Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Engineering
Department of Electrical Engineering

Generalized Frequency Division Multiplexing System Based on Hybrid-Chaotic Algorithms for Audio Encryption in 5G Networks

A Dissertation

Submitted to the College of Engineering / University of Babylon in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Electrical Engineering / Electronic and Communications

By

Mohammed Jabbar Mohammed Ameen

(B.Sc. 2007)

(M.Sc. 2017)

Supervised by

Prof. Dr. Saad S. Hreshee

2023 A.D ***1444 A.H***

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ نَرْفَعُ دَرَجَاتٍ مَنْ نشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ ﴾

صَدَقَ اللَّهُ الْعَلِيّ الْعَظِيم

الآية 76 من سورة يوسف

Abstract

Wireless communications face significant security challenges, so there is an ongoing necessity to develop an appropriate security strategy to protect data from eavesdroppers using cryptography based on chaos theory. Generalized frequency division multiplexing (GFDM) is a modern multicarrier waveform adaptable to 5G requirements, but its security issues have not been considered. In this dissertation, four new algorithms for audio encryption based on multiple chaotic maps with DNA encoding and Elliptic Curve (EC) cryptography implemented inside 5G network components, including parallel spatial Modulation (PSM), GFDM, and massive MIMO system, were proposed. The main idea of using several chaotic maps in an unpredicted position is to increase complexity against eavesdroppers.

The first proposed cryptosystem is designed based on multiple chaotic maps named the Hybrid Chaotic Modulo Operator (HCMO) encryption technique. The maps used include Bernoulli, Standard, and Bogdanov maps combined with audio based on the modulo operator. The security tests are Signal to Noise Ratio (SNR)=-23.5969 dB, Peak SNR (PSNR)=4.7569 dB, Spectral Segment SNR (SSSNR)=-31.0528 dB, Linear Predictive Code Distance (d_{LPC})=0.9612, Cepstral Distance (d_{CD})=8.1925, Log Spectral Distance (d_{Log})=21.1417, Frequency Weighted Log Spectral Distance (d_{FWLOG})=23.0908, Mean Square Error (MSE)=0.3344, Root Mean Square (RMS) =0.5773, Crest Factor (CF) =4.7698, Correlation Coefficient (R_{xy})=0.0069, Unified Average Changing Intensity (UACI)=33.334% and Number of Samples Change Rate (NSCR)=99.99%, key space=2^{500}, and speed =6.67×10^{-7} Sec./KB.

The second proposed cryptosystem is designed based on triple chaotic maps, and DNA encoding in the antenna index of PSM called the DNA-AI-PSM technique. The chaotic maps used include Tinkerbell and logistic and Henon maps multiplexed with antenna index using different rules of DNA encoding and two levels of XOR in the frequency domain. The security metrics are SNR=-24.544 dB, PSNR=3.8099 dB, SSSNR=-31.992 dB,

d_{LPC}=1.0257, d_{CD}=7.3827,d_{Log}=21.787, d_{FWLOG}=26.3629, MSE=0.4159, RMS=0.64375, CF=3.8254, R_{xy}=-0.00097, UACI=33.334% and NSCR=99.979%, key space=2^{632}, and speed =9.3×10^{-7}Sec./KB.

The third proposed cryptosystem is designed based on triple chaotic maps and EC-LCG sequence inside the GFDM modulator, named the HC-EC-GFDM technique. The maps used include Ikeda, Tent, and Duffing maps combined with real and imaginary parts of the GFDM subsymbols and then the permuted of the encrypted subsymbols. The security evaluations are SNR=-27.4971 dB, PSNR=0.85673 dB, SSSNR=-34.9912 dB, d_{LPC}=0.14921, d_{CD}=8.9547,d_{Log}=21.9564, d_{FWLOG}=34.7654, MSE=0.82097, RMS=0.90518, CF=0.86503, R_{xy}=-0.0023, UACI=33.334% and NSCR=99.995%, key space=2^{510}, and speed =24×10^{-6}Sec./KB.

The fourth proposed cryptosystem is designed based on triple chaotic maps, the MMSE Linear Precoding Algorithm of Massive MIMO, and the Hybrid Chaotic QR-Decomposition is called the HC-QR-MMSE technique. The maps used include Bernoulli, Henon, and Logistic maps mixed using QR factorization to produce a new hybrid chaotic map. The new sequence is combined with the MMSE precoding matrix with real and imaginary parts and then permuted. The security findings are SNR= -28.2993 dB, PSNR=0.05458 dB, SSSNR=-35.836 dB, d_{LPC}=0.9353, d_{CD}=7.6197,d_{Log}=24.4176, d_{FWLOG}=26.7063, MSE=0.98751, RMS=0.99297, CF=0.0610, R_{xy}=-0.00156, UACI=33.334%, and NSCR=99.9958%, key space=2^{500}, and speed =28.3×10^{-6} Sec./KB.

From the security tests of proposed cryptosystems, the HC-QR-MMSE technique gives a high-security level from other techniques due to very low residual intelligibility. Generally, all proposed cryptosystems have excellent security, resistance to various attacks, high signal recovered quality, large key space, low residual intelligibility, and short computational time, making them suitable for real-time communication.

Dedication

To my parents and brothers

To my wife, the love of my life

To Shams and Fadhl, the blessing of my life

To my supervisors, my teachers and friends

Mohammed

Supervisor Certification

I certify that this dissertation entitled **(Generalized Frequency Division Multiplexing System Based on Hybrid-Chaotic Algorithms for Audio Encryption in 5G Networks)** and submitted by student **(Mohammed Jabbar Mohammed Ameen)** was prepared under my supervision at the Department of Electrical Engineering, College of Engineering, University of Babylon, as a part of requirement for the degree of Doctor of Philosophy in Electrical Engineering \ Electronic and Communications.

Signature:

Name: ***Prof. Dr. Saad S. Hreshee***

Date: / / 2023

I certify that this dissertation mentioned above has been completed in Electronic and Communications Engineering in the college of Engineering\ University of Babylon.

Signature:

Name: ***Prof. Dr. Qais Kareem Omran***

(Head of Electrical Engineering Dept.)

Date: / / 2023

Examining Committee Certificate

We certify that we have read this dissertation entitled (**Generalized Frequency Division Multiplexing System Based on Hybrid-Chaotic Algorithms for Audio Encryption in 5G Networks)**, and as an examining committee, examined that student **(Mohammed Jabbar Mohammed Ameen)** in its contents and that, in our opinion it meets the standard of a dissertation for the degree of Doctor of Philosophy in Electrical Engineering\Electronic and Communication.

Signature:
Name: ***Prof. Dr. Laith Ali Abdul-Rahaim*** (Chairman)
Date: / / 2023

Signature:
Name***: Prof. Dr. Osama Qasim Jumah Al-Thahab*** (Member)
Date: / / 2023

Signature:
Name: ***Prof. Dr. Ehab A. Hussein*** (Member)
Date: / / 2023

Signature:
Name: ***Prof. Dr. Ahmed A. Hamad*** (Member)
Date: / / 2023

Signature:
Name: ***Asst. Prof. Dr. Raed K. Ibrahim*** (Member)
Date: / / 2023

Signature:
Name: ***Prof. Dr. Saad S. Hreshee*** (Supervisor)
Date: / / 2023

Approval of Head of Department

Signature:
Name: ***Prof. Dr. Qais Kareem Omran***
(Head of Electrical Engineering Dept.)
Date: / / 2023

Approval of the Dean of College

Signature:
Name: ***Prof. Dr. Hatem Hadi Obeid***
(Dean of College of Engineering)
Date: / / 2023

Acknowledgments

In the name of **ALLAH**, the Most Gracious and the Most Merciful for giving me the determination and will to complete this research work.

I appreciate the inspirations and guidelines that I have received from my supervisors Prof. Dr. Saad S. Hreshee, for his advice, guidance and encouragement. Without their continuous support and interest, this work would not have been the same as presented here.

I would like to extend my indebtedness to the teaching staff members of the Department of Electrical Engineering, University of Babylon, for their continuing support and fruitful discussion throughout all steps of the research work presented in this dissertation.

Mohammed Jabbar Mohammed Ameen

2023

Table of Contents

Abstract ……. II
Supervisor Certification …… V
Examining Committee Certificate …… VI
Acknowledgements ……... VII
Table of Contents …….. VIII
List of Abbreviations …… XII
List of Symbols…….. XIV
List of Figures ……... XVI
List of Tables …… XIX
List of Publications ……... XXI

Chapter One: Introduction 1
1.1 Overview ……... 1
1.2 General Introduction ……. 1
1.3 Literature Survey …….. 3
1.4 Problem Statement …… 10
1.5 Research Objectives …….. 11
1.6 Dissertation Contributions …… 11
1.7 Organization of Dissertation ……. 12
13

Chapter Two: Principles and Theoretical Approach

2.1 Introduction…… 13
2.2 The Revolution of 5G Wireless Communication Network ……... 13
2.3 GFDM Concepts ……... 15
2.3.1 GFDM Equalization ……. 20
2.3.2 Effects of Pulse Shaping Filters on GFDM waveforms ….. 22
2.4 Massive MIMO Technology ……. 22
2.4.1 Channel Estimation of massive MIMO ……... 23
2.4.2 Massive MIMO Beamforming Configurations …… 24
2.4.3 Massive MIMO Precoding Techniques ……... 25
2.5 Index Modulation for 5G …….. 27
2.5.1 Spatial modulation ……... 27
2.5.2 Parallel spatial modulation …….. 29
2.6 Chaos Theory …… 30
2.6.1 Characteristics of Chaos …….. 31
2.6.2 Lyapunov Exponents (LE) of Chaotic System ……. 31
2.6.3 Type of chaotic system ……. 33
2.6.3.1 Chaotic Flow …… 33
2.6.3.2 Chaotic Maps ……... 33

2.6.4 Hyper-chaos …… 33
2.7 Risks, Threats, and Vulnerabilities in Wireless Communication Networks …….. 38
2.7.1 Security Attacks in Wireless Networks……. 38
2.7.1.1 Passive Wireless Attacks ……... 38
2.7.1.2 Active Attacks …….. 39
2.7.2 Requirements for Security in 5G Wireless Communication Networks ……... 39
2.8 Cryptography …… 40
2.8.1 Cryptography classification ……. 41
2.8.1.1 Secret Key Cryptography ……. 41
2.8.1.2 Public Key Cryptography ……. 42
2.8.2 Physical Layer Security …… 42
2.8.3 Cryptography-Based Chaos Theory …… 44
2.8.4 Benefits and drawbacks of applying chaos theory to cryptography …… 45
2.8.5 DNA Encoding Technique …….. 46
2.8.6 Elliptic Curve Arithmetic Over Finite Field …… 47
2.9 Secure Audio Cryptosystem ……. 49
2.10 Audio Encryption Classifications ……. 49
2.10.1 Time Domain-based techniques ……. 50
2.10.2 Frequency domain-based techniques ……. 50
2.10.3 Two-Dimension based techniques ……. 51
2.10.4 Transform-based techniques ……. 51
2.11 Quality Factors of Secure Audio Encryption System …….. 51
2.11.1 Residual Intelligibility (R.I.)……... 51
2.11.2 Encoding Delay …… 52
2.11.3 Keyspace and key Sensitivity ……. 52
2.12 Secure Audio Assessment Keys …… 52
2.11.1 Subjective Tests ……. 52
2.12.1.1 Figures Observation …… 52
2.12.1.1.1 Waveform Plotting …….. 52
2.12.1.1.2 Histogram analysis ……. 53
2.12.1.1.3 Spectrogram Analysis ……. 53
2.12.1.2 Listeners …….. 53
2.12.2 Objective Tests …….. 54
2.12.2.1 Signal to Noise Ratio …… 54
2.12.2.2 Peak Signal to Noise Ratio …… 54
2.12.2.3 Correlation Analysis ……. 54
2.12.2.4 Linear Predictive Code Distance ……... 55
2.12.2.5 Log Spectral Distance Measure …… 56
2.12.2.6 Frequency Weighted Log Spectral Distance ……. 56
2.12.2.7 Spectral Segment SNR ……. 57

2.12.2.8 Cepstral Distance …….. 57
2.12.2.9 UACI and NSCR Analysis …… 57
2.12.2.10 Root Mean Square and Crest Factor ……... 58

Chapter Three: The Proposed Audio Encryption Techniques 59

3.1 Introduction …….. 59
3.2 Hybrid Chaotic Modulo Operator (HCMO) Encryption Technique …….. 60
3.2.1 Encryption/Decryption algorithm of the proposed HCMO Technique …….. 63
3.3 DNA Coding in the Antenna Index of PSM Encryption Technique …….. 65
3.3.1 Encryption/Decryption Algorithm of the Proposed DNA-AI-PSM Encryption Technique ……. 66
3.4 Audio Encrypted based on Elliptic Curve and Hybrid Chaotic Maps inside GFDM Modulator (HC-EC-GFDM) …… 68
3.4.1 Encryption/Decryption algorithm of the proposed HC-EC-GFDM Modulator Scheme ……... 69
3.5 Audio Encrypted based on Linear Precoding Algorithm of Massive MIMO and Hybrid Chaotic QR-Decomposition …… 71
3.5.1 Encryption/Decryption algorithm of the proposed HC-QR-MMSE System …….. 72

Chapter Four: Simulation Results of the Proposed Cryptosystems 74

4.1 Introduction …….. 74
4.2 Simulation Results of the HCMO Technique…… 74
4.2.1 Subject Test of HCMO Encryption Technique…… 75
4.2.2 R.I. of HCMO Encryption Technique…….. 75
4.2.3 Key Space, Sensitivity, and time Analysis for HCMO Technique …….. 76
4.2.4 Resistance against differential attacks for HCMO Technique …….. 78
4.2.5 Waveforms Plot of HCMO Technique …… 78
4.2.6 Noise Effect on HCMO Technique for massive PSM GFDM System …….. 84
4.2.7 Performance Analysis of HCMO Technique ……... 87
4.3 Simulation Results of DNA-AI-PSM Encryption Technique …... 88
4.3.1 Subject Test of DNA-AI-PSM Encryption Technique …… 88
4.3.2 R.I. of DNA-AI-PSM Encryption Technique …….. 88
4.3.3 Key Space, Sensitivity, and time Analysis for DNA-AI-PSM Technique ……. 90

4.3.4 Resistance against differential attacks for DNA-AI-PSM Technique …….. 92
4.3.5 Noise Effect on DNA-AI-PSM Technique over massive MIMO GFDM System …….. 92
4.3.6 Performance Analysis of DNA-AI-PSM Technique ……. 96
4.4 Simulation Results of HC-EC-GFDM Encryption Scheme …….. 96
4.4.1 Subject Test of HC-EC-GFDM Encryption Scheme …… 96
4.4.2 R.I. of HC-EC-GFDM Encryption Scheme ……. 96
4.4.3 Key Space, Sensitivity, and time Analysis for HC-EC-GFDM Scheme ……. 98
4.4.4 Resistance against differential attacks for HC-EC-GFDM Scheme …….. 99
4.4.5 Noise Effect on HC-EC-GFDM Scheme over massive MIMO PSM System …….. 100
4.4.6 Performance Analysis of HC-EC-GFDM Scheme …… 103
4.5 Simulation Results of HC-QR-MMSE Encryption Technique …. 104
4.5.1 Subject Test of HC-QR-MMSE Encryption Technique ….. 104
4.5.2 R.I. of HC-QR-MMSE Encryption Technique …… 104
4.5.3 Key Space, Sensitivity, and time Analysis for the Proposed HC-QR-MMSE Encryption Technique …… 105
4.5.4 Resistance against differential attacks for the proposed HC-QR-MMSE Encryption Technique …….. 107
4.5.5 Noise Effect on HC-QR-MMSE Encryption Technique over massive MIMO PSM System …… 107
4.5.6 Performance Analysis of HC-QR-MMSE Encryption Technique ……. 110
4.6 R.I Simulation Results Discussion of The Proposed Cryptosystems ……... 111
4.7 Comparing the Studies …….. 112

Chapter Five: Conclusions and Future Works 114

5.1 Conclusions ……. 114
5.2 Suggestions for Future Works ……. 115
Appendix A 116
References 118

List of Abbreviations

1G	First Generation
2G	Second Generation
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
MC	Multicarrier Modulation
MIMO	Multiple-Input Multiple-Output
GFDM	Generalize Frequency Division Multiplexing
OFDM	Orthogonal Frequency Division Multiplexing
OOB	Out-Of-Band
CP	Cyclic Prefix
PAPR	Peak-To-Average Power Ratio
PSD	Power Spectral Density
DFT	Discrete Fourier Transform
IDFT	Inverse Discrete Fourier Transform
BER	Bit Error Rate
ICI	Intercarrier Interference
ISI	Intersymbol Interference
RRC	Root Raised Cosine
RC	Raised Cosine
AWGN	Additive White Gaussian Noise
MF	Matched Filter
ZF	Zero Forcing
MMSE	Minimum Mean Square Error
GS	Guard Symbol
DL	Downlink
UL	Uplink
BS	Base Station
CSI	Channel State Information
FDD	Frequency Division Duplexing
TDD	Time Division Duplexing
PTP	Point to Point
MU	Multi-User
MRT	Maximum Ratio Transmission
EE	Energy Efficiency
SE	Spectrum Efficiency
IM	Index Modulation
SM	Spatial modulation
SM_X	Spatial Multiplexing
GSM	Generalized Spatial Multiplexing
MASM	Multiple Active Spatial Modulation

VGSM	Variable Generalized Spatial Multiplexing
ESM	Enhanced Spatial modulation
QSM	Quadrature Spatial modulation
PSM	Parallel Spatial modulation
SDIC	Sensitive Dependence upon Initial Conditions
LE	Lyapunov Exponents
PLS	Physical Layer Security
IoT	Internet of Things
PRNG	Pseudorandom number generators
ECC	Elliptic Curve Cryptography
LCG	Linear Congruential Generator
DCT	Discrete Cosine Transform
IDCT	Inverse Discrete Cosine Transform
HT	Hadamard Transform
R.I.	Residual Intelligibility
SNR	Signal to Noise Ratio
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
LPC	Linear Predictive Code
FWLOG	Frequency Weighted Log Spectral
SSSNR	Spectral Segment SNR
CD	Cepstral Distance
NSCR	Number of Samples Change Rate
UACI	Unified Average Changing Intensity
RMS	Root Mean Square
CF	Crest Factor
ADC	Analog Digital Converter
DAC	Digital Analog Converter
DNA	Deoxyribonucleic Acid

List of Symbols

K	Number Of Subcarrier
M	Number Of Subsymbols
$d_{k,m}$	Data Symbols
$g[.]_N$	Pulse Shaping Filter
$x[n]$	Transmitted Signal
$h[n]$	Channel Impulse Response
$w[n]$	Additive White Gaussian Noise
$y[n]$	Received Signal
σ_n^2	Noise Variance
σ_d^2	Data Variance
$y_{eq}[n]$	Equalized Received Signal
A	Modulation Matrix
B	Equalization Matrix
I_n	Identity Matrix
$(.)^H$	Hermitian Operator
$(.)^*$	Conjugate Operator
R_{GS}	GS-GFDM Throughput
R_w	W-GFDM Throughput
$w[n]$	Time Window Function
$w_{up}[n]$	Ramp-Up Time Window Function
$w_{down}[n]$	Ramp-Down Time Window Function
N_{CS}	Cyclic Suffix Length
N_{CH}	Channel Impulse Response Length
N_W	Window Transition Length
N_{CP}	Cyclic Prefix Length
N_t	Transmitter Antennas
N_r	Receiver Antennas
H	Channel Matrix
P_{MRT}	Maximum Ratio Transmission Precoding Matrices
P_{ZF}	Zero Forcing Precoding Matrices
P_{MMSE}	Minimum Mean Square Error Precoding Matrices
β	Scaling Power Factor
F_p	Finite Field of P
Mod	Modulus Operator
$\lfloor . \rfloor$	Floor Operator
$\binom{\cdot}{\cdot}$	Number of Combinations
N	Number of Audio Samples
x_i	Original Audio Samples
y_i	Encrypted Audio Samples

R_{xy}	Correlation Coefficient
$E(x)$	Expected Value Of Original Audio Samples
$E(y)$	Expected Value Of Encrypted Audio Samples
σ_x	Standard Deviation Of The Original Audio
σ_y	Standard Deviation Of The Encrypted Audio
$cov(x, y)$	Covariance Between Audios
d_{LPC}	Linear Predictive Code Distance Measure
$v(i, j)$	Normalizing Correlation Coefficients Matrix
p	Filter Order
P	Distance Order
$s(f)$	PSD Of Original Audio
$s'(f)$	PSD Of Encrypted Audio
d_{CD}	Cepstral Distance Measure
d_{LOG}	Log Spectral Distance Measure
d_{FWLOG}	Frequency Weighted Log Spectral Distance Measure
$C_x(i)$	Cpestral Coefficient Of Original Audio
$C_y(i)$	Cpestral Coefficient Of Encrypted Audio
A_i	Amplitude Of Audio
V_{peak}	Peak Value Of Audio
V_{RMS}	Effective Value Of Audio
$\circledast$	Circular Convolution

List of Figures

Figure 2.1	The comparison between OFDM and GFDM block...	16
Figure 2.2	A Comparison of GFDM and OFDM in terms of PSD	17
Figure 2.3	GFDM symbol mapping structure……..	18
Figure 2.4	GFDM scheme structure…….	19
Figure 2.5	The self-interference in the k^{th} subcarrier from neighboring subcarriers……..	19
Figure 2.6	Block diagram of the GFDM receiver……	20
Figure 2.7	Impulse and frequency response of pulse shaping filters …….	22
Figure 2.8	Massive MIMO uplink and downlink……	23
Figure 2.9	Transmission Protocols……..	24
Figure 2.10	PTP-DL massive MIMO link…….	25
Figure 2.11	Schematic diagram of the linear precoding……	26
Figure 2.12	The block diagram of PSM……	30
Figure 2.13	SDIC of Hénon map indicated by X(0) and Y(0)…..	31
Figure 2.14	The LE of such orbits…….	32
Figure 2.15	Behavior of chaotic maps……	37
Figure 2.16	Passive attack……..	38
Figure 2.17	Jammer Attack……	39
Figure 2.18	Process of Cryptography……	40
Figure 2.19	Symmetric encryption scheme……	41
Figure 2.20	Asymmetric encryption scheme…….	42
Figure 2.21	Wiretap channel Model……..	43
Figure 2.22	The comparison between cryptography and PLS approaches……..	44
Figure 2.23	Graphs of the Elliptic curves……..	49
Figure 2.24	Classification of Analog Audio Scrambling Algorithms……..	50
Figure 2.25	Time domain Encryption……	50
Figure 2.26	Correlation coefficient result for audio……..	55
Figure 3.1	The proposed Encryption algorithms in a massive MIMO-PSM-GFDM system……..	60
Figure 3.2	Block diagram of the proposed HCMO encryption Technique……	61
Figure 3.3	Block diagram of the proposed HCMO decryption Technique……	62
Figure 3.4	The proposed HCMO over massive MIMO GFDM cryptosystem……	63
Figure 3.5	Encryption/Decryption algorithm of the proposed HCMO technique over massive MIMO-GFDM system.....	64

Figure 3.6	Block diagram of the proposed DNA-AI-PSM encryption technique.....	65
Figure 3.7	The Proposed DNA-AI-PSM over massive MIMO GFDM cryptosystem.....	66
Figure 3.8	Encryption/Decryption algorithm of proposed DNA-AI-PSM technique over massive MIMO-GFDM system.....	67
Figure 3.9	Block diagram of the proposed HC-EC-GFDM modulator.....	68
Figure 3.10	The proposed HC-EC-GFDM modulator over massive MIMO cryptosystem…….	69
Figure 3.11	Encryption/Decryption algorithm of the proposed HC-EC-GFDM modulator over massive MIMO system……..	70
Figure 3.12	Block diagram of the proposed HC-QR sequence……	72
Figure 3.13	The proposed HC-QR-MMSE over massive MIMO GFDM cryptosystem……...	72
Figure 3.14	Encryption/Decryption algorithm of the proposed HC-QR-MMSE over massive MIMO-GFDM system	73
Figure 4.1	Waveform Results of Audio-1…….	79
Figure 4.2	Waveform Results of Audio-2…….	80
Figure 4.3	Waveform Results of Audio-3…….	81
Figure 4.4	Waveform Results of Audio-4…….	82
Figure 4.5	Waveform Results of Audio-5…….	83
Figure 4.6	Variation of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS and CF, respectively, for the recovered audio-3 of the proposed HCMO Encryption Technique……	87
Figure 4.7	BER performance of authorized and eavesdropper receiver of HCMO technique……..	88
Figure 4.8	Variation of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of the proposed DNA-AI-PSM Encryption Technique…….	95
Figure 4.9	BER of legitimate and eavesdropper receiver for DNA-AI-PSM encryption technique……...	96
Figure 4.10	Variations of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of the proposed HC-EC-GFDM Scheme…….	103
Figure 4.11	BER of authorized and eavesdropper receiver for HC-EC- GFDM Scheme…….	103

Figure 4.12 Variations of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of HC-QR-MMSE Encryption Technique…… 110
Figure 4.13 BER of authorized and eavesdropper the Proposed HC-QR-MMSE Encryption Technique…….. 111

List of Tables

Table 2.1	Equalization matrices…….	21
Table 2.2	Linear Precoding matrices……..	26
Table 2.3	Spatial Modulation types ……...	29
Table 2.4	List of Chaotic Maps …….	34
Table 2.5	DNA XOR Operation…….	46
Table 2.6	DNA coding rules……..	46
Table 2.7	DNA Addition Operation……...	46
Table 2.8	DNA Subtraction Operation……..	47
Table 3.1	Simulation parameters……	62
Table 4.1	Audio parameters……...	74
Table 4.2	R.I. in terms of SNR, PSNR, and SSSNR for HCMO Technique……	75
Table 4.3	R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for HCMO Technique……	75
Table 4.4	R.I. in terms of MSE, RMS, CF and R_{xy} for HCMO Technique……	76
Table 4.5	Key Space of Chaotic Maps used in HCMO Technique……	76
Table 4.6	Key sensitivity test of HCMO using audio-3……..	77
Table 4.7	Time analysis for HCMO Technique……..	77
Table 4.8	UACI and NSCR analysis for HCMO Technique…...	78
Table 4.9	R.I. in terms of SNR, PSNR, and SSSNR for DNA-AI-PSM Technique…….	89
Table 4.10	R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for DNA-AI-PSM Technique…….	89
Table 4.11	R.I. in terms of MSE, RMS, CF and R_{xy} for DNA-AI-PSM Technique……..	89
Table 4.12	Key Space of Chaotic Maps used in DNA-AI-PSM Technique……	90
Table 4.13	Key sensitivity test of DNA-AI-PSM Technique using audio-3……..	91
Table 4.14	Time analysis for DNA-AI-PSM Technique……..	91
Table 4.15	UACI and NSCR analysis for DNA-AI-PSM Technique……	92
Table 4.16	R.I. in terms of SNR, PSNR, and SSSNR for the HC-EC-GFDM scheme…….	97
Table 4.17	R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for the HC-EC- GFDM scheme……	97
Table 4.18	R.I. in terms of MSE, RMS, CF and R_{xy} for the HC-EC-LCG-GFDM scheme……	97
Table 4.19	Key Space of the proposed HC-EC-GFDM scheme…	98

Table 4.20	Key sensitivity examination of HC-EC-LCG-GFDM scheme using Audio-3……	98
Table 4.21	Time analysis for the HC-EC-GFDM scheme……	99
Table 4.22	UACI and NSCR analysis for HC-EC-GFDM Scheme……	99
Table 4.23	R.I. in terms of SNR, PSNR, and SSSNR for the HC-QR-MMSE Encryption Technique…….	104
Table 4.24	R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for the HC-QR-MMSE Encryption Technique…….	104
Table 4.25	R.I. in terms of MSE, RMS, CF and R_{xy} for the HC-QR-MMSE Encryption Technique…….	105
Table 4.26	Key Space of the proposed HC-QR-MMSE Technique……	105
Table 4.27	Key sensitivity test Proposed HC-QR-MMSE Encryption Technique using audio-3……..	106
Table 5.28	Time analysis of the proposed HC-QR-MMSE Encryption Technique…….	106
Table 4.29	UACI and NSCR analysis for HC-QR-MMSE Encryption Technique…….	107
Table 4.30	Comparisons between proposed cryptosystems and previous works using Audio-3……	113

List of Publications

The following papers were published while this dissertation was being prepared.

1. M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic Modulo Operator Encryption Technique for Massive Multiple Input Multiple Output Generalized Frequency Division Multiplexing system," International Journal on Electrical Engineering and Informatics, vol. 14, no. 2, 2022.
2. M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic Based Encrypted Audio Transmission via Massive MIMO - GFDM system using DNA Coding in the Antenna Index of PSM," 5th International Conference on Engineering Technology and its Applications (IICETA) pp. 19-24, 2022.
3. M. J. M. Ameen and S. S. H. Hreshee, "Securing Physical Layer of 5G Wireless Network System over GFDM Using Linear Precoding Algorithm for Massive MIMO and Hyperchaotic QR Decomposition," International Journal of Intelligent Engineering and Systems, vol. 10, no. 6, pp. 5932–5939, 2022.
4. M. J. M. Ameen and S. S. H. Hreshee, " Security Analysis of Encrypted Audio based on Elliptic Curve and Hybrid Chaotic Maps within GFDM Modulator in 5G Networks" Bulletin of Electrical Engineering and Informatics, vol. 12, no. 4, 2023.

Chapter One

Introduction

1.1 Overview

This chapter outlines an overview of the study, reviews the literature, and explains the significance of encryption based on chaos theory in data transmission. It provides the last information of literature that constitutes this dissertation basis. The literature review also includes proper techniques and algorithms for current cryptography systems. After establishing the research problem, the study motivation and objectives are defined. Finally, the chapter has concluded the outline of the dissertation chapters.

1.2 General Introduction

The development of 5G wireless communications has resulted in a significant increase in data transfer and massive growth in the number and types of mobile programs. When data are transmitted in the public wireless channel, they are exposed to passive attacks that affect the security of the information represented by the authenticity, confidentiality, and integrity of data, which is a major concern. Consequently, data must be encrypted on many systems before being sent to provide security [1].

Communications security based on chaos theory has emerged as a new subject in wireless communication research in recent years due to its providing the strongest approaches to protect data that travel through insecure channels. The chaos signal is deterministic, aperiodic, nonlinear, and long-term prediction. Since it is highly sensitive to initial conditions and control parameters, no two chaotic systems will develop identically. The chaotic system is classified into one-dimensional and multidimensional based on the number of positive Lyapunov exponents in the chaos system. Multidimensional chaotic systems are more complex and unexpected than

one-dimension because of their numerous control parameters and initial conditions [2, 3].

The production of unpredictable amounts, large enough and random enough, is necessary for the security of the majority of known cryptographic systems. Pseudo-random number generators (PRNG) can be generated using elliptic curves. Elliptic Curve Cryptography (ECC) is a public-key algorithm that is significant in cryptography. Because ECC has a small key space and offers a similar level of protection to other public-key algorithms that use larger key spaces, additionally, it provides higher security levels while utilizing less computational power, memory, and bandwidth [4, 5]. Deoxyribonucleic Acid (DNA) cryptography is a modern and simple security technique that is characterized by faster computations, large capacity, and high-power savings. The combination of DNA cryptography with chaotic sequence will create a highly secure system [6]

Audio-based communication is increasing in the administrative, military, and various aspects of life. Audio has distinct characteristics, structure, and format from images and texts. The encryption process guards the data against being accessed or destroyed by unofficial parties. The silent portion of the audio is filled with noise signals during encryption, so only a legitimate receiver can determine the audio content [7].

Massive Multiple-Input-Multiple-Output (MIMO) is an interesting wireless technique for meeting 5 G's requirements by maximizing capacity, throughput, and reliability. In order to improve the spectral efficiency of the transmission system, massive MIMO allows attaching thousands of device antennas to one base station. Also, Spatial Modulation (SM) scheme is employed with a 5G network to exploit some information resources in transmission [8]. The parallel SM (PSM) divides the transmitted antennas

into subgroups, and SM is then carried out independently in each group using similar signal constellations [9].

Furthermore, a massive MIMO must integrate with a multi-carrier scheme to deal with the frequency-selective channels in 5G wireless networks. Generalized frequency division multiplexing (GFDM) is a promising new waveform for multi-carrier design and is regarded as a generalized form of orthogonal frequency division multiplexing (OFDM) because it is more adaptable to the parameter selection process. Arranging the data in a two-dimensional time-frequency block minimizes the number of cyclic prefixes (CP) compared to valuable information [10]. The combination of massive MIMO-GFDM is very attractive to meet the ever-increasing needs for higher link readability and spectrum efficiency in 5G wireless communication networks [11].

1.3 Literature Survey

Several algorithms for audio encryption based on chaos have been proposed in previous studies. However, it has shortcomings and limitations, such as inequity between encrypted and recovered voice, an increased value in correlation coefficient, increased encryption/decryption time, small key space, high computational processing, high Residual Intelligibility (R.I.), and slow processing speed. The highlights and evaluation of some literature reviews are as follows:

E. Mosa et al. in 2010 [12] proposed a voice encryption technique based on the permutation and masking principles of voice samples using three private keys generated by baker map in both times and transform domains. At the same time, a second secret key is the inversing of the main (first) key, while the third secret key is created using the main key after splitting it into two reversed parts. The audio randomization is conducted using circular shifts using the main secret key and then masked. Discrete Cosine/Sine Transform

(DST/DCT) is applied, and the permutation and masking are performed by the second key. In the last stage, applying IDST/IDCT and the permutation and masking performed by the third key.

S. M. Alwahbani and E. B. Bashier in 2013 [13] introduced a voice encryption method using a Circle map and Logistic maps. The locations of the speech signal segments are moved about using the indices of the ordered created sequence of the circle map. Then, a one-time pad produced by the logistic map is utilized for the diffusion phase. The security metrics results are key space=10^{84}, correlation coefficient = 0.0043, SNR= –14.009 dB, P.Diff.= 99.92% and processing time = 0.79 seconds.

N. R. Raajan et al. in 2013 [14] proposed a secure OFDM scheme using chaotic interleaving to improve security and enhance audio transmission performance. Chua chaotic flow was used to interleave the audio samples and then XORed with the chaotic flow before applying IFFT. BER plotted in this work to show improvement in the system.

M. Ahmad et al. in 2014 [15] proposed a new chaotic sequence by utilizing high-dimensional systems such as Lorenz and Chen to scramble audio. The generated sequence is more complex and unexpected and has six chaotic sequences. The system generates a cryptographically strong encryption keystream through the quantization and mixing processes. The experimental security test results explain that the generated keystream has high randomness and is effective for audio encryption.

A. Mostafa et al. in 2015 [16] presented an audio encryption algorithm using substitution and permutation principles. The audio samples were transformed using the DST/DCT. The 2D logistic and Henon maps are used to substitute coefficients of DST/DCT, while the Baker map performs the

permutation process. The cryptosystem was limiting in SNR to -3.025 dB and d_{lpc} to 0.7253.

X. Zhang et al. in 2015 [17] suggested a secure OFDM based on chaotic maps. The phase rotation of 16-QAM is performed using a Logistic map, and the subcarrier mapping of OFDM is performed using the segmented logistic map. The proposed method presented a good BER performance.

H. N. Abdullah et al. in 2015 [18] presented an efficient, secure, and immune against channel noise communication network using feedback from the Lorenz system to encrypt audio samples. The simulation results obtained d_{LPC}= 0.9725, SSSNR= -19.7017 dB, d_{CD}= 3.9531, and MSE of noise is reduced from 0.1 to 0.02 at SNR=10 dB, which indicates a good security level.

A. Mahdi and S. S. Hreshee in 2016 [19] suggested that voice encryption utilizes XOR operation between input audio and Henon map using Analog-to-Digital Converter (ADC), threshold, and comparator methods to convert the Henon sequence into bits. The comparator method is the best to give more bits and hence more security-level. This work presented a good d_{lpc} of about 4.336 and moderate d_{CD} to 7.097, and it has limits in SSSNR to -4.2272 dB and suitable key space reach to 2^{427}.

H. 2016 Liu et al. in 2016 [20] suggested a dual-channel voice encryption algorithm that uses a chaotic sequence with variable multi-scroll to produce key streams that confuse and diffuse voice segments. The one-time keys, such as initial values of state variables, scroll numbers, and initial iteration times of the chaotic system, depend on both external keys and hashing value of the voice to increase the randomness of the chaotic trajectory. A modest correlation coefficient characterizes the system at 0.004, a low key space reaching 2^{268}, and not considering encryption/decryption time.

A. Mahdi et al. in 2016 [21] presented a security system based on a duffing map to encrypt speech samples. The proposed encryption algorithm was examined in the domains of time, frequency, two-dimensional, analog, and digital. The results show that the best values are: d_{lpc} =5.082 and d_{cd}=6.996 in the digital domain, whereas SSSNR=-4.2272 dB in the analog domain.

H. A. Ismael and S. B. Sadkhan in 2017 [22] introduced audio encryption using Chen, Lorenz, and Henon chaotic maps. Each of these maps is converted to the digital domain by an IEEE 754 converter, combined using linear and nonlinear functions to provide the secret key needed to encrypt the clear audio. The speech signal's highest confusion is caused by using three chaotic maps to construct the secret key. This work has key space=2^{480}, correlation coefficients = 0.38339, and SSSNR=-16.723 dB.

E. A. Albahrani in 2017 [23], proposed a voice encryption system using a combination of a block cipher and chaotic maps. The cryptosystem divided the voice into blocks of size 625 bytes, and each of them passes through three stages: Permutation, XOR-Adding, and Substitution. The permutation process is performed using a chaotic Tent map. Then the resulting block is XORed with the key block generated by the Chebyshev polynomial, and the last stage is to substitute the block depending on the multiplication inverse. This cryptosystem presented a good Correlation coefficient with a low key space of 2^{319} and a very slow speed of encryption, reach to 10.4 sec./KB.

P. Sathiyamurthi and S. Ramakrishnan in 2017 [24] proposed a chaotic voice encryption technique by permuting voice samples based on the Chen map and then separating samples into four levels according to sample value and permuting-substituting each using Logistic, Tent, Quadric, and Bernoulli maps. The security tests are correlation coefficient =0.0119, NSCR=99.99%, and UACI =33.3218.

F. Farsana and K. Gopakumar in 2017 [25] presented voice encryption based on the principle of confusion and diffusion by using logistic and Duffing chaotic maps. The voice samples are masked by the key generated by the logistic map, and the encryption voice is under permutation process by Duffing map. DCT compresses the voice scrambles to minimize residual intelligibility. The work's simulation findings are SNR= -7.76 dB, correlation coefficient = 0.00613, and key space=2^{192}, demonstrating that the encryption algorithm produces voice samples with little residual intelligibility, strong key sensitivity, and high-quality decrypted voice signal.

S. S. Hreshee et al. in 2018 [26] presented an audio security communication system based on chaos theory in two phases. The first phase is chaotic scrambling using the logistic map, while the second is chaotic masking using the Lorenz system. The security evaluations are d_{LPC}=0.9998, SSSNR=-20.7803 dB, and d_{CD}=4.2583.

K. Kordov in 2019 [27], introduced an audio encryption algorithm based on permutation-substitution by pseudo-random generators that were generated using a chaotic circle map and rotation equations. This work has a limitation in key space = 2^{149}, SNR = -16.04 dB, and correlation coefficient = 0.004794, which can consider an insufficient security level.

A. M. Raheema et al. in 2020 [28] proposed a speech scrambling using five separate chaotic sequences, including the Logistic, Baker, Hénon, Rössler, and Lorenz systems, which convert to binary, then mixed with speech samples and transmitted over 64-QAM OFDM modulation. The security tests yield of the speech encryption for this system is d_{LOG}= 14.54150, d_{LPC}= 0.97410, d_{CD}= 8.85030, SSSNR= -26.5060 dB, and d_{FWLOG}= 20.99760.

R. I. Abdelfatah in 2020 [6] proposed three stages of voice encryption combining chaotic maps, DNA encoding, and SHA-512. The first stage is performed by self-adaptive bits encryption by applying SHA-512 to input

voice to get the first private key which uses employed cyclic shift of the input voice bits to reduce correlation coefficients between voice samples. The second stage generates a pseudo-random sequence (second private key) using a specific design combining Sine, Chebyshev, and Logistic chaotic maps with DNA encoding. The third stage is to generate a third private key by a specific design between Henon, Logistic and Gaussian maps with DNA encoding and AND-XOR gates to combine the third and second stages. The security evaluations for audio-6 are histogram ,spectrogram , time representation , correlation coefficient = 0.0004, UACI=36.22%, NSCR=100%, SNR=-29.96 dB speed=190×10^{-6} sec./KB, RMS=0.6038 ,CF=4.3817 and key space=2^{928} .

E. A. Hussein et al. in 2020 [29] proposed an audio security system based on two-stage chaotic masking using the Lorenz and Rössler chaotic systems. The purpose of this technique is to increase the key space and decreases the residual intelligibility of the audio transmitted over the AWGN channel. The simulation results are d_{LPC}=0.9751, SSSNR=-21.5620 dB, d_{CD}=3.9661, and key space=10^{15}.

P. Sathiyamurthi and S. Ramakrishnan in 2020 [30] introduced an audio encryption technique using the FFT and a combination of chaotic maps named (3D) Lorenz-Logistic map to minimize residual intelligibility and increase the quality of decrypted audio. The input audio is applied to FFT to get real and imaginary parts. The chaotic output sequences are used to permute and substitute real and imaginary parts and then apply IFFT. Eight private keys were obtained by mixing the Lorenz-Logistic map. The security system's performance was plotted using a histogram and Spectrogram, demonstrating a large key space and improved correlation coefficient to 0.0312, NSCR = 99.978, and UACI=33.341.

D. Shah et al. in 2021 [31] presented a voice encryption technique based on elliptic curve arithmetic operations. The proposed method creates several substitution boxes by employing a higher-order Galois field. The security metrics are correlation coefficient =-0.001, RMS=0.7654, CF=4.087, histogram, Spectrogram, and time analyses reflecting that this method is robust, secure, and appropriate for voice encryption requirements.

R. I. Abdelfatah et al. in 2021 [32] presented ECC to encrypt voice samples. The suggested algorithm is based on the ECC, 2D Logistic, Lorenz chaotic map, and hash function. The main feature of ECCs, a small key space, is utilized to get a high-security level compared to other algorithms. Several security tests are obtained (for Audio-3) correlation coefficient =-0.0015, UACI=33.33%, NSCR=99.99%, SNR=-9.484 dB, and processing time=68.8 seconds, guaranteeing high performance and security.

T. Bonny et al. in 2022 [33] introduced an audio cryptosystem using traditional cryptography methods with two stages of a chaotic masking algorithm and employing a unified hyperchaotic system to enhance security. Several security measurements proved the proposed cryptosystem's high specificity and resistance to various cryptographic threats.

S. Mokhnache et al. in 2022 [34] proposed a secure voice transmission algorithm based on the nonlinear combination of Logistic and Cubic maps to confuse and diffuse voice samples. The security measurements obtained are SNR=-11.8293 dB, correlation coefficient = -0.0002537, and Spectrogram, which show the effectiveness of the proposed cryptosystem.

According to the survey study above, It is evident that numerous encryption criteria are still not fulfilled or require to improve, such as:

1. The speed of encryption/decryption techniques should be compatible with 5G wireless network requirements.

2. Design a new hybrid chaotic algorithm to enhance security and implement it in different locations of communication networks to increase randomness against eavesdroppers.
3. Simple implementation of encryption audio techniques to substitute and permute audio samples to minimize residual intelligibility of encrypted audio.

1.4 Problem Statement

This dissertation deals with the problem of providing cryptographic techniques of secure audio transmission compatible with high-speed wireless networks that can deliver powerful security warranties for many applications in the military and civilian. Most conventional secure ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), are not appropriate for quick real-time encryption of large volumes of data. The security of traditional wireless communication also depends primarily on the higher layer encryption, whereas the physical layer information has not been well safeguarded. Therefore, the research problems statement is as follows:

1- The security issues of the GFDM system are not taken into account.
2- High residual intelligibility tests of encrypted audio.
3- It did not consider the importance of the location of the encryption algorithm within the communications system.
4- High processing time of encryption-decryption algorithm.
5- It did not exploit the wireless MIMO channel properties such as noise and fading.

1.5 Research Objectives

Numerous security techniques required by pervasive applications are provided by using cryptographic algorithms, such as protecting data transfer against attacks. However, the current cryptographic techniques might not satisfy 5G requirements, such as big data and high speed. Therefore, the challenge concerns finding powerful cryptographic techniques to guarantee secure data transmission in the 5G infrastructure and should provide an optimization trade-off between security level, cost, and performance. The main objectives of this work are as follows:

1- Securing the GFDM system against eavesdroppers based on hybrid chaotic algorithms.
2- Minimizing Residual Intelligibility and high reconstructed audio signal quality.
3- Applying encryption algorithms inside the communications components system to increase randomness.
4- Reducing the required time for the encryption-decryption process.
5- Encrypt data with the help of environmental conditions of the wireless channel.

1.6 Dissertation Contributions

The literature analysis shows that many encryption requirements remain unfulfilled yet and need improvement to be compatible with 5G wireless networks. Therefore, the following is a list of the contributions made by this work:

1. A new algorithm of secure audio transmission based on hybrid chaotic maps with a combination of DNA encoding and ECC, suitable for 5G network requirements, has been developed to increase security levels.

2. New approaches were proposed inside communication components (PSM modulator, GFDM modulator, and channel precoding of massive MIMO channel), which makes hardness for the eavesdropper prediction the position, types, and algorithm of chaotic maps used to discover the original audio.
3. A new hybrid chaotic sequence with the help of QR decomposition has been designed to increase randomness and key space.
4. Minimal residual intelligibility and high reconstructed audio signal quality have been obtained.
5. The performance analysis and security tests of the proposed cryptosystems were studied over the wireless channel at a different signal-to-noise ratio (SNR).
6. Proposed cryptosystems have obtained good chaotic behavior, high key sensitivity, large key space, low calculation cost, and fast encryption-decryption processing.

1.7 Organization of Dissertation

This dissertation is organized into five chapters, including the introduction chapter,

Chapter 2 describes the concepts of GFDM modulation and 5G wireless network requirements. Also, explain the features of a massive MIMO system and spatial modulation. In addition, chaos theory is clarified with its properties and types of chaotic sequences. Highlights vulnerabilities in wireless communication networks, the cryptography concept, and the advantage of encryption in the physical layer based on chaos theory. In addition, it presents ECC and DNA coding principles. The technical audio tests used to determine the encryption quality are displayed in the last of this chapter.

Chapter 3 describes the design of the proposed audio cryptosystems and encryption-decryption process within PSM-GFDM-massive MIMO wireless networks.

Chapter 4 presents the simulation results of the proposed audio encryption algorithms. Compares the results and discusses the proposed cryptosystems with past studies to evaluate the weakness and strong points.

Chapter 5 concludes the study reported in this dissertation and offers ideas for future research to be improved.

Chapter Two

Principles and Theoretical Approach

2.1 Introduction

This chapter presents the basic concepts of the GFDM scheme with its features and how to implement it in the 5G wireless network. The significant role of the massive MIMO system and spatial modulation in increasing the spectral efficiency of the wireless system is also explained in this chapter. Also, chaotic behavior is clarified in detail with its properties and types. In addition, vulnerabilities in wireless communication networks, types of attacks, security services, concepts of cryptography using chaos theory in the physical layer, Elliptic curve arithmetic, DNA coding, key factors of audio encryption, classifications of audio encryption, and concludes with an encrypt audio evaluation**.**

2.2 The Revolution of 5G Wireless Communication Network

Mobile communications have become vital tools for contemporary society. Communication needs to become personal instead of being fixed to particular places. The first generation (1G) cellular networks only supported voice communication. The audio has been digitalized in the second generation (2G) to improve system capacity, device battery life, and Quality of Service. In addition, it launched the Short Message Service, which completely changed how people communicate. The third generation (3G) made it possible for mobile Internet connection, and its data rates were comparable to wired networks. The fourth generation (4G) is moving towards even higher throughput due to the emergence of smartphones equipped with high capabilities of storage, high-speed processing data, high-definition (HD) displays, and cameras, together with social media that allowed users to turn from media consumers to content producers [35].

The evolution of the Fifth Generation (5G) wireless networks is driven by requests for high-speed communications and reliability. The capacity of 5G wireless networks should be at least 1000 times greater than that of 4G. Also, spectral efficiency (SE) increased ten times compared to 4G, corresponding to a maximum data rate of 10 Gbps for low mobility consumers and 1 Gbps for high mobility consumers [36]. The 5G communication network can deal with a collection of services, each having several requirements, like the Internet of Things (IoT) applications [37].

The 5G networks employ Multiple-Input Multiple-Output (MIMO) techniques to exploit its benefits, such as high data rate, enhanced robustness, and the increased degree of freedom of multiuser interference [38]. In addition, Multi-carrier Modulation (MC) schemes have been widely used for broadband wireless communications to meet the 5G needs. The main reason for this usage is because they have attractive qualities, including support for multiuser diversity, easier equalization, adaptive modulation, robustness against multipath channels, and simplicity of implementation [39].

2.3 GFDM Concepts

GFDM is a digital and generic multi-carrier modulation technique with pulse shaping, and it satisfies the different requirements of 5G networks. GFDM represents a non-orthogonal modulation method carried out on separate time-frequency blocks, each of which contains a collection of subcarriers in frequency and subsymbols in time. By circularly shifting in the time and frequency domain, the subcarriers on each subsymbol are filtered with applications that require a prototype filter. This approach will eliminate unwanted out-of-band (OOB) radiation and pave the way for spectrum distribution to succeed. Also, GFDM provides additional properties in terms of reducing Inter-carrier and inter-symbol interferences by using CP and pulse shaping. Furthermore, the time-frequency grid layout

necessitates highly adaptable sophisticated methods in the receiver to achieve demodulating activities [40].

A single CP is utilized for the whole block in GFDM, even if it contains multiple subsymbols, whereas one CP should be used for every subsymbol in OFDM, raising the overhead as shown in Figure 2.1 a. Therefore, GFDM outperforms OFDM in terms of spectral efficiency (SE) [37]. OFDM has a considerably high peak-to-average power ratio (PAPR). It could be decreased by raising the subcarrier's bandwidth and decreasing the number of subcarriers. When designing GFDM and OFDM with the same length, as seen in Figure 2.1 b, the subcarriers become wider, and the block has lower subcarriers, lowering the PAPR in the GFDM block [35].

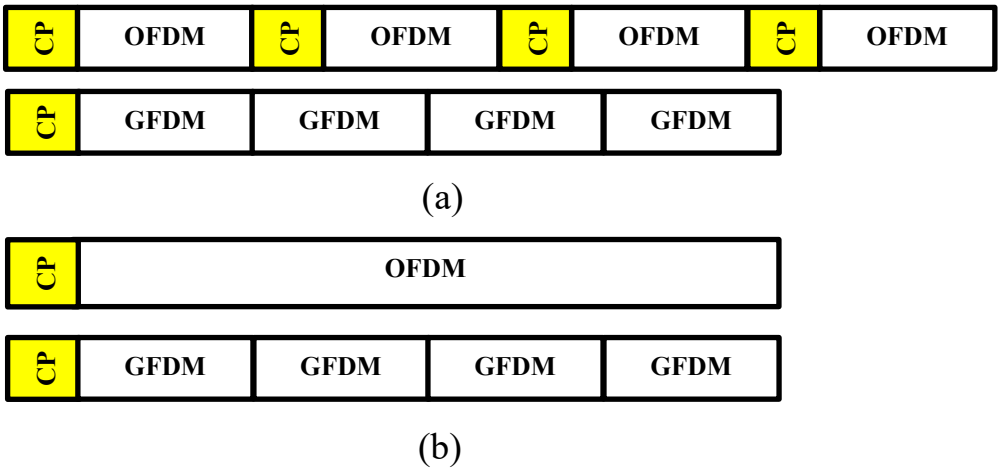


Figure 2.1 The comparison between OFDM and GFDM block (a) CP saving by GFDM (b) lowering PAPR in GFDM more than OFDM [37]

The Power Spectral Density (PSD) of multi-carrier modulation depends on transmitted signal operations: inverse discrete Fourier transform (IDFT), CP, and pulse shaping filtering. A pulse shaping filter is used to minimize the radiation. Therefore, each subcarrier in GFDM is individually formed with a filter, as shown in Figure 2.2, which allows for major improvements in spectral properties [10, 41].

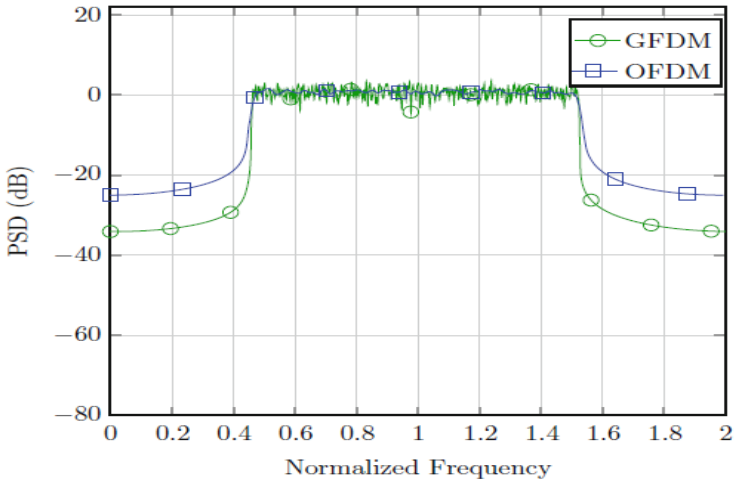


Figure 2.2 A Comparison of GFDM and OFDM in terms of PSD [37]

The time-frequency resource grid of GFDM is shown in Figure 2.3, where $d_{k,m}$ are data symbols (modulated), K and M denote the numbers of subcarriers and subsymbols, respectively. There are KM sample locations in each resource block. As a result, if KM=N is met, the quantity of information transmission by GFDM will equal the amount of transmission data for OFDM across the same symbol time and bandwidth. A pulse-shaping filter is used to identify the position of each resource block. The mathematical formula for the GFDM signal is as follows:

$$X[n] = \sum_{k=0}^{K-1} \sum_{m=0}^{M-1} d_{k,m}\, g[\langle n - mK \rangle_N]\, e^{j2\pi \frac{nk}{K}} \tag{2.1}$$

In Equation (2.1), $g[\langle n - mK \rangle_N]$ is the pulse shaping filter with mK time-shifting. The GFDM modulator and demodulator are described in Figure 2.4. Equation (2.1) can simplify to OFDM when M = 1 and the rectangular pulse shaping filter is used; similarly, Equation (2.1) can convert to the single carrier transmission in the case of K = 1; therefore, this method is known as GFDM [42]. The types of GFDM waveforms have appeared in Appendix A.

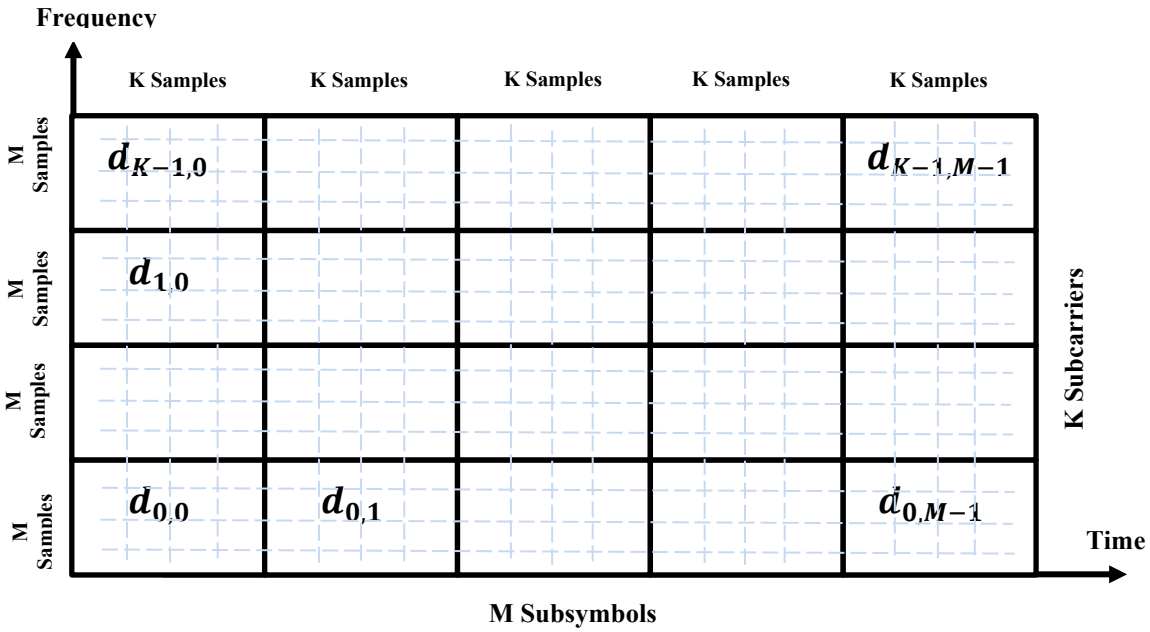
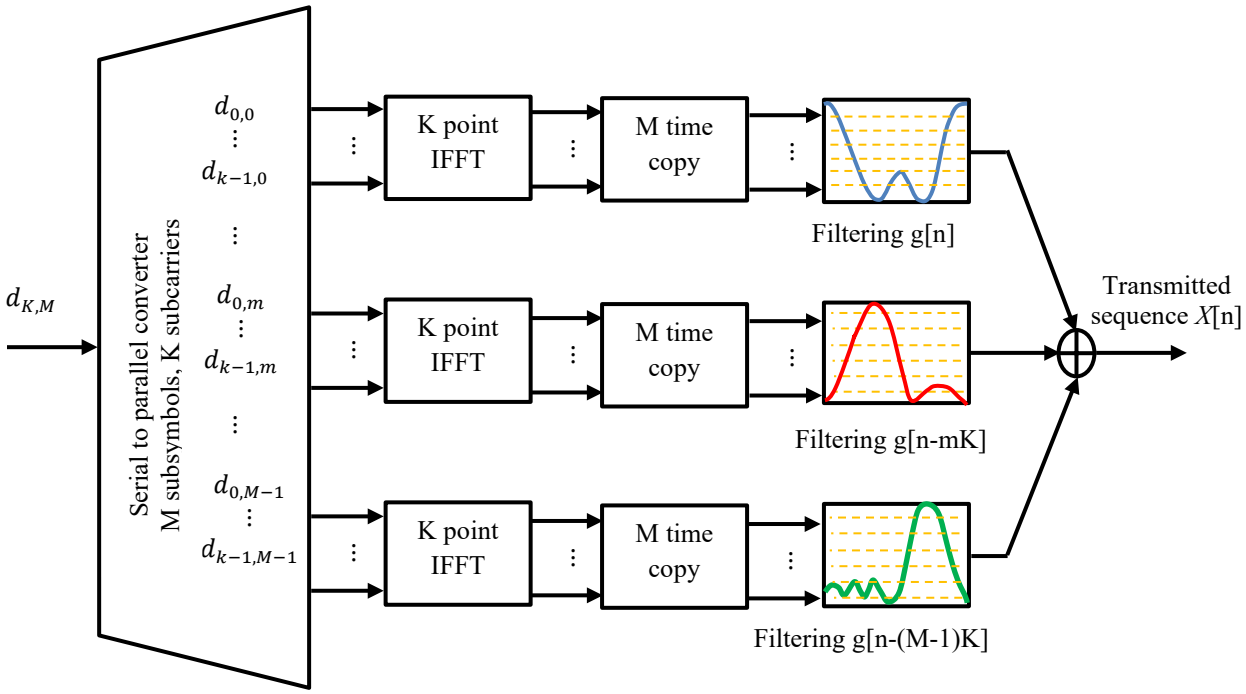
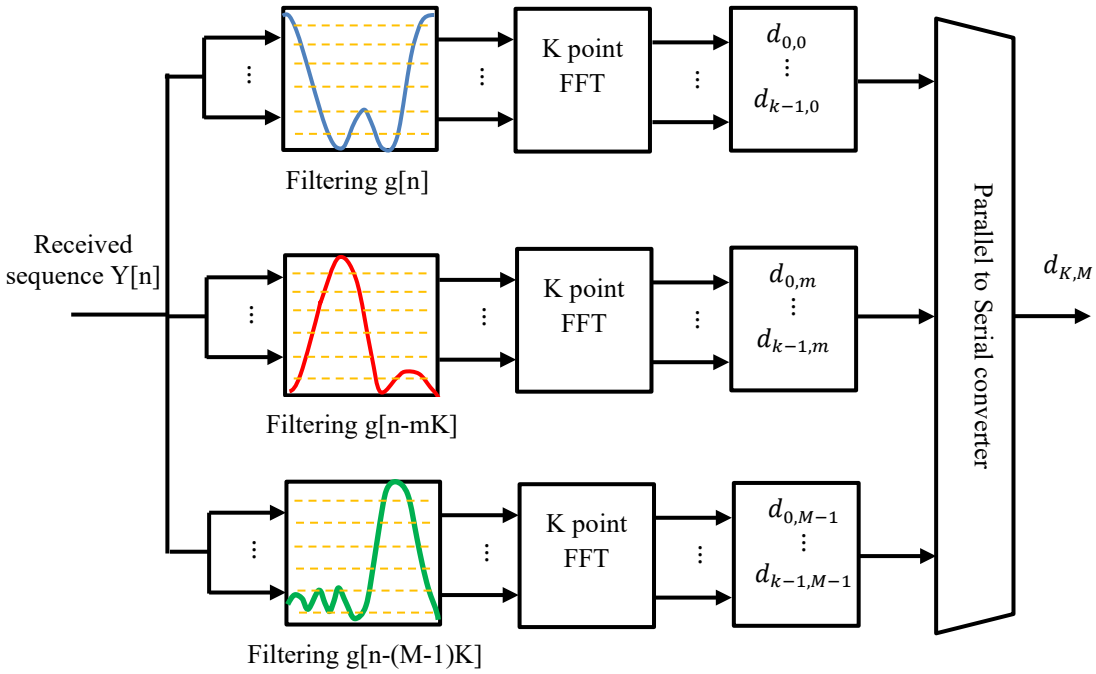


Figure 2.3 GFDM symbol mapping structure [42]



(a) GFDM modulator



(b) GFDM demodulator

Figure 2.4 GFDM scheme structure [42]

As previously stated, the pulse shaping filters have caused GFDM to lose the orthogonality between subcarriers. Because of this, self-interference arises, which leads to an increased bit error rate (BER) compared to OFDM. In the frequency domain, Figure 2.5 illustrates how the data on the Kth subcarrier interferes with neighboring subcarriers. Only neighboring subcarriers interfere when Root Raised Cosine (RRC) filters are employed as transmit and receive filters, leading to intercarrier interference (ICI). This interference is the main reason why GFDM is worse than OFDM in terms of BER performance [43].

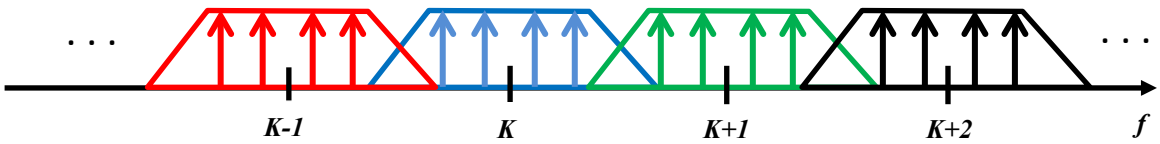


Figure 2.5 The self-interference in the k^{th} subcarrier from neighbouring subcarriers [43]

2.3.1 GFDM Equalization

The key feature of the GFDM scheme is the employment of a circular pulse shaping filter due to its benefits comprise preserving the GFDM signal's time compactness and increasing signal processing complexity. As in Equation (2.1), adding the CP protects the GFDM signal from multipath propagation. Supposing that the CP size is greater than the impulse response of the channel, as shown in Figure 2.6, the received signal following the removal of the CP is defined by:

$$y[n] = x[n] \circledast h[n] + w[n] \tag{2.2}$$

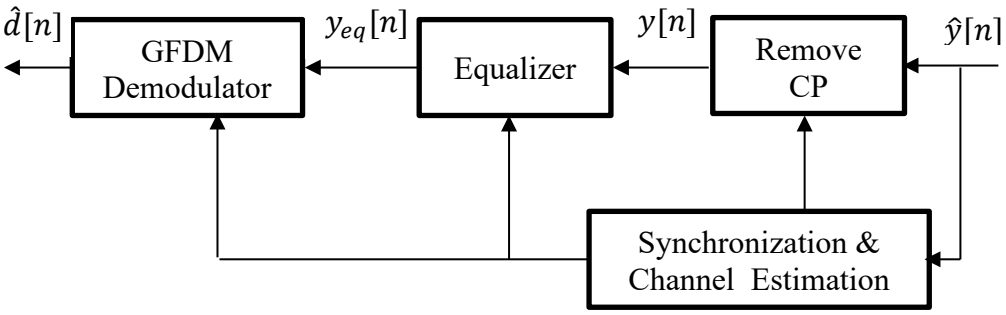


Figure 2.6 Block diagram of the GFDM receiver [37]

Where $\circledast$ indicates the circular convolution, $h[n]$: impulse response of the channel ,$w[n]$: additive white Gaussian noise (AWGN) with variance σ_n^2. After the process of synchronization and channel estimation, equalization is employed to compensate for the impact of the multipath propagation, resulting in an equalized received signal $y_{eq}[n]$.To extract the data symbols, various receive filters can be utilized and designing linear GFDM receivers using matrix notation, and the modulation matrix can be structured according to:

$$A = [g_{0,0} \cdots g_{K-1,0} \cdots g_{0,1} \cdots g_{0,M-1} \cdots g_{K-1,M-1}] \tag{2.3}$$

Data symbols (KM) are organized for the GFDM block to the (K×M) matrix as follows:

$$D = \begin{bmatrix} d_{0,0} & \cdots & d_{0,M-1} \\ \vdots & \ddots & \vdots \\ d_{K-1,0} & \cdots & d_{K-1,M-1} \end{bmatrix} = [d_{c,0}, d_{c,1}, \dots d_{c,M-1}] = \begin{bmatrix} d_{r,0} \\ d_{r,1} \\ \vdots \\ d_{r,K-1} \end{bmatrix} \quad (2.4)$$

The GFDM transmitted vector is represented by:

$$x = Ad \quad (2.5)$$

Where the vector d is created by placing D columns following each other.

The transmitter prototype filter causes a non-orthogonality between subcarriers, indicating that the modulation process can produce intersymbol interference (ISI) and ICI between data symbols. Therefore, the GFDM demodulator must be capable of dealing with self-interference to reduce the influence on the BER performance. The procedure for demodulation might be achieved as follows:

$$\hat{d} = By_{eq} \quad (2.6)$$

Where B denotes the equalization matrix, the demodulation of the GFDM signal can be performed in various ways depending on the transmit matrix, as shown in Table 2.1. SNR is maximized by the Matched filter (MF) equalizer, but self-interference cannot be eliminated. The Zero Forcing (ZF) equalizer can reduce interference but increases noise. Considering SNR, the minimum mean square error (MMSE) equalizer maintains a proper balance between MF and ZF. Additionally, because the MMSE already includes the channel matrix, equalization is not required prior to the demodulation [37] [44].

Table 2.1. Equalization Matrices **[37]**

MF	$B_{MF} = A^H$
ZF	$B_{ZF} = A^{-1}$
MMSE	$B_{MMSE} = (\frac{\sigma_n^2}{\sigma_d^2} I_n + A^H A)^{-1} A^H$

Where $[.]^H$ Hermitian operator, I_n identity matrix, and σ_d^2 data variance

2.3.2 Effects of Pulse Shaping Filters on GFDM waveforms

The amount of energy emitted outside the specified bandwidth (B) is known as OOB radiation. The main source of high OOB radiation is the sidelobes of the subcarriers. So, selecting a pulse shaping filter strongly influences the OOB radiation and BER performance of the GFDM waveform. Circular pulse shaping filters commonly employed in the GFDM scheme are: root-raised cosine (RRC), raised cosine (RC), Xia pulse, Gaussian pulse, and Dirichlet pulse. The impulse and frequency response of pulse shaping filters are illustrated in Figure 2.7. In the next subsections, two appropriate strategies are described in order to increase the effectiveness of pulse shaping in minimizing OOB radiation [37].

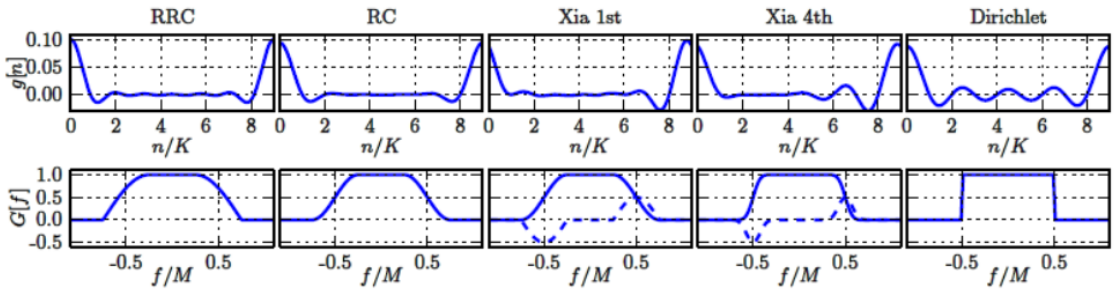


Figure 2.7 Impulse and frequency response of pulse shaping filters [35]

2.4 Massive MIMO Technology

The massive MIMO technology is the most attractive for 5G and future networks. It is an evolution of the MIMO techniques now utilized in networks, which comprise hundreds of transmitting antennas at the base station (BS) and provide service to multiple users simultaneously. Massive MIMO antennas will aid in concentrating energy into a smaller area to enhance SE and throughput. When the number of antennas increases, the transmitted beams narrow and focus on the specified user. The spatially concentrated antenna beams enhance throughput for the particular user and minimize interference to the neighboring user. In massive MIMO, there are two different channel transmission modes: uplink (UL) and downlink (DL),

as depicted in Figure 2.8. In UL mode, the information and the pilot sequence are transmitted from the user to the BS via a channel, while in DL mode, the channel estimation and transmitting data between the BS and user will be done utilizing the pilot sequence.

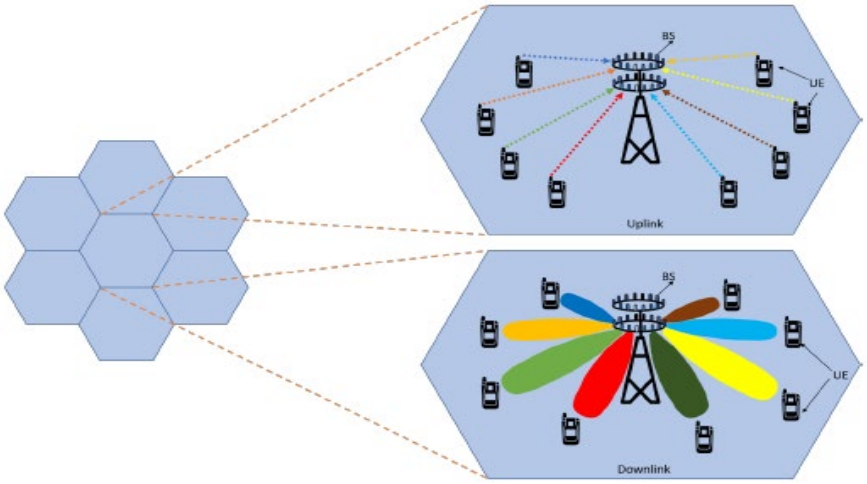


Figure 2.8 Massive MIMO uplink and downlink [8]

2.4.1 Channel Estimation of massive MIMO

Massive MIMO system depends on Channel State Information (CSI) to detect and decode the received signal. CSI provides information on the status of the communication link between the transmitter and the receiver, including any effects of fading, scattering, and other effects that may be present. When the CSI is ideal, the performance of the massive MIMO system rises linearly as the number of transmitter and receiver antennas increases.

In addition, there are two transmission protocols in a massive MIMO system: Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD), as shown in Figure 2.9. In the FDD system, CSI must be calculated during both DL and UL modes. During the UL mode, the channel estimation is performed by BS with the aid of a pilot sequence transmitted by the user equipment. Furthermore, during DL mode, the BS transmits the pilot sequence to the user equipment, and the user acknowledges the channel

information estimated for DL transmission. Further, for massive MIMO with an FDD-DL system, the channel estimate approach becomes extremely complicated and impractical to use in real-world scenarios.

The issue with DL transmission in the FDD system is resolved by the TDD system. In TDD, by utilizing the channel reciprocity characteristic, the BS can calculate the DL channel information with UL channel information. During UL, the user equipment transmits the pilot sequence to the BS, and according to this pilot sequence, the BS can calculate the CSI to the user equipment [8].

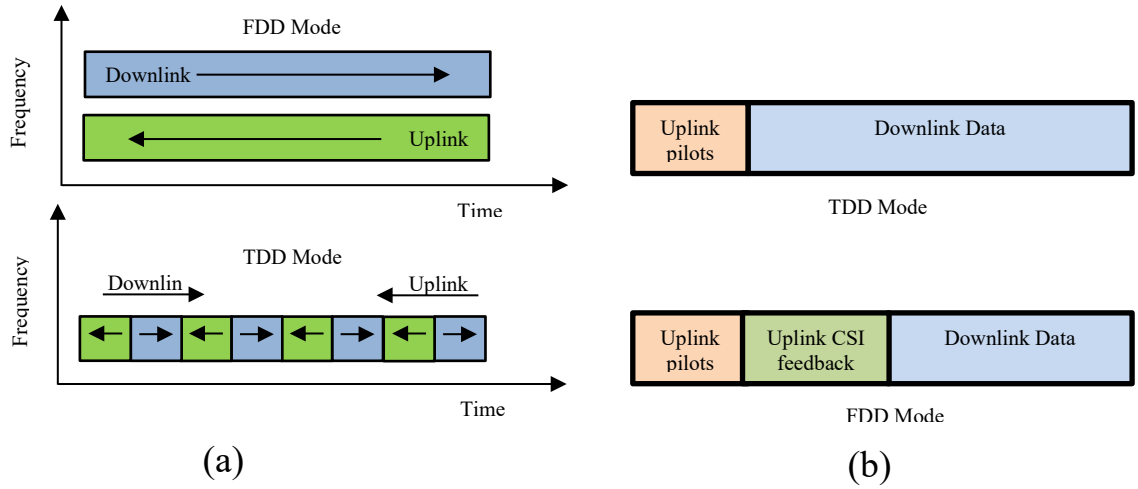


Figure 2.9 Transmission protocols (a) FDD and TDD transmission mode (b) Pilot transmission and CSI feedback mechanism in FDD and TDD [8].

2.4.2 Massive MIMO Beamforming Configurations

Beamforming is a method that makes it possible to concentrate the signal from several antennas into a single powerful beam while reducing energy at the transmitter side. Beamforming at the receiver is a type of spatial multiplexing in which the signals are combined to add up in one direction while refusing the signals arriving from any other direction and treating them as interference. The classifications of MIMO beamforming configurations are as follows:

- Point-to-Point MIMO (PTP): in this configuration, each antenna on the transmitter terminal will only connect to a single antenna on the receiver

terminal, as depicted in Figure 2.10. To enhance the data rate without expanding the bandwidth, several antennas are installed on the transmitter and receiver sides. PTP systems generally assume a slow-fading, frequency-flat channel. In this thesis, the PTP configuration will be used.

- Multiuser MIMO (MU-MIMO): where a BS and severalusers' equipment communicate simultaneously. As a result, MU-MIMO may require low-cost and energy-saving hardware elements at the BS [45].

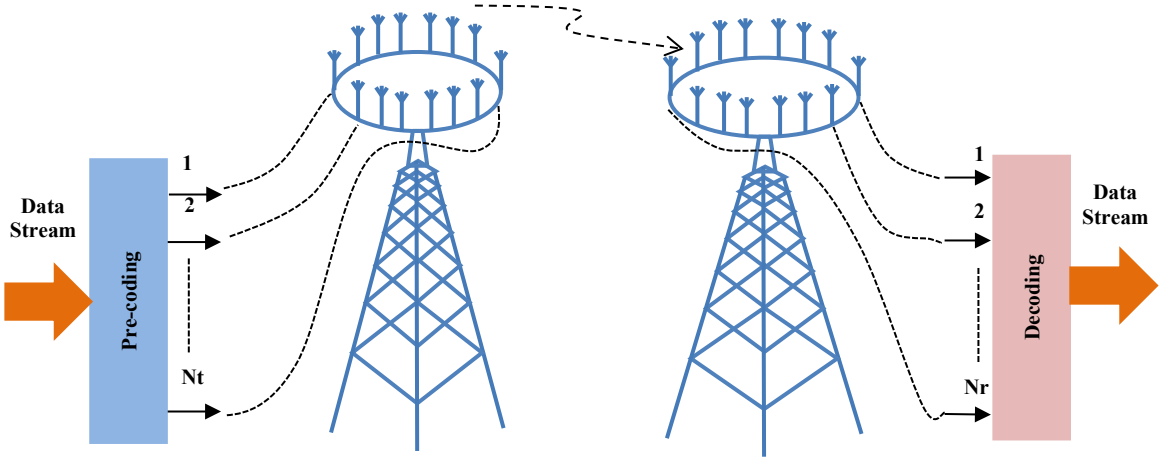


Figure 2.10 PTP-DL massive MIMO link [45]

2.4.3 Massive MIMO Precoding Techniques

The key feature of a massive MIMO system is a precoding technique that converts the complexity of the system from the receiver terminal to the BS with the aid of powerful signal processing techniques, as shown in Figure 2.11. Generally, in a real wireless transmission scenario, the performance of DL transmission mainly relies on CSI, making it difficult to obtain a reliable CSI. The precoding technique can be used to deal with non-ideal CSI.

Massive MIMO precoding methods take different forms. A brief explanation of linear precoding will be given in this thesis. Let the number of transmitter and receiver antennas be $N_t \geq N_r$, respectively, then the transmitted signal in DL mode can be described by:

$$x = \sqrt{\rho}\, Pa, \qquad x \in C^{N_t \times 1} \tag{2.7}$$

Where $P \in C^{N_t \times N_r}$ is a feedforward matrix of linear precoding, $a \in C^{N_t \times 1}$ is the vector transmitted before the precoding procedure, and $\sqrt{\rho}$ is the transmitted power.

P is related to the channel matrix (H). Furthermore, the precoding methods usually include a matrix inversion operation in the P matrix, which increases computational complexity.

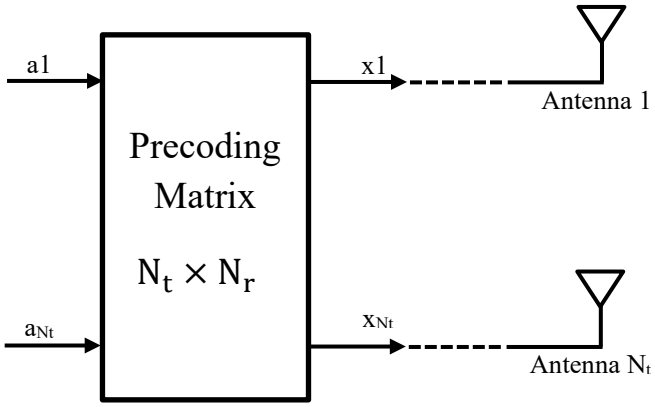


Figure 2.11 schematic diagram of the linear precoding [46]

Various algorithms, such as Maximum Ratio Transmission (MRT), ZF, and MMSE, can be applied to deal with the matrix inversion process. The mathematical expressions of each are listed in Table 2.2. The MMSE algorithm outperforms ZF and MRC in the wide range of SNR values, while in the low SNR values, MRT is better than ZF and vice versa in the high SNR values.

Table 2.2 Linear Precoding matrices

MRT	$P_{MRT} = \sqrt{\beta} H^*$
ZF	$P_{ZF} = \sqrt{\beta} H^* (H^T H^*)^{-1}$
MMSE	$P_{MMSE} = \sqrt{\beta} H^* (H^T H^* + \sigma_n^2 I_n)^{-1}$

Where β is a scaling power factor, σ_n^2 is the noise variance, and I_n is the identity matrix. So, the received vector in TDD-DL mode becomes [46, 47]:

$$y = H^T x + w$$

$$y = \sqrt{\rho}\, H^T P a + w, \qquad y \in C^{N_r \times 1} \tag{2.8}$$

2.5 Index Modulation for 5G

The 5G wireless network must improve spectrum efficiency (SE), greater energy efficiency (EE), and mobility due to the fast growth of mobile data services and the increasing use of smartphones. Unfortunately, the MIMO-based modulation techniques currently in use cannot meet these 5G criteria. Traditional MIMO can achieve high SE with many antennas, but EE is reduced due to the scaled power consumption of several RF chains. Recently, index modulation (IM) approaches have appeared as an attractive candidate to satisfy 5G standards [48].

IM is a simple digital modulation scheme with high SE and EE, which uses the building block indices of the communication systems to transmit extra information. IM systems offer alternate methods of information transfer, in contrast to conventional digital modulation techniques, which depend on the amplitude, phase, and frequency of a sinusoidal carrier signal. On the other hand, IM opens entirely new ways of data transmission. The indices of the building blocks can be employed to convey information via an on/off keying technique, the IM technique can transfer the saved transmission power from the inactive to the active transmit entities, and this leads to an improved BER performance compared with conventional techniques that use the same transmission energy [49].

2.5.1 Spatial Modulation (SM)

SM and its versions belong to the group of IM, which involves transmitting extra data bits via active transmit antenna indices. Since SM methods have been shown to balance SE and EE successfully, they can replace spatial multiplexing (SM_X) in wireless devices more effectively. In the SM technique, for each time instant, a single antenna is activated to send the modulated symbol. In particular, the incoming bits are split into two groups. The first group of bits is mapped to transmit the antenna index, and

one antenna is activated. The second group of bits is mapped to a traditional M-ary modulation. When enabling a single transmitting antenna, SM eliminates numerous drawbacks of traditional MIMO systems, such as ICI and the need for multiple RF chains. The main problems with SM are: the total number of transmit antennas must be a power of two, which is the first drawback, while the second drawback is lower SE when compared to a traditional MIMO system because its SE increases logarithmically with modulation order and the number of transmitting antennas.

Generalized SM (GSM) overcomes SM limitations by activating several transmit antennas simultaneously. There are several transmit antenna combinations available depending on the number of active antennas at any one time. Multiple transmit active antennas can be chosen based on combinations of the number of transmitting antennas. Even if more antennas can be activated, the impact of ICI is reduced by sending the same signal from every activated transmit antenna.

Multiple Active Spatial Modulation (MASM) is an extension of GSM to improve SE further. In MASM, multiple transmit antenna combinations can transmit different modulated symbols simultaneously. The BER performance of MASM is high due to ICI.

Variable GSM (VSGM) is also an extension of GSM to improve SE. In VSGM, the number of transmitting antennas can be changed from one to all antennas and transmit the same signal constellations.

One or two transmit antennas are activated simultaneously in the Enhanced SM (ESM) technique. When a single transmit antenna is active, higher-order modulation is employed. When two transmit antennas are active, a lower modulation order is applied, whose order is half the order of the higher modulation order.

Quadrature SM (QSM) scheme can enhance SE and BER performance. The modulated signal is partitioned into real and imaginary

parts, and each part is transmitted from a different antenna (one antenna for an in-phase part and one for a quadrature part). As a type of SM, the indices of both activated antennas transmit extra information bits. The major drawback of QSM is that the total number of transmit antennas should be a power of two [50]. The parallel SM (PSM) splits the total transmit antennas into equal-sized groups, and the traditional SM is independently achieved in each group using the same constellation signal. The PSM design can increase SE while keeping the transmitter simple. In other words, a single RF chain can be used to build the PSM system for each group [9]. The mathematical description of SM techniques mentioned previously is listed in Table 2.3, where N_T represents the total number of antennas, N_A is the number of activated antennas, $\binom{N_T}{N_A}$ represents the number of combinations , $\lfloor . \rfloor$ indicate to floor operator ,M modulation order ,and P number of group.

Table 2.3. Spatial Modulation types [50]

Scheme	SE (bps/Hz)	Number of active antennae (RF chain)
SM	$log_2(N_T M)$	1
GSM	$\left\lfloor \log_2 \binom{N_T}{N_A} \right\rfloor + log_2(M)$	$< N_T$
MASM	$\left\lfloor \log_2 \binom{N_T}{N_A} \right\rfloor + N_A\ log_2(M)$	$< N_T$
VGSM	$N_T - 1 + \ log_2(M)$	1 to N_T
ESM	$log_2\left({N_T}^2 M\right)$	1 or 2
QSM	$log_2\left({N_T}^2 M\right)$	1 or 2
PSM	$P \times log_2(g) + log_2(M)$	P

2.5.2 Parallel spatial modulation (PSM)

The working principle of PSM can be summarized in the following steps [9]:

1. The transmitter antennas are partitioned into P equal-sized groups, the size of each one $g=N_T/P$, where $2 \leq g \leq N_T$ and only one transmitter antenna is activated for each group individually. Therefore, SM can be regarded as a special case of PSM when P=1 ($g=N_T$).
2. As illustrated in Figure 2.12, the information to be transmitted is divided into (P+1) sets of bits, with the first part consisting of $log_2(M)$ bits, and the subsequent P parts consisting of $log_2(g)$ bits.
3. The signal constellation is achieved by applying the first part of the bits. Then, SM is applied in parallel for each group independently, with the same signal constellation being used.

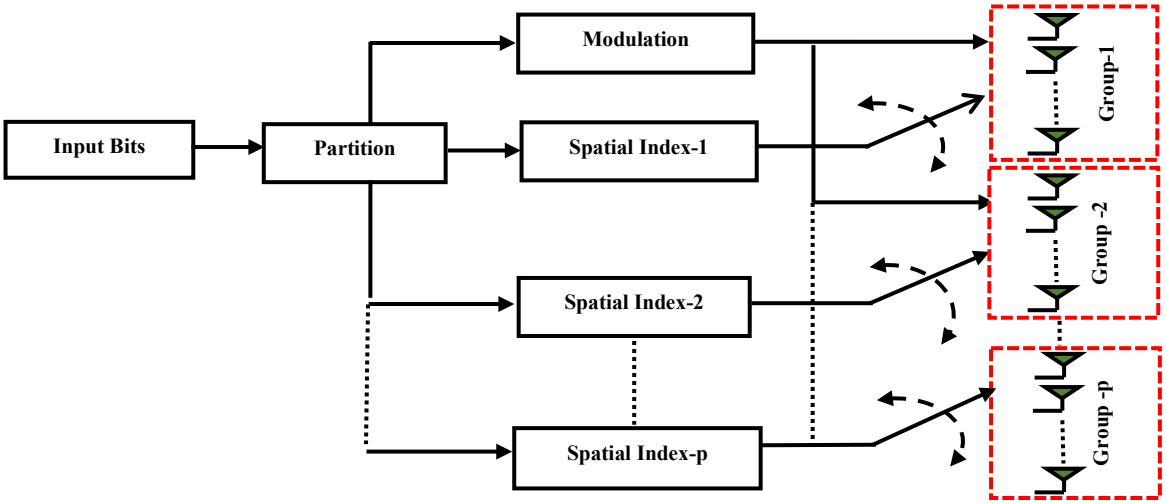


Figure 2.12 The block diagram of PSM [9]

2.6 Chaos Theory

Chaos theory is a mathematical area of research that describes nonlinear, dynamical, and complex systems that are apparently random but deterministic. Chaos theory deals with the study of deterministic difference differential mathematical equations that exhibit sensitive dependence upon initial conditions (SDIC) by producing time pathways that appear random. Even if a tiny variation in measuring the system's state causes decreased predictability, this will make long-term prediction by any method useless. Chaos theory can be applied in various scientific disciplines [51, 52].

2.6.1 Characteristics of chaos

The main characteristics of chaos are:

I. **Nonlinearity**. When it is linear, it is impossible to be chaotic.

II. **Determinism**. It has fundamental principles that must adhere to all future states of the system (as opposed to probabilistic).

III. **SDIC**. A very small change in the initial conditions can result in drastically different behavior in the end state.

IV. **Irregularity**. A continuous irregularity in thesystem's behavior

V. **Long-term prediction**. It is almost impossible to know, which can only be known with limited accuracy [53].

2.6.2 Lyapunov Exponents (LE) of Chaotic System

The key idea of any chaotic system is that it is highly SDIC and deterministic. High SDIC is a rapid phase space divergence of the two paths (trajectories or orbits), beginning from an extremely small difference in initial conditions. The time series of the Hénon map, as seen in Figure 2.13, illustrates this phenomenon. The chaotic system can be predicted precisely if the initial conditions are known [54].

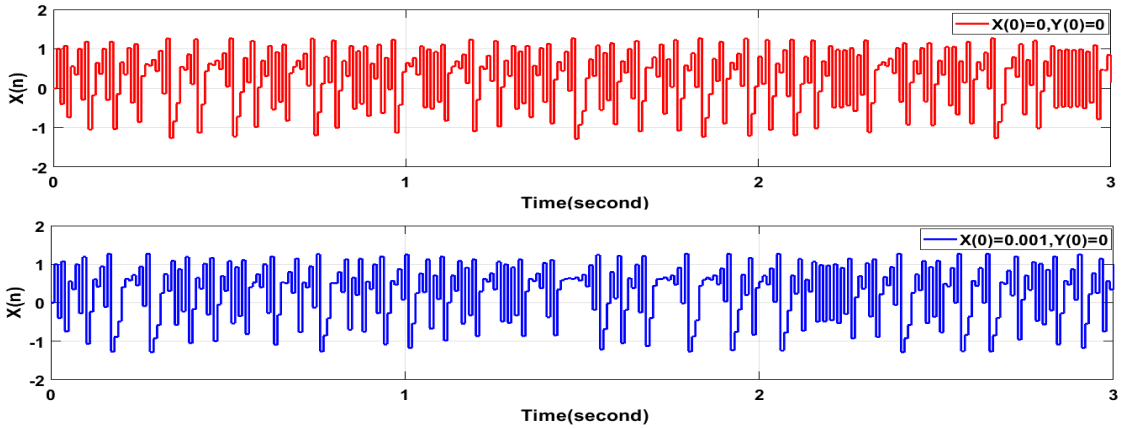


Figure 2.13 SDIC of Hénon map indicated by X(0) and Y(0)

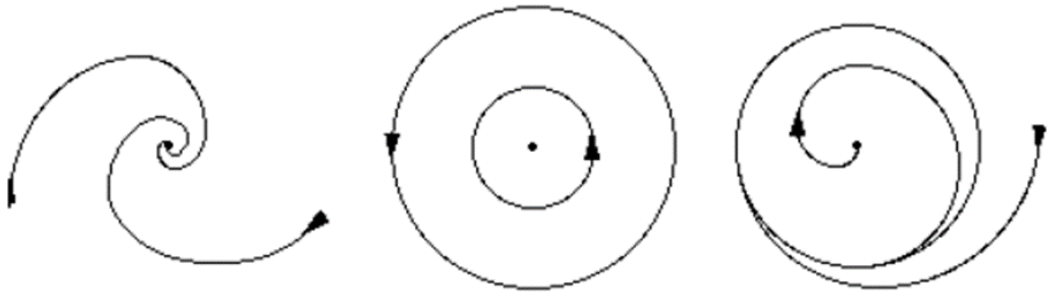
The LE represents the natural characteristics of a particular system. LE may be the most effective diagnostic tool for identifying whether the system is chaotic or not. LE can be conceptualized as the logarithmic rate of

convergence or divergence of two neighboring points of two-time series J_n and K_n separated by an initial distance $\Delta w_o = \|J_o - K_o\|_2$ [6]:

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln \left| \frac{\Delta w_i}{\Delta w_o} \right| \tag{2.9}$$

When determining the LE value, three probable scenarios are:

1. LE < 0.It means that the system is stable (non-chaotic), and its orbit is attracted to a fixed point or periodic.
2. LE = 0. It means that the system is in steady-state mode, and the orbit is a neutral fixed point (non-chaotic).
3. LE > 0. It means that the orbit is unstable and has chaotic behavior. No matter how close together they are, nearby points will diverge at any random distance; Figure 2.14 illustrates the LE with various values of such orbits[55].



LE < 0	LE = 0	LE > 0
attracting fixed point	attracting orbits	neutral fixed point

Figure 2.14 The LE of such orbits [55]

The number of LE of any chaotic sequence is equal to its number of dimensions. However, the largest LE is the most significant because it decides whether or not the sequence is chaotic. For example, one dimension (1D) logistic map has one positive LE. The 2D Henon map has two LE, positive and negative. Additionally, the 3D Lorenz system has three LE: positive, negative, and zero [54].

2.6.3 Type of chaotic system

The chaotic systems can be classified into two categories: one represented by difference-equations and referred to as maps, and the other one represented by differential equations often referred to as flows. Chaotic system dynamics behavior is described using the time domain called time series or in phase space called a strange attractor [54].

2.6.3.1 Chaotic Flow

The chaotic flow system is formed from a group of differential equations so that it can be regarded as a continuous time system. The strange attractor of chaotic flow is called a trajectory, which is characterized by a uniform and continuous nature. Numerous well-known chaotic flow systems exist, like the Lorenz, Rössler, Chua, and Nien systems.

2.6.3.2 Chaotic Maps

The chaotic map is formed from a set of difference-equation and can be considered a discrete-time system. In this thesis, several chaotic map types are used, and a description of each type is in Table 2.4 and Figure 2.15.

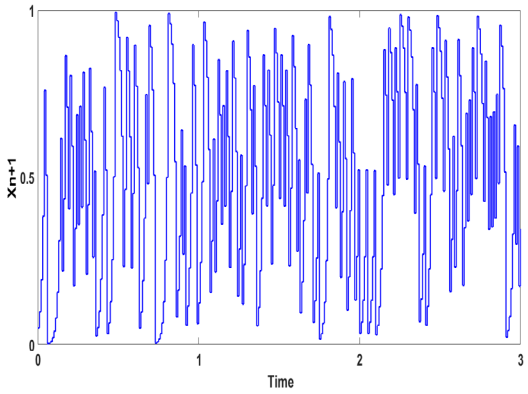
2.6.4 Hyper-chaos

In a hyperchaotic system, there is more than one positive LE. As a whole, the hyperchaotic system is more disorganized than the conventional chaos system, and hyper-chaotic systems feature more complex topological structures and behaviors than traditional chaotic ones. Recently, several scientific and engineering societies have begun to pay more attention to hyper-chaos. However, it is well recognized that a conventional chaotic system has significant drawbacks for such technological applications since it only contains one positive LE, which means that its degree of disorder is not large and because its orbits are somewhat periodic [56].

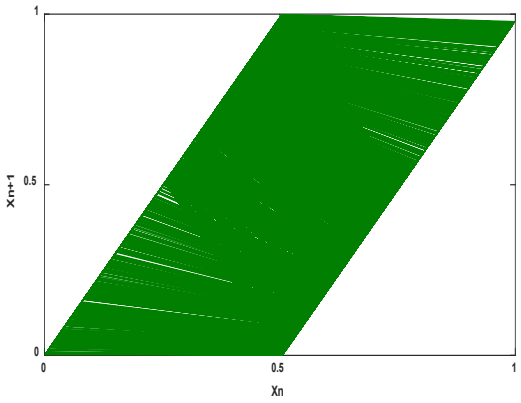
When mixing two or more types of chaotic maps, a chaotic hybrid map can be created with a more complicated chaotic property than the majority of single chaotic maps and more SDIC. Furthermore, the hybrid approach takes advantage of all the strengths of the combined chaotic maps and attempts to reduce the weakness of one of the weak chaotic maps as much as possible [57, 58].

Table 2.4. List of Chaotic Maps

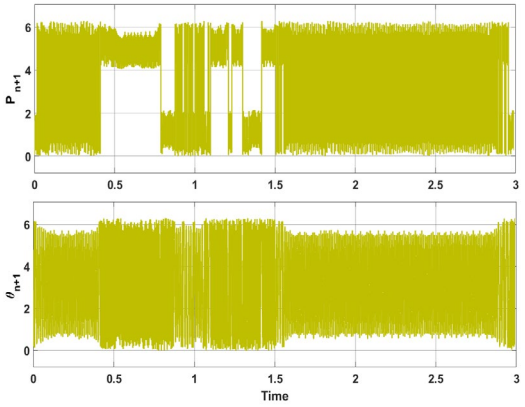
Chaotic Maps	Time domain	Equations	Number of space Dimensions	Parameter values and Initial condition
Bernoulli [59]	Discrete	$X_{n+1} = \begin{cases} 2\mu X_n, & 0 \le X_n < 0.5 \\ 2\mu(1-X_n), & 0.5 \le X_n < 1 \end{cases}$	1	$X(0) \in [0-1]$ $\mu \in [0-1]$
Standard [60]	Discrete	$P_{n+1} = P_n + K\sin(\theta)\ Mod(2\pi)$ $\theta_{n+1} = \theta_n + P_{n+1}\ Mod(2\pi)$	2	$P(0) = 0;\ \theta(0) = 0.1$ $K \in [0-5.19]$
Bogdanov [61]	Discrete	$X_{n+1} = Y_{n+1} + X_n$ $Y_{n+1} = Y_n + \epsilon Y_n + kX_n(X_n - 1) + \mu X_n Y_n$	2	$X(0) = 0.9$; $Y(0) = 0.37;$ $\mu = -0.02;$ $\epsilon = -0.17; k = 1.2$
Henon [6]	Discrete	$X_{n+1} = 1 + Y_n - aX_n^2$ $Y_{n+1} = bY_n$	2	a= 1.4, b = 0.3 and X (0)=Y (0)=0
Logistic [6]	Discrete	$X_{n+1} = rX_n(1-X_n)$	1	3.57≤ r ≤4 and 0.5< X(0) <1
Tinkerbell [62]	Discrete	$X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n$ $Y_{n+1} = 2X_nY_n + cX_n + dY_n$	2	a = 0.9, b =-0.6013, c=2,d=0.5, $X(0)$ = 0.72, $Y(0)$ =-0.64
Duffing [21]	Discrete	$X_{n+1} = Y_n$ $Y_{n+1} = -bX_n + aY_n - Y_n^3$	2	$a = 2.75; b = 0.2$ $X(0) = -1.7$ $Y(0) = -1$
Ikeda [63]	Discrete	$X_{n+1} = 1 + u(X_n\cos t_n - Y_n\sin t_n)$ $Y_{n+1} = u(X_n\sin t_n + Y_n\cos t_n)$ $t_n = 0.4 - \frac{6}{1+X_n^2+Y_n^2}$	2	$X(0) = Y(0) = 0$ $u = 0.708$
Tent [24]	Discrete	$X_{n+1} = \begin{cases} \mu X_n, & X_n < 0.5 \\ \mu(1-X_n), & X_n \ge 0.5 \end{cases}$	1	$X(0) = 0.4$ $\mu = 1.9$



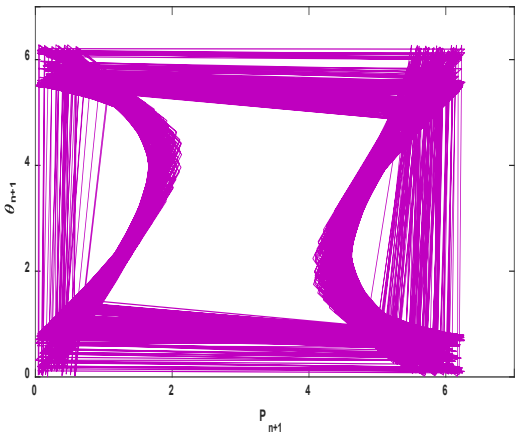
A



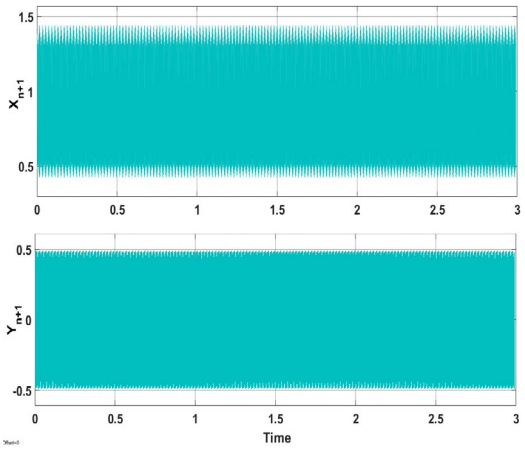
B



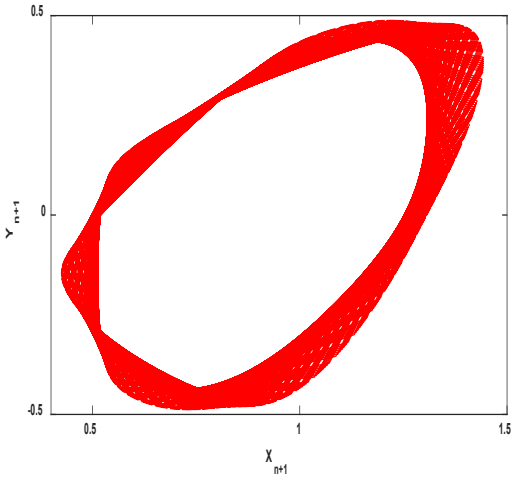
C



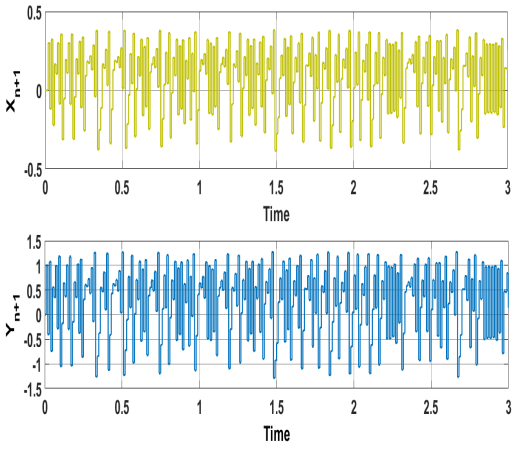
D



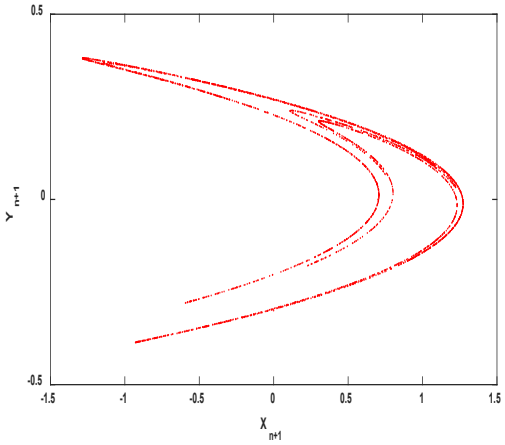
E



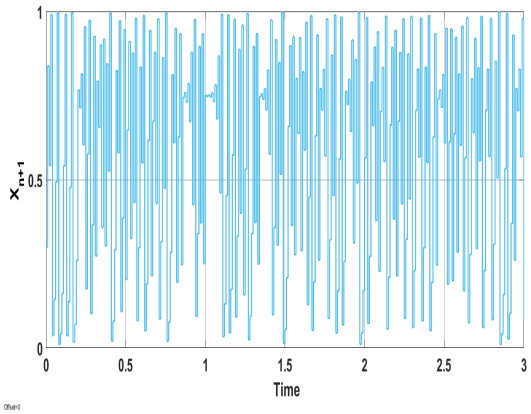
F



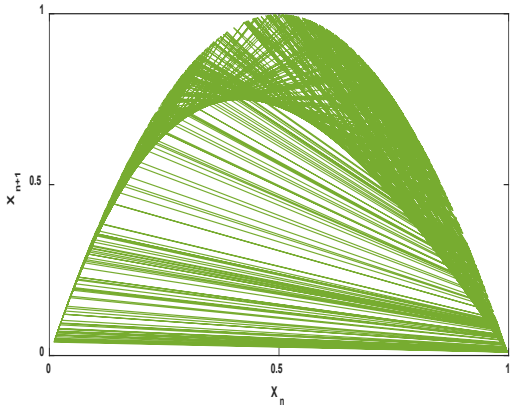
G



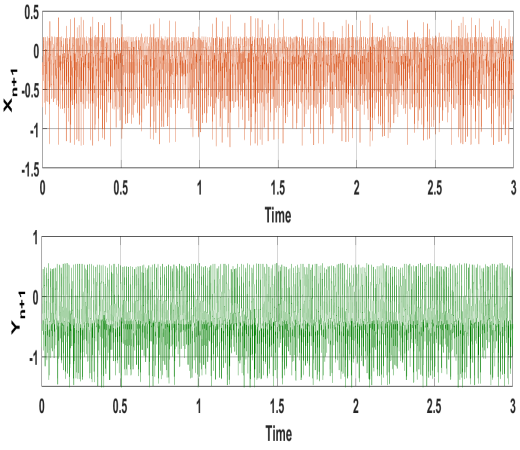
H



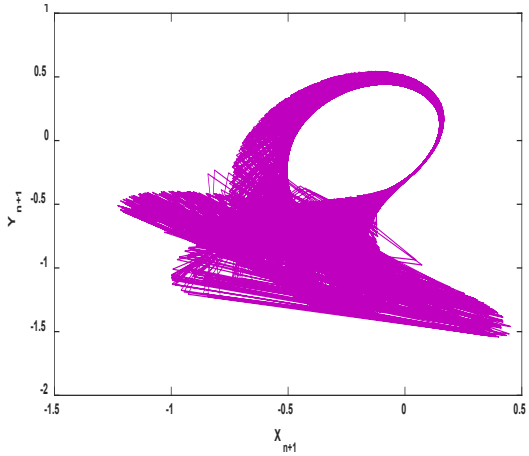
I



J



K



L

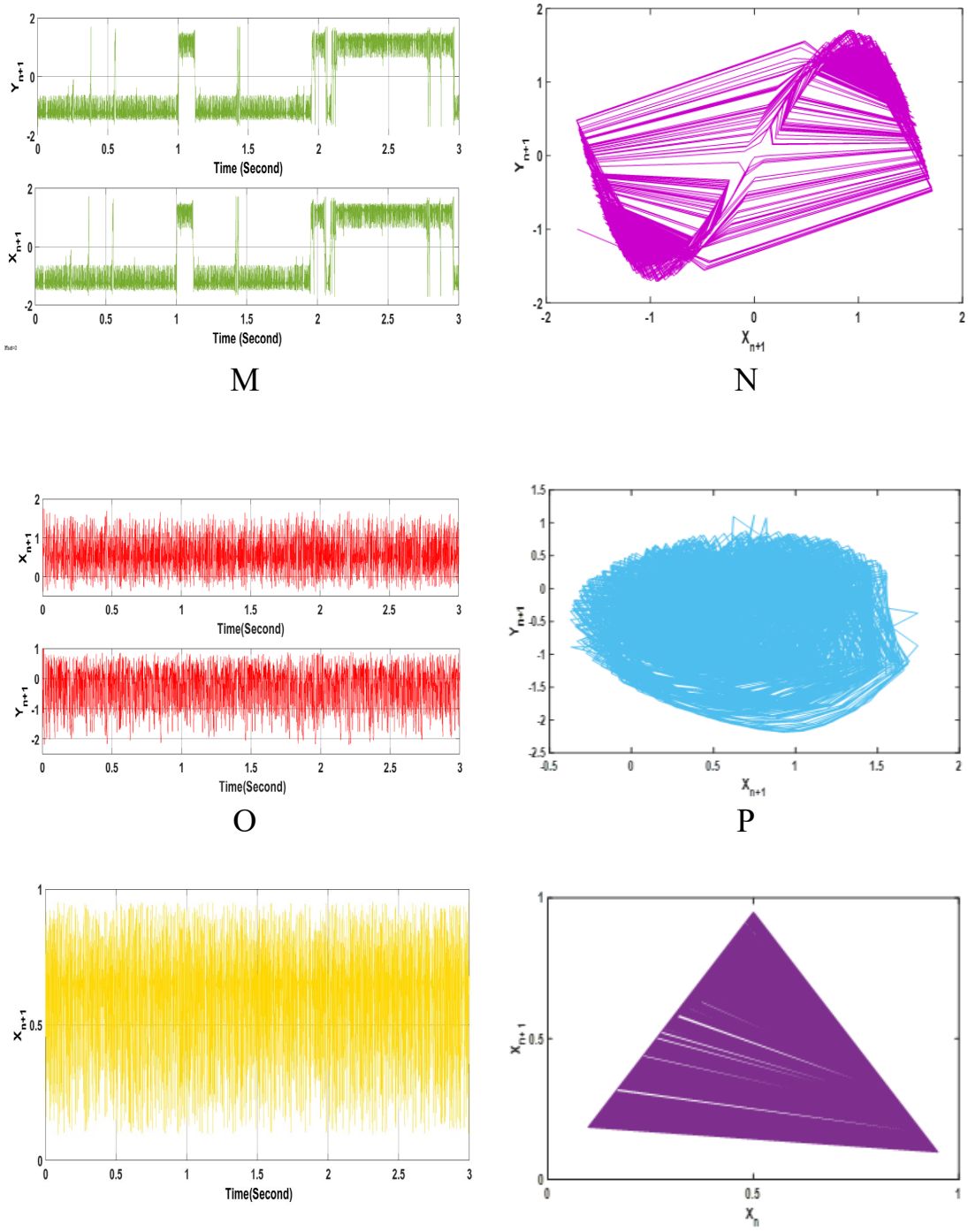


Figure 2.15 Behavior of chaotic maps [(A), (C), (E), (G), (I), (K), (M), (O), (Q)] time series, [(B), (D), (F), (H), (J), (L), (N), (P), (R)] attractor of Bernoulli, standard, Bogdanov, Henon, Logistic, Tinkerbell, Duffing, Ikeda, and Tent map respectively

2.7 Risks, Threats, and Vulnerabilities in Wireless Communication Networks

The wireless air interface is open and available to authorized and unauthorized users due to the broadcast nature of radio frequency propagation. The usage of wireless networks in both civilian and military applications has become an essential component of daily life. Security is a crucial concern in wireless applications when people rely heavily on wireless networks to transmit sensitive information, such as credit card transactions or banking-related data transmissions. Attackers could launch various attacks to get access to information without authorization, change it, or even stop information flows. Therefore, wireless security aims to stop hackers from harming devices or gaining unauthorized access [64, 65].

2.7.1 Security Attacks in Wireless Networks

Attacks can be divided into two primary groups: passive and active, depending on how they interfere with wireless communications.

2.7.1.1 Passive Wireless Attacks

A passive wireless attack involves scanning and monitoring a wireless network system for weaknesses and open nodes. This attack allows the attacker to obtain wireless network data without interrupting wireless communication. These attacks' primary objective is to learn as much as possible about the target; no data is altered or changed on the target systems. Eavesdropping is the most well-known instance of a passive wireless attack. Although privacy is breached, the information is unchanged, as shown in Figure 2.16.

Figure 2.16 Passive attack [66]

2.7.1.2 Active Attacks

In an active wireless attack, an attacker tries to break into the wireless network system. This attack involves the attacker damaging system data and perhaps changing system data. The attacker interrupts the wireless network's regular operations during this attack. It can be distinguished by features of information modification, information disruption, and information fabrication [67]

The most popular example of an active wireless attack is jamming, in which the attacker purposefully interferes by using radio frequency transmission to disrupt wireless network connections. Jamming, instead of eavesdropping, can fully interfere with authorized users' communications. An example of a jamming attack is shown in Figure 2.17. The jammer can produce deliberate interference, interfering with authorized users' data transmission. Jamming can also make it impossible for legitimate users to use radio resources [66, 67].

Figure 2.17 Jammer Attack [66]

2.7.2 Requirements for Security in 5G Wireless Communication Networks

Wireless networks must meet specific security standards to safeguard wireless transmissions from wireless attacks. In general, secure wireless communications should meet the following criteria:

1. **Authenticity**: A network node's true identity is verified to differentiate between authorized and unauthorized users. Before creating a communications link for data transmission in wireless networks, a pair of communicating nodes must first carry out mutual authentication [65].

2. **Confidentiality**: Data confidentiality and privacy are the two components that make up confidentiality. By preventing unauthorized users from accessing or disclosing data, data confidentiality safeguards transferred data against passive threats by limiting data access to authorized users only. Data privacy protects traffic flows from any attack-related analysis and inhibits the manipulation and control of data relevant to legitimate users.
3. **Integrity**: Integrity protects the information against active attacks from unauthorized individuals and prevents change or modification of the data. It is challenging to discover these attacks since attackers have valid identities. Mutual authentication can be used to deliver integrity services and produce an integrity key. The authentication schemes can offer message integrity.
4. **Availability**: Availability means that it may be accessed to the service and used by any legitimate user at any time or location. Availability considers how resilient the system is to various threats and is a key feature in the 5G network [66].

2.8 Cryptography

The process of converting data into an unintelligible format such that only the desired recipient may understand and be able to decode it is known as cryptography. Figure 2.18 depicts the main cryptographic operations. Encryption uses coding to convert plain text into an unintelligible format, whereas decryption employs decoding to turn the unintelligible text into meaningful data using some unique keys [68].

Figure 2.18 Process of Cryptography [68]

2.8.1 Cryptography classification

Cryptography can be divided into secret-key cryptography and public-key cryptography.

2.8.1.1 Secret Key Cryptography

It is commonly referred to as symmetric encryption; Figure 2.19 gives a brief explanation of this sort of encryption; the original data (plaintext) is transformed and encrypted in this form of encryption into what appears to be random unintelligible data known as ciphertext through an encryption process that consists of an algorithm and a key. The encryption technique generates an output based on the key used, and the value of the encryption key is independent of the plaintext. When the key is changed, the algorithm's output is altered. The basic conditions of symmetric key encryption require powerful algorithms, and the private key must be kept secure between authorized users only. The main advantage of this type is fast encryption processing, while the disadvantage is that the ciphertexts employing this key are readable if the key has been found by one of the attackers and the algorithm is known.

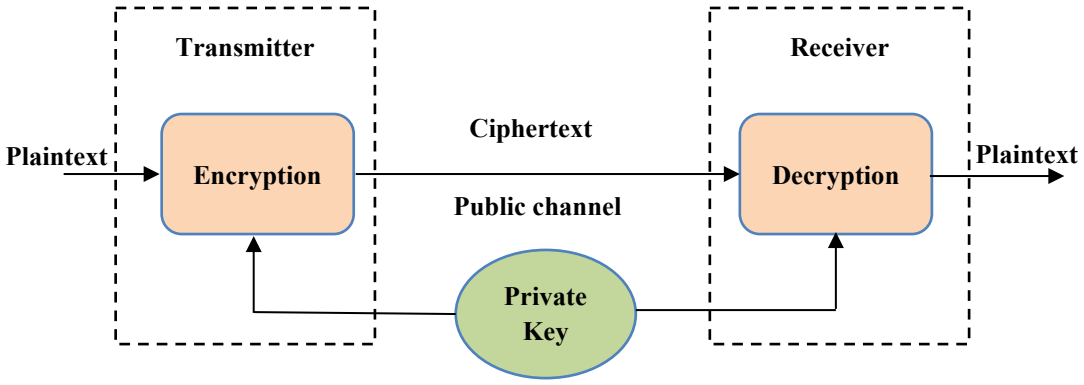


Figure 2.19 Symmetric encryption scheme [69]

2.8.1.2 Public Key Cryptography

The second kind of encryption, known as asymmetric encryption (or public key cryptography), requires two keys instead of one, the first of which is referred to as a public key and the second as a private key, as shown in Figure 2.20. The public key is familiar to everyone, but only users are familiar with the second key. Public key encryption can solve the problem of managing secret keys better than symmetric key encryption, but it is also mathematically more vulnerable to attacks due to this property. Due to the need for higher computational processing capacity, asymmetric encryption is generally slower than symmetric key encryption by roughly one thousand times [70].

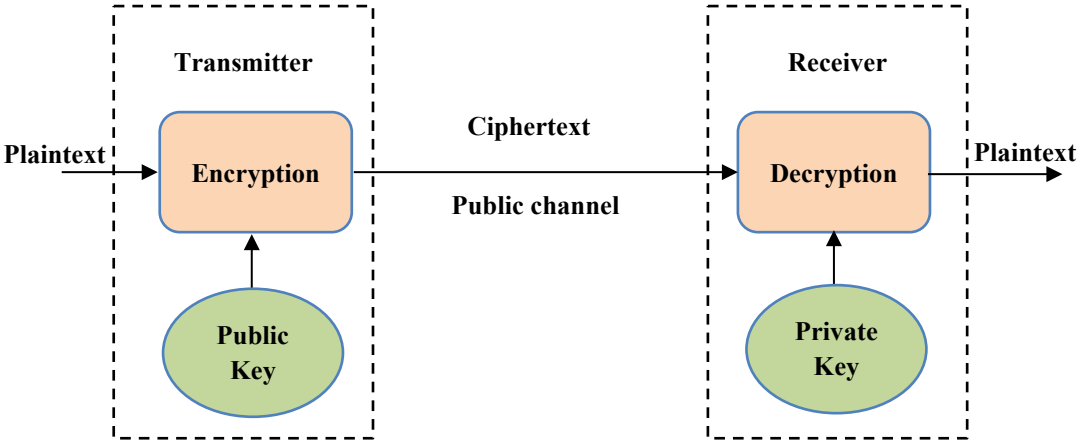


Figure 2.20 Asymmetric encryption scheme [69]

2.8.2 Physical Layer Security

Physical layer security (PLS) exploits the wireless channel's inherent randomness (such as noise and fading) to secure communications in the physical layer, in contrast to conventional security solutions dependent on upper-layer cryptographic techniques. Since PLS is not dependent on computing complexity, it has a significant advantage over other encryption techniques. In light of this, even if the eavesdropper has unlimited computing power, the security level attained will not be impacted. In contrast, encryption-based methods assume that an eavesdropper has limited computer resources and can only solve challenging mathematical problems

for a finite time. Shannon wrote a whole article that served as the foundation for secrecy systems and contained the earliest concepts of PLS. Later, Wyner introduced the wiretap channel in 1975. In that study, Wyner demonstrated that secret communications could be conveyed when the wiretap channel is a degraded (noisier) version of the authorized link. Thus, the greatest data rate may be transferred securely without being deciphered by an eavesdropper is known as the secrecy capacity [71]. The PLS idea represents the communication between two authorized users and the presence of an unintended user by a wiretap channel. A general example of a wiretap channel is shown in Figure 2.21, in which two authorized users are communicating on the primary channel while being watched by an outsider via a wiretap channel.

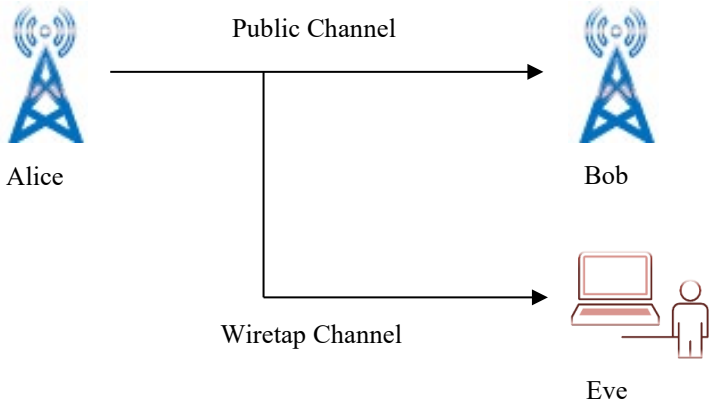


Figure 2.21 Wiretap channel Model [68]

Figure 2.22 highlights the key distinctions between PLS and cryptography [68]. PLS technique has the following characteristics above conventional encryption technologies: First, PLS approaches can be utilized by the time-varying and random characteristics of wireless channels. Second, PLS offers features that suit the Internet of Things (IoT) network, including low latency, small computational cost, minimal power consumption, long working times, and lifetime. Third, PLS is not relying on the eavesdropper channel conditions. Even if eavesdroppers have more antennas and more powerful reception equipment, PLS can still ensure safe data delivery.

Fourth, PLS offers improved signal-level security. Traditional cryptography works in the Boolean algebraic Domain; PLS also performs in the complex signal domain. Fifth, it is unnecessary to consider how security procedures are carried out or to include any additional security measures on layers above the physical layer. The PLS technique can also provide keyless security, meaning no encryption or decryption steps are necessary. MIMO and spatial modulation in transmission systems can increase the degrees of freedom and boost the wireless network's security capabilities [72, 73].

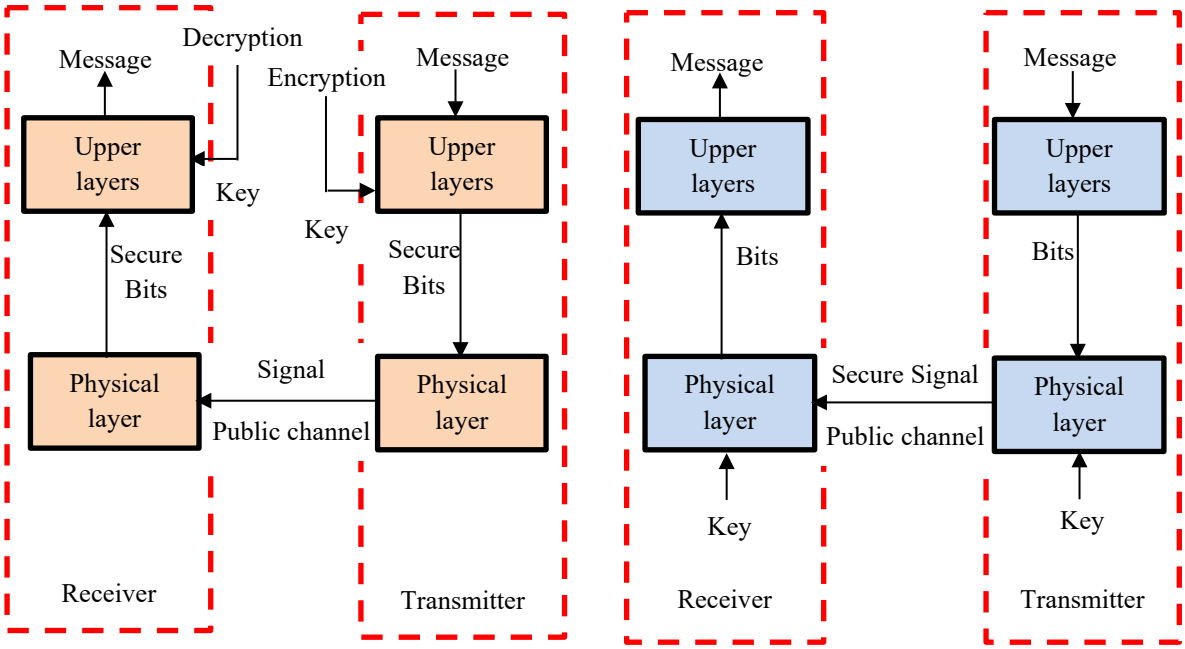


Figure 2.22 The comparison between cryptography and PLS approaches [68]

2.8.3 Cryptography-Based Chaos Theory

In recent years, scientific establishments have given substantial interest to studying chaotic systems and their applications to cryptography. Chaotic systems are characterized by SDIC, behavior resembling randomness, unstable periodic orbits with lengthy periods, and a continuous broadband power spectrum. Compression, encryption, and modulation are structural components of a digital communications system that could all benefit from the use of chaos. The primary objective in the early stages was to create encryption and modulation systems that utilized a single chaotic

system. Chaos-based modulation and chaos-based cryptography are separate study fields from this strategy [74]. The main benefit of chaotic encryption comes from the realization that unauthorized users who ignore the mechanism generate the chaotic signal and perceive it as noise. Also, the initial conditions and control parameters of the chaotic generating function significantly impact how the chaotic signal evolves over time. Minor changes to these parameters result in distinctly diverse time evolutions. Thus, an encryption system can effectively employ beginning states and control parameters as keys. Additionally, chaotic signal generation is inexpensive, making it appropriate to encrypt huge, bulky data [75].

2.8.4 Benefits and drawbacks of applying chaos theory to cryptography

Cryptography can use a pseudo-chaotic system that is based on chaos theory. Pseudo-Chaos has an infinite number of states. It involves approximating continuous chaos with floating- or fixed-point arithmetic; this leads to a discrete chaos-like system with a low cycle length. Chaos initial conditions and parameters can be utilized as a cryptographic key. Cryptography use diffusion, representing the sensitivity of chaotic parameters to the initial condition. The initial state of the chaos sequence can be mixed with the plaintext to produce keys in cryptography. The final state of the chaos sequence represents ciphertext in cryptography. Asymptotic independence of initial and final states in chaos can be employed as confusion in cryptography. Chaos-based cryptography has another advantage. It encrypts the continuous waveforms of the signal without the need for sampling and quantization. Since the algorithms of chaos-based cryptography can be defined over continuous number fields compared with traditional cryptography algorithms, they can be defined over integer number fields. There are a few drawbacks compared to traditional cryptography, such as floating point numbers, low cycle length, and redundant data [76].

2.8.5 DNA Encoding Technique

In biology, a DNA sequence is classified into four nucleic acids: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G), which make up the majority of a nucleotide. According to DNA encoding and complementary rules, the four bases are encoded using binary 00, 01, 10, and 11; A is paired with T, and C is coupled with G, yielding eight coding methods. The mathematical operations and basic rules of DNA encoding are illustrated in the tables below.

Table 2.5. DNA XOR Operation [6]

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Table 2.6. DNA coding rules [6]

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

Table 2.7. DNA Addition Operation [6]

add	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 2.8. DNA Subtraction Operation [6]

sub	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

To understand DNA encoding rules, for example, if the sequence form is "00111111000100010110000100111101" then, when encoding it according to the DNA rule 4, it will get "TAAATCTCCGTCTAAC" [6, 77].

2.8.6 Elliptic Curve Arithmetic Over Finite Field

The production of unpredictable amounts, large enough and random enough, is necessary for the security of the majority of known cryptographic systems. PRNG can be generated using elliptic curves. Elliptic Curve Cryptography (ECC) is a public-key algorithm that is significant in cryptography. Because the fact of ECC has a small key space and offers a similar level of protection to other public-key algorithms that make use of larger key spaces. Additionally, it provides higher security levels while utilizing less computational power, memory, and bandwidth [4, 5].

For a given prime number p, suppose Fp represents the finite field of p, so the Elliptic Curve (EC) over Fp can be defined by the relation:

$$[y^2 = x^3 + ax + b]\ mod\ p \qquad (2.10)$$

Where the coefficients a,b ∈ Fp, a,b less than p and should be satisfied by the following Equation:

$$[4a^3 + 27b^2 \neq 0]\ mod\ p \qquad (2.11)$$

Scalar multiplication is necessary to perform point multiplication on EC. The fundamental operations of EC are point addition and point doubling. By assuming there are two points, P (x_1, y_1) and Q (x_2, y_2), belonging to Fp, the

coordinate addition P+Q yields the third point, R (x_3, y_3), satisfying the EC equation as in the following:

$$x_3 = [\lambda^2 - x_1 - x_2] \, mod \, p \tag{2.12}$$

$$y_3 = [\lambda(x_1 - x_3) - y_1] \, mod \, p \tag{2.13}$$

$$\lambda = \begin{Bmatrix} \left(\frac{y_2 - y_1}{x_2 - x_1}\right) mod \, p \xrightarrow{when} P \neq Q \\ \left(\frac{3x_1^2 + a}{2y_1}\right) mod \, p \xrightarrow{when} P = Q \end{Bmatrix} \tag{2.14}$$

In the subtraction case, the sign inversion of the y-coordinate of the second point is needed and solved as follows:

$$P\,(x_1, y_1) - Q\,(x_2, y_2) = P\,(x_1, y_1) + Q\,(x_2, -y_2) \tag{2.15}$$

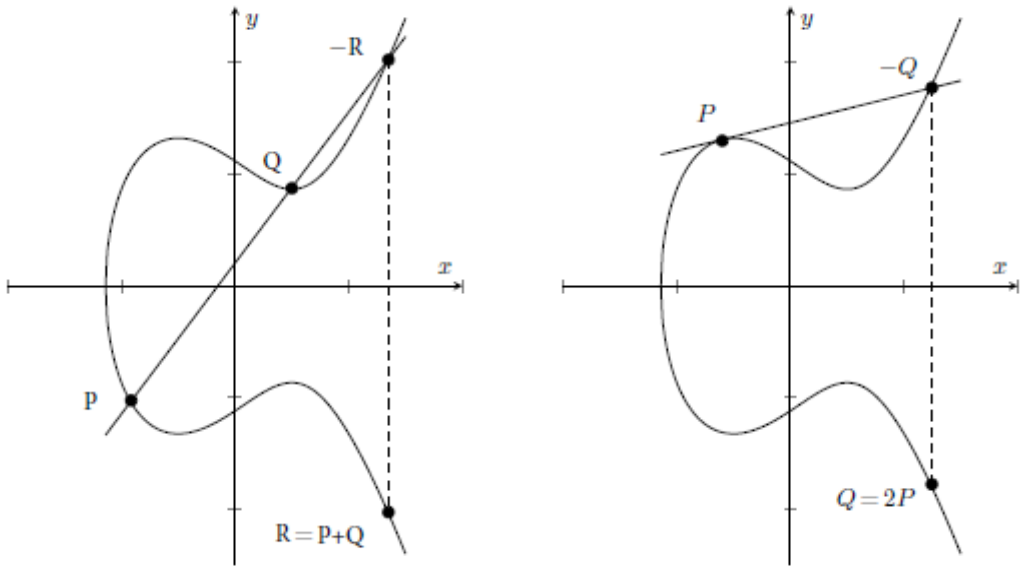
Point multiplication calculations can be improved by effectively using point addition and doubling operations. Point multiplication can be calculated as many points are added together; the EC operation is depicted in Figure 2.23. For instance, when one needs to estimate nP, where n is a positive integer, then:

$$nP = P + P + \cdots, n = 1,2, \ldots .. \tag{2.16}$$

PRNG can be generated based on the group of points of an EC defined over a prime finite field. This work uses a Linear Congruential Generator on EC (EC-LCG), a type of PRNG sequence. The EC-LCG sequence for a given Uo and G ∈ Fp, where G represents the generating point, and Uo represents the initial value (seed), is defined as:

$$U_n = U_{n-1} + G = nG + U_o \, , \quad n = 1,2 \ldots .. \tag{2.17}$$

The initial value $U_0 = (x_0, y_0)$, and the constants G, a, and b can be taken as secret keys in the cryptographic algorithm [78-80]. In this work, the parameter values used are p=4093, a=9,b=7, G=(4,1110), and U_0 =(332,1395). Therefore, the key space of the EC-LCG sequence is 2^{60}, assuming a and b are constant.



Point addition Point doubling

Figure 2.23 Graphs of the Elliptic curves [81]

2.9 Secure Audio Cryptosystem

Many studies have dealt with speech encryption methods in the analog/digital domain due to the fast growth of communications technologies. Audio encrypting techniques must meet several criteria, including that the encrypted audio is unintelligible, uses the same amount of bandwidth as the original signal, and has the same formatting and length. The recovered audio should be of high quality on the receiver device. Also, it should be cryptanalytically robust and immune to various attacks, including chosen/known plaintext attacks, statistical attacks, and brute force attacks. Additionally, the encrypting process should involve the least amount of time delay possible [82].

2.10 Audio Encryption Classifications

The audio signal can be encrypted in the analog and digital domains, as shown in Figure 2.24.

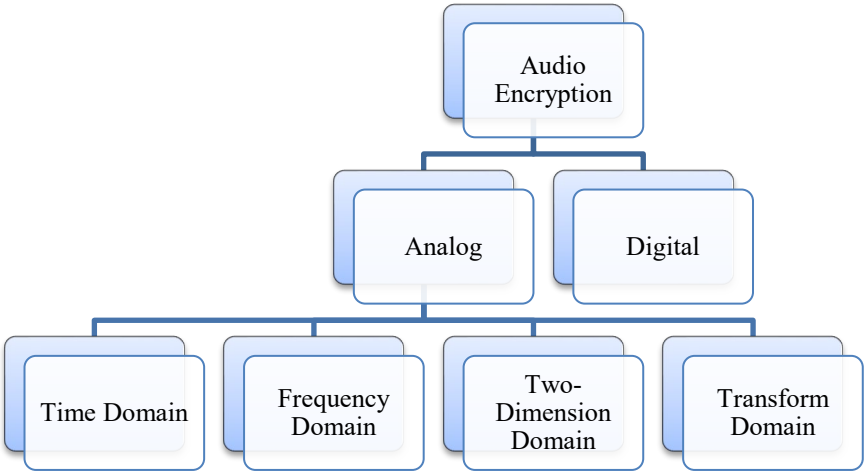


Figure 2.24 Classification of Analog Audio Scrambling Algorithms [83]

2.10.1 Time Domain-based techniques

The audio signal is partitioned into segments, and the segments are subsequently permuted using the PRNG sequence, as illustrated in Figure 2.25. Encryptors that use permutation do not alter the features of the signal. Because these algorithms only utilize a portion of the audio samples, the key space is small, and the block-wise operation creates a time delay directly proportional to the block size [83, 84].

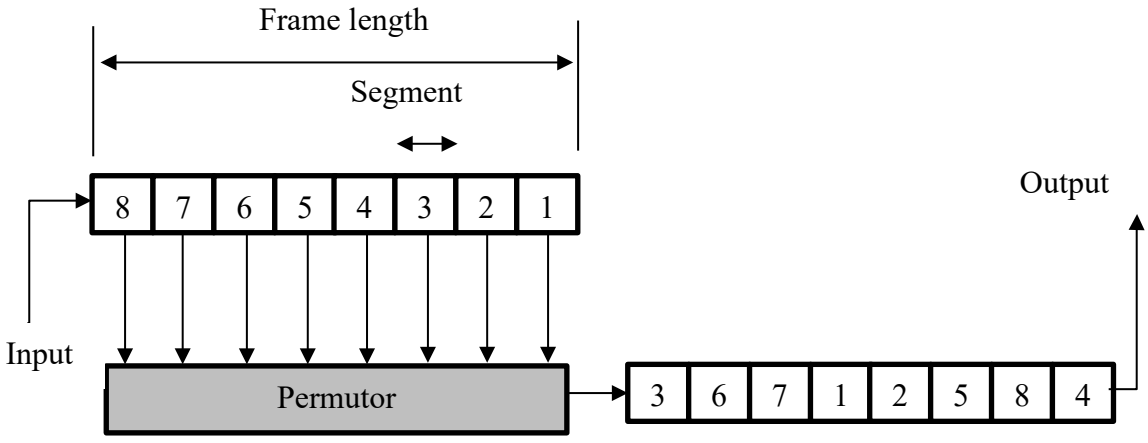


Figure 2.25 Time domain encryption[84]

2.10.2 Frequency domain-based techniques

A frequency-domain encryptor divides each audio signal block's frequency content into M frequency bands. In order to create a temporal sequence with encrypted frequency contents in place of the original audio

signal block, these bands are permuted by a predetermined rule (or key). Due to the algorithms' utilization of only a portion of the audio samples and their rather long time delays, the key space is small [85, 86].

2.10.3 Two-Dimension based techniques

Two-Dimensional encryptors manipulate signals together in the time and frequency domains. The speech-silence rhythm is destroyed by time-domain manipulations, while some of the audio components' spectral properties are changed by frequency-domain alterations. These encryptors have a higher level of complexity, a longer encoding time, and a smaller key space [83].

2.10.4 Transform-based techniques

The operations carried out on the audio samples' linear transform coefficients constitute the basis of this family of analog encryptors. Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Hadamard Transform (HT), Wavelet Transform, and OFDM are examples of the transform types that are employed. These algorithms operate on a greatly increased number of permutable transform coefficients, which results in a high key space. These encryptors manipulate the time and frequency domains, resulting in a significant encoding delay [83].

2.11 Quality Factors of Secure Audio Encryption System

The encryption algorithm should be efficient enough to give an ambiguous voice signal when hearing it. The following evaluation parameters evaluate the effectiveness of the voice encryption algorithm.

2.11.1 Residual Intelligibility (R.I.)

R.I. is a useful metric for evaluating and determining the security requirement of a system. When the R.I. of the audio is low, it indicates that the audio is unclear (more security) [87].

2.11.2 Encoding Delay

Other crucial features of a strong encryption algorithm are its speed of execution. The encryption/decryption time is the time the encryption/decryption algorithm takes to complete its process. This time is proportional to the length of the audio [88].

2.11.3 Key space and key Sensitivity

Two factors affect audio encryption quality, which is key space and key sensitivity. The group of secret keys used during audio encryption is known as Keyspace. The key sensitivity means that the decryption of the audio cannot be achieved when there is little variation in the secret key. In order to get a secure system against attacks, a powerful audio encryption algorithm must have a large keyspace and high sensitivity [89].

2.12 Secure Audio Assessment Keys

There are two types of tests used in this thesis. Subjective tests and objective tests. It uses for evaluating the performance of system security as follows:

2.12.1 Subjective Tests

The tests can be done using the following criteria.

2.12.1.1 Figures Observation

This test requires a speech signal drawing through several representations, including original and encrypted audio waveform, Histogram, and Spectrogram.

2.12.1.1.1 Waveform Plotting

Waveform plotting, which shows how the audio signal's amplitude is changed across time, is one of the most popular methods for audio signal analysis. The difference between the original and encrypted audio plot

demonstrates good encryption. The great change makes it impossible to restore the original audio, even partially [27].

2.12.1.1.2 Histogram analysis

Histogram analysis is a reliable method of determining the quality of encrypted audio. A stronger encryption system should convert the original audio to random-like noise (uniform distribution) with a roughly flat sample value distribution. In addition, the filling of the muted portion of audio by noisy signals with approximately similar values explains why the histogram of encrypted audio resulting becomes approximately flat, while the histogram of the original audio is random and concentrates on the zero point [6].

2.12.1.1.3 Spectrogram Analysis

The spectrogram is the three-dimensional representation of information using time, frequency, and energy values. The colors describe the energy value in the audio; when the color is darker, it refers to high energy content. Color gradation starts from blue (low energy) to yellow (medium energy) to red (high energy) [77].

2.12.1.2 Listeners

The encrypted audio would have to be heard by many experienced and untrained human listeners in subjective tests. There are three degrees of R.I. in these tests: word, phrase, and digit.

The range of R.I. scores is (0-100) percent and as follows:

- When R.I. (0) %, this is a perfect case (good encryption scheme).
- When R.I. (1-10) %, this gives a low case
- When R.I. (11-30) %, this gives a medium case.
- When R.I. (31-50) %, this gives a high case (poor encryption scheme).

These tests have the disadvantages of taking a long time in the laboratory and requiring many audiences [89].

2.12.2 Objective Tests

Other tests can be used, called objective tests, which serve as indicators for encrypted audio R.I. and the quality of the retrieved audio. The most popular methods are:

2.12.2.1 Signal to Noise Ratio (SNR)

The SNR is a simple measure for evaluating the quality of the audio encryption algorithm. The noise value in the encrypted audio is high. Thus, low SNR is required for good encrypted. The SNR values of encrypted audio are estimated as follows:

$$SNR = 10\ log_{10} \frac{\sum_{i=1}^{N} {x_i}^2}{\sum_{i=1}^{N} (x_i - y_i)^2} \tag{2.18}$$

Where x_i, y_i are original and encrypted audio samples, respectively.

2.12.2.2 Peak Signal to Noise Ratio (PSNR)

The mean square error of the original (x_i) and encrypted (y_i) audio samples can be estimated as follows:

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2 \tag{2.19}$$

Then, PSNR can be determined using the following formula:

$$PSNR = 10\ log_{10} \left(\frac{MAX^2}{MSE} \right) \tag{2.20}$$

Where MAX represents the maximum value of the encrypted audio samples, lower PSNR indicates the high noise level in the audio, which means a good encryption algorithm and resistance against attacks.

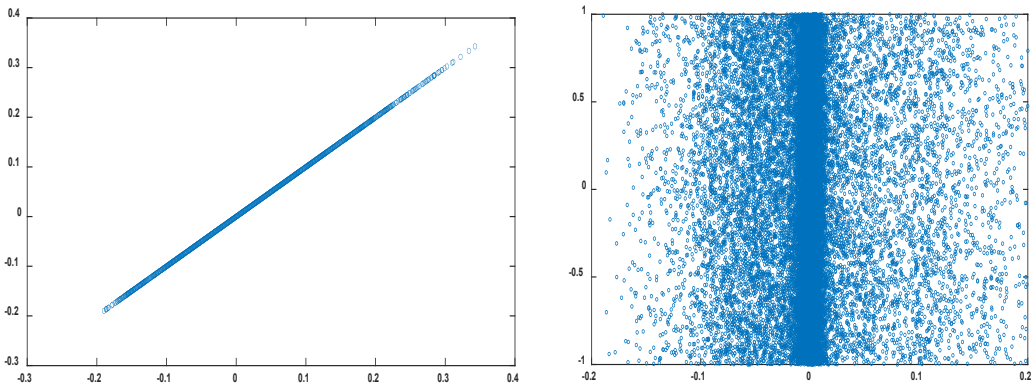
2.12.2.3 Correlation Analysis

Correlation coefficient (R_{xy}) is a tool metric for evaluating a cryptographic algorithm against different attacks. Its measures the relationship between equal portions of the original and encrypted audio. A good audio encryption algorithm converts the audio into a noisy signal with a low value of R_{xy} between original and encrypted audio. In general,

original audio has R_{xy} close to one while the encrypted audio has R_{xy} close to zero. R_{xy} can be estimated as follows:

$$R_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (2.21)$$

Where N is the number of audio samples, x_i and y_i are the samples value of the original and encrypted audio, respectively, E(x) and E(y) are the expected value of the original and encrypted audio samples, $\sigma_x, \sigma_y \neq 0$ are the standard deviation of the original audio and encrypted audio, respectively, and $\mathrm{cov}(x, y)$ is the covariance between audios [6]. Figure 2.26, the scatter plot was presented for audio and the corresponding encrypted audio. It is clear that there is no similarity between the adjacent encrypted samples.



(a) (b)

Figure 2.26 Correlation coefficient result for audio (a) original (b) encrypted

2.12.2.4 Linear Predictive Code Distance (d_{LPC})

The d_{Lpc} can be expressed as:

$$d_{LPC} = ln\left(\frac{cVc^T}{dVd^T}\right) \quad (2.22)$$

Where $c = [1, c_1, c_2, \cdots, c_p]$is the LPC coefficients vector estimated from original (clean) audio, $d = [1, d_1, d_2, \cdots, d_p]$ is the LPC coefficients vector calculated from encrypted (distorted) audio, and V=V(i,j) , i, j = 0, 1, …. , p,

is the normalizing correlation coefficients matrix estimated from encrypted audio as:

$$v(i,j) = \frac{1}{p}\sum_{n=-i}^{p-i-1} b(n)b(n+i-j) \tag{2.23}$$

Where p is the filter order, high d_{LPC} indicates good encrypted quality.

2.12.2.5 Log Spectral Distance Measure (d_{LOG})

The d_{LOG} can be determined using the following formulas:

$$V(f) = \log\big(s(f)\big) - \log\big(s'(f)\big)\ , f = 0,1,\cdots N-1 \tag{2.24}$$

Where $s(f)$ and $s'(f)$ represent the PSD of original and encrypted audio, respectively, so

$$d_{LOG} = \frac{1}{N}\sum_{f=0}^{N-1} |V(f)|^P\ , f = 0,1,..N-1 \tag{2.25}$$

Where P is the distance order, and a high value of d_{LOG} indicates a good encryption algorithm [28].

2.12.2.6 Frequency Weighted Log Spectral Distance (d_{FWLOG})

Audio with a frequency range of 300-500 Hz can be understood reasonably well. In other meaning, the residual audio intelligibility components are found within the 300-500 Hz frequency range. As a result, distance measurements more suited to the cryptanalysis of transform domain audio encrypted would prioritize proper coefficient relocation in this frequency region. One way to perform this is to mask portions of the spectra of the original and cryptanalyzed audio waveform to zero, limiting the distance measurements to the 300-500 Hz band. Modifying the d_{Log} would be a useful approach. Before using Equation (2.25) to calculate the d_{Log}, a masking window can be implemented to the spectra of the two frames to compare only the 300-500 Hz components. The use of such a window permits Equation (2.25) to be simplified to:

$$d_{FWLOG} = \frac{1}{n}\sum_{f=a}^{b}\left|\log\left(s(f)\right) - \log\left(s'(f)\right)\right|^{P} , f = a, a+1, \cdots, b \quad (2.26)$$

Where a and b are the index of spectral coefficients of frequencies 300 Hz and 500 Hz, respectively, and n=b-a+1, when the d_{FWLOG} value increases, it indicates a high-security level [84].

2.12.2.7 Spectral Segment SNR (SSSNR)

The SSSNR is abbreviated as:

$$SSSNR = 10\ log\left[\frac{\sum_{i=0}^{N-1}|x_i|^2}{\sum_{i=0}^{N-1}(|x_i| - |y_i|)^2}\right] \quad (2.27)$$

Where x_i and y_i are DFT of clean and encrypted audio samples, respectively, when SSSNR is minimized, it represents low R.I. and, therefore, High-security levels.

2.12.2.8 Cepstral Distance (d_{CD})

The (d_{CD}) is expressed in the following way:

$$d_{CD} = 10\ log\sqrt{2\sum_{i=1}^{p}(C_x(i) - C_y(i))^2} \quad (2.28)$$

Where $C_x(i)$ and $C_y(i)$ are the Cpestral coefficient of original and encrypted audio, respectively, and p is the number of frames [19]. The high value of d_{CD} in the encrypted audio means that low R.I.

2.12.2.9 UACI and NSCR Analysis

Resistance against differential threats is a key indicator of encryption strength. To determine this level of resistance, modified audio is obtained by inverting the least significant bit of the sample. The same secret key encrypts the original and modified audio, resulting in two encrypted audios. After that, the encrypted audio signals are then compared by the number of samples

change rate (NSCR) and the unified average changing intensity (UACI); they are represented by:

$$NSCR = \sum_{i} \frac{D_i}{N} \times 100\% \ , D_i = \begin{cases} 1, A_i \neq A'_i \\ 0, otherwise \end{cases} \quad (2.29)$$

$$UACI = \frac{1}{N}\left[\sum_{i} \frac{|A_i - A'_i|}{65535}\right] \quad (2.30)$$

Where A and A' are encrypted of original and modified audio, respectively, which have a difference in one sample only, N represents the number of samples in audio. The optimal NSCR and UACI values are 100 % and 33.3 %, respectively [88].

2.12.2.10 Root Mean Square (RMS) and Crest Factor (CF)

The average amplitude of audio determines the RMS value, which is calculated as follows:

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} |A_i|^2} \quad (2.31)$$

CF can be defined as the ratio between the peak and effective values of audio; CF is estimated by the following [6]:

$$CF = 20 \log_{10} \frac{|V_{peak}|}{V_{RMS}} \quad (2.32)$$

The increasing value of RMS means a low R.I. of the encrypted audio, and the reduction value in CF means a low R.I.

Chapter Three
The Proposed Audio Encryption Techniques

3.1 Introduction

The number of users and devices has substantially increased due to the rapid growth of modern wireless technologies and networks. These technologies transfer sensitive information, such as audio, over open-access networks. Transferring this information through networks may be subject to eavesdroppers. Therefore, an urgent need for modern encryption techniques to safeguard these contents. 5G wireless communications technology has great challenges in ensuring security. Therefore, it required a suitable approach to provide security. Using chaos theory in cryptosystems is one of these ways.

This chapter presents new approaches for secure audio transmission using multiple chaotic sequences with the combination of an elliptic curve and DNA encoding inside communications system components. Four techniques are proposed with their algorithms in the analog and digital domains to increase security and get a minimum R.I. in encrypted audio. Each approach includes independent chaotic sequences that act as a secure key generator mixing with original audio components in a certain manner to perform encryption in the time and frequency domains before being transmitted. The proposed techniques were implemented with a 5G infrastructure that contains GFDM, PSM, and massive MIMO, as illustrated in Figure 3.1.

Also, this chapter states the mathematical design of the proposed audio cryptosystem with its essential components, requirements, and methodologies for construction and implementation, including

encryption/De-decryption algorithm, GFDM Modulator/ Demodulator, PSM Modulator/ Demodulator, the channel including Additive White Gaussian Noise (AWGN) and Rayleigh fading, chaotic maps including Bernoulli, Standard, Bogdanov, Henon, Logistic, Tinkerbell, Duffing, Ikeda, and Tent maps.

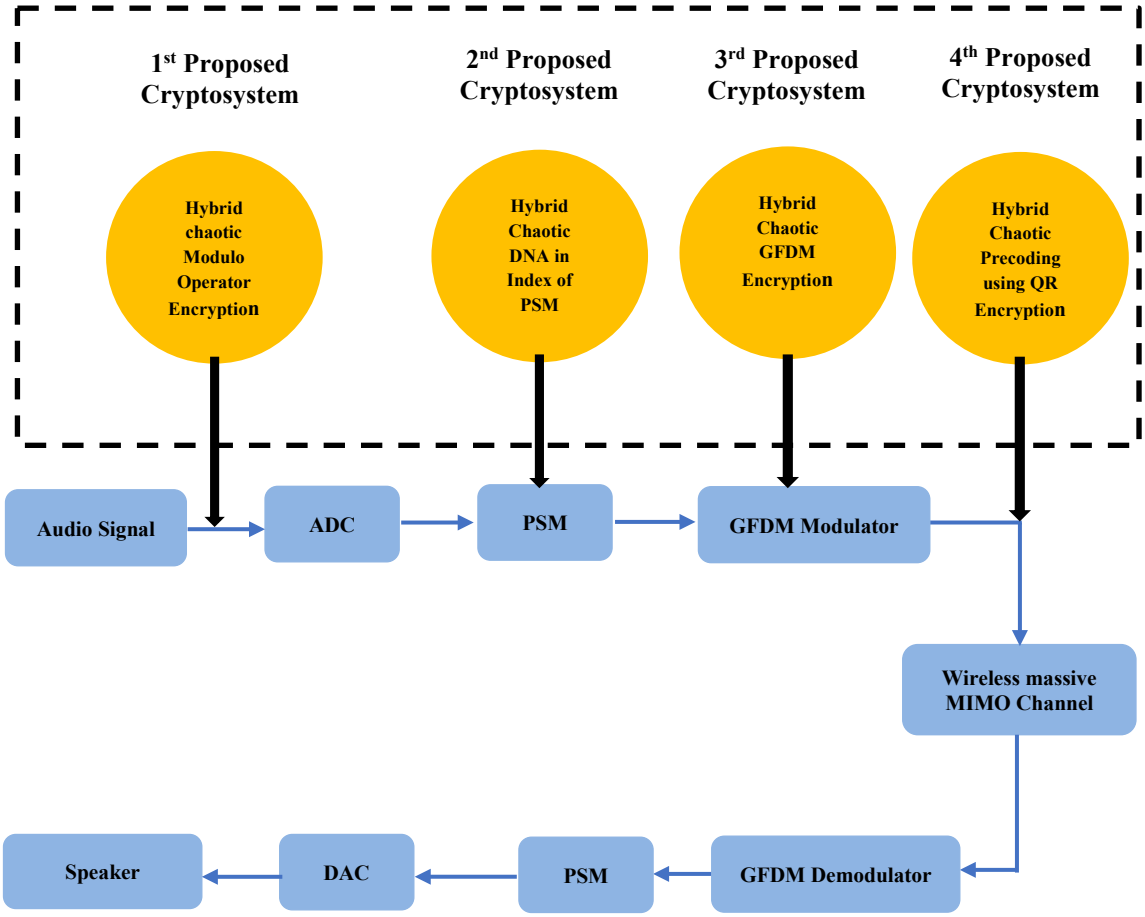


Figure 3.1 The proposed Encryption algorithms in a massive MIMO-PSM-GFDM system

3.2 Hybrid Chaotic Modulo Operator (HCMO) Encryption Technique

The first proposed cryptosystem to protect audio will be formulated based on triple chaotic maps utilized as secret keys PRNG. There are own series for each chaotic map, known by both sender and receiver. On the transmitter side, the generated PRNGs are utilized to encrypt directly and decrypt audio using the modulo principle to create an HCMO, as demonstrated in Figure 3.2 and Figure 3.3, resulting in a cryptosystem with

an excellent security level and low R.I. The proposed HCMO parameters details and system are illustrated in Table 3.1 and Figure 3.4. The mathematical representation of the encryption process is as follows:

$$A \bmod B = (R, Q) \tag{3.1}$$

Where A is the dividend (Audio), B is the divisor ($B = X_{Bogdanov}$), Q is the quotient, and R is the remainder. To rebuild (A) again, use the following formula:

$$A = R + Q \times B \tag{3.2}$$

By adding PRNGs for each part of the above equation to achieve audio encryption results:

$$A_{encrypted} = (R + P_{\text{Standard}}) + (Q + X_{\text{Bernoulli}}) \times X_{Bogdanov} \tag{3.3}$$

After encryption, an analog-to-digital converter (ADC) converted the audio to a binary system and transmitted data over PSM-GFDM massive MIMO system. On the receiver side, the decryption process can perform using the equation:

$$A_{decrypted} = (R - P_{\text{Standard}}) + (Q - X_{\text{Bernoulli}}) \times X_{Bogdanov} \tag{3.4}$$

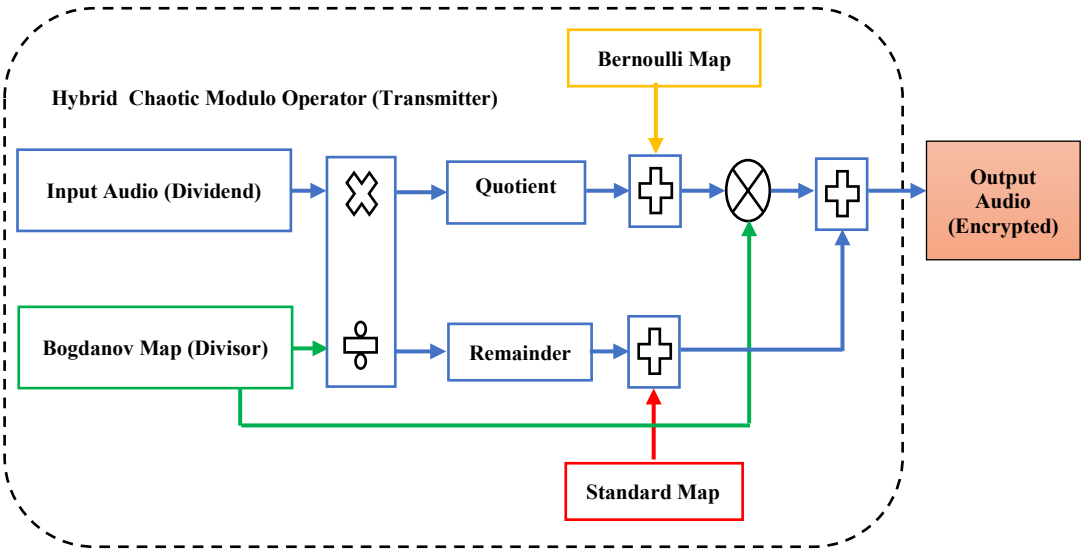


Figure 3.2 Block diagram of the proposed HCMO encryption Technique

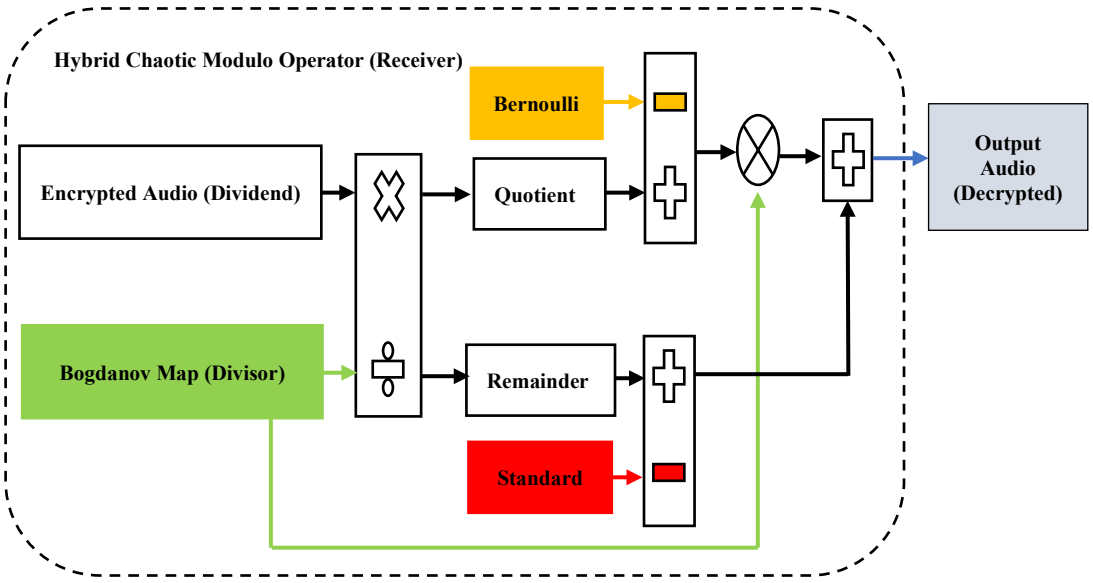


Figure 3.3 Block diagram of the proposed HCMO decryption Technique

Table 3.1. Simulation parameters

Scheme	Parameter	Value
GFDM parameters	Number of subcarriers(K)	16
	Number of time slots(M)	5
	Pulse shaping filter	Raised cosine filter
	Roll-off factor	0.2
	Modulation scheme	16-QAM
	Length of cyclic prefix (CP)	20
Massive MIMO	Number of transmit antennas (N_t)	80
	Number of Receive antennas (N_r)	80
	Channel Fading	Rayleigh-Flat
PSM	Number of the group (p)	5
	Group size (g)	16
ADC	Bits/sample	16

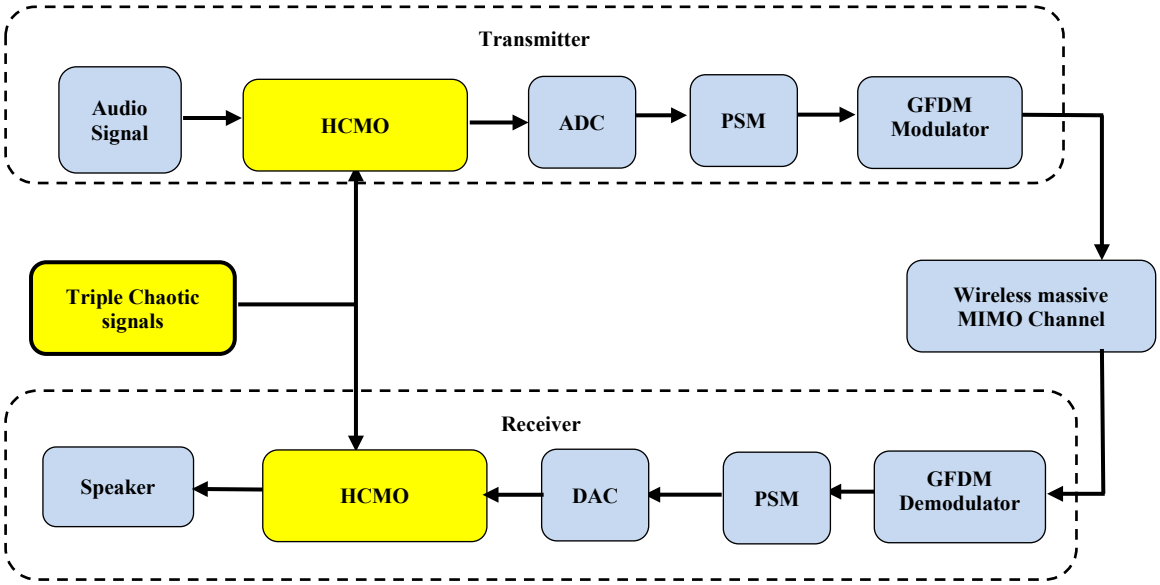


Figure 3.4 The proposed HCMO over massive MIMO GFDM cryptosystem

3.2.1 Encryption/Decryption algorithm of the proposed HCMO Technique

The original audio of frequency 8 kHz, WAV audio format, and double data entering into the system are discrete into 16 samples/frame. At the same time, it creates chaotic PRNG using Bogdanov, Standard, and Bernoulli with 16 samples/frame sizes for each sequence representing secret keys. The encryption algorithm will use HCMO yielding 16 samples/frame sizes. Each sample will be converted to binary using 16-bit ADC; hence the frame size will be 16×16=256 bits. In this stage, the incoming bits are reshaped into 24 bits/frame to satisfy the PSM requirement. Also, the bitstream is partitioned into six groups, each with 4 bits, one group is used for 16-QAM modulation, and the remaining groups are used for antenna index. To construct the GFDM modulator, regrouped the modulated data into five groups, each with 16 complex symbols, to perform IFFT and filtering using the RRC filter, resulting in 80 complex symbols per frame. Finally, add CP to the frame with a length of 20 complex symbols yielding 100 complex symbols and transmitted over antennas, as shown in Figure 3.5.

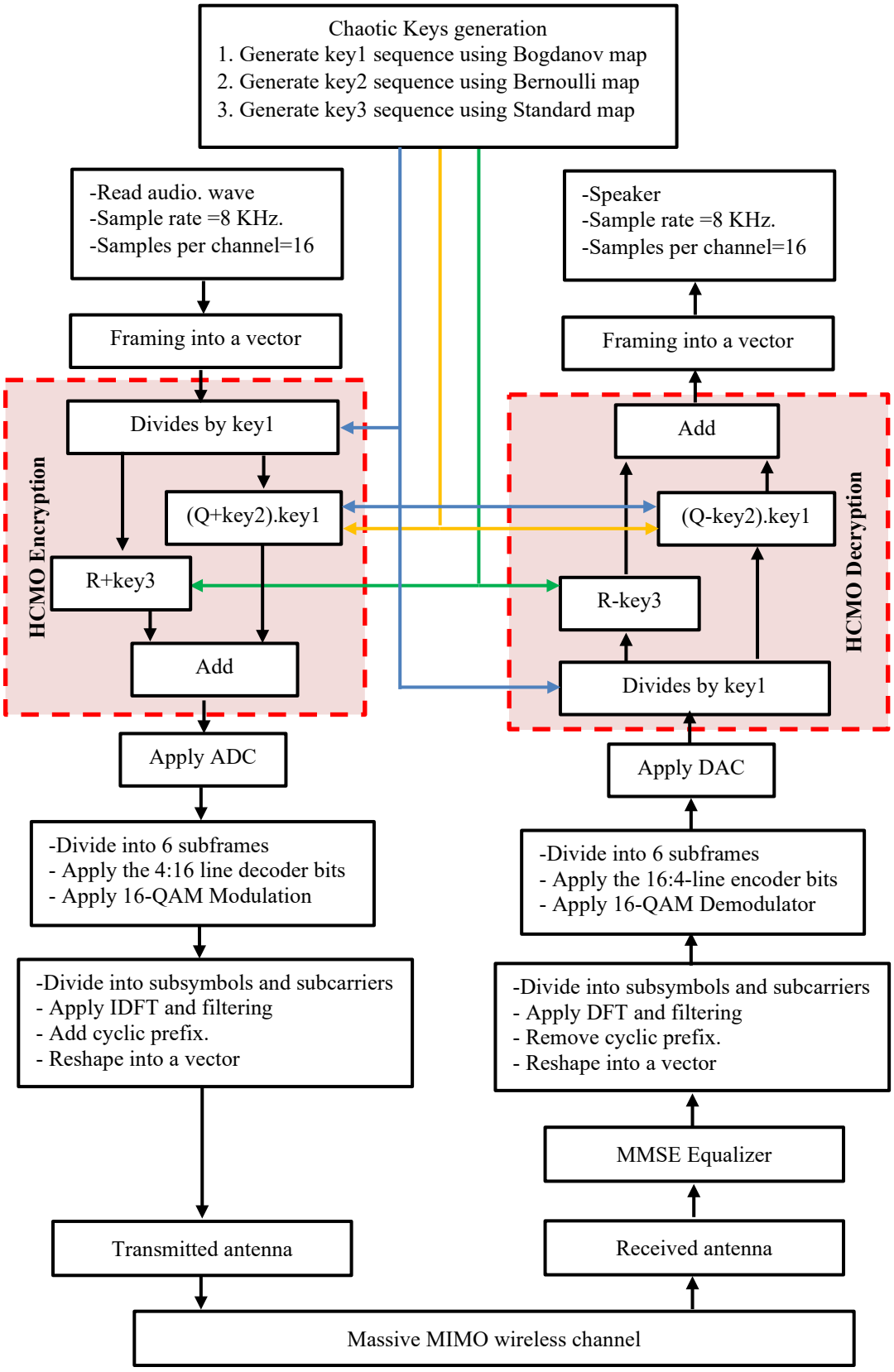


Figure 3.5 Encryption/Decryption algorithm of the proposed HCMO technique over massive MIMO-GFDM system

3.3 DNA Coding in the Antenna Index of PSM Encryption Technique

The second proposed technique to protect audio is based on triple chaotic maps and DNA coding utilized as a secret key, known as the DNA-antenna index of PSM (DNA-AI-PSM) technique**.** The x-sequence of Henon and the x,y sequences of Tinkerbell and logistic maps are multiplexed to one sequence. The multiplexer output is modulus-ed by the y-sequence of the Henon map and then converted to binary, after which the resulting sequence is coded into the DNA encoding to generate secret keys. Two-level XOR operations are used inside PSM to achieve audio encryption, and the first XOR is performed between the index of the active antenna and the secret key. The second XOR is executed between signal constellation bits and the other secret key, as illustrated in Figure 3.6. After the encryption process is complete within PSM, the audio data are modulated using GFDM and transmitted to a wireless channel, as shown in Figure 3.7.

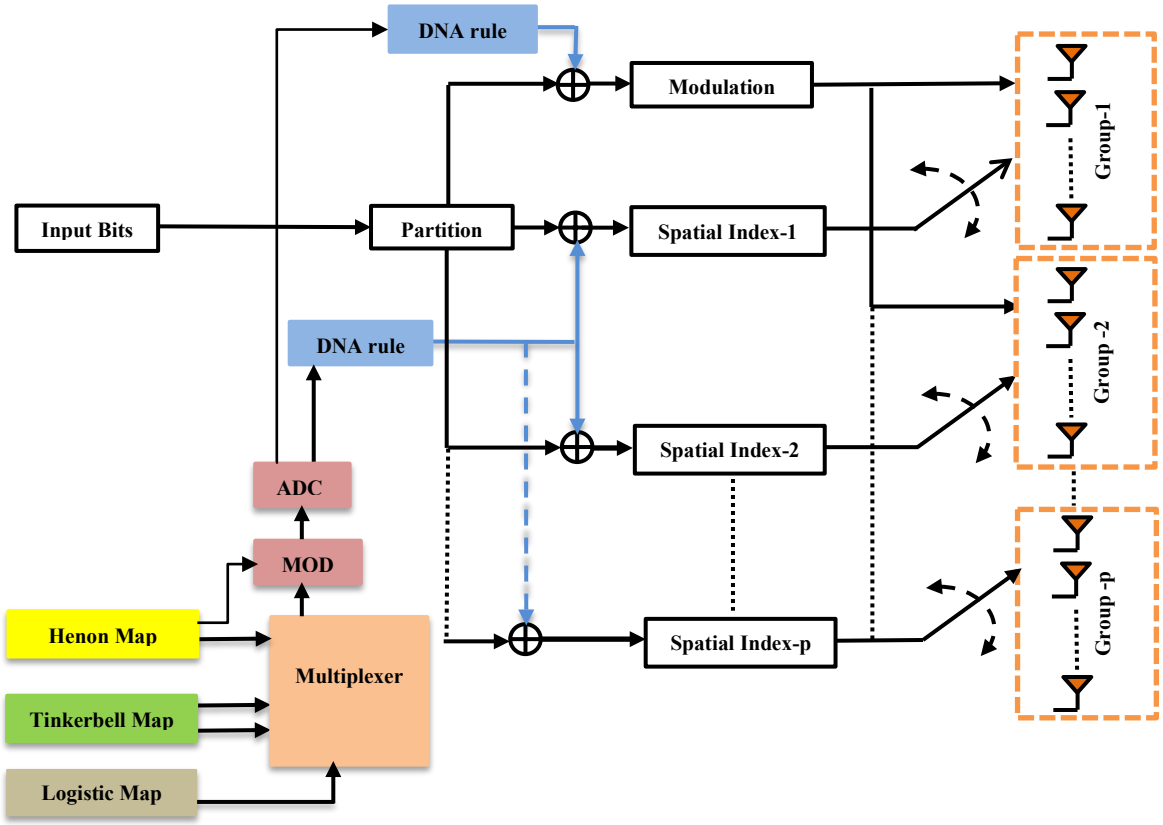


Figure 3.6 Block diagram of the proposed DNA-AI-PSM encryption technique

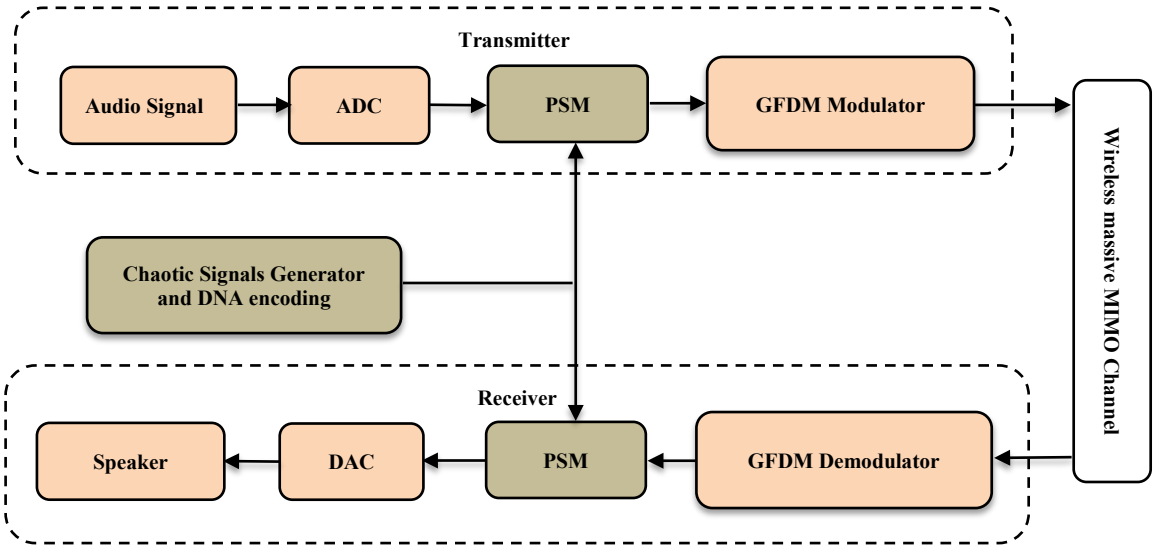


Figure 3.7 The Proposed DNA-AI-PSM over massive MIMO GFDM cryptosystem

3.3.1 Encryption/Decryption Algorithm of the Proposed DNA-AI-PSM Encryption Technique

The algorithm of the transmitter and receiver side of the proposed audio encryption can be summarized in the Block diagram shown in Figure. 3.8.

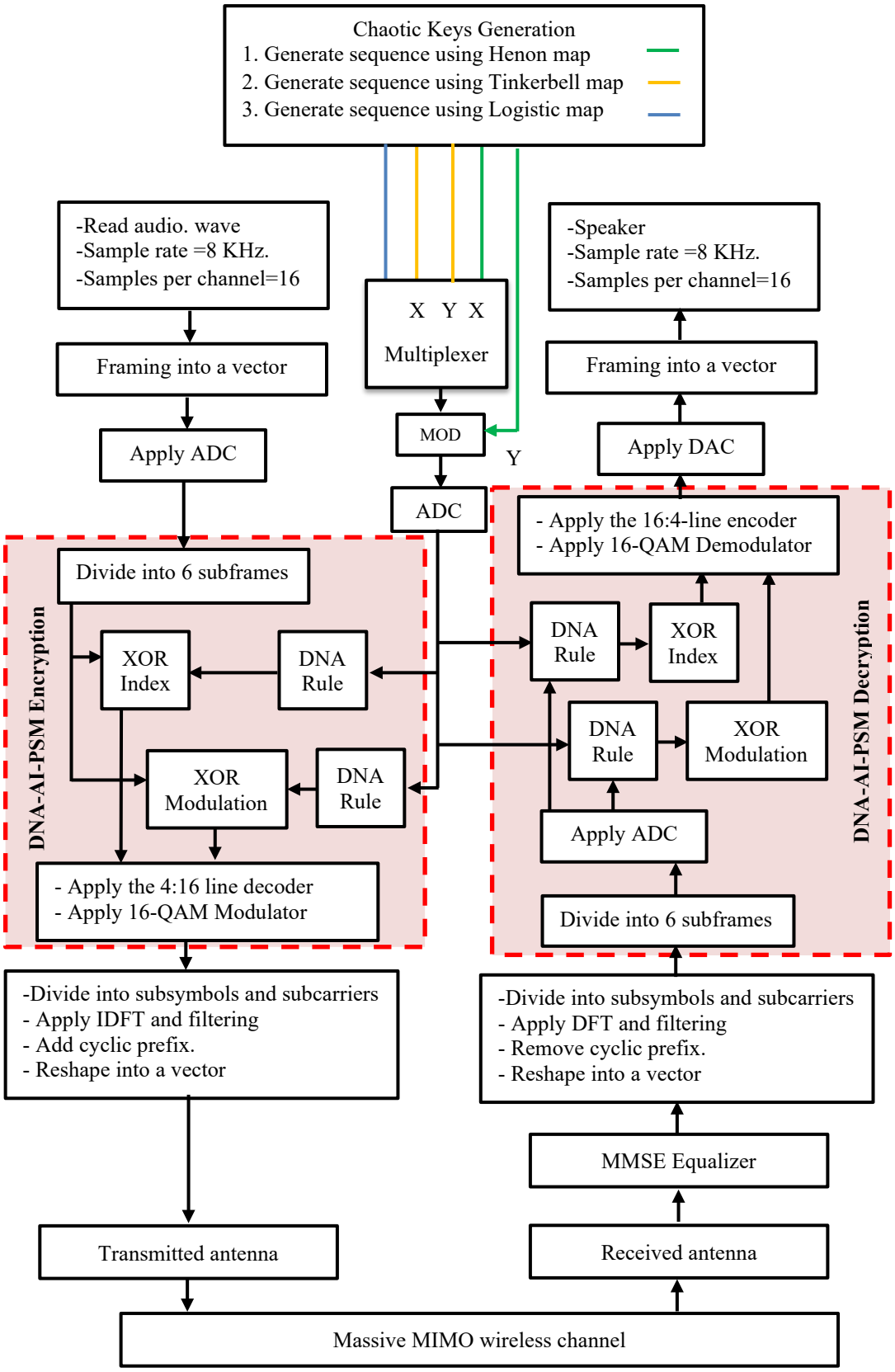


Figure 3.8 Encryption/Decryption algorithm of proposed DNA-AI-PSM technique over massive MIMO-GFDM system

3.4 Audio Encrypted based on Elliptic Curve and Hybrid Chaotic Maps inside GFDM Modulator (HC-EC-GFDM)

The Third proposed secure system depends on substitution and permutation principles. Three chaotic maps and Linear Congruential Generators on Elliptic Curve (EC-LCG) sequences are mixed separately with the data inside GFDM. The proposed GFDM modulator is shown in Figure 3.9. Substitution is performed inside the GFDM system by separating subsymbols into real and imaginary parts. Then the result of the modulo operation between the Ikeda map and the x-coordinate of EC-LCG is combined with the real part of the GFDM subsymbol. Similarly, the result of the modulo operator between the Tent map and the y-coordinate of EC-LCG is combined with the imaginary part of the GFDM subsymbol. After that, the real and imaginary parts are swapped and reconstructed data again to complex-valued. For permutation operation, the data index is randomized using the Duffing map, as shown in Figure 3.8. Now, the proposed GFDM is being implemented into 5G wireless communication networks architecture, as illustrated in Figure 3.10.

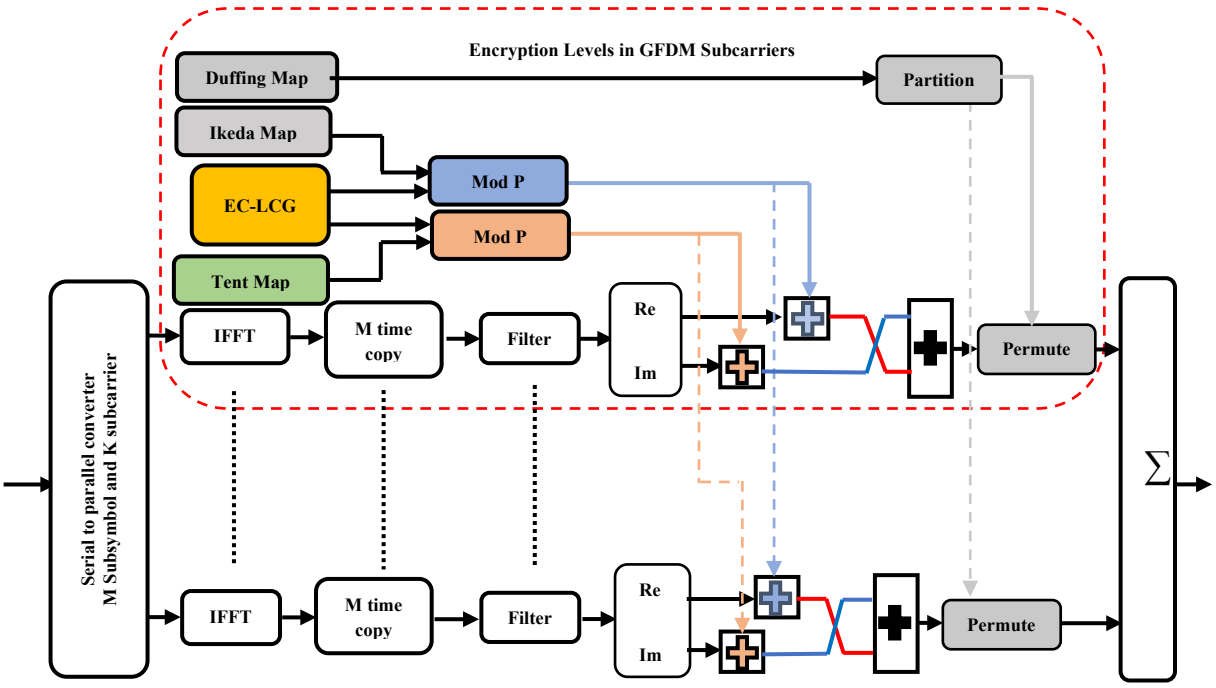


Figure 3.9 Block diagram of the proposed HC-EC-GFDM modulator

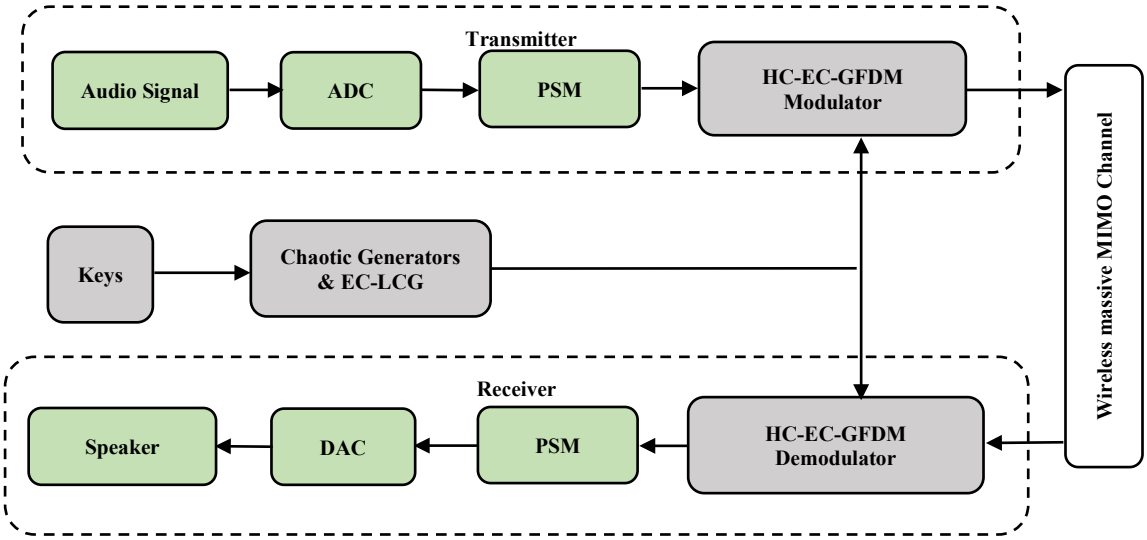


Figure 3.10 The proposed HC-EC-GFDM modulator over massive MIMO cryptosystem

3.4.1 Encryption/Decryption algorithm of the proposed HC-EC-GFDM Modulator Scheme

The algorithm of the proposed audio encryption for the transmitter and receiver side can be abbreviated in the Block diagram shown in Figure 3.11.

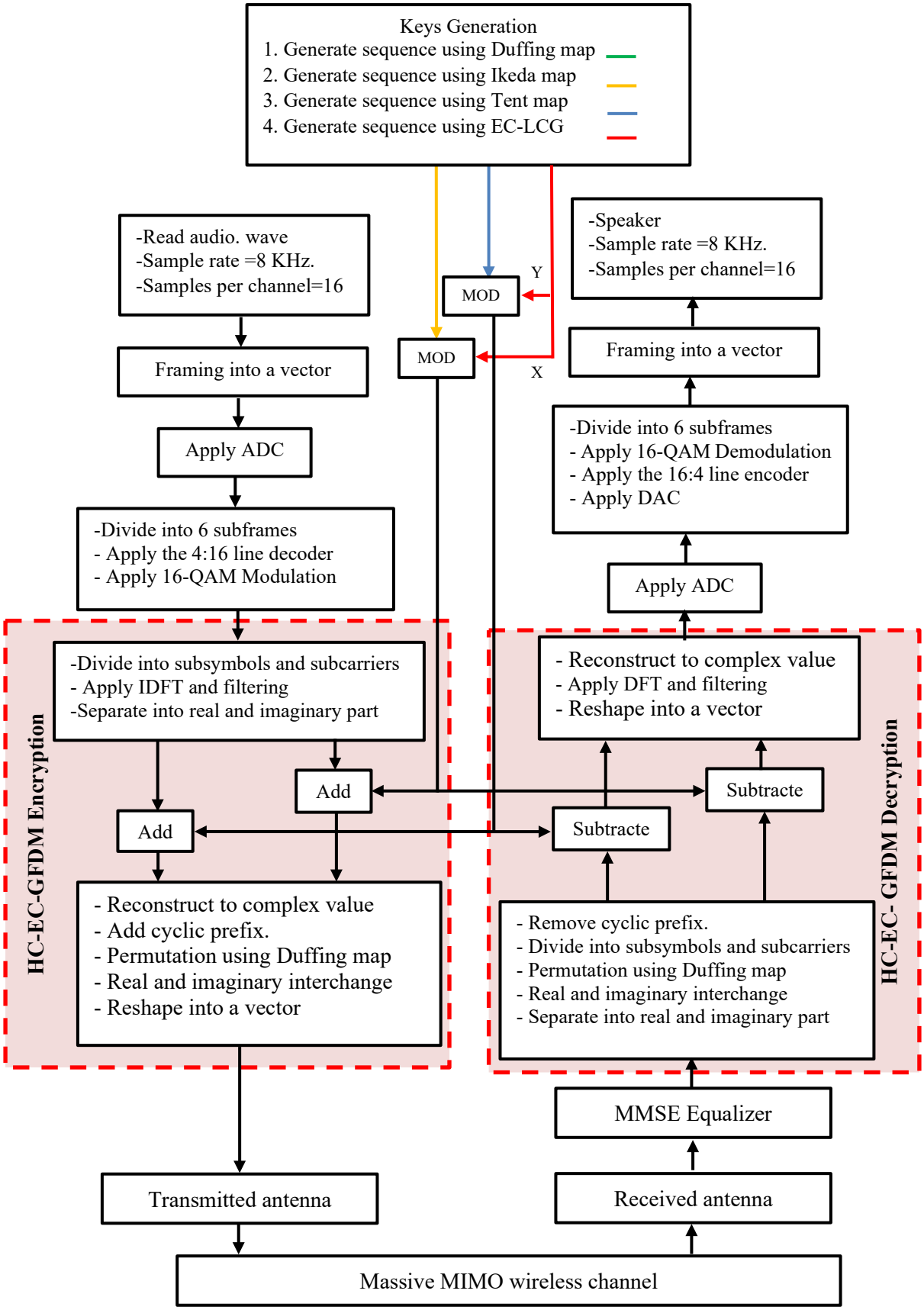


Figure 3.11 Encryption/Decryption algorithm of the proposed HC-EC-GFDM modulator over massive MIMO system

3.5 Audio Encrypted based on Linear Precoding Algorithm of Massive MIMO and Hybrid Chaotic QR-Decomposition

The fourth proposed cryptosystem introduces a new method of voice encryption wireless system based on the characteristics of massive Multiple Input Multiple Output (MIMO) wireless channels. By exploiting the Minimum Mean Square Error (MMSE) precoding technique, channel fading values are permutated and substituted using various chaotic generators. The voice samples are mixed with channel values and a chaotic sequence before being transmitted. A new two-chaotic sequence was proposed using one chaotic map's QR decomposition technique.

Let $Xh_{(n+1)}$ be a Henon signal reshaped to matrix Z_{n+1}, $Z_{n+1} \in C^{w \times w}$, $w \geq MK$, where K and M denote the numbers of subcarriers and subsymbols of GFDM modulation, respectively. Then factorization process is taken to matrix Z_{n+1} with linearly independent columns is decomposed to give an orthogonal matrix Q and an upper triangular matrix R, as in the equation below:

$$Z_{n+1} = Q_{n+1} \times R_{n+1} \tag{3.5}$$

Then after convert $Q_{n+1}\ and\ R_{n+1}$ to vector again, combining it with Bernoulli and Logistic maps, respectively, as in equations:

$$Q_{Chaotic} = Xb_{n+1} + Q_{n+1} \tag{3.6}$$

$$R_{Chaotic} = Xl_{n+1} + R_{n+1} \tag{3.7}$$

The schematic diagram of the new PRNG sequence is shown in Figure 3.12. Two PRNGs were constructed using triple chaotic maps mixed using QR factorization, called Hybrid Chaotic QR Decomposition (HC-QR).

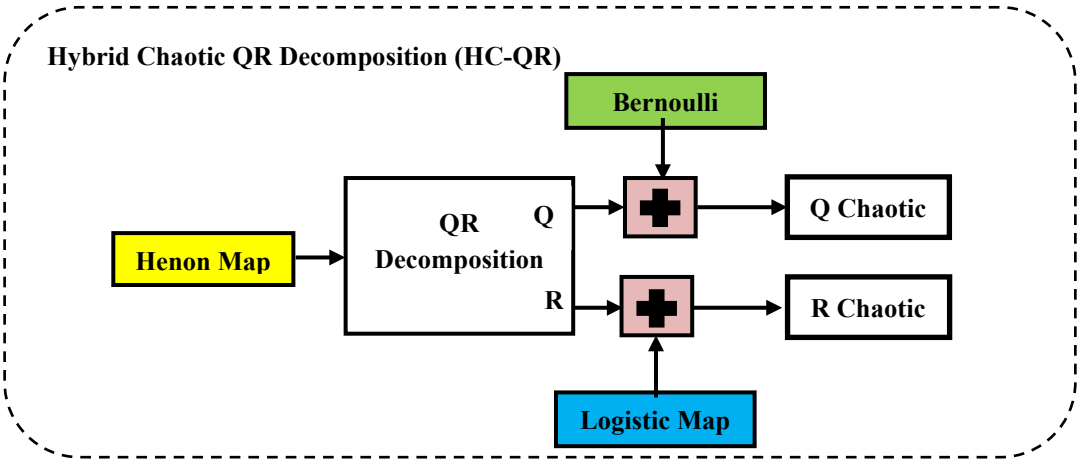


Figure 3.12 Block diagram of the proposed HC-QR sequence

The encryption processes are as follows: MMSE precoding matrix complex data will separate into real and imaginary parts. Then the real part was combined with $Q_{chaotic}$ sequence, while the imaginary part was combined with $R_{chaotic}$ sequence, and finally, reconstructed data to complex-valued and permutation it using a Tent map at the base station. HC-QR-MMSE can denote the proposed encryption algorithm for simplicity. The block diagram of the proposed audio encryption system is illustrated in Figure 3.13.

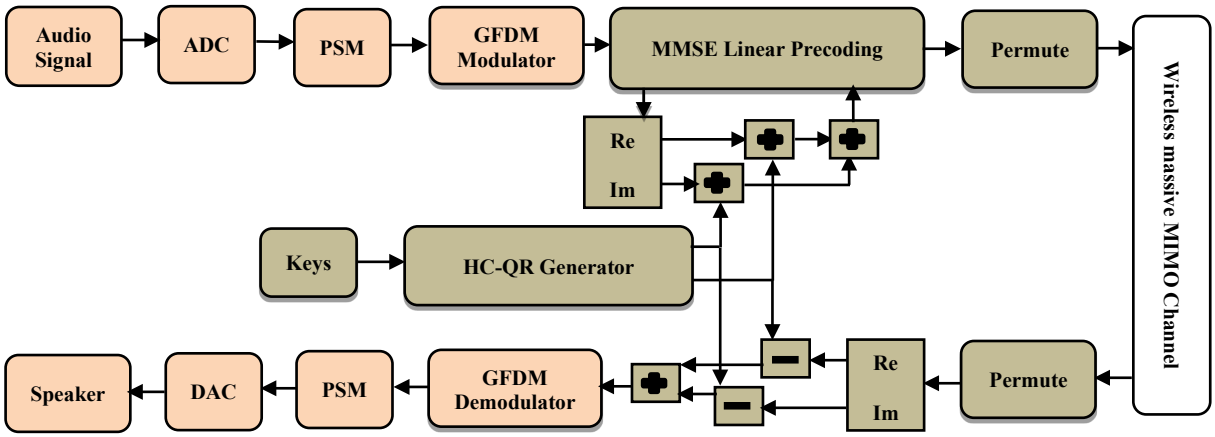


Figure 3.13 The proposed HC-QR-MMSE over massive MIMO GFDM cryptosystem

3.5.1 Encryption/Decryption algorithm of the proposed HC-QR-MMSE System

Figure 3.14 show the proposed audio encryption /decryption algorithm.

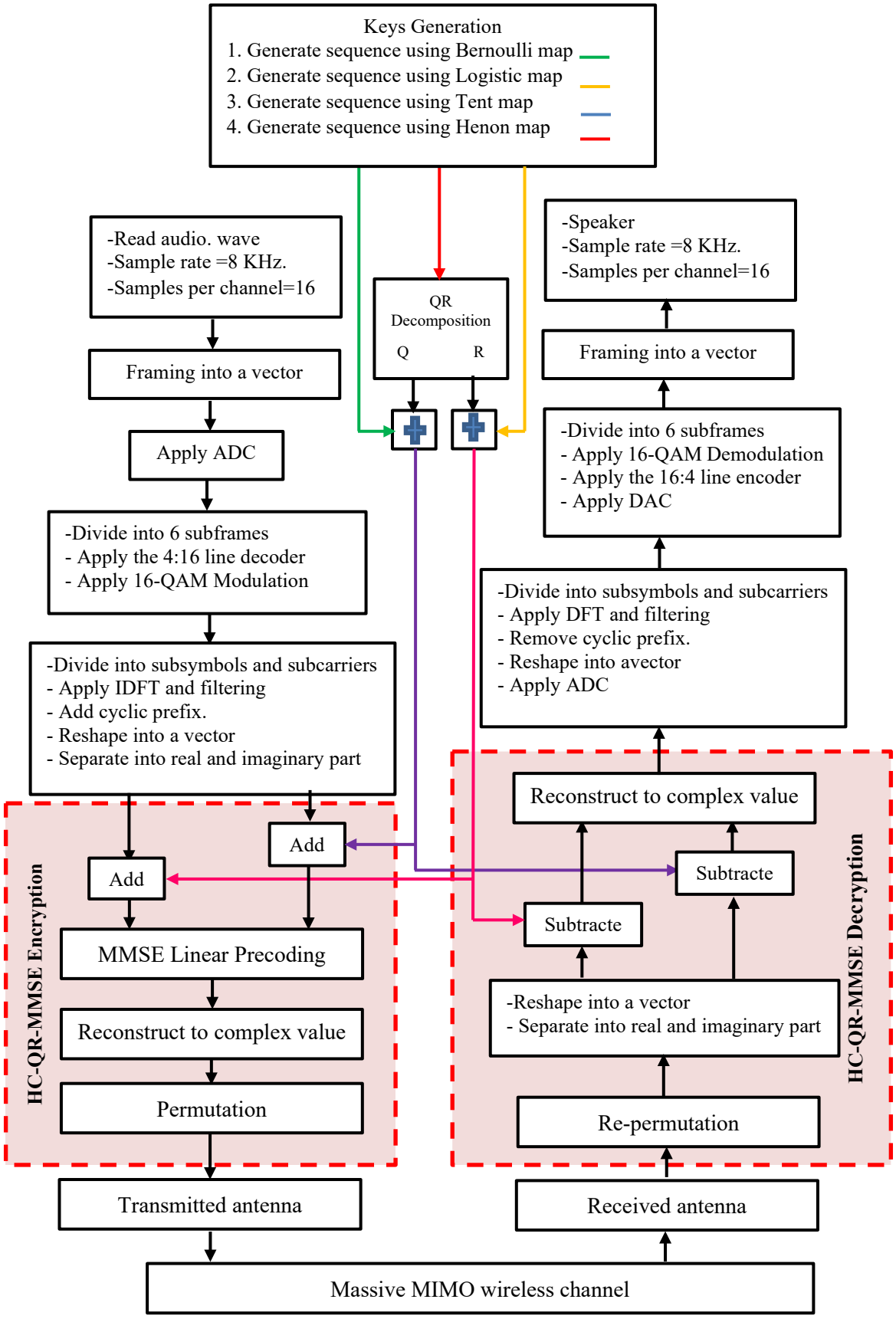


Figure 3.14 Encryption/Decryption algorithm of the proposed HC-QR-MMSE over massive MIMO-GFDM system

Chapter Four

Simulation Results of the Proposed Cryptosystems

4.1 Introduction

Multiple experiments are employed to evaluate the encrypted-decrypted audio quality strength of the proposed techniques against attacks has been verified using histogram, spectrogram, SNR, SSSNR, PSNR, percentage of Difference (P. Diff), MSE, R_{xy}, d_{LPC}, d_{LOG}, d_{FWLOG} ,d_{CD}, RMS, CF, NSCR and UACI, key space, and key sensitivity. Also, present the effect of channel noise on the decrypted audio at different SNR values. Finally, all proposed cryptosystems feature were compared to existing competitors, and the results show that the proposed cryptosystems are superior to the previous ones. Audio parameters were used through the simulation listed in Table 4.1. The proposed algorithm is implemented in Matlab R2020a under Windows 10, using a PC with Intel(R) Core (TM) i7-7500U @ 2.70 GHz 2.9 GHz, 8 GB RAM, and a 64-bit operating system.

Table 4.1. Audio parameters

Audio speech	400-3200 Hz
Sample rate	8000 sample/Sec.
Number of bits per sample	16
Bit rate	128 Kbps
Duration	1,2,3,4 and 5 Sec.

4.2 Simulation Results of the HCMO Technique

Simulation tests are performed to examine the efficiency of using Bogdanov, Bernoulli, and Standard chaotic maps for encrypting audio before its transmission through a massive MIMO PSM GFDM system.

4.2.1 Subject Test of HCMO Encryption Technique

The encrypted audio has been listened to, and it appeared to be incomprehensible, so the HCMO technique has a high-security level.

4.2.2 R.I. of HCMO Encryption Technique

The data should be secure against eavesdroppers; therefore, the encryption system must be strong as possible in proportion to its value. R.I. is a useful metric for evaluating and determining the security requirement of a system. When audio R.I. is low, it indicates that the audio is unclear (more security). Five audio clips at different lengths have been used. A group of tests was used for evaluating R.I., as shown in tables 4.2-4.4.

Table 4.2. R.I. in terms of SNR, PSNR, and SSSNR for HCMO Technique

Audio	Length (Sec.)	SNR (dB)	PSNR (dB)	SSSNR (dB)
Audio-1	1	-19.3106	4.7287	-25.8998
Audio-2	2	-22.4528	4.7324	-30.3125
Audio-3	3	-23.5969	4.7569	-31.0528
Audio-4	4	-21.5716	4.7666	-30.3041
Audio-5	5	-21.5949	4.7552	-30.8738

Table 4.3. R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for HCMO Technique

Audio	Length (Sec.)	d_{LPC}	d_{CD}	d_{LOG}	d_{FWLOG}
Audio-1	1	1.0286	9.2242	20.1622	11.3496
Audio-2	2	1.6094	9.9496	23.6166	12.6138
Audio-3	3	0.9612	8.1925	21.1417	23.0908
Audio-4	4	1.2588	8.9487	20.6966	18.2117
Audio-5	5	1.6202	10.0536	21.7119	19.2973

Table 4.4. R.I. in terms of MSE, RMS, CF,and R_{xy} for HCMO Technique

Audio	Length (Sec.)	MSE	RMS	CF	R_{xy}
Audio-1	1	0.3366	0.5780	4.7601	0.0194
Audio-2	2	0.3363	0.5778	4.7638	-0.0105
Audio-3	3	0.3344	0.5773	4.7698	0.0069
Audio-4	4	0.3336	0.5757	4.7949	0.0024
Audio-5	5	0.3345	0.5766	4.7821	0.00412

From a statistical point of view, the audio signal amplitude varies from one clip to another; therefore, the measurement can take different values in the proposed system.

4.2.3 Key Space, Sensitivity, and time Analysis for HCMO Technique

The key Space of each chaotic Map used in the proposed system is listed in Table 4.5.

Table 4.5. Key Space of Chaotic Maps used in HCMO Technique

Chaotic Maps	Number of Control Parameters	Number of Initial conditions	Keyspace
Bernoulli	1	1	$(10^{15})^2 \approx 2^{100}$
Standard	1	2	$(10^{15})^3 \approx 2^{150}$
Bogdanov	3	2	$(10^{15})^5 \approx 2^{250}$

If the computation precision of Matlab R2020a is around (10^{-15}), which means that the possible values of each secret key can take $(10^{15} \approx 2^{50})$, then the overall keys space of the proposed model has ten secret keys; therefore, the overall key space $(2^{50})^{10} = 2^{500}$. The key sensitivity test of the proposed HCMO technique can be achieved by slightly modifying one of the parameter keys while the rest of the parameters remain unchanged during implementation. The statistical measurements to show the sensitivity key is

the P. Diff., R_{xy},d_{CD}, MSE, and SSSNR are illustrated in Table 4.6. The proposed cryptosystem secret keys are X_b (0)= 0.025, μ_b (0)=0.99, P(0)=0, $\Theta(0)$=0.1 K(0)=0.971635, X_{bog}(0)= 0.9, Y_{bog} (0)=0.37,k(0)=1.2, $\varepsilon(0)$=0 and μ_{bog} (0)=0.

Table 4.6. Key sensitivity test of HCMO Technique using audio-3

Map	Change key	R_{xy}	MSE	d_{CD}	SSSNR	P. Diff
Bernoulli	X_b (0)+10^{-8}	0.0069	0.3344	8.1925	-31.0528	100%
	μ_b (0)+10^{-8}	-0.0044	0.3317	8.2629	-31.015	100%
Standard	P(0)+10^{-8}	-0.0073	0.3336	8.2942	-31.0417	100%
	$\Theta(0)$+10^{-8}	0.0070	0.3329	8.2235	-31.0333	99.995%
	K(0) +10^{-8}	0.0051	0.3324	8.3212	-31.0338	100%
Bogdanov	X_{bog} (0)+10^{-8}	0.1216	0.0929	8.2783	-22.2161	99.98%
	Y_{bog} (0)+10^{-8}	0.0988	0.1159	8.2302	-23.4951	99.98%
	μ_{bog} (0)+10^{-8}	0.0120	0.3299	8.2444	-30.9252	100%
	k(0)+10^{-8}	0.1037	0.10956	8.205	-23.1687	99.98%
	$\varepsilon(0)$+10^{-8}	-0.0026	0.3311	8.2181	-30.932	100%

The computational time required for the encryption/decryption algorithm can be summarized using five audio files in Table 4.7.

Table 4.7. Time analysis for HCMO Technique

Audio file	Length (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	1	16.0 KB	0.017	10.625×10^{-7}
Audio-2	2	32.0 KB	0.021	6.562×10^{-7}
Audio-3	3	48.0 KB	0.032	6.67×10^{-7}
Audio-4	4	64.0 KB	0.036	5.625×10^{-7}
Audio-5	5	80.0 KB	0.038	4.75×10^{-7}

The computational time of the proposed HCMO encryption system is between (0.017-0.038) seconds. The estimated time can be neglected compared to the time required to operate all system components. Therefore, it means that the proposed HCMO technique works in real-time.

4.2.4 Resistance against differential attacks for HCMO Technique

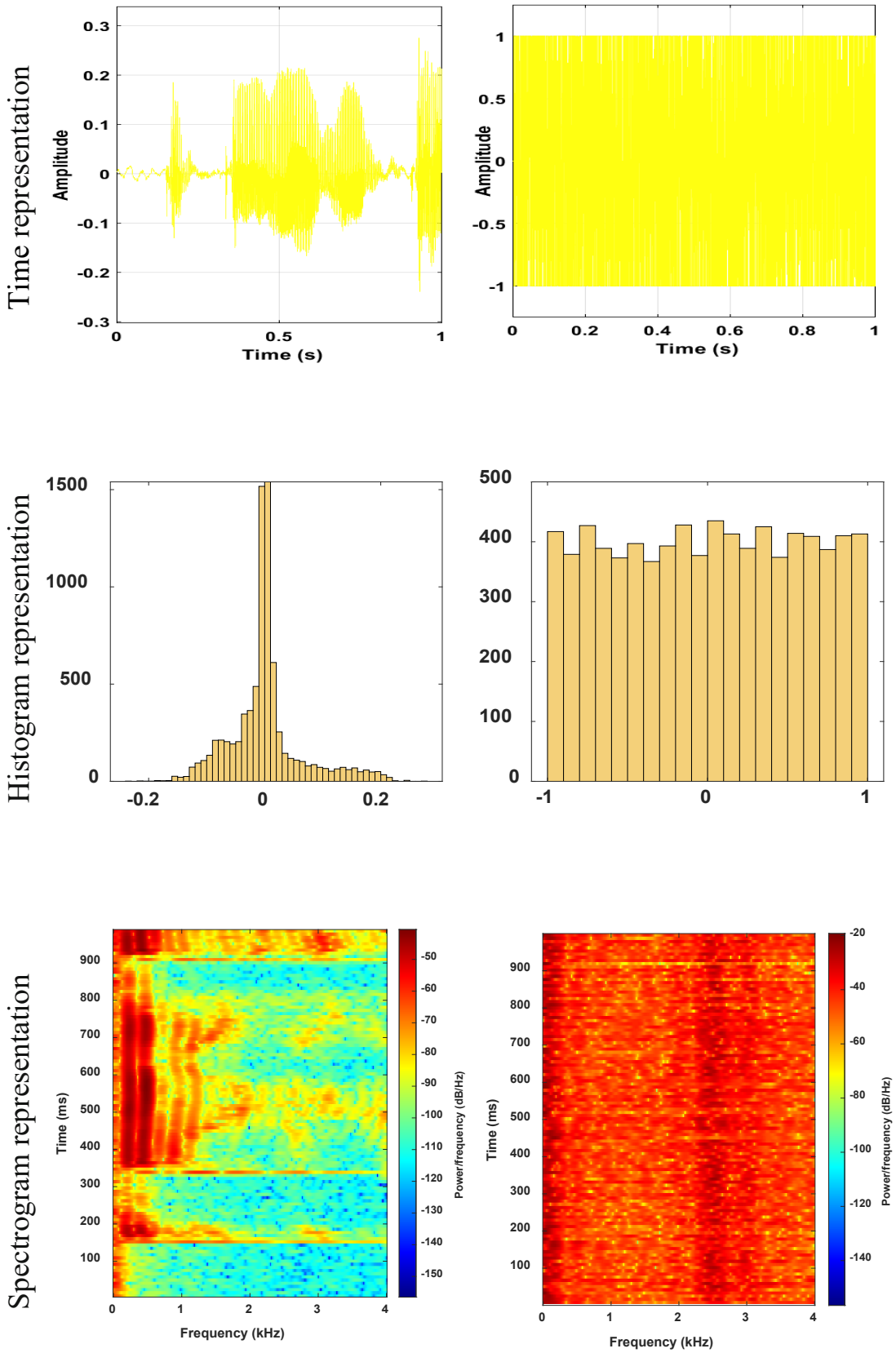
Resistance against differential attacks is a strong indicator of the strength of an encryption algorithm. NSCR and UACI tests are used to evaluate this resistance. Table 4.8 shows the results of the tests, demonstrating that the suggested system is very resistant to differential attacks.

Table 4.8. UACI and NSCR analysis for HCMO Technique

Audio	Length (Sec.)	UACI	NSCR
Audio-1	1	33.337%	99.98%
Audio-2	2	33.335%	99.99%
Audio-3	3	33.334%	99.99%
Audio-4	4	33.334%	99.99%
Audio-5	5	33.334%	99.99%

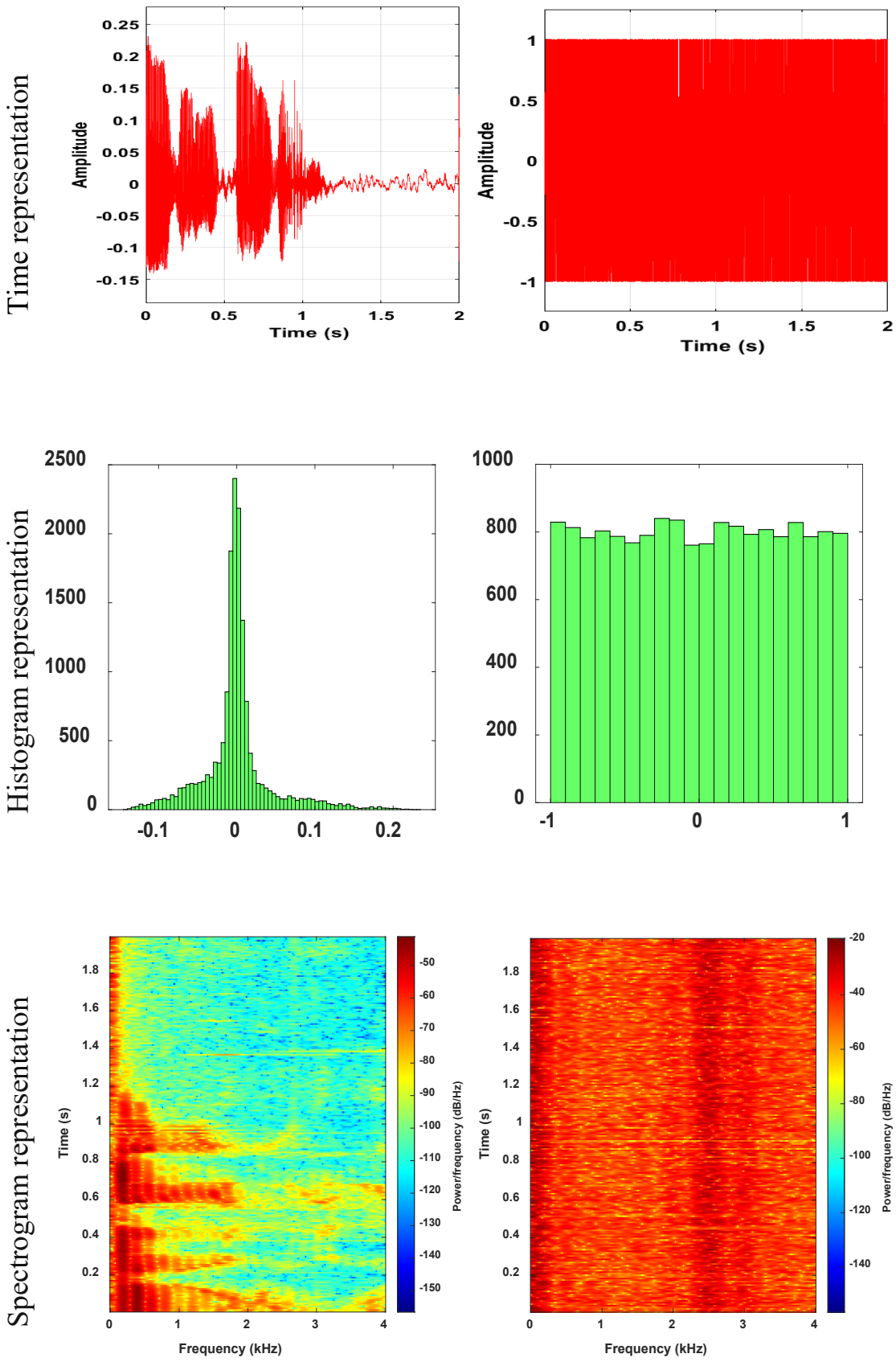
4.2.5 Waveforms Plot of HCMO Technique

Another useful tool for analyzing audio waveforms is a graphical representation of the original and encrypted audio. These include time, histogram, and spectrogram representations, as shown in Figures 4.1, 4.2, 4.3, 4.4, and 4.5 for Audio-1, Audio-2, Audio-3, Audio-4, and Audio-5, respectively.



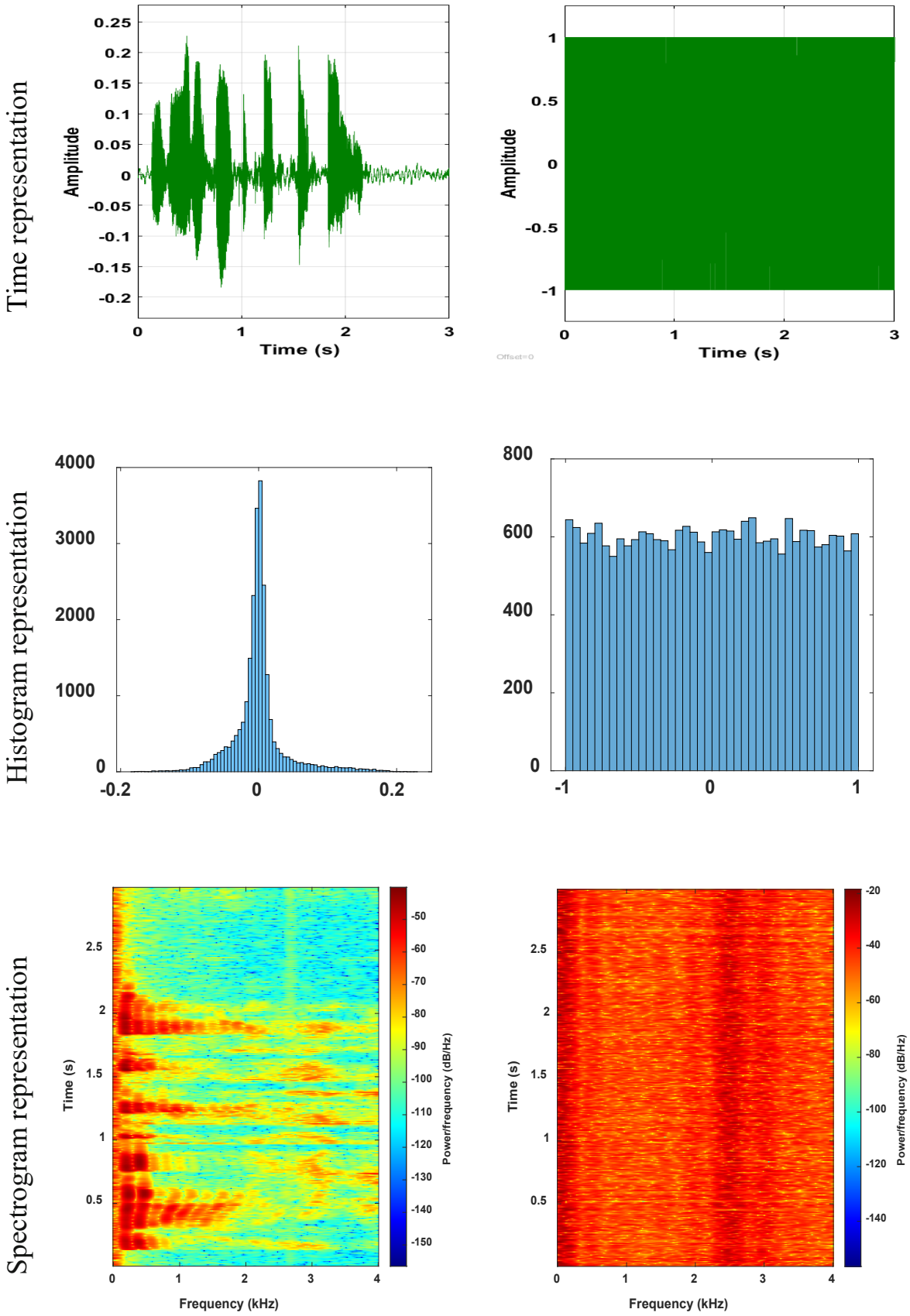
Original audio Encrypted audio

Figure 4.1 Waveform Results of Audio-1



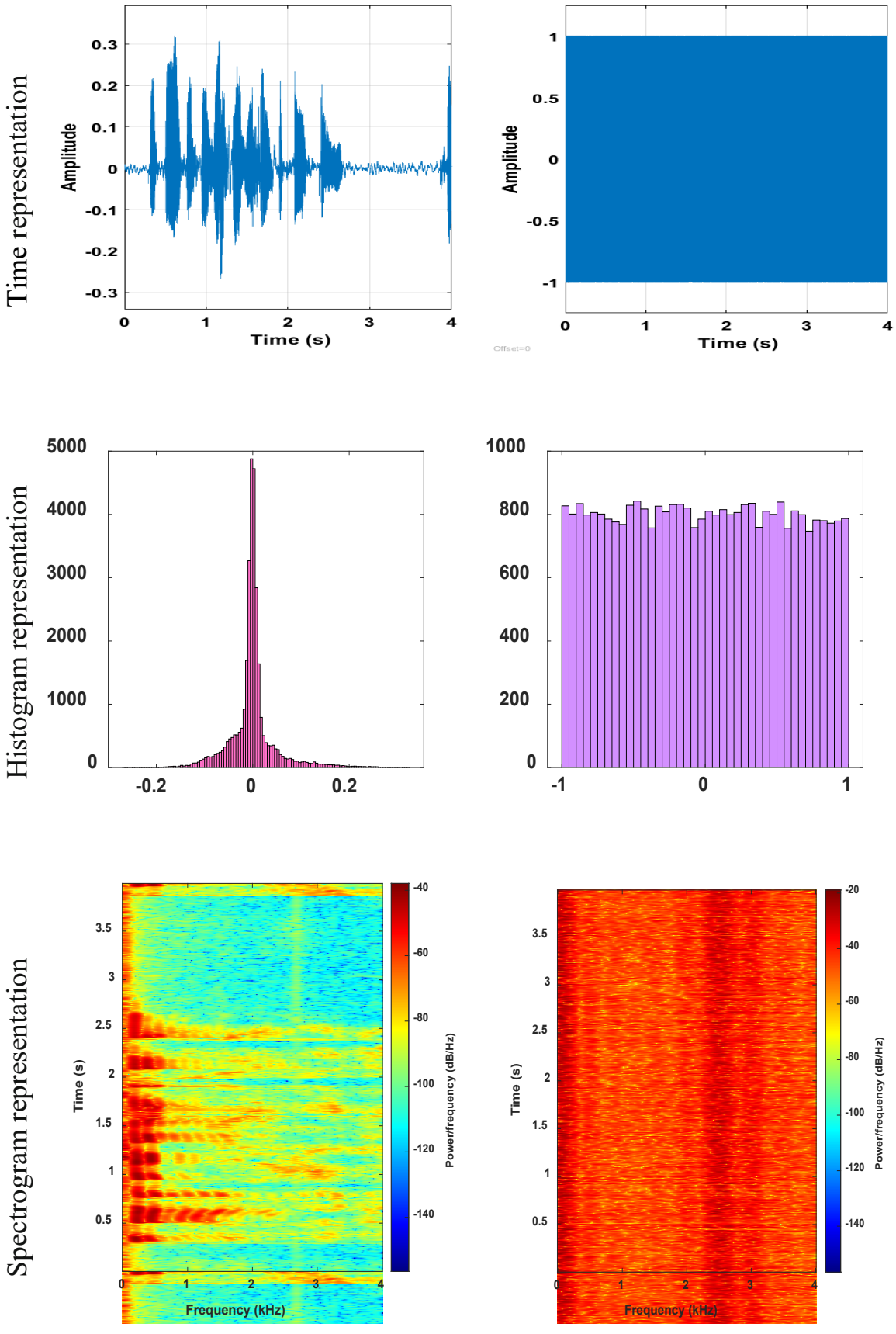
Original audio Encrypted audio

Figure 4.2 Waveform Results of Audio-2



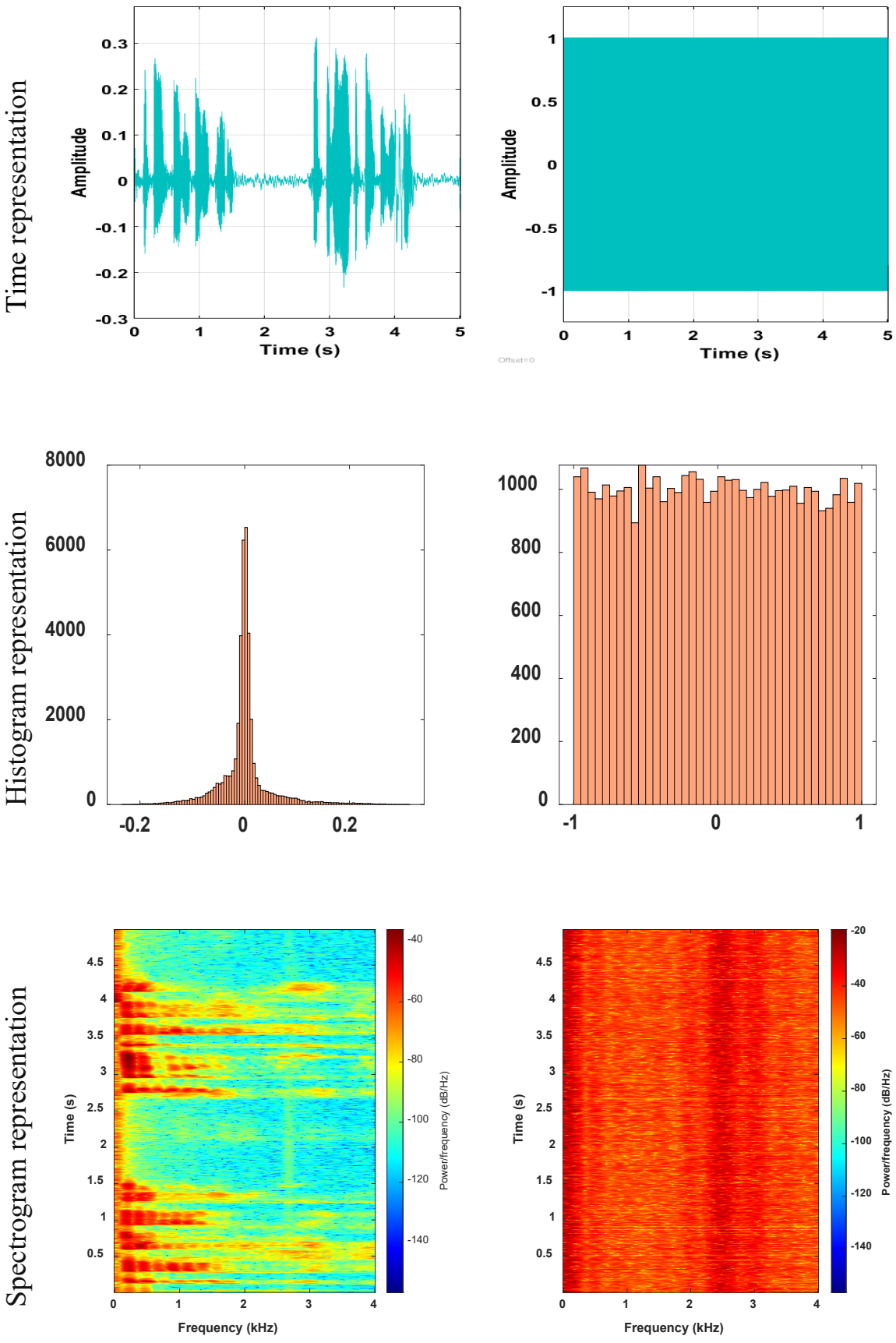
Original audio Encrypted audio

Figure 4.3 Waveform Results of Audio-3



Original audio Encrypted audio

Figure 4.4 Waveform Results of Audio-4



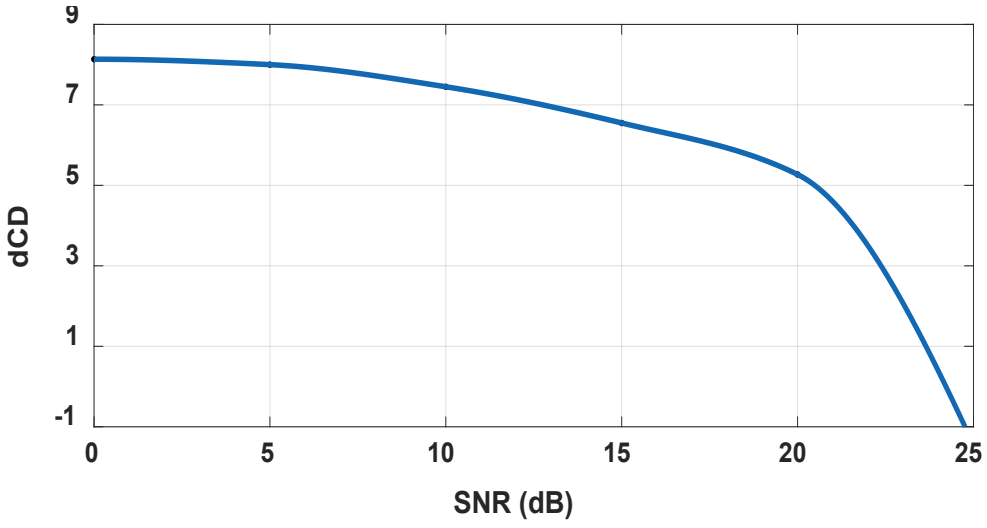
Original audio Encrypted audio

Figure 4.5 Waveform Results of Audio-5

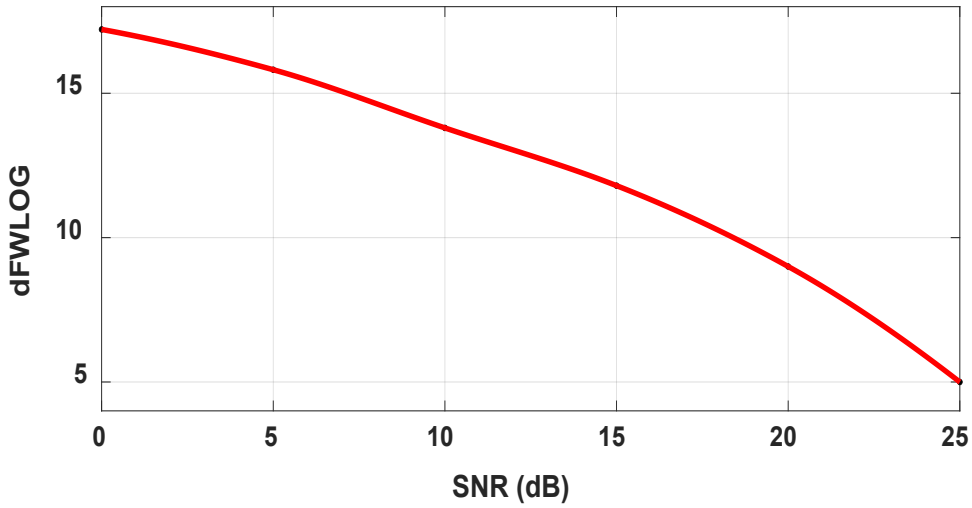
The discussion of Figures 4.1, 4.2, 4.3, 4.4, and 4.5 is as follows: in the time domain, there is no silent part in the encrypted audio, so it seems like noise. The histogram of encrypted audio appears flat, meaning the encrypted audio samples have approximately similar values. In the spectrogram, encrypted audio has higher power and is distributed equally over audio length. Therefore, the eavesdroppers cannot discover any information about the original audio. These statistical analyses proved that the proposed HCMO encryption has a high-security level.

4.2.6 Noise Effect on HCMO Technique for massive PSM GFDM System

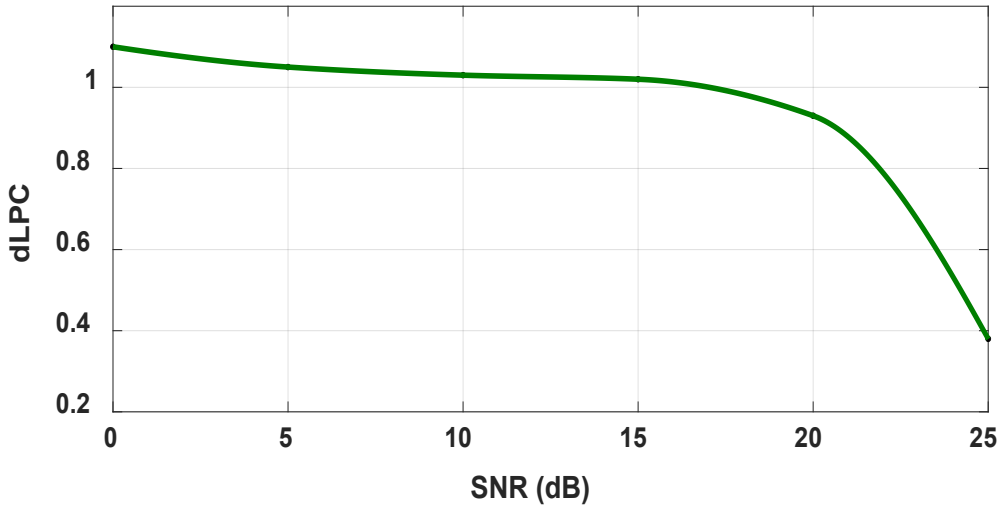
In this part of the simulation results, the impact of noise on the recovered audio at the receiver was examined by calculating d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR, PSNR, MSE, RMS, and CF between original audio and recovered audio of the proposed HCMO technique at different SNR values as shown in Figure 4.6.



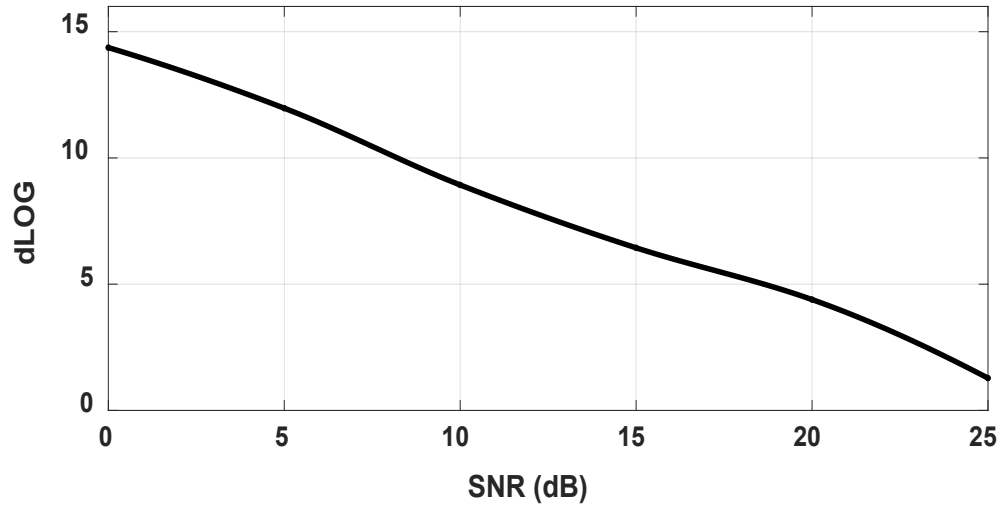
(A)


dFWLOG
15
10
5
0
5
10
15
20
25
SNR (dB)

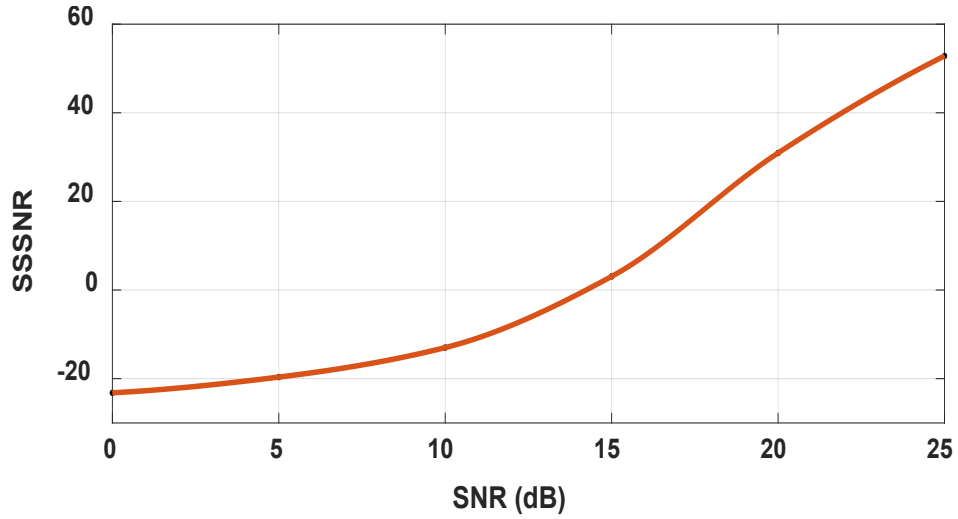
(B)


dLPC
1
0.8
0.6
0.4
0.2
0
5
10
15
20
25
SNR (dB)

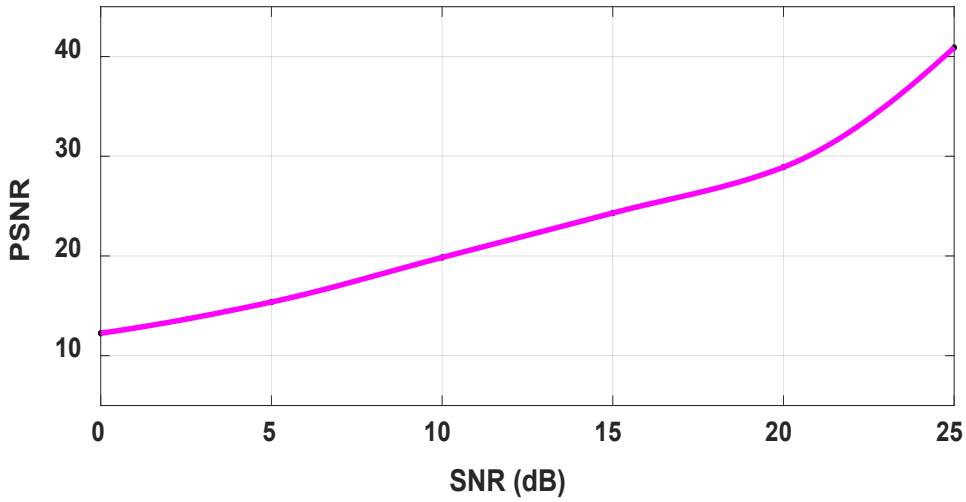
(C)


dLOG
15
10
5
0
0
5
10
15
20
25
SNR (dB)

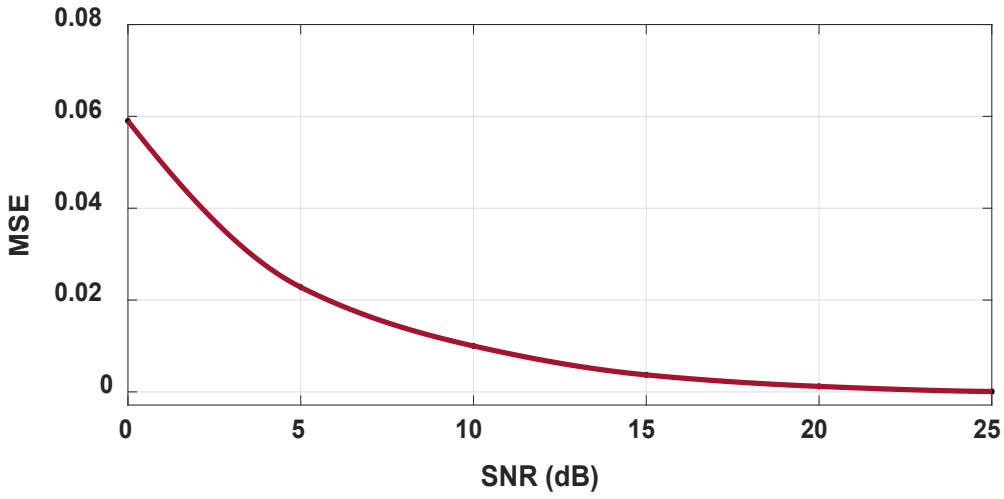
(D)


SSSNR
60
40
20
0
-20
0
5
10
15
20
25
SNR (dB)

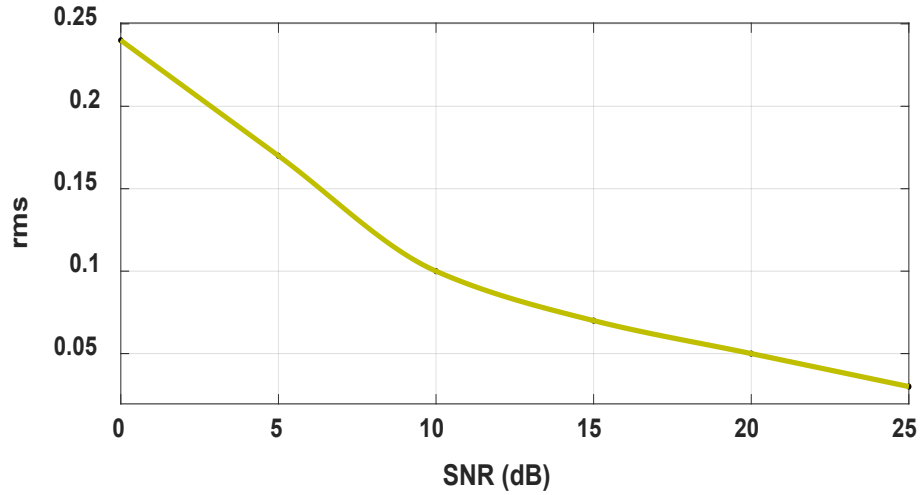
(E)


PSNR
40
30
20
10
0
5
10
15
20
25
SNR (dB)

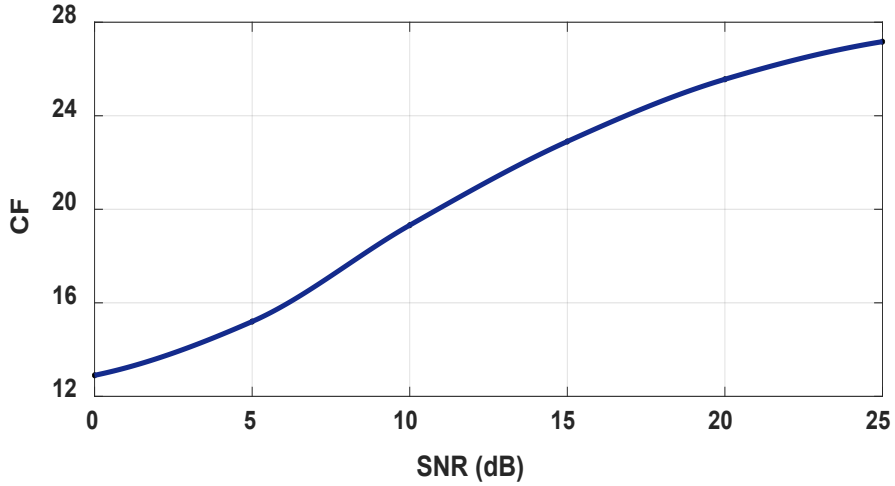
(F)


MSE
0.08
0.06
0.04
0.02
0
0
5
10
15
20
25
SNR (dB)

(G)



(H)



(I)

Figure 4.6. A, B,C,D,E,F,G,H,I variation of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS and CF, respectively, for the recovered audio-3 of the proposed HCMO Encryption Technique

4.2.7 Performance Analysis of HCMO Technique

The investigation of the security performance in terms of the bit error rate (BER) was achieved, as shown in Figure 4.7. The BER of the authorized receiver and the eavesdropping receiver, without knowing the secret keys for chaotic sequences, were tested. The plot shows that the eavesdropper could not retrieve the information without the secret keys due to the high BER of around 0.5. However, the legitimate receiver could obtain the information with an acceptable BER.

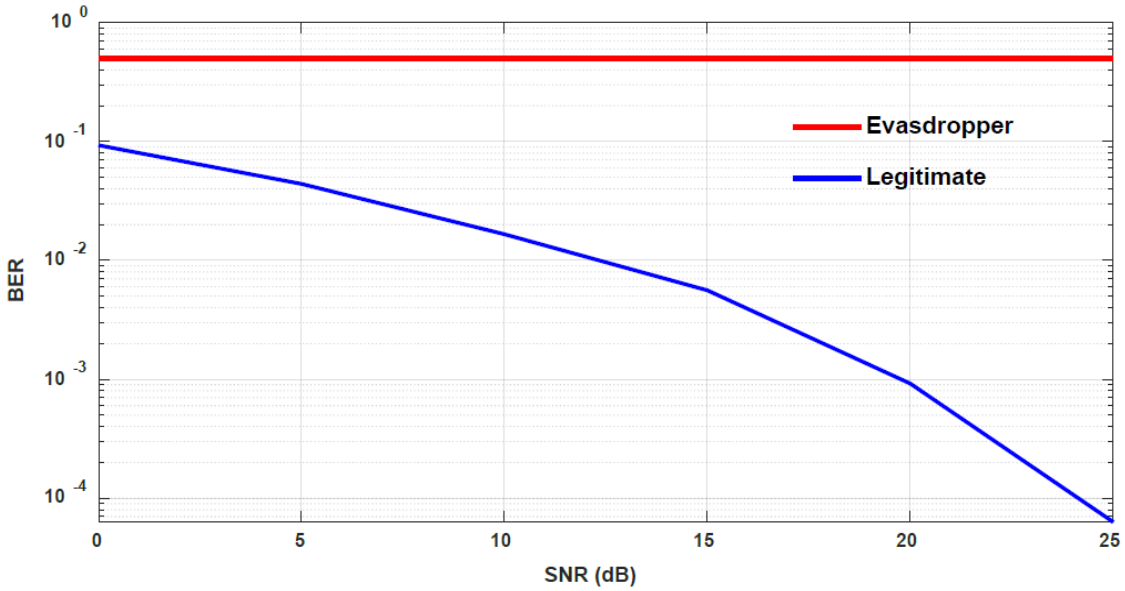


Figure 4.7 BER performance of authorized and eavesdropper receiver of HCMO technique

4.3 Simulation Results of DNA-AI-PSM Encryption Technique

Simulation measurements of the proposed DNA-AI-PSM encryption technique are investigated to determine the system's security level using DNA coding, Henon, Tinkerbell, and Logistic chaotic maps for scrambling audio before transmission through a massive MIMO GFDM system.

4.3.1 Subject Test of DNA-AI-PSM Encryption Technique

Listening to the scrambled audio findings demonstrates that the DNA-AI-PSM approach has a high-security level.

4.3.2 R.I. of DNA-AI-PSM Encryption Technique

The capabilities of the proposed scheme can be evaluated in this section using five audio clips of different lengths. R.I. was assessed using a variety of tests, as can be seen in the tables 4.9-4.11.

Table 4.9. R.I. in terms of SNR, PSNR, and SSSNR for DNA-AI-PSM Technique

Audio	Length (Sec.)	SNR (dB)	PSNR (dB)	SSSNR (dB)
Audio-1	1	-20.131	3.7263	-26.9021
Audio-2	2	-23.4024	3.7828	-31.2501
Audio-3	3	-24.544	3.8099	-31.9924
Audio-4	4	-22.5672	3.771	-31.3039
Audio-5	5	-22.589	3.761	-31.8606

Table 4.10. R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for DNA-AI-PSM Technique

Audio	Length (Sec.)	d_{LPC}	d_{CD}	d_{LOG}	d_{FWLOG}
Audio-1	1	1.1243	8.5414	20.977	12.4163
Audio-2	2	1.8709	9.0687	24.1857	13.8676
Audio-3	3	1.0257	7.3827	21.787	26.3629
Audio-4	4	1.4353	8.084	21.3513	20.792
Audio-5	5	1.8921	9.1695	22.301	21.8465

Table 4.11. R.I. in terms of MSE, RMS, CF, and R_{xy} for DNA-AI-PSM Technique

Audio	Length (Sec.)	MSE	RMS	CF	R_{xy}
Audio-1	1	0.424	0.64922	3.7519	0.0176
Audio-2	2	0.41853	0.94533	3.8041	-0.0028
Audio-3	3	0.4159	0.64375	3.8254	-0.00097
Audio-4	4	0.41966	0.6467	3.7856	0.01422
Audio-5	5	0.42063	0.6466	3.7865	-0.0026

4.3.3 Key Space, Sensitivity, and time Analysis for DNA-AI-PSM Technique

Table 4.12 lists each chaotic Map's key space used in the suggested encryption system.

Table 4.12. Key Space of Chaotic Maps used in DNA-AI-PSM Technique

Chaotic Maps	Number of Control Parameters	Number of Initial conditions	Keyspace
Logistic	1	1	$(10^{15})^2 \approx 2^{100}$
Henon	2	2	$(10^{15})^4 \approx 2^{200}$
Tinkerbell	2	4	$(10^{15})^6 \approx 2^{300}$
DNA	Eight rules		$(2^4)^8=2^{32}$

The keys space of the proposed model has twelve secret keys with eight DNA rules; therefore, the overall keyspace $(2^{50})^{12} .2^{32}= 2^{632}$. The key sensitivity test of the proposed DNA-AI-PSM technique can be achieved by a tiny change to one of the parameter keys, while the rest of the parameters remain unchanged during implementation. The statistical measurements to show the sensitivity key are illustrated in Table 4.13. The proposed system's secret keys are: $a_h = 1.4, b_h = 0.3, X_h(0) = 0.5, Y_h(0) = 0.5, r = 3.7, X_l(0) = 0.5, a_t = 0.9, b_t = -0.6013, c = 2, d = 0.5, X_t(0) = -0.72, and\ Y_t(0) = -0.64$

Table 4.13. Key sensitivity of DNA-AI-PSM Technique using audio-3

Map	Change key	R_{xy}	MSE	d_{CD}	SSSNR	P. Diff
Henon	a_h +10^{-8}	0.016	0.4132	7.3469	-31.9759	99.978%
	b_h+10^{-8}	-0.0041	0.4135	7.4202	-31.9684	99.975%
	$X_h(0) + 10^{-8}$	-0.00097	0.4159	7.3827	-31.9924	99.983%
	$Y_h(0) + 10^{-8}$	-0.00043	0.416	7.4458	-31.9921	99.995%
Logistic	r+10^{-8}	0.00259	0.13321	6.7143	-26.793	99.966%
	$X_l(0) + 10^{-8}$	0.0210	0.13391	6.6668	-26.8085	99.95%
Tinkerbell	a_t +10^{-8}	0.0253	0.2071	7.2966	-28.886	99.958%
	b_t+10^{-8}	0.0127	0.2083	7.2531	-28.875	99.966%
	c +10^{-8}	0.0174	0.2086	7.2415	-28.8884	99.954%
	d +10^{-8}	0.0161	0.2078	7.2832	-28.8753	99.975%
	$X_t(0) + 10^{-8}$	0.0334	0.2072	7.2624	-28.8631	99.966%
	$Y_t(0) + 10^{-8}$	0.0153	0.2059	7.2749	-28.8287	99.975%

The computational time can be summarized using five audio files in Table 4.14.

Table 4.14. Time analysis for DNA-AI-PSM Technique

Audio file	Length (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	1	16.0 KB	0.013	8.12×10^{-7}
Audio-2	2	32.0 KB	0.027	8.4×10^{-7}
Audio-3	3	48.0 KB	0.045	9.3×10^{-7}
Audio-4	4	64.0 KB	0.054	8.4×10^{-7}
Audio-5	5	80.0 KB	0.064	8×10^{-7}

4.3.4 Resistance against differential attacks for DNA-AI-PSM Technique

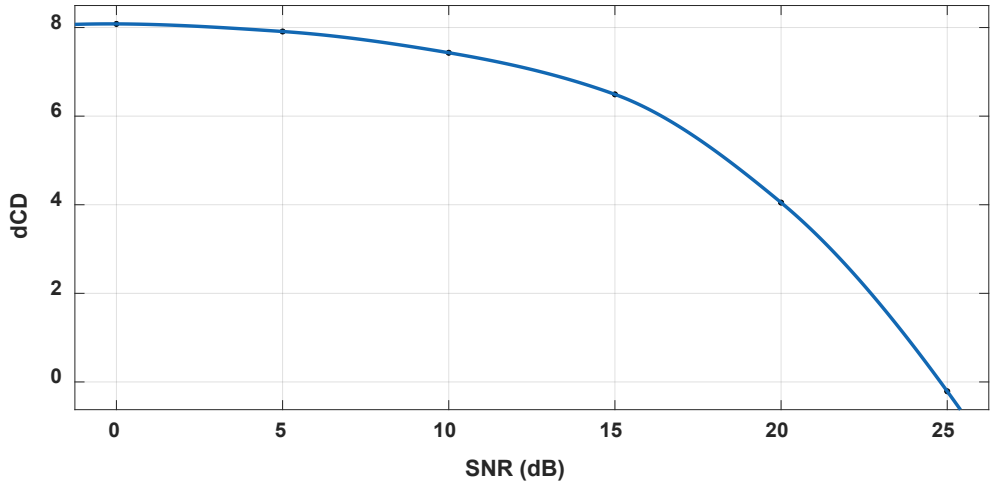
The encryption algorithm can resist a differential attack if tiny changes occur in the clear audio, significantly affecting the scrambled audio. As a result, NSCR and UACI were determined to estimate the robustness of the presented algorithm and how well the algorithm can resist differential attacks. Table 4.15 exhibits test results, demonstrating that the suggested system resists differential attacks.

Table 4.15. UACI and NSCR analysis for DNA-AI-PSM Technique

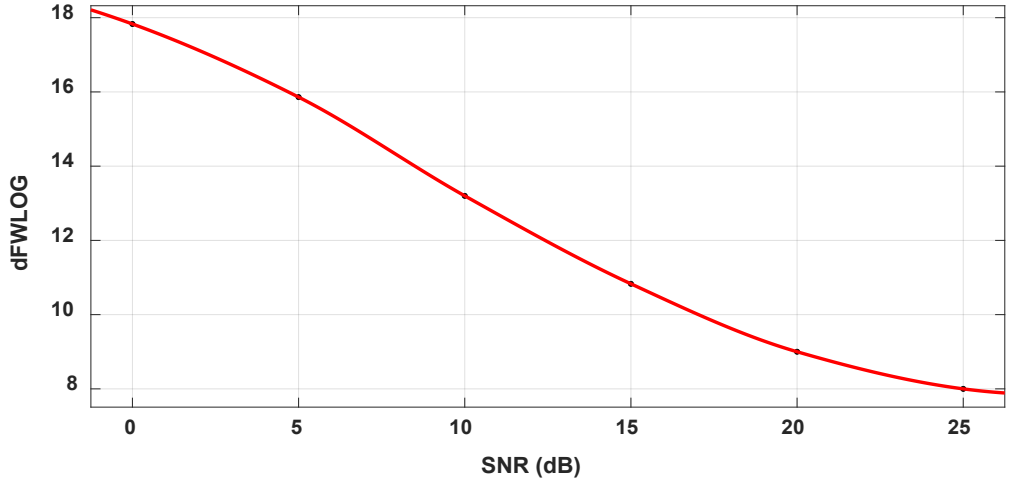
Audio	Length (Sec.)	UACI	NSCR
Audio-1	1	33.334%	99.987%
Audio-2	2	33.334%	99.975%
Audio-3	3	33.334%	99.979%
Audio-4	4	33.334%	99.99%
Audio-5	5	33.334%	99.987%

4.3.5 Noise Effect on DNA-AI-PSM Technique over massive MIMO GFDM System

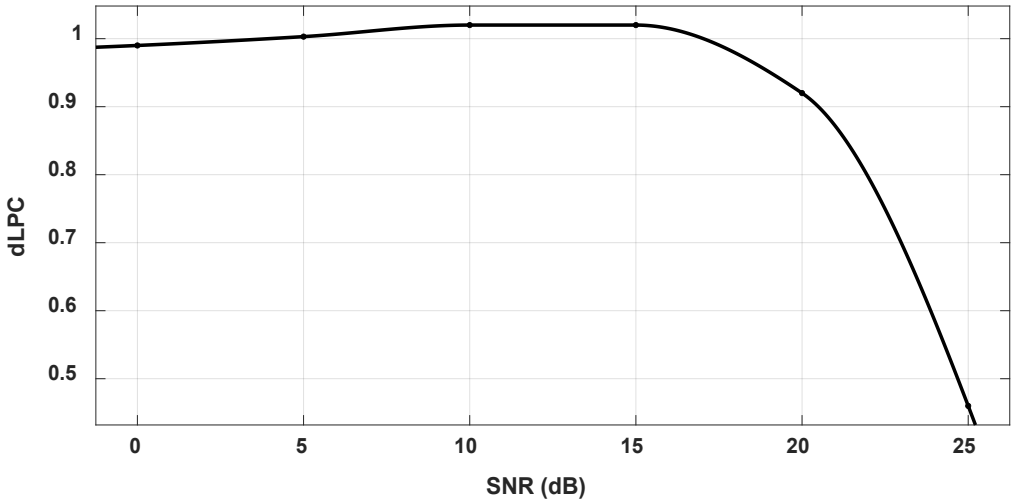
The impact of channel noise on the decrypted audio signal at the receiver was tested by evaluating d_{CD}, d_{FWLOG}, $d_{LPC,}d_{LOG}$, SSSNR ,PSNR ,MSE ,RMS, and CF between the clear and decrypted audio signal of the secure massive MIMO GFDM system at different SNR values as shown in Figure 4.8.


dCD
SNR (dB)
0
2
4
6
8
0
5
10
15
20
25

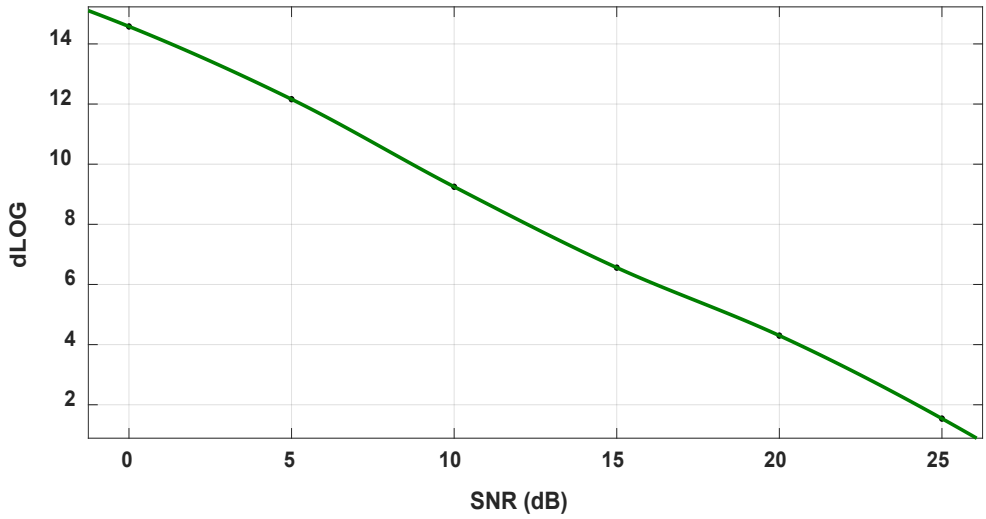
(A)


dFWLOG
SNR (dB)
8
10
12
14
16
18
0
5
10
15
20
25

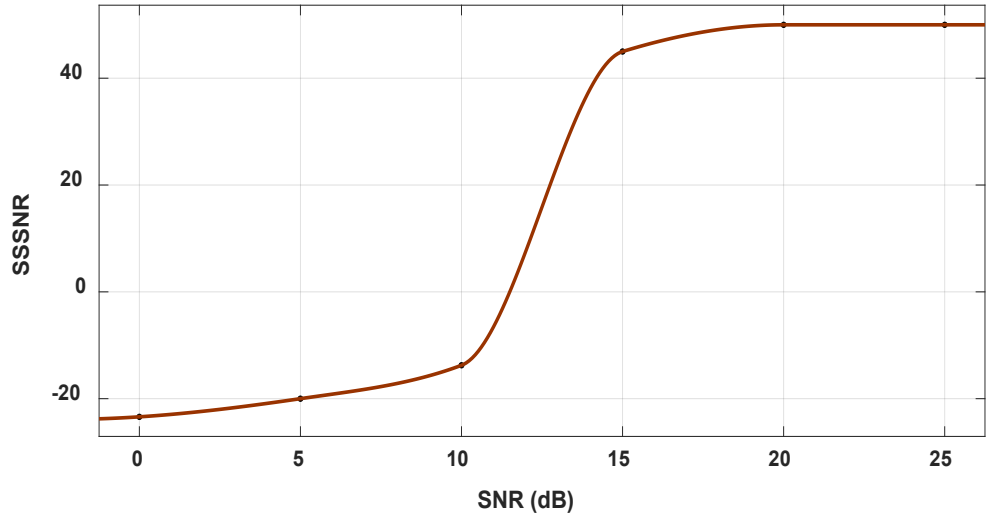
(B)


dLPC
SNR (dB)
0.5
0.6
0.7
0.8
0.9
1
0
5
10
15
20
25

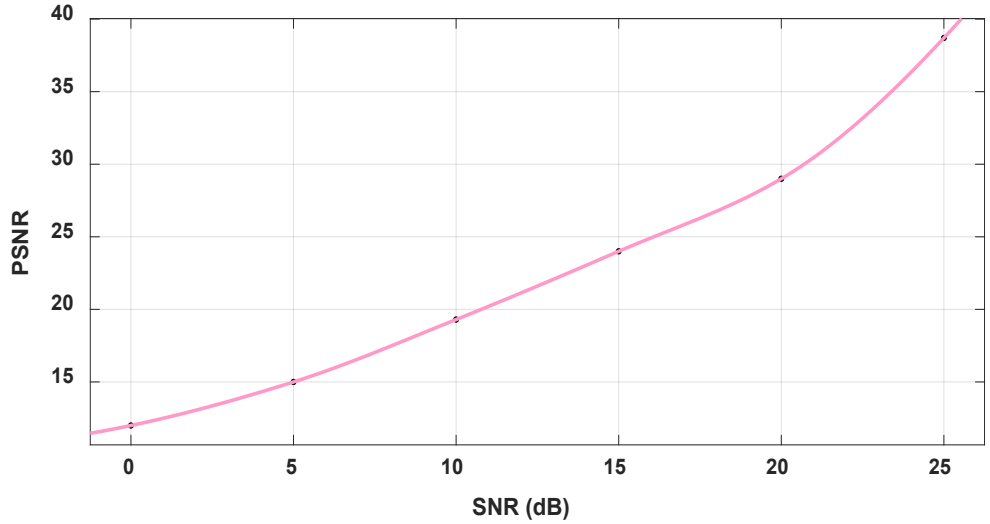
(C)


dLOG
SNR (dB)
14
12
10
8
6
4
2
0
5
10
15
20
25

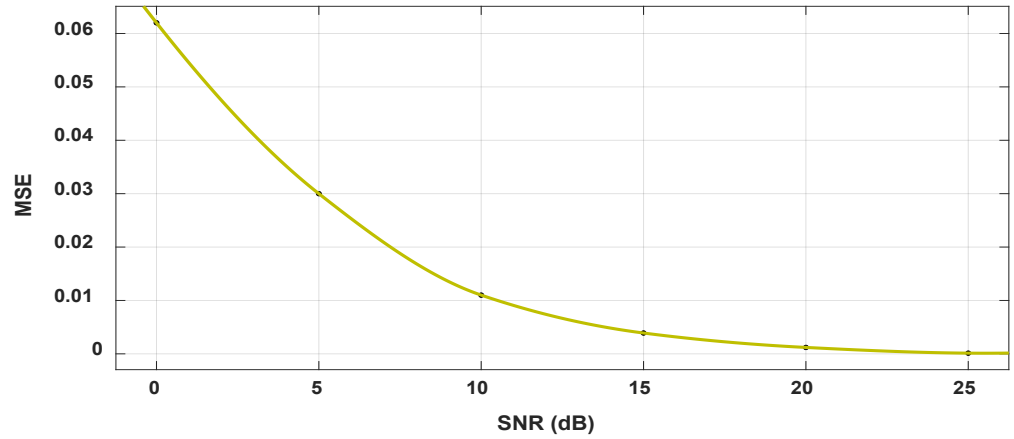
(D)


SSSNR
SNR (dB)
40
20
0
-20
0
5
10
15
20
25

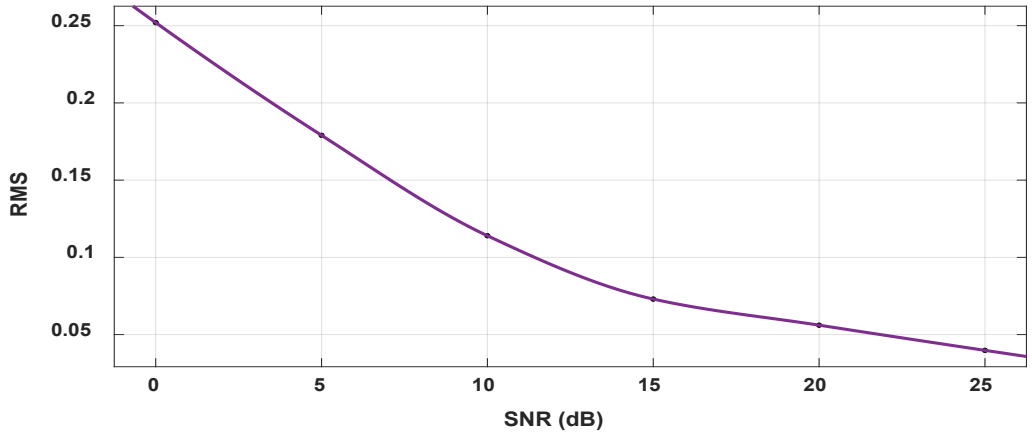
(E)


PSNR
SNR (dB)
40
35
30
25
20
15
0
5
10
15
20
25

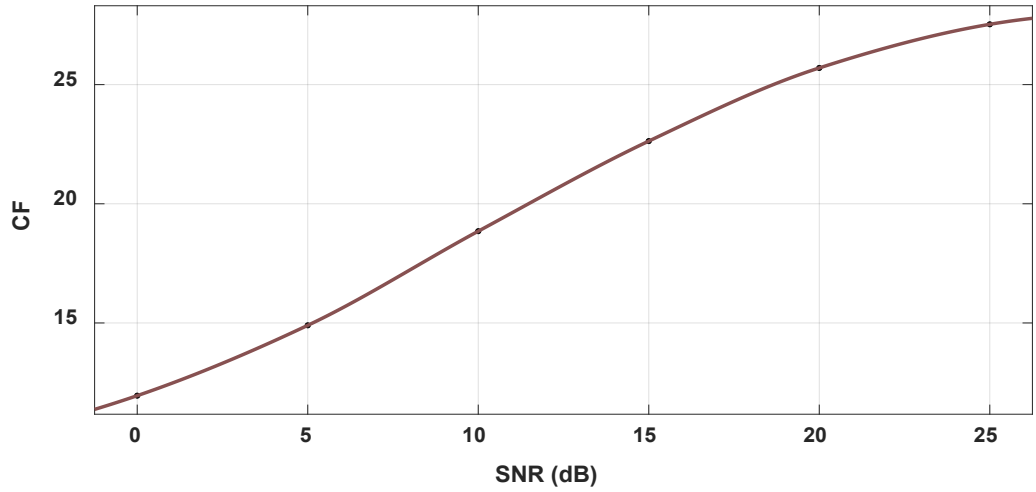
(F)



(G)



(H)



(I)

Figure 4.8. A, B,C,D,E,F,G,H,I variation of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of the proposed DNA-AI-PSM Encryption Technique

4.3.6 Performance Analysis of DNA-AI-PSM Technique

The BER performance of the legitimate and eavesdropping receiver is illustrated in Figure.4.9.

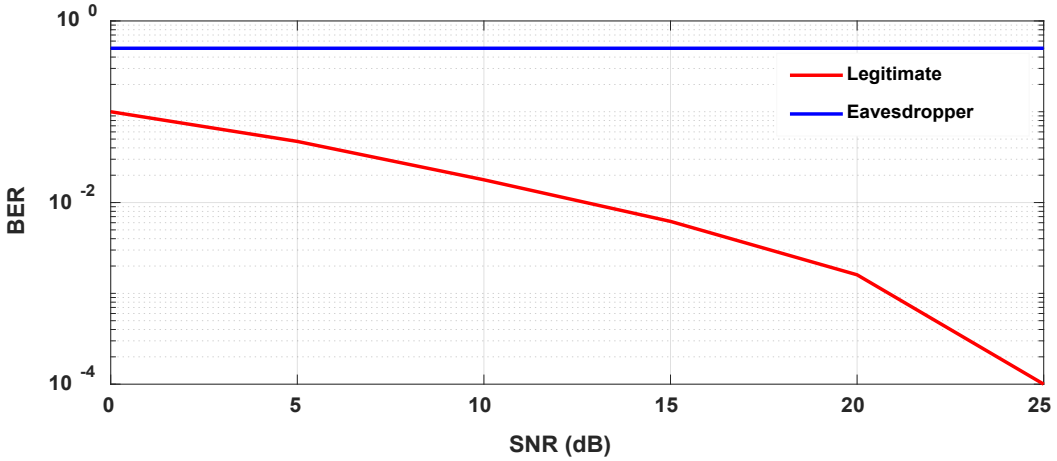


Figure 4.9 BER of legitimate and eavesdropper receiver for DNA-AI-PSM encryption technique

4.4 Simulation Results of HC-EC-GFDM Encryption Scheme

The proposed HC-EC-GFDM encryption scheme is investigated using several security metrics to determine the system's security level.

4.4.1 Subject Test of HC-EC-GFDM Encryption Scheme

Listening to the scrambled audio findings that are incomprehensible and it demonstrates that the HC-EC-GFDM scheme has a high-security level.

4.4.2 R.I. of HC-EC-GFDM Encryption Scheme

The effectiveness of the proposed scheme was assessed using various tests, as seen in tables 4.16-4.18.

Table 4.16. R.I. in terms of SNR, PSNR, and SSSNR for the HC-EC-GFDM scheme

Audio	Length (Sec.)	SNR (dB)	PSNR (dB)	SSSNR (dB)
Audio-1	1	-23.1397	0.8996	-29.7837
Audio-2	2	-26.3234	0.86181	-34.2372
Audio-3	3	-27.4971	0.85673	-34.9912
Audio-4	4	-25.4828	0.85543	-34.2526
Audio-5	5	-25.4839	0.85433	-34.256

Table 4.17. R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for the HC-EC-GFDM scheme

Audio	Length (Sec.)	d_{LPC}	d_{CD}	d_{LOG}	d_{FWLOG}
Audio-1	1	0.23896	9.3861	20.8574	9.861
Audio-2	2	1.1049	10.4602	24.5121	17.2731
Audio-3	3	0.14921	8.9547	21.9564	34.7654
Audio-4	4	0.62384	9.2594	21.4646	29.3418
Audio-5	5	0.62307	9.275	21.4559	29.2892

Table 4.18. R.I. in terms of MSE, RMS, CF, and R_{xy} for the HC-EC-GFDM scheme

Audio	Length (Sec.)	MSE	RMS	CF	R_{xy}
Audio-1	1	0.81291	0.89928	0.92187	-0.00129
Audio-2	2	0.82001	0.90512	0.86559	0.01422
Audio-3	3	0.82097	0.90518	0.86503	-0.0023
Audio-4	4	0.82122	0.90492	0.86752	-0.00033
Audio-5	5	0.82142	0.90497	0.86708	-0.00178

4.4.3 Key Space, Sensitivity, and time Analysis for HC-EC-GFDM Scheme

Table 4.19 lists each chaotic Maps and EC-LCG key Space used in the proposed cryptosystem.

Table 4.19. Key space of the proposed HC-EC- GFDM scheme

Chaotic Maps	Number of Control Parameters	Number of Initial conditions	Keyspace
Duffing	2	2	$(10^{15})^4 \approx 2^{200}$
Ikeda	1	2	$(10^{15})^3 \approx 2^{150}$
Tent	1	1	$(10^{15})^2 \approx 2^{100}$
EC-LCG	3	2	$(2^{12})^5 \approx 2^{60}$

The keys space of the proposed HC-EC-GFDM has fourteen secret keys; therefore, the overall keyspace $(2^{50})^9 .2^{60} = 2^{510}$. The statistical measurements that show the keys sensitivity are illustrated in Table 4.20. The proposed system's secret keys are $ad = 2.75; bd = 0.2; X_d(0) = -1.7; Y_d(0) = -1; X_i(0) = 0.527; Yi\ (0) = -0.5271; u = 0.708; Xt\ (0) = 0.4; \mu\ 1.9; p = 4093\ , a = 9, b = 7, G = (4{,}1110)\ and\ U_0 = (332{,}1395)$.

Table 4.20 Key sensitivity test of HC-EC- GFDM scheme using Audio-3

Map	Change key value	R_{xy}	MSE	d_{CD}	SSSNR	P. Diff
Duffing	a $+10^{-8}$	-0.00599	0.77512	9.0176	-34.7283	100%
	b$+10^{-8}$	-0.00205	0.73861	8.8635	-34.4992	100%
	$X_d(0)+10^{-8}$	-0.00204	0.74226	8.9897	-34.5244	100%
	$Y_d(0)+10^{-8}$	-0.0023	0.82097	8.9547	-34.9912	100%
Ikeda	u$+10^{-8}$	-0.0123	0.71348	6.9245	-34.1827	99.982%
	$X_i(0)+10^{-8}$	-0.01422	0.70772	7.0754	-34.1328	99.987%
	$Y_i(0)+10^{-8}$	0.0016	0.71526	6.9862	-34.1996	99.987%
Tent	$X_t(0)+10^{-8}$	0.0082	0.71542	6.9466	-34.2445	99.975%
	$\mu+10^{-8}$	0.006	0.72796	6.9208	-34.3351	99.983%
EC-LCG	P+1	0.009	0.65034	2.2799	-33.7564	99.995%
	Xo+1	-0.0269	0.63268	2.4718	-33.5828	99.995%
	Yo+1	-0.01338	0.62573	2.4039	-33.4724	99.983%
	Gx+1	0	0.63191	2.3286	-33.6108	99.995%
	Gy+1	0.01411	0.64307	2.3771	-33.6649	99.995%

The computational encryption/decryption time can be evaluated in Table 4.21 using five audio files.

Table 4.21. Time analysis for the HC-EC-GFDM scheme

Audio file	Length (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	1	16.0 KB	0.373	23.3×10^{-6}
Audio-2	2	32.0 KB	0.79	24.7×10^{-6}
Audio-3	3	48.0 KB	1.15	24×10^{-6}
Audio-4	4	64.0 KB	1.728	27×10^{-6}
Audio-5	5	80.0 KB	2.209	27.6×10^{-6}

4.4.4 Resistance against differential attacks for HC-EC-GFDM Scheme

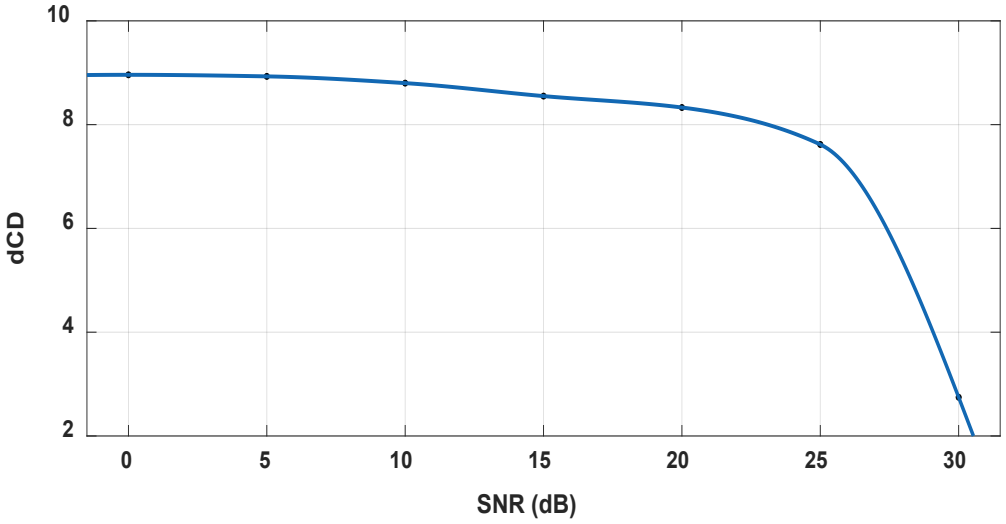
The proposed scheme's robustness and ability to fend against differential attacks were assessed using the NSCR and UACI tests. The results of the tests are displayed in Table 4.22, proving that the proposed system is resistant to differential attacks.

Table 4.22. UACI and NSCR analysis for HC-EC-GFDM Scheme

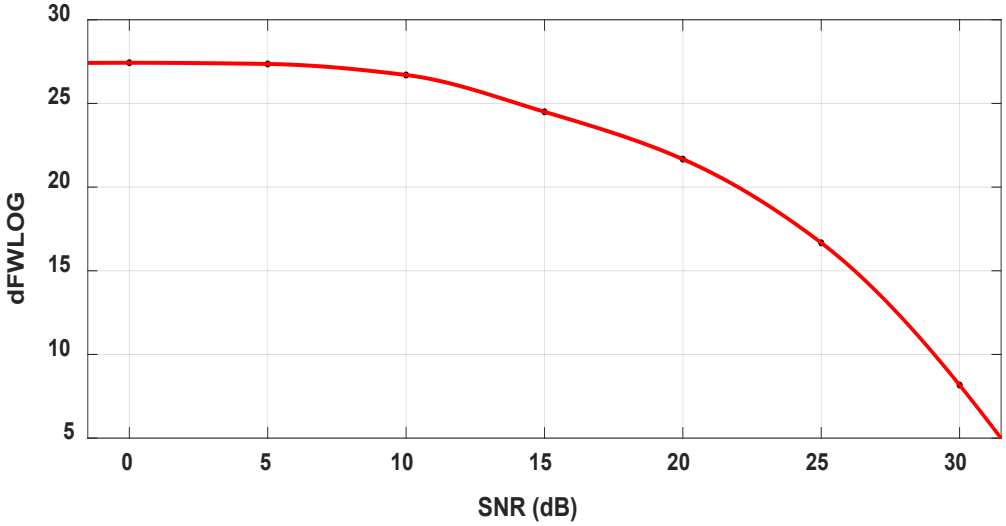
Audio	Length (s)	UACI	NSCR
Audio-1	1	33.337%	99.987%
Audio-2	2	33.335%	99.993%
Audio-3	3	33.334%	99.995%
Audio-4	4	33.334%	99.996 %
Audio-5	5	33.334 %	99.997 %

4.4.5 Noise Effect on HC-EC-GFDM Scheme over massive MIMO PSM System

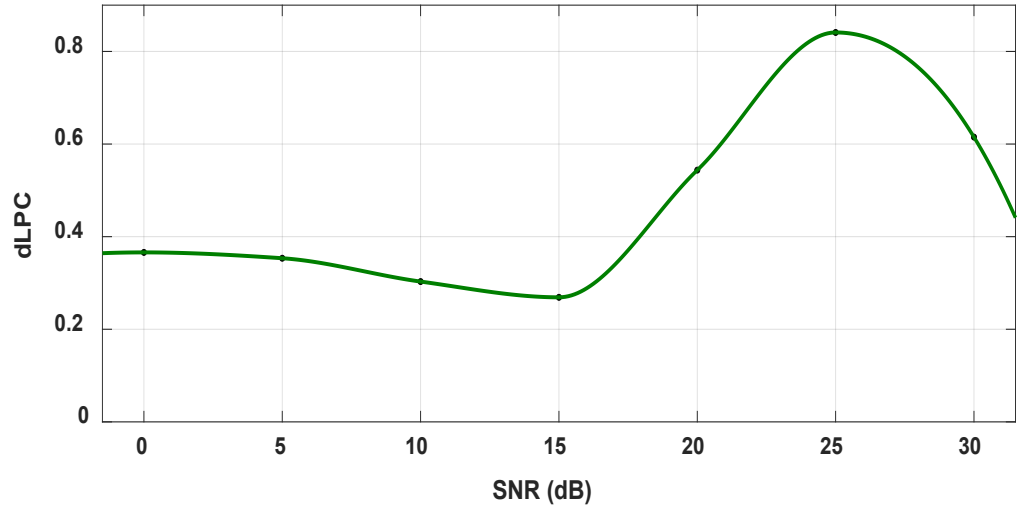
The effect of the channel noise on the received decrypted audio signal was examined by considering d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF between the original and decrypted audio signal of the proposed HC-EC-GFDM scheme at various SNR values as shown in Figure 4.10.



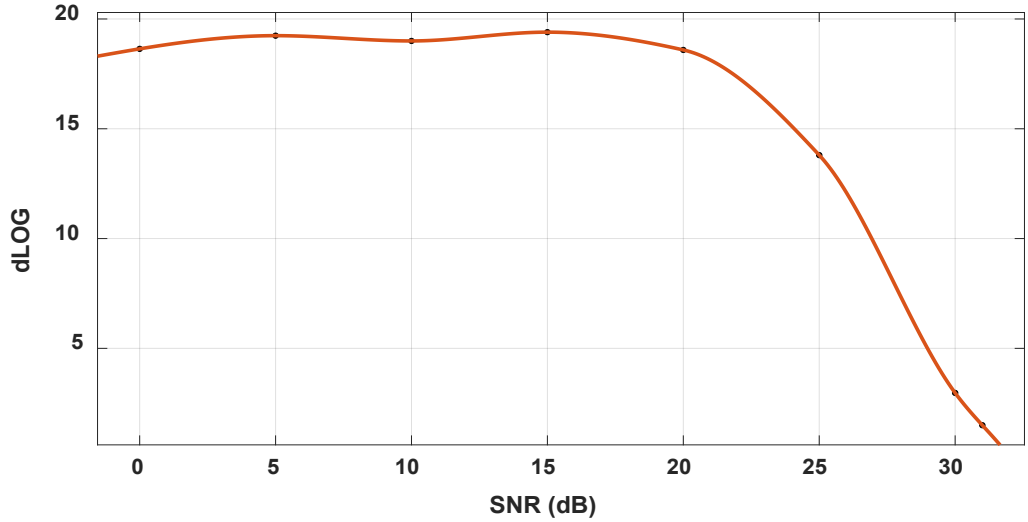
(A)



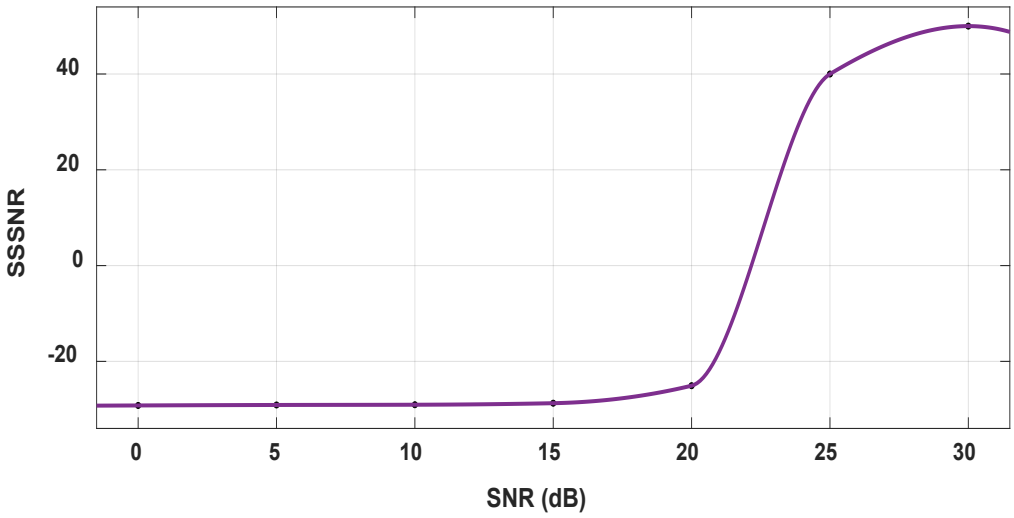
(B)


dLPC
0.8
0.6
0.4
0.2
0
0
5
10
15
20
25
30
SNR (dB)

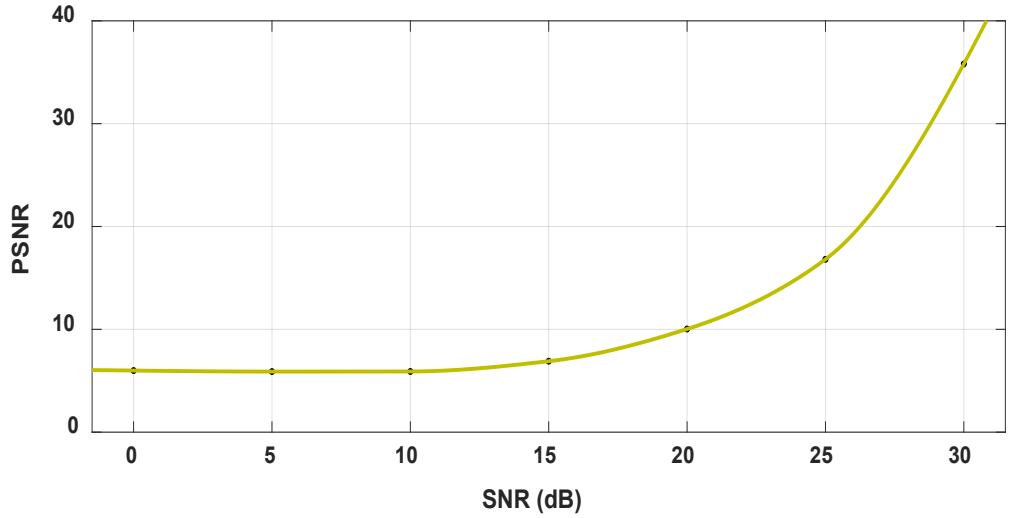
(C)


dLOG
20
15
10
5
0
5
10
15
20
25
30
SNR (dB)

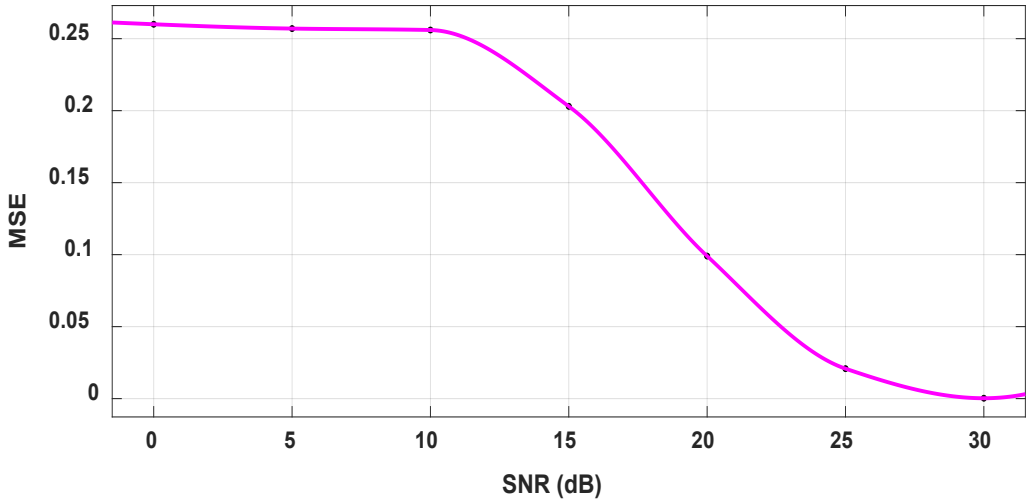
(D)


SSSNR
40
20
0
-20
0
5
10
15
20
25
30
SNR (dB)

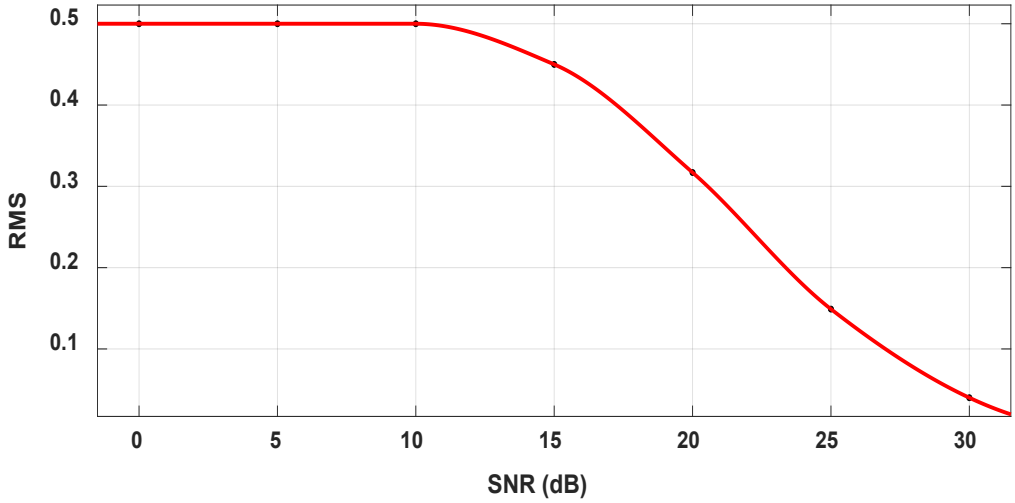
(E)


PSNR
SNR (dB)
0
10
20
30
40
0
5
10
15
20
25
30

(F)


MSE
SNR (dB)
0
0.05
0.1
0.15
0.2
0.25
0
5
10
15
20
25
30

(G)


RMS
SNR (dB)
0.1
0.2
0.3
0.4
0.5
0
5
10
15
20
25
30

(H)

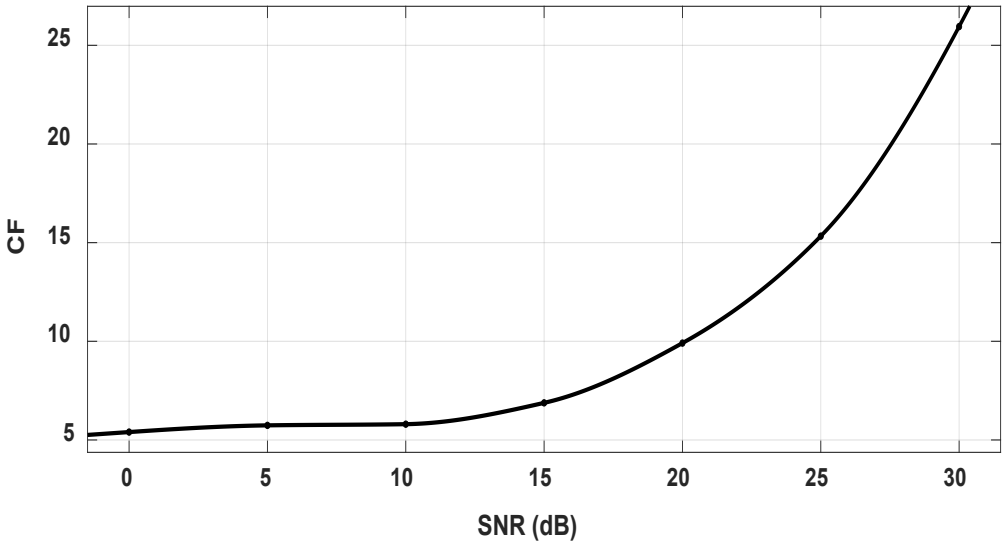


Figure 4.10 A, B,C,D,E,F,G,H,I variations of d_{CD}, d_{FWLOG}, $d_{LPC,}d_{LOG}$, SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of the proposed HC-EC-GFDM Scheme

4.4.6 Performance Analysis of HC-EC-GFDM Scheme

The BER performance of the authorized and eavesdropping receiver is illustrated in Figure 4.11.

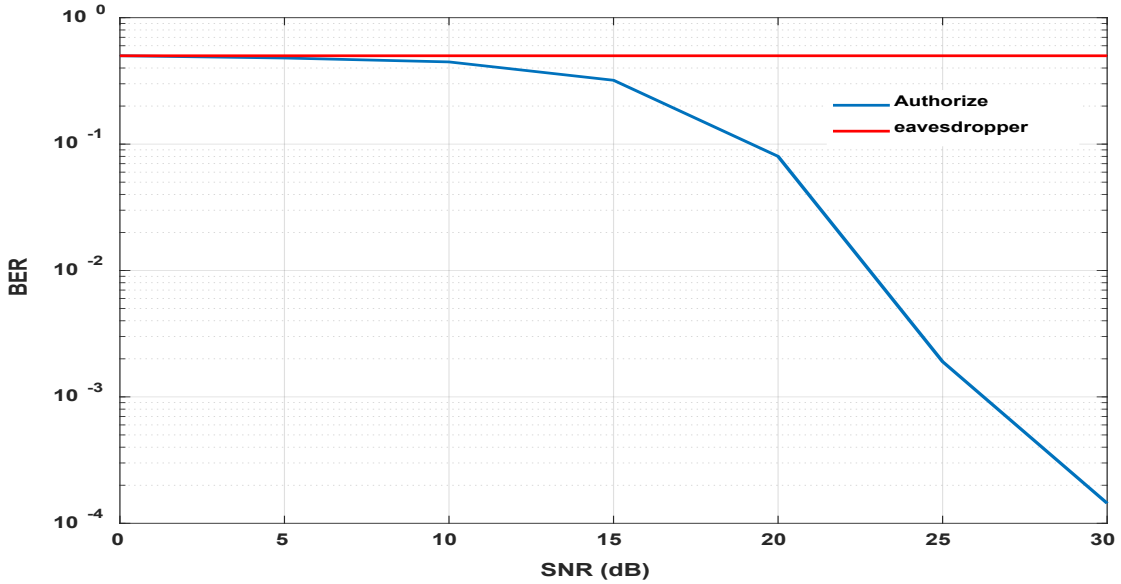


Figure 4.11 BER of authorized and eavesdropper receiver for HC-EC-GFDM Scheme

4.5 Simulation Results of HC-QR-MMSE Encryption Technique

The proposed HC-QR-MMSE encryption technique is investigated using several security metrics to determine the system's security level.

4.5.1 Subject Test of HC-QR-MMSE Encryption Technique

Listening to the scrambled audio findings that are incomprehensible, and it demonstrates that the HCQRPRNG-MMSE encryption technique has a high-security level.

4.5.2 R.I. of HC-QR-MMSE Encryption Technique

The effectiveness of the proposed scheme was assessed using various tests, as seen in tables 4.23-4.25.

Table 4.23. R.I. in terms of SNR, PSNR, and SSSNR for the HC-QR-MMSE Encryption Technique

Audio	Length (Sec.)	SNR (dB)	PSNR (dB)	SSSNR (dB)
Audio-1	1	-23.9942	0.04517	-30.6891
Audio-2	2	-27.1357	0.04944	-35.0888
Audio-3	3	-28.2993	0.05458	-35.836
Audio-4	4	-26.2833	0.05494	-35.1022
Audio-5	5	-26.3009	0.04915	-35.6623

Table 4.24. R.I. in terms of d_{LPC}, d_{CD} ,d_{Log}, and d_{FWLOG} for the HC-QR-G-MMSE Encryption Technique

Audio	Length (Sec.)	d_{LPC}	d_{CD}	d_{LOG}	d_{FWLOG}
Audio-1	1	1.0283	8.7908	23.4658	13.4976
Audio-2	2	1.5747	9.4607	26.9112	13.9275
Audio-3	3	0.9353	7.6197	24.4176	26.7063
Audio-4	4	1.229	8.3961	23.8528	21.5652
Audio-5	5	1.6058	9.5051	24.951	20.7747

Table 4.25. R.I. in terms of MSE, RMS, CF, and R_{xy} for the HC-QR-MMSE Encryption Technique

Audio	Length (Sec.)	MSE	RMS	CF	R_{xy}
Audio-1	1	0.98965	0.99219	0.0678	-0.00427
Audio-2	2	0.98868	0.99309	0.05997	-0.0116
Audio-3	3	0.98751	0.99297	0.0610	-0.00156
Audio-4	4	0.98743	0.99309	0.06	0.0119
Audio-5	5	0.98875	0.99299	0.0608	-0.00465

4.5.3 Key Space, Sensitivity, and time Analysis for the Proposed HC-QR-MMSE Encryption Technique

Table 4.26 lists each chaotic Maps key Space used in the proposed cryptosystem.

Table 4.26 Key space of the proposed HC-QR-MMSE Technique

Chaotic Maps	Number of Control Parameters	Number of Initial conditions	Key Space
Bernoulli	1	1	$(10^{15})^2 \approx 2^{100}$
Logistic	1	1	$(10^{15})^2 \approx 2^{100}$
Henon	2	2	$(10^{15})^4 \approx 2^{200}$
Tent	1	1	$(10^{15})^2 \approx 2^{100}$

The keys space of the proposed algorithm has ten private keys; therefore, the overall keyspace $(2^{50})^{10} = 2^{500}$. The statistical measurements that show the sensitivity of the key are illustrated in Table 4.27. The proposed system's secret keys are $ah = 1.4; bh = 0.3; X_h(0) = 0; Y_h(0) = 0.5; X_l(0) = 0.5; r\ (0) = 3.7; \mu_b = .99; Xb\ (0) = 0.025; \mu_t = 1.9; X_t = 0.4$

Table 4.27. Key sensitivity test Proposed HC-QR-MMSE Encryption Technique using audio-3

Map	Change key	R_{xy}	MSE	d_{CD}	SSSNR	P. Diff.
Henon	$a_h + 10^{-8}$	-0.00654	0.6764	8.2317	-34.1664	100%
	$b_h + 10^{-8}$	-0.00798	0.6786	8.2659	-34.1807	99.992%
	$X_h(0) + 10^{-8}$	-0.00314	0.6788	8.2396	-34.1839	99.996%
	$Y_h(0) + 10^{-8}$	-0.00295	0.6772	8.1859	-34.1756	100%
Logistic	$r + 10^{-8}$	-0.00156	0.9875	7.6197	-35.8360	100%
	$X_l(0) + 10^{-8}$	0.00860	0.9863	7.5141	-35.8332	100%
Bernoulli	$X_b(0) + 10^{-8}$	-0.01259	0.2391	8.1649	-29.5285	99.983%
	$\mu_b + 10^{-8}$	-0.00381	0.2391	8.145	-29.5428	99.992%
Tent	$X_t(0) + 10^{-8}$	-0.01160	0.6730	8.2399	-34.1471	100%
	$\mu_t + 10^{-8}$	-0.00747	0.6930	8.2227	-34.2731	100%

The time and speed of encrypted /decrypted can be evaluated in Table 4.28 using five audio files.

Table 4.28. Time analysis of the proposed HC-QR-MMSE Encryption Technique

Audio file	Length (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	1	16.0 KB	0.406	25.4×10^{-6}
Audio-2	2	32.0 KB	0.87	27.2×10^{-6}
Audio-3	3	48.0 KB	1.356	28.3×10^{-6}
Audio-4	4	64.0 KB	1.8	28.1×10^{-6}
Audio-5	5	80.0 KB	2.326	29.1×10^{-6}

4.5.4 Resistance against differential attacks for the proposed HC-QR-MMSE Encryption Technique

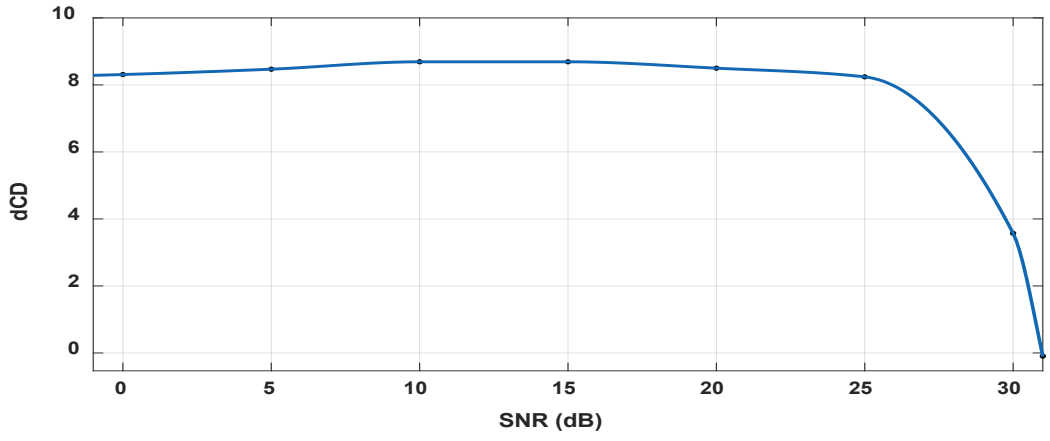
The NSCR and UACI test of the proposed system is determined and listed in Table 4.29. The results indicate that the values produced by the proposed technique are significantly nearer to ideal values.

Table 4.29. UACI and NSCR analysis for HC-QR-MMSE Encryption Technique

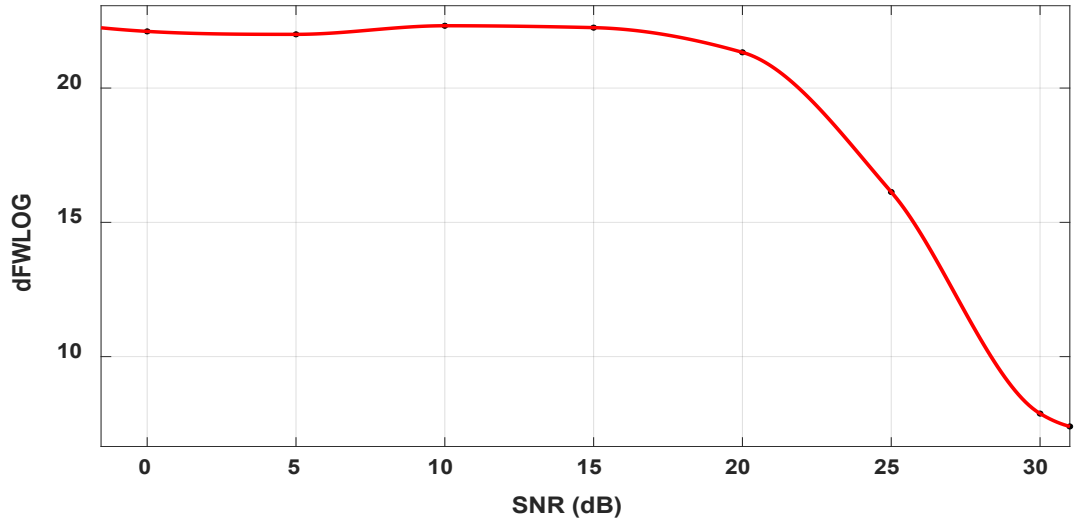
Audio	Length (Sec.)	UACI	NSCR
Audio-1	1	33.337%	99.9875%
Audio-2	2	33.335%	99.9937%
Audio-3	3	33.334%	99.9958%
Audio-4	4	33.334%	99.9968 %
Audio-5	5	33.334 %	99.9975 %

4.5.5 Noise Effect on HC-QR-MMSE Encryption Technique over massive MIMO PSM System

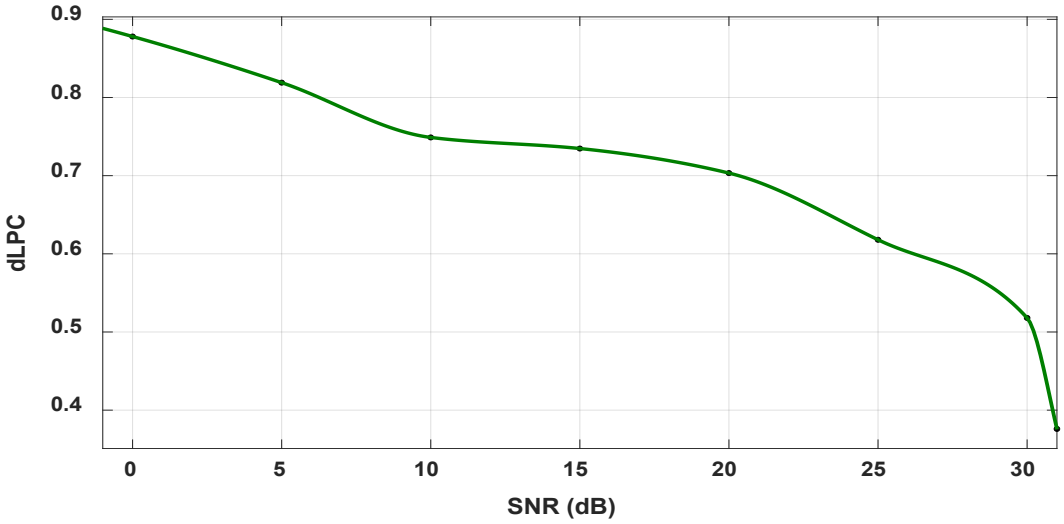
The impact of the channel noise was investigated by taking into d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF between the original d decrypted audio signals of the proposed HC-QR-MMSE technique at various SNR values as shown in Figure 4.12.



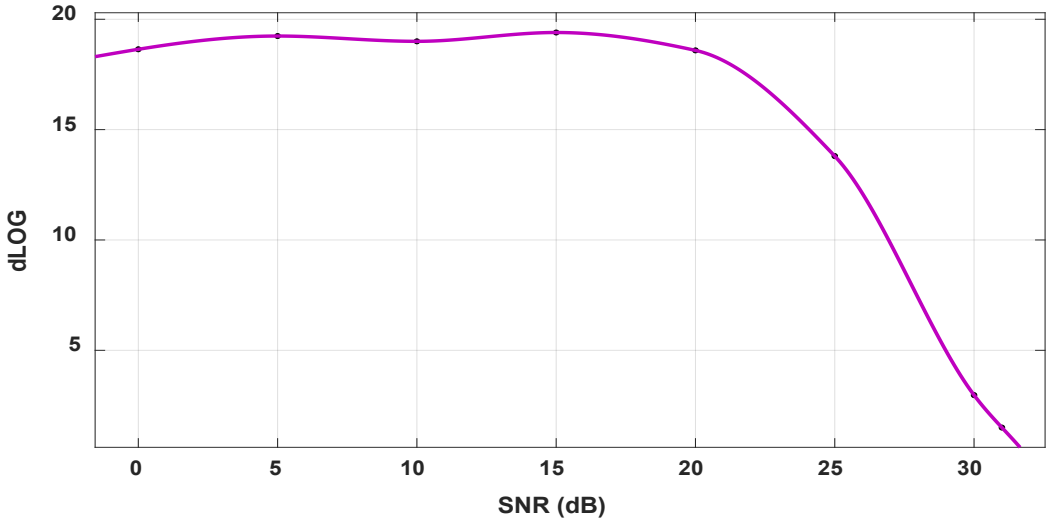
(A)


dFWLOG
20
15
10
0
5
10
15
20
25
30
SNR (dB)

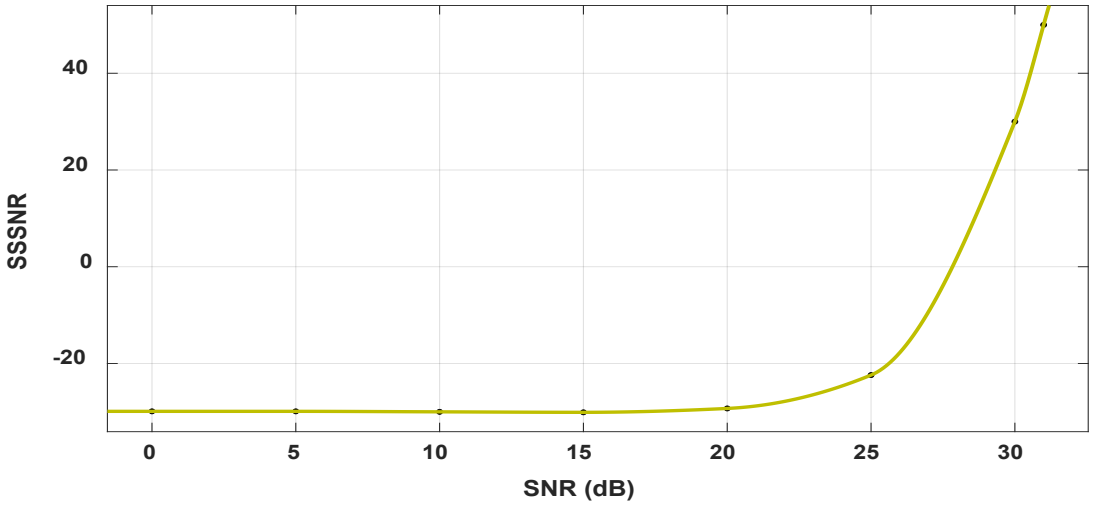
(B)


dLPC
0.9
0.8
0.7
0.6
0.5
0.4
0
5
10
15
20
25
30
SNR (dB)

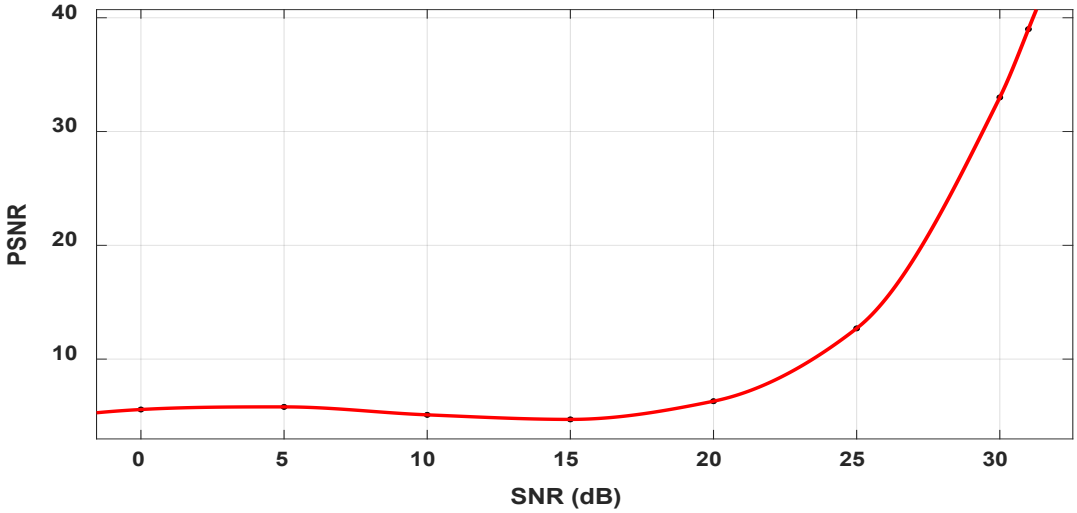
(C)


dLOG
20
15
10
5
0
5
10
15
20
25
30
SNR (dB)

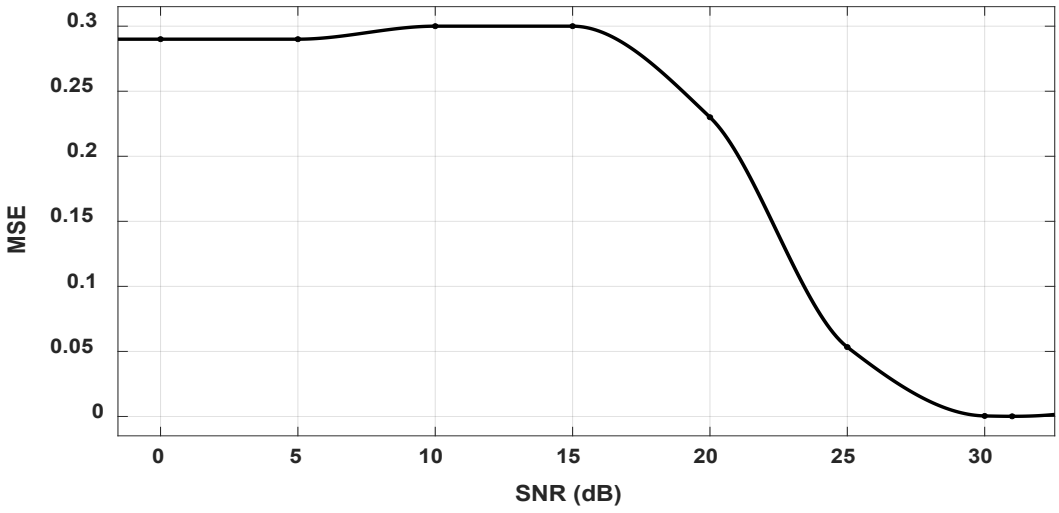
(D)


SSSNR
40
20
0
-20
0
5
10
15
20
25
30
SNR (dB)

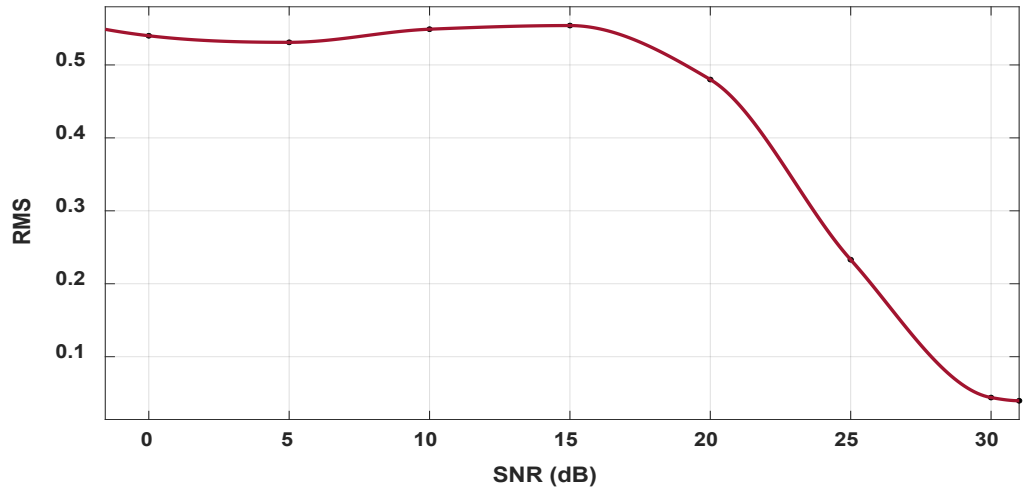
(E)


PSNR
40
30
20
10
0
5
10
15
20
25
30
SNR (dB)

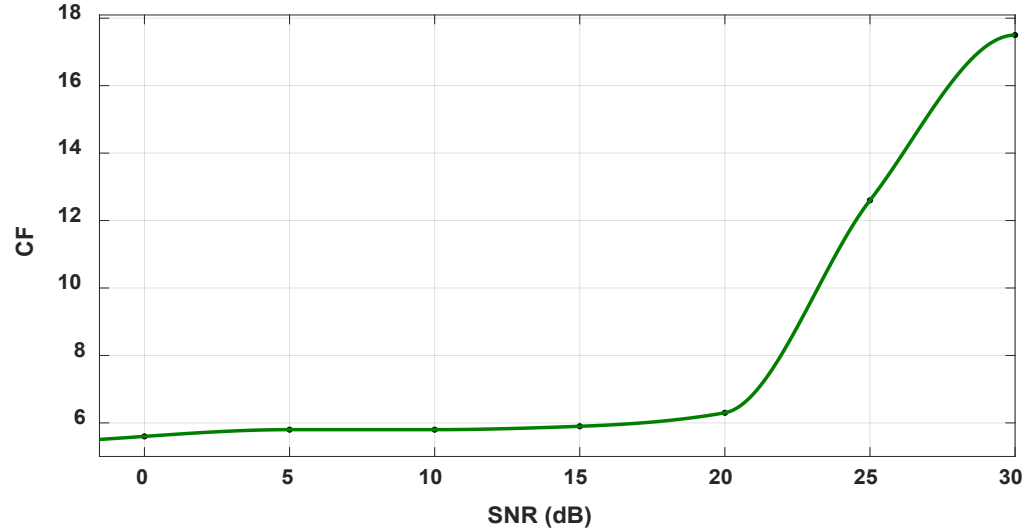
(F)


MSE
0.3
0.25
0.2
0.15
0.1
0.05
0
0
5
10
15
20
25
30
SNR (dB)

(G)



(H)



(I)

Figure 4.12. A, B, C, D, EE, F, G, H, I variations of d_{CD}, d_{FWLOG}, d_{LPC},d_{LOG} , SSSNR ,PSNR ,MSE ,RMS, and CF, respectively, for the recovered audio-3 of HC-QR-MMSE Encryption Technique

4.5.6 Performance Analysis of HC-QR-MMSE Encryption Technique

The BER of the authorized and eavesdropping receiver is illustrated in Figure 4.13.

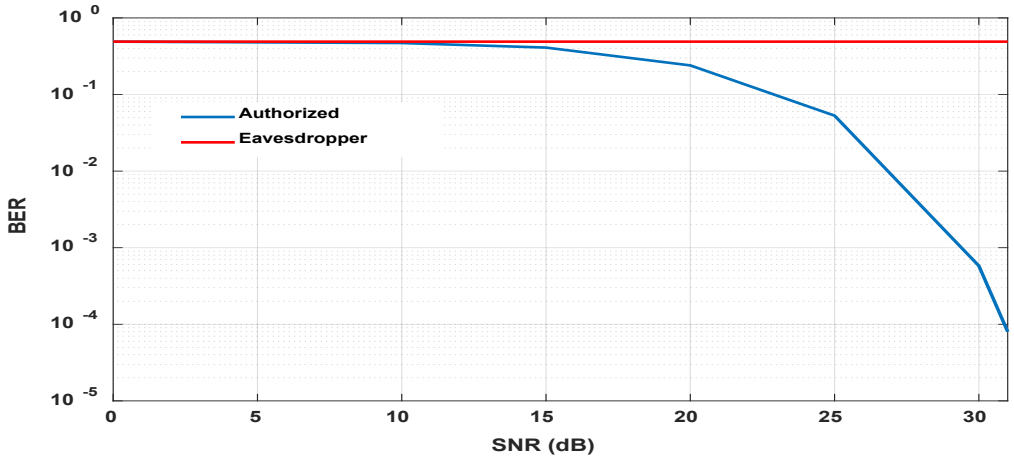


Figure 4.13 BER of authorized and eavesdropper the Proposed HC-QR-MMSE Encryption Technique

4.6 R.I Simulation Results Discussion of The Proposed Cryptosystems

In this section of the chapter, the discussion of results will perform for all proposed algorithms according to the following criteria:

1. When R_{xy} approach zero, it means that low the R.I. of encrypted audio (High-security level)
2. The reduction of SNR, SSSNR, PSNR, and CF values means a low R.I. of the encrypted audio (High-security level)
3. The increasing of MSE, RMS, d_{CD}, d_{FWLOG}, d_{LPC}, and d_{LOG} values means a low R.I. of the encrypted audio (High-security level)

The minimum and maximum values mentioned in the points above reflect the difficulty in retrieving the original audio from encrypted audio without knowing the secret key. In the decryption process, the quality of the received audio at the authorized receiver is as follows:

1. When R_{xy} approaches one, it means good decrypted audio quality.
2. The increased SNR, SSSNR, PSNR, and CF values mean good decrypted audio quality.
3. Reducing MSE, RMS, d_{CD}, d_{FWLOG}, d_{LPC}, and d_{LOG} values means good decrypted audio quality.

4.7 Comparing the Studies

In order to evaluate the weakness and strong points of the proposed cryptosystems, the suggested techniques and their features will be compared among them and with those of existing competing systems. The most widely utilized security criterion include SNR, SSSNR, PSNR, P. Diff, MSE, R_{xy}, d_{LPC}, d_{LOG}, d_{FWLOG}, d_{CD}, RMS, CF, NSCR, UACI, keyspace, key sensitivity, and time. This comparison with different algorithms is shown in Table 4.30. The results show that the proposed cryptosystems have the lowest value of R_{xy}. It is also evident that the proposed cryptosystems have the largest key space from all the others. The proposed cryptosystems exhibit the most negative SNR and SSSNR values and minimum PSNR of the previous approaches.

Furthermore, the proposed cryptosystems have the highest values of UACI, NSCR, d_{LOG}, d_{FWLOG}, d_{CD}, RMS, MSE, and $d_{LPC,}$ among other techniques, so it has the strongest resistance against brute-force attacks. The key sensitivity analysis shows that any tiny change in the chaotic parameters and initial condition leads to unsuccessful voice decryption. In addition to the other results obtained, we can conclude that all proposed algorithms are safe and secure for wireless audio transmission.

Table 4.30 Comparisons between proposed cryptosystems and previous works using Audio-3

Tests	HCMO	DNA-AI-PSM	HC-EC-GFDM	HC-QR-MMSE	[19] In 2016	[90] In 2013	[20] In 2016	[22] In 2017	[16] In 2015	[23] In 2017	[27] In 2019	[28] In 2020	[91] In 2020
SNR (dB)	-23.5969	-24.544	-27.4971	-28.2993	-	-2.616	-	-	-3.025	-	-16.04	-	-
PSNR (dB)	4.7569	3.8099	0.85673	0.05458	-	-	-	-		-	-	-	-
SSSNR (dB)	-31.0528	-31.992	-34.9912	-35.836	-4.227	-2.458	-	-16.723	-3.04	-	-	-26.506	-22.6783
d_{LPC}	0.9612	1.0257	0.14921	0.9353	4.336	-	-	-	0.7253	-	-	0.9741	-
d_{CD}	8.1925	7.3827	8.9547	7.6197	7.097	8.214	-	7.2274	-	-	-	8.8503	-
d_{LOG}	21.1417	21.787	21.9564	24.4176	-	-	-	-	-	-	-	14.5415	-
d_{FWLOG}	23.0908	26.3629	34.7654	26.7063	-	-	-	-	-	-	-	20.9976	-
MSE	0.3344	0.4159	0.82097	0.98751	-	-	-	-	-	-	-	-	0.4175
RMS	0.5773	0.64375	0.90518	0.99297	-	-	-	-	-	-	-	-	-
CF	4.7698	3.8254	0.86503	0.0610	-	-	-	-	-	-	-	-	-
R_{xy}	0.0069	-0.00097	-0.0023	-0.00156	-	-	0.004	0.38339	-	-0.0046	−0.0048	-	-
Key space	2^{500}	2^{632}	2^{510}	2^{500}	2^{427}	-	2^{268}	2^{480}	-	2^{319}	2^{149}	-	-
Time (Sec.)	0.032	0.045	1.15	1.356	-	-	-	-	-	-	-	-	-
Speed (Sec./KB)	6.67×10^{-7}	9.3×10^{-7}	24×10^{-6}	28.3×10^{-6}	-	-	-	-	-	10.4	0.003	-	-
UACI	33.334%	33.334%	33.334%	33.334%	-	-	-	-	-	-	-	-	-
NSCR	99.99%	99.979%	99.995%	99.9958%	-	-	-	-	-	-	99.99%	-	-
P.Diff.	100%	99.995%	100%	100%	-	-	-	99.14%	-	-	-	-	-

Chapter Five

Conclusions and Future Works

5.1 Conclusions

Secure communications based on a chaotic system are the subject of the study reported in this dissertation. Chaos is an excellent candidate for secure communications due to its high sensitivity to initial conditions and parameters that can be utilized as secret keys. So, four new audio encryption systems have been proposed based on chaos theory in combination with DNA encoding and EC-LCG sequence inside communication system components compatible with 5G networks. The following conclusions might be given based on the findings of the proposed encryption methods.

1. All proposed systems employes multiple chaotic maps (hybrid maps) due to their more complicated chaotic property than the single map and more sensitivity to the initial condition and parameters, which are used as private keys.
2. The position of the security algorithm applied in the communication system has important to specify the required security level, so hard to predict from eavesdroppers.
3. Encryption algorithms inside communication components (modulation and channel) provide a higher level of security than using them outside.
4. The proposed encryption algorithm has the most important feature, which is the possibility of implementation in real-time due to the high speed of the encryption/decryption process, which makes it suitable for the needs of the 5G network.
5. The increase in the key space does not affect the security metrics tests.

6. Applying the encryption algorithm in the time domain gives a better security level than the frequency domain, especially in values SNR, SSSNR, PSNR MSE, RMS, and CF.
7. Applying the encryption algorithm in the frequency domain (HCMO and DNA-AI-PSM) gives a more high-speed encryption/decryption process than in the time domain (HC-EC-GFDM and HC-QR-MMSE).
8. The time plot of the encrypted audio signal indicates that it is like noise, making it difficult to predict the original audio signal.
9. The proposed encryption algorithms do not change the file size, so the encrypted audio has the same size (in KB) as the original audio.

5.2 Suggestions for Future Works

1. Investigation of the initial conditions and parameters of the chaotic map to choose the best value using an artificially intelligent network.
2. Implement the proposed systems using images, video, and text.
3. Assessing the effectiveness of the suggested systems under attack.
4. Implement the proposed systems using FPGA.
5. Study the effect of using data compression techniques on audio before the encryption algorithm.
6. Use wavelet transform instead of IFFT in the GFDM modulator and apply a chaotic encryption technique.
7. Implement secure GFDM with the assistance of non-orthogonal multiple access (NOMA) techniques.

Appendix A

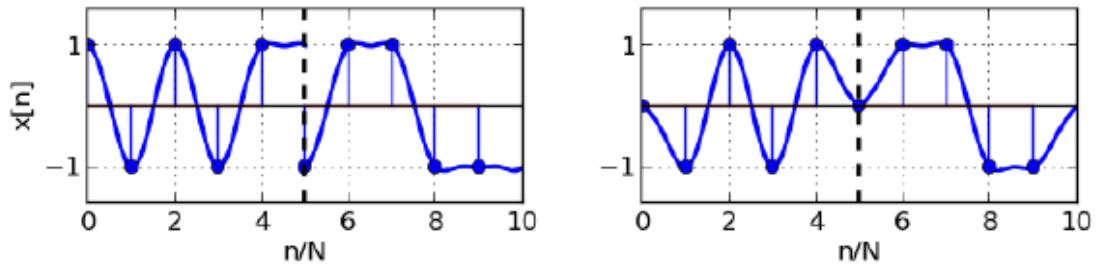
Waveform Engineering

The flexibility of GFDM allows for designing a signal with a very low OOB radiation. This section gives solutions for low OOB radiation.

A.1 Guard Symbol GFDM (GS-GFDM)

The transitions between the GFDM blocks must be smoothed to minimize OOB radiation, but the first subsymbol wraps around the blocks edges and introduces abrupt amplitude discontinuity. When nulling the first subsymbol, GS is inserted among the GFDM blocks, and the signal edges fade towards zero; this smooth transitions among GFDM blocks, as shown in Figure A.1, so this technique is called GS-GFDM. Another problem would occur in transitions between blocks by the insertion of the CP, to solve this issue, make the last subsymbol null $N_{CP} = K$, but the weakness of this method is the decrease in throughput as seen in Equation (A.1) [37]:

$$R_{GS} = \frac{M-2}{M} \times \frac{KM}{KM+K} = \frac{M-2}{M+1} \quad \text{(A.1)}$$



No guard symbol one guard symbol

Figure A.1 Comparison of the GS for two GFDM blocks [92]

A.2 Windowed-GFDM (W-GFDM)

In order to smooth the transition between GFDM blocks, a time window is applied, as shown in Figure A.2. Assuming that the Cyclic Suffix (CS) length = N_{CS}, the channel impulse response length = N_{ch}, the time

window transition length =N_W, N_{CS}= N_w, then the CP (N_{CP}) length = N_{ch}+ N_W. Noting that the CS is a copy of the first GFDM block samples to its end. The time window is given by:

$$w[n] = \begin{cases} w_{up}[n] & 0 \le n \le N_w \\ 1 & N_w \le n \le N + N_{cp} \\ w_{down}[n] & N + N_{cp} \le n \le N + N_{cp} + N_w \end{cases} \quad \text{(A.2)}$$

where n = 0, 1 ⋯, N + N_{cp} − 1 is the time index, where $w_{up}[n]$ and $w_{down}[n]$ are the ramp-up and ramp-down segments of the time window, respectively. The PSD comparison between OFDM, GFDM, GS-GFDM, and W-GFDM is depicted in Figure A.3.

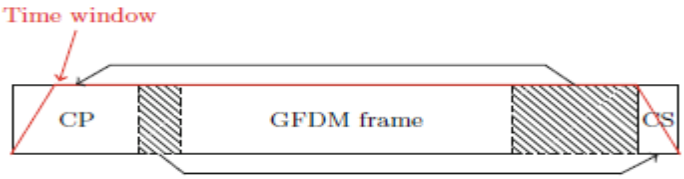


Figure A.2 W-GFDM time-domain configuration [37]

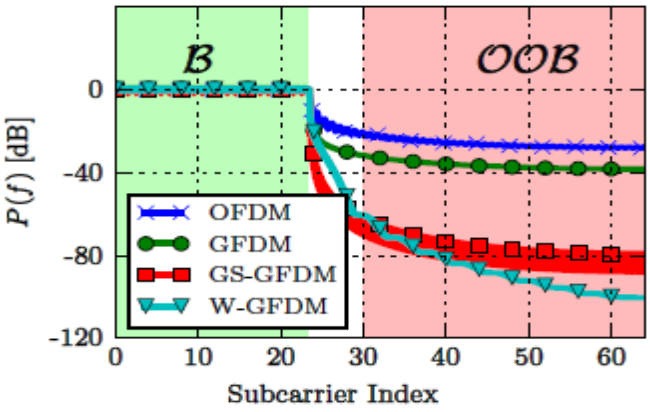


Figure A.3 PSD of OFDM and GFDM types [35]

The loss in data rate introduced by the windowed method is given as:

$$R_w = \frac{N}{N + N_{cp} + N_w} \quad \text{(A.3)}$$

Since the $w_{up}[n]$ and $w_{down}[n]$ sequence lengths are much shorter than the length of a GFDM block, R_W outperforms R_{GS}. As a result, W-GFDM can be considered a more feasible option, more efficient, and with lower OOB radiation [37].

References

[1] M. F. Haroun and T. A. Gulliver, "Secure OFDM with Peak-to-Average Power Ratio Reduction Using the Spectral Phase of Chaotic Signals," *Entropy,* vol. 23, no. 11, p. 1380, 2021, doi: 10.3390/e23111380.

[2] M. M. Elkholy, H. E. Hennawy, and A. Elkouny, "Design and implementation of hyper chaotic masking system for secured audio transmission," in *2015 Tenth International Conference on Computer Engineering & Systems (ICCES)*, 2015: IEEE, pp. 81-85.

[3] F. Farsana and K. Gopakumar, "Speech encryption based on four-dimensional hyperchaotic system," in *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, 2016: IEEE, pp. 279-283.

[4] D. Mahto and D. K. Yadav, "Network security using ECC with Biometric," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, 2013: Springer, pp. 842-853, doi: 10.1007/978-3-642-37949-9_73.

[5] O. Reyad and Z. Kotulski, "Statistical analysis of the chaos-driven elliptic curve pseudo-random number generators," in *International Conference on Cryptography and Security Systems*, 2014: Springer, pp. 38-48, doi: 10.1007/978-3-662-44893-9_4.

[6] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations," *IEEE Access,* vol. 8, pp. 69894-69907, 2020.

[7] M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic Based Encrypted Audio Transmission via Massive MIMO - GFDM system using DNA Coding in the Antenna Index of PSM," *5th International Conference on Engineering Technology and its Applications (IICETA)* pp. 19-24, 2022.

[8] R. Chataut and R. Akl, "Massive MIMO systems for 5G and beyond networks—overview, recent trends, challenges, and future research direction," *Sensors,* vol. 20, no. 10, p. 2753, 2020, doi: 10.3390/s20102753.

[9] M. Mohaisen, "Constellation design and performance analysis of the parallel spatial modulation," *International Journal of Communication Systems,* vol. 32, no. 18, p. e4165, 2019.

[10] N. Michailow, R. Datta, S. Krone, M. Lentmaier, and G. Fettweis, "Generalized frequency division multiplexing: A flexible multi-carrier modulation scheme for 5th generation cellular networks," in *Proceedings of the German microwave conference (GeMiC'12)*, 2012, vol. 62, pp. 1-4.

[11] R. Zayani, H. Shaiek, and D. Roviras, "PAPR-aware massive MIMO-OFDM downlink," *IEEE Access,* vol. 7, pp. 25474-25484, 2019, doi: 10.1109/ACCESS.2019.2900128.

[12] E. Mosa, N. W. Messiha, O. Zahran, and A. El-Samie, "Encryption of speech signal with multiple secret keys in time and transform domains," *International Journal of speech technology,* vol. 13, no. 4, pp. 231-242, 2010.

[13] S. M. Alwahbani and E. B. Bashier, "Speech scrambling based on chaotic maps and one time pad," in *International Conference On Computing, Electrical And Electronic Engineering (ICCEEE)*, 2013: IEEE, pp. 128-133, doi: 10.1109/ICCEEE.2013.6633919.

[14] N. R. Raajan, B. Monisha, R. Vishnupriya, N. Rangarajan, G. N. Jayabhavani, and C. Nishanthini, "Chaotic Interleaving for Secure OFDM," *Research Journal of Information Technology,* vol. 5, no. 3, pp. 449-455, 2013.

[15] M. Ahmad, B. Alam, and O. Farooq, "Chaos based mixed keystream generation for voice data encryption," *arXiv preprint arXiv:1403.4782,* 2014.

[16] A. Mostafa, N. F. Soliman, M. Abdalluh, and F. E. Abd El-samie, "Speech encryption using two dimensional chaotic maps," in *2015 11th International Computer Engineering Conference (ICENCO)*, 2015: IEEE, pp. 235-240, doi: 10.1109/ICENCO.2015.7416354.

[17] X. Zhang, Y. Wang, J. Zeng, and Y. Wang, "A secure OFDM transmission scheme based on chaos mapping," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, 2015: IEEE, pp. 1-6.

[18] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Design of Efficient noise reduction scheme for secure speech masked by chaotic signals," *Journal of American Science,* vol. 11, no. 7, pp. 49-55, 2015.

[19] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using XOR based on Hénon map," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016: IEEE, pp. 1-5, doi: 10.1109/AIC-MITCSA.2016.7759915.

[20] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik,* vol. 127, no. 19, pp. 7431-7438, 2016.

[21] A. Mahdi, A. K. Jawad, and S. S. Hreshee, "Digital chaotic scrambling of voice based on duffing map," *International Journal of Information and Communication Sciences,* vol. 1, no. 2, pp. 16-21, 2016, doi: 10.11648/j.cej.20160102.11.

[22] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017: IEEE, pp. 132-137, doi: 10.1109/NTICT.2017.7976141.

[23] E. A. Albahrani, "A new audio encryption algorithm based on chaotic block cipher," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017: IEEE, pp. 22-27.

[24] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP Journal on Audio, Speech, and Music Processing,* vol. 2017, no. 1, pp. 1-11, 2017, doi: 10.1186/s13636-017-0118-0.

[25] F. Farsana and K. Gopakumar, "Private key encryption of speech signal based on three dimensional chaotic map," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, 2017: IEEE, pp. 2197-2201.

[26] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *Int. J. Commun. Antenna Propag,* vol. 8, pp. 257-264, 2018.

[27] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electronics,* vol. 8, no. 5, p. 530, 2019, doi: 10.3390/electronics8050530.

[28] A. M. Raheema, S. B. Sadkhan, and S. M. A. Satar, "Performance Enhancement of Speech Scrambling Techniques Based on Many Chaotic Signals," in *2020 International Conference on Computer Science and Software Engineering (CSASE)*, 2020: IEEE, pp. 308-313, doi: 10.1109/CSASE48920.2020.9142062.

[29] E. A. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 4, pp. 4270-4278, 2020.

[30] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map," *Multimedia Tools and Applications,* vol. 79, no. 25, pp. 17817-17835, 2020.

[31] D. Shah, T. Shah, M. M. Hazzazi, M. I. Haider, A. Aljaedi, and I. Hussain, "An Efficient Audio Encryption Scheme Based on Finite Fields," *IEEE Access,* vol. 9, pp. 144385-144394, 2021.

[32] R. I. Abdelfatah, M. E. Nasr, and M. A. Alsharqawy, "Realization of Audio Encryption using Elliptic Curve," vol. 13, no. 6, 2021.

[33] T. Bonny, W. A. Nassan, and A. Baba, "Voice encryption using a unified hyper-chaotic system," *Multimedia Tools and Applications,* pp. 1-19, 2022.

[34] S. Mokhnache, M. E. H. Daachi, T. Bekkouche, and N. Diffellah, "A Combined Chaotic System for Speech Encryption," *Engineering, Technology & Applied Science Research,* vol. 12, no. 3, pp. 8578-8583, 2022.

[35] N. Michailow *et al.*, "Generalized frequency division multiplexing for 5th generation cellular networks," *IEEE Transactions on Communications,* vol. 62, no. 9, pp. 3045-3061, 2014, doi: 10.1109/TCOMM.2014.2345566.

[36] S. Wu, "Massive MIMO channel modelling for 5G wireless communication systems," Heriot-Watt University, 2015.

[37] M. Matthé *et al.*, "Generalized frequency division multiplexing: a flexible multi-carrier waveform for 5G," in *5G Mobile Communications*: Springer, 2017, pp. 223-259.

[38] I. Gaspar *et al.*, "GFDM-A Framework for Virtual PHY Services in 5G Networks," *arXiv preprint arXiv:1507.04608,* 2015.

[39] S. K. Antapurkar, A. Pandey, and K. Gupta, "GFDM performance in terms of BER, PAPR and OOB and comparison to OFDM system," in *AIP Conference Proceedings*, 2016, vol. 1715, no. 1: AIP Publishing LLC, p. 020039.

[40] M. Gupta, A. S. Kang, and V. Sharma, "Comparative Study on Implementation Performance Analysis of Simulink Models of Cognitive Radio Based GFDM and UFMC Techniques for 5G Wireless Communication," *Wireless Personal Communications,* pp. 1-31, 2020, doi: 10.1007/s11277-020-07561-2.

[41] T. Van Waterschoot, V. Le Nir, J. Duplicy, and M. Moonen, "Analytical expressions for the power spectral density of CP-OFDM and ZP-OFDM signals," *IEEE Signal Processing Letters,* vol. 17, no. 4, pp. 371-374, 2010.

[42] H. Shimodaira, J. Kim, and A. S. Sadri, "Enhanced next generation millimeter-wave multicarrier system with generalized frequency division multiplexing," *International Journal of Antennas and Propagation,* vol. 2016, 2016, doi: 10.1155/2016/9269567.

[43] R. Datta, N. Michailow, M. Lentmaier, and G. Fettweis, "GFDM interference cancellation for flexible cognitive radio PHY design," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, 2012: IEEE, pp. 1-5.

[44] N. Michailow, S. Krone, M. Lentmaier, and G. Fettweis, "Bit error rate performance of generalized frequency division multiplexing," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, 2012: IEEE, pp. 1-5.

[45] N. Hassan and X. Fernando, "Massive MIMO wireless networks: An overview," *Electronics,* vol. 6, no. 3, p. 63, 2017.

[46] H. Q. Ngo, *Massive MIMO: Fundamentals and system designs*. Linköping University Electronic Press, 2015.

[47] M. A. Albreem, A. H. Al Habbash, A. M. Abu-Hudrouss, and S. S. Ikki, "Overview of precoding techniques for massive MIMO," *IEEE Access,* vol. 9, pp. 60764-60801, 2021.

[48] X. Cheng, M. Zhang, M. Wen, and L. Yang, "Index modulation for 5G: Striving to do more with less," *IEEE Wireless Communications,* vol. 25, no. 2, pp. 126-132, 2018.

[49] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE access,* vol. 5, pp. 16693-16746, 2017.

[50] V. V. Gudla and V. B. Kumaravelu, "Dynamic spatial modulation for next generation networks," *Physical Communication,* vol. 34, pp. 90-104, 2019.

[51] N. J. Smelser and P. B. Baltes, *International encyclopedia of the social & behavioral sciences*. Elsevier Amsterdam, 2001.

[52] H. R. Biswas, M. M. Hasan, and S. K. Bala, "Chaos theory and its applications in our real life," *Barishal University Journal Part,* vol. 1, no. 5, pp. 123-140, 2018.

[53] W. Ditto and T. Munakata, "Principles and applications of chaotic systems," *Communications of the ACM,* vol. 38, no. 11, pp. 96-102, 1995.

[54] B. Jovic, *Synchronization techniques for chaotic communication systems*. Springer Science & Business Media, 2011.

[55] G. Elert, *The chaos hypertextbook: Mathematics in the age of the computer*. Glenn Elert, 2003.

[56] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "On a new hyperchaotic system," *Physics Letters A,* vol. 372, no. 2, pp. 124-136, 2008.

[57] Y. Cao, "A new hybrid chaotic map and its application on image encryption and hiding," *Mathematical Problems in Engineering,* vol. 2013, 2013.

[58] G. Mateescu and M. Vladescu, "A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques," in *2013 Federated Conference on Computer Science and Information Systems*, 2013: IEEE, pp. 659-662.

[59] R. F. Martínez-González, J. A. Díaz-Méndez, L. Palacios-Luengas, J. López-Hernández, and R. Vázquez-Medina, "A steganographic method using Bernoulli's chaotic maps," *Computers & Electrical Engineering,* vol. 54, pp. 435-449, 2016.

[60] S. Sheela, K. Suresh, and D. Tandur, "A novel audio cryptosystem using chaotic maps and DNA encoding," *Journal of Computer Networks and Communications,* vol. 2017, 2017.

[61] S. Ayyappan and C. Lakshmi, "Empirical analysis of robust chaotic maps for image encryption," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 9 no. 11, 2020.

[62] N. A. Abbas and Z. H. Razaq, "Review of dct and chaotic maps in speech scrambling," *Journal of Theoretical and Applied Information Technology,* vol. 97, no. 2, pp. 569-582, 2019.

[63] B. Stoyanov and T. Ivanova, "Novel Implementation of Audio Encryption Using Pseudorandom Byte Generator," *Applied Sciences,* vol. 11, no. 21, p. 10190, 2021, doi: 10.3390/app112110190.

[64] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications,* vol. 18, no. 2, pp. 66-74, 2011.

[65] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE,* vol. 104, no. 9, pp. 1727-1765, 2016.

[66] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access,* vol. 6, pp. 4850-4874, 2017.

[67] R. U. Rahman and D. S. Tomar, "Security attacks on wireless networks and their detection techniques," in *Emerging Wireless Communication and Network Technologies*: Springer, 2018, pp. 241-270.

[68] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An overview of key technologies in physical layer security," *Entropy,* vol. 22, no. 11, p. 1261, 2020.

[69] S. B. S. Hussein Ali Ismael *A Proposed Speech Scrambling Based on Multi Chaotic Maps as key Generators*. Msc.thesis University of Babylon ,Iraq, 2017.

[70] H. N. A. Atheer Jabbar Mansor *FPGA Based Image Encryption Using Chaotic Systems*. PhD thesis ,University of Technology ,Iraq, 2017.

[71] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," *Annals of Telecommunications,* vol. 76, no. 3, pp. 155-174, 2021.

[72] W. Shi *et al.*, "Physical Layer Security Techniques for Future Wireless Networks," *arXiv preprint arXiv:2112.14469,* 2021.

[73] W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Cryptographic primitives and design frameworks of physical layer encryption for wireless communications," *IEEE Access,* vol. 7, pp. 63660-63673, 2019.

[74] I. Mishkovski and L. Kocarev, "Chaos-based public-key cryptography," in *Chaos-based cryptography*: Springer, 2011, pp. 27-65.

[75] Z. Su, S. Lian, G. Zhang, and J. Jiang, "Chaos-based video encryption algorithms," in *Chaos-Based Cryptography*: Springer, 2011, pp. 205-226.

[76] J. M. Blackledge, "Multi-algorithmic Cryptography using Deterministic Chaos with Applications to Mobile Communications," *ISAST Transactions on Electronics and Signal Processing,* vol. 2, no. 1, pp. 23-64, 2008.

[77] X. Wang and Y. Su, "An audio encryption algorithm based on DNA coding and chaotic system," *IEEE Access,* vol. 8, pp. 9260-9270, 2019.

[78] M. S. Khoirom, D. S. Laiphrakpam, and T. Tuithung, "Audio encryption using ameliorated ElGamal public key encryption over finite

field," *Wireless Personal Communications,* vol. 117, no. 2, pp. 809-823, 2021, doi: 10.1007/s11277-020-07897-9.

[79] J. Gutierrez, "Attacking the linear congruential generator on elliptic curves via lattice techniques," *Cryptography and Communications,* vol. 14, no. 3, pp. 505-525, 2022, doi: 10.1007/s12095-021-00535-6.

[80] O. Reyad and Z. Kotulski, "On pseudo-random number generators using elliptic curves and chaotic systems," *Applied Mathematics & Information Sciences,* vol. 9, no. 1, pp. 31-38, 2015, doi: 10.12785/amis/090105.

[81] F. Duemong and L. Preechaveerakul, "Applying Pell Numbers for Efficient Elliptic Curve Large Scalar Multiplication," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, 2018: IEEE, pp. 1-4.

[82] E. Bashier, "Speech scrambling based on chaotic maps and one-time pad, Computing, Electrical and Electronics Engineering (ICCEEE)," in *International Conference on*, 2013, pp. 128-133.

[83] A. S. P. A. Selvan, "A review of analog audio scrambling methods for residual intelligibility," *Innovative Systems Design and Engineering,* vol. 3, no. 7, 2012.

[84] M. Theberge, "Security evaluation of transform domain speech scramblers," University of British Columbia, 1996.

[85] J. Jayakurami and G. Dhanya, "A review of analog speech scrambling for secure communication," *Progress in science and engineering research journal,* vol. 2, pp. 194-198, 2016.

[86] J. Ahmed and N. Ikram, "Frequency-domain speech scrambling/descrambling techniques implementation and evaluation on DSP," in *7th International Multi Topic Conference, 2003. INMIC 2003.*, 2003: IEEE, pp. 44-48.

[87] S. B. Sadkhan and R. S. Mohammed, "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication," *Procedia computer science,* vol. 65, pp. 314-323, 2015, doi: 10.1016/j.procs.2015.09.089.

[88] J. B. Lima and E. F. da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools and Applications,* vol. 75, no. 14, pp. 8403-8418, 2016.

[89] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system," in *Journal of Physics: Conference Series*, 2021, vol. 1804, no. 1: IOP Publishing, p. 012048, doi: 10.1088/1742-6596/1804/1/012048.

[90] S. N. Al-Saad and E. H. Hashim, "A speech scrambler algorithm based on chaotic system," *Al-Mustansiriyah J. Sci,* vol. 24, no. 5, pp. 357-372, 2013.

[91] A. M. Raheema, S. B. Sadkhan, and S. M. A. Sattar, "Performance evaluation of voice encryption techniques based on modified chaotic systems," in *2020 6th International Engineering Conference "Sustainable Technology and Development"(IEC)*, 2020: IEEE, pp. 135-140, doi: 10.1109/IEC49899.2020.9122933.

[92] M. Matthé, N. Michailow, I. Gaspar, and G. Fettweis, "Influence of pulse shaping on bit error rate performance and out of band radiation of generalized frequency division multiplexing," in *2014 IEEE International Conference on Communications Workshops (ICC)*, 2014: IEEE, pp. 43-48.

اقرار لجنة المناقشة

نحن اعضاء لجنة المناقشة, نشهد باننا اطلعنا على اطروحة الدكتوراه الموسومة

نظام تعدد الإرسال بتقسيم التردد العام على أساس فائق الفوضى المدمج للتشفير الصوتي في شبكات الجيل الخامس

وقد ناقشنا الطالب (**محمد جبار محمد امين**) في محتوياتها وفيما له علاقة بها ,نؤيد انها جديرة بالقبول لنيل درجة الدكتوراه فلسفة في علوم الهندسة الكهربائية/ هندسة الالكترونيك والاتصالات.

رئيس اللجنة

التوقيع:
الاسم: أ.د ليث علي عبد الرحيم
التاريخ
عضو اللجنة

عضو اللجنة

التوقيع:
الاسم: أ.د اسامة قاسم جمعة
التاريخ
عضو اللجنة

التوقيع:
الاسم: أ.د يهاب عبد الرزاق حسين
التاريخ
عضو اللجنة

التوقيع:
الاسم: أ.د أحمد عبد الكاظم حمد
التاريخ
عضو اللجنة

التوقيع:
الاسم: أ.م.د رائد خالد ابراهيم
التاريخ
مصادقة رئيس القسم

التوقيع:
الاسم: أ.د سعد سفاح حسون (مشرفا)
التاريخ
مصادقة عميد الكلية

التوقيع:
الاسم: أ.د قيس كريم عمران
التاريخ

التوقيع:
الاسم: أ.د حاتم هادي عبيد
التاريخ

نظام التشفير الثالث المقترح تم تصميمه بناءً على خرائط الفوضى الثلاثية وتسلسل EC-LCG داخل مُعدِّل GFDM ، تدعى تقنية HC-EC-GFDM. تشتمل الخرائط المستخدمة على خرائط Ikeda و Tent و Duffing تخلط مع الاجزاء الحقيقية والخيالية الرموز الفرعية لـ GFDM ثم تبديل الرموز الفرعية المشفرة. التقييمات الأمنية SNR=-27.4971 dB, PSNR=0.85673 dB, SSSNR=-34.9912 dB, d_{LPC}=0.14921, d_{CD}=8.9547,d_{Log}=21.9564, d_{FWLOG}=34.7654, MSE=0.82097, RMS=0.90518, CF=0.86503, R_{xy}=-0.0023, UACI=33.334% and NSCR=99.995%, key space=2^{510}, and speed =24×10^{-6}Sec./KB.

نظام التشفير الرابع المقترح تم تصميمه على أساس الخرائط الفوضوية الثلاثية ، وخوارزمية MMSE Linear Precoding of Massive MIMO ، وتسمى Hybrid Chaotic QR-Decomposition تقنية HC-QR-MMSE. تشتمل الخرائط المستخدمة على خرائط Bernoulli و Henon و Logistic المختلطة باستخدام عامل QR لإنتاج خريطة فوضوية هجينة جديدة. يتم دمج التسلسل الجديد مع مصفوفة الترميز المسبق MMSE بأجزاء حقيقية وخيالية ثم يتم تبديلها. النتائج الأمنية هي SNR= -28.2993 dB, PSNR=0.05458 dB, SSSNR=-35.836 dB, d_{LPC}=0.9353, d_{CD}=7.6197,d_{Log}=24.4176, d_{FWLOG}=26.7063, MSE=0.98751, RMS=0.99297, CF=0.0610, R_{xy}=-0.00156, UACI=33.334%, and NSCR=99.9958%, key space=2^{500}, and speed =28.3×10^{-6} Sec./KB.

من مقاييس الأمان للانظمة المقترحة، توفر تقنية HC-QR-MMSE مستوى أمان عاليًا اكثر من التقنيات الأخرى نظرًا لانخفاض الوضوح المتبقي. بشكل عام ، تتمتع جميع أنظمة التشفير المقترحة بأمان ممتاز ، ومقاومة للهجمات المختلفة ، وجودة عالية للاشارات المستردة ، ومساحة مفاتيح سرية كبيرة ، ووضوح متبقي منخفض ، ووقت حسابي قصير ، مما يجعلها مناسبة للاتصال في الوقت الفعلي.

الخلاصة

تواجه الاتصالات اللاسلكية تحديات أمنية كبيرة ، لذلك هناك ضرورة مستمرة لتطوير إستراتيجية أمنية مناسبة لحماية البيانات من المتلصصين باستخدام التشفير على أساس نظرية الفوضى. نظام تعدد الإرسال بتقسيم التردد العام هو شكل موجة حديث متعدد الموجات قابل للتكيف مع متطلبات الجيل الخامس ، ولكن لم يتم النظر في مشكلاته الأمنية. في هذه الاطروحة ، تم اقتراح أربع خوارزميات جديدة لتشفير الصوت استنادًا إلى خرائط فوضوية متعددة مع تشفير الحمض النووي وتشفير المنحنى الاهليجي تنفذ داخل مكونات شبكة الجيل الخامس ، بما في ذلك نظام تعدد الإرسال بتقسيم التردد العام التظمين المكاني المتوازي - نظام متعدد المدخلات-متعدد المخرجات الضخم. تتمثل الفكرة الرئيسية لاستخدام العديد من الخرائط الفوضوية في مكان غير متوقع الى زيادة التعقيد ضد المتلصصين.

تم تصميم أول نظام تشفير مقترح بناءً على خرائط فوضوية متعددة تسمى تقنية تشفير Hybrid Chaotic Modulo Operator (HCMO). تشتمل الخرائط المستخدمة على خرائط Bernoulli و Standard و Bogdanov تخلط مع الصوت بناءً على modulo operator. اختبارات الأمان هي SNR=-23.5969 dB, PSNR=4.7569 dB, SSSNR=-31.0528 dB, d_{LPC}=0.9612, d_{CD}=8.1925,d_{Log}=21.1417, d_{FWLOG}=23.0908, MSE=0.3344, RMS=0.5773, CF=4.7698, R_{xy}=0.0069, UACI=33.334% and NSCR=99.99%, key space=2^{500}, and speed =6.67×10^{-7} Sec./KB.

نظام التشفير الثاني المقترح تم تصميمه بناءً على خرائط ثلاثية الفوضى ، وترميز الحمض النووي في فهرس هوائي PSM وتسمى تقنية DNA-AI-PSM. تشمل الخرائط الفوضوية المستخدمة خرائط Tinkerbell واللوجستية وخرائط Henon متعددة الإرسال باستخدام فهرس الهوائي باستخدام قواعد مختلفة لتشفير DNA ومستويين من XOR في مجال التردد. مقاييس الأمان هي SNR=-24.544 dB, PSNR=3.8099 dB, SSSNR=-31.992 dB, d_{LPC}=1.0257, d_{CD}=7.3827,d_{Log}=21.787, d_{FWLOG}=26.3629, MSE=0.4159, RMS=0.64375, CF=3.8254, R_{xy}=-0.00097, UACI=33.334% and NSCR=99.979%, key space=2^{632}, and speed =9.3×10^{-7}Sec./KB.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية الهندسة
قسم الهندسة الكهربائية

نظام تعدد الإرسال بتقسيم التردد العام على أساس فائق الفوضى المدمج للتشفير الصوتي في شبكات الجيل الخامس

اطروحة
مقدمة إلى كلية الهندسة في جامعة بابل
وهي جزء من متطلبات الحصول على درجة الدكتوراة
فلسفة في هندسة الالكترونيك والاتصالات

من قبل

محمد جبار محمد امين

باشراف
الاستاذ الدكتور

سعد سفاح حسون

٢٠٢٣م ١٤٤٤ هـ