



**AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO-EGYPT**

Electronics and Communications Engineering Department

Analysis of Secure Hybrid Speech Coding Systems

A dissertation

Submitted in partial fulfillment for the requirements of the degree of PHD in
Electrical Engineering

Submitted by

Eman Mohammed Mahmoud Ibrahim

Master engineering in the Electronics and Communications Eng. Dept.
Modern Academy

Supervised by

Prof. Dr. Abdelhalim Zekry

**Professor in the Electronics and Communications Eng. Dept.
Faculty of Engineering - Ain Shams University**

Prof. Dr. Talaat Abdellatief Elgarf

**Professor in the Electrical and Computer Eng. Dept.
Higher Technical Institute (HTI)**

Dr. Ahmed Abdelhafez

Egyptian Armed Force

2013



**AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO-EGYPT**

Electronics and Communications Engineering Department

Analysis of Secure Hybrid Speech Coding Systems

Examiner Committee

Name: Eman Mohammed Mahmoud
Dissertation: Analysis of Secure Hybrid Speech Coding Systems
Degree: PHD in Electrical Engineering
(Electronics and Communications Engineering)

Title, Name and Affiliation	signature
------------------------------------	------------------

1. **Prof. Dr. Ir. Mostafa Sayed Afifi**
Visitor Professor in Electronics and Computer,
Moor School of Engineering - University of Pennsylvania
2. **Prof. Dr. Wagdy Refaat Anis**
Professor in Electronics and Communications Eng. Dept.
Faculty of Engineering - Ain Shams University
3. **Prof. Dr. Abdelhalim Zekry**
Professor in the Electronics and Communications Eng. Dept.
Faculty of Engineering - Ain Shams University
4. **Prof. Dr. Talaat Abdellatief Elgarf**
Professor in the Electrical and Computer Eng. Dept.
Higher Technical Institute (HTI)

Date: 1 / 7 /2013

STATEMENT

This dissertation is submitted to Ain-Shams University in partial fulfillment for degree of Doctor of philosophy in Electrical Engineering (Electronics and Communication Engineering).

The work included in this dissertation was carried out by the author at the Electronics and Communications Engineering Department, Ain Shams University.

No part of this dissertation has been submitted for a degree or a qualification at any other university or institute.

Name : Eman Mohammed Mahmoud Ibrahim

Signature:

Date: 1 / 7 /2013

**To My Father,
To My Mother,**

I present to you this dissertation.

May I by this express my deepest gratitude and love

Thanks

Without you, I could not have reached this successful step in my life

Abstract

Eman Mohammed Mahmoud Ibrahim

Analysis of Secure Hybrid Speech Coding Systems

Doctor of philosophy dissertation

Ain Shams University, 2013

Key words: Hybrid speech coder, MP-CELP, Variable Bit Rate Speech Coder, Dynamic AES,

In modern communication systems, low bit rate speech coder is widely utilized to increase the channel capacity and the bandwidth efficiency of the networks. It is used to satisfy the growing demand for new speech communication applications in past decades. Speech coders are capable of delivering toll-quality speech at lower rates. Specifically, at present, there is a surge of research and commercial interest to develop high quality speech coders operating at bit rates of 4 kbps and below.

Hybrid coding combines the strength of a waveform coder with that of a vocoder. Like a vocoder, hybrid coding relies on a speech production model. During encoding, model parameters are estimated and optimized in such a way that the decoded speech is as close as possible to the original waveform, with the closeness often measured by a perceptually weighted error signal. As in waveform coders, an attempt is made to match the original signal with the decoded signal in the time domain. A hybrid coder tends to behave like a waveform coder for high bit-rate, and like a vocoder at low bit-rate, with fair to good quality for medium bit-rate.

The main objective of dissertation is to design a variable bitrate speech codec, which provides good speech quality at low bitrate, optimum level of security and high immunity of noise.

In this dissertation:

- Various types of hybrid coding techniques have been discussed.
- Then the standard version of Multi Pulse Maximum Likelihood Quantization (MP-MLQ) coder is implemented. This coder is a generic algorithm for implementing high efficiency and high-quality speech coding. It is used in ITU-T G723.1 standard speech codec, which is based on CELP coder.
- In addition, a variable bit rate MP-MLQ codec is developed and implemented without serious effect on speech quality. The realized bit rates are 5.9, 5.4, 4.9, 4.3 and 3.9 kbps.
- The output of the MP-MLQ coder is applied to AES encryption unit with some nonlinear improvements to enhance its security level and add a customized form of the original standard AES.
- A dynamic AES-128 with key dependent S-box is designed and implemented in this dissertation.
- Moreover, a new channel coding method is presented based on the Joint Channel Coding and Cryptographic approach. This approach is used to increase the channel noise immunity.

-
- Finally, these building blocks are integrated in an Adaptive bit rate speech codec. This integrated codec is operated adaptively in accordance to the condition of the channels. Low bit rate speech coder modes are used in a bad channel conditions.

Dedication

I would like to dedicate this dissertation to my parents, Mohammed Mahmoud and Bader Hanafy who have been an inspiration throughout my life and who have been supportive for all I have achieved. I wish dedicate this dissertation to my brothers Mohammed, Bassem and Mahmoud for their support and encouragement.

ACKNOWLEDGMENTS

All gratitude and praise to ALLAH first and last who helps me to complete this work.

I would like to take this opportunity to express my sincere gratitude to Prof. Dr. Abdelhalim Zekry for his advice and guidance. He has provided me numerous valuable suggestions and encouragement.

I would like to thank and appreciate Dr. Talaat Abdellatief Elgarf for putting his trust on me, his insightful remarks, valuable consultation and support.

A special thanks and appreciation goes to Dr. Ahmed Abdelhafez not only for this supervision, guidance, and suggestions during this work but also for his unlimited assistance and helpful comments.

Sincere thanks are presented to all members of Communication Department of Modern Academy for the unlimited supporting and valuable comments during preparing this desperation.

I would also like to thank my family and friends for their motivation, understanding, advice encouragement and their direct and indirect assistance.

Emar Mohammed Mahmoud Ibrahim

Table of contents

STATEMENT	III
ABSTRACT	V
DEDICATION	VIII
ACKNOWLEDGMENTS.....	IX
TABLE OF CONTENTS.....	X
LIST OF FIGURES	XV
LIST OF TABLES	XVIII
ABBREVIATIONS	XIX
LIST OF SYMBOLS.....	XXI
CHAPTER 1 : INTRODUCTION	2
1.1 Motivation	2
1.2 Scope of Dissertation.....	2
1.3 Organization of the Dissertation.....	3
1.4 Main Contribution	4
1.5 Publications.....	5
CHAPTER 2 : HYBRID SPEECH CODERS 7	
2.1 Introduction	7
2.2 Analysis by Synthesis.....	8
2.3 The Regular Pulse Excitation, Long-Term Prediction (RPE-LTP)	10
2.3.1 RPE-LTP Encoder	10
2.3.2 RPE-LTP Decoder	13
2.3.3 RPE-LTP Applications.....	13
2.3.3.1 GSM FR bit a location	13

2.4	Multi-Pulse Linear Prediction Coding (MP-LPC)	14
2.4.1	MP-LPC Encoder	14
2.4.2	MP-LPC Decoder	16
2.5	Vector-Sum Excited Linear Prediction (VSELP)	16
2.5.1	Encoder steps	16
2.5.2	VSELP Decoder	18
2.5.3	VSELP application	19
2.5.3.1	GSM FR coder Bit allocation	19
2.6	Code Excitation Linear Prediction (CELP)	20
2.6.1	CELP Encoder	20
2.6.2	CELP Decoder	21
2.6.3	CELP Standards	22
2.6.4	Federal Standard 1016	22
2.6.4.1	ITU-T G.728 Low Delay CELP	22
2.6.4.2	ITU-T G.723.1 Algebraic CELP/Multi-Pulse Coder	23
2.6.4.3	ETSI GSM 6.60 Enhanced Full Rate Algebraic CELP	24
2.6.4.4	ETSI GSM 6.90 Adaptive Multi-rate Algebraic CELP	25
2.7	Attributes of speech codec	26
2.8	Measurement of speech quality	26
2.8.1	Subjective analysis	26
2.8.2	Objective analysis	27
2.8.2.1	Absolute error (ABSErr)	27
2.8.2.2	Percentage error	27
2.8.2.3	Mean Squared Error (MSE)	27
2.8.2.4	Root Mean Squared Error (RMSE)	28
2.8.2.5	Signal to Noise Ratio (SNR)	28
2.8.2.6	Segmental Signal to noise ratio (SEGSNR)	28
2.9	Epilog	28
 CHAPTER 3 : MULTI-PULSE CODE EXCITED LINEAR PREDICTIVE MP-CELP 31		
3.1	Introduction	31
3.2	MP-CELP Encoder	31
3.2.1	Framing	34
3.2.2	Preprocessing	34
3.2.3	Linear Prediction Analysis	35
3.2.4	LSP Analysis and Quantization	36
3.2.5	LSF inverse decoder	38
3.2.6	Formant Weighting Filter	39
3.2.7	The Open Loop Pitch Estimation	40
3.2.8	Harmonic Noise Shaping Filter	41
3.2.9	Impulse response calculator	43
3.2.10	Computation of the Target Signal	43

3.2.11	Generation of the Excitation Signal	43
3.2.11.1	Adaptive codebook excitation.....	43
3.2.11.2	Fixed Codebook (Multi-Pulse)	45
3.2.11.2.1	Pitch Repetition	46
3.2.11.2.2	Pulse Positions and Amplitudes	47
3.2.11.2.3	Estimating the Pulse Amplitude.....	48
3.2.11.2.4	Pulse positions	48
3.2.11.3	Excitation parameters coding.....	49
3.2.11.3.1	Coding the Multi-pulse Pulse Positions.....	49
3.2.11.3.2	Combined Gain Coding	50
3.2.12	Bit allocation	50
3.3	MP-CELP Decoder	51
3.3.1	Generation of Excitation signal	51
3.3.1.1	Adaptive codebook	52
3.3.1.2	Fixed codebook (multi-pulse).....	52
3.3.2	Pitch post filter	53
3.3.3	Synthesize filter.....	53
3.3.4	Formant post filter	54
3.4	Evaluation of the standard MP-CELP	54
3.5	Epilog	56
CHAPTER 4 : IMPLEMENTATION OF VARIABLE BIT RATE MP-CELP		58
4.1	Introduction	58
4.2	Variable Bit Rate Speech Coder	58
4.3	The importance of coded bits	59
4.4	The Variable Bit Rate MP-CELP	62
4.4.1	Mode of 6.3 kbps	63
4.4.2	Mode of 5.9 kbps	63
4.4.3	Mode of 5.4 kbps	64
4.4.4	Mode of 4.9 kbps	64
4.4.5	Mode of 4.3 kbps	65
4.4.6	Mode of 3.9 kbps	66
4.5	Evaluation of Variable Bit Rate MP-CELP	66
4.5.1	Mean opinion score	66
4.5.2	Objective tests	67
4.6	Epilog	71
CHAPTER 5 : DYNAMIC AES WITH KEY DEPENDENT S-BOX		73
5.1	Introduction	73

5.2	Overview on Advanced Encrypted Standard.....	73
5.3	Structure of Standard AES-128	75
5.3.1	AES initialize operations.....	76
5.3.1.1	S-box generation operation	77
5.3.1.2	KeyExpansion operation.....	78
5.3.2	AES Cipher Transformations	80
5.3.2.1	The Sub-Byte transformation	80
5.3.2.2	Shift-Row transformation.....	81
5.3.2.3	Mix-Columns Transformation	81
5.3.2.4	Add-Round-Key Transformation	82
5.3.3	AES Inverse Cipher Transformations.....	82
5.3.3.1	Inv.-Shift-Row Transformation	83
5.3.3.2	Inv.-Sub-Bytes Transformation.....	83
5.3.3.3	Inv.-Mix-Column Transformation.....	83
5.3.3.4	Inverse of Add-Round-Key Transformation.....	84
5.4	Dynamic AES with Key Dependent S-Box.....	84
5.4.1	The PN sequence generator.....	84
5.4.2	Permutation block.....	85
5.4.3	The proposed Key Dependent S-Boxes	86
5.5	Security Analysis	88
5.5.1	Randomness tests	88
5.5.2	Avalanche effect	88
5.5.3	Correlation factor.....	88
5.5.4	Simulation time.....	89
5.6	Evaluation of implemented AES with key dependent S-box	89
5.6.1	Image Histogram test.....	89
5.6.2	Avalanche effect due to one bit change in plaintext	91
5.6.3	Avalanche effect due to one bit change in secret key	94
5.6.4	Correlation factor.....	98
5.6.5	Simulation time.....	99
5.7	Epilog	99
CHAPTER 6	CHANNEL CODING	101
6.1	Introduction	101
6.2	Digital Error Correction System	101
6.2.1	Convolution coding	102
6.2.1.1	Soft Decode Algorithm	104
6.2.2	Turbo Coding.....	104
6.3	Proposed Channel Coder	105
6.3.1	Proposed channel coding building blocks.....	107
6.3.1.1	Advanced Encrypting Standard	107
6.3.1.2	Channel encoder	108

6.3.1.3	Soft input soft output decoder	108
6.3.1.4	The Decision block.....	108
6.3.1.4.1	Soft Input Encryption	110
6.3.1.4.2	Soft input Decryption.....	111
6.3.2	Performance of proposed channel coder	112
6.4	Channel Coding in Speech Codec	115
6.4.1	Channel coding of VSELP Codec.....	116
6.4.2	Channel Coding of RPE-LTP Codec	117
6.4.3	Channel coding for ACELP codec.....	118
6.4.4	High protected Channel coding for AMR WB codec	118
6.4.4.1	6.6 kbps mode	119
6.4.4.2	8.85 kbps mode	119
6.4.4.3	19.85 kbps mode	120
6.5	System Model for Standard MP-MLQ Speech Coder	120
6.5.1	Ordinary channel coding	120
6.5.2	High protected channel coding.....	122
6.5.3	Proposed channel coding.....	124
6.5.4	Evaluation of the designed channel coder.....	125
6.6	The proposed Integrated Speech codec.....	126
6.6.1	Mode 1 of the proposed speech codec	127
6.6.2	Mode 2 of the proposed speech codec	128
6.6.3	Mode 3 of the proposed speech codec	128
6.6.4	Mode 4 of the proposed speech codec	129
6.6.5	Mode 5 of the proposed speech codec	130
6.6.6	Mode 6 of the proposed speech codec	131
6.6.7	Comparison between proposed codec modes	131
6.7	Epilog	133
CHAPTER 7	CONCLUSION AND FUTURE WORK.....	135
7.1	Conclusion.....	135
7.2	Future work.....	136
APPENDIX A		139
APPENDIX B		155
APPENDIX C		158
REFERENCE		164

List of Figures

Figure 1.1 Complete integrated speech coder	3
Figure 2.1 Speech quality for different speech coding methods	7
Figure 2.2 Analysis by Synthesis codec	9
Figure 2.3 Block diagram of RPE-LTP speech encoder.....	11
Figure 2.4 Block diagram of the RPE-LTP speech decoder	13
Figure 2.5 Block diagramed of MP-LPC encoder.....	15
Figure 2.6 Block diagram of MP-LPC decoder.....	16
Figure 2.7 Black diagram of the VSELP speech encoder	17
Figure 2.8 General block of CELP encoder.....	21
Figure 2.9 Block diagram of general CELP decoder.....	21
Figure 3.1 Detailed MP-CELP encoder block diagram	33
Figure 3.2 LP analysis steps	35
Figure 3.3 LSP analysis and quantizing steps	36
Figure 3.4 Block diagram of MP-CELP Decoder	51
Figure 3.5 Original and synthesized signal.....	55
Figure 4.1 Bit error sensitivity of CELP coded speech.....	61
Figure 4.2 Bit error sensitivity of LSF sub-vectors.....	61
Figure 4.3 Bit error sensitivity of ACB excitation signal	61
Figure 4.4 Bit error sensitivity of FCB excitation signal.....	62
Figure 4.5 "osdadE.wav" waveform	68
Figure 4.6 Sub-frame 2 of frame 18	69
Figure 4.7 Error predictions of three codec modes with 5 samples	69
Figure 4.8 SEGSNR for designed variable codec with respect to standard codec	70
Figure 5.1 AES block diagram.....	76
Figure 5.2 Secret key rearrange	79
Figure 5.3 Key Expansion Operation.....	80
Figure 5.4 SubByte transformation.....	81
Figure 5.5 Shift-Rows transformation	81
Figure 5.6 Inv.-ShiftRows transformation.....	83