



**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 Ibrahim**

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-Saeed 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 Ibrahim

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 Ibrahim, “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 Ibrahim**

## Table of contents

|                                                                     |      |
|---------------------------------------------------------------------|------|
| ABSTRACT .....                                                      | V    |
| TABLE OF CONTENTS .....                                             | VIII |
| LIST OF FIGURES.....                                                | XI   |
| LIST OF TABLES.....                                                 | XII  |
| ABBREVIATIONS .....                                                 | XIII |
| LIST OF SYMBOLS.....                                                | XIV  |
| CHAPTER ONE: SPEECH CODERS .....                                    | 2    |
| 1.1    OVERVIEW OF SPEECH CODING .....                              | 2    |
| 1.1.1    Speech coding system.....                                  | 2    |
| 1.1.2    Desirable Properties of a Speech Coder.....                | 3    |
| 1.1.3    Applications of Speech Coders .....                        | 4    |
| 1.2    SPEECH PRODUCTION AND MODELLING.....                         | 4    |
| 1.2.1    Origin of speech signal .....                              | 4    |
| 1.2.2    Classifications of speech signals .....                    | 6    |
| 1.2.3    Modelling of speech production mechanism .....             | 7    |
| 1.3    PROPERTIES OF THE HUMAN AUDITORY SYSTEM .....                | 9    |
| 1.4    CLASSIFICATION OF SPEECH CODERS .....                        | 10   |
| 1.4.1    Classification by bit rate .....                           | 10   |
| 1.4.2    Classification by coding techniques .....                  | 11   |
| 1.4.2.1    Waveform coders.....                                     | 11   |
| 1.    Adaptive Predictive Coding (APC) .....                        | 11   |
| 2.    Sub Band Coder (SBC) .....                                    | 12   |
| 1.4.2.2    Parametric Coders (Vocoder) .....                        | 13   |
| 1.    Channel Vocoder .....                                         | 14   |
| 2.    Formant Vocoder .....                                         | 16   |
| 3.    Linear Prediction Coding (LPC).....                           | 16   |
| 4.    Mixed Excitation Linear Prediction (MELP) .....               | 18   |
| 1.4.2.3    Hybrid Coders .....                                      | 19   |
| 1.5    CONCLUSION.....                                              | 20   |
| CHAPTER TWO: LPC VOCODER .....                                      | 22   |
| 2.1    INTRODUCTION .....                                           | 22   |
| 2.2    LP MATHEMATICAL MODEL .....                                  | 23   |
| 2.3    LPC ENCODER.....                                             | 26   |
| 2.3.1    Sub divided voice signal.....                              | 26   |
| 2.3.2    Parameters estimation .....                                | 27   |
| 2.3.2.1    Voice estimation .....                                   | 27   |
| •    Zero crossing rate.....                                        | 27   |
| 2.3.2.2    Pitch detection .....                                    | 29   |
| I.    Preprocessing .....                                           | 29   |
| II.   Pitch estimation algorithm .....                              | 30   |
| •    Algorithm of spectral analysis.....                            | 30   |
| •    Cepstrum.....                                                  | 32   |
| •    Average Magnitude Difference Function (AMDF).....              | 34   |
| •    Auto Correlation Function (ACF).....                           | 35   |
| III.  post processing .....                                         | 37   |
| 2.3.2.3    LPC coefficient estimation .....                         | 37   |
| 2.3.2.4    Computation of gain .....                                | 42   |
| 2.3.2.5    The prediction error signal .....                        | 44   |
| 2.3.3    Binary Encoder.....                                        | 44   |
| 2.4    LPC DECODER.....                                             | 44   |
| 2.4.1    Binary decoder .....                                       | 44   |
| 2.4.2    Synthesis of speech from Linear Predictive parameters..... | 44   |
| 2.5    CONCLUSION.....                                              | 45   |

|                                                                                                            |           |
|------------------------------------------------------------------------------------------------------------|-----------|
| <b>CHAPTER THREE: VOCODING SECURITY SYSTEMS.....</b>                                                       | <b>47</b> |
| 3.1 CRYPTOGRAPHY .....                                                                                     | 47        |
| 3.2 SHANNON'S CIPHER SYSTEM .....                                                                          | 48        |
| 3.3 SECURITY OF CIPHER SYSTEM.....                                                                         | 50        |
| 3.3.1 <i>Theoretical security</i> .....                                                                    | 50        |
| 3.3.2 <i>Practical security</i> .....                                                                      | 52        |
| 3.4 MODERN CIPHER SYSTEM.....                                                                              | 53        |
| 3.4.1 <i>Stream Cipher System</i> .....                                                                    | 53        |
| 3.4.2 <i>Block cipher system</i> .....                                                                     | 54        |
| 3.4.3 <i>Public key system</i> .....                                                                       | 55        |
| 3.5 SECURITY PARAMETERS OF STREAM CIPHER SYSTEMS .....                                                     | 55        |
| 3.5.1 <i>Building elements of the stream cipher</i> .....                                                  | 55        |
| 3.5.2 <i>Periodicity of the stream sequence</i> .....                                                      | 62        |
| 3.5.3 <i>Randomness</i> .....                                                                              | 62        |
| 3.5.4 <i>Key levels</i> .....                                                                              | 62        |
| 3.5.5 <i>Key diversity</i> .....                                                                           | 62        |
| 3.5.6 <i>Linear complexity of the algorithm</i> .....                                                      | 63        |
| 3.6 STATISTICAL TESTS FOR LOCAL RANDOMNESS .....                                                           | 63        |
| 3.6.1 <i>Statistical tests</i> .....                                                                       | 65        |
| 3.6.1.1 <i>Chi squared ( <math>X^2</math> )test</i> .....                                                  | 65        |
| 3.6.1.2 <i>Frequency(Mono-bit) test</i> .....                                                              | 66        |
| 3.6.1.3 <i>Poker test</i> .....                                                                            | 66        |
| 3.6.1.4 <i>Serial test</i> .....                                                                           | 67        |
| 3.6.2 <i>NIST statistical tests</i> .....                                                                  | 67        |
| 3.6.2.1 <i>Serial test</i> .....                                                                           | 67        |
| 3.6.2.2 <i>Frequency test within a block</i> .....                                                         | 68        |
| 3.6.2.3 <i>Linear Complexity Test</i> .....                                                                | 68        |
| 3.6.2.4 <i>Run test</i> .....                                                                              | 69        |
| 3.6.2.5 <i>Approximate Entropy Test</i> .....                                                              | 70        |
| 3.6.2.6 <i>Cumulative Sum (Cusum) Test</i> .....                                                           | 70        |
| 3.6.2.7 <i>Discrete Fourier Transform (Spectral) Test</i> .....                                            | 70        |
| 3.6.2.8 <i>Non-overlapping (Aperiodic) Template Matching Test</i> .....                                    | 70        |
| 3.7 CONCLUSION .....                                                                                       | 70        |
| <b>CHAPTER FOUR: DESIGN AND IMPLEMENTATION OF A SECURE VOCODING SYSTEM .....</b>                           | <b>72</b> |
| 4.1 <i>Introduction</i> .....                                                                              | 72        |
| 4.2 <i>LPC 10 vocoding system</i> .....                                                                    | 74        |
| 4.2.1 <i>LPC encoder part(LPC_speechencoder )</i> .....                                                    | 74        |
| 4.2.1.1 <i>Speech signal preprocessing</i> .....                                                           | 74        |
| 4.2.1.2 <i>Speech signal framing</i> .....                                                                 | 75        |
| 4.2.1.3 <i>The gain and LPC coefficients estimation</i> .....                                              | 77        |
| 4.2.1.4 <i>Pitch estimation and voice decision</i> .....                                                   | 78        |
| 4.2.1.5 <i>Encoding function (LPC_encode)</i> .....                                                        | 79        |
| 4.2.2 <i>LPC decoder part (LPC_speechdecoder )</i> .....                                                   | 80        |
| 4.2.2.1 <i>Decoding function (LPC_decode)</i> .....                                                        | 80        |
| 4.2.2.2 <i>LPC synthesis (LPC_synthese)</i> .....                                                          | 80        |
| 4.3 <i>Nonlinear Stream cipher Algorithm</i> .....                                                         | 83        |
| 4.3.1 <i>Description of our proposed Nonlinear stream cipher</i> .....                                     | 84        |
| 4.3.2 <i>Randomness properties</i> .....                                                                   | 85        |
| 4.3.3 <i>Key sequence period</i> .....                                                                     | 85        |
| 4.3.4 <i>Key diversity</i> .....                                                                           | 86        |
| 4.4 <i>Results of the randomness tests applied to the output of the proposed secure vocoding system</i> 86 |           |
| 4.4.1 <i>Results of randomness Statistical tests</i> .....                                                 | 87        |
| 4.4.1.1 <i>Serial test</i> .....                                                                           | 87        |
| 4.4.1.2 <i>Frequency test:</i> .....                                                                       | 87        |
| 4.4.1.3 <i>Poker Test</i> .....                                                                            | 88        |
| 4.4.2 <i>Results of randomness NIST Statistical tests</i> .....                                            | 90        |
| 4.4.2.1 <i>BLOCK FREQUENCY TEST</i> .....                                                                  | 90        |
| 4.4.2.2 <i>SERIAL TEST</i> .....                                                                           | 90        |
| 4.4.2.3 <i>RUN TEST</i> .....                                                                              | 91        |
| 4.4.2.4 <i>LINEAR COMPLEXITY</i> .....                                                                     | 91        |
| 4.4.2.5 <i>APPROXIMATE ENTROPY TEST</i> .....                                                              | 91        |

|                                                |                                  |     |
|------------------------------------------------|----------------------------------|-----|
| 4.4.2.6                                        | FFT TEST .....                   | 92  |
| 4.4.2.7                                        | CUMULATIVE SUMS.....             | 92  |
| 4.4.2.8                                        | NONPERIODIC TEMPLATES TEST ..... | 93  |
| CHAPTER FIVE: CONCLUSIONS AND FUTURE WORK..... |                                  | 97  |
| 5.1                                            | <i>Conclusion</i> .....          | 97  |
| 5.2                                            | <i>Future work</i> .....         | 98  |
| APPENDIX I.....                                |                                  | 100 |
| APPENDIX II .....                              |                                  | 113 |
| APPENDIX III.....                              |                                  | 117 |
| REFERENCES .....                               |                                  | 121 |

## List of figures

|             |                                                            |    |
|-------------|------------------------------------------------------------|----|
| Figure 1.1  | Block diagram of a speech coding system .....              | 2  |
| Figure 1.2  | Diagram of human speech production system.....             | 5  |
| Figure 1.3  | Waveforms of “six plus three equals nine” .....            | 7  |
| Figure 1.4  | Discrete-time models for speech production.....            | 9  |
| Figure 1.5  | Human auditory system.....                                 | 10 |
| Figure 1.6  | Adaptive Predictive Coding .....                           | 11 |
| Figure 1.7  | Sub Band Coder.....                                        | 13 |
| Figure 1.8  | Channel Vocoder .....                                      | 15 |
| Figure 1.9  | Speech generation model of LPC .....                       | 17 |
| Figure 1.10 | Mixed Excitation Linear Prediction .....                   | 18 |
| Figure 1.11 | Code–Excited Linear prediction.....                        | 20 |
| Figure 2.1  | LPC vocoder.....                                           | 22 |
| Figure 2.2  | LPC model.....                                             | 23 |
| Figure 2.3  | Speech signal .....                                        | 26 |
| Figure 2.4  | Speech windows with and without DC shift .....             | 28 |
| Figure 2.5  | Preprocessing speech signal .....                          | 30 |
| Figure 2.6  | Spectrum of speech windows .....                           | 31 |
| Figure 2.7  | PSD of speech windows .....                                | 32 |
| Figure 2.8  | Cepstrum block diagram.....                                | 33 |
| Figure 2.9  | Cepstrum of speech windows .....                           | 33 |
| Figure 2.10 | AMDF of speech window .....                                | 35 |
| Figure 2.11 | ACF of speech window .....                                 | 36 |
| Figure 2.12 | Normalized error .....                                     | 41 |
| Figure 2.13 | Synthesis filter of LPC model .....                        | 45 |
| Figure 3.1  | Mono-alphabetic machines .....                             | 47 |
| Figure 3.2  | Shannon’s cipher system .....                              | 49 |
| Figure 3.3  | One time pad.....                                          | 51 |
| Figure 3.4  | Stream ciphers .....                                       | 53 |
| Figure 3.5  | Block cipher system .....                                  | 54 |
| Figure 3.6  | Public key systems .....                                   | 55 |
| Figure 3.7  | Fibonacci implementation of LFSR .....                     | 56 |
| Figure 3.8  | Galois implementation of LFSR.....                         | 57 |
| Figure 3.9  | Multiplexer .....                                          | 60 |
| Figure 3.10 | J K flip flop.....                                         | 61 |
| Figure 3.11 | Permuter .....                                             | 61 |
| Figure 4.1  | “LPC_speechencoder” parameters .....                       | 73 |
| Figure 4.2  | LPC encoder part “LPC_speechencoder” .....                 | 74 |
| Figure 4.3  | Speech signal waveform.....                                | 75 |
| Figure 4.4  | Non-periodic windows estimated as unvoiced .....           | 75 |
| Figure 4.5  | Some speech windows.....                                   | 76 |
| Figure 4.6  | Specifications for voiced window .....                     | 77 |
| Figure 4.7  | Specifications for unvoiced window .....                   | 78 |
| Figure 4.8  | Lists of voiced and unvoiced windows .....                 | 78 |
| Figure 4.9  | LPC decoder part “LPC_speechdecoder” .....                 | 80 |
| Figure 4.10 | Waveform of reconstructed voiced and unvoiced window ..... | 81 |
| Figure 4.11 | Generated pulse train with and without random noise .....  | 82 |
| Figure 4.12 | Reconstructed voiced window.....                           | 82 |
| Figure 4.13 | The proposed nonlinear stream cipher algorithm .....       | 83 |

## List of Tables

|                                                     |    |
|-----------------------------------------------------|----|
| Table 1-1 Speech coder classification.....          | 10 |
| Table 1-2 Sub bands of SBC.....                     | 12 |
| Table 3-1 Components of Shannon's Cipher model..... | 48 |
| Table 3-2 Primitive polynomials table.....          | 59 |
| Table 3-3 Chi square distribution table.....        | 65 |
| Table 4-1 Gain and LPC coefficients.....            | 77 |

## 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                                                             |
| $y(n)$             | $n$ th 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                                                    |
| $\alpha_k$         | 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                                         |
| $\hat{R}(i)$       | Autocorrelation coefficients of the predictive filter                |
| $f(x)$             | characteristic polynomial of LFSR                                    |
| $Lc(M)$            | Lower limit of linear complexity                                     |
| $\chi^2$           | Chi square test                                                      |

# **CHAPTER ONE**

## **Speech coders**