq. (3.24) and rewriting the equation in the matrix form will give

$$\begin{aligned}\dot{\mathbf{e}}_i &= ((\mathbf{m}_i \mathbf{x}) \mathbf{y} - (\mathbf{m}_i \mathbf{y}) \mathbf{x}) + \mathbf{M} (x_i \mathbf{y} - y_i \mathbf{x}) \\ &= \sum_{k=1}^n m_{ik} \mathbf{e}_k + \mathbf{M} \mathbf{e}_i.\end{aligned}\quad (3.25)$$

Substituting (3.25) into (3.23) gives

$$\begin{aligned}\dot{V}(\mathbf{e}_i) &= \sum_{i=1}^n \mathbf{e}_i^T \left(\sum_{k=1}^n m_{ik} \mathbf{e}_k + \mathbf{M} \mathbf{e}_i \right) \\ &= \sum_{i=1}^n \sum_{k=1}^n m_{ik} \mathbf{e}_i^T \mathbf{e}_k + \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{M} \mathbf{e}_i).\end{aligned}\quad (3.26)$$

Noting that $\mathbf{e}_i = [e_{i1}, e_{i2}, \dots, e_{in}]^T$ and $\mathbf{e}_i = -[e_{1i}, e_{2i}, \dots, e_{ni}]^T$ where $e_{ik} = x_i y_k - x_k y_i$

and $e_{ik} = -e_{ki}$, the relation $\sum_{i=1}^n \sum_{k=1}^n m_{ik} \mathbf{e}_i^T \mathbf{e}_k = \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{M} \mathbf{e}_i)$ can be utilised so that

$$\dot{V}(\mathbf{e}_i) = 2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{M} \mathbf{e}_i). \quad (3.27)$$

By equating $\dot{V}(\mathbf{e}_i) = \sum_{i=1}^n \mathbf{e}_i^T \dot{\mathbf{e}}_i$ from (3.23) and $\dot{V}(\mathbf{e}_i) = 2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{M} \mathbf{e}_i)$ from (3.27), a useful relationship given in (3.28) is obtained.

$$\sum_{i=1}^n \mathbf{e}_i^T (\dot{\mathbf{e}}_i - 2\mathbf{M} \mathbf{e}_i) = 0. \quad (3.28)$$

Eq. (3.28) allows a variational equation, $\dot{\mathbf{e}}_i = 2\mathbf{M} \mathbf{e}_i$, that is a time-dependent linear system to be modelled. Assuming that the coupling variable z_x is bounded so that $\mathbf{M}$ is bounded all the time, then the stability of the null solution $\lim_{t \rightarrow \infty} \mathbf{e}_i = \mathbf{0}$ is dependent of the Lyapunov exponent of the linear system $\dot{\mathbf{e}}_i = 2\mathbf{M} \mathbf{e}_i$ that is equivalent to the variational equation $\dot{\mathbf{x}}_i = \mathbf{M} \mathbf{x}_i$ in terms of the stability at the

Chapter 3 Projective synchronisation and its stability criteria

origin. In general, a null solution is uniformly asymptotically stable if the Lyapunov exponents of the variational equation are nonpositive.

Therefore, the stability criterion of projective synchronisation in continuous-time systems requires that all Lyapunov exponents of a bounded Jacobian matrix $\mathbf{M}$ to be nonpositive.

Two special cases are further investigated here, namely systems with symmetrical Jacobian matrix $\mathbf{M}$, $m_{ik} = m_{ki}$ and systems with skew-symmetrical Jacobian matrix $\mathbf{M}$, $m_{ik} = -m_{ki}$.

The stability criteria require that the quadratic form of (3.27) to be negative, expressed by

$$2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{M} \mathbf{e}_i) < 0 \quad \text{for } \mathbf{e}_i \neq \mathbf{0}. \quad (3.29)$$

Using inequality (3.29), the stability criteria of the two special cases with systems of arbitrary dimension can be derived.

In the first special case, for a symmetrical $\mathbf{M}$, there must exist a non-singular orthogonal matrix $\mathbf{P}$ with the properties $\mathbf{P}^T = \mathbf{P}^{-1}$ and $\mathbf{P}^T \mathbf{M} \mathbf{P} = \mathbf{\Lambda}$, where $\mathbf{\Lambda}$ is a diagonal matrix and its elements are the eigenvalues λ_k of $\mathbf{M}$. By introducing the orthogonal matrix $\mathbf{P}$ into Eq. (3.27), the quadratic form can be expressed as

$$\sum_{i=1}^n \mathbf{e}_i^T \mathbf{M} \mathbf{e}_i = \sum_{i=1}^n \mathbf{c}_i^T \mathbf{\Lambda} \mathbf{c}_i = \sum_{i=1}^n \sum_{k=1}^n \lambda_k c_{ik}^2 \quad \text{where } \mathbf{c}_i = \mathbf{P}^T \mathbf{e}_i \text{ is the vector of principal}$$

coordinates. Given that the stability condition (3.23) requires $\sum_{k=1}^n \lambda_k \sum_{i=1}^n c_{ik}^2 < 0$ for

$c_{ik} \neq 0$. Therefore, projective synchronisation occurs in systems with symmetrical Jacobian matrix if the summation of the eigenvalues is negative.

In the special second case, consider a skew-symmetrical Jacobian matrix $\mathbf{M}$ with property of $m_{ik} = -m_{ki}$ where $i \neq k$ and $i, k = 1, 2, \dots, n$. The matrix $\mathbf{M}$ can be decomposed as $\mathbf{M} = \mathbf{A} + \mathbf{B}$, where $\mathbf{A}$ is a diagonal matrix $\text{diag}(m_{11}, m_{22}, \dots, m_{nn})$ that is symmetric and $\mathbf{B}$ is skew-symmetrical matrix with zeros on the main diagonal.

From here, Eq. (3.27) can be expressed as $\dot{V}(\mathbf{e}_i) = 2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{A} \mathbf{e}_i) + 2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{B} \mathbf{e}_i)$.

Since for the skew-symmetric $\mathbf{B}$, $m_{ik} \mathbf{e}_i^T \mathbf{e}_k + m_{ki} \mathbf{e}_k^T \mathbf{e}_i = 0$ for $i \neq k$ and $i, k = 1, 2, \dots, n$, therefore, $\sum_{i=1}^n (\mathbf{e}_i^T \mathbf{B} \mathbf{e}_i) = 0$. A simple form is thus derived for the stability condition given as

$$\dot{V}(\mathbf{e}_i) = 2 \sum_{i=1}^n (\mathbf{e}_i^T \mathbf{A} \mathbf{e}_i) = 2 \sum_{i=1}^n m_{ii} \mathbf{e}_i^T \mathbf{e}_i = 2 \sum_{i=1}^n m_{ii} \sum_{k=1}^n e_{ik}^2 < 0. \quad (3.30)$$

Recall that $e_{ik} = -e_{ki}$ and $e_{ii} = 0$, a simple stability criterion for the occurrence of projective synchronisation in systems with skew-symmetrical matrix can be derived from inequality (3.30), that is

$$m_{ii} + m_{kk} < 0, \quad i \neq k, \quad i, k = 1, 2, \dots, n. \quad (3.31)$$

Inequality (3.31) indicates that projective synchronisation occurs in systems with skew-symmetrical Jacobian matrix if the summation of any two diagonal elements of $\mathbf{M}$ is negative.

3.4 Stability criterion of projective synchronisation in discrete-time systems

This section investigates the mechanism of projective synchronisation in discrete-time systems of arbitrary dimensions and provides the condition for its occurrence. It is found that determinant of the multiplication of Jacobian matrices of the system in uncoupled form tends to zero when projective synchronisation occurs [Xu *et al.*, 2004].

Many dynamical systems in physical sciences [Steigilitz, 1974], economics [Shone, 2001], biological and social sciences [Beltrami, 1993] are modelled by difference equations. The governing law of a discrete-time system can be expressed by a map $\mathbf{w}_{(k+1)} = F(\mathbf{w}_{(k)})$, $\mathbf{w}_{(k)} \in \mathfrak{R}^{n+1}$, and k in bracket is an iteration index. For a partially linear discrete-time system, the decomposed form is given as

$$\begin{aligned}\mathbf{x}_{(k+1)} &= \mathbf{M}(z_{x,(k)}) \cdot \mathbf{x}_{(k)}, \\ z_{x,(k+1)} &= H(\mathbf{x}_{(k)}, z_{x,(k)}).\end{aligned}\tag{3.32}$$

The coupled form of two partially linear discrete-time systems is expressed by,

$$\left. \begin{aligned}\mathbf{x}_{(k+1)} &= \mathbf{M}(z_{x,(k)}) \cdot \mathbf{x}_{(k)} \\ z_{x,(k+1)} &= H(\mathbf{x}_{(k)}, z_{x,(k)})\end{aligned} \right\} \text{Drive System,} \tag{3.33}$$

$$\mathbf{y}_{(k+1)} = \mathbf{M}(z_{x,(k)}) \cdot \mathbf{y}_{(k)} \Big\} \text{Response System.}$$

The state vectors of the drive and response systems are given as $\mathbf{x}_{(k)} = [x_{1,(k)}, x_{2,(k)}, \dots, x_{n,(k)}]^T$ and $\mathbf{y}_{(k)} = [y_{1,(k)}, y_{2,(k)}, \dots, y_{n,(k)}]^T$ respectively. The response system is driven by the drive system through the Jacobian matrix $\mathbf{M}(z_{x,(k)}) \in \mathfrak{R}^{n \times n}$ that is dependent on the state variable $z_{x,(k)}$. The function

Chapter 3 Projective synchronisation and its stability criteria

$H(\mathbf{x}_{(k)}, z_{x,(k)})$ is governed by the drive system. The subscript k in bracket denotes the number of iterations.

With respect to the characteristic condition (3.18), $\lim_{t \rightarrow \infty} \|\alpha \mathbf{x} - \mathbf{y}\| = 0$, of projective synchronisation in continuous-time systems, the condition for projective synchronisation in discrete-time systems is given as $\lim_{k \rightarrow \infty} \|\alpha \mathbf{x}_{(k)} - \mathbf{y}_{(k)}\| = 0$. This reveals that ultimately the state vectors $\mathbf{x}_{(k)}$ and $\mathbf{y}_{(k)}$ must be linearly dependent as the numbers of iterations increases. Given n number of vectors $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n$, for the nonzero real constants $\alpha_1, \dots, \alpha_n$, if the following relation holds

$$\alpha_1 \mathbf{q}_1 + \alpha_2 \mathbf{q}_2, \dots, + \alpha_n \mathbf{q}_n = \mathbf{0}, \quad \text{for all } \alpha_i \neq 0 \text{ and } i = 1, 2, \dots, n. \quad (3.34)$$

then the vectors $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n$ are linearly dependent. This idea of linear dependence can be used to derive the criterion of projective synchronisation for the discrete-time systems.

Consider the two time-varying state vectors $\mathbf{x}_{(k)}$ and $\mathbf{y}_{(k)}$. The condition of the linear dependence (3.34) between the two state vectors is

$$\alpha_1 \mathbf{x}_{(k)} + \alpha_2 \mathbf{y}_{(k)} = \mathbf{0}, \quad \alpha_1, \alpha_2 \neq 0. \quad (3.35)$$

Eq. (3.35) can be written as $\alpha_1 \mathbf{M}(z_{x,(k-1)}) \mathbf{x}_{(k-1)} + \alpha_2 \mathbf{M}(z_{x,(k-1)}) \mathbf{y}_{(k-1)} = \mathbf{0}$, which can be further expanded as $\mathbf{M}(z_{x,(k-1)}) \mathbf{M}(z_{x,(k-2)}) (\alpha_1 \mathbf{x}_{(k-2)} + \alpha_2 \mathbf{y}_{(k-2)}) = \mathbf{0}$. Eq. (3.35) can eventually be expressed by

$$\mathbf{M}^{(k)}(z_{x,(0)}) (\alpha_1 \mathbf{x}_{(0)} + \alpha_2 \mathbf{y}_{(0)}) = \mathbf{0}. \quad (3.36)$$

Chapter 3 Projective synchronisation and its stability criteria

The matrix $\mathbf{M}^{(k)}(z_{x,(0)}) = \prod_{i=1}^k \mathbf{M}(z_{x,(i-1)}) = \mathbf{M}(z_{x,(k-1)})\mathbf{M}(z_{x,(k-2)})\dots\mathbf{M}(z_{x,(0)})$. From

(3.36), it can be noted that in order to satisfy condition (3.35) with $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$, there are two possible solutions, namely:

$$(\alpha_1 \mathbf{x}_{(0)} + \alpha_2 \mathbf{y}_{(0)}) = \mathbf{0} \text{ and } \det|\mathbf{M}^{(k)}(z_{x,(0)})| = 0. \quad (3.37)$$

where $\det|\bullet|$ denotes the determinant of a matrix. Since the initial conditions $\mathbf{x}_{(0)}$ and $\mathbf{y}_{(0)}$ can be taken arbitrarily, therefore in general $(\alpha_1 \mathbf{x}_{(0)} + \alpha_2 \mathbf{y}_{(0)}) \neq \mathbf{0}$. As a result, linear dependence requires the necessary condition $\det|\mathbf{M}^{(k)}(z_{x,(0)})| = 0$. Let

$\zeta_{(k)}$ denote $\det|\mathbf{M}^{(k)}(z_{x,(0)})|$ given as

$$\begin{aligned} \zeta_{(k)} &= \det\left|\prod_{i=1}^k \mathbf{M}(z_{x,(i-1)})\right| \\ &= \det|\mathbf{M}(z_{x,(k-1)})| \times \det|\mathbf{M}(z_{x,(k-2)})| \cdots \det|\mathbf{M}(z_{x,(0)})|. \end{aligned} \quad (3.38)$$

From Eq. (3.38), it becomes obvious that there are two possibilities that could lead to the condition $\zeta_{(k)} = 0$. Firstly, a special case where

$$\det|\mathbf{M}(z_{x,(i)})| = 0, \quad \text{for any specific } i. \quad (3.39)$$

And secondly for more general cases, projective synchronisation occurs if

$$\zeta_{(k)} = \lim_{k \rightarrow \infty} \prod_{i=1}^k \det|\mathbf{M}(z_{x,(i-1)})| = 0. \quad (3.40)$$

Either condition (3.39) or (3.40) leads to $\alpha_1 \mathbf{u}_{x,(k)} + \alpha_2 \mathbf{u}_{y,(k)} = \mathbf{0}$ defined by (3.35)

for any selected initial conditions. Thus condition (3.35) can be rewritten as

$\alpha \mathbf{x}_{(k)} - \mathbf{y}_{(k)} = \mathbf{0}$, where $\alpha = -\alpha_1/\alpha_2$ is the scaling factor of projective synchronisation.

Chapter 3 Projective synchronisation and its stability criteria

Criterion (3.40) is the necessary condition that allows us to check the possibility of projective synchronisation from the original uncoupled system (3.32). In the earlier report [Gonzalez-Miranda, 1996], the author observed from numerical simulations that projective synchronisation occurs when the conditional Lyapunov exponent of the Jacobian matrix is null. The necessary condition (3.40), reported in this thesis, theoretically supports this numerical observation [Gonzalez-Miranda, 1996]. Conditional Lyapunov exponents are in fact the eigenvalues of the matrix $\lim_{k \rightarrow \infty} \prod_{i=1}^k \mathbf{M}(z_{x,(i-1)})$. A null conditional Lyapunov exponent actually corresponds to condition (3.40). This is so because the product of the eigenvalues of a matrix is equal to the determinant of the matrix, which implies that a null eigenvalue must correspond to a determinant being zero. From the special condition $\det|\mathbf{M}(z_{x,(i)})| = 0$ we can always obtain an algebraic equation $g(z_x^*) = 0$ by which a critical solution z_x^* can be found for the variable $z_{x,(i)}$ such that when $z_{x,(i)} = z_x^*$, projective synchronisation occurs according to the criterion (3.39). For general cases, projective synchronisation does not occur with $z_{x,(i)} = z_x^*$ but rather with a number of determinants being less than unity. As a result, the product of the determinants defined by (3.40) tends to zero. This feature can be checked directly by computing $\zeta_{(k)}$ numerically.

Chapter 3 Projective synchronisation and its stability criteria

A numerical example is provided here to validate the necessary condition of projective synchronisation in discrete-time systems. In the numerical experiment, the relation between the formation of projective synchronisation and the variation of $\zeta_{(k)}$ will be discussed.

In the following example, the discrete-time system is three-dimensional. The coupled form is expressed as

$$\left. \begin{aligned} \mathbf{x}_{(k+1)} &= \mathbf{M}(z_{x,(k)}) \cdot \mathbf{x}_{(k)} \\ z_{x,(k+1)} &= 0.3x_{1,(k)}x_{2,(k)} - 0.3z_{x,(k)} \end{aligned} \right\} \text{Drive System,} \quad (3.41)$$

$$\mathbf{y}_{(k+1)} = \mathbf{M}(z_{x,(k)}) \cdot \mathbf{y}_{(k)} \} \text{Response System,}$$

$$\text{with } \mathbf{M}(z_{x,(k)}) = \begin{bmatrix} 0.28(6 - z_{x,(k)}) & -0.1 \\ 0.3 & 0.35(3 - z_{x,(k)}) \end{bmatrix}$$

and the state vectors given as, $\mathbf{x}_{(k)} = [x_{1,(k)}, x_{2,(k)}]^T$ and $\mathbf{y}_{(k)} = [y_{1,(k)}, y_{2,(k)}]^T$

Fig. 3.2(a) and (b) show the attractors of the drive and response systems (3.41) respectively with a scaling factor of $\alpha = 1.257$, corrected to four significant figures. Fig. 3.3 (a) shows that $x_{1,(k)}$ and $y_{1,(k)}$ evolve in time under proportional relationship. Fig. 3.3(b) and (c) display the variation of the determinant and $\zeta_{(k)}$ against iteration numbers respectively. The value of $\zeta_{(k)}$ is amplified when $|\det \mathbf{M}(z_{m,(i)})| > 1$ and depressed when $|\det \mathbf{M}(z_{m,(j)})| < 1$. As shown in Fig. 3.3(c), the values of $\zeta_{(k)}$ becomes infinitely small ($\zeta_{(10)} = -0.06$, $\zeta_{(20)} = 0.2 \times 10^{-3}$, $\zeta_{(40)} = -1.4 \times 10^{-11}$) as $k \rightarrow \infty$. Projective synchronisation becomes observable approximately at the 30th iteration with $\zeta_{(30)} = 1.4 \times 10^{-7}$ and the scaling factor stabilises to a constant at $\alpha = 1.267$, corrected to four significant figures, as shown

in Fig. 3.3(d). This example verified the stability criterion of projective synchronisation as stated in (3.40).

Fig. 3.2. Synchronised chaotic attractors of the coupled system (3.41). (a) The attractor of the drive system. (b) The attractor of the response system.

Fig. 3.3. (a) Variation of $x_{1,k}$ (solid line) and $y_{1,k}$ (dashed line) of the system (3.41). (b) The variation of the determinants $\det \mathbf{M}(z_{x,k})$. (c) The variation of $\zeta(k)$. (d) The variation of the scaling factor $\alpha(k)$.

Chapter 4

Control of projective synchronisation

This chapter will introduce control algorithms that are developed to direct the ultimate state of projective synchronisation. The development of control algorithms for projective synchronisation is an important undertaking as the ability to manipulate the scaling factor will be an interesting theoretical breakthrough that may lead to useful applications such as digital communication, secure communication and vibration control.

The first attempt to manipulate the ultimate state of projective synchronisation is carried out on three-dimensional continuous-time systems [Xu, 2001]. The control algorithm requires the drive and response systems to reach phase synchronisation before control can be inputted to direct the scaling factor. This requirement is later on seen as a restriction to useful applications of projective synchronisation. Subsequently, another control algorithm is developed [Xu *et al.*, 2001] to eliminate this restriction. However, this development is only available to three-dimensional systems.

Although the earlier control algorithms have their limitations, they are instrumental to the development of control algorithms for arbitrary dimensional systems [Xu & Chee, 2002] and nonpartially linear systems [Xu & Li, 2002] introduced in this chapter. Besides these, control algorithms for discrete-time

systems [Chee & Xu, 2003] and full state projective synchronisation of continuous-time systems [Wen & Xu, 2004] will also be introduced.

4.1 Manipulating the ultimate state of projective synchronisation in continuous-time systems

The ultimate state of projective synchronisation is unpredictable. The theoretical breakthrough in directing projective synchronisation to any desired scaling factor will lead projective synchronisation to real world applications. This section will introduce a new control algorithm that can be used to manipulate the ultimate state of projective synchronisation in continuous-time systems of any dimension with only a small input. This is an important development as it eliminates all the limitations that restrict the earlier developments [Xu, 2001; Xu *et al.*, 2001] from practical applications.

Consider a coupled partially linear system of any dimension with control given as

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \boldsymbol{\xi} \\ \dot{z}_x &= h(\mathbf{x}, z_x) \end{aligned} \right\} \text{Drive System,} \quad (4.1)$$

$$\dot{\mathbf{y}} = \mathbf{M}(z_x) \cdot \mathbf{y} \} \text{Response System,}$$

where $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and $\mathbf{y} = [y_1, y_2, \dots, y_n]^T$ are the state vectors of the drive and response systems respectively. The matrix $\mathbf{M}(z_x) \in \mathbb{R}^{n \times n}$ contains the variable z_x that is governed by the drive system and relates nonlinearly with other variables. The response system is driven by the drive system through z_x . The column vector $\boldsymbol{\xi} = [\xi_1, \xi_2, \dots, \xi_n]^T$ is the control vector.

The intention is to design the control vector ξ with global stability to direct the ultimate state of projective synchronisation to any desired state from any initial conditions. Therefore Lyapunov stability theory is employed here for this purpose.

In order to construct a proper Lyapunov function, it is necessary to construct an error dynamics of projective synchronisation first. Therefore, consider the error vector given as

$$\mathbf{e} = (e_1, e_2, \dots, e_n)^T = \alpha^* \mathbf{x} - \mathbf{y} \quad (4.2)$$

where the error $e_i = \alpha^* x_i - y_i$ for $i = 1, 2, \dots, n$. The constant α^* is the desired scaling factor. If Eq. (4.2) tends to zero then projective synchronisation takes place with the desired scaling factor expressed by $\lim_{t \rightarrow \infty} [\alpha(t)] = \lim_{t \rightarrow \infty} \|\mathbf{y}\|/\|\mathbf{x}\| = \alpha^*$.

Thus consider a Lyapunov function in the form

$$V(\mathbf{e}) = \frac{1}{2} \sum_{i=1}^n e_i^2. \quad (4.3)$$

According to the Lyapunov stability theory, if the function (4.3) satisfies the first condition: $V(\mathbf{e}) > 0$ when $\mathbf{e} \neq 0$, $V(\mathbf{e}) = 0$ when $\mathbf{e} = 0$, and the second condition: $\dot{V}(\mathbf{e}) < 0$ when $\mathbf{e} \neq 0$, $\dot{V}(\mathbf{e}) = 0$ when $\mathbf{e} = 0$, then the error vector $\mathbf{e}(t)$ asymptotically tends to zero, leading to $\lim_{t \rightarrow \infty} \|\alpha^* \mathbf{x} - \mathbf{y}\| = 0$. Surely, the employed Lyapunov function (4.3) satisfies the first condition. For the second condition, the time derivation of Eq. (4.3) must be negative given as

$$\dot{V}(\mathbf{e}) = \sum_{i=1}^n e_i \dot{e}_i < 0 \text{ for } \mathbf{e} \neq 0. \quad (4.4)$$

Inserting $\dot{e}_i = \alpha^* \dot{x}_i - \dot{y}_i$ into inequality (4.4) gives

$$\dot{V}(\mathbf{e}) = \sum_{i=1}^n e_i (\alpha^* \dot{x}_i - \dot{y}_i) < 0 \text{ for } \mathbf{e} \neq 0 \quad (4.5)$$

Substituting $\dot{x}_i = \mathbf{m}_i \mathbf{x} + \xi_i$ and $\dot{y}_i = \mathbf{m}_i \mathbf{y}$ into (4.5), where $\mathbf{m}_i$ is the i th row of the Jacobian matrix $\mathbf{M}$, the condition $\dot{V}(\mathbf{e}) = \sum_{i=1}^n [e_i (\alpha^* (\mathbf{m}_i \mathbf{x} + \xi_i) - \mathbf{m}_i \mathbf{y})] < 0$ is obtained, which can be rearranged into the form

$$\dot{V}(\mathbf{e}) = \sum_{i=1}^n [e_i \alpha^* \xi_i + e_i \mathbf{m}_i \mathbf{e}] < 0, \text{ for } \mathbf{e} \neq 0. \quad (4.6)$$

The inequality (4.6) carries the control functions ξ_i . If the control functions are selected in such a way that the condition (4.6) is satisfied then the control will bring about $\lim_{t \rightarrow \infty} \mathbf{e}(t) = \mathbf{0}$ and consequently $\lim_{t \rightarrow \infty} \|\alpha^* \mathbf{x} - \mathbf{y}\| = 0$. Ultimately projective synchronisation is realised with the specified scaling factor α^* .

To derive the control functions, we convert the condition (4.6) into an equality by introducing a slack vector, $\mathbf{K} = (K_1, K_2, \dots, K_n)$. A slack variable is defined as

$$K_i = \kappa_i e_i e_i \text{ for } i=1, 2, \dots, n. \quad (4.7)$$

where $\kappa_i > 0$ is called the *slack constant*, which can be any real positive value. The value of κ_i affects the convergence rate of the control, which will be discussed later in the numerical example.

By adding the non-negative slack variable (4.7) into the left side of inequality (4.6) convert (4.6) into an equality form given as

$$\begin{aligned} & e_1 \alpha^* \xi_1 + e_1 \mathbf{m}_1 \mathbf{e} + \kappa_1 e_1 e_1 + \\ & e_2 \alpha^* \xi_2 + e_2 \mathbf{m}_2 \mathbf{e} + \kappa_2 e_2 e_2 + \\ & \dots + \\ & e_n \alpha^* \xi_n + e_n \mathbf{m}_n \mathbf{e} + \kappa_n e_n e_n = 0. \end{aligned} \quad (4.8)$$

A possible solution of the condition (4.8) is that each component corresponding to error e_i can be set to zero, i.e.,

$$\begin{aligned} e_1(\alpha^* \xi_1 + \mathbf{m}_1 \mathbf{e} + \kappa_1 e_1) &= 0 \\ e_2(\alpha^* \xi_2 + \mathbf{m}_2 \mathbf{e} + \kappa_2 e_2) &= 0 \\ \vdots \\ e_n(\alpha^* \xi_n + \mathbf{m}_n \mathbf{e} + \kappa_n e_n) &= 0 \end{aligned} \quad (4.9)$$

Finally the control functions can be formulated as

$$\xi_i = -[\mathbf{m}_i \mathbf{e} + \kappa_i e_i] / \alpha^*, \quad \text{for } i=1,2,\dots,n. \quad (4.10)$$

Note that the control function (4.10) contains the error terms. This means that the maintenance of controlled projective synchronisation requires only a tiny control input, as the errors in the control functions (4.10) tend to zero after synchronisation is realised. As a result, the controlled drive system preserves the dynamical characteristic of the original systems. In what follows, the control algorithm will be applied to a high-dimensional chaotic system to verify its effectiveness. The robustness of the control algorithm under the effect of noise will be discussed in Chapter 6.

In this numerical example, the effectiveness of the control algorithm in bringing about a sharp change in the scaling factor will be demonstrated. At the same time, the effects on the selection of the slack constants will be discussed. The control algorithm is applied to a nineteen-dimensional coupled chaotic system. In the coupled system, the ten-dimensional drive system drives the response system through the nonlinear variable z_x . The coupled chaotic system is given as,

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \xi \\ \dot{z}_x &= 3x_1x_3 - 7z_x \end{aligned} \right\} \text{Drive System,} \quad (4.11)$$

$$\dot{\mathbf{y}} = \mathbf{M}(z_x) \cdot \mathbf{y} \text{ Response System,}$$

with a 9 x 9 Jacobian matrix

$$\mathbf{M}(z_x) = \begin{bmatrix} -14 & 8 & -6 & 1 & 2 & 3 & 4 & 5 & 6 \\ -8 & 12 & -(8+3z_x) & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & (8+3z_x) & -22 & 3 & 4 & 5 & 6 & 7 & 8 \\ -1 & -2 & -3 & -13 & 5 & 6 & 7 & 8 & (9+7z_x) \\ -2 & -3 & -4 & -5 & -14 & 7 & 8 & 9 & 10 \\ -3 & -4 & -5 & -6 & -7 & -15 & 9 & 10 & 11 \\ -4 & -5 & -6 & -7 & -8 & -9 & -16 & 11 & 12 \\ -5 & -6 & -7 & -8 & -9 & -10 & -11 & -17 & 13 \\ -6 & -7 & -8 & -(9+7z_x) & -10 & -11 & -12 & -13 & -12 \end{bmatrix}$$

Fig. 4.1(a) shows the chaotic attractors of the drive and response systems in a three-dimension sub-space (x_4, x_5, x_6) with a scaling factor of $\lim_{t \rightarrow \infty} \alpha(t) = 9.4$. The evolution of the drive system is traced by blue solid line while the evolution of the response system is traced by black dashed line.

The control experiment is repeated three times using different values of slack constants, with $\kappa_i = 2$, $\kappa_i = 4$ and $\kappa_i = 10$ for $i = 1, 2, \dots, 9$. In each control experiment, the scaling factor will be directed first to an initial value of $\alpha^* = 5$ and then redirected to a new desired value of $\alpha^* = 10$. Each experiment runs continuously for 10 time-units in which each specified scaling factor lasts for 5 time-units. The initial conditions and parameters are the same in all the experiments.

The numerical results of each experiment are shown in Fig. 4.1. In Fig. 4.1(b), the control with slack constant $\kappa_i = 2$ directs the scaling factor to $\alpha^* = 5$ after a transient period of 3 time-units. At $t = 5$, the desired scaling factor is adjusted to $\alpha^* = 10$. Large fluctuation is observed during $t = 5 \sim 7$ before the scaling factor settles down to the new desired value. In Fig. 4.1(c), the control is assigned with the slack constant of $\kappa_i = 4$. The control algorithm directs the scaling factor to the different desired values with a shorter transient period and smaller fluctuation. In Fig. 4.1(d), with $\kappa_i = 10$, an even smoother transition from one desired scaling factor to another is observed.

Fig. 4.1. (a) A view of the synchronised chaotic attractors of the coupled system (4.11). The drive system is represent by blue solid line and the response system is represented by dashed line. (b)-(d) The time variation of the scaling factors with slack constants of $\kappa_i = 2$, $\kappa_i = 4$ and $\kappa_i = 10$ respectively. Insets show the zoom-in of the transient period. (e) The time variation of the errors of projective synchronisation. (f) The time variation of the control inputs.

The three experiments show that in directing the scaling factor to a target value, the transient period is reduced with an increase of the value of the slack constant. In another words, a larger slack constant would lead to the faster convergence rate in the control. Fig. 4.1(e) illustrates the time variation of the error $\log|e_4|$ in each of the three controls. It can be seen that the error decreases at different rates with different slack constants used. The larger slack constant leads to faster convergence rate in the control and smaller error in projective synchronisation. Fig. 4.1(f) shows the control inputs corresponding to the different slack constants used. The figure shows that the required control input is relatively smaller in the control with the larger slack constant.

4.2 Manipulating the ultimate state of projective synchronisation in discrete-time systems

This section will introduce a new control algorithm that can be employed to regulate the ultimate state of projective synchronisation in discrete-time systems [Chee & Xu, 2003]. The control algorithm is constructed from the Schur-Chon stability criterion [LaSalle, 1986]. By incorporating the control algorithm into the coupled discrete-time system, the ultimate state of projective synchronisation can be directed to any desired scaling factor.

Consider a coupled discrete-time system given as,

$$\left. \begin{aligned} \mathbf{x}_{(k+1)} &= \mathbf{M}(z_{x,(k)}) \cdot \mathbf{x}_{(k)} \\ z_{x,(k+1)} &= H(\mathbf{x}_{(k)}, z_{x,(k)}) \end{aligned} \right\} \text{Drive System,} \quad (4.12)$$

$$\mathbf{y}_{(k+1)} = \mathbf{M}(z_{x,(k)}) \cdot \mathbf{y}_{(k)} \left. \right\} \text{Response System.}$$

Here $\mathbf{x}_{(k)}$ is the state vector of the drive system defined by $\mathbf{x}_{(k)} = [x_{1,(k)}, x_{2,(k)}, \dots, x_{n,(k)}]^T$ and $\mathbf{y}_{(k)}$ is the state vector of the response system defined by $\mathbf{y}_{(k)} = [y_{1,(k)}, y_{2,(k)}, \dots, y_{n,(k)}]^T$. The response system is driven by the drive system through the Jacobian matrix $\mathbf{M}(z_{x,(k)}) \in \mathbb{R}^{n \times n}$ that is dependent on the state variable $z_{x,(k)}$. The function $H(\mathbf{x}_{(k)}, z_{x,(k)})$ is governed by the drive system. The subscript k in bracket denotes the number of iterations. For subsequent discussion, the abbreviation $\mathbf{M}_{(k)}$ will be used interchangeably with $\mathbf{M}(z_{(k)})$ for simplicity.

When projective synchronisation occurs, there exists a relationship between the states of the drive and response systems, given as $\lim_{k \rightarrow \infty} \|\alpha \mathbf{x}_{(k)} - \mathbf{y}_{(k)}\| = \mathbf{0}$ where the scaling factor α is defined by the limit of the state ratio $\alpha = \lim_{k \rightarrow \infty} \alpha_{(k)} = \lim_{k \rightarrow \infty} \|\mathbf{y}_{(k)}\| / \|\mathbf{x}_{(k)}\|$.

Here $\|\bullet\|$ denotes a vector norm (L_2 -norm). The scaling factor characterises the ultimate proportional relation between the states of the drive and response systems, which is unpredictable. Therefore, a control algorithm is introduced in this thesis to direct the scaling factor such that the outcome of the synchronisation can be managed. Consider a coupled system with a control vector $\boldsymbol{\xi} = [\xi_1, \xi_2, \dots, \xi_n]^T$ attached to the response system given in (4.13),

$$\left. \begin{aligned} \mathbf{x}_{(k+1)} &= \mathbf{M}_{(k)} \cdot \mathbf{x}_{(k)} \\ z_{x,(k+1)} &= H(\mathbf{x}_{(k)}, z_{x,(k)}) \end{aligned} \right\} \text{Drive System,} \quad (4.13)$$

$$\mathbf{y}_{(k+1)} = \mathbf{M}_{(k)} \cdot \mathbf{y}_{(k)} + \boldsymbol{\xi}_{(k)} \Big\} \text{Response System.}$$

The design approach for the control vector is similar regardless of whether it is attached to the drive or response system. The placement of the control vector depends only on its application.

In order to direct the ultimate state of projective synchronisation to any desired scaling factor α^* through the control vector $\xi_{(k)}$, a dynamic error vector must first be constructed. Consider the error vector given as

$$\mathbf{e}_{(k+1)} = \alpha^* \mathbf{x}_{(k+1)} - \mathbf{y}_{(k+1)}. \quad (4.14)$$

By inserting (4.13) into (4.14), the error vector becomes

$$\mathbf{e}_{(k+1)} = \mathbf{M}_{(k)} (\alpha^* \mathbf{x}_{(k)} - \mathbf{y}_{(k)}) - \xi_{(k)}. \quad (4.15)$$

Let control vector $\xi_{(k)}$ take the form of

$$\xi_{(k)} = \chi_{(k)} (\alpha^* \mathbf{x}_{(k)} - \mathbf{y}_{(k)}) \quad (4.16)$$

where $\chi_{(k)} = [\chi_{ij,(k)}] \in \mathbb{R}^{n \times n}$ is the matrix of the control gain and $\chi_{ij,(k)}$ are the elements of $\chi_{(k)}$. Substituting (4.16) into (4.15), the error dynamics becomes

$\mathbf{e}_{(k+1)} = (\mathbf{M}_{(k)} - \chi_{(k)}) \mathbf{e}_{(k)}$, which can also be expressed as

$$\mathbf{e}_{(k+1)} = \prod_{q=0}^k (\mathbf{M}_{(q)} - \chi_{(q)}) \mathbf{e}_{(0)}. \quad (4.17)$$

Note that projective synchronisation occurs at the scaling factor α^* if the error $\mathbf{e}_{(k)}$ tends to be zero. For general cases, the initial conditions $\mathbf{u}_{m,(0)}$ and $\mathbf{u}_{s,(0)}$ can be taken arbitrarily and thus the initial error vector $\mathbf{e}_{(0)} \neq 0$. Therefore, in order for $\lim_{k \rightarrow \infty} \mathbf{e}_{(k)} = 0$, a sufficient condition requires that the spectral radius of the matrix

$\prod_{i=0}^k (\mathbf{M}_{(i)} - \boldsymbol{\chi}_{(i)})$ tends to zero as $k \rightarrow \infty$, where spectral radius of the matrix is the radius of the smallest circle in the complex plane that contains all its eigenvalues. Matrix with spectral radius lesser than one is stable about its origin. A stricter condition will require all the eigenvalues of the characteristic polynomial of the matrix $(\mathbf{M}_{(k)} - \boldsymbol{\chi}_{(k)})$ to lie within the unit circle for $k = 0, 1, 2, 3, \dots$

For discrete-time systems, the Schur-Cohn stability criterion [LaSalle, 1986] can be used to confine the eigenvalues of a matrix $\mathbf{V} = (v_{ij})_{n \times n}$ inside a unit circle.

The characteristic polynomial of matrix $\mathbf{V} = (v_{ij})_{n \times n}$ can be written as

$$p(\lambda) = \lambda^n + v_{n-1}\lambda^{n-1} + \dots + v_1\lambda + v_0, \quad (4.18)$$

where $v_\mu = v_\mu(v_{ij}) \in \mathbb{R}$, $\mu = 0, 1, 2, \dots, n-1$, are the coefficients of the polynomial (4.18) and λ is the eigenvalue of the matrix. According to the Schur-Cohn stability criterion, the eigenvalues λ of the characteristic polynomial (4.18) will lie inside a unit circle if the following conditions are satisfied

$$(i) \quad p(1) > 0 \text{ and } (-1)^n p(-1) > 0. \quad (4.19)$$

$$(ii) \quad \text{The } (n-1) \times (n-1) \text{ matrices}$$

$$\Delta_{n-1}^\pm = \begin{pmatrix} 1 & 0 & \dots & 0 \\ v_{n-1} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ v_2 & \dots & v_{n-1} & 1 \end{pmatrix} \pm \begin{pmatrix} 0 & \dots & 0 & v_0 \\ \vdots & \ddots & v_0 & v_1 \\ 0 & \ddots & \ddots & \vdots \\ v_0 & v_1 & \dots & v_{n-2} \end{pmatrix} \quad (4.20)$$

are both positive innerwise.

Here examples of the explicit expressions of conditions (4.19) and (4.20) are given in terms of the coefficients v_μ . Since a general form of the explicit

expression is not readily available, the conditions are provided up to the dimensions $n=4$. Based on the Schur-Cohn criterion, for $n=2$, the conditions that all the eigenvalues will remain inside the unit circle [Wen *et al.*, 2002] are

$$(C1) \quad |v_1| < 1 + v_0$$

and

$$(C2) \quad |v_0| < 1.$$

For $n=3$, the conditions that all the eigenvalues will remain inside the unit circle are

$$(C3) \quad |v_0 + v_2| < 1 + v_1$$

and

$$(C4) \quad |v_1 - v_0 v_2| < 1 - v_0^2.$$

For $n=4$, the conditions that all the eigenvalues will remain inside the unit circle are

$$(C5) \quad |v_0| < 1,$$

$$(C6) \quad |v_1 + v_3| < 1 + v_0 + v_2,$$

and

$$(C7) \quad |v_2(1 - v_0) + v_0(1 - v_0^2) + v_3(v_0 v_3 - v_1)| < v_0 v_2(1 - v_0) + (1 - v_0^2) + v_1(v_0 v_3 - v_1).$$

Using the Schur-Cohn stability criterion (4.19) and (4.20), the conditions for higher-dimension can be explored but the expression of the conditions may become very complicated.

The above conditions (C1) to (C7) can be applied to design the control function (4.16), $\xi_{(k)} = \chi_{(k)} (\alpha^* \mathbf{x}_{(k)} - \mathbf{y}_{(k)})$. In general, a Jacobian matrix $\mathbf{M}_{(k)}$ consists of both the variable $z_{(k)}$ and constants. The control gain elements $\chi_{ij,(k)}$ can be constructed in a general form of $\chi_{ij,(k)} = g_{ij}(z_{x,(k)}) + C_{ij}$ where $g_{ij}(z_{x,(k)})$ is a function of $z_{x,(k)}$ and C_{ij} is a constant. Note that it is not necessary to assign values to all the elements $\chi_{ij,(k)}$. A simple and feasible way is to set the control function such that it can offset the effects of the z-dependent elements in $\mathbf{M}_{(k)}$ and obtain control over the main diagonal elements. For z-dependent elements $m_{ij,(k)}$ in $\mathbf{M}_{(k)}$, let the corresponding $\chi_{ij,(k)} = m_{ij,(k)}$ for all $i \neq j$ and $\chi_{ii,(k)} = m_{ii,(k)} + C_{ii}$ for $i = j$. For the constant elements $m_{ij,(k)}$ in $\mathbf{M}_{(k)}$, let the corresponding $\chi_{ij,(k)} = 0$ for all $i \neq j$ and $\chi_{ii,(k)} = C_{ii}$ for $i = j$, $i = 1, 2, \dots, n$. Hence, by incorporating the control function into the coupled system (4.13), a constant Jacobian will be obtained in the response system. The constant Jacobian contains the constants C_{ii} in the main diagonal that can be determined by the Schur-Cohn stability criterion (4.19) and (4.20). In what follows, two examples will be presented to demonstrate the design approach and effectiveness of the developed control algorithm.

Example 1

In example 1, detailed construction of the control function based on the proposed method and its effectiveness to direct the scaling factor to any desired

values will be demonstrated. In this example, the desired scaling factor is set as

$\alpha^* = 5$. The coupled chaotic system used here is given as

$$\begin{aligned} \mathbf{x}_{(k+1)} &= \mathbf{M}_{(k)} \cdot \mathbf{x}_{(k)}, \\ z_{x,(k+1)} &= 0.12x_{1,(k)}x_{2,(k)} + 0.3z_{x,(k)}, \\ \mathbf{y}_{(k+1)} &= \mathbf{M}_{(k)} \cdot \mathbf{y}_{(k)} + \xi_{(k)}, \end{aligned} \quad (4.21)$$

with a 2×2 Jacobian matrix

$$\mathbf{M}_{(k)} = \begin{bmatrix} m_{11,(k)} & m_{12,(k)} \\ m_{21,(k)} & m_{22,(k)} \end{bmatrix} = \begin{bmatrix} 0.115 & -1.195(0.5 - 0.21z_{x,(k)}) \\ 0.36(6 - z_{x,(k)}) & -0.285 \end{bmatrix}.$$

System (4.21) behaves chaotically with the largest Lyapunov exponent of 0.12, as shown in Fig. 4.2(b). The sufficient conditions associated with the two-dimensional Jacobian matrix of the controlled system (4.2.1) are (C.1) and (C2). In the conditions (C1) and (C2), the coefficient $v_{0,(k)}$ is the determinant of

$(\mathbf{M}_{(k)} - \chi_{(k)})$ given as

$$v_{0,(k)} = (m_{11,(k)} - \chi_{11,(k)})(m_{22,(k)} - \chi_{22,(k)}) - (m_{12,(k)} - \chi_{12,(k)})(m_{21,(k)} - \chi_{21,(k)}) \quad (4.22)$$

and the coefficient $v_{1,(k)}$ is the summation of the main diagonal given as

$$v_{1,(k)} = (m_{11,(k)} - \chi_{11,(k)}) + (m_{22,(k)} - \chi_{22,(k)}). \quad (4.23)$$

According to Jacobian matrix $\mathbf{M}_{(k)}$ in system (4.21), the elements

$m_{11,(k)}$ and $m_{22,(k)}$ are constants and the elements $m_{12,(k)}$ and $m_{21,(k)}$ are dependent on

$z_{(k)}$. For the z -dependent elements $m_{ij,(k)}$, let the corresponding elements in $\chi_{(k)}$

are set as $\chi_{12,(k)} = m_{12,(k)}$ and $\chi_{21,(k)} = m_{21,(k)}$. For the constant diagonal elements

$m_{ij,(k)}$, let $\chi_{11,(k)} = C_{11}$ and $\chi_{22,(k)} = C_{22}$. In this example, C_{22} is set as 0 and C_{11} is to be solved to satisfy conditions (C1) and (C2). Thus the control vector is designed as

$$\begin{aligned}\xi_{(k)} &= \chi_{(k)} \mathbf{e}_{(k)} \\ &= \begin{bmatrix} C_{11} & m_{12,(k)} \\ m_{21,(k)} & 0 \end{bmatrix} \mathbf{e}_{(k)}.\end{aligned}\quad (4.24)$$

From C1, $\left| m_{11,(k)} - C_{11} + m_{22,(k)} \right| < 1 + (m_{11,(k)} - C_{11})m_{22,(k)}$, the range $-0.885 < C_{11} < 1.115$ is obtained and from C2, $\left| (m_{11,(k)} - C_{11})m_{22,(k)} \right| < 1$, the range $-3.394 < C_{11} < 3.624$ is obtained. Therefore the feasible range for the value of C_{11} is $(C_{11,\min}, C_{11,\max}) = (-0.885, 1.115)$.

In the numerical experiment, C_{11} is set as $0.5C_{11,\max}$. Fig. 4.2(b) shows projective synchronous behaviour between $x_{1,(k)}$ and $y_{1,(k)}$ under the control. The variation of the error $\log|e_{1,(k)}|$ shown in Fig. 4.2(c) is maintained within a range of infinitely small values between $|10^{-30}|$ to $|10^{-40}|$ as the iteration persists. In the inset, the variation of the scaling factor is displayed with respect to k , which indicates system (4.21) responded well to the control input as $\alpha_{(k)}$ is directed to the desired scaling factor $\alpha^* = 5$. Fig. 4.2(d) shows the variation of the control input $\log|\xi_{1,(k)}|$. It can be seen from the figure that once the system is directed to a desired synchronous state, only a tiny control input is required.

Fig. 4.2. (a) The chaotic attractor of the drive system (4.21) with a positive Lyapunov exponent of 0.12. (b) An illustration of projective synchronous behaviour between $x_{1,k}$ (solid line) and $y_{1,k}$ (dashed line). (c) The variation of the error vector $\log|e_{1,k}|$. Inset: the variation of the scaling factor $\alpha(k)$. (d) The variation of the control input $\log|\xi_{1,k}|$. The desired scaling factor α^* is set to 5 and $C_{11} = 0.5C_{11,\max}$. The initial conditions are randomly selected as $\{x_1, x_2, z, y_1, y_2\}_{(0)} = \{-2.2, 0.5, -0.3, 2.5, 2.4\}$.

Example 2

In example 2, the convergence rate in the control process will be discussed. The Schur-Cohn criterion (4.19) and (4.20) is again applied to design the control vector $\xi_{(k)}$, which will be employed to direct the scaling factor to a predestined value of $\alpha^* = -5$. The coupled system used here is given as

$$\left. \begin{aligned} \mathbf{x}_{(k+1)} &= \mathbf{M}_{(k)} \cdot \mathbf{x}_{(k)} \\ z_{x,(k+1)} &= 0.12x_{2,(k)}x_{3,(k)} + 0.3z_{x,(k)} \end{aligned} \right\} \text{Drive System,} \quad (4.25)$$

$$\mathbf{y}_{(k+1)} = \mathbf{M}_{(k)} \cdot \mathbf{y}_{(k)} + \xi_{(k)} \} \text{Response System,}$$

with a 3 x 3 Jacobian matrix

$$\mathbf{M}_{(k)} = \begin{bmatrix} 0.28(6.1 - z_{x,(k)}) & -0.1 & -0.3 \\ 0.3 & -0.2z_{x,(k)} & -0.2 \\ 0.3 & -0.4 & -0.2 \end{bmatrix}.$$

System (4.25) behaves chaotically with the largest Lyapunov exponent of 0.31. For the three-dimensional Jacobian matrix, conditions (C3) and (C4) of the Schur-Cohn criterion will be used to design the control function $\xi_{(k)}$. For the z-dependent elements in the main diagonal of $\mathbf{M}_{(k)}$, the corresponding diagonal elements in $\chi_{(k)}$ can be set as $\chi_{11,(k)} = m_{11,(k)} + C_{11}$, $\chi_{22,(k)} = m_{22,(k)} + C_{22}$ and $\chi_{33,(k)} = C_{33}$. The remaining elements $\chi_{ij,(k)}$ are set to null. To further simplify the design, the diagonal elements C_{22} and C_{33} can also be set to null. In doing so, the control vector is designed as

$$\begin{aligned}\xi_{(k)} &= \chi_{(k)} \mathbf{e}_{(k)} \\ &= \begin{bmatrix} m_{11,(k)} + C_{11} & 0 & 0 \\ 0 & m_{22,(k)} & 0 \\ 0 & 0 & 0 \end{bmatrix} \mathbf{e}_{(k)}.\end{aligned}\quad (4.26)$$

From the design of the control vector given in (4.26), the controlled Jacobian

$$\text{matrix becomes } (\mathbf{M}_{(k)} - \chi_{(k)}) = \begin{bmatrix} -C_{11} & -0.1 & -0.3 \\ 0.3 & 0 & -0.2 \\ 0.3 & -0.4 & -0.2 \end{bmatrix} \text{ and the coefficients are given}$$

as $v_0 = -(0.036 + 0.08C_{11})$, $v_1 = 0.04 - 0.2C_{11}$ and $v_2 = 0.2 + C_{11}$. According to conditions (C3) and (C4), the feasible range of C_{11} is $(C_{11,\min}, C_{11,\max}) = (-1.075, 1.216)$.

To view the effect of the selection of C_{11} from $C_{11,\min}$ and $C_{11,\max}$, the graph of k^* against $C_{11,\min}(\%)$ and $C_{11,\max}(\%)$ is plotted as shown in Fig. 4.3(b). The iteration number k^* is recorded if the error $|e_{1,(k)}|$ falls and remains less than a selected threshold value of 10^{-10} at which the synchronisation is confirmed. The symbols $C_{11,\min}(\%)$ and $C_{11,\max}(\%)$ denote the percentage of $C_{11,\min}$ and $C_{11,\max}$ in which C_{11} is assigned in the control. Fig. 4.3(b) shows the iteration number k^* required under the different selection of C_{11} to direct the scaling factor to the predestined value of $\alpha^* = -5$. The most effective control is the one that requires the least iteration number. This is observed at $C_{11} = 0.23C_{11,\min}$ in this example. As C is set close to the boundaries of $C_{11,\min}$ and $C_{11,\max}$, the required iteration numbers increase significantly and the control becomes much less effective. Fig. 4.3(c)

shows the error dynamics $\log|e_{1,(k)}|$ and the inset shows the variation of the scaling factor with respect to k with $C_{11} = 0.5C_{11,\min}$. Similar to the previous example, Fig. 4.3(d) shows that control input tends to null once the system is directed to the desired synchronous state. The inset shows the projective synchronous behaviour between $x_{1,(k)}$ and $y_{1,(k)}$.

Fig. 4.3. (a) The chaotic attractor of the drive system (4.25) with a positive Lyapunov exponent of 0.31. (b) The graph of k^* against $C_{11,\min}$ and $C_{11,\max}$. (c) The error dynamics $\log|e_{1,(k)}|$. Inset: the variation of the scaling factor $\alpha_{(k)}$. (d) The variation of the control input $\log|\xi_{1,(k)}|$. Inset: projective synchronous behaviour between $x_{1,(k)}$ (solid line) and $y_{1,(k)}$ (dashed line). The desired scaling factor is set as $\alpha^* = -5$ and $C_{11} = 0.5C_{11,\max}$ for (c) and (d).

4.3 Manipulating the ultimate state of projective synchronisation in nonpartially linear chaotic systems

Projective synchronisation is usually observable only in partially linear systems. This section will show that projective synchronisation could by means of control, be extended to general classes of chaotic continuous-time systems with non-partial linearity [Xu & Li, 2002]. The derivation of the control function based on the Lyapunov stability theory is feasible for system of any dimension.

Consider a coupled system with a control vector attached to the response system given as,

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{g}(\mathbf{x}, z_x) \\ \dot{z}_x &= h(\mathbf{x}, z_x) \end{aligned} \right\} \text{Drive System,} \quad (4.27)$$

$$\dot{\mathbf{y}} = \mathbf{g}(\mathbf{y}, z_x) + \boldsymbol{\xi} \text{ Response System.}$$

The state vectors $\mathbf{x} \in \mathfrak{R}^n$ and $\mathbf{y} \in \mathfrak{R}^n$. The control vector is defined as $\boldsymbol{\xi} = [\xi_1, \xi_2, \dots, \xi_n]^T$. The purpose of the control vector is to allow the response system to track and synchronise with the driving dynamics under the desired scaling factor such that $\lim_{t \rightarrow \infty} \|\alpha^* \mathbf{x} - \mathbf{y}\| = 0$. The Lyapunov stability theory is employed to ensure that the designed control vector is globally stable. To begin with the design, the error vector is given as

$$\mathbf{e}(t) = \alpha^* \mathbf{x} - \mathbf{y}. \quad (4.28)$$

The Lyapunov function is defined as

$$V = \frac{1}{2} \mathbf{e}^T \mathbf{e} = \frac{1}{2} \sum_{i=1}^n e_i^2. \quad (4.29)$$

The time derivative of equation (4.29) is defined as

$$\begin{aligned}
 \dot{V} &= \sum_{i=1}^n e_i \dot{e}_i = \mathbf{e}^T \dot{\mathbf{e}} \\
 &= \mathbf{e}^T (\alpha^* \mathbf{g}(\mathbf{x}, z_x) - \mathbf{g}(\mathbf{y}, z_x) - \boldsymbol{\xi}) \\
 &= \varphi(\mathbf{e}, \boldsymbol{\xi}).
 \end{aligned} \tag{4.30}$$

In order for the error vector $\mathbf{e}(t)$ to tend asymptotically to zero, the accompanying conditions are

$$\begin{aligned}
 V(\mathbf{e}) > 0 \quad \mathbf{e} \neq 0, \quad \text{and} \quad \dot{V}(\mathbf{e}) < 0 \quad \mathbf{e} \neq 0, \\
 V(\mathbf{e}) = 0 \quad \mathbf{e} = 0, \quad \dot{V}(\mathbf{e}) = 0 \quad \mathbf{e} = 0.
 \end{aligned} \tag{4.31}$$

Eq. (4.30) is a function of the control vector $\boldsymbol{\xi}$. Therefore the sign of $\dot{V}$ can be determined by an appropriate selection of the control vector $\boldsymbol{\xi}$. One method to design the control function is to satisfy the third inequality in (4.31). This gives

$$\mathbf{e}^T (\alpha^* \mathbf{g}(\mathbf{x}, z_x) - \mathbf{g}(\mathbf{y}, z_x) - \boldsymbol{\xi}) < 0. \tag{4.32}$$

In satisfying inequality (4.32), the coupled system (4.27) will perform projective synchronisation with the desired scaling factor for any initial condition. Hence, inequality (4.32) formed the basis for the formulation of the control functions for the general form of the coupled chaotic system.

As an example, inequality (4.32) is used to design the control function for hyperchaotic Rossler system [Rossler, 1976]. The coupled system with control is given as

$$\left. \begin{aligned} \dot{x}_1 &= -x_2 - x_3 \\ \dot{x}_2 &= x_1 + \mu_1 x_2 + z_x \\ \dot{x}_3 &= \mu_2 + x_1 x_3 \\ \dot{z}_x &= \mu_3 x_3 + \mu_4 z_x \end{aligned} \right\} \text{Drive System,} \quad \left. \begin{aligned} \dot{y}_1 &= -y_2 - y_3 + \xi_1 \\ \dot{y}_2 &= y_1 + \mu_1 y_2 + z_x + \xi_2 \\ \dot{y}_3 &= \mu_2 + y_1 y_3 + \xi_3 \end{aligned} \right\} \text{Response System.} \tag{4.33}$$

The hyperchaotic Rossler system shown in (4.33) is a nonpartially linear system.

The variable z_x is used to denote the coupling term. The parameter set as is assigned as $[\mu_1, \mu_2, \mu_3, \mu_4] = [0.25, 3, -0.5, 0.05]$.

To formulate the control function for system (4.33), consider the inequality $\dot{V}(\mathbf{e}) < 0$ with $\mathbf{e} \neq \mathbf{0}$ in condition (4.31). This gives

$$\begin{aligned} & [\alpha^*(-x_2 - x_3) - (-y_2 - y_3)]e_1 + \\ & [\alpha^*(x_1 + \mu_1 x_2 + z_x) - (y_1 + \mu_1 y_2 + z_x)]e_2 + \\ & [\alpha^*(\mu_2 + x_1 x_3) - (\mu_2 + y_1 y_3)]e_3 - \xi_1 e_1 - \xi_2 e_2 - \xi_3 e_3 < 0. \end{aligned} \quad (4.34)$$

A possible option to ensure $V < 0$ with $\mathbf{e} \neq \mathbf{0}$, of which inequality (4.34) is a sufficient condition, is to design the control function as

$$\begin{aligned} \xi_1 &= -e_2 - e_3 + \kappa_1 e_1 \\ \xi_2 &= e_1 + (\mu_1 + \kappa_2)e_2 + (\alpha^* - 1)z_x \\ \xi_3 &= \alpha^* x_1 x_3 - y_1 y_3 + (\alpha^* - 1)\mu_2 + \kappa_3 e_3. \end{aligned} \quad (4.34)$$

As such, according to Lyapunov stability theory, the drive and response systems of coupled system (4.33) will synchronise in a projective manner under the influence of the control function (4.34). The constants $\kappa_{1,2,3}$ have an effect on the rate of convergence but do not affect the robustness of the control, which can be selected as any real numbers as long as the inequality (4.34) is satisfied.

A numerical experiment will be carried out in the following to demonstrate the proficiency of control function (4.34). The constants $\kappa_{1,2,3}$ are set to 1 and the desired scaling factor is assigned as $\alpha^* = 5$. Fig. 4.4(a) and (b) show the dynamical behaviour of the controlled hyperchaotic Rossler system (4.33). The drive system is represented by solid lines and the response system is represented by dashed lines.

Fig. 4.4(a) shows the strange attractors of the drive and response systems. Fig. 4.4(b) shows the time variation of x_1 and y , where the two variables oscillate in phase according to the desired scaling factor $\alpha^* = 5$. Fig. 4.4(c) shows the time variation of $\log|e_1|$, which remains infinitely small as $t \rightarrow \infty$. This indicates that the state ratio tends asymptotically to the desired scaling factor as time persists. The inset shows that only a tiny control input is required to direct the state ratio to the desired scaling factor. Fig. 4.4(d) shows the time variation of the scaling factor, which indicates that $\lim_{t \rightarrow \infty} \alpha(t) = \alpha^* = 5$. Similar numerical experiments have been carried out on three-dimensional Rossler system and Chua's circuit [Xu & Li, 2002]. These experiments including the shown here verified the possibility of realising projective synchronisation in nonpartially linear systems by means of a control.

Fig. 4.4. (a) Strange attractors of the drive system (solid line) and the response system (dashed line) of controlled hyperchaotic Rossler system (4.33). (b) Time variation of x_1 (solid line) and y_1 (dashed line). (c) The time variation of $\log|e_1|$. Inset: The control input required to direct the state ratio to the desired scaling factor. (d) Time variation of the scaling factor.

4.4 Control for full-state projective synchronisation in continuous-time systems

This section will introduce an observer-based [Nijmeijer & van der Schaft, 1990] control algorithm that can be used to regulate full-state projective synchronisation in continuous-time systems [Wen & Xu, 2004]. Full-state projective synchronisation refers to a state whereby all variables from the drive

system that include also the coupling variable synchronise with the corresponding variables from the response system under a common proportional relationship α . This differs from the previous form of projective synchronisation where z_x and z_y synchronise with a proportional relationship of α^b . The constant b is a real value that depends on the employed system. Furthermore this observer-based control algorithm can be extended to a general class of chaotic systems regardless of partial linearity.

The nonlinear observer technique introduced here to develop the control algorithm has been used effectively in controlling other types of chaotic synchronous behaviour [Morgiil & Solak, 1996; Grassi & Mascolo, 1997]. Consider an n -dimensional continuous-time drive system in the form,

$$\dot{\mathbf{x}} = \mathbf{Ax} + \mathbf{Bf}(\mathbf{x}) + \mathbf{C}, \quad (4.35)$$

where $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{A} \in \mathbb{R}^{n \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times m}$, $\mathbf{C} \in \mathbb{R}^n$ and $\mathbf{f}: \mathbb{R}^n \rightarrow \mathbb{R}^m$ is a nonlinear or piecewise-linear vector function in terms of $\mathbf{x}$. Many chaotic systems such as the Lorenz and Rossler systems can be written as Eq. (4.35).

The most common observer construction scheme involves replicating the system dynamics together with additive output error injection term [Grassi & Mascolo, 1997]. For projective synchronisation, supposed that an artificial output of system (4.35) is given as $\mathbf{s}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) + \mathbf{Kx}$, where $\mathbf{K} \in \mathbb{R}^{m \times n}$ is a feedback gain. The response system, which is referred to as the observer here is then defined as,

$$\dot{\mathbf{y}} = \mathbf{Ay} + \mathbf{Bf}(\mathbf{y}) + \alpha^* \mathbf{C} + \mathbf{B}(\alpha^* \mathbf{s}(\mathbf{x}) - \mathbf{s}(\mathbf{y})) \quad (4.36)$$

where α^* is a desired scaling factor preset for projective synchronisation. Moreover, system (4.36) is considered as a global observer [Nijmeijer & van der Schaft, 1990] of system (4.35) if y tends to α^*x as $t \rightarrow \infty$ for any initial conditions $x(0)$ and $y(0)$

With the observer given as Eq. (4.36) and an error vector defined as $e = \alpha^*x - y$, an error dynamics is obtained as

$$\begin{aligned}\dot{e} &= \alpha^* \dot{x} - \dot{y} \\ &= Ae + \alpha^* Bf(x) - Bf(y) - B(\alpha^* s(x) - s(y)) \\ &= Ae - \alpha^* BKx + BKy \\ &= Ae - BKe.\end{aligned}\tag{4.37}$$

It thus becomes obvious that the error dynamics is governed by a linear differential equation expressed as $\dot{e} = (A - BK)e$ where $-Ke$ is the state feedback.

For a feasible control, the feedback gain K must be selected such that the real parts of all the eigenvalues of $(A - BK)$ in system (4.37) are negative. If the controllability matrix $[B, AB, \dots, A^{n-1}B]$ is of full rank, then system (4.36) is a global observer of system (4.35) such that the state vector y will tend to α^*x as $t \rightarrow \infty$ even though the initial conditions of systems (4.35) and (4.36) are not in the same basin of attraction. In this case, the pole placement technique [Paraskevopoulos, 2002] is usually used to determine the gain vector K for any specified eigenvalues of $(A - BK)$. Note that the value of scaling factor α^* has no effect on the controllability of system (4.37). This is because the eigenvalues of $(A - BK)$ are independent on the desired scaling factor α^* . Thus the observer-

based approach enables α^* to be adjusted to any desired value during the control process.

As an example, consider the Chen system that is expressible by the following three differential equations, $\dot{x}_1 = \mu_1(x_2 - x_1)$, $\dot{x}_2 = (\mu_3 - \mu_1)x_1 - x_1x_3 + \mu_3x_2$ and $\dot{x}_3 = x_1x_2 - \mu_2x_3$. The parameter set μ is chosen as $[\mu_1, \mu_2, \mu_3] = [35, 3, 28]$. The Chen system can take the form according to Eq. (4.35), given as

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -\mu_1 & \mu_1 & 0 \\ \mu_3 - \mu_1 & \mu_3 & 0 \\ 0 & 0 & -\mu_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -x_1x_3 \\ x_1x_2 \end{bmatrix}. \quad (4.38)$$

System (4.38) is structured as $A \in \mathcal{R}^{3 \times 3}$, $B \in \mathcal{R}^{3 \times 2}$, $C = 0$ and $f(x) = [-x_1x_3, x_1x_2]^T$.

In this example, the desired scaling factor is assigned as $\alpha^* = -2$ and the feedback output is given as $s(x) = f(x) + Kx$ with a gain matrix $K \in \mathcal{R}^{2 \times 3}$. Hence, the observer (4.36) is defined as,

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{bmatrix} = \begin{bmatrix} -\mu_1 & \mu_1 & 0 \\ \mu_3 - \mu_1 & \mu_3 & 0 \\ 0 & 0 & -\mu_2 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -y_1y_3 \\ y_1y_2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} [\alpha^* s(x) - s(y)] \quad (4.39)$$

The rank of the controllability matrix $[B, AB, A^2B]_{3 \times 6}$ is in an order of three. The eigenvalues of the error dynamics given in by Eq. (4.37) are assigned as $(-3.5, -3.5, -2.5)$. Using the pole placement technique, the gain matrix

$K = \begin{bmatrix} 22.25, -1, 0 \\ 0, 0, 0.5 \end{bmatrix}$ is obtained. This leads the drive (4.38) and response (4.39)

systems to projectively synchronise according to the assigned desired scaling factor

$\alpha^* = -2$ shown in Fig. 4.5.

Fig. 4.5. Demonstration on using the observer-based control to direct the ultimate state of projective synchronisation to $\alpha^* = -2$. (a) Synchronised chaotic attractors of the drive system (4.38) (top) and response system (4.39) (bottom) with an anti-phase pattern and proportional relationship of $\alpha^* = -2$. (b) Time evolution of $\alpha^* x_i - y_i$, with $\lim_{t \rightarrow \infty} \|\alpha^* \mathbf{x} - \mathbf{y}\| = 0$ implying that all the state variables synchronised under the desired proportional relationship.

Chapter 5

Pseudo-random switching keys

The chapter introduces a new technique known as pseudo-random switching key (PRSK), which can be used to enhance secure communication [Xu & Chee, 2003]. PRSK are system parameters designed as discontinuous functions of the system variables. The main characteristic of PRSK is the discontinuous, rapid and irregular switching behaviour that is exhibited during the time evolution. Along with such a characteristic, the generated time series also exhibits higher unpredictability than the time series generated from the original chaotic system. This finding is verified by measuring the local and global prediction errors of a typical Lorenz and Chen system. The design of PRSK and the time series analyses of chaotic dynamics generated using PRSK will be presented in Section 5.2 and Section 5.3 respectively.

5.1 Introduction

Highly unpredictable chaotic dynamics is an important feature in chaotic encryption schemes. Chaotic encryption schemes based on highly predictability chaos run the risk of information being extracted once the transmitted signal is intercepted. In this thesis, when given an unknown chaotic system, chaos is considered as predictable if (1) the governing equations of the system can be reconstructed from the observed dynamical behaviour or (2) the future dynamics of

the system that can be predicted using the past observed dynamical behaviour. However, generating chaotic time series of low predictability based solely on indicators such as Lyapunov exponent or correlation dimensions without placing consideration on the advance development of the cryptanalysis techniques will be insufficient to provide the necessary security.

As introduced in Chapter 2, there are three fundamental routes of attack taken by chaotic cryptanalysis to break continuous-time chaotic encryption. It is stated that either route (I) or (II) will be used if the information is encrypted using chaotic masking [Kocarev *et al.*, 1992] or chaotic modulation [Halle *et al.*, 1993]. However if the information is encrypted using chaotic shift keying [Parlitz *et al.*, 1992], then route (III) will be used. A brief description of the three routes of attack is given as follows:

- (I) If the dynamical form of the chaotic system is known while the parameter set remains unknown to the intruder, then the cryptanalysis techniques will be based on parameters identification [Stojanovski *et al.*, 1996; Ponomarenko & Prokhorov, 2002; Tao *et al.*, 2004].
- (II) If the dynamical form and parameter set are unknown to the intruder, then the cryptanalysis techniques will be based on approximating the future time series either using a global [Short & Parker, 1998] or local [Zhou & Lai, 1999; Huang *et al.*, 2001] prediction model.
- (III) If the information signal is encrypted using chaotic key shifting, then the cryptanalysis techniques carried out will focus on detecting changes between

two distinct sets of statistical properties over the intercepted time series [Pérez & Cerdeira, 1995; Yang *et al.*, 1998a,b,c; Storm & Freeman, 2002].

Due to the development of the existing cryptanalysis techniques, continuous-time chaotic encryption becomes vulnerable to intrusion. The case is particularly for those schemes that rely on higher dimensional chaos [Kocarev & Parlitz, 1995; Zhang *et al.*, 1999]. This shows that the security issue of chaotic encryption have not been adequately addressed. Therefore, in this chapter it is suggested that in order to enhance the security of chaotic encryption it is required to cope directly with the three fundamental routes of attack (I), (II) and (III).

5.2 Design of pseudo-random switching keys

To overcome the security threat posed by routes (I), (II) and (III), a technique known as pseudo-random switching keys (PRSK) is proposed. A system with PRSK generates chaotic dynamics with persistently transient nature that makes the cryptanalysis that uses parameter detection, reconstruction or detection of changes in statistical properties ineffective.

Consider a system $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\mu})$ where $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ is the state vector. The system parameter set $\boldsymbol{\mu} = [\mu_1, \mu_2, \dots, \mu_\nu]^T$ is assigned as a set of discontinuous functions of $\mathbf{x}$ given as $\boldsymbol{\mu} = \mathbf{g}(\mathbf{x}) = [g_1(\mathbf{x}), g_2(\mathbf{x}), \dots, g_\nu(\mathbf{x})]^T$ that changes values according to the rule

$$g_k(x_i) = b_{k,j}(\mathbf{x}, \boldsymbol{\mu}) \text{ for } a_{k,j} \leq x_i < a_{k,j+1}. \quad (5.1)$$

Here the constant $a_{j,k}$ and function $b_{k,j}(\mathbf{x}, \mathbf{p})$ are pre-defined for $k=1, \dots, v$ $j=1, \dots, L$ with $L > 1$. The rule states that the k th parameter μ_k will be switched to a function of $b_{k,j}(\mathbf{x}, \mathbf{p})$ when a selected state variable x_i falls in a range defined by $a_{k,j} \leq x_i < a_{k,j+1}$.

The Rossler system [Rossler, 1976] given in (5.2) is used here to facilitate the description of PRSK.

$$\dot{x}_1 = -x_2 - x_3, \quad \dot{x}_2 = x_1 + \mu_1 x_2, \quad \dot{x}_3 = \mu_2 + x_3(x_1 - \mu_3). \quad (5.2)$$

For the purposes of illustration, only the third parameter, μ_3 , is assigned as PRSK while μ_1 and μ_2 remain constant for simplicity, given as $\mu_1 = 0.2$, $\mu_2 = 0.2$. Let $\mu_3 = g_3(x_2)$ be a function of x_2 according to the rule

$$g_3(x_2) = \begin{cases} b_{3,1}(\mathbf{x}, \mathbf{p}) & \text{for } a_{3,1} \leq |x_2| < a_{3,2} \\ b_{3,2}(\mathbf{x}, \mathbf{p}) & \text{for } a_{3,3} \leq |x_2| < a_{3,4} \\ b_{3,3}(\mathbf{x}, \mathbf{p}) & \text{for } a_{3,5} \leq |x_2| < a_{3,6} \\ b_{3,4}(\mathbf{x}, \mathbf{p}) & \text{for } a_{3,7} \leq |x_2| < a_{3,8} \\ b_{3,5}(\mathbf{x}, \mathbf{p}) & \text{otherwise} \end{cases} \quad (5.3)$$

where $[a_{3,1} \dots a_{3,8}] = [0, 2, 2, 4, 4, 6, 6, 8]$ and $[b_{3,1} \dots b_{3,8}] = [5.7, 5.5, 5.9, 6.1, 5.3]$. The design of the parameter set $\mathbf{p} = [\mu_1, \mu_2, \mu_3]^T$ can in fact be made more complicated but a simpler example is chosen for the purpose of illustration. Fig. 5.1(a) and (b) show the time series of the state variables x_1 , and x_2 . Examining these figures, it can be noticed that no significant discontinuity is observable along the time series. Hence, it is not possible to detect switching of resulted from PRSK, which makes the generated signal very suitable for secure communication. In Fig. 5.1(b), the

horizontal lines mark the values of $a_{3,1}$ to $a_{3,8}$, which can be used to compare with the corresponding time evolution of $\mu_3 = g_3(x_2)$ shown in Fig. 5.1(c). It can be observed from Fig. 5.1(c) that the dynamics of $\mu_3 = g_3(x_2)$ changes rapidly and irregularly in a discontinuous manner. Besides this, it is worthwhile to point out that the pattern of the time evolutions never repeats with different initial conditions. Fig. 5.1(d) shows the frequency spectrum of $\mu_3 = g_3(x_2)$, which resembles that of a white noise.

Fig 5.1. Illustration of Rossler system (5.2) with PRSK. (a) and (b) The time evolution of the variables $x_1(t)$ and $x_2(t)$ respectively. The horizontal lines in (b) mark the values of $a_{3,1}$ to $a_{3,8}$ given in (5.3). (c)

The time evolution the parameter μ_3 from (5.2) following the rule set in (5.3). (d) The frequency spectrum of $g_3(x)$.

5.3 Time series analysis for secure communication

This section will carry out time series analysis on signals generated using PRSK, which is developed to cope with the fundamental routes of attack (I), (II) and (III) of chaotic cryptanalysis.

First, the effectiveness of PRSK in invalidating type (I) cryptanalysis techniques [Stojanovski *et al.*, 1996; Ponomarenko & Prokhorov, 2002; Tao *et al.*, 2003] is investigated. In type (I) cryptanalysis techniques, identifying a set of system parameter with fixed values requires sampling of a continuous time series of about 40 time-units with respect to Fig. 5.1(a) [Saha *et al.*, 2004]. However, as shown in Fig. 5.1(c) the values of μ_3 under the design of PRSK varies rapidly with each value persisting over a time interval that is much shorter than the required sampling time. Furthermore, the frequency spectrum analysis presented in Fig. 5.1(d) shows that the irregular switches of μ_3 follow a manner similar to white noise. Along with these characteristics, transient chaos is rapidly and continuously induced into the generated signal each time parameter switching takes place. This makes PRSK a favourable feature for secure communication because in data analysis, the presence of transient chaos affects the accuracy of the results and is usually omitted. As such, the functioning of type (I) cryptanalysis techniques is further degenerated. Hence it is stated here that PRSK with its rapid and irregular switching of parameters and the continuous induction of transient chaos make it

impossible to identify the parameter accurately even if the system model is known. The continuous presence of transient chaos in the time series is observed by comparing return maps [PQez & Cerdeira, 1995] constructed in Fig. 5.2.

Fig. 5.2. (a) Return map constructed from time series generated by a typical Lorenz system. (b) Return map constructed from time series generated by the same system with PRSK. The presence of transient chaos diffuses out the attractor.

Next, this section discusses the effectiveness of PRSK against type (II) cryptanalysis techniques. Type (II) cryptanalysis techniques attempt to reconstruct the system model for predicting future dynamics. The reconstructed models for predicting future dynamics are built on available time series with the assumption that the system generating it is stationary. However, this adopted assumption is invalid when used to reconstruct a non-stationary and discontinuous system. As such, security provided by PRSK is derived from the combination of discontinuous switching of parameters and the continuous induction of transient chaos that causes

the time series to be hardly predictable. The claim of higher unpredictability here is based on the measurement of higher local and global prediction errors where a time series with a high prediction error indicates high unpredictability. For the purpose of verification, the predictability of time series with and without PRSK is compared. The Lorenz system [Lorenz, 1963], Chen system [Chen & Ueta, 1999] and hyperchaotic Rossler system [Rossler, 1979] are used for investigation here. The results lead to the conclusion that the time series generated with PRSK is more difficult to be predicted.

In a local modelling [Farmer & Sidorowich, 1987; Short & Parker, 1998], nearby points of a trajectory in an embedding space are used to predict short-time dynamics in the future. Here, the measurement of the local prediction error $\varepsilon_L(x, t)$ is carried out with a similar algorithm used to estimate non-negative Lyapunov exponent [Wolf *et al.*, 1985]. The non-negative Lyapunov exponent λ is estimated by plotting the graph of local prediction error $\varepsilon_L(x, t)$ against prediction time t where $\varepsilon_L(x, t)$ is the distance between two nearby points in the neighbourhood of a trajectory.

The graphs of the local prediction error $\varepsilon_L(x, t)$ against prediction time t of Lorenz and Chen systems are produced on Fig. 5.3. From Fig. 5.3 it is shown that the time series generated with the effect of PRSK represented by the solid line indeed brought about a higher local prediction error over short-term prediction when compare to time series generated by the original system without PRSK represented by dashed line. Unfortunately this advantage of PRSK fades away in long-term prediction as $t \rightarrow \infty$. However such advantage for long-term prediction

is trivial. This is so because in long-term prediction, $\varepsilon_L(x, t)$ of both the time series with and without PRSK have already reached such a high level that is consider unacceptable for good prediction. In order to rectify the high error resulted from long-term prediction, the local model will have to relocate a set of nearby points on the trajectory to again carry out short-term prediction. Hence the advantage of PRSK will again re-surface. The insets in Fig. 5.3(a) and (b) show the ratio $R_L = \varepsilon_{L,PRSK} / \varepsilon_{L,Orig}$ where $\varepsilon_{L,PRSK}$ and $\varepsilon_{L,Orig}$ are the prediction errors from time series with and without PRSK respectively. The insets indicate that the solid lines and the dashed lines do not intersect near the origin, $t \approx 0$, with the advantage of the systems with PRSK presiding over the original systems.

Fig. 5.3. Measurements of local prediction error $\varepsilon_L(x, t)$ from (a) Lorenz system and (b) Chen system. The solid and dashed lines represent data taken from the system with and without PRSK respectively. The insets in (a) and (b) show the ratio $R_L = \varepsilon_{L,PRSK} / \varepsilon_{L,Orig}$.

In global modelling, the prediction of future dynamics of a time series can be carried out by a generalised mathematical model consisting of a polynomial or other basis functions. To compare predictability of the time series between the original system and the system with PRSK, a method similar to the one given in [Barahona & Poon, 1996] is employed. The design of the global model works within the closed-loop version of the discrete Volterra series whereby the input x_n is identically equals to the output y_{n-1} , where $n=1,2,\dots,N$ is the discrete-time index. Based on this context, a discrete Volterra-Wiener-Korenberg series of degree d and system memory k is used as a global model to calculate the predicted time series given as,

$$y_n^* = a_0 + a_1 y_{n-1} + a_2 y_{n-2} + \dots + a_k y_{n-k} + a_{k+1} y_{n-1}^2 + a_{k+2} y_{n-1} y_{n-2} + \dots + a_{M-1} y_{n-k}^d \quad (5.4)$$

The predicted output y_n^* has a total dimension of $M = (k+d)!/(d!k!)$. The coefficients a_i are obtained by using the least squares fitting method. The global prediction error is then given as

$$\varepsilon_g(d, k)^2 = \sum_{n=1}^N \left(y_n^*(d, k) - y_n \right)^2 / \sum_{n=1}^N (y_n - \bar{y})^2. \quad (5.5)$$

where $\bar{y}$ is the mean of y_n for $n=1$ to N . For the purpose of comparing the unpredictability of both the time series with and without PRSK, an identical standard for both the models is required in which we select the optimum model $y_n^*(d_{opt}, k_{opt})$. Consider an information criterion [Akaike, 1974] given as

$$C(r) = \log \varepsilon_G(r) + r/N. \quad (5.6)$$

The optimum model for Eq. (5.4) is obtained by computing a pair of (d,k) that minimises Eq. (5.6) based on the parsimony principle.

From the optimum models constructed as such a number of sets of global prediction errors $(\varepsilon_{G,1}^2, \varepsilon_{G,2}^2)$ based on different time steps Δt_s can be obtained where $\varepsilon_{G,1}^2$ and $\varepsilon_{G,2}^2$ are the errors corresponding to the time series generated with and without PRSK respectively. Fig. 5.4(a) and (b) show the plots of the ratio $R_G = \varepsilon_{G,1}^2 / \varepsilon_{G,2}^2$ against Δt_s for Lorenz and Chen systems. In the figures, when $R_G > 1$, it can be concluded that the time series generated with PRSK bring about higher unpredictability as compared to the original system. From Fig. 5.4(a) and (b) it can be seen that for smaller time step, systems with PRSK has indeed higher unpredictability compared to the original systems. Although this effect may not always be observed at larger time step but it is worthwhile to note that by using a time step larger than 0.05 time-units to model a time series will generally results in poor modelling and hence poor prediction regardless of the present of PRSK. From here the effectiveness of PRSK against type (II) cryptanalysis techniques is verified.

Fig. 5.4. Measurements of the error ratio $R_G = \varepsilon_{G,1}/\varepsilon_{G,2}$ against time step Δt_s from (a) Lorenz system and (b) Chen system where $\varepsilon_{G,1}$ and $\varepsilon_{G,2}$ are the global errors from predicting time series with and without PRSK respectively.

Finally in this section wish to show that PRSK can also be used effectively against type (III) cryptanalysis techniques. This is because binary parameter switching events are masked by numerous false switching events from PRSK. The close and irregular switching patterns that never repeats itself causes different statistical properties' over different time intervals. In such a way, the two distinct statistical properties resulted from binary parameter switching is covered up in the midst of an infinite number of possible sets of statistical properties. Thus it is no longer possible for type (III) cryptanalysis techniques to detect the changes between two distinct sets of statistical properties. This claim is supported by the following example. Consider a Lorenz system given as

$$\begin{aligned}
\dot{x}_1 &= \mu_{x,1}(x_2 - x_1), \\
\dot{x}_2 &= (\mu_{x,2} - x_3)x_1 - x_2, \\
\dot{x}_3 &= x_1x_2 - \mu_{x,3}x_3.
\end{aligned} \tag{5.7}$$

Let $x_1(t)$ shown in Fig. 5.5(a) be the transmitted signal that is intercepted. From the parameter set $\mathbf{\mu}_x = [\mu_{x,1}, \mu_{x,2}, \mu_{x,3}]$, let $\mu_{x,1} = 10$, $\mu_{x,3} = 2$ and $\mu_{x,2}$ switches between the values of 62 and 60 in alternate interval of 10 time-units. Thus in a chaotic shift keying scheme [Parlitz et al., 1992], $\mu_{x,2}$ acts as a binary parameter switch that is used to encode a binary sequence $m(t)$ shown in Fig. 5.5(b). It was first thought that the encoded message is secure against an unauthorised receiver since the intruder, who has no knowledge of the parameter set $\mathbf{\mu}_x$, cannot retrieve the information through a synchronisation process [Pecora & Carroll, 1990] as shown in Fig. 5.5(c).

However, an intruder can unmask the information by analysing the statistical properties of the intercepted time series $x_1(t)$ with the existing characteristic cryptanalysis [Pérez & Cerdeira, 1995; Yang et al., 1998a, 1998b, 1998c; Storm & Freeman, 2002], which are the type (III) cryptanalysis techniques.

Here, the measurement of generalised synchronisation transformations [Yang et al., 1998c] is used to verify the effectiveness of PRSK against type (III) cryptanalysis techniques. This technique is chosen because it is, so far, the most powerful type (III) cryptanalysis technique that is easy to implement and effective even against complex high-dimensional chaotic. This technique uses the intercepted signal to drive an arbitrary system. Assume that the system employed by the intruder is identical to system (5.7) but with a parameter set estimated as

$\mu_y = [9.7, 57, 2.1]$. Since synchronisation cannot be achieved with such setting, the error variable $e_1(t) = x_1 - y$, thus does not respond to the binary switching events.

In order to detect the switching events, the moving average square error of $e(t)$ is computed to reflect changes in the statistical property of the intercepted time series.

The moving average square error of $e(t)$ is computed with the formula given as

$$\delta(t) = T_w^{-1} \int_t^{t+T_w} e^2(t) dt. \quad (5.8)$$

where $T_w > 0$ is the observation window length for the averaging. Using Eq. (5.8) with $T_w = 2.3$ time-units, a dynamical response of $\delta(t)$ is produced in Fig. 5.5(d), which corresponds to the binary sequence shown in Fig. 5.5(b) and thus exposing the binary switching events.

To demonstrate that PRSK can be used effectively to mask the binary switching events, design $\mu_{x,3} = g_3(x_2)$ according to the rule given in (5.3) with

$$[a_{3,1} \dots a_{3,8}] = [0, 5, 31, 33, 23, 28, 10, 16] \quad \text{and} \quad [b_{3,1} \dots b_{3,5}] = [10/3, 8/3, 2/3, 4/3, 2].$$

The dynamical response of $\delta(t)$ is reproduced in Fig. 5.5(e). From the figure, it is clear that the statistical properties of the intercepted signal $x_1(t)$ have been masked up. Fig. 5.5(e) shows that $\delta(t)$ no longer respond to the binary switching events.

Fig 5.5. Demonstration on the effectiveness of PRSK in masking statistical properties along an intercepted information carrier signal. (a) A chaotic time series from system (5.7) with the parameter set switching between two sets of values at alternate intervals of 10 time-units. (b) A binary sequence that correspond to the binary switching events. (c) The time variation of the error from a synchronisation process that responds to the binary switching events. (d) and (e) The moving average square error computed using Eq. (5.8) from a time series without and with PRSK respectively.

5.4 Higher order pseudo-random switching keys

The PRSK technique designed in Section 5.2 is one-dimensional in which the variation of the values depend only on a single state variable. In this section, a

more complex form of design for PRSK will be introduced. This form of design referred to as higher order PRSK makes use of more than one state variable to trigger changes in the values of PRSK. In fact, the number of state variable that can be used is equal to the dimension of the system involved. Hence in higher order PRSK, an n-dimensional chaotic attractor is used as reference instead of using the time evolution as shown in Fig. 5.1(b).

In this section a two-dimensional PRSK is illustrated using a Lorenz system given by the following three differential equations,

$$\dot{x}_1 = \mu_1 (x_2 - x_1), \quad \dot{x}_2 = (\mu_2 - x_3) x_1 - x_2, \quad \dot{x}_3 = x_1 x_2 - \mu_3 x_3. \quad (5.9)$$

The parameters μ_1 and μ_2 are set as 10 and 60 respectively and μ_3 is designed as 2D PRSK that depends on the evolutions of x_2 and x_3 . The design of μ_3 can be mathematically expressed as

$$\mu_3 = g_3(x_2, x_3) = b_{3,j}(\mathbf{x}, \boldsymbol{\mu}) \left\{ \begin{array}{l} \text{for } a_{3,j} \leq |x_2| < a_{3,j+1} \\ \quad \& \\ \text{for } c_{3,j} \leq |x_3| < c_{3,j+1} \end{array} \right. \quad (5.10)$$

and

$$g_3(x_2, x_3) = \begin{cases} b_{3,1}(\mathbf{x}, \mu) & \text{for } a_{3,1} \leq |x_2| < a_{3,2} \text{ and } c_{3,1} \leq |x_3| < c_{3,2} \\ b_{3,2}(\mathbf{x}, \mu) & \text{for } a_{3,2} \leq |x_2| < a_{3,3} \text{ and } c_{3,2} \leq |x_3| < c_{3,3} \\ b_{3,3}(\mathbf{x}, \mu) & \text{for } a_{3,3} \leq |x_2| < a_{3,4} \text{ and } c_{3,3} \leq |x_3| < c_{3,4} \\ b_{3,4}(\mathbf{x}, \mu) & \text{for } a_{3,4} \leq |x_2| < a_{3,5} \text{ and } c_{3,4} \leq |x_3| < c_{3,5} \\ b_{3,5}(\mathbf{x}, \mu) & \text{for } a_{3,5} \leq |x_2| < a_{3,6} \text{ and } c_{3,5} \leq |x_3| < c_{3,6} \\ b_{3,6}(\mathbf{x}, \mu) & \text{for } a_{3,6} \leq |x_2| < a_{3,7} \text{ and } c_{3,6} \leq |x_3| < c_{3,7} \\ b_{3,7}(\mathbf{x}, \mu) & \text{for } a_{3,7} \leq |x_2| < a_{3,8} \text{ and } c_{3,7} \leq |x_3| < c_{3,8} \\ b_{3,8}(\mathbf{x}, \mu) & \text{otherwise} \end{cases}$$

with

$$[a_{3,1} \dots a_{3,8}] = [-30, -20, -10, 0, 10, 20, 30, 40] \quad (5.11)$$

$$[b_{3,1} \dots b_{3,8}] = \left[\frac{12}{4}, \frac{11}{4}, \frac{10}{4}, \frac{9}{4}, \frac{8}{4}, \frac{7}{4}, \frac{6}{4}, \frac{5}{4} \right]$$

$$[c_{3,1} \dots c_{3,8}] = [20, 30, 40, 50, 60, 70, 80, 90]$$

Fig. 5.6 shows a chaotic attractor used as reference to trigger changes in the values of PRSK. The horizontal and vertical lines in the background mark the values of $a_{3,1}$ to $a_{3,8}$ and $c_{3,1}$ to $c_{3,8}$.

Fig. 5.6. A chaotic attractor used as reference to trigger changes in the values of PRSK.

Fig. 5.7. (a) Time evolution of x_1 from the Lorenz system (5.9). (b) Time evolution of the 2D PRSK μ_3 according to (5.11).

5.5 Synchronisation of pseudo-random switching keys

As the functioning of chaos-based secure communication is dependent on chaos synchronisation, in particular on identical synchronisation, it becomes essential that synchronous behaviour must be realisable in coupled systems incorporated with pseudo-random switching keys. This thesis reports the observation of identical synchronisation in coupled systems incorporated with pseudo-random switching keys [Xu & Chee, 2003]. This form of synchronisation will be shown and explained in this section. This observation opposes the earlier belief that identical synchronisation can only be realised with identical and fixed system parameters.

To demonstrate that synchronisation between a drive and response system is realisable even with parameters mismatched at the initial condition, this section consider a coupled Lorenz system given as

$$\begin{aligned}
 & \left. \begin{aligned} \dot{x}_1 &= \mu_{x,1}(x_2 - x_1) \\ \dot{x}_2 &= (\mu_{x,2} - x_3)x_1 - x_2 \\ \dot{x}_3 &= x_1x_2 - \mu_{x,3}x_3 \\ \mu_{x,3} &= g_3(x_2) \end{aligned} \right\} \text{Drive System,} \\
 & \left. \begin{aligned} \dot{y}_1 &= \mu_{y,1}(y_2 - y_1) \\ \dot{y}_2 &= (\mu_{y,2} - y_3)x_1 - y_2 \\ \dot{y}_3 &= x_1y_2 - \mu_{y,3}y_3 \\ \mu_{y,3} &= g_3(y_2) \end{aligned} \right\} \text{Response System.}
 \end{aligned} \tag{5.12}$$

The drive system drives the response system using the variable x_1 . The parameters $\mu_{x,1}=10$ and $\mu_{x,2}=60$. The symbol y is used to represent both x and y . The third parameter $\mu_{x,3}$ is assigned as PRSK that is designed according to (5.13).

$$g_3(\gamma_2) = \begin{cases} b_{3,1} & \text{for } a_{3,1} < |\gamma_2| < a_{3,2} \\ b_{3,2} & \text{for } a_{3,3} < |\gamma_2| < a_{3,4} \\ b_{3,3} & \text{for } a_{3,5} < |\gamma_2| < a_{3,6} \\ b_{3,4} & \text{for } a_{3,7} < |\gamma_2| < a_{3,8} \\ b_{3,5} & \text{otherwise} \end{cases} . \tag{5.13}$$

According to (5.13), the state variables x_2 and y_2 are used as reference. The constants $[a_{1,1} \dots a_{1,8}] = [0, 5, 31, 33, 23, 28, 10, 16]$ and

$[b_{1,1} \dots b_{1,5}] = [10/3, 8/3, 2/3, 5/3, 2]$. The initial conditions are randomly selected as

$$[x_1, x_2, x_3, y_1, y_2, y_3] = [-5, -6, -2, 3, -2, 4].$$

Although the drive and response system possess the same system parameters, different initial conditions between the two systems cause a mismatch of PRSK. To examine whether the mismatch of $\mu_{x,3}$ and $\mu_{y,3}$ persists with time, numerous numerical trials were conducted with arbitrarily selected initial conditions. The test results show that synchronisation eventually occurs under PRSK and an initial mismatch of $\mu_{x,3}$ and $\mu_{y,3}$ does not bring about long-term difference between the drive and response systems. To explain this phenomenon, the parameters $\mu_{x,3}$ and $\mu_{y,3}$ could be seen as the fourth variable of their respective systems governed by the rule $g_3(\gamma_2)$. At same point of time the variables x_2 and y_2 will fall within the same state space defined by $g_3(\gamma_2)$. As a result, PRSK will assign the same parameter value for the drive and response systems such that the two systems tend to a synchronous behaviour. Since the variables x_2 and y_2 are chaotic, the ergodicity of chaos will eventually bring the two chaotic trajectories close to each other causing $g_3(x_2)$ and $g_3(y_2)$ to synchronise.

To illustrate the occurrence of this phenomenon, Fig. 5.8(a) shows the evolutions of x_2 and y_2 with the horizontal lines marking the values of $a_{1,1}$ to $a_{1,8}$. By comparing Fig. 5.8(a) and (b), it can be observed that an immediate and concurrent result of $\mu_{x,3} = \mu_{y,3}$ occurring when x_2 and y_2 come between a pair of adjacent lines at the same instant. Some spikes are observed in Fig. 5.8(b) when x_2 and y_2 come close after $t > 2$. The spikes appear when x_2 and y_2 cross the boundary lines defined by $a_{3,j} < |x_2| \leq a_{3,j+1}$ because x_2 and y_2 are separated by

the boundary line although they are very close to each other. The mismatch of the parameters last only for an extremely short time span during the crossing of the boundary lines. Therefore, the parameter mismatch due to crossing the boundary lines will not significantly affect the synchronisation process. As such identical synchronisation is always observable under the pseudo-random parameter switching events. Fig. 8.5(c) shows the error dynamics $\lim_{t \rightarrow \infty} e_1 = \lim_{t \rightarrow \infty} (x_1 - y_1) = 0$. This indicates the occurrence of identical synchronisation between the drive and response systems.

Fig. 5.8. Demonstration on the robustness of synchronisation with initial mismatch of PRSK. (a) Time evolution of x_2 (red line) and y_2 (blue line). (b) Mismatch between $g_3(x_2)$ and $g_3(y_2)$, which indicates the difference between $\mu_{x,3}$ and $\mu_{y,3}$. (c) Time evolution of the error dynamics $e_1 = x_1 - y_1$. The occurrence $\lim_{t \rightarrow \infty} e_1 = 0$ indicates the realisation of identical synchronisation.

Chapter 6

Transmission of M-ary digital signals using controlled projective synchronisation

This chapter introduces a new technique for transmitting digital information using projective synchronisation of coupled chaotic systems with control [Chee & Xu, 2004a]. Using the control algorithm developed in Section 4.1 [Xu & Chee, 2002], this technique shifted chaos-based digital communication to truly M-ary transmission where each digital symbol can now consist of more than one bit, which allows a faster transmission rate without increasing the system complexity.

Furthermore, numerical results show that the proposed technique is superior over conventional and other chaos-based digital communication techniques in terms of bit error rate at low E_b/N_0 . Hence, this becomes the first chaos-based communication technique to show better performance when compared with conventional techniques in single-user environment.

6.1 Introduction

The idea of using a chaotic signal as the carrier to transmit digital information was first proposed in a technique known as chaotic shift keying [Parlitz *et al.*, 1992]. This technique was developed to explore the potential utilisation of chaotic signals for encryption and spread spectrum communication applications. It is known that spread spectrum technique was first introduced as an anti-jamming

technique for military purposes and the motivation to achieve highly jam-resistant communications systems subsequently resulted in an assortment of the techniques in areas such as multipath access.

In recent years, a number of chaos-based schemes [Sushchik *et al.*, 2000; Kolumban, 2001] have been proposed with the intention of providing a simple solution for robust wideband communications. For spread spectrum communication, a chaotic signal with its inherent wideband characteristic, offers the cheaper alternative to conventional methods [Kennedy *et al.*, 1998; Kolumbán, 2000]. Furthermore, due to a lower cross correlations between segments of chaotic waveforms than between segments of periodic waveforms, a chaotic signal will also generate better performance under multipath propagation conditions.

However, chaos-based techniques still face two major challenges from conventional techniques in term of bit error rate (BER) and transmission rate. Firstly, chaos-based techniques exhibit poor BER performances. So far in terms of BER performances, the two more promising chaos-based techniques, namely symbol dynamics - differential chaos shift keying (SD-DCSK) [Maggio & Galias, 2002] and ergodic chaos shift keying (ECSK) [Leung *et al.*, 2002] are still inferior to conventional techniques such as phase shift keying (PSK) and frequency shift keying (FSK) [Sklar, 2002] when comparisons are made over additive white Gaussian noise (AWGN) channel. Some of these BER evaluations and comparisons can be found in the literature [Leung *et al.*, 2002; Kennedy *et al.*, 1998; Galias & Maggio, 2001]. Secondly, most chaos-based techniques were developed for binary-only transmission where each transmitted digital symbol

consists only 1 bit of information. This reduces the efficiency of chaos-based techniques in terms of transmission rate. Therefore, transmission of symbols with more than one bit, referred to as M-ary transmission, has been proposed in conjunction with chaos-based techniques [Kolumbán *et al.*, 1997; Kennedy *et al.*, 1998; Galias & Maggio, 2001]. However implementing these techniques result in further degradation of BER performance relative to the conventional techniques and require an increase of the system complexity.

To overcome these major challenges, this chapter introduces a new digital communication technique [Chee & Xu, 2004a] that uses projective synchronisation of coupled chaotic systems [Mainieri & Rehacek, 1999] with control [Xu & Chee, 2002]. This development is considered essential and important to chaos-based digital communication as it allows flexibility in choosing higher bits per symbol without increasing the system complexity, which previously was not possible. On top of this, it is the first chaos-based technique that outperforms the conventional techniques in terms of BER performances.

6.2 Mechanism of digital communication system based on controlled projective synchronisation

The setup of a communication system based on controlled projective synchronisation consists of a drive system at the transmitter end and a response system at the receiver end. The coupled system with the drive system driving the response system with the variable $z_x(t)$ is expressed by

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \boldsymbol{\xi} \\ \dot{z}_x &= g(\mathbf{x}, z_x) \end{aligned} \right\} \text{Drive System,} \quad (6.1)$$

$$\left. \begin{aligned} \dot{\mathbf{y}} &= \mathbf{M}(z_x) \cdot \mathbf{y} \\ \dot{z}_y &= g(\mathbf{y}, z_y) \end{aligned} \right\} \text{Response System.}$$

In the coupled system (6.1), the state vectors $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and $\mathbf{y} = [y_1, y_2, \dots, y_n]^T$ relate linearly with their respective time derivatives $\dot{\mathbf{x}}$ and $\dot{\mathbf{y}}$ through the Jacobian matrices $\mathbf{M}$ and the variables z_x and z_y are related nonlinearly to $\mathbf{x}$ and $\mathbf{y}$. According to this arrangement, the drive and response systems are effectively partially linear system. In (6.1), z_x is used to couple the linear portion of the response system, therefore projective synchronisation will be observed as described in Section 3.1.

In the coupled system (6.1), the control vector $\boldsymbol{\xi} = [\xi_1, \xi_2, \dots, \xi_n]^T$ introduced in section 4.1 is employed to direct the proportional relationship between $\mathbf{x}$ and $\mathbf{y}$ to the desired scaling factor, α^* . The control function is formulated as

$$\xi_i = -[\mathbf{m}_i \mathbf{e} + k e_i] / \alpha^*, \quad \text{for } i=1, 2, \dots, n. \quad (6.2)$$

The row matrix $\mathbf{m}_i$ is the i th row of $\mathbf{M}$ and k is the slack constant as defined in Section 4.1. With control input from $\boldsymbol{\xi}$, the relationship between $\mathbf{x}$ and $\mathbf{y}$ can be expressed as $\lim_{t \rightarrow \infty} \|\alpha^* \mathbf{x} - \mathbf{y}\| = 0$. As a consequent, the proportional relationship $\lim_{t \rightarrow \infty} \|(\alpha^*)^b z_x - z_y\| = 0$ arises. The index constant b depends on the nonlinear system used and is independent of the system parameters and initial conditions.

The development of the control algorithm allows the scaling feature of projective synchronisation to be employed for M-ary digital communication. To do

Chapter 6 Projective synchronisation in digital communication

so, a unique desired scaling factor is assigned to each digital symbol. The control function (6.2) can then be used to fulfil the assignment of the desired scaling factors according to the digital symbols. To facilitate further description of the technique a coupled Lorenz system is employed, given as

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \boldsymbol{\xi} \\ \dot{z}_x &= g(\mathbf{x}, z_x) \end{aligned} \right\} \text{Drive System,}$$

$$\left. \begin{aligned} \dot{\mathbf{y}} &= \mathbf{M}(z_x) \cdot \mathbf{y} \\ \dot{z}_y &= g(\mathbf{y}, z_y) \end{aligned} \right\} \text{Response System.} \quad (6.3)$$

Fig.6.1 shows a configuration of this communication scheme with the system parameters assigned as $[\mu_1, \mu_2, \mu_3] = [10, 60, 2]$ and $k = 100$. The transmitter generates the information carrier signal z_x from the drive system to drive the response system at the receiver end. In order to transmit the intended information, the digital symbols to be transmitted must first be encoded onto pre-assigned desired scaling factors and then input into the control function (6.2). Here the assignment of desired scaling factors to digital symbols is carried out in accordance to Gray coding, see Table 6.1. An example is shown in Table 6.1 for $M = 8$, where $M = 2^\beta$ and $\beta = 3$ is the number of bits per symbol.

Fig. 6.1. Schematic of a controlled projective synchronisation digital communication scheme based on coupled Lorenz system (6.2).

Digital Symbol	Decimal Value	Desired Scaling Factor, α^*
000	0	1
001	1	2
011	3	3
010	2	4
110	6	5
111	7	6
101	5	7
100	4	8

Table 6.1. Assignment of desired scaling factors to M -ary digital symbols according to Gray coding with $M = 8$. The first column shows the digital symbols and the decimal values are given in the second column. The assigned desired scaling factors to the respective symbols are given in the third column. Note that according to Gray coding, each unit increment of the scaling factor has the corresponding symbol having only one bit difference from the previous symbol.

At the receiver end, the receiver sends feedback signals, y_1 and y_2 to the transmitter end. This is required for eliminating the error vector in the control function (6.2), so that projective synchronisation can occur according to the desired scaling factors. Besides being a necessary input to eliminate the error vector, the feedback signals are also desirable as a form of authentication and check when the technique is used for anti-jamming applications. Meanwhile, the desired scaling factors are retrieved by computing

$$\hat{\alpha}^* = \sqrt[b]{z_y / z_x + N} \quad (6.4)$$

with input from the received signal $z_x + N$ and the self-generated signal z_y . For the coupled Lorenz systems, b in Eq. (6.4) is equals to 2 and N denotes channel noise. Decoding is then carried out to retrieve the transmitted symbols from the computed scaling factors, $\hat{\alpha}^*$

6.3 Numerical experiments

This section describes an example that demonstrates M-ary transmission using controlled projective synchronisation according to the setup shown in Fig. 6.2(a) with $M = 8$. Fig. 2(a) shows the intended digital symbols transmitted to the receiver. The symbol duration used here is equal to 5 time-units. The typical transmitted signals, $z_x(t)$ of 5 time-units duration, from the Lorenz system (6.3) over AWGN channel with no noise and $E_b/N_0 = 10\text{dB}$ are shown in Fig. 6.3(a) and (b) respectively. N_0 denotes additive white Gaussian noise. Fig. 6.2(b) shows the computed scaling factor at the receiver end with zero channel noise, $N = 0$.

Chapter 6 Projective synchronisation in digital communication

The proportional relationship between the drive and response systems converges to a constant value after approximately 2 time-units. Hence this allows the digital symbols to be retrieved accurately with no errors. This can be checked by comparing the transmitted symbols and the desired scaling factors given in Fig 6.2(a) and (b) with the applied Gray coding shown in Table 6.1.

However, the BER performance of this scheme is graded when noise is added to the channel. Fig. 6.2(c) shows the computation of the scaling factor at the receiver end with AWGN of $E_b/N_0 = 10\text{dB}$ added to the channel. It can be seen that under the influence of noise the scaling factor fluctuates around a constant within each symbol duration. To retrieve the transmitted symbols from the varying scaling factor and reduce the effect of noise, the average value of the scaling factor is computed for each symbol duration before rounding off to the nearest integer that is bounded between 0 and $M - 1$. As shown in Fig. 6.2(d), the average value before rounding off is indicated by the vertical line at the end of each symbol duration and the cross indicates the rounded off value, which is the retrieved scaling factor. There is an error bit occurred at $t = 35$.

Fig. 6.2. Decoding process at the receiver end with symbol duration of 5 time-units. (a) The intended digital symbols to be transmitted to the receiver. (b) The computed scaling factors at the receiver end with no channel noise. (c) The computed scaling factors at the receiver end with AWGN of $E_b/N_0 = 10\text{dB}$ added to the channel. (d) The average of the scaling factors at the end of each symbol duration indicated by the vertical lines with the crosses indicating the rounded off values.

Fig. 6.3. Sample transmitted signal, $z_x(t)$, of 5 time-units. (a) Signal transmitted over channel with no noise, $N = 0$. (b) Signal transmitted over AWGN channel with $E_b/N_0 = 10\text{dB}$

It is stated earlier that the proposed digital communication technique is the first chaos based technique, and presently the only one to exhibited better BER performances against the conventional techniques. To demonstrate this claim, BER performances obtained from numerical experiment are used to comparison. Fig. 6.4 shows the BER performances of binary transmission using different techniques. In this figure, the BER performance of digital communication using controlled projective synchronisation (PS) is compared with coherent binary phase shift keying (BPSK), which is a conventional technique and ergodic chaotic parameter modulation (ECPM) [Leung *et al*, 2002] and differential chaos shift keying (DCSK) [Kolumbán *et al.*, 1998], which are chaos-based techniques. These techniques are selected for comparison due to their outstanding BER performances under their respective classification. The results from Fig. 6.4 showed that for binary transmission, PS clearly outperformed the other techniques in terms of BER performance.

In the comparison of BER performances for M-ary transmission, $M > 2$, shown in Fig. 6.5, the performance of PS as compared to the other techniques is not as straight forward as the binary case. For the purpose of comparison, conventional technique coherent M-ary phase shift keying (MPSK) and chaos-based technique quadrature chaos shift keying (QCSK) [Galias & Maggio, 2001] are used to compare with PS. In Fig. 6.5, the BER performance curves for PS are plotted for M equals to 4, 8 and 16. For MPSK, the curves are plotted for M equals to 4 and 8. QCSK as the name suggested has $M = 4$. In the figure, when PS with $M = 4$ is compared to chaos-based QCSK, PS outperformed QCSK across the whole range

of E_b/N_0 shown on the graph. However when compared to MPSK the BER performance of PS with M equal to 4 and 8 is only superior at lower E_b/N_0 range up to 4.6dB and 7.6dB respectively.

Fig. 6.4. The BER performance results for binary symbols transmission. The BER performance of controlled projective synchronisation technique (PS) is compared with the conventional technique represented by coherent binary phase shift keying (BPSK) and two chaos-based techniques represented by ergodic chaotic parameter modulation (ECPM) and differential chaos shift keying (DCSK).

Fig. 6.5. The BER performance results for M-ary symbols transmission. The BER performance of controlled projective synchronisation technique (PS) is compared with the conventional technique represented by M-ary phase shift keying (MPSK) and chaos-based technique represented by quadrature chaos shift keying (QCSK).

In conclusion, this chapter proposed a chaos-based digital communication technique using controlled projective synchronization. This technique enables the transmission of binary symbols as well as M-ary symbols by utilizing only a simple coupled chaotic system. The development of this technique contributes to chaos-based digital communication in two areas. Firstly, so far to our knowledge this is the first and only chaos-based technique that has superior BER performance over the conventional techniques. Secondly, the proposed technique shifted chaos-based digital communication to a truly M-ary transmission process. This allows faster transmission rate by increasing bits per symbol without increasing the system complexity.

Transmission of Images Through Additive White Gaussian Noise Channel

Original Image

$E_b/N_0 = 5\text{dB}$

$E_b/N_0 = 10\text{dB}$

$E_b/N_0 = 15\text{dB}$

Fig. 6.6. Digital images transmitted using controlled projective synchronisation over AWGN channel. Clockwise from top left hand corner: original image, image transmitted over channel with signal to noise ratio of $E_b/N_0 = 5\text{dB}$, 15dB and 10dB .

Chapter 7

Secure digital communication using controlled projective synchronisation

This chapter proposes a new chaotic encryption approach to mask digital information using controlled projective synchronisation [Chee & Xu, 2005]. The scheme encrypts a binary sequence by manipulating the scaling feature of synchronisation from the coupled system. The transmitted signal therefore embeds only a single set of statistical properties. This prevents cryptanalysts from breaking the chaotic encryption scheme by using characteristic cryptanalysis that aims to detect switching of statistical properties in the intercepted information carrier signal. The techniques of using a pseudo-random switching key is incorporated into the scheme to mask out the deterministic nature of the underlying coupled system.

7.1 Introduction

Encryption schemes based on chaotic shift keying (CSK) employ the basic concept of chaos synchronisation [Pecora and Carroll, 1990] in the process. The communication setup consists of two identical chaotic systems with one system (drive system) at the transmitter end driving the other system (response system) at the receiver end using a state variable of the drive system, which is referred to as a coupling variable. To transmit digital signals, the coupling variable, which is the

information carrier signal, is produced at the drive system by slightly shifting a parameter according to the binary sequence.

CSK has its security flaws since the binary message is encrypted by shifting the parameter sets between two fixed sets of values. This will inevitably cause the transmitted signal to possess two sets of statistical properties that correspond to bit 0 and bit 1. Hence, the encrypted information could be easily revealed by detecting switches of statistical properties within the intercepted information carrier signal. The detection techniques which are collectively referred to as characteristic cryptanalysis include constructing attractors from return maps [Pérez & Cerdeira, 1995; Yang *et al.*, 1998a], using a spectrogram [Yang *et al.*, 1998b], measuring the errors from generalised synchronisation transformations [Yang *et al.*, 1998c] and measuring the weighted density of localised dynamics about a test trajectory [Storm & Freeman, 2002]. Another weakness found in CSK schemes is the deterministic nature of the transmitted signal. Although the transmitted signal exhibits chaotic behaviour that appeared to be random, it is always governed by an underlying deterministic rule. Cryptanalysts thus exploit the deterministic nature of chaos by using reconstruction methods to recover the governing rule and then extract the encrypted information from the transmitted signal without prior knowledge of the underlying system. The methods include parameter detection [Stojanovski *et al.*, 1996], neural networks analysis [Yang *et al.*, 1998d], wavelet multi-scale decomposition [Huang *et al.*, 2001] and delay-coordinate reconstruction [Ponomarenko & Prokhorov, 2002].

These explored security flaws weaken the confidence on the use of the CSK scheme. In spite of this, extensions of CSK have being developed to enhance the security. The derivation for higher security include the utilization of multi-channel communications to achieve higher complexity [Sundar & Minai, 2000] and the application of phase synchronisation to chaos communication by using the mean value of two corresponding variables to obtain the instantaneous phase and operating it as the transmitted signal [Chen *et al.*, 2003]. However, in the strictest sense, these schemes that are based on the original idea of CSK still require two chaotic attractors to encrypt the binary sequence and therefore a probable attack from characteristic cryptanalysis remains.

In this chapter, a new chaotic encryption approach to mask digital information using controlled projective synchronisation is developed. This new technique, which is different from CSK, does not require the shifting of parameter values but transmits digital signals by manipulating the scaling feature of projective synchronisation [Mainieri & Rehacek, 1999].

In projective synchronisation, two identical systems are employed with one system (*drive system*) at the transmitter end driving the other system (*response system*) at the receiver end using the information carrier signal. The evolution of the response system is asymptotically a scalar multiple of the evolution of the drive system [Mainieri & Rehacek, 1999] with the dynamics of the response system converging to the required state to fulfil the desired scalar multiple. Therefore, in a projective synchronisation scheme the transmitter uses only a single attractor to encrypt a binary sequence by manipulating the scaling features of the coupled

system with control [Xu & Chee, 2002]. The receiver then retrieves the information by observing changes in the scalar multiple between the transmitted signal and the corresponding variable of the response system. This is a desirable feature since the characteristic cryptanalysis will be rendered ineffective to reveal the encrypted information from the intercepted signal. On top of this pseudo-random switching key [Xu & Chee, 2003] is incorporated into the scheme to prevent reconstruction methods from uncovering the underlying governing rule of the coupled system.

7.2 Secure communication scheme

The standard setup of a chaos-based digital communication scheme that employs controlled projective synchronisation consists of two partially linear systems with a drive system at the transmitter end coupling a response system at the receiver end with a information carrier signal z_x . The coupled system is expressed as

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \xi \\ \dot{z}_x &= f(\mathbf{x}, z_x) \end{aligned} \right\} \text{Drive System,} \\ \left. \begin{aligned} \dot{\mathbf{y}} &= \mathbf{M}(z_x) \cdot \mathbf{y} \\ \dot{z}_y &= f(\mathbf{y}, z_y) \end{aligned} \right\} \text{Response System.} \quad (7.1)$$

Adding PRSK into system (7.1) gives

$$\left. \begin{aligned} \dot{\mathbf{x}} &= \mathbf{M}(z_x) \cdot \mathbf{x} + \boldsymbol{\xi} \\ \dot{z}_x &= f(\mathbf{x}, z_x) \\ \boldsymbol{\mu}_x &= \mathbf{g}(\mathbf{x}) \end{aligned} \right\} \text{Drive System,}$$

$$\left. \begin{aligned} \dot{\mathbf{y}} &= \mathbf{M}(z_y) \cdot \mathbf{y} \\ \dot{z}_y &= f(\mathbf{y}, z_y) \\ \boldsymbol{\mu}_y &= \mathbf{g}(\mathbf{y}) \end{aligned} \right\} \text{Response System.}$$
(7.2)

It can be noted from system (7.2) that the control vector $\boldsymbol{\xi} = [\xi_1, \xi_2, \dots, \xi_n]^T$ which is given in (4.10) where $\xi_i = -[\mathbf{m}_i \mathbf{e} + \kappa_i e_i] / \alpha^*$ and $i = 1, 2, \dots, n$ requires feedback from the response system. However, by sending butfeedback signals from the response system will breach the security of the proposed scheme. This is because once the feedback signals, which respond to the changes in the desired scaling factor are intercepted, the information could easily be revealed. In order to overcome this problem, the proposed chaotic encryption scheme is designed as

$$\left. \begin{aligned} \dot{\mathbf{x}}_1 &= \mathbf{M}(\zeta_x) \mathbf{x}_1 & \dot{\mathbf{x}}_2 &= \mathbf{M}(z_{x,2}) \mathbf{x}_2 + \boldsymbol{\xi} \\ \dot{z}_{x,1} &= f(\mathbf{x}_1, z_{x,1}) & \dot{z}_{x,2} &= f(\mathbf{x}_2, z_{x,2}) \\ \boldsymbol{\mu}_x &= \mathbf{g}(\mathbf{x}_1) & \boldsymbol{\mu}_x &= \mathbf{g}(\mathbf{x}_1) \end{aligned} \right\} \text{Transmitter end,}$$

$$\left. \begin{aligned} \dot{\mathbf{y}} &= \mathbf{M}(\zeta_y) \mathbf{y} \\ \dot{z}_y &= f(\mathbf{y}, z_y) \\ \boldsymbol{\mu}_y &= \mathbf{g}(\mathbf{y}) \end{aligned} \right\} \text{Receiver end.}$$
(7.3)

A schematic diagram is provided in Fig. 7.1. The transmitter now consists of two systems denoted by subscripts 1 and 2 with the state vectors given as $\mathbf{x}_1 = [x_{1,1}, x_{1,2}, \dots, x_{1,n}]^T$ and $\mathbf{x}_2 = [x_{2,1}, x_{2,2}, \dots, x_{2,n}]^T$. The state vector $\mathbf{x}$, serves as a reference state for the control $\boldsymbol{\xi}$ to eliminate the dependency on feedback signals from the response system. For time $t < T_c$, the variables ζ_x and ζ_y are set as

$\zeta_x = z_{x,1}$ and $\zeta_y = z_y$. At the same time, a variable from the state vector $\mathbf{x}_1$ is used to couple the response system at the receiver end such that y_i is replaced by $x_{1,i}$ to achieve identical synchronisation [Pecora and Carroll, 1990]. The initiation time span before the actual transmission of the information is carried out is denoted by T_c which must be sufficiently large in order for the limit $\lim_{t \rightarrow T_c} |\mathbf{x}_1 - \mathbf{y}| = \mathbf{0}$ to occur. At $t = T_c$, the coupling between the drive and response systems through $x_{1,i}$ ceases and this is replaced with $z_{x,2}$ such that $\zeta_x = \zeta_y = z_{x,2}$ to achieve projective synchronisation. Note that once identical synchronisation is achieved between drive system 1 and response system through the coupling variable $x_{1,i}$, the future time evolutions of the two systems will always remain identical even with $x_{1,i}$ being replaced back by y_i in the response system. Hence, at the instant $t = T_c$ when these two systems are coupled simultaneously to drive system 2 through $z_{x,2}$, they will projectively synchronise in a similar manner with respect to system 2. Thus this allows the control function to be redesigned as

$$\xi_i = -[\mathbf{m}_i \mathbf{e}_x + \kappa_i e_{x,i}] / \alpha^* \quad (7.4)$$

with $\mathbf{e}$ given in (4.10) being replaced by the error vector $\mathbf{e}_x = [e_{x,1}, e_{x,2}, \dots, e_{x,n}]^T = \alpha^* \mathbf{x}_2 - \mathbf{x}_1$ and $i = 1..n$. $\mathbf{m}_i$ is the i th row of the matrix $\mathbf{M}$, κ_i is the slack constant as explained in (4.7) and α^* is the desired scaling factor. This allows the scaling factor to be manipulated with feedback signals directly obtained within the transmitter end. By doing so, the drive system at the

transmitter end no longer requires feedback signals from the response system. This eliminated the risk of the information being revealed by sending feedback signals from the response system through the communication channel.

Fig. 7.1. Schematic of controlled projective synchronisation secure digital communication scheme based on system (7.3). Note that for $t < T_c$, $x_{1,i}$ from $\mathbf{x}_1$ is used as the coupling variable to drive the response system. Here, the choice of $x_{1,1}$ is used only as an example. In fact any variable from $\mathbf{x}_1$ can be used as long as identical synchronisation is achievable between the transmitter system 1 and the response system.

To illustrate a controlled projective synchronisation based scheme, consider a coupled Lorenz system that is designed according to (7.3), given as

$$\left. \begin{aligned} \dot{x}_{1,1} &= \mu_1 (x_{1,2} - x_{1,1}) \\ \dot{x}_{1,2} &= (\mu_{x,2} - \zeta_x) x_{1,1} - x_{1,2} \\ \dot{z}_{x,1} &= x_{1,1} x_{1,2} - \mu_3 z_{x,1} \\ \mu_{x,2} &= g_2 (x_{1,1}) \end{aligned} \right\} \text{Transmitter End,}$$

$$\left. \begin{aligned} \dot{x}_{2,1} &= \mu_1 (x_{2,2} - x_{2,1}) + \xi_1 \\ \dot{x}_{2,2} &= (\mu_{x,2} - z_{x,2}) x_{2,1} - x_{2,2} + \xi_2 \\ \dot{z}_{x,2} &= x_{2,1} x_{2,2} - \mu_3 z_{x,2} \\ \mu_{x,2} &= g_2 (x_{1,1}) \end{aligned} \right\} \text{Receiver End.}$$

(7.5)

In this scheme, when $t < T_c$, the variables ζ_x and ζ_y are set as $\zeta_x = z_{x,1}$, $\zeta_y = z_y$ and in the response system, $\psi_1 = x_{1,1}$. Thus the transmitted signal $s(t)$ is equal to $x_{1,1}$. When $t \geq T_c$, ζ_x and ζ_y are set as $\zeta_x = \zeta_y = z_{x,2}$, $\psi_1 = y_1$ and the transmitted signal $s(t) = z_{x,2}$. An initiation time span of $T_c = 10$ time-units will be sufficient to achieve identical synchronisation between drive system 1 and the response system. The system parameters are set as $\mu_1 = 10$ and $\mu_3 = 2$. The pseudo-random switching key $\mu_{\gamma,2}$ is designed as

$$\mu_{\gamma,2} = g_2(\gamma_1) = \begin{cases} b_{1,1} & \text{for } a_{1,1} < |\gamma_1| < a_{1,2} \\ b_{1,2} & \text{for } a_{1,3} < |\gamma_1| < a_{1,4} \\ b_{1,3} & \text{for } a_{1,5} < |\gamma_1| < a_{1,6} \\ b_{1,4} & \text{for } a_{1,7} < |\gamma_1| < a_{1,8} \\ b_{1,5} & \text{otherwise} \end{cases} \quad (7.6)$$

The symbol γ_1 is used to represent the variables x and y . The constants are assigned as $[a_{1,1} \dots a_{1,8}] = [0, 5, 10, 16, 23, 27, 30, 34]$ and $[b_{1,1} \dots b_{1,5}] = [60, 60.5, 59.5, 49, 49.5]$. Fig. 7.2(a) shows the transmitted signal $s(t) = x_{1,1}$ for $t < 10$ and $s(t) = z_x$ for $t \geq 10$. The information signal $m(t)$ is in an alternate sequence of bit 0 and bit 1 as shown in Fig. 7.2(b). In the control function $\xi_i = -[\mathbf{m}_i \mathbf{e}_x + k_i e_{x,i}] / \alpha^*$, the slack constant is set as $k_i = 10$ for $i = 1, 2$. The desired scaling factor is pre-assigned as $\alpha^* = 0.999$ to represent bit 0 and $\alpha^* = 1$ to represent bit 1.

Fig. 7.2(c) shows the time evolution of the scaling factor $\alpha_z(t) = z_y / z_{x,2}$ that is computed at the receiver end. For Lorenz systems under projective synchronisation, the scaling factor α_z , which is the ratio between $z_{x,2}$ and z_y , is equal to the square of $\alpha(t) = \|\mathbf{y}\| / \|\mathbf{x}_2\|$ such that $\lim_{t \rightarrow \infty} \alpha_z = (\alpha^*)^2$ (refer to section 3.1). Therefore at the receiver end, a bit 0 is received when $\alpha_z(t) = 0.998$ is observed and bit 1 is received when $\alpha_z(t) = 1$ is observed. Fig. 7.2(d) shows the time evolution of the switching events generated by the secret key $\mu_{x,2}$ for $(20 \leq t \leq 30)$. The switching events appear to be irregular and densely distributed.

Fig. 7.2. Demonstration of a chaotic encryption scheme based on projective synchronisation with a pseudo-random switching key incorporated. (a) The transmitted signal $s(t)=x_{1,1}$ for $t < 10$ and $s(t)=z_{x,2}$ for $t \geq 10$. (b) A binary sequence to be transmitted $m(t)$. (c) The time evolution of the scaling factor $\alpha_z(t) = z_y/z_{x,2}$ observed at the receiver end with $\alpha_z(t)=0.998$ representing bit 0 and $\alpha_z(t)=1$ representing bit 1. (d) The rapid and irregular changes of the parameter $\mu_{x,2}$ defined by the pseudo-random switching key (7.5) for $(20 \leq t \leq 30)$.

7.3 Security analysis

In this section the security of the projective synchronisation approach against characteristic cryptanalysis will be analysed. The security analysis is carried out by first demonstrating how characteristic cryptanalysis could be employed to break

CSK scheme. A similar demonstration will then be carried out on the projective synchronisation scheme to prove that the fundamental basis of characteristic cryptanalysis is ineffective against the proposed approach.

Here a characteristic cryptanalysis technique proposed by [Yang *et al.*, 1998c] is used to carry out the demonstration. This technique as described in Section 5.3 uses the intercepted information carrier signal to couple an arbitrary system. As a result, synchronisation error $e(t)$ may arise since the arbitrary system would probably not be identical to the drive system. However, given that the information carrier signal in CSK scheme is generated by shifting a parameter of the drive system, the error measured from the generalized synchronisation transformation will inevitably possess two sets of statistical properties according to the binary sequence. The intruder could then reveal these two sets of statistical properties by simply measuring the moving average of the error, given as $\delta(t) = T_w^{-1} \int_t^{t+T_w} e^2(t) dt$ where T_w is the window length. This characteristic cryptanalysis technique [Yang *et al.*, 1998c] is chosen for demonstration here because it is simple in implementation and very effective in breaking CSK schemes operating on both low and high dimensional systems.

For the demonstration, consider the drive, response and arbitrary systems in a CSK setup given as

$$\begin{aligned}
& \left. \begin{aligned} \dot{x}_1 &= \mu_1 (x_2 - x_1) \\ \dot{x}_2 &= (\mu_2 - z_x) x_1 - x_2 \\ \dot{z}_x &= x_1 x_2 - \mu_3 z_x \end{aligned} \right\} \text{Drive System} & \left. \begin{aligned} \dot{y}_1 &= 10(y_2 - y_1) \\ \dot{y}_2 &= (60 - z_y) x_1 - y_2 \\ \dot{z}_y &= x_1 y_2 - 2z_y \end{aligned} \right\} \text{Response System} \\
& \left. \begin{aligned} \dot{y}_{a,1} &= 11(y_{a,2} - y_{a,1}) \\ \dot{y}_{a,2} &= (60 - z_a) x_1 - y_{a,2} \\ \dot{z}_a &= x_1 y_{a,2} - 1.7z_a \end{aligned} \right\} \text{Arbitrary System}
\end{aligned} \tag{7.7}$$

The intruder intercepted the transmitted signal $s(t) = x_1(t)$ and used it to couple the arbitrary system in the second and third equations. The parameter set of the drive system is given as $[\mu_1, \mu_2, \mu_3] = [10, 60, 2]$ when bit 1 is to be sent and $[10, 62, 2]$ when bit 0 is to be sent. Fig. 7.3(a) and (b) show the binary information $m(t)$ and the information carrier signal $s(t) = x_1(t)$ respectively. Based on the parameter assignment of the drive and response systems, the receiver will observe no synchronisation error, $e(t) = x_1(t) - y_1(t) = 0$ when bit 1 is received and synchronisation error when bit 0 is received as shown in Fig. 7.3(c). On the other hand, given that the parameter setting of the arbitrary system is always non-identical to the drive system, the intruder will always observe synchronisation error $e(t) = x_1(t) - y_{a,1}(t)$ throughout the transmission as shown in Fig. 7.3(d). However the intruder could reveal two sets of statistical properties that correspond to the binary information (see Fig. 7.3(e)) by measuring the moving average $\delta(t)$ of the synchronisation error in Fig. 7.3(d). Comparing Fig. 7.3(a) with Fig. 7.3(e), we could see that the error corresponding to bit 0's jump to a higher level relative to

the error corresponding to bit 1's. Hence, from Fig. 7.3, it has been demonstrated that the cryptanalysis technique used here [Yang *et al.*, 1998c] like all others characteristic cryptanalysis that aims to reveal two different sets of statistical properties could be used effectively to break CSK schemes.

Fig. 7.3. Security analysis on chaotic shift keying scheme under attack from characteristic cryptanalysis that measures the synchronisation error [Yang *et al.*, 1998c] from the setup shown in (7.7). (a) The binary sequence to be transmitted $m(t)$. (b) The transmitted signal $s(t) = x_t$. (c) The synchronisation error observed at the intended receiver end that correspond to the binary sequence in (a). (d) The synchronisation error observed at the intruder end that does not reveal any useful information. (e) The moving average of the synchronisation error shown in (d) that corresponds to the binary sequence shown in (a). The window length, T_w , employed here is 2.3 time units.

However, the fundamental basis of characteristic cryptanalysis is irrelevant when employed against projective synchronisation scheme. This is because in this approach, the transmitter does not use two attractors to encrypt the binary symbols but rather it uses the scaling features of the coupled system. Although the effect of pseudo-random switching key would generate numerous attractors but these attractors do not contain any digital information. Therefore, it would be reasonable to consider that the transmitted signal possesses only one set of statistical properties where a single attractor resides.

To demonstrate that the characteristic cryptanalysis is ineffective against the projective synchronisation scheme, consider the following setup.

$$\left. \begin{aligned} \dot{x}_{1,1} &= 10(x_{1,2} - x_{1,1}) & \dot{x}_{2,1} &= 10(x_{2,2} - x_{2,1}) + \xi_1 \\ \dot{x}_{1,2} &= (60 - z_{x,2})x_{1,1} - x_{1,2} & \dot{x}_{2,2} &= (60 - z_{x,2})x_{2,1} - x_{2,2} + \xi_2 \\ \dot{z}_{x,1} &= x_{1,1}x_{1,2} - 2z_{x,1} & \dot{z}_{x,2} &= x_{2,1}x_{2,2} - 2z_{x,2} \end{aligned} \right\} \text{Drive System,}$$

$$\left. \begin{aligned} \dot{y}_{a,1} &= 11(y_{a,2} - y_{a,1}) \\ \dot{y}_{a,2} &= (60 - z_{x,2})y_{a,1} - y_{a,2} \\ \dot{z}_a &= y_{a,1}y_{a,2} - 1.7z_a \end{aligned} \right\} \text{Arbitrary System.}$$

(7.8)

Pseudo-random switching key is left out in (7.8) as this demonstration wishes to show that the utilisation of projective synchronisation alone could be employed effectively against characteristic cryptanalysis. Assume that the intruder intercepted the transmitted signal $s(t) = z_{x,2}(t)$ and used it to couple the arbitrary system in the second equation. Using this setup, the intruder could carry out cryptanalysis on the

information carrier signal $z_{x,2}(t)$ by measuring error from the generalised synchronisation transformation [Yang et al., 1998c]. Fig. 7.4(a) shows the binary information $m(t)$. Fig. 7.4(b) shows the measured scaling factor $\alpha(t) = \sqrt{z_a/z_{x,2}}$, which does not correspond to the binary information in (a). This is because the parameter set of the arbitrary system is non-identical to the drive system. Fig. 7.4(c) shows the moving average $\delta_a(t)$ of the scaling factor in Fig. 7.4(b). It can be seen that the moving average here does not reveal any information. Fig. 7.4(d) and (e) presented a further analysis on the intercepted information carrier. Fig. 7.4(d) shows the synchronisation error $e(t) = z_{x,2}(t) - z_a(t)$. The moving average of the synchronisation error shown in Fig. 7.4(e) again does not reveal any information. Hence, it is stated here that the projective synchronisation scheme is secure against the characteristic cryptanalysis as its fundamental basis would be irrelevant.

In conclusion, a new approach to transmit digital signals using controlled projective synchronisation of chaos is developed. This approach eliminates the need to use two attractors to encrypt digital signal in the context of chaotic shift keying. Thus characteristic cryptanalysis [Perez & Cerdeira, 1995; Yang et al., 1998c; Storm & Freeman, 2002], which aims to detect switching of statistical properties in the intercepted information carrier signal would be rendered ineffective when used against future schemes developed based on projective synchronisation. Furthermore, pseudo-random switching key is incorporated to further enhance the security against reconstruction methods [Stojanovski et al.,

1996; Yang et al., 1998d; Huang et al., 2001]. Security analysis carried out proved that the scheme is secure against characteristic cryptanalysis attacks.

Fig. 7.4. Security analysis on projective synchronisation based scheme under attack from characteristic cryptanalysis that measures the synchronisation error [Yang et al., 1998c] from the setup shown in (7.8). (a) A binary sequence to be transmitted $m(t)$. (b) The scaling factor $\alpha(t) = \sqrt{z_a/z_{x,2}}$ observed at the intruder end. (c) The moving average of the scaling factor shown in (d). (d) The synchronisation error $e(t) = z_{x,2}(t) - z_a(t)$ observed at the intruder end. (e) The moving average of the synchronisation error shown in (d). It is observed from the analysis that no useful information is revealed. The window length, T_w , employed here is 2.3 time units.

Chapter 8

Chaotic encryption using discrete-time synchronous chaos with pseudo-random switching keys

This chapter introduces a newly developed cryptosystem that can be implemented in digital communication systems using synchronisation of discrete-time chaotic systems [Chee & Xu, 2004b]. The cryptosystem employs a one-time pad encryption where each message block of M bits is encrypted using a unique set of secret keys that is self-generated within the system. The cryptosystem also features a fast encryption rate that only requires a single iteration to encrypt each message block of up to 52 bits. As a result, the cryptosystem is able to generate a ciphertext storage size that is smaller than the given input information

8.1 Introduction

Chaos, quantum and number theories are employed to develop modern cryptosystems largely due to their capability in creating complex encryptions that protect confidential information against unauthorised access. Beside the security aspect, other considerations such as the rate of encryption and the generated ciphertext size are also important factors to be considered. This chapter introduces a cryptosystem that can be implemented in digital communication systems using synchronisation of discrete-time chaotic systems [Chee & Xu, 2004b]. The

Chapter 8 Discrete-time chaotic encryption

performance of this newly developed cryptosystem under the abovementioned considerations will be discussed in the following sections.

Chaos theory consistently plays an active role in modern cryptography. The attractiveness of using chaos as the basis for developing cryptosystem is mainly due to its random behaviour and sensitivity to initial conditions and parameter settings that fulfil the classic Shannon requirements of confusion and diffusion [Shannon, 1949]. 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.

Discrete-time chaotic encryption employs non-synchronous encryption techniques that use discrete-time systems to encrypt digital information. The two more recent non-synchronous chaotic cryptosystems as described in Section 2.2 are the Baptista-type cryptosystems [Baptista, 1998; Wong *et al.*, 2001; Wong *et al.*, 2003] and the Alvarez-type cryptosystems [Alvarez *et al.*, 1999; Li *et al.*, 2001]. Although security flaws are found in the original Baptista and Alvarez cryptosystems [Baptista, 1998; Alvarez *et al.*, 1999] but the modified and improved versions [Wong *et al.*, 2001; Wong *et al.*, 2003; Li *et al.*, 2001] have shown to provide sufficient security against cryptanalysis. In the Baptista-type cryptosystems, the chaotic attractor is divided into S levels with each level associated with a unique plaintext. The part of the ciphertext is the number of iterations made by the discrete chaotic system from a specified set of initial conditions to the level representing the plaintext. In the Alvarez-type cryptosystems, the discrete chaotic system is iterated from a specified set of initial

Chapter 8 Discrete-time chaotic encryption

conditions to produce a discrete waveform that oscillates about a threshold value to generate a pseudo-random binary bits sequence. The position where the plaintext occurs in the sequence is stored as part of the ciphertext. Although the modified and improved versions of the Baptista-type and Alvarez-type cryptosystems have shown to be secure, they still suffered from three drawbacks. Firstly, for practical and security reasons, the cryptosystems require a long iteration to encrypt a relatively short message block, which slows down the encryption rate. Secondly, due to the design of the encryption process, the generated ciphertext is larger than the inputted information. Thirdly, the initial conditions must be specified and set as part of the secret keys. In doing so, the cryptosystems do not make use of the sensitivity to initial conditions of chaos that is a particularly useful and unique feature of chaos for the purpose of encryption. This is so because if the initial conditions can be arbitrarily chosen then the ciphertext that corresponds to the same information can be totally different each time encryption is carried out with different initial conditions even though the secret keys remain the same. This means that it is equally likely for the same information to be encrypted by infinite possible discrete waveforms. This feature of chaos is useful for protecting the cryptosystem from cryptanalysis techniques that use frequency analysis on corresponding information and ciphertext pairs.

8.2 Basic concept of the cryptosystem

In this chapter, a new discrete-time chaotic cryptosystem for digital communication systems is introduced [Chee & Xu, 2004b]. This new chaotic

Chapter 8 Discrete-time chaotic encryption

cryptosystem differs from the earlier developed chaotic cryptosystems in that it is effectively a chaos synchronisation based cryptosystem. There are three main motivations behind using chaos synchronisation to form the basis of this cryptosystem. First, by using chaos synchronisation, faster encryption rates can be achieved, which requires only a single iteration to encrypt a message block of M bits. The largest block size tested so far is 52 bits. This is a large reduction in term of encryption rate as compared to the earlier developed chaotic cryptosystems, which takes at least a few hundred iterations to encrypt a message block of eight bits or less for security and practical reasons.

Second, by using chaos synchronisation based cryptosystem, ciphertext with storage size that is smaller than the information can be achieved, which is not achievable previously. In this cryptosystem, each message block of M bits is encrypted into a floating-point number, which is the generated value from a selected variable of the employed chaotic system. The ciphertext in the form of floating point number requires a storage size of 32 bits. Hence if each message block has more than 32 bits, it is therefore possible to obtain a corresponding ciphertext that requires a smaller storage size than the inputted information.

Third, the utilisation of chaos synchronisation allows arbitrary selection of initial conditions on the transmitter ends. Although it will be explained later that part of the initial conditions in this cryptosystem must still be set as secret keys, the setting of initial conditions on the whole can still remain nonidentical each time the encryption process is carried out. This flexibility fully utilises the sensitivity to initial conditions of chaos such that similar information encrypted with a

nonidentical set of initial conditions will generate a totally different set of ciphertext. This implies the non-existence of direct relationship between the input information and the generated ciphertext before the synchronisation process. In another words, it is not possible to decrypt the ciphertext without first obtaining the secret keys of the cryptosystem and thus protecting the cryptosystem from cryptanalysis techniques using frequency analysis of corresponding information and ciphertext pairs.

The cryptosystem introduced here consists of two parts, namely the encrypter and the decrypter that is used to encrypt and decrypt information respectively. Consider a discrete-time chaotic system given in (8.1) used to model the encrypter.

$$\mathbf{X}_{(k+1)} = f[\mathbf{X}_{(k)}, \alpha(m_{(k)}), \mu(\mathbf{X}_{(k)})]. \quad (8.1)$$

Here the subscript k in the bracket denotes the iteration number. $\mathbf{X}_{(k)} = [x_{1,(k)}, x_{2,(k)}, \dots, x_{n,(k)}]$ represents the state vector of the encrypter with one of the state variable assigned as the ciphertext $u_{(k)}$. In digital communication systems, the ciphertext $u_{(k)}$ is sent as a package from the transmitter to the receiver end. The initial conditions of the state vector $\mathbf{X}_{(0)}$ except $u_{(0)}$ form the first one-third of the secret key formation, where $u_{(0)}$ can be arbitrarily chosen. The symbol $m_{(k)}$ denotes a block of binary sequence or message block with M bits that has 2^M different combinations. For example when $M = 2$, $m_{(k)}$ may take the form of either one of these combinations (00, 01, 10, 11). The function $\alpha(m_{(k)})$, which will be denoted by $\alpha_{(k)}$ for simplicity, forms the second one-third of the secret key formation refers to as the M -ary switching key (MSK) that is capable of producing

2^M different output values with each value uniquely assigned to each message block combination. The system parameter set $\mu(\mathbf{X}_{(k)}) = [\mu_1(\mathbf{X}_{(k)}), \mu_2(\mathbf{X}_{(k)}), \dots, \mu_v(\mathbf{X}_{(k)})]$ is designed as pseudo-random switching key (PRSK), forms the last one-third of the secret key formation. Here, PRSK is a dynamical memoryless parameter set that changes its values at every iteration such that $\mu(\mathbf{X}_{(k)}) \neq \mu(\mathbf{X}_{(k+1)})$. The symbol $\mathbf{X}_{(k)}$ from $\mu(\mathbf{X}_{(k)})$ will be dropped from now for simplicity and PRSK will simply be expressed by $\mu_{x,(k)} = [\mu_{x,1,(k)}, \mu_{x,2,(k)}, \dots, \mu_{x,v,(k)}]$.

8.3 Mechanism of the cryptosystem

To demonstrate the mechanism and functioning of the encrypter, a block diagram shown in Fig. 8.1 is used. Hénon map [Hénon, 1976] proposed by the French astronomer Michel Hénon is employed here as the underlying discrete-time chaotic system f given in (8.2).

$$\begin{aligned} x_{1,(k+1)} &= 1 - \alpha_{(k)} \mu_{x,1,(k)} x_{1,(k)}^2 + x_{2,(k)}, \\ x_{2,(k+1)} &= \mu_{x,2,(k)} x_{1,(k)}. \end{aligned} \quad (8.2)$$

This section will first describe the working mechanism of the M-ary switching key (MSK), which is the function $\alpha_{(k)}$ that forms the second one-third of the secret key formation. The main role of MSK is to allow the encrypter to encode a particular message block as a fixed value, which in turn allows the decrypter to retrieve the information by reversing the operation. The secrecy of the cryptosystem however does not rely on the MSK. From the top left hand corner of Fig. 8.1, a message block $m_{(k)}$ is inputted into the encrypter through $\alpha_{(k)}$. The

function $\alpha_{(k)}$ can be arbitrarily design using simple mathematical operations as long as two criteria are fulfilled. At first $\alpha_{(k)}$ must be a two-way function that is capable of producing $2M$ different output values with each value uniquely assigned to each message block combination. This is to allow the receiver to reverse the operations with the same function in the decrypter to retrieve information. Then the output value from $\alpha_{(k)}$ that is to be inputted into system (8.2) must allow the system to remain bounded. As an example, for $M = 48$, $\alpha_{(k)}$ can be designed as

$$\alpha_{(k)} = A + Bm_{d,(k)} \quad (8.3)$$

where A and B are constants set as 1.77×10^{-2} and 1.39×10^{-15} respectively and $m_{d,(k)}$ is the decimal value of the message block.

Fig. 8.1. Encryption process of the encrypter with Hénon map (8.2) as the underlying chaotic system.

Chapter 8 Discrete-time chaotic encryption

Next, this section will describe the pseudo-random switching key (PRSK), which is the function $\mu_{x,(k)}$ that forms the last one-third of the secret key formation. The security of the cryptosystem relies on the PRSK. The PRSK is a dynamical and memoryless secret key that never repeats its output values exactly and explicit relationship does not exist between these output values for all k . This is in fact similar in principle to a one-time pad encryption, which is the only known form of unconditionally secure encryption. Unfortunately, the one-time pad encryption is brought down by the impractical heavy logistic burden of regular key distribution. However this logistic burden is solved here by the self-generating capability of PRSK on both the transmitter and receiver ends.

It is shown at the bottom of Fig. 8.1 that $x_{2,(k)}$ from the encrypter (8.2) is inputted into $\mu_{x,(k)}$ to generate a unique set of system parameters at every iteration. In the design of PRSK, explicit relationship between $\mu_{x,(k)}$ and $\mu_{x,(k+1)}$ is eliminated by designing $\mu_{x,(k)}$ using a piecewise function given as

$$\mu_{x,i,(k)} = b_{i,j}(x_{2,(k)}), \quad a_{i,j}(x_{2,(k)}) < x_{2,(k)} \leq a_{i,j+1}(x_{2,(k)}) \quad (8.4)$$

for $i=1, 2$ and $j=1, \dots, L$.

The piecewise function (8.4) states that the i th parameter $\mu_{x,i,(k)}$ will be switched to the function $b_{i,j}(x_{2,(k)})$ when the selected state variable, which is $x_{2,(k)}$ in this case, falls in a range defined by $a_{i,j}(x_{2,(k)}) < x_{2,(k)} < a_{i,j+1}(x_{2,(k)})$ where there is $L \geq 2$ number of levels defined. The functions $a_{i,j}(x_{2,(k)})$ and $b_{i,j}(x_{2,(k)})$ can be arbitrarily designed using simple mathematical operations as long as the output

values from $a_{i,j}(x_{2,(k)})$ is within the interval of $x_{2,(k)}$ and the output values from $b_{i,j}(x_{2,(k)})$ allows system (2) to remain bounded. As an example, the design is given as, $a_{i,j}(x_{2,(k)}) = G_{i,j} + (x_{2,(k)}/H)$ and $b_{i,j}(x_{2,(k)}) = P_{i,j} + (x_{2,(k)}/Q)$, where $G_{i,j}$, H , $P_{i,j}$ and Q are constants. Possible designs of $\mu_{x,1,(k)}$ and $\mu_{x,2,(k)}$ employed here are given as

$$\mu_{x,1,(k)} = \begin{cases} 1.27 + (x_{2,(k)}/10.2), & |x_{2,(k)}| \leq 0.1 + (x_{2,(k)}/1.3) \\ 1.28 + (x_{2,(k)}/10.2), & 0.1 + (x_{2,(k)}/1.3) < |x_{2,(k)}| \leq 0.2 + (x_{2,(k)}/1.3) \\ 1.29 + (x_{2,(k)}/10.2), & 0.2 + (x_{2,(k)}/1.3) < |x_{2,(k)}| \leq 0.3 + (x_{2,(k)}/1.3) \\ 1.30 + (x_{2,(k)}/10.2), & \text{otherwise} \end{cases} \quad (8.5)$$

and

$$\mu_{x,2,(k)} = \begin{cases} 0.29 + (x_{2,(k)}/10), & |x_{2,(k)}| \leq 0.1 + (x_{2,(k)}/1.1) \\ 0.30 + (x_{2,(k)}/10), & 0.1 + (x_{2,(k)}/1.1) < |x_{2,(k)}| \leq 0.2 + (x_{2,(k)}/1.1) \\ 0.31 + (x_{2,(k)}/10), & 0.2 + (x_{2,(k)}/1.1) < |x_{2,(k)}| \leq 0.3 + (x_{2,(k)}/1.1) \\ 0.32 + (x_{2,(k)}/10), & \text{otherwise} \end{cases} \quad (8.6)$$

There are four levels defined in (8.5) and (8.6) where $L=4$ and $j=1 \dots 4$.

This section wishes to demonstrate that any exact repetition of the output values of PRSK is hardly observable. Fig. 8.2(a) shows the variation of $\mu_{x,2,(k)}$ where the dynamics exhibits random behaviour with output values that never identically repeat themselves. Fig. 8.2(b) shows the frequency spectrum of $\mu_{x,2,(k)}$ which resembles that of a white noise where no periodicity occurs in the variation pattern.

Chapter 8 Discrete-time chaotic encryption

Similar behaviour is also observed in $\mu_{x,1,(k)}$. Furthermore it does not require the cryptosystem to store the values of $\mu_{x,(k)}$ from the previous iteration. Hence PRSK inherits the feature that is similar to a one-time pad for encryption.

Fig. 8.2. Demonstration of the dynamical behaviour of PRSK. (a) The variation of $\mu_{x,2,(k)}$. The dynamics exhibits random behaviour with output values that never identically repeat themselves. (b) The frequency spectrum of $\mu_{x,2,(k)}$, which resembles that of a white noise where no periodicity is observed in the variation pattern.

Lastly, this section will introduce the decrypter and the decrypting process to complete the description of the cryptosystem. The role of the decrypter is to retrieve and decode the output values of the MSK from the received ciphertext. A decrypter at the receiver end is given as

$$\alpha_{(k)} = \frac{1 - u_{(k+1)} + y_{2,(k)}}{\mu_{y,1,(k)} u_{(k)}^2}, \quad (8.7)$$

$$y_{2,(k+1)} = \mu_{y,2,(k)} u_{(k)}.$$

By rearranging the first equation, the decrypter (8.7) in the cryptosystem is in fact identical to the encrypter (8.2) with state vector $\mathbf{Y}_{(k)} = [u_{(k)}, y_{2,(k)}]$, $u_{(k)} = x_{1,(k)}$ and $y_{2,(0)} = x_{2,(0)}$. At the receiver end, $u_{(k)}$ received is used to drive the decrypter. Note that both the second equation of the encrypter (8.2) at the transmitter end and the decrypter (8.7) at the receiver end are identical. Hence by inputting $u_{(k)}$ into the decrypter (8.7) and having a common setting of PRSK, synchronisation between the encrypter and decrypter will be observed such that $\mathbf{X}_{(k)} = \mathbf{Y}_{(k)}$ and $\mu_{x,(k)} = \mu_{y,(k)}$ of all k . This allows the receiver to obtain the output values of $\alpha_{,,,}$, which is required for retrieving the information using the inverse function of the MSK

$$m_{d,(k)} = (\alpha_{(k)} - A)/B. \quad (8.8)$$

The cryptosystem developed and encryption and decryption processes are carried out between three PCs with configuration given as P4 2.8 GHz with 2GB RAM, P3 933MHz with 64MB RAM and P2 500MHz with 384MB RAM as illustrated by Fig. 8.3. The ciphertext $u_{(k)}$ is sent as a package during the secure communication processes with message blocks ranging from $M = 4, 8, 12, \dots, 52$. The test achieved zero bit error ratio for all transactions.

Fig. 8.3. Set-up of the cryptosystem using three PCs used to test encryption and decryption processes.

8.4 Security analysis

In this section, the security of the cryptosystem is analysed by dividing cryptanalysis into the analytical and statistical aspects. This section wishes to show that the secret key formation, which involves functions in the form of **MSK** and **PRSK**, is secure and cannot be broken. The Kerchoff's principle is employed as the basis of assumption in the security analysis. It is assumed that a cryptanalyst who wish to decrypt the ciphertext has the knowledge of the design and working mechanism of the cryptosystem except the secret key formation. This means that the cryptanalyst knows the chaotic system used in the cryptosystem but has no knowledge of the functions involved in the design of **MSK** and **PRSK**.

Broadly speaking, the cryptanalyst has two fundamental forms of cryptanalysis to break the cryptosystem as introduced in section 2.3, which are the identification-

based and the characteristic-based cryptanalysis. Identification-based cryptanalysis is analytical analysis that aims to decrypt the ciphertext by reconstructing the secret key formation. The four levels of attack on cryptosystems discussed in [Alvarez *et al.*, 2000] belong to this category, namely ciphertext-only attack, known-plaintext attack, chosen plaintext attack and chosen ciphertext attack. On the other hand, characteristic-based cryptanalysis carried out statistical properties analysis on the ciphertext to obtain the information without reconstructing the secret key formation. Characteristic-based cryptanalysis techniques such as the construction of return maps [Pérez & Cerdeira, 1995; Yang *et al.*, 1998a] were first introduced in cryptanalysis of continuous-time chaotic encryption. This section will prove that the developed cryptosystem is immune to these two forms of cryptanalysis.

This section will first consider the identification-based cryptanalysis to show that the cryptosystem is secure in term of the analytical aspect. It is stated here that the cryptosystem will remain secure even under the most unfavourable condition where the cryptanalyst has the freedom to obtain the corresponding pair of information, $m_{(k)}$ and ciphertext, $u_{(k)}$ with the temporary access to the cryptosystem.

In order to fully understand the capability of the cryptosystem against identification-based cryptanalysis, the section will first demonstrate the extreme sensitivity of the cryptosystem to small error in the **MSK** and **PRSK** settings. Fig. 8.4(a) shows a plaintext to be encrypted.

(a)	(b)
<p>The Vanda Miss Joaquim, an orchid variety, is Singapore's national flower. It is an indigenous hybrid between the Vanda teres and the Vanda hookerana. It was chosen as Singapore's national flower particularly because of its hardy and resilient qualities and its ability to bloom throughout the year. These are characteristics, which reflect Singapore's quest for progress and excellence in all aspects of life.</p>	<p>The Vand"+¶Äss Joaqu)ú□PaméLxhi)q.ñ&iceÖ i\iP□ng\$PM9e'ž... 'ti/□Ú□ fV]f-r- á□ÝGirâÚ Jin)m9-no8Q°5yb/pf×be=N D,n 7□-æV̄a=D-CtelδQÖan- þe)\$%a li"Öer(l □8 I^ O-s #,p̄emçßÄ¶Si>fpyor^q±na7□!Äaké© □we0="Ort*&(Oar5—R□eq¾l? oPñs (ÄÆ□y □8re3úÇ□en;n)Ÿal2"z"s lŸw it8F□)il.°pl tnâ 7~olâ-Yiou)†øut 4AmTMye-i Th56½ ar.†Çar*°giri4 Xs+aŪ8?cgèl f-le'2¿ in,"vürdè)nOue2ø Ÿëoqâš□-gr+ †qan-WgEce4*- cdè- Kal5_C,pe%0-ðoeâTle-ÇRø□</p>

Fig. 8.4. (a) The original plaintext that is to be encrypted. (b) The plaintext with 47% bit error ratio retrieved by a cryptanalyst who made an extremely small error in estimating the secret keys.

On the encrypter, message blocks of 48 bits each is chosen. The initial conditions are selected as $\mathbf{X}_{(k)} = [0.4, 0.5]$. The remaining parts of the secret key formation are assigned according to (8.3), (8.5) and (8.6). Fig. 8.5(a) shows the variation of the generated ciphertext, $u_{(k)}$. Assuming that a cryptanalyst made an extremely close estimation of the secret keys in which he choose the same number of bits in the message block and reconstructed an almost identical secret key formation except that he estimated $P_{1,1}$ at the first level of (8.5) to be 1.27001 instead of 1.27. The result due to this small error in the estimation of the secret key formation is shown in Fig. 8.5(b) and (c). Fig. 8.5(b) shows the difference between $u_{(k)}$ and $y_{1,(k)}^*$ and Fig. 8.5(c) shows the difference between the actual output values of $\alpha_{(k)}$ and the output values of the inaccurately decoded ones, $\alpha_{(k)}^*$. Although the

errors shown in Fig. 8.5(b) and (c) are also extremely small but this caused the cryptanalyst to decrypt the ciphertext with 47% bit error rate. The retrieved plaintext is shown in Fig. 8.4(b).

Fig. 8.5. (a) The variation of the ciphertext, $u_{(k)} = x_{1,(k)}$ of a portion of the plaintext shown in Fig. 8.4(a). The ciphertext is generated using the Hénon map as the underlying chaotic system. (b) & (c) The differences between $(u_{(k)}$ and $y_{1,(k)}^*)$ and $(\alpha_{(k)}$ and $\alpha_{(k)}^*)$ due to an extremely small error in estimating the secret keys that resulted in a 47% bit error rate in the retrieved plaintext shown in Fig. 8.4(b).

Therefore it is shown here that to break the cryptosystem, it is first necessary for the cryptanalyst to determine the underlying functionis used for **MSK** and **PRSK** accurately. To do so, a number of $\alpha_{(k)}$ values must first be obtained with high certainty and precision. This undertaking will prove to be difficult with the presence of **PRSK**. This is because **PRSK** changes its output values at every

Chapter 8 Discrete-time chaotic encryption

iteration that never repeats identically and there is exist no explicit relationship between these output values. As a result, without the knowledge of the exact design of PRSK, it is not possible to form an equation that relates $\mu_{y,(k)}$ to $\mu_{y,(k+1)}$. Hence at the initial stage, $k = 0$, the cryptanalyst will have two equations but five unknowns to solve, namely $y_{2,(0)}$, $y_{2,(1)}$, $\alpha_{(0)}$, $\mu_{y,1,(0)}$ and $\mu_{y,2,(0)}$. Subsequently for every iteration, there will be an addition of two equations and four unknowns, which are $y_{2,(k+1)}$, $\alpha_{(k)}$, $\mu_{y,1,(k)}$ and $\mu_{y,2,(k)}$. With only two given equations to at least four unknowns, the cryptanalyst will face infinite possible solutions and thus will not be able to identify the values involved in the secret key formation with certainty and precision. As a result, it is not possible for the cryptanalyst to reconstruct the secret key formation using identification-based cryptanalysis. Since the security here is derived based on the infinite possible solutions at every iteration, therefore the cryptosystem is secure against brute force attack. Hence the cryptosystem is immune to the computational speed involved in the cryptanalysis.

Next, the characteristic-based cryptanalysis is considered in this section to show that the cryptosystem is secure in term of the statistical aspect. It is known that although dynamical behaviour of a chaotic system can exhibits as many possible waveforms as the setting of initial conditions, the statistical properties of these waveforms actually remain identical if the system constant parameters remain fixed. Therefore given two different chaotic waveforms, it is possible to distinguish whether they are generated from a similar system with identical parameter set by carrying out statistical properties analysis on the waveforms. A good indication of any shift in statistical properties is by constructing return maps [Pérez & Cerdeira,

1995; Yang *et al.*, 1998a] using one of the ciphertext generated by the cryptosystem. Any adjustment in the parameter set will cause stretching and shifting in the position of the return map shown in Fig. 8.6(a). Fig. 8.6(a) is constructed using Hénon map that switches between two sets of parameter.

Fig. 8.6. Return maps constructed using the variable $x_{1,(k)}$ from Hénon map. (a) The system switches between two parameter sets that causes the return map to stretch and shift between two fixed positions represented by blue and red dots. (b) The result of incorporating MSK and PRSK into the system with message blocks of 48 bits each. The return map is diffused out as the system switches to a unique parameter set at every iteration and never converge to a fixed statistical behaviour but constantly in the transient state.

The implication from Fig. 8.6(a) is obvious. Adjustment of system parameters in the generated ciphertext can easily be detected by observing shifting in statistical properties of the waveform. In the case where $M = 1$ with no implementation of PRSK, the cryptosystem will have only two possible parameter sets that represent

Chapter 8 Discrete-time chaotic encryption

bit 0 or 1. To retrieve the information, a cryptanalyst can carry out an analysis of statistical properties techniques on the intercepted ciphertext $u_{(k)}$. If the cryptanalyst chooses to plot a return map, the information can be retrieved without the need to identify the secret keys by observing where the points land on the return map.

However we state that characteristic-based cryptanalysis will not be effective to break the cryptosystem due to the design and implementation of MSK and PRSK. In the example shown in Fig. 8.6(b) with $M = 48$, the cryptosystem generates 2^{48} possible sets of statistical properties. This number of sets induced by MSK is further multiplied by the presence of PRSK that has output values that never identically repeat themselves. Hence the cryptosystem switches to a unique parameter set at every iteration. As a result, the characteristic of the cryptosystem never converges to a fixed statistical behaviour but is in a constant transient state. This makes monitoring of any shift in the statistical properties of the waveform impossible, which is indicated by the return map plotted in Fig. 8.6(b).

In conclusion, a cryptosystem based on synchronisation of discrete chaotic systems has been developed. Security analysis carried out has showed that the cryptosystem is secure against identification-based and characteristic-based cryptanalysis. Furthermore the cryptosystem can achieve faster encryption rates that require only a single iteration to encrypt a message block of up to 52 bits with zero bit error ratio. In doing so, the ciphertext will have a smaller storage size than the inputted information if the inputted message blocks for encryption contain more than 32 bits each.

Chapter 9

Conclusions and futureworks

9.1 Conclusions

To conclude, in Part II of the thesis, the latest development of projective synchronisation in coupled chaotic systems has been systematically introduced. It has delivered the most recent findings pertaining to the mechanism and stability criteria of projective synchronisation and control of the nonlinear phenomena. From Part II of the thesis, three academic contributions have been produced.

- 1) A general control method for manipulating projective synchronisation of arbitrary dimensional continuous-time systems is proposed [Xu & Chee, 2002].
- 2) The stability criteria of projective synchronisation in discrete-time systems [Xu *et al.*, 2004].
- 3) A control approach for directing the ultimate state of projective synchronisation in lower dimensional discrete-time system [Chee & Xu, 2003].

Furthermore, this thesis also discovered a new form of synchronisation phenomenon named here as the pseudo-random switching keys (PRSK). It is observed that identical synchronisation of chaos is still achievable in coupled chaotic system even with the sub-systems having different initial parameters that switch values within a chosen set in a discontinuous, rapid and random-like manner. This observation opposes the earlier belief that identical synchronisation can only be realised with identical and fixed system parameters. This newly

discovered form of synchronisation phenomenon is useful for secure communication applications and an academic contribution has resulted from here.

- 4) The discovery of identical synchronisation of PRSK and a general approach in using PRSK for secure communication [Xu & Chee, 2003]

In Part III of the thesis, new applications that solve some of the existing problems in chaos-based communication are developed. These newly developed applications resulted in three academic contributions.

- 5) A projective synchronisation based digital communication technique is developed [Chee & Xu, 2004a]. This technique uses the knowledge of the stability criteria [Xu *et al.*, 2002] and the control algorithm of projective synchronisation [Xu & Chee, 2002] in Part II. This development shifted chaos-based communication to a truly M-ary process that allows faster transmission rates than the existing chaos-based techniques. Moreover this is the first chaos-based digital communication technique to exhibit better bit error ratio performance over the conventional techniques.
- 6) A secure digital communication technique based on projective synchronisation is developed [Chee & Xu, 2005]. This technique incorporated PRSK and employs the control algorithm [Xu & Chee, 2002] introduced in Part II. As a result the communication scheme has proven to be secure against the fundamentalsof the existing cryptanalysis techniques.
- 7) A cryptosystem from secure internet communication is developed [Chee & Xu, 2004b]. The cryptosystem is based on synchronisation of discrete-time systems

with PRSK. This cryptosystem has been shown to be secure against the fundamentals of the existing cryptanalysis techniques. Furthermore, this cryptosystem allows faster encryption rate than the existing chaos-based cryptosystems and could generate a ciphertext size that is smaller than the inputted plaintext.

In short, these completed works have laid down a theoretical foundation for understanding the physical phenomena of projective synchronisation in continuous-time and discrete-time coupled systems. The accomplishment of these works is seen as the starting point to gain insight into using the mechanism of projective synchronisation for developing useful scientific and engineering applications. This thesis applied this knowledge to develop applications for communication, which can be applied in areas such as secure internet communication, wireless secure communication, banking data transaction and military communication.

9.2 Future works

Having successfully developed a projective synchronisation based digital communication system that has better bit error rate performance when compared to conventional and other existing chaos-based techniques, it will be challenging to look into multi-channels communication system using projective synchronisation. In multi-channels communication, multiple pairs of transmitter and receiver can communicate at the same time using only a single communication media such as a single copper wire. Hence, this will allow projective synchronisation based

communication systems to be implemented in communication network instead of a single channel communication scheme presently achieved in Chapter 6.

To do so, it will be necessary to explore the existence of projective synchronisation in extended systems in the form of discrete-time or continuous-time lattices. This has been shown to be possible in numerical simulation. However, we need to ensure such behaviour is stable mathematically by providing stability criteria. Once this is established, the next step will be focused on deriving of the associated control laws to manipulate the formation of projective synchronisation in the extended system. Achieving controlled projective synchronisation in extended systems may lead to important applications where multi-channel digital communication is one of them.

Finally, we will wish to develop a projective synchronisation based digital communication system for multi-channels communication. The bit error rate and transmission efficiency will then be tested out.

References

- Akaike, H. [1974] "A new look at statistical model identification," *IEEE Trans. Auto. Control* 19, 716-723.
- Alvarez, E., *et al.* [1999] "New approach to chaotic encryption," *Physics Letters A* 263, 373-375.
- Alvarez, G., *et al.* [2000] "Cryptanalysis of a chaotic encryption system," *Physics Letters A* 276, 191-196.
- Baptista, M.S. [1998] "Cryptography with chaos," *Physics Letters A* 240, 50-54.
- Barahona, M. & Poon, C-S. [1996] "Detection of nonlinear dynamics in short, noisy time series," *Nature* 381, 215-217.
- Beltrami, E. [1993] *Mathematical Models in the Social and Biological Sciences*, Jones & Bartlett Publishers.
- Bezruchko, B.P., *et al.* [2001] "Reconstruction of time-delay systems from chaotic time series," *Physical Review E* 56, 056216-056221.
- Behrens, D.A., Feichtinger, G. & Prskawetz, A. [1997] "Complex dynamics and control of arms race," *European Journal of Operational Research* 100, 192-215.
- Blasius, B., Huppert, A & Stone, L. [1999] "Complex dynamics and phase synchronization in spatially extended ecological systems," *Nature* 399, 354-359.

References

- Boon, J.P., Noullez, A. & Mommen, C. [1990] "Complex dynamics and musical structure," *Inteflace Journal of New Music Research* 19, 3.
- Boon, J.P. & Decroly, O. [1995] "Dynamical systems theory for music dynamics," *Chaos* 5,501-508.
- Bullard, E. [1978] "The disk dynamo," *AIP Conference Proceedings* 46,373-389.
- Carroll, T.L., Heagy, J.F. & Pecora, L.M. [1996] "Transforming signals with chaotic synchronisation," *Physical Review E* 54,4676-4680.
- Chai, W.W. [2002] *Synchronization in coupled chaotic circuits and systems*, World Scientific, Singapore.
- Chee, C.Y. & Xu, D. [2003] "Control of the formation of projective synchronisation in lower-dimensional discrete-time systems," *Physics Letters A* 318, 112-118.
- Chee, C.Y. and Xu, D. [2004a] "Transmission of M-ary digital signals using controlled projective synchronisation of chaos," *IEEE 4th International Symposium on Communication Systems, Networks & Digital Signal Processing*, 249-252, Newcastle, UK.
- Chee, C.Y. & Xu, D. [2004b] "Chaotic encryption using discrete-time chaotic encryption," *Physics Letters A*, (submitted).
- Chee, C.Y. and Xu, D. [2005] "Secure digital communication using controlled projective synchronisation of chaos," *Chaos, Solitons and Fractals* 23, 1063-1070.

References

- Chen, G. & Ueta, T. [1999] "Yet another chaotic attractor," *International Journal of Bifurcation and Chaos* 9, 1465-1466.
- Chen, G. & Ueta, T. [2002] *Chaos in circuits and systems*, World Scientific, Singapore.
- Chen, J.Y., *et al.* [2003] "A secure communication scheme based on the phase synchronisation of chaotic systems," *Chaos* 13, 508-514.
- Cuomo, K.M. & Oppenheim, A.V. [1993] "Circuit implementation of synchronised chaos with applications to communications," *Physical Review Letters* 71, 65-68.
- Dabby, D. [1996] "Musical variations from a chaotic mapping," *Chaos* 6, 95-107.
- Farmer, J.D. & Sidorowich, J.J. [1987] "Predicting chaotic time series," *Physical Review Letters* 59, 845-848.
- Galias, Z. & Maggio, G.M. [2001] "Quadrature chaos-shift keying: theory and performance analysis," *IEEE Trans. Circuits and Systems I* 48(12), 1510-1519.
- Gaspard, P., *et al.* [1998] "Experimental evidence for microscopic chaos," *Nature* 394, 865-868.
- Gleick, J. [1998] *Chaos Making a New Science*, Abacus, London.
- Gonzalez-Miranda, J.M. [1996] "Chaotic systems with a null conditional Lyapunov exponent under nonlinear driving," *Physical Review E* 53, R5-R8.
- Gonzalez-Miranda, J.M. [1998] "Amplification and displacement of chaotic attractors by means of unidirectional chaotic driving," *Physical Review E* 57, 7321-7324.

References

- Grassi, G. & Mascolo, S. [1997] "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal," *IEEE Trans. Circuits and Systems I* **44**(10), 1011-1014. ¹
- Halle, K.S., *et al.* [1993] "Spread spectrum communication through modulation of chaos," *International Journal of Bifurcation and Chaos* **3**, 469-477.
- Hayes, S., Grebogi, C. & Ott, E. [1993] "Communicating with chaos," *Physical Review Letters* **70**, 3031-3034.
- Hénon, M. [1976] "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics* **50**, 69-77.
- Howell, K.C., Barden, B.T. & Lo, M.W. [1997] "Application of dynamical systems theory to trajectory design for a libration point mission," *The Journal of Astronautical Sciences* **45**, 161-178.
- Huang, X., *et al.* [2001] "Unmasking chaotic mask by a wavelet multiscale decomposition algorithm," *International Journal of Bifurcation and Chaos* **11**(2), 561-569.
- Kennedy, M.P., *et al.* [1998] "Recent advances in communicating with chaos," *IEEE International Symposium on Circuits and Systems ISCAS'98* **4**, 461-464.
- Kocarev, Lj., *et al.* [1992] "Experimental demonstration on secure communications via chaotic synchronisation," *International Journal of Bifurcation and Chaos* **2**(3), 709-713.
- Kocarev, L. & Parlitz, U. [1995] "General approach for chaotic synchronisation with applications to communication," *Physical Review Letters* **74**, 5028-5031.

References

-
- Kocarev, Lj. & Parlitz, U. [1996] "Generalised synchronisation, predictability, and equivalence of unidirectionally coupled dynamical systems," *Physical Review Letters* 76, 1816-1819.
- Kolumbán, G., et al. [1996a] "Performance evaluation and comparison of chaos communication systems," *IEEE Workshop on Nonlinear Dynamics of Electronic Systems NDES'96*, 105-110.
- Kolumbán, G., et al. [1996b] "Differential chaos shift keying: A robust coding for chaotic communication," *IEEE Workshop on Nonlinear Dynamics of Electronic Systems NDES'96*, 87-92.
- Kolumbán, G., Kennedy, M.P. & Kis, G. [1997] "Multilevel differential chaos shift keying," *IEEE Workshop on Nonlinear Dynamics of Electronics Systems NDES'97*, 191-196.
- Kolumbán, G., et al. [1998] "FM-DCSK: A Robust Modulation Scheme for Chaotic Communications," *IEEE Trans. Fundamentals of Electronics, Communication and Computer Sciences*, **E81-A(9)**, 1798-1802.
- Kolumbán, G. [2000] "Theoretical noise performance of correlator-based chaotic communications schemes," *IEEE Trans. Circuits and Systems I* **47(12)**, 1692-1701.
- Kouda, T., et al. [2001] "Chaos-controlled defrost for microwave ovens," *52nd International Appliance Technical Conference*, Columbus.
- LaSalle, J.P. [1986] *The Stability and Control of Discrete Processes*, (Springer-Verlag, Berlin).

References

- Lau, F.C.M. & Tse C.K. [2003] *Chaos-Based Digital Communication Systems* (Springer, Berlin).
- Leung, H., Yu, H. & Murali, K. [2002] "Ergodic chaos-based communication schemes," *Phys. Rev.* **E66**, 036203-036210.
- Li, T.Y. & Yorke, J.A. [1975] "Period three implies chaos," *American Mathematical Monthly* 82,985-992.
- Li, S., Mou, X. & Cai, Y. [2001] "Improving security of a chaotic encryption approach," *Physics Letters A* 290, 127-133.
- Li, Z. & Xu, D. [2001] "Stability criterion for projective synchronisation in three-dimensional chaotic systems," *Physics Letters A* 282, 175-179.
- Li, S., *et al.* [2004] "Baptista-type chaotic cryptosystems: problem and countermeasures," *Physics Letters A* 332,368-375.
- Lorenz, E.N. [1963] "Deterministic nonperiodic flow," *J. Atmos. Sci.* 20, 130-148.
- Lorenz, E.N. [1993] *The Essence of Chaos*, UCL Press.
- Lü, J. & Chen, G. [2002] "A new chaotic attractor coined," *International Journal of Bifurcation and Chaos* 12,659-661.
- Malhotra, R., Holman, M. & Ito, T. [2001] "Chaos and stability of solar system," *Proceedings of the National Academy of Sciences* 98, 12342-12343.
- Maggio, G.M. & Galias, Z. [2002] "Applications of symbolic dynamics to differential chaos shift keying," *IEEE Trans. Circuits and Systems I* **49**(12), 1729-1735.
- Mainieri, R. & Rehacek, J. [1999] "Projective synchronisation in three-dimensional chaotic systems," *Physical Review Letters* 82, 3042- 3045.

References

- May, R. [1976] "Simple mathematical models with very complicated dynamics," *Nature* 261,459-467.
- Moon, F.C. [1992] *Chaotic and Fractal Dynamics An Introduction for Applied Scientists and Engineers*, John Wiley and Sons, Inc.
- Morgiil, O. & Solak, E. [1996] "Observer based synchronization of chaotic systems," *Physical Review E* 54,4803-4811.
- Neuringer, A. & Voss, C. [1993] "Approximating chaotic behavior," *Psychological Science* 4, 113-119.
- Nijmeijer, H. & van der Schaft, A. [1990] *Nonlinear Dynamical Control Systems*, Springer-Verlag.
- Ott, E., Grebogi, C. & Yorke, J.A. [1990] "Controlling chaos," *Physical Review Letters* 64, 1196-1199.
- Paraskevopoulos, P.N. [2002] *Modem Control Engineering*, Marcel Dekker NY.
- Parlitz, U., *et al.* [1992] "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos* 2(4), 973-977.
- Parlitz, U. [1996] "Estimating model parameters from time series by autosynchronization," *Physical Review Letters* 76, 1232-1235.
- Parlitz, U., Junge, L. & Kocarev, L. [1996] "Synchronisation-based parameter estimation from time series," *Physical Review E* 54,6253-6259.
- Parmananda, P. [1997] "Generalized synchronisation of spatiotemporal chemical chaos," *Physical Review E* 56, 1595-1598.

References

- Peng, J.H., *et al.* [1996] "Synchronizing hyperchaos with a scalar transmitted signal," *Physical Review Letters* 76,904-907.
- Pérez, G. & Cerdeira, H.A. [1995] "Extracting messages masked by chaos," *Physical Review Letters* 74, 1970-1973.
- Pikovsky, A. Rosenblum, M. & Kurths, J. [2000] "Phase synchronisation in regular and chaotic systems," *International Journal of Bifurcation and Chaos* 10, 2291-2305.
- Pecora, L.M. & Carroll, T.L. [1990] "Synchronisation in chaotic systems," *Physical Review Letters* **64**, 821-824.
- Pecora, L.M. & Carroll, T.L. [1991] "Driving systems with chaotic signals," *Physical Review A* 44,2374-2384.
- Ponomarenko, V.I. & Prokhorov, M.D. [2002] "Extracting information masked by the chaotic signal of a time-delay system," *Physical Review E* 66, 026215-026221.
- Poon, C-S. & Merrill, C.K. [1997] "Decrease in cardiac chaos in congestive heart failure," *Nature* 389,492-495.
- Rabinovich, M.I. & Abarbanel, H.D.I. [1998] "The role of chaos in neural system," *Neuroscience* **87**, 5-14.
- Rosenblum, M.G., Pikovsky A.S. & Kurths, J. [1996] "Phase synchronisation of chaotic oscillators," *Physical Review Letters* 76, 1804-1807.
- Rossler, O.E. [1976] "An equation for continuous chaos," *Physics Letters A* 57, 397-398.
- Rossler, O.E. [1979] "An equation for hyperchaos," *Physics Letters A* 71, 155-157.

References

- Rulkov, N.F., *et al.* [1995] "Generalised synchronisation of chaos in directionally coupled chaotic systems," *Physical Review E* 51,980-994.
- Saha, P., Banerjee, S. & Chowdhury A.R. [2004] "Chaos, signal communication and parameter estimation," *Physics Letters A* 326, 133-139.
- Sakaguchi, H. [2002] "Parameter evaluation from time sequences using chaos synchronization," *Physical Review E* 65,027201-027204.
- San Roman, F. S., Boccaletti, S., Maza, D. & Mancini, H. [1998] "Weak synchronisation of chaotic coupled map lattices," *Physical Review Letter* 81, 3639-3642.
- Schafer, C., *et al.* [1998] "Heartbeat synchronised with ventilation," *Nature* 392, 239-240.
- Scholtz, R.A. [1982] "The origins of spread spectrum communications," *IEEE Trans. On Communications*, 30,822-854.
- Shannon, C.E. [1949] "Communication theory of secrecy systems," *Bell System Tech. Journal* 28,656-715.
- Shao, Y. [2002] "Chaos of a simple coupled system generated by interaction and external forcing," *Meteorology and Atmospheric Physics* 81, 191-205.
- Shone, R. [2001] *Introduction to Economic Dynamics*, Cambridge University Press.
- Short, K.M. & Parker, A.T. [1998] "Unmasking a hyperchaotic communication scheme," *Physical Review E* 58, 1159-1162.
- Sklar, B. [2002] *Digital Communications Fundamentals and Applications 2nd Ed* (Prentice Hall).

References

- Smithson, M. [1997] "Judgment under chaos," *Organizational Behavior and Human Decision Processes* **69**, 59-66.
- Sompolinsky, H., Golomb, D. & Kleinfeld D. [1991] "Cooperative dynamics in visual processing," *Physical Review A* **43**, 6990-7011.
- Stark, J. & Hardy, K. [2003] "Chaos: useful at last?," *Science* **301**, 1192-1193.
- Steigilitz, K. [1974] *Introduction to Discrete Systems*, John Wiley & Sons Inc.
- Stewart, I. [2002] *Does God Play Dice, the New Mathematics of Chaos 2nd Edition*, Blackwell Publishers.
- Stojanovski, T., Kocarev, L. & Parlitz, U. [1996] "A simple method to reveal the parameters of the Lorenz system," *International Journal of Bifurcation and Chaos* **6**(12B), 2645-2652.
- Storm, C. & Freeman, W.J. [2002] "Detection and classification of nonlinear dynamics switching events," *Physical Review E* **66**, 057202-057205.
- Strogatz, S.H., Mirollo, R.E. & Matthews, P.C. [1992] "Coupled nonlinear oscillators below the synchronisation threshold: Relaxation by generalised Landau damping," *Physical Review Letter* **68**, 2730-2733.
- Sushchik, M., Tsimring, L.S. & Volkovskii, A.R. [2000] "Performance analysis of correlation-based communication schemes utilising chaos," *IEEE Trans. Circuits and Systems I* **47**(12), 1684-1691.
- Sundar, S. & Minai, A.A. [2000] "Synchronisation of randomly multiplexed chaotic systems with application to communication," *Physics Letters A* **273**, 5456-5459.

References

- Tao, C., *et al.* [2004] "Estimating model parameters by chaos synchronization," *Physical Review E* 69,036204-036208.
- Tass, P., *et al* [1998] "Detection of $n:m$ phase locking from noisy data: application to magnetoencephalography," *Physical Review Letters* 81,3291-3294.
- Thompson, J.M.T. & Stewart, H.B. [2002] *Nonlinear Dynamics and Chaos Geometrical Methods for Engineers and Scientists 2nd Edition*, John Wiley and Sons, New York.
- Tomochi, M. & Kono, M. [1998] "Chaotic evolution of arms races," *Chaos* 8, 808-813.
- Trippi, R.R. [1995] *Chaos and Nonlinear Dynamics in the Financial Market: Theory, Evidence and Applications*, Irwin Professional Publishing, Chicago.
- Wang, L. & Chen, G. [2004] "Using LDPC codes to enhance the performance of FM-DCSK," *Proceedings of IEEE International Midwest Symposium on Circuits and System*, I, 401-404, Hiroshima, Japan.
- Wen, G., Xu, D. & Han, X. [2002] "On creation of Hopf bifurcations in discrete-time nonlinear system *Chaos* 12,350-355.
- Wen, G. & Xu, D. [2005] "Nonlinear observer control for full-state projective synchronization in chaotic continuous-time systems," *IEEE Trans. Circuits and Systems I*, (in press)
- Wolf, A., Swift, J.B., Swinney, H.L. & Vasano, J.A. [1985] "Determining Lyapunov exponents from a time series," *Physica D* 16,285-317
- Wong, W-K., Lee, L-P. & Wong, K-W. [2001] "A modified chaotic cryptographic method," *Computer Physics Communications* 138,234-236.

References

- Wong, W-K., Ho, S-W. & Yung, C-K. [2003] "A chaotic cryptography scheme for generating short ciphertext," *Physics Letters A* **310**, 67-73.
- Xu, D. [2001] "Control of projective synchronization in chaotic systems," *Physical Review E* **63**, 27201-27204.
- Xu, D., Li, Z. & Bishop, S.R. [2001] "Manipulating the scaling factor of projective synchronization in three-dimensional chaotic systems," *Chaos* **11**, 439-442.
- Xu, D. & Li, Z. [2002] "Controlled projective synchronization in nonpartially-linear Chaotic Systems," *International Journal of Bifurcation and Chaos* **12**, 1395-1402.
- Xu, D., Ong, W.L. & Li, Z. [2002] "Criteria for the occurrence of projective synchronization in chaotic systems of arbitrary dimension," *Physics Letters A* **305**, 167-172.
- Xu, D. & Chee, C.Y. [2002] "Controlling the ultimate state of projective synchronization in chaotic systems of arbitrary dimension," *Physical Review E* **66**, 046218-046222.
- Xu, D. & Chee, C.Y. [2003] "Chaotic encryption with transient dynamics induced by pseudo-random switching keys," *International Journal of Bifurcation and Chaos*, (in press).
- Xu, D., Chee, C.Y. & Li, C. [2004] "A necessary condition of projective synchronization in discrete-time systems of arbitrary dimensions," *Chaos, Solitons & Fractals* **22**, 175-180.
- Yang, T., Yang, L-B. & Yang, C-M. [1998a] "Cryptanalysing chaotic secure communications using return maps," *Physics Letters A* **245**, 495-510.

References

- Yang, T., Yang, L-B. & Yang, C-M. [1998b] "Breaking chaotic secure communication using a spectrogram," *Physics Letters A* 247, 105-111.
- Yang, T., Yang, L-B. & Yang, C-M. [1998c] "Breaking chaotic switching using generalized synchronization: examples," *IEEE Trans. Circuits and Systems I* **45**(10), 1062-1067.
- Yang, T., Yang, L-B. & Yang, C-M. [1998d] "Application of neural networks to unmasking chaotic secure communication," *Physica D* 124, 248-257.
- Zhou, C. & Lai, C-H. [1999] "Extracting messages masked by chaotic signals of time-delay systems," *Physical Review E* 60, 320-323.
- Zhang, Y., *et al.* [1999] "A new hyperchaotic synchronization scheme for digital speech communication," *Electronic Letters* 35, 2087-2089.

Appendix A

Construction of controlled projective synchronisation based communication systems using Simulink®

In Appendix A, the construction of controlled projective synchronisation based communication system using Simulink® 5 is illustrated. This is carried out by first introducing the functions of individual building blocks used here. The communication system is made up of the transmitter and receiver ends and the communication channels. The transmitter and receiver ends consist of a number of subsystems, which include the signal generators, control vector, modulator and demodulator. These subsystems, which are constructed by linking the individual building blocks together, will then be introduced.

A.1 Individual building blocks

A.1.1 Simulink blocks

Continuous
Integrator	Integrate a signal.

Appendix A

Functions and tables

<p>Direct Look-up Table (n-D)</p>	Index into an N-dimensional table to retrieve a scalar, vector or 2-D matrix.
---	---

Math

<p>Gain/Matrix Gain</p>	Multiply block input by a specified value.
<p>Math Function</p>	Perform a mathematical function. Functions include exp, log, 10U, log 10, magnitude2, square, sqrt, pow, conj, reciprocal, hypot, rem, mod, transpose, and hermitian.
<p>Product</p>	Generate the element-wise product, quotient, matrix product, or inverse of block inputs.
<p>Sum</p>	Output the sum of inputs.

Signals and systems

<p>Matrix Concatenation</p>	Concatenate inputs horizontally or vertically
---	---

Appendix A

Merge	Combine multiple signals into a single signal.
Reshape	Change the dimensionality of a signal.
Signal Specification	Specify the desired dimensions, sample time, data type, numeric type, and other attributes of a signal.

Sinks

Display	Show the value of the input.
Out	Create an output port for a subsystem or an external output.
Scope	Display signals generated during a simulation.

Sources

Constant	Generate a constant value.
From File	Read data from a file.
In	Create an input port for a subsystem or an external input.

Appendix A

Pulse Generator	Generate square wave pulses at regular intervals.
--	---

Subsystems
If	Implement a C-like if-else control flow statement in Simulink.
If Action Subsystem	Represent a subsystem whose execution is triggered by an If or Switch Case block.

A.1.2 Communication blocksets

Basic comm functions/sequence operations
Repeat	Resample an input at a higher rate by repeating values.

Channel coding/channels
AWGN Channel	Add white Gaussian noise to the input signal.

Appendix A

Channel coding/comm sinks
<p>Error Rate Calculation</p>	Compute the bit error rate or symbol error rate of input data.

Modulation/utility functions
<p>Bit to Integer Converter</p>	Map a vector of bits to a corresponding vector of integers.
<p>Integer to Bit Converter</p>	Map a vector of integers to a vector of bits.

A.1.3 DSP blocksets

Signal management/buffers
<p>Buffer</p>	Buffer the input sequence to a smaller or larger frame size.

Signal management/signal attributes
<p>Frame Status Conversion</p>	Specify the frame status of the output, sample-based or frame-based.

Appendix A

Signal management/switches and counters
<p>Edge Detector</p>	Detect a transition of the input from zero to a nonzero value.
Statistics
<p>Mean/Running Mean</p>	Find the mean value of an input or sequence of inputs.
Math functions/matrix operations
<p>Matrix Multiply</p>	Multiply input matrices.

A.2 Communication system and subsystems

A.2.1 Communication system

Fig. A.1. Communication system setup.

Fig. A.1 shows the communication system setup with transmitter end on the left and receiver end on the right. These two blocks are subsystems that consist of a number of building blocks and other subsystems. The information carrier and feedback signals travel across three AWGN channels with adjustable signal-to-noise ratio, E_b/N_0 . The display on the top left shows the transmitted digital symbols, which in this example is a three bits symbol. The display on the top right shows the BER on the first row, the number of bit detected incorrectly on the second row and the total number of bits received on the third row.

A.2.2 Transmitter end subsystem

Fig. A.2. Transmitter end subsystem.

The transmitter end subsystem consists of four subsystems, two in ports for feedback signals and two out ports for the information carrier and transmitted symbols. In this illustration, the signal generator subsystem generates Lorenz signals. The binary information is inputted into the modulator subsystem to modulate the scaling factor that is then fed into the control vector. The control vector subsystem models the control vector $\xi = [\xi_1, \xi_2]$ given in (4.10) and generates control output $\text{zeta1}(\xi_1)$ and $\text{zeta2}(\xi_2)$.

A.2.3 Signal generator subsystem

Fig. A.3. Signal generator (Lorenz system).

Fig. A.3 shows the signal generator subsystem that is modelled after the Lorenz system given as $\dot{x}_1 = \mu_{x,1}(x_2 - x_1)$, $\dot{x}_2 = (\mu_{x,2} - z)x_1 - x_2$, $\dot{z} = x_1x_2 - \mu_{x,3}z$. The blocks on the left hand side of the integrators model the right hand sides of the differential equations with the top, middle and bottom integrators integrating the first, second and third equations respectively. The Jacobian matrix subsystem at the bottom of the signal generator subsystem formulates the Jacobian matrix to be inputted into the control vector.

A.2.4 Control vector and control function subsystems

Fig. A.4. Control vector subsystem.

The control vector subsystem, $\xi = [\xi_1, \xi_2]$, consists of two control function subsystems, control 1 and control 2, which generate control output $\text{zeta}1$ (ξ_1) and $\text{zeta}2$ (ξ_2). The inputs $\mathbf{M}(1,:)$ and $\mathbf{M}(2,:)$ at the in ports of control 1 and 2 are the first and second row of the Jacobian matrix respectively.

Fig. A.5. Control function subsystem.

Fig. A.5 shows the control function subsystem modelled according to the control function, $\xi_i = -[\mathbf{m}_i \mathbf{e} + \kappa_i e_i] / \alpha^*$, given in (4.10).

A.2.5 Transmitter end system inputs subsystem

Fig. A.6. Transmitter end system inputs subsystem.

A.2.6 Modulator subsystem

Fig. A.7. Modulator subsystem.

The information that is to be transmitted in binary form is inputted into the From File block. The binary stream is then feed into the buffer to produce blocks of n bits. These blocks of n bits are then converted into decimal values using the Bit to Integer Converter. Given that the outputs of the Bit to Integer Converter is in matrix form, it is necessary to convert these outputs into scalar values using the Frame Status Conversion block as the Direct Look-up Table block can only accept scalar value. The Repeat Block is used here to control the symbol duration. For example, if the integration time-step is set as 0.01 time-units then by setting the repeater to 300x will result in a symbol duration of 3 time-units. The Direct Look-up Table maps the received decimal values into the pre-assigned scaling factors according to Gray coding. Given in section 3.1 that $z_y/z_x = \alpha_z = \alpha^b$, where $b = 2$ for Lorenz system, the outputs of the Direct Look-up Table are square rooted (sqrt) so that at the receiver end scaling factor a will be received instead of α^2 when z_y/z_x is computed. The reason the square root function is carried out at the transmitter end instead of at the receiver as this will allow lower energy utilisation

at the receiver end given that $z(y)$ and the feedback signals only need to respond to a proportional relationship of $\sqrt{\alpha}$ as oppose to α

A.2.7 Receiver end subsystem

Fig. A.8. Receiver end subsystem.

The receiver end subsystem consists of three subsystems, one in port to receive the transmitted signal and three out ports for two feedback signals and retrieved digital symbols. The signal generator subsystem driven by the received signal is similar to the one shown in Fig. A.3 except that it does not have a Jacobian matrix subsystem for control. The receiver end system inputs subsystem is also similar to the one located within the transmitter end subsystem except that it does not have an output for slack constant for control vector subsystem.

A.2.8 Demodulator subsystem

Fig. A.9. Demodulator subsystem.

The demodulator subsystem receives $z(y)$ generated by the signal generator at the receiver end and $r = z(x) + N$ to compute the scaling factor $(\sqrt{\alpha})^2$. The computed α is then sampled at a fixed time-step using the Signal Specification block. The sampled values are inputted into the Mean block to compute the running mean, which is reset at the end of each symbol duration controlled by the Pulse Generator block and Edge Detector block. The combined function of these two blocks is also used to obtain the last running mean value at the end of each symbol duration by multiplying it by 1 while the rest of the computed running mean is multiplied by zero. The last running mean values are then rounded off to the nearest integer using the Rounding Function block. These data will undergo further computation to retrieve the decimal values of the information signal. This is carried out by using the integer to binary converter subsystem shown in Fig. A.10.

Fig. A.10. Integer to binary converter subsystem.

Fig. A.10 shows an example of the Integer to Binary Converter subsystem retrieving decimal values for digital symbols of 3 bits each, $M = 8$. The computed scaling factors first undergo If operation to bound the scaling factors within the range from 1 to 8. The three statements on the If block states that if the inputted value, u_1 , is $1 \leq u_1 \leq 8$ then the inputted value is taken as its original state. Otherwise if $u_1 > 8$ or $u_1 < 1$ then u_1 is taken as 8 and 1 respectively. After going through the If operation, all scaling factors are reduced by 1 as the minimum input value for the 1-D look-up table must be zero. The retrieved scaling factors minus 1 are then mapped back to their respective decimal values.