SIGNATURE VERIFICATION SYSTEM BASED ON MULTIPLE CLASSIFIERS AND MULTI FUSION DECISION APPROACH

HAMAM M.IBRAHIM MOKAYED

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JANUARY 2010

To my lovely wife…
To my parents…

ACKNOWLEDGEMENTS

First, I thank my supervisor Prof Dr. Marzuki, for his continuous support in the master program. He is responsible for involving me in the Multimodal Biometric system in the first place. He taught me how to approach a research problem, his insightful critics and guidance have taught me to work persistently to accomplish my goal. I also thank Prof. Dr. Rubiyah Yusof, who as my second supervisor for her enthusiasm and critics that bring life and motivation in my study. Without their encouragement and constant support, I could not have finished this thesis.

Special thanks go to all CAIRO staff for working together. They have kept me in good spirits throughout my study and they let feel as I still live in my country. Thanks, CAIRO! Especially my friends, Fairol and Ridzwan, for their friendship, supporting to me in the programming side and I am sorry because I knew that I disturb them a lot.

During the course of this work, I was supported by in part by research grants from Universiti Teknologi Malaysia and funding from CAIRO Center.

Last, but not least, I like to thank my lovely wife (Lama) for her patience and for her unconditional support to pursue my interests. Also I thank my parents (Maher and Ahlam), for giving me life in the first place, for educating me, and for their supports throughout my study. Also I thank my wife's parents (Shouki and Maha) for their unlimited supporting and encouraging me, they have indirectly influenced me that my research should always be useful and serve good purposes for all humankind.

ABSTRACT

With an increase in identity fraud and the emphasis on security, there is growing and urgent need to verify human identify efficiently. Signature and the handwriting verification application are used in many fields such as banking, public sectors. Documents and cheques verification system has triggered a real need for reliable, accurate and robust system. This work adopts different classification techniques between the local features based and the global features based of the signature system in addition to different fusion techniques between the outputs of the different classifiers and global features based to improve error rate of behavioral system. Main goal is to develop more accurate and robust signature verification system than the previous developed system with False Rejection Rate (FRR) equals to 5.3 and False Acceptance Rate (FAR) equals to 0. To achieve this goal, first multiple classification techniques are applied to the signature verification system which are artificial neural network, support vector machine and Pearson correlation and then these techniques are fused by applying two complicated fusion techniques which are fuzzy logic and sequential fuzzy logic and one simple fusion technique which is max voting. Lastly the rule-based decision is applied to specify whether the signature is genuine or not. Second, the improved signature verification system is extended with the high performance Hitachi system. This biometric based system can be realized in many real world and web based applications where there is a need for higher security and robust identification.

ABSTRAK

Dengan peningkatan pemalsuan identiti dan pencerobohan sistem keselamatan, masyarakat kini amat memerlukan sistem yang lebih efektif untuk mengenalpasti identiti manusia. Kewujudan sistem pengecaman tandatangan dan tulisan di kebanyakan sektor seperti perbankan, sektor awam. Dokumen dan pengesahan cek telah mencetuskan kepentingan dalam membentuk suatu sistem yang lebih dipercayai, tepat dan teguh. Kerja ini mengadaptasi teknik pengelasan yang berbeza di antara sistem tandatangan yang berasaskan sifat lokal dan sifat global sebagai tambahan kepada beberapa teknik lakuran diantara hasil pengelas yang berbeza dan sifat global untuk menambahbaik kadar ralat sistem perlakuan. Matlamat utama adalah untuk membina sistem pengesahan tandatangan yang lebih tepat dan teguh berbanding sistem terdahulu yang dibangunkan oleh dengan FRR bersamaaan 5.3 dan FAR bersamaan 0. Untuk mencapai matlamat ini, pertama, beberapa teknik pengelasan digunakan untuk sistem pengesahan tandatangan antaranya ialah rangkaian neural buatan, mesin vektor buatan dan korelasi Pearson. Kemudian, hasil dari pengelasan ini digabungkan dengan menggunakan dua penggabungan teknik yang rumit iaitu logik kabur dan logik kabur berjujukan serta satu penggabungan teknik yang mudah iaitu undian maksimum. Di akhir proses, keaslian tandatangan tersebut ditentukan berdasarkan peraturan tertentu. Kemudian, sistem pengesahan tandatangan yang ditambahbaik itu digabungkan dengan sistem Hitachi yang berprestasi tinggi. Sistem berasaskan biometrik ini boleh diwujudkan dalam banyak dunia nyata dan aplikasi berasaskan web di mana ada keperluan untuk keselamatan yang lebih tinggi dan kuat pengenalan..

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvii
1	**INTRODUCTION**	1
	1.1. Background	1
	1.2. Motivation for Research	5
	1.2.1. Problems of Signature Verification	5
	1.2.2. Problems of Finger Vein Verification	5
	1.3. Scopes and Objectives	6
	1.4. Research Methodology Adopted	7
	1.4.1 General Methodology	7
	1.4.2 New Methodology Proposed	8
	1.5. Contribution of Thesis	10
	1.6. Outline of this thesis Layout	10

2 LITERATURE REVIEW 12

2.1. Introduction 12
2.2. Data Acquisition Devices 13
2.2.1. Tablet-Based Data Acquisition 13
2.2.1.1 Passive Digitizer Technology 14
2.2.1.2. Active Digitizer Technology 14
2.2.1.3. Tablet Digitized Technology 16
2.3. Signature Verification System 17
2.3.1. Feature Extraction 17
2.3.2. Verification Methods 19
2.4. Multiple Classification Methods 21
2.4.1. Support Vector Machine Classifier (SVM) 21
2.4.1.1. Support Vector Machine's Concepts 22
2.4.1.2. Basic Architecture and Algorithm 22
2.4.1.3. Types of SVM 23
2.4.1.4. Classification by SVM 25
2.4.1.5. Applications of SVM 29
2.4.2 Artificial Neural Network (ANN) Classifier 30
2.4.2.1. Basic Concept of ANN 30
2.4.2.2. Classification of ANN 31
2.4.2.3. Multilayer Perceptron and the Back Propagation Algorithm 31
2.4.2.4. Applications of ANN 36
2.4.3. Pearson Correlation Classifier 36
2.4.3.1. Classification of Pearson Correlation 37
2.5. Multiple Fusion Techniques 38
2.5.1. Majority Voting Fusion 40
2.5.2. Fuzzy Logic 41
2.6. Applications of Proposed System 43
2.7. Summary 43

3 PROPOSED SIGNATURE VERIFICATION SYSTEM 44

3.1. Introduction 44

3.2. Online Signature Verification System 44
3.2.1. Data Acquisition Module 46
3.2.2. Pre-Processing Module 46
3.2.2.1. Normalization Size 46
3.2.2.2. Re-Sampling 47
3.2.3. Validation Module 51
3.2.4. Feature Extraction Module 55
3.2.4.1. Local Features 56
3.2.4.2. Global Features 58
3.2.5. Classifier Module 58
3.2.5.1. Artificial Neural Network Module 58
3.2.5.2. Support Vector Machine Module 61
3.2.5.3. Pearson Correlation Module 67
3.2.5.4. Thresholds Classifier Module 69
3.2.6. Final Decision Module 70
3.2.6.1. Max (Majority) Voting 70
3.2.6.2. Sequential Fuzzy Logic Decision Module 73
3.2.6.3. Fuzzy logic Decision Module 78
3.2.7. Final Result for the Signature Verification System 86
3.3. Summary 86

4 EXPERIMENTAL RESULTS AND DISCUSSION 88
4.1. Introduction 88
4.2. Online Signature Verification system 88
4.2.1. Signature Databases 89
4.2.2. Experimental Results to Specify the Best Threshold Value of ANN 90
4.2.3. Experimental Results to Specify the Best Threshold Values of the Global Features 94
4.2.4. Experimental Results to Specify the Best Threshold Value of the Pearson Correlation Classifier 99
4.2.5. Experimental Results Based on Local Features Using Neural Network, SVM and Pearson Classifiers 103
4.2.6. Experimental Results for the Proposed Signature 108

Verification System
4.2.7. Difficulties Encountered 113
4.2.8 Comparison of the Proposed Signature Verification System 114

5 MULTIMODAL BIOMETRIC SYSTEM 115

5.1 Introduction 115
5.2 Finger Vein Verification System 115
5.2.1. Data Acquisition Module 116
5.2.1.1. Finger Vein Biometric Scanner 116
5.2.1.2. Finger Vein pattern Imagining 117
5.2.2. Pre-Processing Module 120
5.2.3. Feature Extraction Module 120
5.2.3.1. Extraction of the Center Position of the Vein 122
5.2.3.2. Connection of the Vein Centers 124
5.2.3.3. Labeling the Image 125
5.2.4. Matching Module 126
5.3 Multimodal Biometric System 128
5.3.1 Various Level of Fusions 129
5.3.2 Types of Fusion 130
5.3.3 Extension System to the Proposed Biometric System 131

6 CONCLUSIONS 133

6.1 Introduction 133
6.2 Summary of Contribution 134
6.3 Recommendation 134

REFERENCES 137

Appendices A-C 148 – 166

LIST OF TABLES

TABLE NO.	TITLE	PAGE
3.1	Analysis of correlation coefficient of five signatures	53
3.2	Analysis value of correlation coefficient of five signature as reference	55
3.3	Values excluded from the five references signatures	72
3.4	Max voting decision result for some genuine and forged signatures	73
3.5	Fuzzy rules for the first fuzzy logic between length and time	76
3.6	Fuzzy rules for the second fuzzy logic between the output of the first fuzzy logic and ANN	76
3.7	Sequential fuzzy logic decision result for some genuine and forged signatures	78
3.8	Fuzzy rules for the first fuzzy logic between length and time	82
3.9	Fuzzy rules for the second fuzzy logic between the output of ANN and the length	82
3.10	Fuzzy rules for the third fuzzy logic between the output of ANN and the time	83
3.11	Fuzzy rules for the third fuzzy logic between the output of ANN and the output of Pearson Correlation	83
3.12	Sequential fuzzy logic decision result for some genuine and forged signatures	85

4.1	Training and testing of the online signature data sets	90
4.2	Verification results of genuine signature with different thresholds of the ANN classifier	91
4.3	Verification results of simple forgery signature with different thresholds of the ANN classifier	92
4.4	Verification results of professional forgery signature with different thresholds of the ANN classifier	93
4.5	Verification results of genuine signature with different parameters of the threshold classifier	96
4.6	Verification results of simple forgery signature with different parameters of the threshold classifier	97
4.7	Verification results of professional forgery signature with different parameters of the threshold classifier	98
4.8	Verification results of genuine signature with different thresholds of the Pearson classifier	100
4.9	Verification results of simple forgery signature with different thresholds of the Pearson classifier	101
4.10	Verification results of professional forgery signature with different thresholds of the Pearson classifier	102
4.11	Verification results of genuine signature with different classifiers techniques	104
4.12	Verification results of professional forgery signature with different classifiers techniques	105
4.13	Verification results of simple forgery signature with different classifiers techniques	106
4.14	Verification results of genuine signatures	110
4.15	Verification results of professional forgery signatures	111
4.16	Verification results of simple forgery signature with different fusion techniques	112
4.17	Comparison of the error for the proposed signature verification system and Fadlil's system	114

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Zypher analysis for different Biometric system (International Biometric Group)	3
1.2	Signature verification systems using different classification methods	7
1.3	Signature verification and finger vein biometric systems	8
1.4	Proposed signature verification system	9
2.1	SVM basic architecture and algorithm	22
2.2	Clusters of vectors separated by hyperplane	23
2.3	Linearly separable cases	24
2.4	Non-Linearly separable cases	24
2.5	Non-Separable / imperfect separation case	25
2.6	Canonical hyperplane	27
2.7	Generalized optimal separating hyperplane	28
2.8	Architecture of multi layer perceptron with one hidden layer	32

3.1	A block diagram of the proposed online signature verification system	45
3.2	Example of normalization size signature's size	47
3.3	Illustration of the interpolation technique	49
3.4	Processing of re-sampling the distance	50
3.5	Illustration of the re-sampling time process	51
3.6	Flow-chart of the enrolment procedure	52
3.7	Sequence data of five signatures as candidate reference before applying the validation process.	54
3.8	Sequence data of five signatures as candidate reference after applying the validation process.	54
3.9	Illustration of direction X features	56
3.10	Angles extracted based on strokes	58
3.11	A flow chart of the ANN training phase	60
3.12	A flow chart of the ANN testing phase	61
3.13	Mapping from 2-dimensional to 3-dimensional space	62
3.14	"Kernelizing" the optimal margin hyperplane	63
3.15	Flow chart of the SVM training phase	65
3.16	Input space with constructed hyperplane.	66
3.17	A flow chart of the SVM testing phase	67

3.18	Flow chart of the Pearson correlation testing phase	68
3.19	Flow chart of the thresholds classifier module	69
3.20	The five signature references	71
3.21	An example for some genuine and forged signatures	73
3.22.a	ANN membership function of the sequential fuzzy module	74
3.22.b	Length membership function of the sequential fuzzy module	75
3.22.c	Time membership function of the sequential fuzzy module	75
3.23.a	Membership Function of the first fuzzy module.	75
3.23.b	Membership Function of the second fuzzy module	76
3.24	An example for some genuine and forged signatures evaluated by sequential fuzzy logic module	77
3.25.a	ANN membership function of the fuzzy module	79
3.25.b	Length membership function of the fuzzy module	80
3.25.c	Time membership function of the fuzzy module	80
3.25.d	Pearson membership function of the fuzzy module	80
3.26.a	Membership Function of the first fuzzy module	81
3.26.b	Membership Function of the second, third and forth fuzzy modules	81
3.27	An example for some genuine and forged signatures evaluated by sequential fuzzy logic module	84

4.1	One sample of the three collected signatures	90
4.2	Diagram of the threshold adjustment of Th.3	94
4.3	Diagram of the threshold adjustment of Th.4	94
4.4	Diagram of the threshold adjustment of P_Th	94
4.5	The FAR, FRR for the three different classifiers	107
4.6	Verification results for the individual systems and the whole system	113
5.1	Hitachi's finger vein verification system	116
5.2	Different finger vein pattern imaging techniques	118
5.3	Side lighting method applied by Hitachi's company	119
5.4	Cross-sectional profile of veins	122
5.5	Relationships among profile, curvature and probability score of veins	124
5.6	Results of vein extraction	126
5.7	Three levels of fusions	129
5.8	Proposed Multimodal biometric system	132
6.1	The grid features vector of signature	135

LIST OF ABBREVIATIONS

ATM	-	Automatic Teller Machine
AI	-	Artificial Intelligence
AMR	-	Arithmetic Mean Rule
ANN	-	Artificial Neural Network
API	-	Application Programming Interface
ASCII	-	American Standard Code for Information Interchange
BPNN	-	Back propagation NN
CAIRO	-	Center of Artificial Intelligence and Robotics
DCT	-	Discrete Cosine Transform
EER	-	Equal error rate
ERM	-	Empirical Risk Minimization
FAR	-	False acceptance rate
FL	-	Fuzzy Logic
FOSM	-	Fuzzy Ordinal Structure Module
FRR	-	False rejection rate
GE	-	Genuine
GR	-	Genuine with Risk
HMM	-	Hidden Markov Model
HR	-	High Risk
HSV	-	Handwritten Signature Verification
IDE	-	Integrated development environment
IEEE	-	Institute of Electrical and Electronic Engineers
IM	-	Imposter
IMRG	-	International Media and Retail Group
INNS	-	International Neural Network Society
IR	-	Infra red
ISO	-	International Standard Organization
LCD	-	Liquid Crystal Display
LDA	-	Linear discriminate analysis
LED	-	Light-Emitting Diode
LPD	-	Linear Programming Descriptor
LR	-	Low Risk

LVQ	-	Learning Vector Quantization
MI	-	Maybe Imposter
MLP	-	Multi Layer Perceptron
NN	-	Neural Network
PC	-	Personal computer
PCA	-	Principal component analysis
PDA	-	Personal digital assistant
PIN	-	Personal Identification Number
PIN	-	Personal Identification Number
RAM	-	Random access memory
RF	-	Radio Frequency
SDK	-	Software Development Kit
SOM	-	Self Organizing Map
SRAM	-	Static RAM
SRM	-	Structural Risk Minimization
SV	-	Support Vector
SVM	-	Support vector machines
TH	-	Threshold
USB	-	Universal Serial Bus
VLSI	-	Very large scale integration
VPR	-	Vascular Pattern Recognition
WT	-	Wavelet Transform

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	1. An example of genuine signatures	150
	2. An example of a simple forgery signatures	154
	3. An example of professional forgery signatures	158
	4. An example of a typical SIGNATURE set	162
B	Fuzzy Logic System Code	164
C	Publications	168

CHAPTER 1

INTRODUCTION

1.1 Background

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. Thus, biometrics can be defined as the science and technology of measuring and statistically analyzing biological data. Physiological characteristics are based on measurements of data derived from direct measurement of a part of the human body. Fingerprints, hand geometry, and retina, iris, and facial images are leading physiological biometrics. Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements of data derived from an action, and indirectly measure characteristics of the human body. Signatures, voice recordings (which also has a physiological component), and keystroke rhythms are leading behavioral biometric technologies, the terms "Biometrics" and "Biometry" have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Recently, these terms have also been used to refer to the emerging field of information technology devoted to automated identification of individuals using biological traits especially for authentication purposes. (www.ewh.ieee.org , 2007).

Biometrics is nowadays an important area receiving continuously growing interest. The increasing needs for security make biometrics more and more valuable world-wide,

and this method of identification is preferred over traditional methods involving passwords and PIN (Personal Identification Number) for various reasons:

- The person to be identified is required to be physically present at the point-of-identification.
- Identification based on biometric techniques obviates the need to remember a password or carry a token.

By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs (Automatic Teller Machine**)**, cellular phones, smart cards, desktop PCs (Personal Computer), workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Due to these, biometric based systems of identification are receiving considerable interest. Various types of biometric systems are being used for real-time identification, for example, applying the finger print and finger vein techniques in laptops to log into the operating system rather than using passwords.

Any of these biometric measurements can positively identify a person from among hundreds of others. However, biometric measurements are inherently varied because of the existence of background noise, signal distortion, biometric feature changes, and environment variations. For instance, facial biometrics can vary with changes in facial expressions and ambient light, and fingerprint biometrics can vary with press pressure and moisture. As a result, recognition based on a single biometric trait may not be sufficiently robust and has a limited ability to overcome spoofing. If one specifically defines an application, it may be possible to describe the most accurate, easiest to use, easiest to deploy, or cheapest biometric for that particular deployment, but no one biometric technology has a set of criteria which is right for all situations (Dahel, S.K.; Xiao, Q, 2003).

The following Zephyr chart as shown in Figure 1.1 is a general comparison of biometric technologies in terms of ease-of-use, cost, accuracy, and perceived intrusiveness. Symbols represent the relative capabilities of each technology; a perfect

biometric system would have all symbols at the periphery, while a poor biometric system would have symbols near the center of the Zephyr chart.

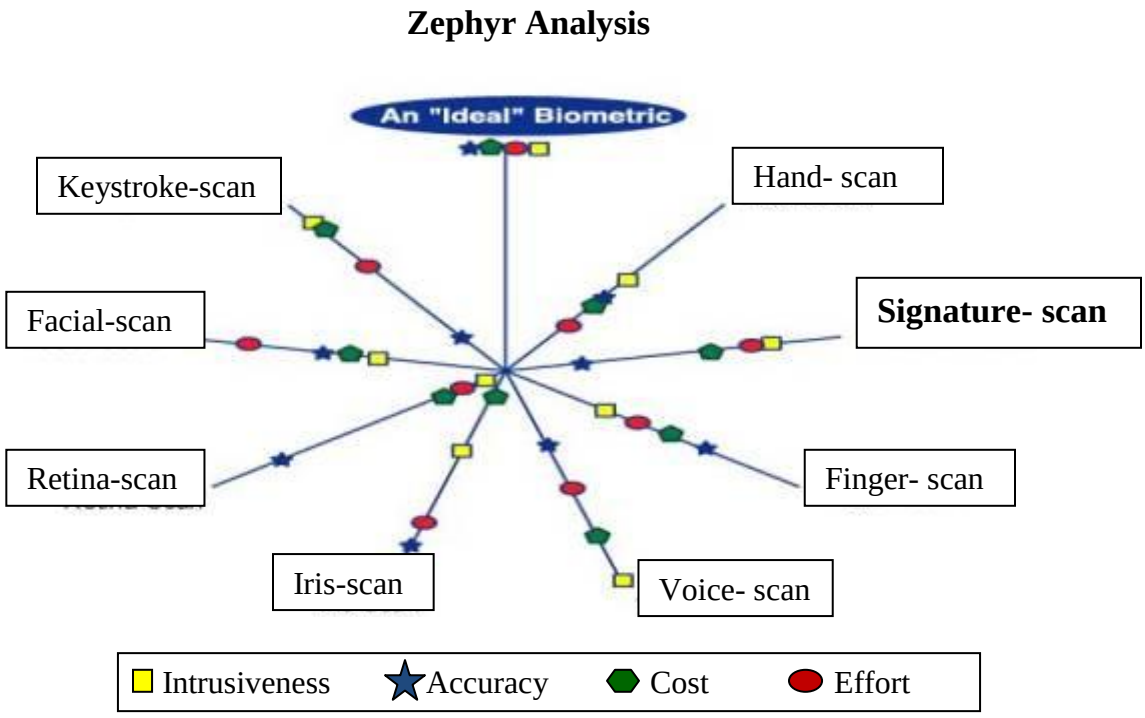

Figure 1.1 Zephyr analyses for different Biometric systems (International Biometric Group).

In order for the biometrics to be ultra-secure such that to solve the previous mentioned problems and to provide more-than-average accuracy, more than one forms of biometric identification is required. Hence, the need arises for the use of multimodal biometrics. This uses a combination of different biometric recognition technologies. Many researchers have proposed multimodal biometric fusion as a solution to this problem.

Multimodal biometric technology uses more than one biometric identifier to compare the identity of the person. Therefore, in the case of a system using say three technologies i.e. face, signature and finger vein, this multimodal biometric identifier can retain high threshold recognition settings. The system administrator can then decide the level of security that is required. For high security, they might require all three biometric identifiers to recognize the person but for a lower security site, only one or two of the

three. With this methodology, the probability of accepting an impostor is greatly reduced. Even if one of the technologies is unable to identify, the system can still use the other to accurately identify the person. Multimodal technologies have been in use commercially since 1998 (Biometric News Portal).

In the previous developed signature verification system by Fadlil 2006 at CAIRO center, a False Rejection Rate (FAR) equals to 5.3 and False Acceptance Rate (FAR) equals to 0. In this research, the focus is to replace the previous mentioned system which is not able to meet the desired performance requirement with more robust signature verification system.

Many research works are on signature verification, finger vein, multimodal biometrics can be summarized as follows:

- Offline signature verification (See and Seng, 1993; Drouhard, *et al.*, 1996; Sabourin, *et al.*, 1997; Mizukmi, *et al.*, 1999; Justino, *et al.*, 2000; Baltzakis and Papamarkos, 2001; Quek and Zhou, 2002; Fang, *et al.*, 2002; Srihari, *et al.*, 2004; Hanmandlu, *et al.*, 2005).
- Online signature verification (Mohankrishnan, *et al.*, 1993; Nalwa, 1997; Dolfing, *et al.*, 1998; Lejtman and George, 2001; Ohishi, *et al.*, 2001 ; Tanabe, *et al.*, 2001; Jain, *et al.*, 2002; Silva and Freitas, 2002; Keit, *et al.*, 2002; Yoon, *et al.*, 2002; Muramatsu and Matsumoto, 2003; Qu, *et al.*, 2003; Li, *et al.*, 2003; Shafiei and Rabiee, 2003; Zou, *et al.*, 2003; F.R.Rioja, *et al.*, 2004 ; Abdul Fadlil and Marzuki, *et al.*, 2004.a ; José Vélez *et al.*, 2008 ; Loris Nanni, *et al.*, 2008).
- Finger vein verification (Zhong Bo Zhang *et al.*, 2006 ; J. Hashimoto *2006* ; Jian-Da Wu and Siou-Huan Ye 2008 ; Lingyu Wang *et al*,. 2008 ; Mulyono, D.Horng Shi Jinn 2008).
- Multimodal biometric system (Andrew L. Rukhin, Igor Malioutov 2005, Anil Jain, Karthik Nandakumar et al 2005, Oleg Ushmaev and Sergey Novikov, 2006 ; Antonia Azzini, Stefania Marrara et al, 2007).

1.2 Motivation for Research

1.2.1 Problems of Signature Verification

Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign in a consistent manner may have difficulty enrolling and verifying their signatures verification. During enrolment subjects must provide a series of signatures that are similar enough such that the system can locate a large percentage of the common characteristics between the enrolment signatures. During verification enough characteristics must remain constant to determine with confidence that the authorized person signed. As a result, individuals with muscular illnesses and people who sometimes sign with only their initials might result in a higher False Rejection Rate (FRR), which measures the likelihood that a system will incorrectly reject an authorized user. Since many users are unaccustomed to signing on a tablet, some digital signatures may differ to their signatures on ink and paper thus increasing the potential for false rejection.

1.2.2 Problems of Finger Vein Verification

Finger Vein verification is designed to verify individuals depending on vascular pattern recognition (VPR) characteristic which provides the ease of use of hand geometry with much improved accuracy, smaller readers and contact less use. In addition to this characteristic solves the problems of inconsistency and habituation that already found in the signature verification but also faced other problems such as, angle and location of the placement on the finger vein device.

1.3 Scopes and Objectives

The scope of this thesis is to enhance the performance of the Online Signature Verification system which is related to inconsistencies in human behavior, by applying a robust validation module in which more consistent sets of signatures are enrolled. In this way, more consistent sets of training patterns are used to train the neural network modules based on the popular back-propagation algorithm and also these patterns are used to train the SVM (Support Vector Machine). Three fusion techniques are applied to fuse the scores of the different thresholds, the first technique applied two fuzzy logic modules sequentially, the second fusion technique implemented four fuzzy logic modules for the time, length, neural network and Pearson correlation then give the result after comparing it with the average threshold, the last technique is max voting fusion module.

The objectives of this thesis can be summarized as follows:

- To investigate various features of signature that is able to discriminate classes during recognition and verification processes.
- To investigate user-independent training and deciding methods where the same technique is used for all the users' samples.
- To investigate classifiers and fusing approaches for combining their results in order to improve verification rate of the system.
- To develop a software development kit (SDK) and to prototype software application for an implementation of the modified approaches of the signature and finger vein verification systems.

1.4 Research Methodology Adopted

1.4.1 General Methodology

In general, the verification system falls into two broad categories according to the biometric technology which is applied. One is the online signature verification system and the other is the finger vein system. Even for the signature verification system, the system splits into separate systems depending on the classification method. Figure 1.2 shows the three separated signature verification systems each one of them using different classification methods while Figure 1.3 shows the two biometric systems signature verification and finger vein.

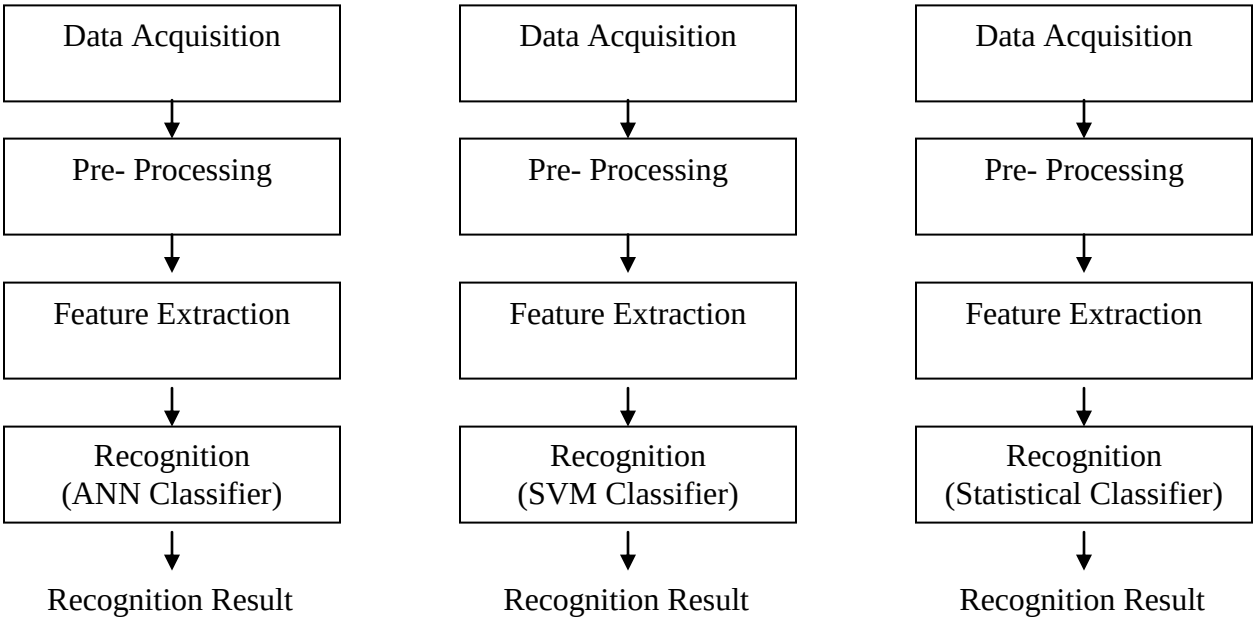

Figure 1.2 Signature verification systems using different classification methods

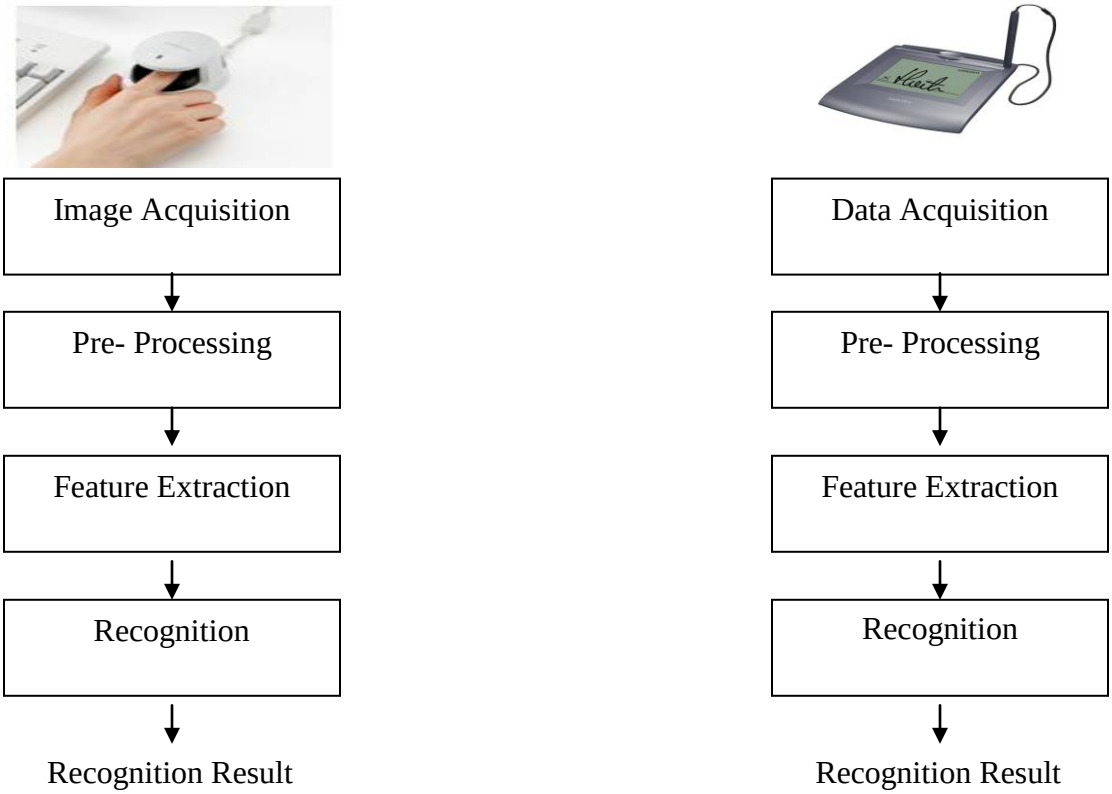

Figure 1.3 Signature verification and finger vein biometric systems.

1.4.2 New Methodology Proposed

The proposed method depends on the scopes and objectives which include two parts. Firstly, signature verification system adopts different classification methods and then used different fusing techniques to fuse them. The overall of the online signature verification system and the detail of the design system will be described in Section 3.3. The system comprises six modules: data acquisition, preprocessing, validation, feature extraction, recognition and decision.

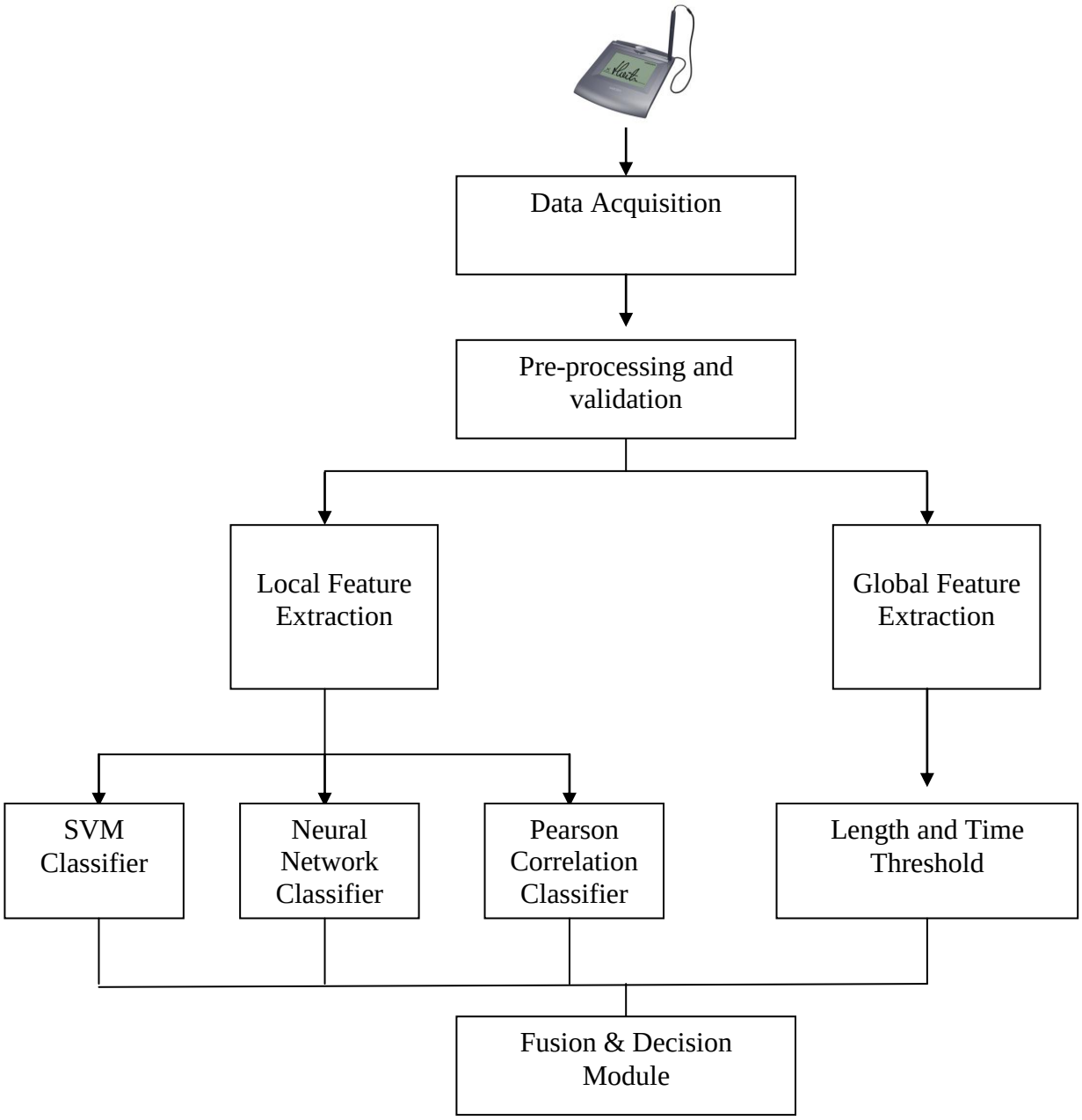

Figure 1.4 Proposed signature verification system

1.5 Contribution of Thesis

The most important contribution of this thesis is the outcome that leads to the design of an online signature verification system. The contributions described in this thesis are as follows:

- A validation module has been proposed in strict conditions such that only the correlated signatures are passed to create consistency of the signatures from each signatory. Employing the Pearson's correlation technique to develop a method for signature verification.
- A new feature selection combining global and local features for higher performance system.
- Applying a different fusing method such as fuzzy logic, sequential fuzzy logic and max voting, to combine the scores of the previous classification methods allow to show better consistency and more robust output.
- Testing the performance and the accuracy of the proposed online signature verification system in case of extending it to biometric system.

1.6 Outline of this Thesis

The thesis has been divided into six chapters:

- Chapter 1 introduces some background information on the biometric system, multimodal biometric system, and the suggested multimodal system which includes signature and finger vein. It also consists of the scope and objectives, research methodology, the contribution and layout of the thesis.
- Chapter 2 discuses the literature review which gives the state-of-the-art methods used in the fields of the signature verification. The summary achievement of other researchers in this field is also discussed. In this chapter, classification method using neural network, support vector machine and Pearson correlation which also

includes a brief history of the techniques applied are also given. Finally multiple fusion techniques using majority voting and fuzzy logic are discussed.

- Chapter 3 describes the signature verification system that has been designed. The validation module applied the Pearson correlation method, feature selection including local features and global features. Different classification methods SVM, neural network and Pearson correlation are applied to decide within the signature are forgery or genuine. Different fusion methods are used to combine the scores of the previous methods by applying sequential fuzzy logic, fuzzy login and max voting. The final fusion with the score of Hitachi's finger vein system to apply the multimodal biometric system concept is described.
- Chapter 4 describes the experimental results and the discussion for the proposed signature verification system. A comparison between the obtained results and the previous results developed by Fadlil 2006 at CAIRO centre are explained.
- Chapter5 describes the Hitachi's finger vein system in addition to the advantage of fusing the high roust Hitachi's finger vein system with the proposed signature verification system.
- Chapter 6 concludes the proposed system and summarizes what has been achieved in this research. Future work that could be carried on from this thesis is also suggested.