# DESIGN AND IMPLEMENTATION OF SECURE CHAOTIC COMMUNICATION SYSTEMS

RUPAK KHAREL

Ph. D. 2011

# Design and Implementation of Secure Chaotic Communication Systems

Rupak Kharel

A thesis submitted in partial fulfilment of the requirements of the University of Northumbria at Newcastle for the degree of Doctor of Philosophy

Research undertaken in the

School of Computing, Engineering and Information Sciences

March 2011

# Abstract

Chaotic systems have properties such as ergodicity, sensitivity to initial conditions/parameter mismatches, mixing property, deterministic dynamics, structure complexity, to mention a few, that map nicely with cryptographic requirements such as confusion, diffusion, deterministic pseudo-randomness, algorithm complexity. Furthermore, the possibility of chaotic synchronization, where the master system (transmitter) is driving the slave system (receiver) by its output signal, made it probable for the possible utilization of chaotic systems to implement security in the communication systems. Many methods like chaotic masking, chaotic modulation, inclusion, chaotic shift keying (CSK) had been proposed however, many attack methods later showed them to be insecure. Different modifications of these methods also exist in the literature to improve the security, but almost all suffer from the same drawback. Therefore, the implementation of chaotic systems in security still remains a challenge. In this work, different possibilities on how it might be possible to improve the security of the existing methods are explored. The main problem with the existing methods is that the message imprint could be found in the dynamics of the transmitted signal, therefore by some signal processing or pattern classification techniques, etc, allow the exposition of the hidden message. Therefore, the challenge is to remove any pattern or change in dynamics that the message might bring in the transmitted signal.

Along with secure methods, the investigation of channel noise in the chaotic synchronization and message extraction needs is investigated. A comparative study on the proportional (P) and proportional integral (PI) observer method of observer based chaotic synchronization is performed for a proposed combinational scheme (masking + inclusion). It is shown that PI observer provides flexibility to the system to handle noise by offering better synchronization in the presence of noise than P-observer. It is also shown that the P-observer imposes restriction on the transmitting message, however the PI observer does not have any such restrictions as it adds degree of freedom to the system by the inclusion of integrator in the design. The idea of digitization of chaotic signal is used for only adding security layer while using the existing digital communication for the transmission. The simulation results show that message is extracted at different bit error rates with possibility at signal-to-noise ratio (SNR) as low as 14 dB when this idea is used. SNR can further be reduced by already available error correction and equalization techniques in the digital domain.

When two equal power chaotic signals are combined together and then used to modulate the transmitting message signal, then it might be difficult for intruders to use the conventional attack methods since there is added complexity in the chaotic carrier signal. Based on this we have proposed a cascaded chaotic masking scheme to improve the security of masking method. Even though the cascaded masking approach adds complexities in the system by making the n-dimensional system to 2n or more dimensional system, more possibilities also needs to be explored.

Next, a new chaotic synchronization method called indirect coupled chaotic synchronization (ICCS) is presented and proven mathematically for both continuous and discrete time system. ICCS allows two independent chaotic oscillators to synchronize with each other consequently can be used to generate same keystream at the transmitter and receiver side which is utilized to encrypt the message signal using an encryption algorithm, and then modulated with the chaotic transmitter. At the receiver, same keystream available due to ICCS is used to decrypt the message back. Security analysis illustrates that the proposed method does not suffer from the shortcomings of the earlier methods. The ICCS is further implemented to modify and improve the security of the CSK method by removing the pattern from the transmitted when switching is made between either 0 or 1. Two different possible implementations are proposed and simulation results verify the successful message extraction at the receiver and security analysis illustrates the improvement.

Finally, the proposed secure communication scheme using ICCS is practically realized in digital signal processing (DSP) board. The message is shown to be successfully extracted and the output from the DSP board is compared with the computer simulations and found that the difference is very insignificant thus proving the effective hardware realization using the DSP board.

# Acknowledgements

This research is done in the school of computing, engineering and information sciences, Northumbria University. I would like to bestow my sincere thanks to Northumbria University for providing me with the studentship for carrying out this research.

I would like to thank my supervisors Dr. Krishna Busawon and Prof. Z. Ghassemlooy for their constant support, guidance and motivation throughout the 3 years of this PhD. Without them reading the materials and providing me with the constructive advices and suggestion, I would not have been able to finish the research and this thesis on time. I am very much indebted to my supervisors.

Special thanks go to the colleagues at the PhD room for providing with friendly environment and making my 3 years of research really enjoyable.

Finally, I would like to express my special thanks to my entire family members, my father, mother, sisters, my in-laws, for their moral support throughout. Without them besides me, this would not have been possible. Special thanks ultimately is for my wife, Kabita, for her constant support and patience through my ups and downs, her ever smiling face and love.

# Declaration

I declare that the work contained in this thesis has not been submitted for any other award and that it is all my own work.

Rupak Kharel

March 2011

# Table of Contents

# List of Figures

# Glossary of Abbreviations

| | |
|---|---|
| ANN | Artificial Neural Network |
| AWG | Additive White Gaussian |
| BER | Bit Error Rate |
| CCS | Code Composer Studio |
| CS | Complete Synchronization |
| CSK | Chaotic Shift Keying |
| DES | Data Encryption Standard |
| DMS | Discrete Memoryless Source |
| DPCM | Differential Pulse Code Modulation |
| DSP | Digital Signal Processing |
| GS | Generalized Synchronization |
| ICCS | Indirect Coupled Chaotic Synchronization |
| LPF | Low Pass Filter |
| NLD | Non-Linear Dynamic |
| NN | Neural Networks |
| OOK | On-Off Keying |
| PCM | Pulse Code Modulation |
| RM | Return Map |
| RTDX | Real-Time Data Exchange |
| SNR | Signal to Noise Ratio |
| SPD | Symmetric Positive Definite |
| TI | Texas Instrument |
| WT | Wavelet Transform |

# Glossary of Symbols

| | |
|---|---|
| $\sigma, \sigma_a, \sigma_b, \sigma_1$ | Lorenz system Prandtl number |
| r | Lorenz System Rayleigh number |
| $D_w$ | Jacobian with respect to w |
| $\omega_{norm}$ | Normalized angular frequency |
| $\omega$ | Angular frequency |
| $N_b$ | Number of bits transmitting during $T_s$ |
| $T_s$ | Switching time for CSK |
| R, $\Re$ | Set of real numbers |
| $O_x$ | Observability matrix |
| $\dot{x}$ | Derivative of x with respect to time, i.e. $dx./dt$ |
| A, B, C, F, $F_A$, $F_B$ | Matrices of appropriate dimensions |
| $G_a, G_b$ | Piecewise linear function constants in Chua's system |
| $\alpha, \beta, \gamma$ | Constants parameters for Chua's system |
| $\hat{x}$ | Estimation of the variable x |
| $e_x$ | Error between variables x and $\hat{x}$ |
| m(t) | Message signal |
| $m_r(t)$, $\hat{m}(t)$ | Extracted/received message signal |
| $A_i$ and $B_i$ | If $x_i$ and $X_i$ are $i^{th}$ maxima and minima for a signal then $A_i = (x_i + X_i)/2$ and $B_i = X_i - x_i$, used in RM |
| $A_m$ and $B_m$ | $i^{th}$ maxima and minima for a signal used in RM |
| $K_p$, K, $K_{Ap}$, $K_{Bp}$ | Gain matrix for observer design |
| $K_i$ | Integral gain matrix for PI observer design |
| $\eta(t)$ | Channel noise |
| P, Q, $P_1$, $P_2$, $Q_1$, $Q_2$ | Symmetric positive definite matrices |
| V(.), W(.) | Candidate Lyapunov function |
| $y_t$ | Transmitted chaotic signal |
| e, $\xi$, $\varepsilon$, $\zeta$ | Error dynamics matrices |
| $I_n$ | Identity matrix of dimension n |
| $\|.\|$ | Norm |
| $Y_i$ | Discrete form of a continuous signal y(t). |
| $\beta$ | Switching parameter in CSK |
| $\beta_m$ | Switching parameter modulating message m in CSK |
| $\beta_0$ | Switching parameter when modulating 0 in CSK |
| $\beta_1$ | Switching parameter when modulating 1 in CSK |
| h(t) | Channel impulse response |
| $\lambda$ | eigenvalue of a system |
| $d_0$ | Amplification/scaling variable |

# Chapter 1 Introductions

In the current digital age, there has been a lot of interest on secure communication links due to the dramatic rise of online shopping, banking and trading transaction and this trend is set to increase exponentially in future. In effect, it does not take much effort to realise that there will be a significant development and usage of digital communication and technology in the next decade and further. Consequently, there is a need to increase the security of data being transmitted in order to avoid hacking of information and fraud.

Secure communication between two parties (or systems) is done in such a way that the identity of the communicating party is confirmed and the confidentiality as well as the integrity of the message is maintained. Hence, confidentiality, authentication and message integrity are three key points for secure communication. Confidentiality means that only the sender and receiver are able to understand the contents of the transmitted message. The idea is to encrypt the message by the sender with some cryptography algorithms. The message can only be decrypted back by the intended receiver, may be by using a special key. Authentication means that if sender A and receiver B are communicating then the identity of both should be confirmed. Message integrity means that whenever sender and receiver are communicating, then it must be ensured that the message content has not been altered. The notion of "secure communication" is most commonly perceived as confidentiality but as explained earlier it is not the case. However, authentication and message integrity can be achieved by the cryptography techniques.

Modern software cryptography has witnessed a continuous development over the past 30 years [2]. The software encryption technique can either be based on the so-called

symmetric or asymmetric key. A number of encryption/decryption techniques have been developed including Data Encryption Standard (DES), Triple-DES, RSA (Rivest, Shamir, and Adelman, the inventors of the technique), Rabin Scheme, Williams scheme, etc [3-10]. Although, many of these techniques are currently being used and form the heart of security, none of these can be regarded as 100% secure due to the availability of high-speed computers and fast algorithms [10-12].

Recently, chaotic signals, due to the properties like limited predictability, aperiodicity, broad spectrum, and high sensitivity to parametric mismatch/initial conditions, has brought forward the idea of implementing them for secure communication and as an alternative to classical cryptography. Chaotic signals can be implemented to achieve security directly at the physical level. Researchers have pointed out that there exists a very close relationship between chaos and cryptography [13, 14]. Various characteristics and properties of chaotic signals such as ergodicity, mixing, randomness, complexity, unpredictably and the sensitivity to initial conditions, can be connected to the well-known confusion and diffusion properties in the classical cryptography. According to Shannon [15], confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible; diffusion refers to the property that the redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. In other words, the non-uniformity in the distribution of the individual letters (and pairs of neighbouring letters) in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect. Diffusion means that the output signal (ciphertext) should depend on the input message (plaintext) in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable manner [15]. Since, chaotic

signals have properties that are very close to what is required for cryptography attention has been recently shifted on implementing secure communication using chaotic signals.

The basic block diagram of a chaotic communication system is shown in Figure 1.1. The modulation technique and the synchronization method employed hold the importance for good performance and security. Also, the performance of the system under the influence of noise and channel model is very important as well.

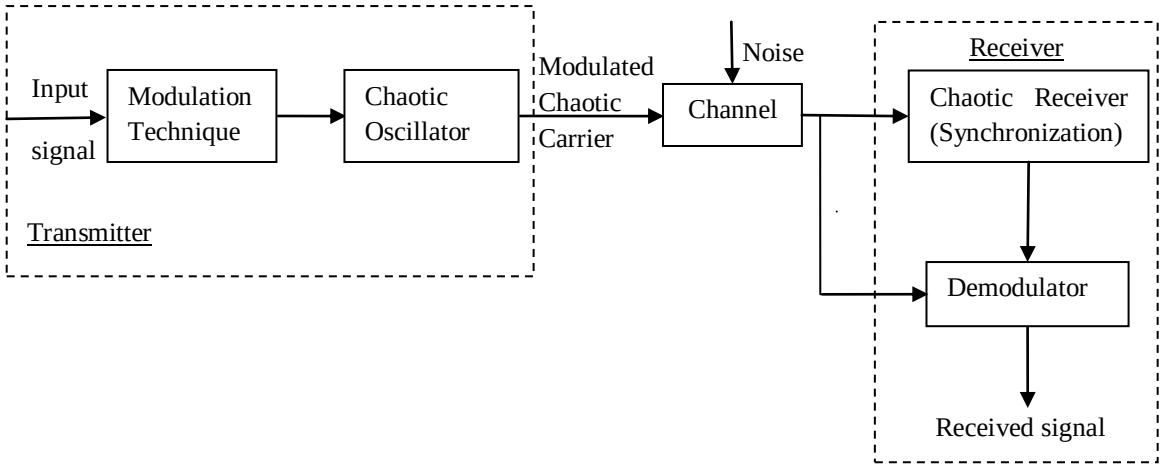


Figure 1.1: Elementary block diagram of chaotic communication system.

As it can be observed in Figure 1.1, the chaotic communication system consists of three main aspects, transmitter, receiver and the channel (noise) performance. In the transmitter, the modulation techniques being used to mix the message signal along with the chaotic carrier are of essence for the overall security of the system. There are various modulation techniques currently available in the literature such as chaotic masking, chaotic modulation, chaotic inclusion and chaotic shift keying (CSK). However, all of these methods have been proven to be insecure. Although chaotic signals have nice inherent properties to be used in security and cryptography, the implementation is not straight forward. Because a signal has to be transmitted from to the receiver, the signal will be

available to the intruders. Therefore, even if the intruders do not know the structure or parameters of the chaotic systems, they can perform some signal processing analysis or apply some more sophisticated algorithms to get the imprint of the message out from the transmitter signal. In the case of chaotic masking, the signal is directly added to the chaotic signal, therefore the variation can be detected by some non-linear dynamic forecasting methods, or if the message amplitude/frequency are high enough then power spectral analysis will reveal the message. In CSK method the binary signal 0 or 1 being transmitted brings pattern in the transmitted signal. Therefore pattern classification problem can be utilized to find out the binary message with having any knowledge about the transmitter. Methods of modulation and inclusion are also vulnerable to various attack methods. Therefore, the mixing of message should be in such a way that there is no pattern or information of the message signal present in the transmitted signal. Once the carrier chaotic signal is transmitted into the channel, then it will get corrupted with channel noise before it reaches to the receiver. In the receiver side, chaotic synchronization is necessary for successful message recovery. Therefore the demodulation process is another challenge in the implementation of the chaotic communication systems. There are many ways to achieve synchronization, but observer method is one of the promising methods. There are many types of observers such as proportional observer, proportional integral (PI) observer, etc, therefore the performance of these observers needs to be investigated in the presence of noise. Chaotic communication provides security to the communication systems but digital communication on its own has developed massively therefore it will be wise to come up with a technique such that chaotic schemes only adds a layer for security while utilizing existing digital communication setup for message transmission.

In this research, we propose new transmission schemes to improve the existing methods whereby eliminating their shortcomings. Therefore, the motivation of this research is to

come up with improved chaotic communication techniques that are robust to various known attack methods and also look upon few other aspects such as channel noise performance and complementation with existing communication setup. Following is the list of original contributions from this research work.

## 1.1 Original Contributions

The original contributions produced from this research are outlined below.

i. Performance analysis of classical proportional (P) observer and PI observer is done for the proposed combinational (masking + inclusion) chaotic communication system. It is shown that PI-observer provides better synchronization performance and therefore message recovery when the driving signal is corrupted by channel noise plus the message. The detail analysis and the simulation results are also published in papers [16, 17] and outlined in Chapter 3.

ii. A new chaotic communication technique called Cascaded Chaotic Masking has been developed. This has been published in [18] and described in Chapter 4.

iii. A new type of chaotic synchronization technique has been developed, which have been called indirectly coupled chaotic synchronization (ICCS). This synchronization method is mathematically proven for a class of chaotic systems for both continuous and discrete time case. This has been described in detail in Chapter 5.

iv. Using the new type of synchronization, ICCS, a new chaotic communication method is developed. This technique implemented the keystream generated via ICCS and used for achieving higher security. The method is described both for

continuous and discrete time case, along with cryptanalysis, in Chapter 6. These methods are also published in [19-21].

v. Hardware realization of the proposed chaotic communication based on ICCS is also done using the digital signal processing (DSP) board and is presented in Chapter 6 and published in [25]. This is a verification of the model based on ICCS.

vi. A new type of chaotic secure communication method for transmitting digital bits has been developed. This is an improved form of the earlier method called CSK. This again used the earlier proposed ICCS method for generating identical keystream at the transmitter and the receiver side. Detail explanation of the method, simulation results and cryptanalysis are presented in the Chapter 7. These results are also published in [22, 23].

vii. A chaotic communication based on digitization of the chaotic signal is proposed and the performance of the system on noisy channel at different level of bit error rate (BER) was shown. This technique had been proposed for the first time in this PhD work. This technique was based on digitization of the chaotic signals and transmitting it with existing digital communication infrastructure in the noisy channel. The results are published in [24] and outlined in Chapter 8.

## 1.2 List of Publications

Following are the list of publications that had been done as part of this PhD research work.

**Journal Paper**

1. R. Kharel, K. Busawon, and Z. Ghassemlooy, "A chaos-based communication scheme using proportional and proportional-integral observers," IJEEE, vol. 4, pp. 127-139, 2008.

**Conference Papers**

2. R. Kharel, K. Busawon, W. Aggoune, and Z. Ghassemlooy, "Implementation of a secure digital chaotic communication scheme on a DSP board " in 7th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP'10), Newcastle Upon Tyne, UK, 2010.
3. R. Kharel, K. Busawon, "Indirectly coupled synchronization of chaotic systems: Application to secure digital communications", 28th International Colloquium on Group - Theoretical Methods in Physics, Group 28, Newcastle Upon Tyne, UK, 2010.
4. R. Kharel, K. Busawon, and Z. Ghassemlooy, "Modified chaotic shift keying using indirect coupled chaotic synchronization for secure digital communication," in 3rd Chaotic Modelling and Simulation International Conference (Chaos2010), Chania, Greece, 2010.
5. R. Kharel, K. Busawon, and Z. Ghassemlooy, "Secure digital communication using discrete-time chaotic systems via indirect coupling synchronization " in American Control Conference (ACC'10), Baltimore, Maryland, USA, 2010.
6. R. Kharel, K. Busawon, and Z. Ghassemlooy, "Indirect coupled oscillators for keystream generation in secure chaotic Communication," in Proceedings of the 48th IEEE conference on Decision and Control and 28th Chinese Control Conference 2009, 2009.
7. R. Kharel, K. Busawon, and Z. Ghassemlooy, "A novel chaotic encryption technique for secure communication," in 2nd IFAC conference on analysis and control of chaotic systems (Chaos 09), London, 2009.

8. W. Aggoune, K. Busawon, and R. Kharel, "On feedback stabilization of nonlinear discrete-time state-delayed systems," in European Control Conference (ECC'09), Budapest, Hungary, 2009.
9. R. Kharel, S. Rajbhandari, K. Busawon, and Z. Ghassemlooy, "Digitization of chaotic signal for reliable communication in non-ideal channels," in Proceeding of International Conference on Transparent Optica*l Networks 'Mediterranean Winter'' (ICTON*-MW'08), Marrakech, Morocco, 2008 pp. Sa1.2 (1-6) - **Invited Plenary Paper.**
10. R. Kharel, K. Busawon, and Z. Ghassemlooy, "Novel cascaded chaotic masking for secure communications," in The 9th annual Postgraduate Symposium on the convergence of Telecommunications , Networking & Broadcasting (PGNET), Liverpool, UK, 2008, pp. 295-298.
11. K. Busawon, R. Kharel, and Z. Ghassemlooy, "A new chaos-based communication scheme using observers," in Proceeding of the 6th Symposium on Communication Systems, Networks and Digital Signal Processing 2008 (CSNDSP 2008), Graz, Austria, 2008, pp. 16-20.

## 1.3 Organization of the Thesis

The thesis is divided into ten main chapters. In Chapter 1, we provide a comprehensive overview of chaos. Different properties of chaotic systems are discussed and few examples of chaos are mentioned. Also different routes from where chaos can occur are also discussed. Then an overview of chaotic synchronization is given and different types of synchronization are discussed. The use of chaotic signal in communication for achieving security is then discussed. This chapter also describes traditional chaotic communication methods along with their problems and also different attack methods are also outlined.

Finally, various other modified methods available in the literature are discussed along with their problem and shortcomings.

The study of two types of observers (P and PI) for the proposed combinational method is presented in Chapter 3. The performance of P and PI-observers under the noisy channel is compared and shown. This chapter focussed on the performance of PI-observer in the noisy channels for better synchronization and message recovery without much emphasis on the security.

Chapter 4 explains an approach of cascaded chaotic masking for realizing secure communication link. Detail of the method is explained and simulation results are presented here. However, it is also pointed out that this method might not be secure enough but is a stride towards finding out other methods. Chapter 3 and Chapter 4 provide an illustration of the approach to this research for finding out secure techniques. Therefore, even though the techniques mentioned in chapter 3 and 4 may not be very secure, they show the step towards more sophisticated and secure methods, which will be seen in later chapters.

In Chapter 5, we propose a new idea of chaotic synchronization called ICCS. This type of synchronization has first been developed in this research. In this chapter, the detail description of ICCS along with examples and mathematical proof (for both continuous and discrete time case) is provided.

In Chapter 6, the ICCS that had been proposed in the earlier chapter is utilized for realizing a secure communication based on cryptography. The details of the method are presented and implemented on the both continuous and discrete time systems. The security analysis of the proposed method is also done in this chapter. The discrete type method is implemented on hardware using a DSP board. Rapid prototyping of the model is done in TMS320C6713 DSK DSP board. First of all, the Simulink model is converted into

assembly code for the TMS320C6713 using Simulink and the code composer studio (CCS). The real-time data exchange (RTDX) link is used to transfer data from the DSP to the computer and vice-versa. The results obtained when the model is implemented on the DSP board and when is implemented in simulation using Matlab are compared and it is found that there is striking similarity between the two. It means that our proposed model could be realized in hardware for practical implementation. All these details have been mentioned in this chapter.

In Chapter 7, a new chaotic communication technique for transmitting digital message is proposed which also utilized ICCS. This technique is modified and improved form of the traditional CSK scheme. Two different implementations are proposed and security analysis are also performed and discussed.

Chapter 8 presents an idea of digitization of chaotic signals to be used in practical environment where the chaotic carrier is converted to digital bits and transmitted using existing digital communication techniques. The method of digitization is very interesting since it allows the use of chaotic communication for adding a layer of security in the already existing digital communication system. Performance of the method in different BERs is shown and is pointed out that the method works up to the moderate signal to noise ratio (SNR) of level of 14 dB.

Finally concluding remarks and future works are outlined in Chapter 9.

# Chapter 2 An Overview of Chaos and its Importance in Communication Systems

## 2.1 Introductions

Chaos is a word derived from the ancient Greek, which means unpredictable behaviour and opposite of the cosmos or order. However, in chaos theory, the term “Chaos” is not an antithesis of cosmos or absence of order but in fact have a very subtle order in itself not quite obvious as ordered systems. The history of chaos in scientific community has to be stretched back to the time when Newton solved the two body problem in universe using his newly invented differential equation. He had disregarded the effect of gravitational effect of one planet on another in his calculations. It was not until late 1800 that Poincare came up with the qualitative method where he showed that it is essentially impossible to solve the 3-body problem. He showed that orbits are aperiodic but not increasing infinitely (meaning deterministic) and not approaching any fixed points or limit cycles. He pointed out that difficulty in solving the three body problem was due the sensitivity to the initial conditions making long term prediction impossible. Therefore, Poincare can be considered to be the first person to envision “Chaos” [26, 27].

Later in 1963, Edward Lorenz of the Massachusetts Institute of Technology came up with a set of three differential equations popularly known as the Lorenz equation [28], for forecasting the weather behaviour using computer simulations. Lorenz was using a 6-digit precision computer for calculation but was using a 3-digit precision printer to print the data being entered to the computer again for simulation. It turned out that the rounding off of

the data that was used as the initial condition caused a significant difference in the long term results making long term prediction an impossible task. The solution never settled to any fixed point or periodic orbits and oscillated irregularly. However, Lorenz also pointed out that there is an order in chaos as well where he came up with a 3-dimensional plot of the solutions. He showed that the trajectory of the system being evolving with time in a complex and non-repeating pattern but in an interesting butterfly shaped set of points known today as the "Strange Attractor". Lorenz concluded that the earth's weather is a chaotic system and therefore, a long-range prediction is an impossible task.

Before going too further in the realm of chaos, let us make an attempt to define it. No definition has been universally accepted yet but the following definition confines the fundamental three nature of chaos, which everyone will agree as mentioned by Strogatz [26].

## 2.2 Chaos: Definition

**Chaos** *is a "aperiodic long*-term behaviour in a deterministic system that exhibits sensitive *dependence on initial conditions"* [26].

The three properties of chaos mentioned in the definition can be explained as follows:

i. **Aperiodic long term behaviour:** This means that the system trajectories do not settle down to any fixed points, periodic orbits or quasiperiodic orbits as $t \rightarrow \infty$. Thus, the trajectory that follows will have a limited predictability.

ii. **Deterministic system:** This means that the system is not random or do not have any stochastic input parameters. The irregular behaviour shown by chaotic systems is due to the system's intrinsic non-linearity rather than the noise.

iii. **Sensitivity to initial conditions:** This means that the trajectories even if they start from very close initial conditions will separate exponentially fast, i.e. the system has a positive Lyapunov exponent. This means a long term predictability becomes impossible.

In order to explain these properties of chaos and its basic idea, let us recall the Lorenz equation mentioned earlier. Lorenz system is a set of three coupled first-order differential equations given as:

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= x(r - z) - y \\ \dot{z} &= xy - bz, \end{aligned} \tag{2.1}$$

where σ is called the Prandtl number and r is called the Rayleigh number. Lorenz chose these parameters to have the following values of $\sigma$ = 10, b = 8/3 and r = 28. When such values are chosen, the Lorenz system defined in (2.1) exhibits chaotic behaviour. Now, we shall attempt to verify the three properties mentioned above in the definition for chaotic systems for Lorenz equations.

To demonstrate the first property of chaos, i.e. aperiodicity, a numerical simulation was done using Matlab. Arbitrary initial conditions were chosen for the simulation. The profile of the output variable x is shown in Figure 2.1**:**, where the state x is evolving with time aperiodically. To be sure that the variable x is indeed aperiodic, an autocorrelation of x is carried out, see Figure 2.2. Note that the time scale is shown as normalized time in these and subsequent figures and this is explained in section 2.7.2 later on.

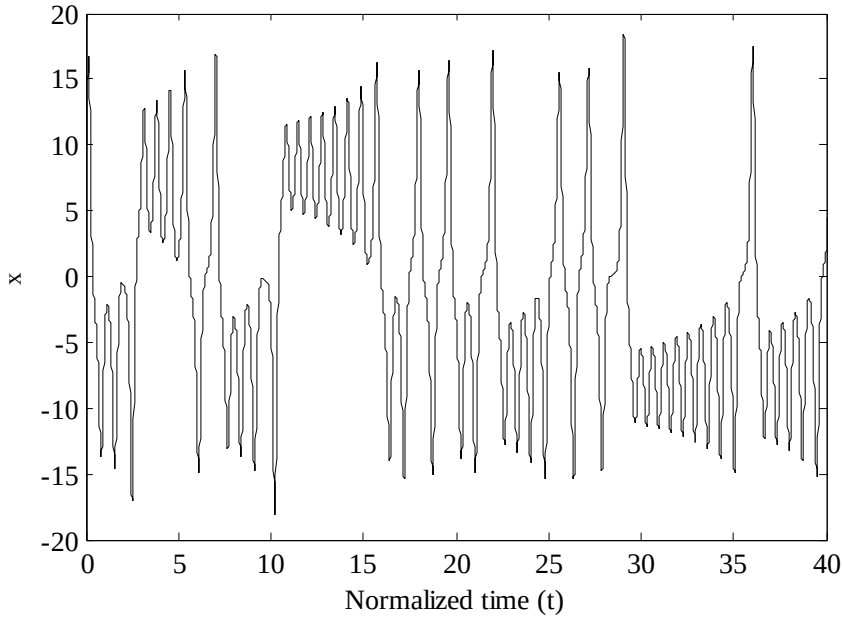


Figure 2.1: Representation of the time series for the x Lorenz variable.

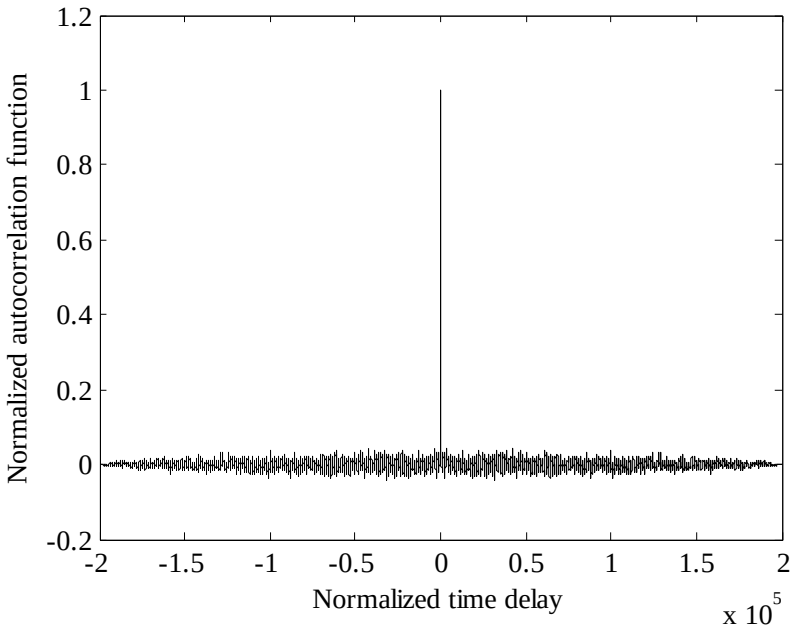


Figure 2.2: The normalized autocorrelation function of x Lorenz variable.

The variable x at any time instant is not similar to itself regardless of any amount of time shift. Therefore, its autocorrelation function only has a single spike at zero time shift. This

clearly demonstrates that the x variable is aperiodic in nature. The irregular behaviour is also true for other variables y and z. The second property in the definition for Lorenz system is trivial. The parameters used in the system are $\sigma$ = 10, b = 8/3 and r = 28, i.e. none of the parameters are stochastic. The irregular behaviour in the Lorenz system is arising because of the intrinsic non-linearity of the system itself rather than the noisy parameters.

Finally, to exhibit the sensitive dependence of system on initial conditions, the simulation is performed again. Two identical Lorenz systems (a & b) are taken with same parameters but starting from different initial conditions (nearly identical however). The difference in initial condition taken between two Lorenz variables $x_a$ and $x_b$ was chosen to be $10^{-6}$. Figure 2.3 depicts the time series of variables $x_a$ and $x_b$ for two Lorenz systems. After some period, the two variables quickly diverge from each other even though they started from identical initial conditions. Figure 2.4 illustrates the two variables diverging exponentially fast (straight line with positive slope on a log plot). This means a long term prediction of chaotic systems is not possible since the slightest error in the initial condition will result in an exponential increase in the error. This effect was explained by Lorenz in his weather forecasting model where he suspected that the long term weather prediction is improbable (butterfly effect).

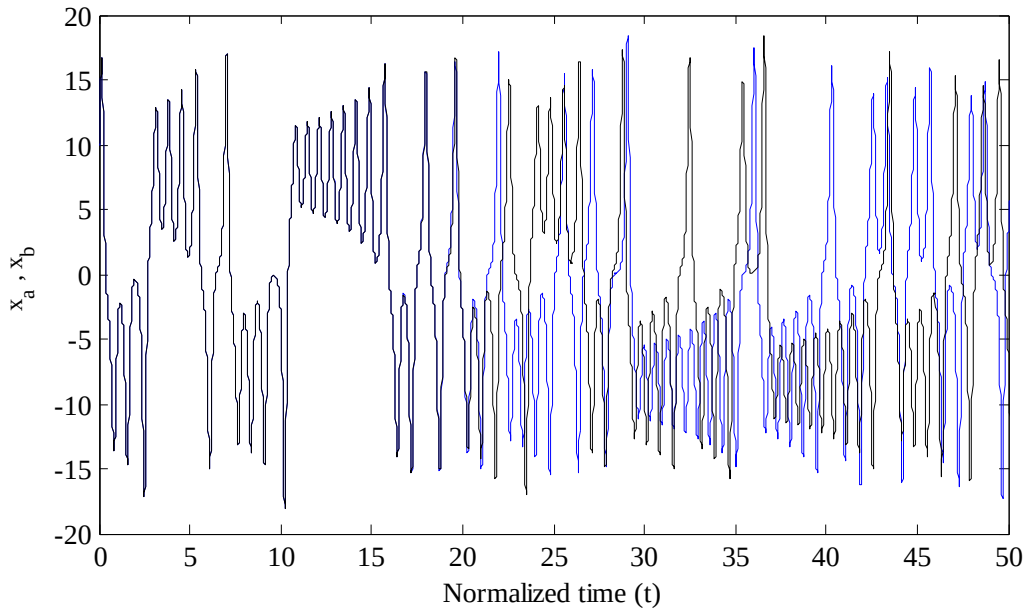


Figure 2.3: Time series plot of variables $x_a$ and $x_b$ of two similar Lorenz systems starting from a nearly identical initial condition.

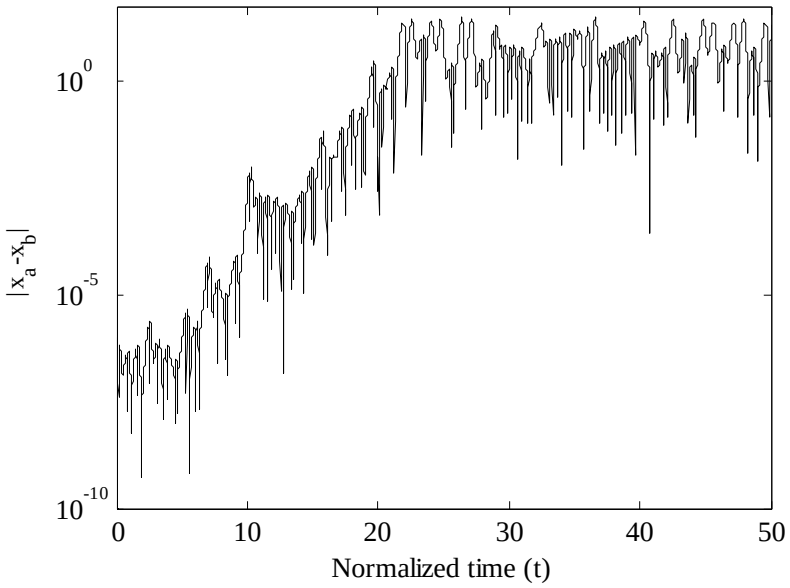


Figure 2.4: Log scale plot of $|x_a - x_b|$ to show exponential divergence of trajectories when started from a nearly identical initial condition in a Lorenz system.

Another nice property of chaos can be seen by plotting the variable z versus x of Lorenz system, see Figure 2.5. The figure shape is called the strange attractor, showing how x and z evolve against time, as well as demonstrating how a simple looking deterministic system could have extremely erratic dynamics where solutions oscillate irregularly, never exactly repeating but always remaining in a bounded region of phase space. The strange attractor is not a point or a curve or even a surface, it's a fractal with a fractional dimension between 2 and 3 [26].

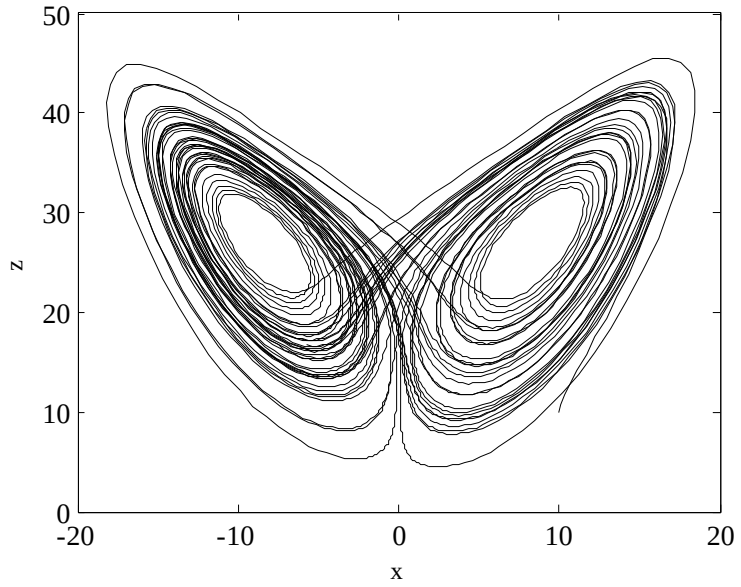


Figure 2.5: Strange attractor of the Lorenz system when plotting z against x.

One property of chaotic systems not included in the above definition but worth mentioning here is the sensitivity to parametric mismatches. Again two identical Lorenz systems (a and b) are taken starting with same initial condition but with nearly identical parametric values. For this, the difference in parameter $\sigma$ in the two Lorenz systems is taken to be $10^{-6}$. Figure 2.6 depicts the time series of variable x for two Lorenz systems, which clearly shows the two time series diverging from each other after some time. Figure 2.7 illustrates

the exponential divergence of trajectories of two systems, the increase in log scale being linear and the slope of which will give the Lyapunov exponent.

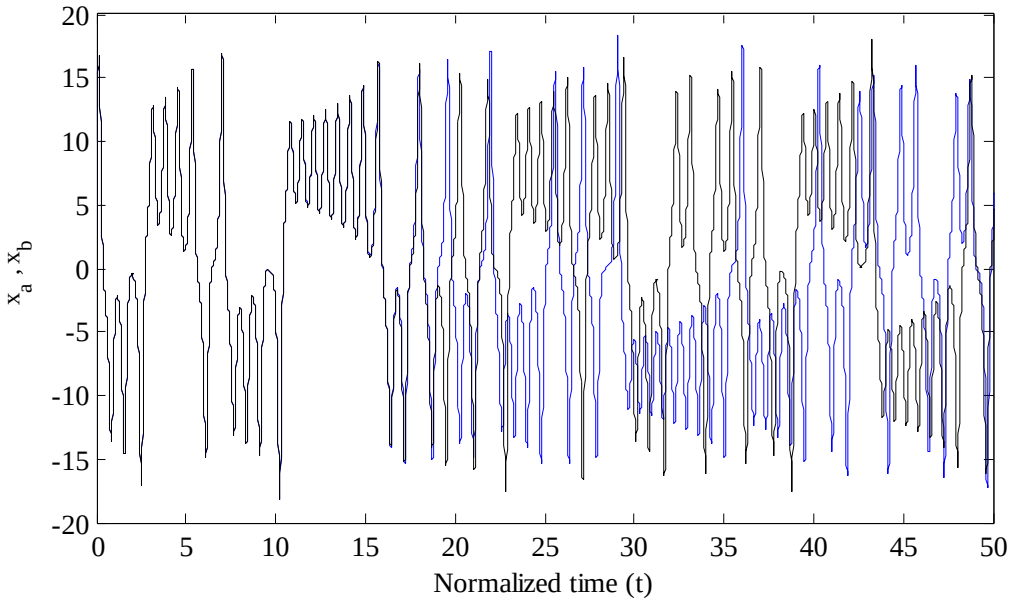


Figure 2.6: Time series plot of variables $x_a$ and $x_b$ of two different Lorenz systems for parameter values of $\sigma_a = 10$ and $\sigma_a - \sigma_b = 10^{-6}$ starting from the same initial condition.

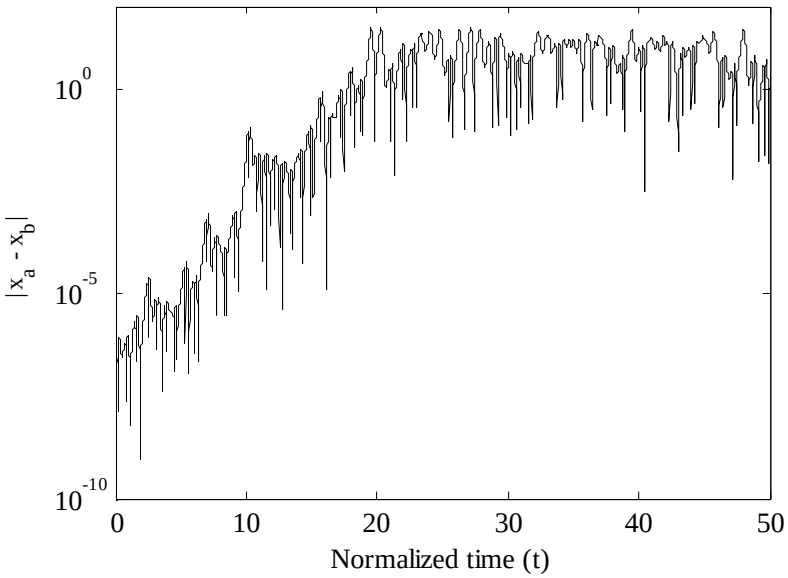


Figure 2.7: Log scale plot of $|x_a - x_b|$ to show exponential divergence of trajectories when a parameter mismatch of only $10^{-6}$ exists between $\sigma_a$ and $\sigma_b$.

## 2.3 Route to Chaos

When the parameters of a system are changed, chaotic behaviour may appear and disappear for a dynamical system. The idea of chaos and how it occurs in a system can be visualized by means of a bifurcation diagram. Bifurcation means splitting into two parts and is used extensively in the study of non-linear dynamics to illustrate any sudden change in the behaviour of the system when some parameters are varied. Therefore, bifurcation diagram shows qualitative changes in the system dynamics with a variation of certain system parameter values. For this purpose, let us take another example used to model population growth over time, known as the Logistic equation. The model is given in the form of a difference equation as [29]:

$$x_{n+1} = kx_n(1 - x_n). \tag{2.2}$$

where $x_{n+1}$ is the current population that depends on the previous population, $x_n$, and the growth rate is dependent on the parameter k. Depending on the value of parameter k, the behaviour of the system will be different. This is shown in the Figure 2.8, which is the bifurcation diagram for the Logistic equation. In this diagram, a plot is done for k in x-axis and different possible long term values of x on y-axis taking initial condition as $x_0 = 0.5$. It can be seen that when k is between 0 and 1, the orbit converges to zero. When k is between 1 and 3, the trajectory converges to some fixed point. At point k = 3, both the bifurcation and the trajectory enter an attracting periodic orbit of period 2. As k increases the period continues doubling with the bifurcation diagram splitting from period 2, 4, 8 onwards and with the trajectory being attracted to these periodic orbits. This will continues until k > 3.57, beyond which chaos become visible. It can be seen in Figure 2.8 that for value of k > 3.57, the trajectory of $x_n$ is not settling down to any fixed points or periodic orbits.

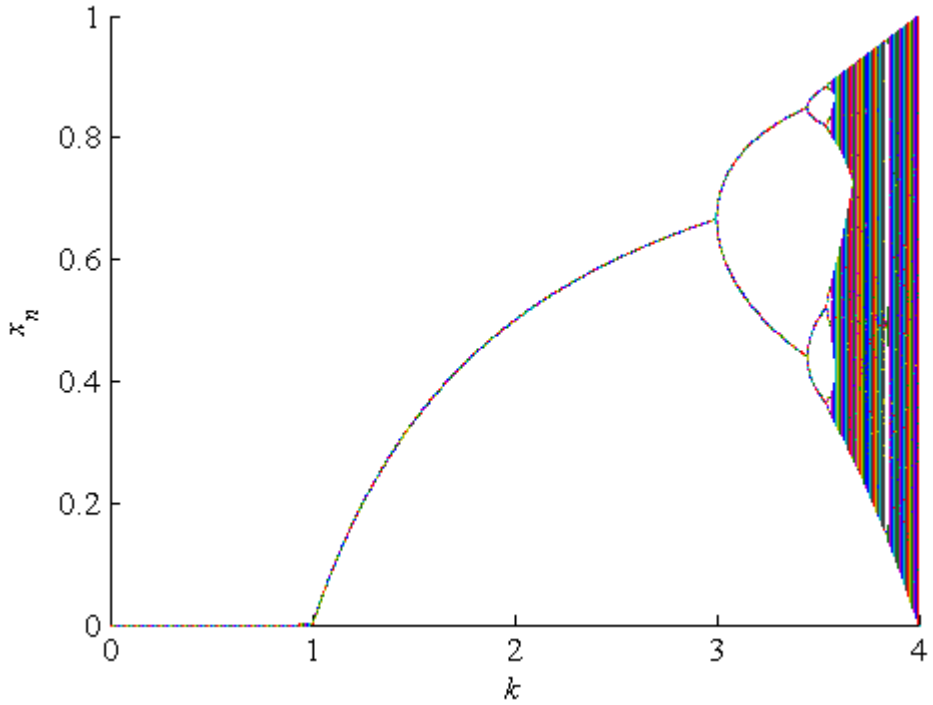


Figure 2.8: Bifurcation diagram for the logistic equation with varying k for initial condition $x_0 = 0.5$.

Now, let us consider the continuous 3-dimensional case of the Rossler equation [30]. Rossler equation is a set of 3 differential equations given as:

$$\begin{aligned} \dot{x} &= -y - z \\ \dot{y} &= x + ay \\ \dot{z} &= b + z(x - c). \end{aligned} \tag{2.3}$$

For the value of $a = b = 0.1$ and $c = 14$, the system will exhibit a chaotic behaviour. The bifurcation diagram for the system (2.3) is shown in Figure 2.9 for a range of parameter c. The diagram was plotted in Matlab by taking the local maxima of x for each varying parameter c value. Initial transients of the system were neglected. As shown, for lower values of c, system (2.3) has a periodic solution. At $c = 6$, period doubling is taking place and this will continue with increasing value of c until the system reaches a state of chaos. It

is now clear how bifurcation diagrams give the visual indication of potential chaotic behaviour on a system.

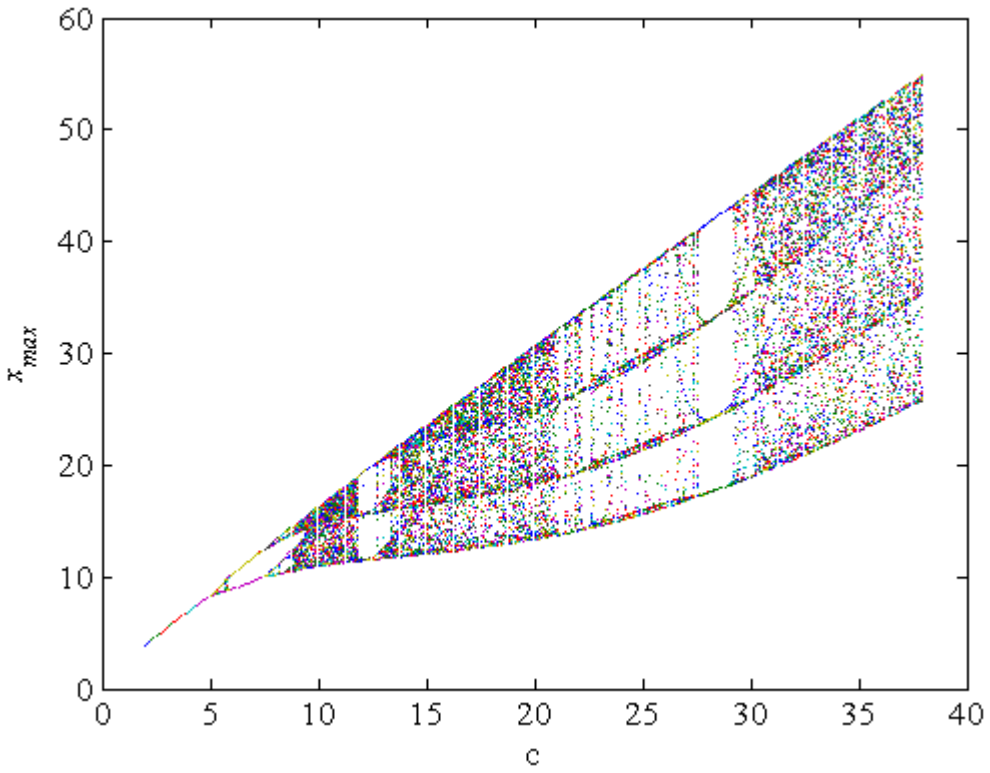


Figure 2.9: Bifurcation diagram for the Rossler equation.

The above examples demonstrated one particular route to chaotic behaviour. This is the most common route. We saw that there was splitting of the period, i.e. from period 1 to 2, then to 4 and so on until chaos emerged. This route is therefore called the period doubling route. Although there might be other routes to chaos that are not discovered yet, three routes are outlined in the literature which are:

i. **Period doubling route:** This is the simplest route and is the most extensively studied type of transition. As we have seen previously, examples are the Logistic and Rossler equations where the period increases from 2, 4, 8 and so on until chaos emerged.

ii. **Intermittency route:** In this route, a periodic signal (with no period doubling) has disturbances at random intervals from bursts of chaos/noise. When a chaotic parameter is increased, the frequency bursts increases making the oscillation totally chaotic [31, 32]. Intermittency appears in electronics, lasers, chemical reactions, hydrodynamics etc [33, 34]. Intermittency can also occur in Lorenz equation [26].

iii. **Quasiperiodicity route:** This route to chaos is caused by two or more simultaneous periodicities whose different frequencies are out of phase with one another such that the oscillations can never repeat itself exactly. However, it might seem (only) to repeat itself, thus the name Quasiperiodicity. A simple time plot cannot reveal the chaoticity but will require sophisticated mathematical tools for analysis. This route to chaos has been seen in electrical conductivity in crystals and heart cells of chickens [32].

## 2.4 Current Chaotic Systems

So we have looked at the Lorenz system and Rossler system, which are continuous time cases, and the Logistic map, which is a discrete time case. In this section other chaotic systems, which are quite popular and extensively studied, will be discussed. We shall see the systems both in continuous and discrete time domains.

### 2.4.1 Continuous Time Case

A) **Chua's circuit** – This is a simple electronic circuit that exhibits classic chaos theory behaviour, and was introduced by Leon O. Chua in 1983. It is a third order, reciprocal and has only one nonlinear element; a 3-segment piecewise-linear resistor and exhibits

a double scroll attractor [35, 36]. The Chua's circuit in the normalised form can be written as:

$$\begin{aligned} \dot{x} &= \alpha\big(y - x - f(x)\big) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y - \gamma z, \end{aligned} \tag{2.4}$$

where f(x) is the piece-wise linear function with constants $G_a$ and $G_b$ given as:

$$f(x) = G_b x + 0.5(G_a - G_b)(|x+1| - |x-1|). \tag{2.5}$$

$\alpha, \beta$ and $\gamma$ are the parameters of the system that governs the chaotic property, with a typical values of $\alpha = 10, \beta = -14.87, \gamma = 0, G_a = -1.27$ and $G_b = 0.68$. Figure 2.11 shows the circuit diagram of the Chua's oscillator consisting of two capacitors, one linear resistor, one inductor and one non-linear diode.

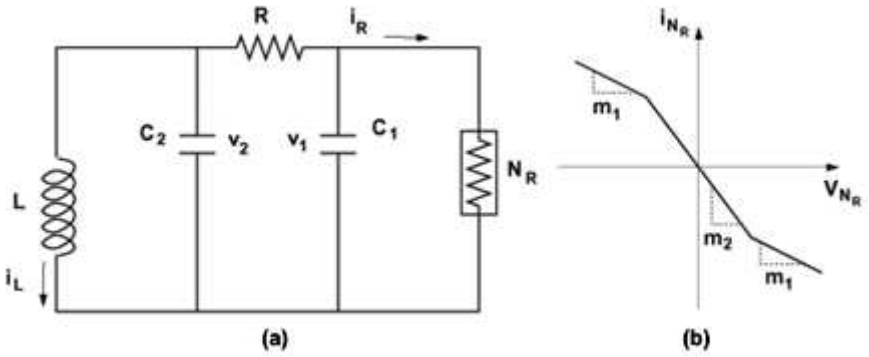


Figure 2.10: (a) Chua's circuit with two capacitors ($C_1$ and $C_2$), one linear resistor (R), one inductor (L) and once non-linear diode ($N_R$). (b) Characteristic curve of the non-linear diode.

B) **Duffing oscillator** – This is an example of a periodically forced oscillator with a nonlinear elasticity [37]. The following is the set of differential equation for which it exhibits chaotic property:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -\frac{x_1}{4} - x_1^3 + 11cost. \end{aligned} \tag{2.6}$$

### 2.4.2 Discrete Time Case

A) **Henon map –** Is a discrete-time dynamical system [38], and is one of the most studied examples of dynamical systems that exhibit a chaotic behaviour. It is represented by a set of difference equation given as:

$$\begin{aligned} x(n+1) &= y(n) + 1 - ax^2(n) \\ y(n+1) &= bx(n), \end{aligned} \tag{2.7}$$

where the parameters a and b determines the chaotic property of the map. Typically the value of a and b are taken as 1.4 and 0.3, respectively. The map was introduced by Michel Henon as a simplified model of the Poincare section of the Lorenz model [38].

B) **Henon 3D map –** This is a hyperchaotic system and is given as:

$$\begin{aligned} x_1(n+1) &= -bx_2(n) \\ x_2(n+1) &= 1 + x_3(n) - ax_2^2(n) \\ x_3(n+1) &= x_1(n) + bx_2(n), \end{aligned} \tag{2.8}$$

where a and b are the control parameters and for $a = 1.07$ and $b = 0.3$, the system exhibits a hyperchaotic behaviour [39, 40].

C) **Lorenz discrete map –** This is the discrete case of the Lorenz system and is given in the following difference equation [41]:

$$\begin{aligned} x_1(n+1) &= x_1(n)x_2(n) - x_3(n) \\ x_2(n+1) &= x_1(n) \\ x_3(n+1) &= x_2(n) \end{aligned} \tag{2.9}$$

Figure 2.11 shows the attractor for different chaotic system outlined above and also of the Rossler system that was encountered earlier.

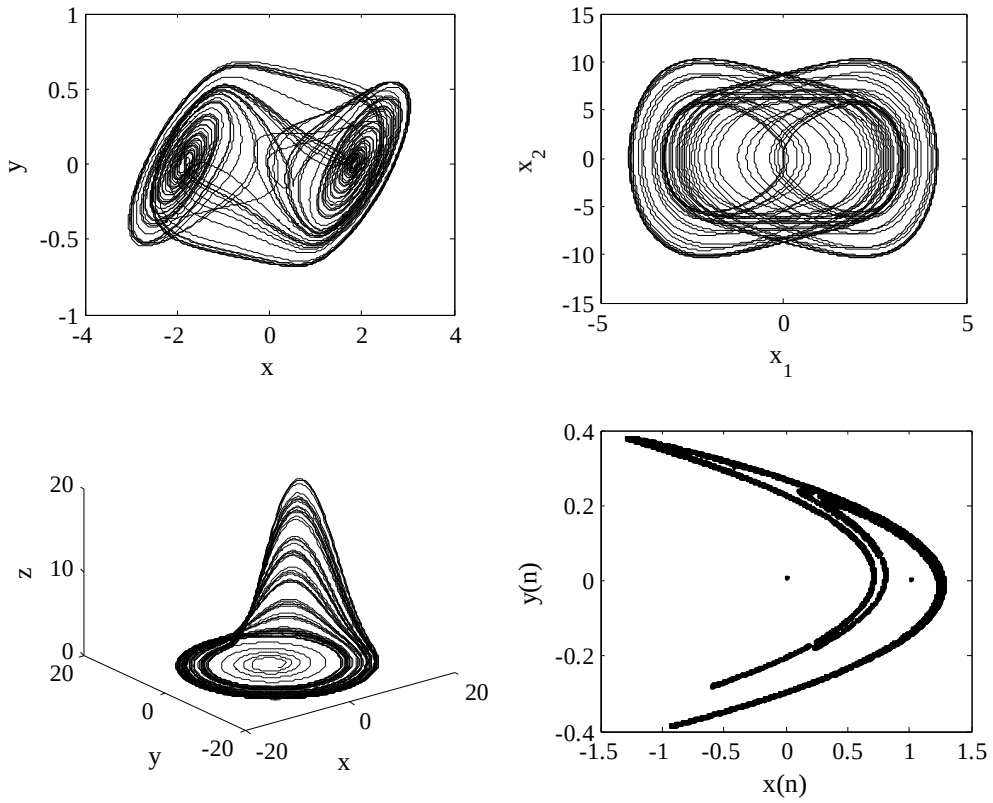


Figure 2.11: Chaotic attractors for different chaotic systems: (a) Chua's circuit, (b) Duffing oscillator, (c) Rossler system, and (d) Henon map.

## 2.5 Synchronization in Chaotic Systems

It might seem that chaotic synchronization is impossible to achieve in chaotic systems since they are very sensitive to initial conditions and slightest difference in the initial conditions will ultimately lead to totally different trajectories. But after the seminal work done by Pecora and Carroll [42] where they showed that it is however possible to synchronize two chaotic systems starting from different initial conditions under certain condition. They wrote;

"Chaotic systems would seem to be dynamical systems that defy synchronization. Two identical autonomous chaotic systems started at nearly the same initial points

in phase space have trajectories which quickly become uncorrelated, even though each maps out the same attractor in phase space. It is thus practical impossibility to construct, identical, chaotic, synchronized system in laboratory"

However, they showed subsequently that if two chaotic systems are linked together by a common signal, it is possible to obtain chaotic synchronization regardless of the initial conditions [42-44]. The word synchronization should not be taken in the sense of the periodic systems. In periodic systems, for example two pendulums are said to be synchronized when they are in phase, i.e. when their frequency of oscillation matched. But in a chaotic system, because chaotic signals are broadband in nature with no apparent frequency (aperiodic), synchronization has to be visualized in a different way. Synchronization in chaotic systems takes place when the trajectories of two or more systems converge to the same value, i.e. same trajectories, and will remain in step with each other [42]. For example, if x and y are two chaotic systems then they are said to be synchronized if $\lim_{t\to\infty}(x(t) - y(t)) \to 0$, i.e. all states of x and y are equal respectively as they evolve in time.

To describe the synchronization method developed by Pecora and Carroll, let's define an autonomous n-dimensional system as:

$$\dot{u} = f(u). \tag{2.10}$$

Now, the system in (2.10) is divided into two subsystems $[u = (v, w)]$ with dimensions m and k such that $n = m + k$.

$$\dot{v} = g(v, w), \dot{w} = h(v, w), \tag{2.11}$$

where $v = (u_1, \dots, u_m), g = \big(f_1(u), \dots, f_m(u)\big), w = (u_{m+1}, \dots, u_n),$

$g = \left(f_{m+1}(u), \ldots, f_n(u)\right)$.

Now, one of the subsystems is used as a drive system v in this case. Therefore, the response of subsystem $w'$ is identical to w with $v'$ being replaced by v as:

$$\dot{w}' = h(v, w'). \tag{2.12}$$

Note, the $w'$ being driven by v of drive system. w and $w'$ will synchronize only if $w - w' = \Delta w \to 0$ as $t \to \infty$. Now we have:

$$\begin{aligned} \dot{\xi} &= \dot{w} - \dot{w}' = h(v, w) - h(v, w') \\ &= D_w h(v, w)\xi \quad \text{for } \xi = \Delta w \to 0, \end{aligned} \tag{2.13}$$

where $D_w h$ is the Jacobian of h with respect to w only.

The behaviour of the system (2.13) will depend on the eigenvalues of the Jacobian matrix. Since the system is a chaotic there will be complication. If systems were to be periodic, then the eigenvalues of the appropriate Jacobain matrix would have determined the stability. But in this case, the eigenvalues are changing because the variables v and w are chaotically evolving with time. Therefore, average of the eigenvalues (transverse Lyapunov exponent) at each time instant should be taken in order to determine the Lyapunov exponent over the entire attractor of w subsystem. This average of the eigenvalues (transverse Lyapunov exponent) is called the conditional Lyapunov exponent (conditional because it depends on the chaotic variables) [43]. Pecora and Carroll have mentioned that systems will synchronize only if real parts of the Lyapunov exponents are negative [42]. However, the method does not mention about the initial conditions for which the systems will achieve synchronization. But since both the systems have same attractors, with time, the states of the systems will eventually come close enough in the

state space such that the condition put in (2.13) hold true. Therefore, the conditional Lyapunov exponent having a negative real part is only a necessary condition for achieving synchronization but not sufficient.

Let us now verify the synchronization method of Pecora and Carroll using the Lorenz system defined in (2.1). The drive system is given by:

$$\begin{aligned} \dot{x} &= \sigma y - \sigma x \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz, \end{aligned} \tag{2.14}$$

where the constants are taken as earlier.

The system (2.14) is decomposed such that y is the coupling signal for the response system and is equivalent to v in the proof shown earlier. Therefore, now the response system driven by y can be written as:

$$\begin{aligned} \dot{\hat{x}} &= \sigma y - \sigma \hat{x} \\ \dot{\hat{z}} &= \hat{x} y - b\hat{z}. \end{aligned} \tag{2.15}$$

Here we can see that the variable $\hat{y}$ has completely been replaced by y. The error dynamics can be written as:

$$\begin{pmatrix} \dot{e}_x \\ \dot{e}_z \end{pmatrix} = \begin{pmatrix} -\sigma & 0 \\ y & -b \end{pmatrix} \begin{pmatrix} e_x \\ e_z \end{pmatrix} \tag{2.16}$$

The eigenvalue for the error matrix fortunately is not dependent on the drive variable y. Therefore, the eigen value or the Lyapunov exponent of the subsystem can easily be calculated to be $\lambda_1 = -\sigma, \lambda_2 = -b$. This means both are negative at all times. Therefore,

the error variable $e_x$ & $e_z \rightarrow 0$ as $t \rightarrow \infty$, thus achieving full synchronizing of two systems despite the initial conditions.

Simulation is performed for (2.14) and (2.15) in Matlab. Figure 2.12 shows the variables x and $\hat{x}$ synchronizing quite fast to the same trajectory despite starting from a different initial condition. Figure 2.13 depicts the log plot of the error for variables x and $\hat{x}$ showing exponential convergence.

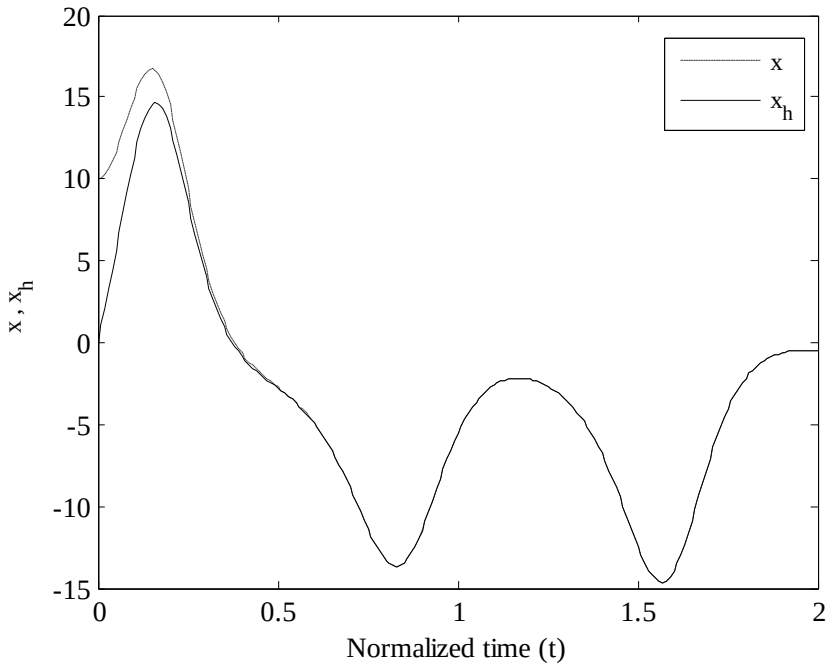


Figure 2.12: Convergence of two Lorenz systems starting from different initial conditions when coupled together showing synchronization using the Pecora and Carroll method.

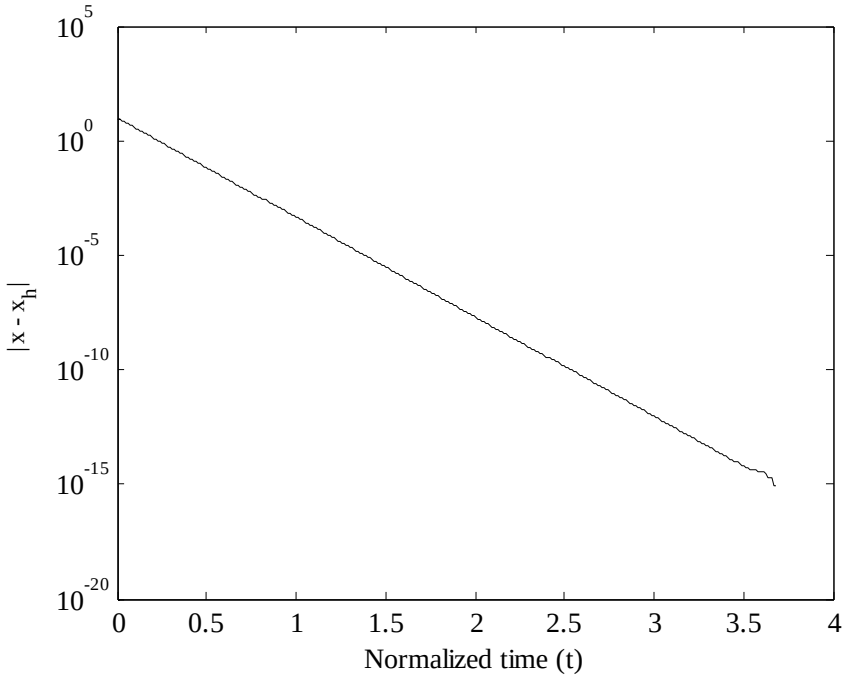


Figure 2.13: Log plot of $|x - \hat{x}|$ showing exponential convergence of two systems.

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

1. **Complete synchronization (CS):** The trajectories of the master and the slave systems converge to be exactly the same. This is the earliest and the simplest form of synchronization [42, 44, 45]. This occurs in coupled identical systems and is also referred as a conventional synchronization or an identical synchronization. Two continuous-time chaotic systems:

$$\dot{x}(t) = \mathrm{F}(x(t)) \tag{2.17}$$

and

$$\dot{\hat{x}}(t) = \mathrm{F}(\hat{x}(t)) \tag{2.18}$$

are said to obtain CS if:

$$\lim_{t\to\infty} \|\hat{x}(t) - x(t)\| = 0 \tag{2.19}$$

for any combination of initial conditions x(0) and $\hat{x}(0)$.

The nature of the coupling can have two possibilities. When the evolution of one of the coupled system is unaffected by the coupling mechanism, then this is unidirectional coupling or a drive-response coupling. However, when both the systems are connected to each other such that the evolution of both affects each other, then this type of coupling is called bi-directional coupling mechanism. CS can be achieved by various types of schemes such the Pecora-Carroll method [42, 44, 46] as explained above, the negative feedback [47], the sporadic driving [48], the active-passive decomposition [49, 50], diffusive coupling/hybrid methods [51] and observer based methods [52-57].

2. **Generalized synchronization (GS):** The trajectories of the slave system to the master's trajectories are one-to-one mapping of the function $\phi$ [45, 58, 59]. GS is used for synchronization for completely different systems where the output of one system is the function of the output of another system [60, 61]. System (2.17) and (2.18) are said to exhibit GS if:

$$\lim_{t\to\infty} \|\hat{x}(t) - \phi(x(t))\| = 0, \tag{2.20}$$

where the properties of the transformation $\phi$ are independent of the initial conditions x(0) and $\hat{x}(0)$. CS is a special case of GS where the mapping function $\phi$ is unity.

3. **Projective synchronization:** This is a special case of GS where one-to-one mapping function is a simple linear function $\phi(x) = \alpha x$ [62, 63].
4. **Phase synchronization:** The slave system phase converges to the masters but their amplitude may not be the same [64], thus can be formed by a weak coupling and is mostly achieved in coupled non identical systems.

5. **Lag synchronization:** The output of the slave system and the master system lock their phase and amplitude with a presence of a time delay $\tau_{lag}$. This is a special case of CS and phase synchronization [45, 65].
6. **Impulsive Synchronization:** In this case, the driving signal from master system is not sent continuously but sent as impulses determined by a fixed or time varying interval $\tau$ [66].
7. **Adaptive Synchronization:** Here some adaptive methods are applied for synchronizing the master and slave systems [67, 68].

It is seen that the synchronization of two chaotic systems, identical or non identical, is possible even it seems initially that the chaotic systems defy synchronization because of their inherent properties. There should be a coupling mechanism present between the two systems that are being synchronized.

## 2.6 Importance of Chaotic Signals in Communication Systems

One might feel that since the signals generated from chaotic systems are irregular in nature, therefore, these types of signals cannot have any practical applications and should be avoided. However, the properties of the chaotic signal can in fact be used in different field of communications engineering particularly spread spectrum applications. To achieve chaotic synchronization, there had to be some sort of coupling present between the two chaotic systems. If we consider unidirectional coupling, then a signal from one chaotic oscillator (drive system) is being transmitted to another chaotic oscillator (response system). This is analogous to communication systems where a carrier signal is modulated by a message signal prior to transmission. Therefore, the chaotic signals can be used as the carrier signal.

A range of chaotic signals properties as well as its advantages when used in communication systems are outlined as follow.

1. **Broadband spectrum** – This property is desirable for applications that require robustness against interference, jamming and low detection probability. Traditional communication systems address these issues by using spread spectrum and frequency hopping schemes, which have relatively complex synchronization between the transmitter and the receiver. For example, communication schemes utilizing frequency hopping entail re-synchronization of the receiver whenever the carrier frequency is altered. With chaotic systems, synchronization is easy to obtain while allowing the transmission of the broadband signal. Also, the inclusion of the message does not change the properties of transmitted signal.

2. **Aperiodic waveforms** – The chaotic signals are aperiodic in nature therefore the long term prediction of the trajectories can prove to be impossible. The distance between trajectories that start their evolution in the state space in close proximity increases exponentially with the positive Lyapunov exponent. This is an attractive property for secure communications since periodicity results in undesirable spectral peaks. Also, it is more difficult to develop forecasting models for non-periodic dynamics than it is for a periodic case.

3. **Sensitivity to initial conditions and parameters** – The chaotic system is extremely sensitive to small changes in initial conditions and parametric mismatches, i.e. the trajectory will be diverge completely if even slightly different values are used. This increases interest for the concept of chaotic hardware key for secure communications.

It is seen that the chaotic signals can be used in implementing secure communication links where the message spectrum can be hidden in the broad chaotic spectrum. Chaotic signals also provide limited predictability, anti jamming capabilities and reduced multi path effect [69, 70] as well because of its inherent properties. However, there are few disadvantages of the chaotic signals as compared to traditional communication systems. Studies have shown that chaotic communication schemes requires a larger signal to noise ratio (SNR) to obtain the same bit error rate (BER) performance as traditional communication schemes therefore are less efficient [71, 72]. Chaotic communication schemes are highly sensitivity to the noise and would normally require additional 3 dB or more of SNR than its traditional counterpart to deliver the same BER [71].

The focus of this thesis is to explore the different possibilities for chaotic signals to be used in secure communications and also remove the shortcomings of some of the methods that are available in the literature. Before that, let us see the relationships between the chaos and cryptography. Interestingly, the use of chaos in cryptography can be traced back to the Shannon's classic paper on cryptography [15, 73] where he gave a tight relationship between the two.

> *"Good mixing transformations are often formed by* repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, e*tc."*

This statement showed that Shannon's discussed about a typical route to chaos via stretching and folding [74]. Table 2.1 gives an overview of the relationship of the chaotic systems and cryptography.

Table 2.1: Comparison between chaos and cryptography properties [14].

| **Chaotic Property** | **Cryptographic Property** | **Description** |
|---|---|---|
| Ergodicity | Confusion | The output has the same distribution for any input |
| Sensitivity to initial conditions/ control parameter | Diffusion with a small change in the plaintext/secret key | A small deviation in the input can cause a large change at the output |
| Mixing property | Diffusion with a small change in one plain-block of the whole plaintext | A small deviation in the local area can cause a large change in the whole space |
| Deterministic dynamics | Deterministic pseudo-randomness | A deterministic process can cause a random-like (pseudo-random) behaviour |
| Structure complexity | Algorithm (attack) complexity | A simple process has a very high complexity |
| System parameters | Key | A small deviation in the system parameter can cause large change at the output |

There exist two main approaches of designing chaos-based cryptosystems: analogue and digital. Analogue based chaotic cryptosystems are secure communication links that are based on the unidirectional chaotic synchronization. Digital chaos-based cryptosystems (also called digital chaotic ciphers), on the other hand, are designed for digital computers, where one or more chaotic maps are implemented in finite computing precision to encrypt the plain-message in various ways, see [75-81] and references therein. Digital chaotic ciphers do not depend on the chaotic synchronization but they have initial conditions and/or control parameters used as the secret key. Analogue based chaotic cryptosystem can be implemented on continuous-time chaotic system or in discrete time chaotic maps. This thesis will deal with the analogue based chaotic crypto system. In the next section of this chapter, different methods that are available in the literature for implementing analogue based chaotic cryptosystem will be discussed.

## 2.7 Survey of Chaotic Communication Schemes

It is now known that since chaotic signals are aperiodic in nature and it is fundamentally broadband then it can be used to hide message signals in its wide frequency spectrum. Also, the sensitivity to initial conditions can also be exploited for multiple access techniques where different initial conditions might correspond to different codes for distinguishing between multiple users. But an interesting application remains the application of the chaos in providing security at the physical level for the message signal to be transmitted. Indeed, a number of techniques have been proposed [66, 75, 82-84]. Regardless of the method adopted, chaotic synchronization is required for successful message recovery.

### 2.7.1 Different Chaotic Communication Methods

Chaotic Masking, Parametric Modulation, Chaotic Shift Keying (CSK) and the Inclusion techniques are the most popular methods used for chaotic communications. Many other methods have also been proposed but almost all fall under one or more of these categories.

#### 2.7.1.1 Chaotic masking

This is one of the earlier methods to use chaotic signals for transmitting a message signal as described in [85-90] and is illustrated in Figure 2.14. In this scheme, a message signal is added, i.e. masked, to the output of a chaotic oscillator at the transmitter side prior to transmission.

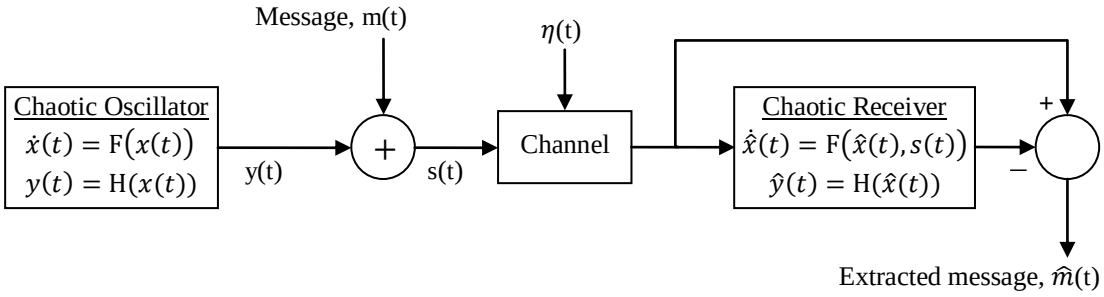


Figure 2.14: Chaotic communication scheme based on chaotic masking.

Upon receiving the signal at the receiver side, a chaotic synchronization is performed and the estimate of the chaotic component is subtracted from the received signal, thus recovering the original message signal m(t). The transmitter is given by the following state space representation as given by:

$$\begin{aligned} \dot{x}(t) &= \mathrm{F}\big(x(t)\big) \\ y(t) &= \mathrm{H}\big(x(t)\big). \end{aligned} \tag{2.21}$$

The output signal is y(t) which is the function of the transmitter state x(t). This is added to m(t) to form the transmitted signal s(t) which is given by:

$$s(t) = y(t) + m(t). \tag{2.22}$$

The common practice to choose y(t) is to opt for one of the components of x(t), however, in a general case $\mathrm{H}\big(x(t)\big)$ can be any function of x(t) as long as, at the receiver, chaotic synchronization is possible with the choice of the output signal. The receiver dynamic, which is being driven by s(t), is given by the following state space representation:

$$\dot{\hat{x}}(t) = \mathrm{F}(\hat{x}(t), s(t))$$
$$\hat{y}(t) = \mathrm{H}\big(\hat{x}(t)\big). \tag{2.23}$$

Now, when the receiver synchronizes with the transmitter, then:

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

Now, the estimate of m(t) can be done simply by subtracting the estimated $\hat{y}(t)$ from s(t):

$$\hat{m}(t) = s(t) - \hat{y}(t) \tag{2.24}$$

The addition of m(t) at the output y(t) of the transmitter can cause the degradation of the quality of synchronization at the receiver side since the driving signal is not quite the output of the transmitter but s(t). Therefore, the amplitude of m(t) has to be very small as compared to the chaotic signal, otherwise, the synchronization may not be possible and also the chaotic signal will no longer be able to hide the message spectrum. Chaotic masking has the advantage of simplicity and can be implemented very easily in electronic circuits [89]. However, the method of masking has been shown to be insecure and various cryptanalysis methods exist [91-96] that makes it possible to estimate the sender dynamics and decoding of the message signal.

#### 2.7.1.2 Chaotic parametric modulation

In the chaotic modulation technique, the message signal is used to modulate (change) one or many chaotic system parameters of the transmitter such that its trajectories keep changing in different chaotic attractors. This method is proposed and described in [88, 89, 97-100] and illustrated in Figure 2.15. The idea is to utilize the complex bifurcation space of the chaotic system such that the change in the parameter(s) due to the modulation of

message signal will not be known to the intruders even if they know the structure of the chaotic system. The output of the chaotic system is the transmitted signal.

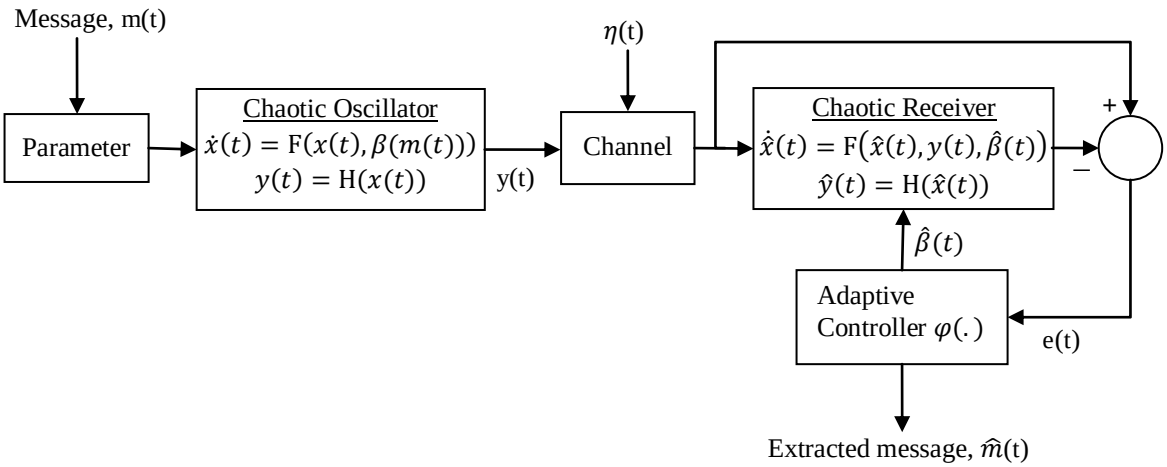


Figure 2.15: Chaotic communication scheme based on chaotic parametric modulation.

Now, at the receiver side, chaotic synchronization is performed along with some adaptive tuning of the parameter(s) such that the synchronization error approached to zero thus recovering the message signal. The transmitter is given by the following state space representation:

$$\begin{aligned} \dot{x}(t) &= \mathrm{F}(x(t), \beta(m(t))) \\ y(t) &= \mathrm{H}\big(x(t)\big). \end{aligned} \tag{2.25}$$

Here, the parameter $\beta$ of the system is being changed with m(t), thus resulting in different chaotic attractors. The output signal y(t) is the function of the transmitter state x(t) and is the transmitted signal.

Upon receiving y(t), the receiver dynamics is given by the following state space representation:

$$\begin{aligned}\dot{\hat{x}}(t) &= \mathrm{F}\left(\hat{x}(t), \hat{\beta}(t)\right)\\ \hat{y}(t) &= \mathrm{H}\left(\hat{x}(t)\right)\\ e(t) &= \hat{y}(t) - y(t)\\ \hat{\beta}(t) &= \varphi\left(e(t)\right).\end{aligned} \tag{2.26}$$

where $\varphi(.)$ is an adaptive function tuning the parameter $\hat{\beta}(t)$ such that e(t) approaches to zero thus achieving synchronization and recovering the message signal $\hat{m}(t)$. Although the method of modulation provides better security than the masking method, it is still shown to be insecure by various cryptanalysis methods [94, 95, 101-103].

#### 2.7.1.3 Chaotic shift keying

CSK is basically a special case of the parametric modulation technique devise to transmit digital message securely over a communication channel. In this method, depending on either 0 or 1 to be transmitted, outputs from two statistically similar chaotic attractors are taken. These two attractors are generated by the two chaotic systems that have slightly different parameters but having same structure. At the receiver, the chaotic system is tuned to the parameter corresponding to either 0 or 1 and thus synchronization will be achieved if the correct bit is transmitted else there will be no synchronization. Thus, by simply passing the error signal through a low pass filter and then thresholding the error signal, the digital bits could be recovered. This method was proposed and explained in [104, 105] and illustrated in Figure 2.16.

In CSK, switching between multiple attractors is also possible, see ref [106] thus transmitting a symbol in a duration of $T_s$. The number of bits $N_b$ that could be transmitted during $T_s$ is given by $N_b = log_2 M$ where M is the number of switching attractor.

Therefore, if we need to transmit either '0' or '1' in the symbol duration for binary signal, the required attractor is 2 as it was explained earlier.

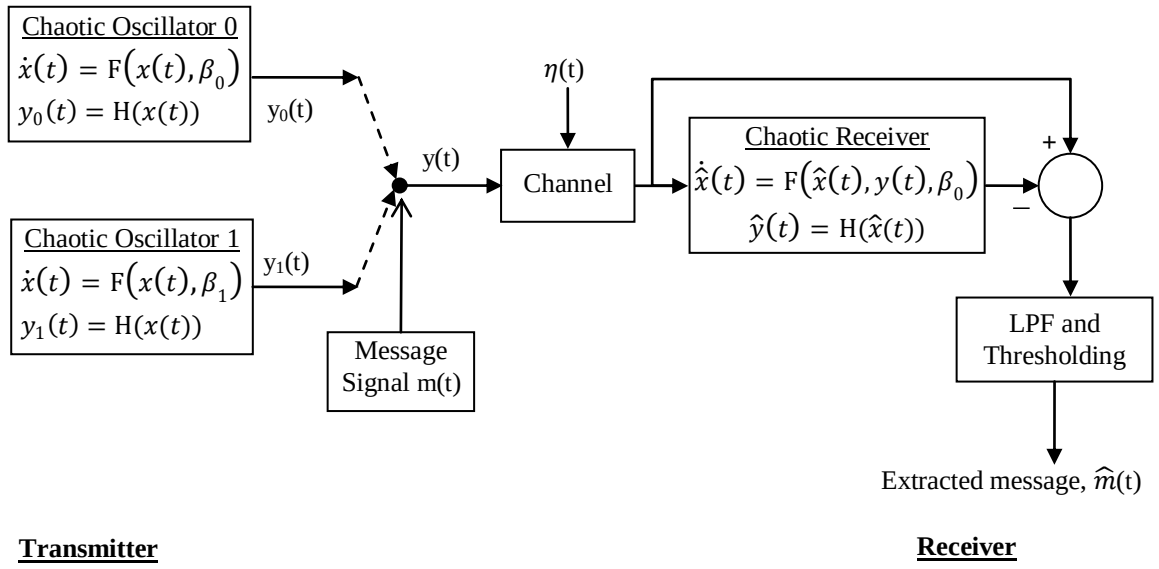


Figure 2.16: Chaotic communication scheme based on chaotic shift keying.

$T_s$ has to be long enough to ensure that the chaotic dynamics converges to one of the allowed attractors otherwise synchronization will not be possible at the receiver side in order to recover the message. $T_s$ depends on the largest negative Lyapunov exponent determining the rate of convergence to the attractor. The transmitter is given as:

$$\begin{aligned} \dot{x}(t) &= \mathrm{F}(x(t), \beta(m(t))) \\ y(t) &= \mathrm{H}\big(x(t)\big). \end{aligned} \tag{2.27}$$

If the binary signal (0, 1) is to be transmitted then, we have $M = 2$, therefore two parameters need to be defined for $\beta$, hence:

$$\beta(m(t)) = \begin{cases} \beta_0 \; when \; m(t) = 0 \\ \beta_1 \; when \; m(t) = 1. \end{cases} \tag{2.28}$$

y(t) is the output transmitted signal. At the receiver side, upon receiving the signal, chaotic synchronization is performed. The receiver is given as:

$$\begin{aligned}\dot{\hat{x}}(t) &= \mathrm{F}(\hat{x}(t), \beta_0) \\ \hat{y}(t) &= \mathrm{H}\big(\hat{x}(t)\big).\end{aligned} \tag{2.29}$$

The synchronization error signal will now be:

$$e(t) = \|\hat{y}(t) - y(t)\|. \tag{2.30}$$

such that,

$$e(t) = \begin{cases} 0 \; when \; 0 \; transmitted \\ otherwise \; when \; 1 \; transmitted. \end{cases} \tag{2.31}$$

So, from the error signal, the message could easily be recovered because of the obvious synchronization error that will exist because of the parametric mismatch. This type of message recovery is the coherent detection type. The message could also be recovered via a non-coherent detection scheme where synchronization is not required. The extraction of the bits is done by looking at the statistical attributes (such as bit energy distribution, variance, mean, etc) of the transmitted signal to which the attractor corresponds [107]. However, these statistical properties may allow the intruders to decode the message without any knowledge of the transmitter dynamics thus making it less secure than its counterpart, the coherent detection. Although CSK method is found to be robust with noise and parametric mismatches, it has also been found to be insecure [93-95, 101, 108, 109].

#### 2.7.1.4 Chaotic inclusion method

In this method, instead of changing the chaotic parameter as in the modulation, the message signal is used to change the chaotic attractor directly in the phase space. In

parameter modulations, switching was made between different trajectories in different chaotic attractors, however, in this technique, switching is made between different trajectories of the same attractor. Care should however be taken such that the inclusion of the message does not take the system away from the bifurcation space and destroy the chaotic nature of the system. At the transmitter, the message is included at one of states (or more) of the chaotic system and the output is transmitted. At the receiver, once synchronization is achieved, the message is recovered by some inverse operation. This method is explained in [54, 86, 110-112] and depicted in Figure 2.17.

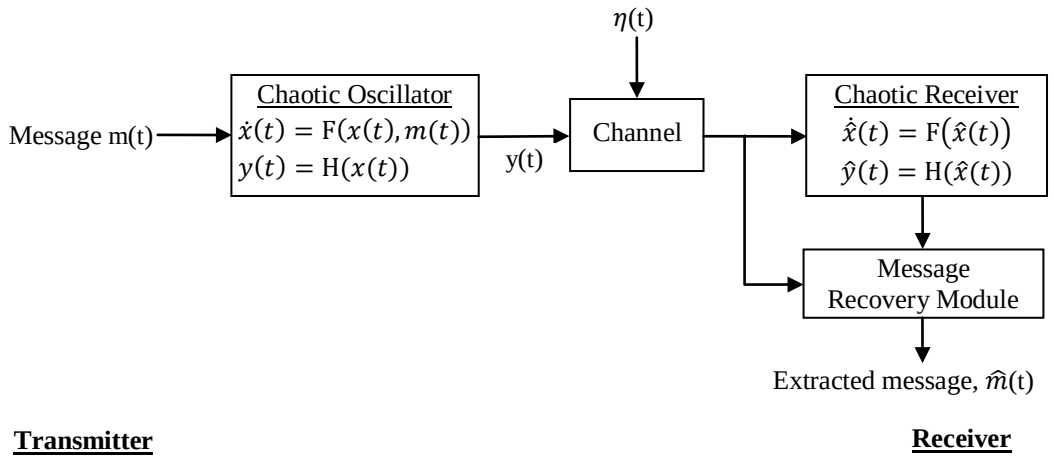


Figure 2.17: Chaotic communication scheme based on chaotic inclusion.

Since, the inclusion of the message as the input in the transmitter dynamics, the message recovery becomes unknown input problem in case of control theory where observers are used. Therefore, the system further has to satisfy the observability matching condition [54, 113-115] as well as the left invertibility property [115-118] so that it guarantees the possibility of recovering all states and the unknown input message at the receiver from y(t) and its derivates [55]. The transmitter is given as:

$$\begin{aligned} \dot{x}(t) &= \mathrm{F}(x(t), m(t)) \\ y(t) &= \mathrm{H}\big(x(t)\big). \end{aligned} \tag{2.32}$$

Here the message m(t) is included in the states of the chaotic system. At the receiver, the receiver dynamics is given as:

$$\begin{aligned} \dot{\hat{x}}(t) &= \mathrm{F}\big(\hat{x}(t)\big) \\ \hat{y}(t) &= \mathrm{H}\big(\hat{x}(t)\big). \end{aligned} \tag{2.33}$$

Now by applying the inversion as shown in [54, 86], the message is recovered under the left invertibility condition.

The method based on inclusion is also shown to be vulnerable to some attack methods [95] and therefore unsatisfactory without further modifications.

### 2.7.2 Some Considerations Regarding the Implementation of Chaotic Secure Communication

Few things are worth mentioning regarding the implementation of the chaotic communication system which will also be helpful in the later results chapters. One point worth pointing out is, are the chaotic signals really broadband? Since, the basic idea was to hide the narrow band message spectrum within the wide band of chaotic signals, therefore the chaotic signals being used as the carrier should have a wide spectrum. However, the power spectrum of the output signal from the Lorenz oscillator illustrates that the spectrum hardly exceeds beyond 4-5 Hz, certainly not a broad band signal by any means. Therefore, a message signal e.g. a sine wave with a frequency of 5 Hz after being masked with that chaotic signal will be easily detected from the observed spectrum of the masked signal. A simple high pass filter is all one needs to capture the message signal. Also, the power of the message signal should be considerably lower than the power of the chaotic carrier; otherwise once again the message signal will be clearly visible in the spectrum. This is

illustrated in Figure 2.18 where a sine wave with amplitude 1V and a frequency 5 Hz is masked with the output of the Lorenz oscillator.

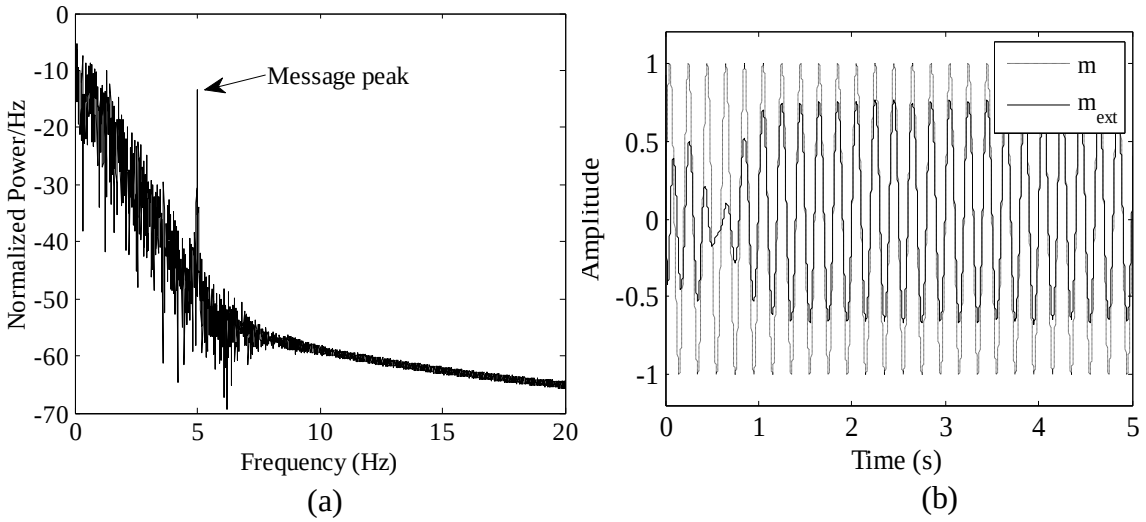


Figure 2.18: (a) Power spectrum of the chaotic carrier, and (b) message extraction using a high pass filter.

This example simply illustrate that this chaotic signal generated by the Lorenz equation is not really broadband. The chaotic signals are aperiodic, and are more or less noise like (chaotic signals are deterministic however). Even the autocorrelation function of the chaotic and noise signals are the same where the former is only equal to itself when there is no time delay, otherwise it's not related to itself in any time shift. The autocorrelation function for the output of the Lorenz oscillator is shown in Figure 2.2. The explanation of the spectrum of chaotic signals generated by the Lorenz equation not spanning more than 4-5 Hz is such that, the equation can be thought to be generating signals with respect to a normalized time. Therefore the Lorenz equation in its normalized form will generate a very slow time varying signal, but with no repeatability. So, if the time scale is de-normalized, then the chaotic signals can easily be made a broadband signal. Hence, it should be understood that a chaotic oscillator generates signal in the normalized form i.e. $\dot{x}$ should be seen as $dx/d\tau$ such that the normalized time $\tau$ = t/T. T is a normalizing time factor and

therefore, normalized angular frequency $\omega_{norm} = \omega T$. In this thesis, we provide all results by taking T equals to 1.

Therefore, a key point when using chaotic signals as the carrier is that the frequency of message signal should be such that it is completely buried inside the spectrum of the chaotic signal. This means when a chaotic system is used for demonstrating any of the above methods, the message signal should have considerably lower frequency well within the power spectrum of the chaotic carrier regardless of frequency being used. The system can easily be extended to support higher frequencies by de-normalizing the chaotic carrier signal. Therefore, all illustrations later on in this thesis will show a very low frequency message signal being transmitted i.e. when taking normalized time T = 1. Therefore, with the earlier explanation, it should be clear that it is not the limitation of the chaotic communication and the examples are shown only for verification purposes.

### 2.7.3 Chaos-based Attack Methods

Various attack methods were proposed in the literature to break the methods of masking, modulation, inclusion and CSK and decode the message signal without any information about the transmitter dynamics. The methods were mostly based on signal processing. The cryptanalysis of chaos based communication systems can be done in either of the three possibilities [14].

a) Extraction of the chaotic carrier signal from the transmitted signal to recover the message signal by removing the estimated carrier signal from the transmitted signal.
b) Direct extraction of the message signal from the transmitted chaotic signal.

c) Estimation of the secret parameters of the chaotic systems from the transmitted chaotic signal to completely break the system.

Now, let us talk about various well known chaos-based attack methods that are available in the literature.

#### 2.7.3.1 Chaotic carrier extraction based on non-linear dynamic (NLD) forecasting

This method is one of the first proposed methods to attack the chaotic communication methods. This method is useful in extracting message signal that use chaotic masking and modulation techniques. In the NLD forecasting method, first of all, the chaotic carrier signal is extracted from the transmitted signal which is then removed from the transmitted signal to reveal the message signal. Although well known and quite popular technique, this suffers from not being able to extract the message accurately and also may not be used in varied modulation technique. The details of this technique are available in these references [91, 102, 119-121].

#### 2.7.3.2 Power spectral analysis and filtering

As it was pointed out in the earlier section of some consideration regarding the implementation of the chaotic communication system, the message spectrum may peak out if spectral analysis of the transmitted chaotic signal is done. This is because, popular chaotic systems like Lorenz, Duffing, Rossler, Chua's, etc in its standard normalized form do not produce a really broadband signal but instead produce a narrow band signal. Consequently, the chaotic signal will not be able to hide the message spectrum successfully if higher frequency for message is chosen for implementation. Attackers therefore will be able to use this information and simply high pass filter the transmitted signal to accurately

extract the message signal as shown in Figure 2.18. This attack is very powerful because no prior knowledge of the system structure or configuration is required. However, if the consideration in the section 2.7.2 is fulfilled then this attack can be avoided. This technique is the direct extraction of message signal from the transmitted chaotic signal and details are available in these references [93, 96, 103, 122, 123].

#### 2.7.3.3 Generalized synchronization technique

The GS method that had been discussed earlier can also be used an attack options to chaotic communication methods, particularly the CSK method. The GS attack method is first proposed on [108]. In this technique, the precise knowledge of the chaotic transmitter is not known. It is also assumed that the chaotic receiver designed using GS will never synchronize to the unknown chaotic transmitter because there exists some significant difference both in the structure and parameters (which is regarded as key in the cryptosystem) between the transmitter and the intruder receiver. However, this technique will be able to decode the binary message signal as good as the legible receiver that has same structure and parameters as of the transmitter. In CSK, the trajectory of the transmitter is switched between two chaotic attractors, and hence GS transformation is also switched to two different ones. Now, if the difference between the GS transformation corresponding to 0 and 1 is big enough, then the hidden message can be detected. The key thing is to measure the synchronization error over time, then will be possible to detect the switching of the two attractors in the transmitter as a variation in a square error. GS is used for breaking other type of method as mentioned in [124]. The GS based attack is depicted in Figure 2.19. The CSK system is based on Lorenz system with parameter b switched between 4 and 4.4 when 0 or 1 is transmitted respectively and at the intruder receiver the parameter is set blindly at 4.6.

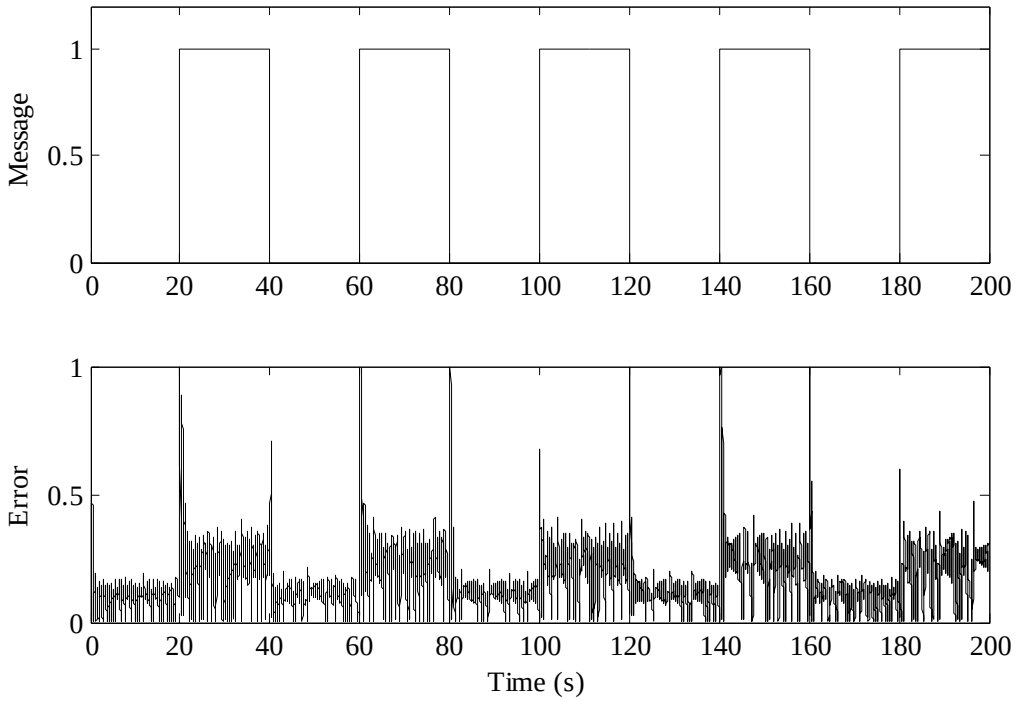


Figure 2.19: GS based attack on the CSK method that uses the Lorenz system: (a) the transmitted binary message, and (b) the error signal at the intruder receiver.

#### 2.7.3.4 Artificial neural network (ANN) technique

Neural networks can also be used to attack the chaotic communication methods especially the CSK. In CSK, switching is done between two attractors depending on the transmitted binary value. Although the information is concealed in the time domain analysis of the signal, other analysis may not be able to hide the message. In [94], the authors had proposed a technique to attack CSK method based on NN. It consisted of 2 steps. In the first step, the time series of the transmitted signal are transferred in the spectral-temporal space by using a spectrogram that is a moving window of FFT of the time series. The spectrogram is used of retrieving the evolution of the spectral characteristics of the transmitted signal thus the cryptanalysis problem is transferred in a two-dimensional pattern classification. In the second step, the pattern classification problem is solved by two single layers NNs. The 2 layers of NNs is first trained using some sample training sets

for optimization. Since, the CSK method clearly makes switching between two signals, the cryptanalysis simply became a pattern classification problem and can be cracked by intruders using ANN.

#### 2.7.3.5 Return map (RM) technique

RM is one of the popular methods to attack the chaotic communication methods. In [93], the RM was successfully utilized to break methods based on CSK and in [95], it is further shown that RM could be used to attack methods based on masking, modulation, inclusion and CSK. The RM looks for the maximum and the minimum return of the signal, analyses them and plot against each other. If $x_i$ and $X_i$ are the i-th minima and maxima for a signal y, respectively, then RM can be obtained by plotting $x_i$ versus $X_i$ in a simple case. Also if RM is to be obtained as explained in [93], then lets define $A_i = (X_i + x_i)/2$ and $B_i = (X_i - x_i)$. The plot of $B_i$ with respect to $A_i$ will be the return map of the signal y. Figure 2.20 illustrates the RM of the transmitted signal using CSK method that implements the Lorenz system switching between values 4.0 and 4.4 for the parameter b. Distinct two branches are seen and by checking which strip the point ($A_i$, $B_i$) falls on, one can easily unmask the current value of the binary message signal. Since one has to assign either 0-bit or 1-bit to a strip in each segment, it was claimed in [93] that there are only seven chances to make wrong assignments, which can be easily detected by observing the waveform of the reconstructed message signal.

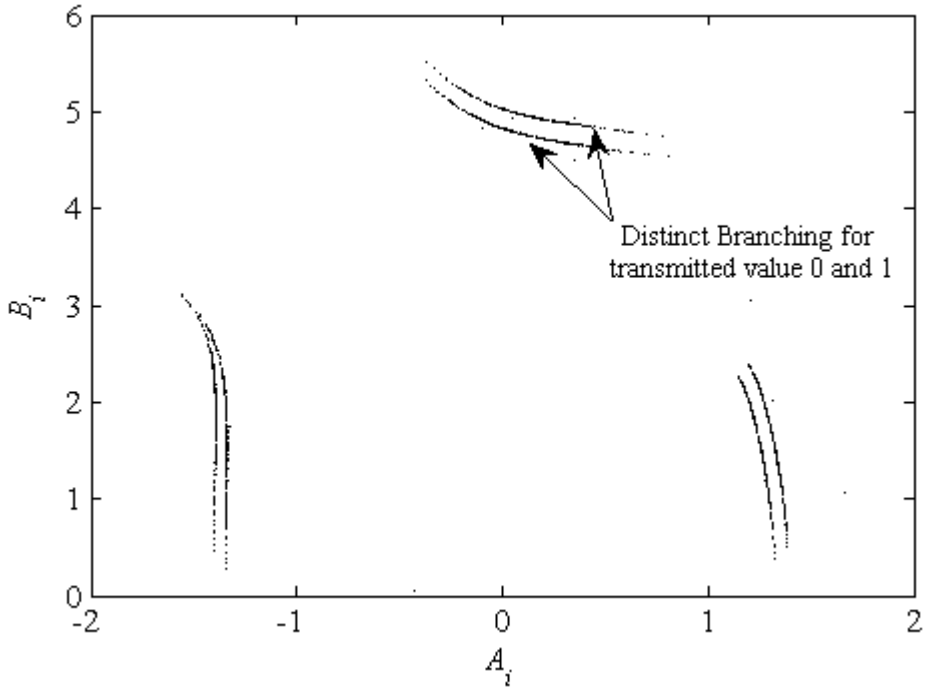


Figure 2.20: Return map of the transmitted implementing CSK method.

### 2.7.4 Various Other Modified Techniques

It is seen that various chaos based communication systems are available in the literature but along with them different attack methods are also available such that intruders are able to extract the message signal without actually knowing the chaotic transmitter structures, dynamics, parameters, etc. Be it masking, modulation, inclusion or CSK methods, all methods are found to be insecure by one method or two. Researchers have moved forward and proposed various modifications on these methods. Indeed, various other methods have been proposed, see [40, 63, 66, 70, 84, 90, 125-153] and references therein. These methods were based on concepts such as two channel transmissions, modifications of masking or modulation or inclusion techniques. But, almost all techniques repeated the same shortcomings as mentioned for previous methods and did not quite took into considerations of various attack methods, since researchers concentrated on only proposing newer

methods. Other proposed methods based on the projective synchronization [63], phase synchronization [99], GS [154] were broken as well [124, 155]. Researchers also suggested to use hyperchaos in order to improve the security of the communication system [156-158], because hyperchaos increased the randomness and unpredictability of the chaotic system. However, it was shown later that NLD forecasting can be used to attack hyperchaos based methods of a six dynamics [120]. Next, it was the use of time-delay systems. It is known that even simple time-delay systems exhibit hyperchaotic property [159]. Therefore, time-delay system was used [160] as an alternative for providing secure methods with low detectability since chaotic attractors of time-delay systems can have much higher dimension and many more positive Lyapunov exponents. But the time-delay based method was broken as well [161]. A method based on cryptography was also proposed which used an additional encryption algorithm to add complexity of the system [1], however NLD based forecasting method was later employed to attack this type of system as shown in [119]. The method based on cryptography has nevertheless good scope to improve the security. Heterogeneous chaos based cryptosystem was also proposed which used a combination of masking and modulation technique or CSK and modulation as shown in [162, 163] however this was shown to be insecure by method mentioned in [164]. Another method based on adaptive chaotic synchronization and modulation as proposed in [165] but was soon broken in [103]. The list of different methods and then subsequent attack methods has kept on growing over the last decade.

Researchers also tried to improve the existing modulation techniques and CSK techniques and provided security analysis by showing that methods such as NLD or RM are not useful. In [134], a periodic signal is combined with one state of the transmitter to modulate the transmitted signal so as to blur the reconstructed RM in order to frustrate the attacker. However, it was soon broken in the work described in [135, 166, 167] by distinguishing

the phase and angular frequency of the periodic modulating signal and then removing it. A modified scheme of the original method of [134] was proposed in [135] to further improve its security. However, in the work mentioned in [168] this modified modulating scheme is still shown not to be secure enough and that the modulating signal can even now be effectively removed via parameters estimation. CSK method has also been modified such as in [136, 169] etc, but was shown to be not quite secure enough as pointed out in [109, 144]. Therefore, it shows that still proposing new techniques for secure communication using chaotic signals is quite a challenging task considering different attack methods and various challenges. This thesis will therefore talk about various possibilities on how the challenges can be met and newer and secure methods are possible.

## 2.8 Summary

In this chapter, an introduction to chaos and its possibility to be used in chaotic communication for implementing security directly at the physical was presented. The introduction of chaos was provided with its fundamental properties. It was known that chaotic systems are highly sensitive to initial conditions, generates fundamentally broadband signals that are aperiodic. Although, chaotic signals seem like random signal, they have deterministic dynamics. These properties therefore are useful for implementing them in secure communication. Furthermore, different route to chaos were discussed and few examples were mentioned. It was also discussed that even though chaotic systems shows sensitivity to initial conditions, etc, it is still possible to synchronize two chaotic systems starting from different initial conditions under some conditions. The possibility of chaotic synchronization further opened the door to implement them in analog based secure communication. We also in brief showed how synchronization is possible mathematically

and talked about various types of synchronization and various ways of obtaining synchronization. Different methods available in the literature for implementing chaotic communication was then discussed, methods such as chaotic masking, modulation, CSK and inclusion methods were discussed in detail since these models form the foundation of chaotic communication and are very important to understand newer techniques. It was also presented that these methods were not very secure and lots of different attack methods existed such as NLD based forecasting, power spectral analysis, RM, ANN, etc. Different variations and techniques were also discussed and it was concluded that there still exists the requirement to come up with a better technique such that secure communication can be realized where the existing attack methods will not be useful. Now, in the chapters to follow in this thesis, newer modified methods will be proposed and explained.

# Chapter 3 Observer Based Synchronization: Application to Secure Communication

## 3.1 Introductions

In the previous chapter, we had talked about chaotic synchronization and we saw that different form of synchronization exist such as CS, GS, etc. The use of chaotic systems in communication systems will mean that it is necessary to transmit a signal from one system to another, thus forming a unidirectional coupling, which is essential for synchronization. The attention of this chapter will be limited to CS on unidirectional coupled system and will discuss an idea of observers for achieving CS. From here on wards the term synchronization for CS will be used throughout the chapter unless stated explicitly.

Many methods have been proposed for achieving synchronization such as Pecora & Caroll method [42, 43], an active-passive decomposition [170], an Extended Kalman filtering approach [171, 172], an observer based approach [52, 53, 57, 173] etc. Amongst all these methods, the observer based synchronization is the most promising method which is the focus of this chapter. Before going into details of observer based synchronization, we start by recalling some basic concepts on observer design theory.

## 3.2 Some Recalls on Observers

Roughly speaking an observer is basically a software sensor that permits to provide an estimation of the unmeasured states variables of a system. In more precise terms, an observer is a dynamical system that uses the available measurements (inputs and outputs)

to provide an estimation of the state variables that are not available to be measured. The basic block diagram of the observer is shown in Figure 3.1.

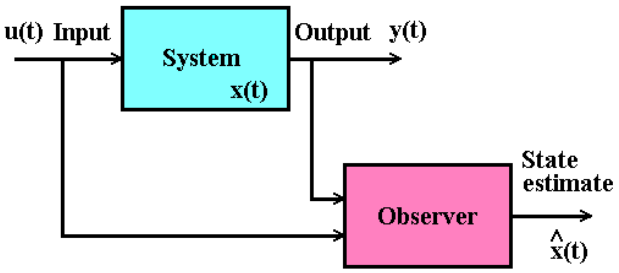


Figure 3.1: Block diagram of an observer.

### 3.2.1 Mathematical Description of Observers

Consider the general nonlinear system described by

$$\begin{cases} \dot{x} = f(x,u) \\ y = h(x) \end{cases} \tag{3.1}$$

where $x \in R^n$, $y \in R^p$, $u \in R^m$, $f : R^n \times R^m \to R^n$ and $h : R^n \to R^p$ are assumed to be smooth functions.

The observation problem is addressed when $p < n$ (we have less sensors than the number of state variables). This means that we do not know the initial condition of part of the state variables. The observer is generally described as:

$$\begin{cases} \dot{z} = g(z,u,y) \\ \hat{x} = l(z) \end{cases} \tag{3.2}$$

where $z \in R^n$ is the state of the observer and $\hat{x}$ is the estimate of the state $x$ such that $\lim_{t\to\infty} \|x - \hat{x}\| = 0.$

The above is a general definition of observer. In practice, it is not easy to design an observer for a general system. Also, there is no systematic method to design the function

g and l for any given dynamical system given by (3.1).

For this reason, we generally impose a specific structure for an observer as follows:

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}, u) + \psi(y - h(\hat{x})) \\ y_{obs} = \hat{x}. \end{cases} \tag{3.3}$$

Such a structure is interesting in the sense that if $y(t) - h(\hat{x}(t)) = 0$ after some time, say $t_1$, then the two systems (3.1) and (3.2) become identical and $\hat{x}(t) = x(t)$ for all $t \geq t_1$; due to the unicity of solution of the above system.

The observer therefore mainly amounts to the design of the function $\psi$ - known as the gain of the observer - such that the estimation error $\lim_{t\to\infty} \|x - \hat{x}\| = 0.$

Note that the observation problem is basically an initial condition problem because if we know $x(0)$ then there is no need for an observer. The integration of the above model (3.1) would suffice to find all state variables provided the model is perfect and there is no measurement noise.

Various types of observers exists in the literatures such as the classical Luenberger observer also called proportional observer as will be explained later, the sliding-mode observer [55], the proportional-integral (PI) observer [174], adaptive observer [148, 175], the neural observer [176], etc.

### 3.2.2 Observability

In order to design an observer for a system, we need to analyse the observability of the system. Observability is the property of a system that determines whether an observer design is possible or not.

Definition 1. The system (3.2) is said to be observable on a time interval [0, T] if for any two distinct initial conditions $x_0$, $\bar{x}_0$ there is an input $u(t)$ defined on $[0,T]$ such that the

output $y(x_0,u,t)$, $\bar{y}(\bar{x}_0,u,t)$ corresponding to these initial conditions when the input $u(t)$ is applied to the system, are also distinct.

Roughly speaking for two different initial conditions we should obtain two different outputs. Note the above definition suggest that the observability of a system depends on the inputs applied to the system.

For linear systems, however, the above definition is true for all inputs and in particular for the input $u = 0$. Because of this special property, the observability of linear systems of the form

$$\begin{cases} \dot{x} = Ax + Bu \\ y = Cx, \end{cases} \tag{3.4}$$

where $x \in R^n$, $y \in R^p$, $u \in R^m$ amounts to checking whether its corresponding observability matrix

$$O_x = \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} \tag{3.5}$$

has full rank or not. This is the so-called observability rank condition. Note also that for linear systems $O_x$ does not depend on $u$.

### 3.2.3 Nonlinear Observer Design

As mentioned above the observability of nonlinear systems depends on the inputs. This means that the same nonlinear system can be observable for some set of inputs while being unobservable for another set of inputs. The sets of inputs that render the nonlinear system unobservable are called singular inputs. The sets of inputs that render the nonlinear system observable are called universal inputs.

The singular inputs, in fact, constitute the main bottleneck for nonlinear observer design. Such a situation does not occur in the linear case as we have seen previously.

Let us consider an example in order to clarify the issue with singular inputs. In effect, consider the following 2-dimensional system:

$$\begin{aligned} \frac{dx_1}{dt} &= x_2 + ux_2 \\ \frac{dx_2}{dt} &= 0 \\ y &= x_1. \end{aligned} \tag{3.6}$$

For $u(t) = -1$ , this system is not observable. Therefore, u(t)= -1 is a singular input for the above systems. Every input $u(t) \neq -1$ are universal.

As a matter of fact, we cannot speak of observability in a broad sense as in the linear case. We can only design observers for classes of nonlinear systems; that is, we have to characterise those classes of nonlinear systems for which we can design an observer.

In particular, we can ask the following question: is there a class of nonlinear systems which is observable for all inputs? The answer to this question is yes and the class of such systems is called uniformly observable systems. For this class of system, the theory of observer design is well established. For more details see [177-179].

One important subclass of uniformly observable systems are those that have linearisable error dynamics and will be discussed next.

### 3.2.4 System with Linearisable Error Dynamics

One important subclass of nonlinear systems of the form (3.2) are those that can be transformed via a change of coordinates into the following output injection form as:

$$\begin{cases} \dot{x} = Ax + Bf(y) \\ y = Cx. \end{cases} \tag{3.7}$$

where the pair of matrices (A,C) is rank observable. Such systems are also uniformly observable; that they are observable for all inputs.

A fairly large class of chaotic systems are transformable into the above form as we shall see in the subsequent chapters.

An observer for the above system (3.8) can be defined as:

$$\dot{\hat{x}} = A\hat{x} + Bf(y) + K(y - C\hat{x}). \tag{3.8}$$

Setting $e = x - \hat{x}$, then the error dynamics is given as

$$\dot{e} = (A - KC)e = A_c e. \tag{3.9}$$

The observer gain K can be chosen such that all the eigenvalues of matrix (A - KC) have negative real part. Then, the error will converge exponentially to zero. Hence, the state x will converge exponentially to the estimated state $\hat{x}$ regardless of the initial conditions x(0) and $\hat{x}(0)$.

### 3.2.5 Proportional Integral (PI) Observers

Note that in the above observer (3.9) the correction term $K(y - C\hat{x})$ is proportional to the output observation error ($(y - C\hat{x})$). For this reason, the above observer is called a 'proportional observer'. However, nothing prevents one to add an additional term to the observer that is proportional to the integral of the output observation error; that is,

$$\dot{\hat{x}} = A\hat{x} + Bf(y) + K(y - C\hat{x}) + K_i \int (y - C\hat{x})dt \tag{3.10}$$

In such a case the observer is called a proportional integral observer; in short a PI observer.

It is shown in [174] PI-observer shows more resilience to noise. Also, it is simpler in terms of its design compared to sliding-mode observers which is also robust with respect to measurement noise.

For these reasons, in this work, we are going to use PI-observer to propose a new chaos based communication scheme. This is discussed in detail in the next section.

## 3.3 PI-observer Based Communication System

In this section, a new scheme for chaos based communication will be proposed where a combinational technique of chaotic masking and inclusion method is used as shown in Figure 3.2. As was discussed in previous chapters, the chaotic masking method is insecure while the inclusion method brings left invertibility problem making message extraction difficult. Therefore, this method facilitates the message recovery process and also increases the security. The performance of P and PI observers are studied for the proposed method and the performance of both observers on successfully recovering the message in presence of channel noise is studied. It will be shown that the PI-observer indeed provides improved performance and flexibility compared to other observer. This chapter is focussed on showing that PI observers are best suited for using in communication systems since they show high resistant to system noise. The security analysis is not done for the combinational scheme and is left for new and better schemes in the later chapters.

We assume that the chaotic oscillator at the transmitter is described by:

$$\begin{aligned} \dot{x} &= \mathrm{A}x + \mathrm{B}f(y) + h(t) \\ y &= \mathrm{C}x, \end{aligned} \tag{3.11}$$

where h is the forcing function, and f is a continuous nonlinear function satisfying the following Lipschitz condition:

$$\|f(y) - f(\bar{y})\| \leq \kappa \|y - \bar{y}\|, \tag{3.12}$$

where $\|\cdot\|$ is the Euclidean norm, and $\kappa > 0$ is the Lipschitz constant. The matrices A, B and C are of the following form:

$$\mathrm{A} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ & & & 1 \\ a_1 & & \cdots & a_n \end{pmatrix}, \mathrm{B} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{3.13}$$

$$\mathrm{C} = (1 \quad 0_{1\times n-1}).$$

Note that chaotic systems not defined by the above equations can simply be defined by transformation/change of coordinates.

### 3.3.1 Proposed Combinational Scheme

The proposed scheme is shown in Figure 3.2. Here we propose to inject the message in the oscillator as well as adding the message to the output of the oscillator. The injecting of message in the derivate of the state changes the attractor directly at the phase space and therefore will increase the security while the adding of the message in the output will facilitate the message recovery process.

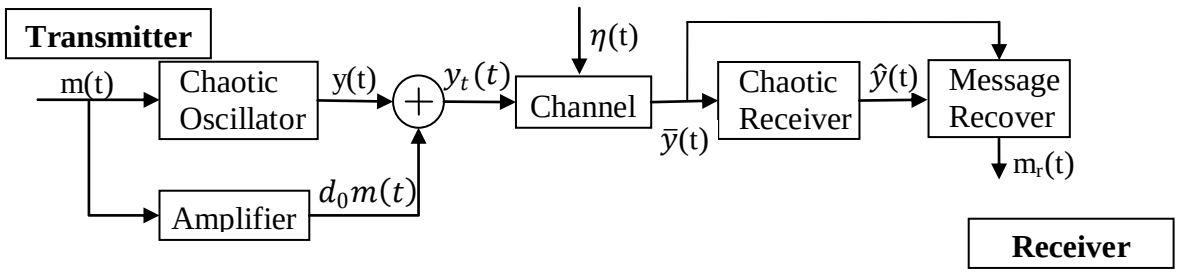


Figure 3.2: A block diagram of the combinational scheme implementing chaotic masking and inclusion method.

The system is described as:

$$\begin{aligned} \dot{x} &= \mathrm{A}x + \mathrm{B}f(y_t) + h(t) + \mathrm{B}m(t) \\ y_t &= \mathrm{C}x + d_0 m(t). \end{aligned} \tag{3.14}$$

Note, the message signal m(t) is included at the derivative of the state variable $x_n$ and at the output $y_t$. The received signal with the noise $\eta$(t) is given by:

$$\bar{y} = y_t + \eta(t). \tag{3.15}$$

### 3.3.2 Problem with Proportional Observer

A classical proportional observer designed for synchronization with system (3.14) can be written as:

$$\begin{aligned} \dot{\hat{x}} &= \mathrm{A}\hat{x} + \mathrm{B}f(\bar{y}) + h(t) + \mathrm{K}_p(\bar{y} - \mathrm{C}\hat{x}) \\ \dot{\hat{x}} &= \big(\mathrm{A} - \mathrm{K}_p\mathrm{C}\big)\hat{x} + \mathrm{B}f(\bar{y}) + h(t) + \mathrm{K}_p\bar{y}, \end{aligned} \tag{3.16}$$

where $\mathrm{K}_p = (k_1 \quad k_p \quad \cdots \quad k_n)^{\mathrm{T}}$ is the gain chosen such that $\big(\mathrm{A} - \mathrm{K}_p\mathrm{C}\big)$ is stable.

Now let $e = x - \hat{x}$ be the error between real and estimated states. Then, from (3.14) and (3.16) the error dynamics is given by:

$$\begin{aligned} \dot{e} &= \mathrm{A}e + \mathrm{B}\big(f(y_t) - f(\bar{y})\big) + \mathrm{B}m(t) - \mathrm{K}_p(\bar{y} - \mathrm{C}\hat{x}) \\ &= \mathrm{A}e + \mathrm{B}\big(f(y_t) - f(\bar{y})\big) + \mathrm{B}m(t) - \mathrm{K}_p(\mathrm{C}x + d_0 m(t) + \eta(t) - \mathrm{C}\hat{x}) \\ &= \big(\mathrm{A} - \mathrm{K}_p\mathrm{C}\big)e + \mathrm{B}\big(f(y_t) - f(\bar{y})\big) + \big(\mathrm{B} - \mathrm{K}_p d_0\big)m(t) - \mathrm{K}_p\,\eta(t). \end{aligned} \tag{3.17}$$

In (3.17), it can be seen that one needs to arbitrarily choose the value of $\mathrm{K}_p$ in order to make the matrix $\big(\mathrm{A} - \mathrm{K}_p\mathrm{C}\big)$ stable, but since higher the value of $\mathrm{K}_p$ the effect of noise $\eta(t)$ and $m(t)$ in error dynamics will also be amplified because of the terms $\mathrm{K}_p\,\eta(t)$ and $\mathrm{B} - \mathrm{K}_p d_0$ in the error dynamics. We need to be able to choose $\mathrm{K}_p = 0$ (or at least very small) for removing the influence of noise on the error dynamics and $\mathrm{B} - \mathrm{K}_p d_0 = 0$ for

eliminating the influence of the message. This means higher value of $d_0$ will now affect the chaotic property of transmitter oscillator. Therefore, the value of $\mathrm{K}_p$ has to be chosen judiciously such that the matrix $(\mathrm{A}-\mathrm{K}_p\mathrm{C})$ is stable while at the same time reducing the influence of message and noise. Hence, it is too much constraint on the sole proportional gain and therefore the P-observer is not the suitable observer to be implemented in this scenario. The following section will show that the PI-observer provides a better solution in terms of much reduced influence of the message signal and noise on the error dynamics.

### 3.3.3 Proportional-Integral Observer

Figure 3.3 depicts a channel and receiver block diagram of chaotic communication system using the PI-observer. Note that the integrator is located at the input of the receiver, thus eliminating the need for sending two signals from the transmitter. The transmitter is as shown in Figure 3.2.

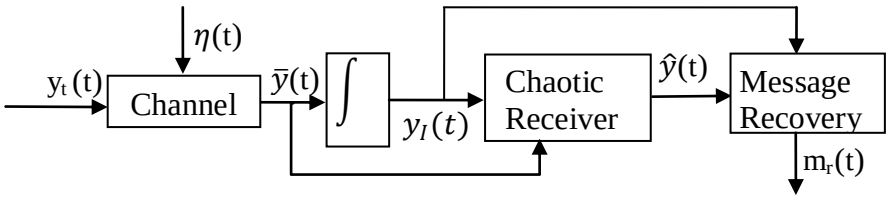


Figure 3.3: A block diagram for PI-observer based receiver.

To design a PI-observer, we set $x_0 = \int_0^t \bar{y}(\tau)d\,\tau = y_I$. In other words $\dot{x}_0 = \bar{y} = \mathrm{C}x + d_0 m(t) + \eta(t)$. We are using $\bar{y}$ instead of $\mathrm{y_t}$ because the integrator is placed at the receiver side, i.e. once the transmitted signal is corrupted by the noise. We now have the following expressions:

$$\begin{aligned} \dot{x}_0 &= \mathrm{C}x + d_0 m(t) + \eta(t) \\ \dot{x} &= \mathrm{A}x + \mathrm{B}f(y_t) + h(t) + \mathrm{B}m(t) \\ y_t &= \mathrm{C}x + d_0 m(t) \\ \bar{y} &= \mathrm{C}x + d_0 m(t) + \eta(t). \end{aligned} \tag{3.18}$$

An augmented system can be written for (3.18) as follows:

$$\begin{aligned} \dot{x}_{aug} &= \bar{\mathrm{A}}x_{aug} + \bar{\mathrm{B}}f(y_t) + \bar{h}(t) + \mathrm{C}_0^{\mathrm{T}}(d_0 m(t) + \eta(t)) + \bar{\mathrm{B}}m(t) \\ y_t &= \bar{\mathrm{C}}x_{aug} + d_0 m(t) \\ y_I &= \mathrm{C}_0 x_{aug} \\ \bar{y} &= \bar{\mathrm{C}}x_{aug} + d_0 m(t) + \eta(t), \end{aligned} \tag{3.19}$$

where

$$\begin{aligned} x_{aug} &= \begin{bmatrix} x_0 \\ x \end{bmatrix}, \bar{\mathrm{A}} = \begin{bmatrix} 0 & \mathrm{C} \\ 0_{\mathrm{n}\times 1} & \mathrm{A} \end{bmatrix} \\ \bar{\mathrm{B}} &= \begin{bmatrix} 0 \\ \mathrm{B} \end{bmatrix}, \bar{h}(t) = \begin{bmatrix} 0 \\ h(t) \end{bmatrix} \\ \mathrm{C}_0 &= [\,\mathrm{C} \quad 0], \bar{\mathrm{C}} = [\,0 \quad \mathrm{C}]. \end{aligned}$$

Now a PI-observer for (3.19) can be designed as:

$$\dot{\hat{x}}_{aug} = \bar{\mathrm{A}}\hat{x}_{aug} + \bar{\mathrm{B}}f(\bar{y}) + \bar{h}(t) + \bar{\mathrm{L}}_I\big(y_I - \mathrm{C}_0\hat{x}_{aug}\big) + \bar{\mathrm{K}}_p\big(\bar{y} - \bar{\mathrm{C}}\hat{x}_{aug}\big), \tag{3.20}$$

where $\bar{\mathrm{K}}_p = (k_0 \quad \mathrm{K}_p)^{\mathrm{T}} = (k_0 \quad k_1 \quad \cdots \quad k_n)^{\mathrm{T}}$ and $\bar{\mathrm{L}}_I = (l_0 \quad \mathrm{L}_I)^{\mathrm{T}} = (l_0 \quad l_1 \quad \cdots \quad l_n)^{\mathrm{T}}$ are the proportional and integral gains, respectively.

By defining the error signal $e_{aug} = x_{aug} - \hat{x}_{aug}$, from (3.19) and (3.20) and following few calculation steps, the error dynamics is defined as:

$$\begin{aligned} \dot{e}_{aug} &= \big(\bar{\mathrm{A}} - \bar{\mathrm{L}}_I\mathrm{C}_0 - \bar{\mathrm{K}}_p\bar{\mathrm{C}}\big)e_{aug} + \bar{\mathrm{B}}\big(f(y_t) - f(\bar{y})\big) \\ &\quad + \mathrm{C}_0^{\mathrm{T}}\big(d_0 m(t) + \eta(t)\big) + \bar{\mathrm{B}}m(t) - \bar{\mathrm{K}}_p d_0 m(t) - \bar{\mathrm{K}}_p\eta(t) \\ &= \mathrm{F}e_{aug} + \bar{\mathrm{B}}g(y_t, \bar{y}) + (\mathrm{C}_0^{\mathrm{T}} - \bar{\mathrm{K}}_p)(d_0 m(t) + \eta(t)) + \bar{\mathrm{B}}m(t), \end{aligned} \tag{3.21}$$

where $\mathrm{F} = \big(\bar{\mathrm{A}} - \bar{\mathrm{L}}_I\mathrm{C}_0 - \bar{\mathrm{K}}_p\bar{\mathrm{C}}\big)$ and $g(y_t, \bar{y}) = \big(f(y_t) - f(\bar{y})\big)$.

Ideally, one could choose $(\mathrm{C}_0^{\mathrm{T}} - \overline{\mathrm{K}}_p) = 0$, to keep the effect of noise and message on the error dynamics to a minimum. However, by setting $\overline{\mathrm{K}}_p = \mathrm{C}_0^{\mathrm{T}}$, the noise term could be eliminated but at the cost of the overall system (3.18) becoming unobservable, thus making it unfeasible to choose $\bar{\mathrm{L}}_I$ to stabilize the overall augmented system. Consequently, we have chosen the followings conditions:

$$\begin{aligned} k_0 &= 1 - \epsilon \\ k_1 = k_2 &= \cdots = k_{n-1} = 0 \\ k_n &= {}^{1}/_{d_0}. \end{aligned} \tag{3.22}$$

Equation (3.21) can be re-written using the special gains in (3.22) as:

$$\dot{e}_{aug} = \mathrm{F}e_{aug} + \overline{\mathrm{B}}g(y_t, \bar{y}) + d_0\epsilon\, \mathrm{C}_0^{\mathrm{T}} m(t) + (\epsilon\, \mathrm{C}_0^{\mathrm{T}} + {}^{1}/_{d_0}\, \overline{\mathrm{B}})\eta(t). \tag{3.23}$$

Since F is stable, there exist P and Q, symmetric positive definite (SPD) matrices, such that:

$$\mathrm{F}^{\mathrm{T}}\mathrm{P} + \mathrm{PF} = -\mathrm{Q} \tag{3.24}$$

Let $\mathrm{V}(e_{aug}) = e_{aug}^{\mathrm{T}}\, \mathrm{P} e_{aug}$ be the candidate Lyapunov function. Then using (3.23), (3.24) and (3.12), we get the followings:

$$
\begin{aligned}
\dot{\mathrm{V}} &= 2e_{aug}^{\mathrm{T}}\,\mathrm{P}\dot{e}_{aug} \\
&= 2e_{aug}^{\mathrm{T}}\,\mathrm{PF}e_{aug} + 2e_{aug}^{\mathrm{T}}\,\mathrm{P}\bar{\mathrm{B}}g(y_t,\bar{y}) + 2\epsilon d_0 e_{aug}^{\mathrm{T}}\,\mathrm{P}\,\mathrm{C}_0^{\mathrm{T}} m(t) \\
&\qquad + 2e_{aug}^{\mathrm{T}}\,\mathrm{P}(\epsilon\,\mathrm{C}_0^{\mathrm{T}} + {}^{1}\!/_{d_0}\,\bar{\mathrm{B}})\eta(t) \\
&\leq -e_{aug}^{\mathrm{T}}\,\mathrm{Q}e_{aug} + 2\left\|\mathrm{P}e_{aug}\right\|\|g(y_t,\bar{y})\| + 2\epsilon d_0\left\|\mathrm{P}e_{aug}\right\||m(t)| \\
&\qquad + 2\left\|\mathrm{P}e_{aug}\right\|\left|\epsilon + \frac{1}{d_0}\right||\eta(t)| \\
&\leq -e_{aug}^{\mathrm{T}}\,\mathrm{Q}e_{aug} + 2\kappa\left\|\mathrm{P}e_{aug}\right\||\eta(t)| + 2\epsilon d_0\left\|\mathrm{P}e_{aug}\right\||m(t)| \\
&\qquad + 2\left\|\mathrm{P}e_{aug}\right\|\left|\epsilon + \frac{1}{d_0}\right||\eta(t)| \\
&\leq -e_{aug}^{\mathrm{T}}\,\mathrm{Q}e_{aug} + 2\left\|\mathrm{P}e_{aug}\right\|\left(\kappa + \epsilon + \frac{1}{d_0}\right)|\eta(t)| \\
&\qquad + 2\left\|\mathrm{P}e_{aug}\right\|\epsilon d_0|m(t)|.
\end{aligned}
\tag{3.25}
$$

We know,

$$
\begin{aligned}
-\lambda_{\min}(\mathrm{Q})\|e\|^2 \geq -e^T\mathrm{Q}e \geq -\lambda_{\max}(\mathrm{Q})\|e\|^2 \\
-\lambda_{\min}(\mathrm{P})\|e\|^2 \geq -e^T\mathrm{P}e \geq -\lambda_{\max}(\mathrm{P})\|e\|^2,
\end{aligned}
\tag{3.26}
$$

where $\lambda_{\min}$ and $\lambda_{\max}$ are minimum and maximum eigen values for the respective matrices. Now from (3.26),

$$
\begin{aligned}
-e^T\mathrm{Q}e &\leq -\lambda_{\min}(\mathrm{Q})\|e\|^2 \\
&\leq -\lambda_{\min}(\mathrm{Q})\frac{e^T\mathrm{P}e}{\lambda_{\max}(\mathrm{P})} \\
-e^T\mathrm{Q}e &\leq -\lambda_0 e^T\mathrm{P}e = -\lambda_0\mathrm{V},
\end{aligned}
\tag{3.27}
$$

where $\lambda_0$ is the ratio between minimum eigen value of Q and maximum eigen value of P.

Also, we can write,

$$
\|e\|^2 \leq \frac{\mathrm{V}}{\lambda_{\min}(\mathrm{P})} \tag{3.28}
$$

$$\|e\| \leq \frac{\sqrt{\mathrm{V}}}{\sqrt{\lambda_{\min}(\mathrm{P})}}$$

Therefore, from (3.27) and (3.28), provided that $m(t)$ and $\eta(t)$ are bounded (3.25) can now be written as:

$$\dot{\mathrm{V}} \leq -\lambda_0 \mathrm{V} + \frac{\mathrm{c}}{\sqrt{\lambda_{\min}(\mathrm{P})}}\sqrt{\mathrm{V}} = -\lambda_0 \mathrm{V} + \lambda_1 \sqrt{\mathrm{V}}. \tag{3.29}$$

The value $\lambda_1$ depends on the minimum eigen value of P and $\epsilon$ and $d_0$.

Hence, by choosing $\epsilon$ and $d_0$ judiciously we can make $\lambda_1 < \lambda_0$, in which case $\dot{\mathrm{V}} \leq 0$, thus proving synchronization is achieved.

Here, $\bar{\mathrm{L}}_I$, $\epsilon$ and $d_0$ are chosen in such a way to ensure that the matrix F is stable and the effect of noise and message as minimum as possible. Also, the value of $d_0$ can be made small enough such that masking of message does not affect the chaotic property of the transmitter oscillator. By doing the PI-observer scheme adds degree of freedom and flexibility. The integral and proportional gains can be selected to achieve rapid synchronization and reduced noise impact, respectively.

Having achieved the desired convergence, the message signal can be retrieved by calculating the following difference equation:

$$\begin{aligned} \bar{y}(t) - \hat{y}(t) &= y(t) - \hat{y}(t) + d_0 m(t) + \eta(t) \\ &= \varphi(t) + \eta(t). \end{aligned} \tag{3.30}$$

With $\lim_{t\to\infty} |y(t) - \hat{y}(t)| \to 0$, the recovered message signal is given by:

$$m_r(t) \approx \frac{\varphi(t)}{d_0} + \eta(t). \tag{3.31}$$

The noise $\eta(t)$ term can simply be removed using a low pass filter.

The proposed method will be implemented using the Duffing oscillator and P and PI-observer will be designed. The simulation will be carried out using Matlab/Simulink and the performance for both the observers will be observed and compared.

## 3.4 Implementation of PIO using Duffing Oscillator

The Duffing oscillator is defined as:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -\frac{x_1}{4} - x_1^3 + 11\cos(t). \end{aligned} \tag{3.32}$$

We assume that state variable $x_1$ is measured, i.e. the output equation is $y = x_1$ so that the system can be written in a matrix form as:

$$\begin{aligned} \dot{x} &= \mathrm{A}x + \mathrm{B}f(y) + \mathrm{h}(t) \\ y &= \mathrm{C}x, \end{aligned} \tag{3.33}$$

where

$$\mathrm{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \mathrm{B} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \mathrm{C} = (1 \quad 0)$$
$$f(y) = -\frac{y}{4} - y^3, \mathrm{h}(t) = \begin{pmatrix} 0 \\ 11\cos(t) \end{pmatrix}.$$

Then this system is in the form described by (3.11). Now the proposed combinational system can be expressed as:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -\frac{y_t}{4} - y_t^3 + 11\cos t + m(t) \\ y_t &= x_1 + d_0 m(t). \end{aligned} \tag{3.34}$$

Note that $m(t)$ is present in the derivative of the second state variable $x_2$ and the output of the system $y_t$. This combinational system is of the form (3.14).

### 3.4.1 P-Observer Based Scheme

As described earlier in the paper, the classical proportional observer for system (3.34) is given by:

$$\begin{aligned}\dot{\hat{x}}_1 &= \hat{x}_2 + k_1(\bar{y} - \hat{x}_1)\\ \dot{\hat{x}}_2 &= -\frac{\bar{y}}{4} - \bar{y}^3 + 11\cos t + k_2(\bar{y} - \hat{x}_1)\end{aligned} \tag{3.35}$$

where $(k_1 \quad k_2)^{\mathrm{T}} = \mathrm{K}_p$ is the proportional gain.

#### 3.4.1.1 Simulation results

A simulation of the above observer (3.35) was carried out using Matlab/Simulink. The poles of the observer were set as $p_1 = p_2 = 0.1$ so that $k_1 = 0.2$ and $k_2 = 0.01$. The values of gain have been chosen to be small in order to reduce the effect of message and the channel noise. Therefore, $d_0 = -k_2^{-1} = -100$. In addition, the initial conditions for the oscillator at the transmitter and receiver are chosen to be arbitrarily different. The message signal m(t), channel and its specification used in simulation are given in Table 3.1.

Figure 3.4 depicts the transmitted signal with a non-chaotic profile. This partly is due to the requirement of having to choose very a high value for $d_0$ where the oscillator is operating in the normal periodic mode. Figure 3.5 illustrates the time waveforms for $x_1(t)$ and $\hat{x}_1(t)$, whereas the plot of state $x_1(t)$ against $\hat{x}_1(t)$ is shown in Figure 3.6. Both figures illustrate that the synchronization has not been achieved satisfactorily. The recovered message (in dotted lines) signal together with m(t) are shown in Figure 3.7. Both the synchronization problem and distorted $m_r(t)$ can be explained by $\left(\mathrm{B} - \mathrm{K_p}\, d_0\right)m(t)$ and $\mathrm{K}_p\eta(t)$ terms in (3.17), which are non-zero with real values. The best scenario would be to make $\left(\mathrm{B} - \mathrm{K_p}\, \mathrm{d}_0\right)m(t) = 0$, however by doing so the eigenvalue of matrix (A – $\mathrm{K_p}$C)

cannot be chosen arbitrarily. This effect can be minimized by choosing a high value for $d_0$ but at the cost of possible loss of chaotic behaviour of the oscillator (in fact, the chaotic property is already lost for current value of $d_0$). To regain or reinstate the chaotic behaviour the amplitude of $m(t)$ should be reduced significantly by more than 100 times. This constraint on message to be transmitted as well as synchronization susceptibility to the inherent channel noise, make the use of P-observer based receiver less attractive.

Table 3.1: Parameters used in the simulation.

| **Parameters** | **Values** |
|---|---|
| Message signal m(t) | sint |
| Channel | Additive white Gaussian |
| Signal-to-noise ratio | 25 dB |
| Filter type | Butterworth LPF |
| Filter order | 8 |
| Filter cut-off | 3 rad/sec |

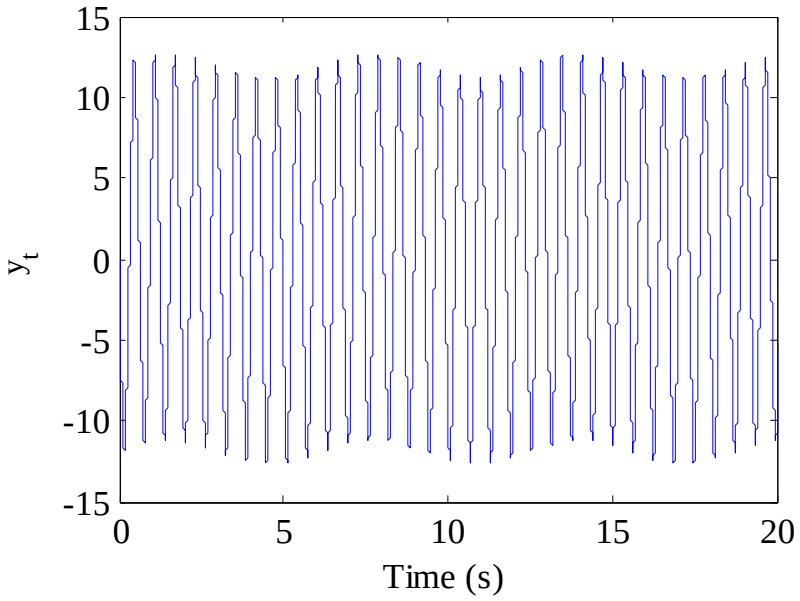


Figure 3.4: Transmitted chaotic signal $y_t$ using the P-observer.

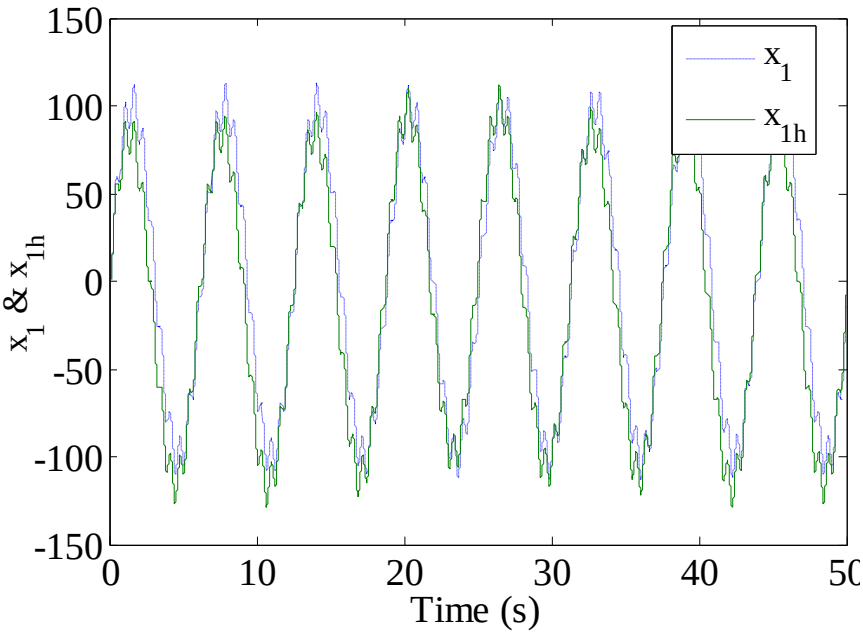


Figure 3.5: Time waveforms of $x_1(t)$ and $\hat{x}_1(t)$.

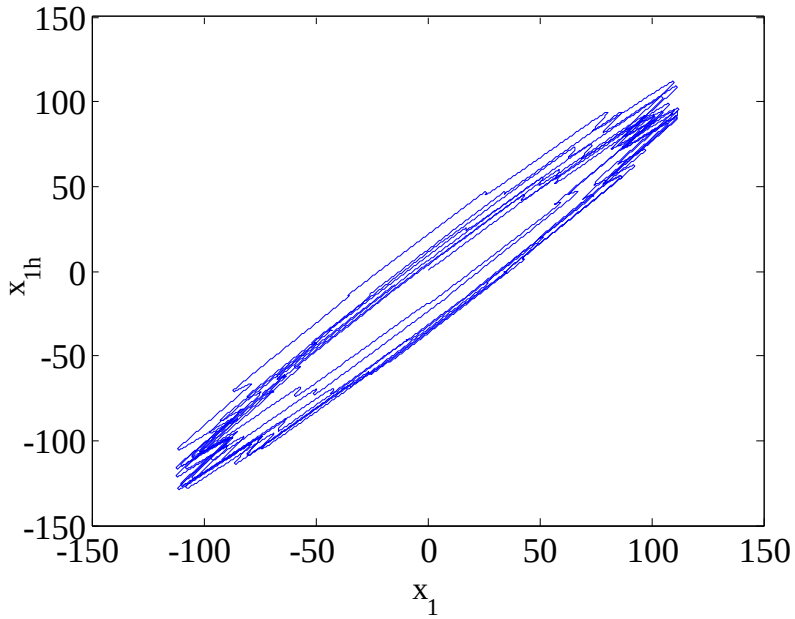


Figure 3.6: Plot of the state of $x_1(t)$ versus $\hat{x}_1(t)$ using the P-observer.

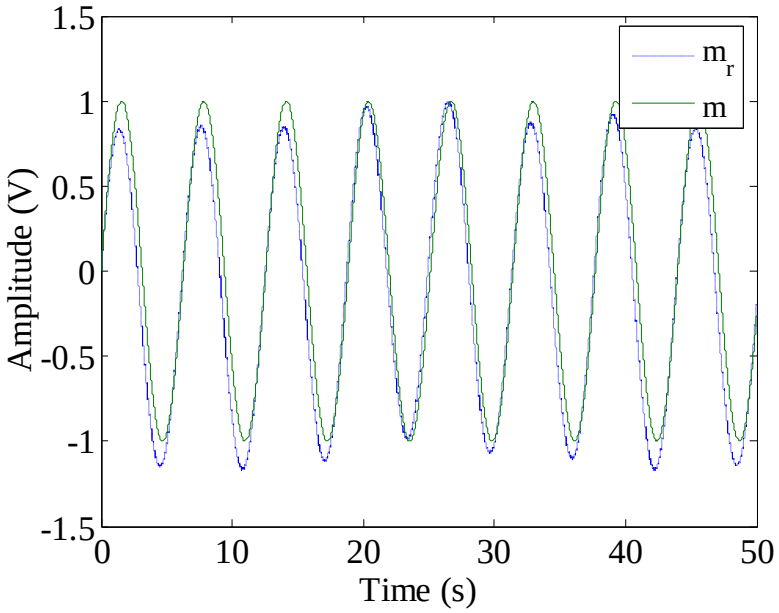


Figure 3.7: Transmitted and recovered message signals for the P-observer based system.

### 3.4.2 PI-Observer Based Scheme

Following the PI-observer methodology described above, we set $x_0 = \int_0^t \bar{y}(\tau)d\,\tau = y_I$. In other words, $\dot{x}_0 = \bar{y} = x_1 + d_0 m(t) + \eta(t)$. We then have the following augmented system using the Duffing oscillator:

$$\begin{aligned} \dot{x}_0 &= x_1 + d_0 m(t) + \eta(t) \\ \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -\frac{y_t}{4} - y_t^3 + 11\cos t + m(t) \\ y_t &= x_1 + d_0 m(t) \\ y_I &= x_0. \end{aligned} \tag{3.36}$$

The PI-observer for the above system is given by:

$$\begin{aligned} \dot{\hat{x}}_0 &= \hat{x}_1 + k_0(\bar{y} - \hat{x}_1) + l_0(x_0 - \hat{x}_0) \\ \dot{\hat{x}}_1 &= \hat{x}_2 + k_1(\bar{y} - \hat{x}_1) + l_1(x_0 - \hat{x}_0) \end{aligned} \tag{3.37}$$

$$\dot{\hat{x}}_2 = -\frac{\bar{y}}{4} - \bar{y}^3 + 11\cos t + k_2(\bar{y} - \hat{x}_1) + l_2(x_0 - \hat{x}_0),$$

where $(k_0 \quad k_1 \quad k_2)^{\mathrm{T}} = \bar{\mathrm{K}}_p$ is the proportional gain, and $(l_0 \quad l_1 \quad l_2)^{\mathrm{T}} = \bar{\mathrm{L}}_I$ is the integral gain of PI-observer.

#### 3.4.2.1 Simulation results

With the parameters in Table 3.1 and by selecting $d_0 = \epsilon = 0.01$ so that $k_0 = 0.99$ and $k_2 = 100$, and all poles are to 0.1 so that $l_0 = 0.3, l_1 = -99.7$ and $l_2 = -29.99$ and equations (3.36) and (3.37) the PI-observer based system was simulated using Matlab. Although exact comparison between the P and PI observers is not possible since the former and the latter are of the order 2 and 3, respectively. However approximate comparison can be made provided the poles are fixed at the same location. Here too the initial conditions are chosen to be arbitrarily different for transmitter and receiver oscillators. Figure 3.8 shows the transmitted chaotic signal for the PI-observer illustrating that the chaotic regime is being maintained. Figure 3.9 depicts the plot of $x_1(t)$ and $\hat{x}_1(t)$ and Figure 3.10 shows the plot of $x_1(t)$ against $\hat{x}_1(t)$. The $45^0$ line shown in Figure 3.10 illustrates almost perfect synchronization that has been achieved compared to Figure 3.6. The recovered message signal is very similar to the transmitted message as shown in Figure 3.11. The improved performance offered by the PI-observer compared to the P-observer is because of the proportional and integral gains being selected independently. In the P-observer, the constraint imposed on the proportional gain affects the stability of the error dynamics as well the message/noise impact on the error dynamics. On the other hand, with the PI-observer, the integrator gain improves the stability of the error dynamics while the proportional gain reduces the effect of noise and message signal on the error dynamics.

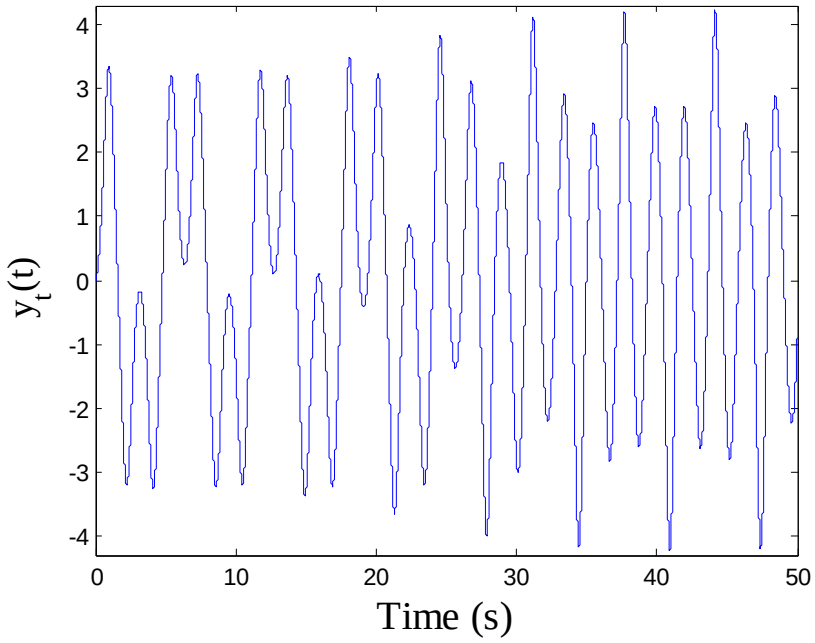


Figure 3.8: Transmitted chaotic signal $y_t$ using the PI-observer.

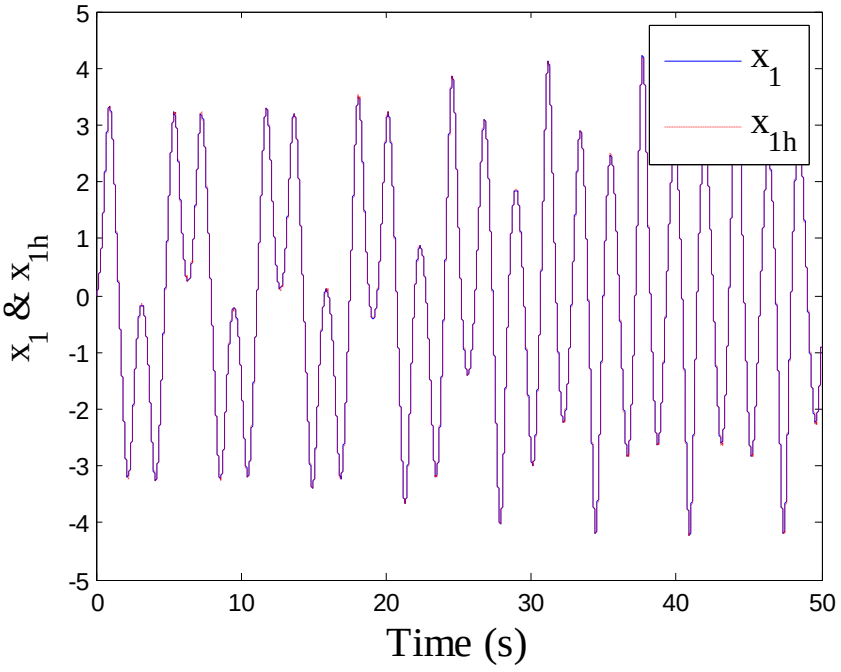


Figure 3.9: Plot of states $x_1(t)$ and $\hat{x}_1(t)$ versus the time.

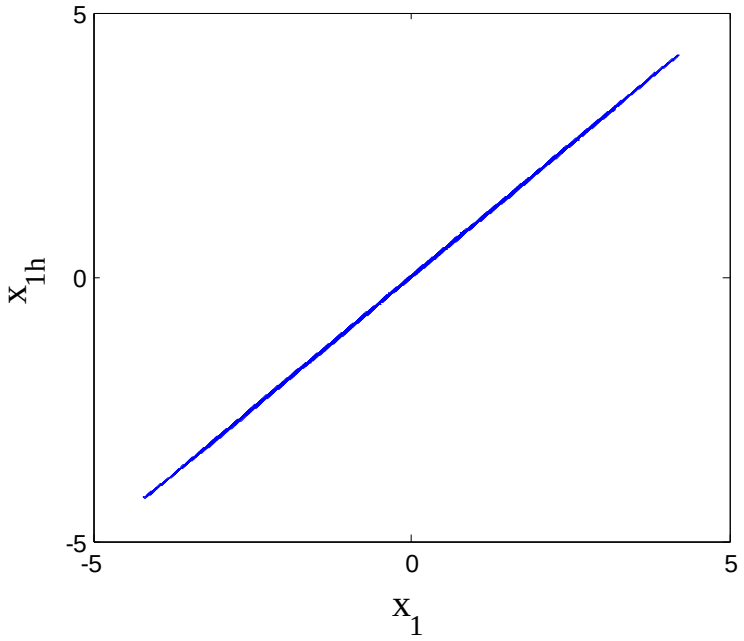


Figure 3.10: Plot of state $x_1(t)$ versus $\hat{x}_1(t)$ using the PI-observer.

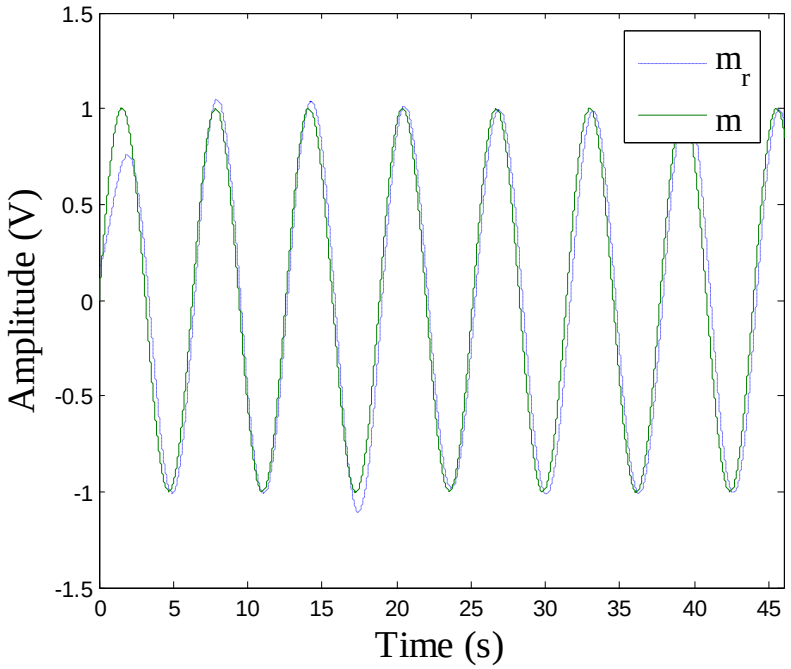


Figure 3.11: Message recovery using the PI-observer.

## 3.5 Summary

The P-observer and PI-observer based chaotic synchronization has been studied and the performance of both observers for the proposed combinational chaotic communication scheme is analysed. It was found that for the proposed scheme, PI-observer showed greater robustness in synchronization in terms of noise immunity and therefore message extraction. This was mainly because the degree of freedom was added in the system due to the integrator in the PI-observer. The integral gain in PI-observer was used to stabilize the error dynamics for better synchronization while the proportional gain was used to reduce the effect of noise/message in the synchronization performance. In P-observer, however, there was only proportional gain available imposing too much constraint on it. The performance of the proposed method using P and PI-observer was simulated taking AWGN channel having SNR equal to 25 dB using Matlab/Simulink.

# Chapter 4 Cascaded Chaotic Masking for Secure Communication

## 4.1 Introductions

As pointed out in the earlier chapters, chaotic systems have potential to be used in implementing secure communication and significant work has been done in realizing this by researchers. However, there are still lots of shortcomings present, particularly in the methods related to security. As mentioned earlier, there exist different attack methods to break the chaotic communication model and schemes. Therefore there is still a requirement and necessity to come up with a scheme that can be potentially secure by eliminating shortcomings of earlier methods such as chaotic masking and modulation schemes.

In this and subsequent chapters, few possibilities of enhancing the security of the previously proposed chaotic communication methods will be proposed and discussed. It will be shown that by employing some techniques, the existing methods could be extended and modified so as to be potentially secure. This chapter proposes one method based on cascaded chaotic masking in order to try to remove the vulnerability of the masking method by increasing the complexities.

## 4.2 Cascaded Chaotic Masking

It is now generally agreed that the traditional chaotic masking technique is not a secure method. To break it, researchers had used methods where they were able to forecast and predict the carrier behaviour. By subtracting the predicted values of the carrier, the spectrum of the hidden signal can be known, thus making relatively easy to reconstruct the

message signal by some signal processing operations [91]. In [91], however, it was also pointed out that it is possible to increase the security capabilities if two chaotic signals can be added together at roughly equal power to create a carrier signal of sufficient complexity such it is not possible to use simple phase geometry to do the forecasting. Hence, to increase the security of the communication link, a new method is proposed in this section where a cascaded chaotic masking method is implemented as shown in Figure 4.1. A cascaded chaotic system has been proposed with improved security by adding together two chaotic signals of almost equal power.

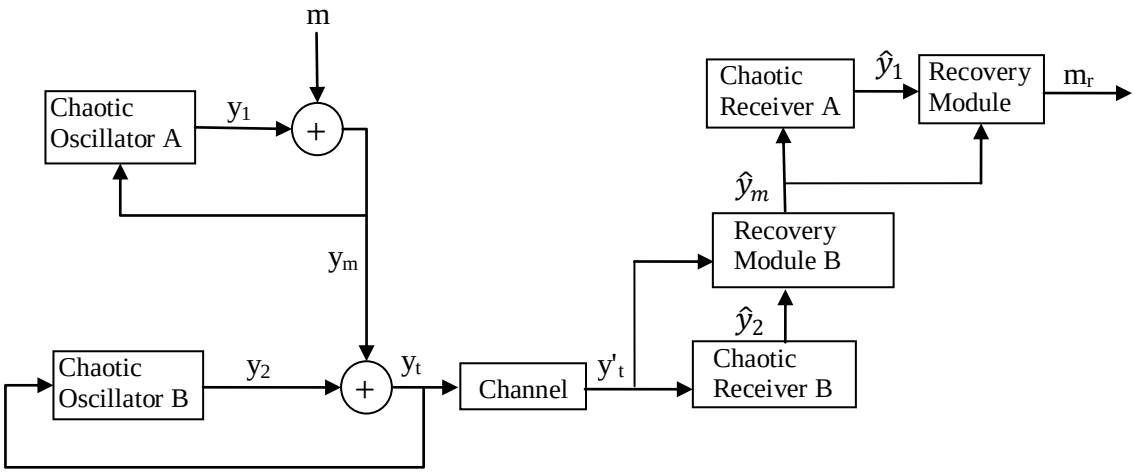


Figure 4.1: Block diagram of chaotic communication using cascaded structure.

In this technique, the message signal m(t) is added to the output $y_1(t)$ of the chaotic oscillator A to produce a chaotic output $y_m(t)$. The chaotic output is added to the output $y_2(t)$ of chaotic oscillator B to produce an output $y_t(t)$. It should be noted that, here a chaotic signal is modulated with another chaotic signal and only one of them contains the information about the message signal. This will hence effectively increase the security of the communication link and make it difficult for intruders to predict the carrier behaviour and therefore find the spectrum of the hidden message signal. On the receiver side, again a

cascaded model is implemented. The chaotic receiver B is used to estimate $\hat{y}_2(t)$ and hence to predict $\hat{y}_m(t)$. The signal $\hat{y}_m(t)$ will now is used to drive a chaotic receiver A and estimate $\hat{y}_1(t)$. Now, the prediction of $m_r(t)$ can simply be carried out by the inverse operation. The synchronization between the transmitter and the receiver oscillators can be achieved by using any existing methods available in the literature [42, 43, 52-54].

### 4.2.1 Cascaded Chaotic Masking Scheme

The transmitter system is described as a class of chaotic system given as:

$$\begin{aligned} \dot{x} &= F(y)x + g(y,t) \\ y &= Cx, \end{aligned} \tag{4.1}$$

where $x \in R^n, y \in R$. Here the matrix F is a function of the output y, C is a constant matrix of appropriate dimension and $g(y,t)$ is a smooth function of y or the driving signal. We also assume that the entries of F(y) are smooth and bounded for all $y \in R$. In addition, the pair (F(y),C) is rank observable or detectable for all $y \in R$. We will now define the proposed system. Here the cascaded method will be using two chaotic oscillator systems A and B as defined in (4.1). The oscillator A will be described as:

$$(A): \begin{cases} \dot{x}_A = F_A(y_1)x_A + g_1(y_1,t) \\ y_m = C_A x_A + m = y_1 + m, \end{cases} \tag{4.2}$$

where $x_A \in R^n, y_1 \in R$. $y_1$ is the output of the oscillator A and m is the message to be transmitted. Hence, $y_m$ is the output due to first step of masking. The oscillator B will be described as:

$$(B): \begin{cases} \dot{x}_B = F_B(y_2)x_B + g_2(y_2,t) \\ y_t = C_B x_B + y_m = y_2 + y_m, \end{cases} \tag{4.3}$$

where $x_B \in R^n, y_2 \in R$. $y_2$ is the output of the oscillator B. Hence, $y_m$ is the output due to second step of masking and is the signal that will be transmitted through the channel.

We have used different $F_A$, $F_B$ and $C_A$, $C_B$ to show that two different types of chaotic oscillator can be used for this design.

For the receivers, one has to design cascaded chaotic oscillators in order to synchronize with (B) and (A) respectively. Simple proportional observers will be defined for designing these cascaded receivers although simple drive response type synchronization as explained in chapter 2 can also be achieved. The key here is to show the potential of cascaded masking approach rather than dwelling too much on the synchronization method to be used.

Let us first design an observer B that can synchronize with the oscillator B given as (4.3) first so that we can estimate $\hat{y}_2$. This value can then be used, as will be shown later, to retrieve signal $\hat{y}_m$.

$$\dot{\hat{x}}_B = F_B(y_2)\hat{x}_B + K_{Bp}(y_t - C_B\hat{x}_B) + g_2(y_2,t), \tag{4.4}$$

where $K_{Bp}$ is the gain matrix of appropriate dimension. Now, if we define error as, $e_B = x_B - \hat{x}_B$, then the error dynamics can again be written as:

$$\begin{aligned}\dot{e}_B &= F_B(y_2)e_B + K_{Bp}(y_t - C_B\hat{x}_B) \\ &= \left(F_B(y_2) - K_{Bp}C_B\right)e_A - K_{Bp}m.\end{aligned} \tag{4.5}$$

We can see the presence of message signal on the error dynamics. For the influence of message on error dynamics, which is affecting the convergence of the error to zero, the value of $K_{Bp}m$ should be zero or at least should be very small. If we choose $K_{Bp}$ as zero, then it implies an observer with zero gains and in effect $F_B(y_2)$ should be stable on its own and hence we cannot improve the convergence rate of the observer. Therefore, the value of gain should be chosen sensibly such that the matrix $\left(F_B(y) - K_{Bp}C_B\right)$ is stable while at the same time reducing the influence of masking signal. After the synchronization is achieved and $\hat{y}_m$ estimated, observer A can be defined to synchronize with oscillator A as:

$$\dot{\hat{x}}_A = F_A(y_1)\hat{x}_A + K_{Ap}(\hat{y}_m - C_A\hat{x}_A) + g_1(y_1,t), \tag{4.6}$$

where $K_{Ap}$ is the gain matrix of appropriate dimension. Now, if we define error as, $e_A = x_A - \hat{x}_A$, then the error dynamics can again be written as:

$$\begin{aligned}\dot{e}_A &= F_A(y_1)e_A + K_{Ap}(\hat{y}_m - C_A\hat{x}_A) \\ &= \left(F_A(y_1) - K_{Ap}C_A\right)e_A - K_{Ap}m.\end{aligned} \tag{4.7}$$

We have assumed in (4.7) that $\hat{y}_m \approx y_m$.

Finally when the convergence is achieved by both observers (4.6) and (4.4), the driving signal $\hat{y}_m$ for (4.6) and message $m$ is retrieved by performing the following difference:

$$\hat{y}_m(t) = y_t(t) - \hat{y}_2(t) = y_2(t) - \hat{y}_2(t) + \hat{y}_m(t) = \xi_B(t). \tag{4.8}$$

Since, $\lim_{t\to+\infty}\left|y_2(t)-\hat{y}_2(t)\right|\to 0$, we have

$$\hat{y}_m(t)\approx\xi_B(t)=y_m(t). \tag{4.9}$$

Once, $\hat{y}_m(t)$ is retrieved from (4.4) the message signal can be decrypted as:

$$m_r(t)=\hat{y}_m(t)-\hat{y}_1(t)=y_1(t)-\hat{y}_1(t)+m(t)=\xi_A(t). \tag{4.10}$$

Since, $\hat{y}_m(t)\approx y_m(t)$ and $\lim_{t\to+\infty}\left|y_1(t)-\hat{y}_1(t)\right|\to 0$ , we now have

$$m_r(t)\approx\xi_B(t)=m(t). \tag{4.11}$$

Hence, it is shown that the retrieved message signal asymptotically converges to the transmitted message signal even when a cascaded approach is taken.

## 4.3 Implementation of the Cascaded Chaotic Masking

Now, the cascaded masking scheme proposed in the earlier section will be verified using Lorenz system. The Lorenz system given in (4.12) is of the form (4.1),

$$\begin{aligned}\dot{x}_1&=-\sigma x_1+\sigma x_2\\ \dot{x}_2&=-20x_1x_3+rx_1-x_2\\ \dot{x}_3&=5x_1x_2-bx_3,\end{aligned} \tag{4.12}$$

where

$$F(y)=\begin{pmatrix}-\sigma & \sigma & 0\\ r & -1 & -20y\\ 0 & 5y & -b\end{pmatrix},\ g(y,t)=0 \text{ and } C=(1\quad 0\quad 0).$$

We will use the Lorenz system (4.12) for both transmitter oscillators (4.2) and (4.3) i.e. $F_A = F_B$ and $C_A = C_B$, hence the cascaded masked system using Lorenz system can be written as:

$$\begin{aligned} \dot{x}_{A1} &= -\sigma x_{A1} + \sigma x_{A2} \\ \dot{x}_{A2} &= -20 y_m x_{A3} + r y_m - x_{A2} \\ \dot{x}_{A3} &= -5 y_m x_{A2} - b x_{A3} \\ y_m &= x_{A1} + m, \end{aligned} \tag{4.13}$$

and

$$\begin{aligned} \dot{x}_{B1} &= -\sigma x_{B1} + \sigma x_{B2} \\ \dot{x}_{B2} &= -20 y_t x_{B3} + r y_t - x_{B2} \\ \dot{x}_{B3} &= -5 y_t x_{B2} - b x_{B3} \\ y_t &= x_{B1} + y_m. \end{aligned} \tag{4.14}$$

Similarly, the observers for the cascaded masked system (4.13) and (4.14) can be written as:

$$\begin{aligned} \dot{\hat{x}}_{B1} &= -\sigma \hat{x}_{B1} + \sigma \hat{x}_{B2} + K_{B1}(\hat{y}_t - \hat{x}_{B1}) \\ \dot{\hat{x}}_{B2} &= -20 y_t \hat{x}_{B3} + r y_t - \hat{x}_{B2} + K_{B2}(\hat{y}_t - \hat{x}_{B1}) \\ \dot{\hat{x}}_{B3} &= -5 y_t \hat{x}_{B2} - b \hat{x}_{B3} + K_{B3}(\hat{y}_t - \hat{x}_{B1}), \end{aligned} \tag{4.15}$$

and

$$\begin{aligned} \dot{\hat{x}}_{A1} &= -\sigma \hat{x}_{A1} + \sigma \hat{x}_{A2} + K_{A1}(\hat{y}_m - \hat{x}_{A1}) \\ \dot{\hat{x}}_{A2} &= -20 \hat{y}_m \hat{x}_{A3} + r \hat{y}_m - \hat{x}_{A2} + K_{A2}(\hat{y}_m - \hat{x}_{A1}) \\ \dot{\hat{x}}_{A2} &= -5 \hat{y}_m \hat{x}_{A2} - b \hat{x}_{A3} + K_{A3}(\hat{y}_m - \hat{x}_{A1}). \end{aligned} \tag{4.16}$$

Note that the observer (4.15) and (4.16) are driven by the signals $y_t$ and $\hat{y}_m$ respectively.

## 4.4 Simulation Results

The simulation of the proposed secure communication system is presented in this section. The value of $\sigma, r, b$ are taken as 16, 45.6 and 4 respectively for the Lorenz system. The values of the gain are chosen to be zero because as discussed earlier this would reduce the influence of message on the error dynamics and also with this choice of gains, synchronization was still possible. Initial conditions for the oscillators were chosen to be arbitrarily different. The message signal to be transmitted is taken as $m(t) = 0.1\sin(2\pi t)$.

Figure 4.2 shows the output after first level of masking which has the message to be transmitted hidden in it. This output $y_m$ is further used to mask the output of the oscillator (4.14). Figure 4.3 depicts the final output $y_t$ which has been obtained after second level of masking, which is the transmitted signal. The signal $y_t$ appears to be chaotic and successfully hides the message in it. In fact, the autocorrelation function of the signal $y_t$, as shown in Figure 4.4, illustrates the function to have only spike at time shift equals to zero.

Now at the receiver side, synchronization is obtained via cascaded receivers. First the signal $y_m$ is estimated. Figure 4.5 demostrates the synchronization error while estimating the signal $y_m$ and it can easily be seen that after some time, the error is rapidly converging to zero. Once $y_m$ is estimated, receiver A will also synchronize with transmitter A and then decrypts the message back. Figure 4.6 depicts the performance of the cascaded receivers for decrypting the message signal where dashed line represents the transmitted message signal.

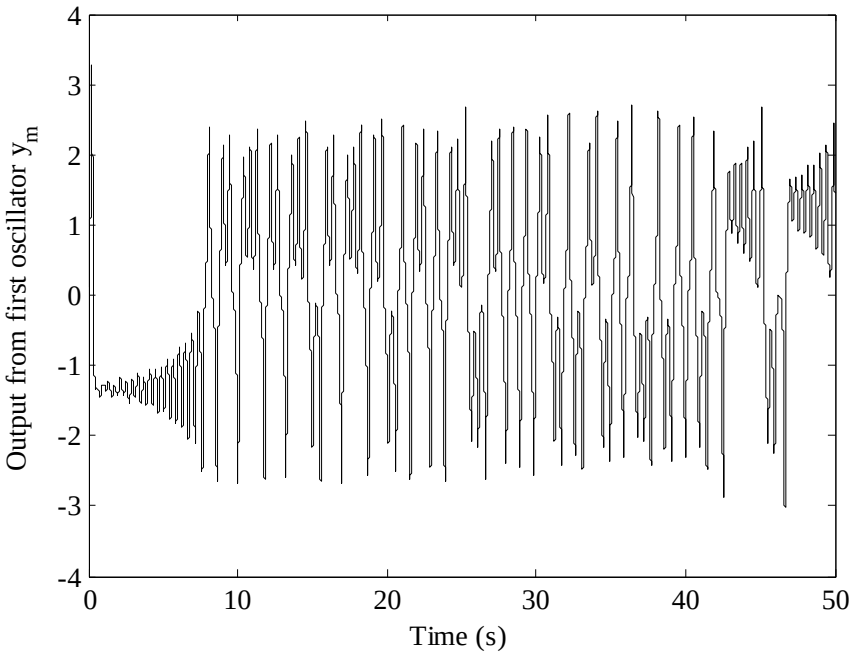


Figure 4.2: Output $y_m$ after first level of masking from oscillator (4.13).

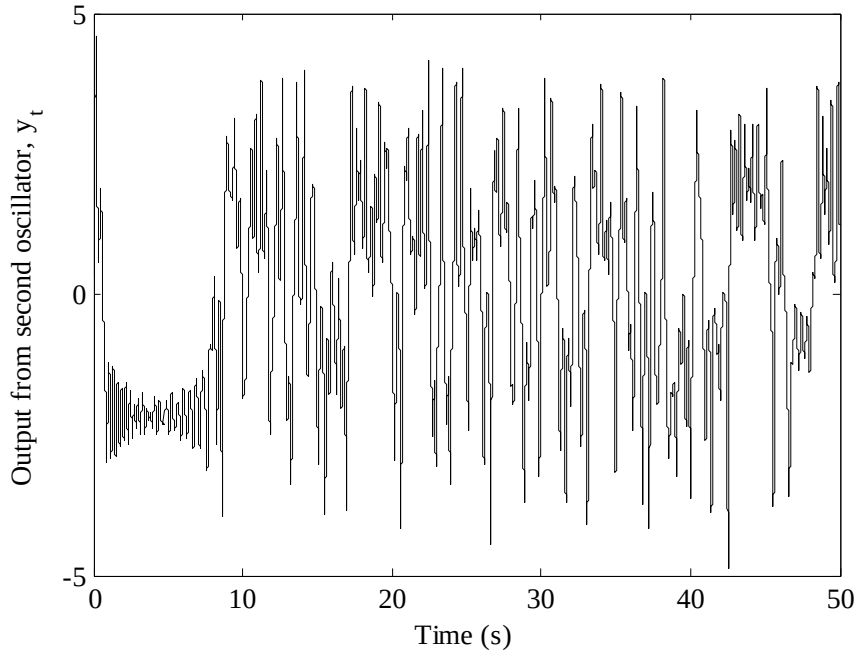


Figure 4.3: Output $y_t$ after second level of masking from oscillator (4.14).

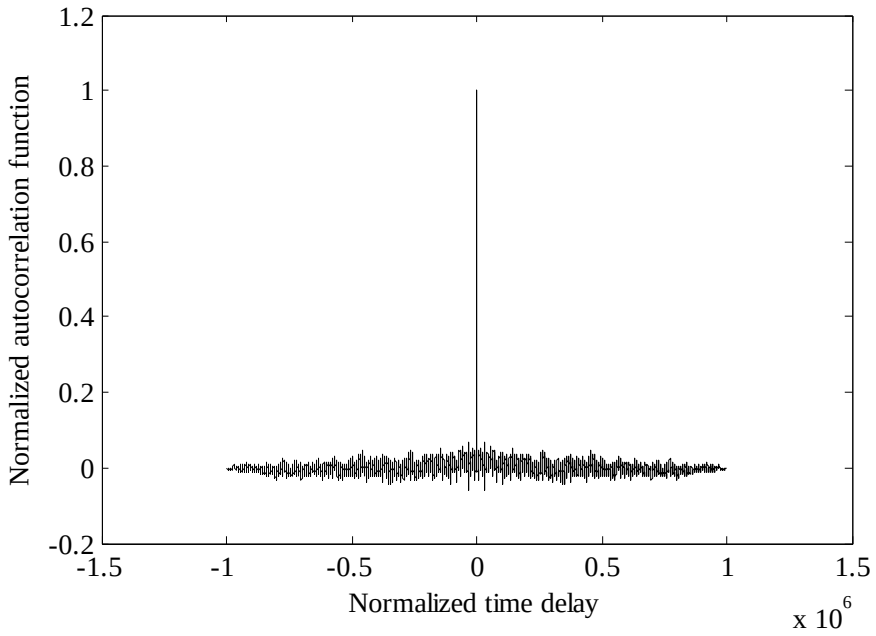


Figure 4.4: Autocorrelation function of the transmitted signal $y_t$.

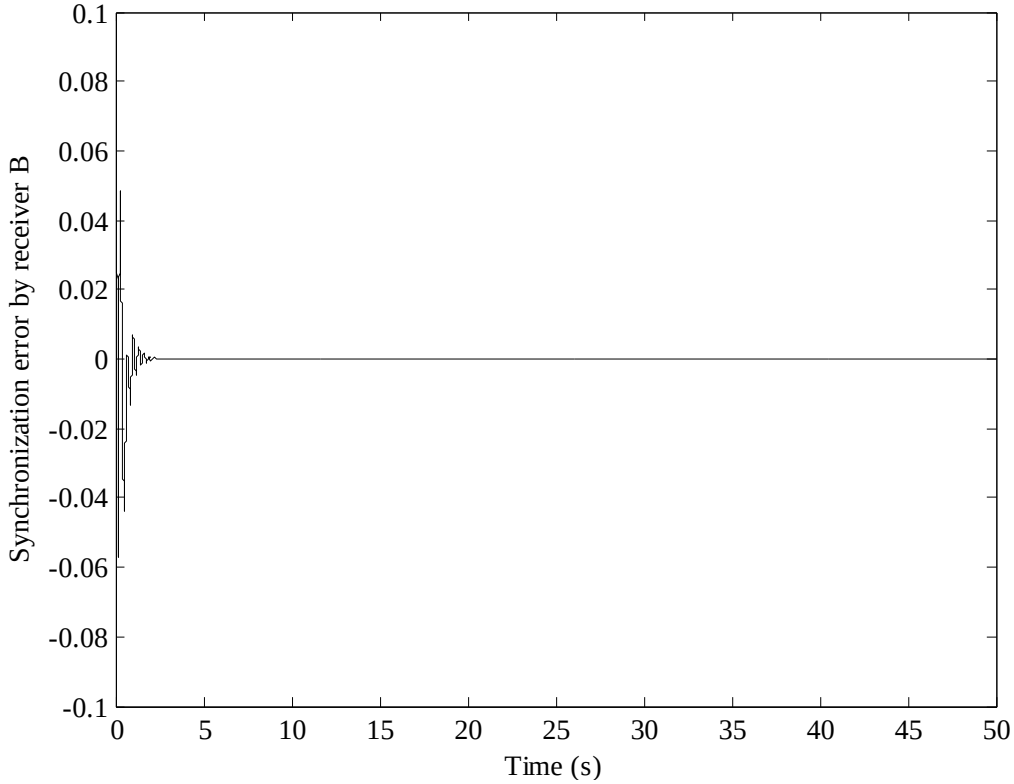


Figure 4.5: Synchronization error while estimating $y_m$ by oscillator (4.15).

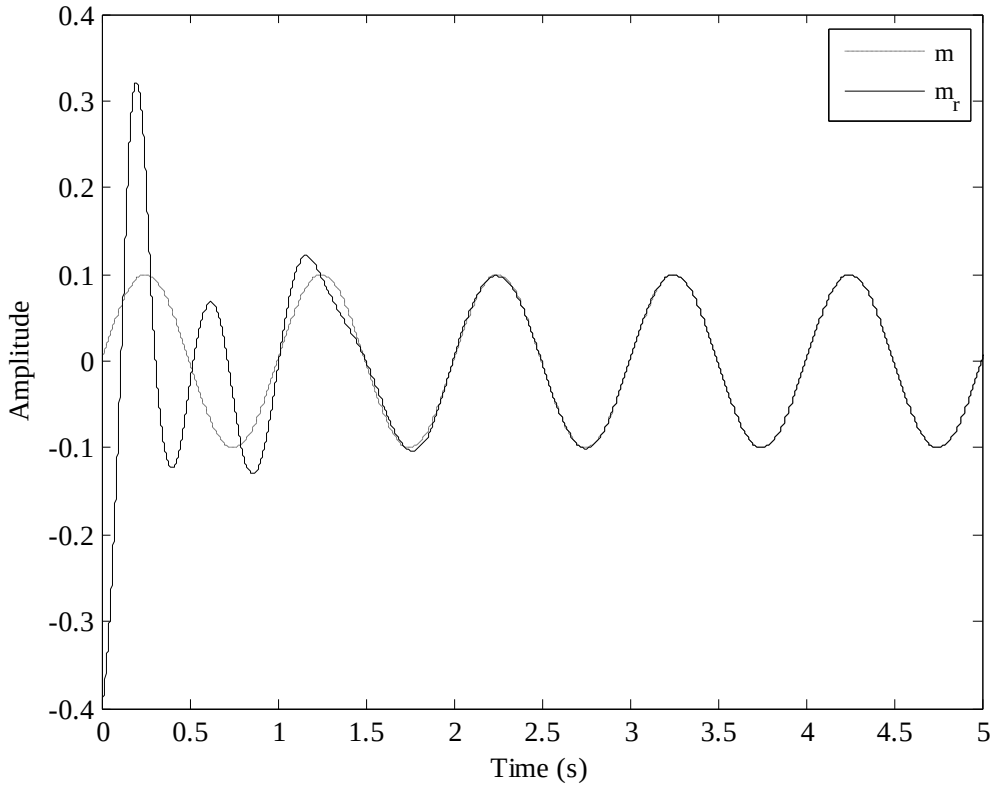


Figure 4.6: Transmitted and received message signal

## 4.5 Summary

In this chapter, a new method by implementing cascaded chaotic transmitter and receivers was proposed to increase the security of the traditional masking. Indeed, since the two roughly equal powered chaotic signals were added together, this will add complexities to the attack methods. However, it is still not convincing that the method proposed as cascaded structured oscillators will indeed make the communication scheme secure enough for intruders. The fact that the message signal is added to the sum of two chaotic signals of equal power means that rather than using 3-dimensional chaotic system for modulation purposes, an equivalent higher dimensional, 6 in this case, chaotic system has been used for modulation of the message. This will indeed make the task of extracting the message harder but it is uncertain that this method will be highly secure enough for motivated

intruders considering the fact that systems implementing hyperchaotic systems or time-delay systems are also proven to be insecure. Therefore, more secure methods need to be tried and investigated. In the subsequent chapters in this thesis, we will discuss about different other possible techniques to improve the security of the different methods.

# Chapter 5 The Concepts of Indirect Coupled Chaotic Synchronization

## 5.1 Introductions

Chaotic synchronization is the most important concept for chaotic signals to be used in communication system application. There are different types of chaotic synchronization as discussed earlier such as CS, GS, Phase Synchronization, Projective Synchronization, Lag Synchronization etc and many ways to achieve these such as drive-response system, active passive decomposition method, and method based on observer theory, etc. No matter what types or methods, there is always a coupling between the two chaotic systems that means an output chaotic signal from one chaotic system is driving another chaotic system thus forming a unidirectional coupling. Synchronization based on bidirectional coupling is also possible but might not be relevant for communication system applications. Since a signal had to be fed from one system to another, if there are two chaotic systems separated by a distance (channel), the unidirectional coupling will be equivalent to the transmission of a signal from the transmitter to the receiver. Therefore, in almost all chaotic communication methods proposed until now uses unidirectional coupling for chaotic synchronization.

In this chapter, however, a different type of chaotic synchronization called Indirect Coupled Chaotic Synchronization is proposed and on subsequent chapters, it will be utilized for implementing a secure communication link. In this method of synchronization, the oscillator to be synchronized is not being driven directly by an output of another oscillator. This method of synchronization is being proposed for the first time in this PhD work. This method is shown in the block diagram as depicted in Figure 5.1.

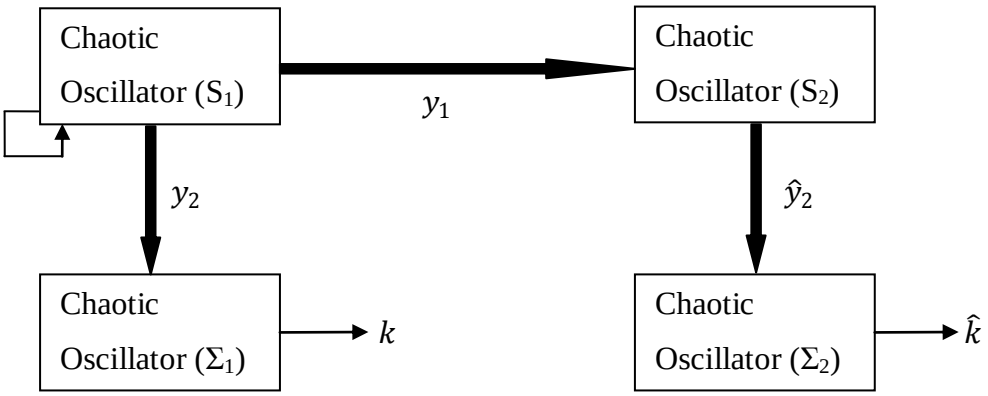


Figure 5.1: Block diagram to show the proposed indirect coupled chaotic synchronization.

As it can be seen in the Figure 5.1, there are 4 chaotic oscillators present. ($S_1$) and ($S_2$) are coupled together such that ($S_2$) is being driven by the output of oscillator ($S_1$) (unidirectional coupling). Now, our motive is to achieve synchronization between ($\Sigma_1$) and ($\Sigma_2$) even though they are not coupled together directly. The idea follows like this. Since, oscillator ($S_1$) and ($S_2$) are coupled together, chaotic synchronization can be achieved between them which mean all states of ($S_1$) and ($S_2$) will coincide once synchronization happens. Now, another output is selected from both oscillator ($S_1$) and ($S_2$). These output $y_2$ and $\hat{y}_2$ are used to drive chaotic oscillators ($\Sigma_1$) and ($\Sigma_2$) independently. Since $y_2$ and $\hat{y}_2$ are going to be equal once synchronization occurs between ($S_1$) and ($S_2$), logically it seems that two chaotic oscillators are being driven by a common signal making them to synchronize as well, just like as if they were unidirectionally coupled. Since, the chaotic oscillators to be synchronized are not directly coupled this scheme of synchronization is termed as Indirect Coupled Chaotic Synchronization.

The Lorenz and Chua's system will be used to demonstrate ICCS. Simulation using Matlab/Simulink will be performed to show that this technique is indeed useful for achieving chaotic synchronization between oscillators ($S_1$) and ($S_2$). However, it should be

noted that the performance of ($\Sigma_1$) and ($\Sigma_2$) oscillators to synchronize with each other is the key for ICCS of ($\Sigma_1$) and ($\Sigma_2$). Oscillators ($S_1$) and ($S_2$) are defined as Lorenz equations as (5.1).

$$
\begin{aligned}
&\dot{u} = \sigma u + \sigma v \\
(S_1): \quad &\dot{v} = -20uw + ru - v \\
&\dot{w} = 5u - bw \\
&y_1 = u \\
&y_2 = v
\end{aligned}
\tag{5.1}
$$

$$
\begin{aligned}
&\dot{\hat{u}} = \sigma \hat{u} + \sigma \hat{v} \\
(S_2): \quad &\dot{\hat{v}} = -20u\hat{w} + ru - \hat{v} \\
&\dot{\hat{w}} = 5u - b\hat{w} \\
&\hat{y}_2 = \hat{v}
\end{aligned}
$$

The oscillators ($\Sigma_1$) and ($\Sigma_2$) are defined as Chua's equations.

$$
\begin{aligned}
&\dot{p} = \alpha(q - p - f(y_2)) \\
(\Sigma_1): \quad &\dot{q} = y_2 - q - s \\
&\dot{s} = -\beta q - \gamma s
\end{aligned}
\tag{5.2}
$$

$$
\begin{aligned}
&\dot{\hat{p}} = \alpha(\hat{q} - \hat{p} - f(\hat{y}_2)) \\
(\Sigma_2): \quad &\dot{\hat{q}} = \hat{y}_2 - \hat{q} - \hat{s} \\
&\dot{\hat{s}} = -\beta \hat{q} - \gamma \hat{s}
\end{aligned}
$$

It can be seen on (5.2) that ($\Sigma_1$) and ($\Sigma_2$) are being driven by output of ($S_1$) and ($S_2$), i.e. $y_2$ and $\hat{y}_2$ respectively. The signals are fed into the non-linearity of the Chua's system in order to remove the effect of non-linearity on error dynamics for achieving synchronization. The parameters used in (5.1) and (5.2) are as follows.

$$\sigma = 16, r = 45.6, b = 4.2, \alpha = 10, \beta = -14.87, \gamma = 0$$

Figure 5.2 shows the states $p$ and $\hat{p}$ of Chua's system ($\Sigma_1$) and ($\Sigma_2$) when the ICCS is not implemented. Therefore, ($\Sigma_1$) and ($\Sigma_2$) are independent chaotic oscillators starting from different initial conditions which means, the trajectory $p$ and $\hat{p}$ will diverge from each other as time progresses as seen on Figure 5.2. Figure 5.3 depicts the states $p$ and $\hat{p}$ when

ICCS is implemented and Figure 5.4 verifies the functionality of ICCS by illustrating the linear decrease of the log plot of the synchronization error between $p$ and $\hat{p}$ showing rapid synchronization. It is clear that when ICCS is implemented, the two systems ($\Sigma_1$) and ($\Sigma_2$) synchronize with each other even if they are starting from different initial conditions. The log plot of the synchronization error is decreasing linearly against time, which proves the exponential convergence of system ($\Sigma_1$) and ($\Sigma_2$).

Simulation results confirm that indirect coupled synchronization for chaotic systems is indeed possible but in next section it will be mathematically proven. The ICCS will be proven for both the continuous and discrete-time chaotic systems. For continuous system, proof will be made for two different forms of the system which shall be useful in subsequent chapters of this thesis when ICCS is utilized for achieving secure communication.

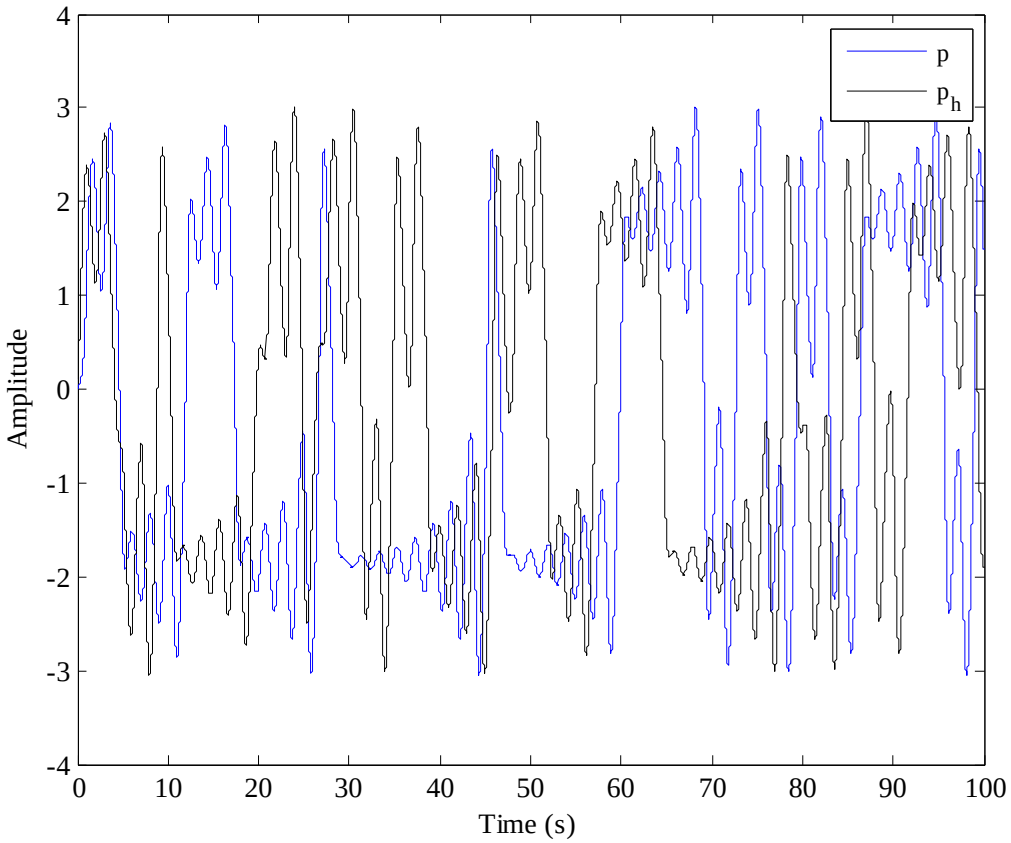


Figure 5.2: Output of Chua's system (A) and (B) when there is not ICCS between them.

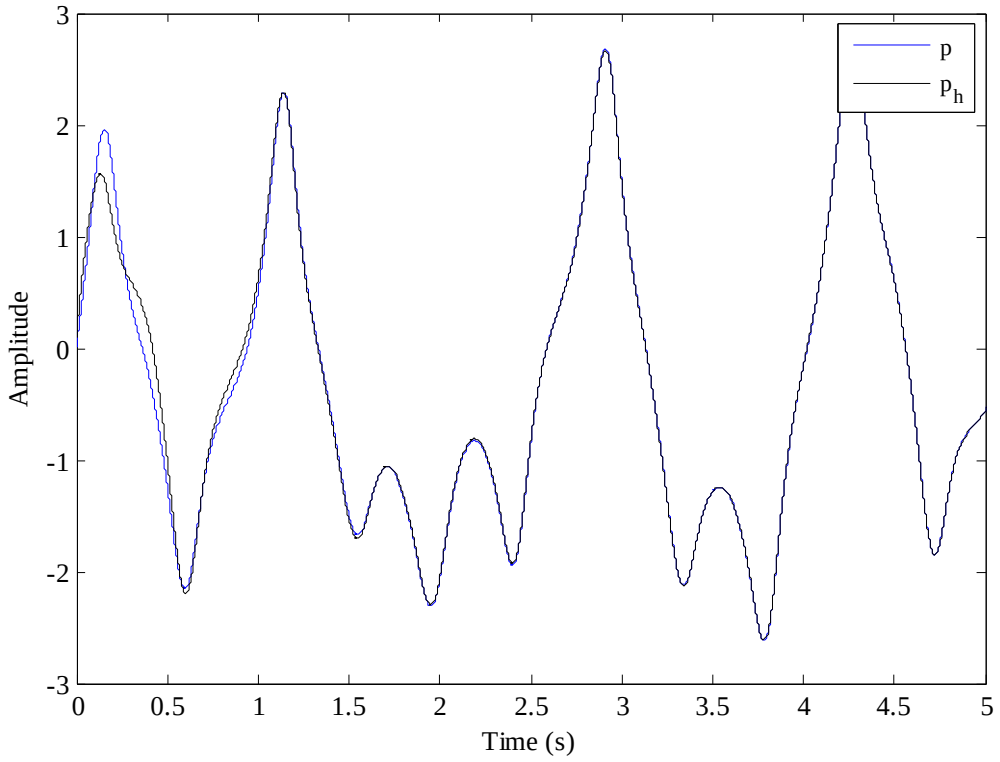


Figure 5.3: Output of Chua's system (A) and (B) when ICCS is implemented.

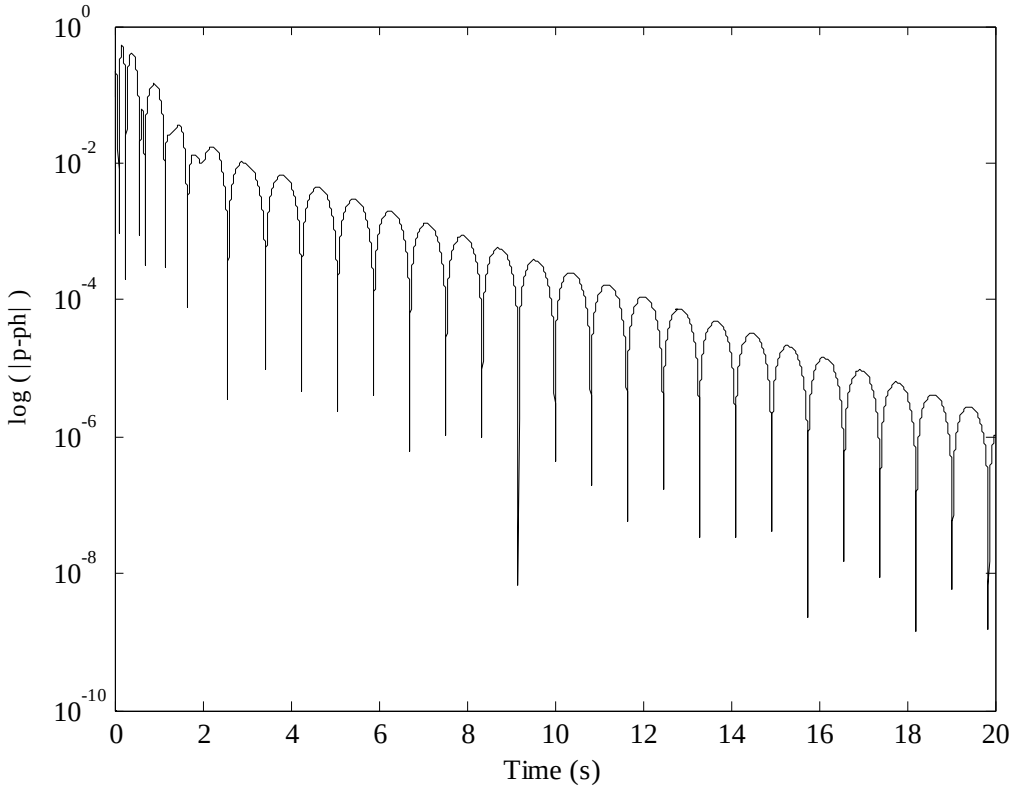


Figure 5.4: Synchronization error for Chua's system (A) and (B) when ICCS is implemented.

## 5.2 Mathematical Proof of Indirect Coupled Chaotic Synchronization

In this section, the stability of the error dynamics of the chaotic systems ($\Sigma_1$) and ($\Sigma_2$) will be analyzed. If the error dynamics of the two systems are stable, then synchronization is achieved. The ICCS proof will now follow for the continuous and discrete-time chaotic systems.

### 5.2.1 Continuous Time Chaotic System Case

Proofs for two different forms of chaotic systems are done in this section. Each of these form are used later on to propose secure chaotic communication technique.

#### 5.2.1.1 Proof 1

Let us consider the chaotic systems $S_1$ and $\Sigma_1$ of the following general form:

$$(S_1): \begin{cases} \dot{x}(t) = f(x(t), y_1(t)) \\ y_1(t) = h_1(x(t)) \\ y_2(t) = h_2(x(t)) \end{cases}$$
$$(\Sigma_1): \begin{cases} \dot{z}(t) = p(z(t), y_2(t)) \\ k(t) = q(z(t)), \end{cases} \tag{5.3}$$

where $x \in R^{n_1}$, $z \in R^{n_2}$ and $y_1, y_2, k \in R$. The output functions $h_1(x)$, $h_2(x)$ and $q(z)$ are assumed to be smooth.

Now, consider the following coupled chaotic systems:

$$(S_2): \begin{cases} \dot{\hat{x}}(t) = f(\hat{x}(t), y_1(t)) \\ \hat{y}_1(t) = h_1(\hat{x}(t)) \\ \hat{y}_2(t) = h_2(\hat{x}(t)) \end{cases}$$
$$(\Sigma_2): \begin{cases} \dot{\hat{z}}(t) = p(\hat{z}(t), \hat{y}_2(t)) \\ \hat{k}(t) = q(\hat{z}(t)) \end{cases} \tag{5.4}$$

We shall assume that:

**A1)** There exist a constant symmetric positive definite matrix $P_1$ and a positive constant $\alpha_1 > 0$ such that for all $\xi \in R^{n_1}$, $y \in R$:

$$P_1 A(\xi, y) + A^T(\xi, y) P_1 \le -\alpha_1 I_{n_1}, \tag{5.5}$$

where $A = \frac{\partial f}{\partial x}(\xi, y)$ and $I_{n_1}$ is the identity matrix of dimension $n_1$.

**A2)** There exist a constant symmetric positive definite matrix $P_2$ and a positive constant $\alpha_2 > 0$ such that for all $\varsigma \in R^{n_2}$, $y \in R$:

$$P_2 F(\varsigma, y) + F^T(\varsigma, y) P_2 \le -\alpha_2 I_{n_2}, \tag{5.6}$$

where $F = \frac{\partial p}{\partial z}(\varsigma, y)$ and $I_{n_2}$ is the identity matrix of dimension $n_2$.

**A3)** There exists a constant $M > 0$ such that $\left\| \frac{\partial p}{\partial y}(z, y) \right\| \le M$ for all $z \in R^{n_2}$, $y \in R$.

**A4)** There exists a positive constant $\upsilon$ such that $\left\| \frac{\partial h_2}{\partial x}(\theta) \right\| \le \upsilon$ for all $\theta \in R^{n_1}$.

Our aim is to show, under the above assumptions, $\lim_{t \to +\infty} \| z - \hat{z} \| = 0$. More precisely, our main result is summarised in the following theorem.

**Theorem 1.** Assume that the pairs of coupled systems $(S_1, \Sigma_1)$ and $(S_2, \Sigma_2)$ satisfy assumption A1) - A4). Then, $\lim_{t \to +\infty} \| x - \hat{x} \| = 0$ and $\lim_{t \to +\infty} \| z - \hat{z} \| = 0$. In other words, $S_1$ synchronises with $S_2$ and $\Sigma_1$ synchronises with $\Sigma_2$.

**Proof**: Set $\varepsilon = x - \hat{x}$, then,

$$\dot{\varepsilon} = f(x, y_1) - f(\hat{x}, y_1). \tag{5.7}$$

By mean value theorem, we know that there exists $\xi$ belonging to the segment with end points $x$ and $\hat{x}$ such that:

$$\begin{aligned} \dot{\varepsilon} &= f(x, y_1) - f(\hat{x}, y_1) \\ &= \frac{\partial f}{\partial x}(\xi, y_1)\varepsilon = A(\xi, y_1)\varepsilon. \end{aligned} \tag{5.8}$$

Similarly, let $\in = z - \hat{z}$, then,

$$
\begin{aligned}
\dot{\epsilon} &= p(z, y_2) - p(\hat{z}, \hat{y}_2) \\
&= p(z, y_2) - p(\hat{z}, y_2) + p(\hat{z}, y_2) - p(\hat{z}, \hat{y}_2) \\
&= \frac{\partial p}{\partial z}(\varsigma, y_2)\epsilon + \frac{\partial p}{\partial y_2}(\hat{z}, \eta)\left(y_2 - \hat{y}_2\right) \\
&= F(\varsigma, y_2)\epsilon + \frac{\partial p}{\partial y_2}(\hat{z}, \eta)\left(h_2(x) - h_2(\hat{x})\right)
\end{aligned}
\tag{5.9}
$$

for some $\varsigma$ belonging to the segment with end points $z$ and $\hat{z}$, and $\eta$ belonging to the segment with end points $y_2$ and $\hat{y}_2$.

Additionally,

$$
\begin{aligned}
\dot{\epsilon} &= \frac{\partial p}{\partial z}(\varsigma, y_2)\epsilon + \frac{\partial p}{\partial y_2}(\hat{z}, \eta)\left(h_2(x) - h_2(\hat{x})\right) \\
&= \frac{\partial p}{\partial z}(\varsigma, y_2)\epsilon + \frac{\partial p}{\partial y_2}(\hat{z}, \eta)\frac{\partial h_2}{\partial x}(\vartheta)\varepsilon \\
&= F(\varsigma, y_2)\epsilon + G(\hat{z}, \eta)C_2(\vartheta)\varepsilon,
\end{aligned}
\tag{5.10}
$$

where $\vartheta$ belongs to the segment with end points $x$ and $\hat{x}$.

Now let $V(\varepsilon) = \varepsilon^T P_1 \varepsilon$ be a candidate Lyapunov function for (5.7). Then,

$$
\dot{V}(\varepsilon) = 2\varepsilon^T P_1 \dot{\varepsilon} = 2\varepsilon^T P_1 \frac{\partial f}{\partial x}(\xi, y_1)\varepsilon = 2\varepsilon^T P_1 A(\xi, y_1)\varepsilon. \tag{5.11}
$$

By assumption A1) we have $2\varepsilon^T P_1 A(\xi, y_1)\varepsilon \le -\alpha_1(\xi, y_1)\varepsilon^T\varepsilon = -\alpha_1\|\varepsilon\|^2$, so that:

$$
\dot{V}(\varepsilon) \le -\alpha_1\|\varepsilon\|^2. \tag{5.12}
$$

Similarly, let $W(\epsilon) = \epsilon^T P_2 \epsilon$ be a candidate Lyapunov function for (5.9). Then,

$$
\begin{aligned}
\dot{W}(\epsilon) &\le -\alpha_2\|\epsilon\|^2 + 2\epsilon^T P_2 G(\hat{z}, \eta)C_2(\vartheta)\varepsilon \\
&\le -\alpha_2\|\epsilon\|^2 + 2\|P_2\epsilon\|\|G(\hat{z}, \eta)C_2(\vartheta)\|\|\varepsilon\|.
\end{aligned}
\tag{5.13}
$$

By assumption A3) and A4), we have:

$$
\dot{W}(\epsilon) \le -\alpha_2\|\epsilon\|^2 + 2M\upsilon\|P_2\epsilon\|\|\varepsilon\|. \tag{5.14}
$$

Now, $\beta_0\|\epsilon\|^2 \le \epsilon^T P_2 \epsilon \le \beta_1\|\epsilon\|^2$ where $\beta_0, \beta_1 > 0$ are respectively the smallest and largest eigenvalue of $P_2$. Similarly, $\gamma_0\|\varepsilon\|^2 \le \varepsilon^T P_1 \varepsilon \le \gamma_1\|\varepsilon\|^2$ where $\gamma_0, \gamma_1 > 0$ are respectively the

smallest and largest eigenvalue of $P_1$. Consequently,

$$\dot{W}(\in) \le -\frac{\alpha_2}{\beta_1} W(\in) + 2\frac{\sqrt{\beta_1}M\upsilon}{\sqrt{\beta_0}\sqrt{\gamma_0}}\sqrt{W(\in)}\sqrt{V(\varepsilon)} \tag{5.15}$$

and

$$\dot{V}(\varepsilon) \le -\frac{\alpha_1}{\gamma_1} V(\varepsilon). \tag{5.16}$$

Additionally, $\dot{W}(\in) = 2\sqrt{W(\in)}\,\dot{\sqrt{W(\in)}}$ and $\dot{V}(\varepsilon) = 2\sqrt{V(\varepsilon)}\,\dot{\sqrt{V(\varepsilon)}}$ so that (5.23) and (5.24) becomes:

$$\begin{aligned} \dot{\sqrt{W(\in)}} &\le -\frac{\alpha_2}{2\beta_1}\sqrt{W(\in)} + \frac{\sqrt{\beta_1}M\upsilon}{\sqrt{\beta_0}\sqrt{\gamma_0}}\sqrt{V(\varepsilon)} \\ \dot{\sqrt{V(\varepsilon)}} &\le -\frac{\alpha_1}{2\gamma_1}\sqrt{V(\varepsilon)}. \end{aligned} \tag{5.17}$$

In other words,

$$\begin{aligned} \begin{pmatrix} \dot{\sqrt{W(\in)}} \\ \dot{\sqrt{V(\varepsilon)}} \end{pmatrix} &= \begin{pmatrix} -\frac{\alpha_2}{2\beta_1} & \frac{\sqrt{\beta_1}M\upsilon}{\sqrt{\beta_0}\sqrt{\gamma_0}} \\ 0 & -\frac{\alpha_1}{2\gamma_1} \end{pmatrix} \begin{pmatrix} \sqrt{W(\in)} \\ \sqrt{V(\varepsilon)} \end{pmatrix} \\ &= F\begin{pmatrix} \sqrt{W(\in)} \\ \sqrt{V(\varepsilon)} \end{pmatrix} \end{aligned} \tag{5.18}$$

Since the matrix $F$ is stable, we have $\lim_{t\to+\infty} W(\in) = 0$ and $\lim_{t\to+\infty}\sqrt{V(\varepsilon)} = 0$. Consequently, $\lim_{t\to+\infty}\|x - \hat{x}\| = 0$ and $\lim_{t\to+\infty}\|z - \hat{z}\| = 0$ which, in turn implies that $\lim_{t\to+\infty}\left|k - \hat{k}\right| = \lim_{t\to+\infty}|q(z) - q(\hat{z})| = 0.$

This completes the proof of Theorem 1 thus proving the ICCS for the chaotic systems of the form defined in (5.3) and (5.4).

**Remark 1:** If system $(S_1)$ was slightly perturbed so that:

$$(S_1): \begin{cases} \dot{x} = f(x(t), y_1(t)) + \Delta f(x(t), y_1(t)) \\ y_1 = h_1 x \\ y_2 = h_2 x \end{cases} \tag{5.19}$$

Then, it can be shown that:

$$\begin{pmatrix} \dot{\sqrt{W(\in)}} \\ \dot{\sqrt{V(\varepsilon)}} \end{pmatrix} = F \begin{pmatrix} \sqrt{W(\in)} \\ \sqrt{V(\varepsilon)} \end{pmatrix} + \begin{pmatrix} \Delta f(x, y_1) \\ 0 \end{pmatrix} \tag{5.20}$$

It is therefore clear that, $\lim_{t\to\infty} \|x - \hat{x}\| = 0$ and $\lim_{t\to\infty} \|z - \hat{z}\| = 0$ if A and F are stable and provided that $\Delta f(x, y_1) = 0$. This idea will be used in the context of in improving the CSK method for secure communication in chapter 7.

#### 5.2.1.2 Proof 2

We assume that the oscillator $(S_1)$ is now described by a dynamical system of the following form:

$$(S_1): \begin{cases} \dot{x} = F(y_1)x + g(t, y_1) \\ y_1 = h_1(x) \\ y_2 = h_2(x), \end{cases} \tag{5.21}$$

where the state $x \in \Re^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator are $y_1 \in \Re$ and $y_2 \in \Re$. The matrix F is of appropriate dimension while $h_1$ and $h_2$ are analytical vector functions and g is a smooth bounded function of time.

The chaotic oscillator $(\Sigma_1)$ is of the similar form:

$$(\Sigma_1): \begin{cases} \dot{z} = Az + b(t, y_2) \\ k = h(z), \end{cases} \tag{5.22}$$

which is driven by the output $y_2(t)$. Here, $z \in \Re^q$ (q is not necessarily equal to n), $k \in \Re$ is the output, h is an analytical vector function and b is a smooth bounded function of time and A is a stable matrix of appropriate dimensions.

The receiving chaotic oscillator ($S_1$) is given by:

$$(S_2): \begin{cases} \dot{\hat{x}} = F(y_t)\hat{x} + g(t, y_t) \\ \hat{y}_1 = h_1(\hat{x}) \\ \hat{y}_2 = h_2(\hat{x}). \end{cases} \tag{5.23}$$

Finally, the key generator ($\Sigma_2$) is given by:

$$(\Sigma_2): \begin{cases} \dot{\hat{z}} = A\hat{z} + b(t, \hat{y}_2) \\ \hat{k} = h(\hat{z}). \end{cases} \tag{5.24}$$

We shall make the following assumptions:

**A5)** There exist symmetric positive definite (SPD) matrices $P_1$ and $Q_1$ such that

$$F^T P_1 + P_1 F = -Q_1. \tag{5.25}$$

**A6)** The function $h_2(x)$ is globally Lipschitzian with respect to x.

**A7)** The function b(t,y) is globally Lipschitzian with respect to y uniformly in t.

The objective is to show that the oscillators ($S_1$) and ($S_2$) synchronize and ($\Sigma_1$) and ($\Sigma_2$) are synchronized with each other when ICCS is implemented. In effect, based on the above assumptions, we state the following:

**Theorem 2.** Under the assumption A5), there exist two constants $\lambda, \eta > 0$ such that $\|x(t) - \hat{x}(t)\| \le \eta e^{-\lambda t} \|x(0) - \hat{x}(0)\|$ for all $t \ge 0$. In other words, the oscillator ($S_2$) synchronizes exponentially with the oscillator ($S_1$).

**Proof**: Let $\varepsilon(t) = x(t) - \hat{x}(t)$, then the error dynamics between ($S_1$) and ($S_2$) is given by:

$$\dot{\varepsilon} = \mathrm{F}(\mathrm{y_t})\varepsilon. \tag{5.26}$$

Owing to assumption A5), a candidate Lyapunov function of the above error dynamics can be chosen as:

$$\mathrm{V}(\varepsilon) = \varepsilon^{\mathrm{T}}\mathrm{P}_1\varepsilon. \tag{5.27}$$

Differentiating $\mathrm{V}(\varepsilon)$ with respect to time, yields:

$$\begin{aligned}\dot{\mathrm{V}}(\varepsilon) &= \dot{\varepsilon}^{\mathrm{T}}\mathrm{P}_1\varepsilon + \varepsilon^{\mathrm{T}}\mathrm{P}_1\dot{\varepsilon} \\ &= \varepsilon^{\mathrm{T}}\left[\mathrm{F}^{\mathrm{T}}(\mathrm{y_t})\mathrm{P}_1 + \mathrm{P}_1\mathrm{F}(\mathrm{y_t})\right]\varepsilon = -\varepsilon^{\mathrm{T}}\mathrm{Q}_1\varepsilon < 0.\end{aligned} \tag{5.28}$$

Since $\mathrm{Q}_1$ is SPD, there exist $\mathrm{c}_1, \mathrm{c}_2 > 0$ such that $\mathrm{c}_1\varepsilon^{\mathrm{T}}\mathrm{P}_1\varepsilon \le \varepsilon^{\mathrm{T}}\mathrm{Q}_1\varepsilon \le \mathrm{c}_2\varepsilon^{\mathrm{T}}\mathrm{P}_1\varepsilon.$ Consequently,

$$\dot{\mathrm{V}}(\varepsilon) = -\mathrm{c}_1\mathrm{V}(\varepsilon).$$

Integrating the last equation results in:

$$\mathrm{V}(\varepsilon(\mathrm{t})) = \mathrm{e}^{-\mathrm{c}_1\mathrm{t}}\mathrm{V}(\varepsilon(0)).$$

Again, since $\mathrm{P}_1$ is SPD, there exist $\lambda_1, \lambda_2 > 0$ such that $\lambda_1\varepsilon^{\mathrm{T}}\varepsilon \le \varepsilon^{\mathrm{T}}\mathrm{P}_1\varepsilon \le \lambda_2\varepsilon^{\mathrm{T}}\varepsilon.$ Consequently:

$$\lambda_1\left\|\varepsilon(\mathrm{t})\right\|^2 \le \lambda_2\mathrm{e}^{-\mathrm{c}_1\mathrm{t}}\left\|\varepsilon(0)\right\|^2. \tag{5.29}$$

In other words:

$$\left\|\varepsilon(\mathrm{t})\right\| \le \sqrt{\frac{\lambda_2}{\lambda_1}}\mathrm{e}^{-\frac{\mathrm{c}_1}{2}\mathrm{t}}\left\|\varepsilon(0)\right\| = \eta\mathrm{e}^{-\lambda t}\left\|\varepsilon(0)\right\|. \tag{5.30}$$

That is:

$$\left\|\mathrm{x}(\mathrm{t}) - \hat{\mathrm{x}}(\mathrm{t})\right\| \le \eta\mathrm{e}^{-\lambda t}\left\|\mathrm{x}(0) - \hat{\mathrm{x}}(0)\right\|. \tag{5.31}$$

This means that $\hat{x}(t)$ converges to $x(t)$ exponentially. In other words, the oscillator $(S_2)$ synchronizes exponentially with $(S_1)$. This completes the proof of Theorem 2.

**Theorem 3.** Assume that system $(\Sigma_1)$ and $(\Sigma_2)$ satisfies assumption A7), then $\lim_{t\to\infty}\|z(t)-\hat{z}(t)\|=0$. That is, the oscillator $(\Sigma_1)$ synchronizes asymptotically with the oscillator $(\Sigma_2)$.

**Proof**: Set $\zeta(t)=z(t)-\hat{z}(t),$ then the error dynamics between the $(\Sigma_1)$ and $(\Sigma_2)$ is given by:

$$\dot{\zeta}=A\zeta+b(t,y_2)-b(t,\hat{y}_2) \tag{5.32}$$

Since A is stable, there exist $P_2$ and $Q_2$ SPD such that $A^TP_2+P_2A=-Q_2$. Consequently, consider the following candidate Lyapunov function:

$$W=\zeta^TP_2\zeta \tag{5.33}$$

Differentiating W with respect to time results in:

$$\begin{aligned}\dot{W}&=2\zeta^TP_2\dot{\zeta}\\&=2\zeta^TP_2\left(A\zeta+b(t,y_2)-b(t,\hat{y}_2)\right)\\&=2\zeta^TP_2A\zeta+2\zeta^TP_2\left(b(t,y_2)-b(t,\hat{y}_2)\right)\\&\le-\zeta^TQ_2\zeta+2\left|\zeta^TP_2\right|\left\|\left(b(t,y_2)-b(t,\hat{y}_2)\right)\right|\\&\le-\beta_1W+\beta_2\|\zeta\|\|\varepsilon\|\\&\le-\beta_1W+\beta_3\sqrt{W}\|\varepsilon\|.\end{aligned} \tag{5.34}$$

for some positive constant $\beta_1$ and $\beta_3$ which depends on the Lipschitz constant of b and $h_2$.

Now,

$$\sqrt{\dot{W}}\le-\frac{\beta_1}{2}\sqrt{W}+\frac{\beta_3}{2}\|\varepsilon(t)\|. \tag{5.35}$$

Therefore,

$$\sqrt{W(\zeta(t))} \le -e^{-\frac{\beta_1}{2}t}\sqrt{W(\zeta(0))} + \frac{\beta_3}{2}\int_0^t e^{-\frac{\beta_1}{2}(t-\tau)}\|\varepsilon(t)\|d\tau. \tag{5.36}$$

From the above inequality, we can see that when $t \to +\infty$

$$\|\zeta(t)\| \to 0. \tag{5.37}$$

This completes the proof of Theorem 3 and therefore ($\Sigma_1$) converges with ($\Sigma_2$) asymptotically.

### 5.2.2 Discrete Time Chaotic System Case

Consider the following discrete-time dynamical systems:

$$(S_1): \begin{cases} x(k+1) = Fx(k) + f(y_1(k)) \\ y_1(k) = h_1(x(k)) \\ y_2(k) = h_2(x(k)), \end{cases} \tag{5.38}$$

where the state $x \in R^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator $y_1 \in R$ and $y_2 \in R$. The functions f, $h_1$ and $h_2$ are smooth. The discrete chaotic oscillator ($\Sigma_1$) is given as:

$$(\Sigma_1): \begin{cases} z(k+1) = g(z(k), y_2(k)) \\ u(k) = h(z(k)), \end{cases} \tag{5.39}$$

where $z \in R^q$ (q is not necessarily equal to n), $u \in R$, and h is an analytical function vector of appropriate dimension.

The chaotic oscillator ($S_2$) to synchronize with ($S_1$) is given by

$$(S_1):\ \begin{cases} \hat{x}(k+1) = F\hat{x}(k) + f(y_1(k)) \\ \hat{y}_1(k) = h_1(\hat{x}(k)) \\ \hat{y}_2(k) = h_2(\hat{x}(k)). \end{cases} \tag{5.40}$$

Finally, the chaotic oscillator ($\Sigma_2$) to synchronize with ($\Sigma_1$) is given as

$$(\Sigma_2):\ \begin{cases} \hat{z}(k+1) = g(\hat{z}(k), \hat{y}_2(k)) \\ \hat{u}(k) = h(\hat{z}(k)). \end{cases} \tag{5.41}$$

Note that the oscillator ($\Sigma_1$) and ($\Sigma_2$) are being driven by signal $y_2(k)$ and $\hat{y}_2(k)$ respectively for ICCS.

We will make the following assumptions:

**A8)** The matrix $F$ of (T) and (R) is stable.

**A9)** The function $g(z, w)$ is globally Lipschitzian with respect to $z$ and $w$. Additionally, there exists a positive constant $0 \le \nu \le 1$ such that $\|g(z(k), w(k)) - g(\hat{z}(k), w(k))\| \le \nu \|z(k) - \hat{z}(k)\|$, for all $k \ge 0$ and all $w \in R$.

**A10)** $\|g(z, y) - g(z, \hat{y})\| \le \gamma \|y - \hat{y}\|$

Our objective is to show that the oscillator ($\Sigma_1$) and ($\Sigma_2$) synchronize with each other to prove the ICCS.

In effect, based on the above assumptions, we state the following:

**Theorem 4.** Under the Assumptions A8), we have $\lim_{k\to\infty} \|x(k) - \hat{x}(k)\| = 0$. In other words, the oscillator ($S_2$) synchronizes exponentially with the oscillator ($S_1$).

**Proof**: Let $\varepsilon(k) = x(k) - \hat{x}(k)$, then the error dynamics between ($S_1$) and ($S_2$) is given by:

$$\xi(k+1) = F\xi(k). \tag{5.42}$$

Since F is stable, it is clear that $\|\xi(k)\| \to 0$ as $k \to \infty$. In other words, ($S_2$) synchronizes with ($S_1$) exponentially. This completes the proof of Theorem 4.

**Remark 2:** If F is not stable, then a discrete observer can easily be designed such that the overall error dynamics is stable. The aim here is to show the ICCS for a discrete system therefore the simplest form of coupled synchronization is employed for ($S_1$) and ($S_2$).

**Theorem 5.** Assume that system *($\Sigma_1$) and ($\Sigma_2$)* satisfies assumptions A8), A9) & A10), then $\lim_{k\to\infty}\|z(k) - \hat{z}(k)\| = 0$ . That is, the oscillator *($\Sigma_1$)* synchronizes asymptotically with *($\Sigma_2$)*.

**Sketch of proof**: Set $\varepsilon(k) = z(k) - \hat{z}(k),$ then the error dynamics between the ($\Sigma_1$) and ($\Sigma_2$) is given by:

$$\varepsilon(k+1) = g(z(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k). \tag{5.43}$$

Now, consider the following candidate Lyapunov function:

$$W(k) = \|\varepsilon(k)\|. \tag{5.44}$$

Then,

$$\begin{aligned} W(k+1) &= \|\varepsilon(k+1)\| \\ &= \|g(z(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k))\| \\ &\le \|g(z(k), y_2(k)) - g(\hat{z}(k), y_2(k))\| \\ &\quad + \|g(\hat{z}(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k))\| \\ &\le \beta\|z(k) - \hat{z}(k)\| + \gamma\|y_2(k) - \hat{y}_2(k)\| \\ &\le \beta\|\varepsilon(k)\| + \gamma\|\xi(k)\|. \end{aligned} \tag{5.45}$$

Finally,

$$W(k+1) - W(k) \le (\beta - 1)W(k) + \gamma \|\xi(k)\|. \tag{5.46}$$

Since from Theorem 4, $\|\xi(k)\| \to 0$ as $k \to \infty$, we will eventually have $W(k+1) - W(k) \le 0$.

This completes the proof of Theorem 5.

## 5.3 Summary

A chaotic synchronization technique where two chaotic oscillators ($\Sigma_1$ and $\Sigma_2$) are not directly coupled with each other is proposed in this chapter. The method, indirect coupled chaotic synchronization, is unique because there is no obvious link between that is there is no signal being fed from one oscillator to another one unlike every other synchronization techniques. However, there has to be some sort of connection between these two chaotic oscillators, starting from different initial conditions, if they are to be synchronized together. Because, if the oscillators have different initial conditions and have no connection between them, then because of the property of chaotic system, "Sensitivity to initial conditions", the trajectory of these two oscillators will diverge rapidly from each other. These two oscillators are therefore being driven independently by the output of two synchronized chaotic oscillators ($S_1$ and $S_2$) that have similar structure. These two chaotic oscillators are achieving synchronization from normal unidirectional coupling therefore the output, which are used to drive the former two chaotic oscillators, will be equal. Hence, equivalently, it will look like two chaotic oscillators are being driven by a common signal. The mathematical proof was done for both continuous-time and discrete-time chaotic systems. For continuous-time case, proof for two special forms was performed. The performance of the ICCS between ($\Sigma_1$) and ($\Sigma_2$) is dependent on the synchronizing performance of ($S_1$) and ($S_2$) which can be obtained from methods that are already

available on the literatures, for example, observer based synchronization. The ICCS can be very useful in realize secure communication, because the output from these indirectly coupled chaotic oscillators can be used as keystream in the transmitter and receiver side, without the need for it to get transmitted in the communication channel. This can have a major advantage, since the intruders will not be able to estimate the keystream being used for encryption purposes simply by having the transmitted signal available. In the coming chapters, it will be shown how ICCS can be implemented to realize secure communication link by removing the shortcomings of the methods that are available in the literature.

# Chapter 6 Application of Indirect Coupled Chaotic Synchronization to Secure Communications

## 6.1 Introductions

It was discussed in the previous chapter that ICCS is possible between two chaotic oscillators. The idea of ICCS can now further be implemented for realizing a secure communication system. In recent years, there have been lots of works where chaotic signals have been utilized for implementing secure communication. Methods like chaotic masking, chaotic modulation, inclusion method and CSK methods have already been discussed in the earlier part of this thesis. Cascaded method was also proposed earlier, but it was also pointed out there is still some vulnerabilities in it. Many modifications of the traditional methods were also discussed earlier and it was also pointed that almost all of those methods were shown to be breakable by a method or two. Hence, there is real incentive to devise new chaotic communication methodologies in order to realize a secure communication link. Even though chaotic signals have inherent properties like being aperiodic and limited predictability along with broad spectrum, etc, using them for secure communication have not become a straightforward task as it was thought to be. There had been significant number of attack methods that could recover the message signals only by performing signal processing of the transmitted signal.

In this chapter, we will see the possibility of implementing ICCS for realizing secure communication such that the attack methods available up to now in the literature will not be effective.

In one of the work proposed by Yang, et. al [1], a method based on encryption technique was proposed, where a different output from chaotic transmitter which was transmitted in the channel was used as a keystream to encrypt the message signal. The encrypted message signal masked with another output of the chaotic oscillator was employed as the transmitted signal. It was claimed that since the intruder could not get hold of the keystream, it was impossible for the attackers to extract the message. Unfortunately a later work done by Parker & Short [119] showed that it was still possible to extract the keystream from the transmitted chaotic signal since the keystream carried the information of the dynamics of the transmitter. In fact, since, both the carrier and keystream were the outputs of same oscillator; the carrier held the dynamics of the keystream as well. Therefore, it was impossible to hide the dynamics of the keystream from intruders, as a signal has to be transmitted from the transmitter to the receiver for synchronization and message transmission purpose. However, since the principle of the method proposed in [1] is nevertheless interesting, there is a real incentive for finding ways for improving the method by eliminating its shortcomings.

Figure 6.1 shows the block diagram of the cryptography based chaotic system for secure communication that had been proposed at [1]. The transmitter consists of the encryption function e(.) and the chaotic system. The key been used in the encryption function to encrypt the plain text m(t) is one of the state variable of the chaotic system. Another state variable is used as a masking signal to generate output $y_t(t)$ that is transmitted in the public channel which the intruders will also have access to. At the receiver side, the signal $y_t(t)$ (assuming minimal influence of channel noise) will be used to achieve synchronization to estimate the key and the encrypted signal. Upon applying the decryption function d(.) on the recovered encrypted signal, the estimate of plain text is achieved.

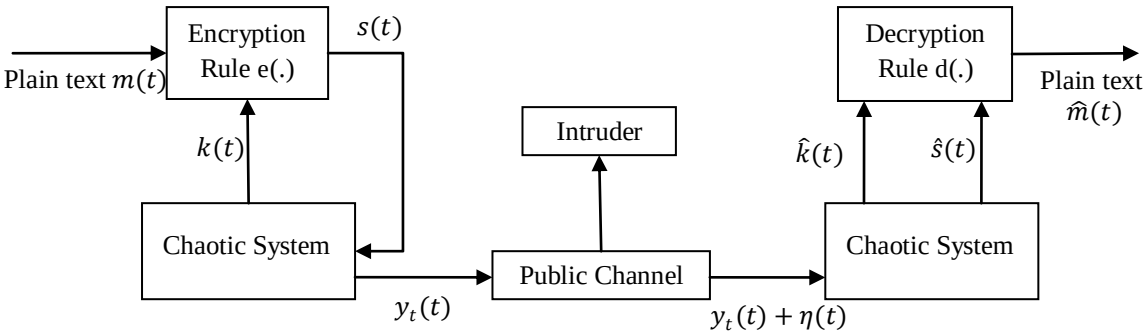


Figure 6.1: Yang's method based on cryptography [1].

For encryption and decryption purposes, n-shift cipher algorithm is used. The encryption algorithm is given as:

$$e(m(t)) = \underbrace{f_1(...f_1(}_{n} f_1(m(t), \underbrace{k(t)), k(t)),..., k(t))}_{n} = s(t), \tag{6.1}$$

where $f_1(*.*)$ is the following non-linear function:

$$f_1(x,k) = \begin{cases} x + k + 2h, & \text{for } -2h \le x + k \le -h \\ x + k, & \text{for } -h \le x + k \le h \\ x + k - 2h, & \text{for } h \le x + k \le 2h, \end{cases} \tag{6.2}$$

where h is the encryption parameter chosen such that m(t) and k(t) lies within the interval (-h, h). The non-linear function given in (6.2) is shown Figure 6.2.

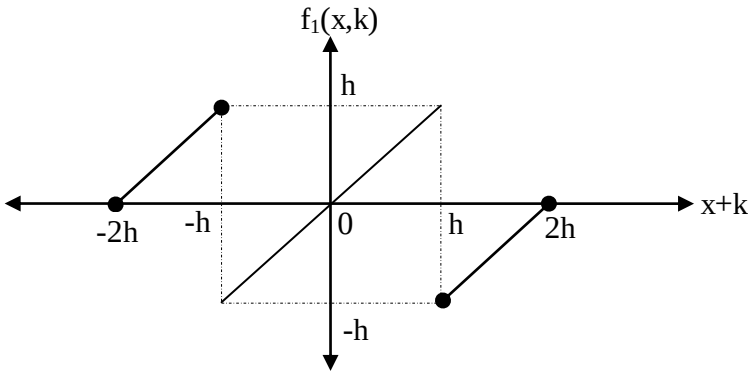


Figure 6.2: Non-linear function used in continuous n-shift cipher.

The corresponding decryption function d(.) to recover the plaintext at the receiver side is same as the encryption rule given as:

$$\hat{m}(t) = d(e(m(t)) = \underbrace{f_1(...f_1(}_{n} f_1(e(m(t), \underbrace{-\hat{k}(t)),-\hat{k}(t)),...,-\hat{k}(t))}_{n}, \tag{6.3}$$

where $\hat{k}(t)$ is recovered at the receiver side and should be approximately equal to k(t).

## 6.2 Proposed Method Based on Cryptography

In this section of this thesis chapter, we will propose a new chaotic communication technique based on indirect coupled chaotic synchronization. This technique is essentially the improvement of the method that had been proposed by Yang, et. al [1] where the shortcomings of that technique are eliminated. Instead of generating the chaotic signal used as a key from the same chaotic oscillator that is used to generate the transmitted signal, we propose to use a chaotic signal, which is an output of a different chaotic oscillator, as the key. The proposed method is demonstrated in the block diagram shown in Figure 6.3.

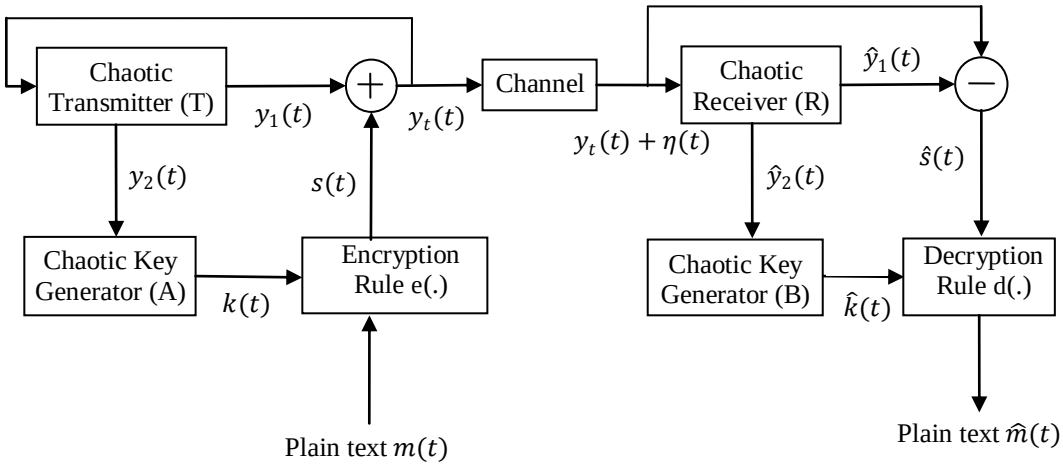


Figure 6.3: Block diagram of the proposed chaotic communication technique based on cryptography using ICCS.

The novelty here lies in the generation of the keystream. The chaotic transmitter (T) is first used to generate two output signals, $y_1(t)$ and $y_2(t)$. The signal $y_1(t)$ is used for modulation purpose while output $y_2(t)$ is used to drive chaotic oscillator (A) whose structure is different from the transmitter (T). The output k(t) of key generator (A) is used as a keystream to encrypt the plain text message m(t) using an encryption rule e(.). The resulting encrypted signal s(t) is modulated using $y_1(t)$ yielding the transmitted signal y(t). The output y(t) is fed back into the transmitter in the form of an output injection with the aim of cancelling the effect of non-linearity while performing synchronization at the receiver side. The modulated transmitted signal y(t) is sent through the channel to the receiver.

At the receiver end, upon receiving the signal $y_t'(t)$, the chaotic receiver (R) - which is similar in structure to the transmitter (T) - permits to obtain an estimate $\hat{y}_1(t)$ and $\hat{y}_2(t)$ of the signals $y_1(t)$ and $y_2(t)$ respectively by synchronization. This can be done by using any techniques existing in the literature such as observers, etc [43, 52, 54, 173]. The signals $\hat{y}_1(t)$ and $y_t'(t)$ are used to generate an estimate $\hat{s}(t)$ of the encrypted signal. The estimate $\hat{y}_2(t)$ is used to drive the chaotic key generator (B) - which is similar in structure to generator (A) – and which yields the keystream estimate $\hat{k}(t)$. Consequently, the plain text message m(t) can be recovered by using the decryption rule d(.).

Note that since, the chaotic key generators (A) and (B) are driven by $y_2(t)$ and $\hat{y}_2(t)$ respectively, an indirect coupled synchronization is required between these two chaotic oscillators. Also, $y_2(t)$ and $\hat{y}_2(t)$ are outputs of chaotic transmitter (T) and receiver (R) respectively and will be equal once synchronization is achieved. Intuitively, one would

expect this synchronization to take place and ICCS has already been proven in the earlier chapter.

The important part of this method is the generation of the keystream. No information regarding the keystream is transmitted in the channel. In [1], it was possible to estimate the particular state which was used as keystream (as shown in [119]) since the state that was transmitted in the public channel had information of the dynamics of the keystream as they were the state variables of same chaotic oscillator.

In contrast, in this method, the keystream is generated from a chaotic oscillator with a totally different structure. It will not be possible to estimate the dynamics of the chaotic key generator from the signal being transmitted in the channel by using the method mentioned in [119]. Even if the intruder manages to get hold of the encrypted signal from the transmitted signal, without the knowledge of keystream, the message signal cannot be decrypted back. Therefore, a secure communication link can be realized by implementing the proposed method.

The method based on ICCS can however have some disadvantages in its own right. In real time continuous system, the implementation of encryption algorithm along with the chaotic keystream can be a major bottleneck. When this is implemented in continuous time system, the implementation of the encryption algorithm can be very complicated to design specially with electronic components. However, this disadvantage will not exist in discrete time system since it can easily be implemented using digital signal processing. Also, if the intruders can reconstruct the keystream generator driving chaotic output of the transmitter T, then with the knowledge of the structure of the keystream generator, intruders might try to perform ICCS on their side to find out the keystream. Therefore, further studies on how the reconstructed driving chaotic output in T will help the intruders to estimate the

keystream should be done. Also, another point that arises is again the parameter of the key generator oscillator acting as another level of key of the cryptosystem. Therefore, the fact that driving signal could not be perfectly estimated and along with the parameters of key generator acting as another level of key, it can be said that estimating the keystream can be a challenging task for intruders with only the knowledge of the transmitted signal.

The method based on cryptography implementing ICCS will be implemented both on continuous-time and discrete-time context.

### 6.2.1 Continuous Time Scenario

Based on the communication scheme illustrated by Figure 6.3, we assume that the transmitter oscillator (T) described by a dynamical system of the following form:

$$(T): \begin{cases} \dot{x} = F(y_t)x + g(t, y_t) \\ y_1 = h_1(x) \\ y_2 = h_2(x) \\ y_t = y_1 + e(m, k), \end{cases} \tag{6.4}$$

where the state $x \in \Re^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator are $y_1 \in \Re$ and $y_2 \in \Re$. The matrix F is of appropriate dimension while $h_1$ and $h_2$ are analytical vector functions. The signal $y_t \in \Re$ is the transmitted signal and e(.) is the encryption function using key k(t) and the function g is a smooth bounded function of time.

The keystream k(t) is generated using another chaotic oscillator (A) of similar form:

$$(A): \begin{cases} \dot{z} = Az + b(t, y_2) \\ k = h(z), \end{cases} \tag{6.5}$$

which is driven by the output $y_2(t)$. Here, $z \in \Re^q$ (q is not necessarily equal to n), $k \in \Re$ is the keystream, h is an analytical vector function and b is a smooth bounded function of

time and A is a stable matrix of appropriate dimensions. It is assumed that the channel is perfect and that no distortion of the transmitted signal has taken place.

The receiving chaotic oscillator (R) is given by:

$$(R):\begin{cases}\dot{\hat{x}} = F(y_t)\hat{x} + g(t, y_t) \\ \hat{y}_1 = h_1(\hat{x}) \\ \hat{y}_2 = h_2(\hat{x}).\end{cases} \tag{6.6}$$

Finally, the key generator (B) is given by:

$$(B):\begin{cases}\dot{\hat{z}} = A\hat{z} + b(t,\hat{y}_2) \\ \hat{k} = h(\hat{z}).\end{cases} \tag{6.7}$$

The proof done in the Chapter 5, section 5.2.1.2 can be recalled for proving that (T) and (R) synchronize with each other and (A) and (B) synchronize with each other forming the ICCS, however the assumptions made should be verified when implementation is done in the next section of this chapter.

Once the synchronization is obtained between (A) and (B), the message can be decrypted by applying the keystream.

#### 6.2.1.1 Implementation using Lorenz and Chua's system

Now, the proposed system is demonstrated using the Lorenz system as the transmitter (T) and the receiver (R). More specifically, (T) and (R) are chosen as:

$$(T):\begin{cases}\dot{u} = -\sigma u + \sigma v \\ \dot{v} = -20\, y_t w + r y_t - v \\ \dot{w} = 5 y_t v - b w \\ y_1 = u \\ y_2 = v \\ y_t = y_1 + e(m,k).\end{cases} \tag{6.8}$$

$$(R):\begin{cases}\dot{\hat{u}} = -\sigma \hat{u} + \sigma \hat{v} \\ \dot{\hat{v}} = -20\, y_t \hat{w} + r y_t - \hat{v} \\ \dot{\hat{w}} = 5 y_t \hat{v} - b \hat{w} \\ \hat{y}_1 = \hat{u} \\ \hat{y}_2 = \hat{v}.\end{cases} . \tag{6.9}$$

Again it can easily be seen that (6.8) and (6.9) are in the form (6.4**)** and (6.6**)** with $F(y_t)$ given as:

$$F(y_t) = \begin{pmatrix} -\sigma & \sigma & 0 \\ 0 & -1 & -20 y_t \\ 0 & 5 y_t & -b \end{pmatrix}.$$

Now, we need to show that the assumptions made in Chapter 5 while proving the ICCS are valid for these choice of the systems. First of all, assumption A5) in Chapter 5 holds true for the following choice of SPD matrices $P_1$ and $Q_1$:

$$P_1 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \text{and } Q_1 = \begin{pmatrix} 2\sigma l_1 & -\sigma l_1 & 0 \\ -\sigma l_1 & 2 l_2 & 0 \\ 0 & 0 & 2 b l_3 \end{pmatrix}, \tag{6.10}$$

where $l_1, l_2, l_3, \sigma, b, r > 0, l_2 = -\frac{1}{4} l_3$ and $0 < l_1 < \frac{4}{\sigma} l_2$.

**Remark**. Note that, at first sight one would expect the matrices $P_1$ and $Q_1$ to be time dependent since $F(y_t)$ is time dependent. However, interestingly, due to the particular form of $F(y_t)$ the matrices turn out to be constants.

For the key generating oscillators A and B, the Chua's system is adopted given as below:

$$(A):\begin{cases}\dot{p} = \alpha(q - p - f(y_2)) \\ \dot{q} = y_2 - q - s \\ \dot{s} = -\beta q - \gamma s \\ k = d_0 p.\end{cases} \tag{6.11}$$

$$(B):\begin{cases}\dot{\hat{p}} = \alpha(\hat{q} - \hat{p} - f(\hat{y}_2)) \\ \dot{\hat{q}} = \hat{y}_2 - \hat{q} - \hat{s} \\ \dot{\hat{s}} = -\beta\hat{q} - \gamma\hat{s} \\ \hat{k} = d_0 \hat{p}.\end{cases} \tag{6.12}$$

The non-linear $f(\cdot)$ is piecewise linear function given as:

$$f(\psi) = G_b\psi + 0.5(G_a - G_b)(|\psi + 1| - |\psi - 1|).$$

Note that (6.11) and (6.12) are in the form (6.5) and (6.7) respectively, with A and $b_2(t, y_2)$ given as:

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & -1 \\ 0 & -\beta & -\gamma \end{pmatrix}, b(t, y_2) = \begin{pmatrix} -\alpha f(y_2) \\ y_2 \\ 0 \end{pmatrix}.$$

It can also be shown that matrix A is stable since there exist $P_2$ and $Q_2$ SPD such that $A^T P_2 + P_2 A = -Q_2$ for the following matrices:

$$P_2 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \& Q_2 = \begin{pmatrix} 2\alpha l_1 & -\alpha l_1 & 0 \\ -\alpha l_1 & l_2 & 0 \\ 0 & 0 & 2\gamma l_3 \end{pmatrix}, \tag{6.13}$$

where $l_1, l_2, l_3, \alpha > 0$, $\beta < 0, \gamma \geq 0$, $l_2 = -\beta l_3$ and $0 < l_1 < \frac{4}{\alpha} l_2$.

Finally, it is obvious that assumptions A6) and A7) of Chapter 5 are satisfied.

The encryption and decryption function are used same as in (6.1) and (6.3) respectively.

#### 6.2.1.2 Simulation results

The parameters employed in the equations (6.8), (6.9), (6.11) and (6.12) are as follows:

$$\sigma = 16, \mathrm{r} = 45.6, \mathrm{b} = 4.2, \alpha = 10, \beta = -14.87$$
$$\gamma = 0, \mathrm{G_a} = -1.27, \mathrm{G_b} = -0.68, \mathrm{d_0} = 0.05.$$

The encryption parameter $\mathrm{h}$ is chosen to be $0.3$ and the message $\mathrm{m(t)}$ is taken as a square wave modulating digital binary bits. Also in encryption rule (6.1), a 30-shift cipher is used. The initial conditions for each oscillator are chosen to arbitrarily different.

Figure 6.4 illustrates the autocorrelation function of the keystream signal $\mathrm{k(t)}$. It is clear that the keystream is not similar to itself with any amount of time shift so its autocorrelation function has only a single spike at point of zero time shift. This means the keystream generated is chaotic in nature and therefore has limited predictability. Figure 6.5 shows the encrypted message signal using (6.1) and signal $\mathrm{k(t)}$ as keystream. Figure 6.6 depicts the transmitted chaotic carrier and it can be seen that message signal is totally buried inside it. Figure 6.7 illustrates the error in estimating the keystream and it can be seen that although two oscillators are starting from different initial conditions, the error converges rapidly to zero after some initial period taken for synchronization.

Figure 6.8 depicts the performance of the proposed method in decrypting the message signal back and it is readily seen that the transmitted message signal has been estimated convincingly. Once it is clear that the message extraction is possible using the proposed method, security analysis of the method should be discussed.

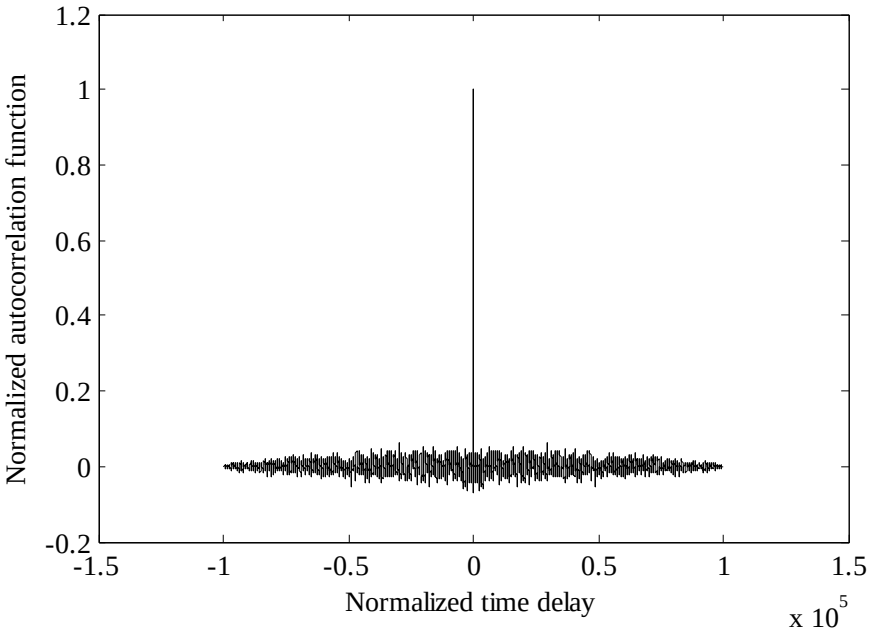


Figure 6.4: Autocorrelation of the key stream signal k(t).

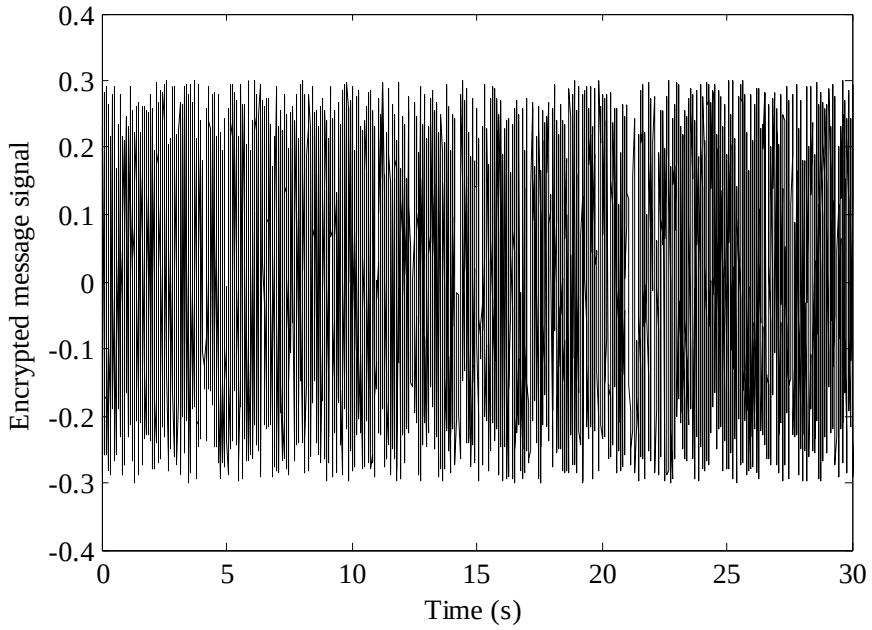


Figure 6.5: Encrypted message signal.

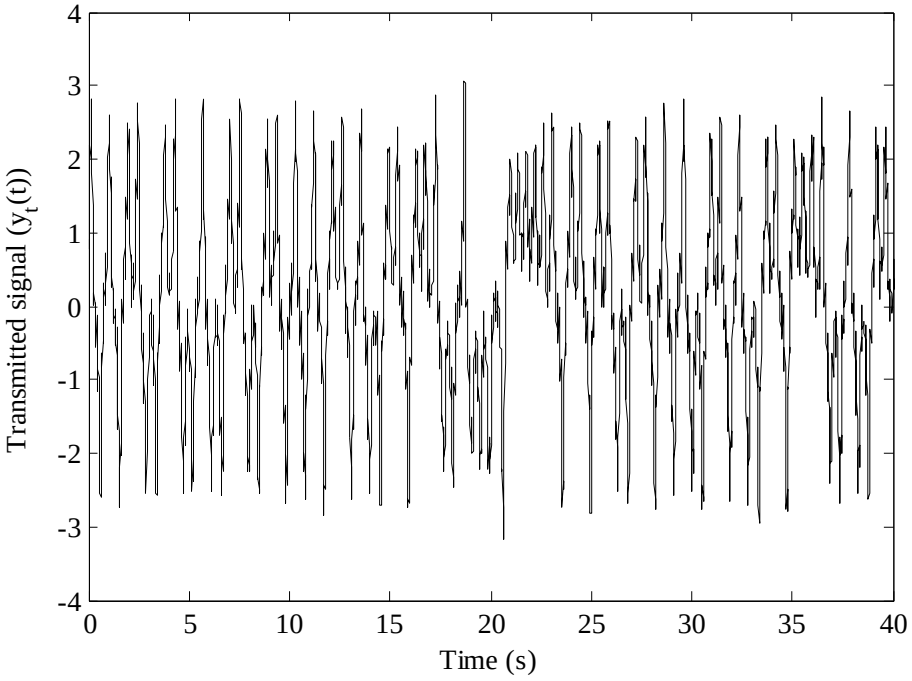


Figure 6.6: Transmitted signal $y_t(t)$ generated from the oscillator T.

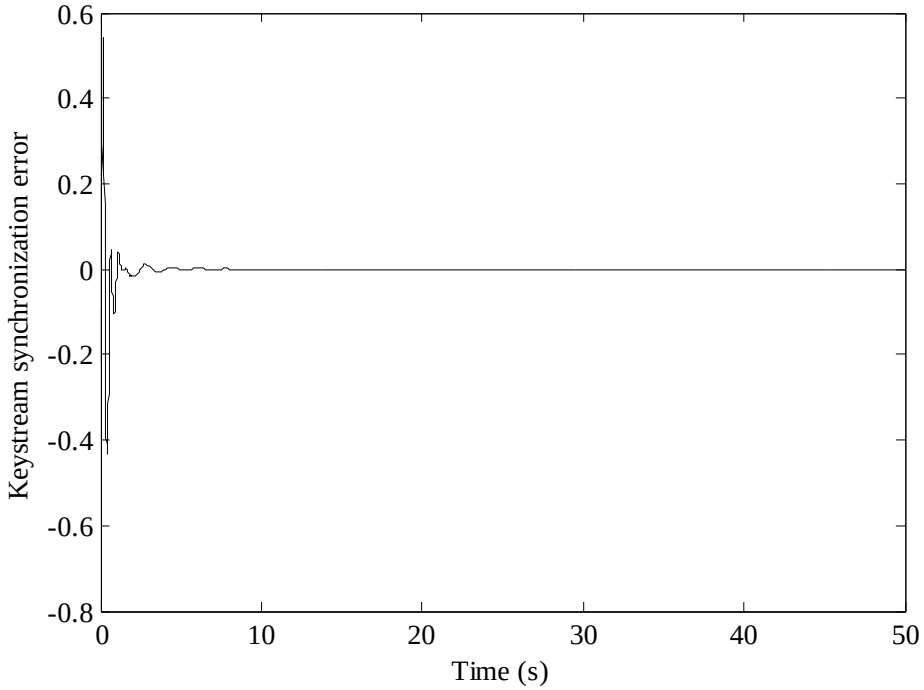


Figure 6.7: Synchronization error in the estimation of the keystream.

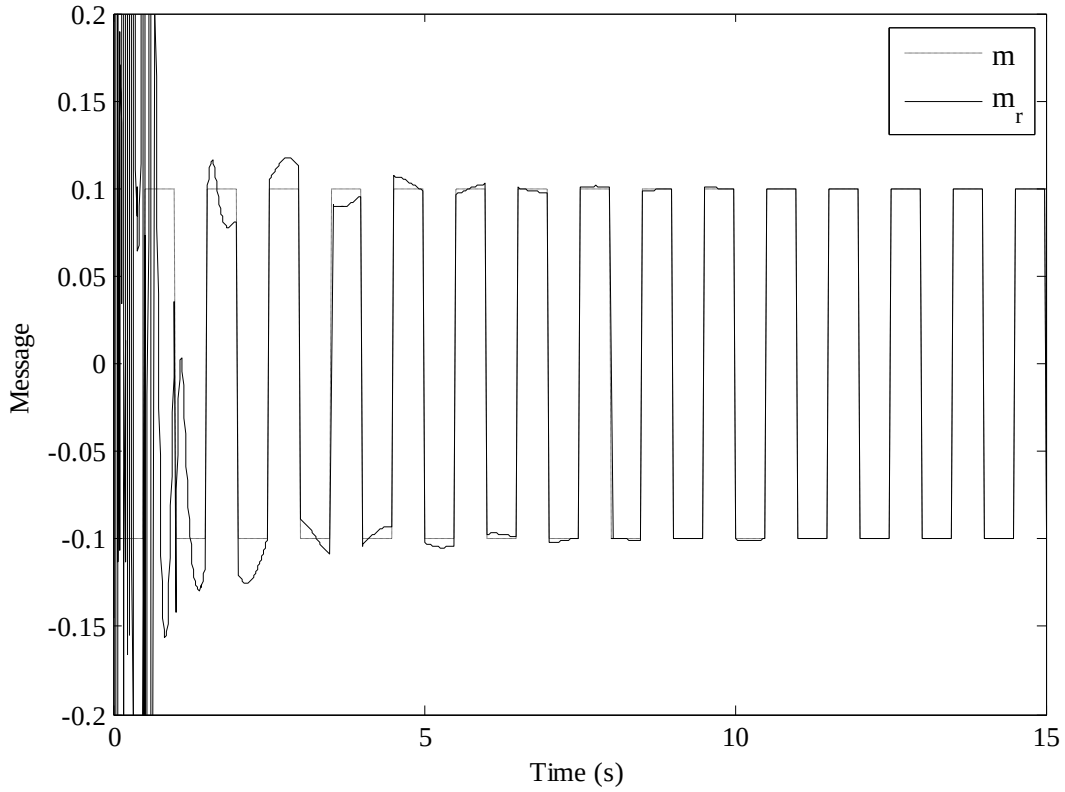


Figure 6.8: Plot of the extracted message $m_r(t)$ and m(t).

#### 6.2.1.3 Security analysis

The method proposed here is an improved technique from the one mentioned in [1] where the keystream is utilized from the chaotic oscillators that have been indirectly coupled. In [1], keystream from the same chaotic oscillator, from where the transmitted chaotic signal was generated, was used. The authors in that paper has successfully shown that attack methods such as [102] that uses NLD based forecasting is not useful for the chaotic system based on cryptography. Therefore, the method proposed here is also immune to the attack method proposed in [102]. The problem in [1] was that the keystream could successfully be estimated as mentioned in [119]. Since keystream was generated from the same oscillator as the transmitted signal, the dynamics of the keystream could be estimated, therefore possibility of revealing the transmitted message. In this method, however, the keystream is generated via indirect coupled synchronization in the transmitter and receiver

from separate chaotic oscillators which have different structure and dynamics from the transmitter. Therefore, the method in [119] will not be useful to estimate the keystream.

Next, we will see another popular attack based on RM on the proposed method. It turns out that it destroys the possibility of the phase space reconstruction of the sender dynamics by analyzing the transmitted chaotic signal using RM since it blurs the map and no distinct branching is seen. Figure 6.9 shows the RM of the transmitted signal generated from the proposed system that modulates the digital bits. It can be seen that the map is totally blurred with no apparent information in it regarding the transmitted bits. Even if the local maxima and minima, i.e. small fluctuations, are filtered out from the transmitted signal, and RM is plotted, as shown in Figure 6.10, there is no distinct branching of the RM to reveal the transmitted bits. Therefore, it can be concluded that the proposed method is immune to methods based on NLD and RM.

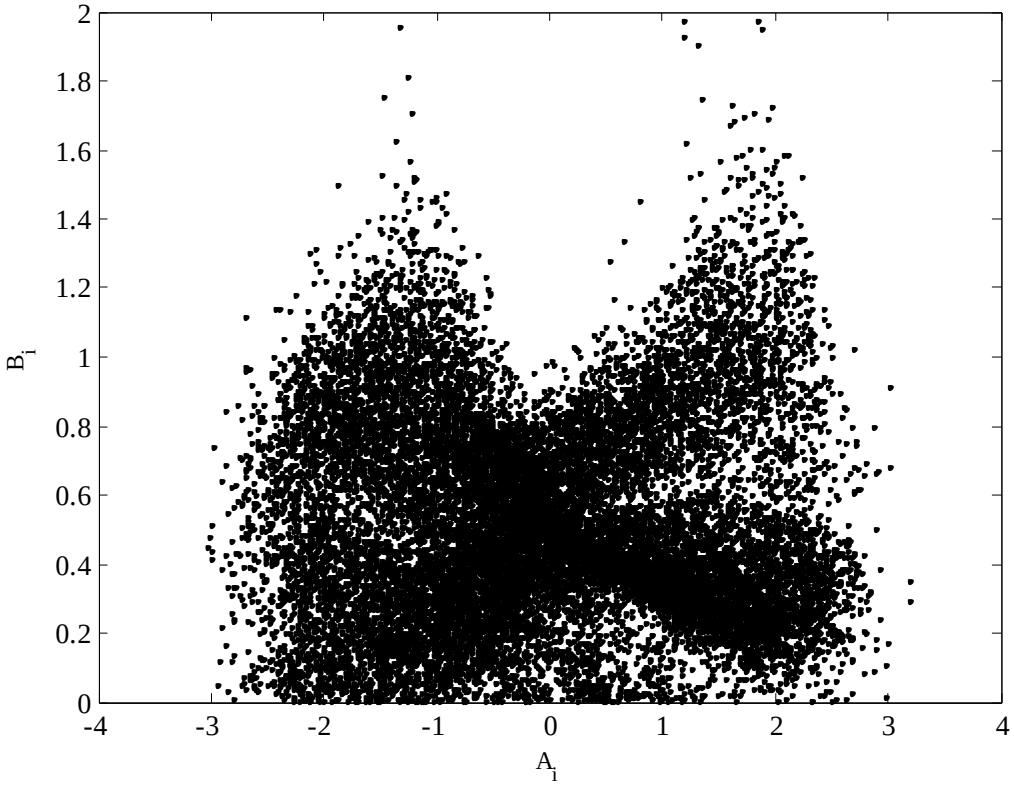


Figure 6.9: Return map of the transmitted signal $y_t(t)$.

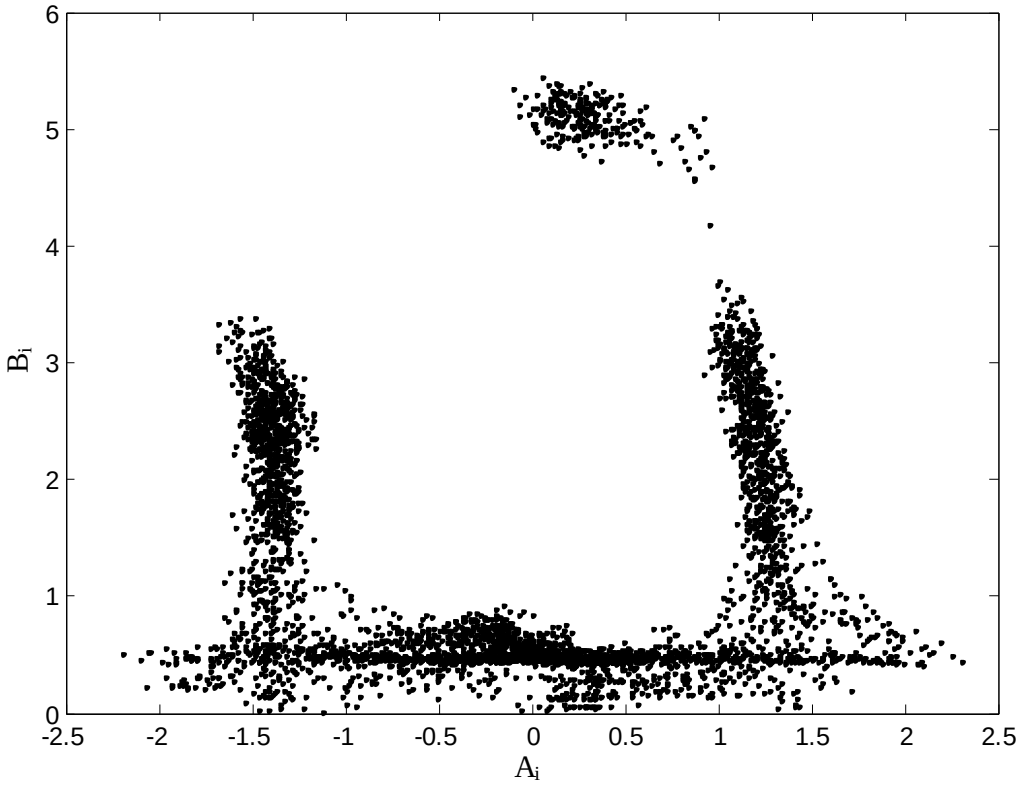


Figure 6.10: Return map (small fluctuations filtered out) of the transmitted signal $y_t(t)$.

### 6.2.2 Discrete Time Scenario

In the earlier section, the ICCS was implemented for proposing a secure chaotic communication method based on cryptography in the context of continuous time system. The same idea can be extended to be implemented in discrete-time context. Implementation of the proposed system in discrete domain is rather interesting because of its simplicity of the practical implementation. In effect, discrete-time system can easily be implemented in digital computers, field programmable gate array, microprocessors or digital signal processor chips, etc. In this way, the technical design/implementation complexities of analog design of continuous time system can be easily overcome while the properties of chaotic systems can still be utilized for secure communication purpose. In this section, the method proposed above in continuous-time system is further implemented

in discrete-time context. The model is same as shown in Figure 6.3 but in discrete context i.e. time, t will be replaced by samples, k.

Consider the following discrete-time dynamical systems:

$$(T): \begin{cases} x(k+1) = Fx(k) + f(y_t(k)) \\ y_1(k) = h_1(x(k)) \\ y_2(k) = h_2(x(k)) \\ y_t(k) = y_1(k) + e(m(k)), \end{cases} \tag{6.14}$$

where the state $x \in R^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator $y_1 \in R$ and $y_2 \in R$. The functions f, $h_1$ and $h_2$ are smooth and m(k) is the message signal. The signal $y_t \in R$ is the transmitted signal where e(.) is an encryption function that uses u(k) and key and the function f is a smooth bounded function.

The key signal u(k) is generated using another chaotic oscillator which is driven by the signal $y_2(k)$; that is:

$$(A): \begin{cases} z(k+1) = g(z(k), y_2(k)) \\ u(k) = h(z(k)), \end{cases} \tag{6.15}$$

where $z \in R^q$ (q is not necessarily equal to n), $u \in R$, and h is an analytical function vector of appropriate dimension.

The chaotic oscillator (R) to synchronize with (T) is given by:

$$(R): \begin{cases} \hat{x}(k+1) = F\hat{x}(k) + f(y_t(k)) \\ \hat{y}_1(k) = h_1(\hat{x}(k)) \\ \hat{y}_2(k) = h_2(\hat{x}(k)). \end{cases} \tag{6.16}$$

Finally, the chaotic oscillator (B) to synchronize with (A) is given as:

$$(B): \begin{cases} \hat{z}(k+1) = g(\hat{z}(k), \hat{y}_2(k)) \\ \hat{u}(k) = h(\hat{z}(k)). \end{cases} \tag{6.17}$$

Note the oscillator (A) and (B) being driven by signal $y_2(k)$ and $\hat{y}_2(k)$ respectively in order to form ICCS. The proof for ICCS for the discrete-time context has already been done in Chapter 5, section 5.2.2 and is valid for the systems (6.14), (6.15), (6.16) and (6.17) since they are of the same form as (5.38), (5.39), (5.40) and (5.41) used for the proof.

#### 6.2.2.1 Implementation using 3-D Henon map and discrete Lorenz system

In this section, the performance of the proposed synchronization and method as shown in Figure 6.3 is demonstrated using the 3D-Henon as the transmitter/receiver system and discrete Lorenz system as the key generating oscillator. The 3D-Henon map is defined for transmitter and receiver as [180]:

$$
\begin{aligned}
(T) &= \begin{cases} x_1(k+1) = -by_t(k) \\ x_2(k+1) = 1 + x_3(k) - ay_t^2(k) \\ x_3(k+1) = x_1(k) + by_t(k) \\ y_1(k) = x_2(k) \\ y_2(k) = x_3(k) \\ y_t(k) = y_1(k) + e(m, key), \end{cases} \\
(R) &= \begin{cases} \hat{x}_1(k+1) = -by_t(k) \\ \hat{x}_2(k+1) = 1 + \hat{x}_3(k) - ay_t^2(k) \\ \hat{x}_3(k+1) = \hat{x}_1(k) + by_t(k) \\ \hat{y}_1(k) = \hat{x}_2(k) \\ \hat{y}_2(k) = \hat{x}_3(k), \end{cases}
\end{aligned}
\tag{6.18}
$$

where a = 1.07 and b = 0.3. The key generating oscillators are represented in discrete Lorenz system as [41]:

$$
(A) = \begin{cases} z_1(k+1) = z_1(k)z_2(k) - y_2(k) \\ z_2(k+1) = z_1(k) \\ z_3(k+1) = z_2(k) \\ key = d_0 z_3(k), \end{cases}
$$

$$
(B) = \begin{cases} \hat{z}_1(k+1) = \hat{z}_1(k)\hat{z}_2(k) - \hat{y}_2(k) \\ \hat{z}_2(k+1) = \hat{z}_1(k) \\ \hat{z}_3(k+1) = \hat{z}_2(k) \\ \hat{key} = d_0 \hat{z}_3(k). \end{cases} \tag{6.19}
$$

Notice that the oscillator (A) and (B) are being driven by $y_2(k)$ and $\hat{y}_2(k)$ respectively to form ICCS. Same n-shift cipher algorithm used earlier for the encryption and decryption is used here as well.

#### 6.2.2.2 Simulation results

The encryption parameter h is taken to be 0.02 and the signal m(k) is modulated by the digital signal simply by making m(k) = 0.01 when bit 1 is present and m(k) = 0 when bit 0 is present. Therefore, the encryption function is basically changing the m(k) in different levels anywhere between -0.02 and 0.02 using the encryption keystream. The initial conditions for each oscillator are chosen to be arbitrarily different. The system is run for 200 samples.

Figure 6.11 shows the digitally modulated message signal to be transmitted securely and Figure 6.13 depicts the encrypted message signal after applying the keystream in Figure 6.12. The resulting transmitted signal is depicted in Figure 6.14. The keystream being generated at the receiver side is shown in Figure 6.15 while Figure 6.16 shows the synchronization error between the keystream generated in the transmitter and the receiver validating the ICCS in discrete-time context. The error converges rapidly to zero after some initial samples due to the time taken for synchronization and finally Figure 6.17

shows the extracted message and it can clearly be seen that after some samples, the modulated digital bits are recovered perfectly. The error due to the initial error in the bits due to synchronization can be removed by transferring few insignificant bits for first few samples.

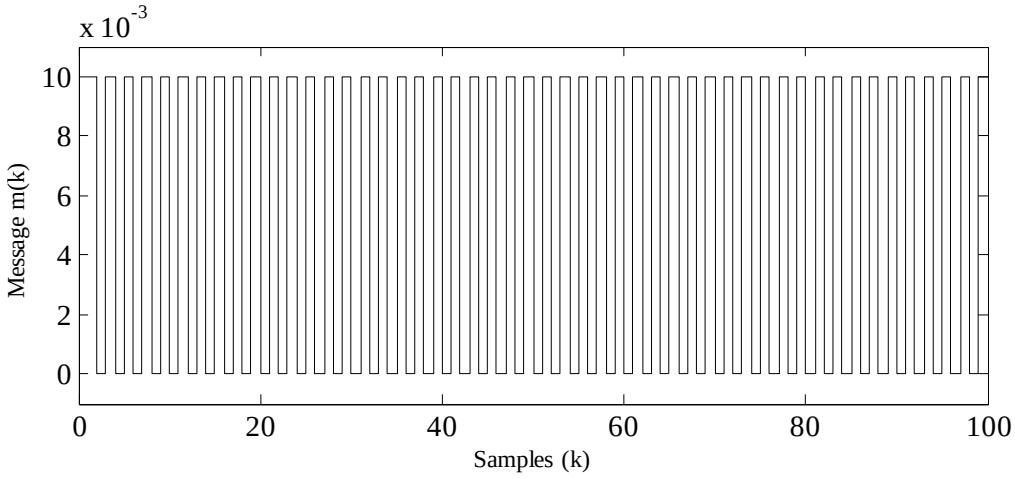


Figure 6.11: Message to be transmitted.

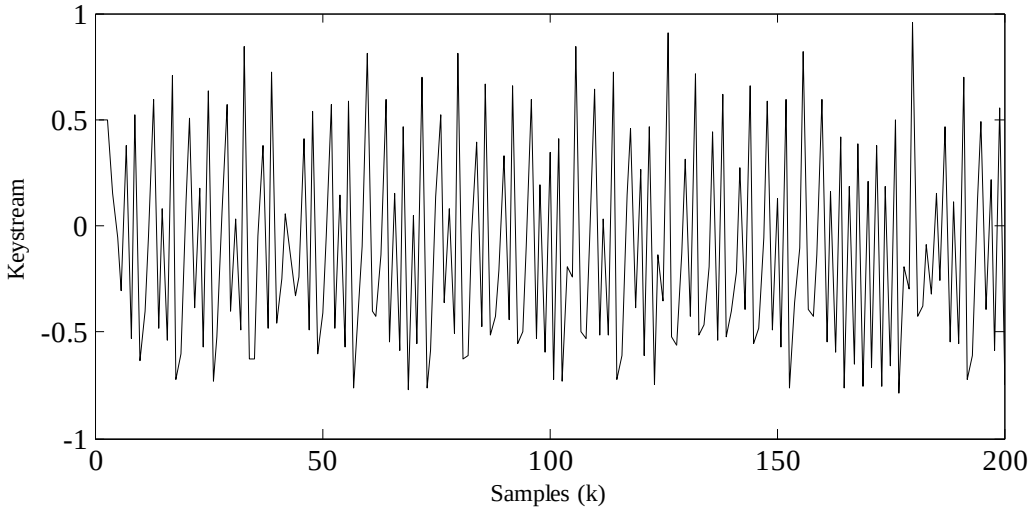


Figure 6.12: Keystream generated at the transmitter side.

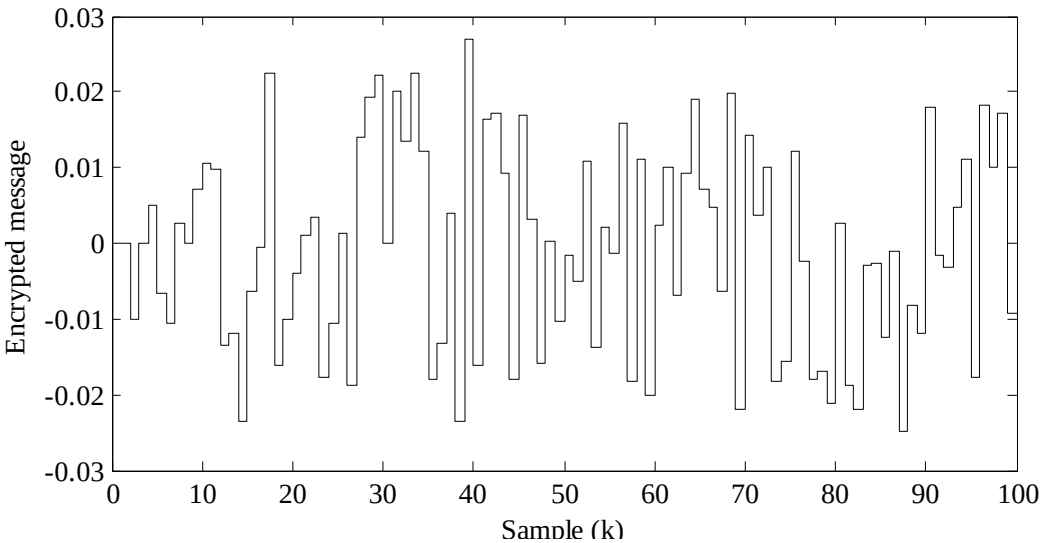


Figure 6.13: Encrypted message after applying the encryption algorithm and the keystream.

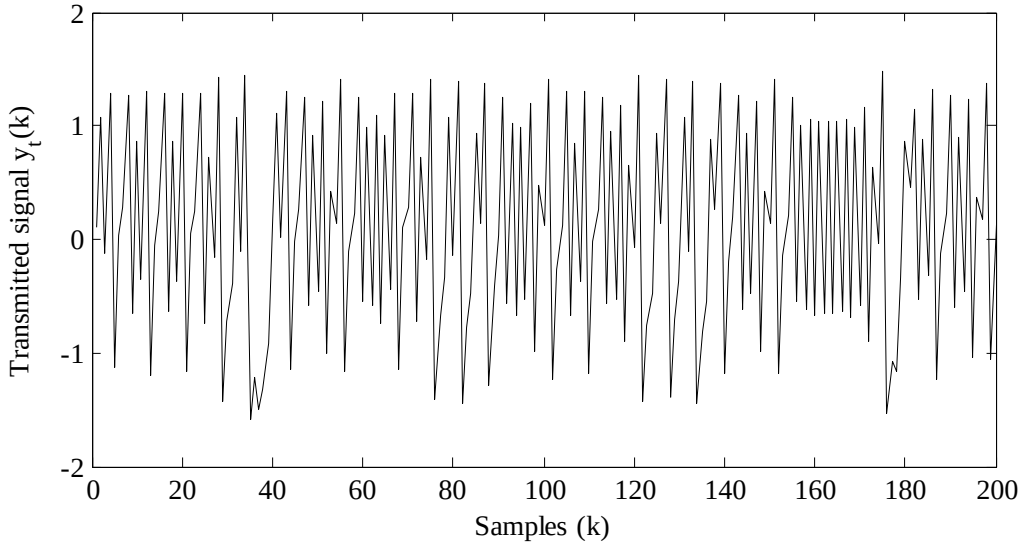


Figure 6.14: The transmitted chaotic signal $y_t(k)$.

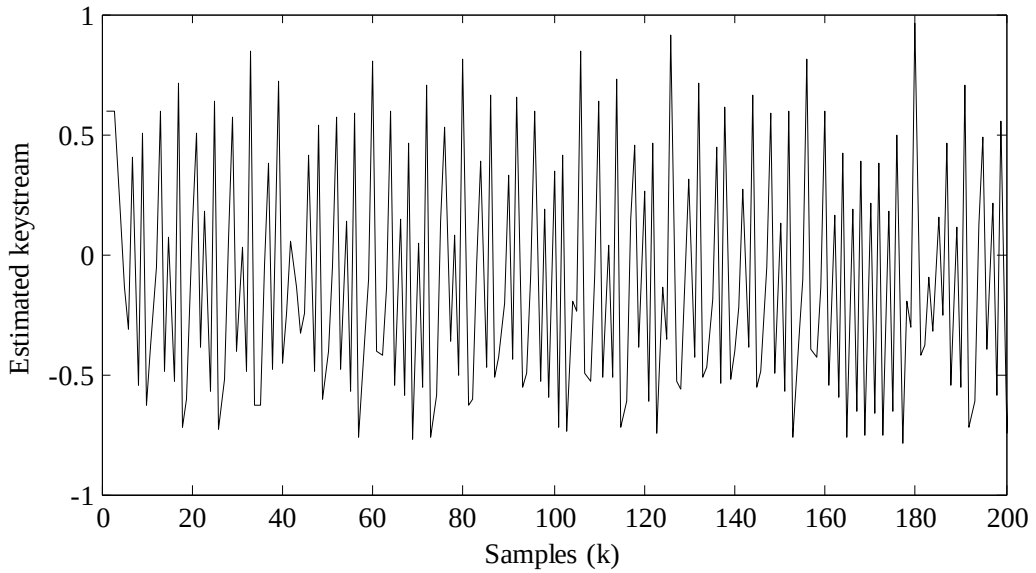


Figure 6.15: Estimated keystream at the receiver.

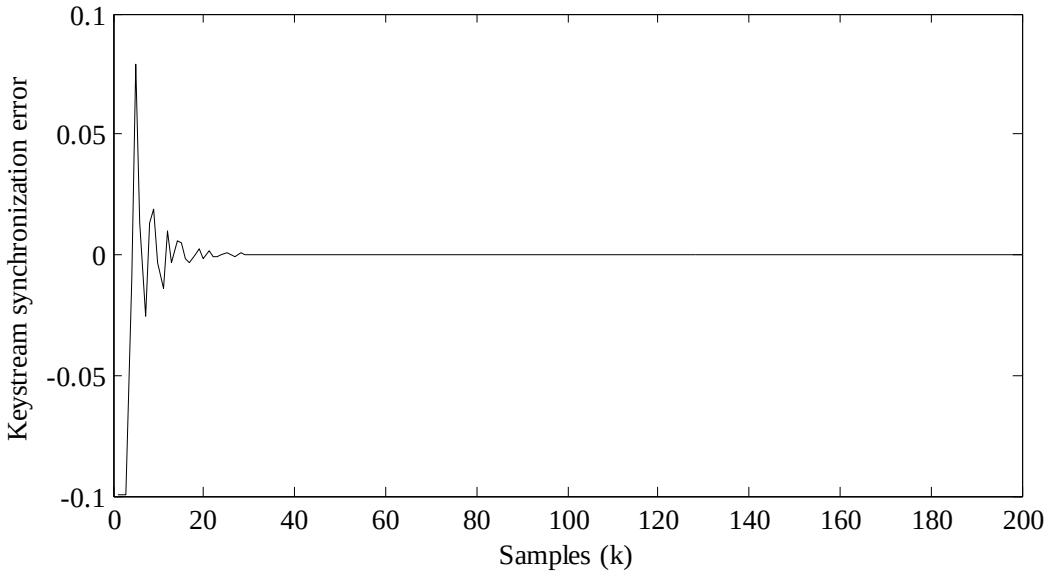


Figure 6.16: Synchronization error in estimating the keystream.

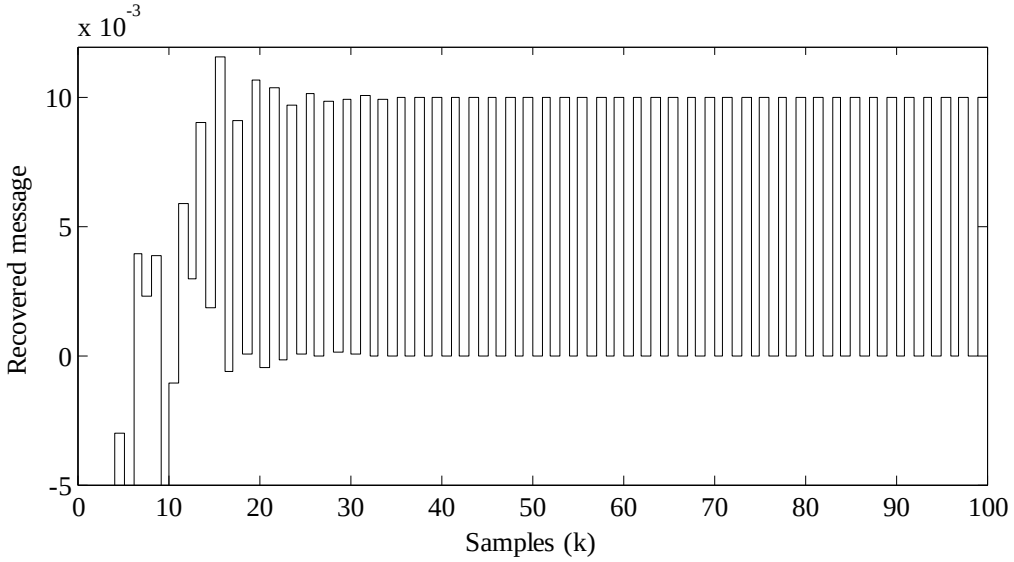


Figure 6.17: Extracted message signal.

#### 6.2.2.3 Security analysis

ICCS is used here as well for the generation of the keystream therefore keystream is not part of the transmitted signal just like in continuous-time case. Therefore, the arguments made earlier in the case of continuous-time system is also valid for discrete-time system. Without, the knowledge of the keystream and the key generating oscillator structures/parameters, the message extraction is impossible for the intruders. Since, the technique is used to transmit the digital bits it is worthwhile seeing if the bits 0 and 1 leave any pattern in the transmitted signal. This is very important for the security point of view because bit extraction can simply amount to the pattern classification problem for intruders if there is any pattern apparent in the transmitted signal which can easily be seen with the help of pattern classification algorithms. Therefore, first of all let us see if the encryption of the binary values is leaving any obvious pattern. Figure 6.18 shows the different levels of the encrypted message signal when binary value 0 or 1 is transmitted for the first 200 samples. It can be seen that the encrypted value is smeared in between the range of -2h and

2h. This means there is no change in the attractor of the transmitter chaotic system in a particular pattern when 0 or 1 is modulated.

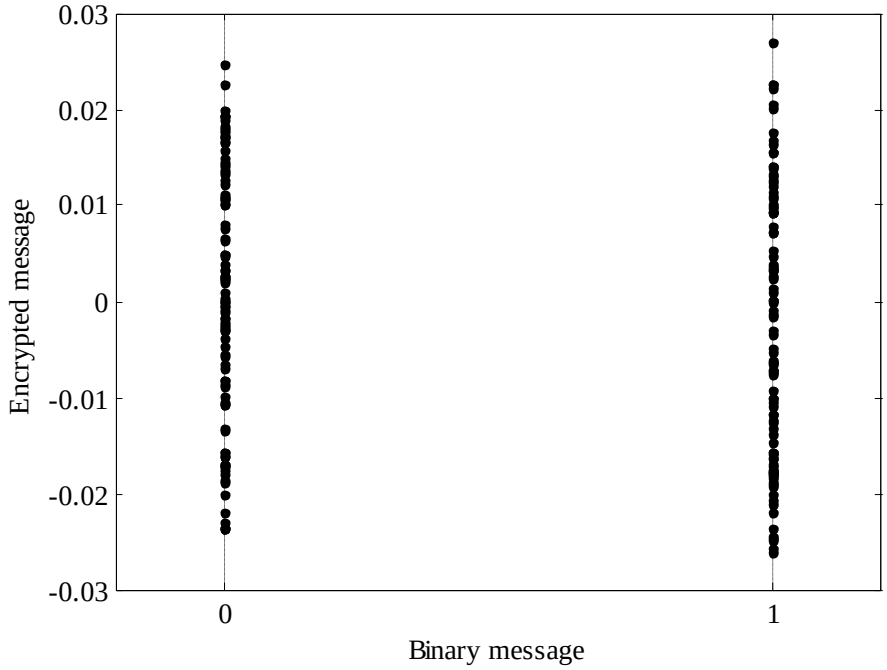


Figure 6.18: Encrypted message versus the binary message to be transmitted to show the digital bit is being modulated in multiple levels.

Now let us see if the RM of the transmitted signal provides any information regarding the transmitted bits. For the sake of comparison, let us also study the RM when CSK is implemented and when no message is transmitted for the 3D-Henon system. This will make the improvement evident of the proposed method. The return maps are plotted for 10,000 samples. If $A_m$ is the vector of maxima and $B_m$ is the vector of minima of the transmitted signal $y_t$, here plot of $A_m$ versus $B_m$ is giving us the return map of the signal $y_t$. Figure 6.19 shows the return map of the transmitted signal when no message is transmitted. When CSK is implemented, however, to transmit digital bits 0 and 1 with parameter b of Henon-3D switching between either 0.26 or 0.3, obvious branching in RM is observed as shown in Figure 6.20. Each of these branches corresponds to either 0 or 1 that is being

transmitted. But, when the proposed method based on cryptography implementing ICCS is used for transmitting digital bits, the information is not revealed in the return map of the transmitted signal as depicted in Figure 6.21. It can be seen that the return map does not necessarily change when binary message is transmitted by the proposed method. RM in Figure 6.21 is very similar to RM in Figure 6.19, however Figure 6.21 is bit dirty due to the presence of fake maxima and minima induced by small changes in the transmitted signal for the proposed method.

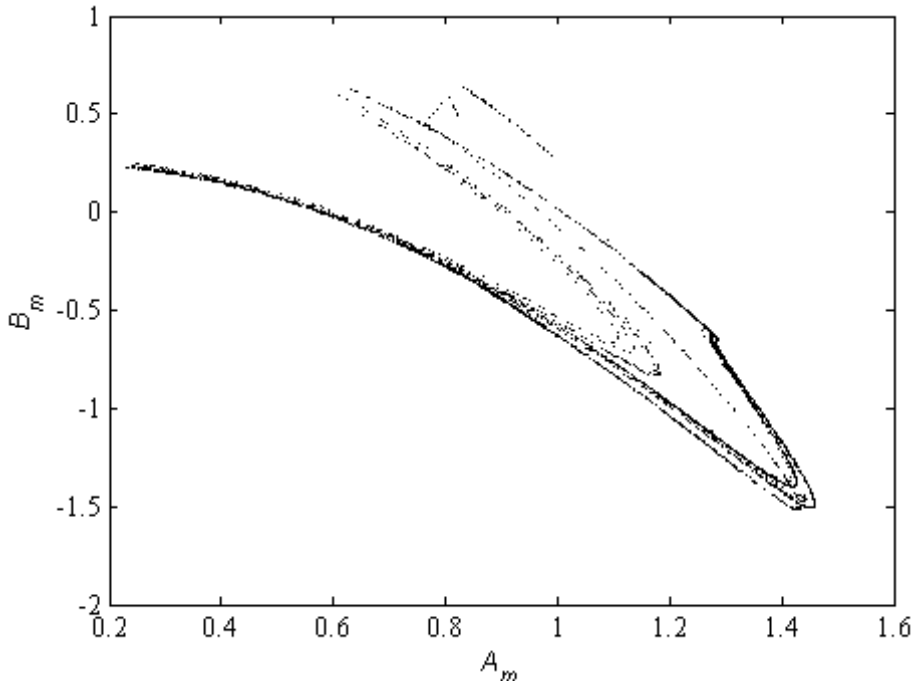


Figure 6.19: Return map of the transmitted signal when no message is transmitted.

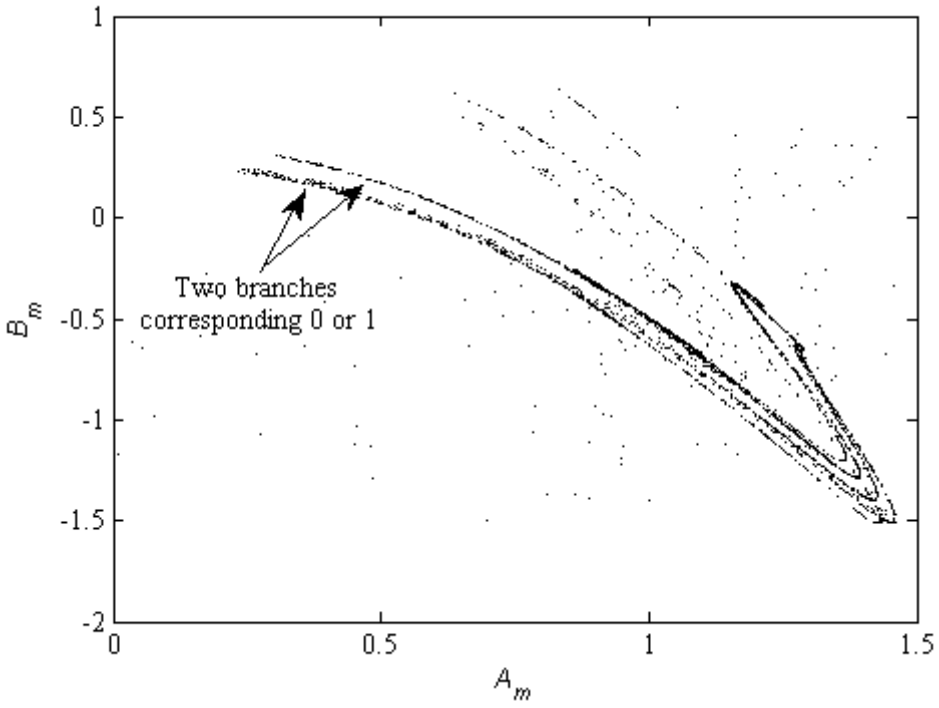


Figure 6.20: Return map of the transmitted signal when CSK is implemented to transmit 0 and 1.

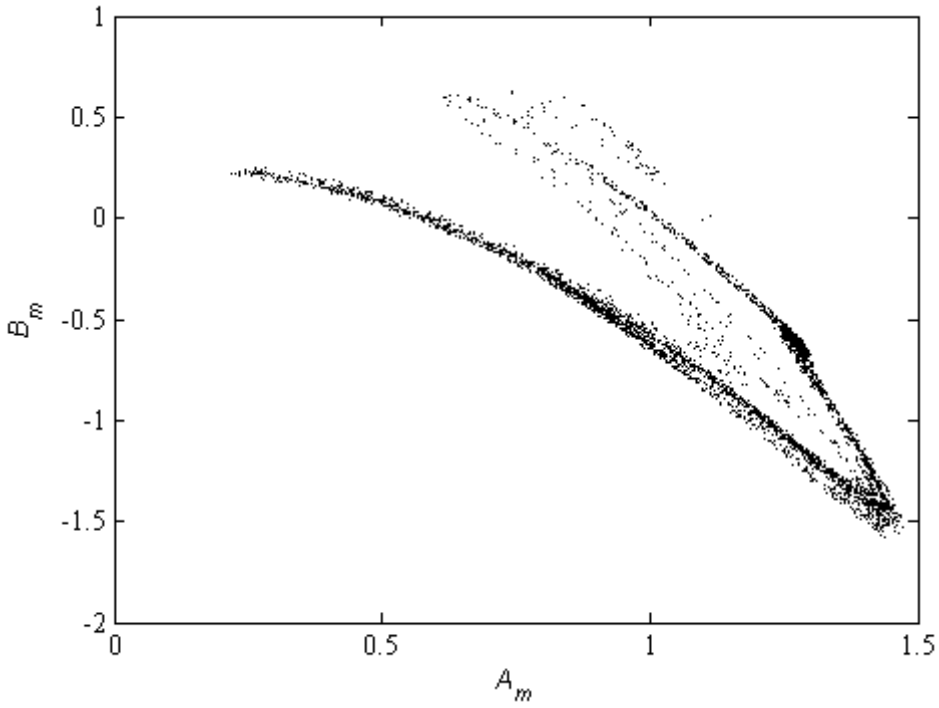


Figure 6.21: Return map of the transmitted signal when message is transmitted using the proposed method based on cryptography using ICCS.

## 6.3 Hardware Realization

In this section, the realization of the proposed discrete system in DSP board is presented. The DSP is preferred over analogue components because of the space, flexibility and ease of use. In effect, in analogue circuits, small change in the design parameters may result in the complete rewiring of the hard-wired analogue circuit, while the same change can be achieved by changing few lines of code in ROM or EPROM of the DSP. Also, chaotic systems are sensitive to slightest parametric mismatches and when implemented on analogue electronic components, the temperature fluctuations and parameter fluctuations can cause significant system error and therefore can be a major issue for the performance of the system. Furthermore, the practical implementation of the system on the analogue components can be hard to realize offering limited flexibility and ultimately being costly. Therefore, digital signal processing seems to be a suitable option that will provide flexibility in the design logic and with minimum effect of temperature and parameter discrepancies.

Matlab/Simulink embedded IDE link [187] in combination with Texas Instrument (TI) CCS is used for the rapid prototyping of the system. Here, the TMS320C6713 DSK DSP board is used for the experimental verification of the proposed method. TMS320C6713 is capable of the floating point operation with clock speed of 225 MHz [188]. Therefore, if the system can be implemented on this board, it could easily be realized successfully in modern DSP board for high speed operations. For the verification and validation of the results, output from the DSP board is imported back to the host computer and the performance is analysed. A comparison of the DSP output with the simulation output from Matlab is done. In what follows, the details of the method and implementation with few outputs are described.

### 6.3.1 Implementing ICCS for Secure Communication in DSP

Let us recall the block diagram of the proposed model in that is to be implemented which is shown in Figure 6.3. Here the discrete time scenario is adapted in the DSP. The proposed method was validated using Matlab/Simulink earlier which provided the deep insight on how the method works. For the practical implementation, the Simulink model of the proposed model is first converted into the C-language which will in turn be used to program the DSP board using the CCS.

The model is divided into two parts: the transmitter part and the receiver part. The Simulink model of the transmitter is shown in Figure 6.22. The input signal is encrypted first using the encryption block. The keystream used has been generated from the ICCS. It can be seen that the transmitter T generates the driving signal which is then in turn fed into the key generator block. The output from the transmitter block is the transmitted signal. The input signal is the message m(k) that has to be transmitted securely. Here, m(k) is a digital signal where m(k) = 1 when bit 1 is present and m(k) = 0 when bit 0 is present.

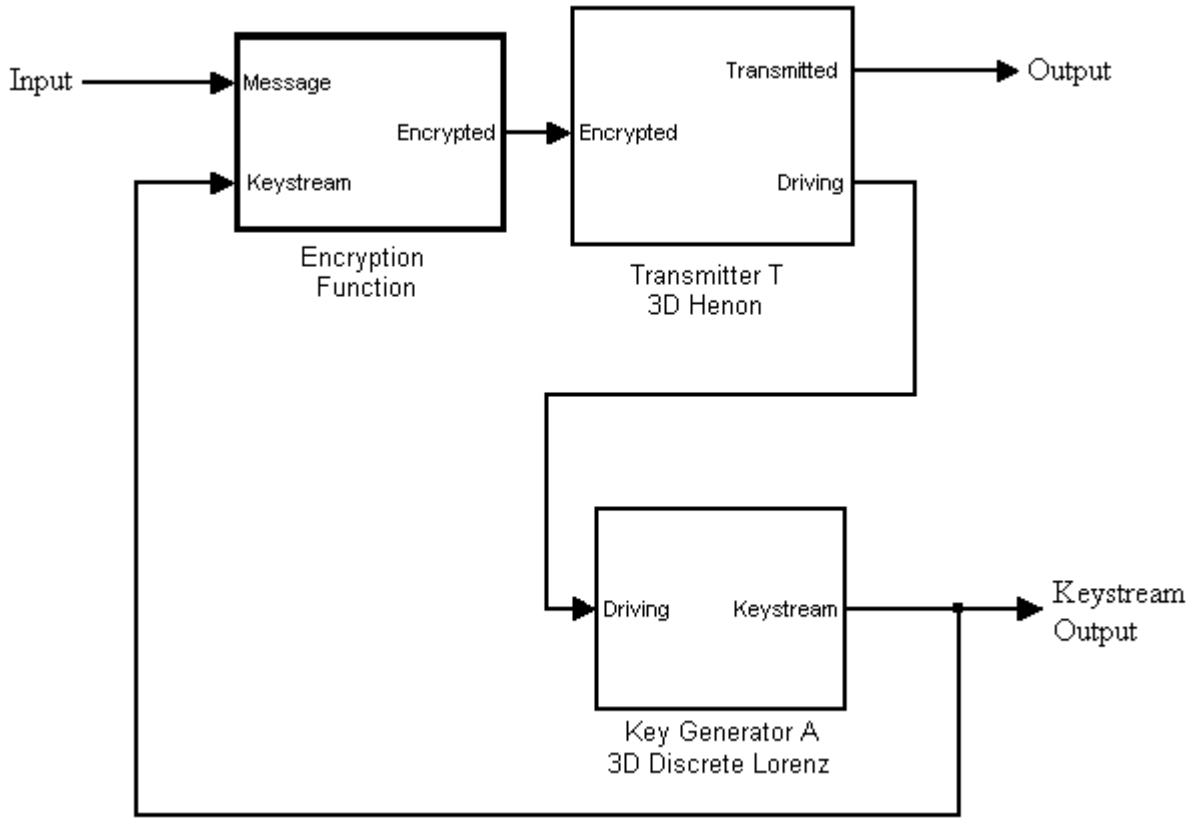


Figure 6.22: Simulink model of the Transmitter implementing ICCS for secure communications.

Figure 6.23 shows the Simulink block diagram of the receiver. For simplicity, the received signal is assumed to be free from any noises and interferences. In the receiver side the ICCS has been performed also. The decrypted signal is the extracted message. This method has been explained in detail in the earlier section.

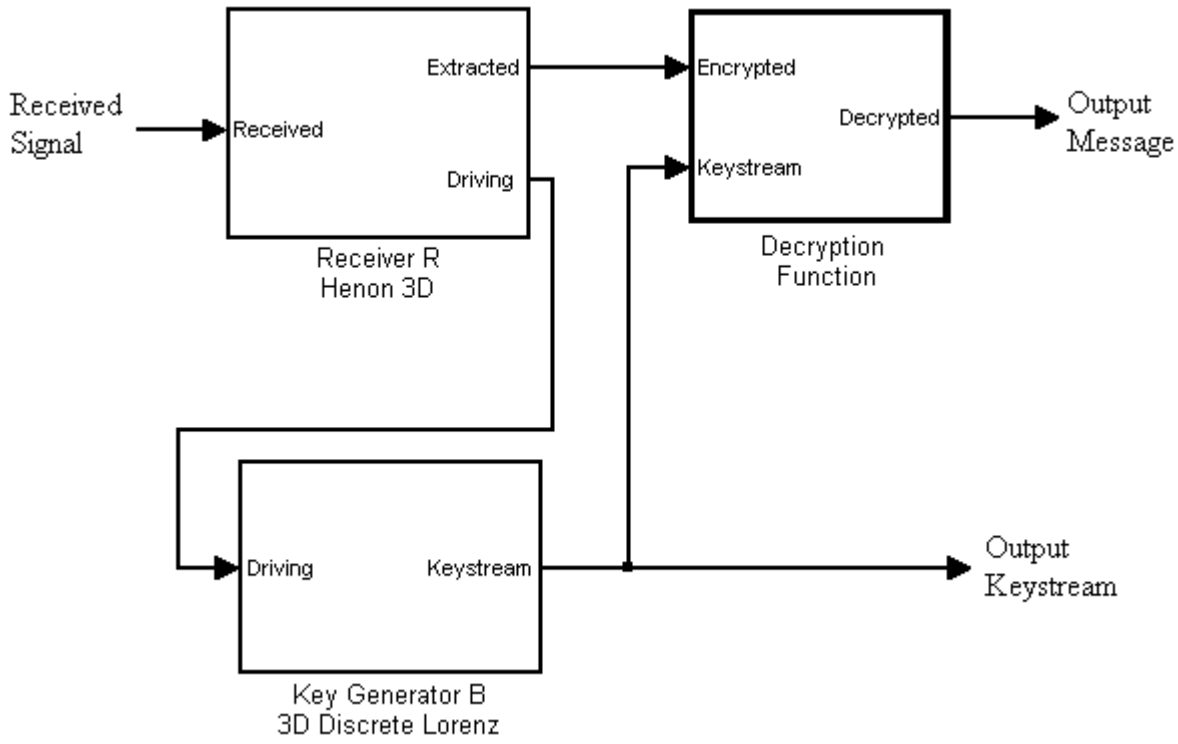


Figure 6.23: Simulink model of the Receiver implementing ICCS for secure communications.

The Simulink model is converted into assembly code for the TMS320C6713 using Simulink and the CCS. The real-time data exchange (RTDX) link is used to transfer data from the DSP to the computer and vice-versa. The message m(k) is fed into the DSP from the host computer using the RTDX and then transmitted using the scheme given in Figure 6.22. The message is extracted using the model given in Figure 6.23. The extracted message is again fed back to the host computer where the comparison of the transmitted message with the extracted message is done. The keystream generated at the transmitter and the receiver side are also fed into the host computer where they are compared as well. Finally, the transmitted signal and the extracted message when both the DSP and Matlab are employed are compared. The running of the model in the DSP board and the data exchange is shown in the Figure 6.24 and Figure 6.25 for the transmitter and the receiver respectively.

It should however be kept in mind that processing in the Matlab and the DSP are independent of each other. Just for the sake of comparison, both are shown in the same setup. The error $e_r$ between the transmitted signals generated by the Matlab and the DSP is calculated by subtraction and is depicted in Figure 6.26. It can be seen that the error signal is equal to zero for all samples, therefore making the implementation of DSP board and the Simulink model equivalent.

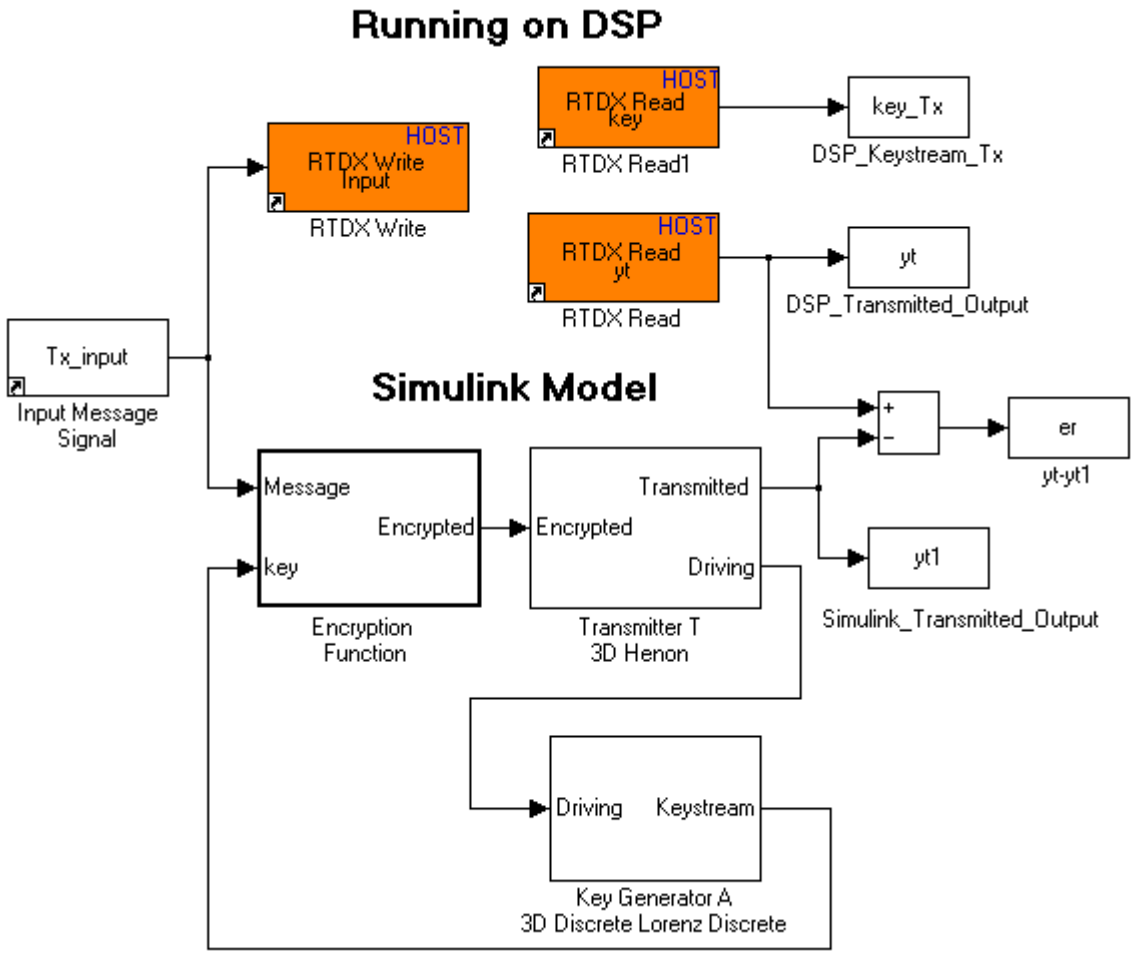


Figure 6.24: The simulink model of the DSP implementation of the transmitter implementing ICCS.

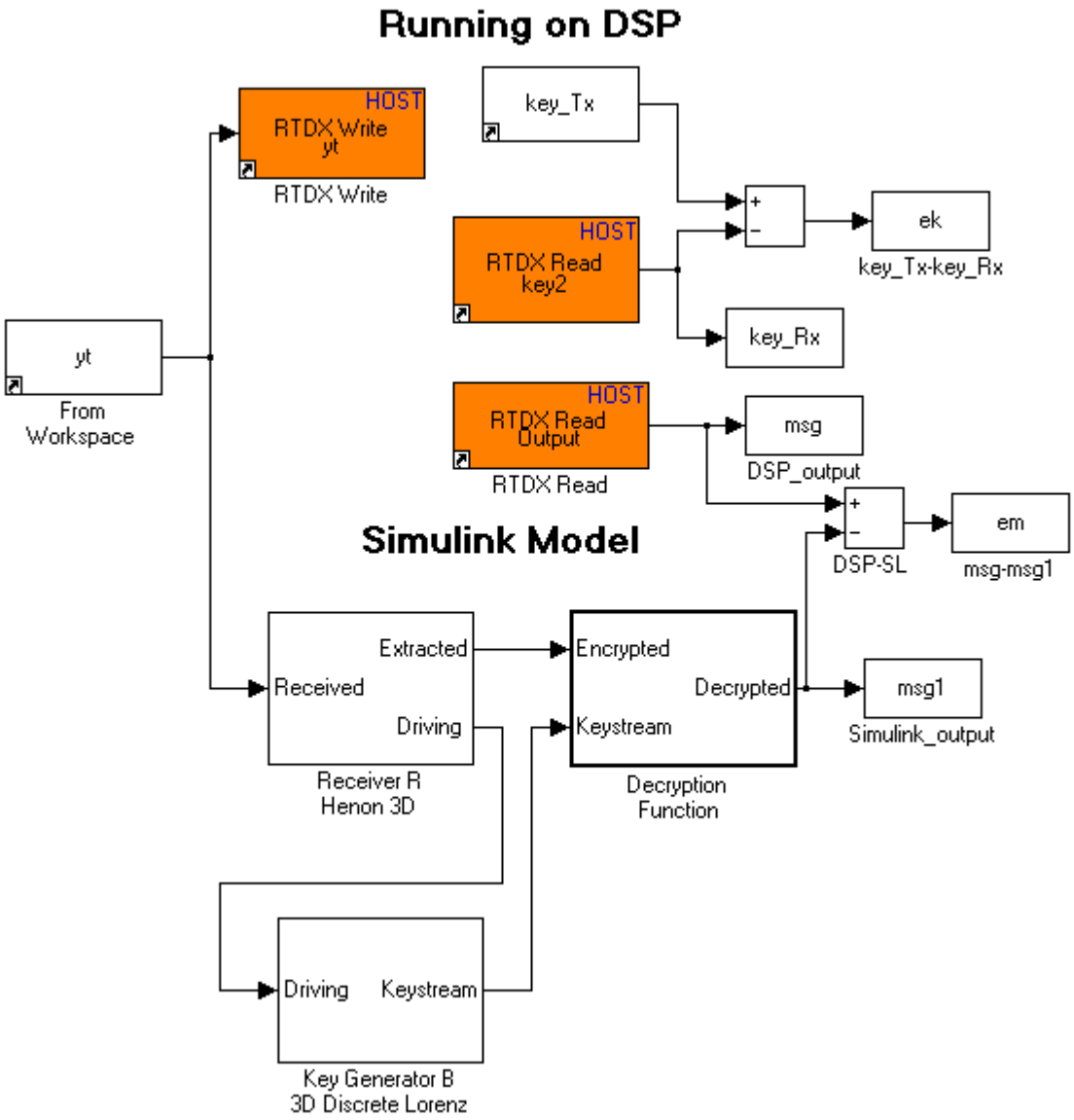


Figure 6.25: The simulink model of the DSP implementation of the receiver implementing ICCS.

Figure 6.27 shows the transmitted signal $y_t$ that has been generated using the DSP board. The signal $y_t$ is the input signal for the receiver. At the receiver, estimate of the keystream is obtained. The synchronization error signal $e_k$ of the keystream generated at the transmitter and the receiver using the DSP is shown in Figure 6.28. It can be seen that the error converges rapidly to zero after some initial samples, which is the time taken for synchronization. Next let us see the message extraction which is depicted in Figure 6.29, in

the receiver, after the keystream is obtained. It can be seen that the after some samples that is taken for synchronization, the message is extracted perfectly. Finally, let us see the comparison between the messages extracted when implemented on Simulink and on DSP board. Figure 6.30 demonstrates the error signal $e_m$ which is calculated by subtracting Matlab output with the DSP output. It can be seen that error is nearly equal to zero for all samples. Therefore, this provides sufficient evidence that ICCS based secure chaotic communication can successfully be implemented in the DSP that has floating point operations capabilities.

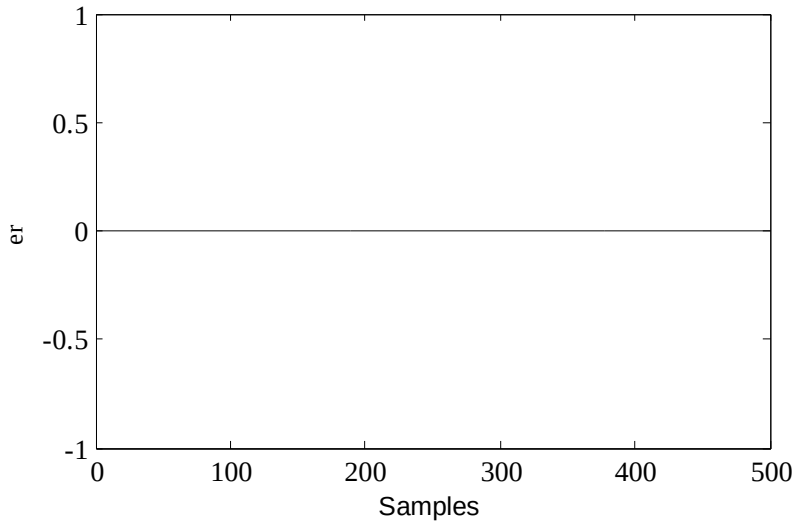


Figure 6.26: Error signal $e_r$ between the DSP and the Matlab generated transmitted signal.

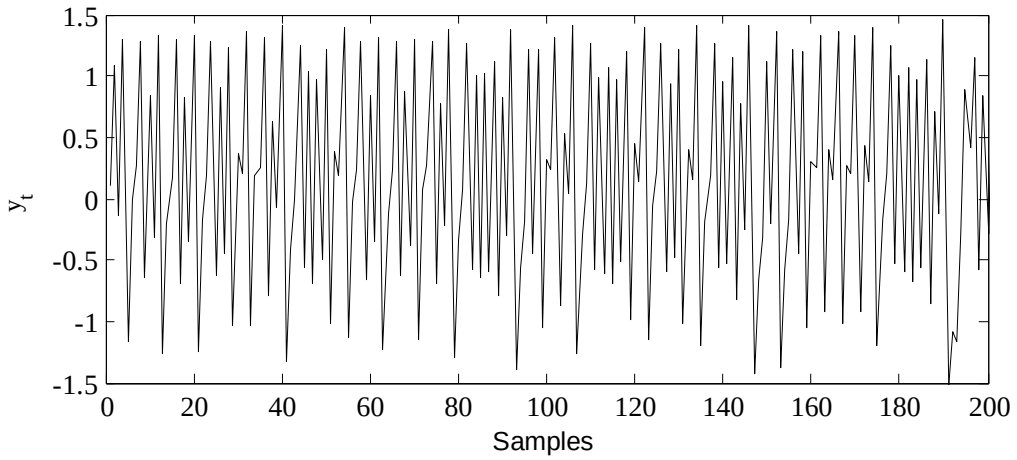


Figure 6.27: Transmitted signal $y_t$ generated from the DSP board.

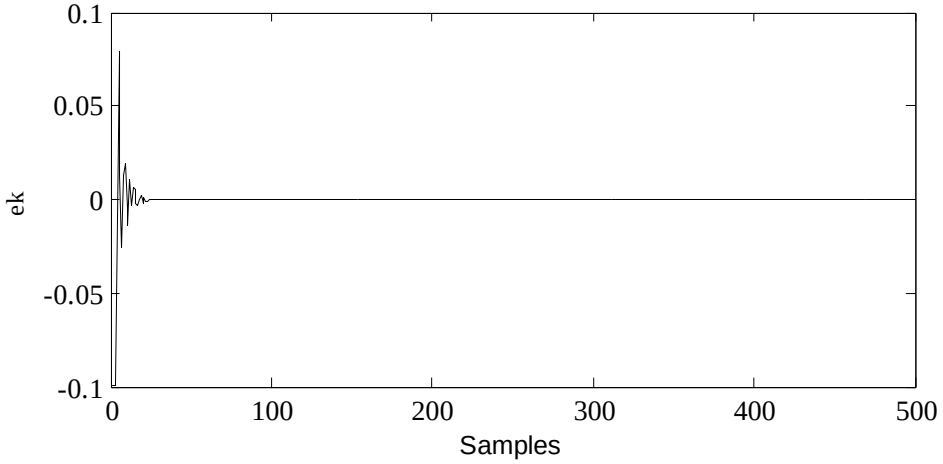


Figure 6.28: Key stream synchronization error generated at the transmitter and receiver side using DSP.

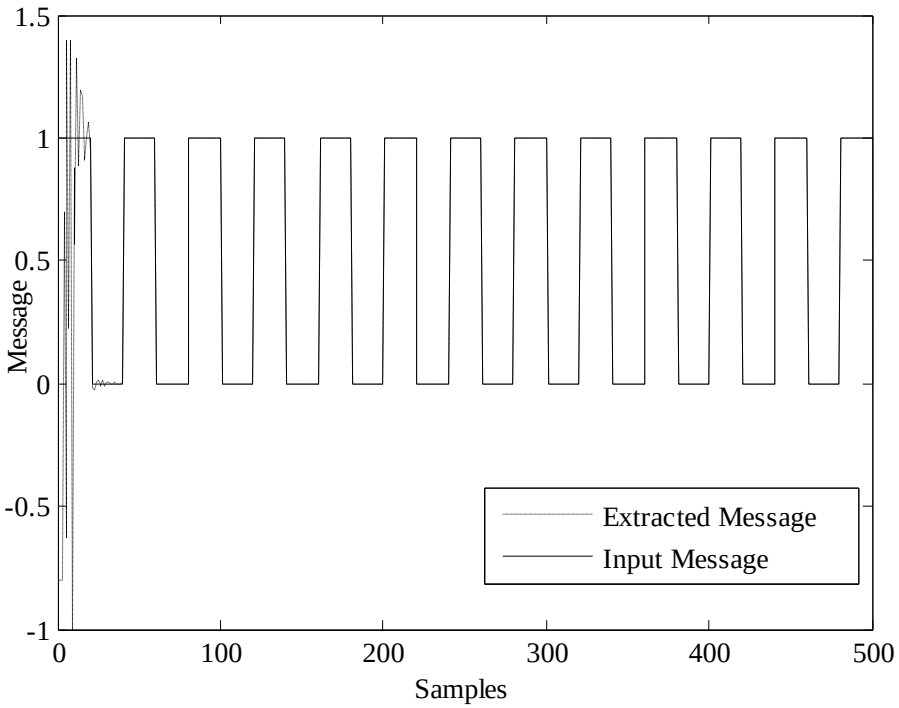


Figure 6.29: Successful extraction of the message signal using the DSP board.

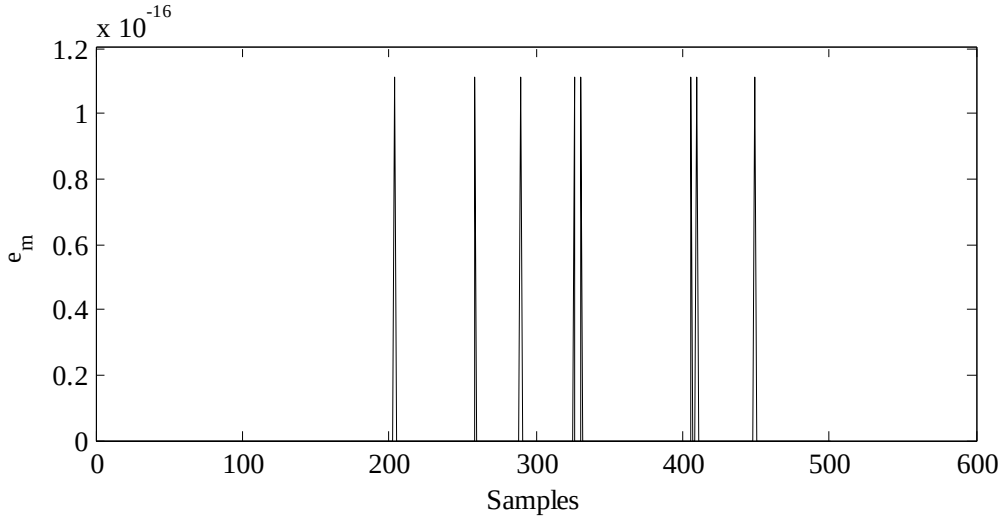


Figure 6.30: Error signal $e_m$ between the DSP and Matlab outputs against the number of samples.

## 6.4 Summary

In this chapter, the ICCS has been utilized to propose a new chaotic communication method based on cryptography that is implemented both on continuous time and discrete time context. This proposed method was different from previous methods available in the literature because it used keystream generated from two chaotic oscillators at transmitter and receiver side that are indirectly coupled with each other. ICCS allowed to generate same keystream at the transmitter and the receiver side. The transmitted signal was generated from a different chaotic oscillator from the keystream generating oscillator. The keystream is not part of the transmitted signal therefore the dynamics of the keystream and the keystream generating oscillator is always hidden from the intruders. Without the knowledge of the valid keystream, the intruders will not be able to extract the message signal ensuring secure transmission of message signal. In continuous time, the method was implemented using Lorenz and Chua's system while in discrete time, 3D-Henon map and discrete Lorenz map is used. Simulation results verified the validity of the proposed

method to successfully extract the transmitted message signal using the authentic receiver. Therefore, the use of ICCS successfully allowed us to implement secure communication system using chaotic systems. Next, the realization of the proposed ICCS based secure chaotic communication method is achieved in TMS320C6713 DSK DSP board. First of all, the Simulation model of the proposed technique was designed. The transmitter and the receiver model were implemented independently. The message to be transmitted was loaded into the DSP board from the host computer by using RTDX and then the transmitted signal was generated. Furthermore, the transmitted signal was imported into the host computer. Next, the receiver model was implemented where the transmitted signal was loaded and then the message extraction was performed. Comparison of the transmitted signal and message output was done when DSP and Matlab were used. The results showed that the results obtained when DSP was implemented were almost identical to what was achieved from Matlab implementation. This was due the fact that both Matlab and DSP operation operated at the same floating point precision. This indicates that the proposed chaotic communication method can successfully be implemented on the DSP board that has capability of doing floating point operations.

# Chapter 7 Modified Chaotic Shift Keying Method Using Indirect Coupled Chaotic Synchronization

## 7.1 Introductions

The problem with CSK method is that the value of the parameter had to be switched between two values when 0 and 1 is to be transmitted. Therefore there will be an imminent pattern in the transmitter output signal that has the information regarding the message signal. Hence, recovering bits for the intruders can simply amount to a classification problem which can easily be done by methods such as RM, ANN and therefore message signal could be extracted only by analysing the transmitted signal without knowing the dynamics and structure of the transmitter chaotic systems. Also GS can be used to break the CSK method. The method of CSK and its vulnerabilities to different attack methods were discussed in the Chapter 2 of this thesis. In this chapter we will use the concept of ICCS proposed earlier to modify the CSK method to improve the security of it such that the attack methods in questions become futile.

In the literatures, different researchers have proposed various countermeasures for resisting the attack based on RM. In [134], a periodic signal is combined with one state of the transmitter to modulate the transmitted signal so as to blur the reconstructed RM in order to frustrate the attacker. However, it was soon broken in the work described in [135, 166, 167] by distinguishing the phase and angular frequency of the periodic modulating signal and then removing it. A modified scheme of the original method of [134] was proposed in [135] to further improve its security. However, the work mentioned in [168], this modified

modulating scheme is still not secure enough and that the modulating signal can still be effectively removed via parameters estimation.

Few more works to modify the CSK method and increase the security are proposed in [136, 169] where the authors have claimed that the information regarding the bit will not be present on the RM of the transmitted signal. In [169], two new countermeasures were proposed and combined to enhance the security of CSK against RM attacks. The first countermeasure is to increase the number of strips in the RM by modulating the parameter $\beta_{\mathrm{m}}$ between 2n different values: $\beta_{0,1}, \beta_{0,2}, ..., \beta_{0,\mathrm{n}}$ corresponding to bit value 0 and $\beta_{1,1}, \beta_{1,2}, ..., \beta_{1,\mathrm{n}}$ corresponding to bit value 1. It was claimed that the chances to make wrong assignments become $(2^{2n} - 2)^3 - 1 \approx 2^{6n}$ and that the security against RM attacks is dramatically enhanced even when n is not too large [109, 169]. The second countermeasure is to alternatively use two states of the transmitter as output, i.e., as the driving signal to allow the receiver system to synchronize with the transmitter, which will further split the constructed return map into two parts corresponding with each states [169]. However, the cryptanalysis work done later in [109] showed that the security estimated for the first countermeasure was over-estimated and the combination of two countermeasures can easily be separated. This proved that the work proposed in [169] is still vulnerable against the known attack methods.

In [136], another variation to the CSK method is proposed where the parameter $\beta_{\mathrm{m}}$ was not only switched between two values according to the bit values, but some more additional random switches are introduced to confuse a possible intruder. However, in [144], it is shown that when the RM of the transmitted signal, using this method, is zoomed, there still existed close but distinct branching.

In this work, an effort is made to modify the existing CSK method to strengthen the security by removing any pattern that will be imminent in the transmitted chaotic signal due to switching of binary values in CSK method.

## 7.2 Proposed Modified CSK Method for Secure Communication

In this section the ICCS proven in the previous Chapter 5 section 5.2.1.1 is employed for proposing a new improved CSK scheme for secure digital communication. Using the ICCS, same keystream is generated at the transmitter and the receiver side. This keystream in turn will be used to encrypt the binary message to be transmitted. Two methods are proposed by which CSK can be modified to improve the security.

### 7.2.1 Modified CSK Method 1

Consider the following system as to be used as a transmitter:

$$(\mathrm{T}):\begin{cases} \dot{\mathrm{x}} = \mathrm{f}(\mathrm{x}, \mathrm{y}_1, \beta_{\mathrm{m}}) \\ \mathrm{y}_1 = \mathrm{g}_1(\mathrm{x}) \\ \mathrm{y}_2 = \mathrm{g}_2(\mathrm{x}), \end{cases} \tag{7.1}$$

$\beta_m$ is the parameter value given as:

$$\beta_{\mathrm{m}} = \begin{cases} \beta_0 = \beta + \mathrm{e}(0, \mathrm{k}) \text{ if } \mathrm{m} = 0 \\ \beta_1 = \beta + \mathrm{e}(\rho, \mathrm{k}) \text{ if } \mathrm{m} = 1. \end{cases} \tag{7.2}$$

where e(.) is an encryption algorithm, $\rho$ is a scalar constant and k is the keystream for performing encryption. The output of $\mathrm{e}(\mathrm{z}, \mathrm{k})$ is such that it falls within interval [-h, h] where h is an encryption parameter. Therefore, we will always have $-\mathrm{h} + \beta \le \beta_{\mathrm{m}} \le \mathrm{h} + \beta$. With the proper choice of h, it can be ensured that $\beta_{\mathrm{m}}$ always falls within the range such

that system (7.1) is chaotic. $y_1$ is the transmitted signal for synchronization to the receiver (R).

$$(R): \begin{cases} \dot{\hat{x}} = f(\hat{x}, y_1, \hat{\beta}_m) \\ \hat{y}_2 = g_2(\hat{x}), \end{cases} \tag{7.3}$$

where

$$\hat{\beta}_m = \beta_0 = \beta + e(0, \hat{k}). \tag{7.4}$$

Here also $-h + \beta \le \hat{\beta}_m \le h + \beta$. Now according to Remark 1 in section 5.2.1.1, we have a slightly perturbed systems when 1 is transmitted therefore if synchronization is achieved, it can be concluded that 0 is transmitted otherwise 1 is transmitted. The keystreams $k$ and $\hat{k}$ are generated using ICCS and the systems for generating them are defined as:

$$\begin{aligned} (A): &\begin{cases} \dot{u} = p(u, y_2) \\ k = q(u) \end{cases} \\ (B): &\begin{cases} \dot{\hat{u}} = p(\hat{u}, \hat{y}_2) \\ \hat{k} = q(\hat{u}). \end{cases} \end{aligned} \tag{7.5}$$

The systems defined by Eqs. (7.4) and (7.5) are driven by $y_2$ and $\hat{y}_2$ respectively to perform ICCS. It should be noted that $y_2$ and $\hat{y}_2$ are not always equal since the parameter $\beta_m$ in the transmitter and $\hat{\beta}_m$ in the receiver are varying differently depending on the transmitted bits. In the transmitter, it is changing according to both binary values; but in the receiver, it is changing only due to the binary value 0 therefore will be useful for message recovery since we will have a slightly perturbed system as was pointed in the remark 1 of the proof in chapter 5.

The main disadvantage of the CSK method was that it performed switching based on one parameter, into two values. Therefore, when 0 was to be transmitted one parameter was used and when 1 was to be transmitted, another value was used. Therefore, the change in parameter could easily be detected by pattern recognition algorithms and by GS. In this proposed method, the switching is not happening between two values. In fact the parameter is such that $-\mathrm{h}+\beta \le \beta_{\mathrm{m}} \le \mathrm{h}+\beta$, i.e. it is switching between a range with infinite possibility. Therefore, it will not leave any pattern in the output transmitted signal.

The proposed method is shown in the Figure 7.1.

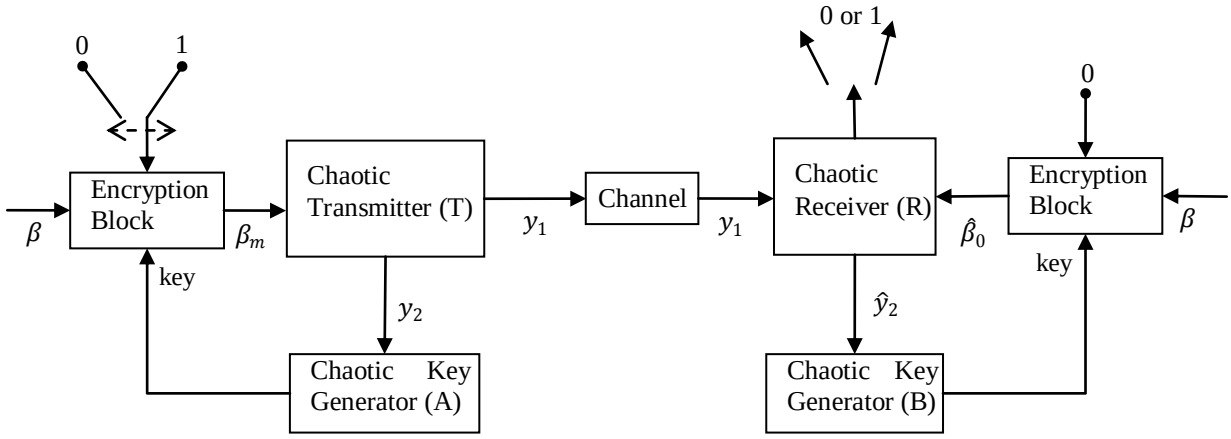


Figure 7.1: Block diagram for the proposed modified CSK method 1.

**Note:** The form of the systems taken in (7.1), (7.3) and (7.5) that are used to define the proposed method implementing ICCS are of the same form as taken for proving ICCS in (5.3) and (5.4) in Chapter 5. This means that the ICCS could be employed in the proposed method.

### 7.2.2 Modified CSK Method 2

The CSK method proposed in method 1 can be varied by not changing the parameter of the system but by directly including the encrypted message in one of the state such that the attractor is changed directly at the phase space. This method can be written mathematically as follows:

$$(\mathrm{T}):\begin{cases} \dot{\mathrm{x}} = \mathrm{f}(\mathrm{x}, \mathrm{y}_1, \beta) + \mathrm{Be}(\eta_{\mathrm{m}}, \mathrm{k}) \\ \mathrm{y}_1 = \mathrm{g}_1(\mathrm{x}) \\ \mathrm{y}_2 = \mathrm{g}_2(\mathrm{x}), \end{cases} \tag{7.6}$$

$$(\mathrm{R}):\begin{cases} \dot{\hat{\mathrm{x}}} = \mathrm{f}(\hat{\mathrm{x}}, \mathrm{y}_1, \beta) + \mathrm{Be}(0, \hat{\mathrm{k}}) \\ \hat{\mathrm{y}}_2 = \mathrm{g}_2(\hat{\mathrm{x}}). \end{cases}$$

Here $\eta_{\mathrm{m}}$ is 0 or $\rho$ depending on either message is 0 or 1 and B is a matrix of appropriate dimension. The keystream $\mathrm{k}$ and $\hat{\mathrm{k}}$ are generated using ICCS as shown in method 1. This method is depicted in Figure 7.2.

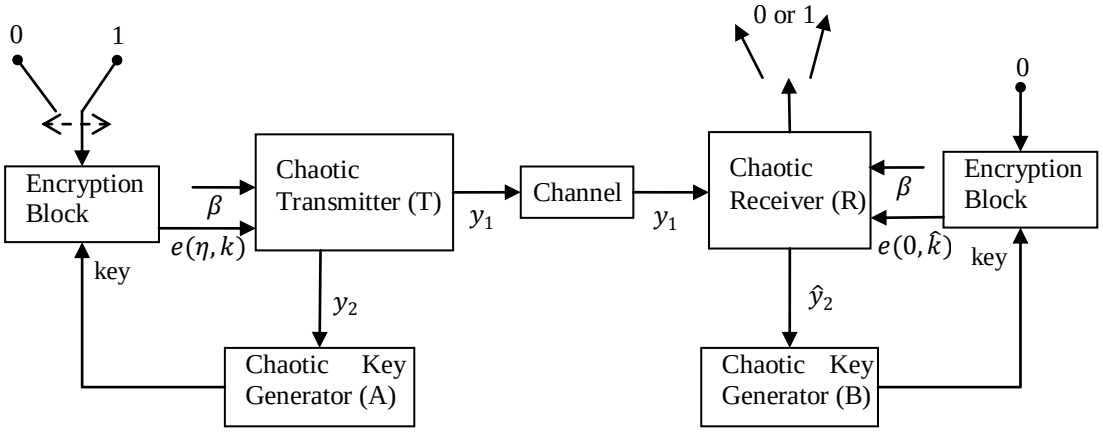


Figure 7.2: Block diagram for the proposed modified CSK method 2.

## 7.3 Implementation using Lorenz and Chua's system

Now the proposed both methods will be implemented using the Lorenz and Chua's system. Lorenz system will be implemented as the transmitter (T) and receiver (R) while the Chua's system is implemented as the key generators (A) and (B). The encryption function e(.) to be used in the proposed design is chosen to be n-shift cipher algorithm as used earlier. To recall,

$$e(z,k) = \underbrace{f_1(...f_1(}_{n} f_1(z,\underbrace{k),k),...k)}_{n} \tag{7.7}$$

where $f_1(z,k)$ is given as:

$$f_1(z,k) = \begin{cases} (z+k)+2h, & -2h \le (z+k) \le -h \\ (z+k), & -h < (z+k) < h \\ (z+k)-2h, & h \le (z+k) \le 2h. \end{cases} \tag{7.8}$$

and h is the encryption parameter.

### 7.3.1 Implementation Method 1

The Lorenz system acting as transmitter is given as:

$$(T): \begin{cases} \dot{x}_1 = -\sigma_1 x_1 + \sigma_1 x_2 \\ \dot{x}_2 = -20 y_1 x_3 + r y_1 - x_2 \\ \dot{x}_3 = 5 y_1 x_2 - \beta_m x_3 \\ y_1 = x_1 \\ y_2 = x_2, \end{cases} \tag{7.9}$$

where parameter $\beta_m$ modulates the binary message signal in the same manner as given in (7.2).

The keystream k is generated using the Chua's system and is driven by signal $y_2$ generated in (7.9).

$$(A):\begin{cases}\dot{u}_1 = \alpha(u_2 - u_1 - \varphi(y_2)) \\ \dot{u}_2 = y_2 - u_2 - u_3 \\ \dot{u}_3 = -\delta u_2 - \gamma u_3 \\ k = d_0 u_1, \end{cases} \tag{7.10}$$

where $d_0$ is a scaling factor such that k(t) lie within the interval [-h, h]. Note that here the signal $y_2$ is injected in the nonlinearity $\varphi(y_2)$ of the Chua's system which is given as:

$$\varphi(y_2) = G_a y_2 + 0.5(G_a - G_b)(|y_2 + 1| - |y_2 - 1|) \tag{7.11}$$

The receiver is given as:

$$(R):\begin{cases}\dot{\hat{x}}_1 = -\sigma_1 \hat{x}_1 + \sigma_1 \hat{x}_2 \\ \dot{\hat{x}}_2 = -20 y_1 \hat{x}_3 + r y_1 - \hat{x}_2 \\ \dot{\hat{x}}_3 = 5 y_1 \hat{x}_2 - \beta_0 \hat{x}_3 \\ \hat{y}_2 = \hat{x}_2. \end{cases} \tag{7.12}$$

The parameter $\beta_0$ is given in (7.4) and $\hat{k}$ is generated using Chua's system synchronizing with (7.10) and is given as:

$$(B):\begin{cases}\dot{\hat{u}}_1 = \alpha(\hat{u}_2 - \hat{u}_1 - \varphi(\hat{y}_2)) \\ \dot{\hat{u}}_2 = \hat{y}_2 - \hat{u}_2 - \hat{u}_3 \\ \dot{\hat{u}}_3 = -\delta \hat{u}_2 - \gamma \hat{u}_3 \\ \hat{k} = d_0 \hat{u}_1. \end{cases} \tag{7.13}$$

Eq. (7.13) is driven by $\hat{y}_2$ such that (A) and (B) synchronize with each other forming an indirect coupling. The non linearity here will then be

$$\varphi(\hat{y}_2) = G_a \hat{y}_2 + 0.5(G_a - G_b)(|\hat{y}_2 + 1| - |\hat{y}_2 - 1|) \tag{7.14}$$

In order to show that the systems (7.9), (7.10), (7.12) and (7.13) synchronize respectively as described in Section 5.2.1.1 of Chapter 5, the assumptions A1), A2), A3) and A4) made should be shown to be valid for the systems (7.9), (7.10), (7.12) and (7.13).

A1): For the transmitter and receiver defined by Lorenz system in (7.9) and (7.12), the matrix A can be written as:

$$A = \begin{pmatrix} -\sigma_1 & \sigma_1 & 0 \\ 0 & -1 & -20y_1 \\ 0 & 5y_1 & -\beta \end{pmatrix}$$

It can be shown that for the following choice of SPD matrices $P_1$ and $Q_1$

$$P_1 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \text{and } Q_1 = \begin{pmatrix} 2\sigma l_1 & -\sigma l_1 & 0 \\ -\sigma l_1 & 2l_2 & 0 \\ 0 & 0 & 2\beta l_3 \end{pmatrix},$$

with $l_1, l_2, l_3, \sigma, \beta, r > 0, l_2 = -\frac{1}{4} l_3$ and $0 < l_1 < \frac{4}{\sigma} l_2$, equation (7.15) holds true.

$$A^T P_1 + P_1 A = -Q_1 \leq -\lambda_{\min}(Q_1) I_1. \tag{7.15}$$

Here $\lambda_{\min}(Q_1) > 0$ is the smallest eigenvalue of the matrix $Q_1$ and $I_1$ is an identity matrix. Therefore assumption A1) holds true.

A2) For the keystream generating oscillator defined by Chua system defined in (7.10) and (7.13), the matrix F can be written as:

$$F = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & -1 \\ 0 & -\delta & -\gamma \end{pmatrix}$$

It can be shown that for the following choice of SPD matrices $P_2$ and $Q_2$

$$P_2 = \begin{pmatrix} l_4 & 0 & 0 \\ 0 & l_5 & 0 \\ 0 & 0 & l_6 \end{pmatrix} \text{and } Q_2 = \begin{pmatrix} 2\alpha l_3 & -\alpha l_3 & 0 \\ -\alpha l_3 & l_5 & 0 \\ 0 & 0 & 2\gamma l_6 \end{pmatrix},$$

with $l_4, l_5, l_6, \alpha > 0, \delta < 0, \gamma \geq 0, l_5 = -\delta l_6$ and $0 < l_4 < \frac{4}{\alpha} l_5$ , equation (7.16) holds true.

$$F^T P_2 + P_2 F = -Q_2 \le -\lambda_{\min}(Q_2) I_2. \tag{7.16}$$

Here $\lambda_{\min}(Q_2) > 0$ is the smallest eigenvalue of the matrix $Q_2$ and $I_2$ is an identity matrix. Therefore assumption A2) holds true.

A3) The Jacobian of the function p for the system defined in (7.10) and (7.13) can be written as:

$$\frac{\partial p(z, y)}{\partial y} = \begin{bmatrix} -\alpha \dfrac{\partial \varphi(y)}{\partial y} \\ 1 \\ 0 \end{bmatrix} \tag{7.17}$$

Now since the function $\varphi(y)$ is of the class $C^1$, the $\dfrac{\partial \varphi(y)}{\partial y}$ is bounded, i.e. $\left\| \dfrac{\partial p(z, y)}{\partial y} \right\| \le M$ thus proving assumptions A3).

A4) In (7.9) and (7.12), the function $h_2(x)$ is a linear function and therefore Lipschitz continuous, hence the assumption A4) will hold true.

### 7.3.2 Implementation Method 2

Method 2 is quite similar to method 1, the only difference being that the encrypted message is included in one of the states rather than changing the chaotic system parameter. (T) and (R) can now be written as

$$\begin{aligned} (T): & \begin{cases} \dot{x}_1 = -\sigma_1 x_1 + \sigma_1 x_2 \\ \dot{x}_2 = -20 y_1 x_3 + r y_1 - x_2 \\ \dot{x}_3 = 5 y_1 x_2 - \beta x_3 + e(\eta_m, k), \end{cases} \\ (R): & \begin{cases} \dot{\hat{x}}_1 = -\sigma_1 \hat{x}_1 + \sigma_1 \hat{x}_2 \\ \dot{\hat{x}}_2 = -20 y_1 \hat{x}_3 + r y_1 - \hat{x}_2 \\ \dot{\hat{x}}_3 = 5 y_1 \hat{x}_2 - \beta \hat{x}_3 + e(0, \hat{k}), \end{cases} \end{aligned} \tag{7.18}$$

with everything else remaining the same as in method I.

## 7.4 Simulation Results

Systems (7.9), (7.10), (7.12), (7.13) and (7.18) are simulated using Matlab/Simulink for the transmission of randomly generated digital bits. The different values used for the systems are taken as

$\sigma_1$ = 16, r = 45.6, $\beta$ = 4.2, $\rho$ = 0.1, h = 0.2, $\alpha$ = 10, $\delta$ = -14.87, $\gamma$ = 0, $d_0$ = 0.05

and n for cipher shift algorithm is taken as 30.

#### 7.4.1.1 Method 1 results

Figure 7.3 shows the randomly generated binary message signal to be transmitted. Figure 7.4 shows the scatter plot of the switching parameter $\beta_m$ encrypted by the algorithm mentioned in (7.7) using the keystream k shown in Figure 7.5. It can be seen that the switching parameter is varying between the ranges 4 to 4.4 with no particular order. Now, one question that might arise is with this variation of parameter in the system (7.9), will the system still remain in the chaotic regime. The answer is provided by the strange attractor of the system (7.9) depicted in Figure 7.6. It can clearly be seen that the shape of the attractor is still preserved and is same as the standard Lorenz attractor. Therefore, even with the implementation of the proposed method, the inherent chaotic property of the Lorenz system will not be compromised. Finally, the transmitted signal, i.e. output from the Lorenz oscillator (7.9) is shown in Figure 7.7 which is the signal transmitted to the receiver through the public channel.

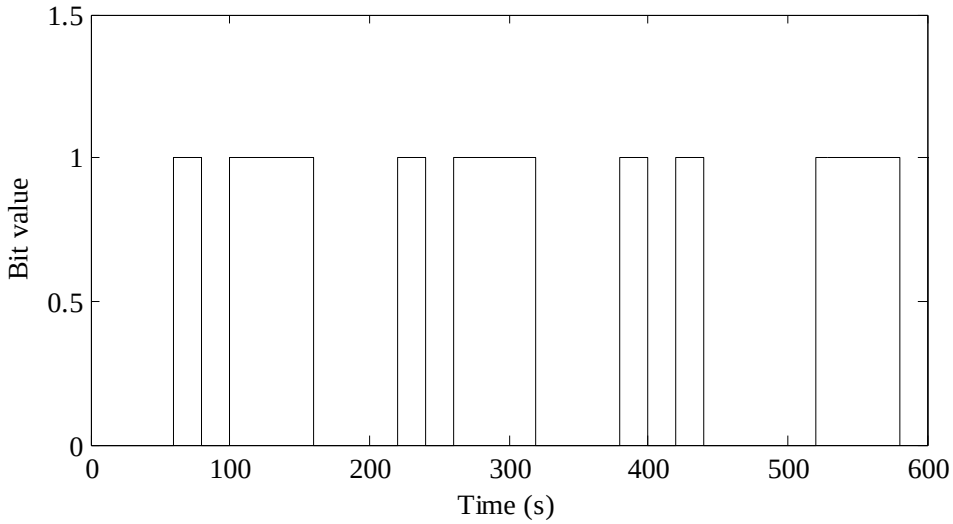


Figure 7.3: Randomly generated bits to be transmitted.

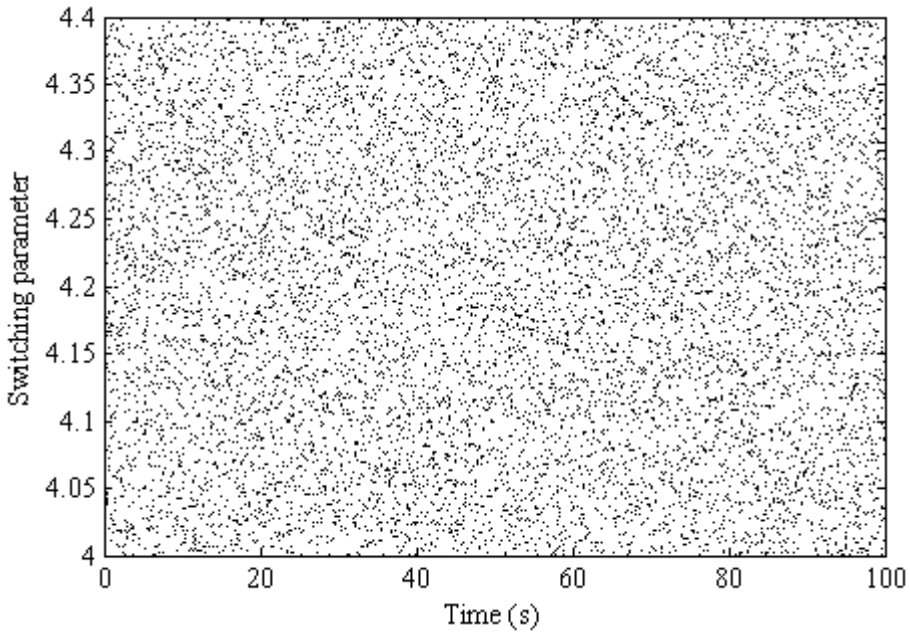


Figure 7.4: The switching parameter $\beta$ varying within the range of 4 to 4.4.

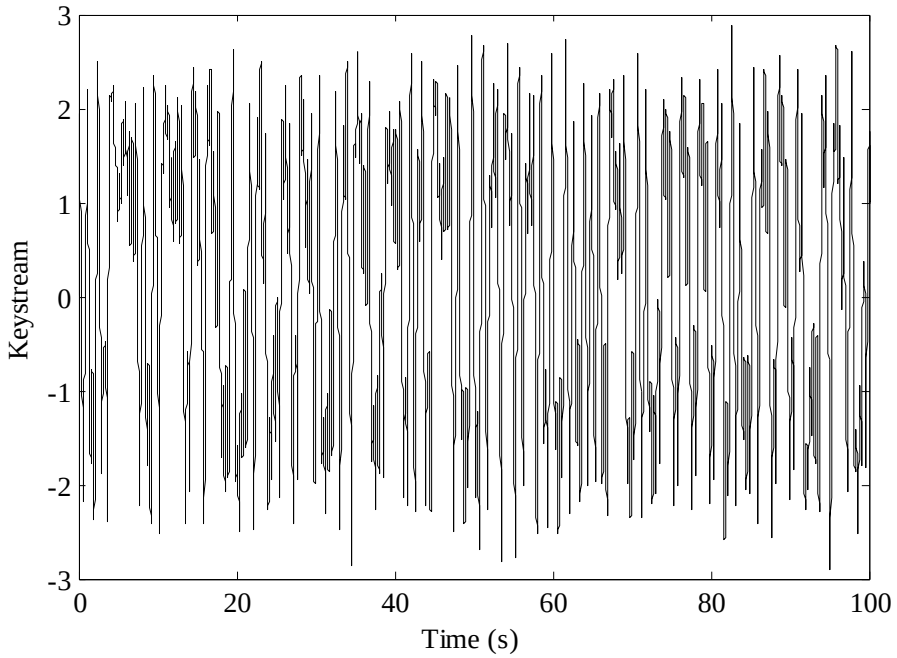


Figure 7.5: Keystream generated at the transmitter.

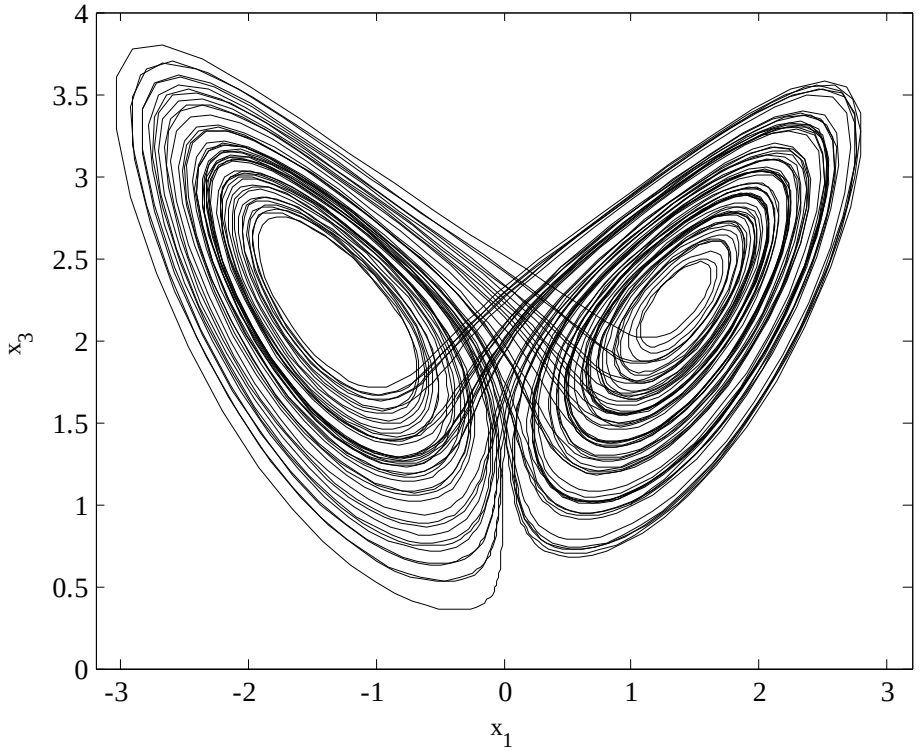


Figure 7.6: Strange attractor of the Lorenz system (7.9).

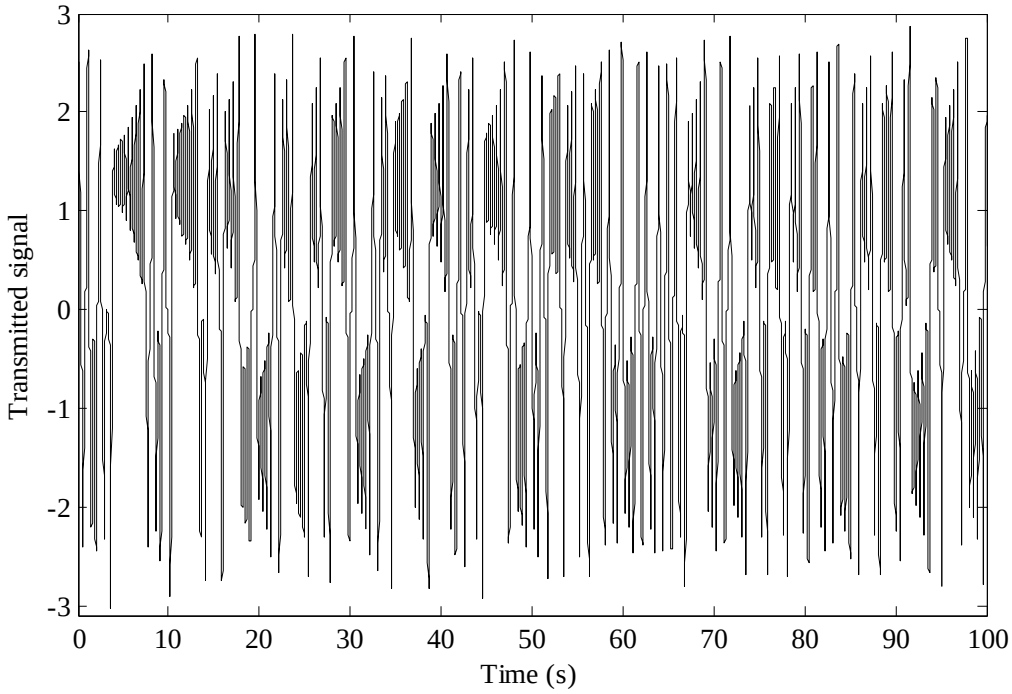


Figure 7.7: Output from the transmitter (T) i.e. transmitted chaotic signal.

Now at the receiver side, upon receiving the transmitted signal, synchronization is performed. First let us see how the switching parameter and keystream differ in the receiver side with their counterpart in the transmitter side which are shown in Figure 7.8 Figure 7.9. Note, the difference for the time interval when bit 1 and 0 is transmitted. When 0 is transmitted, the switching parameter will be same, therefore synchronization between (T) and (R) is achieved, which means same driving signal for ICCS, consequently same keystream, and again same switching parameter. This is some sort of vicious cycle. But in simple terms, when 0 is transmitted, key generated and the switching parameter are equal that means both (T) and (R) synchronize with each other.

But when 1 is transmitted, the scenario changes however. In the transmitter side, the parameter is being switched due to the encrypted value corresponding to 1. But in the receiver side, the value to be encrypted is always tuned at 0, therefore, the parameter is being switched due to the encrypted value corresponding to only 0. With similar arguments

as before, when 1 is transmitted key generated and switching parameters are different in the transmitter and receiver side implying the synchronization error in (T) and (R).

This means that the binary message signal that has been transmitted can successfully recovered by examining the synchronization error that will exists between (T) and (R). The successful message extraction is shown in Figure 7.10, where there exists obvious synchronization error when 1 is transmitted while the error rapidly approaches to zero when 0 is transmitted.

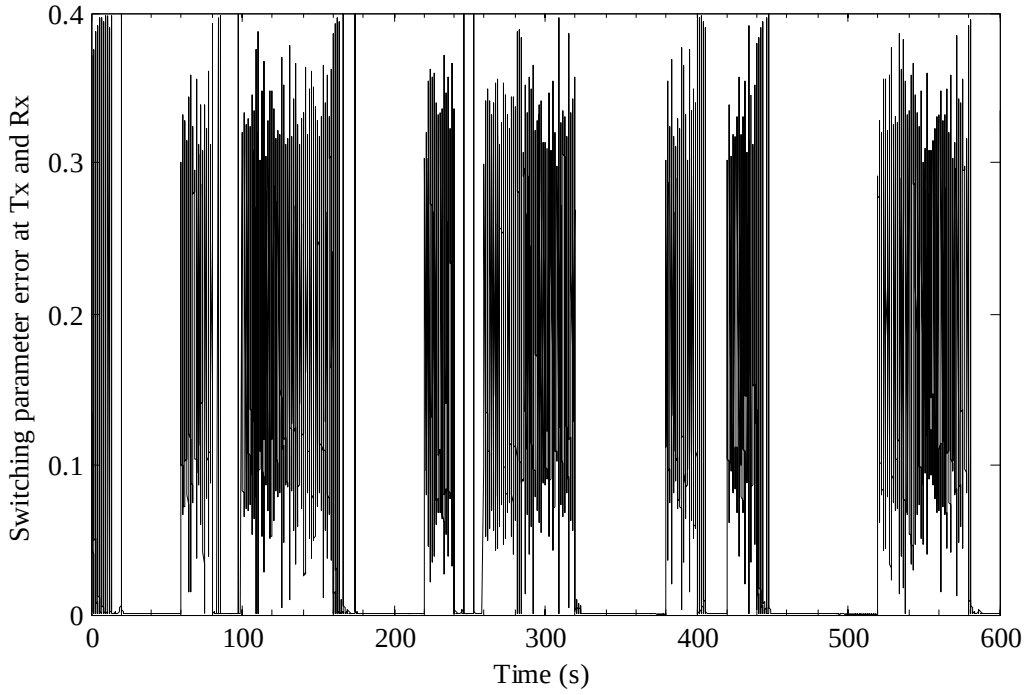


Figure 7.8: Error between the switching parameter used at the transmitter and receiver.

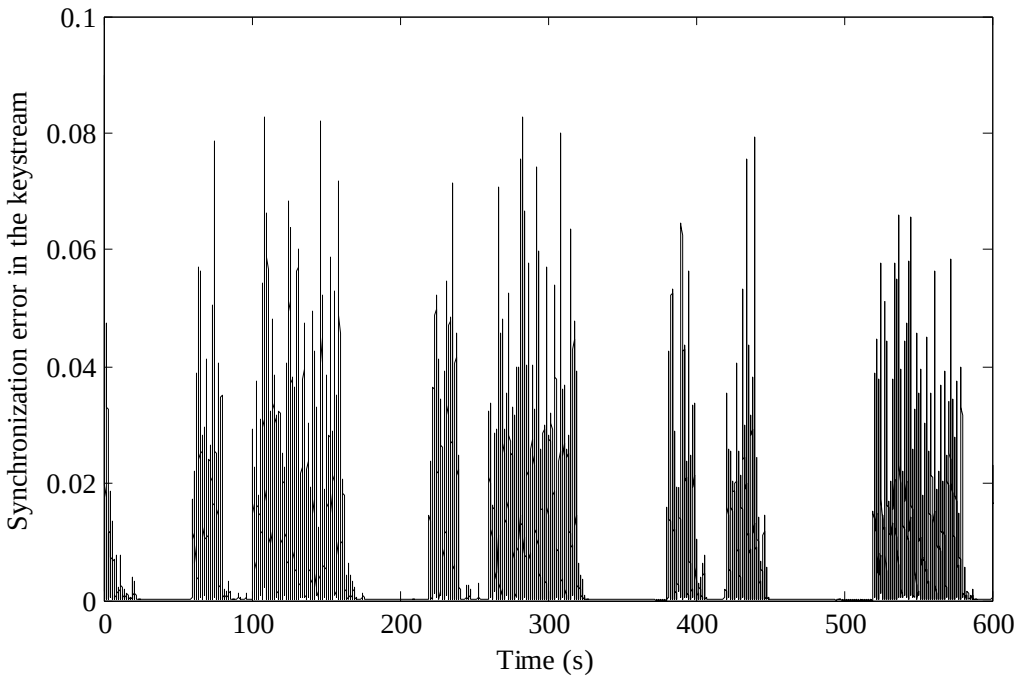


Figure 7.9: Synchronization error between the keystream generated at the transmitter and receiver.

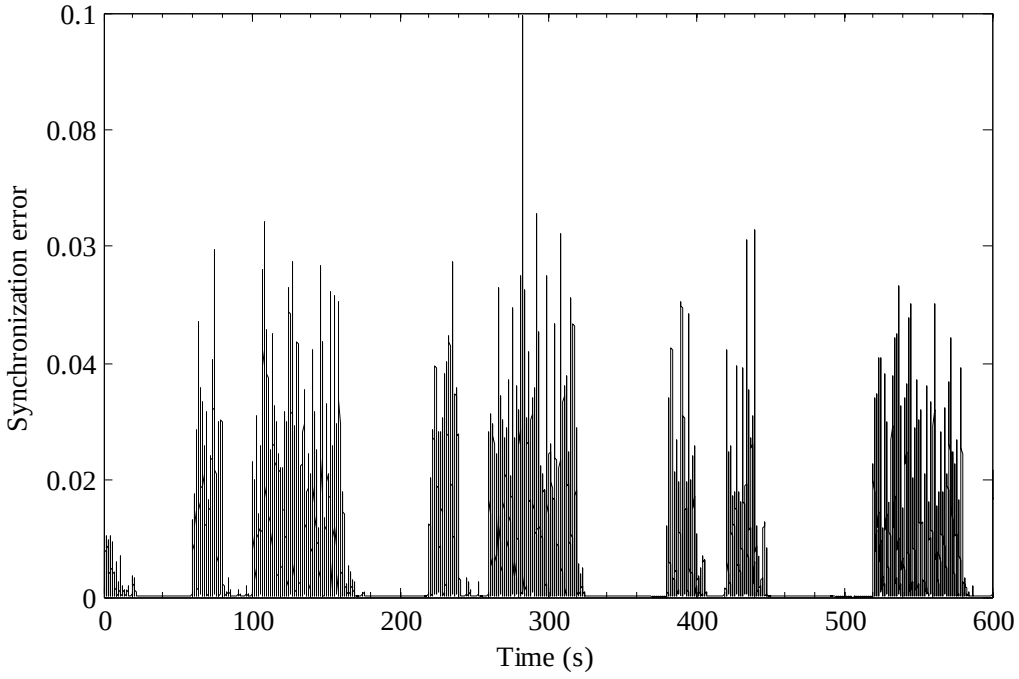


Figure 7.10: Synchronization error between the transmitter and receiver to recover the transmitted message.

#### 7.4.1.2 Method 2 results

Figure 7.11 shows the random binary message that has to be transmitted securely. Figure 7.12 shows the scatter plot of the encrypted inclusion parameter corresponding to bit value that uses the encryption algorithm given in (7.7) and keystream k as shown in Figure 7.13. Here again, there is no apparent order in which the inclusion parameter value is changing. Here again, the analysis of the chaoticity of the Lorenz system after implementing the proposed method 2 is done. For this, the strange attractor is plotted for the Lorenz transmitter and is shown in Figure 7.14 and is same as the attractor of the standard Lorenz system. Therefore, with the implementation of the method 2, even when one time varying inclusion parameter is added to one of the states of the Lorenz system, for implementing CSK, chaotic property of it is maintained. Finally, Figure 7.15 shows the resulting output signal that has to be transmitted.

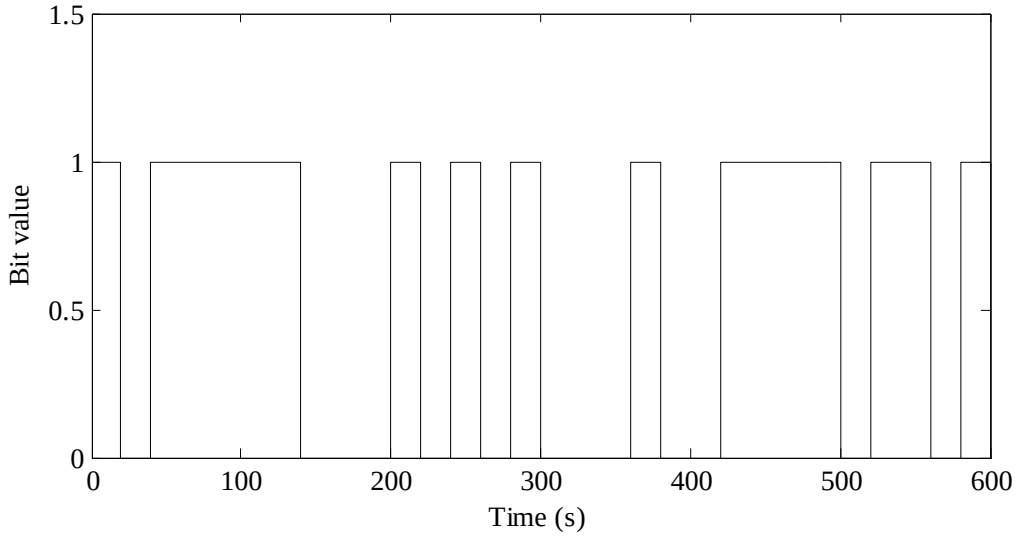


Figure 7.11: Randomly generated bits to be transmitted.

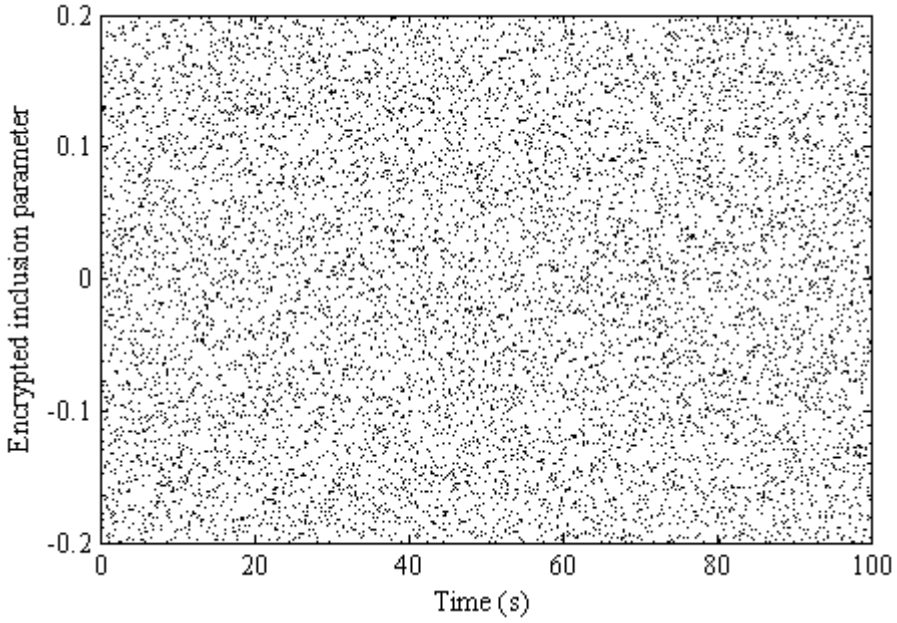


Figure 7.12: The inclusion parameter varying within the range of -0.2 to 0.2.

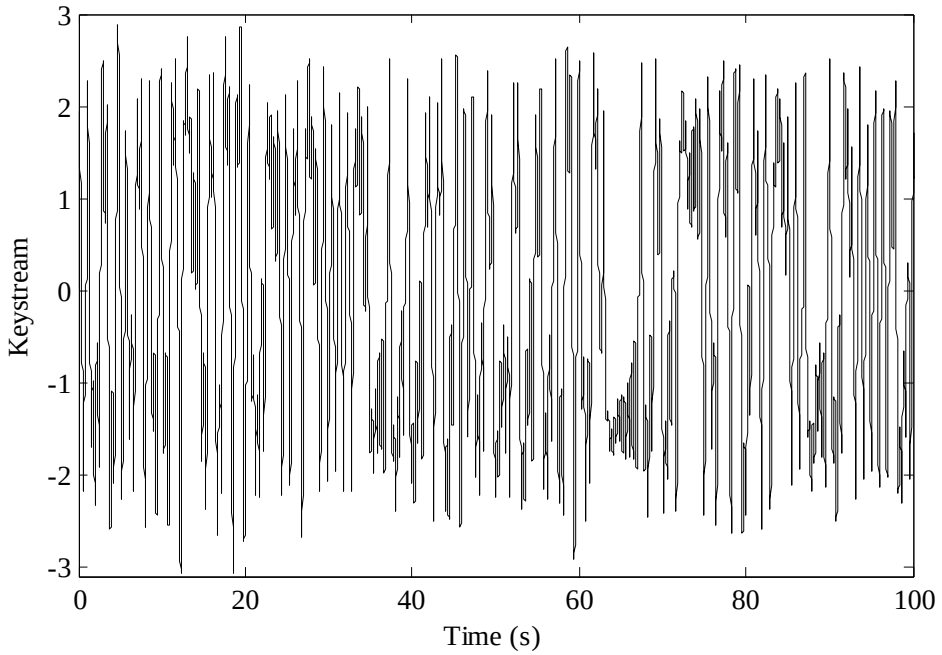


Figure 7.13: Keystream generated at the transmitter.

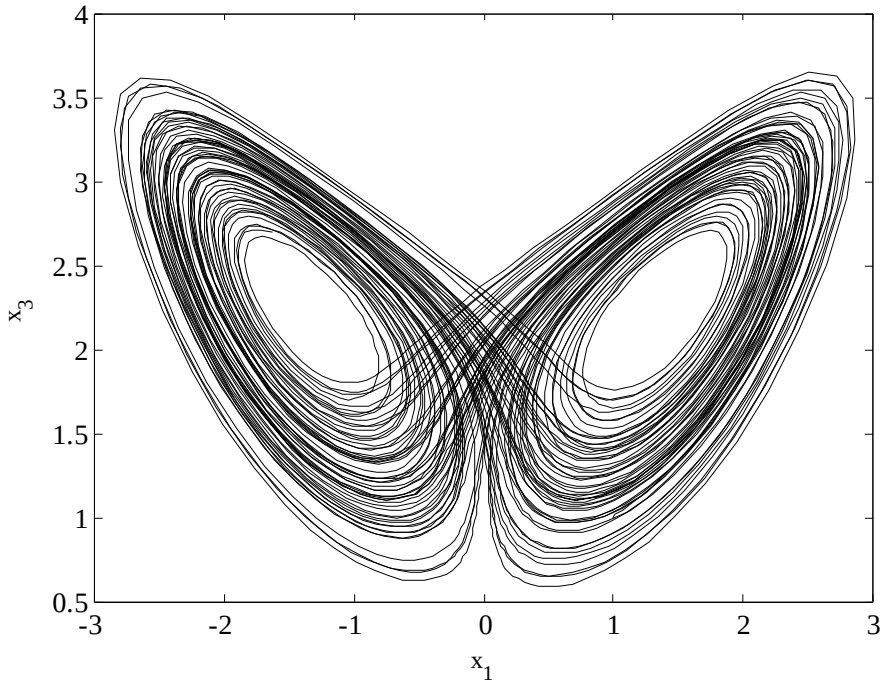


Figure 7.14: Strange attractor of the Lorenz system used as the transmitter.

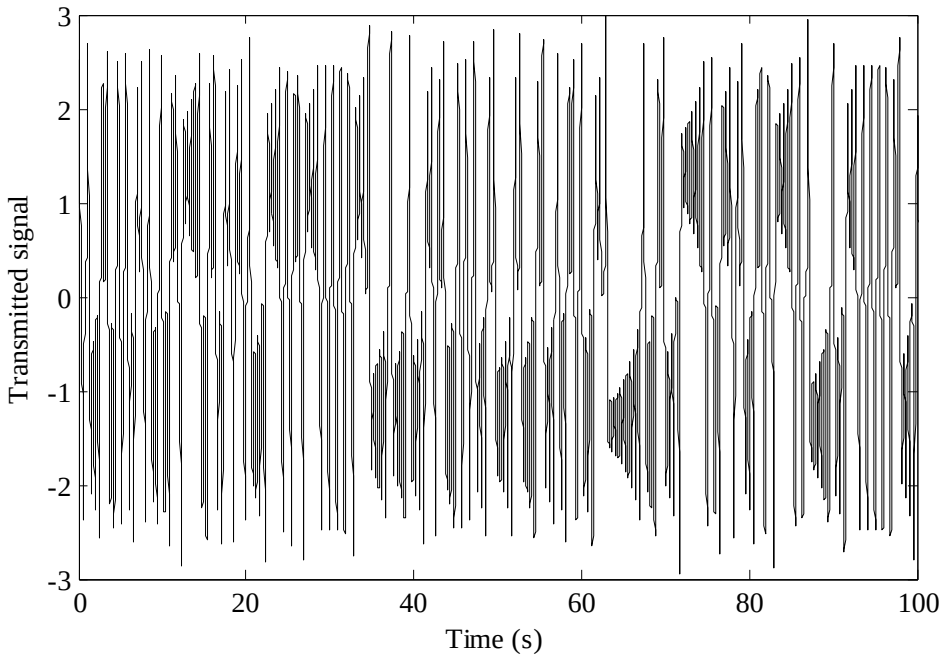


Figure 7.15: Output from the transmitter (T) i.e. transmitted chaotic signal.

Now at the receiver side, upon receiving the transmitted signal synchronization is performed, keystream is regenerated and inclusion parameter is also produced. Depending on which bit value is transmitted, we will get error in the inclusion parameter and also in the keystream generated. Same reasoning mentioned for Method 1 is valid in this case as well. Figure 7.16 shows the error in the inclusion parameter while Figure 7.17 shows the synchronization error in the generation of the keystream. Finally, Figure 7.18 shows the synchronization error between (T) and (R) which shows significant error when 1 is transmitted while error converges rapidly to zero when 0 is transmitted, thus successfully recovering the message.

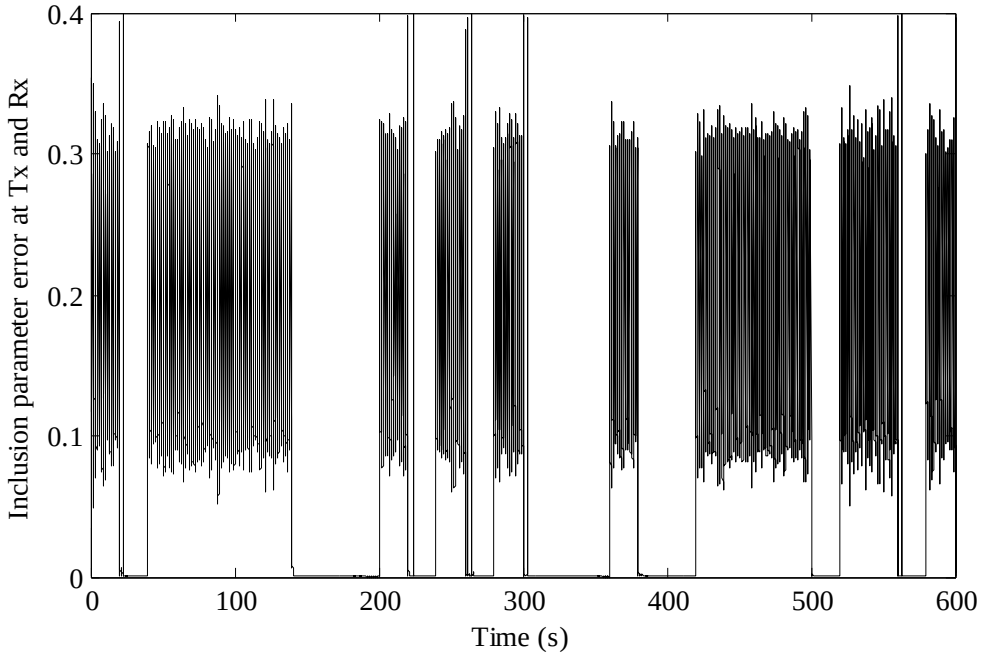


Figure 7.16: Error between the inclusion parameter used at the transmitter and receiver.

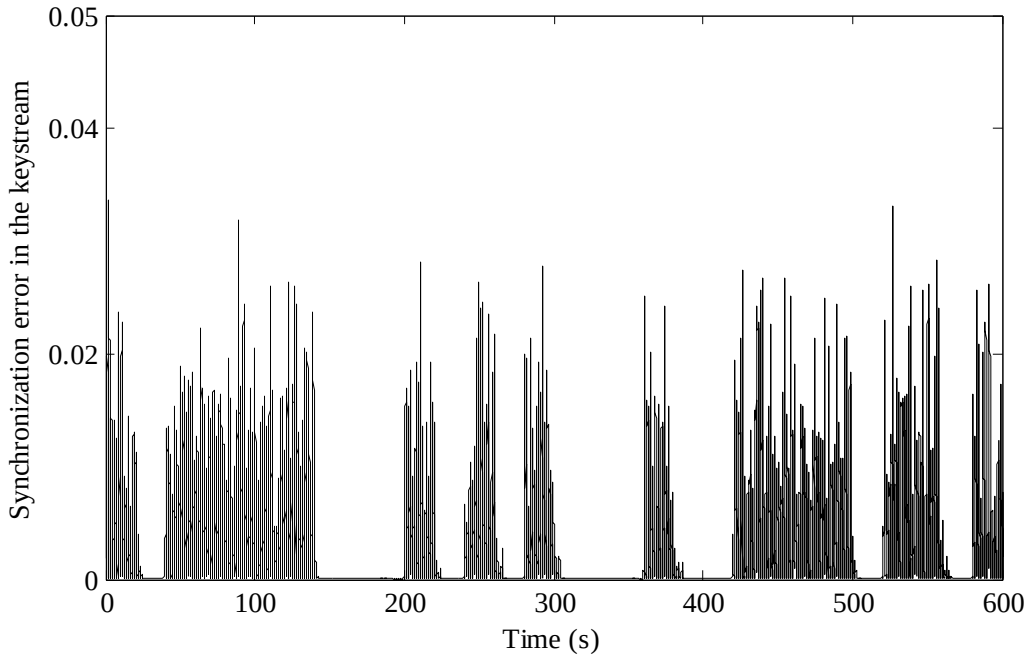


Figure 7.17: Synchronization error between the keystream generated at the transmitter and receiver.

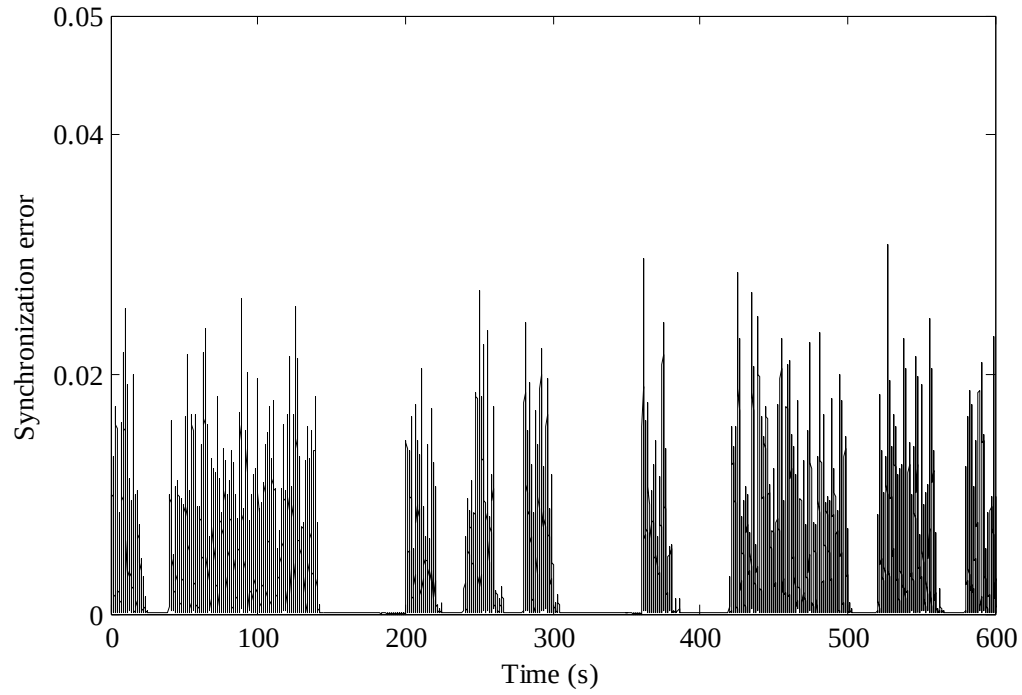


Figure 7.18: Synchronization error between the transmitter and receiver to recover the transmitted message.

## 7.5 Security Analysis

In this section, security analysis of the both proposed methods using the most common decryption attack will be done. Not all of the attack methods are possible to be taken into consideration. However, RM being the common and the most powerful decryption method for attacking CSK, it is used here in this work. RM sees the extraction of bits as a classification problem. In fact, extraction of either 0 or 1 from the transmitted signal is a classification problem which is how digital equalization is also performed [181] in digital communication. Other pattern classification tools can also be studied; however, if there is no pattern to classify for one method (RM in this case), it will generally imply that it will be valid for the remaining tools.

The method proposed here has improved the security of the CSK technique. The use of the keystream, generated by ICCS at the transmitter and the receiver, will generate the parameter $\beta_{\mathrm{m}}$ (or inclusion parameter) of different values, in fact infinite possibilities within a boundary. The keystream generated is not part of the transmitted signal therefore there is no way that the intruders will be able to generate it from only the knowledge of the transmitted carrier signal. Without the knowledge of the keystream, it will be impossible for the intruders to find the change in the parameter $\hat{\beta}_{\mathrm{m}}$ (or the inclusion parameter) in the receiver to perform synchronization/desynchronization for extracting the bits.

Figure 7.19 and Figure 7.20 shows the return maps of the transmitted signal that is generated using proposed method 1 and 2. It can clearly be seen that RM of the transmitted signal does not change according to the bit values being sent. This therefore will remove the possibility of seeing extraction of the bits as a classification problem. Therefore, by implementing the proposed methods a secure communication can be realized. For comparison, the RM of the transmitted signal is plotted when CSK is not implemented, i.e.

when the transmitted bits does not modulate the parameter of the transmitter. It can be seen in Figure 7.21 that the RM is similar as in Figure 7.19 and Figure 7.20 concluding that the proposed method does not necessarily change the RM of the transmitted carrier chaotic signal. Even when the return map is zoomed in, the RM does not split.

Brute force attacks also will not be valid because of the large key space to choose from. Switch detection that detect the discontinuities of the first derivative of the transmitted signal to reveal the transmitted bits will also not be a convincing option because the encryption rule will generate range of values in the interval [-h, h] thus bringing about infinite levels of switching. Exhaustive cryptanalysis such as known plaintext attack, known ciphertext attack, etc may be done as part of the future work of this research.

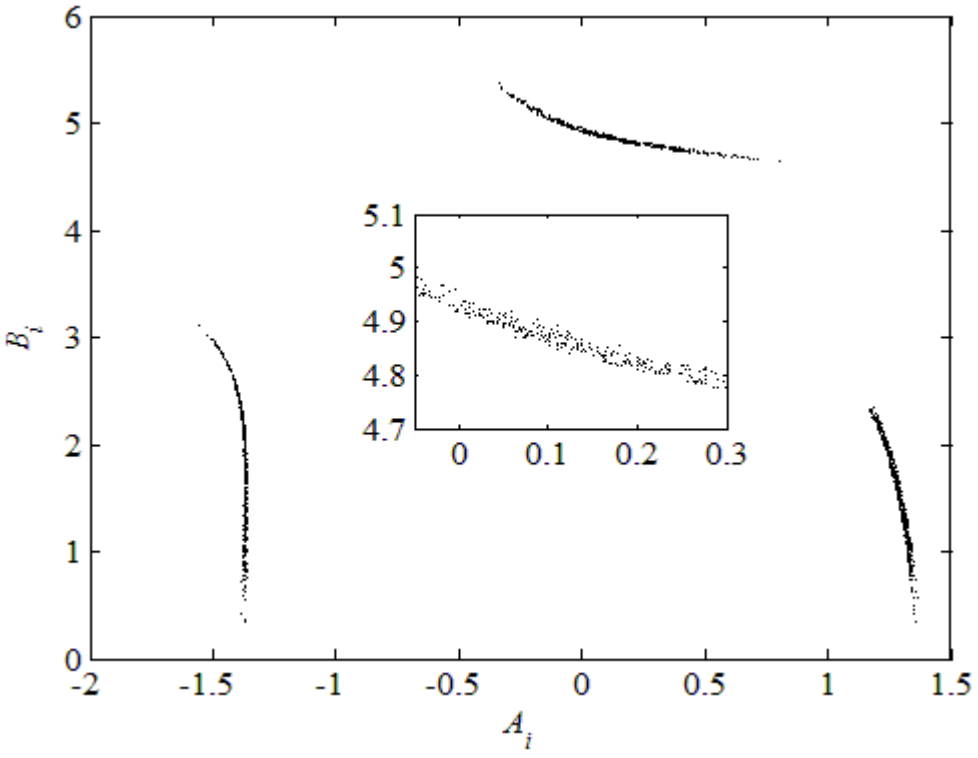


Figure 7.19: Return map of the transmitted carrier signal using method 1.

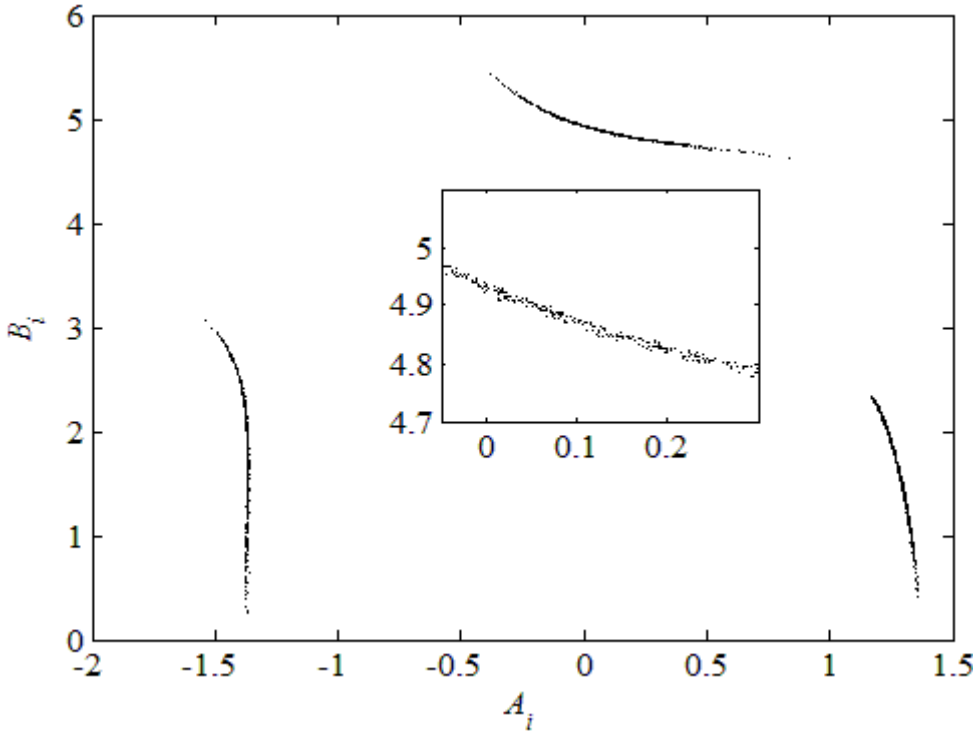


Figure 7.20: Return map of the transmitted carrier signal using method 2.

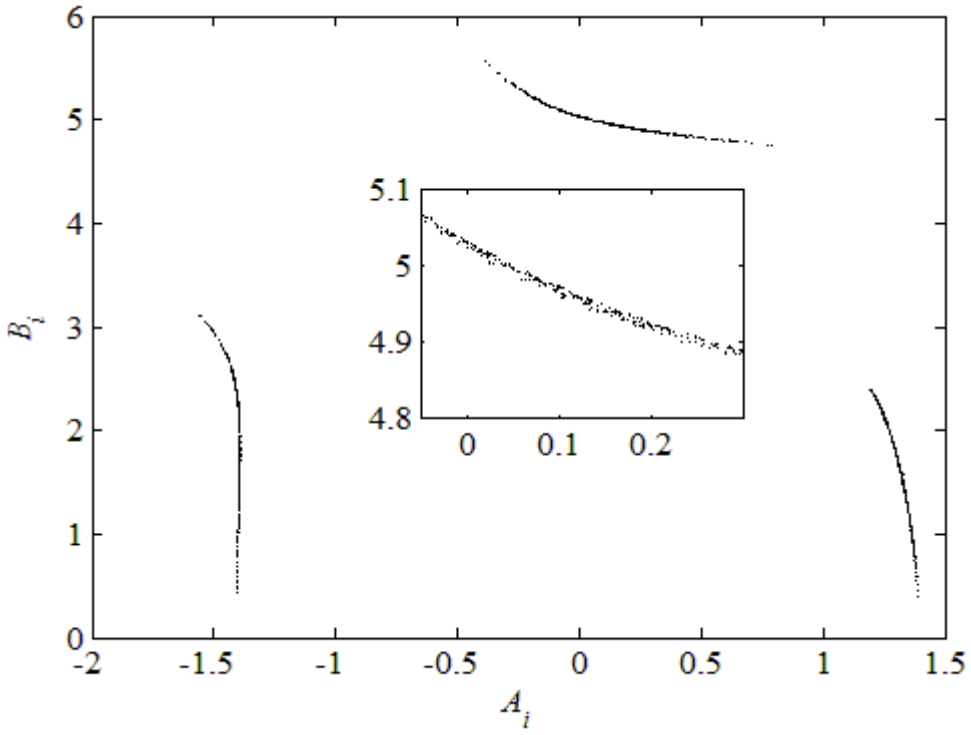


Figure 7.21: Return map of the transmitted carrier signal when CSK is not implemented.

## 7.6 Summary

In this chapter, improved CSK method was proposed to transmit digital bits securely. This new method was suggested using the ICCS where the generated keystream was used to encrypt the switching parameter that modulated the digital bits. Two different variations of the methods were proposed. The method proposed was implemented using Lorenz and Chua's system and the simulation results confirmed the possibility of extracting the transmitted message signal. Further, the security analysis of both methods was performed and the RM of the transmitted signal was shown for both methods. It was seen that no information regarding the message was revealed in RM unlike in traditional CSK or other modified CSK methods, available in the literature, giving the proposed method distinct advantage to the existing techniques.

# Chapter 8 Digitization of Chaotic Signals: Application in Non-Ideal Channels

## 8.1 Introductions

Chaotic communication has promised a lot in secure communication and there is still a great scope for it to be implemented for security purposes even though many attack methods are proposed. The existing methods can be modified, as seen in earlier chapters, and more new methods will be devised gradually eventually. However, in order to implement chaotic carriers for security purpose in real environment, channel noise and channel model have to be considered as well. Synchronization methods for reducing the effect of noise have been proposed in the literatures (see e.g. [182-184]) but they were mainly concentrated on either spread spectrum applications or in CSK methods or only focussed on synchronization issues. Also, the majority of the chaotic communication methods proposed do not complement with the existing digital communication schemes but requires to be implemented differently thus leading to parallel development of error correction, equalisation, and dispersion compensation schemes. Therefore, it would be logical and a step forward move if future development in chaotic communication systems can be built on the existing technologies where the nature of chaotic signals will provide advantages of security while the existing digital communication building blocks will be utilized for all other aspects of communication.

In this chapter, we propose a method where the chaotic carrier containing the message signals are first digitized and converted into binary data sequences. These binary sequences are transmitted using the conventional digital communication links. At the receiving end,

the digital sequence is regenerated using existing technology where the error correction, equalisation and dispersion compensation can readily be applied. The recovered chaotic signal can be used for chaotic synchronization and extraction of the actual hidden message signal. In this method, it is shown that message recovery is possible with a high degree of accuracy at moderate SNR of 14 dB even when the BER is very high. The SNR required to recover the message can further be reduced by implanting the error correction codes and digital signal processing tools which are already well established in digital communication. The security issues are not taken into consideration in this study and a simple chaotic masking is used to demonstrate the concept of digitization. However, other methods can easily be implemented using the same concept. The idea here is to show the potential of the method of digitization.

## 8.2 Digitization of Chaotic Signals

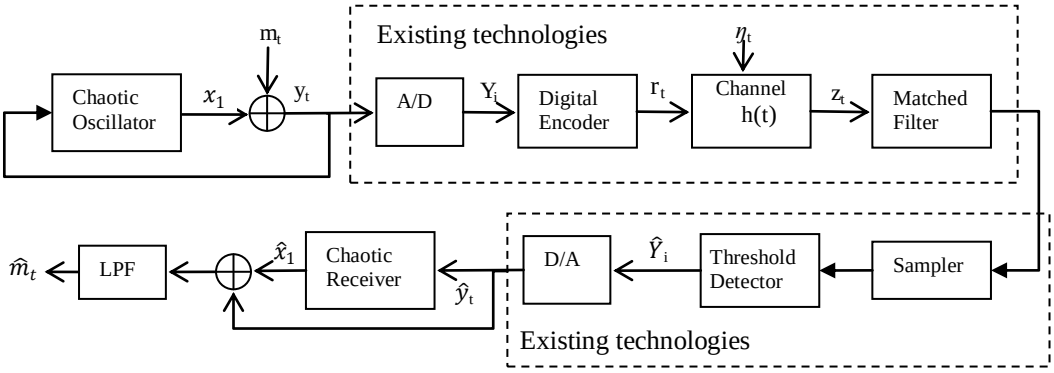


Figure 8.1: Block diagram of the proposed chaotic communication system using digitization.

The schematic block diagram of the proposed system is shown in the Figure 8.1. Assuming a band limited chaotic signal and provided the sampling rate is higher than the Nyquist rate the continuous chaotic signal y(t) can be represented in discrete format $Y_i$. y(t) is converted into a digital format with uniform sampling before being digitally encoded. Assuming the

Discrete Memoryless Source (DMS), the simplest encoding scheme of fixed length code word of n-bits per sample is used for representing the binary digits. Different coding techniques (i.e. Pulse Code Modulation (PCM), Differential PCM (DPCM), adaptive PCM, delta modulation) could be applied to reduce the quantization error and hence improve the performance. In this work, PCM with uniform quantization level is used. Investigating the systems performance using other coding techniques could be a subject of further study. Simple baseband modulation technique of On-Off keying (OOK) with 100% duty cycle is used for the digital transmission.

The channel h(t) is assumed to be Additive White Gaussian (AWG). At the receiver a matched filter followed by a sampler and a threshold detector are used to regenerated the binary sequence $\hat{Y}_i$. The binary sequence is converted back into analogue chaotic signal using D/A. A chaotic receiver can be used for chaotic synchronization and to recover the original message signal. Any existing method at chaotic receiver can be used for achieving synchronization.

Converting the chaos signal into a digital format has the advantages of being able to transmit it through existing communications links wired or wireless (radio or optical) taking advantage of the existing infrastructure. Problems including noise, multipath induced distortion and dispersion, and fading can readily be dealt with in the digital domain. For example, it is rather complicated and challenging to design equalizing filters for chaotic communications since it has a broad spectrum. However, with digitization of chaotic signal this is no longer a major problem. One key advantage of the proposed system is the perfect reconstruction of the chaotic signal at the receiver having been propagated through a real channel. The metric for comparing the performance and measuring the reliability of digital communication system is the bit error rate (BER). In this chapter, we study the performance of the communication system for different BER.

Once the minimum BER require for message recovery is set, the error control coding, (e.g. convolutional, turbo and a low parity density codes) can be used to improve the BER performance and hence increase reliability [185].

It is to be noted that in the analysis of chaotic system, researchers generally tend to consider the channel to be noise-free and non-dispersive. However, physical channels are always noisy and may be dispersive. Nevertheless, with the digitization concept proposed, the dispersion can simply be compensated by means of equalizers including like linear equalizer, decision feedback equalizers and the more recently reported WT and ANN based equalizer [186].

## 8.3 Simulation Results and Discussions

Simulation of the proposed chaotic communication system using digitization is done using the Matlab/Simulink. We have used the popular Lorenz system [88] as a chaotic oscillator and the chaotic synchronization obtained is from classical drive-response principle. The masking method adopted includes the message of $m = \sin(\omega t)$ with $\omega = 1$ rad/sec and the resulting output signal is sampled and quantized using an A/D converter. The quantization resolution n is 6. The digital sequence in OOK format is transmitted through the non-ideal channel. The SNR is varied in order to achieve BER of different order. To accurately estimate the message signal, the performance of the system is examined for over a range of BER and a threshold BER is determined.

Figure 8.2 illustrates the synchronization between the observed state $\hat{x}_1$ and the transmitter state $x_1$ when BER obtained is $10^{-6}$. The $45^0$ line indicates perfect synchronization illustrating that chaotic synchronization is still possible after A/D and D/A conversion of the chaotic carrier signal. One thing that should be pointed out is the signal used to drive

the chaotic receiver for synchronization is obtained after the channel noise had its effect on the carrier. So, this means that without the need of any other complex method, synchronization can easily be obtained if concept of digitization is employed.

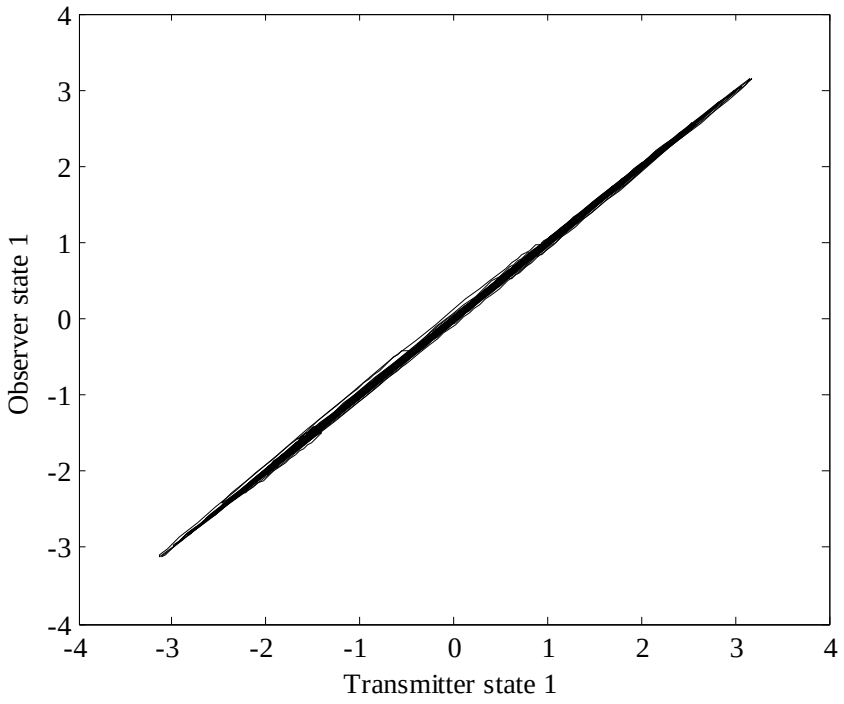


Figure 8.2: Synchronization between states used for masking when BER is $10^{-6}$.

Now let us see how accurately the message is recovered for a given BER. Figure 8.3 depicts time waveforms for transmitted and recovered message signal m at a BER of $10^{-6}$. Since, method of masking is used; the received quantized chaotic carrier is subtracted to obtain the message signal. Therefore, the quantization error because of A/D conversion will have effect on message recovery. So, to reduce the effect of quantization error an 8th order low-pass Butterworth filter with a cut off frequency of 2 rads/sec is employed to recover the message signal. For a reliable digital communication link the optimum BER is considered to be $10^{-6}$. We can see in Figure 8.3 that the perfect recovery of message is possible at BER of $10^{-6}$. Figure 8.4 shows the recovered message time waveform at BER of $10^{-3}$, $10^{-4}$ and $10^{-6}$. The proposed scheme is still able to extract the message signal with

reasonable quality at BER of $10^{-4}$. However, there is some distortion for higher values of BER (i.e.$10^{-3}$). These results demonstrate the potential of this scheme for BER of < $10^{-4}$ over noisy channel condition. The proposed system can readily be implemented using existing commercial components. To further increase the performance of the system, quantization error can be reduced using DPCM scheme, or other advanced source coding, which can be a subject of further study.

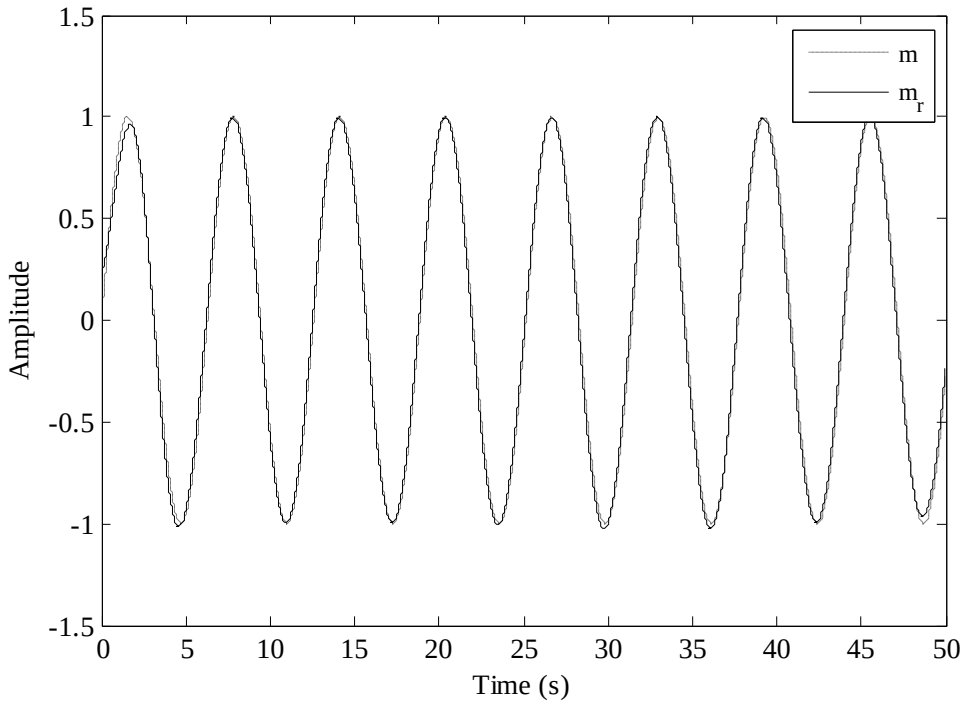


Figure 8.3: Transmitted and recovered message at BER $10^{-6}$.

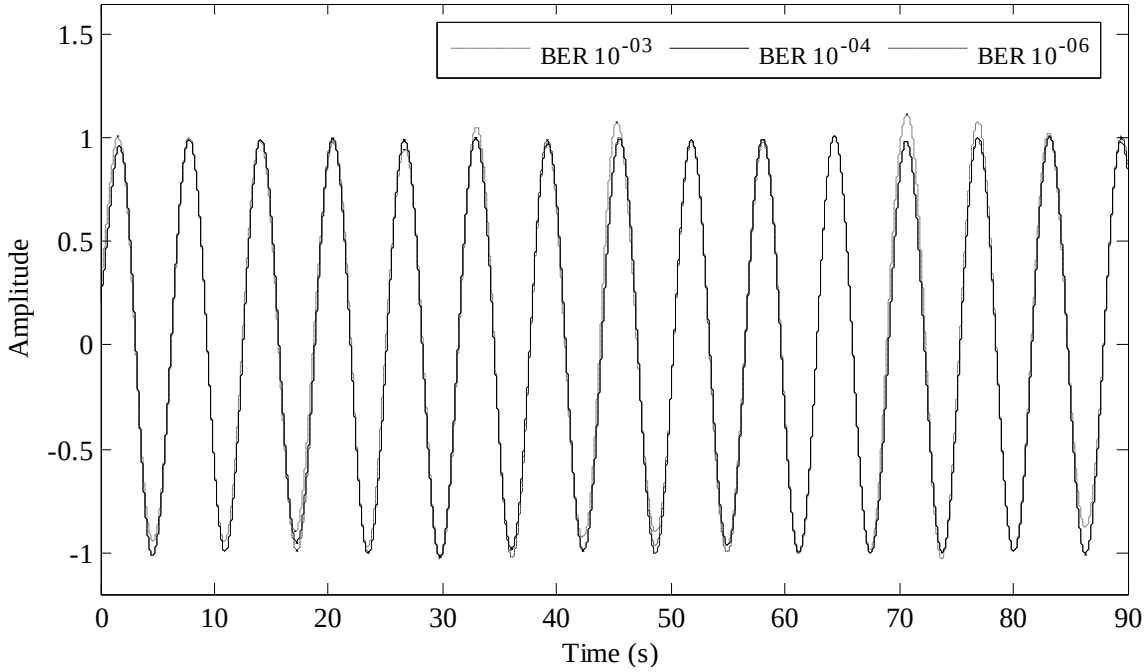


Figure 8.4: Recovered message at different BERs.

## 8.4 Summary

It is quite a known fact that chaotic signals has a lot of potential to be utilized for secure communication however the real environment and channels might bring on the problem of dispersion and interferences due to noise. Equalisation techniques, error correction techniques have to be realized for chaotic communication if it has to be implemented in practical applications. However, the development of digital communication and all the tools that are available can be utilized in chaotic communication without the need of parallel development. In this chapter, a method based on digitization of chaotic signals acting as a transmitted carrier signal is proposed. It was shown that the chaotic synchronization and thus message recovery was possible for the BER as low as $10^{-4}$ and moderate SNR of 14 dB. This meant that the idea of digitization can be implemented. Simple baseband modulation technique of OOK with 100% duty cycle was used to

transmit the digitally encoded bits; however other techniques can easily be implemented. Also, simple masking method was used to mix message signal with the chaotic carrier for simplicity to demonstrate the concept of digitization, but other form of methods enhancing the security can easily be implemented as well.

# Chapter 9 Conclusions and Future Works

## 9.1 Conclusions

The objective of this research was to explore techniques to exploit the properties of chaotic signals to implement secure communication. The facts that chaotic signals were aperiodic, broadband and sensitive to initial conditions/parameters mismatches were important for them to be utilized in security. Therefore the chaotic parameters acted some sort of hardware key and hence same dynamical system was necessary for the transmitter and the receiver with proper chaotic synchronization techniques. Different techniques exist in the literature to implement secure chaotic analog based communication such as chaotic masking, modulation, inclusion or CSK methods. However, all of these methods suffered from various disadvantages mainly being vulnerable to different attack methods to extract the hidden message even when the intruders where not aware of the dynamics of the chaotic transmitter system. The attack methods were based on NLD methods, power filtering methods, pattern classification methods such as RM or ANN, etc. Various other modifications for these methods and some other newer techniques could also be found in the literature, however all suffered again from similar issues. Therefore, there is a real incentive to exploit the chaotic signals in such a way that it thwarted existing attack methods. In this research, various different methods were revisited and the possible improvements in them were pointed out.

In Chapter 3 it was found that the Proportional Integral observer is a better choice for obtaining chaotic synchronization. When the performance of both P and PI observer were done for the combinational masking + inclusion method, it was found that PI observer

showed better resilient to the noise and better message recovery. Therefore, PI observer is better suited for performing chaotic synchronization.

One of the main aims of this research was to find a method that will allow secure transmission of the message such that the intruders will not be successful to extract the message without the legible receiver. In Chapter 4, cascaded chaotic masking technique was proposed and it was found that when two equal powered chaotic signals were added to each other and message was modulated in it, then it adds complexity to the transmitted signal thus making NLD method more or less ineffective. However, it should be noted that by using cascaded chaotic structures, the dimension of the dynamical system was increased from n to 2n, 3 to 6 in case of Lorenz implementation, so for motivated enough users, they might be able to crack the system from the methods that were used to attack hyperchaotic systems. Even though, the no attack methods are reported yet to break cascaded structures, more possibilities were still needed to be explored.

In Chapter 5 a new type of chaotic synchronization technique called ICCS was proposed. ICCS is a unique type of synchronization technique where the two oscillators were not uni directionally coupled, i.e. the output of one oscillator was not used for driving another chaotic oscillator, and instead both were being driven independently from the output that was originating from two different chaotic oscillators. The ICCS was very useful because the output from these indirectly coupled chaotic oscillators were used as keystream in the transmitter and receiver side, without the need for it to get transmitted in the communication channel. This has a major advantage, since the intruders will not be able to estimate the keystream being used for encryption purposes simply by having the transmitted signal available. The application of this was done in Chapter 6 and 7 where existing communication schemes were modified to propose secure methods. The security

analysis performed showed that the methods proposed were indeed secure and popular attack methods were not able to extract the transmitted message signal. It was seen that NLD based forecasting method will not be feasible for the proposed method implementing ICCS, since the dynamics of the keystream generator was not be present in the transmitted signal, hence without knowing the keystream, even if the intruders got hold of the encrypted message, message extraction was not be possible. The practical realization of the proposed system done in the DSP board (TMS320C6713 DSK) showed that the proposed method is feasible to implement practically in real time.

Along with the investigation for increasing the security, fundamental aspects of communication like combating noise and dispersion/fading effects plays a vital role in the performance of the method. Already much advancement has been made in digital communication with different methods available for error correction codes and dispersion compensation. Therefore, it will be wise to use all these existing methods while chaotic signals adding the security layer to the communication framework. Hence, a concept of digitization was proposed in Chapter 8. The proposed method takes the advantage of using the existing tools available in digital domain on the digitized chaotic signals to combat the noise and channel model. The simulation results showed the performance of the method to successfully recover the message signal at a moderate SNR of 14 dB. The system was able to recover the message at BER up to $10^{-4}$. The BER could easily be improved by using error control codes and equalization techniques already available in digital domain.

## 9.2 Future Works

Though extensive work had been carried out for implementing chaotic signals for secure communication, it is very essential to provide a list of further works that is necessary to

make the system more efficient and effective. A number of encouraging methods were proposed however there might be needed to perform some further investigation.

One of the key points was in the implementation of the methods that were proposed in the research. In most of the cases, the message signal that was used to be transmitted was very low frequency signal. Therefore, further investigation to modify the proposed method to be used to support higher bandwidth is necessary. This research only focused in developing newer ideas for implementing chaotic signals for secure communication, so further works can be made in this aspect.

The implementation of the method was done mostly by using Lorenz and Chua's system therefore, the performance of the methods in other chaotic systems, preferably higher order systems, or time delay systems, can also be done in order to improve the security further. Moreover, other sophisticated encryption algorithms instead of just n-shift cipher algorithm can be investigated for enhancing the security.

The proposed discrete method in Chapter 6 was implemented in DSP board as shown in the same chapter. The implementation was just a prototype of the model and was done to show that actually the proposed method is realizable in DSP board. The message signal and transmitted signal were analysed using RTDX in the computer only, therefore, a full communication setup can be implemented as part of the future work to transmit real time electrical signal.

The system performance and comparison of the digitization concept proposed in Chapter 8 using other source coding techniques like delta modulation, DPCM, etc can also be done. First implementation of a simple equalizer to show the potential of digitization concept can be performed after which more complex equalization methods can also be looked into.

All of the methods proposed in the research were concentrated on radio frequency implementation though the methods can also be easily adapted to optical based chaotic systems. Since the ICCS was proven mathematically for a class of chaotic systems, implementation of ICCS in optical domain is theoretically possible. Therefore, the application of the proposed method in optical domain along with practical applications can be a subject for further research.

# Appendix A

In this appendix, few definitions and theorems are listed that will be useful to understand some of the mathematical notion used in the thesis.

## Stability of Dynamical Systems

The very first concept considered when studying a dynamical system is the stability of its equilibrium point(s).

**Definition 1.** Equilibrium point: A point $x_e$ is said to be an equilibrium point or a fixed point for the system $\dot{x} = f(t, x(t))$ if $x_e$ satisfies

$$0 = f(t, x_e)$$

In other words, if the system is initialised at $x = x_e$, the solution will stay there for all future times.

The stability of a system is concerned with its behaviour near its equilibrium point(s). This intuitive idea is actually very complex for non-linear and time-delay systems in particular. Consequently, a large variety of definitions have been proposed, which differ in very subtle ways. The main objective of the theory of stability is to be able to draw conclusions on the system behaviour without actually calculating its solution.

Now let us have some of the definitions mentioned in the literatures most importantly: Lyapunov stability, asymptotic stability, uniform stability, and exponential stability.

Consider the general autonomous nonlinear system

$$\dot{x} = f(t, x(t)),\ t \geq 0;\ x(0) = x_0 \tag{A1}$$

where $f : R^n \times R^+ \to R^n$ is continuous. Since $f$ is continuous, we are assuming that the above system has a unique solution corresponding to each initial condition. This is true, in particular, if $f$ is a global Lipschitz function. Note that $f$ is global Lipschitz if there exist finite positive constants $T$ and $k$, such that

$$\| f(t, x) - f(t, y) \| \le k \| x - y \|, \ \forall x, y \in R^n, \ \forall t \in [0, T]. \tag{A2}$$

A function satisfying the Lipschitz condition (A2) is said to be Lipschitz continuous, and is continuously differentiable.

Recall also that a state $x_e \in R^n$ is an equilibrium point for system (A1) if $f(t, x_e) = 0$, $\forall t \ge 0$. In what follows, we shall assume that $x_e$ is an equilibrium point for system (A1). We also denote by $x(t, t_0, x_0)$, the solution of (A1) at time instant $t$ corresponding to the initial condition $x_0 = x(t_0, t_0, x_0)$.

**Definition 2.** Lyapunov stability: The equilibrium point $x_e$ of system (A1) is stable or Lyapunov stable if for all $\varepsilon > 0$, there exists $\delta(\varepsilon, t_0) > 0$ such that

$$\| x_0 - x_e \| < \delta(\varepsilon, t_0) \Rightarrow \| x(t, t_0, x_0) - x_e \| < \varepsilon \ \forall \ t \ge t_0.$$

On the other hand, the equilibrium point $x_e$ is unstable if $x_e$ is not Lyapunov stable.

**Definition 3.** Uniform stability: The equilibrium point $x_e$ of system (A1) is uniformly Lyapunov stable if for all $\varepsilon > 0$, there exists $\delta(\varepsilon) > 0$ such that

$$\| x_0 - x_e \| < \delta(\varepsilon) \Rightarrow \| x(t, t_0, x_0) - x_e \| < \varepsilon \ \forall \ t \ge t_0.$$

Equivalently, when $\delta$ depends only on $\varepsilon$, the equilibrium point $x_e$ is said to be uniformly stable.

Lyapunov stability does not guarantee that the solution $x(t, t_0, x_0)$ will converge to the equilibrium point $x_e$. It simply says that the solution will remain in some region around the equilibrium point as time passes, but will not necessarily ever approach it, so long as the initial condition was within a certain distance, $\delta$, of the equilibrium point. A system with a limit cycle, in particular, is stable in the sense of Lyapunov.

As a result of such a bounded-based type of stability definition, the notions of attractivity, asymptotic stability, and exponential stability are defined.

**Definition 4.** Attractivity: The equilibrium point $x_e$ of system (A1) is attractive or convergent if for each $t_0 \in R^+$, there exists an $\eta(t_0) > 0$ such that

$$\| x_0 - x_e \| < \eta(t_0) \Rightarrow x(t_0 + t, t_0, x_0) \to x_e \text{ as } t \to \infty.$$

**Definition 5.** Uniform attractivity: The equilibrium point $x_e$ of system (A1) is uniformly attractive if there exists a number $\eta > 0$ such that

$$\|x_0 - x_e\| < \eta, t_0 \geq 0 \Rightarrow x(t_0 + t, t_0, x_0) \to x_e \text{as } t \to \infty, \text{uniformly in } t_0 \text{and } x_0.$$

By combining the above definitions, we obtain the important notion of asymptotic stability and uniform asymptotic stability.

**Definition 6.** Asymptotic stability: The equilibrium point $x_e$ of system (A1) is asymptotically stable if it is stable and attractive. It is uniformly asymptotically stable if it is both uniformly stable and uniformly attractive.

In many practical situations such as in the convergence of observers, exponential stability is preferred to asymptotic stability.

**Definition 7.** Exponential stability: The equilibrium $x_e$ is exponentially stable if there exist constants $r$, $a$, $b > 0$ such that

$$\|x(t_0 + t, t_0, x_0) - x_e\| \leq a\|x_0 - x_e\| \exp(-bt), \ \forall t, \ t_0 \geq 0, \ \forall x_0 \in B_r$$

where $B_r$ is a ball of radius $r$.

The above definitions are local in nature in the sense that they describe the behaviour of the system solution initialised near the equilibrium point. In other words, there is some region around the equilibrium point in which the initial condition vectors will lead to asymptotically or exponentially stable responses. This region is called the zone of attraction to the equilibrium point.

The following definitions are given in the sense of the global behaviour of system trajectories.

**Definition 8.** Global uniform asymptotic stability: The equilibrium $x_e$ is globally uniformly asymptotically stable if (i) it is uniformly stable, and (ii) for each pair of positive numbers $M$, $\varepsilon$ with $M$ arbitrarily large and $\varepsilon$ arbitrarily small, there exists a finite time $T = T(M, \varepsilon)$ such that

$$\|x_0 - x_e\| < M, t_0 \geq 0 \Rightarrow \|x(t_0 + t, t_0, x_0) - x_e\| < \varepsilon, \forall t \geq T(M, \varepsilon).$$

This definition says that the solution will converge to the equilibrium point and remain there as time passes (since $T(M, \varepsilon)$ is finite), in response to any initial condition (since $M$ is arbitrarily large).

**Definition 9.** Global exponential stability: The equilibrium $x_e$ is globally exponentially stable if there exist constants $a,\ b > 0$ such that

$$\|x(t_0 + t, t_0, x_0)\| \le a\|x_0 - x_e\| \exp(-bt),\ \forall t,\ t_0 \ge 0,\ \forall x_0 \in R^n.$$

It is worth noting that these kinds of definitions can only be satisfied for systems having a single equilibrium point at which the system can come to rest. This is the case of linear systems where the origin is the unique equilibrium point.

In practice, the study of stability is done using Lyapunov's second, or direct, method. This consists of defining a Lyapunov function with appropriate properties; the existence of which will imply the type of desired stability. The second method allows the determination of stability without having to solve the system equations (or find the eigenvalues in the linear case). Consequently, it is a useful method for nonlinear and time-varying systems where the solution of the state equations is very difficult to find in general. Recall that Lyapunov's first method comprises studying the stability of a nonlinear system in the vicinity of an equilibrium point by calculating the eigenvalues of a linearised model of the nonlinear system around the equilibrium point.

Note that we can always consider $x_e = 0$ since we can always bring the equilibrium point to the origin by a change of coordinates. In what follows, we shall effectively assume that such is the case.

**Definition 10.** Lyapunov function: A Lyapunov function for the system (A1) is a real-valued function $V(x,t)$, which possesses the following properties:

i) $V(x,t)$ is of class $C^1$ such that $V(x_e,t) = 0$.

ii) $V(x,t)$ is positive definite. In other words, there exists a nondecreasing real continuous function $\alpha$ such that $\alpha(0) = 0$ and $0 < \alpha(\|x\|) \le V(x,t)$, for all $t$ and for all $x \ne 0$ with $\alpha(\|x\|) \to \infty$ as $\|x\| \to \infty$.

iii) $\dot{V}(x,t)$ is negative definite. In other words, there exists a nondecreasing real continuous function $\gamma$ such that $\gamma(0) = 0$ and the time derivative $\dot{V}(x,t)$ of $V(x,t)$ along the trajectories of system (A1) is such that: $\dot{V}(x,t) \le -\gamma(\|x\|) < 0$ for all $t$ and for all $x \ne 0$.

iv) There exists a nondecreasing real continuous function $\beta$ such that $\beta(0) = 0$ and $V(x,t) \le \beta(\|x\|)$ for all $t$.

The following theorem shows that the existence of such a Lyapunov function is a necessary and sufficient condition for uniform asymptotic stability of system (A1).

**Theorem 1:** The origin of system (A1) is uniformly asymptotically stable if and only if system (A1) admits a Lyapunov function.

The properties on $V(x,t)$ can be weakened according to the type of stability desired. We therefore have the following corollary:

**Corollary 1.** The origin of system (A1) is:

a) stable if and only if system (A1) admits a Lyapunov function which satisfies conditions i), ii) and the following condition : iii*) $\dot{V}(x,t) \leq 0$ for all $t$ and for all $x$

b) uniformly stable if and only if system (A1) admit a Lyapunov function which satisfies conditions i), ii), iii*) and iv)

**Corollary 2:** For the autonomous system

$$\dot{x} = f(x),\ f(0) = 0$$

the asymptotic stability is guaranteed by the existence of a Lyapunov function $V(x)$ of class $C^1$, such that

1) $V(0) = 0,$

2) $V(x) > 0\ ,\ \forall x \neq 0,$

3) $V(x) \to \infty$ as $\|x\| \to \infty,$ and $\dot{V}(x) < 0\ ,\ \forall x \neq 0$

## Stability of Linear Time-Invariant (LTI) Systems

In general, the Lyapunov direct method can also be applied to linear systems, whether they are time-varying or time-invariant. However, for time-invariant systems

$$\dot{x} = Ax,\ x \in R^n \tag{A3}$$

the concept of positive and negative definite functions are readily defined in terms of quadratic functions involving positive and negative definite matrices, respectively. More precisely, the quadratic form $V(x) = x^T P x$ , where $P$ is a SPD matrix, is usually employed

as a candidate Lyapunov function. Having chosen an SPD matrix $P$, the derivative of $V(x)$ with respect to time, along the trajectories of the system (A3), is calculated to test for negative definiteness:

$$\begin{aligned}\dot{V}(x) &= x^T P\dot{x} + \dot{x}^T Px \\ &= x^T PAx + x^T A^T Px = x^T Qx\end{aligned} \tag{A4}$$

where

$$PA + A^T P = Q. \tag{A5}$$

The equation (A5) is called an algebraic Lyapunov equation. If the matrix $Q$ turns out to be negative definite with the particular choice of $P$, then the origin of system (A3) will be asymptotically stable.

Note that since the origin is the only (trivial) isolated equilibrium point of system (A3) we generally speak of the asymptotic stability of the system rather than the asymptotic stability of the origin. It is also clear that asymptotic stability of the LTI system (A3) also means global asymptotic stability of the latter since there is only one critical point.

Another interesting feature of the above LTI system is that its eigenvalues can also provide information regarding the stability of the system. Indeed, it is known that any matrix $A$ can be transformed into the Jordan form by a change of coordinates. Let $z = Sx$ be a transformation such that $SAS^{-1} = J$, where $J$ is in Jordan form. More precisely,

$$\dot{z} = S\dot{x} = SAS^{-1}z = Jz.$$

We know that the diagonal elements of $J$ are the eigenvalues of $A$. In addition, $z(t) = e^{Jt}z(0) = \sum_{i=1}^{r}\sum_{j=1}^{m_i} p_{ij}t^{j-1}e^{\lambda_i t}$ where $r$ is the number of distinct eigenvalues of $A$; $\lambda_1,\ldots,\lambda_r$; $m_i$ is the multiplicity of the eigenvalues $\lambda_i$, and $p_{ij}$ are interpolating polynomials. It is clear that $z(t) \to 0$ as $t \to \infty$ if the eigenvalues of $A$ are all negative. This is summarised in the following theorem.

**Theorem 2:** The autonomous LTI system (A3) is globally asymptotically stable if and only if all the eigenvalues of $A$ have negative real parts; that is, all the eigenvalues of $A$ lie in the left-half complex plane.

# References


[1] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44, pp. 469-472, 1997.

[2] S. Singh, The code book : the evolution of secrecy from Mary, Queen of Scots, to quantum. New York: Doubleday, 1999.

[3] D. E. Denning, Cryptography and data security. Reading: Addison- Wesley, 1982.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communication of the ACM, vol. 2, pp. 120-126, 1978.

[5] G. M. J. Pluimakers, "Authentication: A concise survey," Computer & Security, vol. 5, pp. 243-250, 1986

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644-654, 1976.

[7] T. ElGamal, "A public-key cryptosystem and signature scheme based on discrete algorithms," IEEE Transactions on Information Theory vol. 31, pp. 469-472, 1985.

[8] D. Davies, "A Brief History of Cryptography," Information Security Technical Report, vol. 2, pp. 14-17, 1997.

[9] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Technical Report 212, vol. 212, 1979.

[10] H. C. Williams, "A modification of the RSA public-key encryption procedure," IEEE Transactions on Information Theory, vol. 26, pp. 726-729, 1980.

[11] T. Kean and A. Duncan, "DES key breaking, encryption and decryption on the XC6216," IEEE Symposium on FPGAs for Custom Computing Machines, vol. 15-17, pp. 310 - 311, 1998.

[12] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Transactions Information Theory, vol. 36, pp. 553-558, 1990.

[13] L. Kocarev, "Chaos-based cryptography: A brief overview," IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.

[14] G. Alvarez and S. Li, "Some Basic Cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, pp. 2129-2151, 2006.

[15] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, pp. 656-715, 1949.

[16] K. Busawon, R. Kharel, and Z. Ghassemlooy, "A new chaos-based communication scheme using observers," in Proceeding of the 6th Symposium on Communication Systems, Networks and Digital Signal Processing 2008 (CSNDSP 2008), Graz, Austria, 2008, pp. 16-20.

[17] R. Kharel, K. Busawon, and Z. Ghassemlooy, "A chaos-based communication scheme using proportional and proportional-integral observers," Iranian Journal of Electrical & Electronic Engineering, vol. 4, pp. 127-139, 2008.

[18] R. Kharel, K. Busawon, and Z. Ghassemlooy, "Novel cascaded chaotic masking for secure communications," in The 9th annual Postgraduate Symposium on the convergence of Telecommunications , Networking & Broadcasting (PGNET), Liverpool, UK, 2008, pp. 295-298.

[19] R. Kharel, K. Busawon, and Z. Ghassemlooy, "A novel chaotic encryption technique for secure communication," in 2nd IFAC conference on analysis and control of chaotic systems (Chaos 09), London, 2009.
[20] R. Kharel, K. Busawon, and Z. Ghassemlooy, "Indirect coupled oscillators for keystream generation in secure chaotic communication," in Proceedings of the 48th IEEE conference on Decision and Control and 28th Chinese Control Conference 2009, 2009.
[21] R. Kharel, K. Busawon, and Z. Ghassemlooy, "Secure digital communication using discrete-time chaotic systems via indirect coupling synchronization " in American Control Conference (ACC'10), Baltimore, Maryland, USA, 2010.
[22] R. Kharel, K. Busawon, and Z. Ghassemlooy, "Modified chaotic shift keying using indirect coupled chaotic synchronization for secure digital communication," in 3rd Chaotic Modeling and Simulation International Conference (Chaos2010), Chania, Greece, 2010.
[23] R. Kharel and K. Busawon, "Indirectly coupled synchronization of chaotic systems: Application to secure digital communications," in 28th International Colloquium on Group - Theoretical Methods in Physics, Group 28, Newcastle Upon Tyne, UK, 2010.
[24] R. Kharel, S. Rajbhandari, K. Busawon, and Z. Ghassemlooy, "Digitization of chaotic signal for reliable communication in non-ideal channels," in Proceeding of *International Conference on Transparent Optical Networks 'Mediterranean Winter'' (ICTON*-MW'08), Marrakech, Morocco, 2008 pp. Sa1.2 (1-6) - Invited Plenary Paper.
[25] R. Kharel, K. Busawon, W. Aggoune, and Z. Ghassemlooy, "Implementation of a secure digital chaotic communication scheme on a DSP board " in 7th IEEE, IET International Symposium on COMMUNICATION SYSTEMS, NETWORKS AND DIGITAL SIGNAL PROCESSING (CSNDSP'10), Newcastle Upon Tyne, UK, 2010.
[26] S. H. Strogatz, Non linear dynamics and chaos: Preseus Books Publishing, LLC, 1994.
[27] J. Gleick, Chaos: Making a New Science: Viking, New York, 1987.
[28] E. N. Lorenz, "Determistic nonperiodic flow," Journal of the Atmospheric Sciences, vol. 20, pp. 130-141, 1963.
[29] R. M. May, "Simple mathematical models with very complicated dynamics," Nature, vol. 261, pp. 459 - 467, 1976.
[30] O. E. Rossler, "An equation for continuous chaos," Physics Letters A, vol. 57, pp. 397-398, 1976.
[31] B. Pierre, P. Yves, and V. Christian, Order within Chaos: Wiley-Interscience, 1987.
[32] H. G. Schuster, Deterministic Chaos: An Introduction: John Wiley & Sons Ltd, 1995.
[33] Y. Pomeau and P. Manneville, "Intermittent transition to turbulence in dissipative dynamical systems," Communications in Mathematical Physics, vol. 74, pp. 189-197, 1980.
[34] P. Cvitanovic, Universality in Chaos: Taylor & Francis, 1989.
[35] T. Matsumoto, "A Chaotic Attractor from Chua's Circuit," IEEE Transactions on Circuits and Systems, vol. CAS-31, pp. 1055-1058, 1984.
[36] L. O. Chua, T. Matsumoto, and M. Komuro, "The double scroll," IEEE Transactions on Circuits and Systems, vol. CAS-32, 1985.
[37] P. Holmes, "A nonlinear oscillator with a strange attractor," Philosophical Transactions of the Royal Society A, vol. 292, pp. 419-448, 1979.

[38] M. Henon, "A two-dimensional mapping with a strange attractor," Communications in Mathematical Physics, vol. 50, pp. 69-77, 1976.
[39] D. L. Hitzl and F. Zele, "An exploration of the Hénon quadratic map," Physica D, vol. 14, pp. 305-326, 1985.
[40] H.-L. An and Y. Chen, "The function cascade synchronization scheme for discrete-time hyperchaotic systems," Communication Nonlinear Science Numerical Simulation, vol. 14, pp. 1494-1501, 2009.
[41] J. C. Sprott, Chaos and Time-Series Analysis: Oxford University Press, 2003.
[42] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., vol. 64, pp. 821-824, 1990.
[43] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 38, pp. 453-456, 1991.
[44] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," Phys. Rev. A., vol. 44, pp. 2374-2383, 1991.
[45] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou, "The synchronization of chaotic systems," Physics Reports, vol. 366, pp. 1-101, 2002.
[46] R. He and P. G. Vaidya, "Analysis and synthesis of synchronous periodic and chaotic systems," Phys. Rev. A, vol. 46, pp. 7387-7392, 1992.
[47] T. Kapitaniak, "Synchronization of chaos using continuous control," Phys. Rev. E, vol. 50, pp. 1642-1644, 1994.
[48] R. E. Amritkar and N. Gupte, "Synchronization of chaotic orbits: The effect of a finite time step," Phys. Rev. E, vol. 47, pp. 3889-3895 1993.
[49] L. Kocarev and U. Parlitz, "General Approach for Chaotic Synchronization with Applications to Communication," Phys. Rev. Lett., vol. 74, pp. 5028-5031, 1995.
[50] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, "Encoding messages using chaotic synchronization " Phys. Rev. E, vol. 53, pp. 4351 - 4361, 1996.
[51] J. Guemez, C. Martín, and M. A. Matias, "Approach to the chaotic synchronized state of some driving methods," Phys. Rev. E, vol. 55, pp. 124-134, 1997.
[52] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," IEEE Transactions on Circuits and Systems - I: Fundamental thoery and applications, vol. 44, pp. 882-890, 1997.
[53] O. Morgul and E. Solak, "Observer based snchronization of chaotic systems," Physical Review E, vol. 54, pp. 4803-4811, 1996.
[54] M. L'Hernault, J.-P. Barbot, and A. Ouslimani, "Feasibility of analog realization of a Sliding-Mode Observer: Application to Data Transmission," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 55, pp. 614-624, 2008.
[55] J. P. Barbot, M. Djemai, and T. Boukhobza, "Sliding mode observers," in Sliding mode control in engineering: Marcel Dekker, 2002, pp. 103-130.
[56] H. J. C. Huiberts, T. Lilge, and H. Nijmeijer, "Nonlinear discrete-time synchronisation via extended observers," International Journal of Bifurcation and Chaos, vol. 11, pp. 1997-2001, 2001.
[57] O. Morgul, "Necessary condition for observer-based chaos synchronization," Phys. Rev. Lett., vol. 82, pp. 169-176, 1999.
[58] S. S. Yang and C. K. Duan, "Generalized synchronization in chaotic systems," Chaos, Solitons & Fractals, vol. 9, pp. 1703-1707, 1998.
[59] Y.-W. Wang and Z.-H. Guan, "Generalized synchronization of continuous chaotic system " Chaos, Solitons & Fractals, vol. 27, pp. 97-101, 2006.

[60] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," Phys. Rev. E, vol. 51, pp. 980-994, 1995.
[61] L. Kocarev and U. Parlitz2, "Generalized synchronization, predictability, and equivalence of unidirectionally coupled dynamical systems," Phys. Rev. Lett., vol. 76, pp. 1816-1819, 1996.
[62] R. Mainieri and J. Rehacek, "Projective synchronization in three-dimensional chaotic systems," Phys Rev Lett, vol. 82, pp. 3042–3045, 1999.
[63] Z. Li and D. Xu, "A secure communication scheme using projective chaos synchronization," Chaos, Solitons & Fractals, vol. 22, pp. 477-481, 2004.
[64] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "Phase synchronization of chaotic oscillators," Phys. Rev. Lett, vol. 76, pp. 1804-1807, 1996.
[65] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "From Phase to Lag Synchronization in Coupled Chaotic Oscillators," Phys. Rev. Lett, vol. 78, pp. 4193-4196, 1997.
[66] T. Yang, "A survey of chaotic secure communication systems," International Journal of Computational Cognition, vol. 2, pp. 81-130, 2004.
[67] S. Boccaletti, A. Farini, and F. T. Arecchi, "Adaptive synchronization of chaos for secure communication," Physical Review E, vol. 55, pp. 4979-4981, 1997.
[68] X. Liang, J. Zhang, and X. Xia, "Adaptive Synchronization for Generalized Lorenz Systems," IEEE Transactions on Automatic Control, vol. 53, pp. 1740-1746, 2008.
[69] A. S. Dmitreiv, M. Hasler, A. I. Panas, and K. V. Zakharchenko, "Basic principles of direct chaotic communications," Nonlinear Phenomena in Complex Systems, vol. 1, p. 14, 2002.
[70] F. C. M. Lau and C. K. Tse, Chaos-Based Digital Communication Systems: Springer Verlag, 2003.
[71] C. Williams, "Chaotic communications over radio channels," IEEE Transactions on Circuits and Systems-I:Fundamental Theory and Applications, vol. 48, pp. 1394-1404, 2001.
[72] Z. Galias and M. Gian-Mario, "Quadrature Chaos- Shift Keying: Theory and Performance Analysis," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 48, pp. 1510-1518, 2001.
[73] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379-423, 1948.
[74] R. L. Devaney, An Introduction to Chaotic Dynamical Systems: (Addison-Wesley, Redwood City, California, USA), 1989.
[75] L. Kocarev, "Chaos-based cryptography: A brief overview," IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.
[76] M. S. Baptista, "Cryptography with chaos," Physics Letters A, vol. 240, pp. 50-54, 1998.
[77] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," Physics Letters A, vol. 298, pp. 238-242, 2002.
[78] W. Wong, L. Lee, and K. Wong, "A modified chaotic cryptographic method," Comput Phys Commun, vol. 138, pp. 234-236, 2001.
[79] K. W. Wong, "A combined chaotic cryptographic and hashing scheme," Phys Lett A, vol. 307, pp. 292-298, 2003.
[80] S. Li, G. Chen, K. W. Wong, and X. Mou, "Baptista-type chaotic cryptosystems: problems and countermeasures," Phys Lett A, vol. 332, pp. 368-375, 2004.
[81] B. Mi, X. Liao, and Y. Chen, "A novel chaotic encryption scheme based on arithmetic coding," Chaos, Solitons & Fractals, vol. 38, pp. 1523-1531, 2008.

[82] M. Hasler, "Synchronization of chaotic systems and transmission of information," International Journal of Bifurcation and Chaos, vol. 8, pp. 647-659, 1998.
[83] C. P. Silva and A. M. Young, "Introduction to chaos-based communications and signal processing," Proc. IEEE Aerospace Conference, pp. 279-299, 2000.
[84] S. Li, G. Alvarez, Z. Li, and W. A. Halang, "Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey " in International IEEE Scientific Conference on Physics and Control (PhysCon) Potsdam, Germany, 2007.
[85] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, pp. 709-713, 1992.
[86] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," International Journal of Bifurcation and Chaos, vol. 3, pp. 1619-1627, 1994.
[87] O. Morgul and M. Feki, "A chaotic masking scheme by using synchronized chaotic systems," Phys. Lett. A, vol. 251, pp. 169-176, 1999.
[88] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., vol. 71, pp. 65-68, 1993.
[89] K. M. Cuomo, A. V. Openheim, and S. H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," IEEE Trans. Circuits Syst. II, vol. 40, pp. 626-633, 1993.
[90] Q. Memon, "Synchronized chaos for network security," Comp. Comm., vol. 26, pp. 498-505, 2003.
[91] K. M. Short, "Steps toward unmasking secure communications," International Journal of Bifurcation and Chaos, vol. 4, pp. 959-977, 1994.
[92] X. Huang, J. Xu, W. Huang, and Z. Lu, "Unmasking chaotic mask by a wavelet multiscale decomposition algorithm," International Journal of Bifurcation and Chaos, vol. 11, pp. 561-569, 2001.
[93] G. Perez and H. A. Cerdeira, "Extracting messages masked by chaos," Phys. Rev. Lett., vol. 74, pp. 1970-1973,, 1995.
[94] T. Yang, L. B. Yang, and C. M. Yang, "Application of neural networks to unmasking chaotic secure communication," Physica D, vol. 124, pp. 248-257, 1998.
[95] T. Yang, L. B. Yang, and C. M. Yang, "Cryptanalyzing chaotic secure communication using return maps," Physics Letters A, vol. 245, pp. 495-510, 1998.
[96] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking Two Secure Communication Systems Based on Chaotic Masking," IEEE Transaction on Circuit and Systems-II: Express Briefs, vol. 51, pp. 505-506, 2004.
[97] M. Itoh, H. Murakami, and L. O. Chua, "Communication systems via chaotic modulations," IEICE Transaction Fundamentals, vol. E77-A, pp. 1000-1006, 1994.
[98] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos in Chua's circuit," International Journal of Bifurcation and Chaos, vol. 3, pp. 469-477, 1993.
[99] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, "A secure communcation scheme based on the phase synchronization of chaotic systems," Chaos, vol. 13, pp. 508-514, 2003.
[100] T. Yang and L. O. Chua, "Secure Communication via parameter modulation," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 43, pp. 817-819, 1996.

[101] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic secure communication using a spectrogram," Physics Letters A, vol. 247, pp. 105-111, 1998.
[102] K. M. Short, "Unmasking a modulated chaotic communications scheme," International Journal of Bifurcation and Chaos, vol. 6, pp. 367-375, 1996.
[103] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking parameter modulated chaotic secure communication systems," Chaos Solitons & Fractals, vol. 21, pp. 783-787, 2004.
[104] 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 Transaction on Circuit and Systems-II, vol. 40, pp. 634-642, 1993.
[105] U. Parlitz, "Transmission of digital signals by chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, pp. 973-977, 1992.
[106] T. L. Carroll and L. M. Pecora, "Using multiple attractor chaotic systems for communication," Chaos, vol. 9, pp. 445-451, 1999.
[107] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The Role of Synchronization in Digital Communications Using Chaos-part II: Chaotic Modulation and Chaotic Synchronization," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 45, pp. 1129-1140, 1998.
[108] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic switching using generalized synchronization: examples," IEEE Transactions on Circuits and Systems - I: Fundamental thoery and applications, vol. 45, pp. 1062-1067, 1998.
[109] S. Li, G. Chen, and G. Alvarez, "Return-map cryptanalysis revisited," International Journal of Bifurcation and Chaos, vol. 16, pp. 1557-1568, 2006.
[110] M. L'Hernault, J.-P. Barbot, and A. Ouslimani, "Sliding mode observer for a chaotic communication system: Experimental Results " in IFAC Conference on Analysis and Control of Chaotic Systems, 2006, pp. 411-416.
[111] J. P. Barbot, I. Belmouhoub, and L. Boutat-Baddas, "Observability bifurcations: application to cryptography," in Chaos in Automatic Control, W. Perruquetti and J. P. Barbot, Eds.: Taylor and Francis, 2005.
[112] H. Zhou and X. Ling, "Problems with the chaotic inverse system encryption approach," IEEE Trans. Circuits Syst. I, vol. 44, pp. 268-271, 1997.
[113] S. Diop and M. Fliess, "On nonlinear observability," in Proc. 1st Europ. Control Conf., Hermes, 1991, pp. 152-157.
[114] S. Diop and M. Fliess, "Nonlinear observability, identifiability and persistent trajectories," in Proc. 36th IEEE Conf. Decision Control, Brighton, 1991, pp. 714-719.
[115] J.-P. Barbot, M. Fliess, and T. Floquet, "An algebraic framework for the design of nonlinear observers with unknown inputs," in 46th IEEE Conference on Decision and Control, New Orleans, LA 2007, pp. 384-389.
[116] R. W. Brockett and M. D. Mesarovic, "The reproducibility of multivariable systems," J. Math. Anal. Appl., vol. 11, pp. 548-563, 1965.
[117] M. K. Sain and J. L. Massey, "Invertibility of linear time-invariant dynamical systems," IEEE Trans. Automat. Control, vol. 14, pp. 141-149, 1969.
[118] L. M. Silverman, "Inversion of multivariable linear systems," IEEE Trans. Automat. Control, vol. 14, pp. 270-276, 1969.
[119] A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 48, pp. 624-630, 2001.
[120] K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," Physical Review E, vol. 58, pp. 1159-1162, 1998.

[121] K. M. Short, "Signal extraction from chaotic communications," International Journal of Bifurcation and Chaos, vol. 7, pp. 1579-1597, 1997.
[122] G. Alvarez and S. Li, "Breaking network security based on synchronized chaos," Computer Communications, vol. 27, pp. 1679-1681, 2004.
[123] G. Alvarez, L. Hernández, J. Muñoz, F. Montoya, and S. Li, "Security analysis of communication system based on the synchronization of different order chaotic systems," Physics Letters A, vol. 345, pp. 245-250, 2005.
[124] G. Alvarez, S. Li, F. Montoya, M. Romera, and G. Pastor, "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," Chaos Solitons & Fractals, vol. 24, pp. 775-883, 2005.
[125] N. J. Corron and D. W. Hahs, "A new approach to communications using chaotic signals," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44, pp. 373-382, 1997.
[126] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: the inverse system approach," Proc. ISAS'95, pp. 680-683, 1995.
[127] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: The inverse system approach," Int. J. Circuit Theory Appl, vol. 24, pp. 551-579, 1996.
[128] V. Milanovic and M. E. Zaghloul, "Improved masking algorithm for chaotic communication systems," Electronics Letters, vol. 32, pp. 11-12, 1996.
[129] T. L. Liao and N. S. Huang, "An observer-based approach to chaotic synchronization with applications to secure communications," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 46, pp. 1144-1150, 1999.
[130] Z. P. Jiang, "A note on chaotic secure communication systems," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 49, pp. 92-96, 2002.
[131] M. Feki, B. Robert, G. Gelle, and M. Colas, "Secure digital communication using discrete-time chaos synchronization," Chaos, Solitons & Fractals, vol. 18, pp. 881-890, 2003.
[132] Z. Li, K. Li, C. Wen, and Y. C. Soh, "A new chaotic secure communication system," IEEE Transactions on Communications., vol. 51, pp. 1306-1312, 2003.
[133] C. Aguilar-Ibanez, M. S. Surez-Castanon, H. Sossa-Azuela, and R. Barron-Fenandez, "Synchronizing Hyperchaotic maps to encode/decode information," Computacion y Sistames, vol. 8, pp. 150-161, 2004.
[134] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," Chaos Solitons & Fractals, vol. 19, pp. 919-924, 2004.
[135] X. Wu, H. Hu, and B. Zhang, "Analyzing and improving a chaotic encryption method," Chaos Solitons & Fractals, vol. 22, pp. 367-373, 2004.
[136] D. Xu and C. Y. Chee, "Chaotic encryption with transient dynamics induced by pseudorandom switching keys," International Journal of Bifurcation and Chaos, vol. 14, pp. 3625–3631, 2004.
[137] T. Chien and T. Liao, "Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization," Chaos Solitons & Fractals, vol. 24, pp. 241-255, 2005.
[138] C. Hua, B. Yang, G. Ouyang, and X. Guan, "A new chaotic secure communication scheme," Physics Letters A, vol. 342, pp. 305-308, 2005.

[139] P. Johnson and K. Busawon, "Chaotic synchronisation for secure communication using PI-observers," in IFAC Conference on Analysis and Control of Chaotic Systems, Reims, France, 2006, pp. 205-210.
[140] P. Stavroulakis, Chaos application in telecommunication: Taylor & Francis Group, 2006.
[141] J. P. Yeh and K. L. Wu, "A simple method to synchronize chaotic systems and its application to secure communications" Mathematical & Computer Modelling, vol. 47, pp. 894-902, 2008.
[142] M. Chen and W. Min, "Unknown input observer based chaotic secure communication," Physics Letters A, vol. 372, pp. 1595-1600, 2008.
[143] K. Fallahi, R. Raoufi, and H. Khoshbin, "An application to Chen system for secure communication based on extended Kalman filter and multi-shift cipher algorithm," Communications in Nonlinear Science and Numerical Simulation, vol. 13, pp. 763-781, 2008.
[144] D. Materassi and M. Basso, "Time scaling of chaotic systems: application to Secure communications," International Journal of Bifurcation and Chaos, vol. 18, pp. 567-575, 2008.
[145] M. D. Prokhorov and V. I. Ponomarenko, "Encryption and decryption of information in chaotic communication systems governed by delay-differential equations," Chaos, Solitons & Fractals, vol. 35, pp. 871-877, 2008.
[146] F. Tang, "An adaptive synchronization strategy based on active control for demodulating message hidden in chaotic signals," Chaos, Solitons & Fractals, vol. 37, pp. 1090-1096, 2008.
[147] W. D. Chang, "Digital secure communication via chaotic systems," Digital Signal Processing, vol. 19, pp. 693-699, 2009.
[148] C. H. Hyun, C. W. Park, J. H. Kim, and M. Park, "Synchronization and secure communication of chaotic systems via robust adaptive high-gain fuzzy observer," Chaos, Solitons & Fractals, vol. 40, pp. 2200-2209, 2009.
[149] X. Y. Wang and M. J. Wang, "A chaotic secure communication scheme based on observer," Communications in Nonlinear Science and Numerical Simulation, vol. 14, pp. 1502-1508, 2009.
[150] X.-Y. Wang and M.-J. Wang, "A chaotic secure communication scheme based on observer," Communications in Nonlinear Science and Numerical Simulation, vol. 14, pp. 1502-1508, 2009.
[151] C. Hua, B. Yang, G. Ouyang, and X. Guan, "A new chaotic secure communication scheme," Physics Letters A, vol. 342, pp. 305-308, 2005.
[152] M. Chen, D. Zhou, and Y. Shang, "A new observer-based synchronization scheme for private communication," Chaos, Solitons and Fractals, vol. 24, pp. 1025-1030, 2005.
[153] Z.-P. Jiang, "A note on chaotic secure communication systems," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 49, pp. 92-96, 2002.
[154] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized state-space observers for chaotic synchronization and secure communication," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 49, pp. 345-349, 2002.
[155] G. Alvarez, F. Montoya, G. Pastor, and M. Romera, "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," Chaos, vol. 14, pp. 274-278, 2004.

[156] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," Phys. Rev. Lett. , vol. 74, pp. 5028-5031, 1995.
[157] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, "Synchronizing Hyperchaos with a Scalar Transmitted Signal," Phys. Rev. Lett., vol. 76, pp. 904-907, 1996.
[158] L. Kocarev, U. Parlitz, and T. Stojanovski, Phys. Lett. A, vol. 217, p. 280, 1996.
[159] J. D. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," Physica D, vol. 4, pp. 366-393, 1982.
[160] B. Mensour and A. Longtin, "Synchronization of delay-differential equations with application to private communication," Phys. Lett. A, vol. 244, pp. 59-70, 1998.
[161] C. Zhou and C. H. Lai, "Extracting messages masked by chaotic signals of time-delay systems," Physical Review E, vol. 60, pp. 320-323, 1999.
[162] K. Murali, "Heterogeneous chaotic systems based cryptography," Physics Letters A, vol. 272, pp. 184-192, 2000.
[163] K. Murali, "Digital signal transmission with cascaded heterogeneous chaotic systems," Physical Review E, vol. 63, pp. 016217–23, 2001.
[164] C. Tao, G. Du, and Y. Zhang, "Decoding digital information from the cascaded heterogeneous chaotic systems," International Journal of Bifurcation and Chaos, vol. 13, pp. 1599-1608, 2003.
[165] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," Chaos, Solitons & Fractals, vol. 18, pp. 141-148, 2003.
[166] C. Y. Chee, D. Xu, and S. R. Bishop, "A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation," Chaos Solitons & Fractals, vol. 21, pp. 1129-1134, 2004.
[167] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value," Chaos, Solitons & Fractals, vol. 23, pp. 1749-1756, 2005.
[168] S. Li, G. Alvarez, and G. Chen, "Breaking a choas-based secure scheme designed by an improved modulation method," Chaos, Solitons and Fractals, vol. 25, pp. 109-120, 2005.
[169] P. Palaniyandi and M. Lakshmanan, "Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables," International Journal of Bifurcation and Chaos, vol. 11, pp. 2031–2036, 2001.
[170] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," Phys. Rev. Lett., vol. 75, pp. 5028-5031, 1995.
[171] D. J. Sobiski and J. S. Thorp, "PDMA-1: Chaotic Communication via the Extended Kalman Filter," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 45, pp. 194-197, 1998.
[172] K. Fallahi, R. Raoufi, and H. Khoshbin, "An application of Chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm " Communications in Nonlinear Science and Numerical Simulation, vol. 13, pp. 763-781, 2008.
[173] O. Morgul, E. Solak, and M. Akgul, "Observer based chaotic message transmission," International Journal of Bifurcation and Chaos., vol. 13, pp. 1003-1017, 2003.
[174] K. Busawon and P. Kabore, "Disturbance attenuation using proportional integral observers," International Journal of Control, vol. 74, pp. 618-627, 2001.
[175] Y.-L. DONG and S.-W. MEI, "Adaptive observer for a class of nonlinear systems," Acta Automatica Sinica, vol. 33, pp. 1081-1084, 2007.

[176] M. R. Napolitano, C. I. Chen, and R. Nutter, "Application of a neural observer as state estimator in active vibration control of a cantilevered beam," Smart Materials and Structures, vol. 1, pp. 69-75, 1992.
[177] G. Bornard, N. Couenne, and F. Celle, "Regularly persistent observers for bilinear systems," Contr. Inform. Sci., vol. 122, pp. 130-140., 1989.
[178] J. P. Gauthier, H. Hammouri, and S. Othman, "A simple observer for nonlinear systems applications to bioreactor," IEEE Transactions on Automatic Control, vol. 37, pp. 875-879, 1992.
[179] K. Busawon and M. Saif, "A state observer of nonlinear systems," IEEE Transactions on Automatic Control, vol. 44, pp. 2098-2103, 1999.
[180] H.-L. An and Y. Chen, "The function cascade synchronization scheme for discrete-time hyperchaotic systems," Communication Nonlinear Science Numerical Simulation, vol. 14, pp. 1494-1501, 2009.
[181] S. Rajbhandari, Z. Ghassemlooy, and M. Angelova, "Effective denoising and adaptive equalization of indoor optical wireless channel with artificial light using the discrete wavelet transform and artificial neural network," IEEE Journal of Lightwave Technology, vol. 27, pp. 4493-4500, 2009.
[182] T. L. Carroll, "Noise-Robust Synchronized Chaotic Communications," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 48, pp. 1519-1522, 2001.
[183] L. O. Chua, T. Yang, G.-Q. Zhong, and C. W. Wu, "Synchronization of Chua's circuits with time-varying channels and parameters," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 43, pp. 862-868, 1996.
[184] N. Sharma and E. Ott, "Combating channel distortions in communication with chaotic systems," Physics Letters A, vol. 248, pp. 347-352, 1998.
[185] T. K. Moon, Error correction coding: Mathematical methods and algorithms. New Jersey: Wiley-Interscience, 2005.
[186] R. J. Dickenson and Z. Ghassemlooy, "Bit error rate performance of 166Mb/s OOK diffuse indoor IR link employing wavelets and neural networks," IEE Electronics Letters, vol. 40, pp. 753-755, 2004.
[187] Mathworks, "Embedded IDE Link$^{TM}$ CC 3 user's guide," 2009.
[188] T. Instrument, "TMS320c6713 floating point digital signal processor," 2005.