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.

Eman Mohammed Mahmoud Ibrahim

Table of contents

List of Figures