Synchronization of chaotic systems with application to communications

Ji, Yuan

2007

Ji, Y. (2007). Synchronization of chaotic systems with application to communications.
Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/3486>

<https://doi.org/10.32657/10356/3486>

Nanyang Technological University

Downloaded on 26 Apr 2023 20:55:34 SGT

**Synchronization of Chaotic Systems
with
Application to Communications**

Ji Yuan

School of Electrical & Electronic Engineering

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

2007

Acknowledgement

I would like to extend my gratitude to those whom in one way or another contributed to the completion of this thesis. First and foremost, I am profoundly grateful to my thesis advisor, Assoc. Prof. Wen Changyun, for his patient support and wise counsel throughout my years at NTU and for introducing me into the field of chaotic secure communications. Without his mentoring, my graduate work would not have been meaningful and pleasant.

I must also thanks to Dr. Li Zhengguo for his intelligent guidance. The numerous discussions through emails and phone and by personal talks with him have helped greatly on my development. Dr. Li Kun should also be thanked for the detailed discussions about her previous work on the same area.

I must thank my family for always acting as the better half of me. And to my fellow schoolmates at NTU, friends in Singapore and elsewhere, thank you all. Not only do you share with me your insights into the nature of scholarship in various disciplines, but also help making my graduate life smooth and social life enjoyable.

Finally, I would like to thank the School of Electrical and Electronic Engineering, Nanyang Technological University for offering me the award of a scholarship and the research facilities.

Contents

Acknowledgements	i
List of Figures	vi
Summary	x

1 Introduction

1.1 Motivation and Objectives.....	1
1.2 Major Contributions.....	7
1.3 Organization of the Thesis.....	9

2 Chaotic Systems and Review of Chaotic Secure Communication Systems

2.1 Typical Chaotic Systems.....	12
2.2 Historical Review of Chaotic Secure Communication Schemes.....	20
2.2.1 Continuously Synchronized Chaotic Secure Communication.	22
2.2.2 Impulsively Synchronized Chaotic Secure Communication.....	29

3 Impulsive Synchronization of Chaotic Systems via Linear Matrix Inequalities

3.1 Introduction.....	34
3.2 Basic Theory of Impulsive Differential Equations.....	36
3.3 Impulsive Synchronization of Chaotic Systems.....	40
3.3.1 Driving System and Driven System.....	40
3.3.2 Choice of Impulsive Intervals.....	44

3.3.3 Effectiveness Studies.....	50
3.3.4 Numerical Examples	51
3.4 Concluding Remark.....	56
 4 Time Varying Sampling Scheme With an Application to Chaotic Cryptosystems	
4.1 Introduction.....	57
4.2 A Time Varying Sampling Scheme.....	60
4.3 Application to Chaotic Cryptosystems.....	64
4.4 Simulation Results.....	71
4.5 Randomness Analysis of Time Varying Sampling Scheme.....	75
4.6 Concluding Remark.....	79
 5 Synchronization of Chaotic Systems with Parametric Uncertainty and Mismatch	
5.1 Introduction.....	80
5.2 Problem Formulation.....	82
5.2.1 System Models.....	82
5.2.2 The Lorenz Model.....	86
5.2.3 The Chua's Circuit.....	87
5.3 Synchronization Scheme.....	89
5.3.1 Scheme I.....	89
5.3.2 Scheme II.....	95
5.4 Illustrative Examples	97
5.4.1 Simulation Results with Scheme I.....	97

5.4.2 Simulation Results with Scheme II.....	103
5.5 Concluding Remark.....	108
 6 Synchronization of Chaotic Systems in the Presence of Noise	
6.1 Introduction.....	109
6.2 Problem Formulation.....	111
6.2.1 System Models.....	111
6.2.2 The Lorenz Model.....	115
6.2.3 Chen's Equation.....	117
6.3 Synchronization Scheme.....	119
6.4 Illustrative Examples.....	124
6.5 Concluding Remark.....	130
 7 Practical Impulsive Synchronization of Chaotic Systems with Parametric Uncertainty and Mismatch	
7.1 Introduction.....	131
7.2 System Models.....	133
7.3 Synchronization Scheme.....	140
7.4 Illustrative Examples.....	145
7.5 Concluding Remark.....	154
 8 Application Examples of Chaotic Secure Communication System	
8.1 Introduction of Chaotic Cryptosystems.....	156
8.2 System Design and Selection Scheme of Impulsive Intervals.....	159

8.2.1 Design of Chaotic Systems.....	161
8.2.2 Selection of Impulsive Intervals.....	164
8.2.3 Design of Key Sequences and Encryption Scheme.....	165
8.3 Text Encryption and Transmission.....	167
8.3.1 Design of Chaotic Systems.....	167
8.3.2 Selection of Impulsive Intervals.....	169
8.3.3 Simulation Studies and Results.....	169
8.4 Speech Encryption and Transmission.....	171
8.4.1 Design of Chaotic Systems.....	172
8.4.2 Selection of Impulsive Intervals	172
8.4.3 Simulation Studies and Results.....	173
8.5 Image Encryption and Transmission.....	177
8.5.1 Design of Chaotic Systems and Selection of Impulsive Intervals.....	177
8.5.2 Simulation Studies and Results.....	178
8.6 Concluding Remark.....	181
9 Conclusion and Recommendations	
9.1 Conclusions.....	182
9.2 Recommendations.....	185
Author's Publications	187
Bibliography	189

List of Figures

- 1.1 Chaos Dependence on Initial Conditions
- 1.2 Chaos Dependence on System Parameter
- 1.3 Spectral Characteristics for Lorenz system
- 2.1 Lorenz Double-Scroll Attractor
- 2.2 Response of $x(t)$ with slightly different initial conditions
- 2.3 Response of $x(t)$ with slightly different system parameters
- 2.4 Spectral Characteristics of $x(t)$ of Lorenz system
- 2.5 Chua's Circuit
- 2.6 The piecewise linear characteristics of Chua's diode
- 2.7 Responses of Chua's State Variables
- 2.8 The block diagram of the additive chaotic masking scheme
- 2.9 Block diagram of chaotic shift keying
- 2.10 The block diagrams of chaotic parameter modulation
- 2.11 The block diagrams of the non-autonomous modulation
- 2.12 Block diagram of the chaotic cryptosystem
- 2.13 Block diagram of the chaotic secure communication system
- 2.14 Illustration of the concept of a time frame and its component
- 3.1 Flowchart for the computation of $a_{\min}$
- 3.2 Stable region of the scheme in [9]

3.3 Stable region of the proposed scheme

4.1 An example of the proposed time varying sampling scheme with $N_1 = 2$ and $N_2 = 1$.

4.2 The relationship between sampled sequence and impulsive instant

4.3 Frequency spectra of X_s with fixed sampling frequency and time varying sampling frequency for Chua's circuit

4.4 Frequency spectra of X_s with fixed sampling frequency and time varying sampling frequency for Lorenz system

4.5 Autocorrelation of the variable X of the Lorenz system

4.6 Autocorrelation of the sampled Y_s of the Lorenz system

4.7 Autocorrelation of the variable X of the Chua's circuit

4.8 Autocorrelation of the sampled Y_s of the Chua's circuit

5.1 The synchronization errors of Lorenz model with the proposed control

5.2 The synchronization errors of the Lorenz model with the scheme in [71] but without the proposed control

5.3 The synchronization error of the Chua's circuit with the proposed controller

5.4 The synchronization errors of the Chua's circuit without the controller

5.5 The synchronization errors of Lorenz model with the proposed control

5.6 The synchronization errors of the Lorenz model with the scheme in [71] but without the proposed control

5.7 The synchronization error of the Chua's circuit with the proposed controller

5.8 The synchronization errors of the Chua's circuit without the controller

6.1 Synchronization Error e_x

6.2 Synchronization Error e_y

6.3 Synchronization Error e_z

6.4 Synchronization Error e_x

6.5 Synchronization Error e_y

6.6 Synchronization Error e_z

7.1 $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.01$)

7.2 $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.01$, Close-up View)

7.3: $\|e(t)\|$ of Example 7.2 for Lorenz Model

7.4: $\|e(t)\|$ of Example 7.2 for Lorenz Model (Close-up View)

7.5 $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.1$)

7.6 $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.1$, Close-up View)

7.7 $\|e(t)\|$ of Chen's Equation ($\varepsilon_0 = 0.01$)

7.8 $\|e(t)\|$ of Chen's Equation ($\varepsilon_0 = 0.01$, Close-up View)

8.1 System block diagram of chaotic cryptosystem

8.2 The original audio signal

8.3 The recovered audio signal

8.4 The difference between the recovered audio signal and the original audio signal

8.5 The recovered audio signal

8.6 The difference between the recovered audio signal and original audio signal without our scheme

8.7 The original image

8.8 The recovered image

8.9 The recovered image without our scheme

Summary

Chaotic signals generated by chaotic systems are unpredictable and have random noise like property. Such kind of property and the discovery of synchronization of chaos make chaotic secure communication a promising field both in research and in practical applications.

In this thesis, the author first proposes a new scheme for the synchronization of a class of chaotic systems by linear matrix inequality method. With this scheme, the condition for impulsive synchronization of chaotic systems is less conservative than those of existing ones and the efficiency of bandwidth utilization is improved.

A time varying sampling scheme for chaotic synchronization is then introduced. This technique can achieve a higher overall sampling rate than existing techniques where the sampling rate is fixed. This scheme can also produce a high degree of randomness for the chaotic key sequence, thus it enhances the security of the chaotic cryptosystems.

In practice, the parameters of the chaotic systems may not be constant and identical for the driving chaotic system and driven chaotic system. To improve the robustness of chaotic synchronization, the author proposes a scheme by including a controller in the driven system. In addition, the author proposes a scheme for the synchronization of

chaotic systems in noisy environment. The bound of the noise is taken into consideration in the design of impulsive schemes and controllers.

To improve the security, the controller is removed and a pure impulsive synchronization scheme is proposed. With this scheme, a guideline for choosing the impulsive intervals is given and the synchronization error can be guaranteed to converge to an arbitrary prescribed bound chosen by users.

Finally, applications to the design of chaotic cryptosystems are given with the use of pure impulsive synchronization scheme for chaotic system with parametric uncertainty and mismatch.

Chapter 1

Introduction

1.1 Motivation and Objectives

Cryptography is a technique to make information secure and the encrypted message is unintelligible to unauthorized parties. In the past, cryptography was used in military and diplomatic communities. Nowadays, increase in demand for cryptography was driven by diversified interests, (e.g., financial services like ATM which requires secure electronic transactions and businesses that need secure trade secrets stored in computers, secure wireless communications for individuals and so on). Digital communication is an obvious candidates for encryption.

There are two types of encryption algorithms in cryptography: One is symmetric algorithm and the other is asymmetric algorithm. The symmetric algorithm is also called secret key algorithm and it uses the same key for encryption and decryption. The key must be kept in secret and cannot be released to intended parties. For example, DES (Data Encryption Standard) is a type of symmetric key algorithm. However, it is found that the DES is vulnerable to some attack based on differential-linear cryptanalysis. Another example of symmetric algorithm is one-time pad used in cryptography. It is a perfectly unbreakable encryption algorithm where the plaintext is encrypted by a random key and each key is used exactly once and for only one message, the key is not shorter than the length of the message. However, it is not practical to be widely used in cryptosystems because a large memory is required to store the random and non-reused key bits. To overcome such a problem, chaotic signals can be used since their properties of randomness, aperiodicity and sensitivity to initial conditions of chaotic signals enable the chaotic system to effectively generate the one-time-pad-like key sequences for cryptosystem.

The asymmetric algorithm is also known as the public key algorithm. In the public key algorithm, the key used for encryption is different from the one used for decryption. A well known public key algorithm is RSA[1]. RSA is named with the initial of its three inventors' names, i.e., Ron Rivest, Adi Shamir and Len Adleman. The key used for encryption is a public key, implying that it may be known to public. The key for decryption is a private key, which means it should only be known to intended

parties. The sender can send a confidential message by just using public key and all communications involve only public keys, and no private key is ever transmitted. However, the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. This kind of encryption algorithm has high security level due to the difficulty of prime factorization. However, the public key algorithm like RSA has much lower encryption speed than the private key algorithm like DES both at hardware implementation and at software implementation. Traditional cryptosystems, such as RSA need huge memory and computational time, which is problematic for real-time secure communication. The problem can be solved by chaotic encryption which can realize encryption and decryption in real time. Consequently chaotic encryption can be an alternative to secure communication.

The discovery of synchronization of chaotic systems has led to the development of new cryptosystems which employ chaotic signals as a reliable, secure and rapid encryption tool in symmetric cryptography.

In 1963, the meteorologist E. N. Lorenz [2] found that even a simple set of three coupled, first order, and nonlinear differential equations can lead to completely unpredictable trajectories. He found that even very small changes in initial conditions for the nonlinear system can produce vastly different results. This discovery is considered as the milestone in the history of chaos theory. Since then, a lot of research work has been done for chaos dynamics which have important development both at

depth and width. An important development is the discovery of control and synchronization of chaos which was presented in 1990. Ott, Grebogi and Yorke firstly presented OGY scheme to control chaos by using small perturbation [3]. At the same year, Pecora and Carroll presented a synchronization scheme for the driving chaotic system and driven chaotic system [4], i.e., using the state of the driving system to drive the driven chaotic system. If there is one negative Lyapunov exponent subsystem, then the two chaotic systems can achieve synchronization. This idea is firstly applied to electronic circuit for the synchronization of chaotic system [5]. The random behavior of the chaotic system, the nonperiodical trajectories of the chaotic system, the continuous wideband spectrum, and the random like characteristics make chaotic signal suitable to encrypt messages.

The chaotic cryptosystem uses symmetric key algorithm therefore the sender and the receiver should have the exactly the same key sequence to encipher and decipher the message. Consequently, it is essential for the two chaotic systems to be synchronized when the message is enciphered by the chaotic signal in the sender side and deciphered by the chaotic signal generated by the chaotic system at the receiver side.

A brief definition of synchronization is given as follows:

Consider two dynamic systems, $\dot{X} = F(t, X)$ and $\dot{\tilde{X}} = F(t, \tilde{X})$ where t is time, $F : R^n \times R \rightarrow R^n$ is a continuous function and $X \in R^n$ and $\tilde{X} \in R^n$ are state vectors. The two systems are said to be synchronized when $\lim_{t \rightarrow \infty} \|X(t_0, X_0, t) - \tilde{X}(t_0, \tilde{X}_0, t)\| = 0$, where

t_0 is the initial time, X_0 and $\tilde{X}_0$ are initial conditions of the two systems and $\|\cdot\|$ is the Euclidean norm.

Chaotic synchronization has been developed from the stage of continuous synchronization to the stage of impulsive synchronization. For continuous synchronization, the chaotic signals are transmitted all the time in the public channel. On the other hand, for impulsive synchronization approach, the impulses are transmitted from the encrypter side to the decrypter side only at impulsive instants. The impulsive synchronization [6-15] of chaotic systems outperforms the continuous synchronization [16-22] in terms of security enhancing and transmission bandwidth efficiency. After the synchronization is achieved, the message can be encrypted in the encrypter side and sent to the decrypter side. The impulses are still needed for transmission to maintain the synchronization status. It is desirable to transmit the impulses less frequently so as to gain more bandwidth for the message and also increase security level. Therefore we will consider new approaches to achieve this.

For some chaotic communication schemes [23], frequency aliasing is obtained where sampling frequency of the chaotic signal is below the its bandwidth. For this kind of chaotic secure communication scheme, the randomness of the key sequence is improved and the key sequence has the white noise-like spectrum and autocorrelation properties. However, the bandwidth utilization of the channel is low for this scheme.

Therefore, it is necessary to develop a scheme to keep randomness properties of the key sequence while increasing the bandwidth utilization of the channel.

For most existing chaotic synchronization schemes, the chaotic model is considered with no parametric uncertainties and mismatches between the chaotic systems in the encrypter and in the decrypter. Unfortunately, parameters of chaotic systems are usually uncertain and there are mismatches between the parameters of the chaotic systems in the encrypter and decrypter because of imperfect manufacturing, ambient noise, temperature fluctuation and some other reasons. Therefore it is necessary to consider these parametric uncertainties and mismatches in the chaotic communication models and find schemes to achieve synchronization ensuring the synchronization error approach to and stay within a prescribed bound.

Furthermore, in many chaotic synchronization schemes, it is considered noise-free environment for chaotic systems. However, in practice, chaotic systems are inevitably interfered with certain internal and external noise, which may be caused by temperature variation, voltage fluctuation and other factors. A synchronization scheme should be developed to cope with this practical issue.

It is important to explore potential applications of chaotic secure communication systems such as text encryption, speech encryption and image encryption.

The main objectives of this project are to solve the problems mentioned above.

1.2 Major Contributions

In this section, major contributions are summarized as following:

Firstly, a less conservative condition which gives guideline for choosing impulsive intervals is obtained by linear matrix inequality method. With this approach, synchronization impulses can be sent less frequently therefore it improves the utilization of the channel bandwidth. Moreover, the security of the chaotic secure communication system is increased because fewer chaotic variables are to be transmitted.

Secondly, a time varying sampling scheme is introduced to enhance the security of the chaotic cryptosystem and achieve better bandwidth utilization in comparison with the existing frequency aliasing sampling scheme for chaotic systems [23]. For our time varying sampling scheme, the chaotic signals are sampled at time-varying rate, which can produce a higher degree of randomness. This scheme improves the security and is more bandwidth efficient than the scheme in [23].

Thirdly, a control method is designed for the synchronization of chaotic systems with parametric uncertainties and mismatches. Previous works in chaotic synchronization usually consider that the parameters of chaotic systems are invariant and identical for

the two systems in the encrypter and decrypter. In practical situation, the parameters of chaotic systems are not constant as they may change in a small range. By applying this control method, chaotic synchronization can be achieved with parametric uncertainties and mismatches.

Fourthly, a control scheme is designed for synchronization of chaotic systems in the presence of noise. It is practical to consider noise in the chaotic systems, while previous works only consider noise-free environment for chaotic systems. This problem is solved by an approach similar to the scheme for solving the parametric uncertainties and mismatches.

Fifthly, a pure impulsive synchronization scheme is designed for chaotic systems with parametric uncertainties and mismatches. With this scheme, it can be guaranteed that the synchronization error stay within a predefined arbitrary bound. An explicit bound on the length of impulse interval is established as a function of the prescribed error bound and the bounded parametric uncertainties and mismatches. This is the first result that gives a quantitative relationship between the synchronization error and the time intervals between impulses. Therefore a clear guideline is available on how to choose the impulsive intervals for given bound.

Finally, this scheme is applied to text encryption, speech encryption and image encryption for chaotic secure communication systems. Comparisons with existing

schemes are made and simulation results show the effectiveness of the proposed scheme.

1.3 Organization of the Thesis

The rest of the thesis is organized as follows.

Chapter 2 gives some typical chaotic systems which are usually used in chaotic secure communication systems and reviews the history of chaotic secure communications. In this chapter, the structure of chaotic secure communication system is also introduced.

Chapter 3 studies impulsive synchronization of a class of chaotic systems. Firstly the basic theory of impulsive differential equations is presented. The models of driving chaotic system and driven chaotic system are given. An LMI (linear matrix inequality) method is introduced to derive a less conservative condition for impulsive synchronization. Synchronization of Lorenz system and Chua's circuit with LMI method are given as numerical examples respectively.

Chapter 4 proposes a time varying sampling scheme for chaotic signals. With this scheme, chaotic signals are sampled at a lower rate to achieve better randomness property for the key sequence. A tradeoff between the security and the bandwidth utilization is obtained by this method.

Chapter 5 proposes two schemes solving the parametric uncertainty and mismatch problem which inevitably exists in chaotic systems. The results give guidelines for choosing impulse intervals. Numerical examples are given to verify the performance of the proposed scheme.

Chapter 6 proposes a scheme for the synchronization of chaotic systems in the presence of noise. The control strategy guarantees the synchronization of chaotic systems. Simulation studies are carried out on the Lorenz model and Chen's system. The result shows that the states of the driven chaotic system can quickly converge to the states of the driving chaotic system.

Chapter 7 presents a practical pure impulsive synchronization scheme for chaotic systems with parametric uncertainties and mismatches. A guideline is provided for choosing impulsive intervals. With the given guideline, the synchronization error can converge to a pre-specified bound.

Chapter 8 applies the practical impulsive synchronization scheme of Chapter 7 to chaotic cryptosystem. A text encryption, a speech encryption and an image encryption are presented respectively. Simulation results are given to show the effectiveness of the proposed scheme.

Chapter 9 gives the conclusion of the thesis and points out some possible future research directions of chaotic secure communication systems.

Chapter 2

Chaotic Systems and Review of Chaotic Secure Communication Systems

Chaos is currently one of the most intriguing topics in nonlinear system research. A chaotic dynamical system is a deterministic system that exhibits random behavior. Since, in practice, initial conditions can never be neglected, the behavior of a chaotic system is unpredictable, and therefore, random-like. Over the past decade, many synchronizing chaotic schemes [24-36] have been proposed and applied to chaos-based communication systems.

In this chapter, we review some typical chaotic systems and the history of chaotic secure communication systems.

2.1 Typical Chaotic Systems

1) Lorenz Model

Lorenz is a meteorologist studying weather forecasting. He introduced a simplified model of fluid and discovered chaos in his computer simulation. This discovery made chaotic systems soon begin to be recognized and studied in many branches of science. The application of the Lorenz equations to weather forecast has led to a popular metaphor known as the *butterfly effect* [37]. That is, if the conditions were such that the atmosphere displays a chaotic behavior, even the flapping of a butterfly's wings would make long-term predictions of weather meaningless!

The generalized three ordinary differential equations, namely Lorenz model, are given as:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = rx - y - xz \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (2.1)$$

The equations are autonomous, which means time does not explicitly appear on the right hand side, nonlinear which can be seen in the second and third equations, and dissipative as volume in phase space shrink in dynamics. In addition, their solutions are bounded and aperiodic.

We use a typical chaotic system-Lorenz Model below and give some experimental examples to illustrate some chaotic properties. We now look at an example of the Lorenz dynamics. For a particular case, we let the Lorenz oscillator's initial condition be $[-2.12, -0.05, 0.8]$ and the parameter be $\sigma=16, r=45.6, b=4$. Then the Lorenz double scroll oscillator simulated by Matlab is observed in Figure 2.1.

Figure 2.1: Lorenz Double-Scroll Attractor

Now we study the property of dependence on initial conditions by changing the initial condition to $[-2.12, -0.05, -0.88]$. The result is shown in Figure 2.2, where the solid waveform and the dash-dotted waveform correspond to the trajectories of the previous initial condition set and the modified one respectively. From the figure, the trajectories diverge very quickly even though the initial conditions are quite close.

If we change the parameters slightly to $\sigma=16.1, r=45.6, b=4$, we can have similar observation, i.e. the trajectories diverge quickly from each other as shown in Figure 2.3.

The spectral characteristic of the x component of the Lorenz system is shown in Figure 2.4. We can see from the figure that it has a continuous and broad banded frequency spectrum.

Figure 2.2: Response of $x(t)$ with slightly different initial conditions

Figure 2.3: Response of $x(t)$ with slightly different system parameters

Figure 2.4: Spectral Characteristics of $x(t)$ of Lorenz system

From the simulation, it is shown that the chaotic system can produce wideband noise-like signals which make the chaotic parameters a good key seed for cryptosystems to generate pseudorandom numbers.

2) Chua's Circuit

Chua's circuit is a simple electronic circuit showing chaotic dynamics, developed by Leon O. Chua [38-40]. The circuit is shown in Figure 2.5 and is a third-order autonomous, dissipative electrical circuit featured by its simplicity, which became popular for the study of chaos. The Chua's circuit allows almost all of the dynamical behavior seen in computer simulations to be implemented in an electronics lab and viewed on an oscilloscope. It is an RLC circuit that contains only four linear elements

(two capacitors with capacitances C_1 and C_2 , one linear resistor with resistance $1/G$, and one inductor with inductance L) and a nonlinear resistor, N_R , called Chua's diode. This diode is responsible for the complexity of dynamical behavior that the circuit can describe.

Figure 2.5: Chua's Circuit

The state equations for Chua's oscillator are given by:

$$\begin{cases} C_1 \frac{dv_1}{dt} = \frac{1}{R}(v_2 - v_1) - f(v_1) \\ C_2 \frac{dv_2}{dt} = \frac{1}{R}(v_1 - v_2) + i_3 \\ L \frac{di_3}{dt} = -v_2 - R_0 i_3 \end{cases} \quad (2.2)$$

where v_1 , v_2 and i_3 are the voltage across the capacitor C_1 , the voltage across the capacitor C_2 , and the current through the inductor L , respectively. We define $G = \frac{1}{R}$.

The term $R_0 i_3$ is added to account for small resistance of the inductor in the physical circuit. The piecewise linear function v - i characteristic $f(v_1)$ is given by

$$f(v_1) = G_b v_1 + \frac{1}{2} (G_a - G_b) \left\{ |v_1 + B_p| - |v_1 - B_p| \right\}$$

where B_p is the breakpoint voltage of the Chua's diode as show in Figure 2.6.

Figure 2.6: The piecewise linear characteristics of Chua's diode

(2.2) can be rewritten in the following generalized form:

$$\begin{cases} \frac{dx}{dt} = \alpha(y - x - f(x)) \\ \frac{dy}{dt} = x - y + z \\ \frac{dz}{dt} = -\beta y - \gamma z \end{cases} \quad (2.3)$$

where α , β and γ are three constant parameters, and $f(x)$ is the piece-wise linear function of the Chua's diode, which is given by

$$f(x) = bx + \frac{1}{2}(a-b)(|x+1| - |x-1|)$$

where $a < b < 0$ are two constants.

For example, if the parameters are $a = -\frac{8}{7}$, $b = -\frac{5}{7}$, $\alpha = 16$, $\beta = 10$ and $\gamma = 0.0385$, then the

response of Chua's state variables are shown in the Figure 2.7.

Figure 2.7: Responses of Chua's State Variables

3) Chen's Equation

A new chaotic attractor, Chen's attractor, which is given in (2.4), was observed and reported in [41-43]. In contrast to the Lorenz butterfly attractor, Chen's attractor is topologically more complex [42] but without changing the smooth quadratic function.

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x + cy - xz \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (2.4)$$

where a , b and c are parameters of Chen's equation.

It can be noted that all the above chaotic systems can be decomposed into two parts, the linear part and nonlinear part.

We let $X^T = (x, y, z)$, and then chaotic systems can be rewritten as:

$$\frac{dX}{dt} = AX + \psi(X) \quad (2.5)$$

For Lorenz system,

$$A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix}, \quad (2.6)$$

$$\psi(X) = [0 \quad -xz \quad xy]^T \quad (2.7)$$

For Chua's oscillator,

$$A = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix}, \quad (2.8)$$

$$\psi(X) = [-\alpha f(x) \quad 0 \quad 0]^T \quad (2.9)$$

For Chen's equation,

$$A = \begin{bmatrix} -a & a & 0 \\ c-a & c & 0 \\ 0 & 0 & -b \end{bmatrix}, \quad (2.10)$$

$$\psi(X) = [0 \quad -xz \quad xy]^T \quad (2.11)$$

2.2 Historical Review of Chaotic Secure Communication Schemes

In the chaotic secure communication systems, there are two identical chaotic systems in the transmitter and in the receiver. The one in the transmitter is called the driving system while the one in the receiver is called the driven system. Pecora and Carroll's seminal paper demonstrated that two chaotic systems can be synchronized under certain conditions when a coupling is imposed onto the chaotic systems [4]. The method proposed is to divide the original chaotic systems into a driving subsystem and an identical copy of the driving subsystem in the receiver. The response system is driven by the state variables of the driving system. The two subsystems will synchronize when their conditional Lyapunov exponents are all less than zero. Ever since then, chaos synchronization of nonlinear oscillators has been widely studied for applications in

secure communications [44-47]. In chaotic secure communication systems, the message signal is modulated with the chaotic spread signals. Although the bandwidth utilization for transmission is not as good as the conventional schemes, it will be more difficult for attackers to decipher the scrambled message. In conventional cryptosystems, the spectrum of encrypted message is limited in a narrow bandwidth, which will ease the cryptanalysis. However, in chaotic secure communication systems, the scrambled message is hidden in the chaotic spread spectrum carrier.

A number of schemes have been proposed for analog and digital communications using chaotic signals as the information carrying signals. e.g., chaos masking, chaos-shift-keying (CSK), chaos modulation, chaotic cryptosystem etc. [16,18-22,31]. Although the approaches are different in utilizing chaos in secure communication to some extent, the basic ideas are all the same, i.e., utilizing the chaotic signal to mask the information-bearing signal, by transmitting signal information hidden in the chaotic signal. At the receiver side a synchronized chaotic signal is used to decipher the scrambled message. The chaos encrypted signal become long-term unpredictable and its spectrum is broadband, which makes the cryptanalysis a very difficult task.

The synchronization between two chaotic systems can be achieved by continuous driving chaotic synchronization approach or impulsive synchronization approach. In the continuous driving synchronization approach, the synchronization signals are transmitted to the receiver continuously and thus approaches synchrony. The first three

generations of chaotic secure communication are all based on the continuous synchronization. In the impulsive synchronization approach, the synchronization signals are transmitted to the receiver discontinuously and this gives the fourth generation of chaotic secure communication.

For the first three generations of chaotic secure communication, chaotic systems are often unidirectional-coupled to each other. Driving signals are transmitted continuously to the response systems such that synchronization errors can be controlled within a given range or converge to zero. When the transmitter and the receiver are synchronized, the states of the chaotic systems in the transmitter can be used as key sequence to encipher the message signal and the states of the identical chaotic system in the receiver can be used as key sequence to decipher the message.

2.2.1 Continuously Synchronized Chaotic Secure Communication

A number of methods developed for the first three generations of chaotic secure communication from 1993 to 1997. In this section, we review these methods.

a. The First Generation

(i) Chaotic Masking

The first generation is known as additive chaotic masking, which was developed in 1993 proposed by K. M. Cuomo *et al* [16]. As illustrated in Figure 2.8, the main idea is to simply add the chaotic signal to the message signal so as to hide the information-bearing signal. In the transmitter and the receiver, we have two identical chaotic systems. The chaotic signal denoted by $c(t)$ is one of the state variables of the chaotic

system in the transmitter. At the transmitter, the message signal $m(t)$ is added to the chaotic signal $c(t)$. After the receiver receives the scrambled signal $r(t)=m(t)+c(t)$, the chaotic signal $c(t)$ generated in the receiver is subtracted from the encrypted signal $r(t)$, so the message can be recovered. Since the chaotic signal is generally 20dB to 30dB higher than the message signal, the message signal is very sensitive to channel noise and parameter mismatch. If the channel noise is comparable to the message signal, the message may not be recovered. Therefore, this approach is impractical. In addition, this scheme has very low degree of security [48]. As pointed out in [48], *nonlinear dynamic forecasting* analysis approach was used to predict the carrier dynamics and then subtract away the predicted values to reveal the hidden signal. By dividing the phase space into several local regions, each local region will have some pieces of small trajectory, which can be studied as a group to determine the local behavior in that patch of the phase space. It is possible to build up the global behavior of the dynamical system after studying all the patches of phase space separately. It can be concluded that chaotic masking scheme can offer some privacy but cannot provide high level of communication security.

Figure 2.8: The block diagram of the additive chaotic masking scheme

(ii) Chaotic Shift Keying

Chaotic shift keying, alias chaotic switching, is a method that can be applied to digital communication systems proposed by H. Dedieu *et al.* [18]. In this scheme, as shown in Figure 2.9, the message signal is a binary signal, which is used to switch the chaotic system between two similar chaotic attractors. The two attractors encode bit 0 and bit 1 of the message signal respectively. These two attractors are generated by a chaotic system switching between two different parameter sets. At the receiver, the received signal $r(t)$ is used to drive a chaotic system, which is identical to the chaotic system in the transmitter. The message signal is recovered by low-pass filtering and then thresholding the synchronization error signal $e(t)$. This simple method was demonstrated by Parlitz *et al.* based on laboratory experimental test [19]. This scheme is robust to noise and parameter mismatch.

However, it has low degree of security as analyzed in [49]. The short-time zero-crossing rate (STZCR) of the derivative of $s(t)$ is calculated and the distribution is sufficient to distinguish the binary bit, thus the digital signal encoded by chaotic switching technique is recovered even without knowing the values of parameters of the chaotic systems.

Figure 2.9: Block diagram of chaotic shift keying

b. The Second Generation

The second generation was presented from 1993 to 1995 proposed by Yang and Wu *et al.*, which is called chaotic modulation. Two different ways are used to modulate information-carrying signals into chaotic carriers, i.e., chaotic parameter modulation [20] and chaotic non-autonomous modulation [21].

(i) Chaotic Parameter Modulation

This scheme is shown in Figure 2.10 employing message signal to change the parameters of the chaotic transmitter. The message signal $m(t)$ is used to modulate some parameters of the chaotic system in the transmitter such that its trajectories keep changing in different chaotic attractors. Since the space of the chaotic system is very complex, it is very hard to figure out how parameters change even though the intruder knows some partial knowledge of the structure of the chaotic system in the transmitter. At the receiver, an adaptive controller is used to adaptively tune the parameters of the chaotic system such that the synchronization error approaches zero. By doing this, the output of the adaptive controller can recover the message signal.

Figure 2.10: The block diagram of chaotic parameter modulation

(ii) Chaotic Non-autonomous Modulation

This scheme is shown in Figure 2.11. Rather than changing the parameters of the chaotic transmitter, this method uses the message signal to perturb chaotic attractor directly in the phase space. Unlike in the chaotic parameter modulation approach, the transmitter in chaotic non-autonomous modulation is switched among different trajectories of the same chaotic attractor.

These schemes improve the degree of security to some extent but is still found unsatisfactory [50]. As mentioned in [50], the phase space can be reconstructed by local prediction method. The message signal distorts the phase space enough to allow for the detection and extraction of the message signal. The prediction process is sufficient accurate to recover the spectrum of the hidden message. Once the spectrum of the message is revealed, the extraction of the message turns into a signal processing problem.

Figure 2.11: The block diagrams of the non-autonomous modulation

c. The Third Generation

The third generation, also called chaotic cryptosystem, is shown in Figure 2.12 and was proposed in 1997 by Yang *et al.* [22]. This generation improves the degree of security to a much higher level than the first two generations. In this generation, the combination of the classical cryptographic technique and chaotic synchronization is used to enhance the degree of security.

In the chaotic cryptosystem, the plain text signal $p(t)$ is encrypted by an encryption rule with a key signal, $k(t)$, which is generated by the chaotic system in the transmitter. The scrambled signal is used further to drive the chaotic system such that the chaotic dynamics is changed continuously in a very complex way. Then another state variable $s(t)$ of the chaotic system in the transmitter is transmitted through the public channel which can be accessed by the intruder. Since the intruder cannot get access to the chaotic hardware key, it is very difficult to find $p(t)$ out from $s(t)$. At the receiver, the received signal $r(t)=s(t)+n(t)$, where $n(t)$ is the channel noise, is used to synchronize both chaotic systems in the transmitter and the receiver. After the chaotic synchronization is achieved, the signal $k(t)$ and $y(t)$ can be recovered at the receiver with some noise as denoted by $k'(t)$ and $y'(t)$. By feeding $k'(t)$ and $y'(t)$ into the decryption rule at the receiver, the plain text signal can be recovered with some noises as $p'(t)$.

Figure 2.12: Block diagram of the chaotic cryptosystem

All of the above- mentioned schemes, except for chaotic cryptosystem, have low level of security as they need to transmit the state of the chaotic systems continuously from the transmitter side to the receiver side. The state of chaotic system can be collected at any time by attackers and reconstruction of the phase space can be created. When viewed in some suitable phase space, the chaotic dynamical system exhibits very regular geometric structures. The geometric structures are nonperiodic and are often fractal, so they are far from random. These structures in phase space can be used to predict the behavior of the chaotic carrier so that the hidden message can be extracted, or at least to improve significantly the ratio of message signal power to noise power.

2.2.2 Impulsively Synchronized Chaotic Secure Communication

The chaotic secure communication via impulsive synchronization, also called the fourth generation, as shown in Figure 2.13, is the latest generation up to now and was proposed in 1997 by Yang *et al.* [6,51] and was further developed by Li *et al.* [10,13]. In this generation, discontinuous driving synchronization was introduced. Samples of the state variables of the driving system at discrete instances are used to drive the

response system. These samples are called the synchronization impulses and are employed to impulsively control the error system between the driving and response system.

The system contains two parts-the encrypter and the decrypter. In both the encrypter and the decrypter, there exist two identical chaotic systems and two identical conventional cryptographic schemes. In the encrypter, the message is firstly digitized and then act as plaintext $p(t)$ in the encryption process. A function of the state variables generated by the chaotic systems is used as the cipher key sequences. The scrambled message are generated by the conventional cryptographic scheme $e(\cdot)$. The encryption algorithm combines the plaintext $p(l)$ and the running key sequence $k(l)$ to generate the ciphertext $c(l)$. There is also a magnifying glass to enlarge the parameter mismatch between the encrypter and the decrypter. The scrambled message and the synchronization drive impulses are composed together as packets before transmission.

At the decrypter, the packets are decomposed into scrambled message and synchronization impulses. The separated synchronization impulses are used to make the chaotic system in the decrypter to synchronization with the one in the encrypter. At the decrypter, we use the conventional cryptographic scheme $d(\cdot)$ to decrypt the scrambled message to obtain the recovered plaintext. When the chaotic system in the receiver is synchronized with that in the transmitter, the decrypter reproduces the running-key sequence $\tilde{k}(l)$, same as that generated in the encrypter, $k(l)$. After the decrypter

synchronizes with the encrypter, the message can be transmitted and thus decrypted by the decrypter.

Figure 2.13: Block diagram of the chaotic secure communication system [13]

In this scheme, impulsive synchronization and the conventional cryptography are combined together. By this means, we can increase the complexity of the transmitted signal and reduce the redundancy in the transmitted signal.

After the driving and response chaotic systems pass through the transient state, message can be encrypted and transmitted to the receiver in the synchronized system. The message and the synchronization impulses are packtized together before transmission as shown in Figure 2.14. In packtization, the transmitted signal has two regions in each time frame. The first region of the time frame is a synchronization region consisting of synchronization pulses. The synchronization pulses are used to impulsively synchronize the chaotic systems in both the encrypter and the decrypter. The second region of the time frame is the scrambled signal region where the scrambled signal is contained.

Figure 2.14 Illustration of the concept of a time frame and its components

The composition block in Figure 2.14 is used to combine the synchronization pulses and the scrambled signal. The simplest combination method is to substitute the synchronization pulses in the beginning Q seconds of each time frame with synchronization pulses. The decomposition block is used to separate the

synchronization region and the scrambled signal region within each frame at the receiver end. Then the separated synchronization pulses are used to ensure that the chaotic system in the receiver synchronizes with that in the transmitter.

Chapter 3

Impulsive Synchronization of Chaotic Systems via Linear Matrix Inequalities

3.1 Introduction

The synchronization of two chaotic systems is very important for chaotic secure communication and can be achieved by either continuous synchronization approach or impulsive synchronization approach. The synchronization impulses are transmitted at discrete time instants in the latter approach while they are transmitted continuously in the former one.

Recently, Yang *et al.* [6] applied stability results of impulsive differential equation in [52] to obtain some sufficient conditions for the stability of impulsive synchronized chaotic systems with equidistant impulsive intervals. It is worth to point out that these conditions are conservative in the sense that the Lyapunov function is required to be nonincreasing along the whole sequence of the switchings. Li *et al.* [10] and Xie *et al.* [9] derived some less conservative conditions as the Lyapunov function is only required to be nonincreasing along a subsequence of the switchings. As a result, the length of impulsive intervals can be varying and increased. However, there is still a lot of space to improve the result by exploring the structure knowledge of chaotic systems.

In this chapter, we utilize the fact that the linear part of a chaotic system is usually composed of a stable subsystem to further relax the synchronization conditions. Using the method of linear matrix inequalities (LMI) [53], we can find a more appropriate Lyapunov function to analyze the chaotic systems. In [15], matrix inequalities were employed to provide a general design procedure for the impulsive synchronization of master-slave systems by measurement feedback where the matrix inequalities are solved by a nonlinear optimization method. The synchronization conditions in [15] are still conservative in the sense that the Lyapunov function is required to be nonincreasing along the complete switching sequences. The length of impulsive interval is also fixed. In this chapter, our method is much simpler than that in [15] because linear matrix inequalities are used, which result in a linear optimization approach. Our approach can give the largest bound on impulsive intervals among all the available methods including the one in [15]. This implies the length of these intervals

can be further allowed longer and synchronization impulse can be transmitted less frequently to the decoder to synchronize the decoder and the encoder. In other words, less bandwidth is required for the transmission of synchronization impulses and hence the bandwidth efficiency is enhanced. The results can therefore improve the efficiency of existing technologies on secure communications and secure spread communications.

3.2 Basic Theory of Impulsive Differential Equations

Before we study the impulsive synchronization scheme, some preliminaries about the impulsive differential equations are given. Instead of studying the stability of the original impulsive differential equation, we define a comparison system. The stability of the original impulsive differential equation can be determined by the stability of the comparison system.

Consider the general nonlinear system

$$\dot{X} = f(t, X) \quad (3.1)$$

where $f : R^+ \times R^n \rightarrow R^n$ is continuous, $X \in R^n$ is the state variable, and $\dot{X} \triangleq \frac{dX}{dt}$.

Consider a discrete set of time instants $\{\tau_i\}$ satisfying

$$0 < \tau_1 < \tau_2 < \cdots < \tau_i < \tau_{i+1} < \cdots, \quad \tau_i \rightarrow \infty \text{ as } i \rightarrow \infty$$

$$\text{Let } U(i, X) = \Delta X \big|_{t=\tau_i} \triangleq X(\tau_i^+) - X(\tau_i^-) \quad (3.2)$$

be the “jump” of the state variable at time instant τ_i . Then an impulsive differential system is described by

$$\begin{cases} \dot{X} = f(t, X), & t \neq \tau_i \\ \Delta X = U(i, X), & t = \tau_i \\ X(t_0^+) = X_0, & t_0 \geq 0, i = 1, 2, \dots \end{cases} \quad (3.3)$$

This is called an impulsive differential equation [52]. To study the stability of the impulsive differential equation (3.3), we use the following definitions and theorems [52].

Definition 3.1 Let $V : R^+ \times R^n \rightarrow R^+$, then V is said to belong to class V_0 if

(1) V is continuous in $(\tau_{i-1}, \tau_i] \times R^n$ and for each $X \in R^n, i = 1, 2, \dots$

$$\lim_{(t,y) \rightarrow (\tau_i^+, X)} V(t, y) = V(\tau_i^+, X) \quad (3.4)$$

exists.

(2) V is locally Lipschitzian in X .

Definition 3.2 For $(t, y) \rightarrow (\tau_i^+, X) \times R^n$ we define

$$D^+V(t, X) = \limsup_{h \rightarrow 0} \left(\frac{1}{h} [V(t+h, X+hf(t, X)) - V(t, X)] \right) \quad (3.5)$$

Since the system in (3.3) is an n^{th} -order impulsive differential equation, instead of studying the stability of (3.3), it is convenient to study that of a first-order impulsive differential equation which is given by the following definition.

Definition 3.3 Comparison system

Let $V \in V_0$ and assume that

$$\begin{cases} D^+V(X, t) \leq g(t, V(t, x)), & t \neq \tau_i \\ V(t, X + U(i, X)) \leq \psi_i(V(t, X)), & t = \tau_i \end{cases} \quad (3.6)$$

where $g : R_+ \times R_+ \rightarrow R$ is continuous and $\psi_i : R_+ \rightarrow R_+$ is nondecreasing. Then the following system

$$\begin{cases} \dot{w} = g(t, w), & t \neq \tau_i \\ w(\tau_i^+) = \psi_i(w(\tau_i)) \\ w(t_0^+) = w_0 \geq 0 \end{cases} \quad (3.7)$$

is called the *comparison system* of (3.3).

Definition 3.4

Denote set S_ρ as

$$S_\rho = \{X \in R^n \mid \|X\| < \rho\} \quad (3.8)$$

where $\|\cdot\|$ denotes the Euclidean norm on R^n .

Definition 3.5 A function α is said to belong to class K if $\alpha \in C[R_+, R_+]$, $\alpha(0) = 0$ and $\alpha(x)$ is strictly increasing in x .

Assumption 3.1 $\mathbf{f}(t, 0) = 0, U(i, 0) = 0$ and $g(t, 0) = 0$ for all i .

Remark: With the above assumption we find that the trivial solutions of (3.3) and (3.7) are identical for all time except at the discrete set $\{\tau_i\}$.

Theorem 3.1 below shows that the stability of an n^{th} -order impulsive differential equation is equivalent to that of first-order impulsive equation, i.e., the comparison system.

Theorem 3.1 (Theorem 3.2.1, page 139, [52]): Assume that the following three conditions are satisfied:

- (1) $V : R_+ \times S_\rho \rightarrow R^+$, $\rho > 0$, $V \in V_0$, $D^+V(t, X) \leq g(t, V(t, X))$, $t \neq \tau_i$.
- (2) There exists a $\rho_0 > 0$ such that $X \in S_{\rho_0}$ implies that $X + U(i, X) \in S_{\rho_0}$ for all i and $V(t, X + U(i, X)) \leq \psi_i(V(t, X))$, $t = \tau_i$, $X \in S_{\rho_0}$
- (3) $\beta(\|X\|) \leq V(i, X) \leq \alpha(\|X\|)$ on $R^+ \times S_\rho$, where $\alpha(\cdot), \beta(\cdot) \in K$.

Then the stability properties of the trivial solution of the comparison system (3.7) imply the corresponding stability properties of the trivial solution of (3.3).

In the next theorem, we present the stability criterion of a first-order impulsive differential equation, which is the general form of the comparison system of a synchronization error system that we will study in this thesis.

Theorem 3.2 (Corollary 3.2.1, page 142, [52]):

Let $g(t, \omega) = \lambda(t)\omega$, $\lambda \in C^1[R_+, R_+]$, $\psi_i(\omega) = d_i\omega$, $d_i \geq 0$, for all i . Then the origin of system (3.3) is asymptotically stable if the conditions

$$\lambda(\tau_{i+1}) + \ln(\xi d_i) \leq \lambda(\tau_i), \text{ for all } i, \text{ where } \xi > 1 \quad (3.9)$$

and

$$\dot{\lambda}(t) \geq 0 \quad (3.10)$$

are satisfied.

3.3 Impulsive Synchronization of Chaotic Systems

In this section, we first discuss some conditions obtained in previous impulsive synchronization schemes and then derive a new scheme to obtain a larger impulsive interval in order to achieve better bandwidth utilization.

3.3.1 Driving System and Driven System

In the impulsive synchronization scheme, the driving system is given as

$$\dot{X}(t) = AX(t) + \psi(X(t)) \quad (3.11)$$

where $X(t) \in R^n$ is the state vector and globally bounded, $A \in R^{n \times n}$ is a constant matrix, and $\psi: R^n \rightarrow R^n$ is a nonlinear function which gives rise to chaotic dynamics and satisfies the following inequalities:

$$\|\psi(X(t))\| \leq L \|X(t)\| \quad (3.12)$$

where L is a positive number and $\|\cdot\|$ denotes the Euclidean norm on R^n .

At discrete instant τ_i , $i=1,2,\dots$, the state variables of the driving system are transmitted to the driven system and the state variables of the driven system are subject

to sudden changes at these instants. Therefore, the driven system can be written in the form of

$$\begin{cases} \frac{dX'}{dt} = AX' + \psi(X'), & t \neq \tau_i \\ \Delta X'|_{t=\tau_i} = -Be, & i = 1, 2, \dots \end{cases} \quad (3.13)$$

where $X' = (x', y', z')$ denotes the state variables of the driven system, $e = (x - x', y - y', z - z')^T$ is the synchronization error between the driving and the driven system, and $\Delta X'|_{t=\tau_i} = X'(\tau_i^+) - X'(\tau_i^-)$. Note that τ_i^+ and τ_i^- are the times immediately after and before τ_i (i.e., $\tau_i^+ = \lim_{\varepsilon \rightarrow 0^+} (\tau_i + \varepsilon)$, $\tau_i^- = \lim_{\varepsilon \rightarrow 0^+} (\tau_i - \varepsilon)$), ($i = 1, 2, \dots$) $B \in R^{n \times n}$ is a constant diagonal matrix and the spectral radius of $I + B$ satisfies $\|I + B\| < 1$ where I denotes identity matrix.

This thesis focuses on considering three-dimensional chaotic systems because they have many applications.

Define $\phi(X, X') = \psi(X) - \psi(X')$ and it is assumed that the chaotic systems given in (3.11) and (3.13) satisfy the following condition:

$$2(X - X')^T \phi(X, X') \leq (X - X')^T (H + H^T) (X - X') \quad (3.14)$$

The error system of impulsive synchronization is given by

$$\begin{cases} \dot{e} = Ae + \phi(X, X'), & t \neq \tau_i \\ \Delta e|_{t=\tau_i} = Be, & i = 1, 2, \dots \end{cases} \quad (3.15)$$

Two typical examples of chaotic systems are given as follows:

(i) Lorenz system [2]

$$A = \begin{bmatrix} -\delta & \delta & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} \quad (3.16)$$

$$\psi(X) = [0 \quad -xz \quad xy]^T \quad (3.17)$$

$$H = \begin{bmatrix} \sqrt{2}M/2 & 0 & 0 \\ 0 & \sqrt{2}M/2 & 0 \\ 0 & 0 & \sqrt{2}M/2 \end{bmatrix} \quad (3.18)$$

where δ, r , and b are three constants, M is the upper bound of y and z .

(ii) Chua's oscillator [40]

$$A = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix} \quad (3.19)$$

$$\psi(X) = [-\alpha f(x) \quad 0 \quad 0]^T \quad (3.20)$$

$$H(X) = \begin{bmatrix} |\alpha a| & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (3.21)$$

where $f(x) = bx + \frac{1}{2}(a-b)\{|x+1| - |x-1|\}$, $|\cdot|$ denotes absolute value, a and b are two constants and $a < b < 0$, α , β and γ are three constant parameters.

To synchronize the two chaotic systems, the impulsive interval $\Delta_i = \tau_i - \tau_{i-1}$ should be chosen appropriately. There are two types of methods. One with constant interval is provided by Yang *et al.* [6], while the other proposed by Li *et al.* [10] and Xie *et al.* [9] gives piecewise constant intervals defined as follows:

$$\Delta_1 = \tau_1 - \tau_0 = \tau_3 - \tau_2 = \dots = \tau_{2i+1} - \tau_{2i} = \dots \quad (3.22)$$

$$\Delta_2 = \tau_2 - \tau_1 = \tau_4 - \tau_3 = \dots = \tau_{2i+2} - \tau_{2i+1} = \dots \quad (3.23)$$

$$\Delta_2 = \varepsilon \Delta_1; 0 < \varepsilon < 1 \quad (3.24)$$

Such a choice of the piecewise constant intervals is currently the best choice and we will also adopt it for comparison with existing schemes in this thesis.

3.3.2 Choice of Impulsive Intervals

It is important to have a larger bound for impulsive intervals because less bandwidth is required for the transmission of synchronization impulses and hence the bandwidth efficiency is enhanced. In this section, linear matrix inequalities are used to study the impulsive synchronization of chaotic systems [53]. Some less conservative conditions are derived utilizing the fact that the linear part of the chaotic system is a stable subsystem. Compared with previous schemes in [6,10,15], a larger bound of impulsive intervals is allowed. We present the new synchronization conditions in the following theorem.

Theorem 3.3. The error system given by (3.15), is asymptotically stable if

$$0 \leq a_{\min} \leq -\frac{2}{(1+\varepsilon)\Delta_1} \ln(\xi d_1), \xi > 1 \quad (3.25)$$

where $a_{\min}$ denotes the solution of the following optimization problem

$$\min_p \{a\} \text{ such that } (A+H)^T P + P(A+H) < aP \quad (3.26)$$

and d_1 satisfies

$$(I+B)^T P(I+B) < d_1 P \text{ and } \xi d_1 < 1 \quad (3.27)$$

where matrix $P = P^T > 0$ is symmetric positive definite.

(i) For Chua's oscillator,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_1 & p_2 \\ 0 & p_2 & p_3 \end{bmatrix} \quad (3.28)$$

(ii) For Lorenz system,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_1 & 0 \\ 0 & 0 & p_1 \end{bmatrix}; p_1 \leq 1 \quad (3.29)$$

Proof: Choose the Lyapunov function as $V(e) = e^T P e$. It can be shown that when

$t \neq \tau_i$, we have

$$2e^T P \phi(X, X') \leq e^T (PH + H^T P)e \quad (3.30)$$

It follows from (3.15) that

$$\begin{aligned} \dot{V}(e) &= e^T (A^T P + PA)e + \phi^T(X, X')Pe + e^T P \phi(X, X') \\ &= e^T (A^T P + PA)e + 2e^T P \phi(X, X') \\ &\leq e^T (A^T P + PA)e + e^T (PH + H^T P)e \\ &= e^T ((A + H)^T P + P(A + H))e \\ &\leq a_{\min} V(e) \end{aligned} \quad (3.31)$$

When $t = \tau_i$, we have

$$V(e(\tau_i)) = e^T (I + B)^T P(I + B)e \leq d_1 V(e(\tau_i)) \quad (3.32)$$

Based on Theorem 3.1, the following comparison system can be obtained for (3.31) and (3.32):

$$\begin{cases} \dot{\omega}(t) = a_{\min} \omega(t), & t \neq \tau_i \\ \omega(\tau_i^+) = d_1 \omega(\tau_i), & t = \tau_i \\ \omega(t_0^+) = \omega_0 \geq 0 \end{cases} \quad (3.33)$$

It follows from (3.31)-(3.33) that

$$\begin{aligned} a_{\min}(\tau_{2i+1} - \tau_{2i-1}) &= a_{\min}(\tau_{2i+1} - \tau_{2i} + \tau_{2i} - \tau_{2i-1}) \\ &\leq a_{\min}(\Delta_1 + \Delta_2) \\ &\leq a_{\min}(1 + \varepsilon)\Delta_1 \\ &\leq -2\ln(\xi d_1) \end{aligned} \quad (3.34)$$

Clearly, from Theorem 3.2, the error system given by (3.15) is asymptotically stable.

□□□

3.3.3 Effectiveness Studies

Refer to the packet composition illustration in Figure 2.14; we define some factors to evaluate the effectiveness of the proposed scheme.

Define the bandwidth efficiency for each time frame as

$$TE(n) = 1 - \frac{Q}{\Delta_i} \quad (3.35)$$

where Q is the length of synchronization impulse and Δ_i is the length of the i^{th} impulsive interval. The bandwidth efficiency for the scrambled signal is illustrated in Figure 2.14. $\frac{Q}{\Delta_i}$ stands for the bandwidth taken by the synchronization impulse. $1 - \frac{Q}{\Delta_i}$ stands for the bandwidth for the scrambled signal.

Define the average effectiveness factor of n time frame as:

$$ATE(n) = 1 - \frac{nQ}{\sum_{i=1}^n \Delta_i} \quad (3.36)$$

and the bandwidth efficiency of a scheme can be defined as

$$STE = \lim_{n \rightarrow \infty} ATE(n) \quad (3.37)$$

We now compare our new scheme with the previous schemes in [6] and [10] via Chua's circuit. The maximum effectiveness of each scheme is calculated as given below:

- For scheme in [6] $STE_{1\max} = 1 - \frac{Q(q+2|\alpha a|)}{\ln(\xi d_1)}$ as $\xi \rightarrow 1^+$ (3.38)

- For scheme in [10] $STE_{2\max} = 1 - \frac{Q(q+2|\alpha a|)}{\ln(\xi d_1)}$ as $\xi \rightarrow 1^+$ (3.39)

- For our new scheme $STE_{3\max} = 1 - \frac{Qa_{\min}}{\ln(\xi d_1)}$ as $\xi \rightarrow 1^+$ (3.40)

Clearly we can see that our new scheme's effectiveness is much better than the previous ones.

Remark 3.1. Based on the stability of subsystem governed by $\begin{bmatrix} -1 & 0 \\ 0 & -b \end{bmatrix}$ of Lorenz system and the stability of subsystem governed by $\begin{bmatrix} -1 & -1 \\ -\beta & -\gamma \end{bmatrix}$ of Chua's oscillator, the matrix P is chosen as in (3.28) and (3.29) respectively. Such choices of P make the result in Theorem 3.3, especially (3.30) available.

Remark 3.2. Based on (3.25), the impulse interval bound by using the new scheme can be computed as

$$\Delta_{\max}(\xi) = -\frac{2 \ln(\xi d_1)}{(1 + \varepsilon) a_{\min}} \quad (3.41)$$

The impulsive interval bound by using Li *et al.* [10] is computed as

$$\Delta_{\max} = \frac{-2 \ln(\xi d_1)}{(1 + \varepsilon)(q + 2|a\alpha|)} \quad (3.42)$$

As $a_{\min} < q + 2|a\alpha|$, so the impulsive interval bound with the new scheme is larger than the one in [10]. Therefore it can be concluded that the bandwidth efficiency is improved. As shown in Figure 2.14, the synchronization impulse occupies the beginning Q seconds of each time frame. We assume that the transmission rate of the

channel is fixed at m bits/s. The synchronization impulse occupies Qm bits and the whole region can allow $\Delta_{\max} m$ bits to be transferred for each time frame. The bandwidth efficiency is defined as the ratio of the bits occupied by signal to the bits transferred in the whole region for each time frame. The bandwidth efficiency improvement for the proposed scheme in comparison with the one in [10] is calculated as

$$\frac{\Delta_{\max}(\xi)m - Qm}{\Delta_{\max}(\xi)m} - \frac{\Delta_{\max}m - Qm}{\Delta_{\max}m} = \frac{Q}{\Delta_{\max}} - \frac{Q}{\Delta_{\max}(\xi)} = \frac{Q(1+\varepsilon)(a_{\min} - q - 2|a\alpha|)}{2\ln(\xi d_1)}.$$

Remark 3.3 Note that the design of the controller in [15] is done by solving a nonlinear optimization problem which involves a matrix inequality. The matrix inequalities are solved by using sequential quadratic programming which is a nonlinear optimization method. However, linear matrix inequalities used in this chapter result in a linear optimization approach. In our approach, we use the structure information of the nonlinear systems to get (3.18) for Lorenz systems and (3.21) for Chua's circuit. This gives us a linear bound for the nonlinear component $\phi(X, X')$ of the system in term of H as specified in (3.14). Thus we are able to convert the nonlinear optimization problem to linear optimization problem which can be solved by LMIs.

Remark 3.4 Also note that in [15], the difference between the states of the master system and the slave system is used as input to the controller in the slave system, which requires the states of the master system to be transmitted through the channel to the

receiver all the time. But in this chapter, the states of the driving system only are transmitted at impulse instants to the driven system. Thus our method is much simpler and more secure than that in [15].

Note that for any given a , inequality (3.26) can be easily solved by the method of linear matrix inequalities [53]. An algorithm, as illustrated in Figure 3.1, is set up to compute $a_{\min}$ as follows:

Step 1: Initialize the computation by setting $L = 0$, $U = \lambda_{\max}((A + H) + (A + H)^T)$,

$a_0 = \frac{L+U}{2}$, $i = 0$ and choosing a small positive number η as the tolerance of the

difference between the values of a_i computed at two successive iterations.

Step 2: Check if there is a positive definite matrix P satisfies the inequality (3.26). If the inequality (3.26) is valid, $U = a_i$; otherwise, $L = a_i$.

Step 3: Let $i = i + 1$, and $a_i = \frac{L+U}{2}$

Step 4: If $|a_i - a_{i-1}| < \eta$. Go to Step 5; otherwise, go to Step 2.

Step 5: Terminate the program and output the smallest value of a_i .

Figure 3.1: Flowchart for the computation of $a_{\min}$

3.3.4 Numerical Examples

In this section, we use two numerical examples to make comparison between the scheme in [9,10] and the proposed scheme.

Example 3.1 Consider the Lorenz systems with the following parameters and the initial conditions: $\delta = 16$, $r = 45.6$, $b = 4$, $X(0) = [-27, 15, 12]^T$ and $X'(0) = [25, 40, 5]^T$.

Matrix B is chosen as $\begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix}$.

Then from (3.26), and using the algorithm in Figure 3.1,

$$a_{\min} = 152.186, P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.3509 & 0 \\ 0 & 0 & 0.3509 \end{bmatrix}, \text{ also from (3.27),}$$

$$d_1 > \lambda_{\max}((I+B)^T P(I+B)P^{-1}) = 0.09.$$

Further choose $\xi = 1.1$ and $\varepsilon = \frac{2}{3}$. From (3.35), the upper bounds of the impulsive

intervals are calculated by

$$\Delta_1 = \frac{-2 \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 1.823 \times 10^{-2}, \Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 1.215 \times 10^{-2}$$

With the same parameters, it is noted that with the method used in [9]

$$\Delta_1 = \frac{-2 \ln(\xi d)}{(1+\varepsilon)(q+2M)} = 1.344 \times 10^{-2}, \Delta_2 = \frac{-2\varepsilon \ln(\xi d)}{(1+\varepsilon)(q+2M)} = 0.896 \times 10^{-2}$$

where q is the largest eigenvalue of $(A+A^T)$ and $d > \lambda_{\max}((I+B)(I+B)^T)$.

Example 3.2. Consider Chua's system with the following parameters and initial conditions:

$$\alpha = 10, \beta = 16, \gamma = 0.0385, a = -\frac{8}{7}, b = -\frac{5}{7}, X(0) = [-17, 26, 18]^T \text{ and } X'(0) = [25, 36, 5]^T.$$

$$\text{Matrix } B \text{ is chosen as } \begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix}.$$

Similarly we have that $a_{\min} = 6.0279$,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12.4058 & 1.8355 \\ 0 & 1.8355 & 0.7754 \end{bmatrix}, d_1 > \lambda_{\max}((I+B)^T P(I+B)P^{-1}) = 0.099.$$

Again consider $\xi = 1.1$ and $\varepsilon = \frac{2}{3}$. The upper bounds of the impulsive intervals are calculated as follows.

$$\Delta_1 = \frac{-2 \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 0.4414$$

$$\Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 0.2943$$

With the same parameters, the upper bound with the method used in [10] is

$$\Delta_1 = \frac{-2 \ln(\xi d)}{(1+\varepsilon)(q+2|a\alpha|)} = 7.202 \times 10^{-2}$$

$$\Delta_2 = \frac{-2\varepsilon \ln(\xi d)}{(1+\varepsilon)(q+2M)} = 4.801 \times 10^{-2}$$

Note that $d > \lambda_{\max}((I+B)(I+B)^T) = 0.09$ and q is the largest eigenvalue of $(A+A^T)$.

It is shown by the above two examples that with our new result, the upper bounds of impulsive intervals are increased by 35.64% for Lorenz system and 512.89% for the Chua's system. Thus, it can be concluded that the bandwidth efficiency can be improved remarkably by the proposed scheme.

In the end of this section, we shall compare the stable region of our scheme with that of [10].

Choose impulsive control matrix $B = \begin{bmatrix} k & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$, and Chua's oscillator's

parameters as those in Example 3.2.

It is easy to show that $d_1 = (k+1)^2$. With $\varepsilon = \frac{2}{3}$, $q = 15.6753$, $q + 2|a\alpha| = 38.5324$, $a_{\min} = 6.0279$, an estimated boundary of the stable regions are given as follows:

- For the scheme in [10]

$$\Delta_{\max}(\xi) = -\frac{2 \ln(\xi(k+1)^2)}{(1+\varepsilon)(q+2|a\alpha|)} \quad (3.43)$$

- For the new scheme

$$\Delta_{\max}(\xi) = -\frac{2\ln(\xi(k+1)^2)}{(1+\varepsilon)a_{\min}} \quad (3.44)$$

Based on (3.43) and (3.44), we plot the above two functions for different ξ in Figure 3.2 and Figure 3.3 respectively. For each given ξ the region below the corresponding curve is stable. It is obvious to see that under our new scheme, the impulsive interval could be much larger for all values of ξ than the scheme in [10]. This means that the synchronization impulse can be transmitted less frequently, which results in better bandwidth efficiency.

Figure 3.2: Stable region of the scheme in [10]

Figure 3.3: Stable region of the proposed scheme

3.4 Concluding Remark

In this chapter, structure knowledge of chaotic systems and linear matrix inequalities has been employed to derive some less conservative conditions for the synchronization of chaotic systems. With the proposed conditions, a larger bound of impulsive interval is obtained, resulting in higher bandwidth efficiency. The results are thus very helpful to improve the existing technologies on chaotic secure communications and chaotic spread communications.

Chapter 4

Time Varying Sampling Scheme with an Application to Chaotic Crypto- systems

4.1 Introduction

In this chapter, we introduce a new type of sampling scheme where the sampling period can be time varying so as to produce a flatter sampled power spectrum. The time varying sampling scheme is then applied to study chaotic cryptosystems. Compared to a scheme with a fixed sampling frequency, it reduces the synchronization

time between two chaotic systems in an encrypter and a decrypter while maintaining the security of chaotic cryptosystems. Thus, a good trade-off between the bandwidth utilization and the security of chaotic cryptosystem can be obtained by our scheme.

The sampling theorem has been well known in signals and systems [54]. It provides a condition under which a band-limited continuous-time signal can be completely represented by and reconstructed from its discrete time samples. Specifically, if the spectrum $\hat{X}(\omega)$ of a continuous time signal $X(t)$ is band limited such that $\hat{X}(\omega) = 0$ for all frequencies $|\omega| > \omega_M$ with some $\omega_M > 0$, $X(t)$ is then uniquely determined by its sampled values $x_s(lT_s)$ ($l = 0, \pm 1, \pm 2, \dots$), if the sampling frequency $\omega_s = 2\pi/T_s$ satisfies $\omega_s > 2\omega_M$, where T_s is the sampling period. If $\omega_s < 2\omega_M$, there is an overlap between the shifted replicas of $\hat{X}(\omega)$ which is no longer replicated in the spectrum of the sampled $\hat{X}_s(\omega) = \frac{1}{T_s} \sum_{k=-\infty}^{+\infty} \hat{X}(\omega - k\omega_s)$. In the case that the signal is considerably under-sampled, the contiguous shifted replicas of $\hat{X}(\omega)$ overlap, which can yield a roughly “flat” spectrum of $\hat{X}(\omega)$. This phenomenon is known as frequency aliasing [54].

Frequency aliasing can be exploited to enhance the security of chaotic cryptosystems [23,55]. The chaotic cryptosystems have received a great deal of attention since Pecora & Carroll proposed a method to synchronize two identical chaotic systems [56-60]. It has been claimed that a chaotic carrier offers possibly several advantages over classical

carrier signal like frequency spreading and security can be offered at no extra cost. It is also very competitive when compared with standard communication techniques due to inexpensive implementations [16,61,62]. The major problem with these systems is that they are vulnerable under the proposed attacks in [48,50,63-67]. To improve this, the sampling frequency of chaotic signals should be below its bandwidth such that the running key sequence has a high degree of randomness [23]. The sampling frequency is fixed and always below its bandwidth in [23]. Although the security is improved, the bandwidth utilization is a little low. Normally, bandwidth utilization and security contradict with each other. It is desirable to design a new sampling scheme to obtain a good trade-off between them [55].

In this chapter, we introduce a time-varying frequency sampling scheme where the sampling frequency is sometimes below $2\omega_M$ and sometimes above $2\omega_M$ with its average sampling frequency above $2\omega_M$. With our scheme, the original time varying signal cannot be completely represented by and reconstructed from its discrete time samples even though the average sampling frequency is greater than $2\omega_M$. That is, it is possible to produce frequency aliasing in our time varying sampling scheme when the average sampling frequency is greater than $2\omega_M$. The scheme is then applied to study chaotic cryptosystems. Same as the scheme in [23], the original signal cannot be reconstructed, and thus the security can be ensured. Meanwhile, the synchronization time can be reduced when compared to a sampling scheme with a fixed frequency in

[23], and thus bandwidth utilization is also efficient. Our scheme can be therefore used to obtain a good trade-off between security and bandwidth utilization.

4.2 A Time Varying Sampling Scheme

In this section, we shall first introduce our time varying sampling scheme such that the original signal $X(t)$ cannot be completely represented by and reconstructed from its discrete time samples even though the average sampling frequency is greater than $2\omega_M$.

We assume that N_1 and N_2 are two positive integers that are chosen by the user and N_1 is greater than N_2 . Choose a constant γ based on the following condition:

$$\frac{2(N_1 + N_2)}{N_1} < \gamma < 2(N_2 + 1) \quad (4.1)$$

The initial sampling frequency is set as

$$\omega_s = \gamma\omega_M \quad (4.2)$$

Let

$$T_s = \frac{2\pi}{\omega_s} \quad (4.3)$$

The sampling function is

$$p_1(t) = \sum_{i=-\infty}^{+\infty} \delta(t - iT_s) \quad (4.4)$$

The sampled sequence is obtained by multiplying the original signal with the sampling pulse train as follows:

$$X_s(i) = X(t)p_1(t)\big|_{t=iT_s} \quad (4.5)$$

The sampled values $X_s(i)$ are further filtered as

$$Y_s(N_1l) = X_s((N_1 + N_2)l) \quad (4.6)$$

$$Y_s(N_1l + 1) = X_s((N_1 + N_2)l + 1) \quad (4.7)$$

•
•
•

$$Y_s(N_1l + N_1 - 1) = X_s((N_1 + N_2)l + N_1 - 1) \quad (4.8)$$

where Y_s is the final sampled value. In other words, the overall sampling function is given by

$$\begin{aligned} p_2(t) &= \sum_{i=-\infty}^{+\infty} [\delta(t - (N_1 + N_2)iT_s) + \delta(t - ((N_1 + N_2)i + 1)T_s) \\ &\quad + \dots + \delta(t - ((N_1 + N_2)i + N_1 - 1)T_s)] \\ &= \sum_{i=-\infty}^{+\infty} \sum_{l=0}^{N_1-1} \delta(t - ((N_1 + N_2)i + l)T_s) \end{aligned} \quad (4.9)$$

and the final sampled sequence is

$$Y_s(i) = X(t)p_2(t)\big|_{t=iT_s} \quad (4.10)$$

The average sampling frequency is computed as

$$\tilde{\omega}_s = \frac{N_1}{N_1 + N_2} \omega_s > 2\omega_M \quad (4.11)$$

However, the sampling frequency between $Y_s(N_1l + N_1 - 1)$ and $Y_s((N_1 + 1)l)$ is

$$\tilde{\omega}_s = \frac{\omega_s}{N_2 + 1} < 2\omega_M \quad (4.12)$$

In other words, there is frequency aliasing between $Y_s(N_1 l + N_1 - 1)$ and $Y_s((N_1 + 1)l)$.

Thus, the signal cannot be completely represented by and reconstructed from Y_s .

Theorem 4.1. The spectrum relationship between $Y_s(l)$ and $X_s(l)$ is described by

$$Y_s(e^{j\omega}) = \frac{1}{N_1 + N_2} \sum_{k=0}^{N_1+N_2-1} \left[\sum_{i=0}^{N_1-1} e^{\frac{-2ik\pi j}{N_1+N_2}} \right] X_s(e^{(\omega - \frac{2k\pi}{N_1+N_2})j}) \quad (4.13)$$

Proof. Note that the relationship between Y_s and X_s is represented by

$$\begin{aligned} Y_s(l) &= \frac{1}{N_1 + N_2} \sum_{i=0}^{N_1-1} \sum_{k=0}^{N_1+N_2-1} e^{\frac{2(l-i)k\pi j}{N_1+N_2}} X_s(l) \\ &= \frac{1}{N_1 + N_2} \sum_{k=0}^{N_1+N_2-1} \left[\sum_{i=0}^{N_1-1} e^{\frac{-2ik\pi j}{N_1+N_2}} \right] e^{\frac{2lk\pi j}{N_1+N_2}} X_s(l) \end{aligned}$$

Taking z-transforms on both sides gives

$$Y_s(z) = \frac{1}{N_1 + N_2} \sum_{k=0}^{N_1+N_2-1} \left[\sum_{i=0}^{N_1-1} e^{\frac{-2ik\pi j}{N_1+N_2}} \right] X_s(ze^{-\frac{2k\pi j}{N_1+N_2}}) \quad (4.14)$$

Replacing z by $e^{j\omega}$, we can obtain the spectrum relationship as (4.13).

An interesting case is that $N_1 = 2$ and $N_2 = 1$. In this case, the sampling function is

$$p_2(t) = \sum_{i=-\infty}^{+\infty} [\delta(t - 3iT_s) + \delta(t - 3i + 1)T_s]$$

The relationship between Y_s and X_s , as illustrated in Figure 4.1, is described by

$$Y_s(2l) = X_s(3l) \quad (4.15)$$

$$Y_s(2l+1) = X_s(3l+1) \quad (4.16)$$

Figure 4.1: An example of our time varying sampling scheme with $N_1 = 2$ and $N_2 = 1$.

The average sampling frequency is computed to be

$$\tilde{\omega}_s = \frac{2}{3} \omega_s > 2\omega_M \quad (4.17)$$

The resulting sampled signal will not be exactly equal to $X(t)$. This is because there is frequency aliasing between $Y_s(2l+1)$ and $Y_s(2l+2)$ ($l = 0, 1, 2, \dots$).

From Theorem 4.1, we obtain

Corollary 4.1. *Let $N_1 = 2$ and $N_2 = 1$. The spectrum relationship between $Y_s(l)$ and $X_s(l)$ is described by*

$$Y_s(e^{j\omega}) = \frac{2}{3} X_s(e^{j\omega}) + \frac{e^{\frac{\pi}{3}j}}{3} X_s(e^{(\omega + \frac{2\pi}{3})j}) + \frac{e^{-\frac{\pi}{3}j}}{3} X_s(e^{(\omega - \frac{2\pi}{3})j}) \quad (4.18)$$

The power spectral density of $Y_s(l)$ is

$$\begin{aligned}
 P(e^{j\omega}) &= \frac{1}{N} |Y_s(e^{j\omega})|^2 = \frac{1}{N} \left| \frac{2}{3} X_s(e^{j\omega}) + \frac{e^{\frac{\pi}{3}j}}{3} X_s(e^{(\omega+\frac{2\pi}{3})j}) + \frac{e^{-\frac{\pi}{3}j}}{3} X_s(e^{(\omega-\frac{2\pi}{3})j}) \right|^2 \\
 &= \frac{4}{9N} \left| X_s(e^{j\omega}) + \frac{e^{\frac{\pi}{3}j}}{2} X_s(e^{(\omega+\frac{2\pi}{3})j}) + \frac{e^{-\frac{\pi}{3}j}}{2} X_s(e^{(\omega-\frac{2\pi}{3})j}) \right|^2
 \end{aligned}$$

4.3 Application to Chaotic Cryptosystems

In this section, we apply our time varying sampling scheme to chaotic cryptosystems with a block diagram shown in Fig 2.13 in Chapter 2. A good trade-off between the bandwidth utilization and the security can be achieved. The details of the chaotic systems at the encrypter and decrypter are described below.

The chaotic system at the encrypter side is called the driving system and it can be represented by

$$\dot{X}(t) = AX(t) + \psi(X(t)) \quad (4.19)$$

where $X \in R^r$ is a state vector, A is an $r \times r$ constant matrix, and $\psi : R^r \rightarrow R^r$ is a nonlinear function that gives rise to chaotic dynamics, and it satisfies

$$2X^T(t)\psi(X(t)) \leq X^T(t)(H + H^T)X(t) \quad (4.20)$$

where H is a matrix that is known in advance.

The chaotic system at the decrypter side is called the driven system and is described by

$$\begin{cases} \dot{\tilde{X}} = A\tilde{X} + \psi(\tilde{X}); & t \neq t_k \\ \Delta\tilde{X} = -Be; & t = t_k, k = 1, 2, \dots \end{cases} \quad (4.21)$$

where $\tilde{X} = (\tilde{x}, \tilde{y}, \tilde{z})^T$ is the state variables of the driven system,

$e^T = (e_x, e_y, e_z) = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})$ is the synchronization error, B is an $r \times r$ constant

matrix, the discrete instant $t_k (k = 1, 2, \dots)$ are time varying and satisfy

$$t_{2k+1} - t_{2k} = \frac{1}{2}(t_{2k} - t_{2k-1}) \quad (4.22)$$

Denote

$$\Delta_1 = \sup \{t_{2k} - t_{2k-1}\} < \infty \quad (4.23)$$

$$\Delta_2 = \sup \{t_{2k+1} - t_{2k}\} < \infty \quad (4.24)$$

and

$$\Psi(X, \tilde{X}) = \psi(X) - \psi(\tilde{X}) \quad (4.25)$$

Clearly, $\Delta_1 = 2\Delta_2$. It should be noted that that (4.22) is designed such that $N_1 = 2$ and $N_2 = 1$ so that it yields a spectrum as presented in Theorem 4.1. The relationship between sampled sequence and impulsive instant is illustrated in Figure 4.2.

Figure 4.2: The relationship between sampled sequence and impulsive instant

The error system of the impulsive synchronization is then given by

$$\begin{cases} \dot{e} = Ae + \Psi(X, \tilde{X}); & t \neq t_k \\ \Delta e = Be; & t = t_k, k = 1, 2, \dots \end{cases} \quad (4.26)$$

As in Chapter 5 of [55], we can show that the impulsive synchronization of two chaotic systems, with the error system given by (4.26), is asymptotically stable if

$$0 \leq \chi(A, H) \leq -\frac{2}{1.5\Delta_1} \ln\left(\frac{d_1}{L}\right) \quad (4.27)$$

where $0 < L < 1$ and $d_1 = \rho^2(I + B) < 1$, $d_1 < L$, and

$$\chi(A, H) = \lambda_{\max}(A + H + (A + H)^T) \quad (4.28)$$

We shall now show that our time varying sampling scheme can be used to obtain a good tradeoff between the synchronization time and the security.

For any $0 < L < 1$ satisfying $d_1 < L$, which is required by [5], we choose that

$$\Delta_1 = -\frac{2 \ln(\frac{d_1}{L})}{1.5 \chi(A, H)} \quad (4.29)$$

It can be shown that (4.27) holds. Thus, the origin of the error system (4.26) is asymptotically stable. We have the following two observations from (4.29):

1. With a smaller L , less time is required to synchronize the two chaotic systems while the bound of the impulsive intervals after two systems are synchronized is smaller.
2. With a larger L , more time is required to synchronize the two chaotic systems while the bound of impulsive intervals after the two systems are synchronized is larger.

Better still, the advantage of the two choices can be combined to design a two-stage impulsive control strategy as follows:

Stage 1 The constant L is chosen as L_1 which is as small as possible under the condition $L_1 > 0$. For example, L_1 can be selected as 0.0001. The impulsive intervals for synchronization can be chosen as $t_{2k} - t_{2k-1} = \min\{2T_s, \Delta_2(L_1)\}$ and $t_{2k+1} - t_{2k} = \min\{T_s, \frac{\Delta_2(L_1)}{2}\}$, where T_s is given in (4.3).

Stage 2 In this stage, the constant L is selected to be L_2 which is as large as possible under the condition $L_2 < 1$. For example, L_2 can be chosen as 0.99999. The

impulsive interval can then be chosen as $t_{2k} - t_{2k-1} = 2 \min\{T_s, \Delta_2(L_2)\}$ and $t_{2k+1} - t_{2k} = \min\{T_s, \Delta_2(L_2)\}$, respectively.

To maintain the synchronization of the chaotic systems after the impulsive intervals are increased, it is required to properly define the time instant at which the system is to switch from stage 1 to stage 2. Similar to the results in [9], we have

Lemma 4.1. For any $\eta > 0$ as the specified tolerance error, define an $n_{0q}(\eta)$ as

$$n_{0q}(\eta) = \log_{\tilde{L}} \frac{\|e_0\|}{\tilde{L}\omega} \left(\eta - \frac{\tilde{L}\omega}{\tilde{L}-1} \right) \quad (4.30)$$

where e_0 is the initial error vector, q is the quantization parameter, and

$$\tilde{L} = \frac{1}{L_1} e^{\frac{3}{2}\chi(A,H)(\Delta_2(L_1) - \min\{T_s, \frac{\Delta_2(L_1)}{2}\})}$$

$$\omega = d_1^{\frac{1}{2}} c_1 \left(e^{\chi(A,H) \frac{3 \min\{T_s, \frac{\Delta_2(L_1)}{2}\}}{2}} + e^{\chi(A,H) \min\{T_s, \frac{\Delta_2(L_1)}{2}\}} \right)$$

$$c_1 = \frac{\|B\|}{2} + q^{-\frac{1}{2}} (\|B\| d_1^{\frac{1}{2}} \sup \|e(t_k^-)\|)^{\frac{1}{2}}$$

If $k \geq n_{0q}(\eta)$, then $\|e(t_{2k}, t_0, e_0)\| < \eta$.

Proof. Define a Lyapunov function for the error system (4.26) as

$$V(e) = \sqrt{e^T e} = \|e\| \quad (4.31)$$

We have

$$\dot{V}(e) \leq \frac{1}{2} \chi(A, H) V(e); \quad t \neq t_k \quad (4.32)$$

$$V(e(\tau_i)) \leq d_1^{1/2} V(e(t_k^-)) + c_1 q \quad (4.33)$$

It follows that

$$V(e(\tau_{2n}, t_0, e_0)) \leq d_1 e^{\chi(A, H) \frac{3 \min\{T_s, \frac{\Delta_2(L_1)}{2}\}}{2}} + \omega q \quad (4.34)$$

It can be shown from (4.27) that

$$d_1 \leq \frac{L_1}{e^{1.5 \chi(A, H) \Delta_2(L_1)}} \quad (4.35)$$

Thus,

$$d_1 e^{\chi(A, H) \frac{3 \min\{T_s, \frac{\Delta_2(L_1)}{2}\}}{2}} \leq \frac{1}{\tilde{L}} \quad (4.36)$$

We then obtain

$$V(e(\tau_{2k}, t_0, e_0)) \leq \frac{V(e_0)}{\tilde{L}^k} + \frac{\tilde{L} \omega}{\tilde{L} - 1} q \quad (4.37)$$

Clearly, when $k \geq n_{0q}(\eta)$, we have $\|e(t_{2k}, t_0, e_0)\| < \eta$. □

For any $\eta > 0$, we denote

$$\tilde{\eta} = \min\left\{(\eta - \tilde{\omega} q) \frac{1}{L_2}, \left(\frac{\eta}{e^{2 \chi(A, H) \min\{T_s, \Delta_2(L_1)\}}} - c_1 q\right) d_1^{-1/2}\right\}$$

$$\omega = d_1^{\frac{1}{2}} c_1 (e^{\chi(A, H) \frac{3 \min\{T_s, \Delta_2(L_1)\}}{2}} + e^{\chi(A, H) \min\{T_s, \Delta_2(L_1)\}})$$

Then we have

Theorem 4.2. When $\tilde{k} \geq n_{0q}(\tilde{\eta})$, $\|X\| - \|\tilde{X}\| < \eta$.

Proof. From Lemma 4.1, we know that when $\tilde{k} \geq n_{0q}(\tilde{\eta})$, we have $\|e(t_{2\tilde{k}}, t_0, e_0)\| < \tilde{\eta}$

We consider the following two cases:

Case 1 For any $t_{2\tilde{k}} < t < t_{2\tilde{k}+1}$, we have

$$\begin{aligned} V(e(t, t_0, e_0)) &\leq V(e(t_{2\tilde{k}}^+, t_0, e_0)) e^{\frac{\chi(A, H)}{2}(t-t_{2\tilde{k}})} \\ &\leq (d_1^{1/2} V(e(t_{2\tilde{k}}^-, t_0, e_0)) + c_1 q) e^{\frac{\chi(A, H)}{2}(t-t_{2\tilde{k}})} \\ &\leq (d_1^{1/2} V(e(t_{2\tilde{k}}^-, t_0, e_0)) + c_1 q) e^{\chi(A, H)\Delta_2(L_2)} \\ &< \eta \end{aligned}$$

Case 2 For any $t_{2\tilde{k}+1} < t < t_{2\tilde{k}+2}$, we obtain

$$\begin{aligned} V(e(t, t_0, e_0)) &\leq V(e(t_{2\tilde{k}+2}, t_0, e_0)) \\ &\leq L_2 V(e(t_{2\tilde{k}}, t_0, e_0)) + \tilde{\omega} q \\ &< \eta \end{aligned}$$

Note that $\|X\| - \|\tilde{X}\| \leq V(e(t, t_0, e_0))$.

Therefore, when $k \geq n_{0q}(\tilde{\eta})$, we have $\|X\| - \|\tilde{X}\| \leq \eta$. $\square$

With the above theorem, the estimate of the required synchronization time is given by

$$T_{syn} = 3n_{0q} \min\{T_s, \Delta_2(L_1)\} \quad (4.38)$$

Thus, the synchronization time is reduced by choosing a smaller T_s . However, T_s cannot be too small to maintain the security of the system at the first stage. Thus, T_s should be properly selected such that a good trade-off between synchronization time and security can be achieved.

Note that a sampling scheme with a fixed frequency was adopted in [23]. To maintain the security, the sampling frequency is below the bandwidth, i.e. $\hat{\omega}_s < 2\omega_M$. However, with our time varying sampling scheme, the average sampling frequency $\tilde{\omega}_s$ is greater than $2\omega_M$. This implies that $\tilde{\omega}_s > \hat{\omega}_s$. Thus, $\frac{2\pi}{\tilde{\omega}_s} > \frac{2\pi}{\hat{\omega}_s}$. That is, a smaller T_s can be selected by using our time varying sampling scheme. Therefore, the synchronization time is reduced.

Meanwhile, the state variables of the chaotic system are used to produce the running-key sequences. It is desired to improve the randomness in the running-key sequences as in [23]. Note that in [23] the sampling frequency of chaotic signals is below its bandwidth. While it will produce frequency aliasing and the running-key sequences will have a high degree of randomness for secure encryption, bandwidth utilization is a little low in [23].

Overall, our time varying sampling scheme can be used to obtain a good trade-off between bandwidth utilization and security.

4.4 Simulation Results

In this section, we shall test our time varying sampling schemes in two third-order chaotic systems: the Lorenz system and the Chua's circuits [40]. They have been widely studied in the chaotic cryptosystems.

Example 4.1 The matrices A , $\psi(X)$, and H of the Chua's circuits are

$$A = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix}, \quad (4.39)$$

$$\psi(X) = [-\alpha f(x) \quad 0 \quad 0]^T, \quad (4.40)$$

$$H = \begin{bmatrix} |\alpha a| & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \quad (4.41)$$

where $\alpha, \beta, \gamma, \mathcal{G}_1$ and $\mathcal{G}_2$ are five constants and $f(x) = \mathcal{G}_2 x + \frac{1}{2}(\mathcal{G}_1 - \mathcal{G}_2)(|x+1| - |x-1|)$.

Consider the Chua's circuit with the following parameters and initial conditions: $\alpha = 10$,

$\beta = 16$, $\gamma = 0.0385$, $\mathcal{G}_1 = -\frac{8}{7}$, $\mathcal{G}_2 = -\frac{5}{7}$, $X(0) = [-0.2, -0.02, 0.1]^T$. A fourth order

Runge-Kutta method with step size 10^{-4} is used. We consider four fixed sampling periods and they are chosen as $0.02 t_u$, $0.04 t_u$, $0.06 t_u$, and $0.08 t_u$, respectively, where t_u is the simulation time unit. The time varying sampling periods are switched between $0.03 t_u$ and $0.06 t_u$. The time varying sampled values are generated by the following two steps:

Step 1 Generate the initial sampled sequence by $0.03 t_u$ and denote them by

$$X_s(l) \quad (1 \leq l \leq +\infty).$$

Step 2 Sample them to generate the desired values by (4.15)-(4.16).

The experimental results are illustrated in Figure 4.3. Clearly, the sampled signal with the time varying sampling frequency is flatter than the time invariant sampling with sampling periods $0.02t_u$ and $0.04t_u$. □

Figure 4.3: Frequency spectra of X_s with fixed sampling frequency and time varying sampling frequency for Chua's circuit

Example 4.2 The matrices A , $\psi(X)$, and H of the Lorenz system are

$$A = \begin{bmatrix} -\delta & \delta & 0 \\ \vartheta_3 & -1 & 0 \\ 0 & 0 & -\vartheta_4 \end{bmatrix}, \quad (4.42)$$

$$\psi(X) = \begin{bmatrix} 0 & -xz & xy \end{bmatrix}^T, \quad (4.43)$$

$$H = \begin{bmatrix} 0 & J & J \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \quad (4.44)$$

where δ , $\mathcal{G}_3$, and $\mathcal{G}_4$ are three constants, J is the upper bound of both $|y(t)|$ and $|z(t)|$.

The parameters of the Lorenz system are $\delta = 10$, $\mathcal{G}_3 = 28$ and $\mathcal{G}_4 = \frac{8}{3}$. The initial state is $[-36, 30, 0.5]^T$. The continuous-time Lorenz system is numerically integrated by the fourth-order Runge-Kutta method with a fixed step size of 10^{-4} .

Similarly, four fixed sampling periods are studied and they are selected as $0.02 t_u$, $0.04 t_u$, $0.06 t_u$, and $0.08 t_u$, respectively. The time varying periods are switched between $0.03 t_u$ and $0.06 t_u$. The experimental results are illustrated in Figure 4.4.

It is clear that the time varying sampling scheme can be used to generate a much flatter chaotic signal than a fixed sampling scheme. □

Figure 4.4: Frequency spectra of X_s with fixed sampling frequency and time varying sampling frequency for Lorenz system

4.5 Randomness Analysis of Time Varying Sampling Scheme

In a chaos-based cryptosystem, the parameters of the chaos systems play a role as random seeds and the state variables of the system generated from the chaotic dynamics are the running-key sequences. Since the behavior of chaotic systems are sensitive to initial conditions as well as parameter variations, the parameter space of some chaotic

systems is large enough for the random key seeds. It is expected that the running-key sequence has a high degree of randomness to produce a high degree of security for the cryptosystem.

It has been known that the power spectrum of some continuous-time chaotic signals decays exponentially in the high frequency band [68]. By contrast, a white noise signal is known to have a “flat” power spectrum and an impulse function as its autocorrelation. Thus, in order to have a high degree of randomness, it is desirable that the running-key sequences should have a white-noise-liked power spectrum and autocorrelation.

With the time varying sampling scheme, the randomness of the running-key sequence is improved due to frequency aliasing. For evaluation of the randomness of the sampled signal, autocorrelation function is used. The autocorrelation of the continuous Lorenz signal X and its sampled signal Y_s with sampled period $0.04t_u$ and $0.08t_u$ according to (4.15)-(4.16) are computed with 5000 samples. The resultant autocorrelation functions of the continuous-time signal X and that of the sampled signal Y_s are shown in Figure 4.5 and Figure 4.6 respectively. It is shown that the autocorrelation of the sampled signal is more impulse like. This is due to aliasing in the frequency domain and it improves the degree of randomness of the sampled signal. Another example was using Chua’s circuit to for the comparison of the continuous Chua’s signal and its sampled signal with sampled period $0.04t_u$ and $0.08t_u$ according to (4.15)-(4.16). The resultant autocorrelation functions of the continuous-time signal X and that of the sampled

signal Y_s are shown in Figure 4.7 and Figure 4.8 respectively. It is clearly observed that the autocorrelation of the sampled signal is more impulse like than the one of the continuous signal.

Figure 4.5: Autocorrelation of the variable X of the Lorenz system

Figure 4.6: Autocorrelation of the sampled Y_s of the Lorenz system

Figure 4.7: Autocorrelation of the variable X of the Chua's circuit

Figure 4.8: Autocorrelation of the sampled Y_s of the Chua's circuit

4.6 Concluding Remark

A time varying sampling scheme is introduced in this chapter and applied to study chaotic cryptosystems. With this scheme, the chaotic sequence can get more randomness than original chaotic signal, thus the security is improved. Moreover, a good trade-off between the bandwidth utilization and the security of chaotic cryptosystem can be obtained by the proposed scheme.

Chapter 5

Synchronization of Chaotic Systems with Parametric Uncertainty and Mismatch

5.1 Introduction

In recent years, impulsive control has been proposed as a possible technique for chaos synchronization and impulsive synchronization has been applied to secure communication systems. The chaotic secure communication system has a driving chaotic system at the encypter and one driven chaotic system at the decrypter. Under

the condition that the parameters of both the driving chaotic system and the driven chaotic system are identical and time invariant, the states of the driven system can converge to those of the driving system. However, this condition is impractical as it is impossible for the parameters of the two chaotic systems to be identical and invariant all the time due to a number of reasons such as inaccurate implementation of the two systems and variation of parameters resulted from environment changes including fluctuation of ambient temperature and power supply as well as other external influences. Thus the usefulness of these synchronization schemes has been challenged by such impractical assumptions. Therefore, it is of both practical and theoretical importance to consider the synchronization issues in the presence of parametric uncertainties and mismatch between the two systems. To the knowledge of authors, there is still no existing result available dealing with parametric mismatch. In [69], only uncertainties of the two systems were taken into account in the design and analysis. But there is no parametric mismatch between the two systems as the uncertainties considered should be identical for both systems.

In this chapter, the parameters of the chaotic systems studied are uncertain, time varying and are not necessarily identical for the driving and driven chaotic systems. To achieve synchronization of the two chaotic systems, a controller is designed for the driven system. In the design, bounds on the parametric uncertainties and mismatch between the two systems are used. Sufficient conditions are derived to ensure synchronization of the two uncertain chaotic systems. The effectiveness and robustness

of the proposed schemes are also numerically verified by simulation studies. Our methods can be applied to a larger class of chaotic systems and is helpful to improve the existing technologies used in chaotic secure communication systems.

5.2 Problem Formulation

5.2.1 System Models

We first present the models of the two chaotic systems. The driving system in the presence of uncertainty is described by

$$\dot{X} = (A + \Delta A(t))X + \Delta \psi(X) + \psi(X) \quad (5.1)$$

where $X \in R^3$ is the state vector, $A \in R^{3 \times 3}$ is the nominal constant matrix and $\psi(X) = [\theta_1^T \phi_1(X), \theta_2^T \phi_2(X), \theta_3^T \phi_3(X)]^T$ is the nonlinear part of the chaotic system,

where

$$\Delta A(t) = \begin{bmatrix} \Delta A_1(t) & \Delta A_2(t) & \Delta A_3(t) \\ \Delta A_4(t) & \Delta A_5(t) & \Delta A_6(t) \\ \Delta A_7(t) & \Delta A_8(t) & \Delta A_9(t) \end{bmatrix}, \quad \theta_i^T = [\theta_{i1}, \theta_{i2}, \theta_{i3}] \quad , \quad \phi_i^T(X) = [\phi_{i1}(X), \phi_{i2}(X), \phi_{i3}(X)] \quad ,$$

$$\Delta \psi(X) = [\Delta \theta_1^T \phi_1(X), \Delta \theta_2^T \phi_2(X), \Delta \theta_3^T \phi_3(X)]^T \quad , \quad \Delta \theta_i^T = [\Delta \theta_{i1}, \Delta \theta_{i2}, \Delta \theta_{i3}] \quad , \quad i=1,2,3.$$

$\Delta A_i(t)$, $i = 1 \dots 9$, and $\Delta \theta_i(t)$, $i=1,2,3$, denote the time-varying parametric uncertainties in the driving system. Note that the dimension is not limited to R^3 and the analytical results in this chapter can be extended to R^n . We analyze the system in R^3 just in order to have simpler presentation in this chapter.

Similarly, the driven system in the presence of system uncertainties and an external control variable is described by

$$\begin{cases} \dot{\tilde{X}} = (A + \Delta\tilde{A}(t))\tilde{X} + \psi(\tilde{X}) + \Delta\psi(\tilde{X}) + u(t) & t \neq \tau_i \\ \Delta\tilde{X}|_{t=\tau_i} = -Be, & i = 1, 2, \dots \end{cases} \quad (5.2)$$

where

$$\Delta\tilde{A}(t) = \begin{bmatrix} \Delta\tilde{A}_1(t) & \Delta\tilde{A}_2(t) & \Delta\tilde{A}_3(t) \\ \Delta\tilde{A}_4(t) & \Delta\tilde{A}_5(t) & \Delta\tilde{A}_6(t) \\ \Delta\tilde{A}_7(t) & \Delta\tilde{A}_8(t) & \Delta\tilde{A}_9(t) \end{bmatrix}, \quad \Delta\psi(\tilde{X}) = [\Delta\tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta\tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta\tilde{\theta}_3^T \phi_3(\tilde{X})]^T,$$

$\Delta\tilde{\theta}_i^T = [\Delta\tilde{\theta}_{i1}, \Delta\tilde{\theta}_{i2}, \Delta\tilde{\theta}_{i3}]$ with $\Delta\tilde{A}_i(t)$ and $\Delta\tilde{\theta}_i(t)$ also denoting the time varying parametric uncertainties in the driven systems and $u(t)$ being a control signal used to regulate the states of the driven system towards those of the driving system, B is a 3×3 matrix and $e = (e_x, e_y, e_z)^T = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})^T$ is the *synchronization error*.

Time sequence $\{\tau_i : i = 1, 2, \dots\}$ denotes the time instants at which impulses are sent to the driven system from the driving system. In this chapter, the sequence is chosen based on the idea in [70] with varying intervals defined as

$$\Delta_1 = \sup_i \{\tau_{2i+1} - \tau_{2i}\} < \infty, \quad \Delta_2 = \sup_i \{\tau_{2i} - \tau_{2i-1}\} < \infty \quad (5.3)$$

and for a given constant ε such that $1 > \varepsilon > 0$

$$\tau_{2i+1} - \tau_{2i} \leq \varepsilon(\tau_{2i} - \tau_{2i-1}), \forall i \in \{1, 2, \dots\}.$$

We now derive a model for the error system

$$\begin{aligned}
 \dot{e} &= \dot{X} - \dot{\tilde{X}} \\
 &= (A + \Delta A(t))X + \Delta \psi(X) + \psi(X) - ((A + \Delta \tilde{A}(t))\tilde{X} + \psi(\tilde{X}) + \Delta \psi(\tilde{X}) + u(t)) \\
 &= Ae + \Delta A(t)X - \Delta \tilde{A}(t)\tilde{X} + \Psi(X, \tilde{X}) + \Delta \psi(X) - \Delta \psi(\tilde{X}) - u(t) \\
 &= Ae + \Psi(X, \tilde{X}) + \Delta A(t)(X - \tilde{X}) + \Delta A(t)\tilde{X} - \Delta \tilde{A}(t)\tilde{X} + \Delta \psi(X, \tilde{X}) - u(t) \\
 &= (A + \Delta A(t))e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t))\tilde{X} + \Delta \psi(X, \tilde{X}) - u(t) \quad t \neq \tau_i
 \end{aligned} \tag{5.4}$$

where $\Psi(X, \tilde{X}) = \psi(X) - \psi(\tilde{X})$

$$\begin{aligned}
 \Delta \psi(X, \tilde{X}) &= \Delta \psi(X) - \Delta \psi(\tilde{X}) \\
 &= [\Delta \theta_1^T \phi_1(X), \Delta \theta_2^T \phi_2(X), \Delta \theta_3^T \phi_3(X)]^T - [\Delta \tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta \tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta \tilde{\theta}_3^T \phi_3(\tilde{X})]^T \\
 &= [\Delta \theta_1^T \phi_1(X) - \Delta \tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta \theta_2^T \phi_2(X) - \Delta \tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta \theta_3^T \phi_3(X) - \Delta \tilde{\theta}_3^T \phi_3(\tilde{X})]^T \\
 &= \begin{bmatrix} \Delta \theta_1^T (\phi_1(X) - \phi_1(\tilde{X})) + (\Delta \theta_1^T - \Delta \tilde{\theta}_1^T) \phi_1(\tilde{X}) \\ \Delta \theta_2^T (\phi_2(X) - \phi_2(\tilde{X})) + (\Delta \theta_2^T - \Delta \tilde{\theta}_2^T) \phi_2(\tilde{X}) \\ \Delta \theta_3^T (\phi_3(X) - \phi_3(\tilde{X})) + (\Delta \theta_3^T - \Delta \tilde{\theta}_3^T) \phi_3(\tilde{X}) \end{bmatrix}
 \end{aligned} \tag{5.5}$$

Then the error system is described by

$$\begin{cases} \dot{e} = (Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t))\tilde{X} + \Delta \psi(X, \tilde{X}) - u(t), & t \neq \tau_i \\ \Delta e|_{t=\tau_i} = Be, & i = 1, 2, \dots \end{cases} \tag{5.6}$$

Remark 5.1: It is noted that $\Delta A(t) - \Delta \tilde{A}(t)$, $\Delta \theta_i - \Delta \tilde{\theta}_i$, $i=1,2,3$ denote the parametric mismatch between the driving and driven systems. Such mismatch is unavoidable in practice. For example, it is impossible to implement two identical systems and/or

maintain them to be identical all the time during their operation. So far, there is no result available addressing such a problem.

Usually, we have some a priori knowledge about the uncertainties as given below.

Assumption 5.1:

The parametric uncertainties and mismatch $\Delta A_i(t)$, $\Delta \tilde{A}_i(t)$ and $\Delta \theta_i(t)$, $\Delta \tilde{\theta}_i(t)$ are bounded as follows:

$$\begin{aligned} |\Delta A_i(t)| &\leq a_i, \quad |\Delta A_i(t) - \Delta \tilde{A}_i(t)| \leq b_i \quad i = 1-9 \\ \|\Delta \theta_i\| &\leq c_i, \quad \|\Delta \theta_i - \Delta \tilde{\theta}_i\| \leq g_i, \quad i = 1, 2, 3 \end{aligned}$$

for some known constant a_i , b_i , c_i and g_i , where $\|\cdot\|$ denotes the Euclidean norm.

Remark 5.2: The bounds can be estimated based on apriori knowledge about the systems. For example, when chaotic systems are implemented as analog circuits, the estimation of the bounding parameters turns into the estimation of the bounding of the electronic components. Since most electronic components have an allowed tolerance to the stated specification. The bounding parameters can be determined according to the tolerance of the electronics components on the specifications.

We now use two typical chaotic systems for illustrations.

5.2.2 The Lorenz Model

The Lorenz model [2] with parametric perturbation is given by:

$$\begin{cases} \frac{dx}{dt} = (\sigma + \Delta\sigma)(y - x) \\ \frac{dy}{dt} = -xz + (r + \Delta r)x - y \\ \frac{dz}{dt} = xy - (\eta + \Delta\eta)z \end{cases} \quad (5.7)$$

where σ, r , and η are three constant parameters, $\Delta\sigma$, Δr and $\Delta\eta$ are three bounded parametric perturbations.

Comparing with the form in (5.1), we have

$$\psi(X) = [0 \quad -xz \quad xy]^T, A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -\eta \end{bmatrix}, \Delta A = \begin{bmatrix} -\Delta\sigma(t) & \Delta\sigma(t) & 0 \\ \Delta r(t) & 0 & 0 \\ 0 & 0 & -\Delta\eta(t) \end{bmatrix}$$

Similarly, the parametric uncertainties in the receiver side can be denoted as

$$\Delta\tilde{A} = \begin{bmatrix} -\Delta\tilde{\sigma}(t) & \Delta\tilde{\sigma}(t) & 0 \\ \Delta\tilde{r}(t) & 0 & 0 \\ 0 & 0 & -\Delta\tilde{\eta}(t) \end{bmatrix}$$

where $\Delta\tilde{\sigma}$, $\Delta\tilde{r}$ and $\Delta\tilde{\eta}$ are three bounded parametric perturbations. Compared with

Assumption 1, $a_3 = a_5 = a_6 = a_7 = a_8 = 0$, $c_i = 0, g_i = 0, i = 1, 2, 3$.

5.2.3 The Chua's Circuit

The Chua's circuit with parametric perturbation is given by:

$$\begin{cases} \frac{dx}{dt} = (\alpha + \Delta\alpha)(y - x - (f(x) + \Delta f(x))) \\ \frac{dy}{dt} = x - y + z \\ \frac{dz}{dt} = -(\beta + \Delta\beta)y - (\gamma + \Delta\gamma)z \end{cases} \quad (5.8)$$

where $f(x) = bx + \frac{1}{2}(a-b)\{|x+1| - |x-1|\}$, $\Delta f(x) = \Delta bx + \frac{1}{2}(\Delta a - \Delta b)\{|x+1| - |x-1|\}$.

a, b, α, β and γ are constant parameters with a and b satisfying $a < b < 0$, $\Delta\alpha, \Delta\beta, \Delta\gamma, \Delta a$ and Δb are the bounded parametric perturbations.

In this case,

$$\psi^T(X) = [-\alpha f(x) \quad 0 \quad 0] \quad , \quad \theta_1^T = \begin{bmatrix} b & \frac{1}{2}(a-b) & -\frac{1}{2}(a-b) \end{bmatrix} \quad ,$$

$$\phi_1^T(X) = \begin{bmatrix} x & |x+1| & |x-1| \end{bmatrix} \quad , \quad \theta_2^T = \theta_3^T = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \quad , \quad A = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix} \quad ,$$

$$\Delta A = \begin{bmatrix} -\Delta\alpha & \Delta\alpha & 0 \\ 0 & 0 & 0 \\ 0 & -\Delta\beta & -\Delta\gamma \end{bmatrix} \quad , \quad \Delta\theta_1^T = \begin{bmatrix} -\Delta\alpha(b + \Delta b) - \alpha\Delta b \\ -\frac{1}{2}\Delta\alpha(a + \Delta a - b - \Delta b) - \frac{1}{2}\alpha(\Delta a - \Delta b) \\ \frac{1}{2}\Delta\alpha(a + \Delta a - b - \Delta b) + \frac{1}{2}\alpha(\Delta a - \Delta b) \end{bmatrix}^T .$$

Likewise, the parametric perturbation at the receiver side can be denoted as

$$\Delta \tilde{A} = \begin{bmatrix} -\Delta \tilde{\alpha} & \Delta \tilde{\alpha} & 0 \\ 0 & 0 & 0 \\ 0 & -\Delta \tilde{\beta} & -\Delta \tilde{\gamma} \end{bmatrix},$$

$$\Delta \tilde{\theta}_1^T = \begin{bmatrix} -\Delta \tilde{\alpha}(b + \Delta \tilde{b}) - \alpha \Delta \tilde{b} & -\frac{1}{2} \Delta \tilde{\alpha}(a + \Delta \tilde{a} - b - \Delta \tilde{b}) - \frac{1}{2} \alpha(\Delta \tilde{a} - \Delta \tilde{b}) & \frac{1}{2} \Delta \tilde{\alpha}(a + \Delta \tilde{a} - b - \Delta \tilde{b}) + \frac{1}{2} \alpha(\Delta \tilde{a} - \Delta \tilde{b}) \end{bmatrix}$$

where $\Delta \tilde{a}$, $\Delta \tilde{b}$, $\Delta \tilde{\alpha}$, $\Delta \tilde{\beta}$ and $\Delta \tilde{\gamma}$ are bounded and $a_3 = a_4 = a_5 = a_6 = a_7 = 0$ compared

with Assumption 5.1.

To make the driving and driven systems synchronized, we need the following assumption, similar to [70]:

Assumption 5.2:

The class of chaotic systems considered satisfies the following inequalities:

$$2(X - \tilde{X})^T \Psi(X, \tilde{X}) \leq (X - \tilde{X})^T (H + H^T)(X - \tilde{X}) \quad (5.9)$$

Both the Lorenz system and the Chua's Circuit satisfy this assumption.

For Lorenz system

$$H = \begin{bmatrix} \sqrt{2}M_1/2 & 0 & 0 \\ 0 & \sqrt{2}M_1/2 & 0 \\ 0 & 0 & \sqrt{2}M_1/2 \end{bmatrix}, \quad (5.10)$$

where M_1 is the upper bound of y and z .

For Chua's circuit

$$H(X) = \begin{bmatrix} |\alpha a| & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (5.11)$$

5.3 Synchronization Scheme

To ensure the states of the driven system converging to those of the driving system, we need to choose the time interval Δ_1 given in (5.3) appropriately and also design a suitable control law for the control signal $u(t)$ in the driven system. Two schemes are proposed in this section.

5.3.1 Scheme I

As in [70], we choose the time interval Δ_1 according to the following conditions.

$$0 \leq a_{\min} \leq -\frac{2}{(1+\varepsilon)\Delta_1} \ln(\xi d_1), \xi > 1 \quad (5.12)$$

where $a_{\min}$ denotes the solution of the following optimization problem

$$\min_p \{a\} \text{ such that } (A+H)^T P + P(A+H) < aP \quad (5.13)$$

and d_1 satisfies

$$(I+B)^T P(I+B) < d_1 P \text{ and } \xi d_1 < 1 \quad (5.14)$$

where matrix $P = P^T > 0$ is symmetric positive definite given by

(i) For Chua's oscillator,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_{22} & p_{23} \\ 0 & p_{32} & p_{33} \end{bmatrix} \quad (5.15)$$

(ii) For Lorenz system,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_{22} & 0 \\ 0 & 0 & p_{33} \end{bmatrix} \quad (5.16)$$

Clearly, $p_{23} = p_{32} = 0$ for the Lorenz system.

In order to counteract the effect of parametric uncertainties and mismatch between the two systems, we now design the control $u(t)$ as follows.

Let $e_1 = e_x$ $e_2 = p_{22}e_y + p_{23}e_z$ $e_3 = p_{23}e_y + p_{33}e_z$, then

$$\begin{aligned} u(t) = & \begin{bmatrix} b_1 |\tilde{x}(t)| \text{sgn}(e_1) \\ b_4 |\tilde{x}(t)| \text{sgn}(e_2) \\ b_7 |\tilde{x}(t)| \text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} b_2 |\tilde{y}(t)| \text{sgn}(e_1) \\ b_5 |\tilde{y}(t)| \text{sgn}(e_2) \\ b_8 |\tilde{y}(t)| \text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} b_3 |\tilde{z}(t)| \text{sgn}(e_1) \\ b_6 |\tilde{z}(t)| \text{sgn}(e_2) \\ b_9 |\tilde{z}(t)| \text{sgn}(e_3) \end{bmatrix} \\ & + \begin{bmatrix} c_1 \|\phi_1(X) - \phi_1(\tilde{X})\| \text{sgn}(e_1) \\ c_2 \|\phi_2(X) - \phi_2(\tilde{X})\| \text{sgn}(e_2) \\ c_3 \|\phi_3(X) - \phi_3(\tilde{X})\| \text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} g_1 \|\phi_1(\tilde{X})\| \text{sgn}(e_1) \\ g_2 \|\phi_2(\tilde{X})\| \text{sgn}(e_2) \\ g_3 \|\phi_3(\tilde{X})\| \text{sgn}(e_3) \end{bmatrix} \end{aligned}$$

$$+ \begin{bmatrix} (a_1 |e_x| + a_2 |e_y| + a_3 |e_z|) \operatorname{sgn}(e_1) \\ (a_4 |e_x| + a_5 |e_y| + a_6 |e_z|) \operatorname{sgn}(e_2) \\ (a_7 |e_x| + a_8 |e_y| + a_9 |e_z|) \operatorname{sgn}(e_3) \end{bmatrix} \quad (5.17)$$

Based on the design of the control $u(t)$, the controller for Lorenz model is

$$u(t) = \begin{bmatrix} b_1 |\tilde{x}(t)| \operatorname{sgn}(e_1) + b_2 |\tilde{y}(t)| \operatorname{sgn}(e_1) \\ b_4 |\tilde{x}(t)| \operatorname{sgn}(e_2) \\ b_9 |\tilde{z}(t)| \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} (a_1 |e_x| + a_2 |e_y|) \operatorname{sgn}(e_1) \\ a_4 |e_x| \operatorname{sgn}(e_2) \\ a_9 |e_z| \operatorname{sgn}(e_3) \end{bmatrix}$$

The controller for Chua's circuit is

$$u(t) = \begin{bmatrix} b_1 |\tilde{x}(t)| \operatorname{sgn}(e_1) + b_2 |\tilde{y}(t)| \operatorname{sgn}(e_1) + c_1 \|\phi_1(X) - \phi_1(\tilde{X})\| \operatorname{sgn}(e_1) + g_1 \|\phi_1(\tilde{X})\| \operatorname{sgn}(e_1) \\ 0 \\ b_8 |\tilde{y}(t)| \operatorname{sgn}(e_3) + b_9 |\tilde{z}(t)| \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} (a_1 |e_x| + a_2 |e_y|) \operatorname{sgn}(e_1) \\ 0 \\ (a_8 |e_y| + a_9 |e_z|) \operatorname{sgn}(e_3) \end{bmatrix}$$

Theorem 5.1. The error system given by (5.6), is asymptotically stable if $u(t)$ is designed based on (5.17) and the time interval Δ_1 is chosen according to the conditions (5.12)-(5.16).

Proof: Choose the Lyapunov function as $V(e) = e^T P e$. It can be shown that when $t \neq \tau_i$,

$$\begin{aligned}
 \dot{V}(e) &= \dot{e}^T P e + e^T P \dot{e} \\
 &= ((Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) - u(t))^T P e \\
 &\quad + e^T P (Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) - u(t)) \\
 &= e^T A^T P e + e^T \Delta A(t)^T P e + \tilde{X}^T (\Delta A - \Delta \tilde{A}(t))^T P e + \Delta \psi^T(X, \tilde{X}) P e \\
 &\quad + \Psi^T(X, \tilde{X}) P e - u^T(t) P e + e^T P A e + e^T P \Delta A(t) e + e^T P (\Delta A - \Delta \tilde{A}(t)) \tilde{X} \\
 &\quad + e^T P \Psi(X, \tilde{X}) + e^T P \Delta \psi(X, \tilde{X}) - e^T P u(t) \\
 &= e^T (A^T P + P A) e + 2e^T P \Psi(X, \tilde{X}) + \tilde{X}^T (\Delta A - \Delta \tilde{A}(t))^T P e \\
 &\quad + e^T P (\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi^T(X, \tilde{X}) P e + e^T P \Delta \psi(X, \tilde{X}) \\
 &\quad + e^T \Delta A(t)^T P e + e^T P \Delta A(t) e - u^T(t) P e - e^T P u(t) \\
 &= e^T (A^T P + P A) e + 2e^T P \Psi(X, \tilde{X}) \\
 &\quad + \left[\tilde{X}^T (\Delta A - \Delta \tilde{A}(t))^T + \Delta \psi^T(X, \tilde{X}) + e^T \Delta A(t)^T - u^T(t) \right] P e \\
 &\quad + e^T P \left[(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) + \Delta A(t) e - u(t) \right] \\
 &\leq e^T (A^T P + P A) e + e^T (P H + H^T P) e \\
 &\quad + 2e^T P \left[(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) + \Delta A(t) e - u(t) \right] \tag{5.18}
 \end{aligned}$$

Considering the last term of (5.18) with the use of (5.17), we have

$$\begin{aligned}
 &e^T P \left[(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) + \Delta A e - u(t) \right] \\
 &= \begin{pmatrix} e_x & e_y & e_z \end{pmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_{22} & p_{23} \\ 0 & p_{23} & p_{33} \end{bmatrix} \left[(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) - u(t) \right] \\
 &= \begin{pmatrix} e_x & p_{22}e_y + p_{23}e_z & p_{23}e_y + p_{33}e_z \end{pmatrix} \\
 &\quad \times \left(\begin{bmatrix} (\Delta A_1 - \Delta \tilde{A}_1)\tilde{x}(t) - b_1 |\tilde{x}(t)| \text{sgn}(e_1) \\ (\Delta A_4 - \Delta \tilde{A}_4)\tilde{x}(t) - b_4 |\tilde{x}(t)| \text{sgn}(e_2) \\ (\Delta A_7 - \Delta \tilde{A}_7)\tilde{x}(t) - b_7 |\tilde{x}(t)| \text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} (\Delta A_2 - \Delta \tilde{A}_2)\tilde{y}(t) - b_2 |\tilde{y}(t)| \text{sgn}(e_1) \\ (\Delta A_5 - \Delta \tilde{A}_5)\tilde{y}(t) - b_5 |\tilde{y}(t)| \text{sgn}(e_2) \\ (\Delta A_8 - \Delta \tilde{A}_8)\tilde{y}(t) - b_8 |\tilde{y}(t)| \text{sgn}(e_3) \end{bmatrix} \right) \\
 &\quad + \begin{bmatrix} (\Delta A_3 - \Delta \tilde{A}_3)\tilde{z}(t) - b_3 |\tilde{z}(t)| \text{sgn}(e_1) \\ (\Delta A_6 - \Delta \tilde{A}_6)\tilde{z}(t) - b_6 |\tilde{z}(t)| \text{sgn}(e_2) \\ (\Delta A_9 - \Delta \tilde{A}_9)\tilde{z}(t) - b_9 |\tilde{z}(t)| \text{sgn}(e_3) \end{bmatrix} \Bigg) +
 \end{aligned}$$

$$\begin{aligned}
 & \left(e_x \quad p_{22}e_y + p_{23}e_z \quad p_{23}e_y + p_{33}e_z \right) \\
 & \times \left\{ \begin{aligned} & \left[\begin{aligned} & \Delta\theta_1^T (\phi_1(X) - \phi_1(\tilde{X})) - c_1 \|\phi_1(X) - \phi_1(\tilde{X})\| \text{sgn}(e_1) \\ & \Delta\theta_2^T (\phi_2(X) - \phi_2(\tilde{X})) - c_2 \|\phi_2(X) - \phi_2(\tilde{X})\| \text{sgn}(e_2) \\ & \Delta\theta_3^T (\phi_3(X) - \phi_3(\tilde{X})) - c_3 \|\phi_3(X) - \phi_3(\tilde{X})\| \text{sgn}(e_3) \end{aligned} \right] \\ & + \left[\begin{aligned} & (\Delta\theta_1^T - \Delta\tilde{\theta}_1^T) \phi_1(\tilde{X}) - g_1 \|\phi_1(\tilde{X})\| \text{sgn}(e_1) \\ & (\Delta\theta_2^T - \Delta\tilde{\theta}_2^T) \phi_2(\tilde{X}) - g_2 \|\phi_2(\tilde{X})\| \text{sgn}(e_2) \\ & (\Delta\theta_3^T - \Delta\tilde{\theta}_3^T) \phi_3(\tilde{X}) - g_3 \|\phi_3(\tilde{X})\| \text{sgn}(e_3) \end{aligned} \right] \\ & + \left[\begin{aligned} & \Delta A_1 e_x + \Delta A_2 e_y + \Delta A_3 e_z - (a_1 |e_x| + a_2 |e_y| + a_3 |e_z|) \text{sgn}(e_1) \\ & \Delta A_4 e_x + \Delta A_5 e_y + \Delta A_6 e_z - (a_4 |e_x| + a_5 |e_y| + a_6 |e_z|) \text{sgn}(e_2) \\ & \Delta A_7 e_x + \Delta A_8 e_y + \Delta A_9 e_z - (a_7 |e_x| + a_8 |e_y| + a_9 |e_z|) \text{sgn}(e_3) \end{aligned} \right] \end{aligned} \right\} \\
 & = e_1 \left((\Delta A_1 - \Delta \tilde{A}_1) \tilde{x}(t) - b_1 |\tilde{x}(t)| \text{sgn}(e_1) \right) + e_2 \left((\Delta A_4 - \Delta \tilde{A}_4) \tilde{x}(t) - b_4 |\tilde{x}(t)| \text{sgn}(e_2) \right) + e_3 \left((\Delta A_7 - \Delta \tilde{A}_7) \tilde{x}(t) - b_7 |\tilde{x}(t)| \text{sgn}(e_3) \right) \\
 & + e_1 \left((\Delta A_2 - \Delta \tilde{A}_2) \tilde{y}(t) - b_2 |\tilde{y}(t)| \text{sgn}(e_1) \right) + e_2 \left((\Delta A_5 - \Delta \tilde{A}_5) \tilde{y}(t) - b_5 |\tilde{y}(t)| \text{sgn}(e_2) \right) + e_3 \left((\Delta A_8 - \Delta \tilde{A}_8) \tilde{y}(t) - b_8 |\tilde{y}(t)| \text{sgn}(e_3) \right) \\
 & + e_1 \left((\Delta A_3 - \Delta \tilde{A}_3) \tilde{z}(t) - b_3 |\tilde{z}(t)| \text{sgn}(e_1) \right) + e_2 \left((\Delta A_6 - \Delta \tilde{A}_6) \tilde{z}(t) - b_6 |\tilde{z}(t)| \text{sgn}(e_2) \right) + e_3 \left((\Delta A_9 - \Delta \tilde{A}_9) \tilde{z}(t) - b_9 |\tilde{z}(t)| \text{sgn}(e_3) \right) \\
 & + e_1 \left(\Delta\theta_1^T (\phi_1(X) - \phi_1(\tilde{X})) - c_1 \|\phi_1(X) - \phi_1(\tilde{X})\| \text{sgn}(e_1) \right) + e_2 \left(\Delta\theta_2^T (\phi_2(X) - \phi_2(\tilde{X})) - c_2 \|\phi_2(X) - \phi_2(\tilde{X})\| \text{sgn}(e_2) \right) \\
 & + e_3 \left(\Delta\theta_3^T (\phi_3(X) - \phi_3(\tilde{X})) - c_3 \|\phi_3(X) - \phi_3(\tilde{X})\| \text{sgn}(e_3) \right) \\
 & + e_1 \left((\Delta\theta_1^T - \Delta\tilde{\theta}_1^T) \phi_1(\tilde{X}) - g_1 \|\phi_1(\tilde{X})\| \text{sgn}(e_1) \right) + e_2 \left((\Delta\theta_2^T - \Delta\tilde{\theta}_2^T) \phi_2(\tilde{X}) - g_2 \|\phi_2(\tilde{X})\| \text{sgn}(e_2) \right) \\
 & + e_3 \left((\Delta\theta_3^T - \Delta\tilde{\theta}_3^T) \phi_3(\tilde{X}) - g_3 \|\phi_3(\tilde{X})\| \text{sgn}(e_3) \right) \\
 & + e_1 \left(\Delta A_1 e_x + \Delta A_2 e_y + \Delta A_3 e_z - (a_1 |e_x| + a_2 |e_y| + a_3 |e_z|) \text{sgn}(e_1) \right) + e_2 \left(\Delta A_4 e_x + \Delta A_5 e_y + \Delta A_6 e_z - (a_4 |e_x| + a_5 |e_y| + a_6 |e_z|) \text{sgn}(e_2) \right) \\
 & + e_3 \left(\Delta A_7 e_x + \Delta A_8 e_y + \Delta A_9 e_z - (a_7 |e_x| + a_8 |e_y| + a_9 |e_z|) \text{sgn}(e_3) \right)
 \end{aligned} \tag{5.19}$$

Note from Assumption 5.1 that

$$\text{when } e_1 \geq 0 \quad e_1((\Delta A_1 - \Delta \tilde{A}_1) \tilde{x}(t) - b_1 |\tilde{x}(t)| \text{sgn}(e_1)) \leq 0$$

$$\text{when } e_1 < 0 \quad e_1((\Delta A_1 - \Delta \tilde{A}_1) \tilde{x}(t) - b_1 |\tilde{x}(t)| \text{sgn}(e_1)) < 0$$

Therefore $e_1((\Delta A_1 - \Delta \tilde{A}_1) \tilde{x}(t) - b_1 |\tilde{x}(t)| \text{sgn}(e_1)) \leq 0$ for any e_1 .

Similarly, we can show that each term of the right side of (19) is non-positive.

Therefore we have

$$e^T P((\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) + \Delta A e - u(t)) \leq 0 \quad (5.20)$$

Thus from (5.12), (5.13), (5.18) and (5.20), we get

$$\dot{V}(e) \leq a_{\min} V(e) \quad (5.21)$$

When $t = \tau_i$

$$\begin{aligned} V(e(\tau_i)) &= e^T (I + B)^T P(I + B) e \\ &\leq d_1 V(e(\tau_i)) \end{aligned} \quad (5.22)$$

Now the following comparison system can be obtained:

$$\begin{cases} \dot{\omega}(t) = a_{\min} \omega(t), & t \neq \tau_i \\ \omega(\tau_i^+) = d_1 \omega(\tau_i), & t = \tau_i \\ \omega(t_0^+) = \omega_0 \geq 0 \end{cases} \quad (5.23)$$

We have

$$\begin{aligned} a_{\min} (\tau_{2i+1} - \tau_{2i-1}) &= a_{\min} (\tau_{2i+1} - \tau_{2i} + \tau_{2i} - \tau_{2i-1}) \\ &\leq a_{\min} (\Delta_1 + \Delta_2) \\ &\leq a_{\min} (1 + \varepsilon) \Delta_1 \\ &\leq -2 \ln(\xi d_1) \end{aligned} \quad (5.24)$$

Therefore the error system (5.6) is proved to be asymptotically stable by Corollary 3.2.1 in [52].

□□□

5.3.2 Scheme II

In the second scheme, we choose the control $u(t)$ as follows.

$$\begin{aligned}
 u(t) = & \begin{bmatrix} b_1 |\tilde{x}(t)| \text{sgn}(e_x) \\ b_4 |\tilde{x}(t)| \text{sgn}(e_y) \\ b_7 |\tilde{x}(t)| \text{sgn}(e_z) \end{bmatrix} + \begin{bmatrix} b_2 |\tilde{y}(t)| \text{sgn}(e_x) \\ b_5 |\tilde{y}(t)| \text{sgn}(e_y) \\ b_8 |\tilde{y}(t)| \text{sgn}(e_z) \end{bmatrix} + \begin{bmatrix} b_3 |\tilde{z}(t)| \text{sgn}(e_x) \\ b_6 |\tilde{z}(t)| \text{sgn}(e_y) \\ b_9 |\tilde{z}(t)| \text{sgn}(e_z) \end{bmatrix} \\
 & + \begin{bmatrix} c_1 \|\phi_1(X) - \phi_1(\tilde{X})\| \text{sgn}(e_1) \\ c_2 \|\phi_2(X) - \phi_2(\tilde{X})\| \text{sgn}(e_2) \\ c_3 \|\phi_3(X) - \phi_3(\tilde{X})\| \text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} g_1 \|\phi_1(\tilde{X})\| \text{sgn}(e_x) \\ g_2 \|\phi_2(\tilde{X})\| \text{sgn}(e_y) \\ g_3 \|\phi_3(\tilde{X})\| \text{sgn}(e_z) \end{bmatrix}
 \end{aligned} \tag{5.25}$$

To handle $e^T (\Delta A(t)^T + \Delta A(t))e$ in the derivative of the Lyapunov function, we need to select time interval Δ_1 appropriately.

We also re-write ΔA as $\Delta A = DF(t)E$, where $F(t)$ is the time varying term also D and E are constant matrices. Let

$$\lambda_{AH} = \lambda_{\max}(A + A^T + H + H^T) + 2\lambda_{\max}(F(t))\|D\|\|E\|, \tag{5.26}$$

where $\lambda_{\max}$ denotes the largest eigenvalue of the matrix.

Then Δ_1 is chosen according to the following conditions:

$$0 \leq \lambda_{AH} \leq -\frac{2}{(1+\varepsilon)\Delta_1} \ln(\xi d_1), \quad \xi > 1 \tag{5.27}$$

$$d_1 > \lambda_{\max}((I+B)^T(I+B)) \tag{5.28}$$

Theorem 5.2 The error system given by (5.6), is asymptotically stable if $u(t)$ is designed based on (5.25) and the time interval Δ_1 is chosen according to the conditions (5.27)-(5.28).

Proof: Choose the Lyapunov function as $V(e) = e^T e$. It can be shown that when $t \neq \tau_i$,

$$\begin{aligned}\dot{V}(e) &= \dot{e}^T e + e^T \dot{e} \\ &\leq e^T ((A + H + \Delta A(t))^T + (A + H + \Delta A(t)))e \\ &\quad + 2e^T [(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) - u(t)]\end{aligned}\tag{5.29}$$

Also following similar analysis as in (19) we have

$$e^T ((\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}) - u(t)) \leq 0\tag{5.30}$$

So from (5.29) and (5.30),

$$\dot{V}(e) \leq \lambda_{AH} V(e)$$

When $t = \tau_i$,

$$\begin{aligned}V(e(\tau_i)) &= e^T (I + B)^T (I + B)e \\ &\leq d_1 V(e(\tau_i))\end{aligned}\tag{5.31}$$

Now the following comparison system can be obtained:

$$\begin{cases} \dot{\omega}(t) = \lambda_{AH} \omega(t), & t \neq \tau_i \\ \omega(\tau_i^+) = d_1 \omega(\tau_i), & t = \tau_i \\ \omega(t_0^+) = \omega_0 \geq 0 \end{cases}\tag{5.32}$$

It follows from Corollary 3.2.1 in [52] that the trivial solution of (5.6) is asymptotically stable. $\square\square\square$

Remark 5.3: Note that the conditions in Theorems 5.1 and 5.2 are sufficient only. So if the bounding parameters are underestimated, we are uncertain if the driving chaotic system and driven chaotic system can be synchronized or not.

5.4 Illustrative Examples

In this section, we use the Lorenz model and Chua's circuit as examples to illustrate the effectiveness of the two schemes proposed.

5.4.1 Simulation Results with Scheme I

Example 5.1

Suppose that the Lorenz model at the driving system and the driven system are perturbed with parametric uncertainties $\Delta\delta = \Delta r = \Delta\eta = \sin t$, $\Delta\tilde{\delta} = \Delta\tilde{r} = \Delta\tilde{\eta} = \cos t$, i.e.

$$\Delta A = \begin{bmatrix} -\Delta\delta & \Delta\delta & 0 \\ \Delta r & 0 & 0 \\ 0 & 0 & -\Delta\eta \end{bmatrix} = \begin{bmatrix} -\sin t & \sin t & 0 \\ \sin t & 0 & 0 \\ 0 & 0 & -\sin t \end{bmatrix}$$

$$\Delta \tilde{A} = \begin{bmatrix} -\Delta\tilde{\delta} & \Delta\tilde{\delta} & 0 \\ \Delta\tilde{r} & 0 & 0 \\ 0 & 0 & -\Delta\tilde{\eta} \end{bmatrix} = \begin{bmatrix} -\cos t & \cos t & 0 \\ \cos t & 0 & 0 \\ 0 & 0 & -\cos t \end{bmatrix}$$

Then the bounding parameters in Assumption 5.1 can be chosen as $a_1 = a_2 = a_4 = a_9 = 1$,

$$b_1 = b_2 = b_4 = b_9 = \sqrt{2}.$$

According to (5.17),

$$u(t) = \begin{bmatrix} \sqrt{2}|\tilde{x}(t)|\text{sgn}(e_1) + \sqrt{2}|\tilde{y}(t)|\text{sgn}(e_1) \\ \sqrt{2}|\tilde{x}(t)|\text{sgn}(e_2) \\ \sqrt{2}|\tilde{z}(t)|\text{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} (|e_x| + |e_y|)\text{sgn}(e_1) \\ |e_x|\text{sgn}(e_2) \\ |e_z|\text{sgn}(e_3) \end{bmatrix}$$

For simulation, the parameter and initial conditions are chosen as follows:

$$\delta = 10, r = 28, \eta = \frac{8}{3}, M_1 = 50, X(0) = [27, 5, 2]^T \text{ and } \tilde{X}(0) = [5, 3, 5]^T.$$

Matrix B is chosen to be $\begin{bmatrix} -0.1 & 0 & 0 \\ 0 & -0.1 & 0 \\ 0 & 0 & -0.1 \end{bmatrix}.$

Then from (5.11), $a_{\min} = 94.355$, $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.35714 & 0 \\ 0 & 0 & 0.35714 \end{bmatrix}$, also from (5.12),

$$d_1 > \lambda_{\max}((I + B)^T P(I + B)P^{-1}) = 0.81.$$

Consider $\xi = 1.0001$ and $\varepsilon = 0.5$. The upper bounds of the impulsive intervals are calculated as follows.

$$\Delta_1 = \frac{-2\ln(\xi d_1)}{(1 + \varepsilon)a_{\min}} = 2.9763 \times 10^{-3}, \Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1 + \varepsilon)a_{\min}} = 1.4881 \times 10^{-3}.$$

We choose $\Delta_1 = 2.8 \times 10^{-3}$, $\Delta_2 = 1.4 \times 10^{-3}$ in the simulation.

The experimental results are illustrated in Figure 5.1. It is clear that the state errors between the driving system and the driven system converge to zero with the proposed

scheme. It is calculated that the synchronization error

$$\|e\| = \sqrt{e_x^2 + e_y^2 + e_z^2} = 3.4350 \times 10^{-2} \text{ at } T = 0.336.$$

Figure 5.1: The synchronization errors of Lorenz model with the proposed control applied

For comparison with the scheme in [70], we set all the parameters the same as above but without applying the control. The simulation results are shown in Figure 5.2 and it is computed that $\|e\| = 0.1424$ at $T = 0.336$. From the Figure 5.2, it is observed that the error does not converge to zero.

Figure 5.2: The synchronization errors of the Lorenz model with the scheme in [70] but without the proposed control

Example 5.2

Choose the parameters of Chua's Circuit as $\alpha=10, \beta=16, \gamma=0.0385, a=-\frac{8}{7}, b=-\frac{5}{7}$.

Suppose that the driving system and driven system are perturbed with the following parametric uncertainties

$$\Delta\alpha = \Delta\beta = 0.5 \sin t, \Delta\gamma = 0.03 \sin t, \Delta a = 0.05 \sin t, \Delta b = 0.03 \sin t,$$

$$\Delta\tilde{\alpha} = \Delta\tilde{\beta} = 0.5 \cos t, \Delta\tilde{\gamma} = 0.03 \cos t, \Delta\tilde{a} = 0.05 \cos t, \Delta\tilde{b} = 0.03 \cos t, \text{ i.e.}$$

$$\Delta A = \begin{bmatrix} -0.5 \sin t & 0.5 \sin t & 0 \\ 0 & 0 & 0 \\ 0 & -0.5 \sin t & -0.03 \sin t \end{bmatrix}, \Delta \tilde{A} = \begin{bmatrix} -0.5 \cos t & 0.5 \cos t & 0 \\ 0 & 0 & 0 \\ 0 & -0.5 \cos t & -0.03 \cos t \end{bmatrix},$$

$$\Delta\theta_1^T = \begin{bmatrix} 0.0571 \sin t - 0.015 \sin^2 t & -0.0929 \sin t - 0.005 \sin^2 t & 0.0929 \sin t + 0.005 \sin^2 t \end{bmatrix}$$

$$\Delta\tilde{\theta}_1^T = \begin{bmatrix} 0.0571 \cos t - 0.015 \cos^2 t & -0.0929 \cos t - 0.005 \cos^2 t & 0.0929 \cos t + 0.005 \cos^2 t \end{bmatrix}.$$

Then the bounding parameters in Assumption 1 are chosen as

$$a_1 = a_2 = a_8 = 0.5, a_9 = 0.03, b_1 = b_2 = b_8 = 0.7071, b_9 = 0.0424, c_1 = 0.1312, g_1 = 0.2051.$$

According to (5.17),

$$u(t) = \begin{bmatrix} 0.7071|\tilde{x}(t)|\text{sgn}(e_1) + 0.7071|\tilde{y}(t)|\text{sgn}(e_1) + 0.1312\|\phi_1(X) - \phi_1(\tilde{X})\|\text{sgn}(e_1) \\ 0 \\ 0.7071|\tilde{y}(t)|\text{sgn}(e_3) + 0.0424|\tilde{z}(t)|\text{sgn}(e_3) \end{bmatrix}$$

$$+ \begin{bmatrix} 0.5(|e_x| + |e_y|)\text{sgn}(e_1) + 0.2051\|\phi_1(\tilde{X})\|\text{sgn}(e_1) \\ 0 \\ (0.5|e_y| + 0.03|e_z|)\text{sgn}(e_3) \end{bmatrix}$$

For the simulation, the initial conditions are chosen as follows:

$$X(0) = [17, 6, 18]^T \text{ and } X'(0) = [25, 4, 1]^T.$$

Matrix B is chosen as
$$\begin{bmatrix} -0.1 & 0 & 0 \\ 0 & -0.1 & 0 \\ 0 & 0 & -0.1 \end{bmatrix}.$$

Similarly, we have that $a_{\min} = 6.0279$,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12.4058 & 1.8355 \\ 0 & 1.8355 & 0.7754 \end{bmatrix}, d_1 > \lambda_{\max}((I + B)^T P (I + B) P^{-1}) = 0.81.$$

Then consider $\xi = 1.01$ and $\varepsilon = 0.5$. The upper bounds of the impulsive intervals are calculated as follows.

$$\Delta_1 = \frac{-2 \ln(\xi d_1)}{(1 + \varepsilon) a_{\min}} = 4.4409 \times 10^{-2}, \quad \Delta_2 = \frac{-2 \varepsilon \ln(\xi d_1)}{(1 + \varepsilon) a_{\min}} = 2.2205 \times 10^{-2}.$$

We choose $\Delta_1 = 3 \times 10^{-2}$, $\Delta_2 = 1.5 \times 10^{-2}$ in the simulation.

The synchronization error $\|e\| = \sqrt{e_x^2 + e_y^2 + e_z^2} = 6.4676 \times 10^{-3}$ at $T = 2.97$ and the simulation results are illustrated in Figure 5.3.

Figure 5.3: The synchronization error of the Chua's circuit with the proposed controller

For comparison with the scheme in [70], we set all parameters the same as above but without the proposed controller. The simulation results are shown in Figure 5.4 and the synchronization error $\|e\| = 0.7151$ at $T = 2.97$. It is observed that the error does not converge to zero.

Figure 5.4: The synchronization errors of the Chua's circuit without the controller

5.4.2 Simulation Results with Scheme II

Example 5.3 Consider the Lorenz model in Example 5.1 again. It can be noted that

$$\Delta A = DF(t)E, D = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

With the same bounding parameters in Example 1, i.e., $b_1 = b_2 = b_4 = b_9 = \sqrt{2}$, the

control based on (5.25) is

$$u(t) = \begin{bmatrix} \sqrt{2} |\tilde{x}(t)| \operatorname{sgn}(e_x) + \sqrt{2} |\tilde{y}(t)| \operatorname{sgn}(e_x) \\ \sqrt{2} |\tilde{x}(t)| \operatorname{sgn}(e_y) \\ \sqrt{2} |\tilde{z}(t)| \operatorname{sgn}(e_z) \end{bmatrix}$$

For the simulation, parameters and initial conditions are chosen as the same as Example

5.1. Then from (5.29), $\lambda_{AH} = 101.9873$, also from (5.28),

$$d_1 > \lambda_{\max}((I+B)^T(I+B)) = 0.81.$$

With $\xi = 1.0001$ and $\varepsilon = 0.5$, the upper bounds of the impulsive intervals are calculated as follows.

$$\Delta_1 = \frac{-2\ln(\xi d_1)}{(1+\varepsilon)\lambda_{AH}} = 2.7536 \times 10^{-3}, \quad \Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1+\varepsilon)\lambda_{AH}} = 1.3768 \times 10^{-3}.$$

We choose $\Delta_1 = 2.6 \times 10^{-3}$, $\Delta_2 = 1.3 \times 10^{-3}$ in the simulation. The cases with and without control are simulated. The experimental results are illustrated in Figures 5.5-5.6. It is clear that the state errors between the driving system and the driven system can converge to zero with the proposed control applied rapidly. Also at $T = 0.4095$, $\|e\| = \sqrt{e_x^2 + e_y^2 + e_z^2} = 3.5424 \times 10^{-2}$ with control applied whereas $\|e\| = 0.1081$ without control.

Figure 5.5: The synchronization errors of Lorenz model with the proposed control applied

Figure 5.6: The synchronization errors of the Lorenz model with the scheme in [70] but without the proposed control

Example 5.4:

Consider the Chua's circuit in Example 5.2 again. It can be noted that

$$\Delta A = DF(t)E, \quad D = \begin{bmatrix} -0.5 & 0.5 & 0 \\ 0 & 0 & 0 \\ 0 & -0.5 & -0.03 \end{bmatrix}, \quad F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, \quad E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

With the same bounding parameters in Example 5.2,

i.e., $b_1 = b_2 = b_8 = 0.7071$, $b_9 = 0.0424$, $c_1 = 0.1312$ and $g_1 = 0.2051$,

the control based on (5.25) is

$$u(t) = \begin{bmatrix} 0.7071|\tilde{x}(t)|\text{sgn}(e_x) + 0.7071|\tilde{y}(t)|\text{sgn}(e_x) \\ 0 \\ 0.7071|\tilde{y}(t)|\text{sgn}(e_z) + 0.0424|\tilde{z}(t)|\text{sgn}(e_z) \end{bmatrix} + \begin{bmatrix} 0.1312\|\phi_1(X) - \phi_1(\tilde{X})\|\text{sgn}(e_1) + 0.2051|\phi_1(\tilde{X})|\text{sgn}(e_1) \\ 0 \\ 0 \end{bmatrix}$$

For the simulation, parameters and initial conditions are chosen as the same as Example

5.2. Then we have that $\lambda_{AH} = 19.8170$, $d_1 > \lambda_{\max}((I+B)^T(I+B)) = 0.81$.

Then consider $\xi = 1.01$ and $\varepsilon = 0.5$. The upper bounds of the impulsive intervals are calculated as follows:

$$\Delta_1 = \frac{-2\ln(\xi d_1)}{(1+\varepsilon)\lambda_{AH}} = 1.3508 \times 10^{-2}, \quad \Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1+\varepsilon)\lambda_{AH}} = 6.7542 \times 10^{-3}.$$

We choose $\Delta_1 = 1 \times 10^{-2}$, $\Delta_2 = 5 \times 10^{-3}$ in the simulation. The cases with and without control are simulated. The experimental results are illustrated in Figure 5.7-5.8.

It is clear that the state errors between the driving system and the driven system can converge to zero with the proposed control applied rapidly.

Also at $T = 0.99$, $\|e\| = \sqrt{e_x^2 + e_y^2 + e_z^2} = 1.0819 \times 10^{-3}$ with control applied whereas

$\|e\| = 0.3038$ without control.

From the simulation results, it is observed that all the states of the driven system will converge to those of the driving system with proposed control scheme applied. On the other hand, the states of the driven system may not have such convergence if no control is applied.

Figure 5.7: The synchronization error of the Chua's circuit with the proposed controller

Figure 5.8: The synchronization errors of the Chua's circuit without the controller

5.5 Concluding Remark

In this chapter, the synchronization of two chaotic systems in the presence of parametric uncertainties and parametric mismatch between the two systems were studied. Two schemes are proposed for designing a controller to synchronize the two systems. Theoretical analysis shows that the two chaotic systems can be synchronized with the proposed schemes. Simulation results also verify the effectiveness of these methods.

Chapter 6

Synchronization of Chaotic Systems in the Presence of Noise

6.1 Introduction

Recently, a lot of efforts have been devoted to the synchronization of chaotic systems for chaotic secure communication. However, all the results on perfect synchronization are obtained under the ideal condition that the chaotic systems in both the transmitter side and the receiver side are noise free. In this chapter, we relax this condition by designing a controller for the driven system based on the bounds of the system noise. Perfect synchronization of the two systems is theoretically established. Numerical

results also illustrate the robustness and effectiveness of the proposed scheme. Recently, the problem of synchronization in the presence of system parametric uncertainty and mismatch was addressed in [71]. It is noted that some results on chaotic shift keying in the presence of channel noise were presented in [72-76]. In practice, certain internal and external noise, which may be caused by temperature variation, voltage fluctuation and other factors, inevitably exists in the chaotic systems. So far, no result has been reported in the presence of such kind of system noise. Without taking the noise into consideration in the design process, synchronization may not be ensured. In fact, from our simulation studies, the system synchronization error may diverge even when a small amount of noise is present.

In this chapter, we consider this practical problem. On the basis of the result in [70] where impulsive synchronization is considered, a control scheme is presented to design a controller for the driven system to achieve perfect synchronization of the two chaotic systems. In our design, the bound of the noise is employed to counteract the noise effects. Also, the structural information of the nonlinear parts of the systems is explored and employed in the controller design in order to achieve less conservative results. Based on theoretical analysis, the proposed scheme ensures that the states of the driven system converge to those of the driving system asymptotically. Two example systems, i.e. the Lorenz model and the Chen's equation, are used to illustrate our scheme. Numerical simulation results on the two systems also verify the effectiveness of the scheme, as it prevents the synchronization error from diverging.

6.2 Problem Formulation

6.2.1 System Models

We first present the models of the two chaotic systems. The driving system in the presence of noise is described by

$$\dot{X} = A(X + N(t)) + \psi(X + N(t)) \quad (6.1)$$

where $X \in R^3$ is the state vector and $X = [x, y, z]^T$, $A \in R^{3 \times 3}$ is the nominal constant matrix and $\psi(X) = [\psi_1(X) \ \psi_2(X) \ \psi_3(X)]^T$ is the nonlinear part of the chaotic system, and $N(t) = [N_1(t), N_2(t), N_3(t)]^T$ denotes the noise in the driving system.

Similar to that in chapter 5, the dimension is not limited to R^3 and the analytical results in this chapter can be extent to R^n . We analyze the system in R^3 just in order to have simpler presentation in this chapter.

Similarly, the driven system in the presence of system noise and an external control variable is described by

$$\begin{cases} \dot{\tilde{X}} = A(\tilde{X} + \tilde{N}(t)) + \psi(\tilde{X} + \tilde{N}(t)) + u(t) & t \neq \tau_i \\ \Delta \tilde{X} \Big|_{t=\tau_i} = -Be, & i = 1, 2, \dots \end{cases} \quad (6.2)$$

where $\tilde{N}(t) = [\tilde{N}_1(t), \tilde{N}_2(t), \tilde{N}_3(t)]^T$ denotes the noise in the driven systems and $u(t)$ is a control signal used to regulate the states of the driven system towards those of the driving system, B is a 3×3 matrix and $e = (e_x, e_y, e_z)^T = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})^T$ is the *synchronization error*. Time sequence $\{\tau_i : i = 1, 2, \dots\}$ denotes the time instants at which impulses are sent to the driven system from the driving system. In this chapter, the sequence is chosen based on the idea in [70] with varying intervals defined as

$$\Delta_1 = \sup_i \{\tau_{2i+1} - \tau_{2i}\} < \infty, \quad \Delta_2 = \sup_i \{\tau_{2i} - \tau_{2i-1}\} < \infty$$

and for a given constant ε satisfying $1 > \varepsilon > 0$

$$\tau_{2i+1} - \tau_{2i} \leq \varepsilon(\tau_{2i} - \tau_{2i-1}), \forall i \in \{1, 2, \dots\}. \quad (6.3)$$

The time interval should be chosen properly for the synchronization of the chaotic systems. We will discuss the condition for choosing Δ_1 in the latter part of this chapter.

Usually, we have some a priori knowledge about the noise as specified below.

Assumption 6.1:

The noise terms $N_i(t)$ and $\tilde{N}_i(t)$ are bounded as follows:

$$\|N_i\|_\infty \leq \mu_i, \|\tilde{N}_i\|_\infty \leq \tilde{\mu}_i, \quad i = 1, 2, 3, \quad (6.4)$$

for some known constants μ_i and $\tilde{\mu}_i$, where $\|\cdot\|_\infty$ denotes the L_∞ norm.

Remark 6.1: The bounds can be estimated based on apriori knowledge about the systems. For example, if the noise terms in the chaotic circuits are caused by thermal

noise on resistors, the bounding parameters for the noise terms can be determined given the values of the resistors in chaotic circuit.

We now derive a model for the error system

$$\begin{aligned}
 \dot{e} &= \dot{X} - \dot{\tilde{X}} \\
 &= A(X + N(t)) + \psi(X + N(t)) - A(\tilde{X} + \tilde{N}(t)) - \psi(\tilde{X} + \tilde{N}(t)) - u(t) \\
 &= Ae + A(N(t) - \tilde{N}(t)) + \psi(X + N(t)) - \psi(\tilde{X} + \tilde{N}(t)) - u(t) \\
 &= Ae + A(N - \tilde{N}) + \Psi(X, \tilde{X}) + \Phi(N, \tilde{N}) - u(t), \quad t \neq \tau_i
 \end{aligned} \tag{6.5}$$

where

$$\Psi(X, \tilde{X}) = \psi(X) - \psi(\tilde{X}), \Phi(N(t), \tilde{N}(t)) = \psi(X + N(t)) - \psi(\tilde{X} + \tilde{N}(t)) - \Psi(X, \tilde{X})$$

Then the error system is described by

$$\begin{cases} \dot{e} = Ae + A(N - \tilde{N}) + \Psi(X, \tilde{X}) + \Phi(N, \tilde{N}) - u(t), & t \neq \tau_i \\ \Delta e|_{t=\tau_i} = Be, & i = 1, 2, \dots \end{cases} \tag{6.6}$$

Denote

$$A(N - \tilde{N}) = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} N_1 - \tilde{N}_1 \\ N_2 - \tilde{N}_2 \\ N_3 - \tilde{N}_3 \end{bmatrix} = \begin{bmatrix} a_{11}(N_1 - \tilde{N}_1) + a_{12}(N_2 - \tilde{N}_2) + a_{13}(N_3 - \tilde{N}_3) \\ a_{21}(N_1 - \tilde{N}_1) + a_{22}(N_2 - \tilde{N}_2) + a_{23}(N_3 - \tilde{N}_3) \\ a_{31}(N_1 - \tilde{N}_1) + a_{32}(N_2 - \tilde{N}_2) + a_{33}(N_3 - \tilde{N}_3) \end{bmatrix} = \begin{bmatrix} \chi_1 \\ \chi_2 \\ \chi_3 \end{bmatrix}$$

Since $N_i(t)$ and $\tilde{N}_i(t)$ are bounded,

$$|\chi_i| \leq b_i, \quad i = 1, 2, 3 \tag{6.7}$$

where $b_i = \sum_{j=1}^3 |a_{ij}|(\mu_j + \tilde{\mu}_j)$.

Assumption 6.2:

We assume the nonlinear part $\Phi(N, \tilde{N})$ of the error system satisfies the following structure condition.

$$\Phi(N(t), \tilde{N}(t)) = \begin{bmatrix} X^T V_1 N - \tilde{X}^T V_1 \tilde{N} \\ X^T V_2 N - \tilde{X}^T V_2 \tilde{N} \\ X^T V_3 N - \tilde{X}^T V_3 \tilde{N} \end{bmatrix} + \begin{bmatrix} N^T k_1 \hat{k}_1^T N - \tilde{N}^T k_1 \hat{k}_1^T \tilde{N} \\ N^T k_2 \hat{k}_2^T N - \tilde{N}^T k_2 \hat{k}_2^T \tilde{N} \\ N^T k_3 \hat{k}_3^T N - \tilde{N}^T k_3 \hat{k}_3^T \tilde{N} \end{bmatrix}$$

where V_i, k_i and $\hat{k}_i$ are known constant matrix and vectors.

$$V_i = \begin{bmatrix} v_{ix1} & v_{ix2} & v_{ix3} \\ v_{iy1} & v_{iy2} & v_{iy3} \\ v_{iz1} & v_{iz2} & v_{iz3} \end{bmatrix}, k_i = [k_{i1} \quad k_{i2} \quad k_{i3}]^T, \hat{k}_i = [\hat{k}_{i1} \quad \hat{k}_{i2} \quad \hat{k}_{i3}]^T, i = 1, 2, 3$$

$$\text{Let } \bar{\mu} = [\mu_1 \quad \mu_2 \quad \mu_3]^T, \bar{X} = [|x| \quad |y| \quad |z|]^T, \bar{\tilde{\mu}} = [\tilde{\mu}_1 \quad \tilde{\mu}_2 \quad \tilde{\mu}_3]^T,$$

$$\bar{\tilde{X}} = [|\tilde{x}| \quad |\tilde{y}| \quad |\tilde{z}|]^T, \bar{k}_i = [|k_{i1}| \quad |k_{i2}| \quad |k_{i3}|]^T, \bar{\hat{k}}_i = [|\hat{k}_{i1}| \quad |\hat{k}_{i2}| \quad |\hat{k}_{i3}|]^T$$

$$\bar{V}_i = \begin{bmatrix} |v_{ix1}| & |v_{ix2}| & |v_{ix3}| \\ |v_{iy1}| & |v_{iy2}| & |v_{iy3}| \\ |v_{iz1}| & |v_{iz2}| & |v_{iz3}| \end{bmatrix}, i = 1, 2, 3$$

We have the following inequalities:

$$\begin{aligned} & \left| X^T V_i N - \tilde{X}^T V_i \tilde{N} + N^T k_i \hat{k}_i^T N - \tilde{N}^T k_i \hat{k}_i^T \tilde{N} \right| \\ & \leq \bar{X}^T \bar{V}_i \bar{\mu} + \tilde{X}^T \bar{V}_i \tilde{\mu} + \bar{\mu}^T \bar{k}_i \hat{k}_i^T \bar{\mu} + \tilde{\mu}^T \bar{k}_i \hat{k}_i^T \tilde{\mu} \quad , i = 1, 2, 3 \end{aligned} \quad (6.8)$$

Remark 6.2:

From the boundedness of the noise and also the states of the systems, $\Phi(N, \tilde{N})$ can be shown bounded by a known constant. If this bound is used to design controllers, the result obtained will be very conservative. If we use certain structural information of the nonlinear function $\psi(X)$ as given in Assumption 6.2, much less conservative result can be achieved, as will be shown later. Given the bounded parameters in Assumption 6.1, it is not difficult to determine V_i, k_i and $\hat{k}_i$.

We now use two typical chaotic systems for illustrations.

6.2.2 The Lorenz Model

The Lorenz model with system noise is given by:

$$\left\{ \begin{array}{l} \frac{dx}{dt} = \sigma((y + N_2(t)) - (x + N_1(t))) \\ \frac{dy}{dt} = -(x + N_1(t))(z + N_3(t)) + r(x + N_1(t)) - (y + N_2(t)) \\ \frac{dz}{dt} = (x + N_1(t))(y + N_2(t)) - \eta(z + N_3(t)) \end{array} \right. \quad (6.9)$$

where δ, r and η are three constant parameters, while $N_1(t)$, $N_2(t)$ and $N_3(t)$ are three bounded noise terms.

Comparing with the form in (6.1), we have

$$\psi(X) = [0 \quad -xz \quad xy]^T, \quad A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -\eta \end{bmatrix}, \quad N(t) = [N_1(t), N_2(t), N_3(t)]^T.$$

$\Phi(N(t), \tilde{N}(t))$ in Assumption 6.2 can be written as

$$\Phi(N(t), \tilde{N}(t)) = \begin{bmatrix} 0 \\ -(xN_3 + zN_1 + N_1N_3) + \tilde{x}\tilde{N}_3 + \tilde{z}\tilde{N}_1 + \tilde{N}_1\tilde{N}_3 \\ xN_2 + yN_1 + N_1N_2 - (\tilde{x}\tilde{N}_2 + \tilde{y}\tilde{N}_1 + \tilde{N}_1\tilde{N}_2) \end{bmatrix},$$

i.e.

$$V_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad V_2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \quad V_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$k_1 = \hat{k}_1 = [0 \ 0 \ 0]^T, \quad k_2 = [1 \ 0 \ 0]^T, \quad \hat{k}_2 = [0 \ 0 \ -1]^T, \quad k_3 = [1 \ 0 \ 0]^T, \\ \hat{k}_3 = [0 \ 1 \ 0]^T.$$

Also the bounds of χ_i can be obtained as

$$b_1 = \sigma(\mu_1 + \mu_2 + \tilde{\mu}_1 + \tilde{\mu}_2), b_2 = r(\mu_1 + \tilde{\mu}_1) + \mu_2 + \tilde{\mu}_2, b_3 = \eta(\mu_3 + \tilde{\mu}_3).$$

6.2.3 Chen's Equation

The Chen's chaotic system with noise term is given by:

$$\begin{cases} \frac{dx}{dt} = a((y + N_2(t)) - (x + N_1(t))) \\ \frac{dy}{dt} = (c - a)(x + N_1(t)) - (x + N_1(t))(z + N_3(t)) + c(y + N_2(t)) \\ \frac{dz}{dt} = (x + N_1(t))(y + N_2(t)) - b(z + N_2(t)) \end{cases} \quad (6.10)$$

where a, b and c are parameters of Chen's equation, while $N_1(t)$, $N_2(t)$ and $N_3(t)$ are three bounded noise terms.

Comparing with the form in (6.1), we have

$$\psi(X) = [0 \quad -xz \quad xy]^T, \quad A = \begin{bmatrix} -a & a & 0 \\ c-a & c & 0 \\ 0 & 0 & -b \end{bmatrix}, \quad N(t) = [N_1(t), N_2(t), N_3(t)]^T.$$

$\Phi(N(t), \tilde{N}(t))$ in Assumption 6.2 can be written as

$$\Phi(N(t), \tilde{N}(t)) = \begin{bmatrix} 0 \\ -(xN_3 + zN_1 + N_1N_3) + \tilde{x}\tilde{N}_3 + \tilde{z}\tilde{N}_1 + \tilde{N}_1\tilde{N}_3 \\ xN_2 + yN_1 + N_1N_2 - (\tilde{x}\tilde{N}_2 + \tilde{y}\tilde{N}_1 + \tilde{N}_1\tilde{N}_2) \end{bmatrix}$$

Thus

$$V_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, V_2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, V_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$k_1 = \hat{k}_1 = [0 \ 0 \ 0]^T, \quad k_2 = [1 \ 0 \ 0]^T, \quad \hat{k}_2 = [0 \ 0 \ -1]^T, \quad k_3 = [1 \ 0 \ 0]^T, \\ \hat{k}_3 = [0 \ 1 \ 0]^T.$$

Likewise, the bounds of $\chi_i, i = 1, 2, 3$ are given by:

$$b_1 = a(\mu_1 + \tilde{\mu}_1 + \mu_2 + \tilde{\mu}_2), \quad b_2 = (c - a)(\mu_1 + \tilde{\mu}_1) + c(\mu_2 + \tilde{\mu}_2), \quad b_3 = b(\mu_3 + \tilde{\mu}_3).$$

Note that some other chaotic systems such as Rössler system [77] also satisfy Assumption 6.2. To make the driving and driven systems synchronized by impulsive control, we also need the following assumption, which is similar to [70]:

Assumption 6.3:

The class of chaotic systems considered satisfies the following inequalities:

$$2(X - \tilde{X})^T \Psi(X, \tilde{X}) \leq (X - \tilde{X})^T (H + H^T)(X - \tilde{X}) \quad (6.11)$$

Note that Lorenz system and the Chen's equation satisfy this assumption with

$$H = \begin{bmatrix} \sqrt{2}M_1/2 & 0 & 0 \\ 0 & \sqrt{2}M_1/2 & 0 \\ 0 & 0 & \sqrt{2}M_1/2 \end{bmatrix}, \quad (6.12)$$

where M_1 is the upper bound of y and z .

6.3 Synchronization Scheme

To ensure that the states of the driven system converge to those of the driving system, we need to choose the time interval Δ_1 given in (6.3) appropriately and also design a suitable control law for the control signal $u(t)$ in the driven system. A scheme is proposed in this section.

As in [70], we choose the time interval Δ_1 according to the following conditions.

$$0 \leq a_{\min} \leq -\frac{2}{(1+\varepsilon)\Delta_1} \ln(\xi d_1), \xi > 1 \quad (6.13)$$

where $a_{\min}$ denotes the solution of the following optimization problem

$$\min_p \{a\} \text{ such that } (A+H)^T P + P(A+H) < aP \quad (6.14)$$

and d_1 satisfies

$$(I+B)^T P(I+B) < d_1 P \text{ and } \xi d_1 < 1 \quad (6.15)$$

where matrix $P = P^T > 0$ is symmetric positive definite given by

$$P = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}$$

For Lorenz system and Chen's equation,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p_{22} & 0 \\ 0 & 0 & p_{33} \end{bmatrix} \quad (6.16)$$

Clearly, $p_{11} = 1$, $p_{12} = p_{13} = p_{21} = p_{23} = p_{31} = p_{32} = 0$ for the Lorenz system and the Chen's equation.

Now denote $e_1 = p_{11}e_x + p_{21}e_y + p_{31}e_z$, $e_2 = p_{12}e_x + p_{22}e_y + p_{32}e_z$,

$$e_3 = p_{13}e_x + p_{23}e_y + p_{33}e_z$$

In order to counteract the effects of the noise terms in the two systems, we now design the control $u(t)$ as follows.

$$u(t) = \begin{bmatrix} b_1 \operatorname{sgn}(e_1) \\ b_2 \operatorname{sgn}(e_2) \\ b_3 \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} \left(\bar{X}^T \bar{V}_1 \bar{\mu} + \tilde{X}^T \bar{V}_1 \tilde{\mu} \right) \operatorname{sgn}(e_1) \\ \left(\bar{X}^T \bar{V}_2 \bar{\mu} + \tilde{X}^T \bar{V}_2 \tilde{\mu} \right) \operatorname{sgn}(e_2) \\ \left(\bar{X}^T \bar{V}_3 \bar{\mu} + \tilde{X}^T \bar{V}_3 \tilde{\mu} \right) \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} \left(\bar{\mu}^T \bar{k}_1 \bar{k}_1^T \bar{\mu} + \tilde{\mu}^T \bar{k}_1 \bar{k}_1^T \tilde{\mu} \right) \operatorname{sgn}(e_1) \\ \left(\bar{\mu}^T \bar{k}_2 \bar{k}_2^T \bar{\mu} + \tilde{\mu}^T \bar{k}_2 \bar{k}_2^T \tilde{\mu} \right) \operatorname{sgn}(e_2) \\ \left(\bar{\mu}^T \bar{k}_3 \bar{k}_3^T \bar{\mu} + \tilde{\mu}^T \bar{k}_3 \bar{k}_3^T \tilde{\mu} \right) \operatorname{sgn}(e_3) \end{bmatrix} \quad (6.17)$$

Theorem 6.1. The error system given by (6.6) is asymptotically stable if $u(t)$ is designed based on (6.17) and the time interval Δ_1 is chosen according to the conditions (6.13)-(6.16).

Proof: Choose the Lyapunov function as $V(e) = e^T P e$. It can be shown that when $t \neq \tau_i$,

$$\begin{aligned}
 \dot{V}(e) &= \dot{e}^T P e + e^T P \dot{e} \\
 &= (Ae + \Psi(X, \tilde{X}) + A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t))^T P e \\
 &\quad + e^T P (Ae + \Psi(X, \tilde{X}) + A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t)) \\
 &= e^T A^T P e + \Psi^T(X, \tilde{X}) P e + (N - \tilde{N})^T A^T P e + \Phi^T(N, \tilde{N}) P e - u^T(t) P e \\
 &\quad + e^T P A e + e^T P \Psi(X, \tilde{X}) + e^T P A (N - \tilde{N}) + e^T P \Phi(N, \tilde{N}) - e^T P u(t) \\
 &= e^T (A^T P + P A) e + 2e^T P \Psi(X, \tilde{X}) + (N - \tilde{N})^T A^T P e + e^T P A (N - \tilde{N}) \\
 &\quad + \Phi^T(N, \tilde{N}) P e + e^T P \Phi(N, \tilde{N}) - u^T(t) P e - e^T P u(t) \\
 &= e^T (A^T P + P A) e + 2e^T P \Psi(X, \tilde{X}) \\
 &\quad + \left[(N - \tilde{N})^T A^T + \Phi^T(N, \tilde{N}) - u^T(t) \right] P e \\
 &\quad + e^T P \left[A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t) \right] \\
 &\leq e^T (A^T P + P A) e + e^T (P H + H^T P) e \\
 &\quad + 2e^T P \left[A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t) \right]
 \end{aligned} \tag{6.18}$$

Considering the last term of (6.18) with the use of (6.17), we have

$$\begin{aligned}
 &e^T P \left[A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t) \right] \\
 &= \begin{pmatrix} e_x & e_y & e_z \end{pmatrix} \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix} \left[A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t) \right] \\
 &= \begin{pmatrix} e_1 & e_2 & e_3 \end{pmatrix} \left(\begin{bmatrix} \chi_1 - b_1 \operatorname{sgn}(e_1) \\ \chi_2 - b_2 \operatorname{sgn}(e_2) \\ \chi_3 - b_3 \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} X^T V_1 N - \tilde{X}^T V_1 \tilde{N} \\ X^T V_2 N - \tilde{X}^T V_2 \tilde{N} \\ X^T V_3 N - \tilde{X}^T V_3 \tilde{N} \end{bmatrix} + \begin{bmatrix} N^T k_1 \hat{k}_1^T N - \tilde{N}^T k_1 \hat{k}_1^T \tilde{N} \\ N^T k_2 \hat{k}_2^T N - \tilde{N}^T k_2 \hat{k}_2^T \tilde{N} \\ N^T k_3 \hat{k}_3^T N - \tilde{N}^T k_3 \hat{k}_3^T \tilde{N} \end{bmatrix} \right)
 \end{aligned}$$

$$\begin{aligned}
 & + (e_1 \quad e_2 \quad e_3) \left[\begin{array}{c} \left[\left(\bar{X}^T \bar{V}_1 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_1 \bar{\tilde{\mu}} \right) \text{sgn}(e_1) \right] \\ \left[\left(\bar{X}^T \bar{V}_2 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_2 \bar{\tilde{\mu}} \right) \text{sgn}(e_2) \right] \\ \left[\left(\bar{X}^T \bar{V}_3 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_3 \bar{\tilde{\mu}} \right) \text{sgn}(e_3) \right] \end{array} \right] + \left[\begin{array}{c} \left(\bar{\mu}^T \bar{k}_1 \bar{\hat{k}}_1^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_1 \bar{\hat{k}}_1^T \bar{\tilde{\mu}} \right) \text{sgn}(e_1) \\ \left(\bar{\mu}^T \bar{k}_2 \bar{\hat{k}}_2^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_2 \bar{\hat{k}}_2^T \bar{\tilde{\mu}} \right) \text{sgn}(e_2) \\ \left(\bar{\mu}^T \bar{k}_3 \bar{\hat{k}}_3^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_3 \bar{\hat{k}}_3^T \bar{\tilde{\mu}} \right) \text{sgn}(e_3) \end{array} \right] \\
 & = e_1 (\chi_1 - b_1 \text{sgn}(e_1)) + e_2 (\chi_2 - b_2 \text{sgn}(e_2)) + e_3 (\chi_3 - b_3 \text{sgn}(e_3)) \\
 & + e_1 \left(X^T V_1 N - \tilde{X}^T V_1 \tilde{N} + N^T k_1 \hat{k}_1^T N - \tilde{N}^T k_1 \hat{k}_1^T \tilde{N} \right) + e_2 \left(X^T V_2 N - \tilde{X}^T V_2 \tilde{N} + N^T k_2 \hat{k}_2^T N - \tilde{N}^T k_2 \hat{k}_2^T \tilde{N} \right) \\
 & + e_3 \left(X^T V_3 N - \tilde{X}^T V_3 \tilde{N} + N^T k_3 \hat{k}_3^T N - \tilde{N}^T k_3 \hat{k}_3^T \tilde{N} \right) - e_1 \left(\bar{X}^T \bar{V}_1 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_1 \bar{\tilde{\mu}} + \bar{\mu}^T \bar{k}_1 \bar{\hat{k}}_1^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_1 \bar{\hat{k}}_1^T \bar{\tilde{\mu}} \right) \text{sgn}(e_1) \\
 & - e_2 \left(\bar{X}^T \bar{V}_2 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_2 \bar{\tilde{\mu}} + \bar{\mu}^T \bar{k}_2 \bar{\hat{k}}_2^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_2 \bar{\hat{k}}_2^T \bar{\tilde{\mu}} \right) \text{sgn}(e_2) \\
 & - e_3 \left(\bar{X}^T \bar{V}_3 \bar{\mu} + \bar{\tilde{X}}^T \bar{V}_3 \bar{\tilde{\mu}} + \bar{\mu}^T \bar{k}_3 \bar{\hat{k}}_3^T \bar{\mu} + \bar{\tilde{\mu}}^T \bar{k}_3 \bar{\hat{k}}_3^T \bar{\tilde{\mu}} \right) \text{sgn}(e_3)
 \end{aligned} \tag{6.19}$$

Based on (6.7), we have the following argument:

If $e_i \geq 0$, then $e_i (\chi_i - b_i \text{sgn}(e_i)) \leq 0$ and if $e_i < 0$, then $e_i (\chi_i - b_i \text{sgn}(e_i)) < 0$

Therefore, $e_i (\chi_i - b_i \text{sgn}(e_i)) \leq 0$ for any e_i .

Similarly, we can show that the other terms on the right side of (6.19) are non-positive based on (6.8). Therefore we have

$$e^T P \left[A(N - \tilde{N}) + \Phi(N, \tilde{N}) - u(t) \right] \leq 0 \tag{6.20}$$

Thus from (6.13), (6.14), (6.18) and (6.20), we get

$$\dot{V}(e) \leq a_{\min} V(e) \tag{6.21}$$

When $t = \tau_i$

$$\begin{aligned}
 V(e(\tau_i)) & = e^T (I + B)^T P (I + B) e \\
 & \leq d_1 V(e(\tau_i))
 \end{aligned} \tag{6.22}$$

Now the following comparison system can be obtained:

$$\begin{cases} \dot{\omega}(t) = a_{\min} \omega(t), & t \neq \tau_i \\ \omega(\tau_i^+) = d_1 \omega(\tau_i), & t = \tau_i \\ \omega(t_0^+) = \omega_0 \geq 0 \end{cases} \quad (6.23)$$

We have

$$\begin{aligned} a_{\min}(\tau_{2i+1} - \tau_{2i-1}) &= a_{\min}(\tau_{2i+1} - \tau_{2i} + \tau_{2i} - \tau_{2i-1}) \\ &\leq a_{\min}(\Delta_1 + \Delta_2) \\ &\leq a_{\min}(1 + \varepsilon)\Delta_1 \\ &\leq -2 \ln(\xi d_1) \end{aligned} \quad (6.24)$$

Therefore the error system (6.6) is proved to be asymptotically stable by Corollary 3.2.1 in [52]. $\square\square\square$

Remark 6.3: Note that the conditions in Theorem 6.1 are sufficient only. If the time interval Δ_1 is not chosen according to the conditions in (6.13)-(6.15), we are uncertain if the error system given by (6.6) is asymptotically stable or not.

6.4 Illustrative Examples

In this section, we conduct simulation studies on the Lorenz model and Chen's equation to illustrate the effectiveness of the scheme proposed.

Example 6.1

Suppose that the Lorenz model has the following parameters and initial conditions

$$\delta = 10, r = 28, \eta = \frac{8}{3}, M_1 = 50, X(0) = [8, 5, 2]^T \text{ and } \tilde{X}(0) = [7, 3, 5]^T.$$

The driving system and the driven system are perturbed with white noise terms satisfying

$$\|N_1(t)\|_\infty \leq 0.05, \|N_2(t)\|_\infty \leq 0.05, \|N_3(t)\|_\infty \leq 0.05, \|\tilde{N}_1(t)\|_\infty \leq 0.06, \|\tilde{N}_2(t)\|_\infty \leq 0.06,$$

$$\|\tilde{N}_3(t)\|_\infty \leq 0.06. \text{ The bounds in Assumption 1 are chosen as } \mu_1 = \mu_2 = \mu_3 = 0.05,$$

$$\tilde{\mu}_1 = \tilde{\mu}_2 = \tilde{\mu}_3 = 0.06.$$

Then it can be calculated that $b_1 = 2.2000$, $b_2 = 2.9200$, $b_3 = 0.3200$.

According to (6.17),

$$\begin{aligned} u(t) &= \begin{bmatrix} b_1 \operatorname{sgn}(e_1) \\ b_2 \operatorname{sgn}(e_2) \\ b_3 \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} 0 \\ \mu_3 |x| \operatorname{sgn}(e_2) + \mu_1 |z| \operatorname{sgn}(e_2) + \mu_1 \mu_3 \operatorname{sgn}(e_2) + \tilde{\mu}_3 |\tilde{x}| \operatorname{sgn}(e_2) + \tilde{\mu}_1 |\tilde{z}| \operatorname{sgn}(e_2) + \tilde{\mu}_1 \tilde{\mu}_3 \operatorname{sgn}(e_2) \\ \mu_2 |x| \operatorname{sgn}(e_3) + \mu_1 |y| \operatorname{sgn}(e_3) + \mu_1 \mu_2 \operatorname{sgn}(e_3) + \tilde{\mu}_2 |\tilde{x}| \operatorname{sgn}(e_3) + \tilde{\mu}_1 |\tilde{y}| \operatorname{sgn}(e_3) + \tilde{\mu}_1 \tilde{\mu}_2 \operatorname{sgn}(e_3) \end{bmatrix} \\ &= \begin{bmatrix} 2.2 \operatorname{sgn}(e_1) \\ 2.92 \operatorname{sgn}(e_2) \\ 0.32 \operatorname{sgn}(e_3) \end{bmatrix} \\ &+ \begin{bmatrix} 0 \\ 0.05 |x| \operatorname{sgn}(e_2) + 0.05 |z| \operatorname{sgn}(e_2) + 0.0025 \operatorname{sgn}(e_2) + 0.06 |\tilde{x}| \operatorname{sgn}(e_2) + 0.06 |\tilde{z}| \operatorname{sgn}(e_2) + 0.0036 \operatorname{sgn}(e_2) \\ 0.05 |x| \operatorname{sgn}(e_3) + 0.05 |y| \operatorname{sgn}(e_3) + 0.0025 \operatorname{sgn}(e_3) + 0.06 |\tilde{x}| \operatorname{sgn}(e_3) + 0.06 |\tilde{y}| \operatorname{sgn}(e_3) + 0.0036 \operatorname{sgn}(e_3) \end{bmatrix} \end{aligned}$$

For simulation, matrix B is chosen to be $B = \begin{bmatrix} -0.1 & 0 & 0 \\ 0 & -0.1 & 0 \\ 0 & 0 & -0.1 \end{bmatrix}.$

Then from (6.14), $a_{\min} = 94.355$, $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.35714 & 0 \\ 0 & 0 & 0.35714 \end{bmatrix}$, and from (6.15),

$$d_1 > \lambda_{\max}((I+B)^T P(I+B)P^{-1}) = 0.81.$$

Consider $\xi = 1.0001$ and $\varepsilon = 0.5$. The upper bounds of the impulsive intervals are calculated as follows:

$$\Delta_1 = \frac{-2\ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 2.9763 \times 10^{-3}, \quad \Delta_2 = \frac{-2\varepsilon\ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 1.4881 \times 10^{-3}.$$

We choose $\Delta_1 = 2.8 \times 10^{-3}$ and $\Delta_2 = 1.4 \times 10^{-3}$ in the simulation.

For comparison with the scheme in [70], we set all the parameters the same as above but without applying the control scheme. The simulations results are illustrated in Figures 6.1-6.3 with solid lines and dashed lines representing respectively the synchronization errors with and without the proposed control scheme.

Figure 6.1: Synchronization Error e_x

Figure 6.2: Synchronization Error e_y

Figure 6.3: Synchronization Error e_z

From the above three figures, it is observed that the error does not converge to zero if without the proposed control, whereas the error is driven to zero asymptotically with the proposed control applied.

Example 6.2:

Choose the parameters of Chen's equation as $a = 35$, $b = 3$, $c = 28$.

Suppose that the driving system and the driven system are perturbed with white noise terms satisfying

$$\|N_1(t)\|_\infty \leq 0.02, \|N_2(t)\|_\infty \leq 0.02, \|N_3(t)\|_\infty \leq 0.02, \|\tilde{N}_1(t)\|_\infty \leq 0.03, \|\tilde{N}_2(t)\|_\infty \leq 0.03, \|\tilde{N}_3(t)\|_\infty \leq 0.03. \text{ Thus } \mu_1 = \mu_2 = \mu_3 = 0.02, \tilde{\mu}_1 = \tilde{\mu}_2 = \tilde{\mu}_3 = 0.03.$$

Then it can be calculated that $b_1 = 3.5000$, $b_2 = 1.9600$, $b_3 = 0.1800$.

According to (6.17),

$$\begin{aligned} u(t) &= \begin{bmatrix} b_1 \operatorname{sgn}(e_1) \\ b_2 \operatorname{sgn}(e_2) \\ b_3 \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} 0 \\ \mu_3 |x| \operatorname{sgn}(e_2) + \mu_1 |z| \operatorname{sgn}(e_2) + \mu_1 \mu_3 \operatorname{sgn}(e_2) + \tilde{\mu}_3 |\tilde{x}| \operatorname{sgn}(e_2) + \tilde{\mu}_1 |\tilde{z}| \operatorname{sgn}(e_2) + \tilde{\mu}_1 \tilde{\mu}_3 \operatorname{sgn}(e_2) \\ \mu_2 |x| \operatorname{sgn}(e_3) + \mu_1 |y| \operatorname{sgn}(e_3) + \mu_1 \mu_2 \operatorname{sgn}(e_3) + \tilde{\mu}_2 |\tilde{x}| \operatorname{sgn}(e_3) + \tilde{\mu}_1 |\tilde{y}| \operatorname{sgn}(e_3) + \tilde{\mu}_1 \tilde{\mu}_2 \operatorname{sgn}(e_3) \end{bmatrix} \\ &= \begin{bmatrix} 3.5 \operatorname{sgn}(e_1) \\ 1.96 \operatorname{sgn}(e_2) \\ 0.18 \operatorname{sgn}(e_3) \end{bmatrix} + \begin{bmatrix} 0 \\ 0.02 |x| \operatorname{sgn}(e_2) + 0.02 |z| \operatorname{sgn}(e_2) + 0.0004 \operatorname{sgn}(e_2) + 0.03 |\tilde{x}| \operatorname{sgn}(e_2) + 0.03 |\tilde{z}| \operatorname{sgn}(e_2) + 0.0009 \operatorname{sgn}(e_2) \\ 0.02 |x| \operatorname{sgn}(e_3) + 0.02 |y| \operatorname{sgn}(e_3) + 0.0004 \operatorname{sgn}(e_3) + 0.03 |\tilde{x}| \operatorname{sgn}(e_3) + 0.03 |\tilde{y}| \operatorname{sgn}(e_3) + 0.0009 \operatorname{sgn}(e_3) \end{bmatrix} \end{aligned}$$

For the simulation, the initial conditions are chosen as follows:

$$X(0) = [0.5, 1, 5]^T \text{ and } X'(0) = [10.5, 20, 38]^T.$$

$$\text{Matrix } B \text{ is chosen as } B = \begin{bmatrix} -0.8 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.8 \end{bmatrix}.$$

Similarly, we have that $a_{\min} = 126.7000$,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5.0000 & 0 \\ 0 & 0 & 5.0000 \end{bmatrix}, d_1 > \lambda_{\max}((I+B)^T P(I+B)P^{-1}) = 0.04$$

Then consider $\xi = 1.01$ and $\varepsilon = 0.5$. The upper bounds of the impulsive intervals are calculated as follows.

$$\Delta_1 = \frac{-2 \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 3.3769 \times 10^{-2}, \Delta_2 = \frac{-2\varepsilon \ln(\xi d_1)}{(1+\varepsilon)a_{\min}} = 1.6885 \times 10^{-2}.$$

We choose $\Delta_1 = 2 \times 10^{-3}$ and $\Delta_2 = 1 \times 10^{-3}$ in the simulation.

Similarly, comparison with the scheme in [70] is made again by setting all the parameters the same as above but without the proposed controller. The simulations results are illustrated in Figures 6.4-6.6 where the solid lines and the dashed lines correspond respectively to the synchronization errors with and without the proposed control scheme applied.

Figure 6.4: Synchronization Error e_x

Figure 6.5: Synchronization Error e_y

Figure 6.6: Synchronization Error e_z

It is observed that the error system is unstable when no control is applied. On the other hand, the error system is stabilized with the proposed scheme and thus perfect synchronization is achieved.

6.5 Concluding Remark

In this chapter, we have presented a control scheme to synchronize a driven chaotic system with the driving chaotic system in the presence of system noise in both systems. With the use of the noise bounds and structural information of the nonlinear parts of the systems, a controller is designed to ensure perfect synchronization of the two systems. Theoretical analysis and numerical simulations show the effectiveness of the control scheme.

Chapter 7

Practical Impulsive Synchronization of Chaotic Systems with Parametric Uncertainty and Mismatch

7.1 Introduction

Synchronization of chaos has great potential to be applied, for example, in chaos based secure communication. However, it is required that the parameters of the chaotic systems are known exactly and time invariant to design the chaotic cryptosystem. More demanding, these parameters should be identical for both chaotic systems, in order to

ensure perfect synchronization. Clearly, these conditions are impractical as chaotic systems are inevitably exposed to an environment which may cause their parameters varying within a small range. It is also difficult to implement chaotic systems with the designed parameter values and ensure two systems to be identical all the time. Thus the applicability of existing impulsive synchronization schemes is hindered and doubtful. Hence to remove the obstacle and worries, a practical scheme that is robust to parametric uncertainties and mismatch between the two systems is highly demanding and should be developed. Perhaps one can conjecture that the magnitude of the synchronization error can approach to a small bound by reducing the length of impulsive intervals when parametric uncertainties and mismatch appear. Nevertheless, no theoretical result has been established to ascertain the conjecture. Furthermore, there is no quantification on how small the intervals and the error bound will be. In other words, there is no clear guideline available on how to choose the intervals for a given error bound.

By proposing a new scheme to design a controller in the driven system, a preliminary solution to such robustness problems has been obtained by Wen *et al.* [71]. However, continuous transmission of signals such as state variables of the driving system is required for the controller to be implemented. Thus the security level is significantly decreased if the scheme is applied to secure communication. Therefore a purely impulsive synchronization scheme is preferred to enhance transmission security, which is the problem to be addressed in this chapter. Theoretically, the synchronization error will approach to zero in the limit with the existing schemes. It is meant that the

synchronization error cannot be ensured zero in finite time even in theory. Thus practically, we can never obtain zero synchronization error. Therefore it is practical to specify an arbitrarily small bound for the error magnitude and ensure it to approach to and stay within the bound. In this chapter, we propose an impulsive synchronization scheme to achieve this by deriving a condition on impulsive intervals based on the pre-specified bound. The condition relates impulsive interval lengths to the prescribed error bound and bounds of uncertainties and mismatch and gives a clear guideline on the choice of impulsive intervals. It is shown that the smaller the prescribed bound and/or the larger the uncertainties/mismatch, the more frequent transmission of impulses will be required. Obviously, this is the conjectured result that one has been expecting for long time. Our established result thus provides a theoretical basis and a firm assurance for impulsive synchronization schemes to be practically applicable including the development of secure communication strategies now.

7.2 System Models

In this section, we present the class of chaotic systems to be considered with illustration of Lorenz system and Chen's equation.

The driving system in the presence of uncertainty is described by

$$\dot{X} = (A + \Delta A(t))X + \Delta \psi(X) + \psi(X) \quad (7.1)$$

where $X \in R^3$ is the state vector, $A \in R^{3 \times 3}$ is the nominal constant matrix and

$\psi(X) = [\theta_1^T \phi_1(X), \theta_2^T \phi_2(X), \theta_3^T \phi_3(X)]^T$ is the nonlinear part of the chaotic system,

where

$$\Delta A(t) = \begin{bmatrix} \Delta A_1(t) & \Delta A_2(t) & \Delta A_3(t) \\ \Delta A_4(t) & \Delta A_5(t) & \Delta A_6(t) \\ \Delta A_7(t) & \Delta A_8(t) & \Delta A_9(t) \end{bmatrix}, \quad \theta_i^T = [\theta_{i1}, \theta_{i2}, \theta_{i3}] , \quad \phi_i^T(X) = [\phi_{i1}(X), \phi_{i2}(X), \phi_{i3}(X)] ,$$

$$\Delta \psi(X) = [\Delta \theta_1^T \phi_1(X), \Delta \theta_2^T \phi_2(X), \Delta \theta_3^T \phi_3(X)]^T, \quad \Delta \theta_i^T = [\Delta \theta_{i1}, \Delta \theta_{i2}, \Delta \theta_{i3}], \quad i=1,2,3.$$

Note that $\Delta A_i(t)$, $i=1 \dots 9$, and $\Delta \theta_i(t)$, $i=1,2,3$, denote time-varying parametric uncertainties in the driving system.

We also re-write ΔA as $\Delta A = DF(t)E$, where the diagonal matrix $F(t)$ is the time varying term, D and E are constant matrices.

Similar to that in Chapter 5, the dimension is not limited to R^3 and the analytical results in this chapter can be extent to R^n . We analyze the system in R^3 just in order to facilitate the latter discussion in this chapter.

The driven system in the presence of system uncertainties is described by

$$\begin{cases} \dot{\tilde{X}} = (A + \Delta \tilde{A}(t))\tilde{X} + \psi(\tilde{X}) + \Delta \psi(\tilde{X}) & t \neq \tau_i \\ \Delta \tilde{X} \Big|_{t=\tau_i} = -Be, & i = 1, 2, \dots \end{cases} \quad (7.2)$$

where

$$\Delta \tilde{A}(t) = \begin{bmatrix} \Delta \tilde{A}_1(t) & \Delta \tilde{A}_2(t) & \Delta \tilde{A}_3(t) \\ \Delta \tilde{A}_4(t) & \Delta \tilde{A}_5(t) & \Delta \tilde{A}_6(t) \\ \Delta \tilde{A}_7(t) & \Delta \tilde{A}_8(t) & \Delta \tilde{A}_9(t) \end{bmatrix}, \quad \Delta \psi(\tilde{X}) = [\Delta \tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta \tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta \tilde{\theta}_3^T \phi_3(\tilde{X})]^T,$$

$\Delta \tilde{\theta}_i^T = [\Delta \tilde{\theta}_{i1}, \Delta \tilde{\theta}_{i2}, \Delta \tilde{\theta}_{i3}]$ with $\Delta \tilde{A}_i(t)$ and $\Delta \tilde{\theta}_i(t)$ also denoting the time varying parametric uncertainties in the driven systems, B is a 3×3 matrix and $e = (e_x, e_y, e_z)^T = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})^T$ is the *synchronization error*.

Time sequence $\{\tau_i : i = 1, 2, \dots\}$ denotes the time instants at which impulses are sent to the driven system from the driving system and we define

$$\Delta_1 = \sup_i \{\tau_{i+1} - \tau_i\} < \infty \quad (7.3)$$

We now derive a model for the error system

$$\begin{aligned} \dot{e} &= \dot{X} - \dot{\tilde{X}} \\ &= (A + \Delta A(t))X + \Delta \psi(X) + \psi(X) - ((A + \Delta \tilde{A}(t))\tilde{X} + \psi(\tilde{X}) + \Delta \psi(\tilde{X})) \\ &= Ae + \Delta A(t)X - \Delta \tilde{A}(t)\tilde{X} + \Psi(X, \tilde{X}) + \Delta \psi(X) - \Delta \psi(\tilde{X}) \\ &= Ae + \Psi(X, \tilde{X}) + \Delta A(t)(X - \tilde{X}) + \Delta A(t)\tilde{X} - \Delta \tilde{A}(t)\tilde{X} + \Delta \psi(X, \tilde{X}) \\ &= (A + \Delta A(t))e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t))\tilde{X} + \Delta \psi(X, \tilde{X}) \quad t \neq \tau_i \end{aligned} \quad (7.4)$$

where $\Psi(X, \tilde{X}) = \psi(X) - \psi(\tilde{X})$

$$\begin{aligned}
 \Delta\psi(X, \tilde{X}) &= \Delta\psi(X) - \Delta\psi(\tilde{X}) \\
 &= [\Delta\theta_1^T \phi_1(X), \Delta\theta_2^T \phi_2(X), \Delta\theta_3^T \phi_3(X)]^T - [\Delta\tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta\tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta\tilde{\theta}_3^T \phi_3(\tilde{X})]^T \\
 &= [\Delta\theta_1^T \phi_1(X) - \Delta\tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta\theta_2^T \phi_2(X) - \Delta\tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta\theta_3^T \phi_3(X) - \Delta\tilde{\theta}_3^T \phi_3(\tilde{X})]^T \\
 &= \begin{bmatrix} \Delta\theta_1^T (\phi_1(X) - \phi_1(\tilde{X})) + (\Delta\theta_1^T - \Delta\tilde{\theta}_1^T) \phi_1(\tilde{X}) \\ \Delta\theta_2^T (\phi_2(X) - \phi_2(\tilde{X})) + (\Delta\theta_2^T - \Delta\tilde{\theta}_2^T) \phi_2(\tilde{X}) \\ \Delta\theta_3^T (\phi_3(X) - \phi_3(\tilde{X})) + (\Delta\theta_3^T - \Delta\tilde{\theta}_3^T) \phi_3(\tilde{X}) \end{bmatrix} \tag{7.5}
 \end{aligned}$$

Then the error system is described by

$$\begin{cases} \dot{e} = Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta\tilde{A}(t)) \tilde{X} + \Delta\psi(X, \tilde{X}), & t \neq \tau_i \\ \Delta e|_{t=\tau_i} = Be, & i = 1, 2, \dots \end{cases} \tag{7.6}$$

Remark 7.1: It is noted that $\Delta A(t) - \Delta\tilde{A}(t)$, $\Delta\theta_i - \Delta\tilde{\theta}_i$, $i=1,2,3$ denote the parametric mismatch between the driving and driven systems. Such mismatch is unavoidable in practice as it is impossible to implement two identical systems and/or maintain them to be identical all the time during their operation. So far, there is no result available on purely impulsive synchronization to handle such cases.

Usually, we have some a priori knowledge about the uncertainties as given below.

Assumption 7.1:

The parametric uncertainties and mismatch $\Delta A_i(t)$, $\Delta\tilde{A}_i(t)$, $\Delta\theta_i(t)$ and $\Delta\tilde{\theta}_i(t)$ are bounded as follows:

$$|\Delta A_i(t)| \leq a_i, |\Delta A_i(t) - \Delta \tilde{A}_i(t)| \leq b_i, \quad i = 1-9$$

$$\|\Delta \theta_i\| \leq c_i, \|\Delta \theta_i - \Delta \tilde{\theta}_i\| \leq g_i, \quad i = 1, 2, 3$$

for some known constant a_i , b_i , c_i and g_i , where $\|\cdot\|$ denotes the Euclidean norm.

We now use two typical chaotic systems for illustration.

(a) The Lorenz Model

The Lorenz model with parametric perturbation is given by:

$$\left\{ \begin{array}{l} \frac{dx}{dt} = (\sigma + \Delta\sigma)(y - x) \\ \frac{dy}{dt} = -xz + (r + \Delta r)x - y \\ \frac{dz}{dt} = xy - (\eta + \Delta\eta)z \end{array} \right. \quad (7.7)$$

where σ , r and η are three constant parameters; $\Delta\sigma$, Δr and $\Delta\eta$ are three bounded parametric perturbations.

Comparing with the form in (7.1), we have

$$\psi(X) = [0 \quad -xz \quad xy]^T, A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -\eta \end{bmatrix}, \Delta A(t) = \begin{bmatrix} -\Delta\sigma(t) & \Delta\sigma(t) & 0 \\ \Delta r(t) & 0 & 0 \\ 0 & 0 & -\Delta\eta(t) \end{bmatrix}$$

Similarly, the parametric uncertainties in the driven system can be denoted as

$$\Delta \tilde{A}(t) = \begin{bmatrix} -\Delta \tilde{\sigma}(t) & \Delta \tilde{\sigma}(t) & 0 \\ \Delta \tilde{r}(t) & 0 & 0 \\ 0 & 0 & -\Delta \tilde{\eta}(t) \end{bmatrix}$$

where $\Delta \tilde{\sigma}$, $\Delta \tilde{r}$ and $\Delta \tilde{\eta}$ are three bounded parametric perturbations. Compared with Assumption 7.1, $a_3 = a_5 = a_6 = a_7 = a_8 = 0$, $c_i = 0, g_i = 0, i = 1, 2, 3$.

(b) Chen's Equation

The Chen's chaotic system with noise term is given by:

$$\begin{cases} \frac{dx}{dt} = (a + \Delta a)(y - x) \\ \frac{dy}{dt} = (c + \Delta c - a - \Delta a)x + (c + \Delta c)y - xz \\ \frac{dz}{dt} = xy - (b + \Delta b)z \end{cases} \quad (7.8)$$

where a, b and c are parameters of Chen's equation, while Δa , Δb and Δc are three bounded parametric perturbations.

Comparing with the form in (7.1), we have

$$\psi(X) = [0 \quad -xz \quad xy]^T, A = \begin{bmatrix} -a & a & 0 \\ c - a & c & 0 \\ 0 & 0 & -b \end{bmatrix}, \Delta A(t) = \begin{bmatrix} -\Delta a(t) & \Delta a(t) & 0 \\ \Delta c(t) - \Delta a(t) & \Delta c(t) & 0 \\ 0 & 0 & -\Delta b(t) \end{bmatrix}$$

Likewise, the parametric perturbation at the receiver side can be denoted as

$$\Delta \tilde{A}(t) = \begin{bmatrix} -\Delta \tilde{a}(t) & \Delta \tilde{a}(t) & 0 \\ \Delta \tilde{c}(t) - \Delta \tilde{a}(t) & \Delta \tilde{c}(t) & 0 \\ 0 & 0 & -\Delta \tilde{b}(t) \end{bmatrix}$$

where $\Delta \tilde{a}$, $\Delta \tilde{b}$ and $\Delta \tilde{c}$ are bounded and $a_3 = a_6 = a_7 = a_8 = 0$, $c_i = 0, g_i = 0, i = 1, 2, 3$ compared with Assumption 7.1.

Assumption 7.2:

The class of chaotic systems considered satisfies the following inequalities:

$$2(X - \tilde{X})^T \Psi(X, \tilde{X}) \leq (X - \tilde{X})^T (H + H^T) (X - \tilde{X}) \quad (7.9)$$

Clearly, both the Lorenz system and the Chen's equation satisfy this assumption with

$$H = \begin{bmatrix} \sqrt{2}M_1/2 & 0 & 0 \\ 0 & \sqrt{2}M_1/2 & 0 \\ 0 & 0 & \sqrt{2}M_1/2 \end{bmatrix}, \quad (7.10)$$

where M_1 is the upper bound of y and z .

Moreover, Chua's circuit also satisfies this assumption with H given in (3.21).

Assumption 7.3:

The states of the system (7.1) and (7.2) are bounded as follows:

$$\sup |x, y, z| = M_a, \sup |\tilde{x}, \tilde{y}, \tilde{z}| = M_b$$

for some known constant M_a and M_b .

The nonlinear parts of system (7.1) and (7.2) are also bounded:

$$\sup \{ \|\phi_1(X)\|, \|\phi_2(X)\|, \|\phi_3(X)\| \} = M_c, \sup \{ \|\phi_1(\tilde{X})\|, \|\phi_2(\tilde{X})\|, \|\phi_3(\tilde{X})\| \} = M_d$$

for some known constant M_c and M_d .

Remark 7.2: These bounding parameters for both parametric uncertainties and states of chaotic system are chosen based on apriori knowledge.

7.3 Synchronization Scheme

It is practical to set an arbitrary small bound ε_0 for the magnitude of the synchronization error between the two chaotic systems. In this section, we propose an impulsive synchronization scheme which can effectively and practically synchronize systems with parametric uncertainties and mismatches. Although perfect synchronization cannot be theoretically guaranteed, the synchronization error magnitude can still be shown to approach and stay within the given arbitrary small desired error bound with the proposed scheme.

Denote

$$M_0 = M_b \sqrt{(b_1^2 + b_2^2 + b_3^2) + (b_4^2 + b_5^2 + b_6^2) + (b_7^2 + b_8^2 + b_9^2)} \\ + (M_c + M_d) \sqrt{(c_1^2 + c_2^2 + c_3^2)} + M_d \sqrt{(g_1^2 + g_2^2 + g_3^2)}$$

Define two set $R_1 = \{t \mid \|e(t)\| \leq \varepsilon_0\}$ and $R_2 = \{t \mid \|e(t)\| > \varepsilon_0\}$ where ε_0 is a pre-specified bound for the synchronization error to converge to. We also define $M_2 = \frac{M_0}{\varepsilon_0}$. Choose a Lyapunov function as $V(t) = V(e(t)) = e^T(t)e(t)$. In proposing a suitable impulsive scheme, we consider the sequence $V(\tau_i^+) = e^T(\tau_i^+)e(\tau_i^+)$. Our idea is to ensure $V(\tau_i^+)$ monotonically decreasing for all $\tau_i^+ \in R_2$. In the case that $\tau_i^+ \in R_1$, the scheme should also ensure that $\tau_{i+1}^+ \in R_1$.

Before giving the main result, we first consider a special case stated in the following lemma.

Lemma 7.1. If $[t_1, t] \subseteq R_2$ and there is no impulse sent over $[t_1, t]$, then

$$V(e(t)) \leq \exp(\lambda_{AH}(t - t_1))V(e(t_1))$$

where $\lambda_{AH} = \lambda_{\max}(A + A^T + H + H^T) + 2\lambda_{\max}(F(t))\|D\|\|E\| + 2M_2$.

Proof: From the conditions of the lemma, we have

$$\begin{aligned}
 \dot{V}(e) &= \dot{e}^T e + e^T \dot{e} \\
 &= (Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X}))^T e \\
 &\quad + e^T (Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X})) \\
 &= e^T A^T e + e^T \Delta A^T(t) e + \tilde{X}^T (\Delta A(t) - \Delta \tilde{A}(t))^T e + \Delta \psi^T(X, \tilde{X}) e + \Psi^T(X, \tilde{X}) e \\
 &\quad + e^T Ae + e^T \Delta A(t) e + e^T (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + e^T \Psi(X, \tilde{X}) + e^T \Delta \psi(X, \tilde{X}) \\
 &= e^T (A^T + A) e + 2e^T \Psi(X, \tilde{X}) + \tilde{X}^T (\Delta A(t) - \Delta \tilde{A}(t))^T e + e^T (\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi^T(X, \tilde{X}) e \\
 &\quad + e^T \Delta \psi(X, \tilde{X}) + e^T \Delta A^T(t) e + e^T \Delta A(t) e \\
 &= e^T (A^T + A + \Delta A^T(t) + \Delta A(t)) e + 2e^T \Psi(X, \tilde{X}) + 2e^T [(\Delta A(t) - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X})] \\
 &\leq e^T (A^T + A + H + H^T + \Delta A(t) + \Delta A^T(t)) e + 2e^T [(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X})] \\
 &\leq \lambda_{\max}(A^T + A + H + H^T + \Delta A(t) + \Delta A^T(t)) V(e) + 2\|e\| \|(\Delta A - \Delta \tilde{A}(t)) \tilde{X} + \Delta \psi(X, \tilde{X})\| \\
 &\leq \lambda_{\max}(A^T + A + H + H^T + \Delta A(t) + \Delta A^T(t)) V(e) + 2\|e\| M_0 \frac{\|e\|}{\varepsilon_0} \\
 &\leq (\lambda_{\max}(A + A^T + H + H^T) + 2\lambda_{\max}(F(t)) \|D\| \|E\|) V(e) + 2M_2 V(e) \\
 &\leq (\lambda_{\max}(A + A^T + H + H^T) + 2\lambda_{\max}(F(t)) \|D\| \|E\| + 2M_2) V(e)
 \end{aligned}$$

The above can be compactly expressed as

$$\dot{V}(e) \leq \lambda_{AH} V(e) \quad \text{for } t > t_1 \quad (7.11)$$

Based on the Corollary 3.1.1 on page 134 in [52], which is

$$V(t, X(t)) \leq \left[V(t_0^+, X_0) \prod_{t_0 < t_k < t} d_k \right] \exp[\lambda(t) - \lambda(t_0)], \quad t \geq t_0,$$

we get

$$V(e(t)) \leq \exp(\lambda_{AH}(t - t_1)) V(e(t_1))$$

□□□

At the impulsive instant, $e(\tau_i^+) = (I + B)e(\tau_i^-)$. Therefore

$$\begin{aligned} V(e(\tau_i^+)) &= e^T(\tau_i^-)(I+B)^T(I+B)e(\tau_i^-) \\ &\leq d_1 V(e(\tau_i^-)) \end{aligned} \quad (7.12)$$

where $d_1 = \lambda_{\max} \{(I+B)^T(I+B)\} < 1$

Theorem 7.1. If the length of the impulsive interval satisfies

$$\Delta_1 < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) \quad (7.13)$$

then $\|e(\tau_i)\| \leq \varepsilon_0$ as $\tau_i \rightarrow \infty$.

Proof: Condition (7.13) implies that

$$d_1 \exp(\lambda_{AH}(\tau_{i+1}^- - \tau_i^+)) < 1 \quad (7.14)$$

To show the results, we consider two cases: $V(e(\tau_i^+)) > \varepsilon_0^2$ and $V(e(\tau_i^+)) \leq \varepsilon_0^2$, respectively.

Case (1) $V(e(\tau_i^+)) > \varepsilon_0^2$

There are two situations in Case (1).

Situation 1. $[\tau_i^+, \tau_{i+1}^-] \subseteq R_2$.

In this situation, applying Lemma 7.1 gives

$$V(e(\tau_{i+1}^-)) \leq \exp(\lambda_{AH}(\tau_{i+1}^- - \tau_i^+))V(e(\tau_i^+))$$

Using (7.12) and (7.14), we have

$$\begin{aligned} V(e(\tau_{i+1}^+)) &\leq d_1 \exp(\lambda_{AH}(\tau_{i+1}^- - \tau_i^+))V(e(\tau_i^+)) \\ &< V(e(\tau_i^+)) \end{aligned}$$

Situation 2. $[\tau_i^+, \tau_{i+1}^-] \not\subseteq R_2$

In this situation, we can show that $V(e(\tau_{i+1}^+)) \leq \varepsilon_0^2$. This can be done by considering two sub-cases:

Sub-Case 1: $\tau_{i+1}^- \in R_1$, i.e., $V(e(\tau_{i+1}^-)) \leq \varepsilon_0^2$

It is obvious that $V(e(\tau_{i+1}^+)) \leq \varepsilon_0^2$ from (7.14).

Sub-Case 2: $\tau_{i+1}^- \in R_2$, i.e. $V(\tau_{i+1}^-) > \varepsilon_0^2$

In this sub-case, there must exist a time instant $t_1 \in [\tau_i^+, \tau_{i+1}^-]$ such that

$$V(e(t_1)) = \varepsilon_0^2 \text{ and } [t_1, \tau_{i+1}^-] \subset R_2$$

Then

$$V(e(\tau_{i+1}^-)) \leq \exp(\lambda_{AH}(\tau_{i+1}^- - t_1))V(e(t_1))$$

$$\leq \exp(\lambda_{AH}(\tau_{i+1}^- - \tau_i^+))\varepsilon_0^2$$

$$V(e(\tau_{i+1}^+)) \leq d_1 \exp(\lambda_{AH}(\tau_{i+1}^- - \tau_i^+))\varepsilon_0^2$$

$$< \varepsilon_0^2$$

Case (2) $V(e(\tau_i^+)) \leq \varepsilon_0^2$

In this case, we can show that $V(e(\tau_{i+1}^+)) \leq \varepsilon_0^2$, similar to Situation 2 of Case (1), by considering $V(\tau_{i+1}^-) > \varepsilon_0^2$ and $V(\tau_{i+1}^-) \leq \varepsilon_0^2$, respectively.

In summary, $V(e(\tau_i^+))$ will be monotonically decreasing when $[\tau_i^+, \tau_{i+1}^-] \subseteq R_2$ from

Situation 1 of Case (1). Otherwise, we have $V(e(\tau_{i+1}^+)) \leq \varepsilon_0^2$. Thus

$$\|e(\tau_i)\| \leq \varepsilon_0 \text{ as } \tau_i \rightarrow \infty.$$

□□□

Remark 7.3: A guideline for choosing the length of impulsive intervals is given in condition (7.13). From this condition, we note that the bound of the interval length depends on the choosing prescribed error bound and system uncertainties as well as mismatch between the two systems. The larger the chosen bound, the longer the impulsive intervals can be allowed. On the other hand, the more uncertain the system parameters and/or the more the mismatch, the shorter the impulsive intervals should be designed. This is consistent with what one expects, but no result has been established to theoretically ensure this so far.

Remark 7.4: If the bounds of parametric uncertainties and mismatch are unavailable, Theorem 7.1 still provides a theoretical basis to ensure that the synchronization error magnitude approaches to a sufficiently small bound if the length of impulsive interval is chosen to be small enough. This implies that all the impulsive schemes have certain degree of robustness. This interpretation is only qualitative. That is, if we choose a very small impulsive interval, we can still achieve the synchronization of the chaotic systems in the presence of parametric uncertainties and mismatch. But it is unclear how small the interval should be, as no guideline is available.

7.4 Illustrative Examples

In this section, we conduct simulation studies on the Lorenz model and Chen's equation to illustrate the effectiveness of the scheme proposed.

Example 7.1

Suppose that the Lorenz model at the driving system and the driven system are perturbed with parametric uncertainties $\Delta\delta(t) = \Delta r(t) = \Delta\eta(t) = \sin t$,

$\Delta\tilde{\delta}(t) = \Delta\tilde{r}(t) = \Delta\tilde{\eta}(t) = \cos t$, i.e.

$$\Delta A(t) = \begin{bmatrix} -\Delta\delta(t) & \Delta\delta(t) & 0 \\ \Delta r(t) & 0 & 0 \\ 0 & 0 & -\Delta\eta(t) \end{bmatrix} = \begin{bmatrix} -\sin t & \sin t & 0 \\ \sin t & 0 & 0 \\ 0 & 0 & -\sin t \end{bmatrix},$$

which can be rewritten in the form of $\Delta A(t) = DF(t)E$, where

$$D = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Delta\tilde{A}(t) = \begin{bmatrix} -\Delta\tilde{\delta}(t) & \Delta\tilde{\delta}(t) & 0 \\ \Delta\tilde{r}(t) & 0 & 0 \\ 0 & 0 & -\Delta\tilde{\eta}(t) \end{bmatrix} = \begin{bmatrix} -\cos t & \cos t & 0 \\ \cos t & 0 & 0 \\ 0 & 0 & -\cos t \end{bmatrix}$$

Then the bounding parameters in Assumption 7.1 can be chosen as $a_1 = a_2 = a_4 = a_9 = 1$,

$b_1 = b_2 = b_4 = b_9 = 1.414$.

For simulation, the parameter and initial conditions are chosen as follows:

$\varepsilon_0 = 0.01, \delta = 10, r = 28, \eta = \frac{8}{3}, M_a = M_b = 50, X(0) = [27, 5, 2]^T$ and $\tilde{X}(0) = [5, 3, 5]^T$.

Matrix B is chosen to be $\begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix}$.

Clearly, $d_1 > \lambda_{\max} \{(I + B)^T (I + B)\} = 0.09$, $M_0 = 141.4214$, $M_2 = \frac{M_0}{\varepsilon_0} = 1.4142 \times 10^4$,

$\lambda_{AH} = 2.8386 \times 10^4$. The upper bound of the impulsive intervals is calculated by

$$\Delta_1 < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 8.4828 \times 10^{-5}$$

We choose $\Delta_1 = 8 \times 10^{-5}$ in the simulation. Simulation results are illustrated in Figure

7.1 and Figure 7.2. It is computed that $\|e(t)\| = 0.0072 < \varepsilon_0$ when $t = 4.6 \times 10^{-4}$ second.

From Figure 7.2, we can see that $\|e(t)\| < 0.01$ for all $t \geq 4.0 \times 10^{-4}$ second.

Figure 7.1: $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.01$)

Figure 7.2: $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.01$, Close-up View)

Example 7.2

For the purpose of comparison, the scheme without considering parametric uncertainties and mismatches in [6] is applied to the systems in Example 7.1. The upper bound of the impulsive intervals using their guideline is calculated as below:

$$\Delta_1 < -\frac{\ln(\xi d_1)}{\lambda_{\max}(A + A^T) + 2M_a} = 1.8727 \times 10^{-2} \quad \text{where } \xi = 1.01$$

We choose $\Delta_1 = 1.8 \times 10^{-2}$ in our simulation studies, with results presented in Figure 7.3 and Figure 7.4. Obviously, it is uncertain what range the synchronization error magnitude approaches to since their guideline of choosing impulsive intervals has no quantification and no guarantee on the bound of the synchronization errors in the presence of parametric uncertainties and mismatch.

Figure 7.3: $\|e(t)\|$ of Example 7.2 for Lorenz Model

Figure 7.4: $\|e(t)\|$ of Example 7.2 for Lorenz Model (Close-up View)

Example 7.3

In this example, we consider the same system as in Example 7.1 again, except changing the prescribed error bound to $\varepsilon_0 = 0.1$. In this case,

$$M_2 = \frac{M_0}{\varepsilon_0} = 1414.2136, \lambda_{AH} = 2930.4251.$$

The upper bound of the impulsive intervals is calculated by

$$\Delta_1 < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 9.0653 \times 10^{-4}$$

We choose $\Delta_1 = 9 \times 10^{-4}$ in the simulation. It is computed that $\|e(t)\| = 0.0792 < \varepsilon_0$ when $t = 2.74 \times 10^{-3}$ second. The simulation results are given in Fig. 5 and Fig. 6. It is noted that $\|e(t)\| < 0.1$ for $t \geq 0.00274$ second. But the response is slower, compared with Example 7.1 as expected.

Figure 7.5: $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.1$)

Figure 7.6: $\|e(t)\|$ of Lorenz Model ($\varepsilon_0 = 0.1$, Close-up View)

Example 7.4:

Choose the parameters of Chen's equation as $a = 35$, $b = 3$, $c = 28$. Suppose that Chen's equation at the driving system and the driven system are perturbed with parametric uncertainties

$$\Delta a(t) = \Delta b(t) = \Delta c(t) = 0.2 \sin t, \quad \Delta \tilde{a}(t) = \Delta \tilde{b}(t) = \Delta \tilde{c}(t) = 0.2 \cos t, \quad \text{i.e.}$$

$$\Delta A(t) = \begin{bmatrix} -\Delta a(t) & \Delta a(t) & 0 \\ \Delta c(t) - \Delta a(t) & \Delta c(t) & 0 \\ 0 & 0 & -\Delta b(t) \end{bmatrix} = \begin{bmatrix} -0.2 \sin t & 0.2 \sin t & 0 \\ 0 & 0.2 \sin t & 0 \\ 0 & 0 & -0.2 \sin t \end{bmatrix},$$

and rewrites $\Delta A(t)$ in the form of $\Delta A(t) = DF(t)E$ with

$$D = \begin{bmatrix} -0.2 & 0.2 & 0 \\ 0 & 0.2 & 0 \\ 0 & 0 & -0.2 \end{bmatrix}, \quad F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, \quad E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\Delta \tilde{A} = \begin{bmatrix} -\Delta \tilde{a}(t) & \Delta \tilde{a}(t) & 0 \\ \Delta \tilde{c}(t) - \Delta \tilde{a}(t) & \Delta \tilde{c}(t) & 0 \\ 0 & 0 & -\Delta \tilde{b}(t) \end{bmatrix} = \begin{bmatrix} -0.2 \cos t & 0.2 \cos t & 0 \\ 0 & -0.2 \cos t & 0 \\ 0 & 0 & -0.2 \cos t \end{bmatrix}$$

Then the bounding parameters in Assumption 7.1 can be chosen as

$$a_1 = a_2 = a_4 = a_9 = 0.2, \quad b_1 = b_2 = b_4 = b_9 = \sqrt{2}/5.$$

For simulation, the parameter and initial conditions are chosen as follows:

$$\varepsilon_0 = 0.01, \quad M_a = M_b = 50, \quad X(0) = [0.5, 1, 5]^T \text{ and } \tilde{X}(0) = [10.5, 20, 38]^T.$$

$$\text{Matrix } B \text{ is chosen as } B = \begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix}. \text{ Then } d_1 > \lambda_{\max} \{ (I + B)^T (I + B) \} = 0.09,$$

$$M_0 = 28.2843, \quad M_2 = \frac{M_0}{\varepsilon_0} = 2828.4271, \quad \lambda_{AH} = 5789.5069. \text{ From (13), the upper bounds}$$

of the impulsive intervals are calculated by

$$\Delta_1 < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 4.1592 \times 10^{-4}$$

We choose $\Delta_1 = 4 \times 10^{-4}$ in the simulation. It is computed that $\|e(t)\| = 8.1832 \times 10^{-3} < \varepsilon_0$

when $t = 2.88 \times 10^{-3}$ second. The experimental results are illustrated in Figure 7.7 and

Figure 7.8.

Figure 7.7: $\|e(t)\|$ of Chen's Equation ($\varepsilon_0 = 0.01$)

Figure 7.8: $\|e(t)\|$ of Chen's Equation ($\varepsilon_0 = 0.01$, Close-up View)

It clearly observed from the Figure 7.8 that $\|e(t)\| < 0.01$ for $t \geq 2.88 \times 10^{-3}$ second.

From our verification, results of both examples illustrate that the magnitude of synchronization errors will rapidly converge to and stay within the pre-specified error bounds.

7.5 Concluding Remark

In this chapter, a purely impulsive scheme to synchronize two chaotic systems in the presence of uncertain parametric uncertainties and parametric mismatch between the two systems is presented. A guideline is obtained for the choice of impulsive interval lengths. Theoretical analysis shows that, under the derived guideline, the synchronization error is guaranteed to approach to and stay within a prescribed bound, which can be arbitrarily small. As expected, the smaller the bound, the more frequent transmission of impulses will be required. Simulation results on a Lorenz model and a Chen's system also verify the effectiveness of this method. With the result, practical applicability of impulsive synchronization schemes, including the development of secure communication strategies, now has a theoretical basis and is thus firmly assured.

Chapter 8

Application Examples of Chaotic Secure Communication System

Chaos-based secure communication has received great attentions from researchers since the discovery of the synchronization of two chaotic systems. Usually, the parameters of the actual implemented system will deviate from their designed values due to many practical factors. This causes parametric uncertainties and mismatches between the two chaotic systems. In most of existing schemes with pure impulsive synchronization, these uncertainties and mismatches are not taken into consideration in

the design and thus signals may not be recovered accurately if the difference between the original signal and the recovered signal is large enough that the recovered signal can not be recognized. In this chapter, we will apply a recently developed synchronization scheme in [78] to design a secure communication system with uncertainties and mismatches allowed. Designers can specify certain tolerance bounds for these uncertainties and mismatches. Based on these bounds and a pre-specified bound of the synchronization error, a scheme is given to determine an upper bound of impulsive intervals. With the scheme, the synchronization error is ensured to approach to and stay within the given pre-specified bound and this in turn guarantees that signals can be decoded accurately. To further enhance system security, it is also proposed to transmit functions of the chaotic states at impulsive instants, instead of the states directly. The designed system is tested and verified with text, audio and image encryption and transmission with comparisons to some existing schemes.

8.1 Introduction of Chaotic Cryptosystems

Chaotic signals generated by chaotic systems are unpredictable, sensitive to initial conditions and system parameters, and have a continuous broadband spectrum. The random noise-like properties and the discovery of the synchronization of chaotic systems make chaotic signals applicable to secure communication systems, including chaotic encryption and chaotic spreading codes for multi-user access in spread spectrum systems. In a typical chaotic secure communication system as shown in Figure 8.1 [13], a typical chaotic cryptosystem is often used. With a suitable

cryptographic scheme, the original signal is hidden in the noise-like chaotic signals. The cryptosystem is composed of two main parts, the encrypter and the decrypter. Each part includes a chaotic system, called driving and driven system respectively. Synchronizing the two chaotic systems is an essential problem to be addressed in order to recover the message from the receiver side.

A variety of schemes have been proposed to synchronize two chaotic systems, see for examples[6,9,10,13,51,55,70,79]. These schemes are obtained under some strong assumptions that the parameters of chaotic systems are time invariant and these parameters should be identical for both chaotic systems, in order to ensure perfect synchronization. In practical situations, these assumptions are difficult to be met because the designed chaotic systems cannot be perfectly implemented and the chaotic systems are inevitably exposed to an environment which may cause their parameters varying within a small range. Thus robust schemes against parametric uncertainties and mismatches are needed for them to be applied in secure communications. Wen *et al.* [71] proposed a robust scheme to design a controller in the driven system to achieve perfect synchronization. However, it is required to transmit the state variables of the driving system to the driven system continuously by the robust scheme. Therefore the security level of the system is decreased if the scheme is applied to secure communication. Recently, an impulsive synchronization scheme was proposed to relax this requirement by Wen *et al.* [78]. Meanwhile, an upper bound of impulsive interval lengths is quantitatively established as a function of a pre-specified bound of the

synchronization error and the bounds of parametric uncertainty and mismatch. This gives a clear guideline on the choice of impulsive intervals. With the scheme, the magnitude of the synchronization error is theoretically ensured to approach to and stay within the pre-specified bound, which can be chosen arbitrarily small.

In this chapter, we will apply the scheme in [78] to design a chaos based secure communication system. In the proposed scheme, designers are allowed to specify certain tolerance bounds for parametric uncertainties and mismatches. These bounds and a pre-specified bound will be used to select impulsive intervals. With the designed system and impulsive intervals, the message recovering error is shown to be within a bound depending on the pre-specified synchronization error bound and transmitted signals can be decoded accurately even in the presence of uncertainties and mismatches. In the encrypter, we also propose to add a new module to convert the system states to their functions for transmission at impulsive instants, while in the decrypter a module which converts the functions to states is also introduced. These functions, i.e. $h(X)$ and $h^{-1}(X)$ in Figure 8.1, can be changed from time to time and are unknown to public. In this way, the states of the chaotic driving system are not transmitted through the channel even at impulsive instants. This clearly further enhances the security level. The designed system is tested by transmitting text, sound and image signals. Comparisons are also made with well-established schemes reported in [55] and [6]. The test results show that the designed system works effectively in transmitting these signals.

The remaining of this chapter is organized as follows. In Section 8.2, the design of several important modules of the system and how to choose impulsive intervals are presented. The system is applied to text encryption, audio encryption and image encryption and transmission in Section 8.3 to 8.5, respectively. Simulation results illustrate the effectiveness of the proposed schemes.

Figure 8.1: System block diagram of chaotic cryptosystem

8.2 System Design and Selection Scheme of Impulsive Intervals

Before presenting the structure of the proposed system and the selection of impulsive intervals, we briefly describe how the system operates.

As shown in Figure 8.1, the digitized plaintext $p(n)$ of the original signal and the running key sequence $k(n)$, a function of the chaotic states from the magnifying glass, are fed into the cryptographic scheme $e(\bullet)$ to generate the ciphertext $c(n)$. Then $c(n)$ is composed with the sequence $h(X(\tau_i)), i = 1, 2, \dots$, a vector of functions of chaotic states in composition block, and sent to the receiver side. The composed message will be decomposed in the decomposition block. The inverse function $h^{-1}(X(\tau_i)), i = 1, 2, \dots$ will generate impulsive sequences $X(\tau_i)$ to synchronize the driven chaotic system with the driving system so that the synchronization error is ensured to be within a pre-specified bound. The only condition of choosing function $h(\cdot)$ is that it has an inverse. The function $h(X)$ and $h^{-1}(X)$ can be changed from time to time and are unknown to public. With the use of such functions, the states of the chaotic driving system are not transmitted through the public channel and therefore the system security level is further enhanced. The decrypter reproduces the running-key sequence $\tilde{k}(n)$. If $\tilde{k}(n)$ is the same as or close to $k(n)$, the original signal can be recovered from $c(n)$ at the output of the receiver. Clearly, it is crucial that the impulsive intervals should be chosen in such a way that $\|X - \tilde{X}\|$ is small enough to ensure $|k - \tilde{k}|$ small. The chaotic systems are also allowed to have certain parametric uncertainty and mismatches satisfying certain given bounds.

8.2.1 Design of Chaotic Systems

The two chaotic systems are designed to be identical as in the following models.

The driving system is in the form of

$$\dot{X} = AX + \psi(X) \quad (8.1)$$

and the driven system is by described by

$$\begin{cases} \dot{\tilde{X}} = A\tilde{X} + \psi(\tilde{X}) & t \neq \tau_i \\ \Delta\tilde{X}|_{t=\tau_i} = -Be, & i = 1, 2, \dots \end{cases} \quad (8.2)$$

where $X = [x, y, z]^T$ and $\tilde{X} = [\tilde{x}, \tilde{y}, \tilde{z}]^T$ are the state vectors of the two systems

respectively, $A \in R^{3 \times 3}$ is a constant matrix, B is a 3×3 constant matrix satisfying the

condition that $\lambda_{\max} \{ (I + B)^T (I + B) \} < 1$ with $\lambda_{\max} \{ \cdot \}$ denoting the maximum eigenvalue

and $e = (e_x, e_y, e_z)^T = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})^T$ is the *synchronization error*,

$\Delta\tilde{X}|_{t=\tau_i} = \tilde{X}(\tau_i^+) - \tilde{X}(\tau_i^-)$, $\psi(\cdot)$ denotes nonlinear part of the chaotic systems which are

selected according to the following structure:

$$\psi(\square) = [\theta_1^T \phi_1(\square), \theta_2^T \phi_2(\square), \theta_3^T \phi_3(\square)]^T$$

where θ_i^T is a vector of design parameters $\theta_i^T = [\theta_{i1}, \theta_{i2}, \theta_{i3}]$ and ϕ_i^T is a vector of given

functions $\phi_i^T(\square) = [\phi_{i1}(\square), \phi_{i2}(\square), \phi_{i3}(\square)]$, $i = 1, 2, 3$.

Matrix A and function $\psi(\cdot)$ are chosen to satisfy the following two conditions:

- 1) The states of the two chaotic systems as well as the nonlinear parts (8.1) and (8.2) are bounded as follows:

$$\sup |x, y, z| = M_a, \sup |\tilde{x}, \tilde{y}, \tilde{z}| = M_b$$

$$\sup \{\|\phi_1(X)\|, \|\phi_2(X)\|, \|\phi_3(X)\|\} = M_c, \sup \{\|\phi_1(\tilde{X})\|, \|\phi_2(\tilde{X})\|, \|\phi_3(\tilde{X})\|\} = M_d$$

for some known constants M_a, M_b, M_c and M_d .

- 2) There exists a constant matrix H such that:

$$2(X - \tilde{X})^T (\psi(X) - \psi(\tilde{X})) \leq (X - \tilde{X})^T (H + H^T) (X - \tilde{X}) \quad (8.3)$$

For the purpose of practical applications, the actual parameters implemented A and vectors θ_i are allowed to have certain deviations from their designed values and we call these deviations as uncertainties. They may be time varying and different for the two chaotic systems. These differences admit certain parametric mismatches between the two systems. We use $\Delta A(t)$ and $\Delta \psi(X)$, $\Delta \tilde{A}(t)$ and $\Delta \tilde{\psi}(\tilde{X})$ to denote such uncertainties in the driving and driven systems, respectively. Suppose that

$$\Delta A(t) = \begin{bmatrix} \Delta A_1(t) & \Delta A_2(t) & \Delta A_3(t) \\ \Delta A_4(t) & \Delta A_5(t) & \Delta A_6(t) \\ \Delta A_7(t) & \Delta A_8(t) & \Delta A_9(t) \end{bmatrix}, \quad \Delta \tilde{A}(t) = \begin{bmatrix} \Delta \tilde{A}_1(t) & \Delta \tilde{A}_2(t) & \Delta \tilde{A}_3(t) \\ \Delta \tilde{A}_4(t) & \Delta \tilde{A}_5(t) & \Delta \tilde{A}_6(t) \\ \Delta \tilde{A}_7(t) & \Delta \tilde{A}_8(t) & \Delta \tilde{A}_9(t) \end{bmatrix},$$

$$\Delta \psi(X) = [\Delta \theta_1^T \phi_1(X), \Delta \theta_2^T \phi_2(X), \Delta \theta_3^T \phi_3(X)]^T,$$

$$\Delta \tilde{\psi}(\tilde{X}) = [\Delta \tilde{\theta}_1^T \phi_1(\tilde{X}), \Delta \tilde{\theta}_2^T \phi_2(\tilde{X}), \Delta \tilde{\theta}_3^T \phi_3(\tilde{X})]^T$$

where

$$\Delta\theta_i^T = [\Delta\theta_{i1}, \Delta\theta_{i2}, \Delta\theta_{i3}], \Delta\tilde{\theta}_i^T = [\Delta\tilde{\theta}_{i1}, \Delta\tilde{\theta}_{i2}, \Delta\tilde{\theta}_{i3}], i=1,2,3.$$

These uncertainties and mismatches are permitted to satisfy

$$\begin{aligned} |\Delta A_i(t)| &\leq a_i, |\Delta A_i(t) - \Delta\tilde{A}_i(t)| \leq b_i, \quad i=1-9 \\ \|\Delta\theta_i\| &\leq c_i, \|\Delta\theta_i - \Delta\tilde{\theta}_i\| \leq g_i, \quad i=1,2,3 \end{aligned}$$

for some given constants a_i , b_i , c_i and g_i , where $\|\cdot\|$ denotes the Euclidean norm. These bound will be used in the selection of impulsive intervals.

We also suppose that ΔA can be written as $\Delta A = DF(t)E$ for a diagonal matrix $F(t)$ and some constant matrices D and E .

As an example, we can use the Lorenz model to design the two systems

In the Lorenz model,

$$A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -\eta \end{bmatrix}, \quad \psi(X) = \begin{bmatrix} 0 & -xz & xy \end{bmatrix}^T.$$

The uncertainties will be $\Delta\sigma, \Delta r$ and $\Delta\eta$ or $\Delta\tilde{\sigma}, \Delta\tilde{r}$ and $\Delta\tilde{\eta}$ associated with the implementation of parameters σ, r and η in the driving and driven systems, respectively. They may be allowed to satisfy the following bounds:

$$\begin{aligned} |\Delta\sigma(t)| &\leq a_\sigma, |\Delta r(t)| \leq a_r, \text{ and } |\Delta\eta(t)| \leq a_\eta, \text{ and} \\ |\Delta\sigma(t) - \Delta\tilde{\sigma}(t)| &\leq b_\sigma, |\Delta r(t) - \Delta\tilde{r}(t)| \leq b_r, |\Delta\eta(t) - \Delta\tilde{\eta}(t)| \leq b_\eta \text{ for some given constants} \end{aligned}$$

$a_\sigma, a_r, a_\eta, b_\sigma, b_\eta$. Also $\Delta\psi(X)=0$ and $\Delta\tilde{\psi}(\tilde{X})=0$ in this case. It can also be noted that the H matrix satisfying (8.3) can be selected as

$$H = \begin{bmatrix} \sqrt{2}M_a/2 & 0 & 0 \\ 0 & \sqrt{2}M_a/2 & 0 \\ 0 & 0 & \sqrt{2}M_a/2 \end{bmatrix} \quad (8.4)$$

8.2.2 Selection of the Impulsive Intervals

Time sequence $\{\tau_i : i = 1, 2, \dots\}$ denotes the time instants at which impulses $h(X(\tau_i))$ are sent to the driven system. We define

$$T = \sup_i \{\tau_{i+1} - \tau_i\} < \infty \quad (8.5)$$

Denote $\Psi(X, \tilde{X}) = \psi(X) - \psi(\tilde{X})$ and $\Delta\psi(X, \tilde{X}) = \Delta\psi(X) - \Delta\psi(\tilde{X})$.

Then the error system can be obtained based on (8.1), (8.2) and the uncertainties discussed in Section 8.2.1

$$\begin{cases} \dot{e} = Ae + \Delta A(t)e + \Psi(X, \tilde{X}) + (\Delta A(t) - \Delta\tilde{A}(t))\tilde{X} + \Delta\psi(X, \tilde{X}), & t \neq \tau_i \\ \Delta e|_{t=\tau_i} = Be, & i = 1, 2, \dots \end{cases} \quad (8.6)$$

Denote

$$\begin{aligned} M_0 = M_b & \sqrt{(b_1^2 + b_2^2 + b_3^2) + (b_4^2 + b_5^2 + b_6^2) + (b_7^2 + b_8^2 + b_9^2)} \\ & + (M_c + M_d) \sqrt{(c_1^2 + c_2^2 + c_3^2)} + M_d \sqrt{(g_1^2 + g_2^2 + g_3^2)} \end{aligned} \quad (8.7)$$

A pre-specified bound of the synchronization error, denoted as ε_0 , is chosen. Define

$M_2 = \frac{M_0}{\varepsilon_0}$. Then based on (8.6) and the scheme presented in [78], the length of

impulsive intervals can be determined according to the following guidelines:

$$T < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) \quad (8.8)$$

where $d_1 > \lambda_{\max}((I+B)^T(I+B))$

$$\lambda_{AH} = \lambda_{\max}(A+A^T+H+H^T) + 2\lambda_{\max}(F(t))\|D\|\|E\| + 2M_2 \quad (8.9)$$

From (8.6) and (8.8) and the proof given in [78], it can be shown that

$$\|e(t)\| \leq \varepsilon_0, \quad \forall t \geq T_N \text{ where } T_N \text{ is a sufficiently large constant.}$$

8.2.3 Design of the Key Sequences and Encryption Scheme

In order for the plaintext to be decoded with acceptable accuracy, the key sequence in the encrypter should be close to the key sequence in the decrypter. In other words,

$|k(n) - \tilde{k}(n)|$ should be small. One design scheme for the key sequences is given below:

$$\begin{aligned} k(n) &= \left\lfloor \left\lceil K \cdot (x^2(n) + y^2(n) + z^2(n))^{1/2} \right\rceil \right\rfloor \bmod N_\alpha \\ \tilde{k}(n) &= \left\lfloor \left\lceil K \cdot (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2} \right\rceil \right\rfloor \bmod N_\alpha \end{aligned}$$

where $\left\lfloor \cdot \right\rfloor$ is a function rounding off a number to ρ decimal places, N_α and ρ are integers, K is a constant representing the magnifying glass. The larger the K is, the more sensitivity to parameter mismatch of the cryptosystem. Then

$$\begin{aligned}
 |k(n) - \tilde{k}(n)| &= \left| \left\lfloor K \cdot (x^2(n) + y^2(n) + z^2(n))^{1/2} \right\rfloor \bmod N_\alpha - \left\lfloor K \cdot (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2} \right\rfloor \bmod N_\alpha \right| \\
 &\leq \left| \left\lfloor K \cdot ((x^2(n) + y^2(n) + z^2(n))^{1/2} - (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2}) \right\rfloor \bmod N_\alpha \right| + 10^{-\rho} \\
 &= \left| (K \cdot (\|X\| - \|\tilde{X}\|)) \bmod N_\alpha \right| + 10^{-\rho} \\
 &\leq (K \cdot (\|X - \tilde{X}\|)) \bmod N_\alpha + 10^{-\rho} \\
 &\leq (K \cdot \varepsilon_0) \bmod N_\alpha + 10^{-\rho}
 \end{aligned}$$

Clearly, the error not only depends on the bound ε_0 of the synchronization error, but also the magnifying glass K and the choice of integer ρ . Thus, the error will not be zero even if the two chaotic systems are perfectly synchronized. This implies that prefect synchronization may not be necessary in practice, due to the presence of round off errors and errors caused by other sources such as quantization.

Next we design the encryption scheme. One possible choice is

$$c(n) = e(p(n), k(n)) = p(n) + k(n)$$

The decryption scheme is designed as

$$\tilde{p}(n) = d(c(n), \tilde{k}(n)) = c(n) - \tilde{k}(n)$$

Then the message recovering error $|\tilde{p}(n) - p(n)|$ satisfies

$$|\tilde{p}(n) - p(n)| = |c(n) - \tilde{k}(n) - (c(n) - k(n))| = |k(n) - \tilde{k}(n)| \leq (K \cdot \varepsilon_0) \bmod N_\alpha + 10^{-\rho}$$

Note that there may be other available approaches for the design of key sequences, the encryption scheme and the decryption scheme.

In order to verify the effectiveness of the entire designed system, we consider the transmission of text, sound and image messages in the following sections.

8.3 Text Encryption and Transmission

In this section, test our design scheme by transmitting text message. Comparison is also made with an impulsive selection scheme given in [55].

8.3.1 Design of Chaotic Systems

The Chen's system [41] can be used to design the two chaotic systems. In this case,

$$A = \begin{bmatrix} -a & a & 0 \\ c-a & c & 0 \\ 0 & 0 & -b \end{bmatrix}, \quad \psi(X) = [0 \quad -xz \quad xy]^T \quad \text{where } a, b \text{ and } c \text{ are parameters of}$$

Chen's equation. Clearly the system satisfies the two conditions in Section 8.2 with H given in (8.4).

The uncertainties will be $\Delta a, \Delta b$ and Δc or $\Delta \tilde{a}, \Delta \tilde{b}$ and $\Delta \tilde{c}$ caused by the implementation of parameters a, b and c in the driving and driven systems, respectively. They may be allowed to satisfy the following bounds:

$$|\Delta a(t)| \leq a_a \quad |\Delta b(t)| \leq a_b \quad \text{and} \quad |\Delta c(t)| \leq a_c, \quad \text{and}$$

$|\Delta a(t) - \Delta \tilde{a}| \leq b_a$, $|\Delta b(t) - \Delta \tilde{b}| \leq b_b$, $|\Delta c(t) - \Delta \tilde{c}| \leq b_c$ for some given constants a_a, a_b, a_c , b_a, b_b, b_c . Also $\Delta \psi(X) = 0$ and $\Delta \tilde{\psi}(\tilde{X}) = 0$.

For the purpose of illustration, we choose $a = 35$, $b = 3$, $c = 28$, $X(0) = [0.5, 1, 5]^T$ and $\tilde{X}(0) = [10.5, 20, 38]^T$. With such choices, $M_a = M_b = 50$. Also the bounds of the parametric uncertainty and mismatch are given as $a_a = a_b = a_c = 0.2$ and $b_a = b_b = b_c = \sqrt{2}/5$, respectively. In the simulation studies, we choose $\Delta a = \Delta b = \Delta c = 0.2 \sin t$, $\Delta \tilde{a} = \Delta \tilde{b} = \Delta \tilde{c} = 0.2 \cos t$. Then

$$\Delta A = \begin{bmatrix} -\Delta a(t) & \Delta a(t) & 0 \\ \Delta c(t) - \Delta a(t) & \Delta c(t) & 0 \\ 0 & 0 & -\Delta b(t) \end{bmatrix} = \begin{bmatrix} -0.2 \sin t & 0.2 \sin t & 0 \\ 0 & -0.2 \sin t & 0 \\ 0 & 0 & -0.2 \sin t \end{bmatrix}.$$

which can be rewritten in the form of $\Delta A(t) = DF(t)E$, where

$$D = \begin{bmatrix} -0.2 & 0.2 & 0 \\ 0 & 0.2 & 0 \\ 0 & 0 & -0.2 \end{bmatrix}, F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We choose matrix B as $B = \begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix}$ for the driven system.

8.3.2 Selection of Impulsive Intervals

Choose a synchronization error bound ε_0 , e.g. $\varepsilon_0 = 0.01$. From (8.7), $M_0 = 28.2843$.

Then $M_2 = \frac{M_0}{\varepsilon_0} = 2828.4271$. It can be computed from (8.9) that $\lambda_{AH} = 5789.5069$ and

$d_1 > \lambda_{\max}((I + B)^T(I + B)) = 0.09$. Then from (8.8), the upper bound of the impulsive intervals is calculated as

$$T < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 4.1592 \times 10^{-4}$$

We choose $T = 4 \times 10^{-4}$ in the simulation.

8.3.3 Simulation Studies and Results

Since we use digital transmission scheme, the analog signals are firstly sampled and quantized to convert into digital signals. We choose sampling period as 10^{-5} second and the quantization value as 5×10^{-8} . Therefore the sampled chaotic signals are

$X(n) = X(t) \sum_{n=0}^{+\infty} \delta(t - nT)$. The original signal is in text form and can be converted to

standard ASCII 128 code format. Then it is used as plaintext in the encrytion process.

The encrytion scheme is

$$c(n) = e(p(n), k(n)) = p(n) + k(n)$$

where $k(n) = \llbracket K \cdot (x^2(n) + y^2(n) + z^2(n))^{1/2} \rrbracket \bmod 128$ which is a combination of all three state variables of the chaotic system,. To enhance the sensitivity to parameter mismatch, we choose a large number $K = 10$ for the magnifying glass. In the decrypter, the running key sequence is $\tilde{k}(n) = \llbracket K \cdot (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2} \rrbracket \bmod 128$ and the plaintext can be recovered via $\tilde{p}(n) = d(c(n), \tilde{k}(n)) = \lfloor c(n) - \tilde{k}(n) \rfloor$

where $\lfloor \cdot \rfloor$ is a function rounding off a number to its nearest integers. The reason to use this round off function is that the recovery of the text needs the plaintext to be integers.

Function $h(X)$ is chosen as $h(X) = (X_1^{1/3}, X_2^{1/3}, X_3^{1/3})^T$ and thus the corresponding

$h^{-1}(X)$ in the decrypter is given by $h^{-1}(X) = (X_1^3, X_2^3, X_3^3)^T$.

In our test, the original plaintext is:

Your friendship is a precious treasure. I want to thank you for being a part of my life. I know I can count on you in difficult times. I know that I can share with you happy moments, and I also know that our friendship is based on mutual love. Your friendship is very special gift; I would not be able to thank you enough for it...

Decoded plaintext is:

Your friendship is a precious treasure. I want to thank you for being a part of my life. I know I can count on you in difficult times. I know that I can share with you happy moments, and I also know that our friendship is based on mutual love. Your friendship

is very special gift; I would not be able to thank you enough for it...

As a comparison, we consider the scheme in [55] to compute an upper bound of the impulsive intervals, where parametric uncertainty and mismatches are not taken into account. With the scheme, it is found that the upper bound needs to satisfy

$$T < -\frac{\ln(\xi d_1)}{\lambda_{\max}(A + A^T) + 2M_a} = 1.4808 \times 10^{-2} \quad \text{where } \xi = 1.01$$

Then we choose $T = 1.4 \times 10^{-2}$ in the simulation. The recovered plaintext is

† &<;i/; ,'-:! 9i :i(i9;,* &<:i=;;(:<;gi r h?)&<h<'h<)&#h1'=h.':h*-&/h)h8):<h'.h%lh\$!.-
fh r h#%\$<k k(*%k(\$>%?k\$%k2\$>k"%k/"--"(>?k?"&.8ek k
%\$<k?">j j)+\$j9"+8/j=#>"j3%?j"+::3j"/\$>9fj+\$j j+&9%j!\$":m9%,9m"8?m+?\$(>#>%\$=
m\$>m/,>)m"#m 898,!m!";(cm¶ "8?l*>%)")(\$%<l%?l:)>5l?<)/%- l+%*8wl | 1;#9 (l"#8l.)l-.)o;
o;.!\$o6 :o*! :(o)=o&;aaa

Clearly, the plaintext is not recovered satisfactorily.

8.4 Speech Encryption and Transmission

Similar to text encryption, we use continuous chaotic signal as running key sequence in the cryptosystem.

8.4.1 Design of Chaotic Systems

As an alternative to the chaotic systems in Section 8.3, we use the Lorenz model described in Section 8.2 to implement the two chaotic systems.

We choose $\delta = 10$, $r = 28$, $\eta = \frac{8}{3}$, $X(0) = [27, 5, 2]^T$ and $\tilde{X}(0) = [5, 3, 5]^T$. Then

$M_a = M_b = 50$. The bounds of the parametric uncertainty and mismatches are chosen as $a_\delta = a_r = a_\eta = 1$ and $b_\delta = b_r = b_\eta = \sqrt{2}$, respectively. In the simulation studies, we set

$\Delta\delta(t) = \Delta r(t) = \Delta\eta(t) = \sin t$, $\Delta\tilde{\delta}(t) = \Delta\tilde{r}(t) = \Delta\tilde{\eta}(t) = \cos t$ and this gives that

$$\Delta A(t) = \begin{bmatrix} -\Delta\delta(t) & \Delta\delta(t) & 0 \\ \Delta r(t) & 0 & 0 \\ 0 & 0 & -\Delta\eta(t) \end{bmatrix} = \begin{bmatrix} -\sin t & \sin t & 0 \\ \sin t & 0 & 0 \\ 0 & 0 & -\sin t \end{bmatrix}, \text{ which can be rewritten in}$$

the form of $\Delta A(t) = DF(t)E$,

$$\text{where } D = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{Matrix } B \text{ is } B = \begin{bmatrix} -0.9 & 0 & 0 \\ 0 & -0.8 & 0 \\ 0 & 0 & -0.7 \end{bmatrix} \text{ for the driven system.}$$

8.4.2 Selection of Impulsive Intervals

The synchronization error bound ε_0 is also set as $\varepsilon_0 = 0.01$. From (8.7),

$M_0 = 141.4214$. Then $M_2 = \frac{M_0}{\varepsilon_0} = 1.4142 \times 10^4$. It can be computed from (8.9) that

$\lambda_{AH} = 2.8386 \times 10^4$ and $d_1 > \lambda_{\max}((I+B)^T(I+B)) = 0.09$. Then from (8.8), the upper bound of the impulsive intervals is

$$T < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 8.4828 \times 10^{-5}$$

We choose $T = 8 \times 10^{-5}$ in the simulation.

8.4.3 Simulation Studies and Results

We choose sampling period as 10^{-5} second and the quantization value as 5×10^{-8} . Let $K = 100$. Since the amplitude of the speech signal is much smaller than the chaotic running key sequence, the stream cipher encryption function is chosen as

$$c(n) = e(p(n), k(n)) = p(n) \times 1000 + k(n)$$

where $k(n) = (K \cdot (x^2(n) + y^2(n) + z^2(n))^{1/2}) \bmod 128$ and $p(n)$ is the plaintext.

In the decrypter, the plaintext is recovered through

$$\tilde{k}(n) = (K \cdot (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2}) \bmod 128$$

$$\tilde{p}(n) = D(c(n), \tilde{k}(n)) = (c(n) - \tilde{k}(n)) / 1000$$

With $h(X) = (X_1^{1/3}, X_2^{1/3}, X_3^{1/3})^T$, $h^{-1}(X) = (X_1^3, X_2^3, X_3^3)^T$.

We use a wave sound file named “applause” from Microsoft Office 2000 as the original signal. Its audio sample rate is 8Khz and its bit rate is 64kbps. Figure 8.2

shows the original signal, while Figure 8.3 presents the recovered signal and Figure 8.4 gives the difference between the two signals.

Figure 8.2: The original audio signal

Figure 8.3: The recovered audio signal

Figure 8.4: The difference between the recovered and the original audio signals

As a comparison, we now apply the scheme in [6] to compute an upper bound of the impulsive intervals

$$T < -\frac{\ln(\xi d_1)}{\lambda_{\max}(A + A^T) + 2M_a} = 1.8727 \times 10^{-2} \quad \text{where } \xi = 1.01.$$

We choose $T = 1.8 \times 10^{-2}$ in the simulation. The recovered audio signal is shown in Figure 8.5 and the difference between the recovered audio signal and the original audio signal is shown in Figure 8.6.

It is easy to see from the simulation that the recovered audio signal with our scheme gives much better result as the difference between the recovered and original audio signals is insignificant compared with the results using the impulsive scheme in [6].

Figure 8.5: The recovered audio signal with the impulsive scheme in [6]

Figure 8.6: The difference between the recovered and original audio signals with the impulsive scheme in [6]

8.5 Image Encryption and Transmission

8.5.1 Design of Chaotic Systems and Selection of Impulsive Intervals

We use the Lorenz model described in Section 8.2 to implement the driving chaotic system and driven chaotic system with the following parameters and initial conditions

$$\delta = 16, r = 45.92, \eta = 4, X(0) = [20, 8, 3]^T \text{ and } \tilde{X}(0) = [6, 15, 7]^T. \text{ Then } M_a = M_b = 50.$$

The bounds of the parametric uncertainty and mismatches are chosen as $a_\delta = a_r = a_\eta = 1$ and $b_\delta = b_r = b_\eta = \sqrt{2}$, respectively. In the simulation studies, we set

$$\Delta\delta(t) = \Delta r(t) = \Delta\eta(t) = \sin t, \Delta\tilde{\delta}(t) = \Delta\tilde{r}(t) = \Delta\tilde{\eta}(t) = \cos t \text{ and this gives that}$$

$$\Delta A(t) = \begin{bmatrix} -\Delta\delta(t) & \Delta\delta(t) & 0 \\ \Delta r(t) & 0 & 0 \\ 0 & 0 & -\Delta\eta(t) \end{bmatrix} = \begin{bmatrix} -\sin t & \sin t & 0 \\ \sin t & 0 & 0 \\ 0 & 0 & -\sin t \end{bmatrix}, \text{ which can be rewritten in}$$

the form of $\Delta A(t) = DF(t)E$,

$$\text{where } D = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, F = \begin{bmatrix} \sin t & 0 & 0 \\ 0 & \sin t & 0 \\ 0 & 0 & \sin t \end{bmatrix}, E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

For the choice of impulsive intervals, the synchronization error bound $\varepsilon_0 = 0.001$. Thus

$$M_2 = \frac{M_0}{\varepsilon_0} = 1.4142 \times 10^5, \lambda_{AH} = 2.8249 \times 10^5 \text{ and } d_1 > \lambda_{\max}((I+B)^T(I+B)) = 0.09.$$

Then from (8.8), the upper bound of the impulsive intervals is calculated by

$$T < \frac{1}{\lambda_{AH}} \ln\left(\frac{1}{d_1}\right) = 8.5104 \times 10^{-6}$$

We choose $T = 8 \times 10^{-6}$ in the simulation.

8.5.2 Simulation Studies and Results

In this application, we consider the encryption of a color image in Figure 8.7. Each pixel contains 256 different levels of intensity of red, green and blue which are combined to obtain a final color. In the representation of the image, 24 bits per pixel are divided into 8 bits for each primary color, i.e. 8 bits for red, 8 bits for green and 8 bits blue. The image file must be re-dimensioned as one-dimensional array before processing and this is reversed in the decrypter. In the encryption and decryption, discrete cosine transform and inverse discrete cosine transform are used respectively.

The encryption rule is given by

$$c(n) = e(p(n), k(n)) = \hat{p}(n) + k(n)$$

where $k(n) = (K \cdot (x^2(n) + y^2(n) + z^2(n))^{1/2}) \bmod 256$, $p(n)$ is the plaintext and $\hat{p}(n)$ is the discrete transform of the original picture $p(n)$, i.e., $\hat{p}(n) = DCT(p(n))$.

In the decrypter side, the plaintext is recovered by

$$\tilde{p}(n) = d(c(n), \tilde{k}(n)) = IDCT(c(n) - \tilde{k}(n))$$

where $\tilde{k}(n) = (K \cdot (\tilde{x}^2(n) + \tilde{y}^2(n) + \tilde{z}^2(n))^{1/2}) \bmod 256$.

Let $K = 100$. The recovered image is shown in Figure 8.8.

Figure 8.7: The original image

Figure 8.8: The recovered image with the proposed scheme

Again, the scheme in [6] is applied to choose impulse intervals for comparison. With the scheme, the upper bound of the impulse interval is still 1.8727×10^{-2} and we also choose $T = 1.8 \times 10^{-2}$. Figure 8.9 presents the recovered image. It is clearly seen that the

quality of the recovered image is much lower than that in Figure 8.8 where our proposed scheme is used.

Figure 8.9: The recovered image with the impulsive scheme in [6]

To have certain quantitative comparison, an index MAD is used. MAD is defined as the average mean difference between the pixel values of the red, green and blue in the recovered image and the original image, i.e.,

$$MAD = \frac{\text{The sum of the value of the difference between the original image and the recovered image}}{\text{Total Pixels} \times 3}$$

It is calculated that the MAD for our scheme is 2.2447×10^{-6} whereas the MAD for the scheme in [6] is 2.495×10^{-3} .

8.6 Concluding Remark

In this chapter, we apply the proposed scheme in chapter 7 in chaotic communication systems. We also propose to transmit functions of the chaotic states at impulsive instants to further enhance system security. The designed system is tested and verified with text, audio and image encryption and transmission. Comparisons are also made between the proposed scheme and some existing schemes. The test results show that the proposed design scheme works effectively when chaotic systems have parametric uncertainties and mismatch.

Chapter 9

Conclusion and Recommendations

9.1 Conclusions

In this thesis, we have studied the synchronization of chaotic systems and its application in cryptosystems. Several schemes were presented to improve the performance of chaotic synchronization. For those schemes, the bandwidth utilization has been increased and the robustness synchronization problem has been solved. The schemes are rigorously analyzed. Some numerical conditions are given for choosing the

impulsive intervals in the presence of uncertain parameters and noise. The major contributions of the thesis are as follows.

1. By exploring the structured knowledge of systems and using linear matrix inequalities, some less conservative conditions than existing results are derived. With the new conditions, the bound of intervals for transmitting impulses can be increased and this results in higher bandwidth efficiency. Our results are thus able to improve the efficiency of the existing technologies on chaotic secure communications and chaotic spread communications.
2. We introduce a new type of sampling scheme where the sampling period can be time varying so as to produce a flatter sampled power spectrum. The time varying sampling scheme is then applied to study chaotic cryptosystems. Compared to schemes with a fixed sampling frequency, it reduces the synchronization time between two chaotic systems in an encrypter and a decrypter while maintaining the security of chaotic cryptosystems. Thus, a good trade-off between the bandwidth utilization and the security of chaotic cryptosystem can be obtained by this scheme.
3. We present two new schemes to synchronize a driven chaotic system with the driving chaotic system in the presence of parametric uncertainties and parametric mismatch between the two systems. A controller is designed for the

driven system based on the bounds of the uncertainties. Sufficient conditions are derived to ensure synchronization of the two systems. Numerical results also show the robustness and effectiveness of the proposed schemes.

4. We have presented a control scheme to synchronize a driven chaotic system with the driving chaotic system in the presence of system noise in both systems. With the use of the noise bounds and structural information of the nonlinear parts of the systems, a controller is designed to ensure perfect synchronization of the two systems. Theoretical analysis and numerical simulations show the effectiveness of the control scheme.
5. In the results of existing impulsive chaotic synchronization schemes, a strong assumption that the two chaotic systems should be identical, i.e. without any mismatch, is usually imposed. Furthermore, system parameters are also assumed known exactly. Clearly, these are impractical. To solve this problem, a practical impulsive synchronization scheme is presented for the synchronization of two chaotic systems in the presence of both parametric uncertainties and mismatch between the two systems. With the proposed scheme, the magnitude of the synchronization error is theoretically ensured to approach to and stay within a pre-specified bound.

6. We apply the recently developed synchronization scheme in [78] to design a secure communication system with uncertainties and mismatches allowed. The scheme has been applied to text, speech and image files. Comparisons have been made with some existing schemes to show the effectiveness of the scheme. Moreover, it is proposed to transmit functions of the chaotic states at impulsive instants, instead of the states directly to further enhance system security.

9.2 Recommendations

In this thesis, we have focused on the synchronization issue for chaotic systems and proposed several schemes to improve the current technology. At the end of the thesis, some problems can be considered for future research for chaotic based secure communication systems.

1. Although the problem for parametric uncertainties and mismatches of the chaotic systems are solved by our scheme [78], the condition for impulsive synchronization of the chaotic systems maybe less conservative. A better condition may be derived to lengthen the impulse interval so that the impulse can be sent less frequently. It is, thus, to increase the bandwidth utilization and improve the security.
2. Possible applications in OFDM [80-83] system maybe explored. Chaotic signals are considered to be used in CDMA communication systems in [84,85]. The continuous pseudo-random time series are to be used as spreading code to spread the message signal. Since OFDM technology is an approach to reduce

inter-symbol interference (ISI), we can consider the possibility to use chaotic signals to substitute the spreading code in OFDM structure. It might be very useful in wireless high-speed communication systems.

3. A theory should be developed on how to choose chaotic spreading codes for chaotic digital code division multiple access (CDMA) communication systems. The chaotic spreading codes should have random noise like autocorrelation and cross-correlation properties. A guideline should be established for users to choose chaotic spreading codes to be used in the chaotic digital code division multiple access (CDMA) communication system.

Author's Publications

Journal Papers

1. Y. Ji, Z. G. Li, and C. Y. Wen, "Impulsive synchronization of chaotic systems via linear matrix inequalities," *International Journal of Bifurcation and Chaos*, vol. 16, no.1, pp. 221-227, 2006.
2. C. Y. Wen, Y. Ji, Z. G. Li, and Y. C. Soh, "Synchronization of chaotic systems with parametric uncertainty and mismatch," *International Journal of Bifurcation and Chaos*, vol. 16, no. 5, pp. 1445-1459, 2006.
3. C. Y. Wen, Y. Ji, and Z. G. Li, "Practical impulsive synchronization of chaotic systems with parametric uncertainty and mismatch," *Physics Letters A*, vol. 361, pp. 108-114, 2007.
4. Y. Ji, C. Y. Wen and Z. G. Li, "Chaotic communication systems in the presence of parametric uncertainty and mismatch," *Submitted to International Journal of Communication Systems*, 2006.
5. Z. G. Li, Y. Ji, C. Y. Wen and Y. C. Soh, "Time varying sampling scheme with an application to chaotic cryptosystem", *Dynamics of Continuous, Discrete & Impulsive Systems, Series A: Mathematical Analysis*, vol. 13b, pp. 117-130, 2006.

Conference Papers

1. Y. Ji, C. Wen, Z. G. Li and Y.C. Soh, “ Synchronization of chaotic systems in the presence of noise”, in *Proc. the 1st IEEE Conference on Industrial electronics and Applications (ICIEA 2006)*, Singapore, May 2006.
2. Y. Ji, C. Wen and Z. G. Li, “A Practical Chaotic Secure Communication Scheme Based on Lorenz Model”, in *Proc. the 4th International IEEE Conference on Industrial Informatics (INDIN06)*, Singapore, August 2006.
3. Y. Ji, C. Wen and Z. G. Li, “A Practical Synchronization Scheme for Chen’s System”, in *Proc. the 9th International Conference on Control, Automation, Robotics and Vision (ICARCV 2006)*, Singapore, December 2006.

Bibliography

- [1] B.Schneier, *Applied cryptography: Protocols, Algorithms, and Source code in C (second edition)*. New York: John Wiley, 1996.
- [2] E.N.Lorenz, "Deterministic nonperiodic flow," *J. of Atmos. Sci*, vol. 20, pp. 130-141, 1963.
- [3] E.Ott, C.Grebogi, and J.A.York, "Controlling chaos," *Phys. Rev. Lett*, vol. 64, no. 11, pp. 1196-1199, 1990.
- [4] L.M.Pecora and T.L.Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett*, vol. 64, no. 2, pp. 821-824, 1990.
- [5] L.M.Pecora and T.L.Carroll, "Synchronizing chaotic circuits," *IEEE Trans. Circuits Syst. , I*, vol. 38, no. 4, pp. 453-456, 1991.
- [6] T.Yang and L.O.Chua, "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication," *IEEE Trans. Circuits Syst. , I*, vol. 44, no. 5, pp. 976-988, 1997.
- [7] T.Yang, L.Yang, and C.Yang, "Impulsive synchronization of Lorenz systems," *Physics Letters A*, vol. 226, no. 6, pp. 349-254, 1997.
- [8] T.Yang, L.Yang, and C.Yang, "Impulsive control of Lorenz system," *Physica D*, vol. 110 1997.
- [9] W.X.Xie, C.Y.Wen, and Z.G.Li, "Impulsive control for stabilization and synchronization of Lorenz systems," *Physics Letters A*, vol. 275, no. 10, pp. 67-72, 2000.
- [10] Z.G.Li, C.Y.Wen, Y.C.Soh, and W.X.Xie, "The stabilization and synchronization of Chua's oscillators via impulsive control," *IEEE Trans. Circuits Syst. , I*, vol. 48, no. 11, pp. 1351-1355, 2001.
- [11] K.Li, Y.C.Soh, and Z.G.Li, "Chaotic cryptosystem with impulsive synchronization of Lorenz system," *Proceedings of the IASTED International Conference*, pp. 315-320, 2002.

- [12] K.Li, Y.C.Soh, and Z.G.Li, "Chaotic cryptosystem with high sensitivity to parameter mismatch," *IEEE Trans. Circuits Syst. , I*, vol. 50, no. 4, pp. 579-583, 2003.
- [13] Z.G.Li, K.Li, C.Y.Wen, and Y.C.Soh, "A new chaotic secure communication system," *IEEE Trans. Circuits Syst. , I*, vol. 51, no. 8, pp. 1306-1312, 2003.
- [14] M.Itoh, T.Yang, and L.O.Chua, "Experimental study of impulsive synchronization of chaotic and hyperchaotic circuits," *International Journal of Bifurcation and Chaos*, vol. 9, no. 7, pp. 1393-1424, 1999.
- [15] J.A.K.Suykens, T.Yang, and L.O.Chua, "Impulsive Synchronization of Chaotic Lur'e Systems by Measurement Feedback," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1371-1381, 1998.
- [16] K.M.Cuomo, A .V.Oppenheim, and S.H.Strogatz, "Synchronization of Lorenz-based chaotic circuits with application to communication," *IEEE Trans. Circuits Syst. , I*, vol. 40, no. 10, pp. 626-633, 1993.
- [17] L.M.Pecora and T.L.Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, no. 4, pp. 2374-2383, 1991.
- [18] H.Dedieu, M.P.Kennedy, and M.Hasler, "Chaos Shift Keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. , II*, vol. 40, no. 10, pp. 634-642, 1993.
- [19] U.Parlitz, L.O.Chua, L.KOCAREV, K.S.HALLE, and A.SHANG, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 4, pp. 973-977, 1993.
- [20] T.Yang and L.O.Chua, "Secure communication via chaotic parameter modulation," *IEEE Trans. Circuits Syst. , I*, vol. 43, no. 9, pp. 817-819, 1996.
- [21] C.W.Wu and L.O.Chua, "A simple way to synchronize chaotic system with application to secure communication system," *International. Journal of Bifurcation and Chaos*, vol. 3, no. 6, pp. 1619-1627, 1993.
- [22] T.Yang, C.W.Wu, and L.O.Chua, "Cryptography based on Chaotic systems," *IEEE Trans. Circuits Syst. , I*, vol. 44, no. 5, pp. 469-472, 1997.
- [23] K.Li, Y.C.Soh, and C.S.Zhang, "A frequency aliasing approach to chaos-based cryptosystems," *IEEE Trans. Circuits Syst. , I*, vol. 51, no. 12, pp. 2470-2475, 2004.

- [24] A.Khadra, X.Z.Liu, and X.Shen, "Impulsively synchronization chaotic systems with delay and applications to secure communication," *Automatica*, vol. 41, no. 9, pp. 1491-1502, 2005.
- [25] A.Khadra, X.Z.Liu, and X.Shen, "Application of impulsive synchronization to communication security," *IEEE Trans. Circuits Syst. , I*, vol. 50, no. 3, pp. 341-351, 2003.
- [26] M.J.Ogorzalek, "Taming Chaos-Part I: Synchronization," *IEEE Trans. Circuits Syst. , I*, vol. 40, no. 10, pp. 693-699, 1993.
- [27] T.L.Carroll, "Communicating using filtered synchronized chaotic signals," *IEEE Trans. Circuits and Systems.*, vol. 42, pp. 105-110, 1995.
- [28] M.Itoh, T.Yang, and L.O.Chua, "Conditions for impulsive synchronization of chaotic and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 11, no. 2, pp. 551-560, 2001.
- [29] G.Grassi and S.Mascolo, "A system theory approach for designing cryptosystems based on hyperchaos," *IEEE Trans. Circuits Syst. , I*, vol. 46, no. 9, pp. 1135-1138, 1999.
- [30] E.M.Elabbasy, H.N.Agiza, and M.M.Dessoky, "Synchronization of modified chen system," *International Journal of Bifurcation and Chaos*, vol. 14, no. 11, pp. 3969-3979, 2004.
- [31] L.Kocarev, K.S.Halle, K.Eckert, L.O.Chua, and U.Parlitz, "Experimental demonstration of secure communication via chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, pp. 709-713, 1992.
- [32] G.Kolumban, P.Kennedy, and L.O.Chua, "The role of synchronization in digital communications using chaos -- Part I: Fundamentals of digital communications," *IEEE Trans. Circuits Syst. , I*, vol. 44, no. 10, pp. 927-935, 1997.
- [33] T.Stojanovski, L.Kocarev, and U.Parlitz, "Digital Coding via Chaotic Systems," *IEEE Trans. Circuits Syst. , I*, vol. 44, no. 6, pp. 562-565, 1997.
- [34] T.Stojanovski, L.Kocarev, U.Parlitz, and R.Harris, "Sporadic driving of dynamical systems," *Physical Review E*, vol. 55, no. 4, pp. 4035-4048, 1997.
- [35] Z.P.Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuits Syst. , I*, vol. 49, no. 1, pp. 92-96, 2002.

- [36] L.Kocarev and U.Parlitz, "General approach for chaotic synchronization with application to communication," *Physical Review Letters*, vol. 74, no. 25, pp. 5028-5031, 1995.
- [37] E.N.Lorenz, *The essence of chaos* University of Washington Press, 1995.
- [38] L.O.Chua, M.Komuro, and T.Matsumoto, "The double scroll family," *IEEE Trans. Circuits and Systems*, vol. 33, no. 11, pp. 1073-1118, 1986.
- [39] L.O.Chua and G.N.Lin, "Canonical realization of Chua's circuit family," *IEEE Trans. Circuits and Systems*, vol. 37, no. 7, pp. 885-902, 1990.
- [40] R.N.Madan, *Chua's circuit: a paradigm for chaos*. Singapore: World Scientific, 1993.
- [41] G.R.Chen, "Yet another chaotic attractor," *International Journal of Bifurcation and Chaos*, vol. 9, no. 7, pp. 1465-1466, 1999.
- [42] T.Ueta and G.R.Chen, "Bifurcation analysis of Chen's equation," *International Journal of Bifurcation and Chaos*, vol. 10, no. 8, pp. 1917-1931, 2000.
- [43] T.Ueta and G.R.Chen, "Bifurcation and chaos of Chen's equation," *Proc. ISCAS00*, vol. 5, pp. 505-508, 2000.
- [44] M.P.Kennedy, *Chaotic Electronics in Telecommunications* CRC press, 2000.
- [45] R.He and P.G.Vaidya, "Implementation of chaotic cryptography with chaotic synchronization," *Physical Review E*, vol. 57, no. 2, pp. 1532-1535, 1998.
- [46] F.C.M.Lau and C.K.Tse, *Chaos-Based Digital Communication Systems*. Heidelberg: Springer-Verlag, 2003.
- [47] P.Stavroulakis, *Chaos applications in telecommunications* CRC Press, 2006.
- [48] K.M.Short, "Steps toward unmasking secure communication," *International Journal of Bifurcation and Chaos*, vol. 4, no. 4, pp. 959-977, 1994.
- [49] T.Yang, "Recovery of digital signals from chaotic switching," *International Journal of Circuit Theory and Applications*, vol. 23, no. 6, pp. 611-615, 1995.
- [50] K.M.Short, "Unmasking a modulated chaotic communications scheme," *International Journal of Bifurcation and Chaos*, vol. 6, no. 2, pp. 367-375, 1996.

- [51] T.Yang, "Chaotic secure communication systems: history and new results," *Telecommunications Review*, vol. 9, no. 4, pp. 597-634, 1999.
- [52] V.Lakshmikantham, D.D.Bainov, and P.S.Simenov, *Theory of Impulsive Differential Equations*. Singapore: World Scientific, 1989.
- [53] S.Boyd, L.E.Ghaoui, E.Feron, and V.Balakrishnan, *Linear Matrix Inequalities in Systems and Control Theory*. Philadelphia: SIAM, 1994.
- [54] A.V.Oppenheim, A.S.Willsky, and S.H.Nawab, *Signals and Systems* Prentice Hall, 1997.
- [55] Z.G.Li, Y.C.Soh, and C.Y.Wen, *Switched and Impulsive Systems: Analysis, Design and Application* Springer-Verlag, 2005.
- [56] N.F.Rulkov, M.M.Sushchik, L.S.Tsimring, and A.R.Volkovskii, "Digital Communication Using Chaotic-Pulse-Position Modulation," *IEEE Trans. Circuits Syst. , I*, vol. 48, no. 12, pp. 1436-1444, 2001.
- [57] T.Yang and L.O.Chua, "Chaotic impulse radio: A novel chaotic secure communication system," *International Journal of Bifurcation and Chaos*, vol. 10, no. 2, pp. 345-357, 2000.
- [58] G.Heidari-Bateni and C.D.McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Communications*, vol. 42, no. 2/3/4, pp. 1524-1527, 1994.
- [59] Z.Y.He, K.Li, L.X.Yang, and Y.H.Shi, "A Robust Digital Secure Communication Scheme Based on Sporadic Coupling Chaos Synchronization," *IEEE Trans. Circuits Syst. , I*, vol. 47, no. 3 2000.
- [60] U.Parlitz, L.Kocarev, T.Stojanovski, and H.Preckel, "Encoding messages using chaotic synchronization," *Phys. Rev. E*, vol. 53, pp. 4351-4361, 1996.
- [61] O.A.Gonzales, G.Han, J.P.de Gyvez, and E.Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: a monolithic implementation," *IEEE Trans. Circuits Syst. , I*, vol. 47, no. 8, pp. 1243-1247, 2000.
- [62] K.V.Cuomo and A.V.Oppenheim, "Circuit Implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65-68, 1993.

- [63] G.Hu, Z.Feng, and R.Meng, "Chosen ciphertext attack on chaos communication based on chaotic synchronization," *IEEE Trans. Circuits Syst. , I*, vol. 50, pp. 275-279, 2003.
- [64] T.Yang, "Recovery of digital signals from chaotic switching," *Int. J. of Circuit Theory and Applications*, vol. 23, no. 6, pp. 611-615, 1995.
- [65] M.J.Ogorzalek and H.Dedieu, "Some tools for attacking secure communication systems employing chaotic carriers," *ISCAS'98*, pp. 522-525, 1998.
- [66] G.Perez and H.A.Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, pp. 1970-1973, 1995.
- [67] H.Zhou and Y.T.Ling, "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits Syst. , I*, vol. 44, no. 3, pp. 268-271, 1997.
- [68] D.E.Sigeti, "Exponential decay of power spectra at high frequency and positive Lyapunov exponents," *Physica D*, vol. 82, no. 136, p. 153, 1995.
- [69] J.Sun, Y.Zhang, L.Wang, and Q.Wu, "Impulsive robust control of uncertain Lure systems," *Physics Letters A*, vol. 304, pp. 130-135, 2006.
- [70] Y.Ji, Z.G.Li, and C.Y.Wen, "Impulsive synchronization of chaotic systems via linear matrix inequalities," *International Journal of Bifurcation and Chaos*, vol. 16, no. 1, pp. 221-227, 2006.
- [71] C.Y.Wen, Y.Ji, Z.G.Li, and Y.C.Soh, "Synchronization of chaotic systems with parametric uncertainty and mismatch," *International Journal of Bifurcation and Chaos*, vol. 16, no. 5, pp. 1445-1459, 2006.
- [72] G.Kolumban, "Theoretical noise performance of correlator-based chaotic communications schemes," *IEEE Trans. Circuits Syst. , I*, vol. 47, no. 12, pp. 1692-1701, 2000.
- [73] F.C.M.Lau and C.K.Tse, "Performance of chaos-based communication systems under the influence of coexisting conventional spread-spectrum systems," *IEEE Trans. Circuits Syst. , I*, vol. 50, no. 11, pp. 1475-1481, 2003.
- [74] A.J.Lawrance and G.Ohama, "Exact calculation of bit error rates in communication systems with chaotic modulation," *IEEE Trans. Circuits Syst. , I*, vol. 50, no. 11, pp. 1391-1400, 2003.

- [75] M.Sushchik, L.S.Tsimring, and A.R.Volkovskii, "Performance analysis of correlation-based communication schemes utilizing Chaos," *IEEE Trans. Circuits Syst. , I*, vol. 47, no. 12, pp. 1684-1691, 2000.
- [76] M.Hasler and T.Schimming, "Chaos communication over noisy channels," *International Journal of Bifurcation and Chaos*, vol. 10, pp. 719-735, 2000.
- [77] G.Chen and X.N.Dong, *From Chaos to Order: Methodologies, Perspectives and Applications* World Scientific Series on Nonlinear Science, Series A, Vol. 24, 1998.
- [78] C.Y.Wen, Y.Ji, and Z.G.Li, "Practical impulsive synchronization of chaotic systems with parametric uncertainty and mismatch," *Physics Letters A*, vol. 361, pp. 108-114, 2007.
- [79] Z.G.Li, C.Y.Wen, and Y.C.Soh, "Analysis and design of impulsive control systems," *IEEE Trans. on Automatic Control*, vol. 46, no. 6, pp. 894-897, 2001.
- [80] N.Yee, J.P.Linnartz, and G.Fettweis, "Multi-Carrier CDMA in indoor wireless radio networks," *PIMRC*, pp. 109-113, 1993.
- [81] A.R.Bahai and B.R.Saltzberg, *Multi-carrier digital communications : theory and applications of OFDM* Kluwer Academic, 1999.
- [82] P.Ramjee, *OFDM for wireless communications systems* Artech House, 2004.
- [83] T.John, *OFDM wireless LANs : a theoretical and practical guide* Sams, 2002.
- [84] P.Ramjee, *CDMA for wireless personal communications* Artech House, 1996.
- [85] T.Yang and L.O.Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *International Journal of Bifurcation and Chaos*, vol. 7, no. 12, pp. 2789-2805, 1997.