AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO-EGYPT
Electronics and Communications Engineering Department

Security of vocoding techniques

A thesis
Submitted in partial fulfillment for the requirements of the degree of Master of Science in Electrical Engineering

Submitted by

Eman Mohammed Mahmoud Ibrahem

Electronics and communications Eng. Dept.
Shoubra Faculty of Engineering- Zagazig University

Supervised by

Prof. Dr. Abd-Elhalim Zekry
Professor in the Electronics and Communications Eng. Dept.
Faculty of Engineering - Ain Shams University

Prof. Dr. Talaat Abdel Latief Elgarf
Professor in the Electrical and Computer Eng. Dept.
Higher Technical Institute (HTI)

Prof. Dr. Mohammed Al-Sٍٍٍٍaed Abdel Aleem
Professor in the Electronics and Communications Eng. Dept.
Modern Academy

2009

STATEMENT

This thesis is submitted to Ain-Shams University in partial fulfillment of the degree of Master of Science in Electrical Engineering.

The work included in this thesis was carried out by the author in the department of electronics and communications engineering, Ain Shams University.

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

Name : Eman Mohammed Mahmoud Ibrahem

Signature:

Date : / / 2009

To My Mother,

To My Father,

I present to you this thesis

May I by this express my deepest gratitude and love

Thanks

Without you, I couldn’t have reached this successful step in my life

Abstract

Eman Mohammed Mahmoud Ibrahem, "Security of vocoding techniques"
Master of Science dissertation, Ain Shams University, 2009

Key words: voice coder, Vocoder, LPC, speech analysis, encryption, LFSR, stream cipher, Pseudo random, randomness.

Secure Vocoding technique, as its name implies, is a combination of a speech coding technique and a secure technique. Speech coding techniques deal with digitizing analog speech signals in an efficient way. Their objective is to represent the speech signal with the lowest number of bits, while maintaining a sufficient level of quality of the synthesized speech. Secure techniques ensure that the transmitted digitized speech is similar to a random binary sequence with the difficulty to estimate any part of it.

Speech coding techniques are classified into three main groups: waveform coders, Vocoders and hybrid coders. Waveform coders offer excellent voice quality with higher bit rates. Vocoders or parametric coders assume that the speech signal is generated from a model which is controlled by some parameters. Parameters of the model are estimated from the input speech signal. This class of coders has lower bit rates but less voice quality and speaker recognition. Hybrid coders combine the advantages of waveform coders and Vocoders.

This thesis includes two main parts, the first part deals with the design and implementation of a vocoding technique of the type Linear Predictive Coder (LPC). This LPC coding technique is based on mathematical approximation of vocal tract by a tube of varying diameter. At a particular time, the speech sample is represented as a linear sum of the previous samples. The speech signal is subdivided into small segments of 30msec to improve performance and quality of the technique. A linear predictive filter is the heart of this technique to predict next sample as a linear combination of previous samples.

The autocorrelation method is applied to estimate the coefficients of LP filter. Voiced and unvoiced segments are determined in addition to pitch frequency. Possible methods for pitch estimation or voice determination are covered.

The second part of this thesis deals with the design and implementation of a secure stream cipher algorithm. Cipher system algorithms including block ciphers, stream ciphers and public key ciphers are introduced. The main building elements of the stream cipher algorithms are presented. A highly Nonlinear and random stream cipher algorithm is designed and implemented to encrypt the output of the LPC coder. To assess the randomness properties and other security parameters of the designed algorithm we applied the standard NIST (National Institute of Standards and Technology) package to test the output sequence of the LPC Vocoder. The proposed algorithm passed all the tests successfully. Other theoretical security parameters of the algorithm are calculated like key diversity, period and linear complexity.

This thesis includes five chapters and three appendices as follows:

- Chapter one: deals with speech coders.
- Chapter two: deals with LPC coders.
- Chapter three: deals with security of vocoding systems
- Chapter four: deals with the design and implementation of a secure vocoding technique.
- Chapter five: includes the conclusions and suggested future work.

The three appendices are:

- Soft ware Simulation (MATLAB) of the secure vocoding system
- Chi- square distribution table.
- Tables of primitive polynomials.

The designed secure vocoding system in this thesis can be implemented in many telecommunication systems to achieve lower bit rates for digitized speech signals and high security level. The software implementation is in MATLAB.

ACKNOWLEDGMENTS

ACKNOWLEDGMENTS

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

I would like to thank Prof. Dr. Abd-Elhalim Zekry for giving me the chance to work under this supervision and for helping me in targeting this field and in this patience with me and full time co-operation he showed along the past three years.

A special thanks and appreciation to Prof. Dr. Talaat Abdel Latief Elgarf not only for this supervision, guidance, and suggestions during this work but also for his unlimited assistance and helpful comments.

I would like also to express my deepest gratitude to Prof. Dr. Mohammed Al-Saed Abdel Aleem for his insightful remarks, valuable consultation and support.

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

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 Ibrahem

Table of contents

List of figures

List of Tables

Abbreviations

ACF	Auto Correlation Function
ADC	Analog to Digital Converter
AMDF	Average Magnitude Difference Function
APC	Adaptive Predictive Coding
CELP	Code–Excited Linear predictor
DF	Degree of Freedom
DFT	Discrete Fourier Transform
EVMS	Electronic Voice Mail Service
IDFT	Inverse Discrete Fourier Transform.
LFSR	Linear Feedback Shift Register
Log	Logarithm
LP	Linear Predictive Analysis
LPC	Linear Prediction Coding
MELP	Mixed Excitation Linear Prediction
NIST	National Institute of Standards and Technology
PCM	Pulse Code Modulation
PRNG	Pseudo Random Number Generator
PSD	Power Spectral Density
RNG	Random Number Generator
SBC	Sub Band Coder
SD	Spectral Density
UMTS	Universal Mobile Telecommunications System
Vocoder	Voice Coder

List of symbols

R_b	Bit rate
$y(n)$	nth output sample of vocal track model
a_k	Vocal track parameter
G	Gain factor
$x(n)$	Excitation source of speech production
p	Order of LPC model
$P_1(z)$	Short term prediction filter
$P_2(z)$	Long term prediction filter
$H(z)$	Transfer function of LP digital filter
$S(z)$	Speech sample
$U(z)$	Excitation source
$\tilde{S}(z)$	Synthesize speech
α_k	Predictor coefficient of LP time varying filter
$e(n)$	Prediction error
$A(z)$	Transfer function of prediction error filter
E_n	Average mean square error
$\tilde{\alpha}_k$	Predictor coefficient of LP time varying filter which minimize E_n
Z_n	Zero crossing rate
SD	Frequency spectrum of speech window
$c(\tau)$	Cepstrum
s(n + k)	The time lagged version of the original signal
T	Period of the signal
N	Number of samples of speech window
R_n	Auto correlation function
$R(i)$	Autocorrelation coefficients
$R\hat{}(i)$	Autocorrelation coefficients of the predictive filter
$f(x)$	characteristic polynomial of LFSR
$Lc(M)$	Lower limit of linear complexity
X^2	Chi square test

CHAPTER ONE

Speech coders