



Kent Academic Repository

Ahmed, Alaael-Din Rohiem Shehata (2000) *Secure computer communications and databases using chaotic encryption systems*. Doctor of Philosophy (PhD) thesis, University of Kent.

Downloaded from

<https://kar.kent.ac.uk/94646/> The University of Kent's Academic Repository KAR

The version of record is available from

<https://doi.org/10.22024/UniKent/01.02.94646>

This document version

UNSPECIFIED

DOI for this version

Licence for this version

CC BY-NC-ND (Attribution-NonCommercial-NoDerivatives)

Additional information

This thesis has been digitised by EThOS, the British Library digitisation service, for purposes of preservation and dissemination. It was uploaded to KAR on 25 April 2022 in order to hold its content and record within University of Kent systems. It is available Open Access using a Creative Commons Attribution, Non-commercial, No Derivatives (<https://creativecommons.org/licenses/by-nc-nd/4.0/>) licence so that the thesis and its author, can benefit from opportunities for increased readership and citation. This was done in line with University of Kent policies (<https://www.kent.ac.uk/is/strategy/docs/Kent%20Open%20Access%20policy.pdf>). If you ...

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in *Title of Journal*, Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

**Secure Computer Communications and
Databases using Chaotic
Encryption Systems**

By

Alaael-Din Rohiem Shehata Ahmed

A thesis submitted for the degree of

Doctor of Philosophy

at the Electronic Engineering Laboratory,

University of Kent,

Canterbury, Kent, England.

2000

PREFACE

Recently, there has been great interest in the possibility of utilising chaos in secure communication systems. Several techniques have been proposed to-date. In this thesis, many of the chaotic generators and chaotic communication systems have been studied. According to the study we found the following:

1. The chaotic masking and the chaotic modulation approaches have some difficulties. The level of the information signal must be lowered to at least 30 dB below the level of the chaotic signal. Moreover, the frequency range of the information signal is limited due to the resonance frequencies of the subsystems.
2. The physically implemented chaotic generators are based on electronic circuits but there is no method to implement those chaotic generators that are represented by the state equations rather than a circuit diagram in real time.
3. Some results on chaotic generators have been reported. However all the developed systems so far have been at low frequencies. The reason for this is that no systematic method exists for designing chaotic microwave generators and predicting their performance.
4. Most publications to-date, dealing with secure communication using chaos, use analogue physical electronic circuits and attempt to develop a real time system. Good synchronisation is very difficult as the element values cannot be controlled to the required accuracy and are functions of age, temperature and manufacturing tolerances. Nowadays most communication is through computers and real time communication systems are mostly digital. E-mail is the most used personal communication medium, especially for official communication which is the kind that will mostly need security. None of the previously published chaotic communication systems use the Internet as the communication media.
5. Most methods of attack of chaotic communication systems assume that the information signal is added to the chaotic signal after the chaotic generator. They try to attack the dynamics of the chaotic generators and then simply subtract the chaotic signal from the received signal. However this is only a special case of chaotic communication systems.

6. Until now, no methods of countering the attack to chaotic communication systems have been developed.

To eliminate these drawbacks we have developed the following:

1. A new system for the analogue chaotic communication system called the multi-channel chaotic communication system is developed. Simulation and experimental results are presented. The implementation of chaotic shift key (CSK) system using one chaotic generator instead of two chaotic generators or two nonlinear functions at the transmitter is introduced. Simulation and experimental results are given.
2. A new method for real time implementations of chaotic generators and chaotic communication systems that are represented by state equations and cannot be implemented by a physical circuit is developed. Simulation and experimental results are presented. A new representation of the Chua nonlinear function is given.
3. A new J-band microwave chaotic generator is developed. A method for systematically analysis of microwave generators is presented. Simulation and experimental results are given. The chaotic radar and the microwave chaotic communication systems are presented. A new expression for the non-linear capacitor function is given. The effects of channel delay and channel attenuation in the chaotic radar and the microwave chaotic communication systems are presented. Results of research have been presented in European microwave conference, Munich-Germany, October 1999, International Microwave Symposium, Boston, Massachusetts, June 2000 and International Microwave Workshop, France, October 2000.
4. New algorithms for encrypting and decrypting text and image files based on, Chua, Rössler and Lorenz, chaotic systems are presented. Signal to chaos ratio of -240 dB is achieved. Results of research have been published in Electronics Letters, May 2000 and International Journal of Bifurcation and Chaos, November 2000.
5. A new algorithm to attack chaotic communication systems is presented.
6. New methods of counter measures to the chaotic attacking algorithm are given.

7. Finally, A method for counter counter measures attacking the chaotic communication systems is presented.

This thesis is divided into eight chapters as follows:

Chapter 1: Chaos is first reviewed and basic features of chaos are introduced. Chaos in electronic circuits is presented. The differences between chaotic communication systems and traditional communication systems are discussed. The basic advantages of using chaotic signals in communication systems are given.

Chapter 2: the basic methods of synchronisation in chaotic communication systems are discussed. A survey of analogue chaotic communication systems, showing the advantages and the disadvantages of these systems, is introduced. A new analogue chaotic communication system called the multi-channel chaotic communication system is developed. A survey of different methods of chaos shift keying (CSK) is introduced. The one generator chaos shift keying is presented.

Chapter 3: A new method for real time implementation of chaotic systems is developed. The description of the method is presented. The real time implementations of several chaotic generators using the developed method are presented. The implementation of the multi-channel chaotic communication system in real time using the developed method is presented.

Chapter 4: A new J-band chaotic generator for radar and microwave communication systems is presented. Theoretical analysis and practical design of the chaotic generator are given. The design of the receiver part of the chaotic radar and microwave communication systems is presented. The effects of the channel attenuation and channel delay are given.

Chapter 5: We start with a survey of classical encryption algorithms and a background of chaotic encryption algorithms. New algorithms for encrypting and decrypting voice, text and image files using chaotic systems are presented. Several examples for encrypting text and image files are given. Comparison between new algorithms and classical encryption algorithms is given.

Chapter 6: We start with a general description of the system security and a background of attacking methods of chaotic communication systems. New attacking algorithm to chaotic communication systems is presented. Several results of the

algorithm in attacking continuous and discrete chaotic communication systems are given.

Chapter 7: New methods for counter measures to the chaotic attacking algorithm are presented. A method for counter counter measures of the chaotic attacker is presented.

Chapter 8: The conclusion and the future work are presented.

Acknowledgment

It is a pleasure to express my sincere gratitude to my supervisor Prof. M. I. Sobhy for his encouragement and invaluable expert guidance throughout this work. It has been a great honor and privilege to work with him.

I would like to express my sincere thanks to my parents, my wife and my children Ahmed and Mohamed. It would not have been possible to finish this work without their support

Last, but by no means least, I am grateful to all the staff of the department of electronic engineering laboratory, University of Kent, for the use of the facilities provided by the department

Alaael-Din Rohiem Shehata

To the my mother

To the soul of my father

To my wife

To my children

PUBLICATIONS

- [1]M. I. Sobhy and A. R. Shehata, "Chaotic J-band generator for microwave communications systems," *European Microwave Conference*, " Munich-Germany, October 1999.
- [2] M. I. Sobhy and A. R. Shehata, "Chaotic J-band generator for microwave communications systems," *MPD Microwave Product Digest*, pp.91-96, May 2000.
- [3]M. I. Sobhy and A. R. Shehata, "Chaotic radar systems," *International Microwave Symposium*, Boston, Massachusetts, June 2000.
- [4]M. I. Sobhy and A. R. Shehata, "Secure computer communication using chaotic algorithms," *International Journal of Bifurcation and Chaos*, will be published in November 2000.
- [5]M. I. Sobhy and A. R. Shehata, "Secure e-mail and databases using chaotic algorithms," *Electronics Letters*, vol. 36, No. 10, May 2000.
- [6]M. I. Sobhy and A. R. Shehata, "Time domain analysis of the chaotic circuits," *European Microwave Workshop*, Paris, October 2000.

TABLE OF CONTENTS

Acknowledgment	i
Preface	ii
Publications	vi
Table of contents.....	vii
List of figures	xi
List of tables	xix
Glossary of abbreviations	xx
1. Introduction	1
1.1 Introduction	1
1.2 Non-linear dynamics	2
1.3 Chaos	2
1.3.1 Bifurcation.....	6
1.3.2 Lyapunov exponents.....	7
1.3.3 Chaos in electronic circuits	8
1.4 Chaotic communication systems	8
1.5 References	11
2. Chaotic communication systems	13
2.1 Introduction	13
2.2 Chaotic synchronisation	13
2.2.1 Drive-response synchronisation	14
2.2.2 General synchronisation method	19
2.2.3 Error-feedback synchronisation	19
2.3 Analogue chaotic communication system	21
2.3.1 Chaotic masking system.....	22
2.3.2 Chaotic modulation system	23
2.3.3 Chaotic communication system based on general synchronisation approach	26
2.4 Multi-channel chaotic communication system (MCCS)	28
2.5 Digital chaotic communication systems	38
2.5.1 Chaos Shift Keying (CSK)	39

Table of contents

2.5.2 Chaotic on-off keying (COOK).....	40
2.5.3 Differential chaos shift keying modulation (DCSK).....	41
2.6 One generator CSK.....	42
2.7 Conclusion.....	50
2.8 References	52
3. Direct representaion of the chaotic state equations with realtime implementation	56
3.1 Introduction	56
3.2 Real time system description.....	57
3.2.1 Software description.....	57
3.2.1.1 <i>MATLAB</i>	57
3.2.1.2 <i>SIMULINK</i>	58
3.2.1.3 <i>Real Time Workshop (RTW)</i>	58
3.2.1.4 <i>Real time windows target</i>	59
3.2.2 Hardware	59
3.2.3 Real time model generation.....	60
3.3 Real time chaotic generators	61
3.3.1 Continuous time chaotic generators	61
3.3.1.1 <i>Real time Chua chaotic generator</i>	61
3.3.1.2 <i>Real time Rössler chaotic generator</i>	65
3.3.1.3 <i>Real time Lorenz chaotic generator</i>	67
3.3.2 Discrete time chaos generator	70
3.3.2.1 <i>Henon map chaotic generator</i>	70
3.4 Real time chaotic communications system.....	72
3.5 Conclusion.....	77
3.6 References	78
4. Microwave chaotic systems.....	81
4.1 Introduction	81
4.2 Chaotic J-band for radar and microwave communication systems	82
4.2.1 Theoretical analysis of chaotic multipliers.....	82
4.2.2 Practical design.....	91
4.3 Chaotic radar and microwave chaotic communication systems.....	94
4.3.1 Receiver design	94
4.4 Conclusion.....	106
4.5 References	107

Table of contents

5. Secure computer communication using chaotic algorithms.....	109
5.1 Introduction	109
5.2 Background of the classical cipher algorithms.....	110
5.2.1 The data encryption standard (DES)	111
5.2.2 International Data Encryption Algorithm (IDEA)	112
5.2.3 Rivest-Shamir-Adleman (RSA) algorithm.....	113
5.2.4 El-Gamal cipher algorithm.....	114
5.3 Chaos encryption algorithms background	115
5.4 New chaotic algorithms for secure computer communication	117
5.4.1 Chaotic encryption algorithms	118
5.4.1.1 <i>The Chua encryption algorithm</i>	119
5.4.1.2 <i>The Rössler encryption algorithm</i>	124
5.4.1.3 <i>The Lorenz encryption algorithm</i>	127
5.4.2 System security.....	130
5.4.3 Results	134
5.5 Conclusion.....	149
5.6 References	150
6. Attacking chaotic encryption systems	153
6.1 Introduction	153
6.2 Chaos attacking background.....	155
6.3 New algorithm for attacking the chaotic communication systems.....	157
6.3.1 Introduction	157
6.3.2 Obtaining the upper and lower boundaries of the optimisation program	161
6.3.3 Attacking the Henon map.....	163
6.3.4 Attacking the Yamakawa chaotic communication system.....	166
6.3.5 Attacking the Van Der Pol-Duffing chaotic communication system.....	168
6.3.6 Attacking the system based on the general approach for chaotic synchronisation.....	170
6.3.7 Attacking the Chua masking chaotic communication system.....	172
6.3.8 Attacking the Rössler encryption algorithm.....	174
6.3.9 Attacking the Lorenz encryption algorithm	176
6.4 Conclusion.....	178
6.5 References	179

Table of contents

7. Counter measures to the chaotic attacking algorithm	181
7.1 Introduction	181
7.2 New methods of counter measures for the chaotic attacker	181
7.2.1 Method 1.....	181
7.2.2 Method 2.....	183
7.2.3 Method 3.....	184
7.2.4 Method 4.....	187
7.3 Counter counter measures of the chaotic attacker.....	192
7.4 Conclusion.....	193
7.5 References	194
8. Conclusion and future work	195

LIST OF FIGURES

Fig. No.	Page
Fig. 1.1 The Rössler strange attractor.....	4
Fig. 1.2 The Henon map attractor.....	4
Fig. 1.3 Frequency spectrum of the Henon map.	5
Fig. 1.4 The y state variable of the Lorenz chaotic system ⁶ at different initial conditions.	6
Fig. 1.5 Bifurcation diagram of the logistic map.	7
Fig. 2.1 Block diagram of the drive system.	14
Fig. 2.2 Pecora-Carroll decomposition into two subsystems.	15
Fig. 2.3 The response system is a copy of the second subsystem in the drive system.	15
Fig. 2.4 Recovery of $g(t)$ in a Pecora-Carroll cascaded drive-response configuration.	16
Fig. 2.5 Chua's circuit diagram.	17
Fig. 2.6 Drive system using Chua's circuit to produce chaotic signal $g(t)$	17
Fig. 2.7 Recovery of $g(t)$ from $r(t)$ using Chua's circuit in a Pecora-Carroll cascaded drive-response configuration.	18
Fig. 2.8 Error-feedback synchronisation.	20
Fig. 2.9 Error-feedback synchronisation in Chua's circuit	21
Fig. 2.10 Chaotic masking system.....	22
Fig. 2.11 Simulation results of the Lorenz masking system.	23
Fig. 2.12 Communication modulation system using Chua's circuit.	25
Fig. 2.13 Simulation results of the chaotic modulation system.....	25

List of figures

Fig. 2.14 Simulation results of the chaotic communication system based on the general approach of synchronisation.	27
Fig. 2.15 Block diagram of multi-channel chaotic communication system.	29
Fig. 2.16 Signal flow representation of multi-channel chaotic communication system.	30
Fig. 2.17 MATLAB results of the MCCA system.	31
Fig. 2.18 Schematic diagram of the multi-channel chaotic communication system.	32
Fig. 2.19 The results of multi-channel chaotic communication system in the case of a square-wave with amplitude 10 mV and a frequency of 1 kHz.	34
Fig. 2.20 The results of multi-channel chaotic communication system in the case of a saw-tooth signal with amplitude 50 mV and a frequency of 2.5 kHz.	34
Fig. 2.21 The results of the multi-channel chaotic communication system in the case of a sine wave with amplitude 100 mV and a frequency of 3 kHz.	35
Fig. 2.22 X-Y plot of $v_{C_2}(t)$ of the transmitter and the receiver.	36
Fig. 2.23 Experimental results in the case of saw-tooth signal with amplitude 200 mV and frequency of 512 Hz. The upper trace is the recovered signal and the lower trace is the transmitted signal.	36
Fig. 2.24 Experimental results in the case of square wave signal with amplitude 500 mV and frequency of 1.0 kHz. Upper trace is recovered signal and lower trace is transmitted signal.	37
Fig. 2.25 Experimental results in the case of sinusoidal signal with amplitude 1.0 V and frequency of 2.5 kHz. Upper trace is recovered signal and lower trace is transmitted signal.	37
Fig. 2.26 Transmission using chaotic switching.	40
Fig. 2.27 Block diagram of the non-coherent COOK modulation scheme.	41
Fig. 2.28 The block diagram of DCSK.	42
Fig. 2.29 Block diagram of the CSK using one chaos generator.	43

List of figures

Fig. 2.30 Signal flow of one channel CSK.....	44
Fig. 2.31 Simulation results of the one generator CSK.....	44
Fig. 2.32 Simplified circuit diagram of the one generator CSK.....	45
Fig. 2.33 Circuit diagram of the subtractor.	46
Fig. 2.34 Circuit diagram of the absolute value calculation.....	46
Fig. 2.35 Low-pass filter circuit diagram.	47
Fig. 2.36 Comparator circuit diagram.	47
Fig. 2.37 The voltage across the capacitor C_1 and the current through the inductor L	48
Fig. 2.38 Transmitted and input signals	48
Fig. 2.39 Receiver output signal.....	49
Fig. 2.40 Absolute value of the receiver output signal and the recovered signal.....	49
Fig. 3.1 Block diagram of the real time system.....	57
Fig. 3.2 Nonlinear characteristic of Chua diode.....	62
Fig. 3.3 Real time Chua chaotic generator.	63
Fig. 3.4 Simulation results of the Chua chaotic generator.	63
Fig. 3.5 Measured capacitor voltage v_{c_1}	64
Fig. 3.6 Measured capacitor voltage v_{c_2}	64
Fig. 3.7 Measured current through the inductor L	64
Fig. 3.8 Real time Rössler chaotic generator.....	65
Fig. 3.9 Simulation results of Rössler chaos generator	66
Fig. 3.10 Measured x state variable of real time Rössler generator.	66
Fig. 3.11 Measured y state variable of real time Rössler chaotic generator.....	66
Fig. 3.12 Measured z state variable of real time Rössler chaotic generator.	67

List of figures

Fig. 3.13 Real time Lorenz chaotic generator.	68
Fig. 3.14 Simulation results of the Lorenz chaotic generator.	68
Fig. 3.15 Measured u state variable of the real time Lorenz chaos generator.....	69
Fig. 3.16 Measured v state variable of the real time Lorenz chaos generator	69
Fig. 3.17 Measured w state variable of the real time Lorenz chaotic generator.....	69
Fig. 3.18 Real time Henon map chaotic generator.	70
Fig. 3.19 Simulation results of the Henon map.	71
Fig. 3.20 Measured $x(n)$ state variable.	71
Fig. 3.21 Measured $y(n)$ state variable.	71
Fig. 3.22 Block diagram of real time chaotic communications system.....	72
Fig. 3.23 Block diagram of the multi-channel chaotic communication system using the developed method.....	74
Fig. 3.24 Measured (a) Synchronisation signal.	75
(b) Transmitted signal.	75
Fig. 3.25 Measured input signal.	75
Fig. 3.26 Measured recovered signal.....	75
Fig. 4.1 (a) Tripler circuit diagram.....	83
(b) Tripler with varactor equivalent circuit.	83
Fig. 4.2 Non-linear capacitor characteristic.	84
Fig. 4.3 Signal-flow representation of the state equation.....	86
Fig. 4.4 Simulation results of the input signal in time and frequency domains.	88
Fig. 4.5 Simulation results of the tripler output in time and frequency domains.	88
Fig. 4.6 Chaotic behaviour in time and frequency domains.....	90
Fig. 4.7 Attractor of the chaos signal.	90
Fig. 4.8 Block diagram of chaotic generator.	91

List of figures

Fig. 4.9 Physical circuit of the J-band chaotic generator.	91
Fig. 4.10 Block diagram of the testing bench of the microwave chaotic generator ...	92
Fig. 4.11 Measured chaotic signal in time and frequency domains.	93
Fig. 4.12 Attractor of the measured chaotic signal.....	93
Fig. 4.13 Simplified block diagram of the microwave chaotic communication system.	95
Fig. 4.14 Circuit diagram of the tripler chaotic generator.....	95
Fig. 4.15 Signal flow diagram of the inverse system.	97
Fig. 4.16 Characteristic of the inverse non-linear capacitor.....	98
Fig. 4.17 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.	99
Fig. 4.18 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains.....	99
Fig. 4.19 Non-linear capacitor characteristic.	100
Fig. 4.20 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.	101
Fig. 4.21 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains.....	102
Fig. 4.22 Inverse system non-linear function characteristic.....	103
Fig. 4.23 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.	103
Fig. 4.24 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains.....	104
Fig. 4.25 Effect of channel attenuation and delay in the radar system.....	104
Fig. 4.26 Effect of channel delay and attenuation in the microwave chaotic communication system.	105
Fig. 4.27 Effect of the loss a part of the received signal.	105

List of figures

Fig. 5.1 Block diagram of the IDEA algorithm.....	113
Fig. 5.2 Block diagram of the chaotic cryptosystem.....	116
Fig. 5.3 The Chua encryption algorithm.	122
Fig. 5.4 The Chua decryption algorithm.	123
Fig. 5.5 The Rössler encryption algorithm.....	125
Fig. 5.6 The Rössler encryption algorithm.....	126
Fig. 5.7 The Lorenz encryption algorithm.....	128
Fig. 5.8 The Lorenz encryption algorithm.....	129
Fig. 5.9 Results of the system simulation for a square, a saw-tooth and a speech signals.....	131
Fig. 5.10 Comparison in time and frequency domains between the information and the chaotic signals.	132
Fig. 5.11 Effect of subtracting the chaos from the ciphertext without and with a random number as the first byte.....	133
Fig. 5.12 Example of encrypting and decrypting of a text file using method 1.....	139
Fig. 5.13 Example of encrypting and decrypting a text file using method2.	140
Fig. 5.14 Encryption and decryption of the image file (flowers.tif) using Chua encryption algorithm.	141
Fig. 5.15 Input, transmitted and recovered signals in the time and the frequency domains.	142
Fig. 5.16 Encryption and decryption of the image file (saturn.tif) using Rössler encryption algorithm.	143
Fig. 5.17 Input, transmitted and recovered signals in the time and the frequency domains.	144
Fig. 5.18 Encryption and decryption of the image file (cameraman.tif) using Lorenz encryption algorithm.	145

List of figures

Fig. 5.19 Input, transmitted and recovered signals in the time and the frequency domains.	146
Fig. 5.20 Effect of changing the signal to chaos ratio.	147
Fig. 6.1 Examples of the continuous time chaotic systems attractors (the upper traces are for Chua and the lower for Rössler systems).....	159
Fig. 6.2 Examples of the continuous time chaotic systems attractors.	159
Fig. 6.3 Examples of discrete time chaotic systems attractors.	160
Fig. 6.4 The flow chart of the attacking algorithm.....	161
Fig. 6.5 Bifurcation diagram of the Lorenz system (a parameter and y state variable).	162
Fig. 6.6 Bifurcation diagram of the Lorenz system (b parameter and y state variable).	162
Fig. 6.7 Bifurcation diagram of the Lorenz system (c parameter and y state variable).	163
Fig. 6.8 Block diagram of the Henon chaotic communication system.....	164
Fig. 6.9 Attacker results of the Henon map.....	165
Fig. 6.10 Attacker results of Yamakawa's chaotic communication system.	167
Fig. 6.11 Attacker results of the Van Der Pol-Duffing chaotic communication system.	169
Fig. 6.12 Attacker results of the general approach for chaotic synchronisation.	171
Fig. 6.13 Attacker results of the Chua masking chaotic communication system.....	173
Fig. 6.14 Attacker results of the Rössler encryption system.	175
Fig. 6.15 Attacker results of the Lorenz encryption system.....	177
Fig. 7.1 Output signals and attractors of the Chua chaotic system.....	182
Fig. 7.2 Rössler chaotic output signals and attractors.	183
Fig. 7.3 The multi-system algorithm block diagram	184

List of figures

Fig. 7.4 The output signals of the multi-system algorithm.	185
Fig. 7.5 Example of encrypting and decrypting a text file using multi-system algorithm	186
Fig. 7.6 Signal flow diagram of the multi-system encryption algorithm.	188
Fig. 7.7 Signal flow diagram of the multi-system decryption algorithm.	189
Fig. 7.8 The output signals in each part of the algorithm.....	190
Fig. 7.9 Example of encrypting a text file using multi-system encryption algorithm with feedback.	191
Fig. 7.10 Symbol by symbol attacker results.	192

LIST OF TABLES

Table No.	Page
Table 2.1 Components list of the multi-channel chaotic communication system.....	33
Table 3.1 Component list of piecewise linear Chua chaotic generator.	61
Table 4.1 Tripler circuit elements values.	87
Table.4.2 Chaotic circuit element values.	89
Table 5.1 The algorithms parameter values.	135
Table 5.2 Systems key lengths.	136
Table 5.3 File size, SCR and average time required for encrypting and decrypting the text file (A4.txt).....	136
Table 5.4 File size, SCR and time required for encrypting and decrypting the image file (Cameraman.tif).	137
Table 5.5 Comparison between the first and second methods of the developed encryption algorithms.....	138
Table 5.6 Comparison between the developed chaotic encryption algorithms and the classical encryption algorithms	148
Table 6.1 Encrypter keys, attacker initial values and attacker resultant keys.	165
Table 6.2 Encrypter keys, attacker initial values and attacker resultant keys.....	167
Table 6.3 Encrypter keys, attacker initial values and attacker resultant keys.	169
Table 6.4 Encrypter keys, attacker initial values and attacker resultant keys.	171
Table 6.5 Encrypter keys, attacker initial values and attacker resultant keys.	173
Table 6.6 Encrypter keys, attacker initial values and attacker resultant keys.	175
Table 6.7 Encrypter keys, attacker initial values and attacker resultant keys.	177

GLOSSARY OF ABBRIVIATIONS

- CDMA...**Code division multiple access.
- DS/CDMA...**Direct sequences code division multiple access.
- SNR...**Signal to noise ratio.
- SCR...**Signal to chaos ratio.
- BER...**Bit error rate.
- MCCS...**Multi-channel chaotic communication system.
- OCMS...**One channel making systems.
- CSK...**Chaos shift key.
- COOK...**Chaotic on-off keying.
- DCSK...**Differential chaos shift keying.
- FPGA...**Field programming gate array.
- VLSI...**Very large scale integration.
- DSP...**Digital signal processor.
- GUI...**Graphical user interface.
- LPF...**Low pass filter.
- DES...**Data encryption standard.
- IDEA...**International data encryption algorithm.
- RSA...**Rivest-Shamir-Adleman.
- AM...**Amplitude modulation.
- IP...**Initial permutation.
- IP⁻¹...**The inverse of the initial permutation.
- ODE...**Ordinary differential equation.
- NLD...**Nonlinear dynamics.

Glossary of abbreviations

LAN...Local area network.

WLAN...Wireless local area network.

Chapter 1

INTRODUCTION

1.1 Introduction

Until only recently, the field of non-linear dynamics has remained within the confines of academia and has found limited practical application to engineering problems. However, this situation is changing. The advent of powerful computing tools make the complex numerical simulation of non-linear phenomena possible. In this chapter we will provide a top-level introduction and surveys of non-linear dynamics, especially the phenomena of chaos and we will touch upon the application of chaos in communication systems. The applications presented here will focus on the utilisation of chaos for private and secure communications and introduce techniques that could compete and replace traditional approaches. In particular, such designs seek to maximise information density, be immune to natural and artificial interference or ensure that the message sent will be received or understood by only the authorised listener. The following list enumerates the applications that have been demonstrated for chaos. Employing the natural pseudo-randomness of chaotic behaviour from non-linear maps, several chaotic key generators have been formulated in traditional digital cryptographic and spread spectrum systems [1]. The chaotic maps have been used as a basis for data and image encryption [2]. The idea here is that a simple non-linear map can give rise to very complicated behaviour in only a few iterations. If the process is reversible, then encryption and decryption can be accomplished. The security of the scheme is embedded in the nature of the map and its parameters. A whole series of base-band communication links have been demonstrated based on various forms of chaotic synchronisation and modulation that have been developed. Chaotic communication systems range from simple additive masking to indirect parameter modulation that could offer enhanced message privacy and security.

1.2 Non-linear dynamics

A dynamical system is said to be linear or non-linear depending on whether the superposition rule holds. That is, does the sum of responses to individual stimuli (inputs or initial conditions) equal the single response to the sum of the stimuli?

The field of non-linear dynamics concerns the study of systems whose internal parameters (called **states**) obey a set of temporal rules. These states describe the behaviour of the system completely. The state equations relate the future states to the past states. The non-linear dynamics are divided into three sub-disciplines, namely [3]:

1. Applied dynamics, which concerns the modelling process that transforms actual system observations into an idealised mathematical dynamical system. Usually sets of difference, ordinary differential or partial differential equations are used to model the system.
2. Mathematical dynamics, which primarily focuses on the quantitative analysis of the dynamical system models.
3. Experimental dynamics, which ranges from controlled laboratory experiments to the numerical simulation of state equations.

The state of temporal behaviour is either viewed as a traditional **time series** (i.e. giving system states versus time) or in a **phase space** perspective where the n system states are plotted against each other in the n -dimensional space with the time as implicit parameter. There are several effects of non-linear dynamical systems and one of the most well known and potentially useful non-linear dynamical effects is called **chaos** [4].

1.3 Chaos

Chaos has been found to occur in a great number of dynamical systems and in frequency ranges from base-band to optical band. The Chaos is the generation of random, unpredictable, behaviour from a simple but non-linear rule. It is neither harmonic nor random. The chaos generator is differing from the noise generator in that the present state of the system depends on the previous state. A chaotic signal

can be identified in different domains such as time and frequency domains, phase plane and correlation function.

The chaotic system is characterised by the following criteria [5]:

1. They are deterministic but non-periodic. A deterministic system can be specified by a set of differential equations (continuous time system) or by a set of difference equations (discrete time system). The chaotic signal is characterised by stretching and folding properties [6]. The stretching and folding implies that there will be some strong non-linearity in the system. If instead of plotting the steady states of the system against time we plot them against each other, we get the **attractor** of the system. The attractor of the chaotic system gives the possible values of the steady states of the system. Classical attractors are equilibrium points, periodic and quasi-periodic cycles. The attractor of a chaotic system does not settle to one of these but explores all of the state space on the attractor for all time without ever repeating. That is, it does not return to some previously visited point in state space. The attractor of a chaotic system is called the **strange attractor**. In continuous time systems, for these conditions to be true the system must have a minimum of three independent functions or two independent functions plus some forcing function. Fig. 1.1 shows the strange attractor of the Rössler system [7] as an example of continuous time systems. Fig. 1.2 illustrates the strange attractor of the Henon map [8] as an example of discrete time systems.

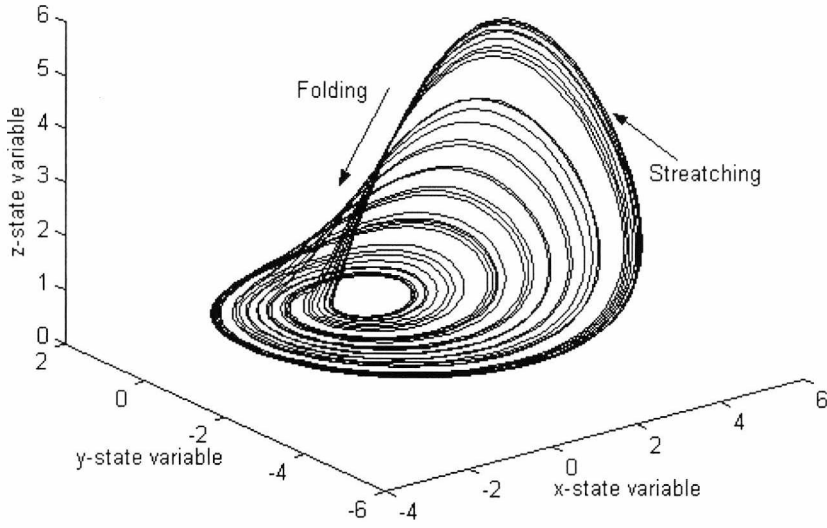


Fig. 1.1 The Rössler strange attractor.

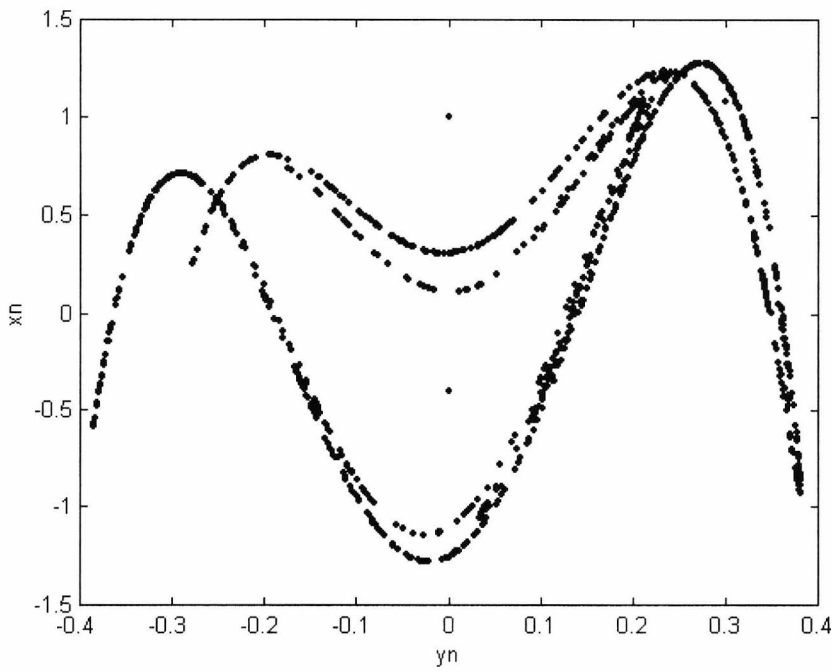


Fig. 1.2 The Henon map attractor.

2. Chaotic systems have a broadband continuous frequency spectrum. The spectrum resembles random noise (many frequencies are excited). The output from a chaotic system sounds "noisy" to the ear. Fig. 1.3 shows the frequency spectrum of the state variable $y(n)$ of the Henon map.

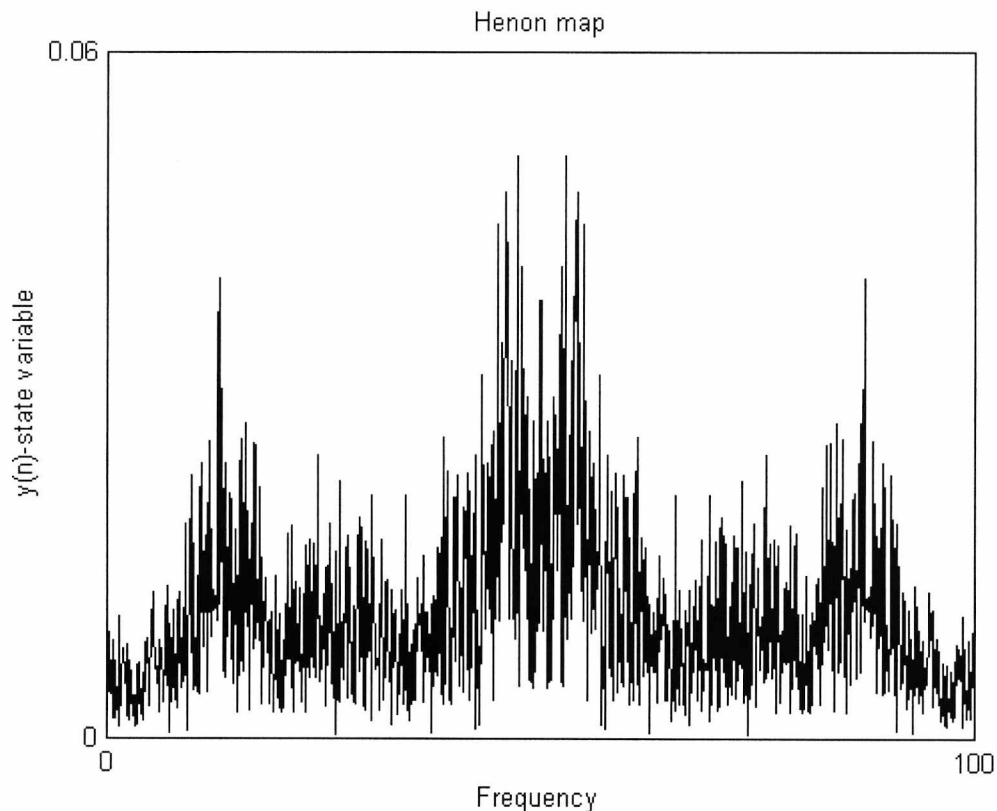


Fig. 1.3 Frequency spectrum of the Henon map.

3. Chaotic systems are sensitive to initial conditions. That is, nearby orbits diverge very rapidly. The third order chaotic system (Lorenz system [9]) is used to illustrate this property. The y state variable is used for the demonstration. A slight change in the initial conditions of the y state variable (y_0) leads quickly to very different orbital futures. In this case, two different initial conditions are set for the state variable y ($y_0 = 0.0$ and 0.01). The initial conditions of the state variables x and z are fixed ($x_0 = 10, z_0 = 30$). Fig. 1.4 illustrates that the state variable y at the two initial conditions starts and stays the same for a short period and differs as time increases.

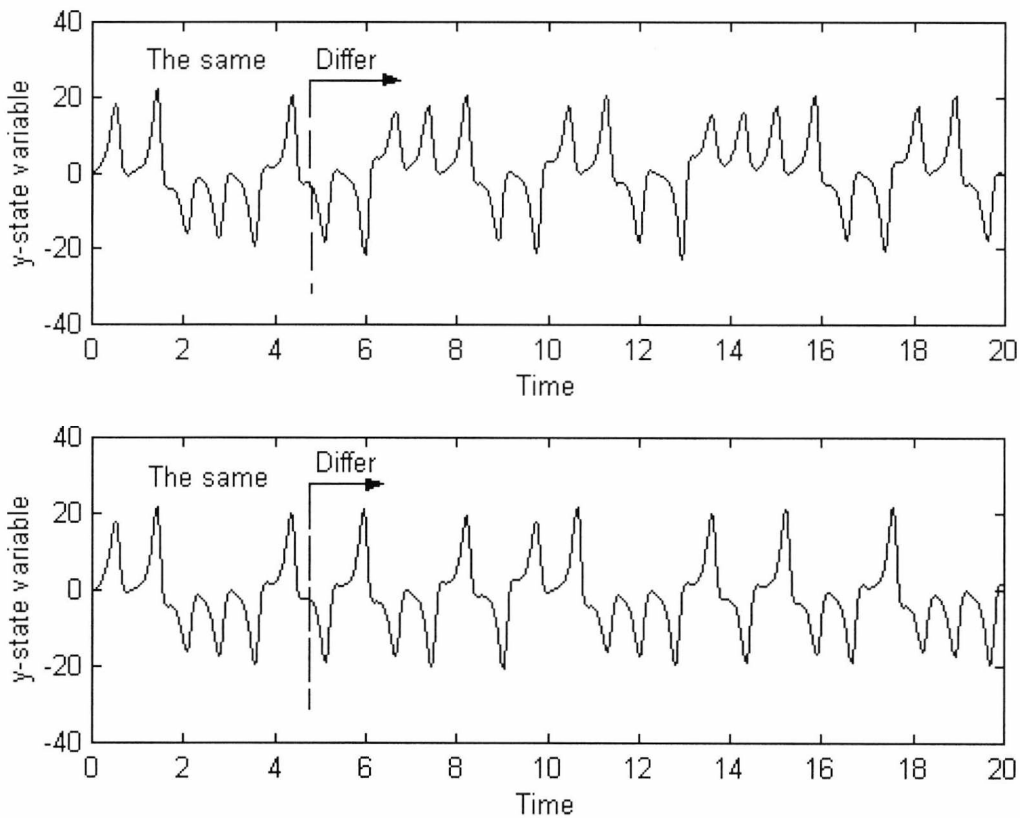


Fig. 1.4 The y state variable of the Lorenz chaotic system at different initial conditions.

4. Chaotic signals rapidly decorrelate with themselves. The auto-correlation function of a chaotic signal has a large peak at zero and decays rapidly. Thus, while chaotic systems share many of the properties of stochastic processes. They also possess a deterministic structure which makes it possible to generate "noise like" chaotic signal in a theoretically reproducible manner.

1.3.1 Bifurcation

The word bifurcation means split into two [10]. In fact, the meaning is extended to split into many parts. In mathematics, bifurcation means splitting in a certain type of graph. Bifurcation theory is important in science because the splitting in the bifurcation graph corresponds to a quantitative change in the system being described. It is used as one of the measures of the chaotic behavior of the system. As an example, the bifurcation diagram of the logistic map [11] is shown in Fig. 5.1.

The dynamics of the logistic map is described by

$$x_{n+1} = a x_n (1 - x_n) \quad (1.1)$$

where x_{n+1} is the current state variable, x_n is the previous state variable and a is a constant in the range $2 < a < 4$.

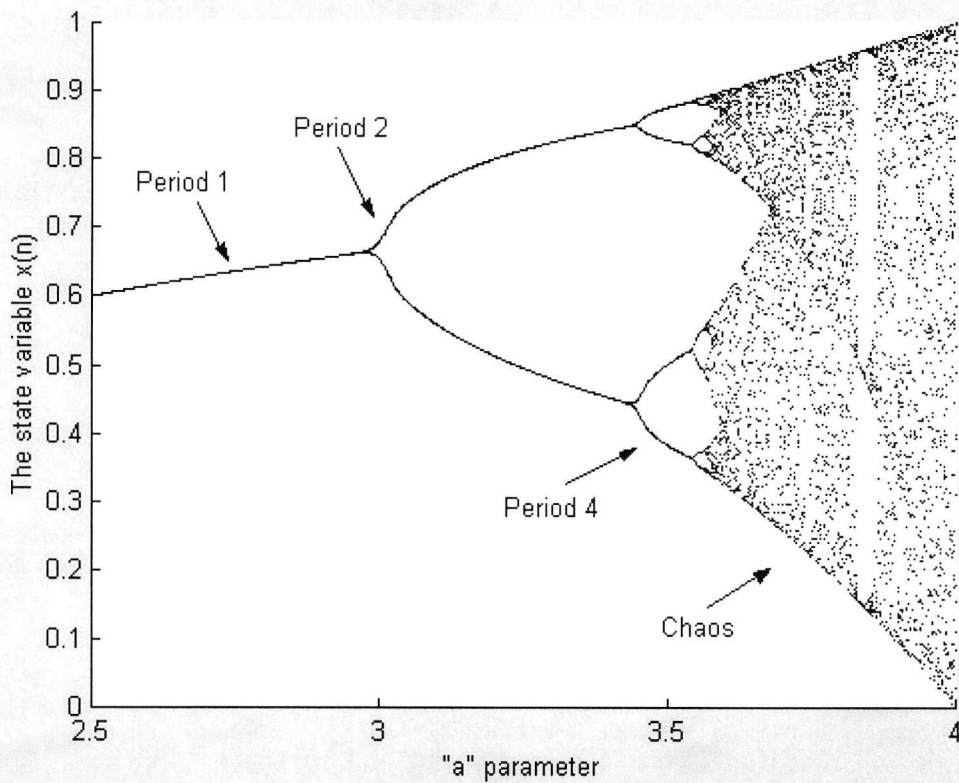


Fig. 1.5 Bifurcation diagram of the logistic map.

1.3.2 Lyapunov exponents

The Lyapunov exponent [12]-[14] is a measure of the rate at which nearby trajectories in the phase-space diverges. Chaotic orbits have at least one positive Lyapunov exponent. For periodic orbits, one of the Lyapunov exponents is zero and the other are negative. It is given in a unit of bits per data sample.

1.3.3 Chaos in electronic circuits

The electronic circuits that include non-linear elements are prone to have chaotic behaviour according to Poincaré-Bendixson theorem [15]. This theorem roughly says that, the solution of a system of two autonomous differential equations of first order converge either to a point or to a closed curve.

Kennedy [16] stated that in order to exhibit chaos an autonomous circuit consisting of resistors, capacitors and inductors must contain:

- At least one non-linear element.
- At least one locally active resistor.
- At least three energy-storage elements.

Chua's circuit [17] is the simplest electronic circuit that satisfies these criteria. The forced Van Der Pol oscillator [18] is an example of the non-autonomous circuits.

1.4 Chaotic communication systems

Chaotic communication methods will be considered into two classes. Those that possess self-synchronisation and those that do not. Self-synchronisation means using the driving signal, we can reproduce copies of the transmitter state variables at the receiver using a synchronisation scheme. latter class includes communication methods, which use chaotic signals as spreading sequences such as in the spread spectrum communication systems [19]. Communication systems using self-synchronisation are novel and potentially hold a great deal of promise [20]. The goal being a low complexity system with inherent synchronisation, modulation and security as fundamental properties of the information transmission process. A chaotic system with self-synchronisation property uses the signal's generating dynamics for synchronisation and discrimination between users.

The main differences between the conventional communication systems and the chaotic communication systems are:

1. The requirement of a broadband spreading signal independent from the information is met.
2. A secure communication may be available due to the randomness of chaos.

3. In conventional DS/CDMA (direct sequence code division multiple access) [21]-[22], accurate acquisitions and tracking depends on the signal's auto-correlation function and discrimination between users depends on the cross-correlation function.
4. A chaotic system with the self-synchronisation property uses the signal's generating dynamics for synchronisation and discrimination between users. Since the synchronisation is inherent in the chaotic system's dynamics.
5. The transmission bandwidth of the chaotic signal can be significantly wider than the information signal but a fundamental difference between the chaotic and conventional communication systems is how the extra bandwidth is used. The conventional system spreads the information over the transmission bandwidth and compresses the signal in the receiver to recover the information.
6. In a chaotic system, the information is nonlinearly mixed with the chaotic signals. The receiver synchronises to the received signal allowing the information to be recovered. This mixing gives the system its inherent security. The greater complexity of the mixing process, such as an increase in the dimensionality of the chaotic signal, means the greater security of the system.
7. Although the chaotic signal may be used to mask the message by direct superposition of the two signals, there are doubts over its security and its robustness against noise.
8. The chaotic communication system has enhanced security properties, since any mismatch in the system parameters will degrade, if not totally corrupt, the system performance.

Further potential advantages of chaotic communication system are as follows:

1. The non-linear system has a greater efficiency than the linear system from the point of view of the power consumption. Since linear systems use large control signals to determine the system output whereas non-linear devices, as a consequence of their greater sensitivity to small perturbations, can control the output signal behaviour with much smaller amounts of energy.

2. Conventional technology requires amplifications and mixing stages to prepare the signal for transmission, non-linear systems can generate the required carrier signal directly. Therefore the weight and volume are reduced.
3. There is a wide range of behaviour for chaotic signals and signals are not limited to the standard spectrum of sinusoidal frequency bands of conventional devices. The limiting factor will be the receiver's ability to distinguish between the different behaviours under operating conditions.
4. Conventional devices are limited by the power for which stable linear operation takes place. Research shows that non-linear devices could operate at much higher power levels [23].
5. The greater simplicity of chaotic communication systems using fewer components and simpler circuits would reduce manufacturing costs. This advantage is achieved when the systems are reliable for practical communication systems.
6. The probability of detection refers to the probability that a receiver will be able to detect the information bearing portion of the signal and further separate it from the chaotic signal in which it is embedded. Since non-linear devices have a rich and complex behaviour, the signal may not be decipherable without knowledge of the system and its parameters.

In this work, we deal in the applications of chaos in communication systems and how to use the chaotic signals to achieve a high degree of security. In chapter 2 a review for chaotic communication systems will be introduced and a new system developed in this work will be explained.

1.5 References

- [1] R. A. J. Matthews, "On derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, pp.29-42, 1989.
- [2] T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A secret key cryptosystem using chaotic map," *IEICE Trans. Fundamentals*, vol. E 73, pp. 1041-1044,1990.
- [3] D. Acheson, "From calculus to chaos: An introduction to dynamics," New York: Oxford University, 1997.
- [4] C. P. Silva, "A survey of chaos and its applications," *IEEE MTT-S digest*, pp. 1871-1874, 1996.
- [5] C. Williams, "Chaotic synchronisation in communication systems," Ph.D thesis, University of Bristol, 1997.
- [6] M. P. Kennedy, "Three steps to chaos -part II: A Chua's circuit primer," *IEEE Trans. Circuits Syst. I*, vol. CAS-40, No. 10, pp. 657-674, 1993.
- [7] T. Yoshinaga, H. Kitajima and H. Kawakami, "Bifurcations in a coupled Rössler system," *IEICE Trans. Fundamentals*, vol. E78-A, No. 10, pp. 1276-1279, Oct. 1995.
- [8] J. M. H. Elmirghani, "Data transmission through chaotic perturbation and associated security issues," *Proc. SPIE (special issue for chaotic circuits for communication)*, vol. 2612, pp. 76-85, Oct. 1995.
- [9] T. L. Carroll and L. M. Pecora, "Cascading synchronised chaotic systems," *Phys. wide band A. I. Mees*, "A plain man's guide to bifurcations," *IEEE Trans. D*, vol. D 67, pp. 126-140, 1993.
- [10] *Circuits Syst.*, vol. CAS-30, No. 8, pp. 512-517, 1983.
- [11] J. M. H. Elmirghani, R. A. Cryan and S. H. Milner, "Performance of a novel echo cancellation strategy based on chaotic modulated speech," *Proc. SPIE (special issue for chaotic circuits for communication)*, vol. 2612, pp. 158-169, Oct. 1995.
- [12] E. J. Kostelich, "Survey of methods for analysing chaotic experimental data," *Proc. 1 st Experimental Chaos Conference*, pp. 3-10, 1991.

- [13] A. Wrixon and M. P. Kennedy, "A MATLAB tool for calculating Lyapunov exponents from a chaotic time-series," *Proc. 3rd Int. Specialist Workshop on Non-linear Dynamics of Electronic Systems NDES'95*, pp. 205-208, 1995.
- [14] Z. Galias, "Local transversal Lyapunov exponents for analysis of synchronisation of chaotic systems," *Int. J. Circuit theory Appl.*, vol. 27, pp. 589-604, 1999.
- [15] Special issue of chaotic system, *Proc. of the IEEE*, Aug. 1987.
- [16] M. P. Kennedy, "Three steps to chaos- Part I: Evolution," *IEEE Trans. Circuits Syst. I*, vol. CAS-40, No. 10, pp. 640-656, Oct. 1993.
- [17] A. S. Elwakil and M. P. Kennedy, "Improved implementation of Chua's chaotic oscillator using current feedback Op Amp," *IEEE Trans. Circuits Syst. I*, vol. CAS-47, No. 1, pp. 76-79, Jan. 2000.
- [18] M. P. Kennedy and L. O. Chua, "Van Der Pol and chaos," *IEEE Trans. Circuits and Syst.*, vol. CAS-33, No. 10, pp. 974-980, Oct. 1986.
- [19] T. L. Carroll, "Spread-spectrum sequences from unstable periodic orbits," *IEEE Trans. Circuits Syst. I*, vol. CAS-47, No. 4, pp. 443-447, Aprl. 2000.
- [20] E. Sánchez, M. A. Matías and V. Pérez-Muñuzuri, "Chaotic synchronisation in small assemblies of driven Chua's circuits," *IEEE Trans. Circuits Syst. I*, vol. CAS-47, No. 5, pp. 644-654, May 2000.
- [21] A. J. Viterbi, *CDMA, principles of spread spectrum communication*. Woringham: Addison-Wesley Pub. Co, 1995.
- [22] F. Swarts, *CDMA techniques for third generation mobile systems*. Boston, London: Academic publisher, 1999.
- [23] M. I. Sobhy and A. R. Shehata, "Chaotic J-band generator for microwave communications systems," *European Microwave Conference*, " Munich-Germany, Oct. 1999.

Chapter 2

CHAOTIC COMMUNICATION SYSTEMS

2.1 Introduction

Chaotic systems provide a versatile technique for the generation of a very wide range of signals that can be used in the context of communication and signal processing [1]. Chaotic signals are naturally broadband and are difficult to predict. This makes them useful for use as masking and modulating waveforms in spread spectrum applications [2]. Several studies have considered the synthesis of chaotic sequences and their use in the field of communication [3]-[4]. There are two basic chaotic systems, namely, analogue chaotic communication systems and digital chaotic communication systems. In addition to these approaches based on continuous time systems, several approaches for communication with chaos in discrete time systems have been proposed [5]-[6].

The basic methods of synchronisation in chaotic communication systems are summarised in section 2.2. Section 2.3 gives a brief discussion about the basic known analogue chaotic communication methodologies. In section 2.4, a new system of analogue communication system called the multi-channel chaotic communication system is developed. Section 2.5 introduces an overview of the digital chaotic communication system. In section 2.6, a modified method of chaotic digital communication systems is presented. Section 2.7 is the conclusion of the chapter and section 2.8 is the references of the chapter.

2.2 Chaotic synchronisation

It has been reported in many studies [7]-[12] that it is possible to design synchronising systems driven by chaotic signals. Two dynamical systems are referred to as being

synchronised if the trajectories of one system converge to the same values as the other and they remain in step with each other. This is true in the case of identical synchronisation but for impulsive synchronisation is not correct [13]. Although the concepts of chaotic systems seem to defy synchronisation, since two identical chaotic systems started at nearly the same initial conditions have trajectories, which quickly become uncorrelated. Pecora and Carroll [14] have theoretically and experimentally shown that it is possible to create a chaotic system in such away that:

- A chaotic system, called the driving system, transmits one of its state variables, called the driving signal, to a second system to synchronise with the corresponding state variable.
- A necessary and sufficient condition for the synchronisation given by Pecora and Carroll is that the conditional Lyapunov exponents associated with the state equations of the response system be negative.

2.2.1 Drive-response synchronisation

In the drive-response synchronisation scheme proposed by Pecora and Carroll [7], the dynamical system (Eq. 2.1) shown in Fig. 2.1 with a scalar output $g(t) = h(x)$ is decomposed into two subsystems with states x_1 and x_2 (Eqs. 2.2 and 2.3) as illustrated in Fig. 2.2.

$$\dot{x} = f(x) \quad (2.1)$$

$$\dot{x}_1 = f_1(x_1, x_2) \quad (2.2)$$

$$\dot{x}_2 = f_2(x_2, g(t)) \quad (2.3)$$

where $x = (x_1, x_2)$ and $g(t) = h(x_1(t), x_2(t))$.

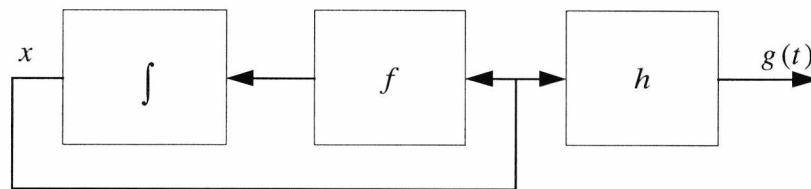


Fig. 2.1 Block diagram of the drive system.

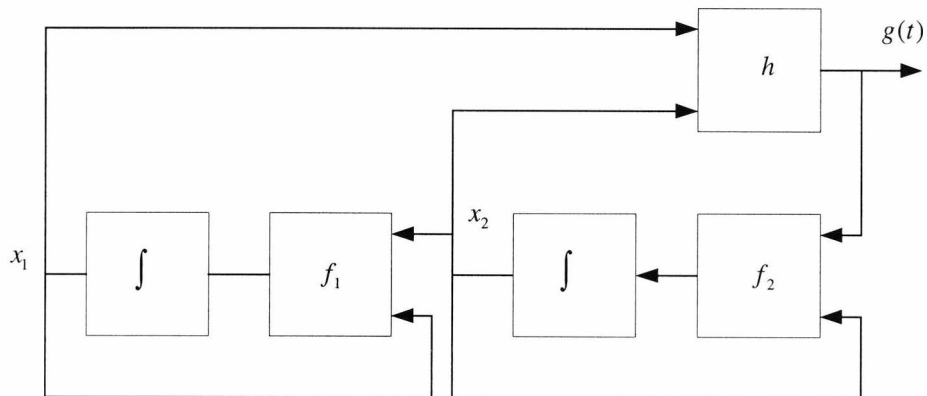


Fig. 2.2 Pecora-Carroll decomposition into two subsystems.

The system is partitioned in such a way that the conditional Lyapunov exponents of the second subsystem are negative. The conditional Lyapunov exponents characterise the stability of the second subsystem (Eq.2.3) when driven by $g(t)$. If all the conditional Lyapunov exponents are negative, the trajectory $x_2(t)$ is asymptotically stable. This means that the states of two or more copies of the second subsystem will synchronise identically when driven by the input $g(t)$.

In particular, we consider subsystem 2 shown in Fig. 2.3.

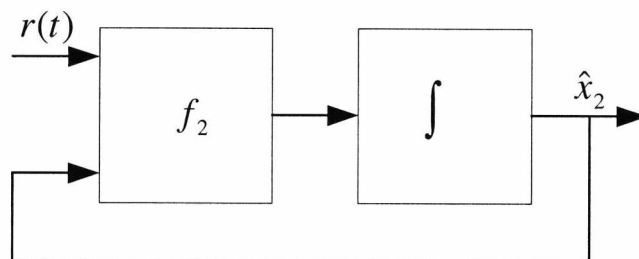


Fig. 2.3 The response system is a copy of the second subsystem in the drive system.

The system is described by

$$\dot{\hat{x}}_2 = f_2(\hat{x}_2, r(t)). \quad (2.4)$$

If the conditional Lyapunov exponents of the response system are all negative, $\hat{x}_2(0)$ is sufficiently close to $x_2(0)$ and $r(t) = g(t)$, then the state \hat{x}_2 of the response system converges asymptotically to x_2 , i.e.

$$\lim_{t \rightarrow \infty} \|\hat{x}_2(t) - x_2(t)\| = 0$$

In terms of communication systems, the drive system (Eq. 2.1) produces a chaotic signal $g(t)$, which we assume is transmitted directly through the channel and received noisy and distorted as $r(t)$. Recall that the objective of synchronisation in a coherent receiver is to estimate $g(t)$ given $r(t) \neq g(t)$. It is not sufficient to recover $x_2(t)$ but we need to recover both $x_1(t)$ and $x_2(t)$. This can be accomplished using cascaded drive-response synchronisation. The second subsystem is added which is driven by the first, as shown in Fig. 2.4.

Here,

$$\dot{\hat{x}}_2 = f_2(\hat{x}_2, r(t)) \quad (2.5)$$

$$\dot{\hat{x}}_1 = f_1(\hat{x}_1, \hat{x}_2). \quad (2.6)$$

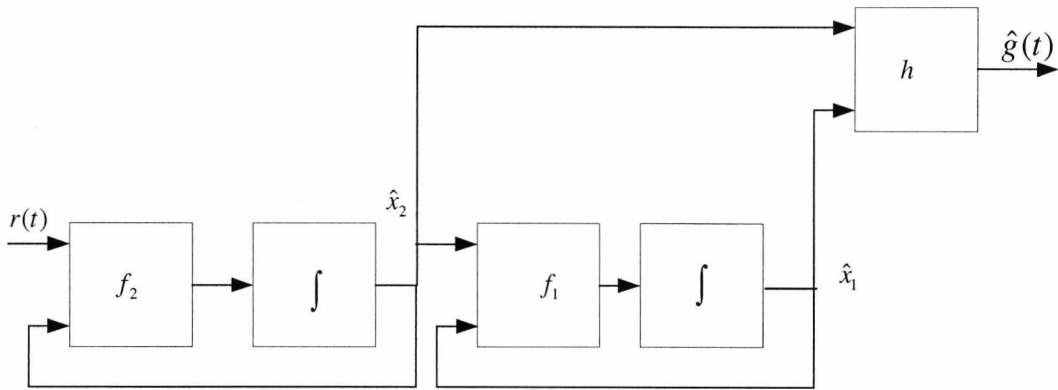


Fig. 2.4 Recovery of $g(t)$ in a Pecora-Carroll cascaded drive-response configuration.

Kolumban *et al* [15] explain this method using Chua's circuit [16] as an example. They illustrate Pecora-Carroll cascade drive response synchronisation using Chua's circuit.

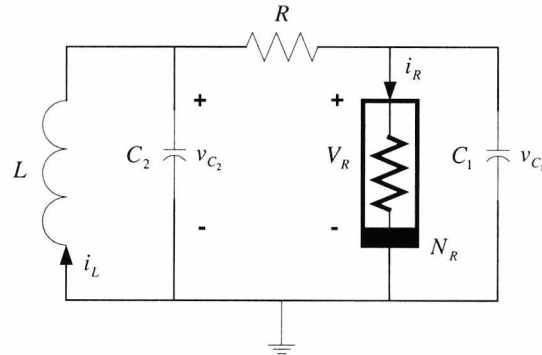


Fig. 2.5 Chua's circuit diagram.

The dynamical behaviour of the circuit is described by the three ordinary differential equations,

$$\begin{aligned} \dot{v}_{C_1} &= \frac{G}{C_1}(v_{C_2} - v_{C_1}) - \frac{1}{C_1}g(v_{C_1}) \\ \dot{v}_{C_2} &= \frac{G}{C_2}(v_{C_1} - v_{C_2}) + \frac{1}{C_2}i_L \\ \dot{i}_L &= -\frac{1}{L}v_{C_2}. \end{aligned} \quad (2.7)$$

The circuit values and the description of the non-linear function are illustrated in [14]. The circuit shown in Fig. 2.6 produces a chaotic signal $g(t)$.

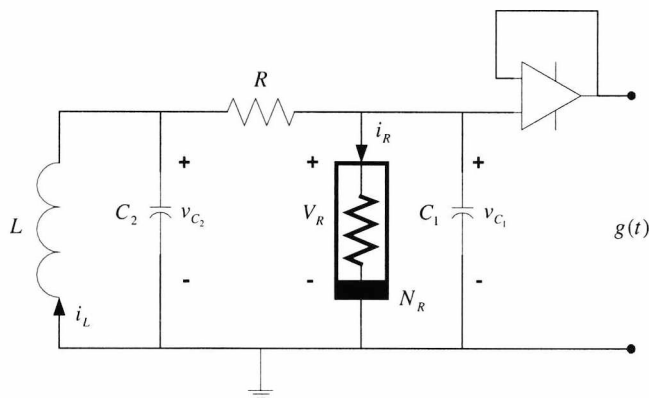


Fig. 2.6 Drive system using Chua's circuit to produce chaotic signal $g(t)$.

The response system contains a cascade drive-response configuration. The first section is denoted subsystem 2 and is described by

$$\begin{aligned}\dot{\hat{v}}_{C_2} &= \frac{G}{C_2}(r(t) - \hat{v}_{C_2}) + \frac{1}{C_2}\hat{i}_L \\ \dot{\hat{i}}_L &= -\frac{1}{L}v_{C_2}.\end{aligned}\quad (2.8)$$

The second section is subsystem 1, which follows subsystem 2 and is described by

$$\dot{\hat{v}}_{C_1} = \frac{G}{C_1}(\hat{v}_{C_2} - \hat{v}_{C_1}) - \frac{1}{C_1}g(\hat{v}_{C_1}).\quad (2.9)$$

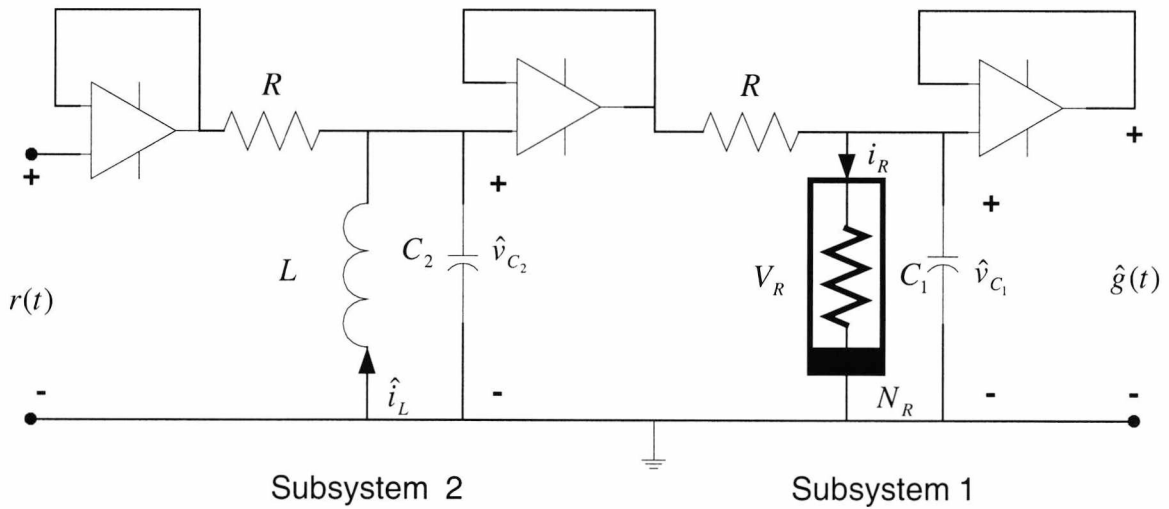


Fig. 2.7 Recovery of $g(t)$ from $r(t)$ using Chua's circuit in a Pecora-Carroll cascaded drive-response configuration.

If $r(t) \approx g(t)$, then $\hat{v}_{C_2}(t)$ approaches $v_{C_2}(t)$ asymptotically. If $\hat{v}_{C_2}(t) \approx v_{C_2}(t)$ and in addition, $\hat{v}_{C_1}(0)$ is sufficiently close to $v_{C_1}(0)$ and the conditional Lyapunov exponents of subsystem 1 are negative, then $\hat{v}_{C_1}(t)$ approaches $v_{C_1}(t)$ asymptotically and $\hat{g}(t) \approx g(t)$.

2.2.2 General synchronisation method

Kocarev and Parlitz [17] and Rullkov *et al* [18] introduce a more general synchronisation method for chaotic communication systems. The method is based on the fact that it is possible to consider more general decompositions of a given dynamical system,

$$\dot{z} = F(z) \quad (2.10)$$

than the decomposition into subsystems proposed by Pecora and Carroll [18]. Starting from a chaotic autonomous system (Eq. 2.10), we can formally rewrite it in different ways as non-autonomous system as

$$\dot{x} = f(x, s(t)) \quad (2.11)$$

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

Let,

$$\dot{y} = f(y, s(t)) \quad (2.12)$$

be a copy of a non-autonomous system that is driven by the same signal $s(t)$. If the differential equation for the difference $e = x - y$,

$$\dot{e} = f(x, s) - f(y, s) = f(x, s) - f(x - e, s), \quad (2.13)$$

possess a stable fixed point at $e = 0$, then there exists for systems (2.11) and (2.12) a synchronised state $x = y$ that is stable. This can be proved using the Lyapunov functions. In general the stability has to be checked numerically using the fact that synchronisation occurs if all conditional Lyapunov exponents [7] of the non-autonomous system (2.12) are negative

2.2.3 Error-feedback synchronisation

In every practical implementation of a telecommunications system, the transmitter and receiver circuits operate under different conditions such as the mismatch between the parameters of the transmitter and the receiver. The effect of parameter mismatch and the effect of the channel on the recovery of $g(t)$ have been widely studied [13] and [20]. Pecora and Carroll show that the performance of the receiver

in the drive-response system may be significantly improved by adding feedback in the state estimator. In the error-feedback synchronisation, the instantaneous difference between the estimate $\hat{g}(t)$ and the received signal $r(t)$ produces a scalar error signal $e(t)$, which modifies the states of the receiver so as to minimise the error. Assuming that the chaotic signal $g(t)$ has been generated by the system shown in Fig. 2.1, then the corresponding error feedback synchronisable system has the structure given in Fig. 2.8.

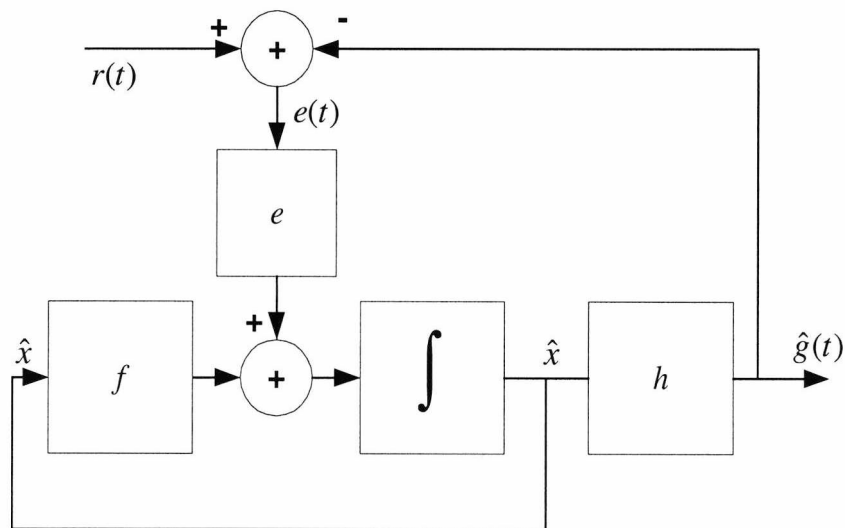


Fig. 2.8 Error-feedback synchronisation.

Here,

$$\dot{\hat{x}} = f(\hat{x}) + e(e(t)) \quad (2.14)$$

where $e(t) = r(t) - \hat{g}(t)$ and $\hat{g}(t) = h(\hat{x})$. With appropriate choices for $h(\cdot)$ and $e(\cdot)$,

$\lim_{t \rightarrow \infty} \|\hat{x}(t) - x(t)\|$ tends to zero.

If \hat{x} converges to x then $\hat{g}(t)$ converges to $g(t)$. Fig. 2.9 shows an example for this method when it is applied to Chua's circuit.

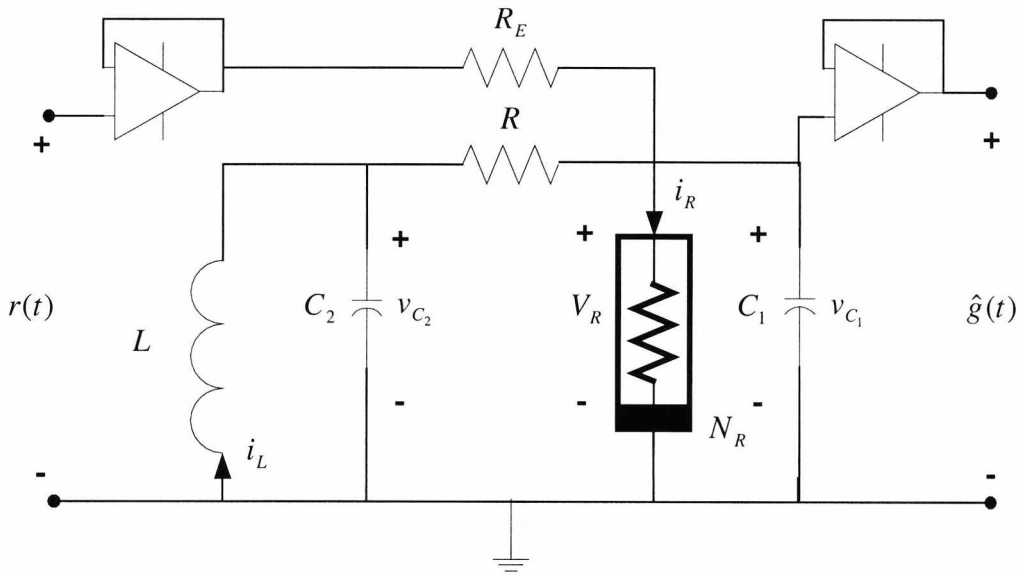


Fig. 2.9 Error-feedback synchronisation in Chua's circuit

For a sufficiently small value of coupling resistor R_E , \hat{v}_{C_1} synchronises with v_{C_1} and $\hat{g}(t) \approx g(t)$.

2.3 Analogue chaotic communication system

During the last few years, there has been considerable interest in the possibility of exploiting chaos in wideband communication systems. Many different modulation techniques have been proposed to-date. They can be divided into two basic categories. In the first category, like the conventional coherent demodulation technique, the chaotic signal has to be recovered from the received noisy signal by chaotic synchronisation. In the second category, the demodulation is carried out without synchronisation.

There are several techniques used for transmitting analogue signals using chaotic synchronisation. Chi-Chung Chen and Kung Yao [21] summarised some of up-to-date well known analogue chaotic communication techniques.

2.3.1 Chaotic masking system

The chaotic masking system is based on masking the information signal by a noise-like chaotic signal at the transmitter and the information signal is recovered at the receiver by a simple subtraction method [22] as shown in Fig. 2.10. The received signal is used to regenerate the masking signal at the receiver. The regeneration of masking signal is done by the synchronisation of the receiver and the transmitter.

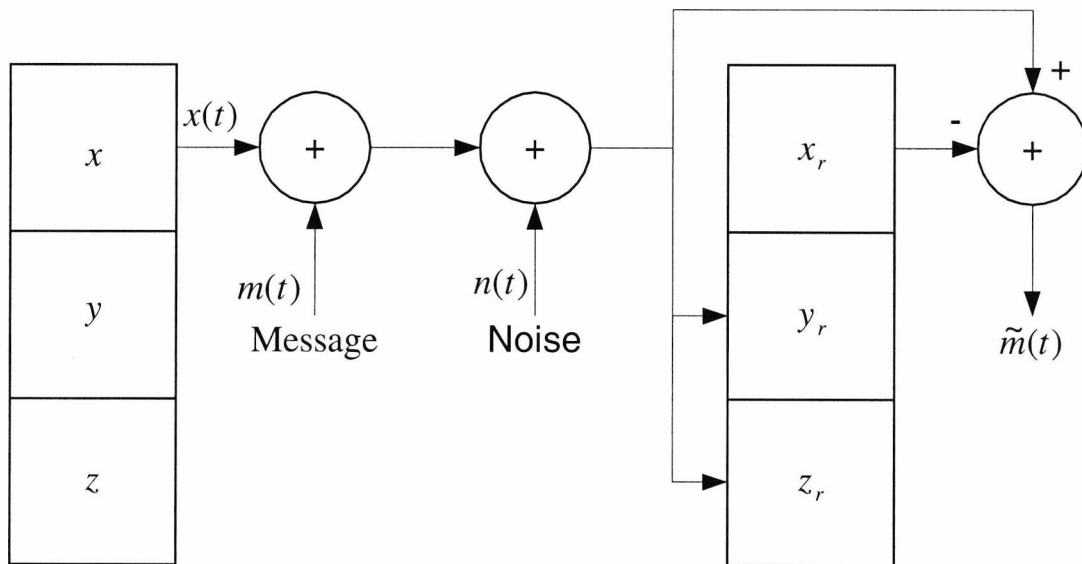


Fig. 2.10 Chaotic masking system.

Cuomo and Oppenheim [23] have built a Lorenz system and have demonstrated the performance of the chaotic masking system with a segment of speech signal. The communication system performance truly relies on the synchronisation ability of the chaotic system. The masking properties of this scheme works only when the amplitude of the information signals are much smaller than the masking signal. To verify the results of the chaotic masking system, we simulate the system and the results are shown in Fig. 2.11. The results show that, the system succeeds in recovering the speech signal. The signal to noise ratio of the recovered signal is 244 dB. The signal to noise ratio is calculated by:

$$\text{Signal to noise ratio [dB]} = 10 \log \frac{\text{The input signal power}}{\text{The error signal power}}$$

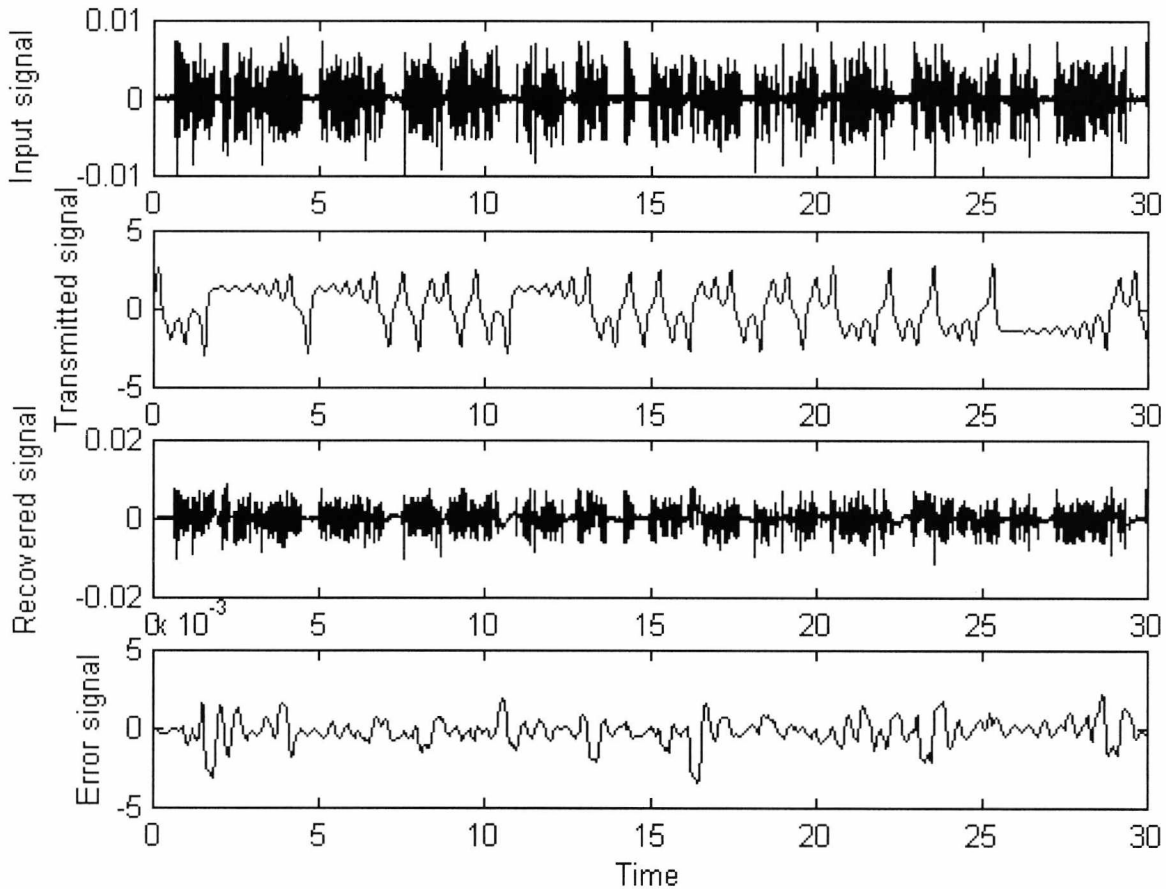


Fig. 2.11 Simulation results of the Lorenz masking system.

2.3.2 Chaotic modulation system

Itoh et al [24]-[25] introduced a communication system based on chaotic modulations. The main idea of this system is to use the chaotic modulation to transmit the information signals $e(t)$. The chaotic synchronisation mechanism introduced by Pecora and Carroll [7] is used to recover the information signals. *Itoh et al* examined the above idea using Chua's circuit [26].

The transmitter state equations are given by

$$\begin{aligned} C_1 \frac{dv_{C_1}}{dt} &= \frac{v_{C_2} - v_{C_1}}{R} - g(v_{C_1}) + \frac{e(t) - v_{C_1}}{R_s} \\ C_2 \frac{dv_{C_2}}{dt} &= \frac{v_{C_1} - v_{C_2}}{R} + i_L \\ L_1 \frac{di_L}{dt} &= -v_{C_2} - ri_L \end{aligned} \quad (2.15)$$

where $g(v_{C_1})$ is a piece-wise linear function and it is defined by

$$g(v_{C_1}) = -G_b v_{C_1} + 0.5(G_a - G_b)(|v_{C_1} + B_p| - |v_{C_1} - B_p|) \quad (2.16)$$

and $e(t)$ is the information signal.

Fig. 2.12 shows the circuit diagram of the chaotic modulation system. The term ri_L is added to the ideal Chua equations in order to take into account the small inductor resistance in the physical circuit. Fig. 2.13 shows the circuit diagram of the chaotic modulation system. The receiver state equations are given by

$$\begin{aligned} C_1 \frac{dv'_{C_1}}{dt} &= \frac{v'_{C_2} - v'_{C_1}}{R} - g(v'_{C_1}) - \frac{v'_{C_1}}{R_s} \\ C_2 \frac{dv'_{C_2}}{dt} &= \frac{v'_{C_1} - v'_{C_2}}{R} + i'_L \\ L \frac{di'_L}{dt} &= -v'_{C_2} - ri'_L \end{aligned} \quad (2.17)$$

where $v_{C_1}(t) = v'_{C_1}(t)$ because of the voltage buffer.

The information signal can be recovered by

$$e(t) = R_s \left[C_1 \frac{dv_{C_1}}{dt} - \frac{v_{C_2} - v_{C_1}}{R} + g(v_{C_1}) + \frac{v_{C_1}}{R_s} \right]. \quad (2.18)$$

Similarly, the current $j(t)$ is given by

$$j(t) = \left[C_1 \frac{dv'_{C_1}}{dt} - \frac{v'_{C_2} - v'_{C_1}}{R} + g(v'_{C_1}) + \frac{v'_{C_1}}{R_s} \right]. \quad (2.19)$$

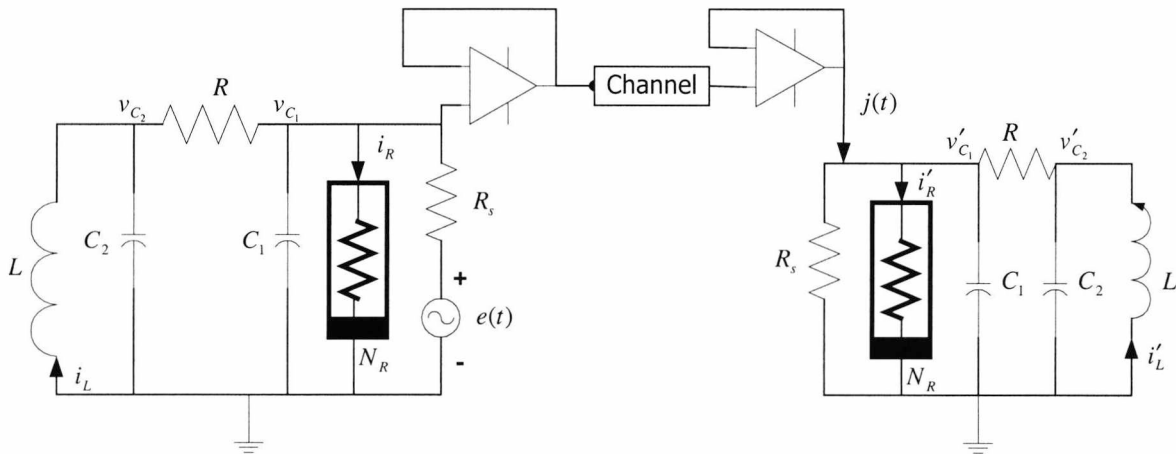


Fig. 2.12 Communication modulation system using Chua's circuit.

Itoh *et al* built the chaotic modulation communication system and the system was tested by various kinds of signals (voice, music...etc).

They showed that:

- The communication system is easily built with a small outlay.
- The waveforms of the transmitted chaotic signal can mask the information signal if the amplitude of the information signal is small enough.
- The transmitted signals have broad spectra and can mask the input signals.

To verify the results of the chaotic modulation system, we simulate the system and the results indicate that the information signals are recovered with sufficient quality as shown in Fig.2.13. The signal to noise ratio in this case is 11.92 dB.

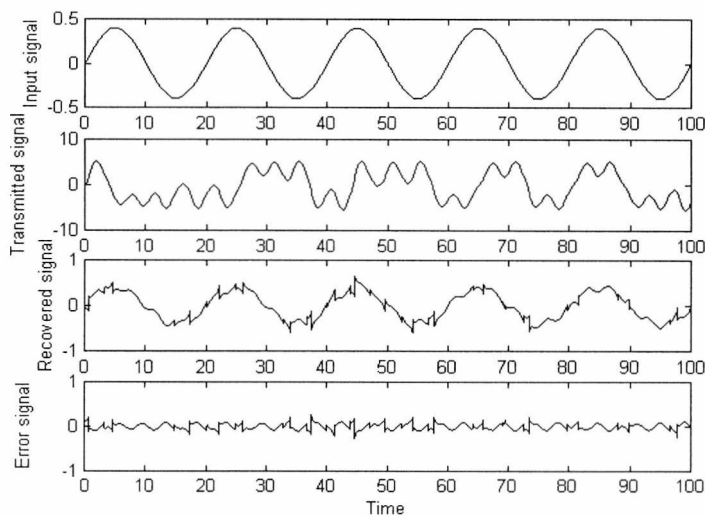


Fig. 2.13 Simulation results of the chaotic modulation system.

2.3.3 chaotic communication system based on general synchronisation approach

Kocarev and Parlitz [16] illustrated the general synchronisation approach using the well-known Lorenz model. The state equations of the transmitter are given by

$$\begin{aligned}\dot{x}_1 &= -10x_1 + s(t) \\ \dot{x}_2 &= 28x_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - 2.666x_3\end{aligned}\tag{2.20}$$

where $s(t) = 10x_2 + ix_3$ and i is the information signal.

The receiver state equations are given by

$$\begin{aligned}\dot{y}_1 &= -10y_1 + s(t) \\ \dot{y}_2 &= 28y_1 - y_2 - y_1y_3 \\ \dot{y}_3 &= y_1y_2 - 2.666y_3.\end{aligned}\tag{2.21}$$

The recovered signal i_R is given by

$$i_R = (s - 10y_2) / y_3.\tag{2.22}$$

To estimate the temporal evaluation of the error $e = x - y$ of the states of the systems Eq. 2.20 and Eq. 2.21, we note first that the difference $e_1 = x_1 - y_1$ of the first components converges to zero because $\dot{e}_1 = -10e_1$. Therefore, the remaining two-dimensional system describing the evaluation of the differences $e_2 = x_2 - y_2$ and $e_3 = x_3 - y_3$ can be written for the limit $t \rightarrow \infty$ as

$$\begin{aligned}\dot{e}_2 &= -e_2 - x_1e_3 \\ \dot{e}_3 &= x_1e_2 - 2.666e_3.\end{aligned}\tag{2.23}$$

Using the Lyapunov function $L = e_2^2 + e_3^2$ one can show that $\dot{L} = -2(e_2^2 + 2.666e_3^2) < 0$. This means that the synchronisation is globally stable and occurs for all types of driving signals $s(t)$. The conditional Lyapunov exponents of this decomposition is given by $\lambda = -1.805$, $\lambda_2 = -1.861$ and $\lambda_3 = -10$. To verify the results of the general synchronisation system, we simulate the system and the results of simulation are shown in Fig. 2.14. The results show that, the information

signal is masked by the chaotic signal and that the receiver succeeds in recovering the information signal with signal to noise ratio equal 218.9 dB.

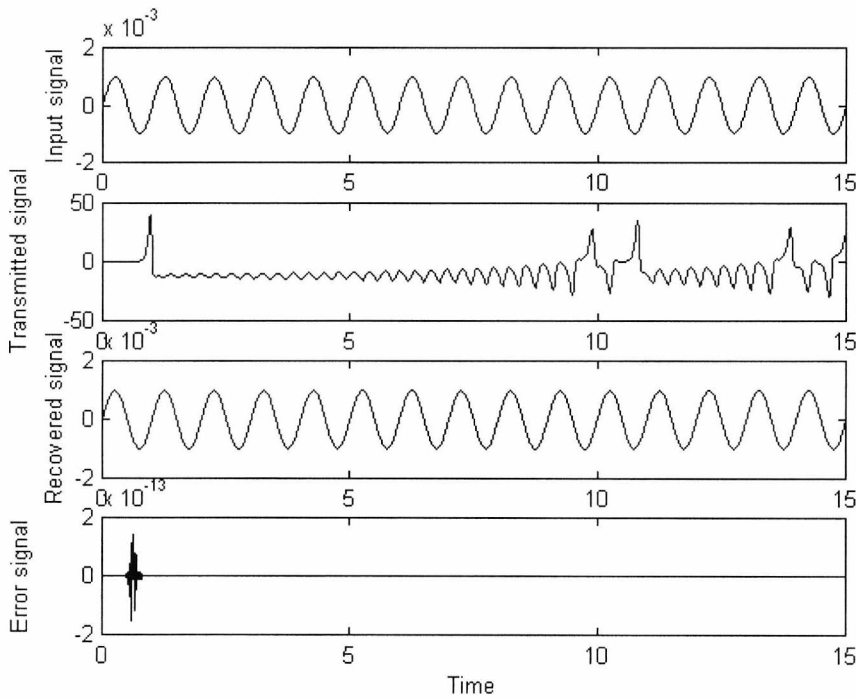


Fig. 2.14 Simulation results of the chaotic communication system based on the general approach of synchronisation.

We conclude that the systems introduced in sections 2.3.1, 2.3.2 and 2.3.3 have the following drawbacks:

1. The chaotic masking and the chaotic modulation approaches have some difficulties which are the level of the information signal must be lowered to at least 30 dB below the level of the chaotic signal [27]. Moreover, the frequency range of the information signal is limited due to the resonance frequencies of the subsystems [28].
2. In the general synchronisation system approach, the information signal is recovered by dividing by the state variable y_3 (Eq. 2.22). If y_3 tends to zero, the system will be unstable. This method is suitable for some chaotic generator such as Lorenz and Rössler chaotic generators where the state variable y_3 does not tend to zero.

We will next introduce a new system for analogue chaotic communication system called the multi-channel chaotic communication system (MCCS).

2.4 Multi-channel chaotic communication system (MCCS)

In the multi-channel chaotic communication system, one channel is used for synchronisation between the transmitter and the receiver and the other channels are used for masking the information signals as shown in Fig. 2.15. The MCCS system is based on Chua's circuit [29]. The system is simulated and also physically implemented. In comparison with one-channel masking systems (OCMS) [22]-[23], the magnitude and the frequency range of the informational signal are not limited. However our system requires two channels to send one information signal, The voltage $v_{C_1}(t)$ is used as a synchronisation signal between the transmitter and the receiver while the voltage $v_{C_2}(t)$ is used as a masking signal for the information signals. Let $s(t)$ be the information-bearing signal and the transmitted signal $r(t) = s(t) + v_{C_2}(t)$, where the power level of $s(t)$ is significantly lower than that of $v_{C_2}(t)$ in order to hide the signal effectively. The state equations of the transmitter are given by

$$\begin{aligned}\dot{v}_{C_1} &= \frac{G}{C_1}(v_{C_2} - v_{C_1}) - \frac{1}{C_1}g(v_{C_1}) \\ \dot{v}_{C_2} &= \frac{G}{C_2}(v_{C_1} - v_{C_2}) + \frac{1}{C_2}i_L \\ i_L &= -\frac{1}{L}v_{C_2}.\end{aligned}\tag{2.24}$$

The state equations of the receiver are given by

$$\begin{aligned}C_2 \frac{dv_{C_2}^r}{dt} &= \frac{1}{R}(v_{C_1}(t) - v_{C_2}^r(t)) + i_l^r \\ L \frac{di_l^r}{dt} &= -v_{C_2}(t)\end{aligned}\tag{2.25}$$

where $v_{C_2}^r(t)$ and $i_l^r(t)$ is the voltage across the capacitor C_2 and the current through the inductor L of the receiver system. The information signals can be recovered by

$$\tilde{s}(t) = r(t) - v_{C_2}^r(t) = s(t). \quad (2.26)$$

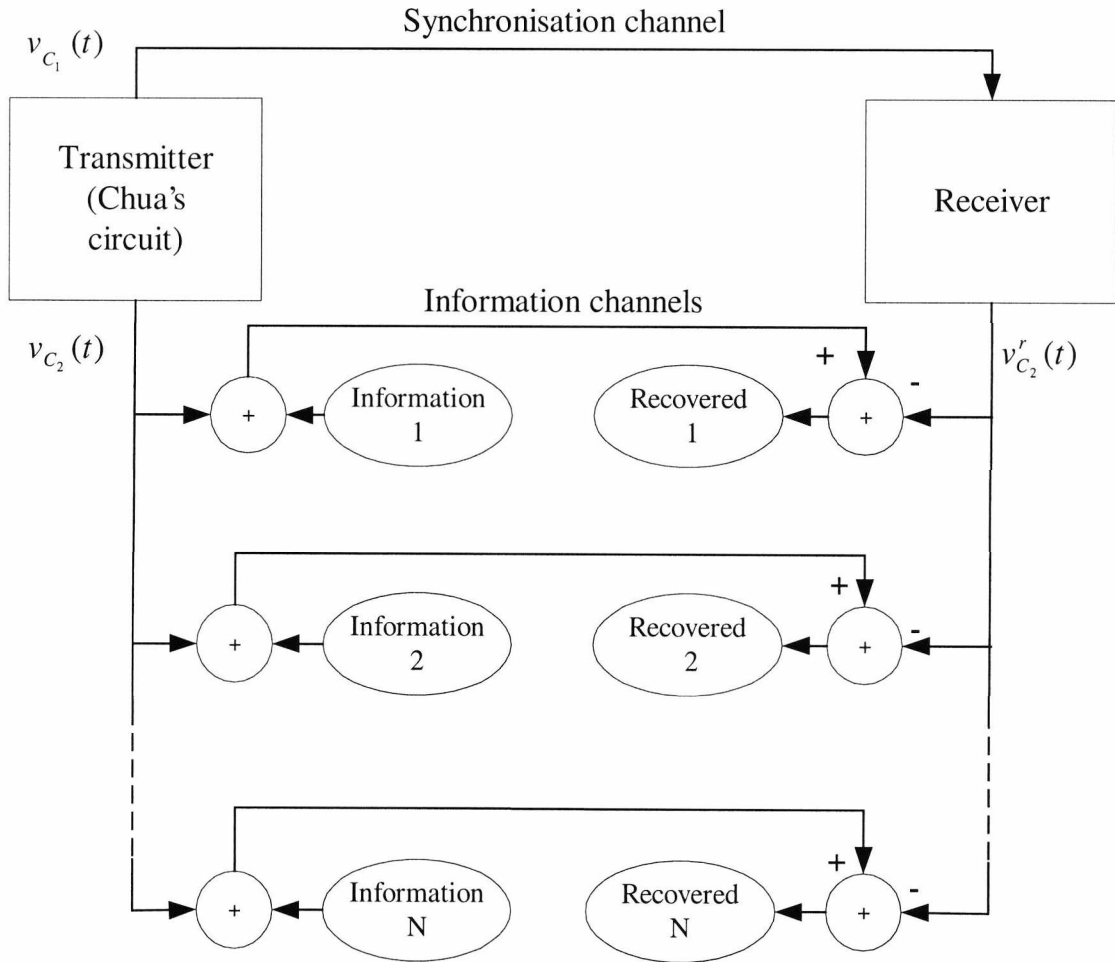


Fig. 2.15 Block diagram of multi-channel chaotic communication system.

MATLAB [30] and the circuit simulator TINA [31] are used to simulate the developed system. Fig. 2.16 represents the signal flow in the simulation using MATLAB. For simplicity, only three channels are shown.

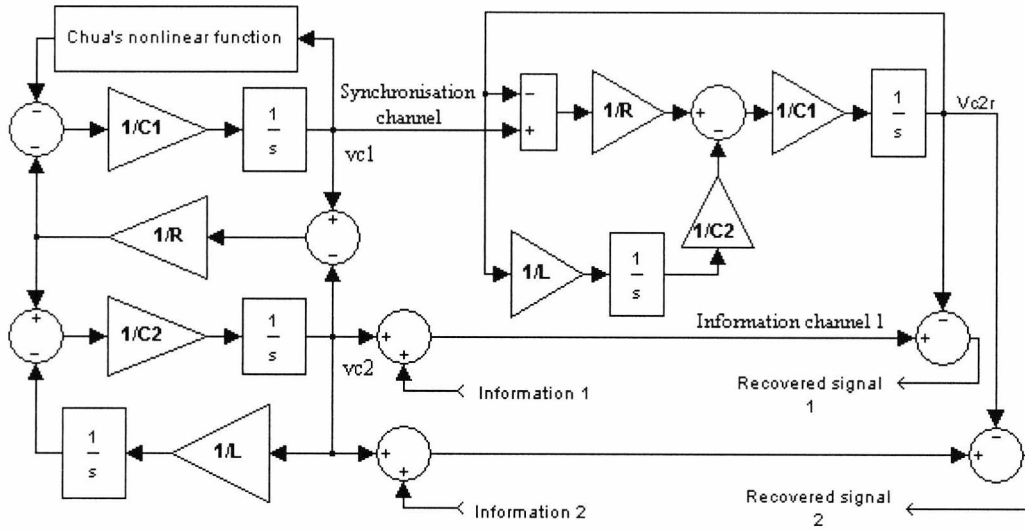


Fig. 2.16 Signal flow representation of multi-channel chaotic communication system.

The circuit component values for the transmitter and the receiver are as follows: $R=1.5 \text{ K}\Omega$, $C_1=10 \text{ nF}$, $C_2=100 \text{ nF}$ and $L=18.5 \text{ mH}$ with series resistance $r=20 \text{ }\Omega$. The normalised parameters in the simulation are $R=1.5$, $C_1=10$, $C_2=1$, $L=1/5.6$ and $r=0.02$. The initial conditions for the integrators are set to 0.1 and the Chua non-linear function is given by

$$g(v_{C_1}) = G_a v_{C_1} + \frac{1}{2}(G_a - G_b)(|v_{C_1} + B_p| - |v_{C_1} - B_p|)$$

where G_a , G_b and B_p are equal to -0.409, -0.758 and 1.8 respectively. The channels are assumed to be ideal which means that the effect of noise, interference and delay are not taken into account. The channels are simulated by unity gain buffer amplifiers. The system is tested by masking different information signals at the transmitter and recovering them at the receiver. Four information channels are tested. Fig 2.17a shows the results of masking of a sinusoidal signal of amplitude 0.1 mV with a signal to chaos ratio (SCR) of -74.7 dB and a frequency of 1.0 kHz. The signal to chaos ratio is calculated using the following formula:

$$\text{Signal to chaos ratio [dB]} = \frac{\text{Power of the input signal}}{\text{Power of the transmitted signal}}$$

Fig. 2.17b shows masking and recovering of a square wave signal with a frequency of 2.0 kHz and a SCR of -11.87 dB. Fig. 2.17c shows masking and recovering of amplitude modulated signal at SCR of -43.96 dB. Fig. 2.17d shows masking and recovering of a frequency-modulated signal at SCR of -34.84 dB. The results indicate that our system is capable of masking different information signals and recovering them even at SCR of -74 dB and that capability is available at different frequencies and amplitudes. In comparison with the OCMS system [32], the MCCA system is working without restrictions on the frequency range and the amplitude of the input signal. The only restriction for the amplitude is that the information signal is small enough to be hidden (SNR= -10 dB).

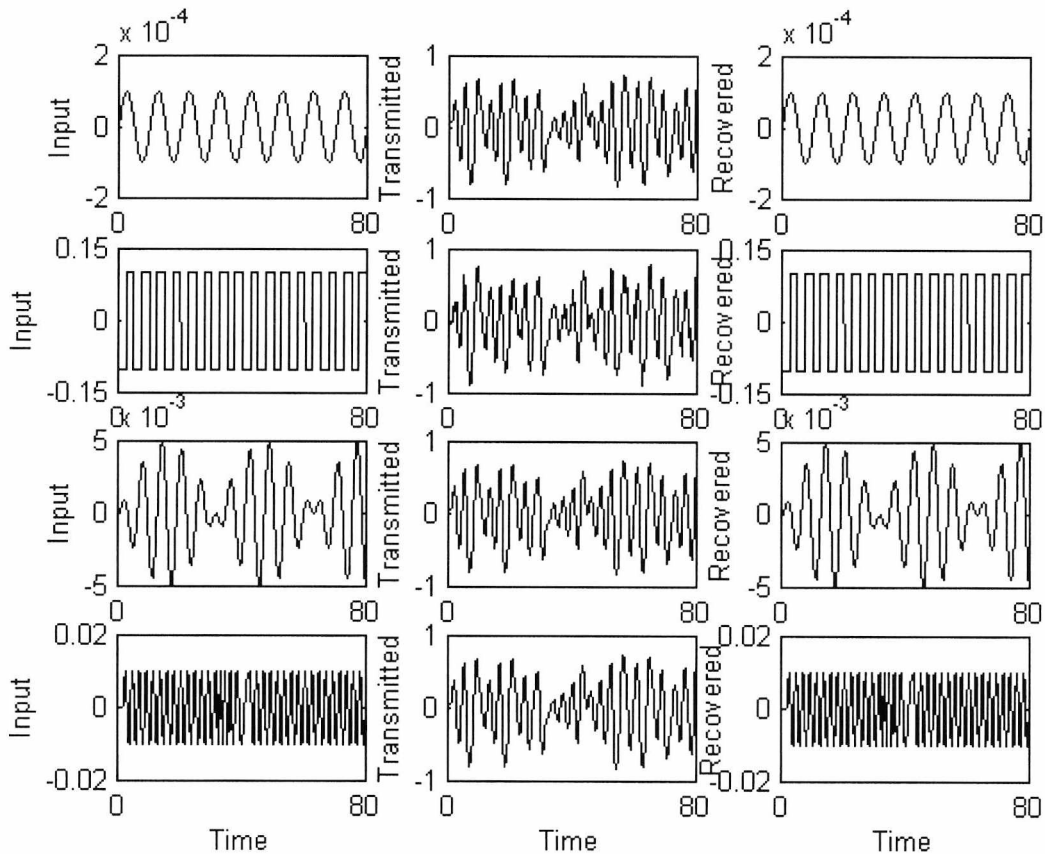


Fig. 2.17 MATLAB results of the MCCA system.

Fig. 2.18 shows the circuit diagram representing the MCCA system simulated by the TINA circuit simulator. For simplicity only two channels are simulated. Table 2.1 gives the component list of the multi-channel chaotic communication system.

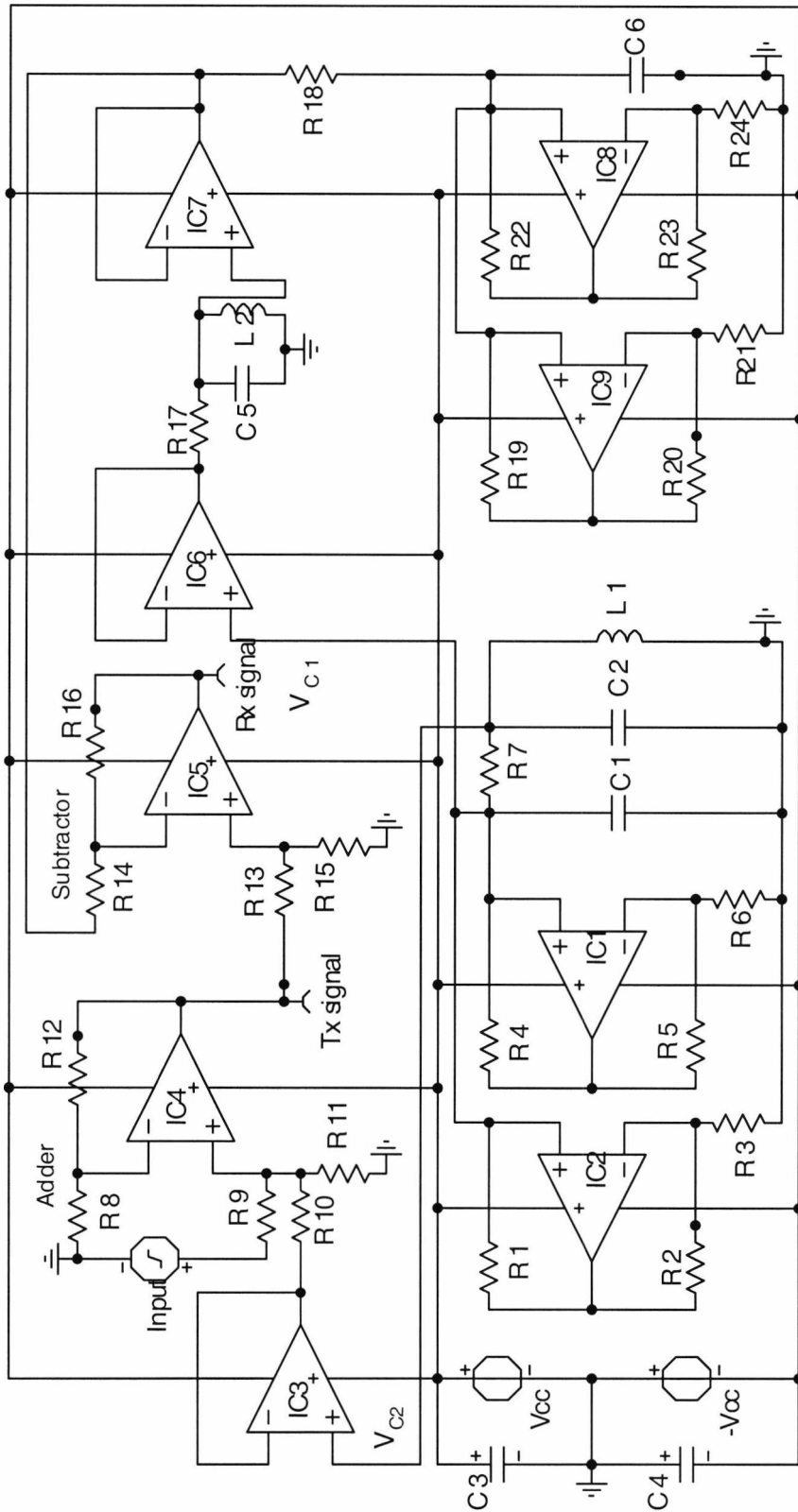


Fig. 2.18 Schematic diagram of the multi-channel chaotic communication system.

Component	Value
R1=R2=R19=R20	220 Ω
R3=R21	2.2 k Ω
R4=R5=R22=R23	22 k Ω
R6=R24	3.3 k Ω
R7=R17=R18 (variable resistors)	4.7 k Ω
R12	1 k Ω
R8=R9=R10=R11=R13=R14=R15=R16	2 k Ω
L1=L2	18 mH, r=20 Ω
C1=C6	10 nF
C2=C5	100 nF
C3=C4	1 μ F, 25 V
IC1=IC2=IC3=IC4=IC5=IC6=IC7=IC8=IC9	TL071C

Table 2.1 Components list of the multi-channel chaotic communication system.

The developed system is examined by masking different information signals with different amplitudes and frequencies. Fig. 2.19 shows the results of masking a square wave of amplitude 10 mV and a frequency of 1 kHz. Fig. 2.20 shows the results of masking of a saw-tooth signal with amplitude 50 mV and a frequency of 2.5 kHz. Fig. 2.21 shows the results of masking a sine-wave signal with amplitude 100 mV and a frequency of 3 kHz. The above results indicate that we can mask and recover the information signal at SCR of -32 dB. In the OCMS system [33], the information signal cannot be completely recovered even at a SCR of -12 dB with restrictions on the frequencies and the amplitudes of the information signals.

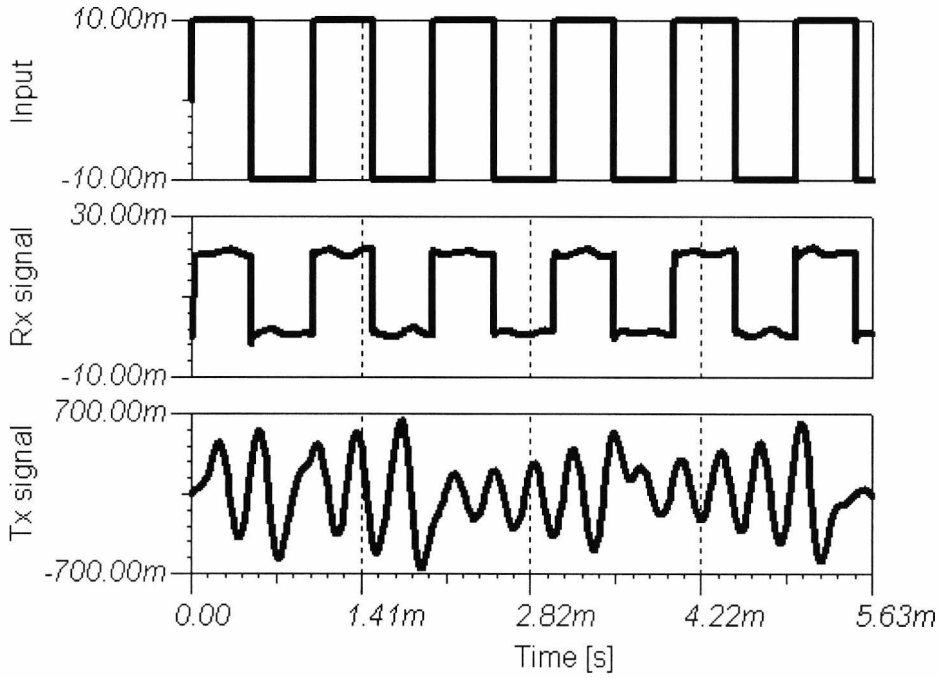


Fig. 2.19 The results of multi-channel chaotic communication system in the case of a square-wave with amplitude 10 mV and a frequency of 1 kHz.

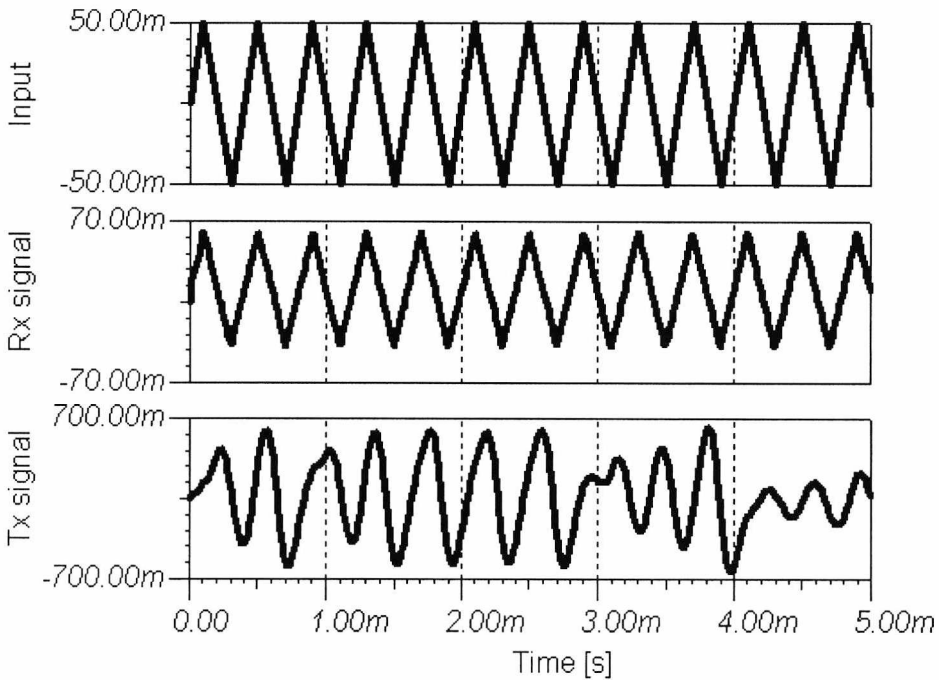


Fig. 2.20 The results of multi-channel chaotic communication system in the case of a saw-tooth signal with amplitude 50 mV and a frequency of 2.5 kHz.

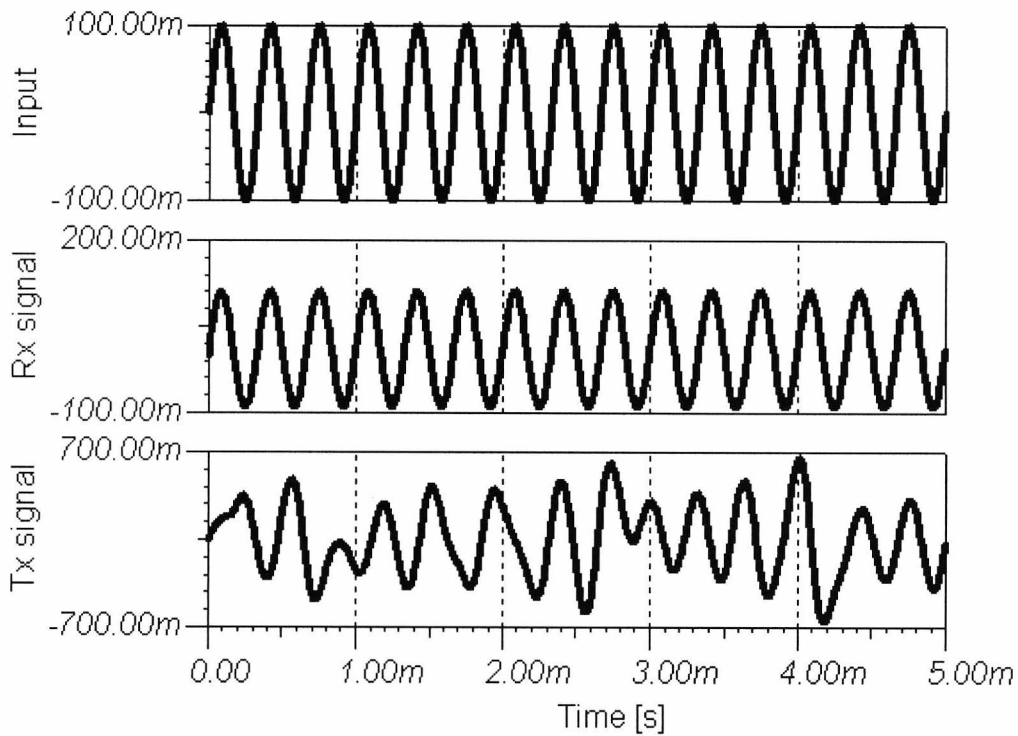


Fig. 2.21 The results of the multi-channel chaotic communication system in the case of a sine wave with amplitude 100 mV and a frequency of 3 kHz.

The multi-channel chaotic communication system shown in Fig. 2.18 was physically implemented and tested using various kinds of information signals. Fig. 2.22 presents the x-y plot of $v_{c_2}(t)$ of the transmitter and the receiver and it shows that the transmitter and the receiver are synchronised. Fig. 2.23 shows the receiver output signal and the transmitter output signal for a saw-tooth input signal with a frequency of 500 Hz and a peak to peak amplitude of 200 mV. In this case, the amplitude of the chaotic carrier signal $v_{c_2}(t)$ is equal to 3.5 V and the SCR is -24 dB. The results indicate that the information signal is completely masked and is recovered correctly. The system is tested by other kind of information signals such as square and sinusoidal signals with frequencies of 1.0 kHz and 2.5 kHz and amplitudes of 500 mV and 1.0 V respectively and the results are shown in Fig. 2.24 and Fig. 2.25.

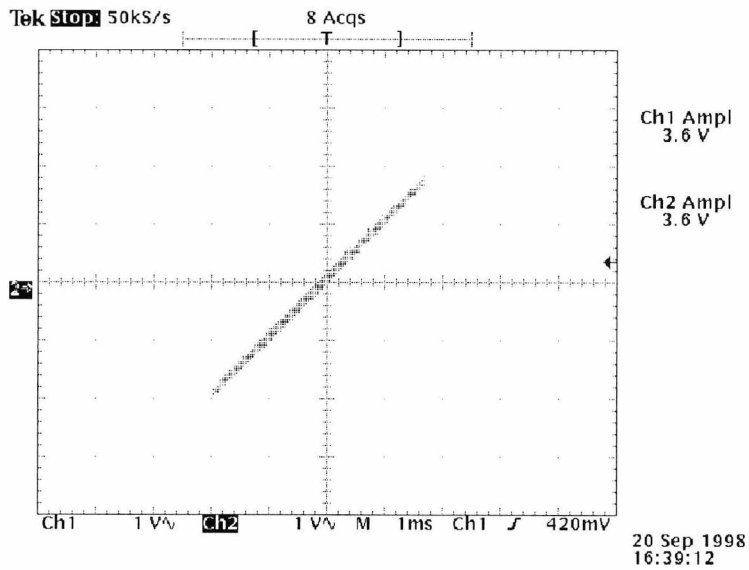


Fig. 2.22 X-Y plot of $v_{C_2}(t)$ of the transmitter and the receiver

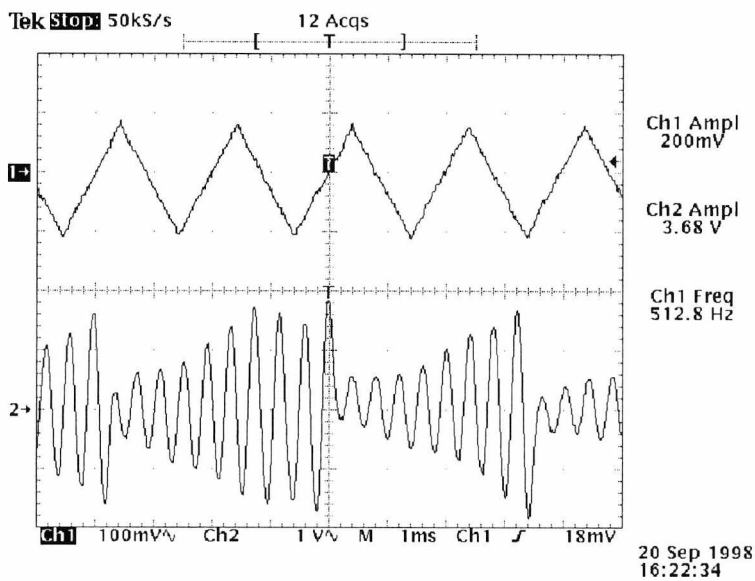


Fig. 2.23 Experimental results in the case of saw-tooth signal with amplitude 200 mV and frequency of 512 Hz. The upper trace is the recovered signal and the lower trace is the transmitted signal.

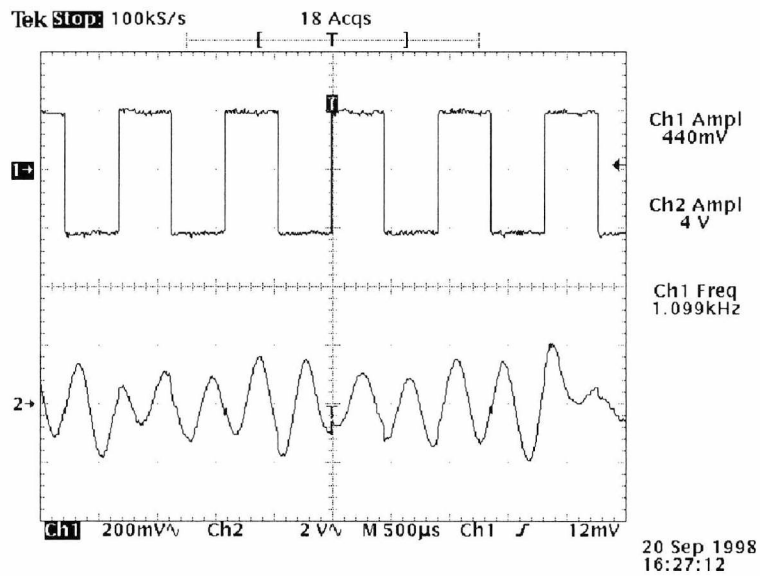


Fig. 2.24 Experimental results in the case of square wave signal with amplitude 500 mV and frequency of 1.0 kHz. Upper trace is recovered signal and lower trace is transmitted signal.

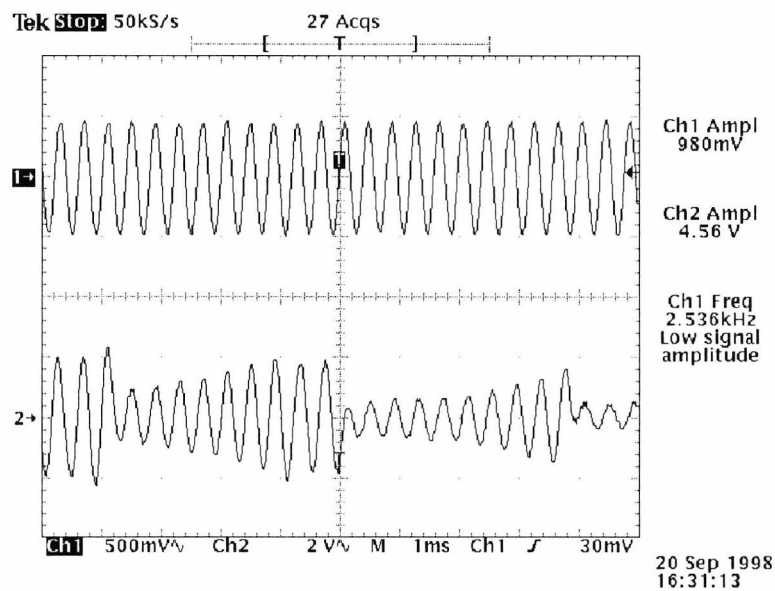


Fig. 2.25 Experimental results in the case of sinusoidal signal with amplitude 1.0 V and frequency of 2.5 kHz. Upper trace is recovered signal and lower trace is transmitted signal.

By comparing the OCMS [32] and the M CCS systems, we conclude the following:

- The simulation results using MATLAB and SIMULINK show that the M CCS system (SCR= -74 dB) are better than the OCMS system (-32 dB).
- The simulation results using the circuit simulator (TINA) show that, the system succeeds in recovering the information signal at SCR=-32 dB and at different frequencies and amplitudes of the input signal. In the OCMS system, the same results cannot be achieved even at SCR=-12 dB.
- Physical implementation of the M CCS system shows that we can easily build the M CCM system and achieve the same results of the TINA simulator at SCR =-24 dB. The OCMS system is easily built but we cannot get the same results of the M CCM even at SCR=-12 dB.
- The main disadvantage of the M CCS is the use of an extra channel for synchronisation between the transmitter and the receiver but this disadvantage can be reduced if the system is used in the transmission of more than one information signal. As an example, in some military applications, it is required to transmit several information signals from one place to another place and all of these information signals have a high degree of security. In this case, we can mask all of these information signals and transmit them to the receiver part of the system. In the M CCS system one extra synchronisation channel is used to transmit these information signals instead of using several systems of OCMS to transmit the same number of information signals.

2.5 Digital chaotic communication systems

In chaos based communication systems the information signal to be transmitted is mapped to a certain property of the chaotic signals. That property can be for example the energy of the chaotic signal or the correlation between the different parts of the transmitted signal. Demodulation can be performed without synchronisation because it is enough to estimate the parameter carrying the transmitted information from the noisy received signal. Kennedy and Dedieu [34] and Kolumban *et al* [35] have shown that, the transmitted symbols can be recognized using either coherent or non-

coherent demodulation techniques. In contrast to conventional communication systems where periodic signals are used, the parameter required for the decision can be precisely estimated in the noise-free case. The variance of the estimation is influenced by both the channel noise and the chaotic signal. For a given noise level, the variance of the estimation can be reduced by increasing the estimation time (the bit duration). The bit duration is bounded by the bit error rate (BER) which has to be achieved at a given signal to noise ratio (SNR).

2.5.1 Chaos Shift Keying (CSK)

Hasler [36] summarised the CSK or the chaos switching introduced by Parlitz *et al* [37] as follows. The information signal $s(t)$ is supposed to be binary data. It controls a switch whose action changes the parameter values of the chaotic system. According to the value of $s(t)$ at any given instant t , the chaotic system has either the parameter vector p or the parameter vector p' . The transmitted output $y(t)$ of the chaotic system is one of two copies of the chaotic system, one with parameter vector p and the other with p' as shown in Fig. 2.26. If the momentary position of the switch in the transmitter is on position p then the system with parameter vector p in the receiver will synchronise whereas the system with parameter vector p' will desynchronise. Thus the error signal $e(t)$ will converge to zero whereas $e'(t)$ will have an irregular waveform with a distinctly nonzero amplitude. If the switch in the transmitter is on position p' then we have the opposite situation. In this case, $e'(t)$ will converge to zero and $e(t)$ will have a nonzero amplitude.

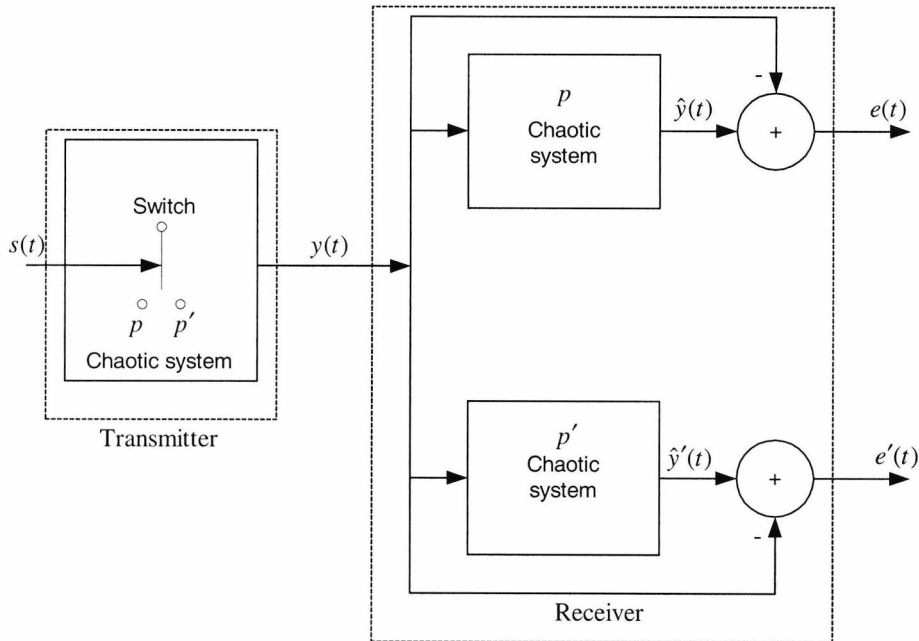


Fig. 2.26 Transmission using chaotic switching.

Consequently, the signal $s(t)$ can be retrieved from the error signals $e(t)$ and $e'(t)$. Clearly, one has to leave the switch in the transmitter a certain time in the same position in order to be able to observe the convergence of the corresponding error signal to zero. In some realisations only one chaotic system is used on the receiver side. In order to distinguish the transmitted bit value, one has to decide between synchronisation and desynchronisation on the basis of a single error signal. In this case, the information rate for the chaotic switch is low. Because the binary signal has a lower information content per unit time than an analogue signal and for each bit that is transmitted, one has to wait until synchronisation and desynchronisation are achieved in the receiver.

2.5.2 Chaotic on-off keying (COOK)

Kis *et al* [38] give a brief description of the COOK scheme. In the COOK scheme, the chaotic signal is switched *off* and *on* according to symbols 0 and 1 respectively as shown in Fig. 2.27. Kolumban *et al* [39] show that the COOK scheme has better noise performance than the CSK. This is the result of the fact that, the difference in

energy per bit between the elements of the signal is increased compared to the CSK method. The demodulator recovers the information signal by correlating the received signal with a copy of itself. The decision is made by a level comparator.

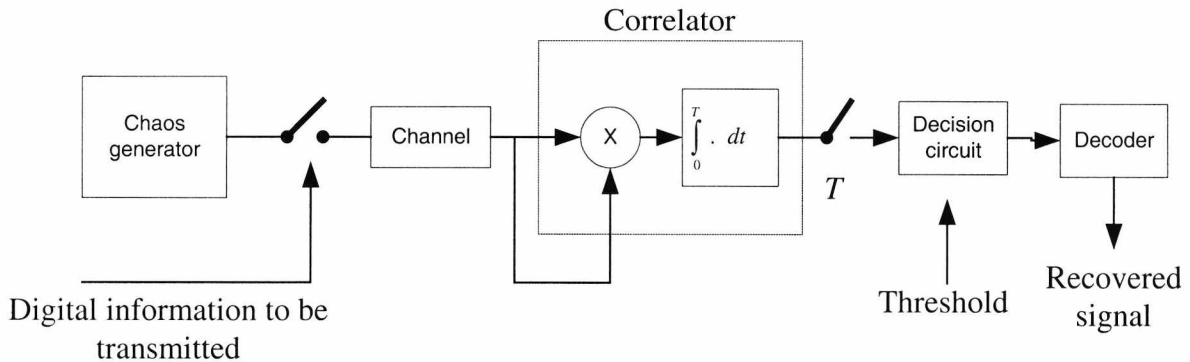


Fig. 2.27 Block diagram of the non-coherent COOK modulation scheme.

2.5.3 Differential chaos shift keying modulation (DCSK)

In the DCSK [40]-[41], every bit to be transmitted is represented by two chaotic sample functions. The first one serves as a reference while the second carries the information. The block diagram of the DCSK is shown in Fig. 2.28. Bit 1 is sent by transmitting a reference signal provided by a chaos generator twice in succession while for bit 0 the reference chaotic signal is transmitted followed by an inverted copy of the same signal. This means that the binary information is mapped to the correlation measured between the two parts of the transmitted signal. The demodulator recovered the information signal by correlating the received signal and the delayed copy of itself. The decision circuit is made by a level comparator. For sufficient large delay T , noise performance of DCSK is comparable to that of a conventional sinusoid-based modulation scheme. In particular, $E_b/N_0 = 13.5$ dB is required for $\text{BER} = 10^{-3}$. Where E_b is the energy per bit and N_0 is the energy of the noise.

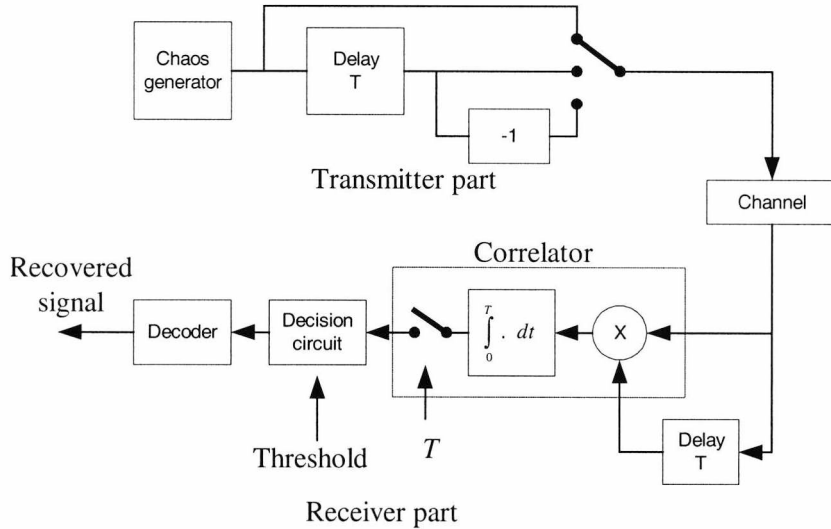


Fig. 2.28 The block diagram of DCSK.

For the systems introduced in 2.5.1, 2.5.2 and 2.5.3, we conclude that:

1. The major disadvantage of the CSK system is that the threshold value of the decision circuit depends on the noise level.
2. The same problem appears in the COOK system, however the COOK system can maximise the energy per bit between the elements of the signal set.
3. In the DCSK, the threshold can be kept constant and does not depend on the noise level but the problem is that every information bit is transmitted by two sample functions so the bit rate will be halved.

2.6 One generator CSK

The CSK is introduced in section 2.5.1. In this system, the driving system uses one non-linear function with two different parameters and in the responding system, there are two subsystems, one synchronised with the first Chua non-linear function and the other synchronised with the second non-linear function. In this work, we develop a modified CSK system using one non-linear function in the transmitter and the receiver synchronises or desynchronises with the transmitter system according to the

transmitted binary information signal. The system is based on Chua's circuit [26] as the chaotic generator. The voltage across the capacitor C_1 is used to transmit the binary information bit 1 and the current through the inductor L , after scaling by a certain factor, is used to transmit the binary information 0. The current i_L is scaled by a constant factor equal to 1.1 to have the same amplitude as $v_{C_1}(t)$. We know that, the receiver system is synchronised with the transmitter system when it is driven by the voltage $v_{C_1}(t)$ [33]. We also know that the current through the inductor L cannot be used as a driving signal because the transmitter and the receiver systems will not synchronise [42]. In the receiver, the difference between the transmitter output and the receiver output signals ($r(t) - v_{C_1}^r(t)$) is calculated. If the absolute value of the difference is minimum then the two systems are synchronised and bit 1 is received. If the absolute value of the difference is maximum then the two systems are desynchronised and bit 0 is received. The block diagram of the system is shown in Fig. 2.29.

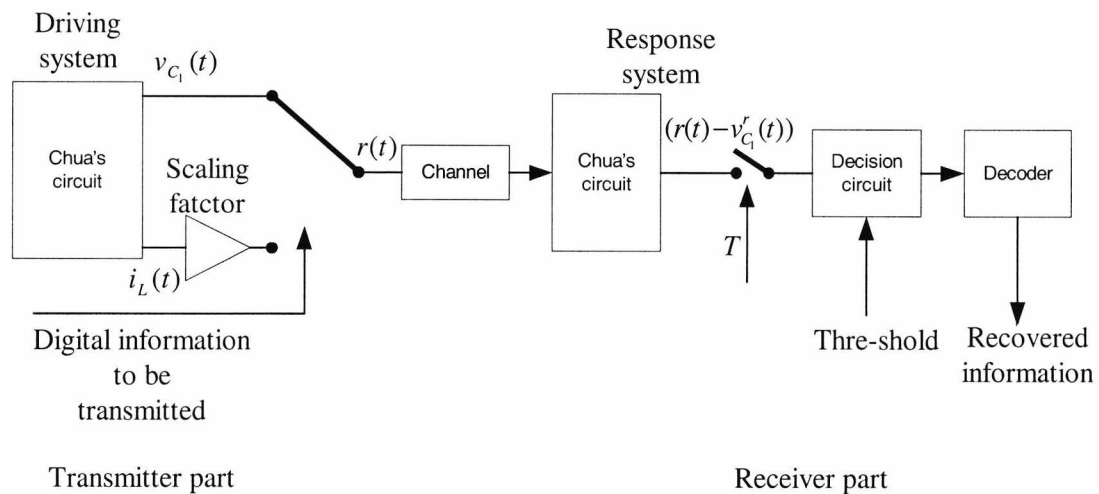


Fig. 2.29 Block diagram of the CSK using one chaos generator.

The system is simulated using SIMULUNK and the signal flow diagram of the system is shown in Fig. 2.30. Fig. 2.31 illustrates the simulation results of the system. The result show that the difference between the transmitter output and the receiver output signals in the case of synchronisation is small compared to the case when the two systems are desynchronised. The absolute value of the difference

$r(t) - v_{C_1}'(t)$ is applied to a LPF and the decision circuit determines which bit is received. The threshold of the decision circuit is determined experimentally.

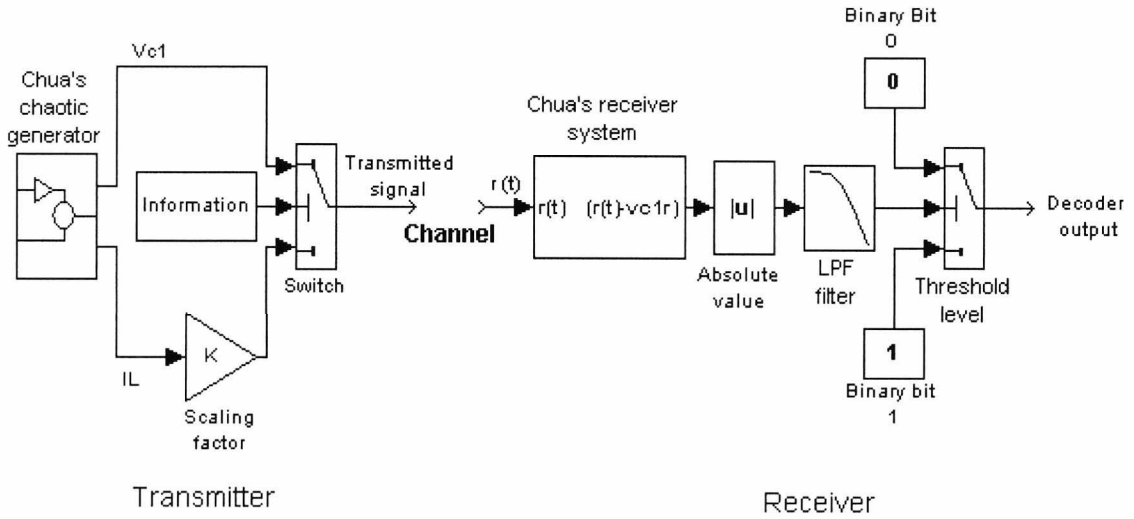


Fig. 2.30 Signal flow of one channel CSK.

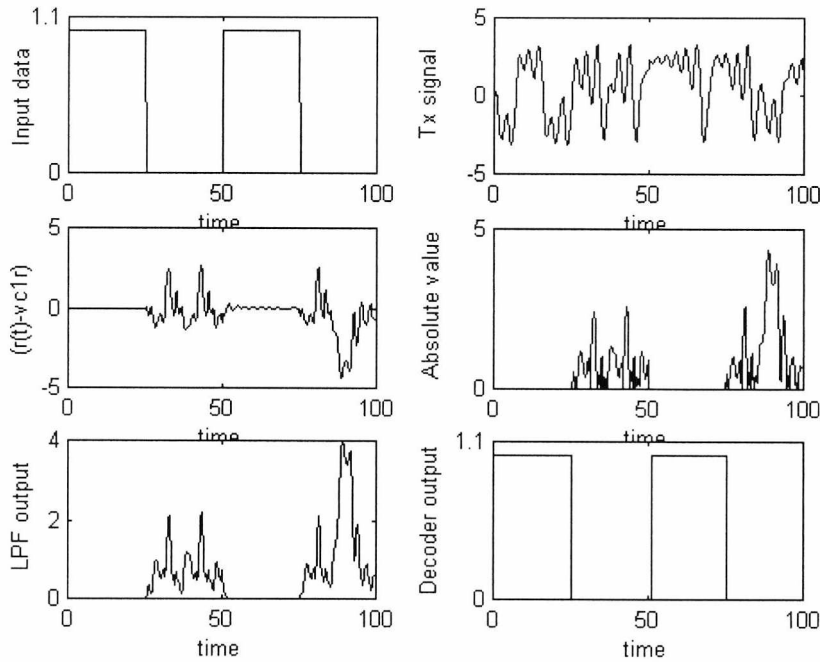


Fig. 2.31 Simulation results of the one generator CSK.

The one generator CSK is physically implemented and the simplified circuit diagram of the system is shown in Fig. 2.32.

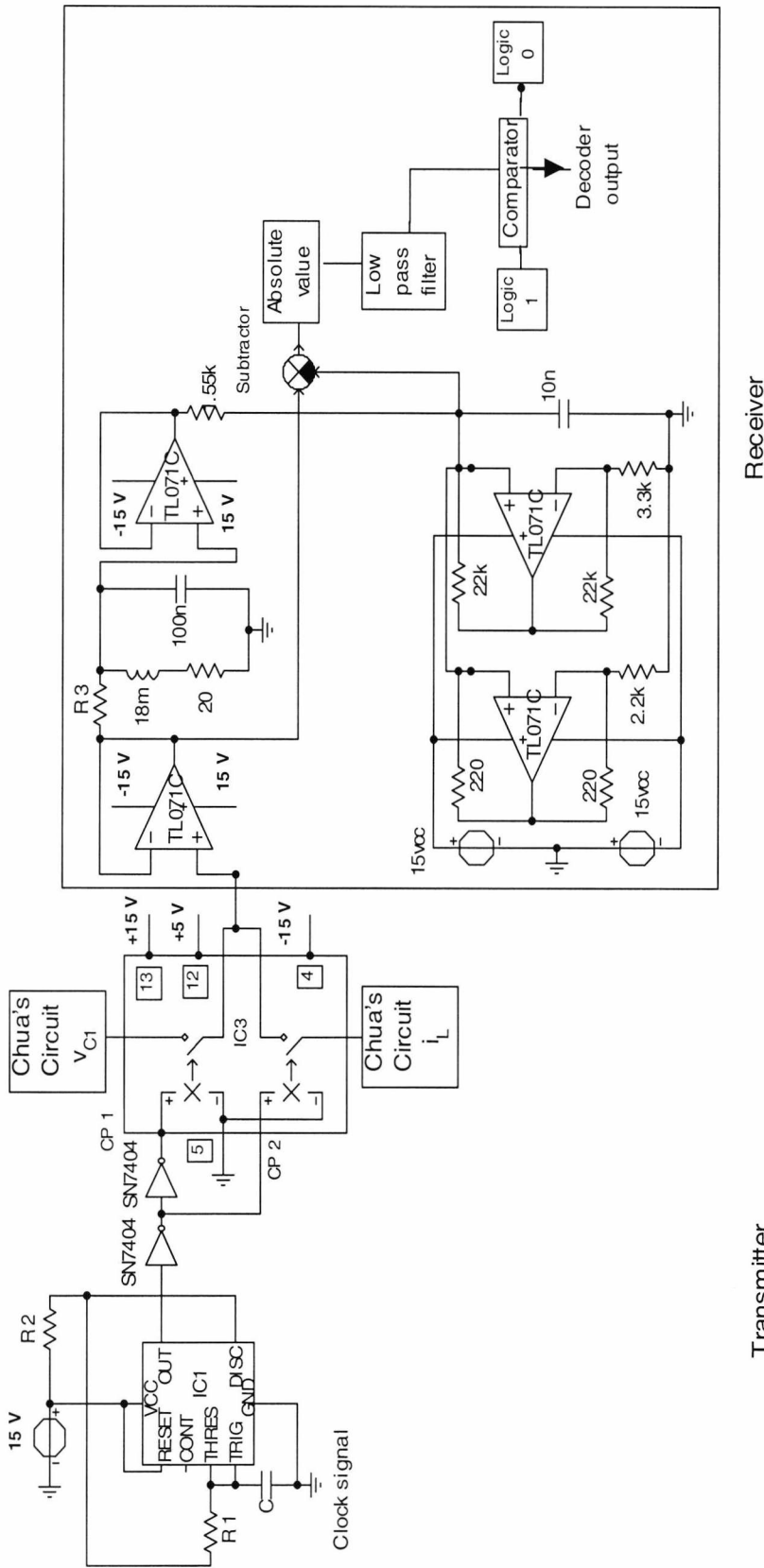


Fig. 2.32 Simplified circuit diagram of the one generator CSK.

In the circuit diagram shown in Fig. 2.32, we have the following:

1. The clock signal is equal to 200 Hz and the clock generator is implemented by using the integrated circuit NE555 [43].
2. The integrated circuit MAX314CPE is used to implement the electronic switch.
3. The chaotic generator is implemented using Chua's circuit [26].
4. The circuit diagram of the subtractor is shown in Fig 2.33.
5. The absolute value of the signal is calculated using the circuit shown in Fig. 34 [44].
6. The low pass filter is an active filter [45] with a cut off frequency of 4 kHz as shown in Fig. 2.35. The decision circuit and the decoder are implemented using the comparator circuit [46] shown in Fig. 2. 36.

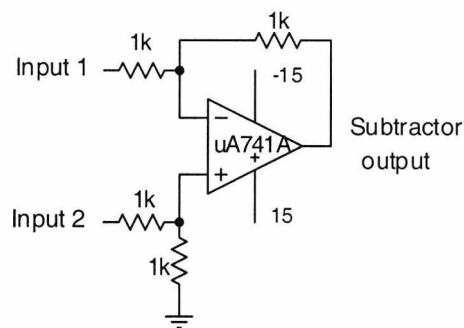


Fig. 2.33 Circuit diagram of the subtractor.

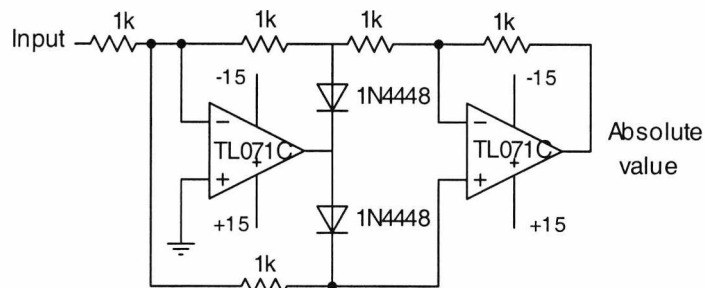


Fig. 2.34 Circuit diagram of the absolute value calculation.

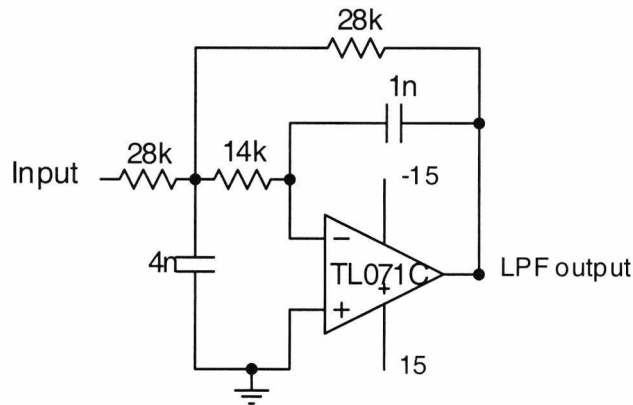


Fig. 2.35 Low-pass filter circuit diagram.

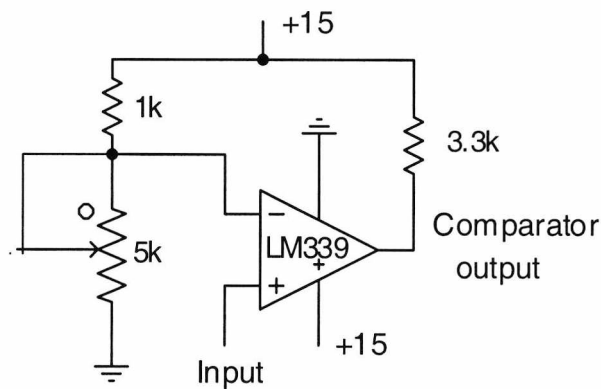


Fig. 2. 36 Comparator circuit diagram.

Fig. 2.37 shows the voltage across the capacitor C_1 and the current through the inductor L and Fig. 2.38 shows the transmitted signal and the input signal. In this case, the frequency of the input signal is 200 Hz. The receiver output signal is shown in Fig. 2.39. The upper part of Fig. 2.40 shows the absolute value of the received signal after low pass filtering and the lower part shows the recovered signal after the comparator circuit.

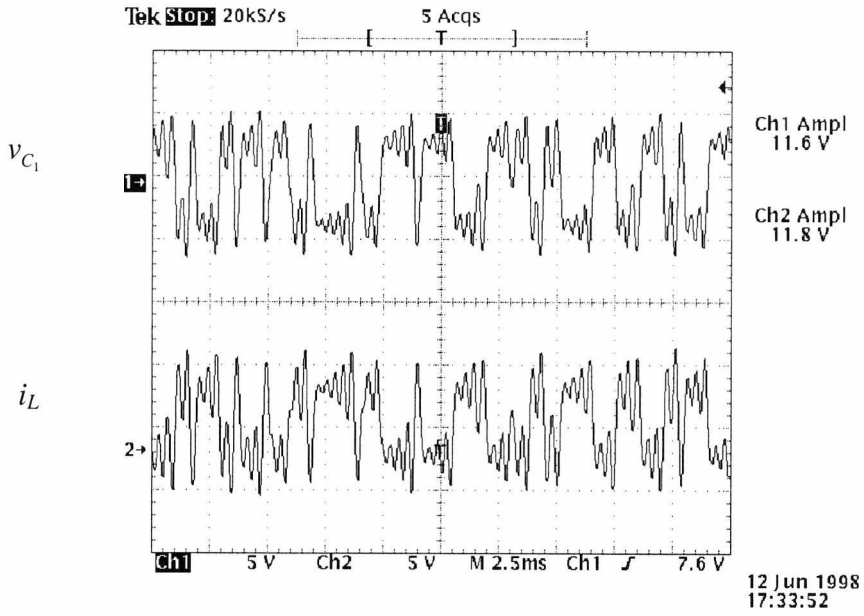


Fig. 2.37 The voltage across the capacitor C_1 and the current through the inductor L .

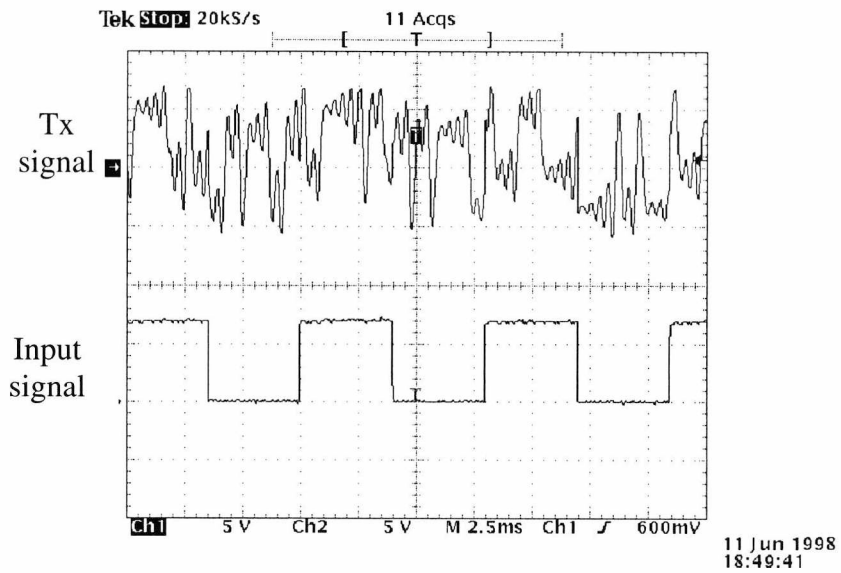


Fig. 2.38 Transmitted and input signals

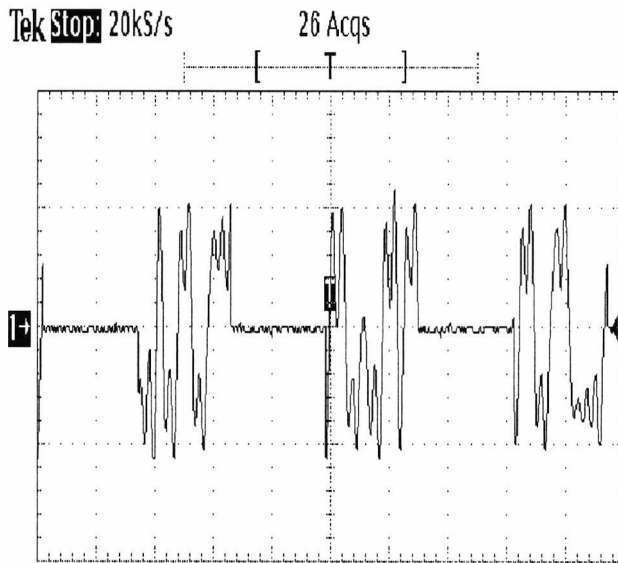


Fig. 2.39 Receiver output signal.

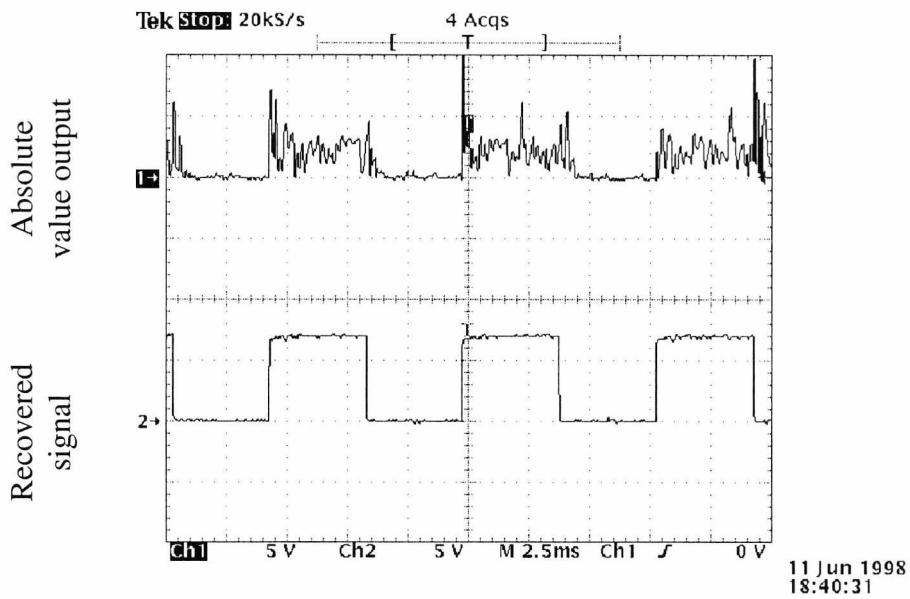


Fig. 2.40 Absolute value of the receiver output signal and the recovered signal

From the above results we can make the following comments:

1. The results show that it is possible to design a chaotic shift key using one chaotic generator with fixed parameters in the Chua nonlinear function at the transmitter and one receiver system.
2. The decoder output is the same as the input signal but there is a small delay of about 0.25 ms and the signal period is 5 ms. This delay is due to the time taken in the receiver for synchronisation after desynchronisation.
3. The recovered signal shown in Fig. 2.40 is just an inversion of the input signal and using an inverter unity gain amplifier we can get the original signal.

2.7 Conclusion

1. In this chapter, we developed a new analogue chaotic communication system (MCCS) and a modified chaos shift key system.
2. MATLAB and SIMULINK simulation results of the MCCS system show that, a SCR of -74 dB is achieved which is better than the results of OCMS system [33]. In the simulation results using the circuit simulator TINA, we succeeded in recovering the information signal at SCR= -32 dB. The simulation results of the OCMS show that, we cannot get the same results even at SCR= -12 dB. The physical implementation of the MCCS system shows that the system is easily built and the information is recovered at SCR = -24 dB. The main disadvantage of multi-channel chaotic communication system is the use of extra channel for synchronisation between the transmitter and the receiver. This disadvantage is reduced if the system is used in the transmission of more than one information signal to the same place.
3. In chaotic digital communication systems, we developed a modified chaotic shift key system using one chaotic generator and one receiver system to transmit the binary information signal. The system is simpler than systems using two chaos generators or two nonlinear Chua functions at the transmitter and two subsystems at the receiver. For the same data transmission rate we achieve similar results.

4. The information transmission rate of the one generator chaos shift key system is rather low because for each transmitted bit, we have to wait until synchronisation and desynchronisation are achieved.

2.8 References

- [1] J. M. H. Elmirghani and R. A. Cryan, "Communication using chaotic masking," *IEE Colloquium on Exploiting Chaos in Signal Processing*, pp. 12-16, 1994.
- [2] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation and Chaos*, vol. 3, No. 2, pp. 469-477, 1993.
- [3] K. M. Cuomo and A. V. Oppenheim, "Chaotic signals and systems for communication," *Proc. IEEE ICASSP'93*, vol III, pp. 137-140, 1993.
- [4] L. M. Pecora, "Overview of chaos and communications research," *Proc. SPIE in Chaos in Communications*, vol 2038, pp. 2-25, July 1993.
- [5] H. D. I. Abarbanel and P. S. Linsay, "Secure communications and unstable periodic orbits of strange attractors," *IEEE Trans. Circuits Syst. II*, vol. CAS-40, pp. 643-645, Oct. 1993.
- [6] D. R. Frey, "Chaotic digital encoding an approach to secure communication," *IEEE Trans. Circuits Syst. II*, vol. CAS-40, pp. 660-666, Oct. 1993.
- [7] L. M. Pecora and T. L. Carroll, "Synchronisation in chaotic systems," *Phys. Rev. Lett.*, vol. 64, No. 8, pp. 821-824, Feb. 1990.
- [8] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signal," *Phys. Rev. A*, vol. 44, No. 4, pp. 821-824, Aug. 1991.
- [9] T. L. Carroll and L. M. Pecora, "Synchronising chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. CAS-38, No. 4, pp. 453-456, Apr. 1991.
- [10] T. L. Carroll and G. A. Johnson, "Synchronising broadband chaotic systems to narrow-band signals," *Phys. Rev. E*, Feb. 1998.
- [11] N. F. N. Rulkov and L. S. Tsimring, "Synchronisation methods for communication with chaos over band-limited channels," *Int. J. Circuit Theory Appl.*, vol. 27, pp. 555-567, 1999.
- [12] G. Kolumban, M. P. Kennedy and L. O. Chua, "The role of synchronisation in digital communications using chaos-part II: Chaotic modulation and synchronisation," *IEEE Trans. Circuits Syst. I*, vol. 45, No. 11, pp. 1129-1140, Nov. 1998.

- [13] J. A. K. Suykens, T. Yang and L. O. Chua, "Impulsive synchronisation of chaotic Lur's systems by measurements feedback," *Int. J. Bifurcation and Chaos*, vol. 8, No. 6, 1998.
- [14] L. M. Pecora and T. L. Carroll, "Synchronised chaotic signals and systems," *Proc. IEEE ICAASSP*, 1992.
- [15] G. Kolumban, M. P. Kennedy and L. O. Chua, "The role of synchronisation in digital communications using chaos-part II: Chaotic modulation and synchronisation," *IEEE Trans. Circuits Syst. I*, vol. 45, No. 11, pp. 1129-1140, Nov. 1998.
- [16] R. N. Madan, *Chua's circuit: A Paradigm for Chaos*. Singapore: World Scientific, 1993.
- [17] L. Kocarev and U. Parlitz, "General approach for chaotic synchronisation with applications to communication," *Phys. Rev. Lett.*, vol. 74, pp. 5028-5031, June 1995.
- [18] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring and H. D. Abarbanel, "Generalised synchronisation of chaos in directional coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp. 980-994, Feb. 1995.
- [19] L. M. Pecora, T. L. Carroll, G. A. Johnson and D. J. Mar, "Fundamentals of synchronisation in chaotic systems, concepts and applications," *Chaos*, vol. 7, No. 4, pp. 520-542, 1997.
- [20] A. I. Panas, "Synchronisation of drive-response systems on condition of a large mismatch of parameters," *IEEE Int. Symposium. on Circuit and System (ISCAS 98)*, 1998.
- [21] Chi-Chung Chen and Kung Tao, "Basic issues in chaotic communication systems," *Proc. 7th Int. Conf. on Advances in Communications and Control (COMCO N'99)*, June 1999.
- [22] K. M. Cumomo, A. V. Oppenheim and S. H. Strogatz, "Synchronisation of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II*, vol. CAS-40, pp. 626-633, 1993.
- [23] K. M. Cumomo and A. V. Oppenheim, "Circuit implementation of synchronised chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, July 1993.

- [24] M. Itoh, H. Murakami and L. O. Chua, "Communication systems via modulations," *IEICE Trans. Fundamentals*, vol. E77-A, No. 6, June 1994.
- [25] M. Itoh and H. Murakami, "New communication system via chaotic synchronisations and modulations," *IEICE Trans. Fundamentals*, vol. E78-A, No. 3, Mar. 1995.
- [26] M. Itoh and L. O. Chua, "Experimental study of forced Chua's oscillator," *ECCTD'95 European Conference on Circuit Theory & Design*, 1995.
- [27] H. Dedieu, M. P. Kennedy and M. Hasler, "Chaos shift keying modulation and demodulation of a chaotic carrier using self-synchronising Chua's circuits," *IEEE Trans. Circuits Syst. II*, vol. CAS-40, No. 10, Oct. 1993.
- [28] A. Sato and T. Endo, "Experiments of secure communications via chaotic synchronisation of phase-locked loops," *IEICE Trans. Fundamentals*, vol. E78-A, No. 10, Mar. 1995.
- [29] M. P. Kennedy, "Experimental chaos via Chua's circuit," *Proc. 1st Experimental Chaos Conference*, pp. 340-351, World scientific, 1992.
- [30] Eva Pärt-Enander and Anders Sjöberg, *The MATLAB 5 handbook*: Addison Wesley Longman Limited, 1999.
- [31] Tina pro 5.5, Copyright © by Design Soft, 1997.
- [32] L. Kocarev, K. S. Halle, K. Eckert and L. O. Chua, "Experimental demonstration of secure communications via chaotic synchronisation, Chua's circuit: A Paradigm for Chaos," pp. 371-378, Singapore: World Scientific, 1993.
- [33] A. Sato and T. Endo, "Experiments of secure communications via chaotic synchronisation of phase-locked loops," *IEICE Trans. Fundamentals*, vol. E78-A, No. 10, pp. 1286-1290, Oct. 1995.
- [34] M. P. Kennedy and H. Dedieu, "Experimental demonstration of binary chaos shift keying using self-synchronising Chua's circuits," *Proc. 1st Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'93*, pp. 67-72, 1993.
- [35] G. Kolmban, B. Vizvari, W. Schwarz and A. Abel, "Differential chaos shift keying A robust coding for chaotic communication," *Proc. 1st Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'93*, pp. 87-92, 1993.

- [36] M. Hasler, "Synchronisation of chaotic systems and transmission of information," *Int. J. Bifurcation and Chaos*, vol. 8, No. 4, pp-647-659, 1998.
- [37] U. Parlitz, L. O. Chua, Lj. Kocarev and K.S Shang, "Transmission of digital signals by chaotic synchronisation," *Int. J. Bifurcation and Chaos*, vol. 2, pp. 973-977, 1993.
- [38] G. Kis, Z. Jako, M. P. Kennedy and G. Kolmban, "Chaotic communications without synchronisation," *6 th. IEE Conference on Telecommunications*, pp. 49-53, 1998.
- [39] G. Kolumban, H. Dedieu, J. Schweizer, J. Ennitis and B. Vizvari, "Performance evaluation and comparison of chaos communication systems," *Proc. 4 th Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'96*, pp. 105-110, 1996.
- [40] G. Kolumban, JB. Vizvari, W. Schwarz and A. Abel, "Differential chaos shift keying A robust coding for chaotic communication," *Proc. 4 th Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'96*, pp. 87-92, 1996.
- [41] Z. Jako, G. Kis, G. Kolumban and M. P. Kennedy, "Design of large signal set for DCSK modulations," *6 th. IEE Conference on Telecommunications*, pp. 44-48, 1998.
- [42] M. Ogorzalek, "Taming chaos-I: Synchronisation," *IEEE Trans. Circuits Syst. I*, vol. CAS-40, No. 10, Oct. 1993.
- [43] C. J. Savant, M. S. Rodengordon and L. Carpenter, *Electronic Design, circuits and system*: Benjamin/Cummings Publishing Company, Inc., 1991.
- [44] J. Batten and L. George, *Design and application of linear computational circuit*: Tab books Inc., 1987.
- [45] C. Wai-Kai, *The circuits and filters handbook*: CRC Press, 1995.
- [46] J. D. Lenk, *Handbook of practical electronic circuits*: Prentice-Hall, 1982.

Chapter 3

DIRECT REPRESENTATION OF THE CHAOTIC STATE EQUATIONS WITH REALTIME IMPLEMENTATION

3.1 Introduction

In this chapter, we develop a new method to implement chaotic generators (continuous or discrete) and chaotic communication systems given by the state equations or a circuit in real time. The method is developed to overcome the following problems:

- Not all chaotic systems are represented by a physical circuit. The developed method is used to implement chaotic systems that are defined by state equations when it needs a complicated circuit to implement it.
- The method solves the problem of component mismatch between the transmitter and the receiver in analogue chaotic communication systems implemented by physical circuits. A software model of the chaotic system integrated with a data acquisition card replaces the physical circuit.

Many methods that use analogue circuits have been proposed in the field of chaotic communication systems [1]-[11]. One deficiency of these systems is that we must build both the transmitter and the receiver with very high component accuracy to ensure correct information recovery, since the recovery characteristics are very sensitive to parameter mismatch between the transmitter and the receiver. However, in practical situations, it is difficult to build both the transmitter and the receiver with very high component accuracy since the component values are function of aging, temperature...etc. Therefore the analogue implementation seems very difficult though it is not impossible to overcome these difficulties to some extent. There are several techniques to implement chaotic generators in digital form.

Namely, using switched capacitor techniques [12], VLSI [13]-[18], analogue CMOS technology [19] and DSP processors [20]-[21].

The developed method is a combination between the hardware (National instruments data acquisition card Lab-PC-1200) and the software (SIMULINK, Real Time Workshop and Real Time Target Window) as shown in Fig. 3.1. All the above mentioned software programs are toolboxes within MATLAB.

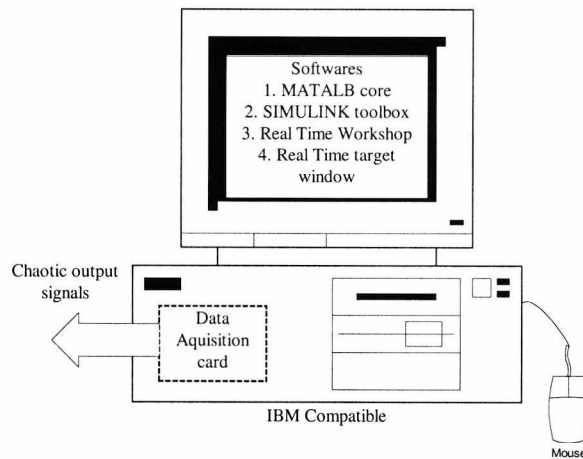


Fig. 3.1 Block diagram of the real time system.

In section 3.2, a brief description of the developed real time system is introduced showing the function of each part of the system. The real time implementation of continuous and discrete chaos generators, using the developed method, is presented in section 3.3. Section 3.4 demonstrates an example of how to implement the chaotic communication systems in real time using the developed method. Section 3.5 is the conclusion of the chapter and section 3.6 is the chapter references.

3.2 Real time system description

3.2 .1 Software description

3.2.1.1 MATLAB

MATLAB is a high-performance language for technical computing [22]. It integrates computation, visualization and programming in an easy-to-use environment where the problems and the solutions are expressed in familiar mathematical notation. The

basic data element of MATLAB is an array that does not require dimensioning. This allows solving of many technical-computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in other language such as C or Fortran. MATLAB features a family of application-specific solutions called toolboxes. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, real time workshop, real time target and many others. Typical usage include:

- Mathematical computations.
- Algorithm development.
- Modelling, simulation and prototyping.
- Data analysis, exploration and visualisation.
- Scientific and engineering graphics.
- Application development including of building graphical user interfaces.

3.2.1.2 SIMULINK

SIMULINK is a software package for modelling, simulating and analysing dynamical systems. It supports linear and nonlinear systems, modelled in continuous time, discrete time or a hybrid of the two. For modelling, SIMULINK provides a graphical user interface (GUI) for building models as block diagrams using click-and-drag mouse operations. With this interface, we can draw the models just as we would with pencil and paper. This is different from previous simulation packages that require the formulation of differential equations and difference equations in a language or program. After we define a model, we can simulate it using a choice of integration methods either from the SIMULINK menus or by entering commands in the MATLAB command window.

3.2.1.3 Real Time Workshop (RTW)

The real time workshop complements SIMULINK by providing automatic C code generation directly from SIMULINK models. We can design the system using MATLAB and SIMULINK and generate a code from the block diagram model. We

can then compile and download the code directly to the target hardware. The RTW supports the WATCOM C++ version 11 and Visual C++ version 6. The RTW supports the execution of dynamical system models on a wide range of computer platforms, including real time hardware, to allow real time simulation and rapid prototyping. With the RTW, we can quickly generate C code for discrete time and hybrid systems. With the RTW, we can run the SIMULINK model in real time on a remote processor. We can run accelerated, stand-alone simulations on the host machine or on an external computer. The RTW provides a real time development environment that features:

- A rapid and direct path from system design to hardware implementation.
- Seamless integration with MATLAB and SIMULINK.
- A simple and easy-to-use interface.
- An open and extensible architecture.

The RTW supports a variety of real time applications such control systems, measurement systems and signal processing systems.

3.2.1.4 Real time windows target

The real time windows target is a turnkey, single PC windows target for C code generated by real time workshop. It used to connect the real time model with the data acquisition card. It is ideal for real time control, real time signal processing, rapid prototyping and other applications.

3.2.2 Hardware

The real time window target supports several hardware products of many companies (National instruments, Analogue devices, Keithley...etc). The hardware is the data acquisition card. In our system we use National instruments (Lab-PC-1200) data acquisition card. The sampling rate is up to 100 ksamples/s, 12-bit performance on 8

single-ended analogue inputs. The 1200 family boards feature two 12-bit analogue outputs and 24 digital I/O lines.

3.2.3 Real time model generation

The steps of the real time model is summarised as follows:

1. Determine the state equations of the chaotic system if it is represented by an electronic circuit.
2. Convert the state equations to a SIMULINK model.
3. Run the SIMULINK model in the internal mode (not real time) and verify that it is working properly.
4. Add the real time input ports (RT in), output ports (RT out) and the adapter blocks to the SIMULINK model. The function of each block is as follows:
 - **RT in** is the real time input that connects the model to one of the analogue input channels of the data acquisition card (Lap-PC 1200).
 - **RT out** is the real time output that connects the model to one of the analogue output channels of the data acquisition card (Lap-PC 1200).
 - **Adapter** is used to define the data acquisition card to the model.
5. Define the sampling rate of the real time input and output ports. The sampling rate should be the same as the time step used in the model parameter menu.
6. Convert the model to the external mode and built the real time model using the real time workshop and the visual C++ compiler or WATCOM C++ compiler.
7. Connect the model to the target (data acquisition card) from the SIMULINK model parameter menu.
8. Now the model is ready to run by clicking start from the parameter menu.

3.3 Real time chaotic generators

3.3.1 Continuous time chaotic generators

3.3.1.1 Real time Chua chaotic generator

Chua's circuit is one of the simplest autonomous circuits that can exhibit bifurcation and chaos [23]. The circuit diagram is shown in chapter 2 (Fig. 2.5). It has been studied extensively and the formal proof of the existence of chaos has been accomplished [24]. The state equations of Chua's circuit are given by

$$\begin{aligned} \dot{v}_{C_1} &= \frac{G}{C_1}(v_{C_2} - v_{C_1}) - \frac{1}{C_1}g(v_{C_1}) \\ \dot{v}_{C_2} &= \frac{G}{C_2}(v_{C_1} - v_{C_2}) + \frac{1}{C_2}i_L \\ i_L &= -\frac{1}{L}v_{C_2} \end{aligned} \quad (3.1)$$

where $g(v_{C_1})$ is the characteristic of the nonlinear resistor and it is given by

$$g(v_{C_1}) = m_o v_{C_1} + 0.5(m_o + m_1)(|v_{C_1} + B_p| - |v_{C_1} - B_p|). \quad (3.2)$$

The component values of the Chua chaos generator are given in table 3.1.

Component	Value	Component	Value
C_1	10 nF	L	18 mH
G	0.63 mS	m_o	-0.309 mS
C_2	100 nF	m_1	-0.758 mS
B_p	1.0 V		

Table 3.1 Component list of piecewise linear Chua chaotic generator.

One advantage of our method of implementation is that we can introduce any mathematical expression for the Chua nonlinear function even if it cannot be implemented using a physical circuit. We introduce a new nonlinear function of the Chua nonlinear resistor, which is given by

$$g(v_{C_1}) = -a \tanh(bv_{C_1}) \quad (3.3)$$

where a and b are constants and $a=2$ and $b=0.38$. The characteristic of this nonlinear function is shown in Fig. 3.2.

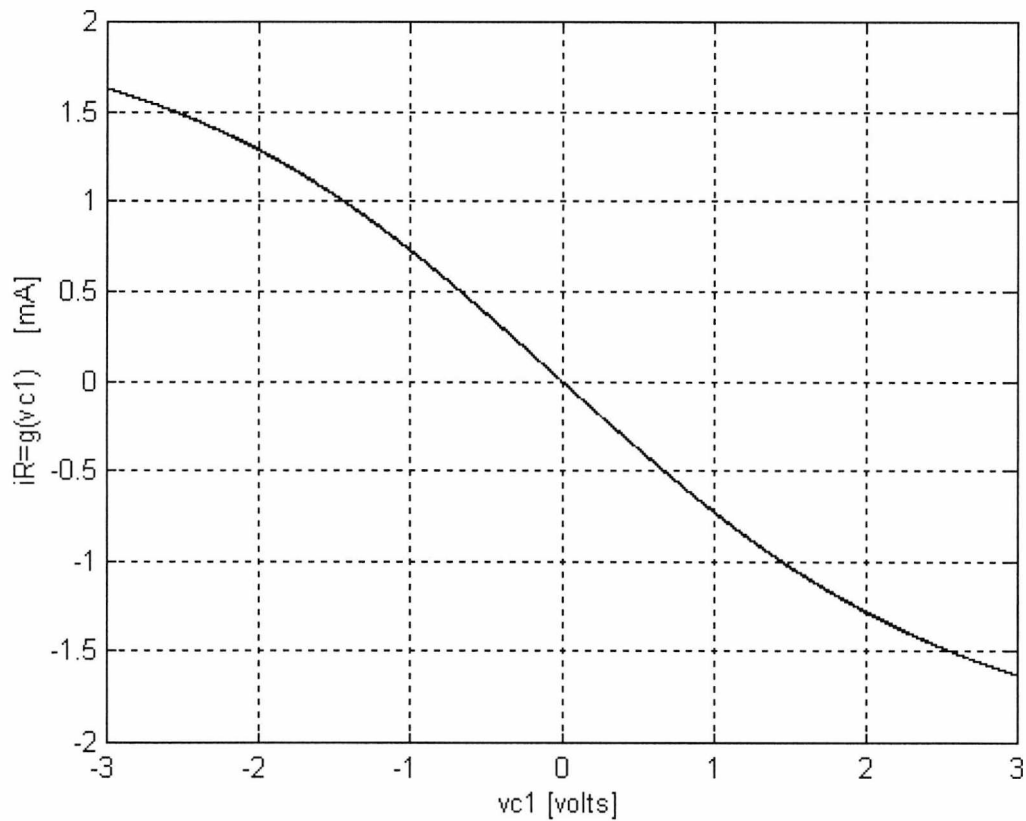


Fig. 3.2 Nonlinear characteristic of Chua diode.

The real time model of the Chua chaotic generator is shown in Fig. 3.3. The scaling factors S_1 , S_2 and S_3 are used to control the frequency band of the output signals. The scaling factors are chosen to be 1000 to have chaotic signals in the frequency band from 0 to 10 kHz.

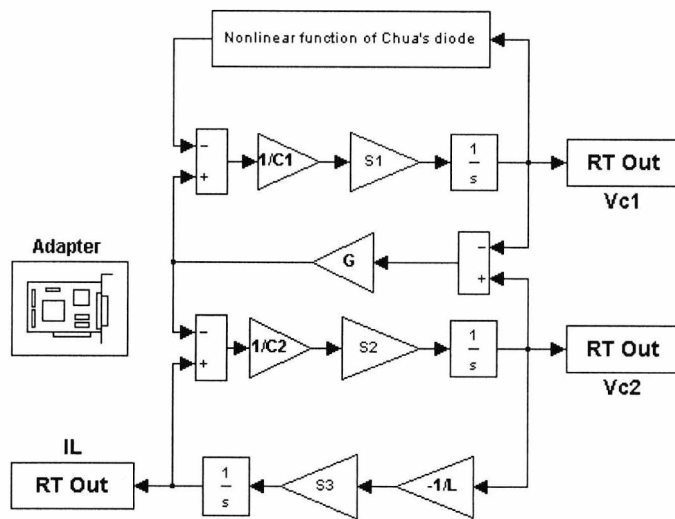


Fig. 3.3 Real time Chua chaotic generator.

Fig. 3.4 shows the results of the simulation of Chua's circuit. Figs. 3.5, 3.6 and 3.7 are the measured outputs of the real time Chua chaotic generator using a Tektronix TDS 360 oscilloscope. The results show that the simulation and the measurement give similar outputs. The results are also the same as the results of the Chua implemented using a physical circuit [23] but with the flexibility of changing the system parameters and controlling the frequency band of the chaotic output. The results prove that the developed method can be used to implement a chaotic system that is defined by the state equations or a circuit such as a Chua chaotic generator.

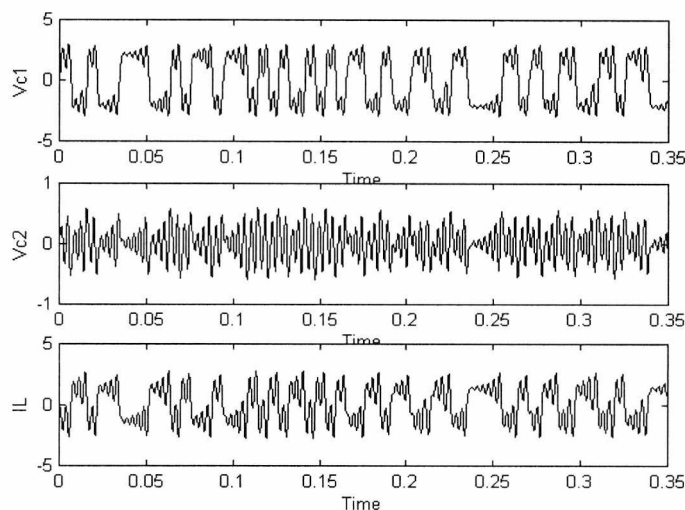


Fig. 3.4 Simulation results of the Chua chaotic generator.

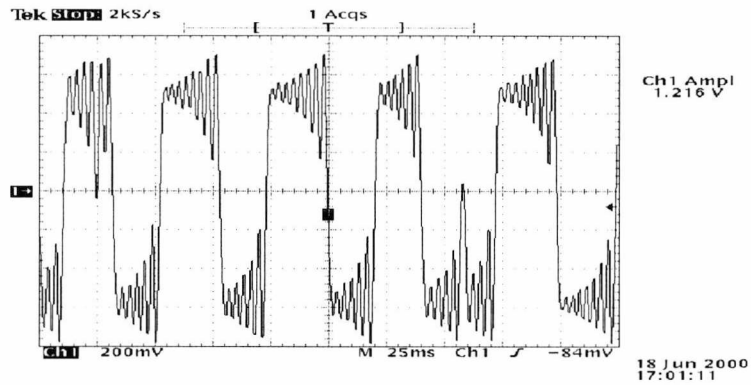


Fig. 3.5 Measured capacitor voltage v_{c_1} .

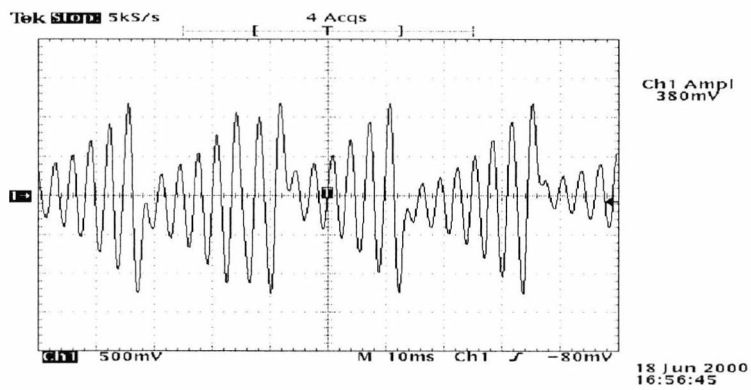


Fig. 3.6 Measured capacitor voltage v_{c_2} .

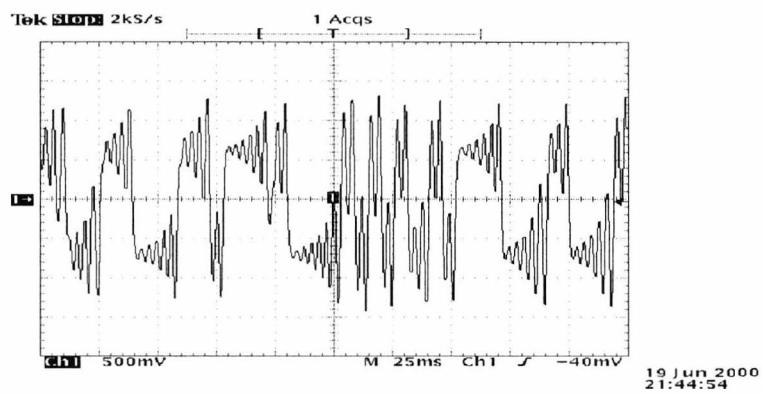


Fig. 3.7 Measured current through the inductor L .

3.3.1.2 Real time Rössler chaotic generator

The state equations of the Rössler chaotic generator are given by [25]

$$\begin{aligned} \dot{x} &= -y - z \\ \dot{y} &= x + Ay \\ \dot{z} &= B + z(x - C) \end{aligned} \tag{3.3}$$

where A , B and C are constants and $A = 0.398$, $B = 2$ and $C = 4$. The real time Rössler model is shown in Fig. 3.8. The scaling factors of the real time model are equal 1000 to have chaotic signals in the frequency range from 0 to 10 kHz. The simulation results are shown in Fig. 3.9. The real time measured results using the developed method are shown in Figs. 3.10, 3.11 and 3.12. The results illustrate that using the developed real time method, the simulation results and the measured results are same. The results prove that the developed method can be used to implement the chaotic systems that are defined by state equations such as Rössler chaotic generator.

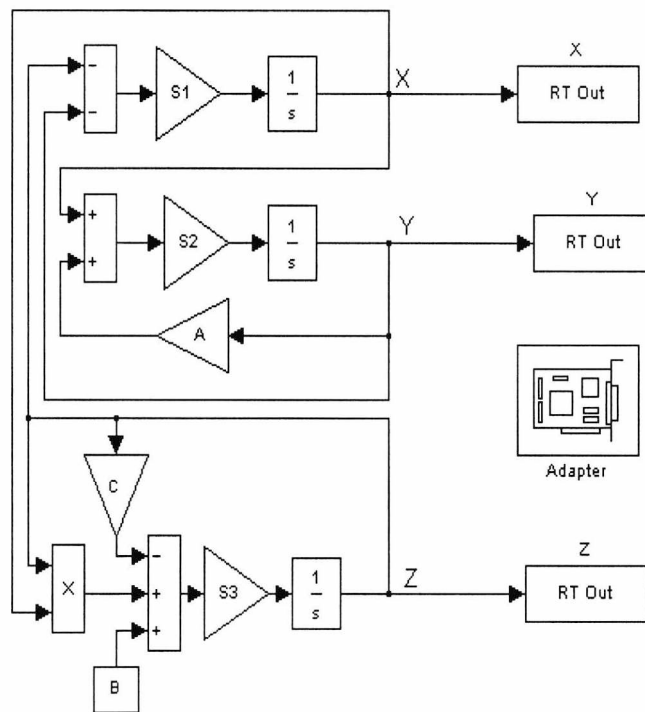


Fig. 3.8 Real time Rössler chaotic generator.

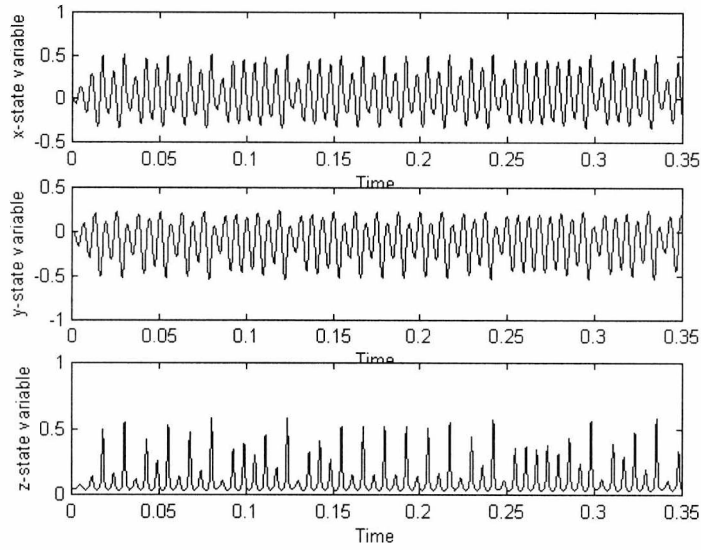


Fig. 3.9 Simulation results of Rössler chaos generator

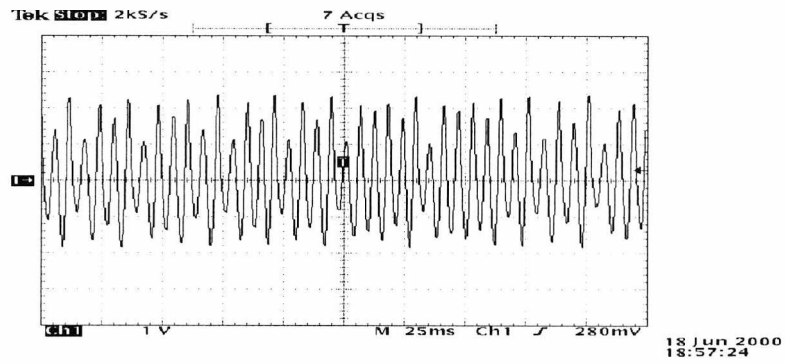


Fig. 3.10 Measured x state variable of real time Rössler generator.

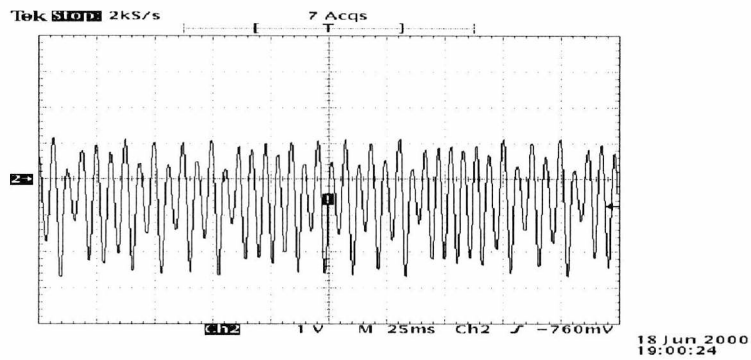


Fig. 3.11 Measured y state variable of real time Rössler chaotic generator

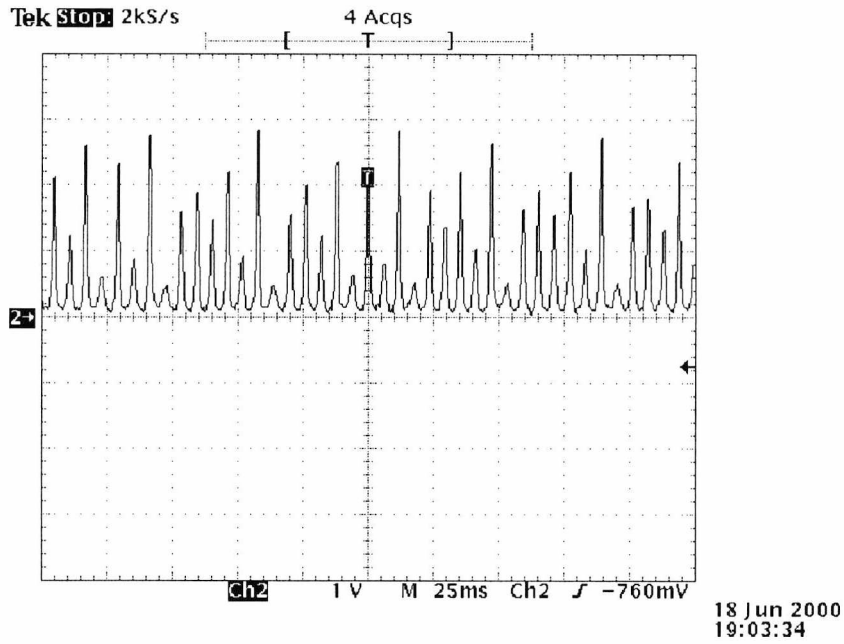


Fig. 3.12 Measured z state variable of real time Rössler chaotic generator.

3.3.1.3 Real time Lorenz chaotic generator

The state equations of the Lorenz chaotic generator are given by [26]

$$\begin{aligned}
 \dot{u} &= A (v - u) \\
 \dot{v} &= B u - v - 20 u w \\
 \dot{w} &= 5 u v - C w
 \end{aligned}
 \tag{3.5}$$

where A , B and C are constants and $A = 10$, $B = 28$ and $C = 2.6667$. The real time model of the Lorenz chaotic generator is shown in Fig. 3.13. The scaling factors S_1 , S_2 and S_3 are chosen to be 1000 to have chaotic signals in the frequency range from 0 to 10 kHz. The simulation results of Lorenz chaotic generator are shown in Fig. 3.14. The measured output signals are illustrated in Figs. 3.15, 3.16 and 3.17. The results indicate that using the developed real time method the simulation and the measurement results are the same.

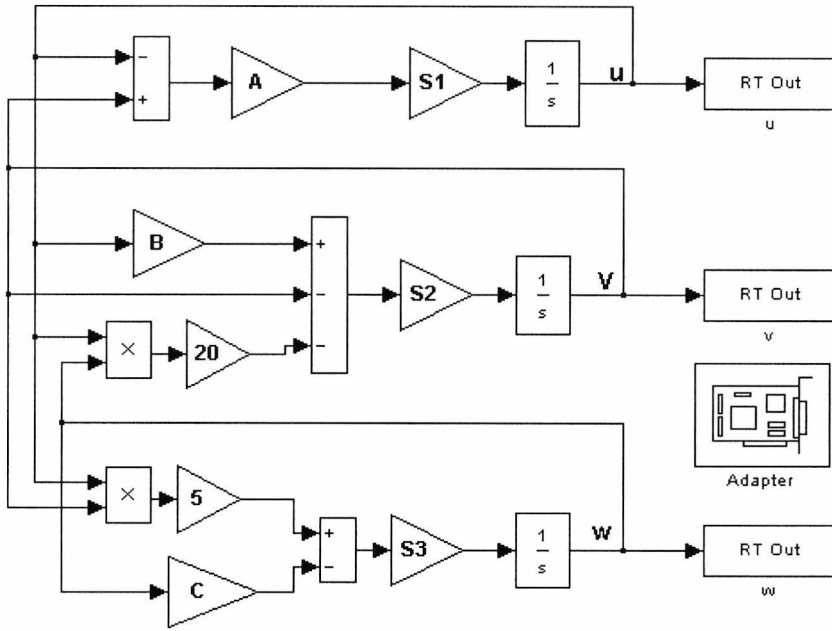


Fig. 3.13 Real time Lorenz chaotic generator.

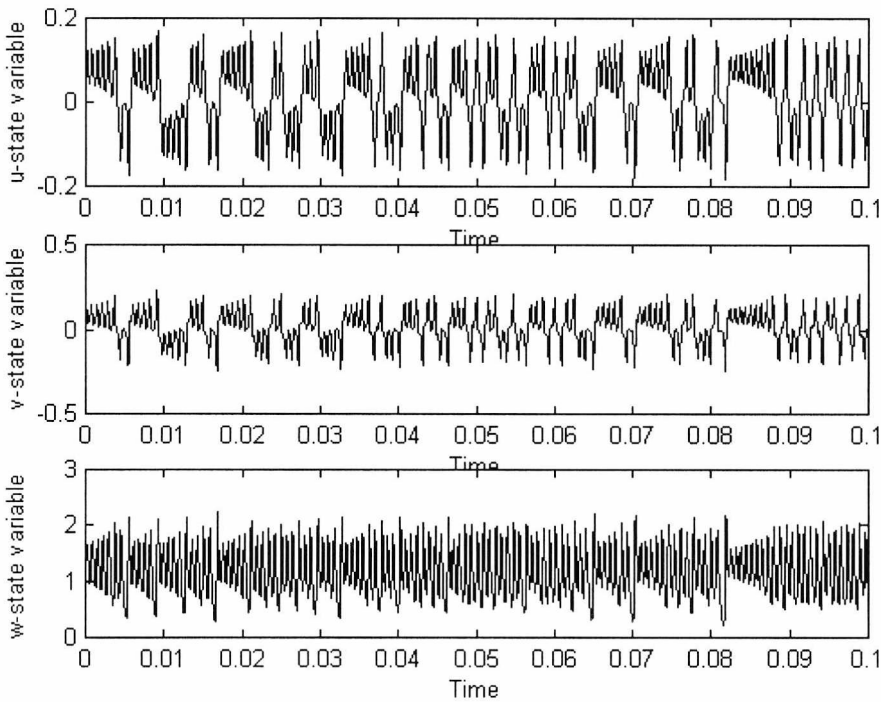


Fig. 3.14 Simulation results of the Lorenz chaotic generator.

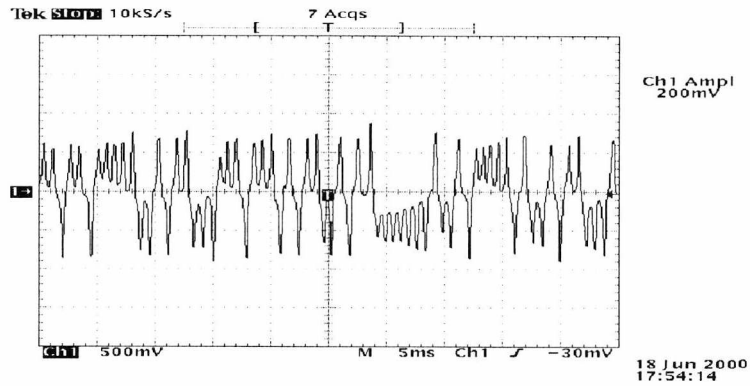


Fig. 3.15 Measured u state variable of the real time Lorenz chaos generator.

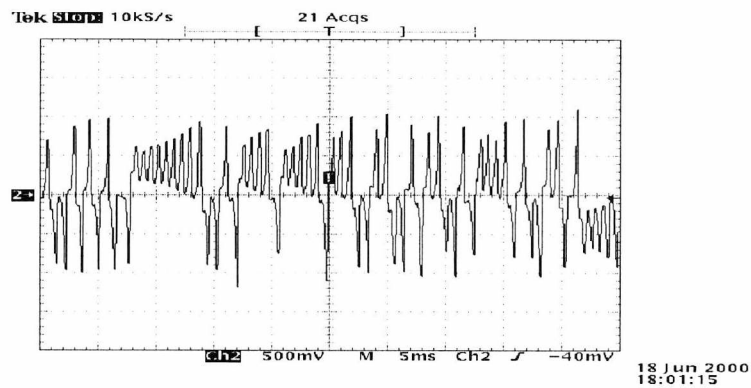


Fig. 3.16 Measured v state variable of the real time Lorenz chaos generator

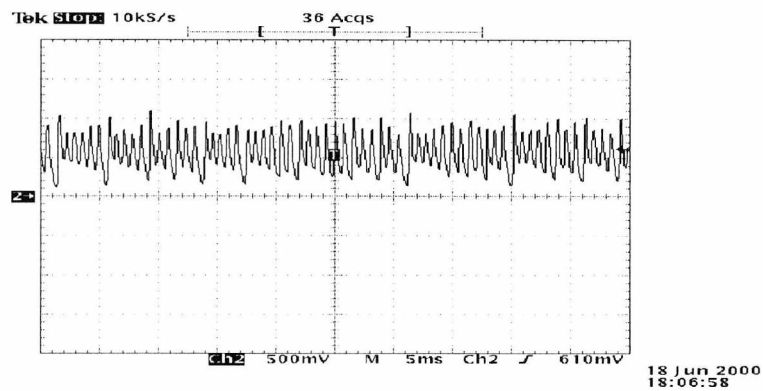


Fig. 3.17 Measured w state variable of the real time Lorenz chaotic generator.

3.3.2 Discrete time chaos generator

3.3.2.1 Henon map chaotic generator

The state equations of the generator are given by [27]

$$\begin{aligned} x_{n+1} &= 1 + y_n - ax_n^2 \\ y_{n+1} &= bx_n \end{aligned} \quad (3.6)$$

where a and b are constants and $a=1.4$ and $b=0.3$. The real time model of the Henon map chaotic generator is shown in Fig. 3.18. The simulation results are shown in Fig. 3.19. The measured results are illustrated in Figs. 3.20 and 3.21. The results show that the simulation and the measured results are same.

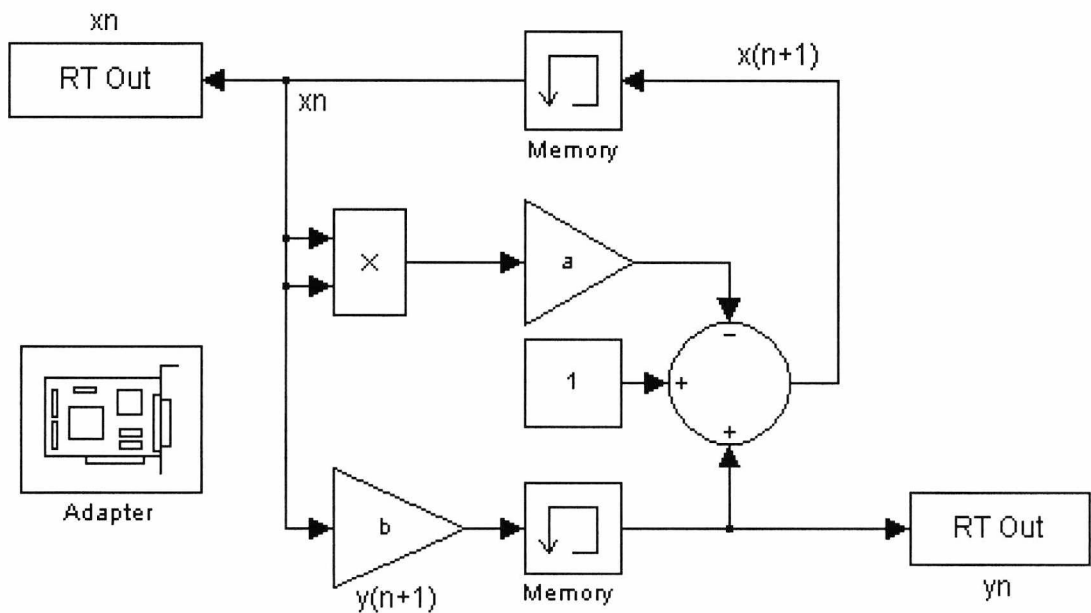


Fig. 3.18 Real time Henon map chaotic generator.

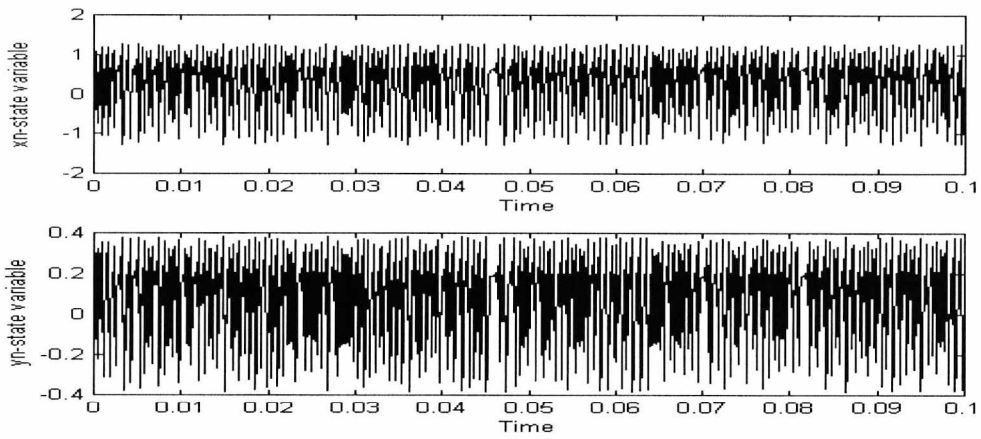


Fig. 3.19 Simulation results of the Henon map.

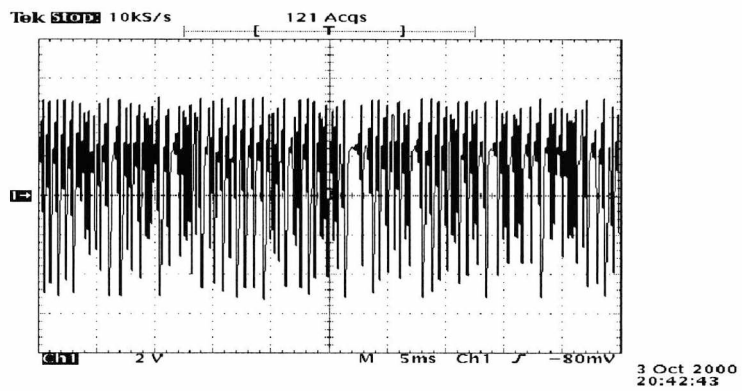


Fig. 3.20 Measured $x(n)$ state variable.

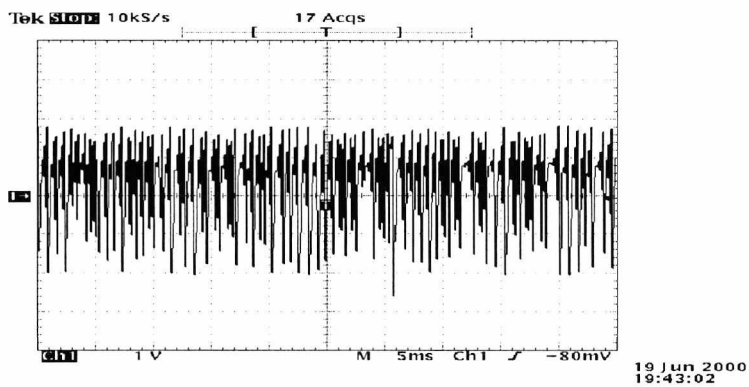


Fig. 3.21 Measured $y(n)$ state variable.

3.4 Real time chaotic communications system

In this section, we introduce an example of how to implement a real time chaotic communications system. The general block diagram of the system is shown in Fig. 3.22.

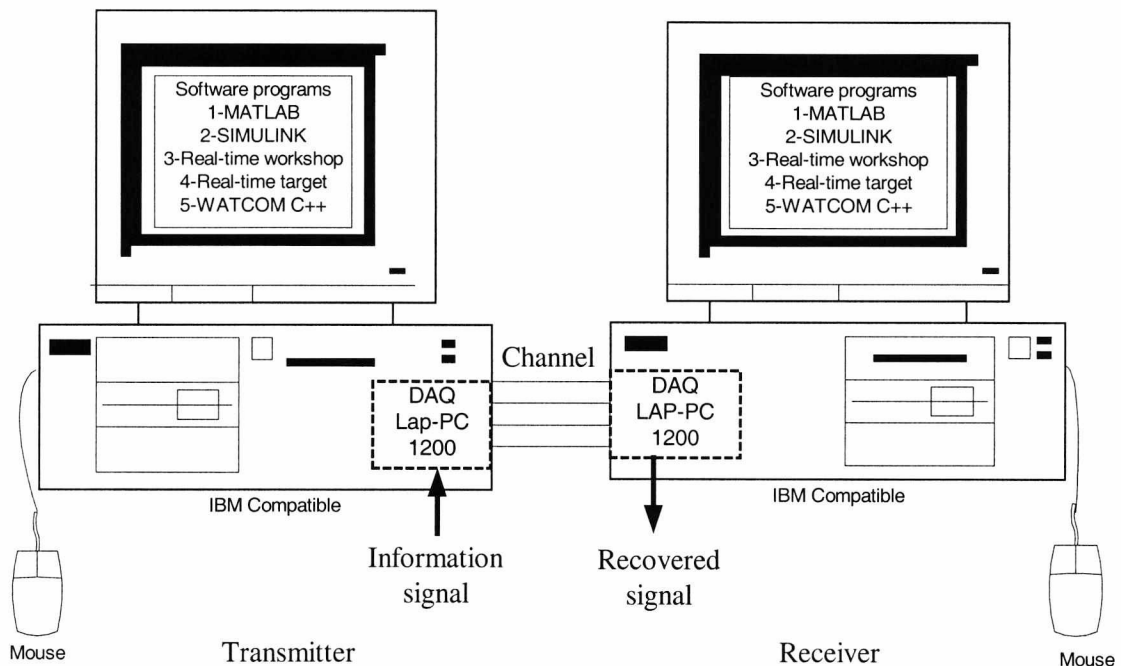


Fig. 3.22 Block diagram of real time chaotic communications system.

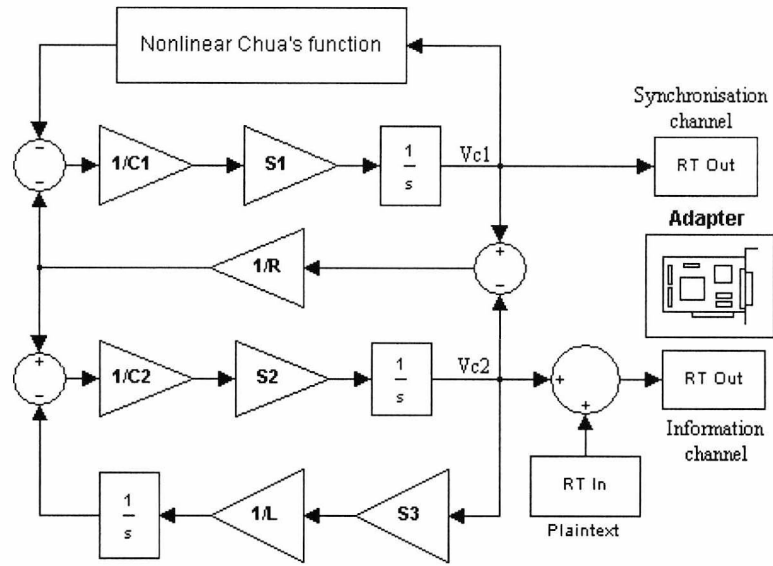
The system works as follows:

1. The transmitter.

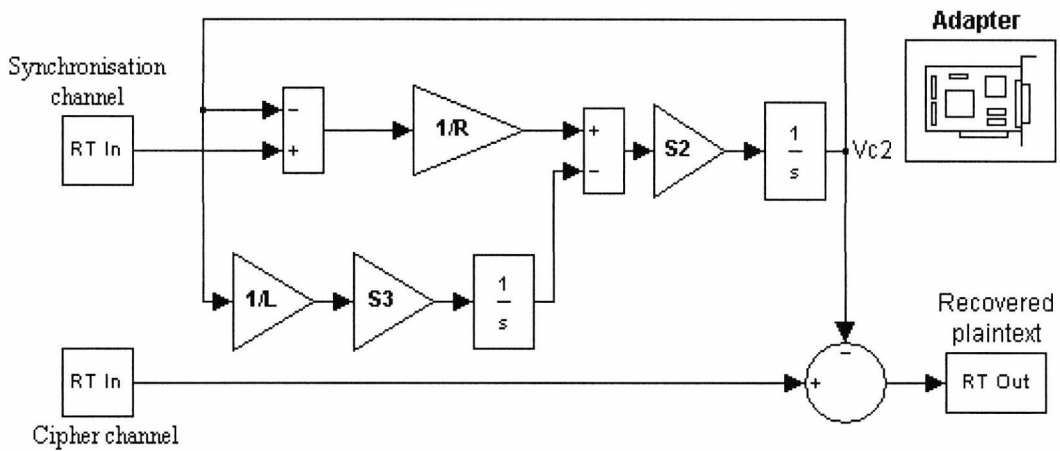
- The transmitter is built as a real time model as in the previous examples.
- The transmitter is connected to the data acquisition card from the transmitter control menu.
- The information source is connected to one of the input ports of the data acquisition card at the transmitter.
- The transmitter model is compiled using WATCOM C++ to generate the C code and the executable program.

- The transmitter is now ready to run and transmit the chaotic transmitted signal to the receiver.
2. The channel
 - A physical channel is achieved between the transmitter and the receiver by connecting the real time output port (transmitted chaotic signal) of the transmitter to the real time input port (received chaotic signal) of the receiver.
 3. The receiver
 - The receiver model is built in real time using the developed method.
 - In the receiver model, we must use the same time step, solver and parameter values as in the transmitter.
 - An oscilloscope is connected to one of the output ports of the data acquisition card to monitor the recovered signal.
 - The receiver model is compiled using WATCOM C++ to generate the C code and the executable program.
 - The receiver model is connected to the data acquisition card from the receiver model menu.
 - The receiver is ready to run and recovered the information signal.

The system is tested using the multi-channel chaotic communication system (MCCS) introduced in Chapter 2 (section 2.4). The real time system model is shown in Fig. 3.23. The measurement results are shown in Figs. 3.24, 3.25 and 3.26. The upper part of Fig. 3.24 is the synchronisation signal while the lower part is the chaotic transmitted signal with a signal to chaos ratio of -14 dB. Fig. 3.25 shows the input signal and the recovered signal is shown in Fig. 3.26. The figure shows that the real time receiver system succeeds in recovering the information signal from the chaotic transmitted signal.



a- Transmitter.



b- Receiver.

Fig. 3.23 Block diagram of the multi-channel chaotic communication system using the developed method.

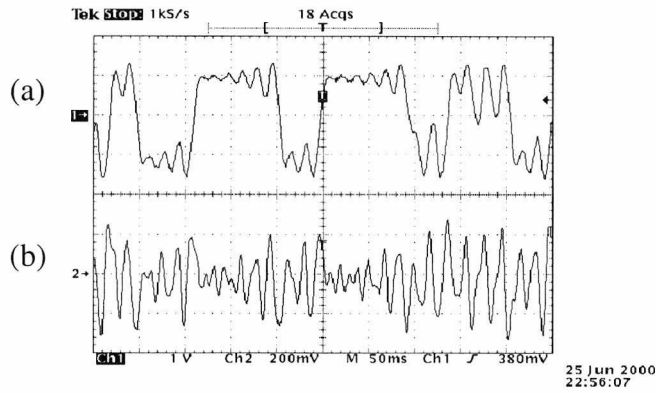


Fig. 3.24 Measured (a) Synchronisation signal.
(b) Transmitted signal.

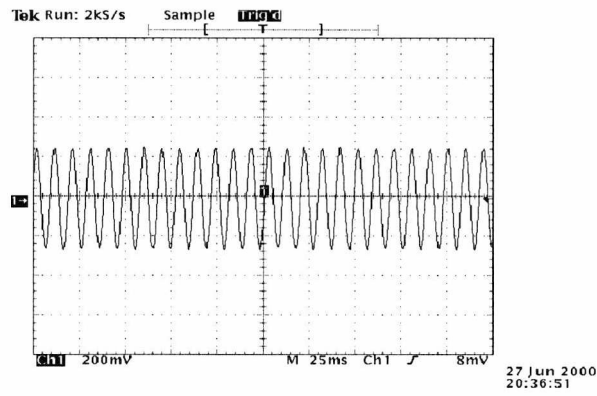


Fig. 3.25 Measured input signal.

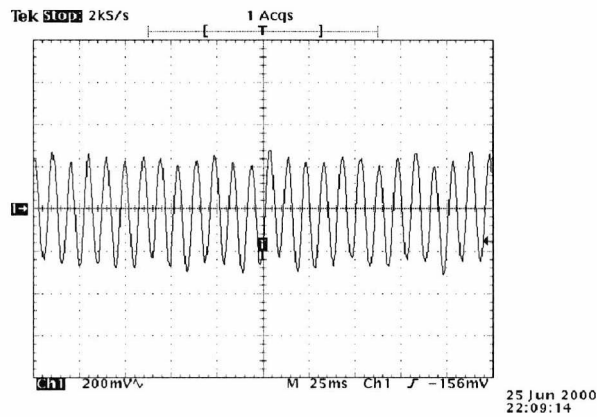


Fig. 3.26 Measured recovered signal.

By comparing the MCCA implemented using the developed real time method with the MCCA implemented by a physical circuit (chapter 2 (section 2.4)), we conclude the following:

1. The results of the circuit implementation of the MCCA (SCR=-24 dB) are better than the results of the real time system (SCR=-14 dB). The reasons of that are:
 - The real time system is tested on a computer with AMD233 processor. The clock of the processor is 233 MHz so the minimum step size that can be used is 0.0005 seconds and this imposes a limitation on the accuracy of the numerical integration solver.
 - The data acquisition card has no reconstructing circuitry (LPF) at its outputs that can be used to decrease the spikes in the recovered signal.
2. The implementation of the MCCA system using the developed real time method is very easy. In this method, we just draw the block diagram of the system using the state equations and define the data acquisition card in the block diagram. The modification of the system is easy since it requires changing the block diagram of the system or changing the parameter values.
3. The problem of component accuracy, which appears in the circuit implementation, is absent here because in the developed real time method we have parameter values not physical component values.
4. The cost of the developed real time system is higher than the circuit implementation of the system. But the cost is decreased when we transmit more than one information signal to the same place using the facilities of the data acquisition cards. Every data acquisition card has several input channels (either 8, 16 or 64) and these channels can be used to transmit several informational signals without any additional hardware. A small modification in the block diagram is required (software).

3.5 Conclusion

A new method to implement chaotic generators and chaotic communication systems in real time is developed. The developed method is capable of implementing the chaotic systems that are given by state equations in real time. This method is established to solve the synchronisation problem present in the chaotic systems implemented by analogue circuits. The method is implemented by MATLAB, SIMULINK, real time workshop, real time target window and the data acquisition card Lab-PC-1200. The method is useful for the implementation of chaotic generators at low frequencies (in the order of a few kHz). The method is used to implement continuous (Chua, Rössler and Lorenz) and discrete (Henon map) chaotic generators. A new nonlinear expression for the Chua nonlinear function is introduced. The developed method is utilised to achieve communication between two computers using the multi-channel chaotic communication system. The advantages and the disadvantages of this method can be summarised as follows:

1. Advantages

- It can be used to implement chaotic generators that are described by state equations and cannot be implemented by a physical circuit.
- It is easy to use and the modification of any system is a simple change in the block diagram or the parameter values within the block.
- It solves the problem of component accuracy that is present in all analogue chaotic communication systems.

2. Disadvantages:

- It can be used to implement only low frequency chaotic generators (in order of a few of kHz) since the maximum sampling rate that can be used in the model is 20 kHz.
- The cost of the developed real time system is higher than the circuit implementation of the system.

3.6 References

- [1] R. W. Newcomb and S. Sathyan, "An RC Op Amp chaos generator," *IEEE Trans. Circuits Syst.*, vol. CAS-30, No. 1, pp.54-56, Jan. 1983.
- [2] T. Matsumoto, "Chaos in electronic circuits," *Proc. of the IEEE*, vol. 75, No. 8, pp. 1033-1046, Aug. 1987.
- [3] T. Endo and L. O. Chua, "Chaos from phase-locked loops," *IEEE Trans. Circuits Syst.*, vol. CAS-35, No. 8, pp.987-1003, Jan. 1988.
- [4] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronised with applications to communications," *Phys. Rev. Lett.*, vol. 71, No. 1, pp. 65-68, July 1993.
- [5] C. A. Murphy and M. P. Kennedy, "Chaos controller for autonomous circuits," *Proc. 3rd Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'95*, pp.225-228, 1995.
- [6] N. J. Carron and D. W. Hahs, "A new approach to communications using chaotic signals," *IEEE Trans. Circuits Syst. I*, vol. CAS-44, No. 5, pp. 373-382, Oct. 1993.
- [7] A. S. Dmitriev, A. I. Panas and S. O. Starkov, "Experiments of RF band communications using chaos," *Int. J. of Bifurcation and Chaos*, vol. 7, No. 11, pp. 2511-2527, 1997.
- [8] A. Panas, T. Yang and L. O. Chua, "Experimental results of impulsive synchronisation between two Chua's circuits," *Int. J. of Bifurcation and Chaos*, vol. 8, 1998.
- [9] M. Storace, M. Parodi and D. Robatto, "A hysteresis-based chaotic circuit: Dynamics and applications," *Int. J. of Circuit. Theory appl.*, pp. 527-542, 1999.
- [10] A. S. Elwakil and M. P. Kennedy, "Chaotic oscillator configuration using a frequency dependent negative resistor," *Int. J. of Circuit. Theory appl.*, pp. 69-76, 2000.
- [11] A. S. Elwakil and M. P. Kennedy, "Improved implementation of Chua's chaotic oscillator using current feedback Op Amp," *IEEE Trans. Circuits Syst.*, vol. CAS-47, No. 1, pp.76-79, Jan. 2000.

- [12] X. D. Jia and R. M. M. Chen, "Design and simulation of nonlinear switched capacitor autonomous circuits containing nonlinear active resistor," *IEEE Int. Symposium. on Circuit and System (ISCAS 95)*, pp. 165-168, 1995.
- [13] A. Rodrigues-Vazquez and M. Delgado-Restituto, "VLSI design of chaotic circuits," *Proc. 1 st int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'93*, pp. 390-310, July 93.
- [14] J. Cruz and L. O. Chua, "An IC chip of Chua's circuit," *IEEE Trans. Circuits II*, vol. CAS-40, No. 10, pp.614-625, Oct. 1993.
- [15] M. Delgado-Restituto, A. Rodriguez, R. Lopez-Ahumada and M. Linan, "Chaotic synchronisation using monolithic Chua's oscillator," *Int. J. Electronics*, pp. 775-785, 1995.
- [16] M. Delgado-Restituto, M. Linan and A. Rodrigues-Vazquez, "IC design for spread spectrum communication exploiting chaos," *IEEE Int. Symposium. on Circuit and System (ISCAS 98)*, 1998.
- [17] T. Tsubone, T. Saito and W. Schwarz, "Chaos generators with piecewise linear trajectories," *IEEE Int. Symposium. on Circuit and System (ISCAS 96)*, pp. 178-181, 1996.
- [18] A. Mogel, "Integrated realisation of analogue systems with chaotic behaviour," *Proc. 1 st Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'93*, pp. 411-418, July 93.
- [19] M. Delgado-Restituto, A. Rodrigues-Vazquez, R. L. Ahumada and M. Linan, "Experimental verification of secure communication using monolithic chaotic circuits," *ECCTD' 95 Conference on Circuit Theory & Design*, pp. 475-478, 1995.
- [20] H. Kamata, T. Endo and Y. Ishida, "Secure communication system using chaos via DSP implementation," *IEEE Int. Symposium. on Circuit and System (ISCAS 95)*, pp. 112-115, 1995
- [21] H. Kamata, T. Endo and Y. Ishida, "Communication with chaos via DSP implementation," *IEEE Int. Symposium. on Circuit and System ISCAS 97*, pp. 1069-1072, 1997.
- [22] P. Marchand, *Graphics and GUIs with MATLAB*: CRC Press, 1999.

- [23] M. P. Kennedy, "Experimental chaos via Chua's circuit," *1 st. Experimental Chaos Conference*, pp. 340-351, 1991.
- [24] L. O. Chua, M. Komuro and T. Matsumoto, "The double scroll family, parts I and II," *IEEE Trans. Circuits Syst.*, vol. CAS-33, No. 11, pp.1073-1118, Nov. 1986.
- [25] T. Yoahinaga, H. Kitajima and H. Kawakami, "Bifurcations in a coupled Rössler system," *IEICE Trans. Fundamentals*, vol. E78-A, No. 10, Oct. 1995.
- [26] L. Pivka, C. W. Wu and A. Huang, "Lorenz equation and Chua's equation," *Int. J. of Bifurcation and Chaos*, vol. 6, No. 12B, pp.2443-2489, 1996.
- [27] J. M. H. Elmirghani, "Data transmission through chaotic perturbation and associated security issues," *SPIE special issue on Chaotic Circuits for Communication*, vol. 2612, pp.76-85, 1994.
- [28] M. Itoh, H. Murakami and L. O. Chua, "Communication systems via modulations," *IEICE Trans. Fundamentals*, vol. E77-A, No. 6, June 1994.
- [29] L. Kocarev, K. S. Halle, K. Eckert and L. O. Chua, "Experimental demonstration of secure communications via chaotic synchronisation, Chua's circuit: A Paradigm for Chaos," pp. 371-378, Singapore: World Scientific, 1993.

Chapter 4

MICROWAVE CHAOTIC SYSTEMS

4.1 Introduction

Some results on chaotic communication systems have been reported [1]-[10]. However,0000 all the developed systems so far have been at low frequencies. The reason for this is that no systematic method exists for designing chaotic microwave generators and predicting their performance. In this chapter we offer an analysis procedure that accurately predicts the performance of microwave chaotic generators based on a frequency multiplier chain [11]-[12]. The choice of this type of chaotic generator is based on the following arguments.

- Multiplier chains use highly non-linear devices such as varactor diodes, step recovery diodes or FETs [13].
- The circuits for multiplier chains are also of high order due to the presence of a large number of energy storing elements for the matching networks and the idlers. These two facts make the multiplier chains liable to become chaotic. Only one of the stages in the multiplier chain can be made chaotic and the rest of the chain is used to multiply the chaotic signal to the desired frequency. This makes the design of the generator easy and the results predictable.

The next question we have to answer is why should we build a chaotic microwave communication system? There are two main advantages in building such systems:

1. The chaotic microwave carrier has a wide spectrum [14]. This gives these systems similar advantages to spread-spectrum communication systems using pseudo random generators [15]. The main advantage is higher narrow band jamming signals. This is particularly important in radar and communication systems.
2. Chaotic signals are deterministic, unlike random signals [16]. This offers the possibility of synchronising the transmitter and the receiver. Synchronisation in

turn offers the possibility of burying the information in the chaotic signal which results in vastly improved system security [17].

In this chapter we will introduce a new chaotic generator in J-band and then we will introduce its applications in radar and in communication systems.

4.2 Chaotic J-band for radar and microwave communication systems

4.2.1 Theoretical analysis of chaotic multipliers

It is important to develop a theoretical method for predicting the performance of the chaotic generator. The method we have used is based on state-space analysis and the solution of the state equations in the time domain. We shall give here an example based on a frequency tripler, which is used later to design the microwave chaotic generator. We shall then compare the theoretical and practical results. The tripler uses a step recovery diode, it has input and output matching sections and an idler at the output to short-circuit the second harmonic signal. The circuit for the tripler is shown in Fig. 4.1.

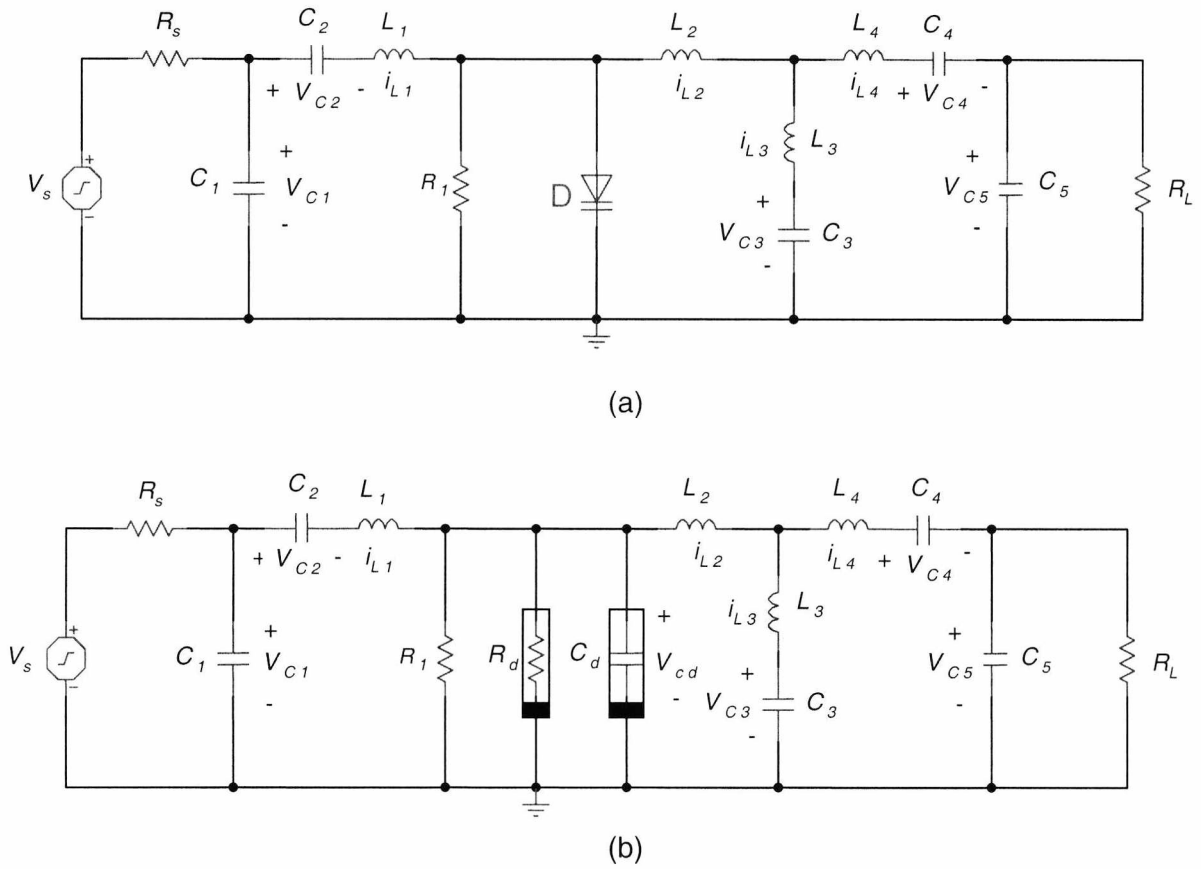


Fig. 4.1 (a) Tripler circuit diagram.
 (b) Tripler with varactor equivalent circuit.

The model used for the diode is a parallel combination of a non-linear capacitor C_d and a non-linear resistor R_d . The non-linear resistor is represented by diode equation

$$I_D = I_s (\exp(v/v_T) - 1) \tag{4.1}$$

where the saturation current I_s is taken as 10^{-13} A and v_T as 25 mV. The non-linear capacitor C_d is a function of the instantaneous charge q and the resulting instantaneous diode voltage v_{cd} is given by [18]

$$v_{cd} = a|q| + bq + E_0 \tag{4.2}$$

where

$$a = \frac{C_b - C_a}{2C_a C_b}$$

$$b = \frac{C_b + C_a}{2C_a C_B}$$

For the chosen diode, $C_a = 2.8571\text{nF}$, $C_b = 5.0\text{ pF}$ and $E_0 = 0.1\text{ V}$. The relation between the capacitor voltage and the capacitor charge is shown in Fig. 4.2a. The nonlinear resistor characteristic is shown in Fig. 4.2b.

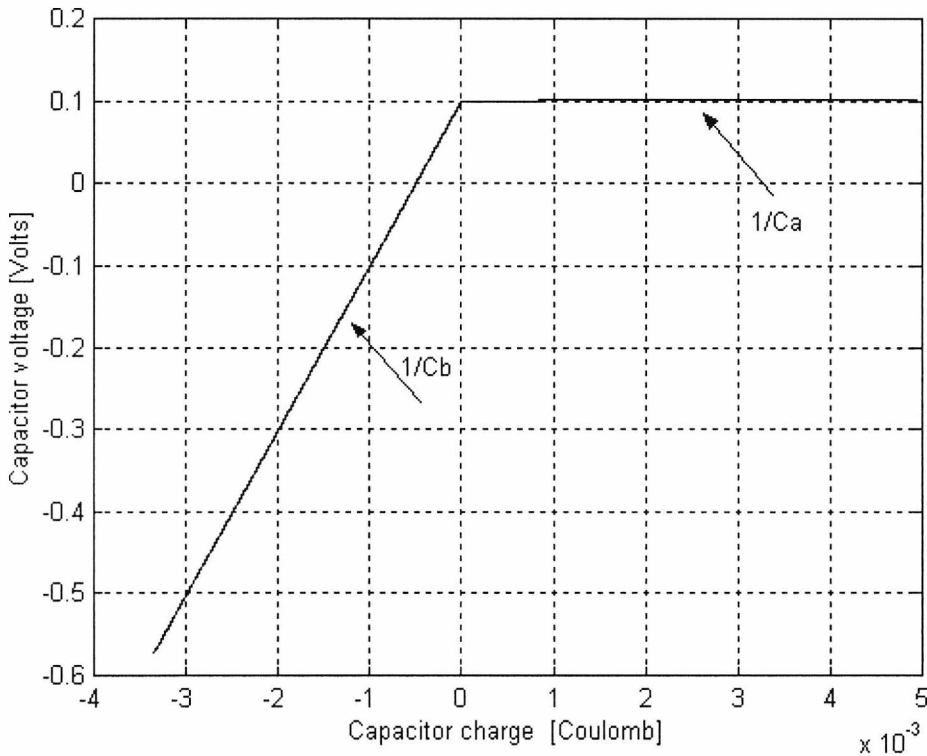


Fig. 4.2 Non-linear capacitor characteristic.

Next we derive the state equations for the circuit shown in Fig. 4.1. One advantage of the state-space representations is that a signal flow diagram can be directly derived and solved in the time domain. There are ten energy-storing elements, however since there is a cut-set consisting entirely of inductors (L_2 , L_3 and L_4) the true order is only nine. The state equations are derived in the normal form $\dot{x} = Ax + Bu$.

After eliminating the dependent state variable i_{L_4} the state equations are given by

$$\frac{d}{dt} \begin{bmatrix} v_{C1} \\ v_{C2} \\ v_{C3} \\ v_{C4} \\ v_{C5} \\ v_{cd} \\ i_{L1} \\ i_{L2} \\ i_{L3} \end{bmatrix} = \begin{bmatrix} -\frac{1}{R_s C_1} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{C_1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{C_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{C_3} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{C_4} & -\frac{1}{C_4} \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{R_L C_5} & 0 & \frac{1}{C_5} & -\frac{1}{C_5} \\ 0 & 0 & 0 & 0 & 0 & -\frac{R_1 + R_d}{R_1 R_d C_d} & \frac{1}{C_d} & -\frac{1}{C_d} & 0 \\ \frac{1}{L_1} & -\frac{1}{L_1} & 0 & 0 & -\frac{1}{L_1} & 0 & 0 & 0 & 0 \\ 0 & \frac{-a_2}{a_1} & \frac{-a_3}{a_1} & \frac{-a_3}{a_1} & \frac{1}{a_1} & 0 & 0 & 0 & 0 \\ 0 & \frac{-b_1}{L_3 + L_4} & \frac{b_2}{L_3 + L_4} & \frac{b_3}{L_3 + L_4} & \frac{b_4}{L_3 + L_4} & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_{C1} \\ v_{C2} \\ v_{C3} \\ v_{C4} \\ v_{C5} \\ v_{cd} \\ i_{L1} \\ i_{L2} \\ i_{L3} \end{bmatrix} + \begin{bmatrix} \frac{1}{R_s} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} v_s$$

where,

$$a_1 = L_2 + \frac{L_2 L_3}{L_3 + L_4}, \quad a_2 = \frac{L_4}{L_4 + L_3}, \quad a_3 = \frac{L_3}{L_3 + L_4},$$

$$b_1 = 1 + L_4 \frac{a_2}{a_1}, \quad b_2 = 1 + L_4 \frac{a_3}{a_1}, \quad b_3 = 1 - L_4 \frac{a_2}{a_1}, \quad b_4 = L_4 \frac{1}{a_1}$$

Next a signal flow diagram representing the state equations directly is developed and simulated in the time domain using SIMULINK. The signal flow chart is shown in Fig. 4.3. One major advantage of this representation is that the circuit elements are identifiable in the diagram and the effect of changing them can be easily studied. This is essential in studying the chaotic conditions and the behavior of the system *en route to chaos*. The input signal of the tripler is a sine wave with amplitude 35 volts and frequency 92.534720 MHz. For simulation the frequency of input signal is normalised to be 0.09253720 and the circuit components are normalised as given in table 4.1. The initial values of the circuit elements for the circuit to operate as a tripler are given in table 4.1.

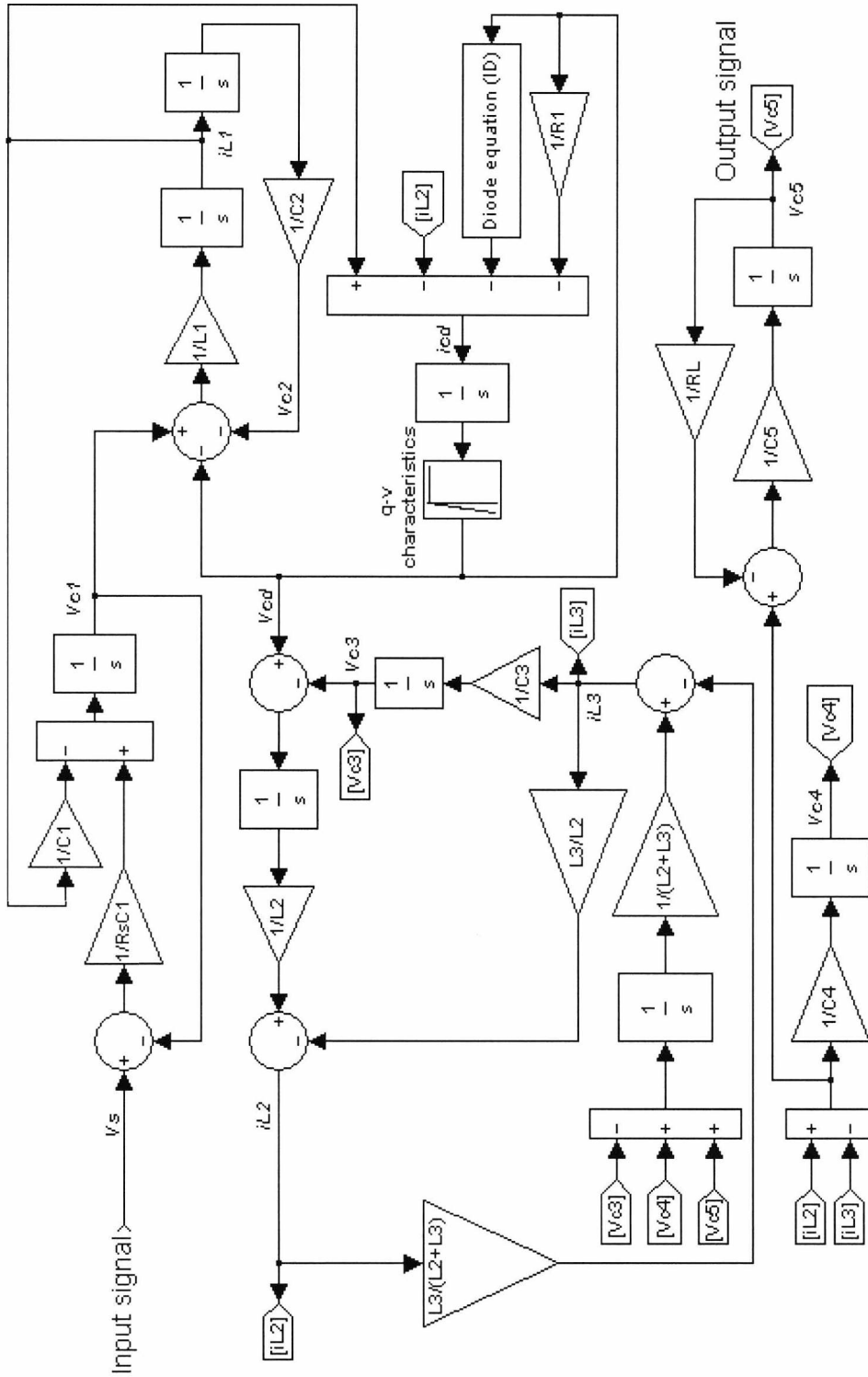


Fig. 4.3 Signal-flow representation of the state equation.

Component	Value	Normalised values
C_1	35 pF	0.035
C_2	820 pF	0.820
C_3	9 pF	0.009
C_4	5 pF	0.005
C_5	15 pF	0.015
L_1	90 nH	90
L_2	20 nH	20
L_3	80 nH	85
L_4	70 nH	70
R_s	50 Ω	50
R_1	10 k Ω	10000
R_L	60 Ω	60

Table 4.1 Tripler circuit elements values.

The simulation results of the tripler input signal in time and frequency domains are shown in Fig. 4.4. The results of tripler output signal in time and frequency domains are illustrated in Fig. 4.5.

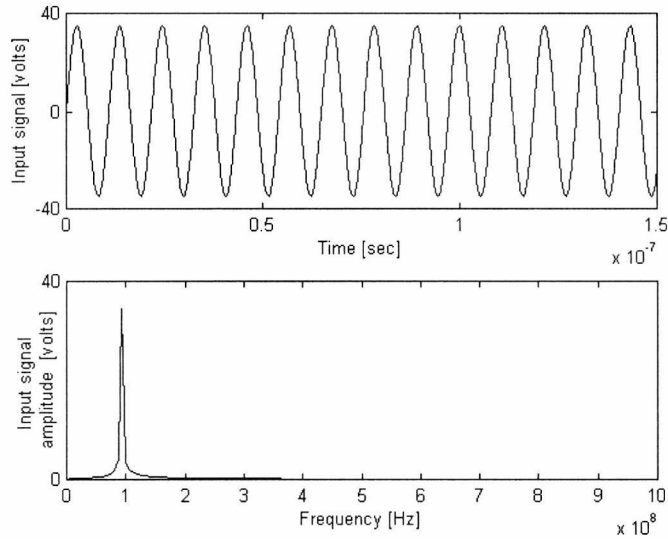


Fig. 4.4 Simulation results of the input signal in time and frequency domains.

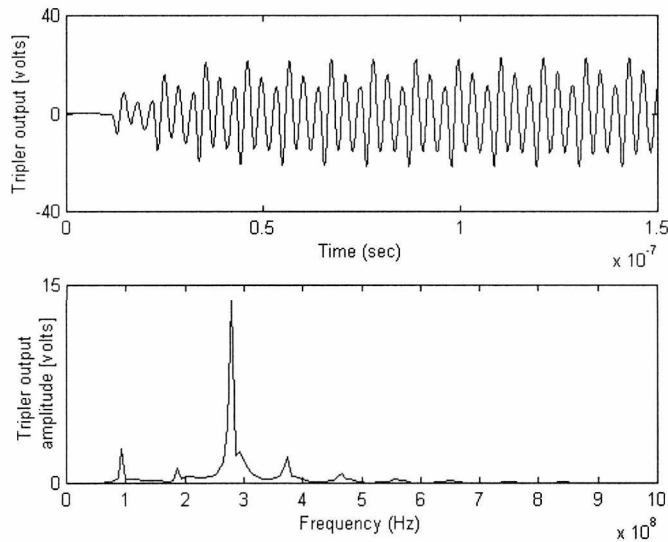


Fig. 4.5 Simulation results of the tripler output in time and frequency domains.

The tripler circuit is in fact a near chaotic circuit operating in period three. To bring the circuit to full chaos the values of the circuit elements were changed as given in table 4.2.

Component	Value	Normalised values
C_1	150 pF	0.15
C_2	85 pF	0.085
C_3	50 pF	0.05
C_4	5 pF	0.005
C_5	80 pF	0.08
L_1	50 nH	90
L_2	15 nH	15
L_3	90 nH	90
L_4	65 nH	65
R_s	50 Ω	50
R_1	100 k Ω	100000
R_L	60 Ω	60

Table 4.2 Chaotic circuit element values.

The result of the chaotic behaviour in the time domain and the spectrum is shown in Fig. 4.6.

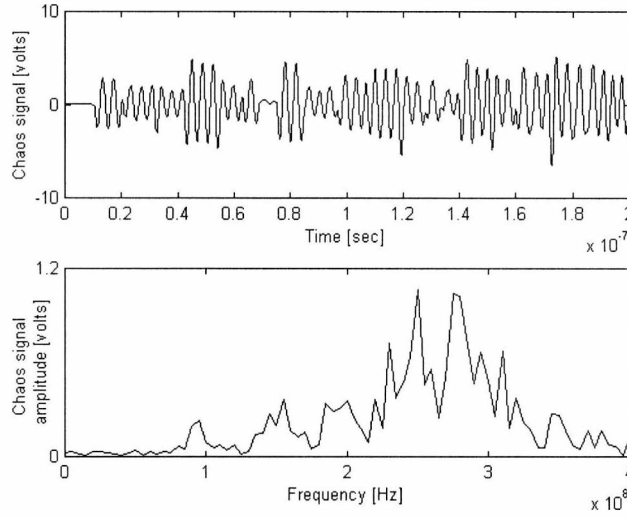


Fig. 4.6 Chaotic behaviour in time and frequency domains.

To obtain the attractor of the signal, a delay T was introduced and the phase plane was plotted of the output $v_5(t)$ versus the delayed output $v_5(t - T)$. The time delay T in this case is 0.3 ns. The resulting attractor is shown in Fig. 4.7. The reason for plotting the attractor in this way rather than use two different state variables is that we wish to compare this result with those obtained from the measurements. In measurements we will only have the final output of the generator.

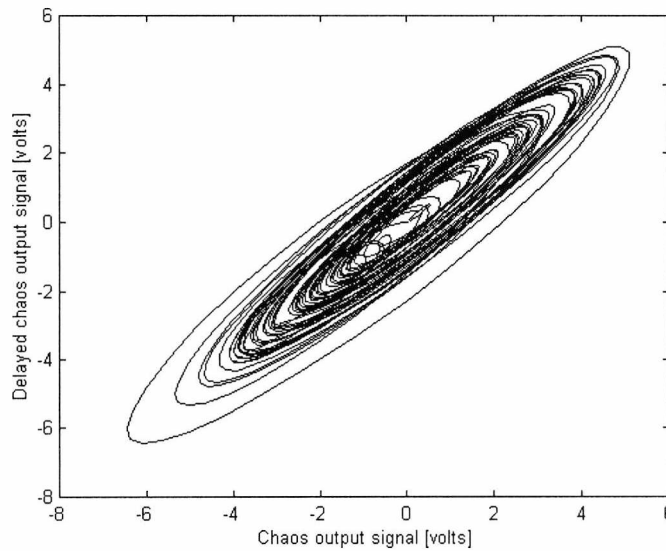


Fig. 4.7 Attractor of the chaos signal.

4.2.2 Practical design

A multiplier chain was built consisting of a crystal controlled oscillator at 92.534720 MHz followed by an amplifier. A multiplier chain multiplies the frequency to 13.32 GHz. The first multiplier is a tripler and this is the stage that was designed to have chaotic behaviour as obtained from the simulation. The block diagram of the generator is shown in Fig. 4.8. The physical circuit of the chaotic generator is shown in Fig. 4.9.

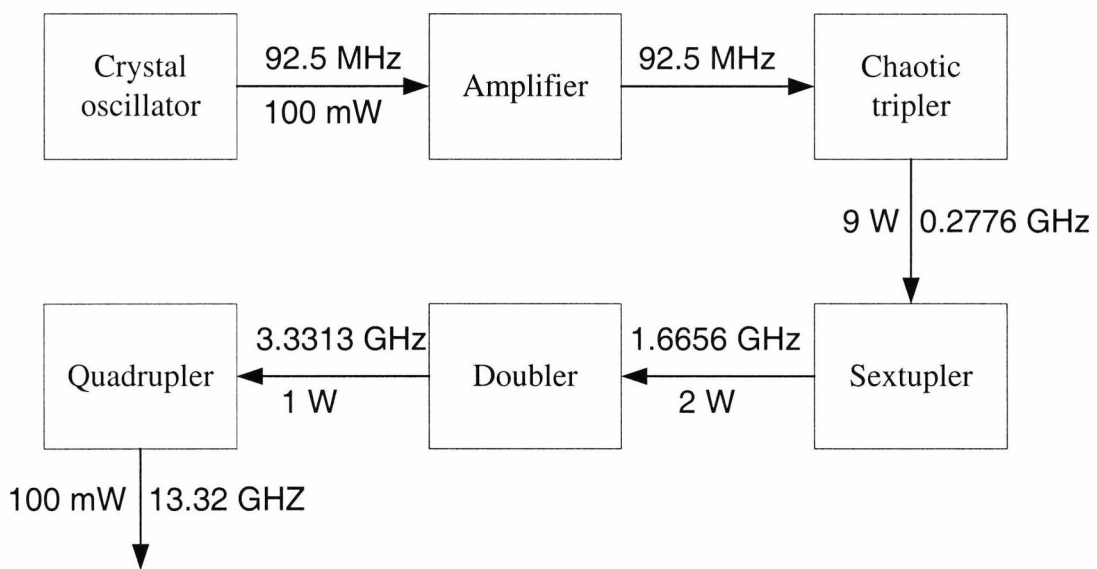


Fig. 4.8 Block diagram of chaotic generator.

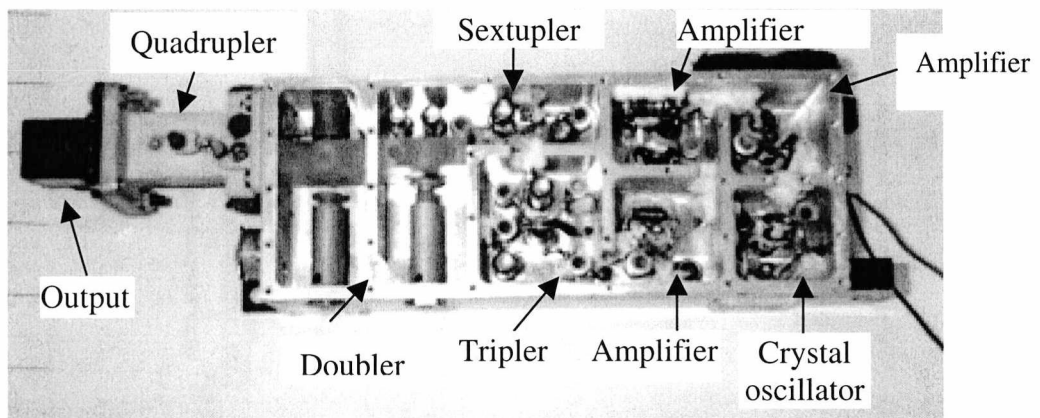


Fig. 4.9 Physical circuit of the J-band chaotic generator.

Measurements were made on the designed generator using a Hewlett-Packard microwave transition analyser (HP70820A). The output of 13.32 GHz was sampled at 0.5 ns intervals. The block diagram of the test bench of the microwave chaotic generator is shown in Fig. 4.10.

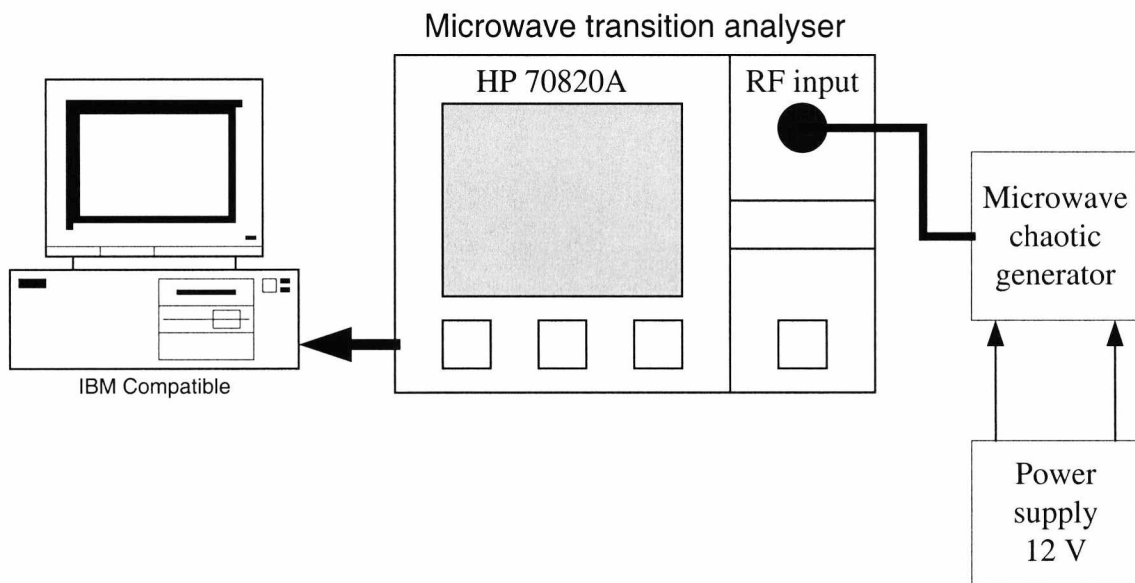


Fig. 4.10 Block diagram of the testing bench of the J-band chaotic generator

The measured output in the time and frequency domains is shown in Fig. 4.11. The attractor for a time delay of 1.5 ns is shown in Fig. 4.12. The results are remarkably similar to those obtained from the simulation, which indicated the validity of the model used and of the simulation process.

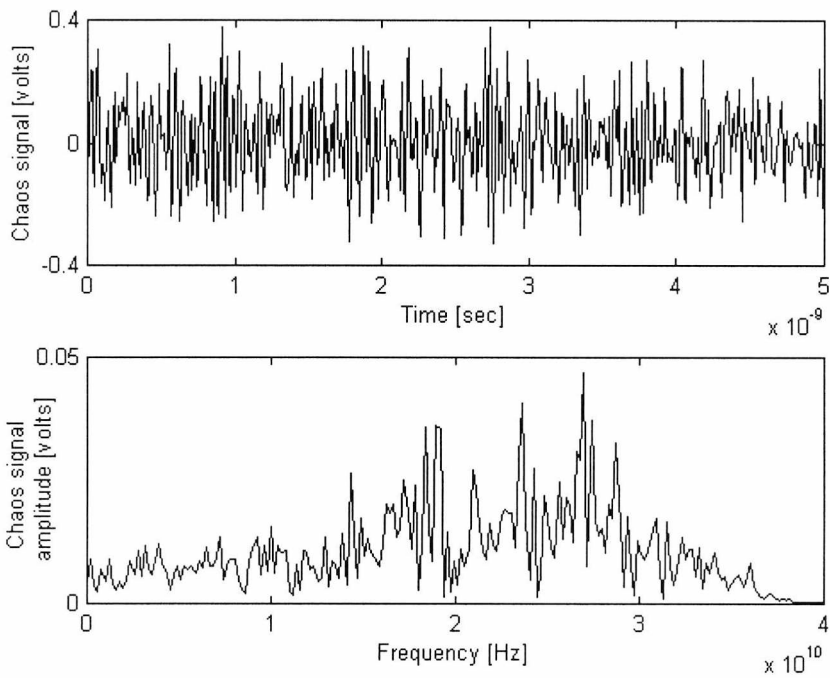


Fig. 4.11 Measured chaotic signal in time and frequency domains.

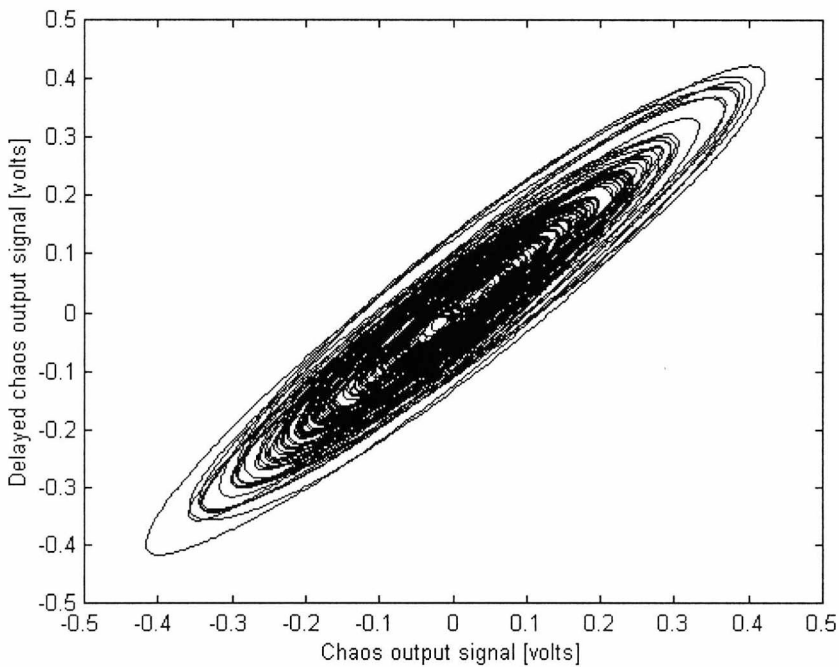


Fig. 4.12 Attractor of the measured chaotic signal

This is the first time that the results of a J-band microwave chaotic generator have been reported. The importance of the presented work is that an analysis procedure has been developed to predict accurately the chaotic behaviour of the generator. This offers the possibility of designing chaotic radar and microwave chaotic communication systems with greater security and narrow band jamming immunity than conventional systems. The developed topology is based on frequency multiplier chains. By adding further multiplier stages higher frequency outputs can be achieved.

4.3 Chaotic radar and microwave chaotic communication systems

In this section, we present the application of the microwave chaotic generator in chaotic radar and microwave chaotic communication systems [19]-[20]. When we transmit a pulsed RF signal, we refer to the system as chaotic radar system and when we transmit a modulated AM signal, we refer to the system as chaotic communication. These systems are based on the chaotic microwave generator introduced in section 4.2. The generator is used as the transmitter and the inverse of this system is used as a receiver. The function of the inverse system is to reconstruct the radar pulse signal or the information signal that is the input to the transmitter.

4.3.1 Receiver design

The most important part of the receiver is the signal processing circuitry that will retrieve the information signal from the chaotic signal. The approach adopted here is based on deriving an inverse system of the original chaotic multiplier and downloading the algorithm on a signal-processing chip. The signal processing does not have to be carried out at microwave frequencies as shown in Fig. 4.13. In this system the information, radar pulses or AM signal, is applied as an input to the tripler chaotic generator. The output of the tripler is a group of multiplier stages and amplifiers so the transmitted signal is a microwave chaotic signal. In the receiver, the frequency of the received signal is down-converted and amplified to the frequency of the tripler chaotic generator. The down-converted signal is applied to the inverse

system which is a signal processing chip has an inverse function of the tripler chaotic generator so the information signal can be recovered.

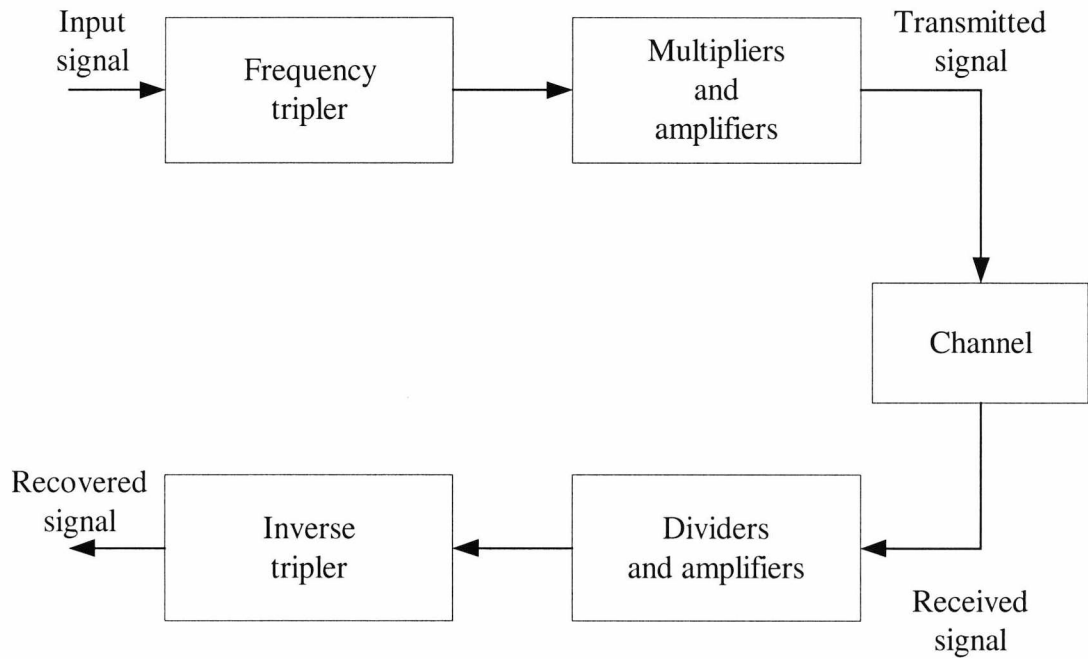


Fig. 4.13 Simplified block diagram of the microwave chaotic communication system.

In the inverse system, we will assign new notations for the currents and voltages as shown in Fig. 4.14.

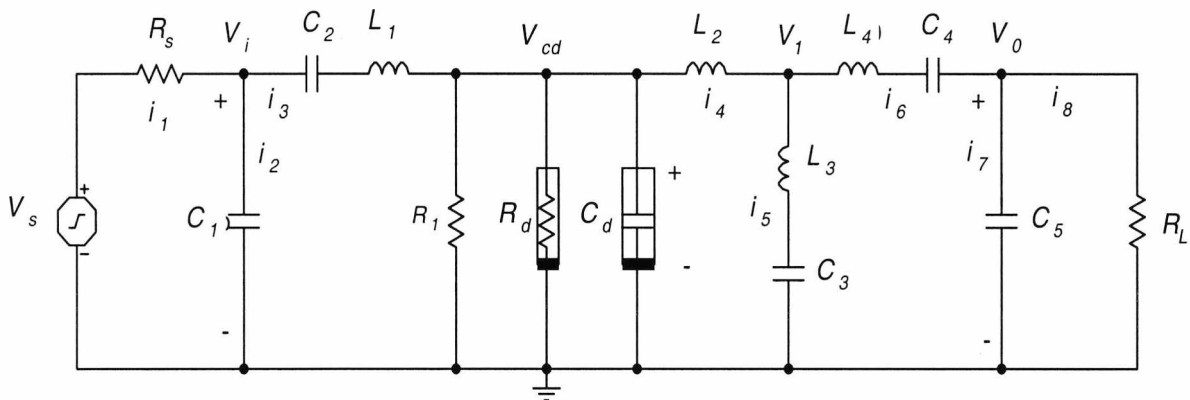


Fig. 4.14 Circuit diagram of the tripler chaotic generator.

The equations of the inverse system are given by

$$i_8 = \frac{v_0}{R_L}$$

$$i_7 = C_5 \frac{dv_0}{dt} \quad (4.3)$$

$$i_6 = i_7 + i_8$$

$$v_1 = L_4 \frac{di_6}{dt} + \frac{1}{C_4} \int i_6 dt + v_0 \quad (4.4)$$

$$i_4 = i_5 + i_6$$

$$i_5 = \frac{1}{L_3} \int v_1 dt - \frac{1}{L_3 C_3} \iint i_5 dt \quad (4.5)$$

$$v_{cd} = L_2 \frac{di_4}{dt} + v_1 \quad (4.6)$$

$$v_i = \frac{1}{C_2} \int i_3 dt + L_1 \frac{di_3}{dt} + v_{cd} \quad (4.7)$$

$$i_2 = C_1 \frac{dv_i}{dt} \quad (4.8)$$

$$i_1 = i_2 + i_3$$

The recovered signal v_s is given by

$$v_s = i_1 R_s + v_i.$$

In this case, the number of state equations is still nine as in the transmitter but we have combined some of the state equations in one equation. For example, Eq. 4.4 is of second order. The signal flow diagram of the inverse algorithm is shown in Fig. 4.15.

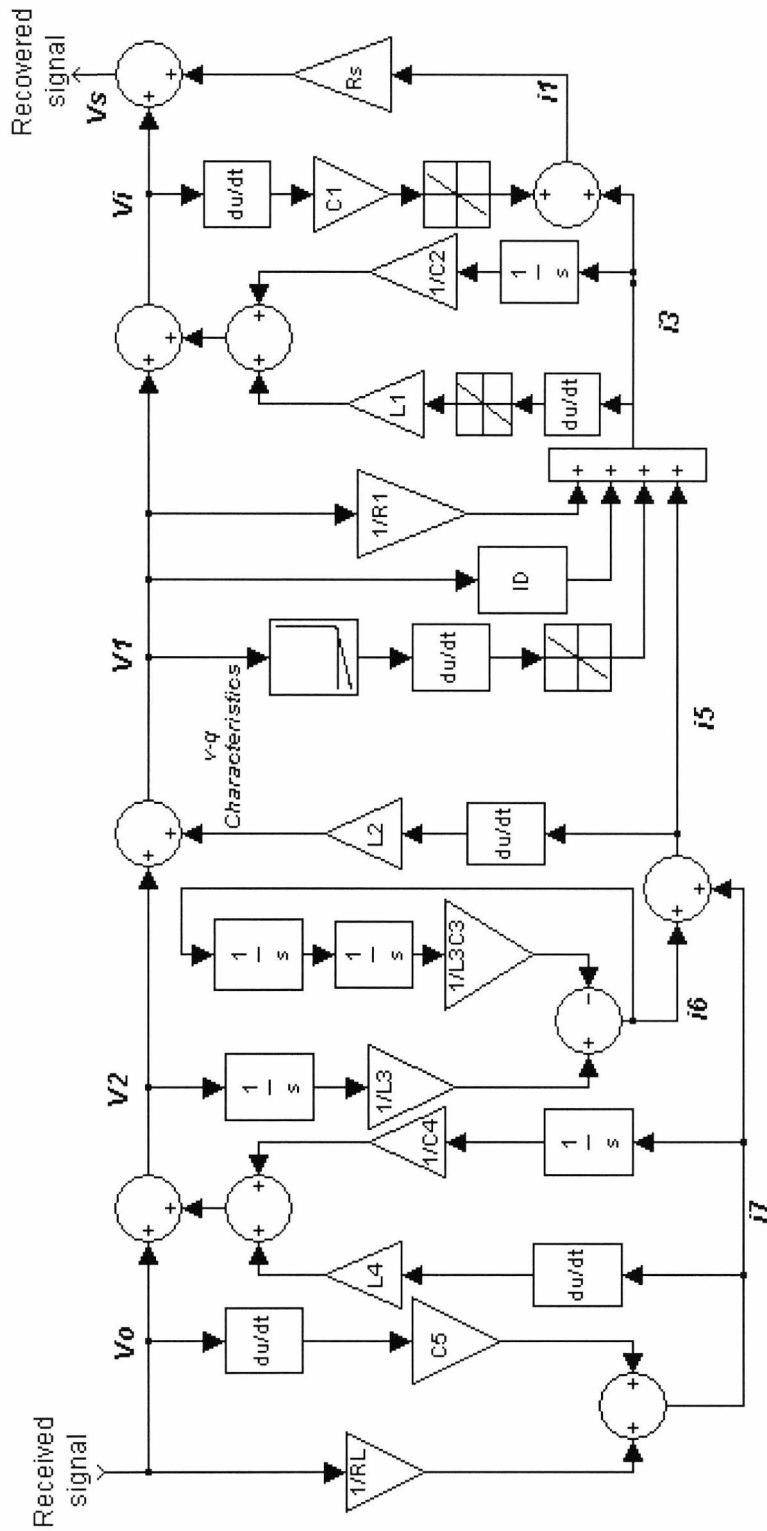


Fig. 4.15 Signal flow diagram of the inverse system.

In the inverse system, a non-linear inverse function has to be developed. The inverse of the non-linear function of Eq. 4.2 is given by

$$q(v_{cd}) = \begin{cases} \frac{v_{cd} - E_o}{a + b} & v_{cd} \geq 0.1 \\ \frac{v_{cd} - E_o}{b - a} & v_{cd} < 0.1 \end{cases} \quad (4.9)$$

Fig. 4.16 shows the characteristic of the inverse of the non-linear capacitor.

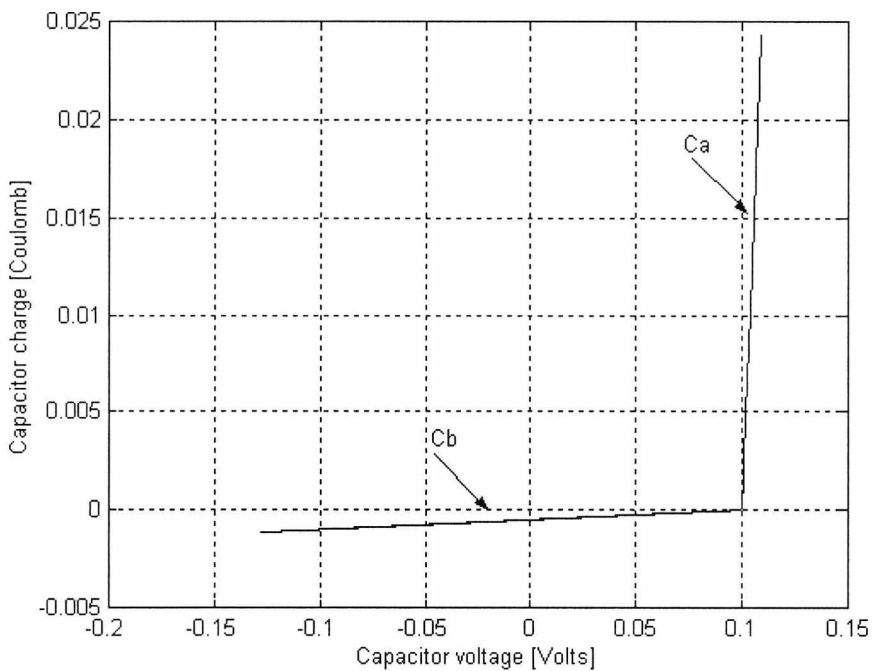


Fig. 4.16 Characteristic of the inverse non-linear capacitor.

The main disadvantage of the above non-linear capacitor function is that there is a discontinuity at the point of transition from the negative charge to the positive charge. In the inverse system, there are differentiators and differentiators will produce large spikes and high error at the discontinuities of the non-linear capacitor function. As a result the recovered signal will be distorted. Fig. 4.17 illustrates the results of the microwave chaotic radar system. Fig. 4.18 shows the results of the AM microwave chaotic communication system in this case. The results show that the

inverse system does not recover the information signals in both cases due to the discontinuity in the non-linear capacitor function.

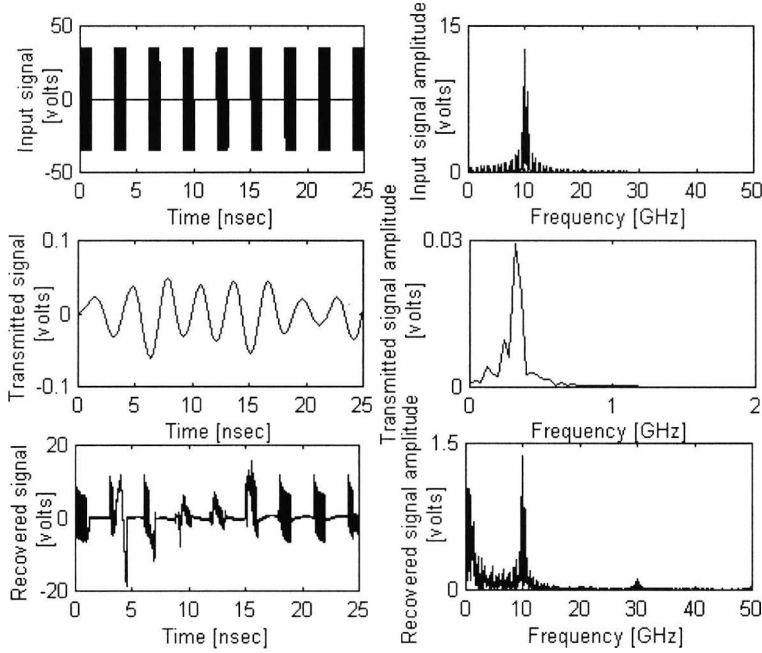


Fig. 4.17 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.

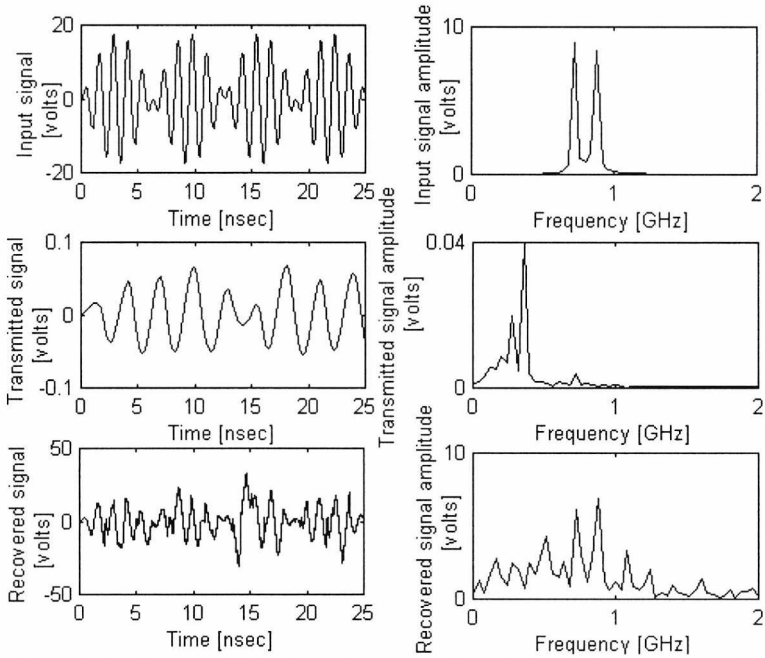


Fig. 4.18 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains.

To overcome the above problems, we introduce a new expression for the q - v characteristic of the capacitor non-linear capacitor instead of the expression given by Eq. 4.2. This expression improves the performance of the inverse system.

The non-linear capacitor function is written as

$$1/C_d = b_1 + 0.5a_2 \tanh(-cq). \quad (4.10)$$

The q - v characteristic of the non-linear capacitor function is given by

$$v_{cd}(q) = b_1q - 0.5\frac{a_2}{c}\log(\cosh(-cq)) + 0.1 \quad (4.11)$$

where

$$a_1 = \frac{1}{C_a}, a_2 = \frac{1}{C_b} \text{ and } b_1 = \frac{a_1 + a_2}{2}$$

and c is a constant that determines the slope of the \tanh function and is set equal to 200. According to Eq. 4.11, the non-linear capacitor of the transmitter is shown in Fig. 4.19.

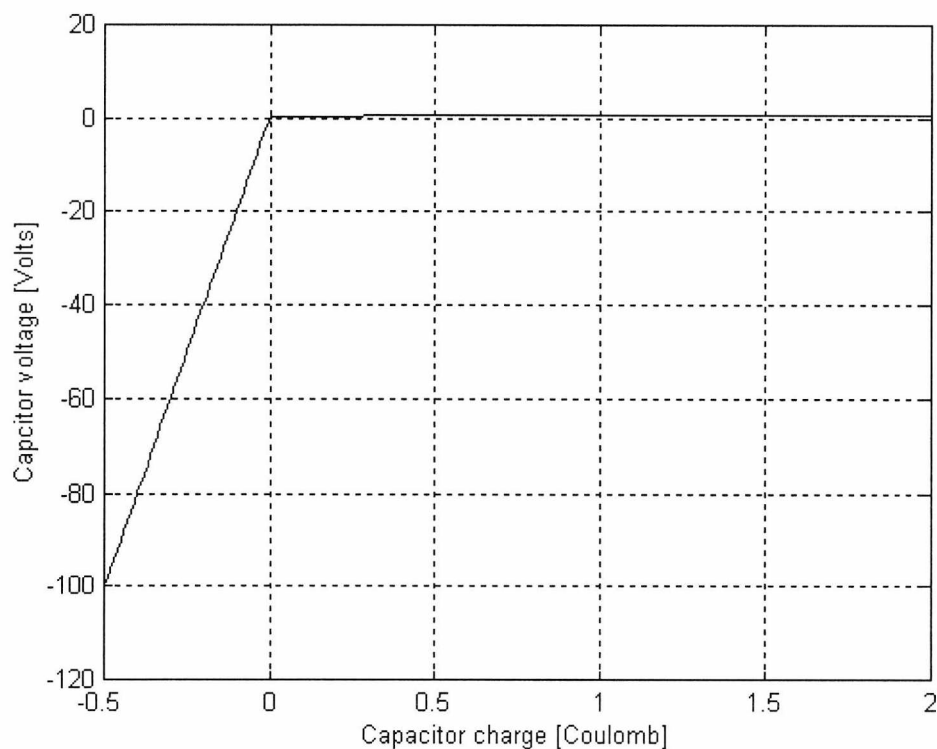


Fig. 4.19 Non-linear capacitor characteristic.

In the receiver, we get the inverse of the capacitor non-linear function (Eq. 4.11) by two methods:

Method 1.

Calculate the current i_{cd} using the voltage v_{cd} from the relation $i_{cd} = c_d \frac{dv_{cd}}{dt}$. The same values given in table 4.1 are used in the simulation and $C_a = 2.8571$ nF and $C_b = 5.0$ pF. The results in this case are shown in Figs. 4.20 and 4.21.

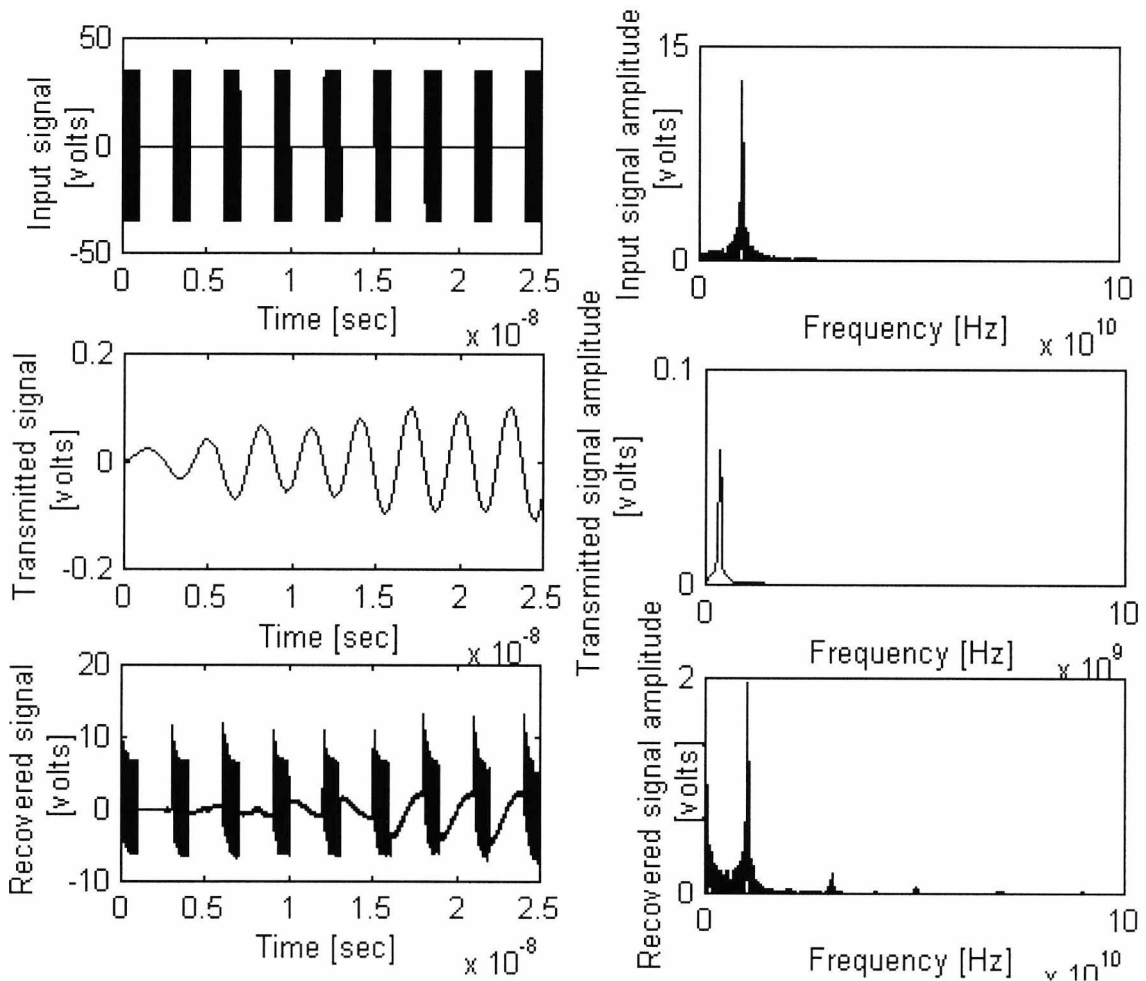


Fig. 4.20 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.



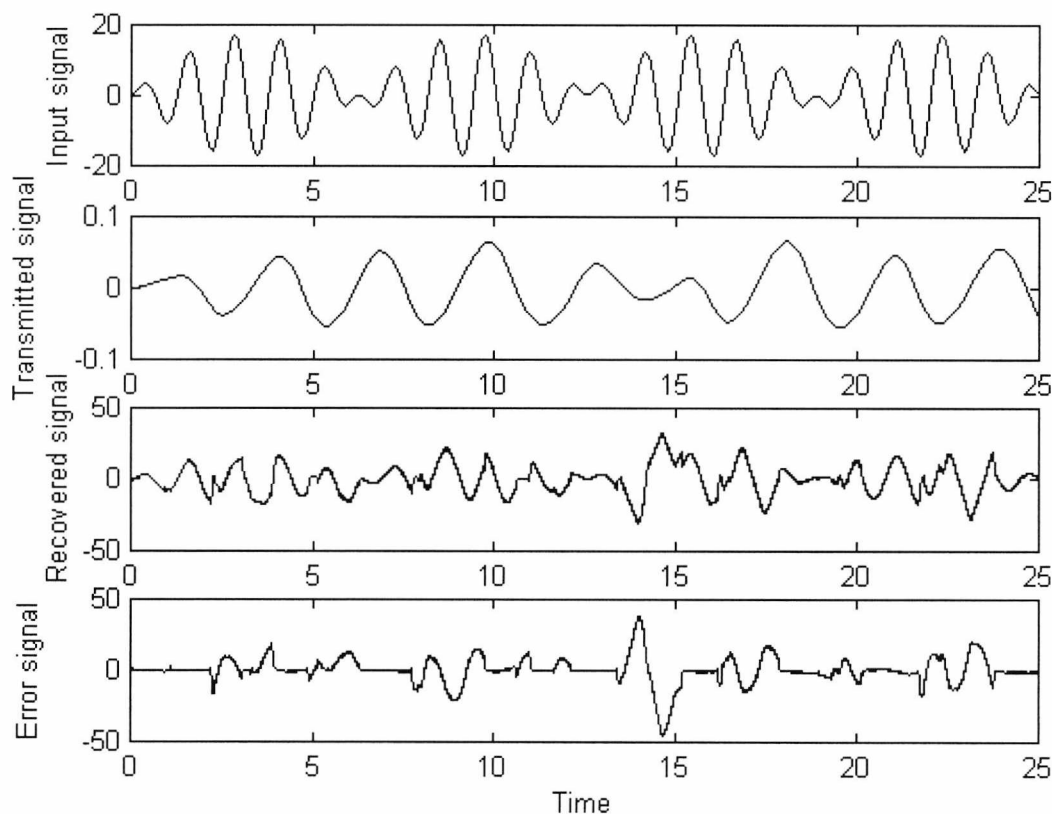


Fig. 4.21 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains

The results show that with the new non-linear capacitor function, the performance of the inverse system is improved and the information signals are recovered with good accuracy and the distortion in the recovered signal is reduced especially in the microwave chaotic communication system (SNR=27.89 dB AM signal).

Method 2.

We use a lookup table as a source of data for the transmitter and the receiver non-linear functions. We put the relation between the charge q (input) and the voltage v_{cd} (output) in the transmitter lookup table. The data can be taken from experimental or from simulation results. In the receiver, the same data of the transmitter non-linear function is used but we use the capacitor voltage v_{cd} as input and the charge q as

output of the receiver lookup table. The inverse of the non-linear capacitor function is shown in Fig. 4.22.

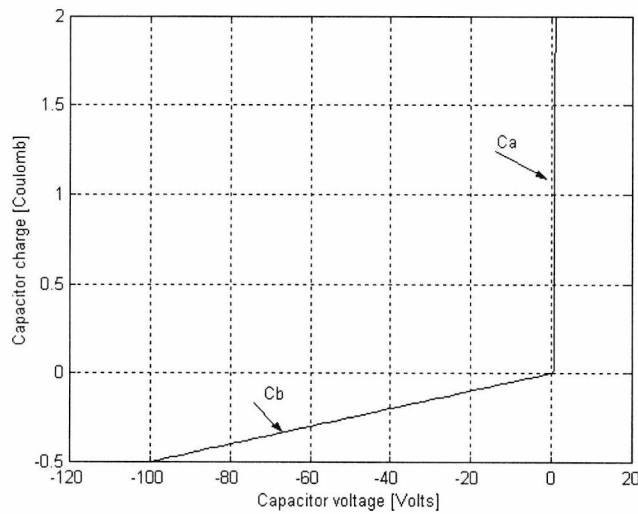


Fig. 4.22 Inverse system non-linear function characteristic.

The system is tested by radar pulses and AM signal and the results are shown in Figs. 4.23 and 4.24. The results show that the performance of the system using the lookup table is better than the system using method 1 in both the cases of radar pulses and AM signal. In this case, the SNR= 27.86 dB while in the first method the SNR=-0.4 dB.

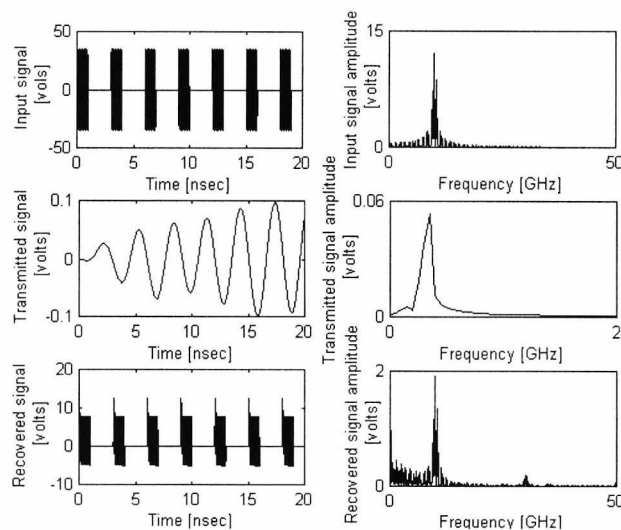


Fig. 4.23 Input radar pulses, transmitted chaotic signal and the recovered radar pulses in time and frequency domains.

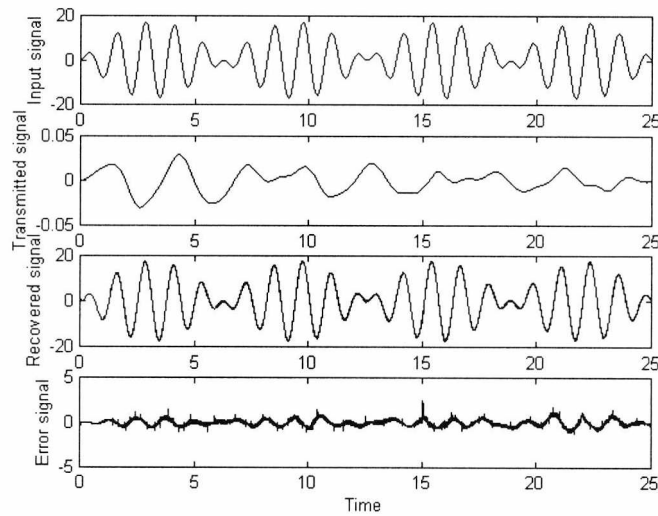


Fig. 4.24 Input AM signal, transmitted chaotic signal and the recovered AM signal in time and frequency domains.

The effect of the channel attenuation and the channel delay are tested in the chaotic radar and microwave chaotic communication systems. Fig. 4.25 shows the effect of the channel attenuation and channel delay in the chaotic radar system. Different attenuation values are chosen (25%, 50% and 75%) and different delay values 5 ns and 10 ns are tested and the system succeeds in recovering the radar pulses under these conditions.

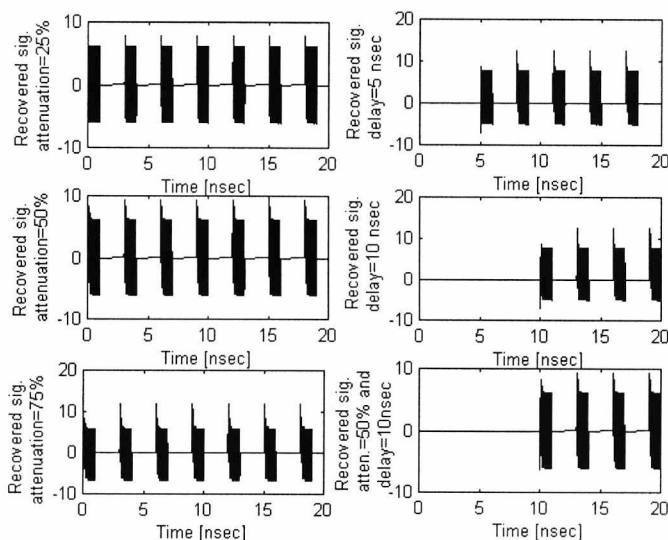


Fig. 4.25 Effect of channel attenuation and delay in the radar system.

Fig. 4.26 shows the effect of the channel attenuation and channel delay in the microwave chaotic communication system. The results show that the system succeeds in recovering the information signal under these conditions.

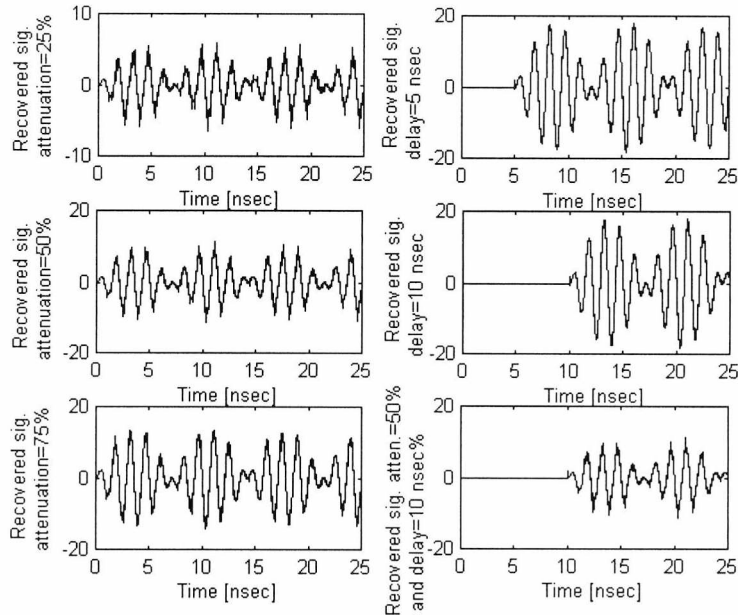


Fig. 4.26 Effect of channel delay and attenuation in the microwave chaotic communication system.

Finally, we suppose that part of the receiver input signal is lost and we would like to check if the system is capable of recovering the radar pulses or not. The results show that, the system succeeds in recovering the radar pluses as shown in Fig. 4.27.

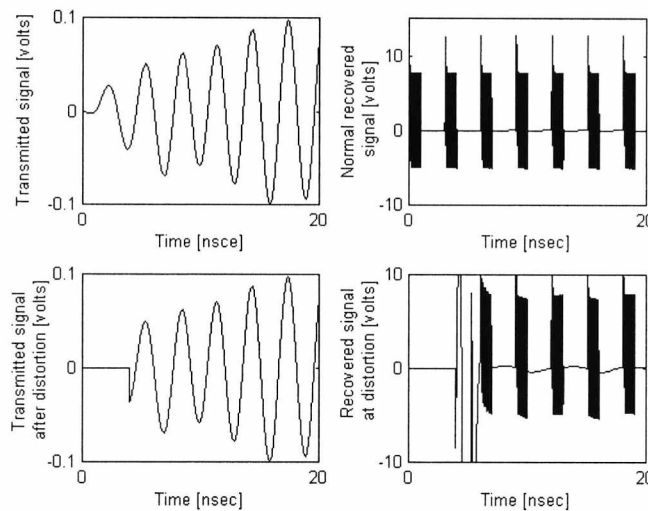


Fig. 4.27 Effect of the loss a part of the received signal.

4.4 Conclusion

The importance of the present work is that an analysis procedure has been developed to predict accurately the chaotic behaviour of the microwave chaotic generators. The developed topology is based on the frequency multiplier chains. By adding further multiplier stages higher frequency outputs can be achieved. This offers the possibility of designing chaotic radar and microwave chaotic communication systems with greater security and noise immunity than conventional systems. The transmitter is based on frequency multiplier chains and the signal is recovered using an inverse system of the transmitter. A new expression of the $q - v$ characteristic of the varactor non-linear capacitor is presented. Different methods to get the inverse of the non-linear capacitor function are presented. The results in each method are presented and the systems succeed to recover the information signals. The effects of the channel delay and channel attenuation are examined. The results show that the input signals are recovered with good quality and the systems have immunity against these effects. The effect of loss part of the received signal is tested and the system is able to recover the information signal under this condition.

4.5 References

- [1] J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman, R. Sherman, A. J. Lichtenberg, J. Y. Huang, W. Wonchoba, M. Steinberg and P. Khoury, "Secure communications by synchronisation to a chaotic signal," *Proc. 1st Experimental Chaos Conference*, pp. 137-144, Oct. 1991.
- [2] C. W. WU and L. O. Chua, "A simple way to synchronise chaotic systems with applications to secure communication system," *Int. J. Bifurcation and Chaos*, vol. 3, No. 6, pp. 1619-1627, 1993.
- [3] K. M. Cuomo and A. V. Oppenheim, "Robustness and signal recovery in a synchronised chaotic system," *Proc. 2nd Experimental Chaos Conference*, pp. 81-98, Oct. 1993.
- [4] F. Böhme, A. Bauer, U. Feldman and W. Schwarz, "Information transmission by chaotising," *Int. J. Electronics*, vol. 79, No. 6, pp. 767-773, 1995.
- [5] Y. H. Yu, K. Kwak and T. K. Lim, "Secure communication through synchronisation of two chaotic systems with continuous feedback method," *Optical and Quantum Electronics*, vol. 27, pp. 535-540, 1995.
- [6] A. Mögel and W. Schwarz, "Chaotic wide band oscillator with delay line," *Proc. 3rd Int. Specialist Workshop on Non-linear Dynamics of Electronic Systems NDES'95*, 1995.
- [7] Y. H. Yu, K. Kwak and K. Lim, "Secure communication using a small continuous feedback," *Phys. Lett. A*, vol. 197, pp. 311-315, 1995.
- [8] C. P. Silva and A. M. Young, "Implementation RF broadband chaotic oscillators: design issues and results," *IEEE Int. Symposium. on Circuit and System (ISCAS 98)*, 1998.
- [9] A. S. Elwakil and M. P. Kennedy, "High frequency Wien-type chaotic oscillators," *Electron. Lett.*, vol. 34, No. 12, pp. 1161-1162, 1998.
- [10] A. S. Elwakil and M. P. Kennedy, "Chaotic oscillator configuration using a frequency dependent negative resistor," *Int. J. Circuit Theory Appl.*, vol. 28, pp. 69-76, 2000.

- [11] M. I. Sobhy and A. R. Shehata, "Chaotic J-band generator for microwave communications systems," *European Microwave Conference*, " Munich-Germany, Oct. 1999.
- [12] M. I. Sobhy and A. R. Shehata, "Chaotic J-band generator for microwave communications systems," *MPD Microwave Product Digest*, pp.91-96, May 2000.
- [13] P. Penfield and R. P. Rafuse, *Varactor applications*: Massachusetts institute of technology, 1962.
- [14] T. L. Carroll and G. A. Johnson, "Synchronising broadband chaotic systems to narrow-band signals," *Phys. Rev. E*, vol. 57, pp.1555-1558, Feb. 1998.
- [15] G. Kolumban, M. P. Kennedy and L.O. Chua, "The role of synchronisation in digital communications using chaos- Part I: Fundamentals of digital communications," *IEEE Trans. Circuits Syst. I*, vol. CAS-44, pp. 927-935, Oct. 1997.
- [16] R. Kaul, "Chaos in microwave systems," *IEEE MTT-S Digest*, 1996.
- [17] R. Lori, "Secure communications via chaotic synchronisation in Chua's circuit and Bonhöeffe-Van Der Pol equation: Numerical analysis of the errors of the recovered signal," *IEEE Int. Symposium. on Circuit and System (ISCAS 95)*, pp. 684-687, 1995.
- [18] T. Matsumoto, L. O. Chua and S. Tanaka, "Simplest chaotic nonautonomous circuit," *Phy. Rev. A*, vol. 30, pp. 1155-1158, 1984.
- [19] M. I. Sobhy and A. R. Shehata, "Chaotic radar systems," *Int. Microwave Symposium*, Boston, Massachusetts, June 2000.
- [20] M. I. Sobhy and A. R. Shehata, "Time domain analysis of chaotic circuits, " *European Microwave Workshop*, Paris, Oct. 2000.

Chapter 5

SECURE COMPUTER COMMUNICATION USING CHAOTIC ALGORITHMS

5.1 Introduction

Cryptography is simply defined as the process of combining some input data called the **plaintext** with a user-specified password to generate an encrypted output called **ciphertext** in such a way that, given the ciphertext no one can recover the original plaintext without the encryption password in a reasonable amount of time [1]. The algorithms that combine the keys and plaintext are called **ciphers**. The process of encoding the data with a particular cipher is known as **encryption**. The reverse process, extracting the original information from the encrypted data, is known as **decryption**. Many ciphers accept a fixed length password (also called a **key**). The **key space** is the total number of possible keys and the **key lengths** are the numbers of digits or bits used as a key. This number increases as the computing power grows. So what makes one cipher better than another? What makes a cipher secure? Although these questions are the essence of cryptography their answers are relatively simple. If there is no other way to **break** the algorithm (recover the plaintext or key given some ciphertext) other than searching through every possible keys, then the algorithm is secure. This is where a large key length comes in. The larger key length means that there are more possible keys to search through and therefore the algorithm is more secure. Practically, there are several methods to break the cipher system without searching for all the keys [2]. Recently, there has been much interest in utilising chaotic signals in cryptography [3]-[4]. Habutsu *et al* [5] proposed a secret key cryptosystem using a chaotic map. This system is based on the

characteristics of chaos that small variations of the parameters make the results of recursive calculations on the chaotic map quite different. Matthews [6] shows that, under certain conditions, even simple non-linear functions are capable of generating chaotic sequences of random numbers. Carroll *et al* [7] utilise the Lorenz chaotic generator as a generator of pseudo-random sequences for cryptographic applications.

In section 5.2, a brief description of the classical cipher systems is introduced. A survey of some chaotic encryption algorithm is presented in section 5.3. A new method for encrypting voice, text and image files using chaotic signals is presented in section 5.4. Section 5.5 is the conclusion and section 5.6 is the chapter references.

5.2 Background of the classical cipher algorithms

There are several algorithms used in cryptographic systems. Some cryptographic methods rely on the secrecy of the algorithm, such algorithms are only of historical or academic interest and are not adequate for real-world needs. All modern algorithms use a key to control the encryption and the decryption. A message can be decrypted only if the key matches the encryption key. The key used for decryption can be different from the encryption key but for most algorithms they are the same. There are two classes of key-based algorithms **symmetric** (or secret-key) and **asymmetric** (or public-key) algorithms [8]. In symmetric algorithms, the encryption and the decryption keys are the same. Symmetric key algorithms require that the sender and the receiver agree on a key before they can communicate securely. The security of the symmetric key system rests in the key itself. Revealing the key means that anyone could encrypt and decrypt the messages. Symmetric algorithms are divided into two categories stream cipher and block cipher. The **stream cipher** operates on the plaintext as a single bit (or sometimes byte) at a time. The **block cipher** operates on a group of

bits. For modern computer algorithms a typical block size is 64 bits. Asymmetric key or **public-key** algorithms are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot be calculated from the encryption key, at least for any reasonable amount of time. These algorithms are called public-key because the encryption key is made public. A complete stranger can use the encryption key to encrypt a message but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the **public key** and the decryption key is often called the **private key**. Strong cryptographic algorithms are designed for execution by computers or specialised hardware devices. Generally, symmetric algorithms are much faster to execute on a computer than asymmetric ones. In practice the two systems are often used together so that a public-key algorithm is used to encrypt a randomly generated encryption key and the random key is used to encrypt the actual message using a symmetric algorithm.

Next a brief description of some examples of the classical encryption algorithms are introduced.




5.2.1 The data encryption standard (DES)

DES is a symmetric algorithm developed in the 1970s [9]. It was made a standard by the US government and has also been adopted by several other governments worldwide. It is widely used, especially in the financial industry. The DES assumes the data are available in binary form. It is designed for enciphering and deciphering blocks of data of 64 bits. The key is also 64 bits long of which 56 bits are used for encryption and the remaining 8 bits are used for parity checks. The total number of keys is thus $2^{56}=7.2 \times 10^{16}$. The DES algorithm consists essentially of a series of permutations and substitutions. A block, which is to be enciphered, is first subjected to an initial permutation, *IP*, then to a complex series of key-dependent operations and finally to a

permutation IP^{-1} which is the inverse of the initial permutation. Since the DES uses 56-bit keys, it is fairly easy to break with modern computers or special-purpose hardware. DES is getting too weak and should not be used in new designs. A variant of DES is the Triple-DES or 3DES, which is based on using DES three times.

5.2.2 International Data Encryption Algorithm (IDEA)

The IDEA is an algorithm developed at ETH Zurich in Switzerland [9]. It works with blocks of 64 bits just as DES does. Each block is divided internally into 4 blocks of 16-bits each. The number of rounds is 8 and the size of the key is 128 bits. The round is a group of XOR, multiplications and additions. The input of the IDEA algorithm consists of 4 blocks of 16-bits each denoted by X_1, X_2, X_3 and X_4 . In every round i , 6 subkeys are used each 16 bits long and they are denoted by $K_{i,1}, \dots, K_{i,6}$. Since there are 8 rounds 48 subkeys are used plus 4 extra keys, which are used after the last round to transform the output. The 4 output blocks are denoted by Y_1, Y_2, Y_3 and Y_4 . In each round, the 16-bit blocks are XOR-ed and multiplied as indicated in Fig. 5.1. There are three algebraic groups whose operations are being mixed and they are easily implemented in both hardware and software:

- XOR 
- Addition modulo 2^{16} 
- Multiplication modulo $2^{16} + 1$ 

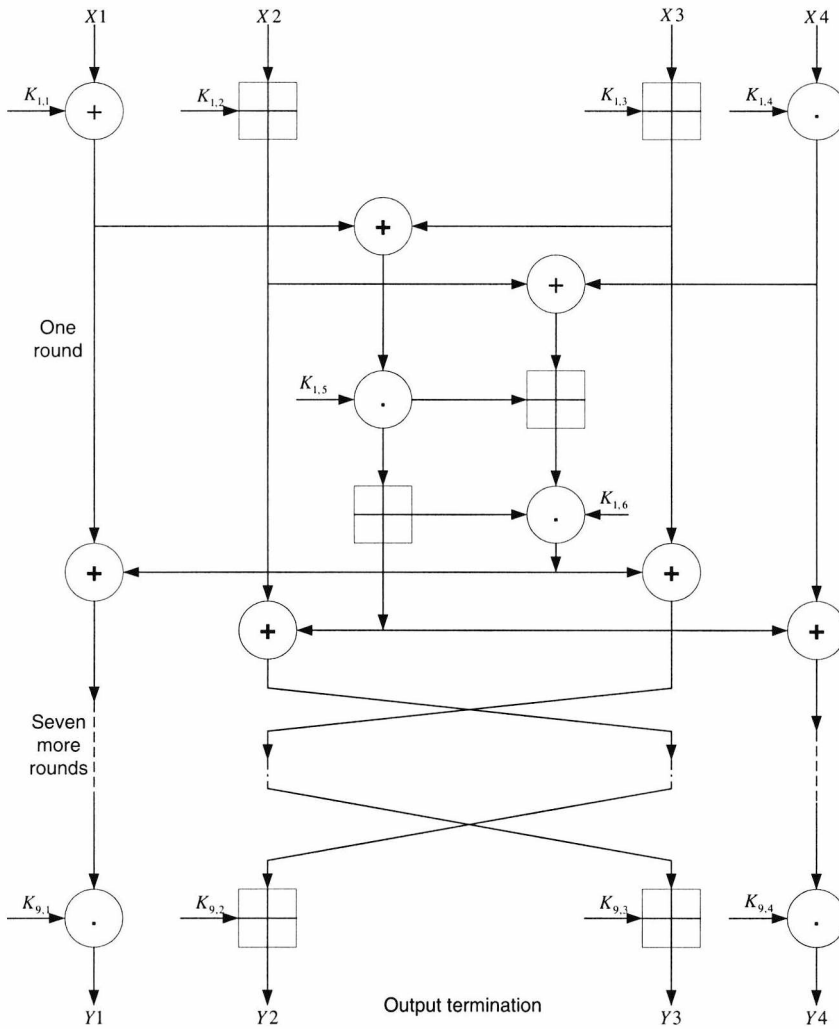


Fig. 5.1 Block diagram of the IDEA algorithm.

5.2.3 Rivest-Shamir-Adleman (RSA) algorithm

RSA is the most commonly used public key algorithm [9]. It is generally considered to be secure when sufficiently long keys are used. The security of RSA relies on the difficulty of factoring large integers. Dramatic advances in factoring large integers would make RSA vulnerable. At present 512 bit keys are considered weak, 1024 bit keys are probably secure enough for most purposes and 2048 bit keys are likely to remain secure for decades. The RSA works as follows:

1. Key generation

- Select two large prime numbers p and q , each about 100 decimal digit long.
- Let $n = pq$ and $\phi(n) = (p-1)(q-1)$.
- Select a random integer e between 3 and $\phi(n)$ which has no common factor with $\phi(n)$.
- Compute d which is the inverse of e modulo $\phi(n)$ [8]

$$d = e^{-1} \text{ mod}(\phi(n)) \quad (5.1)$$

- The public information consists of the pair of integers (e, n) .

2. Encryption

For a plaintext M which is an integer between 0 and $(n-1)$, the ciphertext is computed by:

$$C = M^e \text{ mod}(n) \quad (5.2)$$

3. Decryption

The message M is recovered by computing

$$M = C^d \text{ mod}(n) \quad (5.3)$$

5.2.4 El-Gamal cipher algorithm

El-Gamal cipher is also a public key cipher based on the discrete log problem [9]. If Alice wants to send a binary n -tuple message M to Bob over an insecure channel the processes involved are given below:

1. Key generation:

- Bob selects a random number b as his private key.
- Bob computes Z^b as his public key.

Where Z is an integer number less than the prime number.

2. Encryption

- Alice selects a random integer K and computes Z^K .
- Alice looks up Bob's public key Z^K and computes MZ^{Kb} .
- Alice transmit the pairs Z^K and MZ^{Kb} to Bob.

3. Decryption

- Bob recovers the original message by computing.

$$M = \frac{MZ^{Kb}}{Z^{Kb}} \quad (5.4)$$

5.3 Chaos encryption algorithms background

The problem of finding secure communication methods, which transmit confidential information secretly, has a practical interest in several areas including the protection of communication channels, databases and software. Several techniques have been developed in this area. Yang *et al* proposed a chaos-based secure communication system [10] to overcome the methods of attack proposed recently [11]-[13]. In this method instead of encoding the message signal using a chaotic signal directly, two chaotic signals are used. One signal is used for the synchronisation between the chaotic encrypter and the chaotic decrypter and the other signal is used to encrypt the plain signal using the multi-shift cipher [9] scheme as shown in Fig. 5.2.

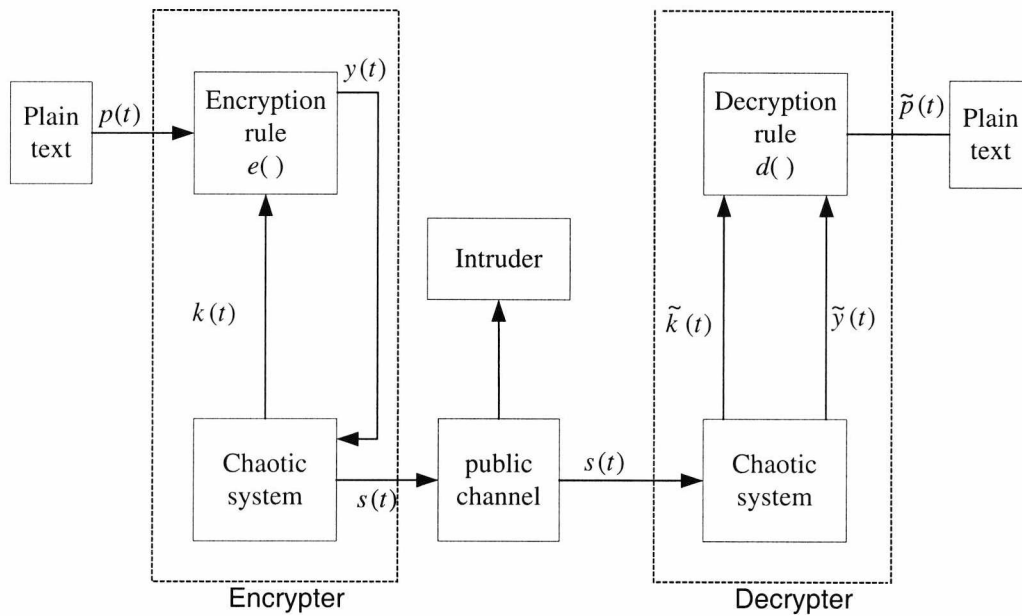


Fig. 5.2 Block diagram of the chaotic cryptosystem.

The system is explained as follows, the chaotic cryptosystem consists of the encrypter and the decrypter. The encrypter consists of a chaotic system and an encryption function $e(k)$ (n-shift cipher [9]). The key signal $k(t)$ is one of the state variables of the chaotic system and another state variable $s(t)$ is the transmitted signal. The encrypted signal $y(t)$ is fed back into the chaotic system. The state variable $s(t)$ is transmitted through a public channel to the decrypter and is used to synchronise the encrypter and decrypter. The decrypter consists of a chaotic system and a decryption function $d(t)$. The decrypter can find the key signal when the decrypter and the encrypter are synchronised. The encrypted signal is also recovered via synchronisation, then $d(t)$ is used to decrypt the encrypted signal. This system differs from the traditional discrete cryptosystem where both the key and the encrypted signal should be transmitted to the decrypter. Tao Yang *et al* uses Chua's circuit [14] to implement this system. The voltage across the capacitor C_2 is used as the key generator while the voltage across the capacitor C_1 is used to synchronised the encrypter and the decrypter.

Grassi and Mascolo [15]–[16] used the same technique introduced by Yang *et al* to encrypt the plaintext but they used a hyperchaos generator [17] as the chaotic system.

Next, a new method for encrypting voice, text and image files using chaotic encryption algorithms is introduced.

5.4 New chaotic algorithms for secure computer communication

Most publication to-date dealing with secure communication using chaos use analogue physical electronic circuits and attempt to develop a real time system [18]–[22]. In our view this approach has little chance of developing a practical system for the following reasons:

- Good synchronisation is very difficult as the element values cannot be controlled to the required accuracy and are functions of age, temperature, manufacturing tolerances ...etc.
- The channel characteristics cannot be predicted or taken into account. This leads most publications in this field to consider only ideal channels. In practice such systems have little value.
- The systems and the non-linearities used are only those that can be implemented using electronic circuitry, which makes an unnecessary restriction.
- The time constants of the system cannot be easily adjusted to ensure that the information signal and the chaotic signal fall within the same frequency band.

Nowadays most communication is through computers and even real-time communication systems are mostly digital not analogue. A computer-based algorithm has the following advantages.

- The communication channel has no effect on the transmitted signal apart from the communication delay.

- Text, images and recorded voice can be transmitted.
- Email is the most used personal communication medium, especially for official communication which is the kind that will mostly need security.
- Any chaotic algorithm can be used without the restriction that it can be implemented using an analogue circuit. The choice is based entirely on reliability and security.
- Non-linearities are described by any mathematical equation and hence any non-linearity can be used.
- There is a freedom in the choice of the transmitted signal.
- The algorithm is easily transportable and can be incorporated in the email communicator.

We shall describe an example of such a system that achieves degrees of synchronisation, security and reliability that cannot be achieved otherwise.

5.4.1 Chaotic encryption algorithms

The algorithm developed is based on the Chua circuit, the Rössler system or the Lorenz system [23]-[24]. Combinations of these systems are also possible. The starting point is to develop computer models for the transmitter and the receiver. One main reason that previous results have a high limit on the signal to chaos ratios is that the receivers use differentiators to retrieve the signal. Differentiators will always produce large spikes and high error if the signal contains discontinuities which is always the case for images and text signals. We next describe transmitter-receiver systems that overcome the above problems. We shall use the Chua circuit to start with and then give the equivalent Rössler and Lorenz systems.

5. 4. 1.1 The Chua encryption algorithm

First we write the equations for the Chua transmitter and since they are treated as a purely mathematical algorithm and we no longer have capacitors and inductors. We shall use the usual symbols for the state variables.

The transmitter state equations are given by

$$\begin{aligned}
 x_1 &= A_1 \int A_2(x_2 - x_1) - f(x_1) dt \\
 x_2 &= A_3 \int A_2(x_1 - x_2) - x_3 + Av_{in} dt \\
 x_3 &= A_4 \int x_2 - A_5 x_3 dt.
 \end{aligned}
 \tag{5.5}$$

In Eq. (5.5) the input plaintext v_{in} is added to the second equation. This results in the plaintext not being a simple addition to the transmitted signal. The plaintext is also multiplied by a constant A to reduce its value with respect to the chaotic signal. We shall present results later where $A = 10^{-13}$ which results in a signal to chaos ratios of about -240 dB. A can take any value rather than 10^{-13} but less than $A = 10^{-13}$, the numerical solver of the algorithm needs less step size to solve the algorithm as a result the algorithm becomes slow and greater than this number means the signal to chaos ratio at the input of the system is increased and the system becomes less secure. The transmitted signal is dx_2/dt instead of any of the state variables and this has the crucial advantage that differentiation is avoided in the receiver. The derivative dx_2/dt is of course readily available in the transmitter before integrating the second equation.

The receiver equations are given by

$$\begin{aligned}
 x'_1 &= A_1 \int A_2(x'_2 - x'_1) - f(x'_1) dt \\
 v_{out} &= \frac{1}{A} \left(\frac{1}{A_3} \frac{dx_2}{dt} - A_2(x'_1 - x'_2) + x'_3 \right) \\
 x'_3 &= A_4 \int x'_2 - A_5 x'_3 dt
 \end{aligned}
 \tag{5.6}$$

where v_{out} is the recovered informational signal.

The above arrangement has the following advantages:

1. The plaintext is not simply added to the chaotic signal and thus cannot be retrieved by subtraction.
2. Differentiation is avoided anywhere in the system and thus eliminating the spikes that are always generated by the process of differentiation of abruptly changing signals. This allows very low signal to chaos ratios.

Eqs. (5.5) and (5.6) can be easily represented using SIMULINK. The signal flow of the encrypter and the decrypter are shown in Figs 5.3 and 5.4. The explanation of the encryption and the decryption algorithms are discussed below.

1. The encryption algorithm

- The plaintext file is read and the total number of characters inside the file is calculated.
- The encryption keys are chosen by the user and stored into a file.
- The total number of the plaintext characters and the encryption keys file are stored into one file called the **keys file**.
- The keys file is loaded to the algorithm and is applied to the demultiplexer.
- The demultiplexer converts the keys file values from a one-dimensional array into individual values to be manipulated by the encryption algorithm. The output of the demultiplexer is fed to the encryption algorithm.
- The encryption algorithm is a direct representation of the Eq. 5.5.
- The plaintext is loaded to the algorithm and is encrypted using the encryption keys.
- The clock is an up-counter used to compare its instantaneous value with the total number of characters. When these are the same and all the plaintext characters are encrypted, the encryption algorithm is stopped.

- The resultant ciphertext is stored into a file and sent to the decrypter through the LAN or WLAN.
2. The decryption algorithm
- The total number of characters inside the received ciphertext is calculated.
 - The decryption keys and the total number of ciphertext characters are stored in one file called the **keys file**.
 - The keys file is applied to the demultiplexer.
 - The demultiplexer converts the keys file values from a one-dimensional array into individual values to be manipulated by the encryption algorithm. The output of the demultiplexer is fed to the encryption algorithm.
 - The decryption algorithm is a direct representation of Eq. 5.6.
 - The received ciphertext is loaded to the algorithm and is decrypted using the decryption keys.
 - The clock is an up-counter whose instantaneous value is compared to the total number of ciphertext characters. When these are the same and all the ciphertext are decrypted, the decryption algorithm is stopped.
 - Finally, the recovered plaintext is stored into a file.

The algorithms have also been converted to standalone C++ programs, which are approximately two orders of magnitude faster than the SIMULINK model.

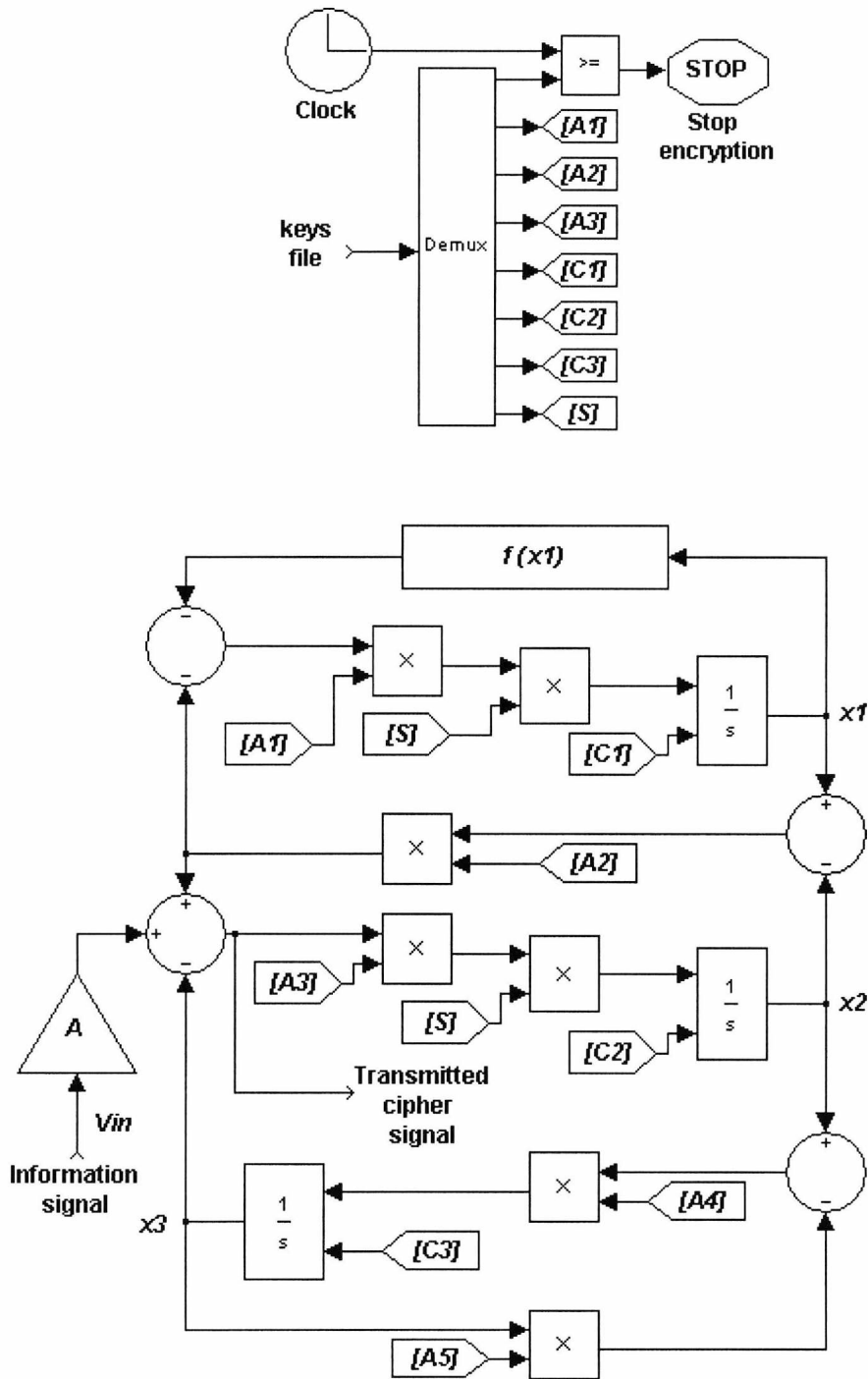


Fig. 5.3 The Chua encryption algorithm.

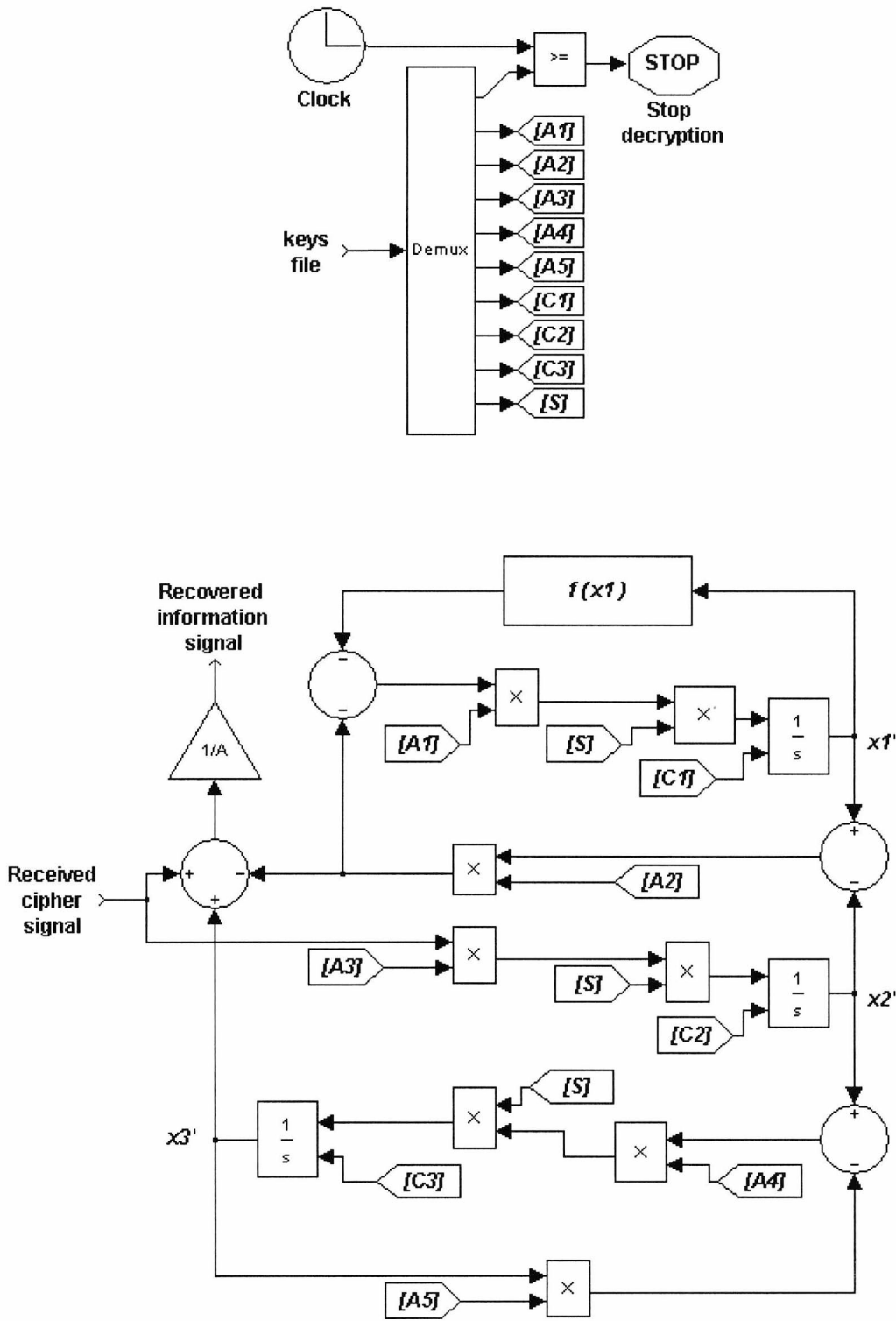


Fig. 5.4 The Chua decryption algorithm.

5.4.1.2 The Rössler encryption algorithm

Similar development is achieved for systems based on the Rössler and the Lorenz equations.

The equations for the Rössler transmitter are given by

$$\begin{aligned}
 x_1 &= -\int x_2 + x_3 \, dt \\
 x_2 &= \int x_1 + A_1 x_2 + A v_{in} \, dt \\
 x_3 &= \int A_3 + x_3 (x_1 - A_2) \, dt
 \end{aligned} \tag{5.7}$$

The transmitted signal is dx_2/dt and the equations for the Rössler receiver are given by

$$\begin{aligned}
 x'_1 &= -\int x'_1 + x'_3 \, dt \\
 v_{out} &= \frac{1}{A} \left(\frac{dx_2}{dt} - x'_1 - A_1 x'_2 \right) \\
 x'_3 &= \int A_3 + x'_3 (x'_1 - A_2) \, dt.
 \end{aligned} \tag{5.8}$$

The signal flow of the transmitter and the receiver is illustrated in Fig. 5.5 and Fig. 5.6. The explanation of the encrypter and the decrypter are similar to the Chua algorithm in the previous system.

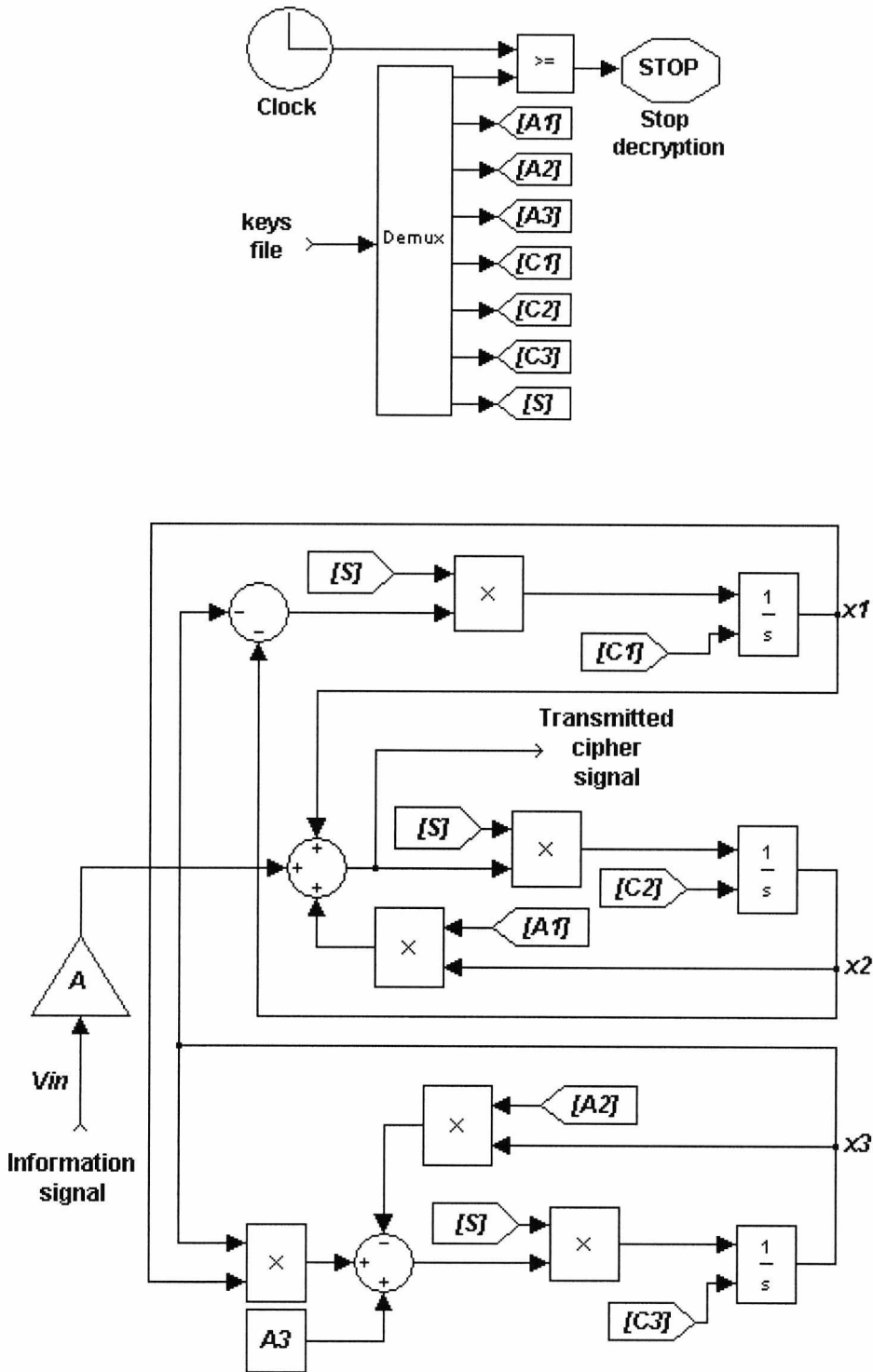


Fig. 5.5 The Rössler encryption algorithm.

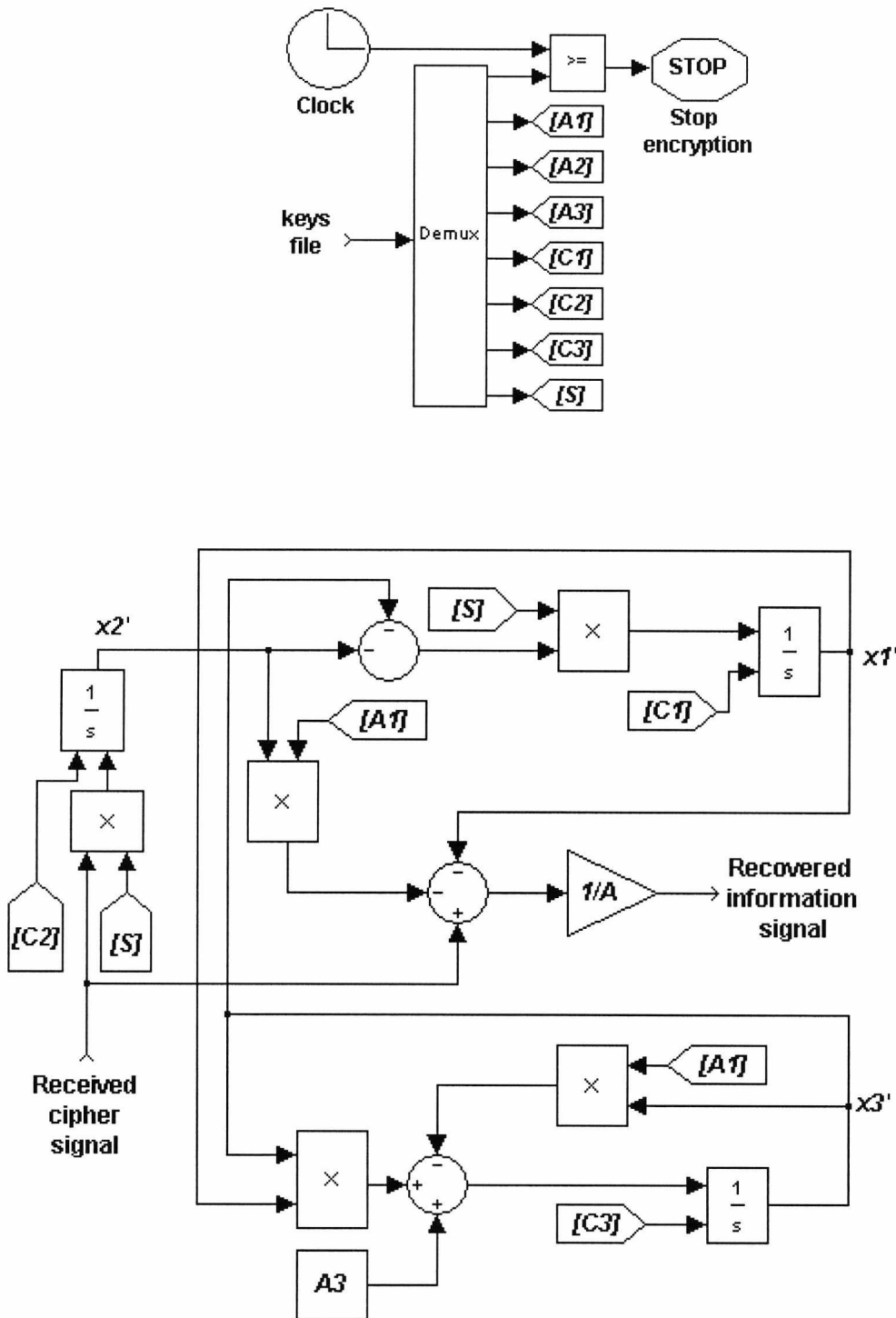


Fig. 5.6 The Rössler encryption algorithm.

5.4.1.3 The Lorenz encryption algorithm

Similarly the equations for the Lorenz transmitter are given by

$$\begin{aligned}
 x_1 &= A_1 \int x_2 - x_3 dt \\
 x_2 &= \int A_2 x_1 - x_2 - x_1 x_3 + A v_{in} dt \\
 x_3 &= \int x_1 x_2 - A_3 x_3 dt.
 \end{aligned}
 \tag{5.9}$$

The transmitted signal is dx_2/dt and the equations for the Lorenz receiver are given by

$$\begin{aligned}
 x'_1 &= A_1 \int x'_2 - x'_1 dt \\
 v_{out} &= \frac{1}{A} \left(\frac{dx_2}{dt} - A_2 x'_1 + x'_2 + x'_1 x'_3 \right) \\
 x'_3 &= \int x'_1 x'_2 - A_3 x'_3 dt.
 \end{aligned}
 \tag{5.10}$$

The transmitter part of the algorithm is shown in Fig. 5.7 while the receiver part of the algorithm is shown in Fig. 5.8. The explanation of the encryption and the decryption algorithms are similar to the Chua algorithm.

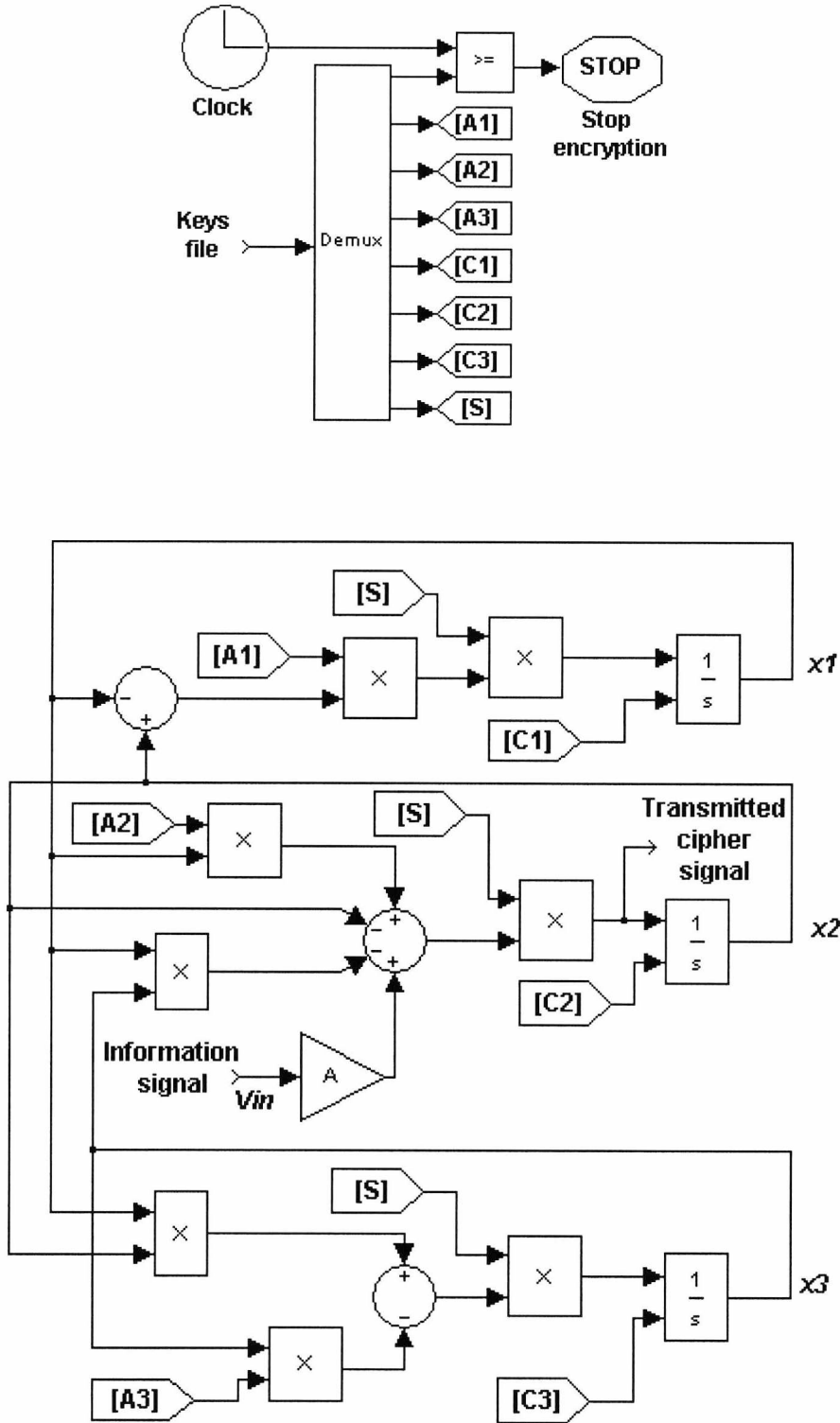


Fig. 5.7 The Lorenz encryption algorithm.

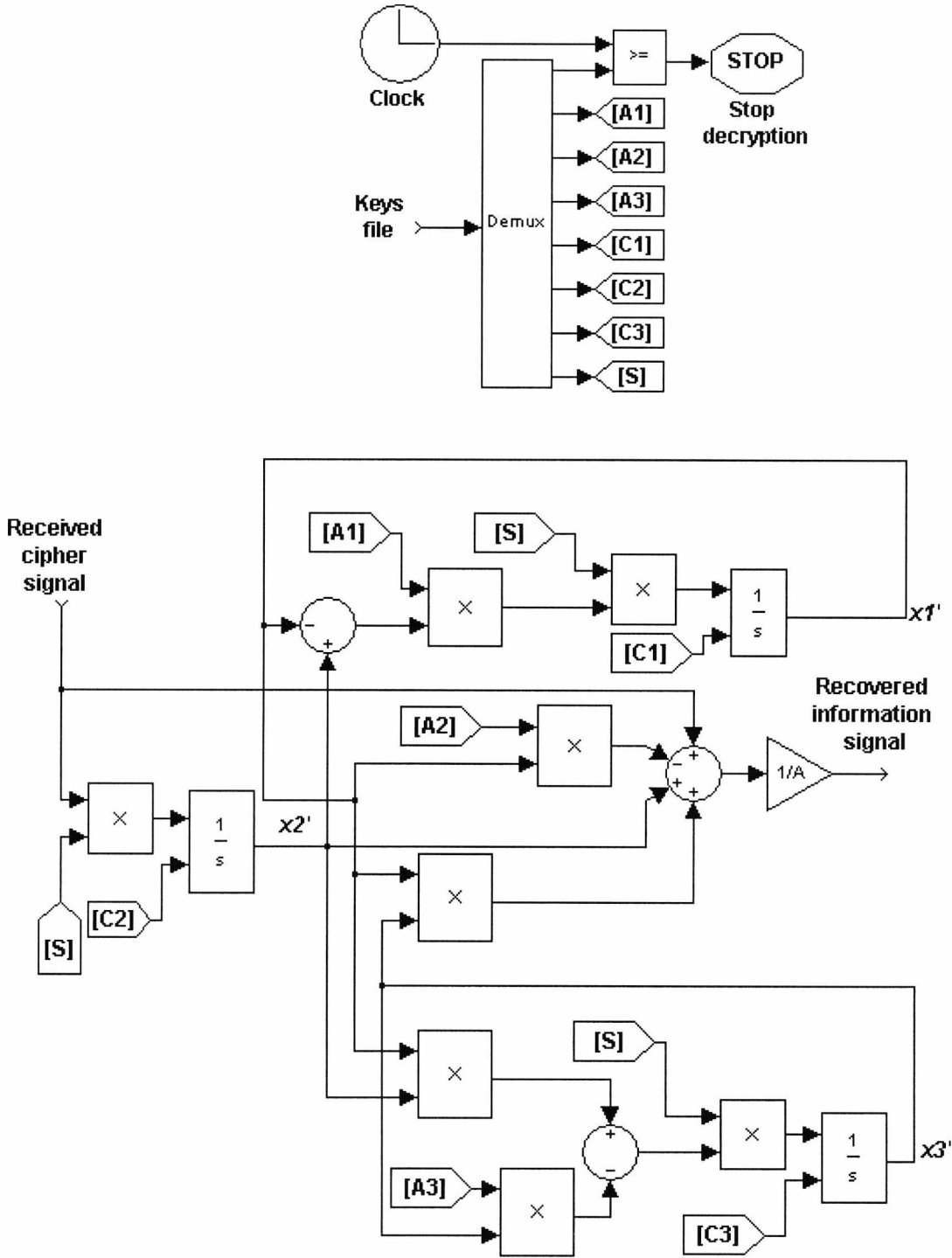


Fig. 5.8 The Lorenz encryption algorithm.

In all cases, differentiation has been avoided which permits a very low signal to chaos ratios. Also in all cases the information signal is not simply added to the chaos and this contributes to the security of the system. Alternative systems can be developed for all the above cases by transmitting the derivative of x_1 instead of that of x_2 .

In all cases, stand alone C++ files have been developed which have the advantage of considerable savings in computer time, especially when transmitting an image. Care has to be taken that both transmitter and receiver use the same ODE solver and the same time step. Otherwise synchronisation will not be achieved and the signal cannot be recovered.

5.4.2 System security

There are several aspects of security that need to be fully investigated. The present algorithms are intended to concentrate on the ability to recover text, image or voice signals accurately. A full investigation on security, methods of attack and counter measures will be given in chapters 6 and 7. However we shall discuss here the features of the algorithms that contribute to security.

The most important aspect of security is the identification of the key and the computational effort required in determining it. If we consider the Chua system, there are five constants in the equations and three initial conditions in the integrators. Each of these has to be adjusted to an accuracy of one part in 10^{13} to achieve synchronisation between transmitter and receiver. One part of 10^{13} is choosing because 10^{-13} multiplies the information signal. Note that, we can multiply the information signal by other values less than or greater than 10^{-13} but the restriction is in the numerical integrator used to solve the algorithm and the minimum step size used by the numerical integrator. Less value need minimise the step size as a result the algorithm becomes very slow. One could jump to the conclusion that these are the system keys and that 10^{104} mathematical steps are required for brute force cryptanalysis. This however is not true as chaotic systems can be analysed using more systematic approaches, which drastically

reduce the computational effort required. A complete evaluation of the mathematical efforts required will be made in the next chapter. We wish to mention here that the constants in the equations can also be non-linear functions of the state variables of any desired complexity and any number of parameters provided that they are bounded and do not take the system out of chaos. This adds considerably to the security of the system.

A very important feature of the systems is the ability to transmit very low signal to chaos ratios and recover the message fully without loss of information. Signals to chaos ratios between -200 dB and -244 dB have been achieved. The exact ratio depends on the complexity of the plaintext and the desired accuracy of the recovered signal. This low signal to chaos ratio makes it almost impossible to retrieve the plaintext from signal processing techniques based on Fourier analysis. Results on the effect of the signal to chaos ratio on the recovery of the signal are given later in this chapter. Fig. 5.9 shows how a square wave, a saw-tooth and a voice signal are accurately recovered with a signal to chaos ratio of approximately -220 dB.

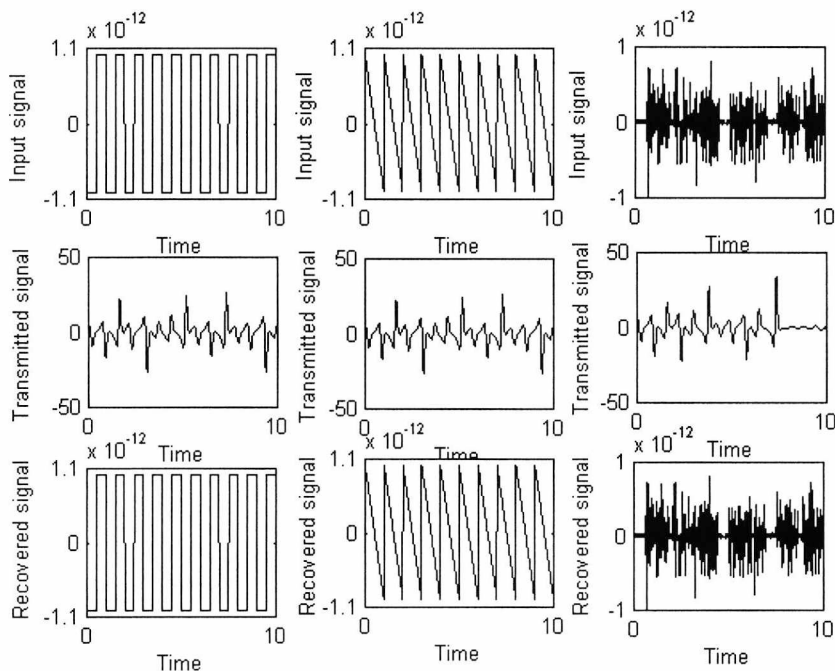


Fig. 5.9 Results of the system simulation for a square, a saw-tooth and a speech signals.

Another aspect of security is that the sample time of the signal and the algorithm time constants have to be adjusted such that the spectrum of the signal falls within the spectral band of the chaos for maximum security. The step size of the solution affects the signal to chaos ratio that can be used. Reducing the step size will allow a reduction in the signal to chaos ratio but will increase the processing time. Fig. 5.10 shows a comparison of the spectrum of the signal (an ASCII input message, the input message text or image is read as ASCII characters) and the chaos signal from a Lorenz system. We note that the ASCII signal has a high DC value as to be expected. The figure indicates that the input message and chaotic signal have the same frequency band and spectrum of the input message is hidden in the spectrum of the chaotic signal.

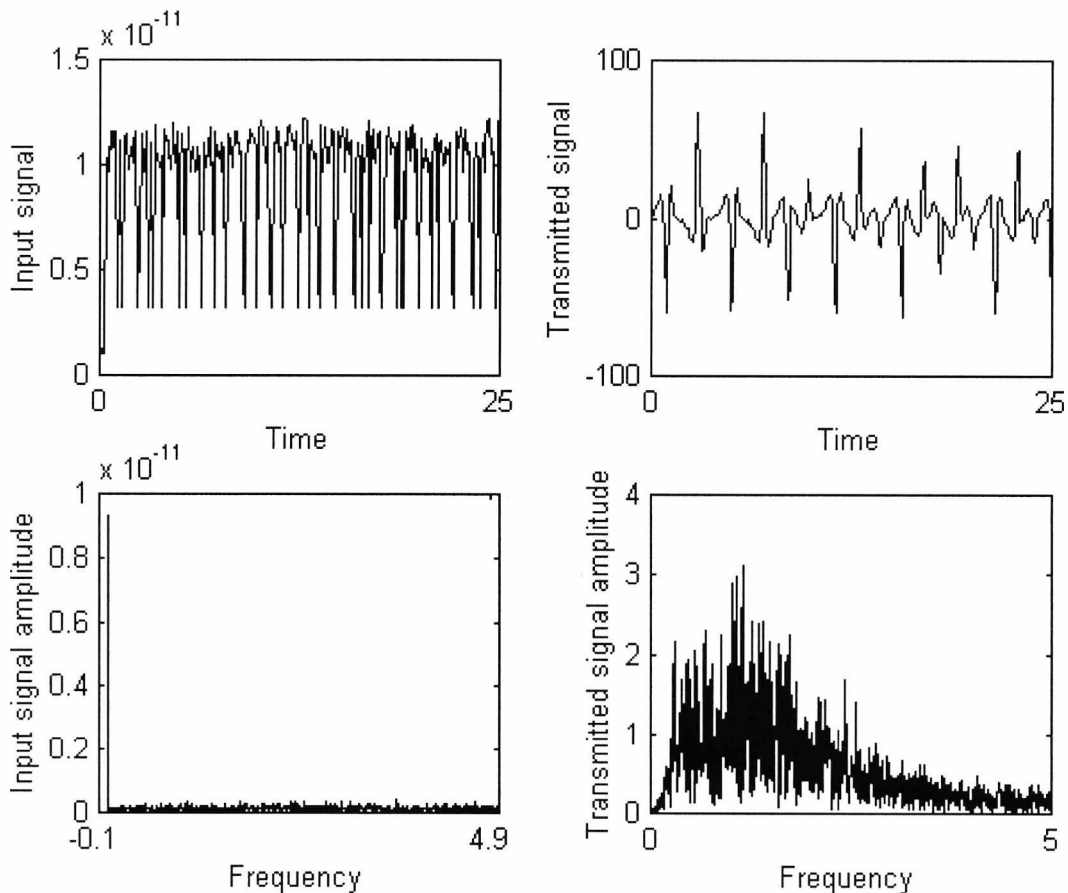


Fig. 5.10 Comparison in time and frequency domains between the information and the chaotic signals.

The third aspect of security is to ensure that simple subtraction of the chaotic signal from the cipher text cannot reveal the message. This is to guard against the cryptanalyst getting hold of a chaotic signal that was once transmitted without a message and then subtracting it from all subsequent transmissions. Fig. 5.11a shows the result of subtracting the chaos from the transmitted signal and clearly indicates that the signal is not retrieved. To improve this aspect of security a random number can be transmitted as the first byte which will alter the chaotic signal for every transmission. The receiver does not require knowledge of the random number as this is recovered automatically. Knowledge of the random number does not help the cryptanalyst in any way to reveal the signal. Fig. 5.11b shows the improvement in security when a random number is used. Needless to say that a different number should be used for every transmission.

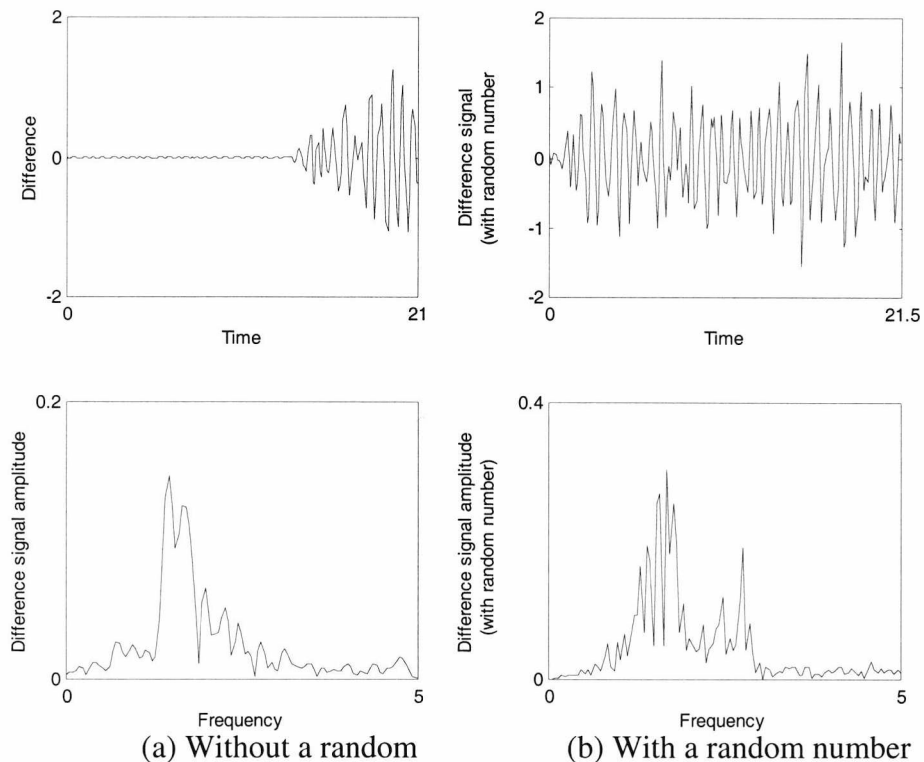


Fig. 5.11 Effect of subtracting the chaos from the ciphertext without and with a random number as the first byte.

5.4.3 Results

The algorithms have been tested with voice signal, ASCII text and images. Formatted files such as Word, Word perfect or Framemaker files are treated as images. Black and white images are two-dimensional arrays and colour images are three-dimensional arrays. As the algorithm can only handle one-dimensional arrays, the signal is always put first into a one-dimensional double precision array before processing. In the case of images, all the information about the image format is already included in the file and no further effort is necessary for restoration at the receiver. For each system (Chua, Rössler and Lorenz), we introduce two methods for the encryption of the plaintext.

- Method 1

In this method, two different time steps are used. One time step is used for reading (0.1) the plaintext and the second time step (0.01) is used in the encryption algorithm for encrypting the plaintext. The reason for that is to make the plaintext and the chaotic signals have the same frequency bands.

- Method 2

The same time steps are used for reading and encrypting the plaintext but new parameter values are used in each algorithm. With these parameters the plaintext and the chaotic signal will have the same frequency band.

The transmitted file in these algorithms is floating point data file. As an example, the transmitted data file when we encrypt the text " This is a test " is:

```

0          0.100000000000000000  0.200000000000000000
0.300000000000000000 -0.0999999999999060  0.04003251496356
0.09743506714715  0.01738905153180  0.4000000000000000
0.500000000000000000  0.6000000000000000  0.7000000000000000
-0.02666325656784  0.04904117572583  0.12460327288093
0.09452765724923  0.8000000000000000  0.9000000000000000
1.0000000000000000  1.1000000000000000 -0.05130176845176
-0.33069190606817  0.46862536345653 -0.13477048692124
1.2000000000000000  1.3000000000000000  1.4000000000000000
0.49030994451921  0.58889188973474  0.1070940525336

```

Table 5.1 gives the parameter values used in each algorithm. Table 5.2 is a comparison between the key length of each algorithm in both methods. Table 5.3 is a comparison between the three algorithms in the case of encrypting text file (A4.txt) which is a complete A4 text page. The table gives the size of the plaintext file, the size of the ciphertext file, the average time used for encrypting and decrypting the text file and the signal to chaos ratio (SCR). Table 5.4 gives a comparison between the three algorithms in the case of encrypting the image file (Cameraman.tif).

System	Parameters	Method 1			Method 2		
Chua	A_1	10			10		
	A_2	0.635			0.53		
	A_3	1.2			1.5		
	A_4	5.6			5.6		
	A_5	0.019			0.019		
	Scaling factors	9	9	9	2	18	1.6
	Integrators initial conditions	0.1	0.1	0.1	0.1	0.1	0.1
Rössler	A_1	0.46			0.4		
	A_2	4			3.255		
	A_3	2			2.85		
	Scaling factors	9	9	9	3.5	3.5	5
	Integrators initial conditions	0.01	0.01	0.85	0.01	0.01	0.85
Lorenz	A_1	10			10		
	A_2	28			28		
	A_3	2.667			2.667		
	Scaling factors	2	2	2	1.5	0.25	1.5
	Initial conditions	0.5	0.5	0.5	0.1	0.1	0.1

Table 5.1 The algorithms parameter values.

System	Method 1		Method 2	
	Key length (Digits)	Key length (Bits)	Key length (Digits)	Key length (Bits)
Chua	81	270	110	336
Rössler	63	210	110	336
Lorenz	63	210	110	336

Table 5.2 Systems key lengths.

File name	System	Method	File size (Kbytes)		Average time (seconds)		SCR in dB
			Plain text	Cipher text	Encrypt	decrypt	
A4.txt (27 lines, 282 words and 1804 characters)	Chua	Method 1	28.4	282	1	2	-214.51
		Method 2	28.4	28.4	0.75	1	-210.83
	Rössler	Method 1	28.4	282	1	2	-228
		Method 2	28.4	28.4	0.7	1	-222.19
	Lorenz	Method 1	28.4	282	0.9	4	-238
		Method 2	28.4	28.4	0.7	1	-244.41

Table 5.3 File size, SCR and average time required for encrypting and decrypting the text file (A4.txt).

File name	System	Method	File size (Mbytes)		Average time (seconds)		SCR in dB
			Plain text	Cipher text	Encrypt	Decrypt	
Cameraman.tif (256x256 pixels)	Chua	Method 1	0.99	9.95	29.793	486.52	-210.48
		Method 2	0.99	0.99	24.375	10.595	-207.50
	Rössler	Method 1	0.99	9.95	46.287	419.143	-224.75
		Method 2	0.99	9.95	23.163	19.718	-218.86
	Lorenz	Method 1	0.99	9.95	53.476	470.406	-234.62
		Method 2	0.99	0.99	15.503	10.075	-240.94

Table 5.4 File size, SCR and time required for encrypting and decrypting the image file (Cameraman.tif).

Next a comparison between the first and the second methods is introduced in Table 5.5.

Chapter 5 Secure computer communication using chaotic algorithms

Comparison	Method 1	Method 2
Key length	Between 210-270 Bits depending on the algorithm used	336 Bits
Solver time steps	Different time steps are used for reading and encrypting the plaintext	The same time steps are used for reading and encrypting the plaintext
Time for encryption and decryption	The time required for encrypting and decrypting the plaintext is much higher than the second method	Less time
File size	The file size of the ciphertext is equal 10 times that of the plaintext	The ciphertext and the plaintext have the same file sizes.
Security	The security of the algorithms is in the fact that each character of the plaintext is encrypted into 10 characters of the ciphertext. So redundancy characters are added to the ciphertext	The security of this method is in the fact that with any error of the key values of order 10^{-11} of its original value, the plaintext cannot be recovered. In the first method the error is of order 10^{-9} .
Usage	It is difficult to use this method for encrypting the image files. This is due to the limitation of the file size transmitting through the e-mail channel since the transmitted file size very large. It is suitable for text files.	Suitable for encrypting text and image files.

Table 5.5 Comparison between the first and second methods of the developed encryption algorithms.

Next, we will introduce the results of encrypting and decrypting text and image files using the different systems. The results of the Chua encryption algorithm as an example for encrypting a text file using the two previously mentioned methods are presented. Fig. 5.12 shows the results of encrypting a text file using the first method. It is clear that the transmitted ciphertext has more characters than the plaintext. The file size of the plaintext is 105 bytes while the transmitted ciphertext file is 1.02 Kbytes. The time for the encryption is 0.598 seconds, the time taken for the decryption is 0.9893 seconds and the SCR is -214 dB.

Plaintext
<p>Recently, Pecora and Caroll demonstrated the possibility of synchronizing of the chaotic systems [1].</p>
Ciphertext
<pre> &/8>CEDA;2(____)17;===;9631/,)\$____"5H YgrxyvnbR?+____!&'(,3=IT_fjkg_TE5#____&+,+)'(+/49=?@>:4,"____"+ 27;>?@?>=;83,#____#8L_mx_€ sfUA_\$\$&*1=KZgrz zshYG3_\$\$&'+2=JWbqpqnf[L;(#(*)(*.5=EKPSRNH>3%____)15763.(!____"##"____%.6<@BA=7/% !*7;>??><:863/(____'<Oaoy~_zpbQ=(____!\$&*2=KZgqwzwpdUC/_%'(*:EQ[d ijgaVI9'____\$*,,)''(+048;<;93\$____&.49=?@?=94+____)>Qbpy~~xn `N:%____"%' +2>KYfpvxumbSA_!&'(* /7ALV^ceb\SF7'____\$+.,,(%#"# %'**)'#____ &+0367651,\$____<ISZ^_[TJ=.____(.10)\$____ ____#*/2431,&____\$+16:=??><93*____ _%8JZfossoeXH6"____%(((*.6?HQW[\YSI=/____&.231'!____ ____ ____%(+--,*& ____*5>EJLJF?6+____#,37::850+%____ ____!*29>@>92)____%.49=???>=;962+!____#8L^mx_€ sfUA,____ ____\$&*1<JYgry zshYG3____\$&'+2<HU`inpmezL;)_____ ____#)*)(),18?FKMNKE=2&____'/589851,%____ ____(/47874/(____'.49=?@A@>;6.\$____"6I[isy{wnbQ>*____ ____"%'(-5@LXbjnmi'TE4!____ </pre>
Recovered Text
<p>Recently, Pecora and Caroll demonstrated the possibility of synchronizing of the chaotic systems [1].</p>

Fig. 5.12 Example of encrypting and decrypting of a text file using method 1.

Fig. 5.13 shows results of encrypting a text file using the second method. In this case, the plaintext and the ciphertext files have the same number of characters and the same size (395 bytes). The time taken to encrypt the plaintext is 0.5828 seconds, the time taken to decrypt the cipher text is 0.9745 seconds and the SCR is equal to -210 dB. It is clear that the second method is faster than the first method and the size of ciphertext file is less than that of the first method.

Plaintext

Recently, Pecora and Carroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Ciphertext

```

2G JY ; >< ^;+% %1_5F__ Z,3r_O_-
_&_(S07q_O/'#_PG_w*L
8_/!&V72v_Q%%_)0_CW iR<H_2% A;_7[_Z`,L_#_
_1*_RK
_z+M: <_O$_CB_cB25"1_=[_a^3K_9*_L<
_I_50_(,L! ?d_D_3_
-].Du_Q_,6_@J_E&_Z,#_*_8( _YH_€_P4_2L_QU_=/_@W
dw6I!_!_7
!_'187|_Q'_
4@_OM_,_*_%020o
K_3&_1_#J!_RA_t,J6_"_(?_9W_)
_4_+\\1?w_Q_'6_9_L,_d'5!_*,>>_0[_Pf_N
    
```

Recovered text

Recently, Pecora and Carroll demonstrated the possibility of synchronizing the chaotic systems [1]. Itho et al [2] introduces a new communication system as a possible application of chaotic synchronization. The main idea of this system is to use the chaotic modulation to transmit the information signals and the chaotic synchronization mechanism to recover the information signals.

Fig. 5.13 Example of encrypting and decrypting a text file using method2.

Next, the results of sending an image via email using the Chua algorithm are given. Fig. 5.14 shows the original image, the transmitted image and the recovered image. The figure shows that the input image is completely hidden and recovered at a SCR of -210 dB. The encryption time is 547.888 seconds, the decryption time is 545.154 seconds and the size of the image is 8.29 Mbytes.

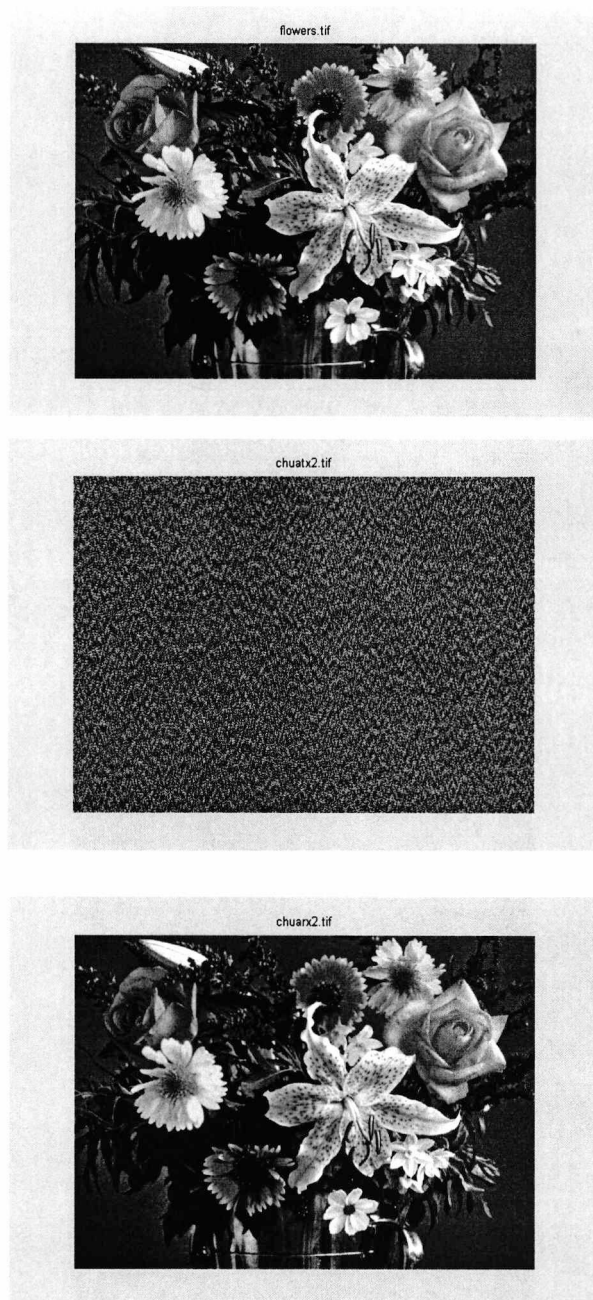


Fig. 5.14 Encryption and decryption of the image file (flowers.tif) using Chua encryption algorithm.

Fig. 5.15 shows the input image signal (flowers.tif) and the Chua transmitted chaotic signal in the time and frequency domains. The figure indicates that the image signal is completely hidden in the transmitted chaotic signal (SCR=-210 dB) and completely recovered. The figure also indicates that the input image signal and the transmitted chaotic signal occupy the same frequency bands.

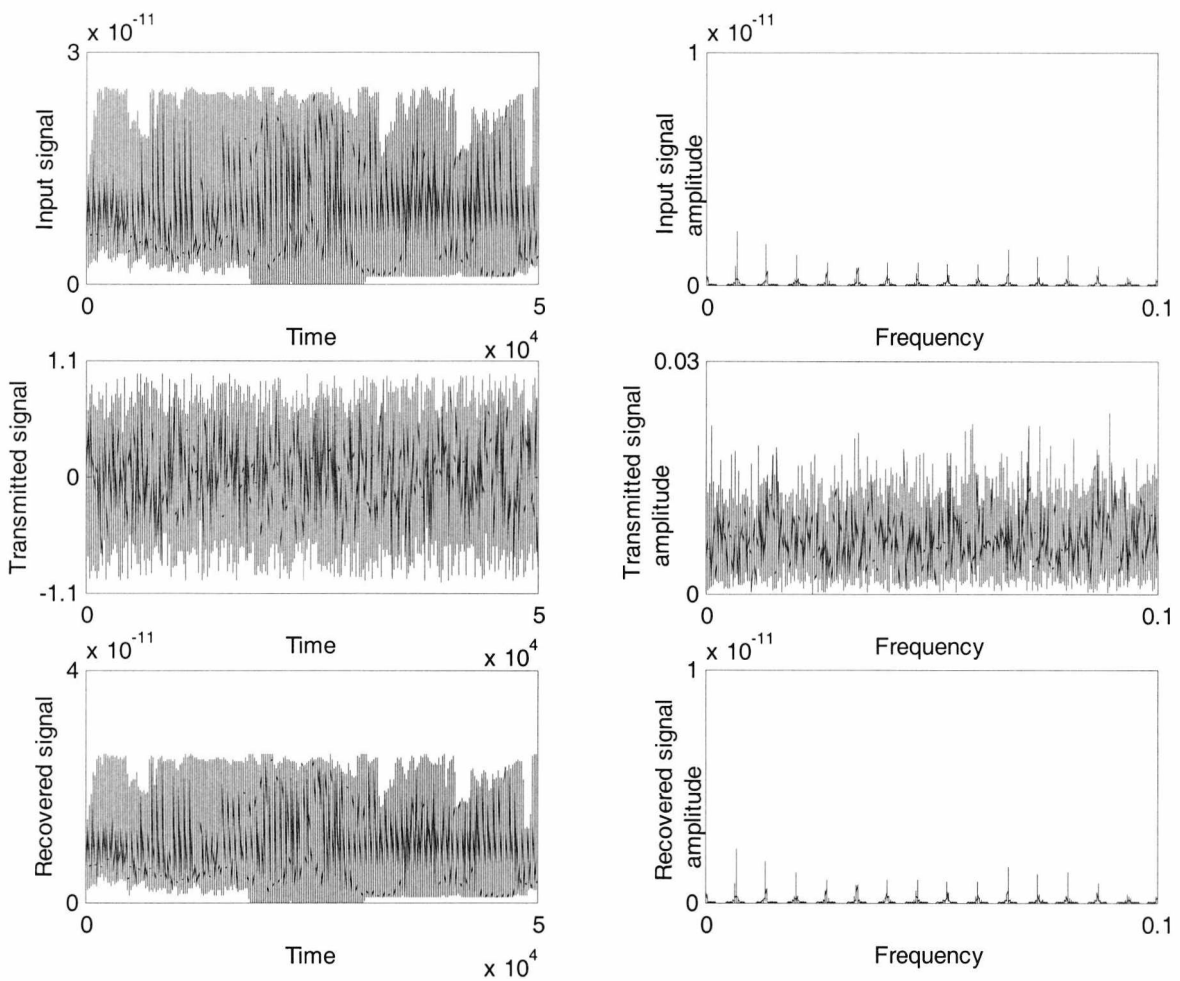


Fig. 5.15 Input, transmitted and recovered signals in the time and the frequency domains.

Fig. 5.16 shows the results of encrypting the image file (saturn.tif) using the Rössler encryption algorithm. The figure illustrates input image, transmitted image, and the recovered image at SCR of -223 dB. The encryption time is

15.413 seconds, the decryption time is 15.412 seconds and the size of the image is 2.19 Mbytes.

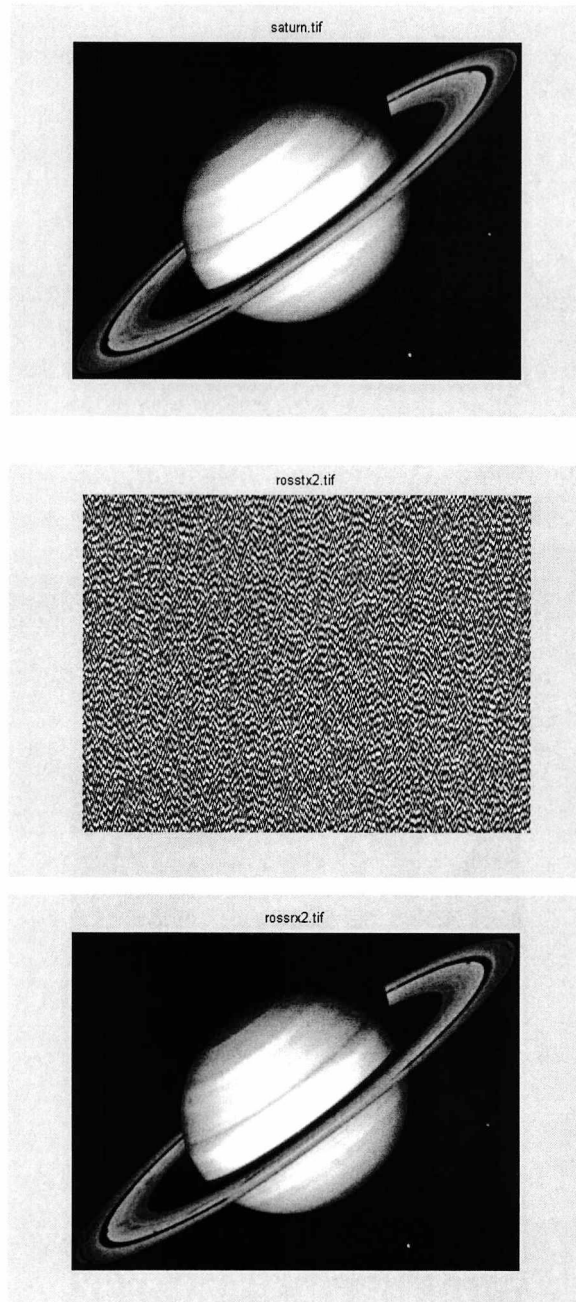


Fig. 5.16 Encryption and decryption of the image file (saturn.tif) using Rössler encryption algorithm.

Figure 5.17 shows the spectrum of the input image (saturn.tif), the transmitted chaotic signal and the recovered signal when it is encrypted using the Rössler encryption algorithm. The figure shows that the image signal is completely hidden in the transmitted signal, in the time and the frequency domains, and completely recovered.

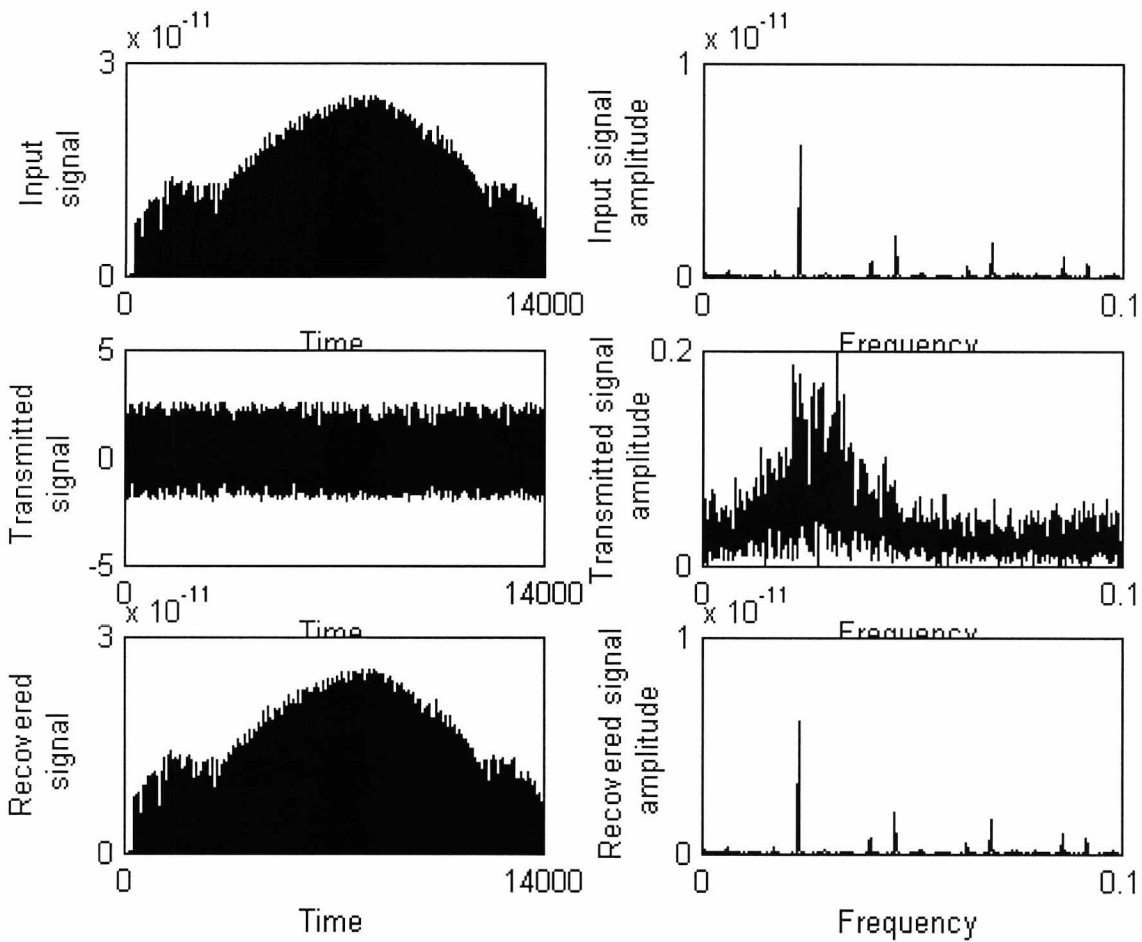


Fig. 5.17 Input, transmitted and recovered signals in the time and the frequency domains.

Fig. 5.18 shows the using of Lorenz encryption algorithm to encrypt the image file (cameraman.tif). It illustrates input image, transmitted image and the

recovered image at SCR=-240 dB. The encryption time is 15.503 seconds, the decryption time is 10.412 seconds and the size of the image is 0.99 Mbytes.

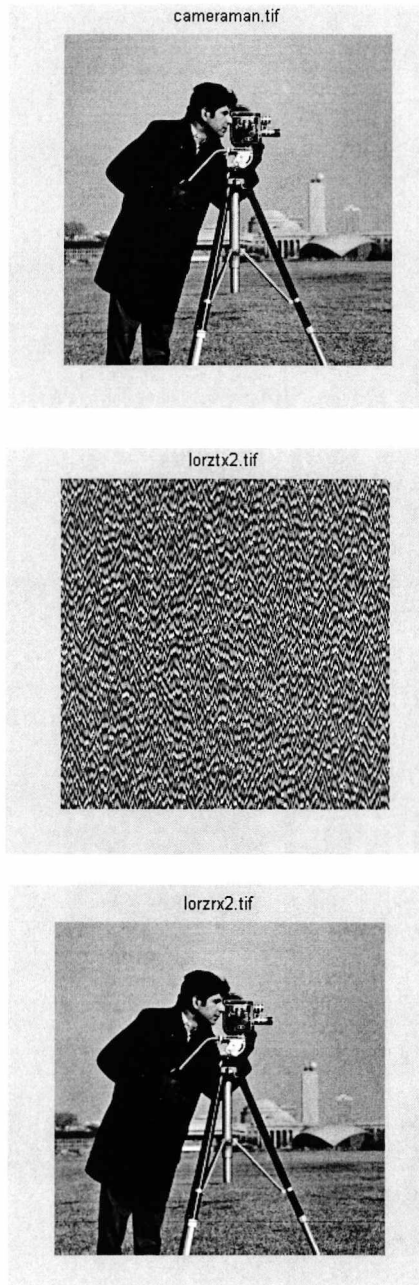


Fig. 5.18 Encryption and decryption of the image file (cameraman.tif) using Lorenz encryption algorithm.

Fig. 5.19 shows the spectrum of the input image, the transmitted Lorenz chaotic signal and the recovered signal in the time and the frequency domains. The figure verifies that the input image and the transmitted chaotic signal occupy the same frequency band and the input image is completely recovered using the decrypter algorithm.

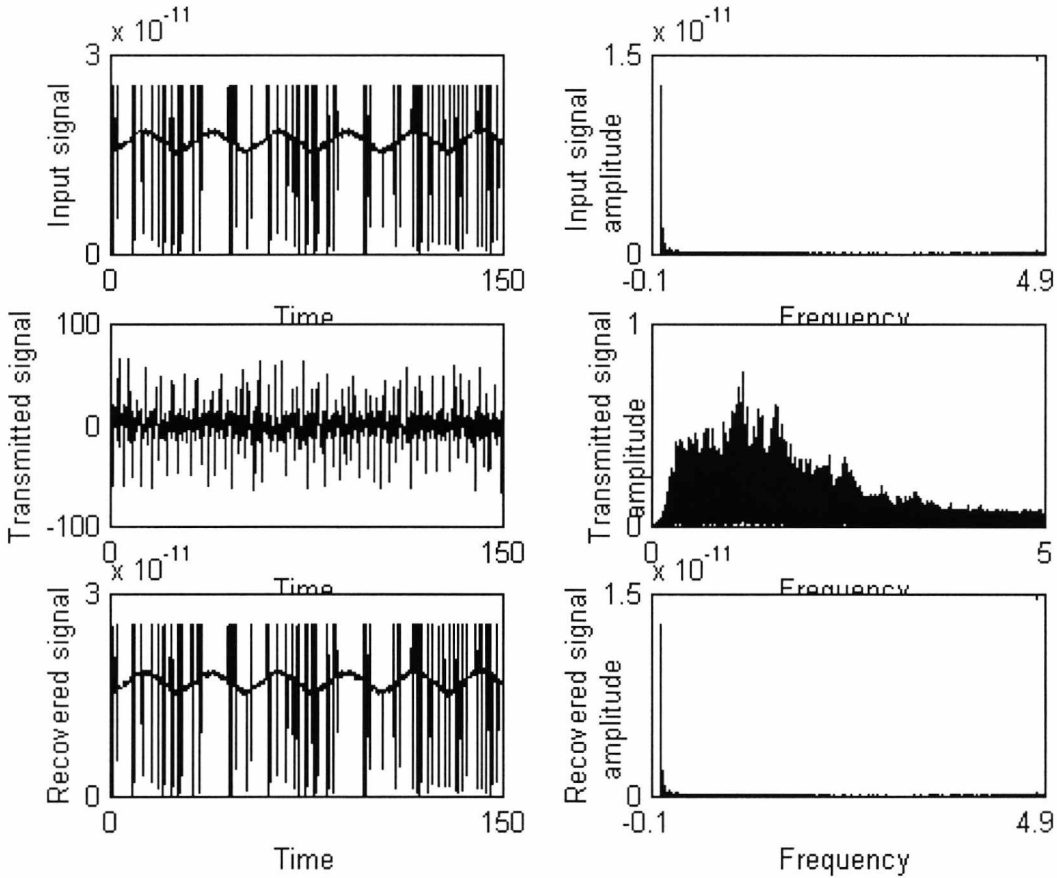


Fig. 5.19 Input, transmitted and recovered signals in the time and the frequency domains.

Chapter 5 Secure computer communication using chaotic algorithms

We next study the effect of reducing the signal to chaos ratio. Fig. 5.20 shows recovered images with various signals to chaos ratio. A good image is still recoverable at -240 dB.

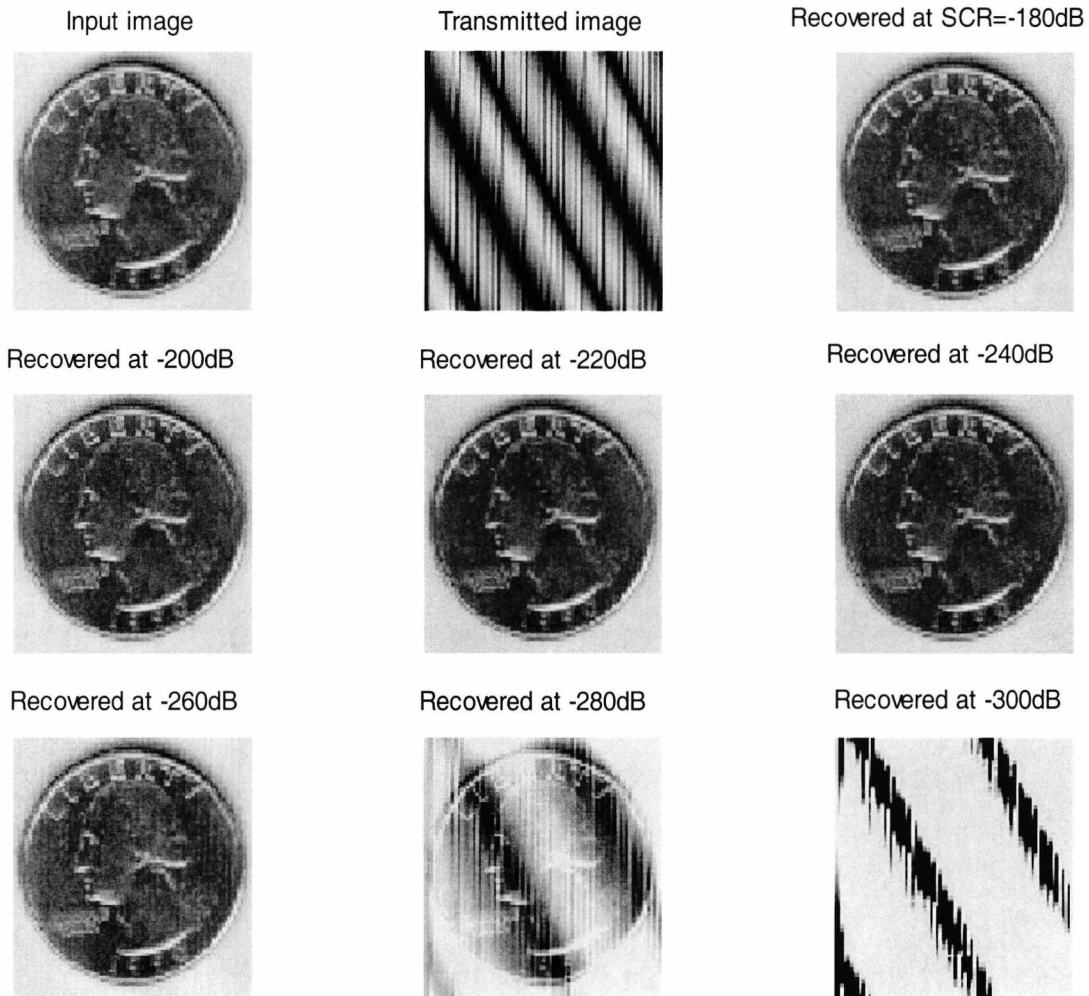


Fig. 5.20 Effect of changing the signal to chaos ratio.

Finally, we introduce a comparison between our chaotic algorithms, classical encryption algorithms and chaotic communication systems. We know that one of the measures of the security of the encryption algorithms is the key length. As the key length increases the security of the system is increased. Table 5.6 shows a comparison between the developed algorithms, which are symmetric algorithms and the classical symmetric encryption algorithms such as the DES and the IDEA.

Algorithm		Key length
DES		64 Bit (56 Bits as a key and 8 Bits as a parity checker)
IDEA		128 Bits
Chaotic encryption algorithms	Method 1	Between 210-270 Bits depending of the encryption algorithm used
	Method 2	336 Bits

Table 5.6 Comparison between the developed chaotic encryption algorithms and the classical encryption algorithms

Next a comparison between the developed chaotic encryption algorithms and the chaotic communication systems is introduced.

- This is the first time that the results of using the chaotic encryption algorithms for encrypting image (B/W and colors image files) are introduced.
- Our developed algorithms achieve a signal to chaos ratio of between -200 and -240 dB, while the minimum signal to chaos ratio in the other chaotic communication systems to-date is around -42 dB [25].

- Our algorithms are tested by sending text and image files through a practical channel (LAN or WLAN) and the information signals are transmitted and recovered without any errors.

5.5 Conclusion

The application of chaotic algorithms to secure communication are most suitable for computer communications where the channel does not affect the synchronisation between the transmitter and the receiver.

The algorithms can be used for text messages, images or recorded voice signals with extremely high security. Signal-to-chaos ratios of 10^{-13} or -240 dB have been achieved. A full analysis of the security aspect and the computational effort required will be given in chapter 6. The developed algorithms run either as SIMULINK files or as stand alone C++ files. The C++ versions are about two orders of magnitude faster than that of the SIMULINK models. We have presented practical results to support our claims. A comparison between the developed chaotic encryption algorithms and the classical symmetric encryption algorithms are presented. The key length of the chaotic algorithms is greater than the key length of the classical symmetric encryption algorithms (DES and IDEA) which means more security. The algorithms are at present used for potential secure computer communication and databases and we expect that they can also be developed to work in real time digital communication systems.

5.6 References

- [1] J. C. A. Van Der Lubbe, *Basic methods for Cryptography*: published by Cambridge University Press 1998.
- [2] F. L. Bauer, *Decrypted secrets: Methods and maxims of cryptology*. Berlin Heidelberg: Springer-Verlag, 1997.
- [3] A. Dmitriev, A. Panas and S. Stakov, "Transmission of complex analog signals by means of dynamical chaos," *Proc. 3rd Int. Specialist Workshop on Nonlinear Dynamics of Electronic Systems NDES'95*, pp.241-244, 1995.
- [4] M. Dai, Y. Zhang, Y. Hua, W. Ni and G. Du, "Implementation of secure digital communication by hyperchaotic synchronisation," *Electron. Lett.*, vol. 34, No. 10, pp. 951-953, May 1998.
- [5] T. Habutsu, Y. Yoshifumi, I. Sasase and S. Mori, "A secret key cryptosystem using a chaotic map," *IEICE Trans. Fundamentals*, vol. E73, No. 7, pp. 1041-1044, July 1990.
- [6] R. Mathews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. XIII, No. 1, 1989.
- [7] J. M. Carroll, J. Verhagen and P. Wong, "Chaos in cryptography: The escape from the strange attractor," *Cryptologia*, vol. XVI, No. 1, 1992.
- [8] B. Schneier, *Applied cryptography*: John Wiley & Sons, Inc, 1996.
- [9] D. Stinson, *Cryptography: theory and practice*. Boca Raton FL: CRC Press, 1995.
- [10] T. Yang, C. W. Wu and L. O. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuits Syst. I*, vol. CAS-44, No. 5, pp. 469-472, May 1997.
- [11] C. W. Wu and L. O. Chua, "A unified framework for synchronisation and control of dynamical systems," *Int. J. Bifurcation and Chaos*, vol. 4, No. 4, pp. 979-998, 1994.
- [12] K. Short, "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurcation and Chaos*, vol. 6, pp. 367-375, 1996.

- [13] C. W. Wu, T. Yang and L. O. Chua, "On adaptive synchronisation and control of nonlinear dynamical systems," *Int. J. Bifurcation and Chaos*, vol. 6, No. 3, pp.455-471, 1996.
- [14] L. O. Chua, "Chua's circuit- an overview ten years," *J. Circuit, Syst., Comput.*, vol. 4, No. 2, pp.117-159, Jan. 1995.
- [15] G. Grassi and S. Mascolo, "A systems theory approach for designing cryptosystems based on hyperchaos," *IEEE Trans. Circuits Syst. I*, vol. CAS-46, No. 9, Sept. 1999.
- [16] G. Grassi and S. Mascolo, "Driving cryptosystems with hyperchaotic signals: An approach involving linear observers," *IEEE Int. Symposium. on Circuit and System. (ISCAS 2000)*, pp. V501-V504, 2000.
- [17] A. Tamaševičius, A. namajūnas and A. Čenys, "Simple 4D chaotic oscillator," *Electron. Lett.*, vol. 32, No. 11, pp.957-958, 1996.
- [18] T. Yang, "Recovery of digital signals from chaotic switching," *Int. J. Circuit theory appl.*, vol. 23, No. 6, pp. 611-615, Dec. 1995.
- [19] C. W. Wu and L. O. Chua, "A unified framework for synchronisation and control of dynamical systems," *Int. J. Bifurcation and. Chaos*, vol. 4, No. 4, pp. 979-998, 1994.
- [20] A. Tamasevicius, G. Mykolaitis, A. Cenys and A. Namajunas, "Synchronisation of 4D hyperchaos oscillators," *Electron. Lett.*, vol. 32(17), pp. 1536-1537, 1996.
- [21] C. K. Pham and M. Tanaka, "Bifurcational communication with novel chaotic transistors circuits," *IEEE Int. Symposium. on Circuit and System (ISCAS 96)*, pp. 100-103, 1996.
- [22] Y. Horio and K. Suyama, "Experimental verification of signal transmission using synchronised chaotic neural networks," *IEEE Trans. Circuits Syst.*, vol. CAS-42, pp. 393-395, July 1995.
- [23] M. I. Sobhy and A. R. Shehata, "Secure e-mail and databases using chaotic algorithms," *Electron. Lett.*, vol. 36, No. 10, May 2000.

Chapter 5 Secure computer communication using chaotic algorithms

- [24] M. I. Sobhy and A. R. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurcation and Chaos*, will be published in Nov. 2000.
- [25] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos*, vol. 4, No. 4, pp. 959-977, 1994.

of outputs 4 in test mode. This type needs one test session to test the whole circuit. This is the selected way in this thesis.

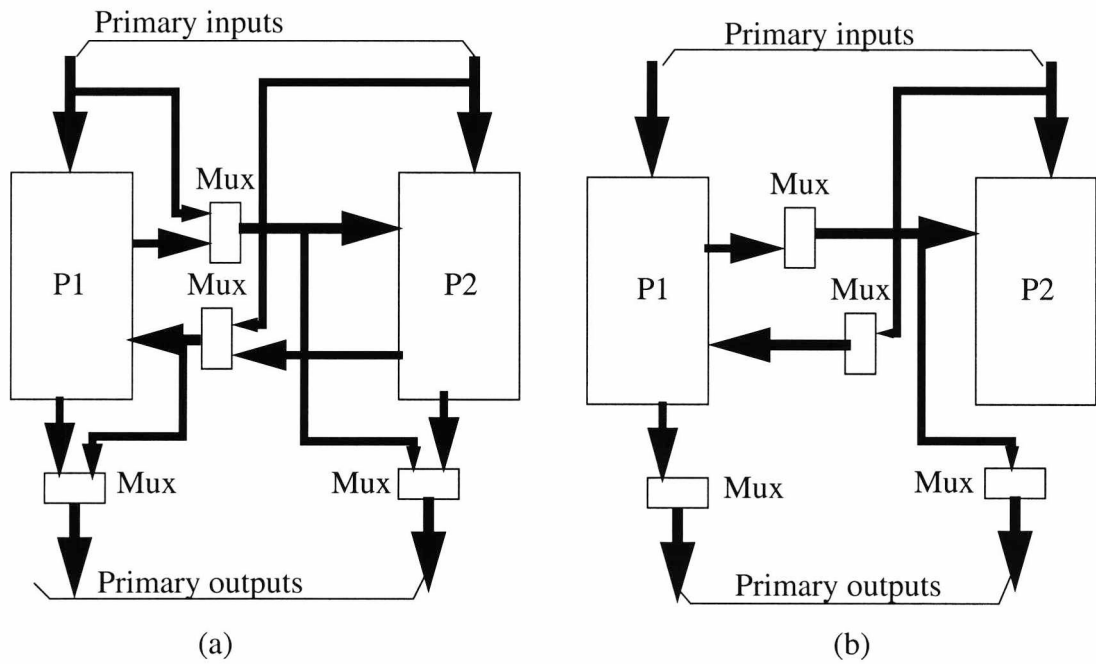


Fig. 3.3 Hardware partitioning (a) General hardware partitioning scheme using multiplexer (b) Configuration to test partition P1.

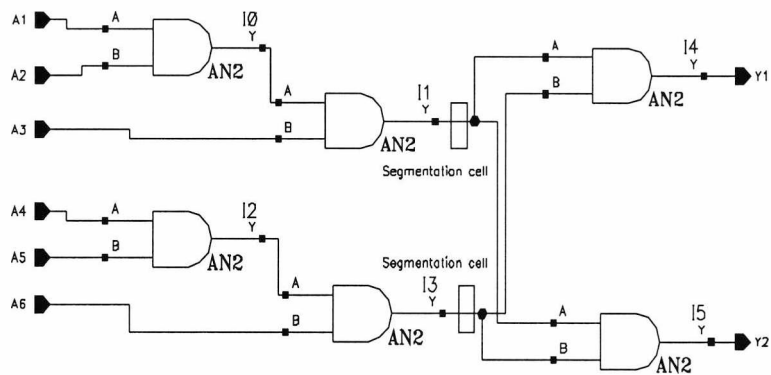


Fig. 3.4a A partitioned circuit in normal mode.

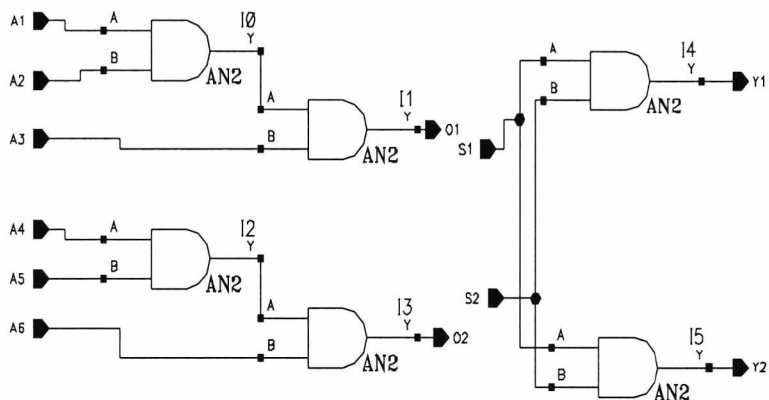


Fig. 3.4b A partitioned circuit in test mode.

Chapter 6

ATTACKING CHAOTIC ENCRYPTION SYSTEMS

6.1 Introduction

The whole point of cryptography is to keep the plaintext (or the key or both) secret from eavesdroppers. Eavesdroppers are assumed to have complete access to the communications between the sender and the receiver. **Cryptanalysis** is the science of recovering the plaintext of a message without access to the key. Successful cryptanalysis may recover the plaintext or the key. It may also find weaknesses in a cryptosystem that eventually lead to recover the plaintext or the key. An attempted cryptanalysis is called an **attack**. There are four general types of attacks. Of course, each of them assumes that the cryptanalyst has complete knowledge of the encryption algorithm used [1]:

1. **Ciphertext-only attack.** The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The cryptanalyst's job is to recover the plaintext of as many messages as possible or deduce the key (or keys) used to encrypt the messages in order to decrypt other messages encrypted with the same keys.
2. **Known-plaintext attack.** The cryptanalyst has access not only to the ciphertext of several messages but also to the plaintext of those messages. The job of the cryptanalyst is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).
3. **Chosen-plaintext attack.** The cryptanalyst has access not only to the ciphertext and associated plaintext for several messages but has also chosen the plaintext that gets encrypted. This is more powerful than the known-plaintext attack because the cryptanalyst can choose specific plaintext blocks to encrypt what might yield more information about the key. His job is to deduce the key (or

keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).

4. **Adaptive-chosen-plaintext attack.** This is a special case of a chosen plaintext attack. Not only can the cryptanalyst choose the plaintext that is encrypted but he can also modify his choice based on the results of previous encryption. In a chosen-plaintext attack a cryptanalyst might just be able to choose one large block of plaintext to be encrypted. In an adaptive chosen-plaintext attack, he can choose a smaller block of plaintext and then choose another based on the results of the first and so forth.

Different algorithms offer different degrees of security depending on how hard they are to break. If the cost required to break an algorithm is greater than the value of the encrypted data then the algorithm is probably safe. If the time required to break the algorithm is longer than the time that the encrypted data must remain secret then the algorithm is probably safe. If the amount of the data encrypted by a single key is less than the amount of data necessary to break the algorithm then the algorithm is probably safe. We say probably because there is always a chance of new breakthroughs in cryptanalysis. On the other hand, the value of most data decreases over time. It is important that the value of the data always remains less than the cost of breaking the security protecting it. An algorithm is said to be **unconditionally secure** if no matter how much ciphertext is available, the cryptanalyst has not enough information to recover the plaintext. An algorithm is said to be **computationally secure** if it cannot be broken with available resources either current or future resources. The complexity of an attack can be measured in different ways:

1. **Data complexity** is the amount of data needed as input to the attack.
2. **Processing complexity** is the amount of processing needed to perform the attack. This is often called the work factor.
3. **Storage requirements** are the amount of memory needed to perform the attack.

As a rule, the complexity of an attack is taken to be the minimum of these three factors.

Lars Knudsen [2] classified the categories of breaking an algorithm as follows:

- **Total break**
The cryptanalyst finds the key.
- **Global deduction**
The cryptanalyst finds an alternate algorithm equivalent to the decryption algorithm without knowing the key
- **Local deduction**
A cryptanalyst finds the plaintext of an intercepted ciphertext.
- **Information deduction**
A cryptanalyst gains some information about the key or plaintext. This information could be a few bits of the key or some information about the form of the plaintext.

Section 6.2 gives some methods of attack of the chaotic communication system. A new algorithm for attacking the chaotic communication systems is introduced in section 6.3. Section 6.4 demonstrates the methods of counter attack of the chaotic communication system. The conclusion and the references of the chapter are in sections 6.5 and 6.6 respectively.

6.2 Chaos attacking background

Many algorithms have been developed to attack the chaotic communication systems [3]-[9]. Short [10] tests the level of security in secure communication systems based on nonlinear dynamics (NLD) or chaos. In these systems, a chaotic carrier is used in a type of spread-spectrum signal with the information signal buried at -30 dB with respect to the chaotic carrier. The analysis process was to use the NLD forecasting to predict the carrier dynamics and then subtract the predicted values to reveal the hidden information signal or at least increase its signal to noise ratio with respect to the carrier. In each case, it was a simple task to determine the power spectrum of the hidden signal once the prediction of the carrier was made. The forecasting approach was extended to allow estimation of the dynamics of the signal using threshold detection so that whenever a signal was detected, multiple predictions of the carrier

behaviour were made. This method was tested on a square wave embedded at -42 dB in a Lorenz carrier. The method was able to reveal the square wave with almost perfect precision except in a few regions where it temporarily lost synchronisation with the carrier.

Stark *et al* [11] consider the problem of extracting a small signal embedded in a stronger background. The desired signal is assumed to be a relatively slowly varying signal. Jaroslav *et al* are able to devise an algorithm, which in simple tests, can recover the signal to a reasonable accuracy when the ratio of amplitudes of signal to chaos background is as low as 10^{-10} . The algorithm essentially takes a time series $\{u_n\}$, which is the sum of a deterministic component $\{x_n\}$ and some other signal $\{S_n\}$ and attempts to separate the two parts. The signal $\{x_n\}$ is usually treated as the desired signal and $\{S_n\}$ as the unwanted noise. Separation is then equivalent to removing the noise component $\{S_n\}$.

Yang *et al* [12] introduce a method for breaking the chaotic switching where the binary message signal is scrambled by two chaotic attractors. In this method the breaking of the chaotic switching is presented using the concept of generalised synchronisation [13]-[14]. They assume that they have no precise knowledge about the chaotic transmitter. They also assume that the receiver system will never synchronise to the unknown chaotic transmitter because there are some significant differences both in structure and in parameters between the chaotic transmitter and the receiver. Yang *et al* get a decoding result as good as that provided by the receiver with the same parameters as those of the transmitter.

As a conclusion, all the above methods, except the breaking of the chaotic switching, assume that the information signal is added to the chaotic signal and they try to separate the information signal from the chaotic signal. This is a special case of the chaotic communication system. The secure communication systems based on hiding the information on chaotic carriers may be useful to increase privacy but are not yet capable of providing a high level of security.

In this chapter, we introduce a new algorithm for attacking the chaotic communication system (continuous or discrete). This algorithm is suitable either when the information signal is added to the chaotic carrier or it is used to modulate

one of the state variables of the chaotic system at signal to chaos ratios of the order of -240 dB.

6.3 New algorithm for attacking the chaotic communication systems

6.3.1 Introduction

A new algorithm for attacking the chaotic communication systems is introduced. It is based on two of the MATLAB optimisation programs [15]. The optimisation finds the optimal solution of a certain problem by finding the maximum or the minimum of a function in an interval, with or without constraints.

Suppose that we want to find a minimum x_{\min} of the function f in an interval.

$$f(x_{\min}) = \min_x f(x). \quad (6.1)$$

An iterative method needs an initial guess x_0 . From this value x_0 , we find a new value x_i which, it is hoped, is closer to x_{\min} . How the better approximation x_i is found, depends on the numerical method used. These iterations continue until an approximation x_i with enough accuracy is found such that $|x_{\min} - x_i|$ is smaller than the required error. If there are several local minima, the optimiser will find one of them. In this work, two optimisation programs are used namely ***E04JAF*** and ***fminsearch***. The ***E04JAF*** is a simple bounded optimisation program and is used to find the minimum of a function of several variables.

The instruction for this program is

$$[x, f(x)] = \text{E04JAF}(x_0, x_1, x_2) \quad (6.2)$$

where x_0 is a vector of the unknown values and is the initial guess, x_1 is a vector of the lower limits of the unknown variables and x_2 is the upper limit. The user must supply a subroutine (target function) *funct1* to calculate the value of $f(x)$ for any given value of x .

The *fminsearch* program is used to find the minimum of a scalar function of several variables starting with an initial estimate. It is generally referred to as unconstrained nonlinear optimisation. It uses the simplex search method [16] and it has the form

$$[x] = \text{fminsearch}(\text{fun}, x_0, \text{options}). \quad (6.3)$$

It returns a vector x that is a local minimiser of the function fun . The vector x_0 contains the initial guesses for the optimiser. The options, for this function, include the maximum number of iterations, allowed termination tolerance of the function value and termination tolerance for x .

In this method of attack, we assume that the dynamics of the system are known but we have no information about the transmitter parameters (encrypter keys) used to encrypt the information. We assume that the receiver output signal (wanted signal) is an error signal of the optimisation algorithm and the algorithm is used to minimise that error. If the error is minimum, then the information signal is recovered. The steps of attacking the chaotic communication systems are summarised as follows:

1. We determine the type of the chaotic communication system under attack from the received ciphertext signal by plotting the attractor of the received data signal. Usually the attractor is a phase-plane of two state variables. However, in this case we have for the transmitted ciphertext only one state variable. To obtain an attractor, we plot the received data samples against the received delayed data samples. For example, if we have 1000 data samples, we plot the data samples from (1:990) against the data samples from (11:1000). These attractors are used as signatures for the chaotic systems. From these signatures, we can determine the type of the system under attack as shown in Figs. 6.1, 6.2 and 6.3.

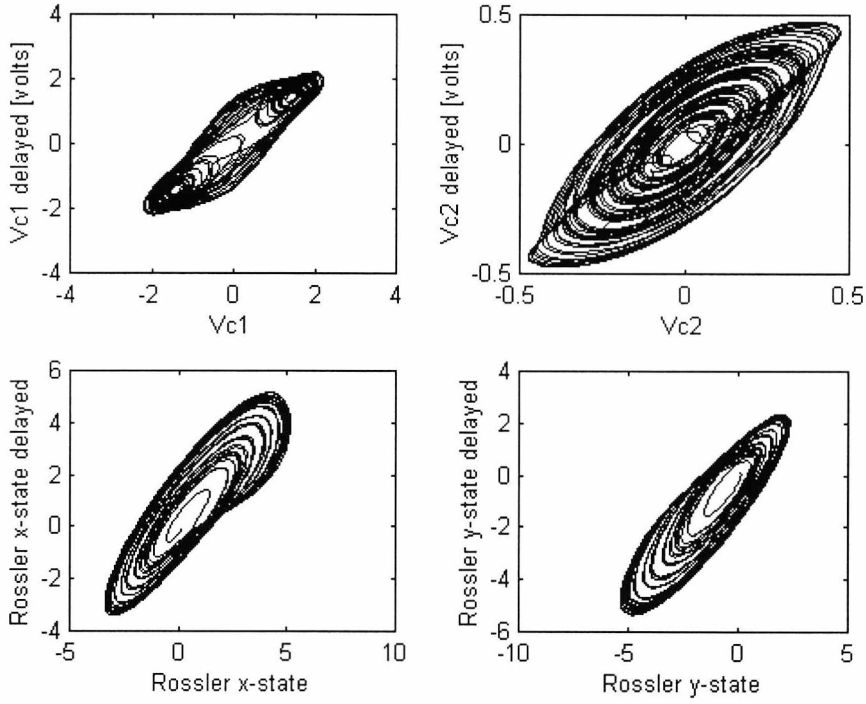


Fig. 6.1 Examples of the continuous time chaotic systems attractors (the upper traces are for Chua and the lower for Rössler systems).

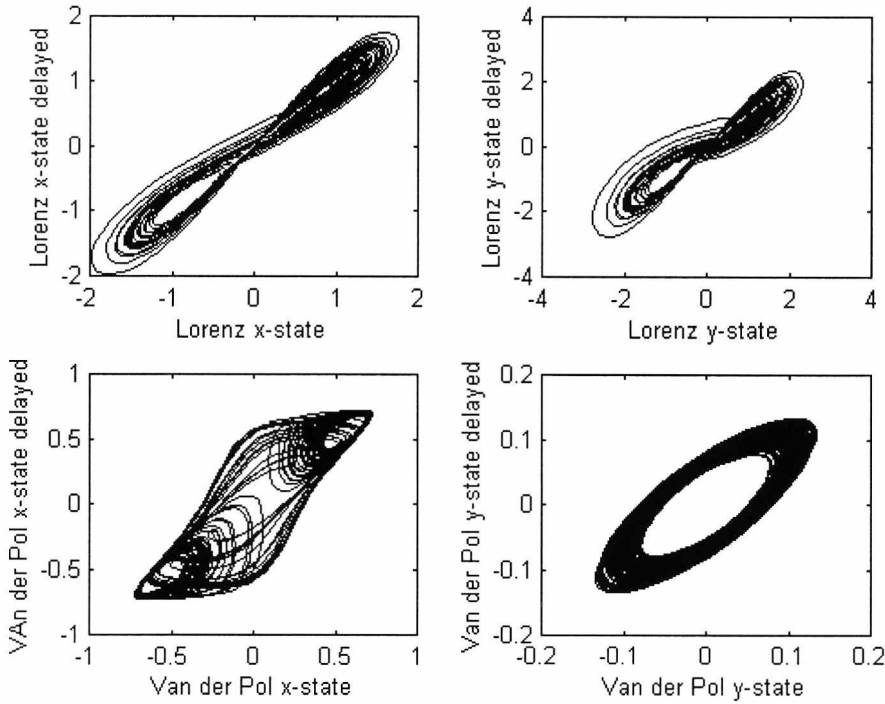


Fig. 6.2 Examples of the continuous time chaotic systems attractors.

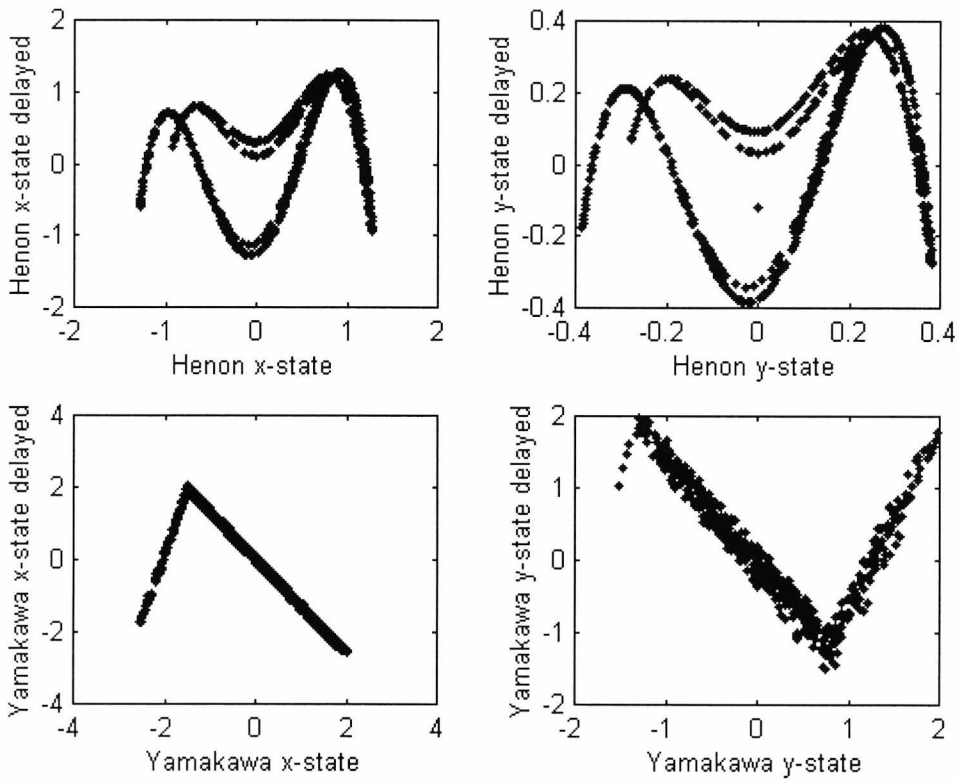


Fig. 6.3 Examples of discrete time chaotic systems attractors.

2. We apply the optimisation program (*E04JAF*) to the system under attack. For this program we assign initial values for the keys, the upper limits and the lower limits of the keys and the number of samples required for attacking the system. The *E04JAF* is used first to ensure that the chaotic system will be in the chaotic band because it is a bounded optimiser. The upper and lower boundaries are chosen such that the system remains chaotic, as we will discuss in section 6.3.2.
3. The resultant keys of the *E04JAF* are applied as initial guesses for the second program (*fminsreach*). This is used after the *E04JAF* program to minimise the error in the resultant keys of the *E04JAF*. Since in some cases, as will see later, we require keys with accuracy up to 10^{-13} .
4. The resultant output keys of the *fminsreach* program are the required keys.

The flow chart shown in Fig. 6.4 demonstrates the above steps.

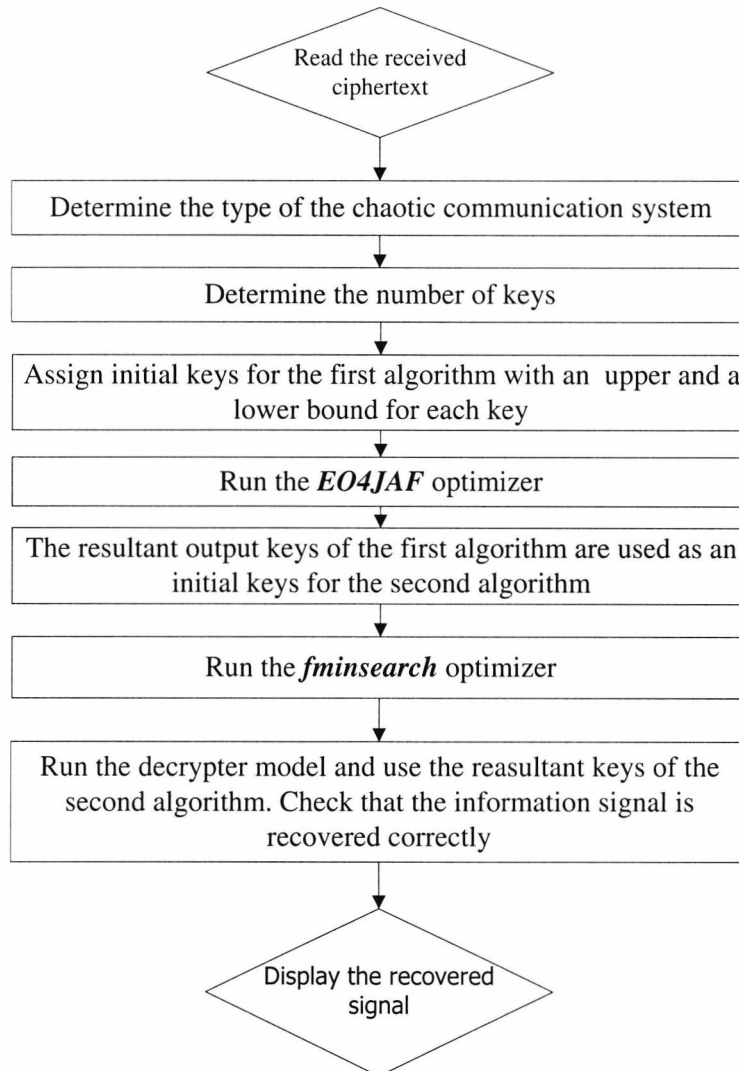


Fig. 6.4 The flow chart of the attacking algorithm.

6.3.2 Obtaining the upper and lower boundaries of the optimisation program

The upper and lower bounds of the chaotic system are chosen such that the system remains chaotic. These bounds are obtained by plotting the bifurcation diagram of the system under attack. We will give an example of the bifurcation diagram of the Lorenz system [17]. In this system we have three state variables and three parameters (a , b and c). We plot the bifurcation diagram of the state variable y as a

function of these three parameters. The bifurcation diagrams of the Lorenz system are shown in Figs 6.5, 6.6 and 6.7.

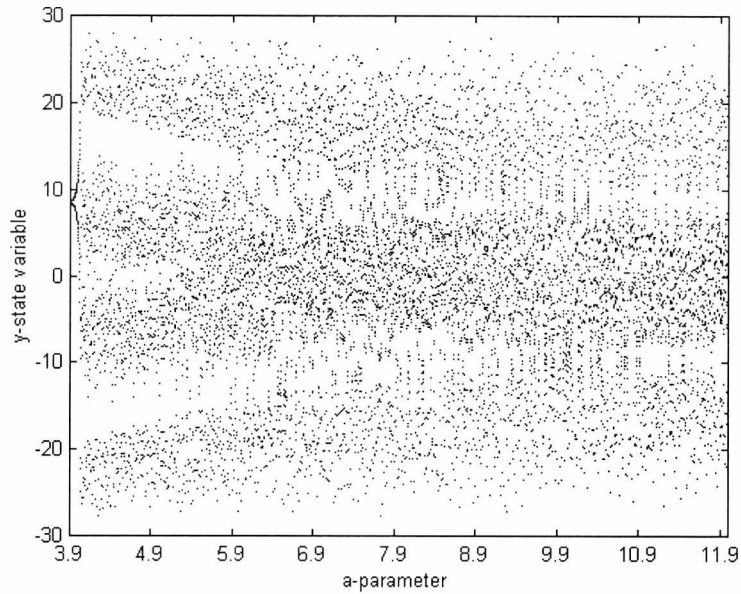


Fig. 6.5 Bifurcation diagram of the Lorenz system (a parameter and y state variable).

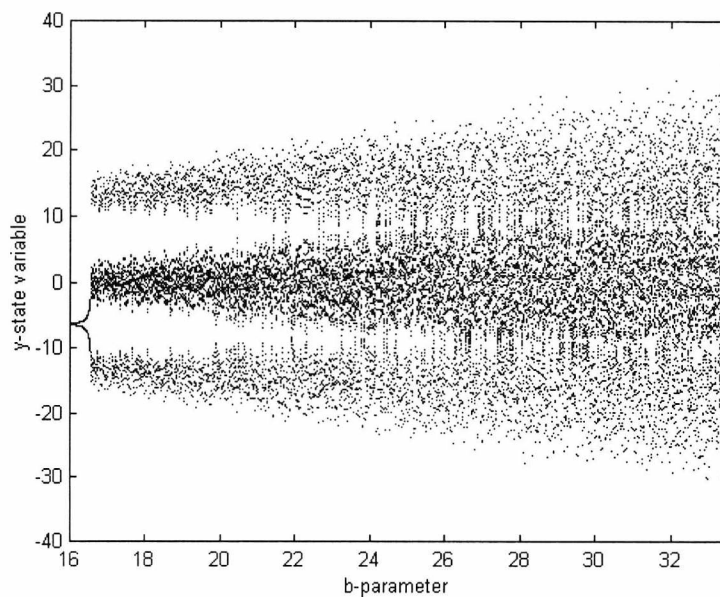


Fig. 6.6 Bifurcation diagram of the Lorenz system (b parameter and y state variable).

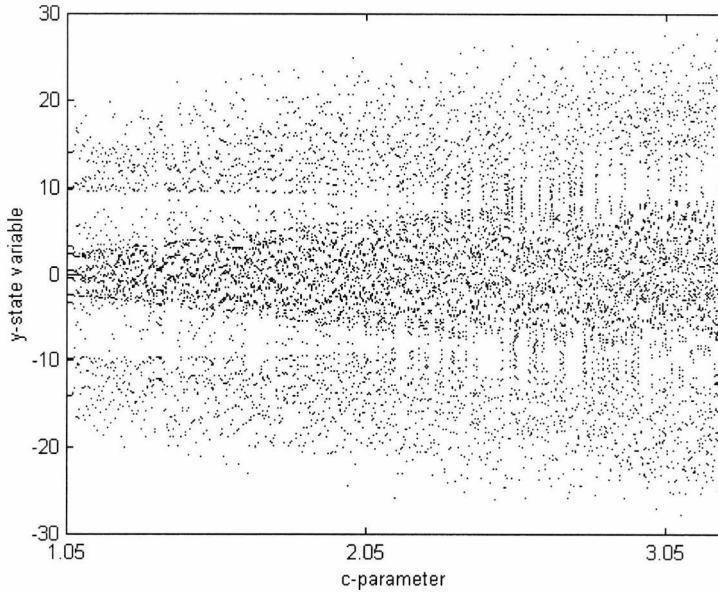


Fig. 6.7 Bifurcation diagram of the Lorenz system
(c parameter and y state variable).

We find that the system has chaotic behaviour if a lies in the range from 6 to 12. We choose the boundaries of a from 8 to 12. For the parameter b the system has chaos output if it lies in the range from 17 to 35. The boundaries of b are chosen from 25 to 35. For the parameter c the system has chaotic response if it lies in the range from 1.2 to 4. The boundaries of c are selected to be in the range from 2 to 4. To determine the ranges of the parameters accurately, the three parameters should be tested simultaneously. For the other system, the same procedures are used.

6.3.3 Attacking the Henon map

Stark *et al.* [11] have presented a method for extracting slowly varying signals from the Henon chaotic map. They succeeded in recovering the information signal with reasonable accuracy when the ratio of amplitudes of the chaotic signal to the information signal is as low as 10^{-10} . Using our algorithm, we succeed in the recovering the information signal when the ratio of amplitudes of the chaotic signal to the information signal is as low as 10^{-12} with an accuracy of 10^{-13} .

The state equations of the transmitter are given by

$$\begin{aligned} x_{n+1} &= 1 + y_n - ax_n^2 \\ y_{n+1} &= bx_n + s(t). \end{aligned} \tag{6.4}$$

$S(t)$...is the information signal.

The state equations of the receiver are

$$\begin{aligned} x'_{n+1} &= 1 + y'_n - ax_n'^2 \\ \hat{s}(t) &= y_{n+1} - bx'_n. \end{aligned} \tag{6.5}$$

The block diagram of the system is shown in Fig. 6.8.

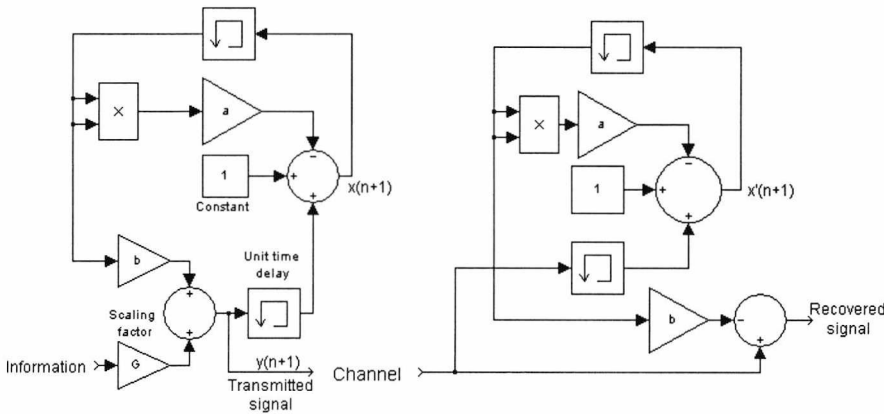


Fig. 6.8 Block diagram of the Henon chaotic communication system.

The attacker algorithm is used to find the exact values for a and b starting from initial values. The signal to chaos ratio, in this example, is -240 dB. The attacker initial key values, the range for each key, the number of points required for the attacker, the time of attack, the number of iterations taken in the attack and the resultant attacker keys are given in table 6.1. The attacker input and output signals are shown in Fig. 6.8. The figure indicates that with the attacker resultant values, the receiver succeeds to recover the information signal. The error between the normal output and the attacker output is around 10^{-13} . We give some explanations about the graphs.

- **Attacker input** is the input signal to the attacker (received signal).
- **Attacker initial output** is the attacker output at the initial guesses of the keys.
- **Normal output** is the decrypter output when we know the encrypter exact keys.

- **Attacker output** is the decrypter output using the attacker resultant keys.
- **Error signal** is the difference between the normal output and the attacker output.
- **Attacker key error** is a graph used to indicate the sensitivity of the system to the error in the attacker resultant keys.

Keys	Encrypter keys														Attacker resultant keys															
	a	1	.	3	9	9	8	7	6	5	4	3	1	1	5	2	1	.	3	9	9	8	7	6	5	4	3	1	1	5
b	0	.	2	9	9	8	7	6	7	9	0	5	6	4	3	0	.	2	9	9	8	7	6	7	9	0	5	6	4	5
Attacker initial values				Optimiser 1				Optimiser 2																						
a		b		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																			
1		0.1																												
Range				0	0.01	.05	6	0	0.01	0.03	4																			
0.5	2	0.05	1																											
Total time of attack		24.636 seconds		Total number of iterations				228																						

Table 6.1 Encrypter keys, attacker initial values and attacker resultant keys.

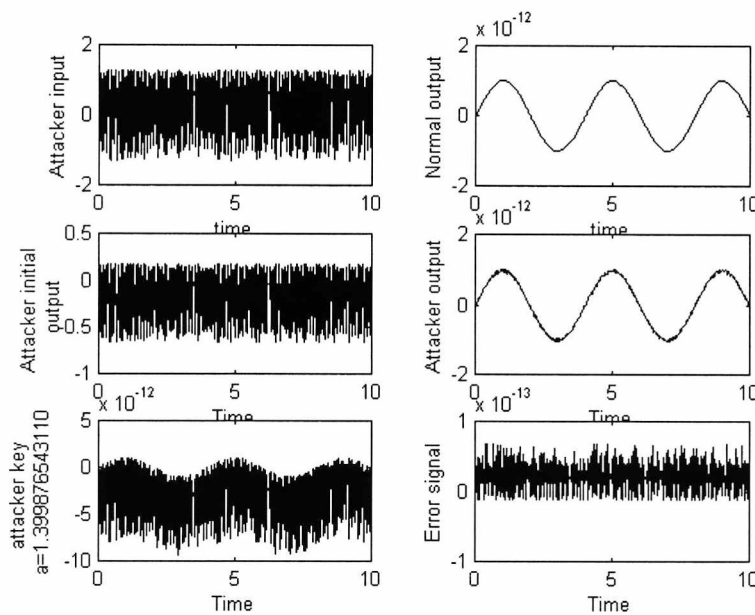


Fig. 6.9 Attacker results of the Henon map.

6.3.4 Attacking the Yamakawa chaotic communication system

Itoh *et al.* [18]-[19] have presented a chaotic communication system based Yamakawa's chaos chip. The chaos chip contains three basic units for constructing chaotic systems. Those are a nonlinear delay unit, a linear delay unit and a summing unit. The transmitter state equations are given by

$$\begin{aligned} x_{n+1} &= f(x_n) + \varepsilon s_n \\ y_{n+1} &= g(y_n) - \alpha z_n + \delta x_n \\ z_{n+1} &= y_n - \beta z_n \end{aligned} \quad (6.6)$$

where,

$$f(x) = \begin{cases} k_1(x - E_1) + k_2 E_1, & x < E_1 \\ k_2 x, & E_1 \leq x \leq E_2 \\ k_3(x - E_2) + k_2 E_2, & x \geq E_2 \end{cases} \quad (6.7)$$

k_1, k_2, k_3, E_1 and E_2 are constants.

y_{n+1} is the transmitted signal.

s_n is the information signal.

The function $g(x)$ has the same form of $f(x)$ but with another constants k_1, k_2, k_3, E_1 and E_2 .

The receiver state equations are given by

$$\begin{aligned} z'_{n+1} &= y_n - \beta z'_n \\ x'_n &= \frac{y_{n+1} - g(y_n) + \alpha z'_n}{\delta} \\ r_n &= \frac{x'_{n+1} - f(x'_n)}{\varepsilon} \end{aligned} \quad (6.8)$$

where r_n is the recovered signal.

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the number of iteration taken by the attacker and the attacker resultant keys are given in table 6.2. The attacker input and output signals are shown in Fig. 6.10. The figure shows that the attacker succeeds in attacking the system and recovering the information signal. The difference between the normal output and the attacker output is around 0.05.

Keys	Encrypter keys														Attacker resultant keys															
a	0	.	1	0	9	9	8	8	5	6	7	4	3	2	1	0	.	1	0	9	9	8	6	7	2	9	4	0	4	0
b	0	.	1	9	5	9	9	8	9	0	0	1	2	3	0	0	.	1	9	6	2	7	2	3	8	6	8	0	9	1
c	9	.	9	8	7	6	3	8	7	5	4	4	5	0	5	9	.	9	8	4	7	0	5	0	0	2	9	1	8	4
Attacker initial values			Optimiser 1				Optimiser 2																							
a	b	C	Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																				
0.085	0.1	8																												
Ranges			0	0.01	0.32	321	0	0.01	1.5	1501																				
0.075	0.2	0.1									0.2	8	12																	
Total time of attack		345.807 seconds	Total number of iterations				1219																							

Table 6.2 Encrypter keys, attacker initial values and attacker resultant keys

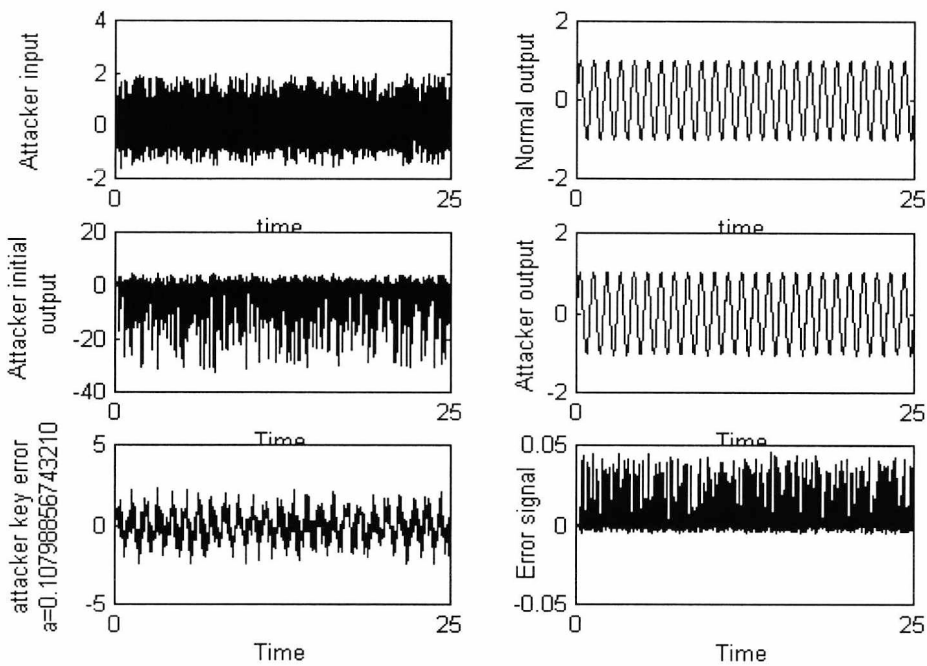


Fig. 6.10 Attacker results of Yamakawa’s chaotic communication system.

6.3.5 Attacking the Van Der Pol-Duffing chaotic communication system

Kocarev and Lakshmanan [20] have proposed a chaotic communication system based on Van Der Pol-Duffing chaotic generator. The system uses a chaotic signal to mask the information signal and a synchronous chaotic system in the receiver to identify the chaotic part of the signal, which is subtracted to reveal the information signal. The state equations of the transmitter are

$$\begin{aligned}\dot{x} &= -\nu[x^3 - ax - y] \\ \dot{y} &= x - y - z \\ \dot{z} &= \beta y.\end{aligned}\tag{6.9}$$

The transmitted signal $r(t)$ is equal to

$$r(t) = x(t) + s(t)\tag{6.10}$$

where $s(t)$ is the information signal.

The state equations of the receiver are

Response 1

$$\begin{aligned}\dot{y}' &= r(t) - y' - z' \\ \dot{z}' &= \beta y'\end{aligned}\tag{6.11}$$

Response 2

$$\dot{x}'' = -\nu[(x'')^3 - \alpha(x'') - y']\tag{6.12}$$

The information signal is recovered by

$$\tilde{s}(t) = r(t) - x''(t).\tag{6.13}$$

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.3. The attacker input and output signals are shown in Fig. 6.11. The figure shows that the attacker algorithm succeeds in attacking the Van Der Pol-Duffing chaotic communication system and the error between the normal output and the attacker output is 10^{-4} .

Keys	Encrypter keys														Attacker resultant keys															
	a	0	.	3	4	9	9	8	8	7	6	0	5	4	3	2	0	.	3	5	0	0	0	7	3	3	5	0	4	7
B	2	9	9	.	9	9	8	8	8	7	6	5	0	2	3	2	9	9	.	9	9	7	6	5	9	1	2	0	7	2
C	1	0	0	.	0	0	1	2	3	8	7	5	4	3	0	1	0	0	.	0	0	7	7	8	8	7	0	4	0	3
Attacker initial values			Optimiser 1				Optimiser 2																							
a	b	c	Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																				
0.32	290	85																												
Ranges			0	0.01	3	301	0	0.01	7.5	751																				
0.24	0.38	250									350	75	125																	
Total time of attack		292.16 second	Total number of iterations				1583																							

Table 6.3 Encrypter keys, attacker initial values and attacker resultant keys.

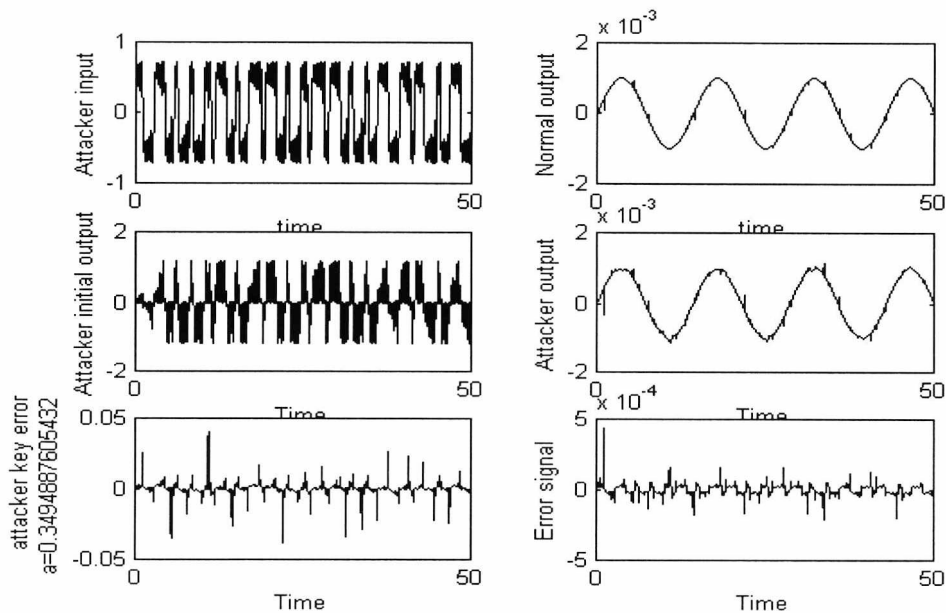


Fig. 6.11 Attacker results of the Van Der Pol-Duffing chaotic communication system.

6.3.6 Attacking the system based on the general approach for chaotic synchronisation

Kocarev and Parlitz presented a secure communication system based on the general synchronisation approach [[21]. The system uses the well-known Lorenz model. The state equations of the transmitter are given by

$$\begin{aligned}\dot{x}_1 &= -ax_1 + s(t) \\ \dot{x}_2 &= bx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - cx_3\end{aligned}\tag{6.14}$$

where a , b and c are constants and $s(t)$ is the transmitted signal and it is given by

$$s(t) = 10x_2 + ix_3\tag{6.15}$$

and i is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{y}_1 &= -ay_1 + s(t) \\ \dot{y}_2 &= by_1 - y_2 - y_1y_3 \\ \dot{y}_3 &= y_1y_2 - cy_3.\end{aligned}\tag{6.16}$$

The information signal is recovered by

$$i_R = (s(t) - 10y_2) / y_3.\tag{6.17}$$

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.4. The attacker input and output signals are shown in Fig. 6.12. The figure illustrates that the information signal is recovered with an error 10^{-5} compared to the normal output signal. As described in section 6.3.3, the normal output is the output of the decrypter when we know the encrypter keys exactly.

Keys	Encrypter keys														Attacker resultant keys															
	a	9	.	9	9	8	8	7	6	5	4	3	4	1	0	2	9	.	9	9	8	8	7	3	6	1	4	0	2	4
b	2	7	.	9	9	9	5	6	7	4	3	2	1	9	8	2	7	.	9	9	9	5	6	4	8	8	7	6	3	2
c	2	.	6	6	6	7	0	0	2	3	4	5	6	3	0	2	.	6	6	6	6	9	9	8	3	9	7	0	2	6
Attacker initial values						Optimiser 1				Optimiser 2																				
a		b		c		Start time	Step	Stop time	No. of points	Start time	Step size	Stop time	No. of point																	
8		26		2.1																										
Ranges						0	0.01	3	301	0	0.01	3	301																	
5	12	25	35	2	4																									
Total time of attack		222.617 seconds		Total number of iterations				1720																						

Table 6.4 Encrypter keys, attacker initial values and attacker resultant keys.

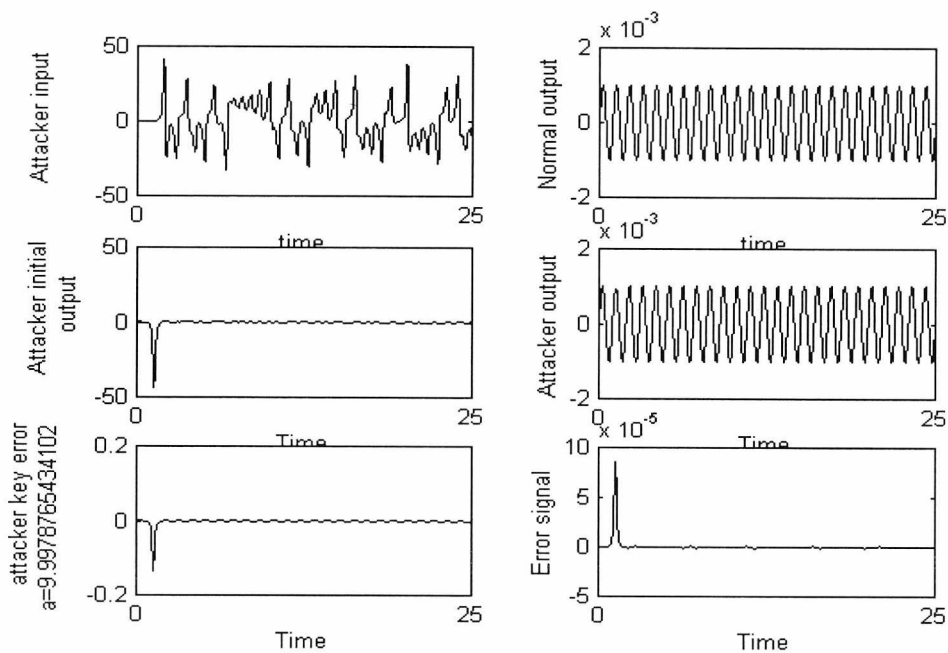


Fig. 6.12 Attacker results of the general approach for chaotic synchronisation.

6.3.7 Attacking the Chua masking chaotic communication system

Kocarev *et al.* [22] have experimentally demonstrated a secure communication system using Chua's circuit. In this method, the information is added at the output of the Chua generator at the transmitter and recovered at the receiver by subtracting the chaotic signal. The state equations of the transmitter are given by

$$\begin{aligned} C_1 \frac{dv_{C_1}}{dt} &= G(v_{C_2} - v_{C_1}) - g(v_{C_1}) \\ C_2 \frac{dv_{C_2}}{dt} &= G(v_{C_1} - v_{C_2}) + i_L \\ L \frac{di_L}{dt} &= -v_2 \end{aligned} \quad (6.18)$$

The transmitted signal $r(t)$ is given by

$$r(t) = v_{C_1} + s(t) \quad (6.19)$$

where $s(t)$ is the information signal.

The receiver is composed of two subsystems, the state equations of the first subsystem are given by

$$\begin{aligned} C_2 \frac{dv_{C_2}^{(1)}}{dt} &= G(r(t) - v_{C_2}^{(1)}) + i_L^{(1)} \\ L \frac{di_L^{(1)}}{dt} &= -(v_{C_2}^{(1)} + ri_L^{(1)}) \end{aligned} \quad (6.20)$$

The second subsystem is given by

$$C_1 \frac{dv_{C_1}^{(2)}}{dt} = \frac{1}{R} (v_{C_2}^{(1)} - v_{C_1}^{(2)}) - g(v_{C_1}^{(2)}) \quad (6.21)$$

The recovered information signal $s(t)$ is given by

$$s(t) = r(t) - v_{C_1}^{(2)}. \quad (6.22)$$

The initial key values for the attacker, the range of each key, the number of data samples required for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.5. The attacker input and output signals are shown in Fig. 6.13. The figure indicates that the input signal is recovered and the difference between the attacker output and the normal output of the system is around 0.1.

Keys	Encrypter keys																Attacker resultant keys															
	a	9	.	9	9	8	6	7	4	3	2	1	9	2	0	0	9	.	9	9	8	6	6	9	8	0	8	1	3	8	4	
b	0	.	6	4	9	9	7	8	6	5	4	3	2	0	1	0	.	6	5	0	3	1	0	3	6	7	2	5	6	5		
c	1	.	0	0	1	2	3	8	9	7	6	5	4	3	0	0	.	9	9	8	7	8	6	7	4	7	0	8	0	7		
d	5	.	5	9	9	8	7	6	9	8	7	6	5	4	0	5	.	6	0	5	2	3	7	3	1	0	0	0	2	2		
Attacker initial values				Optimiser 1				Optimiser 2																								
a	b	c	d	Start time	Step	Stop time	No. of points	Start time	Step	Stop time	NO. of points																					
8	0.5	0.7	4.5																													
Ranges				0	0.01	3.0	301	0	0.01	0.5	51																					
6	12	0.25	0.8									0.75	1.2	4	6																	
Total time of attack		332.829 seconds		Total number of iterations				1558																								

Table 6.5 Encrypter keys, attacker initial values and attacker resultant keys.

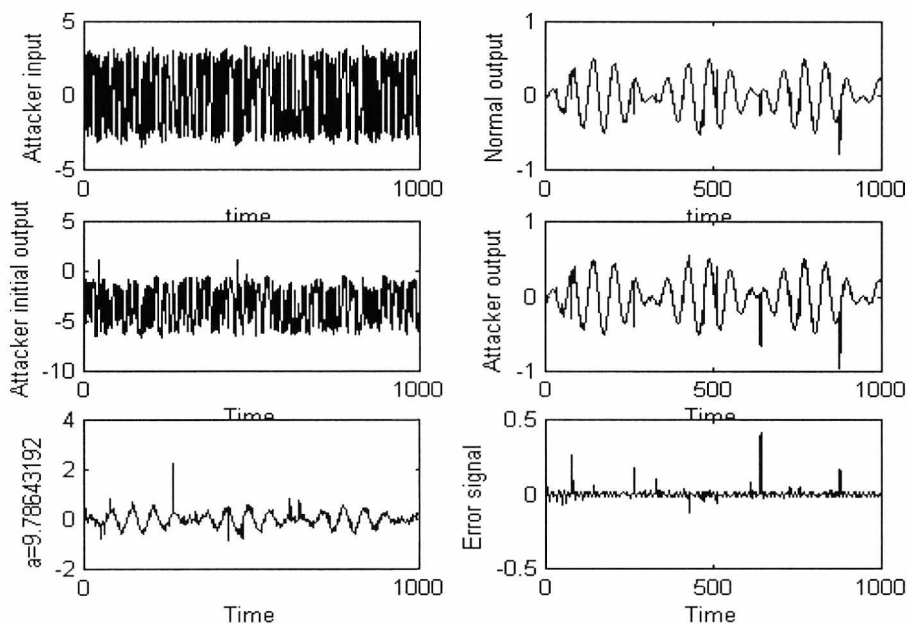


Fig. 6.13 Attacker results of the Chua masking chaotic communication system.

6.3.8 Attacking the Rössler encryption algorithm

The attacker algorithm attacks our developed Rössler encryption algorithm [23]. The details of the algorithm were presented in chapter 5 (section 5.4.1.2). The state equations of the transmitter are given by

$$\begin{aligned}\dot{x} &= -y - z \\ \dot{y} &= x + ay + s(t) \\ \dot{z} &= b + z(x - c)\end{aligned}\tag{6.23}$$

where a , b and c are constants and $s(t)$ is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{x}_r &= -y - z_r \\ \dot{z}_r &= b + z_r(x_r - c) \\ \tilde{S}(t) &= \dot{y} - x_r - ay\end{aligned}\tag{6.24}$$

where $\tilde{S}(t)$ is the recovered information signal.

In this case, the signal to chaos ratio is equal to -246 dB. The initial values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 7.6. The attacker input and output signals are illustrated in Fig. 6.14. The figure shows that with resultant attacker values, the information signal is completely recovered and that the difference between the normal output of the system and the attacker output is equal to zero.

Keys	Encrypter keys													Attacker resultant keys																
	a	0	.	3	9	8	0	1	7	8	4	5	3	2	1	3	0	.	3	9	8	0	1	7	8	4	5	3	2	1
b	1	.	9	9	7	8	6	5	3	4	2	1	8	7	6	1	.	9	9	7	8	6	5	3	4	2	1	8	7	6
c	4	.	0	1	5	6	7	4	3	2	3	1	7	6	2	4	.	0	1	5	6	7	4	3	2	3	1	7	6	2
Attacker initial values						Optimiser 1				Optimiser 2																				
a		b		c		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																	
0.1		0.1		1																										
Ranges						0	0.1	10	101	0	0.1	20	201																	
0.1	0.5	0.1	3	0.1	5																									
Total time of attack			166.44 seconds			Total number of iterations				1424																				

Table 6.6 Encrypter keys, attacker initial values and attacker resultant keys.

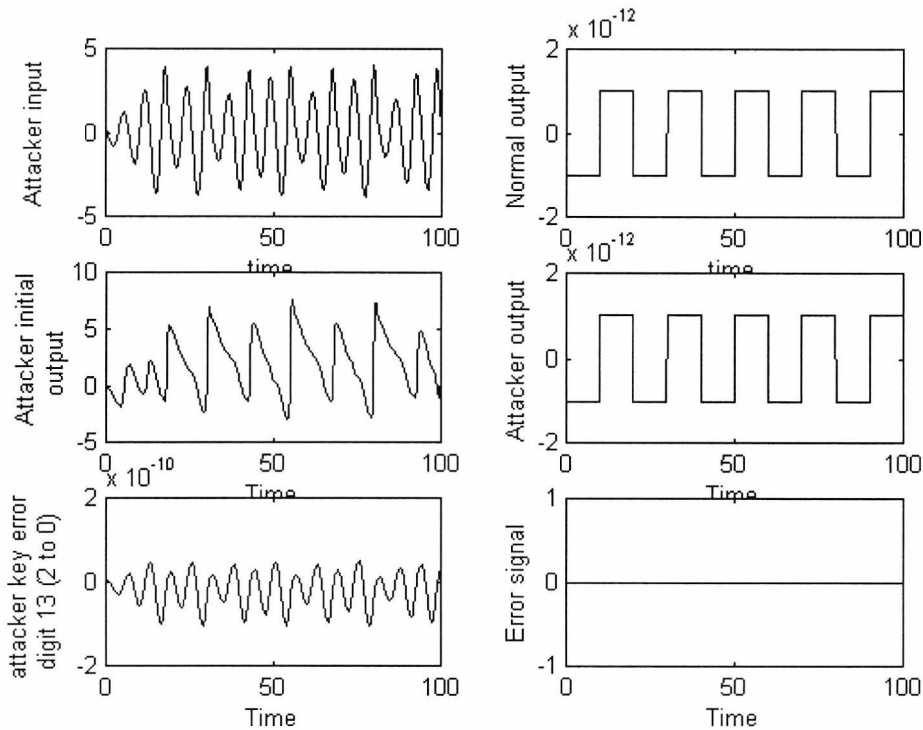


Fig. 6.14 Attacker results of the Rössler encryption system.

6.3.9 Attacking the Lorenz encryption algorithm

The attacker algorithm also attacks our developed Lorenz encryption algorithm [23]. The details of the algorithm were given in chapter 5 (section 5.4.1.3). The state equations of the transmitter are given by

$$\begin{aligned}\dot{x} &= a(y - x) \\ \dot{y} &= bx - y - xz + s(t) \\ \dot{z} &= xy - cz\end{aligned}\tag{6.25}$$

where a , b and c are constants and $s(t)$ is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{x}_r &= a(y - x_r) \\ \dot{z}_r &= x_r y - cz_r \\ \tilde{s}(t) &= \dot{y} - bx + y - xz\end{aligned}\tag{6.26}$$

where $\tilde{S}(t)$ is the recovered signal.

The signal to chaos ratio is equal to -257 dB. The initial key values of the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.7. The attacker output signals are illustrated in Fig. 6.15. The figure illustrates that the attacker recovered the information signal and that the difference between the normal output and the attacker output is equal to 10^{-13} .

Keys	Encrypter keys													Attacker resultant keys																
	a	9	.	9	8	6	7	9	5	4	3	2	1	0	1	2	9	.	9	8	6	7	9	5	4	3	2	1	0	1
b	2	8	.	0	0	2	5	4	7	8	9	6	5	4	2	2	8	.	0	0	2	5	4	7	8	9	6	5	4	3
c	2	.	6	6	6	6	9	0	9	1	2	3	4	5	6	2	.	6	6	6	6	9	0	9	1	2	3	4	5	6
Attacker initial values						Optimiser 1				Optimiser 2																				
a		b		c		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																	
9		25		2																										
Ranges						0	0.1	10	101	0	0.1	10	101																	
8	12	25	35	2	4																									
Total time of attack			123.478 seconds			Total number of iterations				1574																				

Table 6.7 Encrypter keys, attacker initial values and attacker resultant keys.

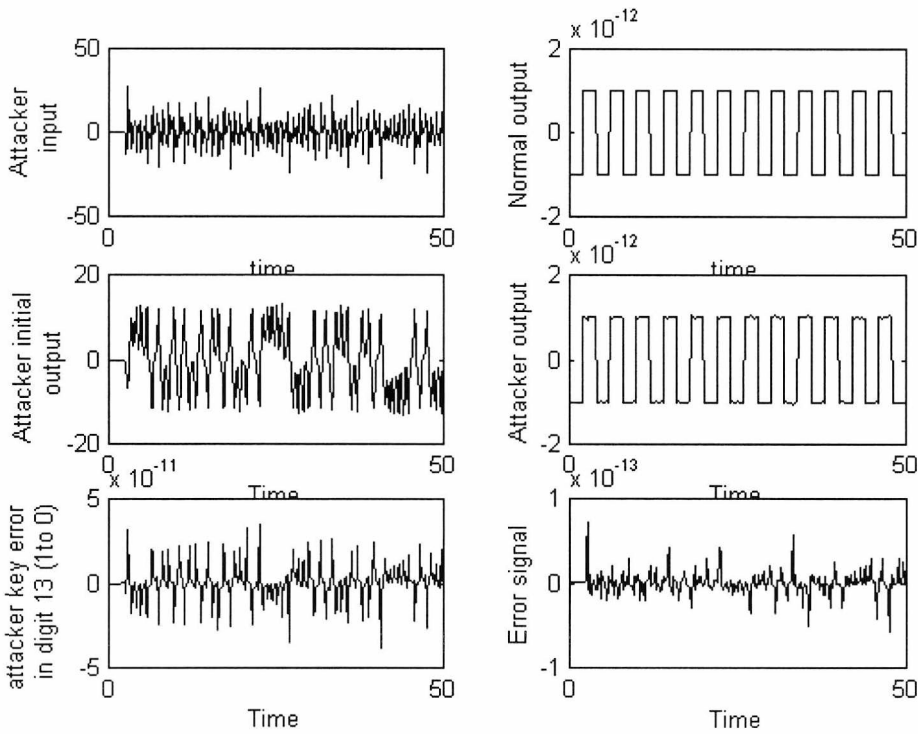


Fig. 6.15 Attacker results of the Lorenz encryption system.

The above results show that the new attacker algorithm breaks the chaotic communication systems under attack and the information signal is recovered. As a result, the above systems are not secure and we should improve their security. In chapter 7, we will give some methods to counter that attacker and improve the security of the chaotic communication systems and counter the attack algorithm.

6.4 Conclusion

A new algorithm for attacking the chaotic communication system is introduced. The algorithm is based on two optimisation programs of the MATLAB. The algorithm is tested on different chaotic communication systems (continuous and discrete time systems). It is tested on systems based on chaos masking or chaos modulating. The algorithm also attacks the new encryption algorithms introduced in chapter 5. The algorithm succeeds in attacking all the chaotic systems under test and finds their keys. The information signal is recovered even at signal to chaos ratios in the order of -240 dB.

6.5 References

- [1] B. Schneier, *Applied cryptography*: Jhon Wiley & Sons, Inc, 1996.
- [2] L. R. Knudsen, "Block cipher-Analysis, design, applications," *Ph.D. dissertation*, Aarrhus University, Nov. 1994.
- [3] A. M. Fraser, "Reconstructing attractors from scalar time series-A comparison of singular system and redundancy criteria," *Physica D*, vol. 34, pp. 391-404, 1989.
- [4] A. I. Mess, "Reconstructing nonlinear systems," *IEEE Int. Symposium. on Circuit and System (ISCAS 96)*, pp. 1-4, 1996.
- [5] M. Casdagli, "Nonlinear prediction of chaotic time series," *Phys. D*, vol. 35, pp. 335-356, 1989.
- [6] L. A. Aguirre and S. A. Billings, "Retrieving dynamical invariants from chaotic data using NARMAX models," *Int. J. Bifurcation and Chaos*, vol. 5, No. 2, pp. 449-474, 1995.
- [7] H. D. I. Abarbanel, R. Brown and J. B. Kadtko, "Predication in chaotic nonlinear systems: Methods for time series with broadband Fourier spectra," *Phys. Rev A*, vol 41, pp. 1782-1807, 1990.
- [8] M. Casdagli, S. Eubank, J. D. Farmer and J. Gibson, "State space reconstruction in the presence of noise," *Phys. D*, vol. 51, pp.52-98. 1991.
- [9] U. Parlitz, R. Zöllner, J. Holzfuss and W. Lauterborn, "Reconstructing physical variables and parameters from dynamical systems," *Int. J. Bifurcation and Chaos*, vol. 4, No. 6, pp. 1715-1719, 1996.
- [10] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos*, vol. 4, No. 4, pp. 959-977, 1994.
- [11] J. Stark and B. V. Arumugam, "Extracting slowly varying signals from a chaotic background," *Int. J. Bifurcation and Chaos*, vol. 2, No.2, pp. 413-419, 1992.
- [12] T. Yang, L. B. Yang and C. M. Yang, "Breaking chaotic switching using generalised synchronisation: examples," *IEEE Trans. Circuits Syst. I*, vol. CAS-45, No. 10, Oct. 1998.

-
- [13] L. Kocarev and U. Parlitz, "Generalized synchronisation, predictability and equivalence of unidirectionally coupled dynamical systems," *Phys. Rev. Lett.*, vol. 76, No. 11, pp. 1816-1819, Mar. 1996.
- [14] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring and H. D. I. Abarbanel, "Generalised synchronisation of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp. 980-994, 1995.
- [15] E. Pärt-Enander and A. Sjöberg, *The MATLAB 5 handbook*: Published by Addison Wesley Longman Limited, 1999.
- [16] J. C. Lagarias, J. A. Reeds, M. H. Wright and P. E. Wright, "Convergence properties of the Nelder-Mead Simplex algorithm in low dimension," *SIAM J. Optimisation*, May 1997.
- [17] M. I. Sobhy and A. R. Shehata, "Secure e-mail and databases using chaotic algorithms," *Electron. Lett.*, vol. 36, No. 10, May 2000.
- [18] M. Itoh, H. Murakami and L. O. Chua, "Secure communication via Yamakawa's chaotic chips and Chua's circuits," *IEEE Int. Symposium. on Circuit and System (ISCAS 94)*, pp. 1293-1296, 1994.
- [19] M. Itoh and H. Murakami, "New communication systems via chaotic synchronisations and modulations," *IEICE Trans. Fundamentals*, vol. E78-A, No. 3, Mar. 1995.
- [20] K. Murali and M. Lakshmanan, "Transmission of signals by synchronisation in a chaotic Van Der Pol-Duffing oscillator," *Phys. Rev. E*, vol. 48, No. 3, pp. R1624-R1626, 1993.
- [21] L. Kocarev and U. Parlitz, "General approach for chaotic synchronisation with applications to communications," *Phys. Rev. Lett.*, vol. 74, No. 25, pp. 5028-5031, June 1995.
- [22] Lj. Kocarev, K. S. Halle, K. Eckert, U. Parlitz and L. O. Chua, "Experimental demonstration of secure communications via chaos synchronisation," *Int. J. Bifurcation and Chaos*, vol. 3, No. 2, pp. 469-477, 1993.
- [23] M. I. Sobhy and A. R. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurcation and Chaos*, will be published in Nov. 2000.

Chapter 6

ATTACKING CHAOTIC ENCRYPTION SYSTEMS

6.1 Introduction

The whole point of cryptography is to keep the plaintext (or the key or both) secret from eavesdroppers. Eavesdroppers are assumed to have complete access to the communications between the sender and the receiver. **Cryptanalysis** is the science of recovering the plaintext of a message without access to the key. Successful cryptanalysis may recover the plaintext or the key. It may also find weaknesses in a cryptosystem that eventually lead to recover the plaintext or the key. An attempted cryptanalysis is called an **attack**. There are four general types of attacks. Of course, each of them assumes that the cryptanalyst has complete knowledge of the encryption algorithm used [1]:

1. **Ciphertext-only attack.** The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The cryptanalyst's job is to recover the plaintext of as many messages as possible or deduce the key (or keys) used to encrypt the messages in order to decrypt other messages encrypted with the same keys.
2. **Known-plaintext attack.** The cryptanalyst has access not only to the ciphertext of several messages but also to the plaintext of those messages. The job of the cryptanalyst is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).
3. **Chosen-plaintext attack.** The cryptanalyst has access not only to the ciphertext and associated plaintext for several messages but has also chosen the plaintext that gets encrypted. This is more powerful than the known-plaintext attack because the cryptanalyst can choose specific plaintext blocks to encrypt what might yield more information about the key. His job is to deduce the key (or

keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).

4. **Adaptive-chosen-plaintext attack.** This is a special case of a chosen plaintext attack. Not only can the cryptanalyst choose the plaintext that is encrypted but he can also modify his choice based on the results of previous encryption. In a chosen-plaintext attack a cryptanalyst might just be able to choose one large block of plaintext to be encrypted. In an adaptive chosen-plaintext attack, he can choose a smaller block of plaintext and then choose another based on the results of the first and so forth.

Different algorithms offer different degrees of security depending on how hard they are to break. If the cost required to break an algorithm is greater than the value of the encrypted data then the algorithm is probably safe. If the time required to break the algorithm is longer than the time that the encrypted data must remain secret then the algorithm is probably safe. If the amount of the data encrypted by a single key is less than the amount of data necessary to break the algorithm then the algorithm is probably safe. We say probably because there is always a chance of new breakthroughs in cryptanalysis. On the other hand, the value of most data decreases over time. It is important that the value of the data always remains less than the cost of breaking the security protecting it. An algorithm is said to be **unconditionally secure** if no matter how much ciphertext is available, the cryptanalyst has not enough information to recover the plaintext. An algorithm is said to be **computationally secure** if it cannot be broken with available resources either current or future resources. The complexity of an attack can be measured in different ways:

1. **Data complexity** is the amount of data needed as input to the attack.
2. **Processing complexity** is the amount of processing needed to perform the attack. This is often called the work factor.
3. **Storage requirements** are the amount of memory needed to perform the attack.

As a rule, the complexity of an attack is taken to be the minimum of these three factors.

Lars Knudsen [2] classified the categories of breaking an algorithm as follows:

- **Total break**

The cryptanalyst finds the key.

- **Global deduction**

The cryptanalyst finds an alternate algorithm equivalent to the decryption algorithm without knowing the key

- **Local deduction**

A cryptanalyst finds the plaintext of an intercepted ciphertext.

- **Information deduction**

A cryptanalyst gains some information about the key or plaintext. This information could be a few bits of the key or some information about the form of the plaintext.

Section 6.2 gives some methods of attack of the chaotic communication system. A new algorithm for attacking the chaotic communication systems is introduced in section 6.3. Section 6.4 demonstrates the methods of counter attack of the chaotic communication system. The conclusion and the references of the chapter are in sections 6.5 and 6.6 respectively.

6.2 Chaos attacking background

Many algorithms have been developed to attack the chaotic communication systems [3]-[9]. Short [10] tests the level of security in secure communication systems based on nonlinear dynamics (NLD) or chaos. In these systems, a chaotic carrier is used in a type of spread-spectrum signal with the information signal buried at -30 dB with respect to the chaotic carrier. The analysis process was to use the NLD forecasting to predict the carrier dynamics and then subtract the predicted values to reveal the hidden information signal or at least increase its signal to noise ratio with respect to the carrier. In each case, it was a simple task to determine the power spectrum of the hidden signal once the prediction of the carrier was made. The forecasting approach was extended to allow estimation of the dynamics of the signal using threshold detection so that whenever a signal was detected, multiple predictions of the carrier

behaviour were made. This method was tested on a square wave embedded at -42 dB in a Lorenz carrier. The method was able to reveal the square wave with almost perfect precision except in a few regions where it temporarily lost synchronisation with the carrier.

Stark *et al* [11] consider the problem of extracting a small signal embedded in a stronger background. The desired signal is assumed to be a relatively slowly varying signal. Jaroslav *et al* are able to devise an algorithm, which in simple tests, can recover the signal to a reasonable accuracy when the ratio of amplitudes of signal to chaos background is as low as 10^{-10} . The algorithm essentially takes a time series $\{u_n\}$, which is the sum of a deterministic component $\{x_n\}$ and some other signal $\{S_n\}$ and attempts to separate the two parts. The signal $\{x_n\}$ is usually treated as the desired signal and $\{S_n\}$ as the unwanted noise. Separation is then equivalent to removing the noise component $\{S_n\}$.

Yang *et al* [12] introduce a method for breaking the chaotic switching where the binary message signal is scrambled by two chaotic attractors. In this method the breaking of the chaotic switching is presented using the concept of generalised synchronisation [13]-[14]. They assume that they have no precise knowledge about the chaotic transmitter. They also assume that the receiver system will never synchronise to the unknown chaotic transmitter because there are some significant differences both in structure and in parameters between the chaotic transmitter and the receiver. Yang *et al* get a decoding result as good as that provided by the receiver with the same parameters as those of the transmitter.

As a conclusion, all the above methods, except the breaking of the chaotic switching, assume that the information signal is added to the chaotic signal and they try to separate the information signal from the chaotic signal. This is a special case of the chaotic communication system. The secure communication systems based on hiding the information on chaotic carriers may be useful to increase privacy but are not yet capable of providing a high level of security.

In this chapter, we introduce a new algorithm for attacking the chaotic communication system (continuous or discrete). This algorithm is suitable either when the information signal is added to the chaotic carrier or it is used to modulate

one of the state variables of the chaotic system at signal to chaos ratios of the order of -240 dB.

6.3 New algorithm for attacking the chaotic communication systems

6.3.1 Introduction

A new algorithm for attacking the chaotic communication systems is introduced. It is based on two of the MATLAB optimisation programs [15]. The optimisation finds the optimal solution of a certain problem by finding the maximum or the minimum of a function in an interval, with or without constraints.

Suppose that we want to find a minimum x_{\min} of the function f in an interval.

$$f(x_{\min}) = \min_x f(x). \quad (6.1)$$

An iterative method needs an initial guess x_0 . From this value x_0 , we find a new value x_i which, it is hoped, is closer to x_{\min} . How the better approximation x_i is found, depends on the numerical method used. These iterations continue until an approximation x_i with enough accuracy is found such that $|x_{\min} - x_i|$ is smaller than the required error. If there are several local minima, the optimiser will find one of them. In this work, two optimisation programs are used namely *E04JAF* and *fminsearch*. The *E04JAF* is a simple bounded optimisation program and is used to find the minimum of a function of several variables.

The instruction for this program is

$$[x, f(x)] = \text{E04JAF}(x_0, x_1, x_2) \quad (6.2)$$

where x_0 is a vector of the unknown values and is the initial guess, x_1 is a vector of the lower limits of the unknown variables and x_2 is the upper limit. The user must supply a subroutine (target function) *funct1* to calculate the value of $f(x)$ for any given value of x .

The *fminsearch* program is used to find the minimum of a scalar function of several variables starting with an initial estimate. It is generally referred to as unconstrained nonlinear optimisation. It uses the simplex search method [16] and it has the form

$$[x] = \text{fminsearch}(\text{fun}, x_0, \text{options}). \quad (6.3)$$

It returns a vector x that is a local minimiser of the function fun . The vector x_0 contains the initial guesses for the optimiser. The options, for this function, include the maximum number of iterations, allowed termination tolerance of the function value and termination tolerance for x .

In this method of attack, we assume that the dynamics of the system are known but we have no information about the transmitter parameters (encrypter keys) used to encrypt the information. We assume that the receiver output signal (wanted signal) is an error signal of the optimisation algorithm and the algorithm is used to minimise that error. If the error is minimum, then the information signal is recovered. The steps of attacking the chaotic communication systems are summarised as follows:

1. We determine the type of the chaotic communication system under attack from the received ciphertext signal by plotting the attractor of the received data signal. Usually the attractor is a phase-plane of two state variables. However, in this case we have for the transmitted ciphertext only one state variable. To obtain an attractor, we plot the received data samples against the received delayed data samples. For example, if we have 1000 data samples, we plot the data samples from (1:990) against the data samples from (11:1000). These attractors are used as signatures for the chaotic systems. From these signatures, we can determine the type of the system under attack as shown in Figs. 6.1, 6.2 and 6.3.

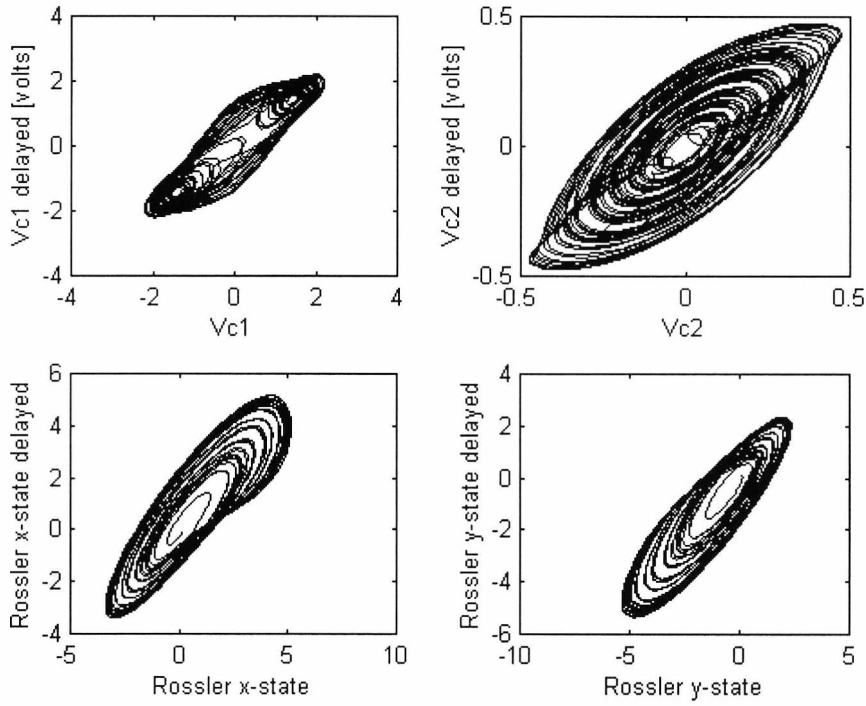


Fig. 6.1 Examples of the continuous time chaotic systems attractors (the upper traces are for Chua and the lower for Rössler systems).

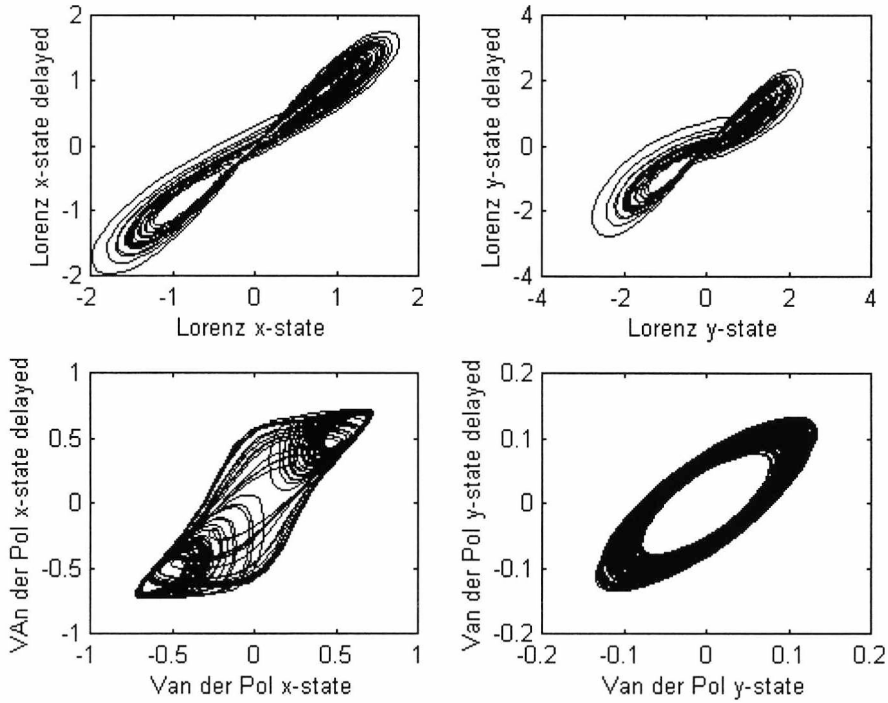


Fig. 6.2 Examples of the continuous time chaotic systems attractors.

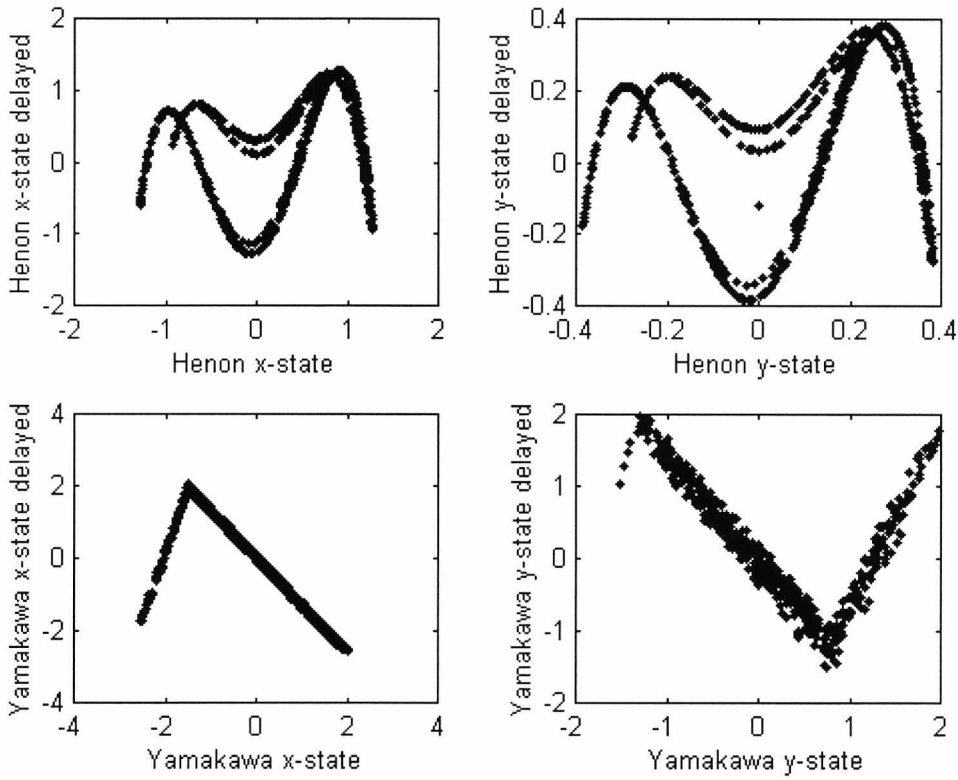


Fig. 6.3 Examples of discrete time chaotic systems attractors.

2. We apply the optimisation program (*E04JAF*) to the system under attack. For this program we assign initial values for the keys, the upper limits and the lower limits of the keys and the number of samples required for attacking the system. The *E04JAF* is used first to ensure that the chaotic system will be in the chaotic band because it is a bounded optimiser. The upper and lower boundaries are chosen such that the system remains chaotic, as we will discuss in section 6.3.2.
3. The resultant keys of the *E04JAF* are applied as initial guesses for the second program (*fminsreach*). This is used after the *E04JAF* program to minimise the error in the resultant keys of the *E04JAF*. Since in some cases, as will see later, we require keys with accuracy up to 10^{-13} .
4. The resultant output keys of the *fminsreach* program are the required keys.

The flow chart shown in Fig. 6.4 demonstrates the above steps.

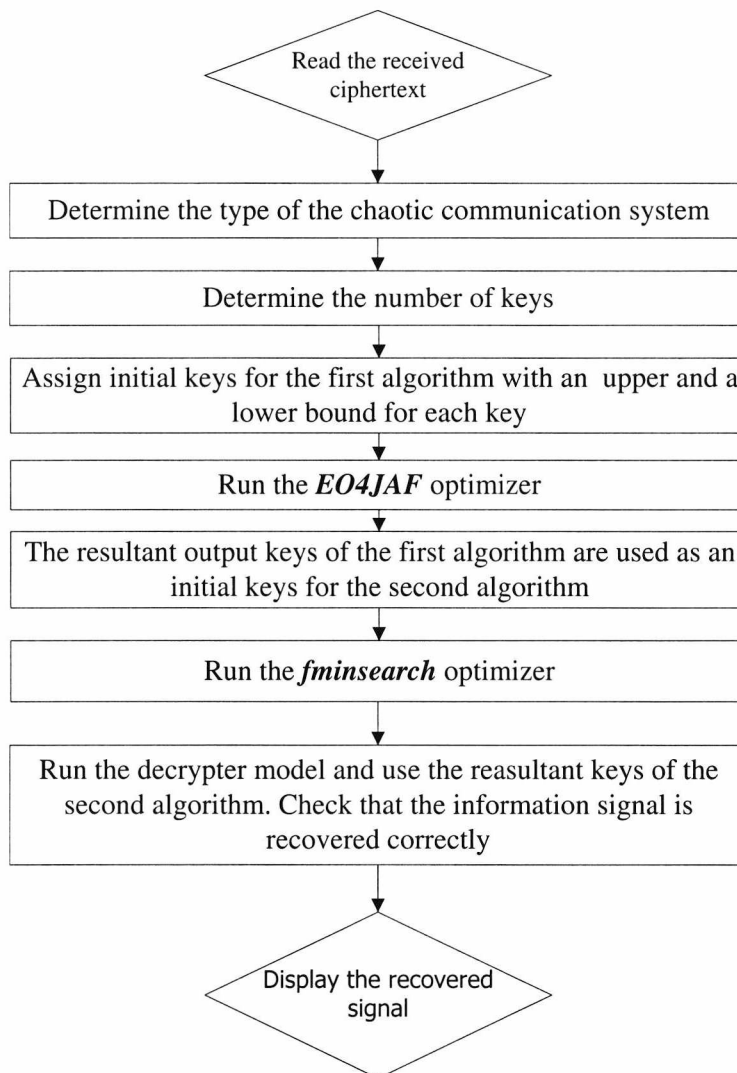


Fig. 6.4 The flow chart of the attacking algorithm.

6.3.2 Obtaining the upper and lower boundaries of the optimisation program

The upper and lower bounds of the chaotic system are chosen such that the system remains chaotic. These bounds are obtained by plotting the bifurcation diagram of the system under attack. We will give an example of the bifurcation diagram of the Lorenz system [17]. In this system we have three state variables and three parameters (a , b and c). We plot the bifurcation diagram of the state variable y as a

function of these three parameters. The bifurcation diagrams of the Lorenz system are shown in Figs 6.5, 6.6 and 6.7.

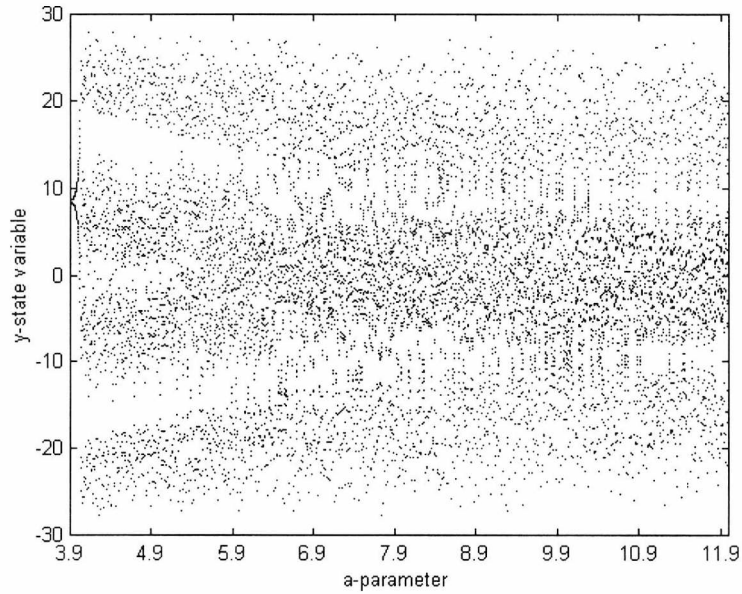


Fig. 6.5 Bifurcation diagram of the Lorenz system (a parameter and y state variable).

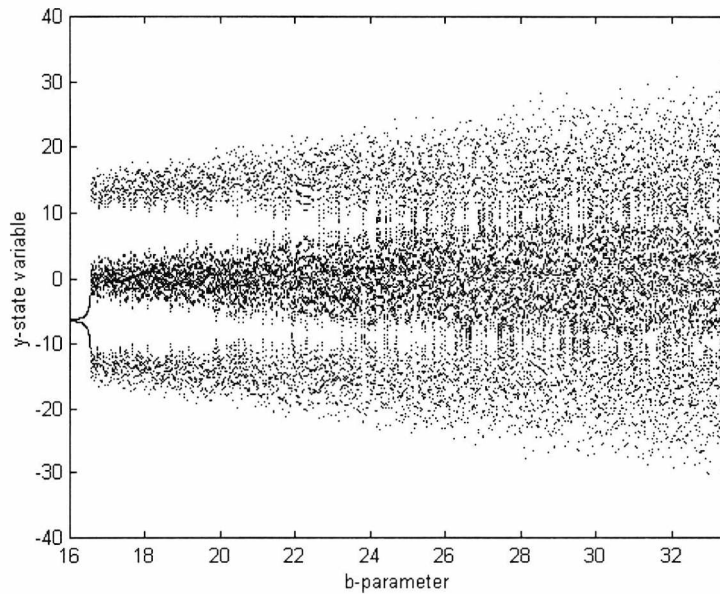


Fig. 6.6 Bifurcation diagram of the Lorenz system (b parameter and y state variable).

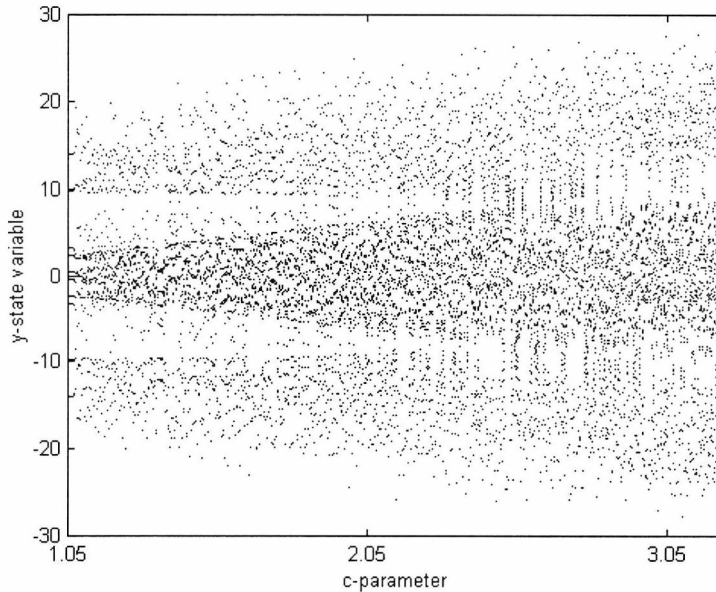


Fig. 6.7 Bifurcation diagram of the Lorenz system
(c parameter and y state variable).

We find that the system has chaotic behaviour if a lies in the range from 6 to 12. We choose the boundaries of a from 8 to 12. For the parameter b the system has chaos output if it lies in the range from 17 to 35. The boundaries of b are chosen from 25 to 35. For the parameter c the system has chaotic response if it lies in the range from 1.2 to 4. The boundaries of c are selected to be in the range from 2 to 4. To determine the ranges of the parameters accurately, the three parameters should be tested simultaneously. For the other system, the same procedures are used.

6.3.3 Attacking the Henon map

Stark *et al.* [11] have presented a method for extracting slowly varying signals from the Henon chaotic map. They succeeded in recovering the information signal with reasonable accuracy when the ratio of amplitudes of the chaotic signal to the information signal is as low as 10^{-10} . Using our algorithm, we succeed in the recovering the information signal when the ratio of amplitudes of the chaotic signal to the information signal is as low as 10^{-12} with an accuracy of 10^{-13} .

The state equations of the transmitter are given by

$$\begin{aligned}x_{n+1} &= 1 + y_n - ax_n^2 \\y_{n+1} &= bx_n + s(t).\end{aligned}\quad (6.4)$$

$S(t)$...is the information signal.

The state equations of the receiver are

$$\begin{aligned}x'_{n+1} &= 1 + y'_n - ax_n'^2 \\ \hat{s}(t) &= y_{n+1} - bx'_n.\end{aligned}\quad (6.5)$$

The block diagram of the system is shown in Fig. 6.8.

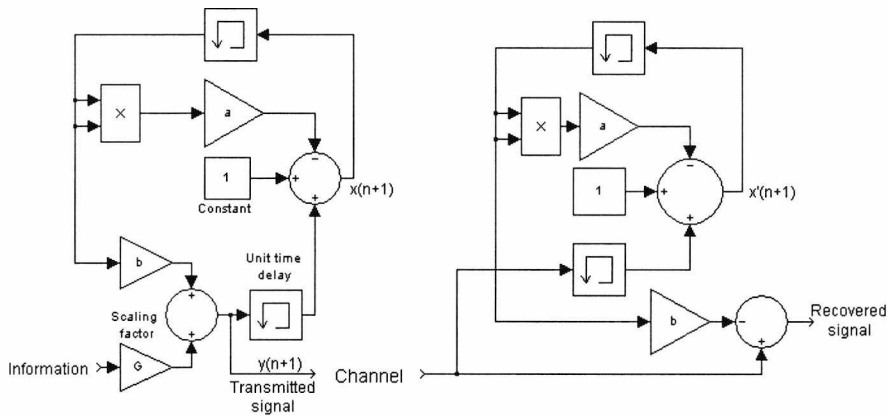


Fig. 6.8 Block diagram of the Henon chaotic communication system.

The attacker algorithm is used to find the exact values for a and b starting from initial values. The signal to chaos ratio, in this example, is -240 dB. The attacker initial key values, the range for each key, the number of points required for the attacker, the time of attack, the number of iterations taken in the attack and the resultant attacker keys are given in table 6.1. The attacker input and output signals are shown in Fig. 6.8. The figure indicates that with the attacker resultant values, the receiver succeeds to recover the information signal. The error between the normal output and the attacker output is around 10^{-13} . We give some explanations about the graphs.

- **Attacker input** is the input signal to the attacker (received signal).
- **Attacker initial output** is the attacker output at the initial guesses of the keys.
- **Normal output** is the decrypter output when we know the encrypter exact keys.

- **Attacker output** is the decrypter output using the attacker resultant keys.
- **Error signal** is the difference between the normal output and the attacker output.
- **Attacker key error** is a graph used to indicate the sensitivity of the system to the error in the attacker resultant keys.

Keys	Encrypter keys																Attacker resultant keys															
	a	1	.	3	9	9	8	7	6	5	4	3	1	1	5	2	1	.	3	9	9	8	7	6	5	4	3	1	1	5	1	
b	0	.	2	9	9	8	7	6	7	9	0	5	6	4	3	0	.	2	9	9	8	7	6	7	9	0	5	6	4	5		
Attacker initial values				Optimiser 1				Optimiser 2																								
a		b		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																					
1		0.1																														
Range				0	0.01	.05	6	0	0.01	0.03	4																					
0.5	2	0.05	1																													
Total time of attack		24.636 seconds		Total number of iterations				228																								

Table 6.1 Encrypter keys, attacker initial values and attacker resultant keys.

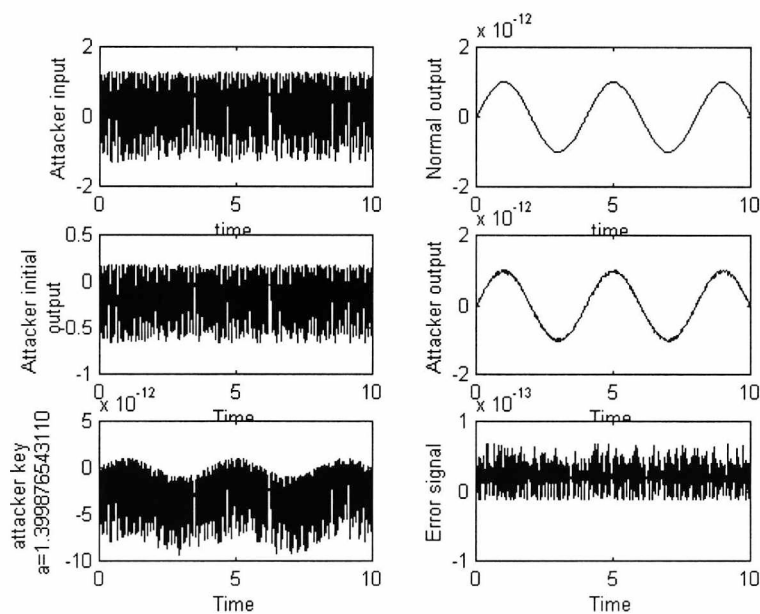


Fig. 6.9 Attacker results of the Henon map.

6.3.4 Attacking the Yamakawa chaotic communication system

Itoh *et al.* [18]-[19] have presented a chaotic communication system based Yamakawa's chaos chip. The chaos chip contains three basic units for constructing chaotic systems. Those are a nonlinear delay unit, a linear delay unit and a summing unit. The transmitter state equations are given by

$$\begin{aligned} x_{n+1} &= f(x_n) + \varepsilon s_n \\ y_{n+1} &= g(y_n) - \alpha z_n + \delta x_n \\ z_{n+1} &= y_n - \beta z_n \end{aligned} \quad (6.6)$$

where,

$$f(x) = \begin{cases} k_1(x - E_1) + k_2 E_1, & x < E_1 \\ k_2 x, & E_1 \leq x \leq E_2 \\ k_3(x - E_2) + k_2 E_2, & x \geq E_2 \end{cases} \quad (6.7)$$

k_1, k_2, k_3, E_1 and E_2 are constants.

y_{n+1} is the transmitted signal.

s_n is the information signal.

The function $g(x)$ has the same form of $f(x)$ but with another constants k_1, k_2, k_3, E_1 and E_2 .

The receiver state equations are given by

$$\begin{aligned} z'_{n+1} &= y_n - \beta z'_n \\ x'_n &= \frac{y_{n+1} - g(y_n) + \alpha z'_n}{\delta} \\ r_n &= \frac{x'_{n+1} - f(x'_n)}{\varepsilon} \end{aligned} \quad (6.8)$$

where r_n is the recovered signal.

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the number of iteration taken by the attacker and the attacker resultant keys are given in table 6.2. The attacker input and output signals are shown in Fig. 6.10. The figure shows that the attacker succeeds in attacking the system and recovering the information signal. The difference between the normal output and the attacker output is around 0.05.

Keys	Encrypter keys												Attacker resultant keys																	
a	0	.	1	0	9	9	8	8	5	6	7	4	3	2	1	0	.	1	0	9	9	8	6	7	2	9	4	0	4	0
b	0	.	1	9	5	9	9	8	9	0	0	1	2	3	0	0	.	1	9	6	2	7	2	3	8	6	8	0	9	1
c	9	.	9	8	7	6	3	8	7	5	4	4	5	0	5	9	.	9	8	4	7	0	5	0	0	2	9	1	8	4
Attacker initial values			Optimiser 1				Optimiser 2																							
a	b		C		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																		
0.085	0.1		8																											
Ranges			0	0.01	0.32	321	0	0.01	1.5	1501																				
0.075	0.2	0.1									0.2	8	12																	
Total time of attack		345.807 seconds		Total number of iterations				1219																						

Table 6.2 Encrypter keys, attacker initial values and attacker resultant keys

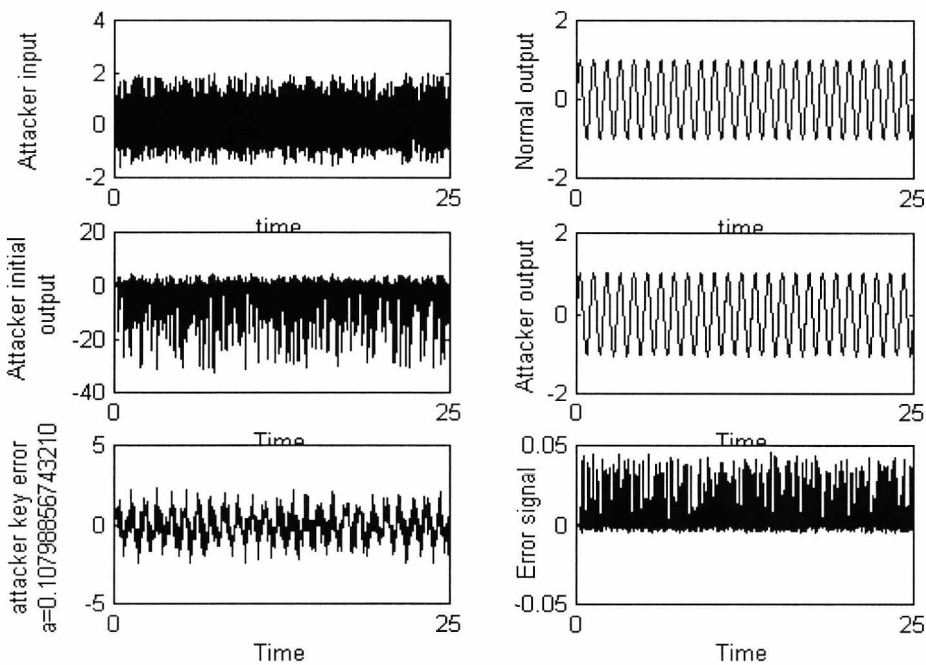


Fig. 6.10 Attacker results of Yamakawa's chaotic communication system.

6.3.5 Attacking the Van Der Pol-Duffing chaotic communication system

Kocarev and Lakshmanan [20] have proposed a chaotic communication system based on Van Der Pol-Duffing chaotic generator. The system uses a chaotic signal to mask the information signal and a synchronous chaotic system in the receiver to identify the chaotic part of the signal, which is subtracted to reveal the information signal. The state equations of the transmitter are

$$\begin{aligned}\dot{x} &= -\nu[x^3 - ax - y] \\ \dot{y} &= x - y - z \\ \dot{z} &= \beta y.\end{aligned}\tag{6.9}$$

The transmitted signal $r(t)$ is equal to

$$r(t) = x(t) + s(t)\tag{6.10}$$

where $s(t)$ is the information signal.

The state equations of the receiver are

Response 1

$$\begin{aligned}\dot{y}' &= r(t) - y' - z' \\ \dot{z}' &= \beta y'\end{aligned}\tag{6.11}$$

Response 2

$$\dot{x}'' = -\nu[(x'')^3 - \alpha(x'') - y']\tag{6.12}$$

The information signal is recovered by

$$\tilde{s}(t) = r(t) - x''(t).\tag{6.13}$$

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.3. The attacker input and output signals are shown in Fig. 6.11. The figure shows that the attacker algorithm succeeds in attacking the Van Der Pol-Duffing chaotic communication system and the error between the normal output and the attacker output is 10^{-4} .

Keys	Encrypter keys															Attacker resultant keys														
	a	0	.	3	4	9	9	8	8	7	6	0	5	4	3	2	0	.	3	5	0	0	0	7	3	3	5	0	4	7
B	2	9	9	.	9	9	8	8	8	7	6	5	0	2	3	2	9	9	.	9	9	7	6	5	9	1	2	0	7	2
C	1	0	0	.	0	0	1	2	3	8	7	5	4	3	0	1	0	0	.	0	0	7	7	8	8	7	0	4	0	3
Attacker initial values			Optimiser 1				Optimiser 2																							
a	b	c	Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																				
0.32	290	85																												
Ranges			0	0.01	3	301	0	0.01	7.5	751																				
0.24	0.38	250									350	75	125																	
Total time of attack		292.16 second	Total number of iterations				1583																							

Table 6.3 Encrypter keys, attacker initial values and attacker resultant keys.

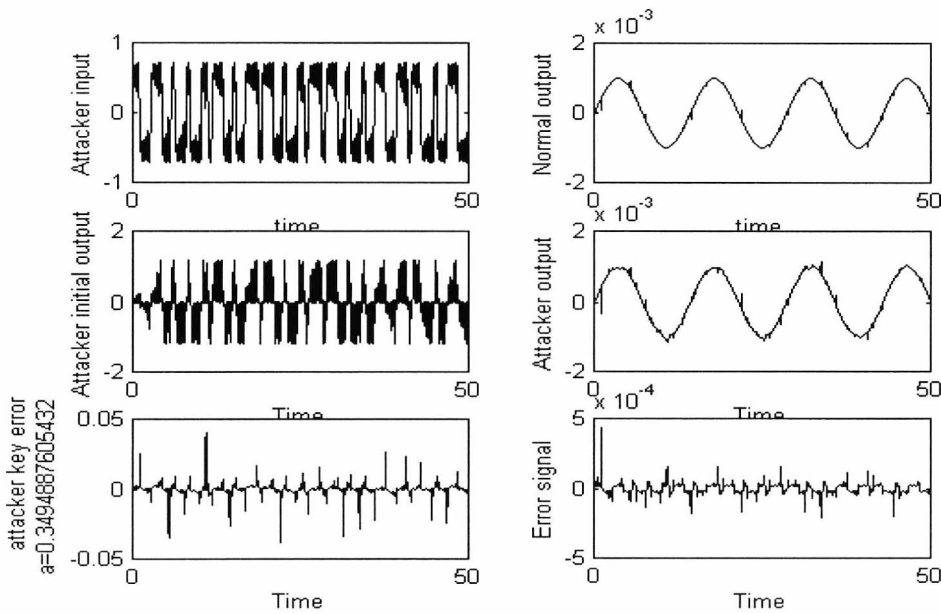


Fig. 6.11 Attacker results of the Van Der Pol-Duffing chaotic communication system.

6.3.6 Attacking the system based on the general approach for chaotic synchronisation

Kocarev and Parlitz presented a secure communication system based on the general synchronisation approach [[21]. The system uses the well-known Lorenz model. The state equations of the transmitter are given by

$$\begin{aligned}\dot{x}_1 &= -ax_1 + s(t) \\ \dot{x}_2 &= bx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - cx_3\end{aligned}\tag{6.14}$$

where a , b and c are constants and $s(t)$ is the transmitted signal and it is given by

$$s(t) = 10x_2 + ix_3\tag{6.15}$$

and i is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{y}_1 &= -ay_1 + s(t) \\ \dot{y}_2 &= by_1 - y_2 - y_1y_3 \\ \dot{y}_3 &= y_1y_2 - cy_3.\end{aligned}\tag{6.16}$$

The information signal is recovered by

$$i_R = (s(t) - 10y_2) / y_3.\tag{6.17}$$

The initial key values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.4. The attacker input and output signals are shown in Fig. 6.12. The figure illustrates that the information signal is recovered with an error 10^{-5} compared to the normal output signal. As described in section 6.3.3, the normal output is the output of the decrypter when we know the encrypter keys exactly.

Keys	Encrypter keys														Attacker resultant keys															
	a	9	.	9	9	8	8	7	6	5	4	3	4	1	0	2	9	.	9	9	8	8	7	3	6	1	4	0	2	4
b	2	7	.	9	9	9	5	6	7	4	3	2	1	9	8	2	7	.	9	9	9	5	6	4	8	8	7	6	3	2
c	2	.	6	6	6	7	0	0	2	3	4	5	6	3	0	2	.	6	6	6	6	9	9	8	3	9	7	0	2	6
Attacker initial values						Optimiser 1				Optimiser 2																				
a	b	c	Start time	Step	Stop time	No. of points	Start time	Step size	Stop time	No. of point																				
8	26	2.1																												
Ranges						0	0.01	3	301	0	0.01	3	301																	
5	12	25	35	2	4																									
Total time of attack			222.617 seconds			Total number of iterations				1720																				

Table 6.4 Encrypter keys, attacker initial values and attacker resultant keys.

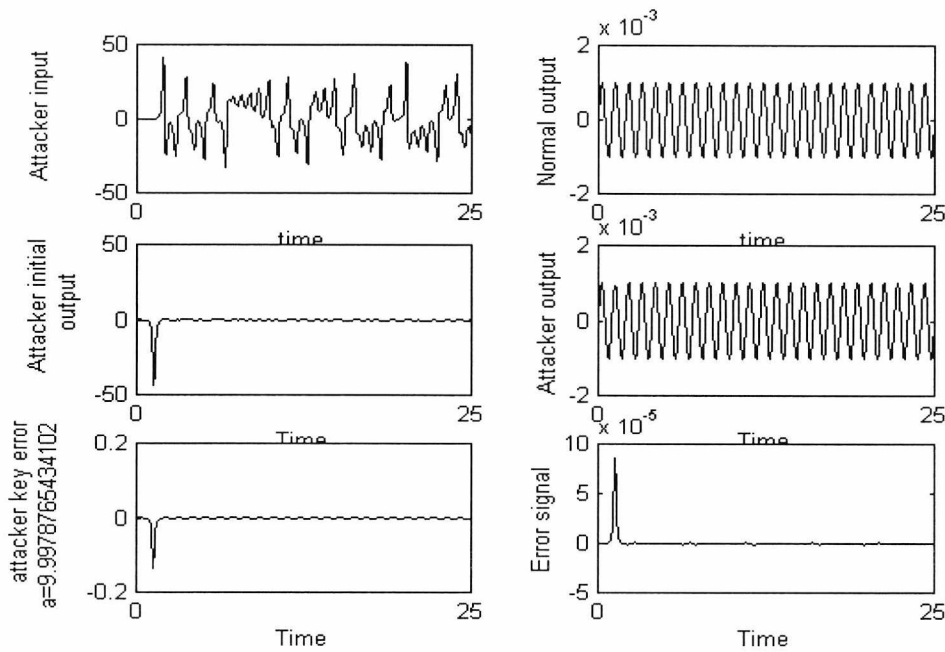


Fig. 6.12 Attacker results of the general approach for chaotic synchronisation.

6.3.7 Attacking the Chua masking chaotic communication system

Kocarev *et al.* [22] have experimentally demonstrated a secure communication system using Chua's circuit. In this method, the information is added at the output of the Chua generator at the transmitter and recovered at the receiver by subtracting the chaotic signal. The state equations of the transmitter are given by

$$\begin{aligned} C_1 \frac{dv_{C_1}}{dt} &= G(v_{C_2} - v_{C_1}) - g(v_{C_1}) \\ C_2 \frac{dv_{C_2}}{dt} &= G(v_{C_1} - v_{C_2}) + i_L \\ L \frac{di_L}{dt} &= -v_2 \end{aligned} \quad (6.18)$$

The transmitted signal $r(t)$ is given by

$$r(t) = v_{C_1} + s(t) \quad (6.19)$$

where $s(t)$ is the information signal.

The receiver is composed of two subsystems, the state equations of the first subsystem are given by

$$\begin{aligned} C_2 \frac{dv_{C_2}^{(1)}}{dt} &= G(r(t) - v_{C_2}^{(1)}) + i_L^{(1)} \\ L \frac{di_L^{(1)}}{dt} &= -(v_{C_2}^{(1)} + ri_L^{(1)}) \end{aligned} \quad (6.20)$$

The second subsystem is given by

$$C_1 \frac{dv_{C_1}^{(2)}}{dt} = \frac{1}{R} (v_{C_2}^{(1)} - v_{C_1}^{(2)}) - g(v_{C_1}^{(2)}) \quad (6.21)$$

The recovered information signal $s(t)$ is given by

$$s(t) = r(t) - v_{C_1}^{(2)}. \quad (6.22)$$

The initial key values for the attacker, the range of each key, the number of data samples required for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.5. The attacker input and output signals are shown in Fig. 6.13. The figure indicates that the input signal is recovered and the difference between the attacker output and the normal output of the system is around 0.1.

Keys	Encrypter keys																Attacker resultant keys															
	a	9	.	9	9	8	6	7	4	3	2	1	9	2	0	0	9	.	9	9	8	6	6	9	8	0	8	1	3	8	4	
b	0	.	6	4	9	9	7	8	6	5	4	3	2	0	1	0	.	6	5	0	3	1	0	3	6	7	2	5	6	5		
c	1	.	0	0	1	2	3	8	9	7	6	5	4	3	0	0	.	9	9	8	7	8	6	7	4	7	0	8	0	7		
d	5	.	5	9	9	8	7	6	9	8	7	6	5	4	0	5	.	6	0	5	2	3	7	3	1	0	0	0	2	2		
Attacker initial values				Optimiser 1				Optimiser 2																								
a	b	c	d	Start time	Step	Stop time	No. of points	Start time	Step	Stop time	NO. of points																					
8	0.5	0.7	4.5																													
Ranges				0	0.01	3.0	301	0	0.01	0.5	51																					
6	12	0.25	0.8									0.75	1.2	4	6																	
Total time of attack		332.829 seconds		Total number of iterations				1558																								

Table 6.5 Encrypter keys, attacker initial values and attacker resultant keys.

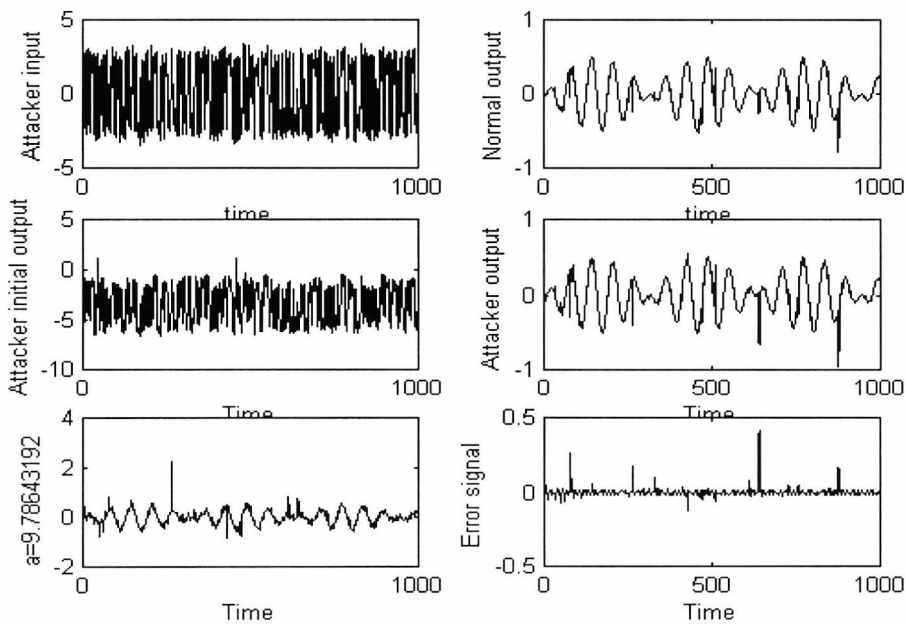


Fig. 6.13 Attacker results of the Chua masking chaotic communication system.

6.3.8 Attacking the Rössler encryption algorithm

The attacker algorithm attacks our developed Rössler encryption algorithm [23]. The details of the algorithm were presented in chapter 5 (section 5.4.1.2). The state equations of the transmitter are given by

$$\begin{aligned}\dot{x} &= -y - z \\ \dot{y} &= x + ay + s(t) \\ \dot{z} &= b + z(x - c)\end{aligned}\tag{6.23}$$

where a , b and c are constants and $s(t)$ is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{x}_r &= -y - z_r \\ \dot{z}_r &= b + z_r(x_r - c) \\ \tilde{S}(t) &= \dot{y} - x_r - ay\end{aligned}\tag{6.24}$$

where $\tilde{S}(t)$ is the recovered information signal.

In this case, the signal to chaos ratio is equal to -246 dB. The initial values for the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 7.6. The attacker input and output signals are illustrated in Fig. 6.14. The figure shows that with resultant attacker values, the information signal is completely recovered and that the difference between the normal output of the system and the attacker output is equal to zero.

Keys	Encrypter keys													Attacker resultant keys																
	a	0	.	3	9	8	0	1	7	8	4	5	3	2	1	3	0	.	3	9	8	0	1	7	8	4	5	3	2	1
b	1	.	9	9	7	8	6	5	3	4	2	1	8	7	6	1	.	9	9	7	8	6	5	3	4	2	1	8	7	6
c	4	.	0	1	5	6	7	4	3	2	3	1	7	6	2	4	.	0	1	5	6	7	4	3	2	3	1	7	6	2
Attacker initial values						Optimiser 1				Optimiser 2																				
a		b		c		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																	
0.1		0.1		1																										
Ranges						0	0.1	10	101	0	0.1	20	201																	
0.1	0.5	0.1	3	0.1	5																									
Total time of attack		166.44 seconds				Total number of iterations				1424																				

Table 6.6 Encrypter keys, attacker initial values and attacker resultant keys.

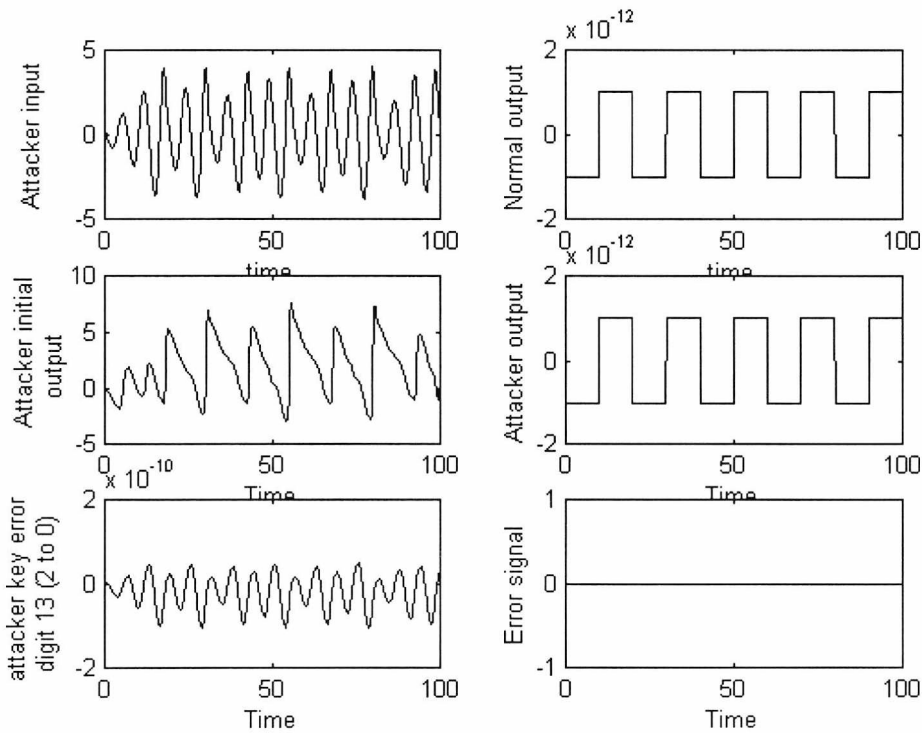


Fig. 6.14 Attacker results of the Rössler encryption system.

6.3.9 Attacking the Lorenz encryption algorithm

The attacker algorithm also attacks our developed Lorenz encryption algorithm [23]. The details of the algorithm were given in chapter 5 (section 5.4.1.3). The state equations of the transmitter are given by

$$\begin{aligned}\dot{x} &= a(y - x) \\ \dot{y} &= bx - y - xz + s(t) \\ \dot{z} &= xy - cz\end{aligned}\tag{6.25}$$

where a , b and c are constants and $s(t)$ is the information signal.

The state equations of the receiver are

$$\begin{aligned}\dot{x}_r &= a(y - x_r) \\ \dot{z}_r &= x_r y - cz_r \\ \tilde{s}(t) &= \dot{y} - bx + y - xz\end{aligned}\tag{6.26}$$

where $\tilde{S}(t)$ is the recovered signal.

The signal to chaos ratio is equal to -257 dB. The initial key values of the attacker, the range of each key, the number of data samples needed for the attacking, the time of attack, the total number of iterations taken by the attacker and the attacker resultant keys are given in table 6.7. The attacker output signals are illustrated in Fig. 6.15. The figure illustrates that the attacker recovered the information signal and that the difference between the normal output and the attacker output is equal to 10^{-13} .

Keys	Encrypter keys													Attacker resultant keys																
	a	9	.	9	8	6	7	9	5	4	3	2	1	0	1	2	9	.	9	8	6	7	9	5	4	3	2	1	0	1
b	2	8	.	0	0	2	5	4	7	8	9	6	5	4	2	2	8	.	0	0	2	5	4	7	8	9	6	5	4	3
c	2	.	6	6	6	6	9	0	9	1	2	3	4	5	6	2	.	6	6	6	6	9	0	9	1	2	3	4	5	6
Attacker initial values						Optimiser 1				Optimiser 2																				
a		b		c		Start time	Step	Stop time	No. of points	Start time	Step	Stop time	No. of points																	
9		25		2																										
Ranges						0	0.1	10	101	0	0.1	10	101																	
8	12	25	35	2	4																									
Total time of attack			123.478 seconds			Total number of iterations				1574																				

Table 6.7 Encrypter keys, attacker initial values and attacker resultant keys.

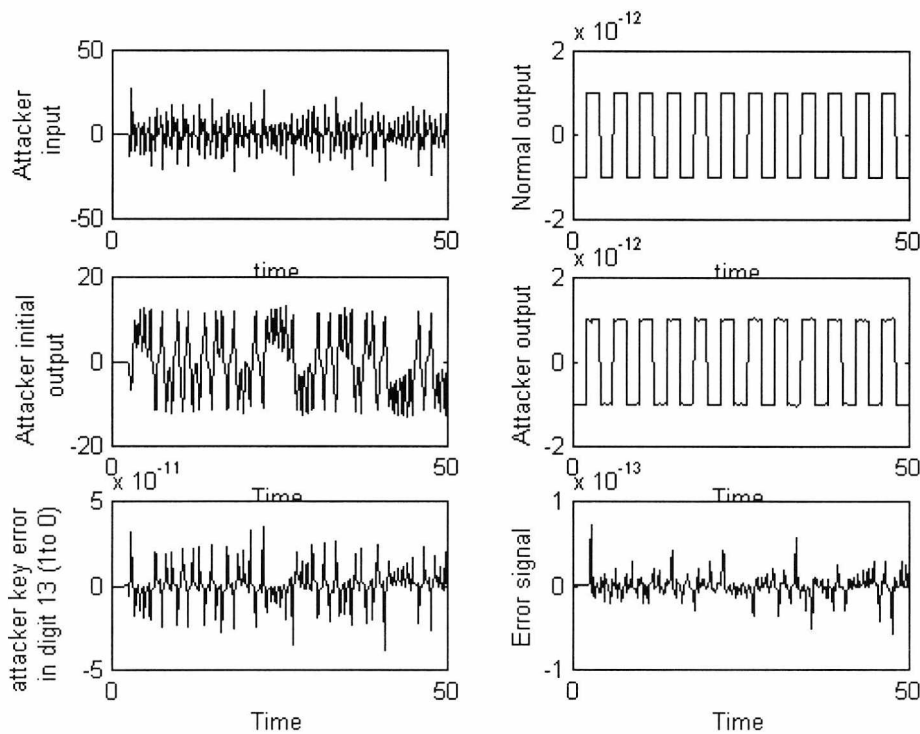


Fig. 6.15 Attacker results of the Lorenz encryption system.

The above results show that the new attacker algorithm breaks the chaotic communication systems under attack and the information signal is recovered. As a result, the above systems are not secure and we should improve their security. In chapter 7, we will give some methods to counter that attacker and improve the security of the chaotic communication systems and counter the attack algorithm.

6.4 Conclusion

A new algorithm for attacking the chaotic communication system is introduced. The algorithm is based on two optimisation programs of the MATLAB. The algorithm is tested on different chaotic communication systems (continuous and discrete time systems). It is tested on systems based on chaos masking or chaos modulating. The algorithm also attacks the new encryption algorithms introduced in chapter 5. The algorithm succeeds in attacking all the chaotic systems under test and finds their keys. The information signal is recovered even at signal to chaos ratios in the order of -240 dB.

6.5 References

- [1] B. Schneier, *Applied cryptography*: Jhon Wiley & Sons, Inc, 1996.
- [2] L. R. Knudsen, "Block cipher-Analysis, design, applications," *Ph.D. dissertation*, Aarrhus University, Nov. 1994.
- [3] A. M. Fraser, "Reconstructing attractors from scalar time series-A comparison of singular system and redundancy criteria," *Physica D*, vol. 34, pp. 391-404, 1989.
- [4] A. I. Mess, "Reconstructing nonlinear systems," *IEEE Int. Symposium. on Circuit and System (ISCAS 96)*, pp. 1-4, 1996.
- [5] M. Casdagli, "Nonlinear prediction of chaotic time series," *Phys. D*, vol. 35, pp. 335-356, 1989.
- [6] L. A. Aguirre and S. A. Billings, "Retrieving dynamical invariants from chaotic data using NARMAX models," *Int. J. Bifurcation and Chaos*, vol. 5, No. 2, pp. 449-474, 1995.
- [7] H. D. I. Abarbanel, R. Brown and J. B. Kadtko, "Predication in chaotic nonlinear systems: Methods for time series with broadband Fourier spectra," *Phys. Rev A*, vol 41, pp. 1782-1807, 1990.
- [8] M. Casdagli, S. Eubank, J. D. Farmer and J. Gibson, "State space reconstruction in the presence of noise," *Phys. D*, vol. 51, pp.52-98. 1991.
- [9] U. Parlitz, R. Zöllner, J. Holzfuss and W. Lauterborn, "Reconstructing physical variables and parameters from dynamical systems," *Int. J. Bifurcation and Chaos*, vol. 4, No. 6, pp. 1715-1719, 1996.
- [10] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos*, vol. 4, No. 4, pp. 959-977, 1994.
- [11] J. Stark and B. V. Arumugam, "Extracting slowly varying signals from a chaotic background," *Int. J. Bifurcation and Chaos*, vol. 2, No.2, pp. 413-419, 1992.
- [12] T. Yang, L. B. Yang and C. M. Yang, "Breaking chaotic switching using generalised synchronisation: examples," *IEEE Trans. Circuits Syst. I*, vol. CAS-45, No. 10, Oct. 1998.

-
- [13] L. Kocarev and U. Parlitz, "Generalized synchronisation, predictability and equivalence of unidirectionally coupled dynamical systems," *Phys. Rev. Lett.*, vol. 76, No. 11, pp. 1816-1819, Mar. 1996.
- [14] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring and H. D. I. Abarbanel, "Generalised synchronisation of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp. 980-994, 1995.
- [15] E. Pärt-Enander and A. Sjöberg, *The MATLAB 5 handbook*: Published by Addison Wesley Longman Limited, 1999.
- [16] J. C. Lagarias, J. A. Reeds, M. H. Wright and P. E. Wright, "Convergence properties of the Nelder-Mead Simplex algorithm in low dimension," *SIAM J. Optimisation*, May 1997.
- [17] M. I. Sobhy and A. R. Shehata, "Secure e-mail and databases using chaotic algorithms," *Electron. Lett.*, vol. 36, No. 10, May 2000.
- [18] M. Itoh, H. Murakami and L. O. Chua, "Secure communication via Yamakawa's chaotic chips and Chua's circuits," *IEEE Int. Symposium. on Circuit and System (ISCAS 94)*, pp. 1293-1296, 1994.
- [19] M. Itoh and H. Murakami, "New communication systems via chaotic synchronisations and modulations," *IEICE Trans. Fundamentals*, vol. E78-A, No. 3, Mar. 1995.
- [20] K. Murali and M. Lakshmanan, "Transmission of signals by synchronisation in a chaotic Van Der Pol-Duffing oscillator," *Phys. Rev. E*, vol. 48, No. 3, pp. R1624-R1626, 1993.
- [21] L. Kocarev and U. Parlitz, "General approach for chaotic synchronisation with applications to communications," *Phys. Rev. Lett.*, vol. 74, No. 25, pp. 5028-5031, June 1995.
- [22] Lj. Kocarev, K. S. Halle, K. Eckert, U. Parlitz and L. O. Chua, "Experimental demonstration of secure communications via chaos synchronisation," *Int. J. Bifurcation and Chaos*, vol. 3, No. 2, pp. 469-477, 1993.
- [23] M. I. Sobhy and A. R. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurcation and Chaos*, will be published in Nov. 2000.

Chapter 7

COUNTER MEASURES TO THE CHAOTIC ATTACKING ALGORITHM

7.1 Introduction

In chapter 6, we introduced a new algorithm for attacking chaotic communication systems, which succeeds in attacking several chaotic communication systems. The systems attacked include, masking systems [1]-[2], systems based on the general synchronisation approach [3] and discrete systems [4]-[5]. Our new developed chaotic encryption algorithms [6] presented in chapter 5 were also attacked by our attacker algorithm. In this chapter, four methods of counter measures are presented in section 7.2. In section 7.3 a method of counter counter measures of the attacker is presented. The conclusion of the chapter and the chapter references are given in sections 7.4 and 7.5.

7.2 New methods of counter measures for the chaotic attacker

The security of chaotic communication systems can be improved by using the following methods.

7.2.1 Method 1

We convert all fixed parameters (keys and the initial conditions) to nonlinear bounded functions (sine, cosine, tanh...etc). The bounded functions are used to ensure that the system still has a chaotic behaviour. The state variables are not multiplied by constant values but by functions of one or several state variables. The attacker must first finds out what the functions used in the system are and then finds

the parameter values. As an example, in the Chua masking system we replace the

term $\frac{1}{C_1}(v_{C_2} - v_{C_1})$ in Eq. 6.18 by

$$\frac{1}{C_1}(v_{C_2} - v_{C_1}) + a_1 \sin(a_2 * (v_{C_2} - v_{C_1})) - a_3 \cos(a_4(v_{C_2} - v_{C_1})) + \dots$$

In this case, the attacker should find out the functions used and then the values of a_1, a_2, a_3 and a_4 . The Chua system is tested using the above equation with the following parameter values; $a_1=0.08, a_2=0.3, a_3=0.1$ and $a_4=0.2$. The results illustrate that the chaotic behavior of the Chua system does not change as shown in Fig. 7.1.

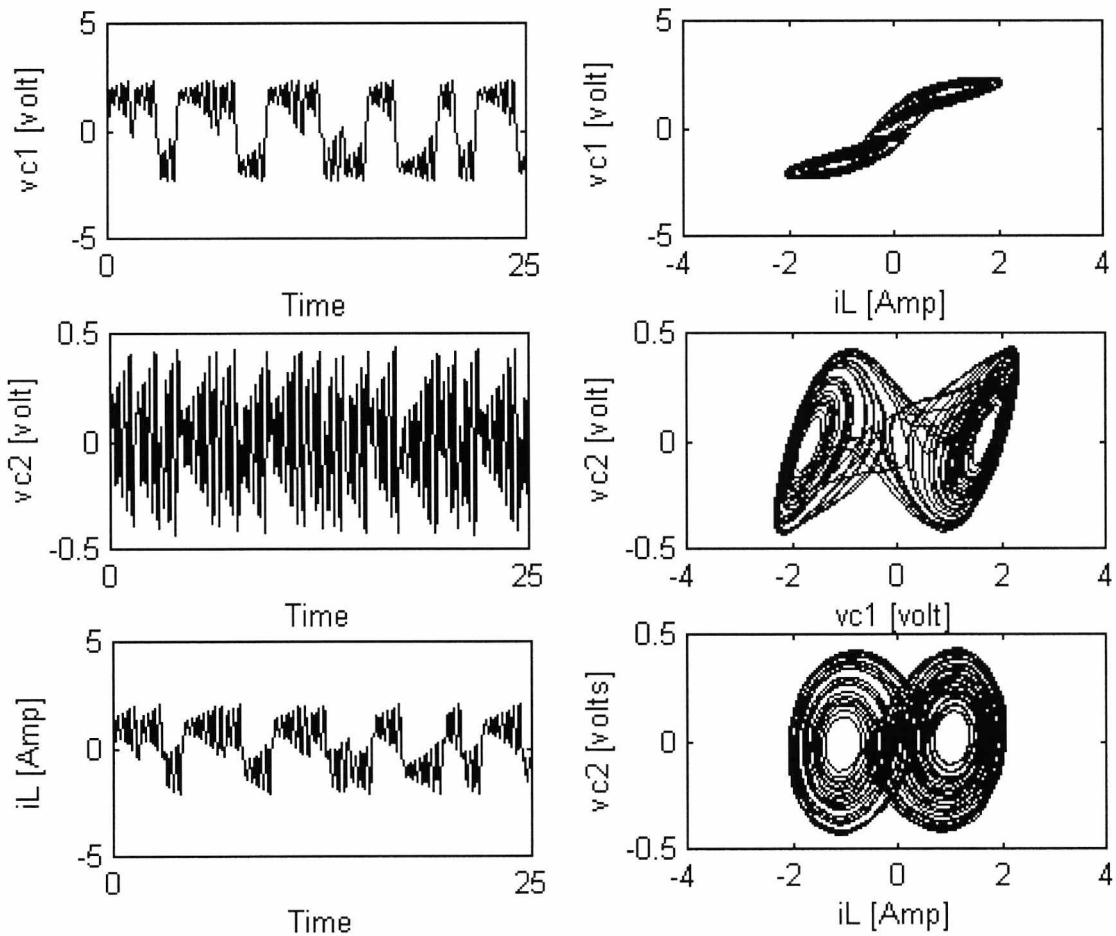


Fig. 7.1 Output signals and attractors of the Chua chaotic system.

7.2.2 Method 2

The security of the system can be improved by making the parameters of the system dependant on two or three state variables instead of one state variable, such that this change does not affect the chaotic behaviour of the system. For example, in the Rössler system instead of writing the equation

$$\dot{y} = x + ay + s(t).$$

we can write it as

$$\dot{y} = x + (a + a_1x + a_2z)y + s(t).$$

The attacker should find out the values of a , a_1 and a_2 instead of only the value of a . The Rössler system is tested using the values $a = 0.398$, $a_1 = 0.05$ and $a_2 = 0.075$ and the results illustrate that the chaotic behaviour of the Rössler system does not change as shown in Fig. 7.2.

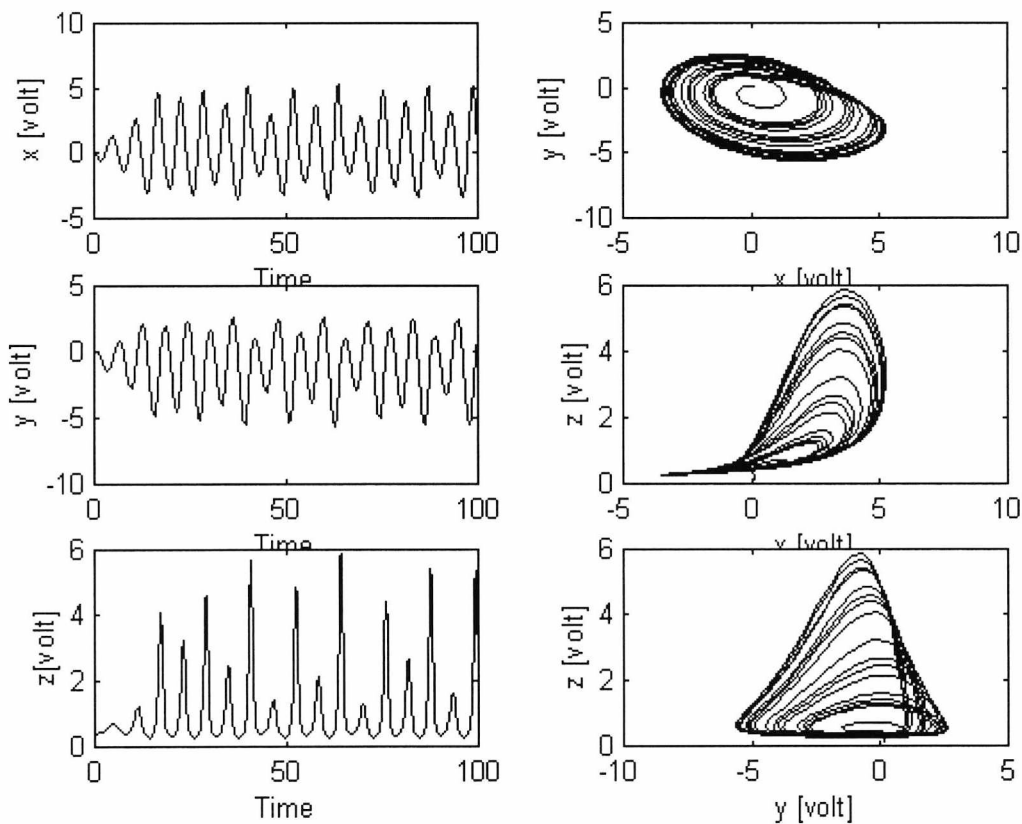


Fig. 7.2 Rössler chaotic output signals and attractors.

7.2.3 Method 3

The security of the system can be improved by using a multi-system encryption algorithm. In this algorithm a combination of Chua, Lorenz and Rössler algorithms are used to encrypt the information signal. The signal flow diagram of the algorithm using the SIMULINK is shown in Fig. 7.3.

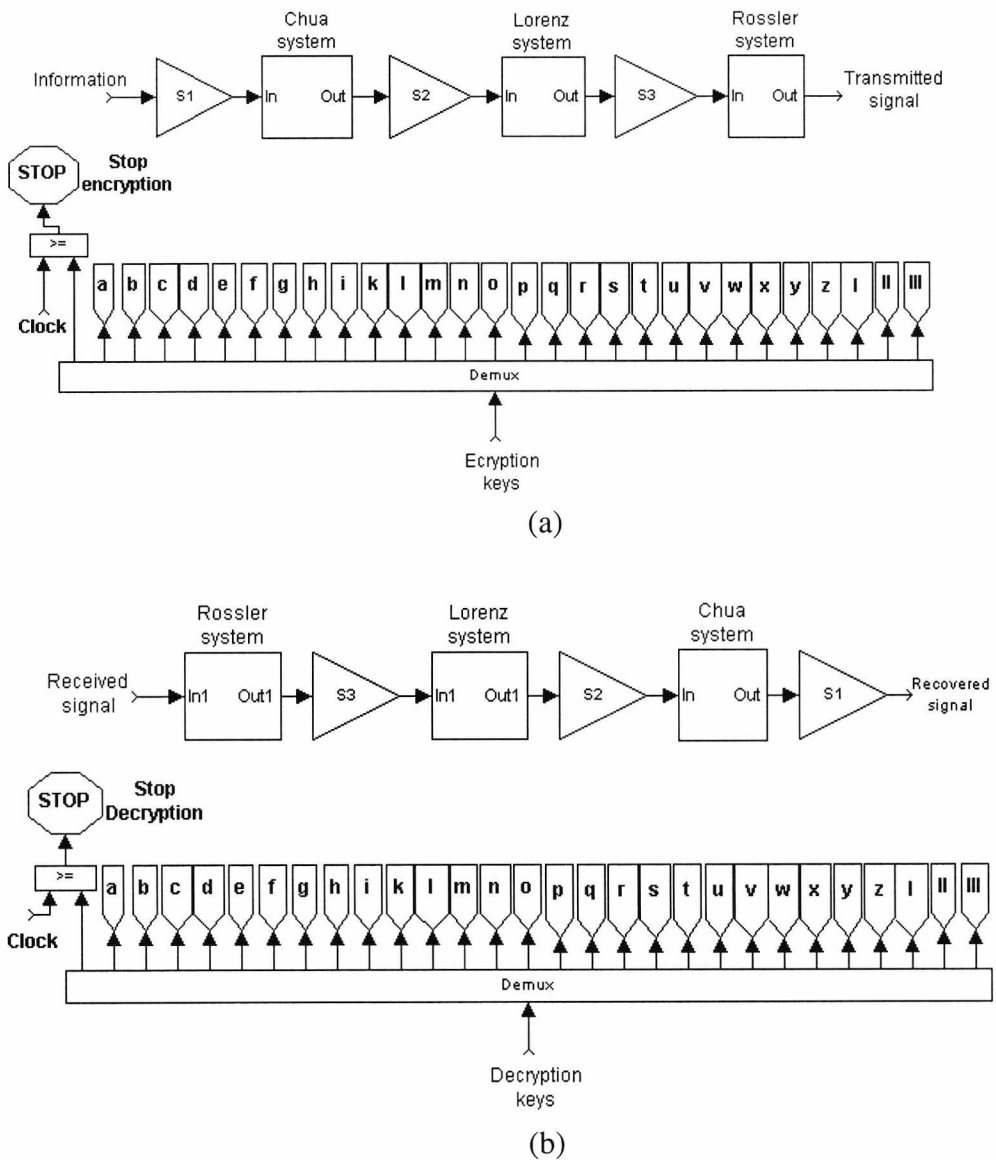


Fig. 7.3 The multi-system algorithm block diagram

(a) Encryption part.

(b) Decryption part.

In the transmitter, the information is scaled by ($S_1=10^{-3}$) and encrypted using the Chua encryption algorithm [6]. The output of the Chua algorithm is scaled by ($S_2=10^{-3}$) and encrypted using the Lorenz encryption algorithm [6]. Finally, the Lorenz algorithm output is scaled by ($S_3=10^{-4}$) and encrypted using the Rössler encryption algorithm [6]. In the receiver, the received signal is decrypted using the Rössler decryption algorithm, then the recovered signal is scaled by 10^4 . The scaled output of the Rössler decryption algorithm is decrypted using the Lorenz decryption algorithm and the Lorenz recovered signal is scaled by 10^3 . The scaled output signal of the Lorenz decryption algorithm is decrypted using the Chua decryption algorithm. The information signal is recovered by scaling the Chua recovered signal by 10^3 . In this case, the number of keys under attack is increased and the attacker must either attack these algorithms in steps (algorithm by algorithm) or simultaneously. The signal outputs of each algorithm are shown in Fig. 7.4. The figure shows that the information signal is encrypted using different chaotic signals and different signal to chaos ratios are achieved after each step of the encryption of the text file (SCR=-10.7 dB (Chua), -93.6 dB (Lorenz) and -57.6 dB (Rössler)).

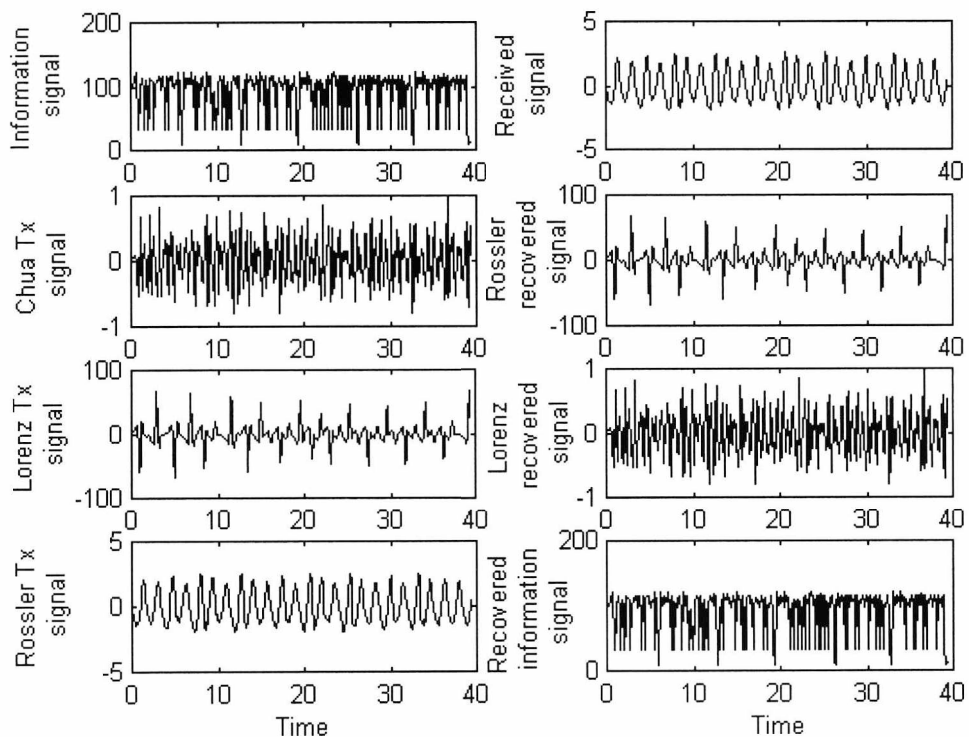


Fig. 7.4 The output signals of the multi-system algorithm.

An example of using this method to encrypt a text file is shown Fig. 7.5. The figure illustrates that the text file is encrypted and recovered without any errors.

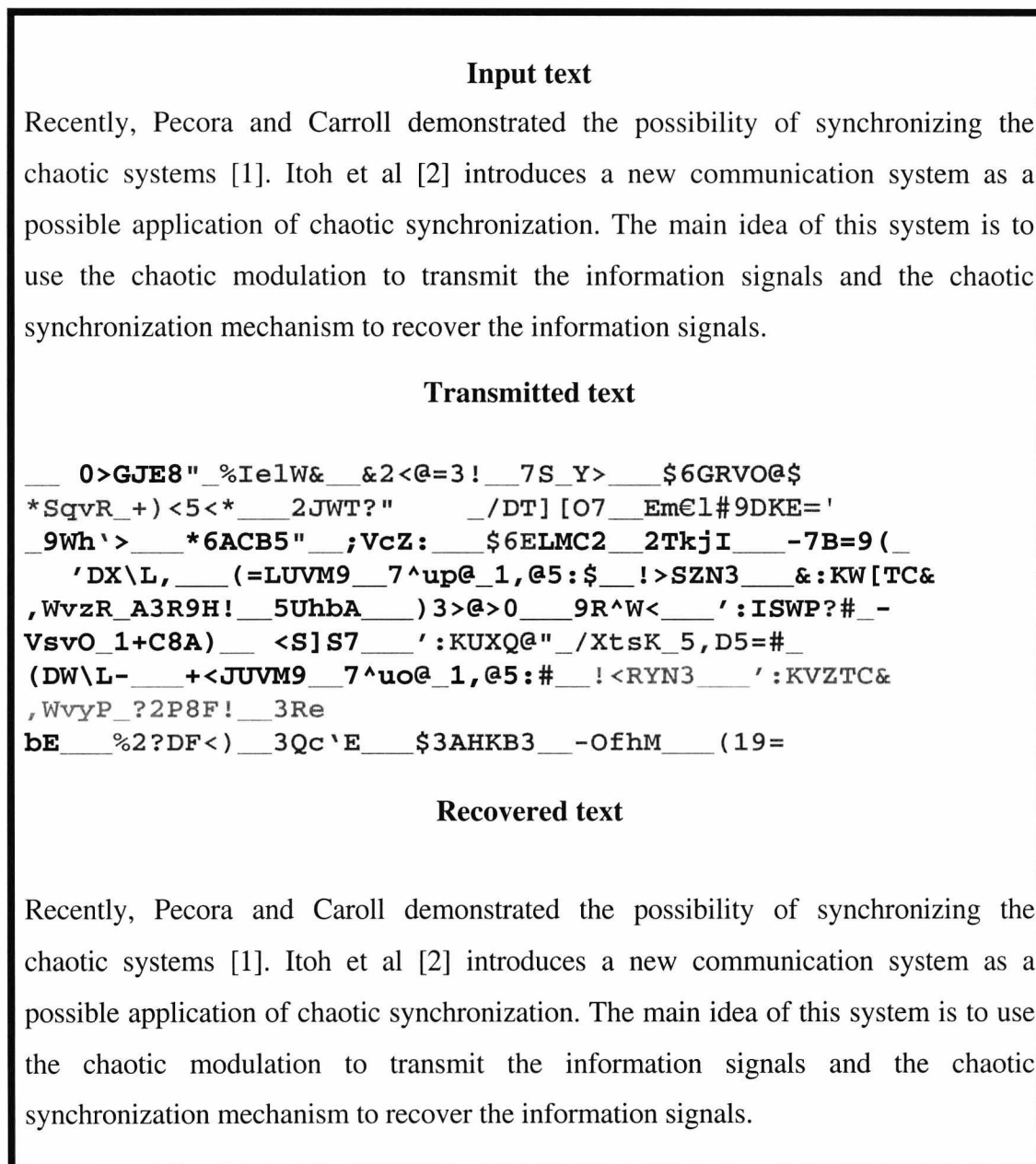


Fig. 7.5 Example of encrypting and decrypting a text file using multi-system algorithm

7.2.4 Method 4

The security of the multi-system algorithm can be improved by making the keys of each system depend on the state variables of the other systems. The attacker must then attack the three systems simultaneously. As an example, we use the state variables x_1 of the Chua system, x_1 of the Lorenz system and x_1 of the Rössler system to control the nonlinear function of Chua system. Normally the Chua nonlinear function is written as

$$-2 \tanh(0.38x_1).$$

We write the Chua nonlinear function as

$$-2 \tanh(0.38x_{1_{Chua}} + 0.01x_{1_{Lorenz}} + 0.02x_{1_{Rössler}}).$$

Fig. 7.6 shows the signal flow diagram of the encryption algorithm. The diagram is a direct representation of the state equation of the Chua, Rössler and Lorenz encryption algorithm but the Chua nonlinear function depends not only on the Chua state variable x_1 but also on the Rössler and Lorenz state variables. The keys of the entire algorithm are defined by the user and stored into a file. The algorithm loads the keys file. The demultiplexer is used to convert the keys file into individual values that can be manipulated by the encryption algorithm. These key values are then fed to the encryption algorithm. The total number of characters of the plaintext is fed to the algorithm from the keys file. The signal flow diagram of the decryption algorithm is shown in Fig. 7.7. The diagram is a direct representation of the Chua, Rössler and Lorenz decryption state equations. The keys file, which is the same as the encryption keys, is loaded by the decryption algorithm and these keys are used to decrypt the received ciphertext.

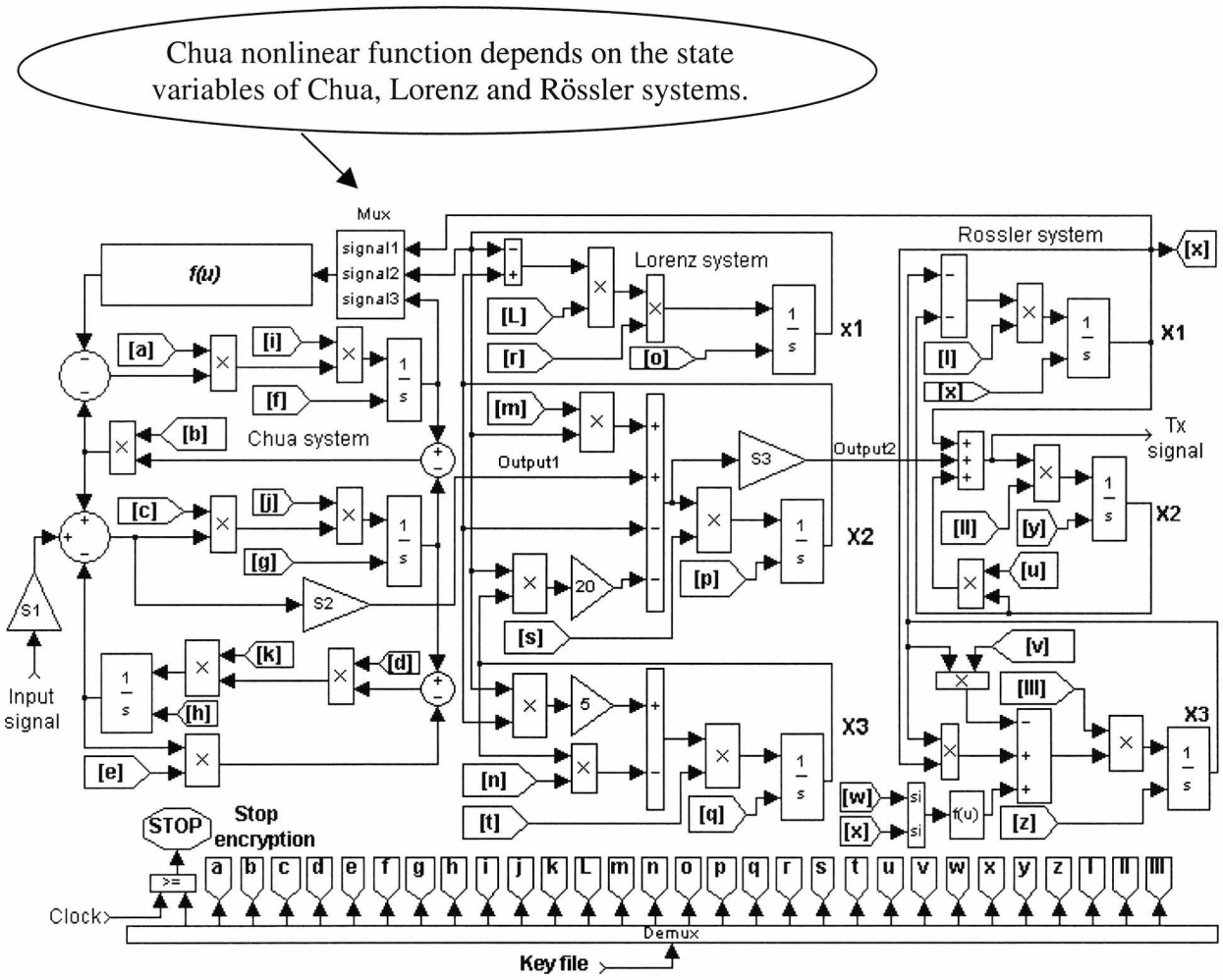


Fig. 7.6 Signal flow diagram of the multi-system encryption algorithm.

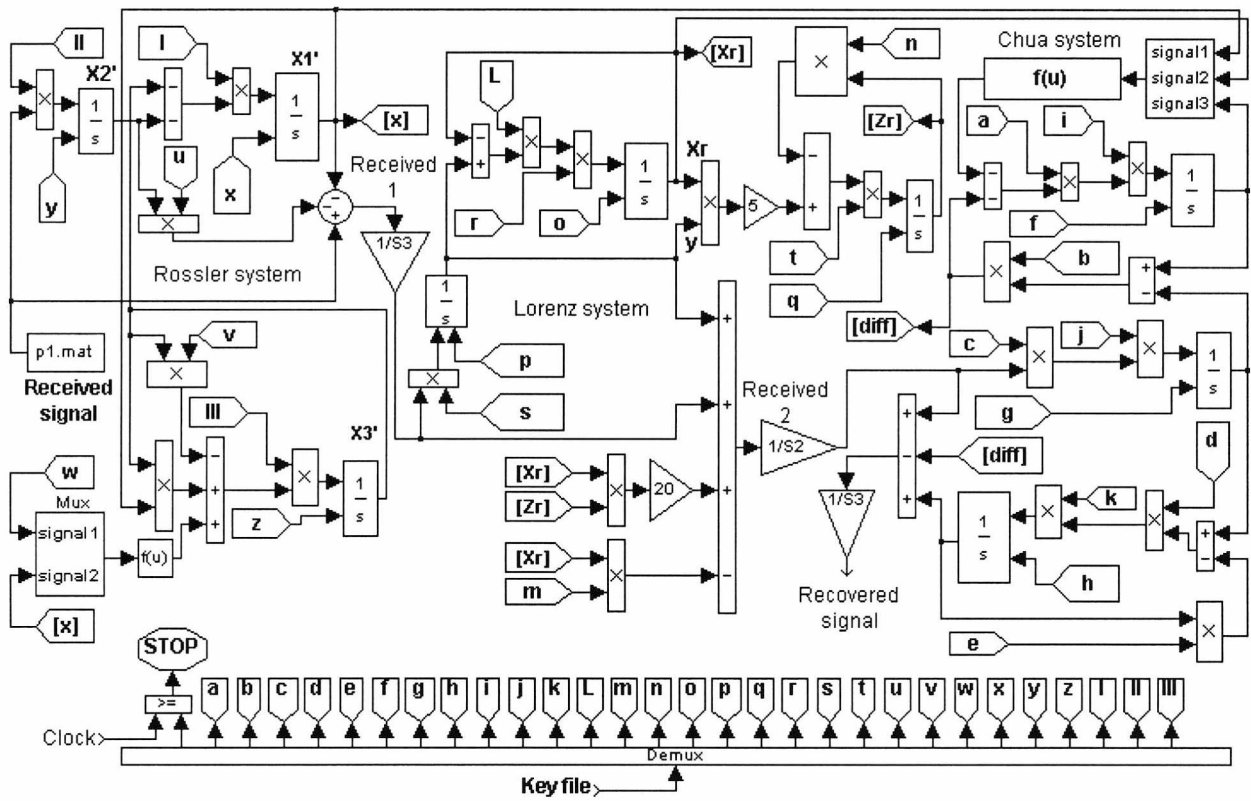


Fig. 7.7 Signal flow diagram of the multi-system decryption algorithm.

Fig. 7.8 shows the signals at each part of the encryption and the decryption algorithms. Different signal to chaos ratios are achieved after each step of the encryption of the text file (-11.2 dB (Chua), -93.1 dB (Lorenz) and -37.6 dB (Rössler)). The figure illustrates that the information signal is completely encrypted through the systems and completely recovered.

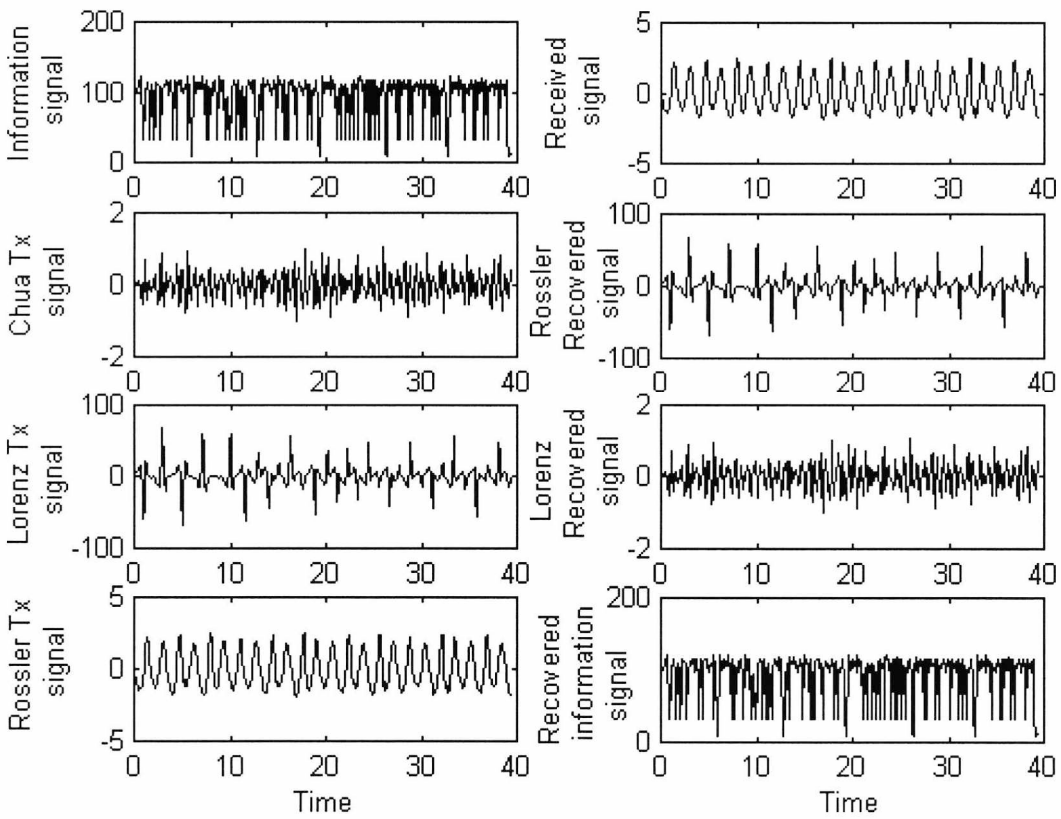


Fig. 7.8 The output signals in each part of the algorithm

Fig. 7.9 shows an example of encrypting a text file using the multi-system encryption algorithm. The figure indicates that the input text file is encrypted and is completely recovered without errors.

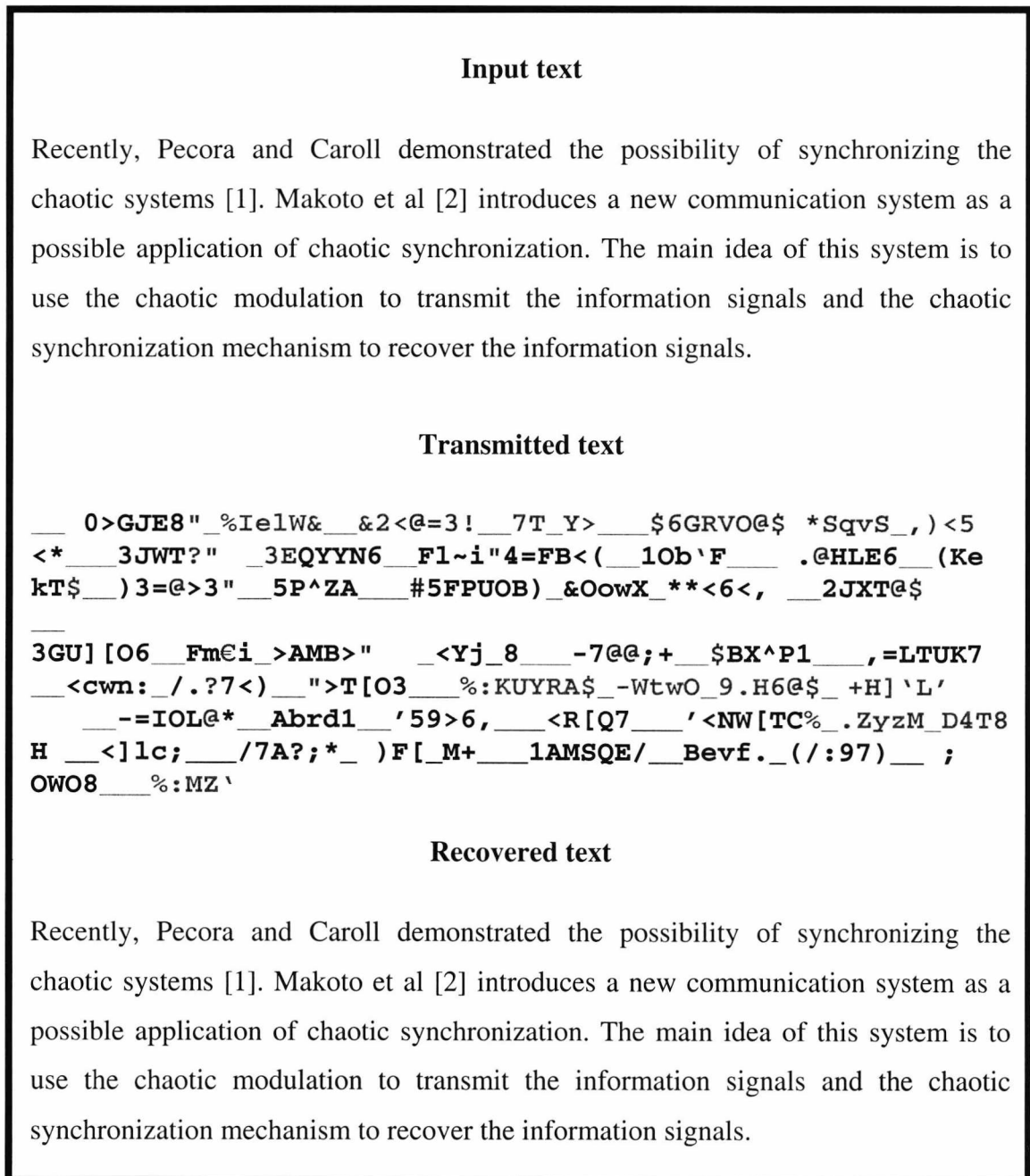


Fig. 7.9 Example of encrypting a text file using multi-system encryption algorithm with feedback.

7.3 Counter counter measures of the chaotic attacker

Since the parameters are now functions of time, the next level of attack is to attack the algorithms symbol by symbol. We apply this method to attack the Lorenz encryption algorithm [6]. Normally, we have the term

$$a(y - x).$$

We rewrite it as follows

$$a(y - x) + \sin(y - x).$$

In this case, the attacker must know what is the added function to equation of a or what is the instantaneous value of the function at each symbol. We will choose the symbol number 500 of the information signal whose value is -0.001 . The corresponding transmitted value is 0.852. We apply the symbol by symbol attack to attack this symbol. The results show that the symbol by symbol attack cannot overcome the counter attack methods of the chaotic communication systems since the resultant value of the symbol is -36.2 instead of the true value of -0.001 . This is shown in Fig. 7.10. As a result, we find that it is difficult to overcome the counter attack methods and these methods give more security to the chaotic communication systems.

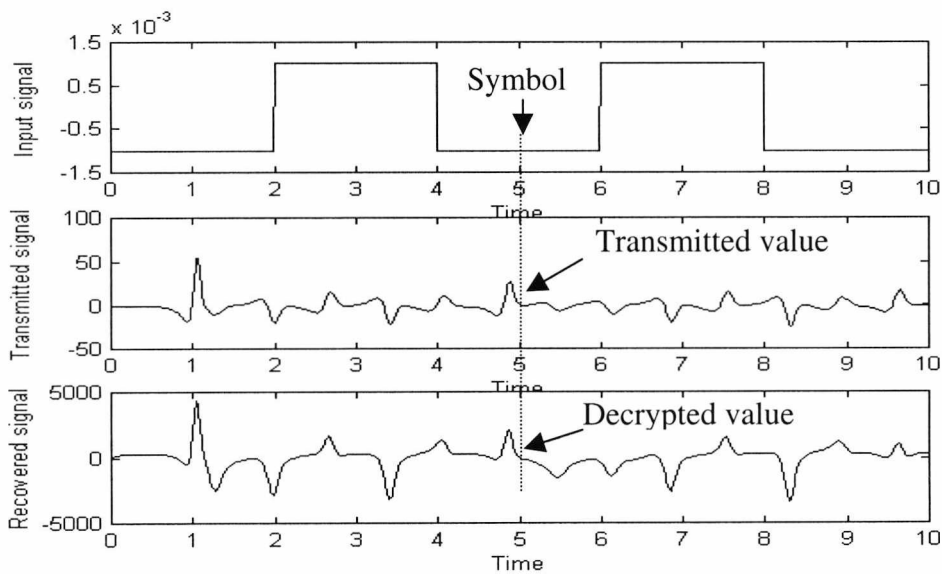


Fig. 7.10 Symbol by symbol attacker results.

7.4 Conclusion

New methods of counter measures are given to improve the security of the chaotic systems. We found that, it is difficult to attack the systems in the following cases:

- When the systems use nonlinear bounded functions instead of constant parameters.
- The parameters of the systems depend not only on all the state variables of the system.
- When we use multi-system algorithm. Especially, when the parameters of one system are controlled by the state variables of the other systems. In this case, the attacker should attack the whole systems simultaneously.
- Finally we introduce the symbol by symbol attack to overcome the counter measures. The results show that the symbol by symbol attack cannot overcome the counter attack methods and this means that the chaotic systems are potentially secure.
- Obviously, these methods of counter measures cannot be implemented in the systems based on physical electronic circuits. Since our attack method can break any chaotic encryption system, we conclude that methods based on electronic circuits are not secure.

7.5 References

- [1] K. Murali and M. Lakshmanan, "Transmission of signals by synchronisation in a chaotic Van der pol-Duffing oscillator," *Phys. Rev. E*, vol. 48, No. 3, pp. R1624-R1626, 1993.
- [2] Lj. Kocarev, K. S. Halle, K. Eckert, U. Parlitz and L. O. Chua, "Experimental demonstration of secure communications via chaos synchronisation," *Int. J. Bifurcation and Chaos*, vol. 3, No. 2, pp. 469-477, 1993.
- [3] L. Kocarev and U. Parlitz, "General approach for chaotic synchronisation with applications to communications," *Phys. Rev. Lett.*, vol. 74, No. 25, pp. 5028-5031, June 1995.
- [4] S. Jaroslav and B. V. Arumugam, "Extracting slowly varying signals from a chaotic background," *Int. J. Bifurcation and Chaos*, vol. 2, No. 2, pp. 413-419, 1992.
- [5] M. Itoh, H. Murakami and L. O. Chua, "Communication system via chaotic modulation," *IEICE Trans. Fundamentals*, vol. E77-A, No. 6, June 1994.
- [6] M. I. Sobhy and A. R. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurcation and Chaos*, will be published in Nov. 2000.

Chapter 8

CONCLUSION AND FUTURE WORK

The basic conclusions from the research presented in this dissertation are summarised below:

1. A new analogue chaotic communication system called the multi-channels chaotic communication system is introduced. In the MCCA system, an extra channel is used for the synchronisation between the transmitter and the receiver and the other channels are used for the transmission of the information signals. The simulation results (SCR=-74 dB) and the practical results (SCR=-24 dB) show that the developed system is better than those systems using one channel for the synchronisation of the communication system and masking the information signal (SCR=-12 dB in simulation and practical implementation). The disadvantage of the MCCA system is the use of an extra channel for synchronisation between the transmitter and the receiver. This problem is minimised when the system is used in transmitting different information signals to the same place.
2. We introduce a modified method to implement CSK using one chaotic generator at the transmitter to encode the binary information signal and one receiver system. The same results of the systems used two chaos generators or two nonlinear functions in encoding the binary information 0 and 1 are achieved.
3. A new method to implement the chaotic generators and the chaotic communication systems is developed. A new expression of the Chua nonlinear function is presented. The developed method is used to achieve communication between two computers using the multi-channel chaotic communication system given in chapter 2. The main advantages of the method are:
 - It can be used to implement the chaotic systems that cannot be implemented by a physical circuit and is described by the state equations.

- It is easy to use and the modification of any system is just a change in the block diagram or the parameters within the block.

The disadvantage of this method is that high frequency chaotic generators cannot be implemented using this method since the maximum sampling rate is 20 kHz.

4. A new method for designing microwave chaotic generators is introduced. The importance of this work is that an analysis procedure has been developed to predict accurately the chaotic behavior of the microwave generator. Simulation and experimental results are given to support our claim. The microwave chaotic radar and microwave communication systems are presented. In the microwave chaotic systems the transmitter is based on frequency multiplier chains and the signal is recovered using an inverse system of first stage of this multiplier chains. A new expression for the $q - v$ characteristics of the nonlinear capacitor is given. We examined the effect of the channel delay and channel attenuation and we have shown that the system has immunity against these effects. The effect of a loss of part of the received signal is tested and the system succeeds in recovering the information signal under these conditions.
5. A new method for encrypting text and image files using chaotic algorithms is presented. The algorithms are used for secure computer communication and secure databases. The importance of this work is that this is the first time that the results of using chaotic encryption algorithm to encrypt image files are presented. The method is tested through the e-mail channel and signal to chaos ratios of order 10^{-13} or -240 dB have been achieved and the information are encrypted and decrypted without errors.
6. A new algorithm for attacking the chaotic communication systems is presented. The algorithm is tested on continuous and discrete time systems. The systems are either based on chaotic masking or chaotic modulation. The algorithm succeeds in attacking these systems and finding their keys. The information signal is recovered even at signal to chaos ratios in the order of -240 dB.
7. New methods of counter measures to the chaotic attacking algorithm are presented. To test whether we can overcome these counter measures, we present the symbol by symbol attack and the results show that this attack cannot

overcome the counter measures. This means that such chaotic systems cannot be broken.

For the Future work, we have the following parts need further research.

1. In microwave chaotic systems, we presented the simulation results for the receiver system but we did not download the algorithm on a chip. In future work we will implement the systems using one of the digital implementation techniques such as field programming gate array (FPGA).
2. In Chapter 5, the secure computer communication using chaotic algorithms are developed. We used the e-mail channel as our communication media but the algorithm is developed to work in real time communication systems as well. In the future, we will test this algorithm in real time digital communication systems and the algorithms will be implemented on a single chip using FPGA.
3. In chapter 7, we have shown that the encryption using nonlinear functions for the parameters are robust and could not be broken and we will continue to work in studying the immunity of the systems against any attack.