

DESIGN AND IMPLEMENTATION OF A
PRESSURE BASED TYPING BIOMETRIC
AUTHENTICATION SYSTEM

BY

WASIL ELSADIG ELTAHIR

INTERNATIONAL ISLAMIC UNIVERSITY
MALAYSIA

JUNE 2005



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

DESIGN AND IMPLEMENTATION OF A
PRESSURE BASED TYPING BIOMETRIC
AUTHENTICATION SYSTEM

BY

WASIL ELSADIG ELTAHIR

A THESIS SUBMITTED IN PARTIAL
FULFILMENT OF THE REQUIREMENT FOR THE
DEGREE OF MASTER OF SCIENCE IN
MECHATRONICS ENGINEERING

KULLIYAH OF ENGINEERING
INTERNATIONAL ISLAMIC UNIVERSITY
MALAYSIA

JUNE 2005

ABSTRACT

The design and development of a pressure sensor based typing biometrics authentication system (BAS) is discussed in this thesis. The dynamic keystroke, represented by its time duration (latency) and force, generates a waveform, which when concatenated results in a pattern for the typed password. Each user types the characters that constitute the password at different speeds and with different forces applied. BAS employs special force sensors to measure the exact amount of force a user exerts while typing. The biometric authentication information acquired by the DAQ consists of an array of two columns, one for the force and the other for the time duration denoted as "latency", the combination of both information are used for the biometric analysis and identification of the user. The design of the BAS is in two stages, whereby the hardware comprising the pressure sensor and the associated data acquisition system (DAS) is first implemented, the design of DAS has been implemented with LabVIEW software where several data preprocessing techniques have been used to improve the quality of the acquired waveforms. The second stage involves the classifier used for authentication; classifiers are implemented to measure the user typing biometrics. This thesis discusses a new data classifier technique based on Autoregressive model of the keystroke signal, AR classifier has been used due to the random nature of pressure-based keystroke biometrics, the modeling algorithm has been developed using MATLAB Tool box and found to produce reliable results. An experiment has been conducted to show the validity of the overall BAS performance. As conventional biometric password authentication systems only utilize the latency information for the users, the biometric information acquired by BAS has proved to be more accurate in measuring the actual biometrics of the keystroke action.

ملخص البحث

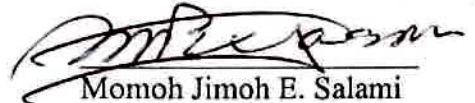
تناقش هذه الأطروحة تصميم وتطوير (BAS) وهو نظام قياسي حيوي للتحقق من هوية المستخدم عن طريق تحليل كيفية طباعته على الآلة الكاتبة (Keyboard). تختلف كيفية الطباعة من شخص لآخر من حيث الزمن وقوة الضغط على الآلة الكاتبة. يستخدم نظام (BAS) محسسات خاصة لقياس القوة والزمن المنصرم بين كل مفاتيح متتاليين من المفاتيح المستخدمة لطباعة كلمة السر. يتم قياس القوة على امتداد زمن الضغط على المفتاح مما يكسبه شكلاً أشبه بالموجة. يتم ضم هذه الموجات المكونة لكلمة السر لتكوين نموذج كلي للقوة يُقرن بهوية مستخدمه ويحفظ في قاعدة البيانات (DATABASE). يتم استخدام المصنفات التقنية للبيانات (DATA CLASSIFIERS) لمقارنة المعلومات المدخلة مع هوية المستخدم بالمعلومات الموجودة في قاعدة البيانات ومن ثم التحقق من صحة الهوية المزعومة.

للتعرف على هوية المستخدم، يستعمل نظام (BAS) مصنفاً تقنياً جديداً يعتمد على مفهوم الارتداد الذاتي (AUTOREGRESSION) ويسمى مصنف الارتداد الذاتي أي آر (AR-CLASSIFIER)، يقوم هذا المصنف بمقارنة نموذج القوة الكلي لكلمة السر المدخلة بتلك الموجودة في قاعدة البيانات والتحقق من مطابقتها لهوية المستخدم. يستعمل أيضاً مصنف آخر للزمن يقوم بمقارنة المعلومات المتعلقة بالزمن في قاعدة البيانات ويعمل سويًا مع مصنف الارتداد الذاتي للتحقق الكلي من الأسلوب القياسي الحيوي لطباعة كلمة السر.

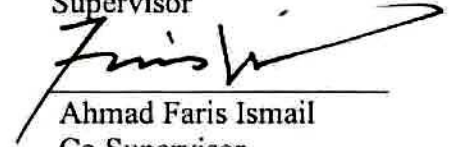
لقد تم استخدام برنامج (LabVIEW) لتصميم العتاد والربط بين عناصر نظام (BAS) المختلفة، واستعمل هذا البرنامج أيضاً للربط بين العتاد والبرمجيات المستخدمة. أما بالنسبة لمصنفات التقنية فقد تم استخدام برمجية الـ (LabVIEW) لتصميم مصنف الزمن وتم استخدام برنامج (MATLAB) لتصميم مصنف الارتداد الذاتي (AR) ومن ثم ربطه مع مصنف الزمن في (LabVIEW) عن طريق برمجية خاصة. لقد تم إجراء تجربة خاصة لاختبار أداء نظام (BAS) للتحقق القياسي الحيوي من هوية المستخدم، وقد برهنت النتائج على كفاءة هذا النظام ودقته المتناهية في قياس وتحديد هوية المستخدم من كيفية طباعته على الآلة الكاتبة.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Master of Science in Mechatronics Engineering.

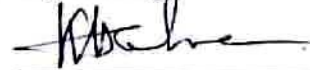


Momoh Jimoh E. Salami
Supervisor

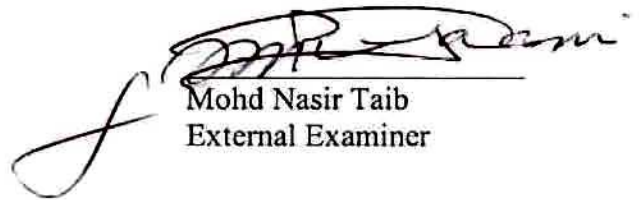


Ahmad Faris Ismail
Co Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Master of Science in Mechatronics Engineering.

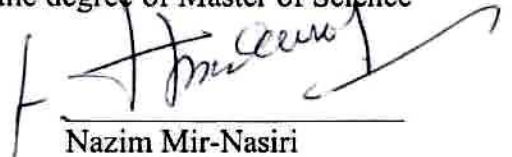


Kazi Mujibur Rahman
Internal Examiner



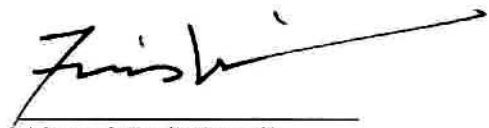
Mohd Nasir Taib
External Examiner

This thesis was submitted to the Department of Mechatronics Engineering and is accepted as partial fulfillment of the requirements for the degree of Master of Science in Mechatronics Engineering.



Nazim Mir-Nasiri
Head, Department of
Mechatronics Engineering

This thesis was submitted to the Kulliyah of Engineering and is accepted as partial fulfillment of the requirements for degree of Master of Science in Mechatronics Engineering.

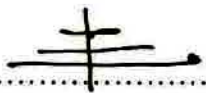


Ahmad Faris Ismail
Dean, Kulliyah of
Engineering

DECLARATION

I hereby declare that this thesis is the result of my own investigation, except otherwise stated. Other sources are acknowledged by giving explicit references and a bibliography is appended.

Name: Wasil Elsadig Eltahir

Signature: 

Date: 8-7-05

INTERNATIONAL ISLAMIC UNIVERSTY MALAYSIA

DECLARATION OF COPYRIGHTHT AND AFFIRMATION

OF USE OF UNPUBLISHED RESEARCH

Copyright © 2004 by Wasil Elsadig Eltahir. All rights are reserved.
Design and Implementation of a Pressure Based Typing Biometric Authentication System.

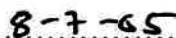
No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the copyright holder except as provided below.

1. Any material combined in or derived from this unpublished research may only be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

Affirmed by: Wasil Elsadig Eltahir



Signature



Date

PUBLICATIONS

Conference Proceedings

Wasil Elsadig, W.K.Lai, Momoh Jimoh E. Salami, and Ahmad Faris Ismail "Design, Development and Evaluation of a Pressure-based typing Biometric Authentication System" (2003), proceedings of the eight's Australian and New Zealand Intelligent Information Systems conference ANZIIS, 10-12 December 2003, Sydney AU.

Wasil Elsadig, Momoh Jimoh E. Salami, Ahmad Faris Ismail, and W.K.Lai "Dynamic Keystroke Analysis Using AR Model" (2004), Proceedings of International Conference on Industrial Technology (IEEE-ICIT04), 8-10 December 2004, Hammamet, Tunisia.

“To my beloved parents with gratitude for their inspiration, guidance, continuous support, and facilitating for me to be where I am today”

TABLE OF CONTENTS

Abstract (English)	ii
Abstract (Arabic)	iii
Approval Page	iv
Declaration	v
Publication	vi
Acknowledgements	ix
List of Tables	xiii
List of Figures	xiv
List of Acronym	xvi
CHAPTER 1: INTRODUCTION	1
1.1 Definition of Biometrics.....	1
1.2 Convenience of Typing Biometric Authentication.....	3
1.3 Bas System for Authentication.....	4
1.4 Problem Statement.....	7
1.5 Research Methodology.....	7
1.6 Thesis Outline.....	8
CHAPTER 2: REVIEW OF KEYSTROKE BIOMETRIC AUTHENTICATION SYSTEMS.....	10
2.1 Introduction	10
2.2 Keystroke Dynamics.....	11
2.3 History.....	12
2.4 Application	14
2.5 Digraph Representation of Keystroke action.....	17
2.6 Other Uses of Keystroke Dynamics.....	19
2.7 Choosing the Right Biometrics.....	20
2.8 Review of State of the Art Research on Keystroke Authentication.....	20
2.8.1 Data Collection and Experimental Methods	24
2.8.2 Clustering Methods.....	29
2.8.3 Classification Algorithms.....	31
2.8.4 Left versus Right Handedness.....	34
2.8.5 Dynamic Identity Verification.....	35
2.9 Validation of BAS Force-Latency Keystroke Verification Approach.....	36
2.10 Summary.....	39
CHAPTER 3: SIGNAL MODELING TECHNIQUES.....	42
3.1 System Definition Review	42
3.1.1 Relationship between Input and Output	43
3.1.2 Moving Average Process	45
3.1.3 Autoregressive Structure.....	46
3.1.4 Parametric Stationarity Test.....	49
3.2 Model Development.....	51
3.2.1 Yule Walker AR Model.....	55
3.2.2 Linear Prediction and Random Data Model.....	56

3.2.3	Levinson-Durbin Algorithm...	58
3.2.4	Burg Method.....	60
3.2.5	Model Order.....	61
3.2.6	Correlation Coefficients	64
3.3	Summary	67
CHAPTER 4: BAS HARDWARE COMPONENTS AND SYSTEM SETUP		68
4.1	BAS Specifications.....	68
4.2	Force Sensor and Pressure Sensitive Keyboard.....	70
4.2.1	Keystroke Action.....	70
4.2.2	FlexiForce Sensor.....	71
4.2.2.1	Advantages of FLexiForce Sensors...	73
4.2.3	FlexiForce Sensor Performance Characteristics.....	74
4.2.4	Conditioning FlexiForce Sensors	76
4.2.5	FlexiForce Sensor Calibration and Performance Testing.....	76
4.2.6	FlexiForce Sensors Arrangement on the Keyboard	81
4.3	Drive Circuit Design and Signal Filtering.....	84
4.3.1	FlexiForce Drive Circuit.....	84
4.3.2	Signal Filtering.....	86
4.4	Data Acquisition System (DAS).....	89
4.5	Summary.....	91
CHAPTER 5: COMPLETE BAS DESCRIPTION		92
5.1	Main BAS Components.....	92
5.2	Algorithm for User Authentication	94
5.3	BAS Software Design in LabVIEW.....	98
5.4	DAS Configuration and Measurements.....	100
5.4.1	Resolution.....	102
5.4.2	Device Range.....	103
5.4.3	Sampling Consideration.....	106
5.4.4	DAQ Circular Buffer.....	106
5.4.5	LabVIEW Performance with Windows Operating System.....	109
5.4.6	Moving Average Algorithm.....	112
5.5	Algorithms and Program Structures.....	114
5.6	Overall BAS Layout.....	117
5.6.1	Main Program.....	118
5.6.2	User Registration VI.....	120
5.6.3	User Validation VI.....	123
5.7	Summary.....	126
CHAPTER 6: BAS KEYSTROKE TEMPLATE ANALYSIS		128
6.1	Signal Analysis for BAS Pressure Template.....	128
6.2	Auto-Regressive Model for BAS Pressure Template.....	128
6.2.1	Signal Modeling.....	129
6.2.2	Parametric Stationarity Test	132
6.2.3	Model Order.....	135
6.3	AR-Burg User Authentication Algorithm.....	141

6.4	Latency Modeling and Classification.....	148
6.4.1	Creating Mean Reference Latency Vector.....	148
6.4.2	Calculating Suitable Threshold.....	148
6.5	Test Experiment.....	150
6.5.1	Test Results.....	152
6.5.2	Observations and Recommendations.....	154
6.6	Summary.....	155
CHAPTER 7: CONCLUSION AND RECOMMENDATIONS.....		157
7.1	Relevance of BAS Design and Implementation.....	157
7.2	Research Project Outputs.....	158
7.3	Suggestions for Future Work.....	160
BIBLIOGRAPHY		162
APPENDEX A.....		166
APPENDIX B.....		190

LIST OF TABLES

Table No.		Page
2.1	Performance test on popular commercial keystroke dynamic software.	16
2.2	Using the Euclidean distance as a similarity measure between the vectors.	32
4.1	SF-2 dimensions.	73
4.2	Typical performance of FlexiForce sensor.	77
4.3	Results of hysteresis test experiment.	80
4.4	Specifications of the FlexiForce drive circuit.	86
6.1	Best model order for each password trial.	137
6.2	Model coefficients for keystroke templates for Safiah.	140
6.3	Reference latency tested against 5 authentic user trials.	150
6.4	Effect of threshold on user acceptance rate.	150
6.5	Users' category and model orders.	152
6.6	Authentic and imposter acceptance rates.	152

LIST OF FIGURES

Figure No.		Page
2.1	Example of reference profile.	26
2.2	Clustering of user profiles based on WPM.	27
2.3	Effect of varying T with respect to the number of outliers removed from the data.	28
2.4	Vector profiles with blank features.	30
2.5	Graph of closest match to one of the more consistent typist.	34
2.6	Reference profile for a left handed user.	35
2.7	PCA for Latency alone.	37
2.8	PCA for Peak Force alone.	38
2.9	PCA for latency and Peak Force.	39
3.1	System block diagram.	42
3.2	Signals with different statistical properties.	49
3.3	NACF for the fifth trial of a user password template.	53
3.4	AR model development criteria for Safiah (4th trial) respectively from up left, Reflection coefficient, FPE, AIC, and residual error.	64
3.5	Two pressure templates for a password user.	66
3.6	Cross Correlation graph of two pressure templates for user password.	66
4.1	Rough BAS block diagram.	68
4.2	Keystroke action.	70
4.3	Typical pattern of keystroke pulse- rise time (0-10), hold time (10-15), and release time (15-35).	71
4.4	FlexiForce sensor model A201.	71
4.5	SF-2 sensor.	73
4.6	FlexiForce sensors are ultra thin and more flexible.	74
4.7	Typical response of FlexiForce sensor.	78
4.8	Experimented response of FlexiForce sensors.	79
4.9	Graph showing continuous decrease in the sensor response as we move away from the center of the sensing area.	80
4.10	FlexiForce sensors fixed on the alphanumeric keyboard.	82
4.11	Testing the sensors for alignment and calibration.	83
4.12	Pressure sensitive alphanumeric keyboard.	83
4.13	FlexiForce drive circuit diagram.	86
4.14	Aliasing effects of an improper sampling rate.	87
4.15	Acquired signal with/out filtering.	89
4.16	Flow of voltage supply and keystroke signal in DAS.	90
5.1	Complete BAS block diagram..	92
5.2	Integration of BAS components.	94
5.3	Flowchart of BAS authentication process.	98
5.4	Types of analog signals.	101
5.5	The effects of resolution on ADC precision.	103
5.6	The effects of range on ADC precision.	104
5.7	The effects of limit settings on ADC precision.	105
5.8	How a circular buffer works.	107
5.9	Keystroke pattern without moving average and interpolation.	112

5.10	Keystroke pattern with Moving average and interpolation.	113
5.11	BAS main algorithm flowchart.	116
5.12	BAS sequence structure (frame 1).	118
5.13	Mode selection window.	119
5.14	BAS Main VI hierarchy.	120
5.15	Front panel of "ID and Password VI".	121
5.16	Front panel of "User Registration VI".	122
5.17	Figure 5.17: User Registration VI hierarchy.	123
5.18	Front panel of "Get ID VI".	124
5.19	Front panel of "Validation VI".	125
5.20	User Validation VI hierarchy.	126
6.1	MATLAB script to find optimal model coefficient.	131
6.2	Segmented keystroke template.	133
6.3	MATLAB script to calculate modeling criteria.	136
6.4	Selection of Model order.	139
6.5	Plot for Predicted vs. actual templates (trial 9).	141
6.6	TSE convergence for a 2nd order AR model.	142
6.7	TSE convergence for 18th order AR model.	143
6.8	Modeling user pressure template.	144
6.9	Algorithm for authenticating the user based on linear prediction and TSE criteria.	146
6.10	MATLAB script to calculate TSE error percentage.	147
6.11	TSE % for Shareeq.	153
6.12	TSE % for Safiah.	153
6.13	TSE % for Salwani.	154
7.1	Customizable FlexiForce Sensor.	161

LIST OF ACRONYM

ACF	Autocorrelation Function
AD	Analog-to-Digital
ADC	Analog to Digital Converter
AIC	Aikake's Information Criteria
AR	Auto Regressive
ARMA	Auto Regressive Moving Average
BAS	Biometric Authentication System
CPU	Central Processing Unit
DAS	Data Acquisition System
DAQ	Data Acquisition System
FAR	False Acceptance Rate
FEA	Finite Element Analysis
FIFO	First In First Out
FPE	Final Prediction Error
FRR	False Rejection Rate
GPB	General Purpose Interface Bus
ID	Identify or Check Identity
LPC	Linear Prediction Coefficient
MA	Moving Average
MIO	Multi Input/Output
NACF	Normalized Autocorrelation Function
PCA	Principal Component Analysis
PCI	Peripheral Component Interconnect

RAM	Random Access Memory
RS	Recommended Standard
RF	Reference Resistance
SSH	Strongly Encrypted Secure Shell
TSE	Total Squared Error
VI	Virtual Instrument
WPM	Word Per Minute

CHAPTER 1

INTRODUCTION

1.1 Definition of Biometrics

The term "Biometrics" has been used to refer to the emerging field of technology devoted to the identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints and face recognition. In the strictest sense, biometrics refers to the application of a statistical analysis of biological data and phenomena. The security community, however, widely uses the term to describe technologies for personal identity verification.

Typing biometrics is the analysis of a user's keystroke patterns. Each user has a unique way of typing on keyboard when entering a password; for example, each user types the characters that constitute the password at different speeds.

Authentication techniques fall into three main categories. The first requires that the user possesses an object, for example, smart cards and magnetic-strip cards. The second entails that the user supplies specific information or answers certain questions, the normal passwords like PIN "Personal Identification Number" fall under this category. The third requires that the authentication device measures physical characteristic of the person being verified. These techniques include biometrical mechanisms such as face recognition, fingerprints, voiceprints, retina scans, keystroke patterns, and signatures.

Biometric devices fall into two categories: those that use physical characteristics, such as fingerprints and hand geometry, and those that use behavioral characteristics, such as signature dynamics and keystroke dynamics.

All authentication devices share the principal goal of preventing the two main types of errors:

Type I: Failing to correctly identify a legitimate user.

Type II: Allowing access to an intruder.

Also, they all aim to avoid placing any extra burden on the users and provide authentication at a reasonable cost. Each category has strengths and weaknesses. Authentication devices that require possession of an object provide a high level of security. However, they are susceptible to loss or theft; for example, magnetic-strip cards can be copied relatively cheaply.

Authentication devices that require users to supply specific information are the cheapest and the most widely used. However, they are extremely vulnerable to trial-and-error attacks, because users normally have difficulty choosing passwords that are memorable but difficult to guess. For example, the infamous Internet worm of 1989 (Eugene H 1989) used a wide-spread password dictionary to compromise the security of many network sites.

Because devices that measure a physical characteristic, that is, biometric techniques use authentication information that cannot be forgotten or stolen, they seem to provide a very attractive solution. However, their inability to eliminate Type I and Type II

Typing biometrics involves the analysis of users' dynamic keystroke patterns. There are many techniques used to treat, analyze and associate users with their distinct typing biometrics, such techniques are called classifiers. In this thesis a new algorithm is suggested based on AR-Signal modeling of users' pressure templates.

The biometric reinforcement in BAS is transparent and indiscernible to the users while they are entering the normal authentication information (user ID and password); this methodology helps prevent the two main types of authentication errors: not giving access to legitimate users and giving access to impostors (W. G. de Ru et al. 1993, 1997; D.L. Jobusch 1989).

1.3 BAS System for Authentication

The hardware setup of a Biometric Keystroke Authentication System (BAS) is discussed in the fourth chapter; the development of BAS required careful study to the dynamics of keystroke typing so as to identify the important parameters that constitute a convenient pattern or dynamic keystroke for users. These parameters are identified as the following:

- 1) The time interval between successive keystroke actions (keystroke latency).
- 2) The amount of force he exerts on each keystroke (F).

The application of force (F) over duration of time (Δt) constitutes a pattern which can be recognized as the typing-template for a sequence of keys pressed.

In our system design, when a new user requests to register a new ID and password to the computer system, or when an existing user's password is to expire, the access-

control system asks the user to type in the user ID and a new password. The system then asks the user to reenter the password several times (10-20) to train his password and improve his keystroke pattern; each trial is saved to a file in the database.

Each new user has an individual folder in database which includes his ID, password and keystroke templates for all the trials he attempted. The system administrator uses these information to compute a typing template for user authentication.

The typing template (keystroke template/pattern) consists of model for pressure template and the keystroke latencies facilitating the use of two keystroke verifiers.

Using two keystroke verifiers enhance the effectiveness of BAS authentication. Two classifiers are modeled for each biometric verifier (force-latency).

On subsequent attempts to access the system, the user goes through the normal password-authentication procedure that is, entering the user ID and the password. The BAS system creates the keystroke pattern based on the user ID and password that has just been entered; it then compares this keystroke pattern with the pattern saved in database for that user. If the password and typing template match those in the system's database, the system grants access to the user.

If the password does not match, the normal password-authentication mechanism will reject the user or ask the user to reenter the password again. If the password does match, the biometrics component will provide a supporting recommendation which verifies that the user is legitimate. If the user ID and password are correct, but the new

typing template does not match the reference template, the security system has several options which can be devised according to the specific use of the system. A typical scenario might be that the BAS advises a security or network administrator that the typing pattern for a user ID and password is not what the system expected it to be and that a security breach might be possible. The security administrator then closely monitors the session to ensure that the user does nothing he or she is not authorized to do.

Another typical situation can occur with users of Automatic Teller Machines (ATM); if the user's pattern doesn't match with the reference template in the database, a restriction can be placed on the amount of money he can withdraw on that occasion.

Some important features of the system hardware were considered in the design and implementation of BAS, these features are:

1. Hardware setup should be compact and should avoid being overly sophistication and bulky.
2. All external hardware should be powered up from the CPU unit and no external power sources should be used.

The hardware components used to construct BAS were the following: Alphanumeric keyboard embedded with Force sensors to measure the pressure while typing, Data Acquisition System (DAS) which includes the Sensor Drive circuit (amplification of signal and filtering), DAQ hardware which includes PCI card and BNC connector for system integration with PC.

1.4 Problem Statement

The design problem of this research work was to develop a biometric authentication system (BAS) with the following main components:

1. Pressure-based electronic keyboard.
2. Encoder for the keyboard (running on Windows).
3. (Pressure) data capture system.
4. Classifier module to correctly classify the data.
5. User interface.

The complete BAS should recognize a user based on typing characteristics.

Measurable characteristics include:

1. Time between keystrokes (latency)
2. Amount of pressure on each key.

1.5 Research Methodology

In achieving the objectives of this research, the following procedures are considered:

1. Design and development of alphanumeric electronic keyboard with additional pressure sensors. Force sensors were used to measure the amount of force applied when typing, the sensors selected for this task were FLexiForce sensors. These sensors are fixed underneath selected keys on the alphanumeric keyboard.
2. Design and development of a data capture module. The data capture module was designed with LabVIEW to integrate both hardware and software platforms of BAS. When compared with other system integration software,

LabVIEW facilitates professional system development with high-end and sophisticated instrumentation. It provides seamless integration with measurement hardware to facilitate rapid data acquisition and analysis, instrument control, and data presentation.

3. Research and development of a suitable DATA classifier. A new data classification methodology using AR-Burg modeling approach was developed. The algorithms were developed in MATLAB, the classifier was written in LabVIEW using the MATLAB script node function.
4. Graphical user interface (GUI) design and development. System GUI was developed in parallel with the software platform of BAS.
5. Overall System integration.
6. Overall System testing. Test the performance of BAS from both hardware and software aspects. Also tested was the AR-Burg data classifier.

1.6 Thesis Outline

This thesis consists of seven chapters; the following points give a brief description of their contents:

1. In Chapter two a review of current typing-biometric systems is discussed and contrasted to the newly developed BAS system.
2. Chapter three discusses the AR-Burg methodology for data classification and authentication. The chapter briefly explains the theory of stochastic signal modeling using the AR “auto-regressive” technique.