

hossam maghraby



شبكة المعلومات الجامعية

بسم الله الرحمن الرحيم



hossam maghraby



شبكة المعلومات الجامعية



شبكة المعلومات الجامعية التوثيق الالكتروني والميكروفيلم



hossam maghraby



شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



hossam maghraby



شبكة المعلومات الجامعية



بعض الوثائق الأصلية تالفة



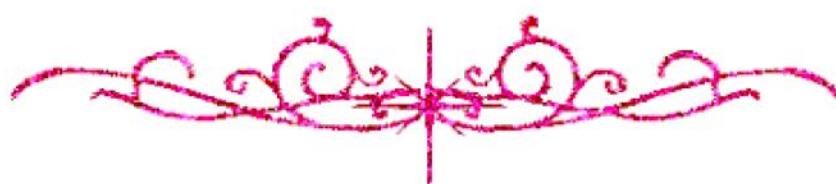
hossam maghraby



شبكة المعلومات الجامعية



**بالرسالة صفحات
لم ترد بالأصل**



ALEXANDRIA UNIVERSITY
FACULTY OF ENGINEERING

SECURITY IN SPEECH COMMUNICATION SYSTEMS

A THESIS SUBMITTED TO :

ELECTRICAL ENGINEERING DEPARTMENT

FACULTY OF ENGINEERING

UNIVERSITY OF ALEXANDRIA

B17759

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

BY

Eng. NOHA OTHMAN KORANY

SUPERVISION

Prof. Dr. ONSY A. ABDEL ALIM

ELECTRICAL DEPARTMENT

FACULTY OF ENGINEERING

ALEXANDRIA UNIVERSITY

Prof. Dr. EL-SAYED A. YOUSSEF

ELECTRICAL DEPARTMENT

FACULTY OF ENGINEERING

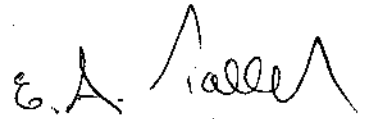
ALEXANDRIA UNIVERSITY

ALEXANDRIA , DECEMBER 1994

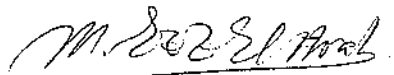
We certify that we have read this thesis and in our opinion it is fully adequate in scope and quality , as a dissertation for the degree of Master of science.

Exam Committee:

1 - Prof. Dr. EL-SAYED ABDEL HADI TALKHAN
Department of Electrical Engineering
Faculty of Engineering - Cairo university



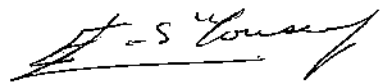
2 - Prof. Dr. MOHAMED AHMED EZZ-EL-ARAB
Department of Electrical Engineering
Faculty of Engineering - Alexandria university



3 - Prof. Dr. ONSY AHMED ABDEL ALIM
Department of Electrical Engineering
Faculty of Engineering - Alexandria university



4 - Prof. Dr. EL-SAYED AHMED YOUSSEF
Department of Electrical Engineering
Faculty of Engineering - Alexandria university



For the faculty council
Prof. Dr. ADEL LOUTFY MOHAMEDEN
Vice dean for graduate studies & research
Faculty of Engineering
Alexandria university

AKNOWLEDGMENT

After thanking God for having terminated this work , I wish to offer my deepest thanks to Prof. Dr. Onsy Abdel Alim for his true guidance , continuous encouragment and valuable support .

I would like to thank Prof. Dr. El-Sayed Youssef for his sincere advice and helpful comments .

Finally , thanks for everyone having participated in editing this work .

ABSTRACT

In recent years there has been an increased interest in cryptographic techniques due to publicity and the impact of recent technological advances such as LSI/VLSI , microprocessors and programmable signal processor chips .

In this thesis we are interested in security of voice communication . A new technique in speech encryption is proposed . This technique is based on masking the amplitudes and the locations of the vocal tract speech parameters that are estimated according to an assumed model . Two different algorithms are proposed . This technique is applied on the cepstrum as well as on the LPC coefficients .

Real speech is used to test and evaluate the performance of the proposed secure system .

CONTENTS

Abbreviations

List of symbols

Summary

Chapter one : Introduction

1.1 The speech signal	1
1.2 Developments in speech communication systems	1
1.3 Why encryption ?	2
1.4 Linear and non linear prediction	4
1.5 Purpose of the thesis	5

Chapter two : Analysis and coding of speech signals

2.1 Introduction	6
2.2 Short time speech analysis	6
2.2.1 Windowing	6
2.2.2 Spectra of windows	9
2.3 Speech analysis techniques	9
2.3.1 Time domain analysis	11
2.3.1.1 Average zero crossing rate	11
2.3.1.2 Short time average energy and magnitude	13
2.3.1.3 Short time autocorrelation function	13
2.3.2 Frequency domain parameters	16
2.3.2.1 Filter bank analysis	16
2.3.2.2 Short time fourier analysis	19

2.4	Coding techniques	19
2.4.1	Pulse Code Modulation	22
2.4.2	Adaptive Pulse Code Modulation	25
2.4.3	Differential Pulse Code Modulation	25
2.4.4	Adaptive Differential Pulse Code Modulation	26
2.4.5	Delta Modulation	27
2.4.6	Subband coders	27
2.4.7	Vector Quantization Coders	27
2.4.8	Vocoders	28
2.5	Summary	28

Chapter three : Different methods of secure speech communication

3.1	Introduction	29
3.2	Analog scramblers	29
3.2.1	Speech encryption based on scrambling in time domain	30
3.2.2	Speech encryption based on scrambling in frequency domain	31
3.3	Digital scramblers	32
3.3.1	Block ciphers	32
3.3.2	Stream ciphers	35
3.3.3	Non linear stream cipher systems	36
3.3.4	Cipher feedback	38
3.3.5	Voice security based on DES	38
3.3.6	Public key ciphers	44
3.3.7	Use of Code Division Multiple Access in speech security	46

3.4 Summary	46
-------------	----

Chapter four : Cepstral analysis and Homomorphic deconvolution of speech signals

4.1 Introduction	47
4.2 Homomorphic systems for convolution - deconvolution	47
4.3 Homomorphic filtering of speech signals	50
4.3.1 The speech model	50
4.3.2 Complex cepstrum computation	51
4.3.3 Estimation of the speech parameters	53
4.3.3.1 The vocal tract parameters estimation	58
4.3.3.2 Excitation modeling	61
4.3.3.3 Pitch estimation	61
4.4 Cepstral vocoder	61
4.5 Modified cepstral vocoder	63
4.6 Transmission techniques and bit rate calculation	65
4.7 Summary	71

Chapter five : Linear predictive coding

5.1 Introduction	72
5.2 Basic principles of linear predictive analysis	73
5.3 The autocorrelation method	78
5.4 The gain model computation	80
5.5 Solution of LPC equations using Durbin's recursive solution	82
5.6 The prediction error signal	83
5.7 LPC vocoder	88
5.8 Multipulse excited LPC vocoder	88

5.9	Transmission details for the multipulse excited LPC vocoder	98
5.10	Summary	98

Chapter six : Proposed method for speech encryption

6.1	Introduction	99
6.2	Proposed technique for speech encryption	99
6.2.1	Simple scrambling algorithm	100
6.2.2	First encryption algorithm	101
6.2.3	Second encryption algorithm	102
6.3	Application of the proposed algorithms on the cepstral coefficients	102
6.4	Application of the second encryption algorithm on the LPC coefficients	107
6.5	Proposed system additional requirements	110
6.6	Methods for evaluating the performance of the proposed secure system	110
6.6.1	Time waveform and spectrum examinations	110
6.6.2	Subjective tests	110
6.6.3	Objective measures	111
6.6.3.1	Mean squared error	111
6.6.3.2	Correlation measure	111
6.7	Summary	112

Chapter seven : Results and discussions

7.1	Introduction	113
7.2	Waveform and spectrum examinations	114
7.3	Objective tests	142

7.4	Subjective tests	146
7.5	General discussions	150

Chapter eight : Conclusions and recommendations	152
--	------------

Appendix A : Software programs

Appendix B : Waveforms and spectra of some tested words

ABBREVIATIONS

A / D	Analog to digital conversion
ADM	Adaptive delta modulation
ADPCM	Adaptive Differential pulse code modulation
APCM	Adaptive pulse code modulation
CDMA	Code division multiple access
CM	Correlation measure
DES	Data encryption standard
DFT	Discrete fourier transform
DM	Delta modulation
DPCM	Differential pulse code modulation
FFT	Fast fourier transform
FIPS	Federal information processing standard
IFFT	Inverse fast fourier transform
IV	Initial vector
LFSR	Linear feedback shift register
LPC	Linear predictive coding
LPF	Low pass filter
MSE	Mean squared error
PCM	Pulse code modulation
PSK	Phase shift keying
RKG	Running key generator
RSA	Rivest , Shamir and Adleman
SBB	Standard building block
SBC	Subband coder