NOTE TO USERS

Université d'Ottawa · University of Ottawa

Université d'Ottawa • University of Ottawa

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Tong QU

AUTEUR DE LA THÈSE - AUTHOR OF THESIS

M. A. Sc. (Electrical Engineering)

GRADE - DEGREE

School of Information Technology and Engineering

FACULTÉ, ÉCOLE, DÉPARTEMENT - FACULTY, SCHOOL, DEPARTMENT

TITRE DE LA THÈSE - TITLE OF THE THESIS

Dynamic Signature Verification System Design Using Stroke Based Feature Extraction Algorithm

A. El Saddik

DIRECTEUR DE LA THÈSE - THESIS SUPERVISOR

A. Adler

CO-DIRECTEUR DE LA THÈSE - THESIS CO-SUPERVISOR

EXAMINATEURS DE LA THÈSE - THESIS EXAMINERS

A. Chan

S. Shirmohammadi

J.-M. De Koninck, Ph.D.

LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

DEAN OF THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Dynamic Signature Verification System Design Using Stroke Based Feature Extraction Algorithm

by

Tong Qu

A thesis
presented to the University of Ottawa
in fulfillment of the
the thesis requirements for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Ottawa, Ontario, Canada 2004

Your file Votre référence
ISBN: 0-494-01582-9
Our file Notre référence
ISBN: 0-494-01582-9

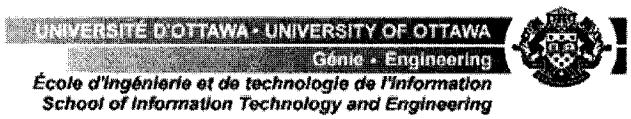
University of Ottawa
Ottawa, Ontario, Canada

April 2004

The undersigned recommend to the Faculty of Graduate Studies
and Research acceptance of the thesis

Dynamic Signature Verification System Design Using Stroke Based Feature Extraction Algorithm

Submitted by Tong Qu
in fulfillment of the thesis requirements for
the degree of Master of Applied Science
Department of Electrical and Computer Engineering
School of Information Technology and Engineering
University of Ottawa



I hereby declare that I am the sole author of this thesis.

I authorize the University of Ottawa to lend this thesis to other institutions or individuals for the purpose of scholarly research.

Tong Qu

I authorize the University of Ottawa to reproduce this thesis by photocopying or other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Tong Qu

The University of Ottawa requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

Dynamic signature verification (DSV) uses the behavioral biometrics of a hand-written signature to confirm the identity of a computer user. This thesis presents a novel stroke-based algorithm for DSV. After individual strokes are identified, a significant stroke is discriminated by the maximum correlation with respect to the reference signatures. Between each pair of signatures, the local correlation comparisons are computed between portions of the pressure and velocity signals using segment alignment by elastic matching. Experimental results were obtained for signatures from 25 volunteers over a four-month period. The result shows that when adding stroke-based features into a non-stroke feature system, the accuracy of the signature verification has been greatly improved to False Reject Rate (FRR) of 6.67% and False Accept Rate (FAR) of 13.33%. The result shows that stroke based features are important features, contain robust dynamic information, and offer greater accuracy for dynamic signature verification, in comparison to results without using non-stroke based features.

Acknowledgments

I would like to thank my supervisors Drs. Abdulmotaleb El Saddik and Andy Adler for all their supports, enthusiasm and guidance. As well the reading of my thesis by Drs. Adrian Chan and Shervin Shirmohammadi, is highly appreciated.

I am thankful to the volunteers who offered their signatures for this study. Most of them are the graduate students and researchers in the Multimedia Communication Research Laboratory and Video, Image, Vision and Audio Research Laboratory, School of Information Technology and Engineering, University of Ottawa.

I would like to thank Dr. Andrew Wong, founder and former director of PAMI lab, University of Waterloo, who led me into the research area of pattern recognition. I am also thankful to Dr. Yang Wang, CTO of the PDS company, who funded me to carry out a feasibility study on a pattern discovery system for signature discrimination which can be regarded as the preliminary work for my current thesis.

The love and support provided by my parents and family have been a source of strength and comfort throughout my life. Without their endless support, this thesis would not have been completed. Words cannot express the love I have for them.

To My Parents

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

2D:	2 Dimensional
3D:	3 Dimensional
BMP:	Bayers Multilayer Perceptrons
DNA:	Deoxyribonucleic Acid
DSV:	Dynamic Signature Verification
EER:	Equal Error Rate
EMR:	Electro-Magnetic Resonance
FAR:	False Accept Rate (Type II error)
FRR:	False Reject Rate (Type I error)
GMM:	General Method of Moments
HMM:	Hidden Markov Model
IC Card:	Integrated Circuit Card
ID:	Identification
IONN:	Input Oriented Neural Networks
PDA:	Personal Digital Assistant
PIN:	Personal Identification Number
RCE:	Restricted Coulomb Energy
RMS:	Root Mean Square
TDNN:	Time Delay Neural Networks
USB:	Universal Serial Bus
WINTAB:	Window Tablet

CHAPTER 1

INTRODUCTION

1.1 Objective and Motivation

The ***objective*** of this research is to identify a new algorithm for dynamic signature verification. Subsequently, this algorithm is implemented on a real signature verification system based on a digital pad device. Finally, the performance of the proposed system is experimentally evaluated. This system is able to extract features from an individual's signatures and discriminate genuine signatures from forgeries.

Biometrics is a rapidly evolving technology, which has been widely used in government identification and some commercial identification applications, etc. A biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Due to the unreliability and inconvenience of passwords and cards, biometrics of identification are preferred over of the traditional methods such as passwords, PIN numbers, key-cards and smart-cards, etc.

Dynamic Signature Verification **(DSV)** is the process of verifying the writer's identity by checking the dynamic parameters of the signature against the templates created during enrolment. DSV not only looks at the signature's appearance, but also at the process an individual uses to form the signature. Various dynamic parameters can be analyzed, such as the shape, speed, stroke, pressure, and timing information during the act of signing. According to Cybersign [Cyber03], DSV is easy to explain and thus facilitates trust. This technology is the least expensive and controversial of current biometrics on the market today. In addition, DSV is hard to forge compared to static signature verification.

In the post September 11 world, biometrics systems are being carefully studied for use in national identification applications. The individual privacy problems get more and more attention from our world. The dynamic signature verification, as well as other biometrics techniques, allow automatic identification of an individual from reasonably easy to measure and hard to falsify characteristics. In addition, the development of personal computer techniques has become powerful enough to allow signature verification to be commercially viable. Therefore, we are promoted to study a new algorithm and evaluate its performance in the area of dynamic signature verification.

1.2 The Research Problem

Dynamic signature verification technology uses the behavioural biometrics of hand written signatures to verify the identity of a user. This method is based on features which define the pattern of execution of the signature. The features that are taken into account

include speed, pen pressure, directions, stroke length, and the times when the pen is lifted from the paper. The algorithm stores these factors in a database for future comparisons. They account for changes in one signature over time by recording the time, history of pressure, velocity, location, and acceleration of a pen each time a person uses the system.

Dynamic signature verification systems undertake the following processing steps: 1) acquisition of several biometric sample signatures, 2) conversion of the sample signatures to a biometric template, 3) comparison of templates to calculate a similarity score (or match score), in order to determine whether a newly acquired test signature represents the same individual as stored signatures. The goal of a biometric such as DSV is to verify a claim to identity, giving an output (the person is or is not the same as the enrolled person). To calculate the decision, the match score is compared to a threshold. The threshold used for confirmation/rejection decision depends on the nature of the application.

A typical dynamic signature verification system is illustrated in Figure 1.1. In general, such a system has following five basic components:

- *Data acquisition* - acquiring signature and converting it to digital form.
- *Signature preprocessing* - transforming the data in a standard format.
- *Feature extraction* - extracting key information from the digital representation of the signature.
- *Comparison process* - matching extracted features with templates stored in a database and output a fit ratio.

- *Performance evaluation* - making decision by comparing the similarity score to a threshold.

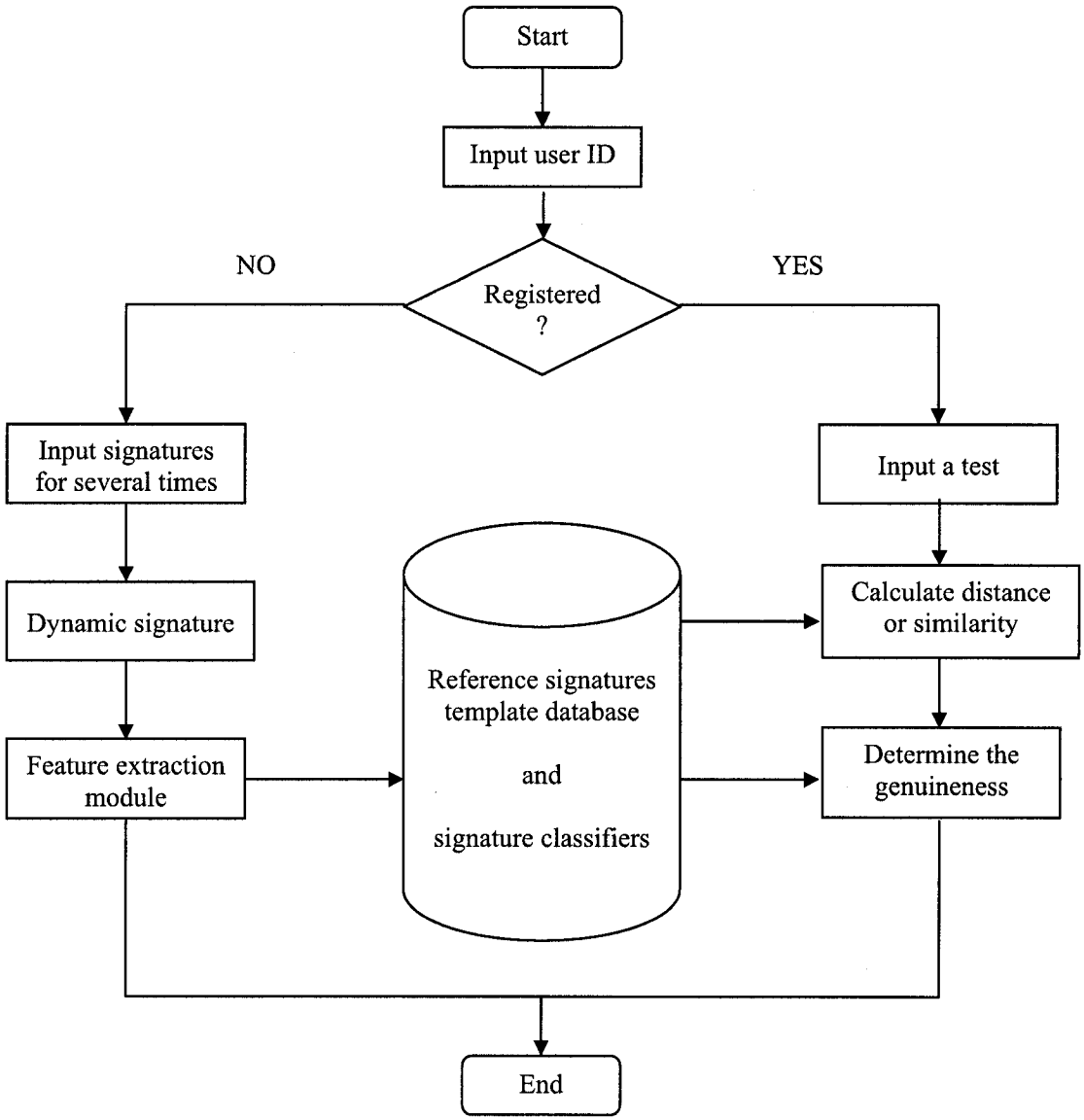


Figure 1.1 A typical model for signature verification system.

Some key steps used in this research are:

- ***Data acquisition*** is done with a digital pad, which inputs data to the microcomputer through serial port. The pad uses the standard Window Tablet input API [Lcs03], and thus this software can be straightforwardly extended to other similar devices.
- ***Feature extraction*** uses a stroke based feature algorithm. A significant stroke is discriminated by the maximum correlation with respect to the reference signatures. Various statistical and time domain features for the significant strokes are extracted for identifying genuine signatures against forgeries. Both features extracted from the significant stroke and other global features are used in the proposed signature verification system.
- ***Signature verification*** is implemented as comparison of templates to calculate a similarity score. The classifiers are designed based on the probabilistic characteristics of the selected features. When evaluating a test signature, its feature values are calculated and compared with the corresponding templates. Both fixed and variable thresholds are used to calculate the false accept rates and false reject rates, and the detection error tradeoffs curve is also estimated.

1.3 Thesis Contributions

The contributions of this thesis can be divided into two categories.

A. Contributions to Knowledge

- A stroke based feature extraction method has been developed for DSV. This study provides an approach to identify the significant strokes and extract an

individual's consistent behavioural characteristics from them. These stroke-based features also can be integrated with other kind of features and applied in the proposed dynamic signature verification system. The experimental results show that stroke based features contain robust dynamic information, and offer great accuracy for dynamic signature verification.

B. Practical Contributions

- An automated dynamic signature verification system has been developed and applied to identify genuine signatures against forgeries. For the convenience of operation, a graphical user interface is designed and the signature verification operation can be conducted conveniently and visually.
- The hardware has been setup for data acquisition. A digital tablet has been connected with microcomputer. The transporting data has been measured by applying a modified WindowTablet application, which is based on a C/C++ developed program.
- A set of signatures from 25 volunteers has been acquired over four-month period. A data acquisition protocol was designed and applied in the data collection.
- Various features have been extracted using an algorithm implemented in Matlab.
- The system performance has been evaluated by conducting various experiments.

1.4 Publications Resulting from This Research

Two papers have been published:

1. Tong Qu, Abdulmotaleb El Saddik and Andy Adler "A Stroke Based Algorithm

for Dynamic Signature Recognition". *In Proceedings of the Canadian Conference on Electrical and Computer Engineering,* Niagara, Ontario, Canada, May 2-5, 2004.

2. Tong Qu, Andy Adler, Abdulmotaleb El Saddik, "Dynamic Signature Verification System Using Stroked Based Features". *In Proceedings of the second IEEE International Workshop on Haptic Virtual Environments and their Applications (HAVE2003)"*, Ottawa, Canada, September 20-21, 2003.

1.5 Organization of the Thesis

In this chapter, the objective and motivation for the current research was presented at first. Then, the dynamic signature verification was briefly introduced based on a typical model. Finally, the thesis contribution, publications resulting and thesis organization were listed, respectively.

Chapter 2 presents the background information related to this thesis, such as the introduction to the biometric techniques and dynamic signature verification. The literature review for the dynamic signature verification has been conducted and the related work has also been discussed.

Chapter 3 provides an overview for the proposed dynamic signature verification system. First, the system architecture is described. Then, the data acquisition and related hardware setup work has been presented in three parts: digital pad setup, data measurement, and data acquisition protocol. Finally, the dynamic signature pre-processing has been realized by developing various functions.

Chapter 4 presents a stroke-based algorithm in feature extraction and signature verification. First, the statistical features and some general feature extraction methods have been introduced. Then, a novel stroke feature extraction algorithm is been described in detail. Finally, the problems about feature selection have been discussed.

Chapter 5 introduces the signature verification and a binary signature classifier has been presented.

Chapter 6 implements the stroke based feature algorithm on the proposed dynamic signature verification system. Both fixed and variable thresholds experiments have been tested for computing false reject rate and false accept rate data. A graphical user interface is also developed for the convenience of conducting signature verification experiments.

Chapter 7 summarizes and concludes the thesis. It presents recommendation for future research.

CHAPTER 2

THE STATE OF THE ART

In this chapter biometric techniques and dynamic signature verification will be introduced. Literature review for dynamic signature verification systems and approaches will be conducted and related work will be discussed. The applications and advantages of the dynamic signature verification will be also presented.

2.1 Biometrics

According to Wayman, biometrics authentication is "automatic identification or identity verification of an individual based on physiological and behavioural characteristics." [Wayman03]. A *physiological characteristic* is a relatively stable physical characteristic, such as a fingerprint, hand silhouette, iris pattern, or blood vessel pattern on the back of the eye. This type of measurement is basically unchanging and unalterable. A *behavioural characteristic* is a reflection of an individual's behavioural makeup, such as a handwritten signature, which is the one of the common behavioural

trails used in identification. Other behaviours that can be used are the manner of typing at a keyboard and the way one speaks.

Biometric technologies include dynamic signature verification, retinal/iris identification, DNA identification, face recognition, voice recognition and fingerprint identification, etc. With the increased use of computers as vehicles of information technology, biometric techniques can be used to prevent unauthorized access or fraudulent use of sensitive or personal data. In addition, biometric techniques can be used to replace traditional smart cards, passwords and PIN numbers since they are easy lost and forgotten. Thus the usage of biometric-based identification systems is gradually increasing.

Recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication for various applications. In the past, only physical objects and behaviour-based-on-memory methods were available for authentication applications. Physical objects include keys and smartcards. Behaviours based-on-memory includes the act of entering a PIN number or a secret password. Recently, biometrics give us alternative ways to realize personal authentication. For physical biometrics, such as DNA, face or fingerprint, they are very difficult to be shared by others, while the behavioural biometrics, such as voice or handwritten signature, are nearly impossible to be replicated by a forger. There are four groups of authentication techniques: physical objects, behavioural objects, physical biometrics and behavioural biometrics. They are summarized in Table 2.1. Among the different biometrics techniques illustrated in Table 2.1, we are interested in dynamic signature verification, which will be introduced in the next section.

Table 2.1 Summary of authentication techniques (I and II represent two different classification methods for all the authentication techniques)

Authentication techniques I / II	Objects (Traditional techniques)	Biometrics (Alternative new techniques)
Physical	Key Stamp IC card PIN number	DNA Face Iris scan Fingerprint
Behavioural	Dynamic passwords	Voice Keyboard typing Static signature Dynamic signature

2.2 Basic of Dynamic Signature Verification

Signature verification is the process used to recognize an individual's handwritten signature. There are two types of signature verification: static and dynamic. Although both of them can be computerized, a static signature comparison only takes into account how the signature looks like, while dynamic signature verification analysis how the signature is made. A static signature verification system captures a 2 dimensional (2D) signature image as input from a camera or a scanner. Static verification methods are based on the limited information available solely from the shape and structural

characteristics of the signature image. A dynamic signature verification system gets its input from a digitizer or other device, usually pen-based, dynamic input device. The signature is then represented as one or several time-varying signals. Dynamic verification methods rely on features, which extracted from the dynamic characteristics of a signing process such as pen motion, pen velocity, personal rhythm, stroke sequences, etc. A copy machine or an expert forger may be able to duplicate the look of a signature, but it is very difficult to duplicate the timing of changes in position, velocity and pressure etc. Therefore, compared with static signature verification, dynamic signature verification has higher potential to increase the authentication trust and to decrease the possibility of fraud. On the other hand, DSV is limited in the sense that it can only function with the required hardware, while static signature verification is able to analyse signatures written on paper.

An individual's signatures are remarkably consistent; however, there will always be slight variations in a person's handwritten signature, but the consistency of an individual's signature makes it natural for biometric identification [Lee92]. So the DSV technology examines the behavioural components of the signature, such as stroke order, speed and pressure, as opposed to comparing visual images of signatures. A graphical dynamic signature example is shown in Figure 2.1. Not only a 2D static signature image can be reconstructed by a dynamic signature, but also more dynamic information can be represented. The pressure values are represented by the dot size and open circles indicate the period when the pen lifted up from the pad surface.

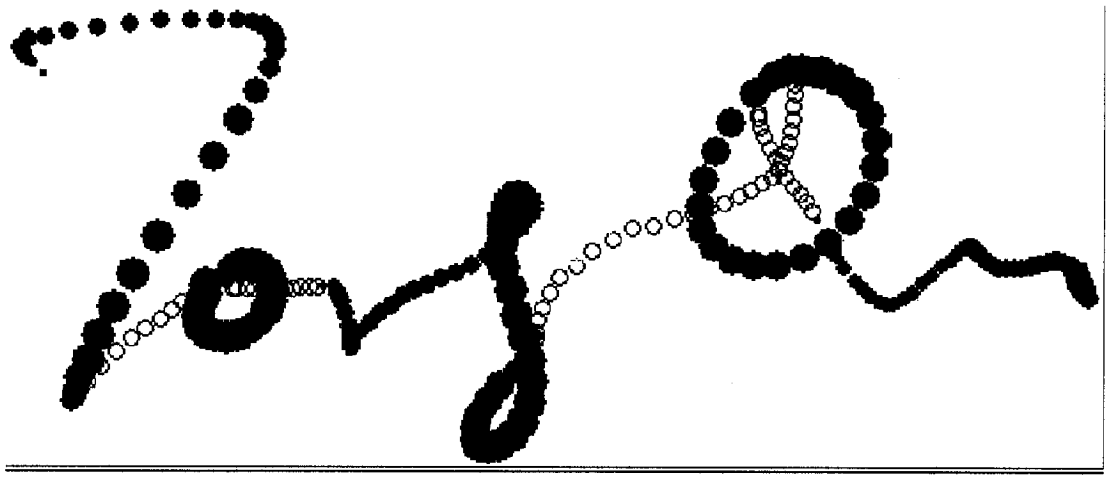


Figure 2.1 A graphical dynamic signature example.

According to Cybersign, "the primary advantage that dynamic signature verification technology has over other types of biometric technologies is that signatures are already accepted as the common method of identity verification" [Cyber03]. This history of trust means that people would be willing to accept a signature based verification system. In addition, DSV is the least controversial of all the biometric technologies because of its natural occurrence in everyday transactions. Individuals are less likely to object to their signature being confirmed as compared to other possible biometric technologies. Some other advantages of DSV are its ease of use and lower cost.

Compared to traditional authentication technologies such as passwords and key cards, which are often shared or easily forgotten, lost and stolen, DSV provides a simple and natural method for increased computer security and trusted document authorization.

There are various applications for dynamic signature verification and other biometrics techniques [Cyber03], such as:

- Access control to buildings
  - Computer room
  - Secure sites (research centre, nuclear site)
- Information systems, launching of operating system
  - Access with network
  - Electronic trade
  - Transactions (financial institutions, data between companies)
- Communications equipment
  - Access terminal with Internet
  - Mobile phone
- Various machine & equipment
  - Safety or comfort with electronic locks
  - Automatic distributors
  - Legal files
  - Identity papers (passport, driving license, residence permit)
  - Electronic voting systems
- Banking and Commerce
  - Home consumer banking
  - Internet eCommerce
- Government
  - Government departments
  - Electronic Signatures

2.3 Literature Review and Related Work

Handwriting is a personal skill that comprises of three main characteristics. It consists of artificial graphical marks on a surface; its purpose is to communicate something; this purpose is achieved by virtue of the mark's conventional relations to language [Colmas80]. Several types of analysis, recognition, and interpretation can be associated with handwriting. According to Plamondon, "*Handwriting recognition* is the task of transforming a language represented in its spatial form of graphical marks into its symbolic representation. *Handwriting interpretation* is the task of determining the meaning of a body of handwriting. *Signature verification* is the task of determining whether or not the signature is that of a given person" [Plamon00].

Handwriting data are converted to digital form either by scanning the writing on paper or by writing with a special pen on an electronic surface such as a digitizer combined with a liquid crystal display. The two approaches are distinguished as *off-line* and *on-line* handwriting, respectively [Plamon00]. In the on-line case, the two-dimensional coordinates of successive points of the writing as a function of time are stored in a specific order, i.e., the order of strokes made by the writer is readily available. In the off-line case, only the completed writing is available as an image. The on-line case deals with a spatio-temporal representation of the input, whereas the off-line case involves analysis of the spatio-luminance of an image [Plamon00].

On-line recognition is defined by Plamondon as methods and techniques dealing with the automatic processing of a message as it is written using a digitizer or an instrumented stylus that captures information about the pen tip, generally its position,

velocity, or acceleration as a function of time [Plamon00]. This has been a research challenge since the beginning of the 1960s, when the first attempts to recognize isolated handprint characters were performed [Earnest63], [Eden62]. Subsequently, numerous methods and approaches have been proposed and tested; many have already been summarized in a few exhaustive survey papers [Nouboud90], [Plamon99], [Tappert90], and [Wakahara92]. Over the years, these research projects have evolved from being academic exercises to developing technology driven applications.

Dynamic signature verification (DSV) refers to the comparison of a test signature with one or a few references that have been collected as a user enrols in a system. This requires the extraction of writer-specific information from the signature signal, irrespective of its handwritten content [Plamon00]. This information has to be almost time-invariant and effectively discriminate. This problem has been a challenge for about three decades. Two survey papers [Leclerc94], [Plamon89], and a journal special issue [Plamon94] have summarized the evolution of this field through 1993.

In general, there are two types of forgeries named as random and skilled forgeries. According to Plamondon, "*Random forgeries* were collected when the forger knew the name and spelling of the genuine signer but no knowledge of the genuine signature. This type of forgery is also called as zero-effort forgery. *Skilled forgeries* were generated by forgers who were provided several samples of genuine signatures on a piece of paper and told that the verifier uses dynamics features of the signature and were allowed to practice on paper and tablet" [Plamon00].

Two types of errors are used to evaluate the performance of a detection system such as DSV, namely Type I error (false rejection) and Type II error (false acceptance). *Type*

I error occurs when an authentic signature is falsely rejected, which corresponds to the *False Rejection Rate* (FRR); while *Type II error* refers to the acceptance of forgeries as being authentic, which corresponds to *False Acceptance Rate* (FAR). If the score distributions of FAR and FRR overlap, their distribution curves will intersect at a certain point. This overlap refers to the match score distributions, not the error curves. The value of the FAR and the FRR at this point, which is the same for both of them, is called the *Equal Error Rate* (EER). The rate of Type I and Type II errors are very important to consider when putting together a signature verification system (or any biometric system for that matter). As a matter of fact, if the rate of Type I errors increases, the rate of Type II errors decreases [Lee92]. The inverse relationship between the two types of errors enables the biometric system designer to balance Type I and Type II errors constantly with the requirements of the system users.

Although useful applications of signature verification have only recently become available, research into the creation of a workable automatic (electronic) signature verification device or system has been conducted for at least the past two decades.

Major successes and promising applications of both on-line and off-line approaches have been indicated in Plamondon's review paper [Plamon00]. However, Plamondon claimed that there is not a clear breakthrough either in signature verification although many projects have been carried out on dynamic signature verification with varying degrees of success [Plamon00]. A variety of new techniques suggests either adjustments or combinations of known methods and has been used with more or less success. Throughout the literature, different approaches and techniques are applied for the DSV

such as: feature values comparison, point to point comparison, neural network training techniques, wavelets, Fourier transform, power spectral and shape comparison, etc.

The earliest cited work on DSV appears to be that of Mauceri [Mauceri65] cited by Herbst and Liu [Herbst77]. Herbst and Liu report that Mauceri took 50 signatures from each of the 40 subjects in order to evaluate his method, which used power spectral density and zero-crossing features extracted from pen acceleration waveform measurements. A FRR of 37% has been reported.

Feature values comparison is based on the assumption that there are remarkably consistent characteristics in a person's signatures; this technique is the most widely used in dynamic signature verification. Various features are used to capture the signature information and these features are computed/compared for the purpose of signature verification. Crane and Ostrem first presented a feature values comparison method and feature selection techniques [Crane83]. They used a strain-gauge instrumented pen to sample three forces of the writing tip: the x and y forces and the download force. They extracted 44 features from these forces such as: scaled means, standard deviations, minimum and maximum values, number of zero-crossings, maximum minus scaled mean, and maximum minus minimum, etc. A total of 5220 genuine signatures for 58 subjects and 648 forgeries from 12 forgers were collected over a four-month period. They achieved the FAR and FRR varying from 0.5% to 3%, but they used different definitions of FRR and FAR which are not normally used in the literature, and they also allowed three tries for verification.

Parks et al. also used features value comparison for DSV [Parks85] and they initially suggested six features: total elapsed time, time in contact, number of segments, sum of

increments in the x direction, maximum increment in the x direction, and sum of increments in the y direction. They used different values of threshold for different individuals and updated the reference signatures by applying a weighting of 90% to stored feature parameters and 10% to the new ones obtained form the test signature.

Lee conducted a comprehensive study in his thesis for the purpose of designing a simple on-line system yielding good performance [Lee92] [Lee96]. From timing, position, velocity and acceleration signals, he extracted 29 dynamic features and 13 static features. Lee noted that a small subset from the 42 features performed better than the whole set [Lee92]. Individualized subsets of features are selected for different individuals. The individualized subsets of features are tested on a larger database that had 1485 genuine signatures and 608 forgeries (how these were selected is not made clear). They achieved 1% FRR and 14% FAR. They also obtained 0.3% FRR and 17% FAR when evaluated one individual who had signed 1000 times.

Gupta and Joyce noted that features derived from the dynamic information of handwritten signatures such as number of velocity sign changes in the x direction are more important than those from the shape of signatures such as the maximum height of a signature [Gupta97a]. They proposed an algorithm with the aim of using a set of features that are simple and easy to compute. In their experiments, they used the following 6 features: the total time, the number of velocity sign changes in the x direction, the number of velocity sign changes in the y direction, the number of acceleration sign changes in the x direction, the number of acceleration sign changes in the y direction, and the total pen-up time. They added additional path length feature to the initial set, and were able to improve the performance to a FRR of 0.5% and a FAR of

10%. They also noted that three signatures are not sufficient to build the reference signature and that at least five signatures should be used while seven and ten signatures would be better.

According to Gupta, point to point comparison is based on the idea of comparison a test signature with a reference signature by comparing the different parts of the signature separately and combining these comparisons to achieve an overall similarity measure [Gupta97]. Since variations exist between the genuine signatures, it is difficult to make a direct point to point comparison. Therefore, in order to make more effective comparisons, a system should perform some type of alignment of the test and reference signatures in an attempt to line-up the corresponding parts of the signatures [Gupta97]. Herbst and Liu presented a technique based on acceleration measurements using regional correlations [Herbst77]. They used two orthogonal accelerometers mounted on an experimental pen to sample a signature at the rate of two hundred samples per second. They found that most signatures were of 2-10 seconds in duration with an average time of about 5 seconds. They claimed that the total time taken for writing signatures by an individual is consistent [Herbst77]. Therefore, they heuristically partitioned each signature into segments and computed the cross-correlation of corresponding segments. The segments were modified based on the duration of the interval and discrepancies between the test signatures and the reference signature. The signatures were separated into a set of segments with 1 or 2 seconds duration. The technique was evaluated using a database of 1682 signatures. An individual's reference signature was selected from the 5 sample signatures of the same individual. The distance between the reference signature and the remaining 4 sample signatures was at least equal to a pre-specified

value. So such selected reference signature was supposed to be the "best" reference signature. A total of 70 reference templates were selected from 350 signatures (5×70) for the 70 users. The test signatures included 695 genuine and 287 forged signatures. Before applying the correlation test, the verification algorithm rejected a signature if its duration is longer than 20% of the duration of the reference signature. A FRR of more than 20% was obtained with a FAR of around 1%.

Plamondon and Parizezu compared the performance of three types of data: position; velocity; and acceleration, using three techniques: regional correlation, dynamic time warping and skeletal tree matching [Plamon88]. The regional correlation method is similar to the correlation method proposed by Herbst and Liu [Herbst77]. Different with 1 or 2 second segment used by Herbst and Liu, Plamondon used 0.7 second piece of the signature as a segment based on a claim that handwriting signals tend to fall out of phase beyond 0.7 seconds [Plamon88]. According to Plamondon, time warping is a nonlinear correlation technique borrowed from speech recognition and is used to map segments from a test signature to segments of the corresponding reference signature through the removal of unwanted timing differences. The distance between two samples can then be computed [Plamon88]. Tree matching is a technique that involves building a tree of peaks and valleys of signatures. The distance between them may be computed in terms of minimum number of operations needed to transform one tree to another [Plamon88]. Each of the three techniques used all the values of position, velocities and accelerations along the x and y directions and no statistical features were used. The database consisted of 50 signatures from each of 39 volunteers; no skilled forgeries were collected and random forgeries were used to determine FAR. Total error rates (FRR+FAR) averaged

over the three types of algorithms are presented. Using random forgeries the FAR average varied between 1.9% and 8.1%. Later, Parizeau and Plamondon also used the same experiments to compare the three types of techniques: regional correlation, dynamic time warping and skeletal tree matching [Parizeau90]. The experimental results of the three techniques showed total error rates between 3% and 17%. It also showed that no technique was globally superior to the other two although regional correlation was often better and much faster.

Neural Network techniques differ from the above techniques in terms of its underlying computational philosophy - the exploitation of different feature types. However, this approach suffers from the somewhat undesirable constraint that relatively large training sample sets are often required if acceptable levels of performance are to be achieved. Lee described three neural network based approaches for dynamic signature verification: Bayes multilayer perceptrons (BMP), time delay neural networks (TDNN), and input oriented neural networks (IONN) [Lee95]. He applied the back propagation algorithm in the network training. Each signature was input as a sequence of instantaneous absolute velocity extracted from a pair of spatial coordinate time functions [Lee95]. The absolute velocity is the only feature used in the study. As many as 1000 sample signatures are collected from the same signer, and every absolute velocity signals for the 1000 sample signatures are used to train the system. The proposed neural network systems automatically discriminates patterns using Bayes decision rule. Besides the 1000 sample signatures from the same signer, they also collected 450 forgeries from 18 forgers. The BMP, TDNN, and IONN provided an equal misclassification error rate of 2.67%, 3.82%, and 6.39%, respectively [Lee95].

Pacut and Czajka proposed a dynamic signature verification system, which applied two neural networks as the classification functions, namely a two layer sigmoidal perceptron and the Restricted Coulomb Energy (RCE) network which is a variety of radial basis network [Pacut01]. They extracted several features from five channel signals: horizontal and vertical pen tip position, pen tip pressure, pen azimuth and altitude angles. The detail for the neural networks was not provided. It was reported that a FAR of 0% and a FRR of 22% were achieved for the two-layer sigmoid perceptron network; and a FRR of 11.11% and a FAR of 8.33% for the RCE network [Pacut01].

In addition to the above mentioned approaches, there are some other approaches in the area of dynamic signature verification. For example, Lejtman and George applied wavelets and back-propagation neural network together for the on-line signature verification [Lejtman01]. They extracted features from the pen tip pressure, velocity, angle of pen movement and applied the Daubechies-6 wavelet transform using coefficients as input to a neural network. They claimed the system achieved a FRR of 0.0% and a FAR of less than 0.1%. Wessels and Omlin used hidden Markov models to model the dynamics of signatures [Wessels00]. They claimed their initial results achieved a FRR of 0% and a FAR of 13%. Lam and Kamins applied Fourier transform on the dynamic signature verification and used the 15 harmonics with the highest frequencies for each signature for verification [Lam89]. A relatively small database was used with one genuine signature and 19 forgers. This limited evaluation lead to a FRR of 0% and a FAR of 2.5%. Nalwa developed a strategy primarily based on the shapes of signatures for dynamic signature verification [Nalwa97]. His approach differs from traditional approaches, which rely primarily on the pen dynamics during the production

of the signature, in the fact that he proposed a local shape based model for handwritten on-line curves. Experiments were conducted based on three databases of signatures. The first database included a total of 904 genuine signatures from 59 signers and 325 forgeries collected from some of the signers; the second database contained 982 genuine signatures and 401 forgeries from 102 signers; and the third database included 790 genuine signatures and 424 forgeries from 43 signers. The equal error rates for the three databases were about 3%, 2% and 5%, respectively [Nalwa97].

CHAPTER 3

SYSTEM OVERVIEW

In this chapter, the proposed dynamic signature verification system will be presented from a system point of view. The system is composed of four parts: data acquisition; signature pre-processing; feature extraction and signature verification. First, the data acquisition and related hardware setup are described. Then, the signature pre-processing and data transformation are introduced. The feature extraction and signature verification will be studied in detail in the next chapters.

3.1 System Description

The proposed dynamic signature verification system is illustrated in Figure 3.1 and is composed of four subsystems: 1) data acquisition; 2) signature pre-processing; 3) feature extraction; and 4) signature verification.

In the data acquisition subsystem, the signatures are acquired and digitized by a digital pad. Then the raw data are sent to a microcomputer through a serial port. The time, position and pressure data are measured by a Window Tablet Application, which monitors the serial port at a sample rate of one per millisecond. A total of four channels

of raw data are measured: the sampling time sequence t, the x position values, the y position values, and the z pressure values.

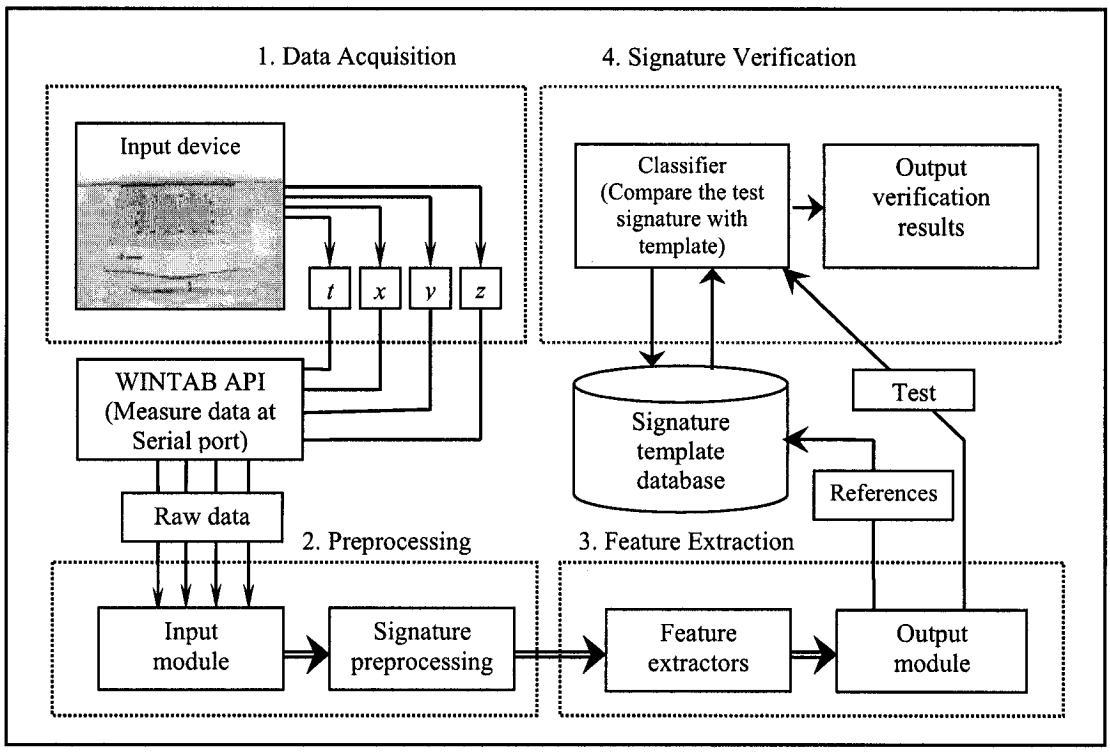


Figure 3.1 The proposed dynamic signature verification system.

Based on the above four channels of raw data, velocity, acceleration and angle signals are computed in the signature pre-processing subsystem. First, the noise is filtered for the raw data. Then, the velocity, the acceleration and the signals are computed. Finally, the dynamic signature signals are re-sampled and normalized before being sent to the feature extraction subsystem.

In the feature extraction subsystem, the key information of the input dynamic signature is calculated by pre-configured feature extractors. Both global feature

extractors and stroke feature extractors are used. These stroke feature extractors are designed based on a novel stroke based feature extraction algorithm, which will be described in more details in chapter 4. For the training signatures, the extracted sampling feature vectors are forwarded and stored in the signature template database; for a test signature, the obtained feature vector is sent to the signature verification subsystem and compared with the template by a signature classifier.

The signature verification system is used to compare the test signature with the templates stored in the database. A test signature is compared to the template of the enrolled signature, and a match score calculated. A decision is made by comparing the score with the threshold value. Signatures with scores above the threshold are authenticated; otherwise, they are judged as a forgery.

3.2 Data Acquisition and Hardware Setup

A Patriot digital pad (Figure 3.2) is used to collect dynamic digital signatures. The acquired raw data are measured at the serial port by a modified Window Tablet Application. A data acquisition protocol is designed to guide the data acquisition processing over an extended testing period.

3.2.1 Patriot Digital Pad Setup and Its Mechanisms

A Patriot digital tablet is used to acquire signatures in this research. This digital pad is manufactured by Huaqi while its technique is patented by Wacom. The technical parameters are illustrated in Table 3.1 [Huaqi03]. The mechanism of this type of digital pad is based on the Electro-Magnetic Resonance (EMR) position sensing technology [WACOM03]. A component-less printed circuit board is used where the copper tracks provide a multitude of over-lapping antenna coils in both the x and y directions. Underneath the sensor is a magnetic reflector used to enhance and shield the magnetic field. The sensor is placed underneath and penetrates the display [WACOM03].

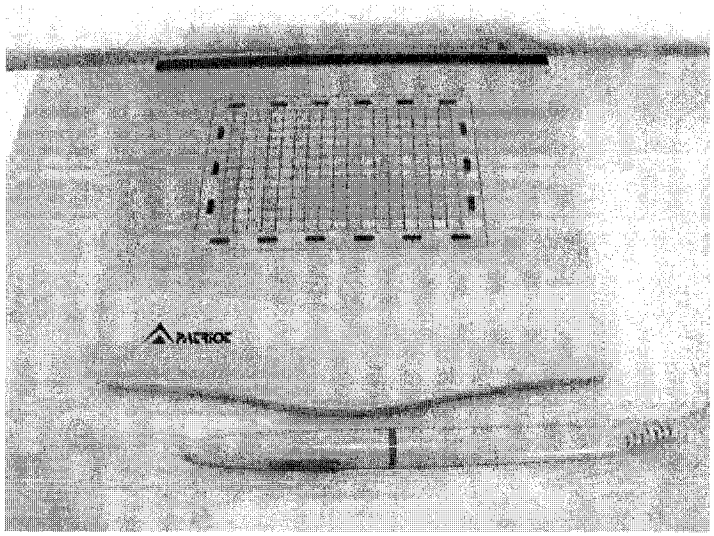


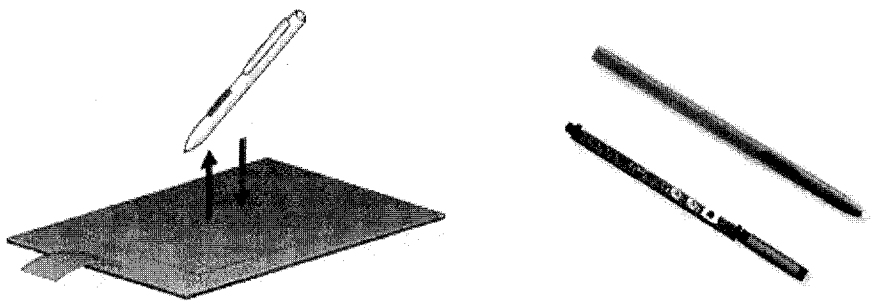
Figure 3.2 A picture of Patriot digital pad.

Energy coupling between pen and pad is illustrated in Figure 3.3 (a). According to Wacom, A close-coupled field is generated at a very low energy level and resonant frequency. This energy couples with a tank circuit, which is located in the pen. The pen

is battery-less and contains just an inductor and capacitor in its simplest embodiment. The inductance and capacitance values of the tank circuit are selected to match the resonant frequency of the antenna coil [WACOM03]. The inside of the digital pen is shown in Figure 3.3 (b).

Table 3.1 The specification of the Patriot digital pad [Huaqi03]

Items	**Description**
Dimensions	166 mm (L) x 177 mm (W) x 9.3 mm (H)
Active Area	4.0" x 3.0"
Weight	8.4 oz (238g) N.W.
Report Rate	At Least 100 points/sec
Resolution	4064 LPI
Pressure Sensitivity	~ 512 Levels



(a) (b)

Figure 3.3 (a) Energy coupling between a pen and digital pad, (b) The inside of a digital pen [WACOM03].

According to Wacom, the coupled energy resonates with the tank circuit and reflects back towards the sensor board by forming a shaped h-domain field at the tip of the pen. As this happens, the same antenna coil is switched to receive this reflected energy and provide an analogue signal. This process is repeated in rapid succession with all antenna coils. All of these analogue data are then collected and converted into digital signals that can be post-processed to give x and y position and pen tilt information. The pen has to be a maximum of 14mm from the sensor surface for it to be acquired. The sensor can track the pen as it hovers above it [WACOM03]. The sensor only detects a "pen down" signal when pressure is applied to the pen tip. The mechanism of generating the x and y position as well as the z pressure information is illustrated in Figure 3.4.

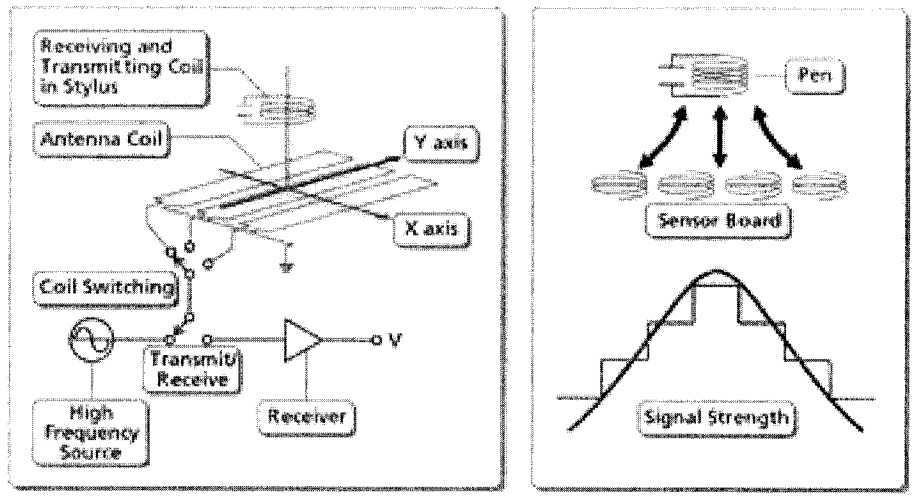


Figure 3.4 The digital pad mechanism of generating x and y position and z pressure information [WACOM03].

3.2.2 Data Measurement at Serial Ports

Software design was based on open industry standard software - Wintab™ Developer Kits developed by LCS Tele-graphics Ltd [Lcs03]. We modified the software and applied it to measure the raw data at RS232C serial port of a standard microcomputer. The developed program was programmed using C/C++ language in the Microsoft Visual Studio environment. Because this modified program is based on open industry standard software, its interface specification is suitable for different tablets with a serial port or a USB port. In this study, the raw data are measured at the serial port at every millisecond. Figure 3.5 shows a screen capture for the serial port monitor interface during the measuring process. The diameter of the white circle in the figure corresponds to the value of the pen tip pressure.

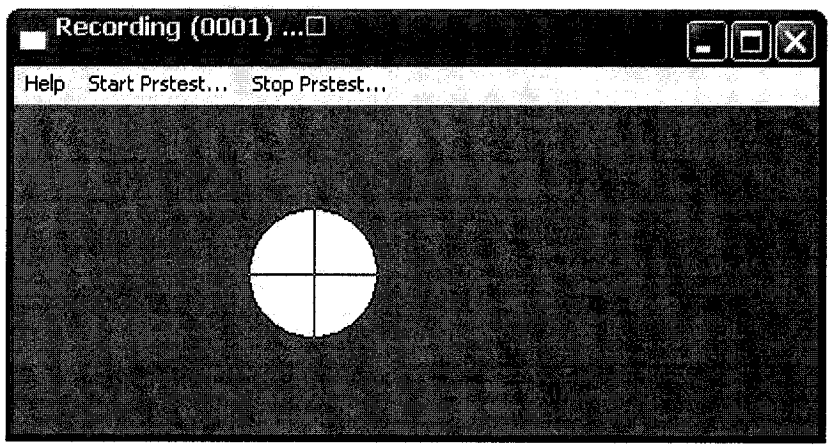


Figure 3.5 Screen capture for serial port monitor interface.

Some samples of the measured data are shown in Table 3.2 and is plotted in Figure 3.6. For the four row signals in Figure 3.6, the first row represents the time information,

which is recorded by the system timer inside the Windows operating system, and the other signals represent the x position, the y position and the z pressure, respectively. In general, the dynamics of the acquired signatures can be represented by equation 3.1.

$$S(t) = [x(t), y(t), z(t)]^T, \qquad (t = 0,1,2,\cdots,n). \tag{3.1}$$

So, $S(t)$ is a collection of x, y position values of the pen tip and the pen tip pressure values at given times (generally, equal time intervals). We treat handwriting pressure as analogue z axis information. The raw data such as in the Figure 3.6 are later re-sampled into a given time intervals.

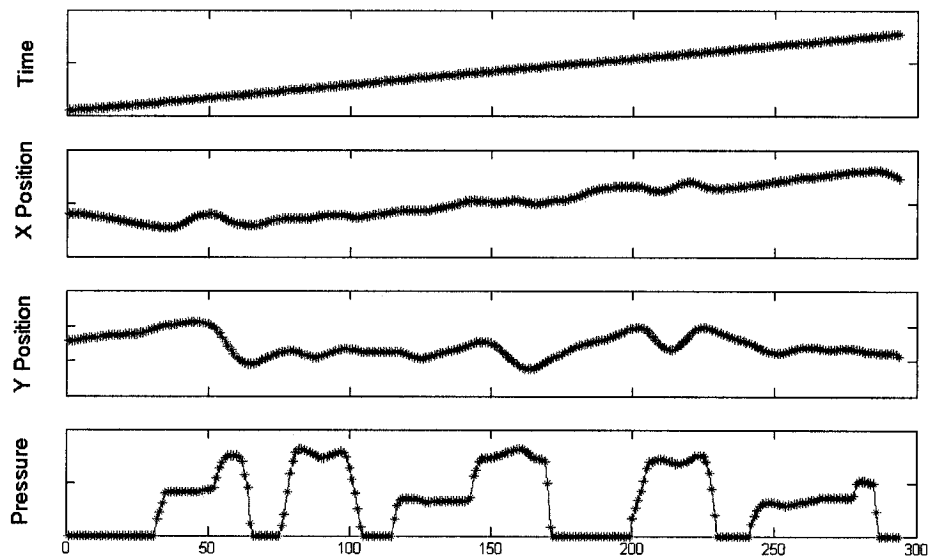


Figure 3.6 Plot raw data example measured at serial port for a set of sampling points.

Table 3.2 A sample segment for the measured data at serial port

Sampling time (millisecond)	***x* position** (0.001 inch)	***y* position** (0.001 inch)	***z* pressure** (1 of 512)
1	2240	6180	0
16	2195	6186	3
31	2190	6186	3
63	2200	6220	4
63	2200	6220	4
⋮	⋮	⋮	⋮
219	3125	5580	15
235	3015	5406	17
235	2890	5260	18
250	2780	5126	17
266	2695	5020	17
⋮	⋮	⋮	⋮

3.2.3 Data Acquisition Protocol

In order to effectively test the performance of current signature verification system, a data acquisition protocol is designed to guide the data acquisition processing over a four-month period. According to the instructions in [Biowork00], a data acquisition protocol including instructions for volunteers is proposed and shown in the appendix.

In the proposed system, each user is required to construct her/his signature template at first. Users must repeat their specimen signature several times in the "same" manner, which means using the "same" speed, pressure, strokes, timing sequence etc. Before recording the signatures, users were asked to practice the signing process until they felt

able to recreate their signature easily and comfortably on the digital pad. In order to obtain a signature template, which reflects the long-term manner of a user's signing process, a set of this user's signatures is recorded at different times and in different emotional situations (happy, sad, excited, or tired, etc). Twenty-five volunteers took part in the data acquisition and their signatures were collected over a period of four months. All the collected genuine signatures were classified into two classes. One was used for training signature template and the other was used for signature verification. In order to reflect the effect of the number of training signatures, some volunteers signed as many as 60 signatures, while others only recorded 15 signatures. Some volunteers were asked to forge other's genuine signatures. They were asked to study not only the 2D structures of the genuine signature but also the dynamic signing process. Between five and eight skilled forgeries were obtained for each signature template.

3.3 Signature Pre-processing

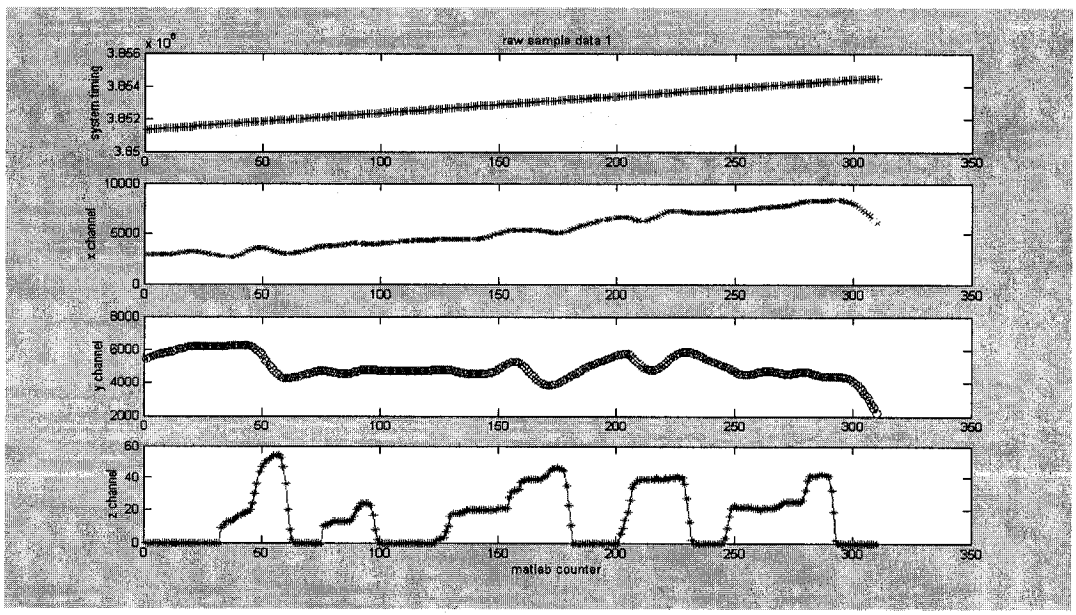
In the signature pre-processing subsystem raw data are re-sampled, normalized, and processed to remove extraneous signals. The velocity, the acceleration and the azimuth angle are computed based on the four channel raw data: time sequence, x position values, y position values and pressure values. In addition to the above, the dynamic characteristics of signature writing will also be discussed.

3.3.1 Signature Pre-processing Functions

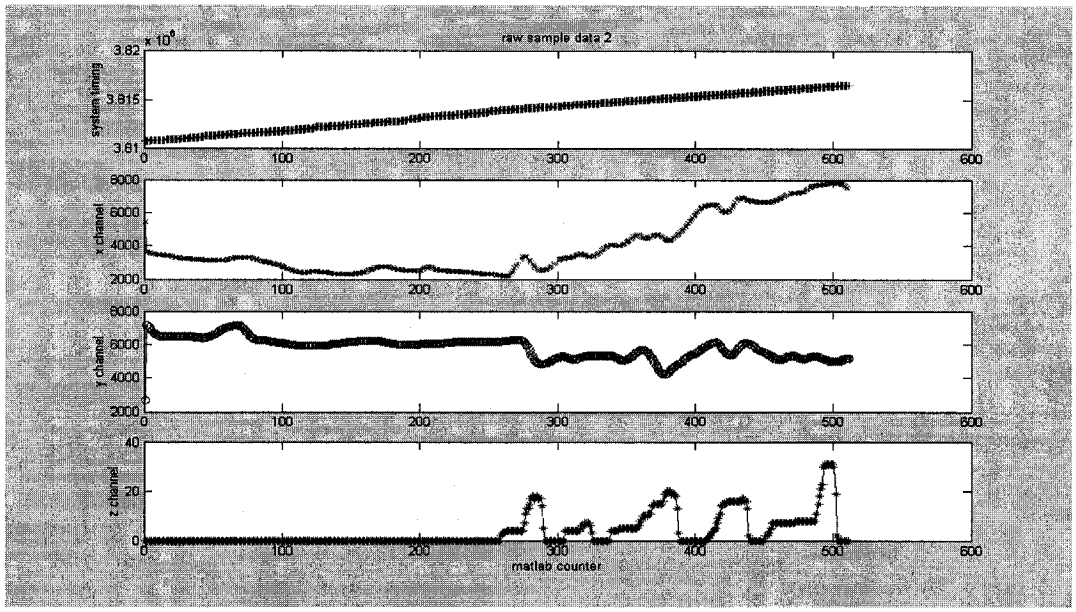
In the signature pre-processing stage, the following functions are used:

Extraneous signal removal is used to remove noise in the raw data. When a digital pen hovers in the sensing area of the pad, even if the pen tip does not touch the pad surface, the pad still generate some position signals while the pressure values are zero. This is due to the electro-magnetic resonance and to the position sensing mechanisms. Since we are only interested in the signals generated during the signing process, the position signals corresponding to zero pressure should be removed from the raw data.

In Figure 3.7, the raw data of two sample signatures signed by the same individual are illustrated. For both signatures, the pad begins to generate position signals before and after the signing process. The signing process can be identified by the pressure signals. The effective signing signals correspond to the time interval between the first and last non-zero pressure point. The signals corresponding to other time intervals are removed. Figure 3.8 shows the effective signing signals for the signature in Figure 3.7 (b) after the extraneous signal are removed.



(a)



(b)

Figure 3.7 Comparison of the raw data of the two sample signatures signed by the same individual, (a) the first sample signature, (b) the second sample signature.

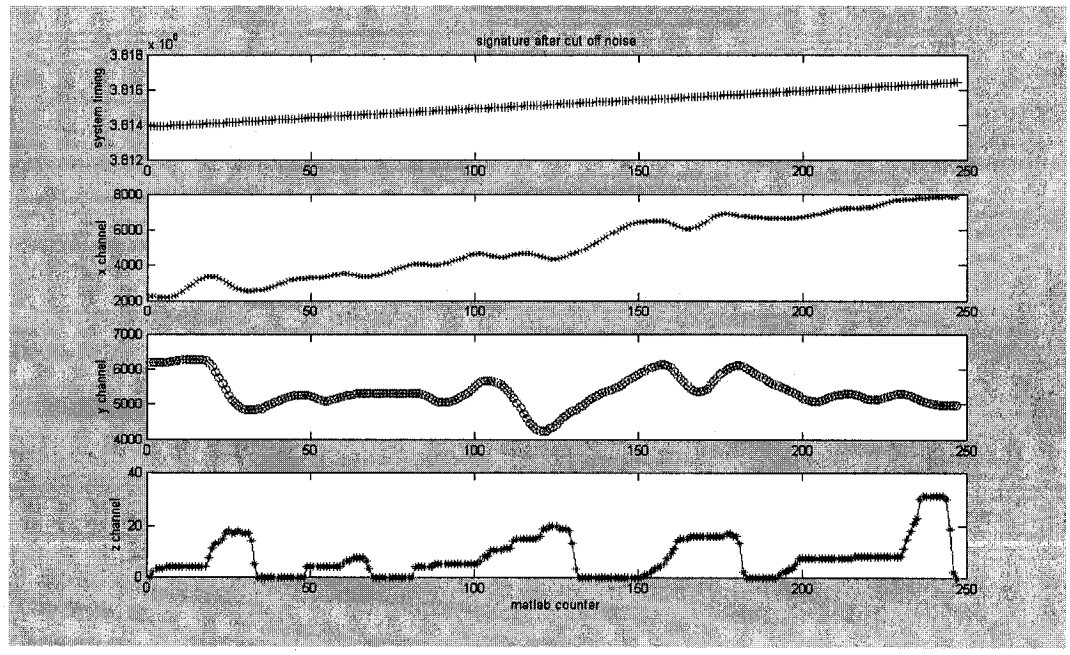


Figure 3.8 Effective signing signals corresponding to the signature in Figure 3.7 (b).

Re-sampling is designed to convert the raw data into standard length in order to facilitate further analysis. It is clear that every time a person signs, the number of samples obtained will be somehow different, that is the raw data length n will have a different value. This variation in genuine signature of the same individual makes it very difficult to compare two sets of values from two different genuine. This can be observed in Figure 3.7. After storing the absolute time, the positions (x and y), and the pressure information in a database for further analysis, we "stretch" all the raw data to a standard length n by a fixed number of sampling points ($n = 1000$ points are used in current study). This re-sampling process can be achieved by using "spline" function in the Matlab signal processing toolbox. In the case of multiple data points recorded at the same time value, only one point is needed and its value is computed as the average of the values of multiple points. In Figure 3.9, the signature data shown in Figure 3.8 are re-sampled to a fixed length of 1000 points. Although there are 247 sampling point in Figure 3.8 and 1000 standard sampling point in Figure 3.9, it is clear that the signals in Figure 3.9 keep the "same" shapes as in Figure 3.8. So the re-sampling process does not loss the significant characters of the original signatures.

Normalization is developed to compensate for the effect of different sizes and scales of the signatures. The digital pad generates the absolute position values for the signatures, but we are only interested in the dynamic sequence of the signature creating process. Therefore, only the relative position values with respect to the first signing point are desired. In addition, we normalize the pressure signal for further analysis. The starting location, the size, the total duration and the pressure of the signature are normalized, so that the signature verification is independent of these characteristics. The

normalization process for a coordinate point in the signature is calculated according to the equation 3.2.

$$Norm\_Value = \frac{Current\_Value - Origin\_Value}{|End\_Value - Origin\_Value|}, \tag{3.2}$$

where $Norm\_Value$ represents the normalized value; $Current\_Value$ is the current coordinate value; $Origin\_Value$ represents the first coordinate of the signature; and End_Value is the last coordinate point of the signature. Figure 3.10 illustrates the effect of normalization for the data in Figure 3.9.

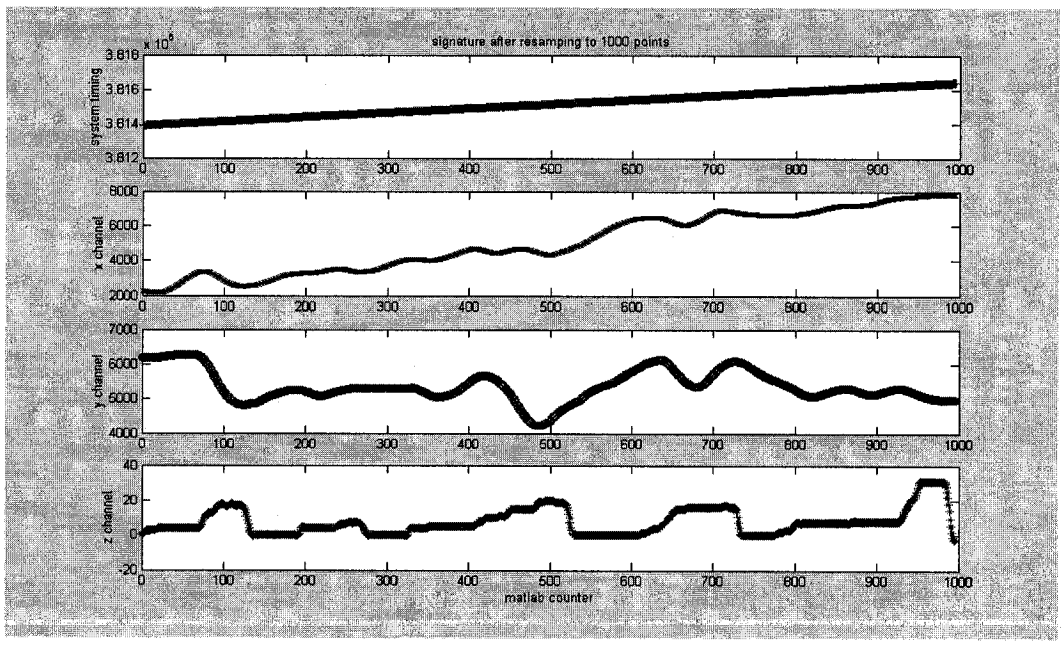


Figure 3.9 Re-sampling the signature data in Figure 3.8 to fixed length of 1000 points.

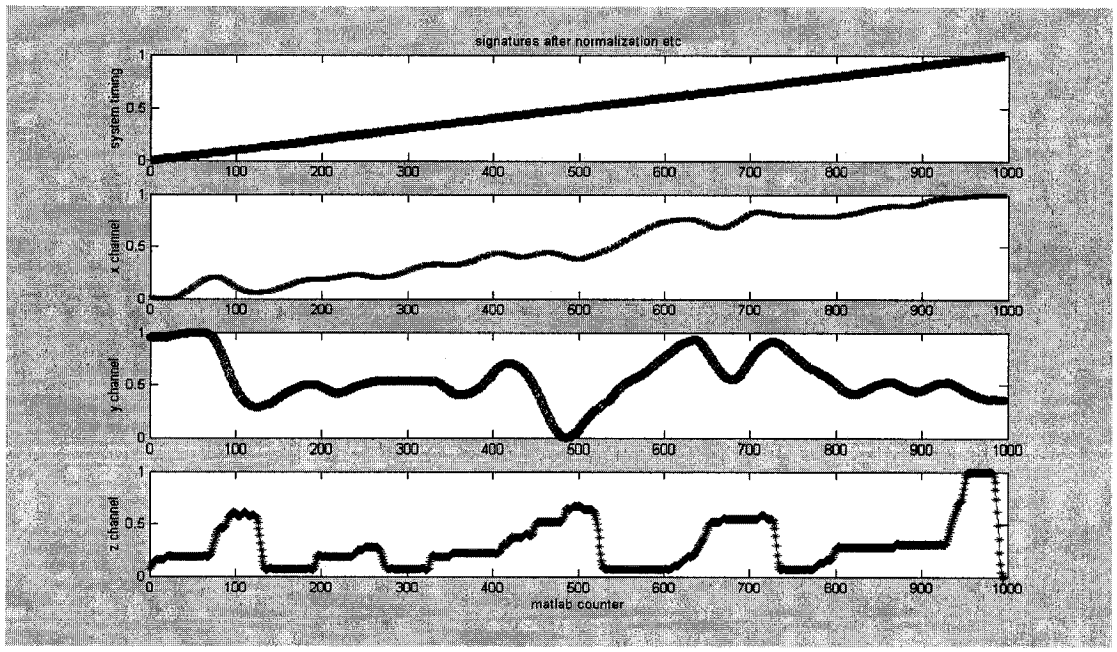


Figure 3.10 The effect of normalization for the data in Figure 3.9.

The above described functions of the input module can not only be applied on the position and the pressure of the acquired data, but they can also be used as velocity, acceleration and writing direction angle data. The generation of theses characteristics is described in the next section.

3.3.2 Representation of Dynamic Signatures

By taking the sampling rate into account, the signature raw data (e.g. data in Figure 3.6), and after appropriate smoothing, may be used to compute the derivatives of x, y and z. The first derivatives "x" and "y" are the velocities in the two directions and the second derivatives are the two accelerations. Once these derivatives have been

computed, the signal vector is calculated according to equation 3.3. The time derivative of the pressure is not used.

$$S'(t) = [x(t), y(t), z(t), v_x(t), v_y(t), a_x(t), a_y(t)]^T, \quad (t = 0,1,2,\cdots,n). \tag{3.3}$$

$x(t)$, $v_x(t)$, and $a_x(t)$ are the pen tip displacement, velocity, and acceleration in the horizontal (x) coordinate; $y(t)$, $v_y(t)$, and $a_y(t)$ represent the pen tip displacement, velocity, and acceleration in the vertical (y) coordinate; $z(t)$ represents the pressure signal. The total velocity and azimuth angle are obtained from $v_x(t)$ and $v_y(t)$. Similarly, the total acceleration is calculated from $a_x(t)$ and $a_y(t)$. They are summarized in equation 3.4.

$$\begin{cases} v(t) = \sqrt{v_x^2(t) + v_y^2(t)} \\ a(t) = \sqrt{a_x^2(t) + a_y^2(t)} \\ ang(t) = \arctan 2\left(v_x(t), v_y(t)\right) \end{cases}, \tag{3.4}$$

where $v(t)$, $a(t)$, and $ang(t)$ represent the total velocity, total acceleration and writing direction angle, respectively. The $ang(t)$ is calculated from the derivatives of $v_x(t)$ and $v_y(t)$. Hence, if required, equation 3.3 can be replaced by equation 3.5 as follows:

$$S'(t) = [x(t), y(t), z(t), v_x(t), v_y(t), a_x(t), a_y(t), v(t), a(t), ang(t)]^T, (t = 0,1,2,\cdots,n). \tag{3.5}$$

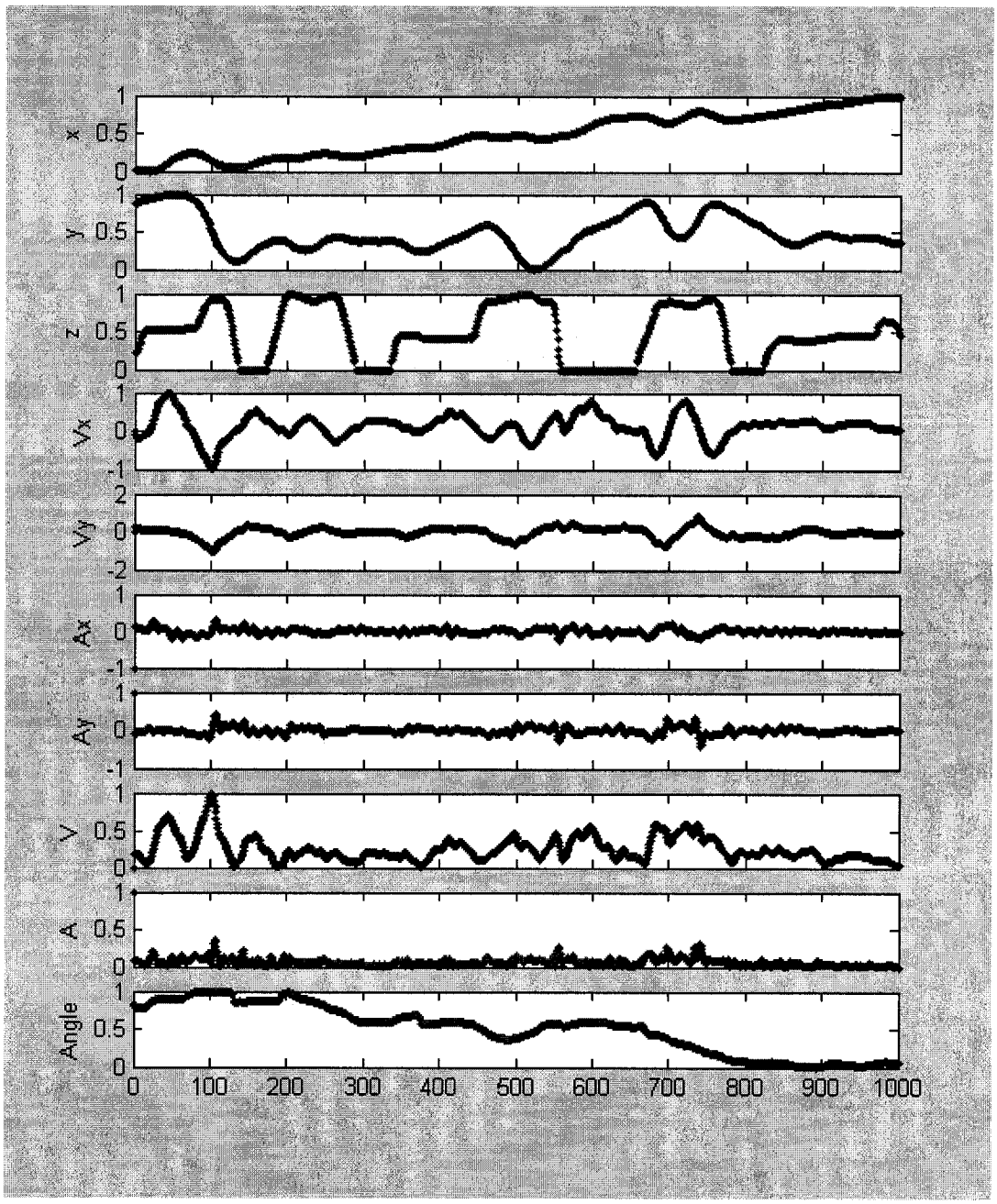
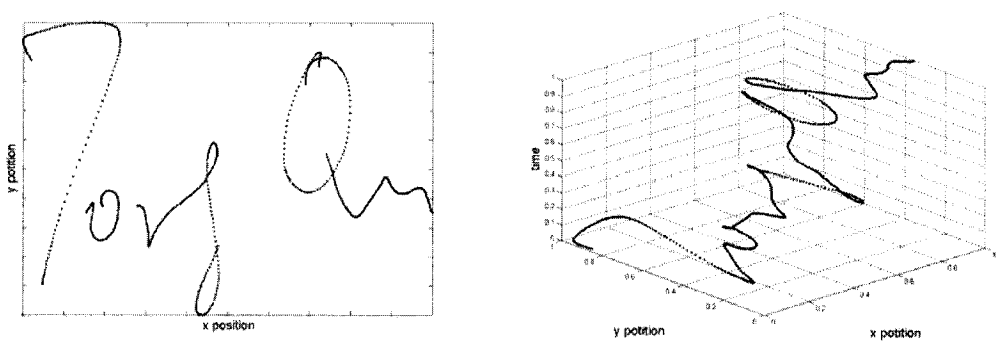


Figure 3.11 A sample signature represented by the dynamic information for a set of sampling points.

The components in the equation (3.5) constitute the dynamic signature. For an example signature, the components in equation 3.5 are plotted in Figure 3.11. The final data can be used to represent most of the effective dynamic information of the acquired digital signature.

If required, 2-D signature image can be reconstructed from the x and y position signals. It is also possible to create a 3-D representation of the signature by showing the time sequences. The 3-D signature not only contains position information, but also includes time information. An example for 2-D and 3-D signature are reconstructed and plotted in Figure 3.12.

Typically a signature is the writing of a person's name. Typically in a signature, the x values grow linearly with time with small variations while the y values show a more oscillatory variation with time, the y values become positive and negative many times during a signature. This can be observed in the Figure 3.11.



(a) (b)

Figure 3.12 A sample signature reconstructed from the components in equation 3.5. (a) 2-D signature, (b) 3-D signature.

CHAPTER 4

FEATURES EXTRACTION AND STROKE BASED ALGORITHM

In this chapter, the statistical features in signature verification are introduced. General feature extraction methods are classified and discussed. The characteristics of signature strokes are studied, and a stroke based feature extraction algorithm is developed. Finally, features selection is also discussed.

4.1 Statistical Features in Signature Verification

Features are symbolic or numeric entities that describe a pattern. For example, a feature for a static signature is the number of loops in the 2-D image, while a feature for a dynamic signature is the average writing speed.

According to Lee, individual's signatures are predefined and consistent [Lee92]. Although there will always be slight variations in a person's handwritten signatures, the consistency created by natural motion and practice over time creates a recognizable

pattern that makes the handwritten signature a natural for biometric identification [Lee92]. We are trying to find those consistent behavioural dynamic characteristics (to which we refer as features), which are inherent to a particular person. Such features can be used to identify genuine signatures from forgeries.

Lee noted that there exist remarkably consistent characteristics when a person repeats his/her signatures [Lee92], so a collection of parameter values can be computed and compared for the purpose of signature verification. These parameter values are sometimes called *statistical features* (or *statistical parameters*). Lee et al. proposed 42 features, some of which are listed below [Lee96]:

- Total time taken in writing the signature.
- Signature path length: displacement in the x and y directions and the total displacement.
- Signature accelerations: variations in horizontal and vertical accelerations, centripetal accelerations, tangential accelerations, total accelerations, as well as there average or root mean square (RMS) values.
- Pen-up time: total pen-up time or the ratio of pen-up time to total time.

Once a set of features has been selected, they can be used to represent the essential biometric characteristics of the original signature. Meantime, the other non-identifying information is ignored.

4.2 Classification of Feature Extraction Methods

Various features can be extracted from dynamic signatures. These features can be

classified in different ways.

The first way of classifying features is based on the measured signals and the measured parameters. The measured signals (i.e., position, velocity, pressure vs. time, etc. shown in Figure 4.1) can be represented by time domain functions whose values directly constitute the feature set (or feature vector). Measured parameters (such signing time, peak number, stroke sequencing, etc.) computed from the measured signals are another source of features. For example, the signing time for a person to sign his 5 samples could be 2.1, 2.4, 2.1, 2.2, 2.0 seconds, respectively. The value of signing time can be considered as a feature with mean of 2.16 seconds.

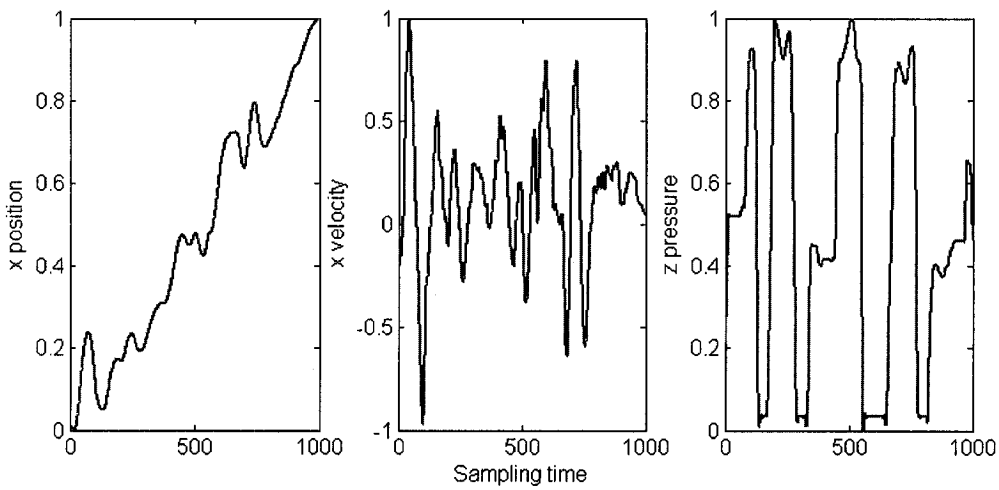


Figure 4.1 An example of complete position, velocity, and pressure signals as features.

Another type of feature classification is based on the feature's domain. There are several basic feature groups used as illustrated in Figure 4.2. Most of the available methods can be classified within time and frequency domains, etc. For example, one of

the frequency domain features can be consider as the fundamental frequency value for the signing movement process

Features can also be classified as global or local features. Global feature refer to the parameters corresponding to completed signals, such as average writing speed and total signing duration. Local features represent the local information of a signature, for example, the time between two peaks, and the average speed within a stroke.

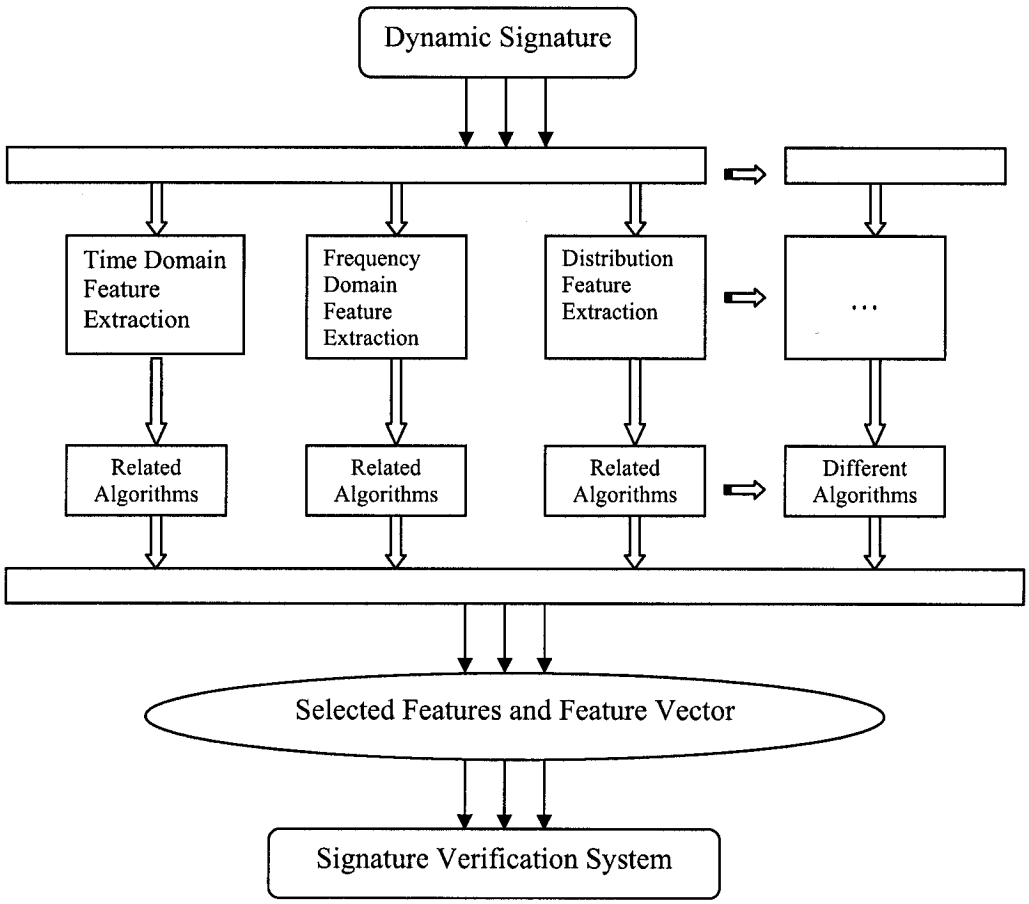


Figure 4.2 Several basic features groups in feature extraction.

4.3 Stroke Based Feature Extraction Algorithm

The generation of handwriting can be described as the vector summation of discontinuous strokes [Denier65]. In this sense, the stroke is the basic component of a signature. In this section, after an introduction to the characteristics of signature strokes, a stroke-based algorithm is developed for the purpose of dynamic signature verification.

4.3.1 Characteristics of Signature Strokes

A signature may be considered as a sequence of strokes. Dimauro et al. define strokes as "a sequence of fundamental components, delimited by abrupt interruptions" [Dimauro94]. The dynamic characteristics for creating a stroke may exhibit in different channels such as velocity and pressure etc. This can be illustrated by drawing a simple dash stroke, which is drawn from a small x value to a large x value. The position, velocity and pressure signals corresponding to this example stroke are shown in Figure 4.3. As expected, the x position signal for this stroke increases smoothly in the x coordinate. In the velocity channel, the v_x velocity values grow from zero and reach a peak stage somewhere mid-way then decline to zero. In the pressure channel, the z pressure values increase steadily until reaching a single peak, and after that, drop down sharply to zero. The figure shows normalized position and pressure signals while the velocity signals maintain the original values. Similarly, another more complex circle stroke example is shown in Figure 4.4. It shows that the characteristics of position, velocity and pressure signals vary reasonably according to the creating process of the circle stroke

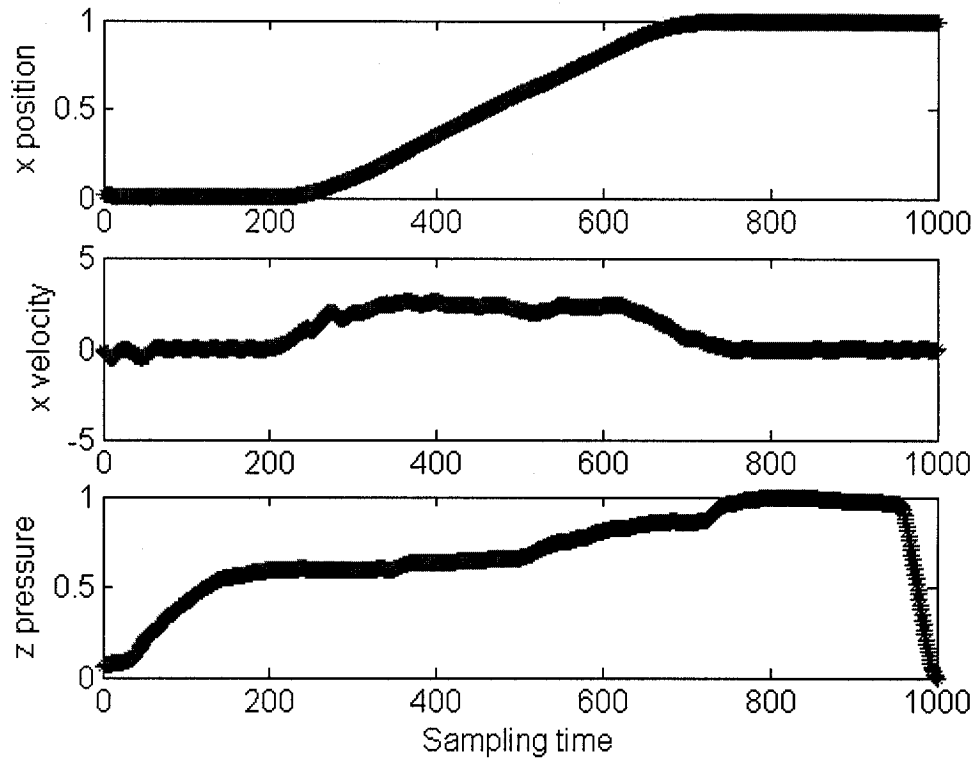


Figure 4.3 A dash stroke example.

Given the dynamics of signature writing, we are interested in how a falsifier forges a signature and how difficult is it for a forger to produce a good forgery. Brault noted that it is believed that a forger cannot write another person's signature in a ballistic motion without a lot of practice and therefore producing good forgeries is never going to be easy [Brault93]. However it is also true that some signatures lend themselves more easily to forgery than others.

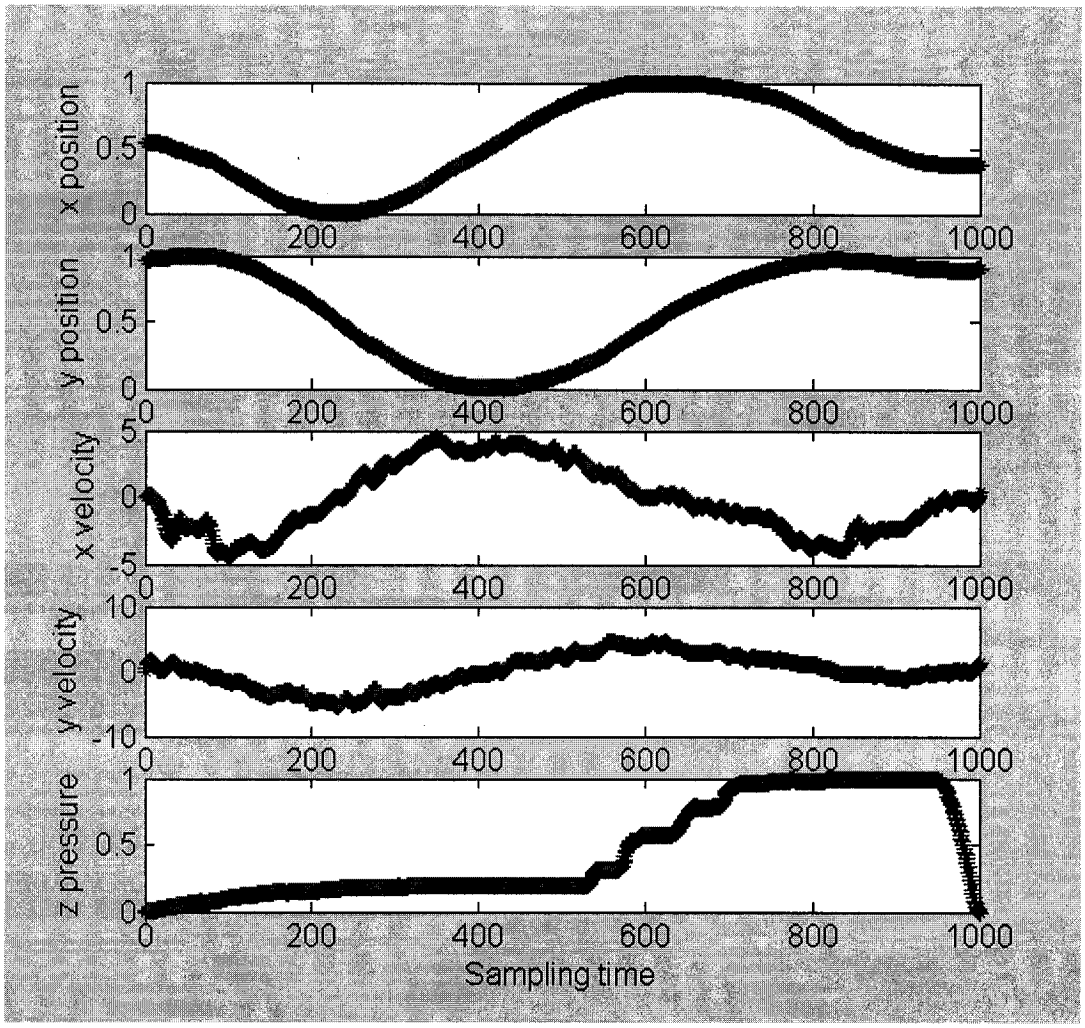


Figure 4.4 A circle stroke example.

Brault and Plamondon studied the problem of forging a signature and estimated the intrinsic risk of a signature being forged. They noted that humans can only remember about seven variations of a signature that is being forged [Brault89], [Brault93]. A process of minimization or recording of information that needs to be remembered takes place. For example, a forger might recode information about the signature of Jason

Smith by first remembering the name and then remembering that Jason Smith's signature has a taller J than the forger would normally write and a rounder S etc.

A deep study of the dynamic characteristics of signature strokes in the literature shows that strokes may contain very important consistent behavioural information, which is inherent to a particular person. This promotes us to develop a stroke-based algorithm to capture useful behavioural features within dynamic signatures. These extracted features can then be applied to design a dynamic signature verification system.

4.3.2 Stroke Identification and Significant Stroke

Plamondon noted that "the major problem with character segmentation is the difficulty of determining the beginning and ending of individual characters" [Plamon00]. Although there is no commonly adequate method to identify strokes for most applications, there are still some effective and simple techniques for current *identification of stroke boundaries*. During signing, individual strokes can be distinguished by finding the points where there is a

1) decrease in pen tip pressure (close to zero),

2) decrease in pen velocity (close to zero), and

3) rapid change in pen angle.

These points imply some internal characteristics of the pressure/velocity/angle sequencing. Therefore, they can be used to locate the strokes for the dynamic signature. In order to show the effectiveness of the above method, let us analyze a simple character first. We select the letter '*T*' since it only contains two dash strokes. Figure 4.5 shows the two dimensional reconstruction of the letter '*T*' in spatial domain.

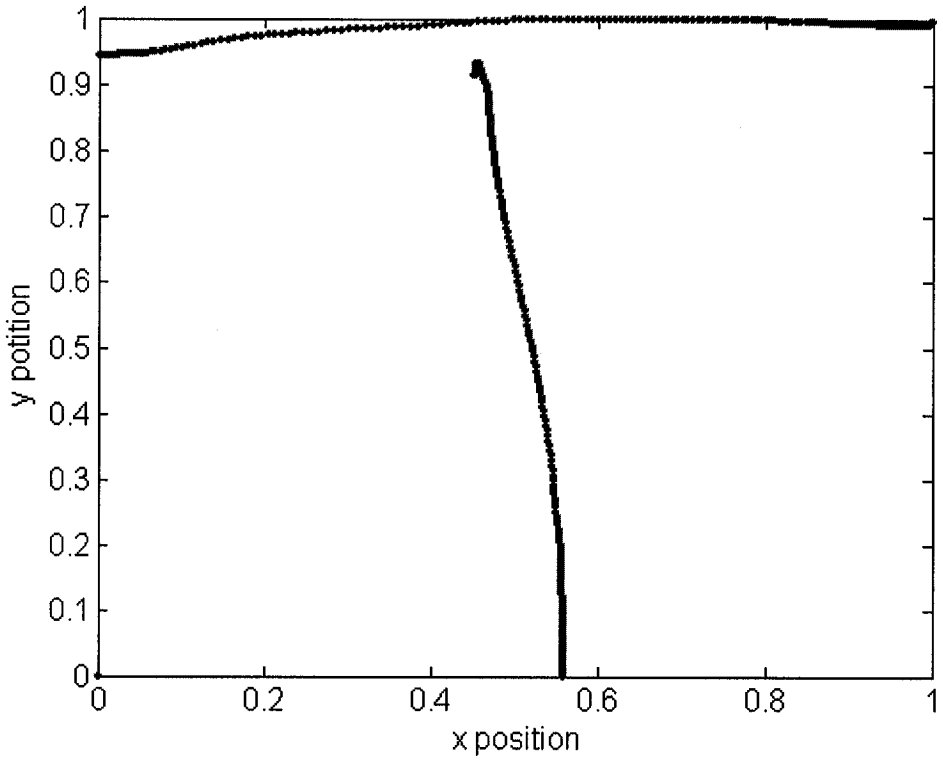


Figure 4.5 2-dimensional figure for letter '*T*'.

The pressure, velocity and angle signals for letter '*T*' are plotted and compared in Figure 4.6. Corresponding to the horizontal dash in the letter '*T*', the pressure values increases from zero; then the values grow and reach a peak; then the values drop down to zero. When the pen tip is lifted from the tablet, the pressure values are consistently close to zero. When the pen tip touches the tablet surface and begins to write the vertical dash, the pressure values increase again from zero and grow to the maximum peak value; after that, they drop down to zero which represents the end of the vertical dash. So the two dash strokes for the letter '*T*' can be separated by detecting the zero pressure region located between the two pressure signal strokes (as shown in Figure 4.6). Similarly, the

two velocity strokes are identified with a similar method to the one used for pressure (the velocity values below 5% of the maximum velocity are set to zero to clarify the figure). In addition, relatively rapid changes in the pen angle signal can also be observed at the beginning and the end of the two dash strokes. So this characteristic can be easily detected and used in angle stroke identification.

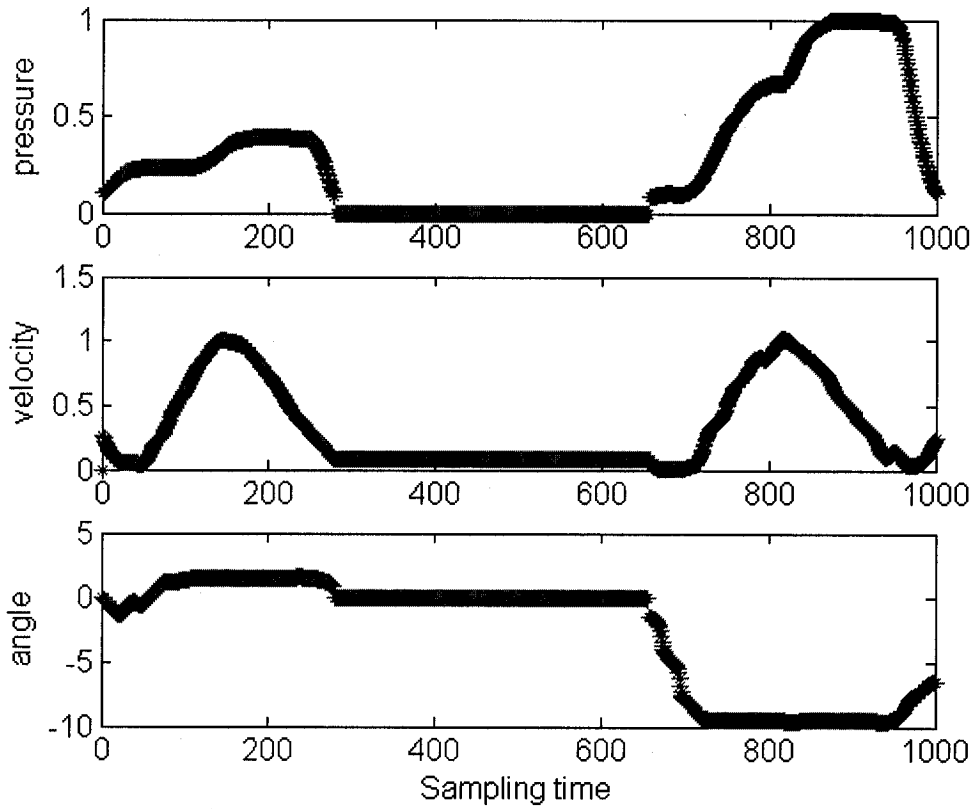


Figure 4.6 Pressure, velocity and angle signals for letter '*T*'.

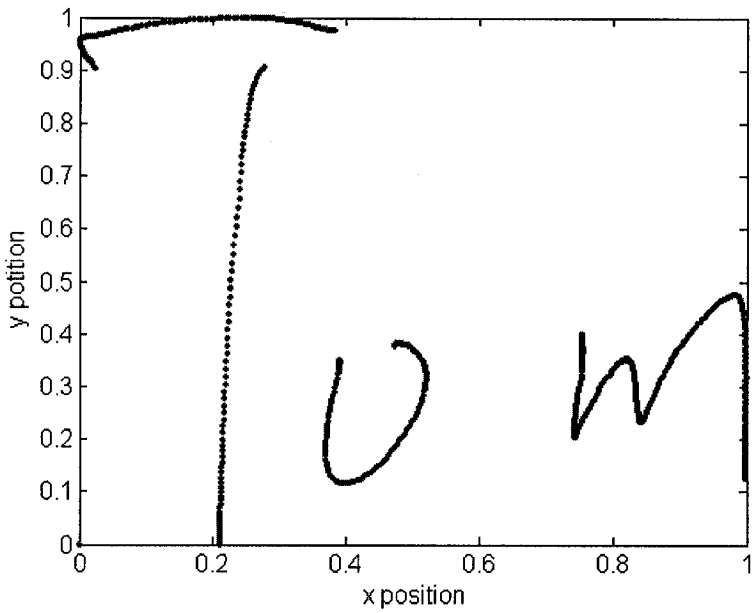


Figure 4.7 2-dimensional figure for a sample signature '*Tom*'.

Furthermore, the stroke boundaries of a sample signature '*Tom*' are identified based on above described methods. The 2-dimensional signature reconstruction in Figure 4.7 shows that this signature should have four strokes: two dashes, one circle and one 'm' character. The corresponding pressure, velocity and angle signals are plotted in Figure 4.8. Applying the above described methods for stroke boundary identification, the letter '*T*' is easy to identify as two strokes, and the letter 'o' is judged as one stroke successfully. However, for the letter 'm', it is clearly identified as one stroke in pressure signal, while it is more likely to be judged as the combination of some sub-strokes in velocity and angle signals. Since there are several minima close to zero in the velocity signal and several rapid changes in the angle signal. This implies that the pressure, velocity and angle signals are all useful in stroke boundary identification while they have

different advantages and disadvantages for different signatures. It is recommended to use the pressure and velocity signals rather than the angle to identify stroke boundaries because rapid changes are more difficult to be detected. In addition, these methods can also be combined together for the stroke boundary identification.

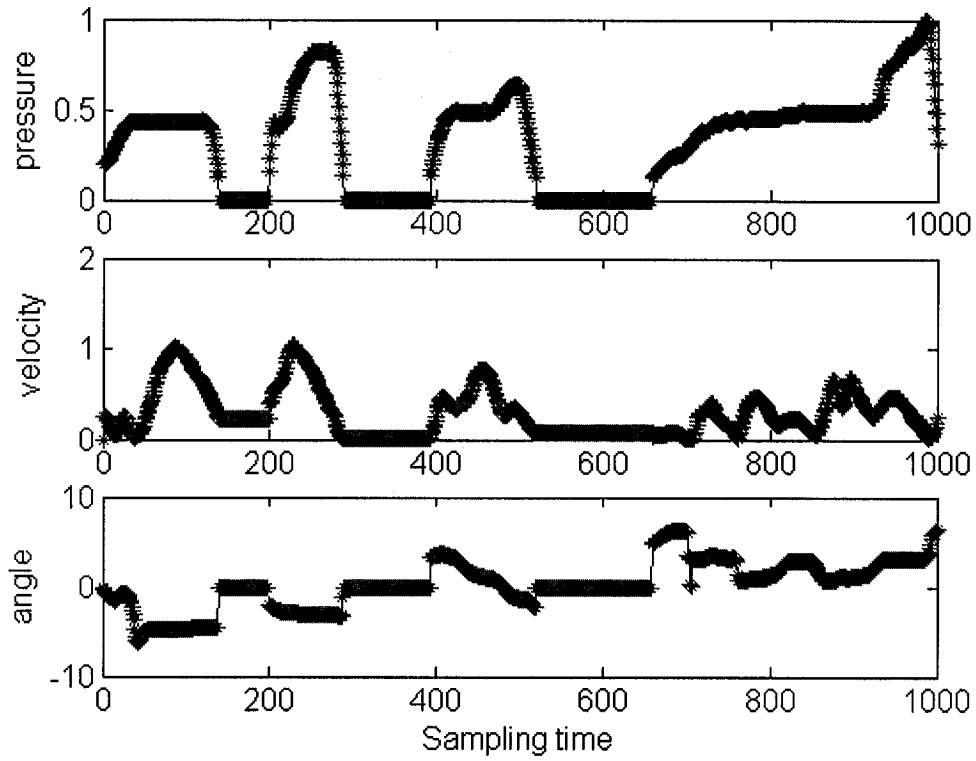


Figure 4.8 Pressure, velocity and angle signals for a sample signature '*Tom*'.

4.3.3 Stroke Alignment

In general, one signature needs to be compared to other signatures in the signature verification. The pressure, velocity, and angle signals of three sample signatures signed by the same individual are illustrated and compared in Figure 4.9.

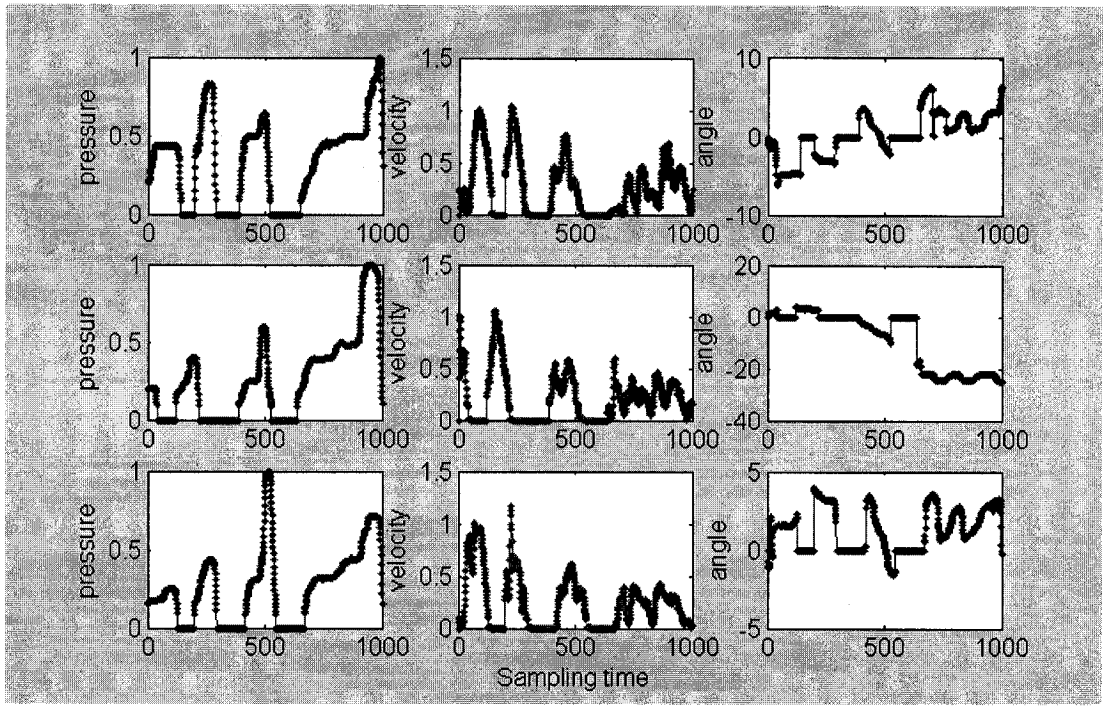


Figure 4.9 Comparison of three sample signatures '*Tom*' signed by the same person.

Table 4.1 Pressure stroke segments for the signatures in Figure 4.9

Stroke number	1st sample signature			2nd sample signature			3rd sample signature		
	Start point	End point	Stroke length	Start point	End point	Length	Start point	End point	Stroke length
1st	1	141	140	1	103	102	1	128	127
2nd	197	289	92	160	253	93	198	294	96
3rd	390	521	131	402	542	140	417	548	131
4th	649	1000	351	652	1000	348	669	1000	331

According to the stroke identification methods in the last section, four pressure signal strokes are identified for all the three sample signatures in Figure 4.9. The related stroke boundaries and lengths are listed in Table 4.1. Since the time interval between any sampling points is the same, so we use the number sampling points within a stroke

to represent the length of that stroke. Due to the different lengths for different strokes, the elastic alignments are to be conducted before stroke comparisons is done. For example, all the pressure strokes can be stretched to a fixed length with 250 sampling points. This can be done by applying spline interpolation (using the spline function in Matlab). After such elastic stroke alignment, the pressure strokes are plotted and sorted sequentially as seen in Figure 4.10. The 1st, 2nd, 3rd and 4th strokes correspond to the strokes located in the regions of [1,250], [251,500], [501,750] and [751,100], respectively.

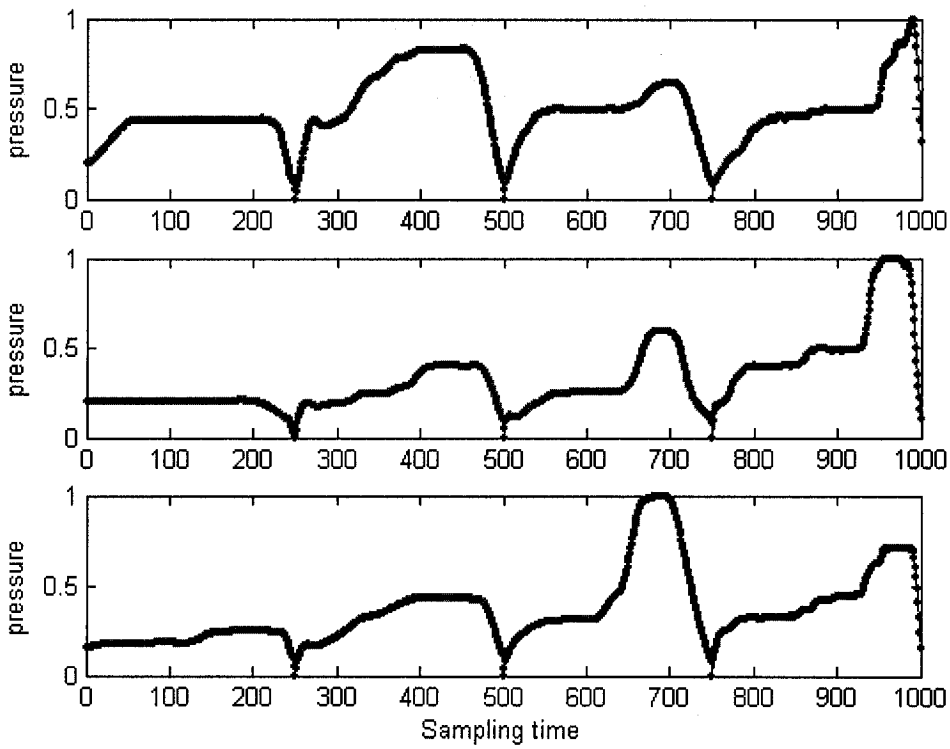


Figure 4.10 Stroke alignment for the pressure signals in Figure 4.9.

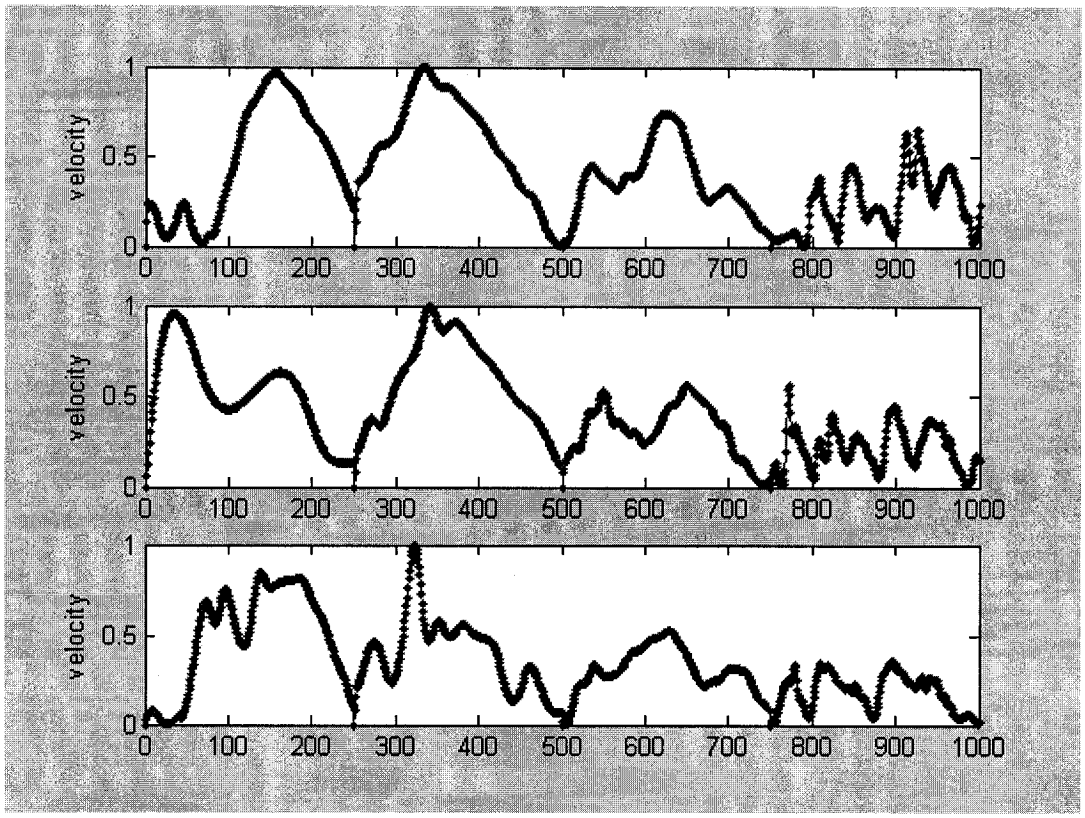


Figure 4.11 Stroke alignment for the velocity signals in Figure 4.9.

Table 4.2 Velocity stroke segments for the signatures in Figure 4.10

Stroke number	1st sample signature			2nd sample signature			3rd sample signature		
	Start point	End point	Stroke length	Start point	End point	Stroke Length	Start point	End point	Stroke Length
1st	1	140	139	1	40	39	1	127	126
2nd	197	289	92	121	218	97	198	294	96
3rd	390	521	131	386	528	142	417	548	131
4th	649	1000	351	637	1000	363	669	1000	331

Similarly, this alignment operation is also applicable for the velocity signals, etc. After the alignment operation, the velocity strokes for the same three sample signatures

are illustrated in Figure 4.11, and the related stroke boundaries and lengths are listed in Table 4.2.

4.3.4 Stroke Matching and Significant Stroke

In order to find the corresponding stroke pairs, stroke cross-correlation coefficients (for the pressure strokes in Figure 4.10) are calculated and illustrated in Table 4.3. The auto-correlation coefficients are not computed so the right box of Table 4.3 is blank.

Table 4.3 Corresponding pressure stroke comparison by computing cross-correlation

	p_1^1	p_1^2	p_1^3	p_1^4	p_2^1	p_2^2	p_2^3	p_2^4
p_2^1	0.8886	0.3287	0.4328	0.0006				
p_2^2	0.5863	0.9176	0.8601	0.2243				
p_2^3	0.5879	0.0943	0.7655	0.1302				
p_2^4	0.2099	0.4184	0.4270	0.8748				
p_3^1	0.8214	0.1535	0.7718	0.1190	0.8629	0.9135	0.7590	0.6607
p_3^2	0.6981	0.8514	0.9434	0.2182	0.1561	0.9289	0.7668	0.6264
p_3^3	0.5302	0.1229	0.8262	0.1107	0.1868	0.9210	0.8618	0.5564
p_3^4	0.1049	0.5231	0.4023	0.8249	0.5157	0.7092	0.4977	0.8540

Table 4.4 Average cross-correlation values for the corresponding pressure strokes

	1^{st} stroke	2^{nd} stroke	3^{rd} stroke	4^{th} stroke
Average values	0.8576	0.8993	0.8178	0.8512

The p_i^j represents the j^{th} pressure stroke in the i^{th} signature. The high correlation values are highlighted which refer to the corresponding strokes. In this example, the j^{th}

stroke of the i^{th} signature matches with the j^{th} stroke of the other two signatures. For instance, the p_1^1, p_2^1, and p_3^1 (the 1^{st} stroke of the three sample signatures) match each other and their average cross-correlation values equal to

$$\frac{0.8886 + 0.8214 + 0.8629}{2} = 0.8576.$$

In similar, all the average cross-correlation values for the j^{th} are computed and listed in Table 4.3. It shows that the average correlation values between the 2^{nd} strokes of the three sample signatures are the largest. It implies that the consistency of the 2^{nd} pressure stroke is relatively higher than other strokes when the signer repeating his/her signatures. If all the strokes carry the same amount of the signer's internal characteristic, the 2^{nd} pressure stroke should have higher ability to keep such characteristic. The above mentioned 2^{nd} pressure stroke also has relatively less variation over time than other strokes. Therefore it is easier to capture the signer's internal characteristic in the 2^{nd} pressure stroke due to its greater robustness and reduced variation. It is convenient to name such kind of stroke as a ***significant stroke*** (or significant stroke pair). For most individuals, a significant stroke can be distinguished by the maximum corresponding stroke cross-correlation of the reference signatures.

However, for some individuals, there still exist difficulties to identify the significant stroke, if computing the correlation does not offer sufficient information to identify the significant stroke. For instance, it is possible that a short stroke correlates well with a non-corresponding long stroke after they are stretched to the same fixed length. In such a case, the corresponding significant stroke still can be identified correctly if taking into

account the effect of the length of the strokes. We therefore define two strokes to have a high similarity if they satisfy two conditions: 1) their cross-correlation coefficient value is high; and 2) their sampling time duration difference is small (as their length difference is small). The stroke time duration corresponds to the stroke length and some stroke length examples are shown in Table 4.1. The product of the cross-correlation coefficient and the stroke length can be used to represent the similarity of two strokes. Consider two strokes of length l_1 and l_2. Let c_{12} represent the correlation coefficient between the two strokes, and set length factor k_{12} to represent the time duration condition and it is calculated according to equation 4.1.

$$k_{12} = \frac{l_1}{|l_1 - l_2|}. \tag{4.1}$$

The product of c_{12} and k_{12} can be used as an indicator to detect the similarity between two strokes. The higher the value of the product $(c_{12} \times k_{12})$, the higher the similarity between them. For example, when comparing the v_1^2 stroke (the 2nd stroke of the 1st signature) with all the 4 strokes (v_2^1, v_2^2, v_2^3, and v_2^4) of the 2nd signature in Figure 4.11, the corresponding indicators $(c_{12} \times k_{12})$ are computed and listed in Table 4.4. Taking the length factors k_{12} into consideration, the highest significant stroke indicator $(c_{12} \times k_{12})$ value of 14.790 indicates the significant stroke. Although v_1^2 and v_2^2 do not have the highest correlation coefficient, their length factor is the highest (18.4162). This additional information helps to judge the $v_1^2 \sim v_2^2$ pair as significant stroke pair, since its indicator value is much bigger than the others.

Table 4.5 Stroke comparison based on both correlation and length factor for velocity strokes in Figure 4.11

Stroke ~ stroke pairs	c_{12}	k_{12}	Indicator $= c_{12} \times k_{12}$
$v_1^2 \sim v_2^1$	0.0604	1.7358	0.1048
$v_1^2 \sim v_2^2$	0.8031	18.4162	14.790
$v_1^2 \sim v_2^3$	0.5918	1.8399	1.0888
$v_1^2 \sim v_2^4$	0.9550	0.6246	0.5965

There are 5 genuine signatures and 2 forgeries are compared in Figure 4.12. Visually, there often exists high similarity between the corresponding strokes of reference signatures, but much lower similarity between the strokes of genuine signatures and that of forgeries. Between each pair of signatures, the correlation comparisons are conducted for strokes.

For the 5 references, different strokes exhibit different variations among the repetitions. The correlation coefficients between the strokes for all the 5 genuine references were calculated and illustrated in Figure 4.12. In this example, the 4^{th}–4^{th} stroke pairs have the highest correlation. Different individuals may have different significant strokes for their dynamic signatures.

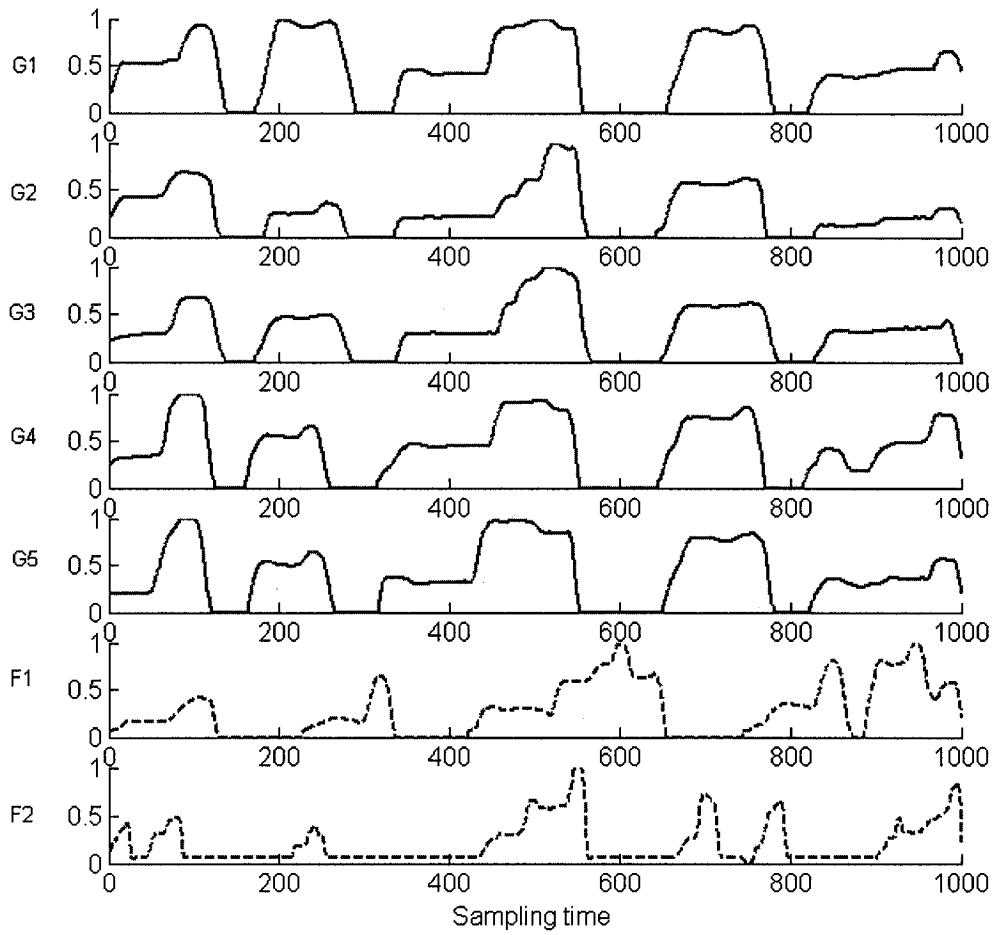


Figure 4.12 Comparison of pressure stroke between genuine signatures and forgeries. (Stroke-based normalized pressure versus time of 5 genuine signatures and 2 forgeries. G1, G2, G3, G4, and G5 represent the pressure signals of the genuine signature while F1 and F2 refer to those of forgeries. The 4^{th} stroke in each genuine signature is the significant stroke.)

For the examples in Figure 4.12, the 4^{th} stroke is the significant stroke and its correlation coefficient values are listed in Table 4.6 for the genuine-genuine pairs and

the forgery-genuine pairs. For the genuine-genuine pairs, the significant stroke's correlation values (e.g. 0.9199 for G1-G2 pair) are higher than those of genuine-forgery pairs (e.g. 0.5561 for G1-F1 pair). The significant stroke's average correlation value for all the genuine-genuine pairs should be higher than those of the genuine-forgery pairs. In this case, for all the genuine-genuine pairs, the significant stroke's average correlation value is 0.9670, which is higher than that of genuine-forgery pairs. We select the mean significant stroke of all the references as a feature in the template. If F1 is a test signature, the 4^{th} stroke's average correlation value between F1 and all the references is only 0.6302 (0.1706 for F2, both are far from the 0.9670).

The correlation value and stroke length for the significant stroke can be extracted as features for identifying genuine signatures against forgeries. In addition, we also use other features related to significant strokes such as stroke length, and stroke duration time. It noted that different signals (e.g. velocity signal) may indicate different significant strokes for the same user.

Table 4.6 4^{th} stroke's correlation between the signatures in Figure 4.12

	G1	G2	G3	G4	G5
G1	1	0.9199	0.9830	0.9575	0.9846
G2	0.9199	1	0.9595	0.9678	0.9643
G3	0.9830	0.9595	1	0.9612	0.9834
G4	0.9575	0.9678	0.9612	1	0.9889
G5	0.9846	0.9643	0.9834	0.9889	1
F1	0.5561	0.6729	0.5573	0.7267	0.6379
F2	0.1508	0.1454	0.0815	0.2807	0.1946

4.3.5 Stroke Based Feature Extraction algorithm

Based on the above presented analysis and discussion, the steps of a stroke based feature extraction algorithm can be summarized as follows:

Step 1. Identify the stroke boundaries based on pressure, velocity or angle signals. Distinguish strokes by finding the points where there is a 1) decrease in pen tip pressure (close to zero); 2) decrease in pen velocity (close to zero); and 3) rapid change in pen angle.

Step 2. Conduct the stroke alignment for the purpose of stroke comparison.

Step 3. Calculate stroke correlation coefficients and find the corresponding strokes which match each other.

Step 4. Find significant strokes based on pressure, velocity or angle signals by computing and finding the maximum correlation match score.

Step 5. Extract features from the significant strokes or other strokes.

According to the presented steps of the algorithm presented above, various features can be extracted such as: 1) correlation coefficient for the pressure/velocity/angle significant strokes (genuine-genuine pairs and genuine-forgery pairs); 2) pressure/velocity/angle significant stroke duration; 3) average/maximum velocity for a significant stroke; 4) variance of the pressure/velocity/angle significant stroke; 5) stroke numbers; 6) the time duration for the first stroke of any signature.

4.4 Feature Selection

Besides the stroke based features described in the last section, some other features are also useful for the presented signature verification system. Some of the effective features that can be calculated from the dynamic signature data are:

- Total time during the signing process
- Pen-up time
- Average velocity over x and over y
- Average writing speed (absolute velocity)
- Variance of pressure signal (in 10 sliding window)
- Pressure changing in 10 sliding windows
- Number of pen ups and downs
- Direction at first pen down, first pen up
- Signature length
- Time of second pen down
- Number of sign changes in the x and y velocities and x and y accelerations
- Number of zero values in the x and y accelerations
- Mean or variance of the x and y displacement signal in 10 or 100 sliding windows

The issue of how many features a method needs to use in order to obtain reliable dynamic signature verification is a very difficult one. There is always a temptation to include more and more features in a method in the hope of improving reliability, for example, Parks et. al. have proposed more than 90 features [Parks85]. However, Lee noted that using many features is unlikely to lead to high performance and may lead to

some difficulties [Lee92]. For example, if a method uses many features, the storage needed for reference signatures is going to be relatively large and may exceed the storage capacity of small devices such as a credit card. Lee also noted that although a large number of features are considered important, it is acceptable to ignore several of them while comparing the test signature to the reference signature [Lee92]. Given that the reference signature is based on a set of sample signatures, and for each element of the set of selected features the mean and standard deviation of the feature values have been computed, the reference signature can then be represented with two vectors: a vector of the means of the features' values of the sample signatures and a vector of the standard deviations. In order to obtain good estimates of the mean and the standard deviations of the features' values of the genuine signatures population it is necessary to have several, perhaps a minimum of three or five, sample signatures. A larger set of sample signatures is likely to lead to a better reference signature and therefore better results but it is recognized that this is not always possible [Lee92].

This chapter presents a stroke-based algorithm for feature extraction and signature verification. After the statistical features and some general feature extraction methods have been introduced, a novel stroke feature extraction algorithm has been developed according to the following steps: identification of stroke boundaries, stroke alignment, stroke correspondence matching and significant stroke feature extractions.

CHAPTER 5

SIGNATURE VERIFICATION

Signature verification is used to discriminate genuine signatures against forgeries. A binary signature classifier is introduced in this chapter.

Based on the observations that most of the feature values tend to be clustered about a mean value with a certain variance that is characteristic to a certain user, it is natural to use Gaussian density to model the distributions of these features. For instance, the distribution of the average writing speed for $N = 40$ signatures of the same signer is illustrated in Figure 5.1. According to Kiran, the unbiased estimator for the mean and variance is [Kiran01],

$$\mu_i = \sum_{j=1}^{N} \frac{X_j}{N}, \tag{5.1}$$

and the estimate for the variance is,

$$Var_i = \sum_{j=1}^{N} \frac{(X_j - \mu)^2}{N-1}. \tag{5.2}$$

Where X_j the feature value is, and i varies from 1 to N. And, i represents the counting number for signatures; j represents the counting feature number for a given signature. Thus, for a given user, (μ_i, Var_i) is the mean and variance which describe the specific feature i. For a m-features system we have: (μ_1, Var_1), (μ_2, Var_2), (μ_3, Var_3),... , (μ_m, Var_m) pair values to be computed for each user. When a person's authenticity is to be verified, the set of mean and variance pair reference values corresponding to the user are used. In this pair-based features approach, the template is represented by both the vector of the means of the features' values of the reference signatures and the vector of the standard deviations.

The signature verification includes two processes: 1) constructing the reference signature template for each user and 2) verifying an unknown signature. For the first process, a set of reference genuine signatures is acquired at first, then, they are represented as a signature template in the feature space. Since not all the features will be used for constructing the template, so only some features are selected during this process and useful pattern are found for each particular signer. For the second process, some unknown signatures (including both genuine signatures and forgeries) are compared to the signature template, and the system performance is evaluated based on the calculated false reject rate and false accept rate.

A signature classifier identifies genuine signatures against forgeries. The basic mechanism is to compare the test signature to the reference template and judge the authentication results. Our proposed signature verification system uses match scores to

express the similarity between a test signature and a template. The higher the score, the higher is the similarity between them. The test signature is authenticated if the score is higher than a specific threshold. Signature verification accounts for the similarity in signatures produced by the same user, but needs to allow for certain variability [Lee92]. According to the equations (5.1, 5.2), an unbiased estimator for the mean and variance will converge to the true mean and variance of a feature, by adding the number of reference signatures (N), the experimental mean (μ_i) and the experimental variance (Var_i). There is a trade off between N and the accuracy of the experimental mean and variance.

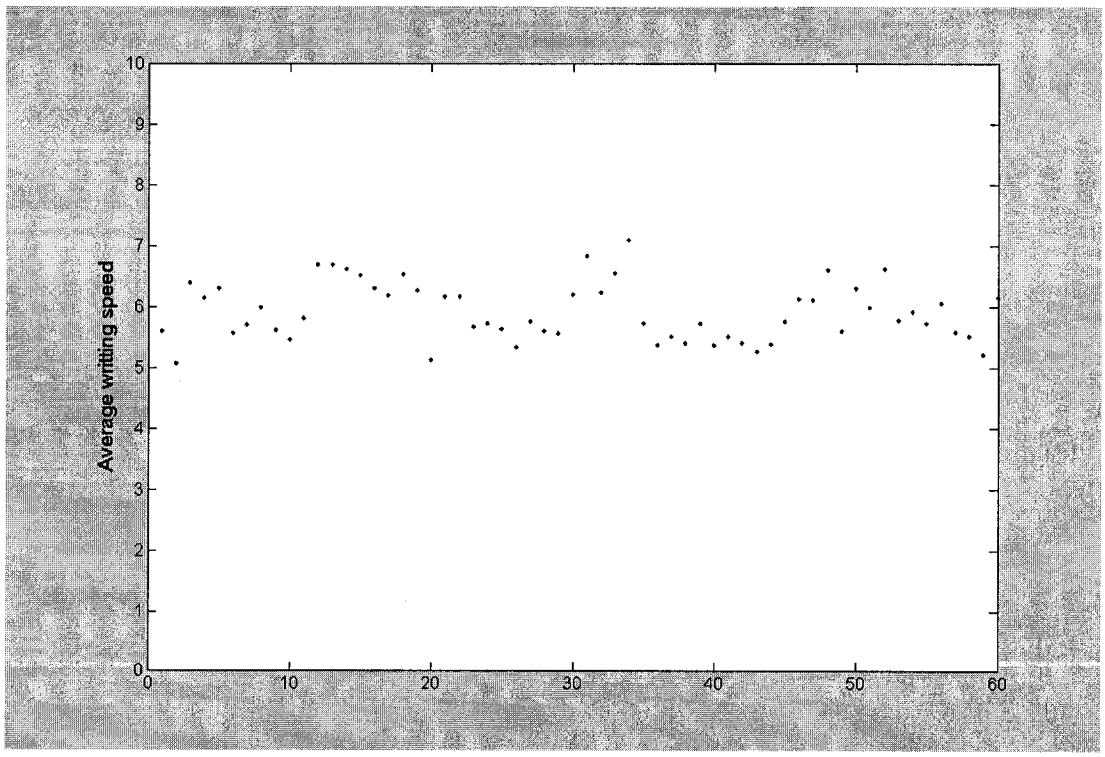


Figure 5.1 Average writing speed for a set of signatures.

If the test feature value falls within a given threshold range, the algorithm will then decide that the used test feature match the template. For a person whose signature is constant, the threshold can be kept low, and the variations of subsequent signatures are expected to be small. For higher variations of the repetitions, a higher threshold is required.

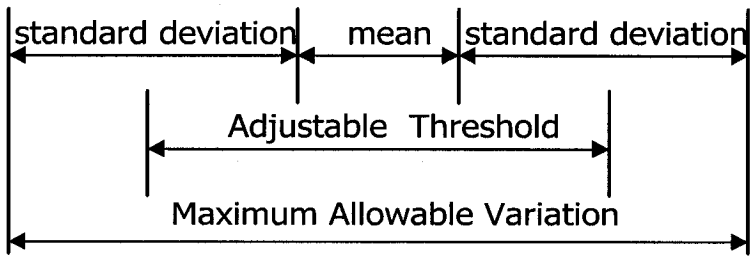


Figure 5.2 Diagram of threshold adjustment for an example feature.

The threshold value is adjustable and can be selected independently for each given user and feature. For instance, the experimental mean, the standard deviation, and the range of the adjustable threshold for an example feature are illustrated in Figure 5.2. If the threshold is set to $\sigma/2$, the probability of the feature value falling in the interval $[\mu-\sigma/2, \mu+\sigma/2]$ is 38%; if set σ as threshold, the probability falling in the interval $[\mu-\sigma, \mu+\sigma]$ is 68%; if use 2σ as threshold, the probability of the feature value falling in the interval $[\mu-2\sigma, \mu+2\sigma]$ is 95%.

For simplification, each feature is represented as a binary variable with two possible values, True or False. In order to illustrate this classification in a visual way, we use "1" to represent True and "0" to represent False as shown in Figure 5.3. (The distribution in Figure 5.3 is not a real one but a pseudo one to show the classification. For example, if a feature of an unknown signature falls into $[\mu-2\sigma, \mu+2\sigma]$, this feature will be considered

as true and will be assigned the value "1" as match score, otherwise, it is considered false and will be given a "0" score. All the selected features will be evaluated according to the same process and the entire accumulated value will be computed by adding the assigned value for each feature.

Such a binary signature classifier is used to verify the identity of an unknown user. For each feature value of the test signature, the system checks to see if it falls in the allowed range for that reference feature. For a given threshold, the FRR and FAR values can be computed. The threshold also varies according to the requirements of desired FRR and FAR level.

For *m*-features based system, each feature of the test signature is compared to the corresponding feature of the reference template. Each feature has an allowed range of authentication as shown in Figure 5.2. The signature classifier discriminates the genuine signature against the forgeries by evaluating the entire accumulated value in the assignment of a percent match of the test signature compared to the signature template.

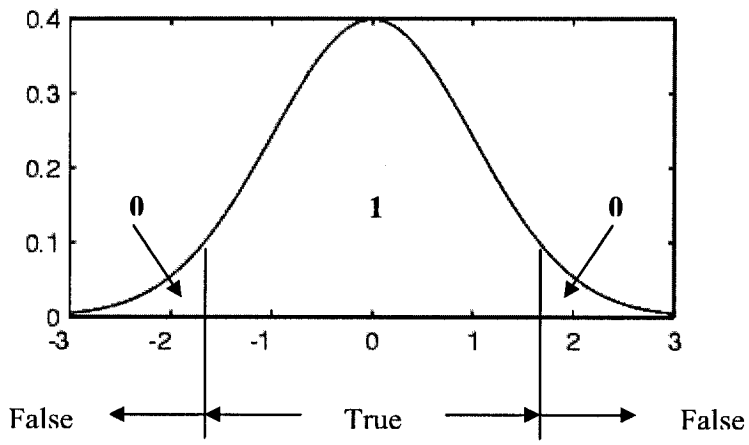


Figure 5.3 Binary representation for a feature value (the feature value is assigned a "0" and "1" if it exists in True or False region. The distribution curve is a pseudo one).

CHAPTER 6

IMPLEMENTATION AND EXPERIMENTS

In this chapter, the proposed stroke based feature extraction algorithm is applied in the process of dynamic signature verification. Both fixed and variable threshold experiments have been conducted to compute the FRR and FAR data.

6.1 Experimental Setup and Interface Design

It is necessary to select some features to build a dynamic signature verification system. The preliminary selection can be conducted by observing the ratios of the standard deviation to the mean for each feature and counting the effect of each feature type. The performance of the system can then be compared by using different features. In the fixed threshold experiment, a predefined threshold is used, and the FRR, FAR and ERR are computed. The comparison between the stroke based features and the other features is also conducted. In the variable thresholds experiment, the FRR and FAR are

calculated for different thresholds, the data are used for plotting an error tradeoffs curve.

In order to conduct the experiment more efficiently, a graphical user interface is designed with Matlab. It is used to control the signature pre-processing, feature extraction and signature classifiers in an easy way. An example of the user interface is shown in Figure 6.1.

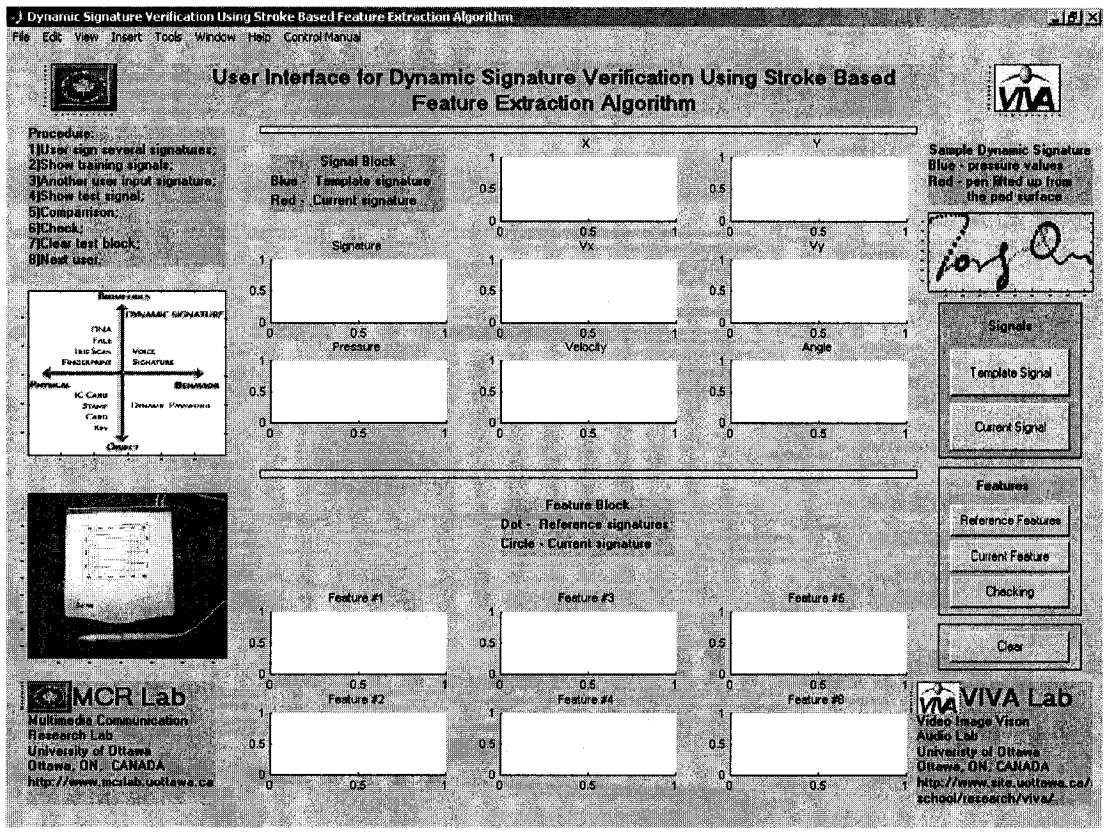


Figure 6.1 A graphical user interface for signature verification.

The user interface consists of two parts: block of dynamic signature representation and block of signature comparison in feature space. The signal block includes 8 windows which are used to display and compare dynamic signatures. The 8 windows

will represent the 2-dimensional image reconstruction of the signature, pressure, position, velocity, acceleration, and angle signals. The feature block includes 6 windows. The comparison between the test signature and corresponding template are illustrated in these windows in feature space.

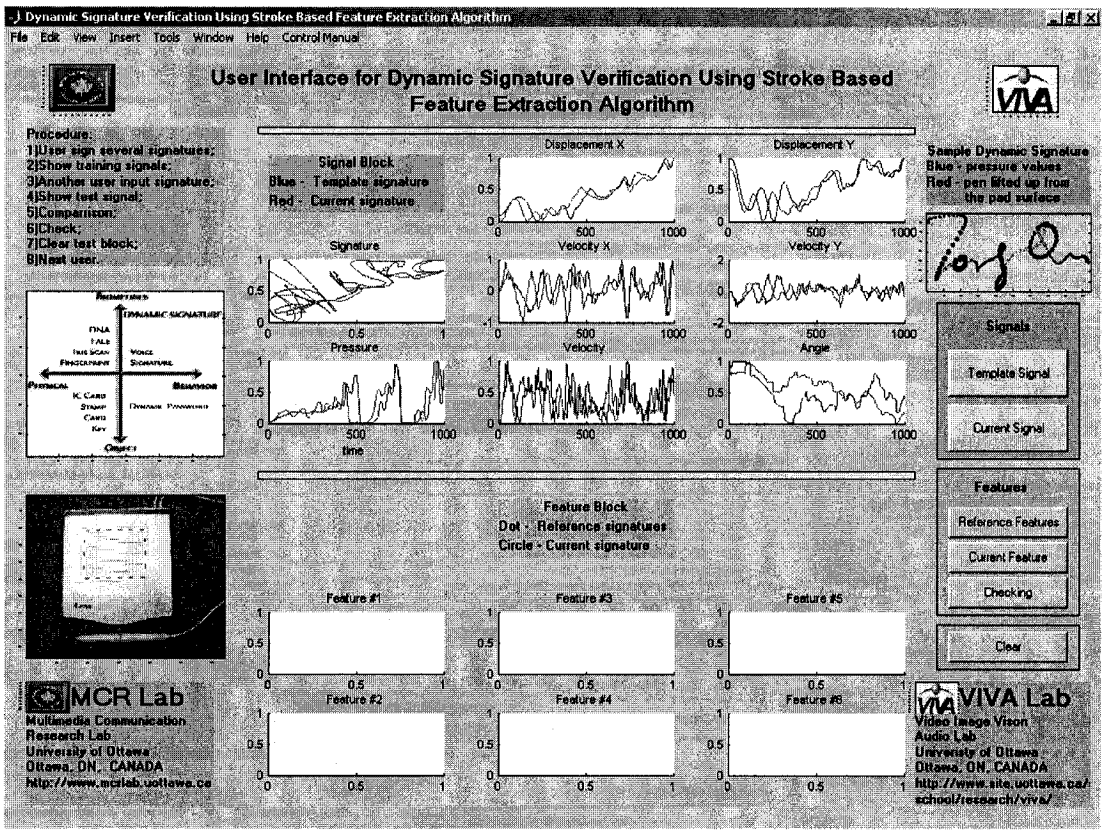


Figure 6.2 Comparison of the test and template signatures in the signal block.

To verify the identity of an unknown user (a genuine user or a forger), he/she first selects a template signature to imitate by clicking on the *Template Signal* button. When clicking on the *Current Signal* button, the representations for the current testing dynamic signature are compared directly and visually with those of the template in the 8 windows

of the signal block. The signals of the current testing signature are plotted in red and the corresponding signals of the template signature are plotted in blue as shown in Figure 6.2.

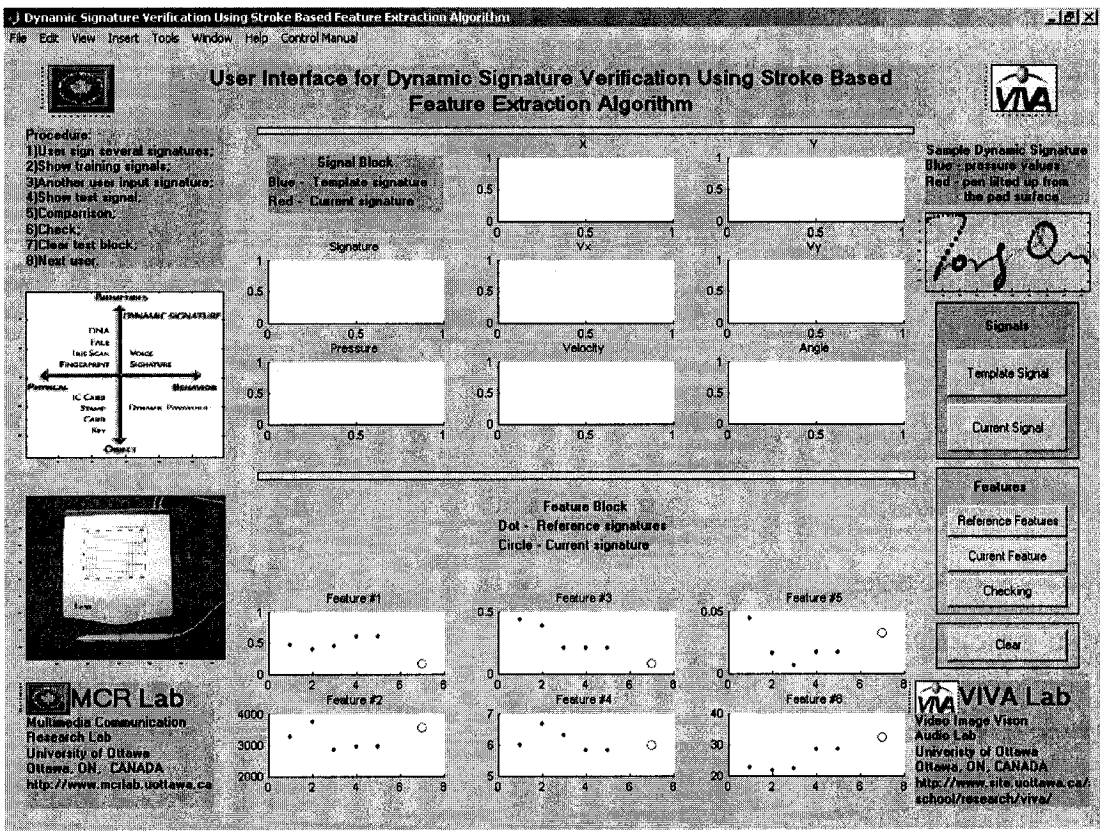


Figure 6.3 Comparison of feature value between current test signature and reference signatures in the feature block.

If the signer clicks on the *Reference Features* button, the features of the reference signatures are displayed in blue in the 6 windows in the feature block. When the signer clicks on the *Current Feature* button, the features of the current testing signature are plotted in red and compared with those of the references in the same windows. An example of such kind of comparison is illustrated in the feature block of Figure 6.3.

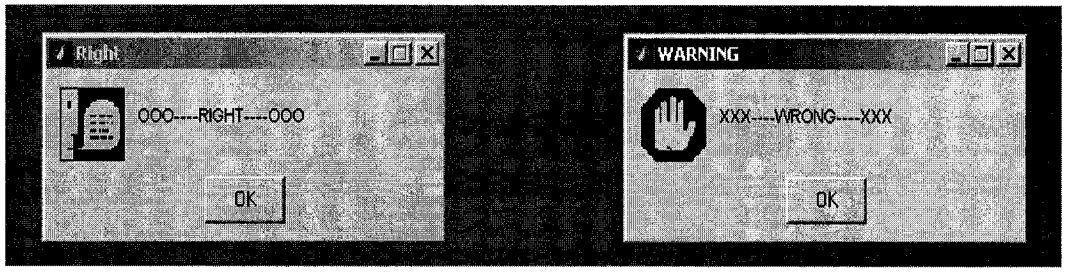


Figure 6.4 Verification judgment pop up windows.

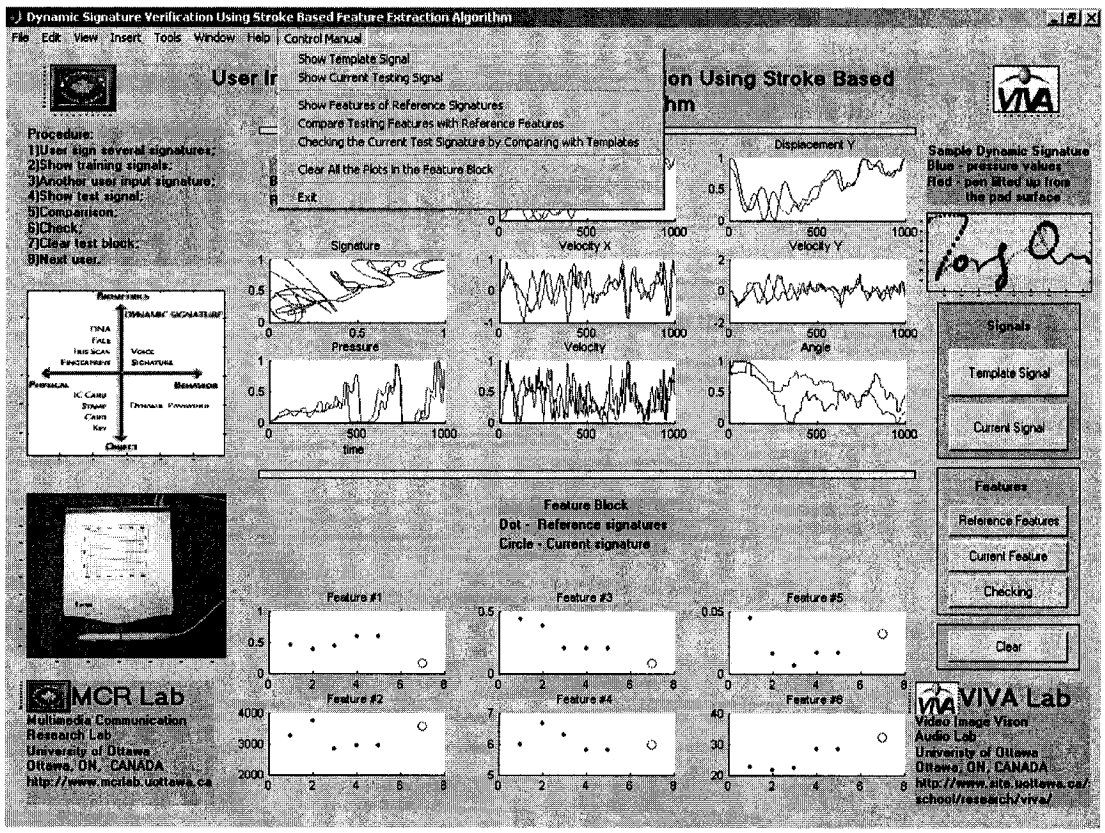


Figure 6.5 Control menu icon on the interface.

Finally, the signature verification results can also be judged by clicking the *Checking* button. A window will pop up showing the verification judgement result for the current testing signature. A screen shot for the two kinds of pop up window is shown in Figure 6.4. By clicking on the *Clear* button, all the plots in the feature block will be cleared. The Control Menu function is available and offers another way to control this system. It is equivalent to the button control method and accomplishes the same operations. If click the *Control Menu* icon on the top of the interface, the manual will be activated as shown in Figure 6.5.

6.2 Experiments

This section describes experiments for fixed and variable threshold calculations. For the fixed threshold experiments, a predefined threshold is used, and the FRR and FAR are computed. The features selection and features comparison are conducted in the fixed threshold experiments. Finally, the FRR and FAR data are calculated for detecting an error tradeoffs curve based on the variable thresholds experiments.

6.2.1 Fixed Threshold Experiments

It is necessary to select features for the dynamic signature verification system. The preliminary selection can be conducted by observing the ratios of the standard deviation to the mean for each feature and counting the effect of each feature type. If a ratio is very large, it means the variance of the feature is large. This implies that such a feature is not stable and not suitable to be used. The performance of the system can then be compared

by using different features. An example of a preliminary feature selection is conducted based on a set of 60 sample signatures. The x velocity feature values are plotted in Figure 6.6. These are the mean, the variance, the sum of the means in 10 sliding windows, and the sum of the variance in 10 sliding windows, respectively, for the x position signal. The corresponding pressure feature signal values are plotted in Figure 6.7. For this individual, the mean of the x velocity feature values and the variance of the pressure feature values in 10 sliding windows can be chosen as a preliminary selection for the proposed signature verification system.

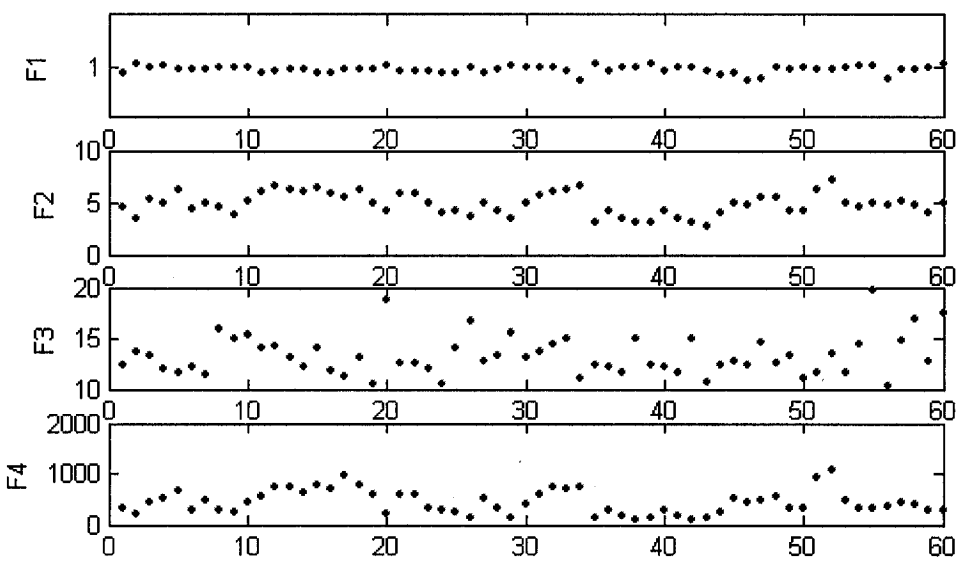


Figure 6.6 Plot of feature values for x velocity signal for a set of signatures.

Similarly, the feature values plots for other group of features and for other persons can also be obtained. In order to reduce the computing cost, the number of features in the initial feature set should not be too big. It has been set to 4 in the current study. In

order to check the performance of the stroke-based features on the verification system, no stroke-based features are selected in the initial feature set. Some stroke-based features are then added into the initial feature set later. This allows their effects on the verification to be evaluated.

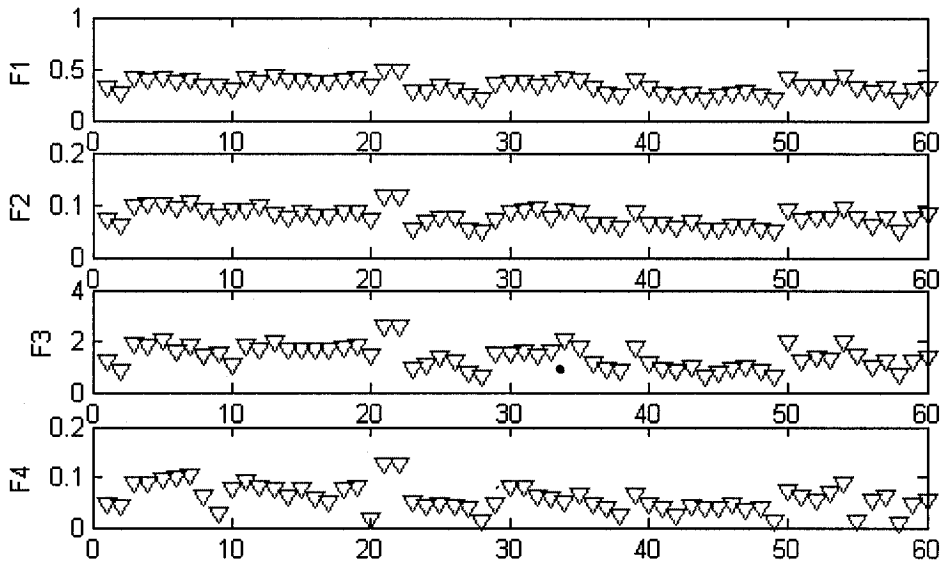


Figure 6.7 Plot of feature values for z pressure signal for a set of signatures.

The initial feature set includes the following features: total time during the signing process, average writing speed, variance of pressure signal in 10 sliding windows, and mean of the x displacement signal in 10 sliding windows. First, the performance of the signature verification system based on the above 4 features is evaluated by a fixed threshold experiment. Then, with adding stroke based features, the performance of the updated signature verification system has also been evaluated and also compared with

the result of the previous system.

In order to evaluate the above signature verification systems, the FRR and FAR needs to be computed when setting a fixed threshold. The fixed threshold is set to 75%.

A total of 110 signatures, split into 50 reference and 60 test signatures, from 10 volunteers were used in this experiment. Each volunteer performed 5 signatures to train their signature template, and performed another 3 genuine signatures as test signatures. In addition, for each template, 3 skilled forgery signatures were performed by other volunteers. By skilled forgery, we mean that volunteers were allowed to practice to create the forgeries while they can observe and study the several genuine signatures freely.

All the signatures were evaluated by using the graphical user interface presented in the previous section, The 50 sample genuine signatures were used to train the 10 signature template for 10 volunteers. Twenty-one out of the 30 genuine test signatures have been authenticated, while 9 have been rejected by the system using initial 4 features. Sixteen out of the 30 test forgeries have been rejected by the system, while 14 have been approved. Therefore, the current 4 feature based system achieved a FRR of 30% and FAR of 46.67%.

Adding one stroke base feature to the above system leads to a 5 feature based verification system. Several stroke based features were added, and their effects on the system performance are listed in Table 6.1.

Since it is more difficult to identify the angle of the signals strokes, the angle signal related stroke features are not listed in Table 6.1. However, the table shows that, most of the stroke based features improve the verification accuracy. Two out of the described

features performed better than the others. These are correlation coefficient for the pressure significant strokes and time duration for velocity significant stroke. Therefore, we combined them together and added them into the initial system. This lead to a 6 features based system. The same experiment was conducted again and we achieved a FRR of 6.67% and FAR of 13.33%. These results are compared with that of the 4 features based system and presented in Table 6.2. Further experiments showed that adding more features (both stroke based features and non stroke based features) did not lead to better performance. Therefore, the six feature based signature verification system was adopted as our optimal system.

Table 6.1 Effects of stroke based features on a fixed threshold verification system

Feature Name	FRR	Reduction in FRR	FAR	Reduction in FAR
number of strokes in pressure signal	20.00%	10%	33.33%	13.34
number of strokes in velocity signal	23.33%	6.67%	36.67%	10%
correlation coefficient for the pressure significant strokes	13.33%	16.67%	20.00%	16.67%
correlation coefficient for the velocity significant strokes	16.66%	13.33%	36.67%	10%
time duration for velocity significant stroke	16.67%	13.33%	13.33%	33.34%
average speed in the velocity significant stroke	20.00%	10%	23.33%	23.34%

Table 6.2 FRR and FAR data comparison for two systems

	FRR	FAR
4 feature based system (without stroke features)	30%	46.67%
6 feature based system (with stroke features)	6.67%	13.33%

In the above experiments, skilled forgeries are used. Using random forgeries, a FAR of 1% can be achieved. It can be concluded that random forgeries are more easily detected.

In the presented experiments, each template was trained by 5 sample signatures. The following experiment was designed to check the effect of using more sample signatures.

A total of 180 signatures, split into 120 reference and 60 test signatures, from 10 volunteers were used in this experiment. In order to study the training effect by the number of signatures, the first volunteer signed 60 signatures and the second signed 20 signatures. The other 8 volunteers each performed 5 signatures to train their signature template. Thus, there were three training sets of sizes 60, 20 and 5 training signatures. The test signatures are generated the same as before, with each volunteer performing 3 genuine signatures as test signatures and 3 skilled forgery signatures were created by other volunteers for each template.

All the above signatures are evaluated by the 6 feature based verification system. The computation of the FRR and FAR data showed that 29 of the 30 authentic signatures were correctly approved by the system, giving a FRR of 3.33%. In addition, 28 forgeries were rejected by the system resulting in a FAR of 6.67%. For the template trained by 60 and 20 signatures, all the 6 genuine test signatures were approved and 5 forgery test signatures were correctly rejected. This result suggests that a large training set should improve the algorithm performance. But if considering the cost of the experiments, it may still be reasonable to choose 5 sample reference signatures since the corresponding result of FRR of 6.67% and FAR of 13.33% may be acceptable in a given application.

6.2.2 Variable Threshold Experiments

The FRR and FAR data computed in the last section vary with changes in threshold value. An experiment has been conducted to detect the error tradeoffs curve by computing the FRR and FAR data with variable thresholds.

A total of 55 signatures, split into 25 reference and 30 test signatures, from 5 volunteers were used in this experiment. Each volunteer performed 5 signatures to train their signature template, and performed another 3 genuine signatures as test signatures. In addition, for each ready template, 3 skilled forgery signatures were performed by other volunteers.

For a 6 feature based system, a test signature is judged to be genuine if its 4 or more features match with the template. In this case, a threshold is computed as 4 over 6 and equal to 67%. In similar, six thresholds have been set in this experiment. The corresponding FRR and FAR data have been calculated and listed in Table 6.3. The FRR and FAR data are plotted in Figure 6.8 to get the error tradeoffs curve.

Table 6.3 FRR and FAR data corresponding to variable thresholds

Threshold values	FRR	FAR
17%	0	36.67%
33%	3.33%	26.67%
50%	6.67%	16.67%
67%	13.33%	6.67%
83%	23.33%	3.33%
100%	30%	0

The above results show a tradeoff between the FAR and the FRR. If either FRR or FAR approaches zero, the opposite rate raises rapidly. When the FRR is approaching to

zero, the FAR reaches its maximum value of 36.67%; the FRR reaches the maximum value of 30% while FAR is zero.

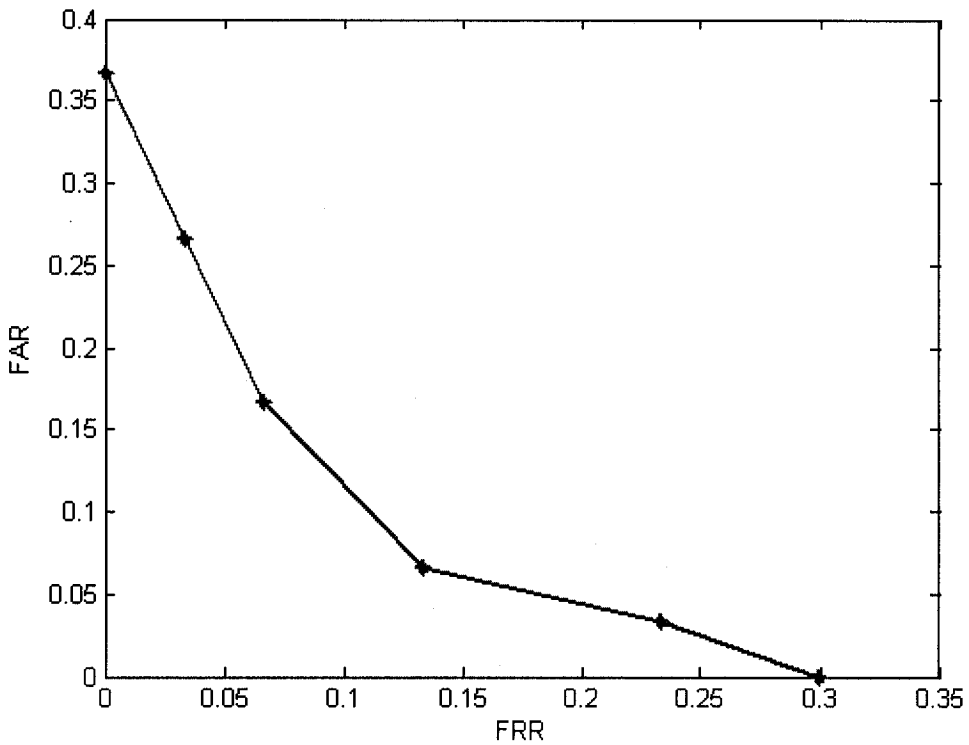


Figure 6.8 FRR and FAR tradeoff curve on variable thresholds.

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

In this thesis, a dynamic signature verification system has been developed and studied based on a novel stroke based features verification algorithm. At first, the system architecture has been described. The system includes three subsystems, the data acquisition system, feature extraction system and signature verification system.

In the data acquisition system, the data acquisition and related hardware setup work has been presented in three parts: digital pad setup, data measurement, and data acquisition protocol; the dynamic signature signal has been represented with various position, pressure, velocity, acceleration and angle channel signals.

Second, a novel stroke based algorithm has been presented in detail following the description for several general feature extraction methods. It requires the following key steps: identification of stroke boundaries, stroke alignment, stroke correspondence matching and significant stroke feature extractions. A significant stroke is discriminated by the maximum correlation with respect to the reference signatures. Between each pair of signatures, the local correlation comparisons are computed between portions of

pressure and velocity values using segments alignment based on elastic matching. In addition, the characteristics of signature strokes are studied, and features selection is also discussed as well.

In the signature verification system, a binary signature classifier has been used; it is designed based on the characteristics of observed feature distribution, which is modelled as a Gaussian. In order to evaluate the proposed system, experiments have been carried out for the case of both fixed and variable thresholds. The effects of stroke-based features on verification have been evaluated in the fixed threshold experiments. The error tradeoffs curve was plotted in the variable threshold experiments. A graphical user interface is developed for the convenience of conducting signature verification experiments.

The key information has been extracted from the significant stroke based on the stroke based algorithm. It has been shown that some of the stroke-based features can improve the accuracy of the verification system than other groups of features. Two stroke based features combined with four global features have been implemented into the current dynamic signature verification system. This 6 feature based system exhibits better accuracy than other feature combinations. Such kinds of stroke based features have great potential for developing high accuracy automated dynamic signature verification systems.

7.1 Conclusions

The conclusions of this thesis can be summarized as follow:

- A novel stroke-based algorithm has been developed for the proposed dynamic signature verification system. A dynamic signature verification system has been developed based this algorithm.
- This thesis presents an approach to identify the significant strokes and extract individual's consistent behavioural dynamic characters from them. The stroke based features also can be integrated with other kind of features and applied in the proposed dynamic signature verification system. The experimental results show that stroke based features contain robust dynamic information, and offer great accuracy for dynamic signature verification.
- An automated dynamic signature verification system has been developed and applied to identify genuine signatures against forgeries. For the convenience of operation, a graphical user interface was designed to allow the signature verification operation to be conducted conveniently and visually.
- It has been shown that the stroke based features extracted from the pressure and velocity signals can improve the verification accuracy over a 4 feature based verification system.
- A 6 feature based system have been shown to perform better than other system designs. It has been developed by adding two stroke based features (correlation coefficient for the pressure significant strokes and time duration for velocity significant stroke) on an optimal 4 feature based system. The FRR has been improved from 30% to 6.67%, while the FAR has been reduced from 46.67% to 13.33%.

- The experiment with more sample signatures exhibited a bit better performance than that of only using 5 sample signatures. But if considering the cost of the experiments, it is still reasonable to choose 5 sample reference signatures.
- The results of variable thresholds experiments show the tradeoff between FAR and FRR. When the FRR approaches zero, the FAR reaches its maximum value of 36.67%; the FRR reaches the maximum value of 30% while FAR close to zero. In addition, an EER of about 11% can be roughly estimated when the threshold is within 50% and 67%.
- Our experiments show that when adding stroke-based feature into a non-stroke feature system, the accuracy of the signature verification has been greatly improved. The experiments show that stroke-based features are important features and they contain robust dynamic information and have great potential to be applied in the dynamic signature verification.

7.2 Future Work

The future work is summarized as follow: 1) The experiment results are expected to be more accurate if using more sample signatures. A bigger reference signature database should be built later. 2) In our current study, a 4 features based system has been set as the initial system, if not considering the cost of experiment, more features (e.g. 10 or 15 features) can be selected for the verification system, the accuracy of the verification are expected to be better. 3) More stroke based features can be extracted and add into the initial feature extraction system. 4) Other types of features can be implemented such as

phase space features. 5) More experiments can be carried out to estimate the error tradeoffs curve. 6) An updated version of the digital pad, digital pen or Personal Digital Assistant (PDA) devices with higher sensitivity and accuracy are recommended to be used. 7) Other types of models can be used to estimate for signature verification, such as General Method of Moments (GMM), Hidden Markov Model (HMM), and Majority Classifier [Lee92, Lee96].

APPENDIX

GUIDELINE OF SIGNAUTURE VERIFICATION

-Volunteer Information for Signature Acquisition

General Information

Our current research is to identify personal electronic signatures acquired by Patriot Digital Pad. We are developing a dynamic signature algorithm which can identify the genuine signatures against the forgeries. In order to test and verify the proposed algorithm and system, we need sample signatures signed by some volunteers. A set of sample signatures for each volunteer will be collected for the analysis, and the collected data will be used only for evaluation and analysis of algorithms for signature analysis and recognition. We appreciate you would like to be one of our volunteers. Your participation will involve signing your signature on our "Patriot Digital Pad" several times during different times when you are available.

Procedures

1. As a volunteer, first, you'd better be familiar with the "Patriot Digital Pad", and sign your signature with the "same" manner, which means using the "same" speed, pressure, strokes, timing sequence etc. Before recording your signatures, you can practise the signing process until you feel you can recreate your signature easily and comfortably.
2. Although we hope you sign your signatures with the "same" manner as possible as you can, but there do exist variances between your own signatures, and these differences maybe become larger if you sign your signatures at different time and different conditions. In order to obtain your template of signature which can reflect the long term manner for your signing process, we hope to record a set of your signatures at different time and different situations (when you feel happy, sad, excite, or tired, etc). So you can come and sign your signatures at random time and different health conditions.
3. For each volunteer, we need about 50 signatures. All of these signatures will be recorded during three months. So each time, please sign at most 5 signatures. Then you can sign your signatures in the next day, next week or next month. Ideally, we would like to obtain signature samples every two weeks for three months. We will contact you by email every two weeks, to setup a time to record your signatures.
4. Each time when you record your signatures, please also record the time and your feeling (such as excitement, sadness, happiness, calmness, etc.). Also please record your signing position (such as sit or stand).

5. Please sign your standard signature with the "same" manner as possible as you can. We recommend you can use the same manner when you sign your cheque or visa, since you are familiar with that manner and only you can re-create that manner with smallest variance.
6. There is an interface for the signing, and two buttons "start signing" and "stop signing" there are shown on the interface. Before sign a signature, please click on the "start signing" button, then the system begin to record your digital signature; when you finish signing, please click on the "stop signing" button, then the system stop recording current signature and wait for next signing.
7. Collected data will be used only for evaluation and analysis of algorithms for signature analysis and recognition. Possible publications from this work will consist of aggregate, analyzed data. Identifiable data (such as signature images) will not be published without your express written permission. Data will be stored on a password protected computer, and be made available only to the graduate researcher and supervisors.

REFERENCES

[Biowork00] Biometric Working Group, "*Best Practices in Testing and Reporting Performance of Biometric Devices*", ver. 1, http://www.afb.org.uk, 2000.

[Brault89] J. Brault and R. Plamondon, "How to Detect Problematic Signers for Automatic Signature Verification", *International Carnahan Conference on Security Technology*, pp. 127-132, 1989.

[Brault93] J. Brault and R. Plamondon, "Segmenting Handwritten Signatures at Their Perceptually Important Points", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 9, pp. 953-957, 1993.

[Crane83] H. D. Crane and J. S. Ostrem, "Automatic Signature Verification Using a Three-Axis Force-Sensitive Pen", *IEEE Transactions on Systems, Man and Cybernetics*, vol. SMC-13, no. 3, pp. 329-337, 1983.

[Colmas80] C. F. Colmas, "*The Writing Systems of the World*", Blackwell, 1980.

[Cyber03] Cybersign, http://www.cybersign.com, 2003.

[Denier65] J. J. Denier van der Gon and J. P. Thuring, "The Guiding of Human Writing Movements," *Kybertenik*, vol. 4, no. 2, pp. 145-148, 1965.

[Earnest63] L. D. Earnest, "Machine reading of Cursive Script", *IFIP Congress*, pp. 462-466, Amsterdam, 1963.

[Eden62] M. Eden, "Handwriting and Patten Recognition", *IRE Transactions on Information Theory*, vol. 8, 1962.

[Gupta97] G. Gupta and A. McCabe, "*A Review of Dynamic Handwritten Signature Verification*", *Technical Report*, Department of Computer Science, James Cook University, Australia, 1997.

[Gupta97a] G. K. Gupta and R. C. Joyce, "A Study of Some Pen Motion Features in Dynamic Handwritten Signature Verification", *Technical Report*, Department of Computer Science, James Cook University of North Queensland, Australia, 1997.

[Herbst77] N. M. Herbst and G. N. Liu, "Automatic Signature Verification Based on Accelerometry", *IBM Journal of Research Development*, pp.245-253, 1977.

[Huaqi03] Huaqi, http://www.huaqi.com, 2003.

[Kiran01] G. V. Kiran, R. S. R. Kunte, and S. Samuel, "On Line Signature Verification System Using Probabilistic Feature Modelling", *International Symposium on Signal Processing and its Application* (ISSPA), pp.355-358, Kuala Lumpur, Malaysia, August 2001.

[Lam89] C. F. Lam and D. Kamins, "Signature Verification Through Spectral Analysis", *Journal of Pattern Recognition*, vol. 22, no. 1, pp. 39-44, 1989.

[Lcs03] Window tablet API, http://www.lcs-telegraphics.com, 2003.

[Leclerc94] F. Leclerc and R. Plamondon, "Automatic Signature Verification: The State of the Art, 1989-1993", *International Journal of Pattern Recognition and Artificial Intelligence*, special issue signature verification, vol. 8, no. 3, pp. 643-660, 1994.

[Lee92] L. L. Lee, "*On-line Systems for Human Signature Verification*", Ph.D Thesis, Cornell University, USA, 1992.

[Lee95] L.L. Lee, "Neural approaches for human signature verification", *Third International Conference on Document Analysis and Recognition,* vol. 2, pp.1,055-1,058, Montreal, Canada, August 1995.

[Lee96] L.L, Lee, T. Berger, and E. Aviczer, " Reliable on-line signature verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 6, pp. 643-647, 1996.

[Lejtman01] D. Z. Lejtman and S. E. George, "On-line Handwritten Signature Verification Using Wavelets and Back-Propagation Neural Networks", *6th International Conference on Document Analysis and Recognition*, Seattle, USA, September 2001.

[Mauceri65] A. J. Mauceri, "Feasibility Studies of Personal Identification by Signature Verification", *Report no. SID 65 24 RADC TR 65 33, Space and Information System Division*, North American Aviation Co., Anaheim, USA, 1965.

[Nalwa97] V. S. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE*, vol. 85, no.2, pp. 215-240, 1997.

[Nouboud90] F. Nouboud and R. Plamondon, "On-Line Recognition of Handprinted Chatracters: Survey and Beta Tests", *Journal of Pattern Recognition*, vol. 25, no. 9, pp. 1,031-1,044, 1990.

[Pacut01] A. Pacut and A. Czajka, "Recognition of Human Signatures", *Proceedings of International Joint Conference on Neural Networks*, vol. 2, pp, 1560-1564, July 2001.

[Parizeau90] M. Parizeau and R. Plamondon, "A Comparative Analysis of Regional Correlation, Dynamic Time Warping, and Skeletal Tree Matching for Signature Verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 7, pp. 710-717, 1990.

[Parks85] J. R. Parks, D. R. Carr and P. F. Fox, "Apparatus for Signature Verification", *US Patent Number 4,494,644*, 1985

[Plamon88] R. Plamondon and M. Parizeau, "Signature Verification from Position, Velocity and Acceleration Signals: A Comparative Study", *Proceedings of the 9th International Conference of Pattern Recognition*, vol.1, pp.260-265, Rome, Italy, 1988.

[Plamon89] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification – The State of the Art", *Journal of Pattern Recognition*, vol. 22, no. 2, pp. 107-131, 1989.

[Plamon94] R. Plamondon et. al., "*Pattern Recognition, Special issue on automatic signature verification*", R. Plamondon ed., vol. 8, no. 3, 1994.

[Plamon99] R. Plamondon, D. Lopresti, L.R.B. Schomaker, and R. Srihari, "On-Line Handwriting Recognition: A Comprehensive Survey", *Encyclopedic of*

Electrical and Electronics Engineering, J.G. Webster, ed., vol. 15, pp. 123-146, New York, Wiley, 1999.

[Plamon00] R. Plamondon and S.N. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 63-84, 2000.

[Tappert90] C.C. Tappert, C.Y. Suen, and T. Wakahara, "The State of the Art in On-Line Handwriting Recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 8, pp. 179-190, 1990.

[WACOM03] Wacom, http://www.wacom.com, 2003.

[Wakahara92] T. Wakahara, H. Murase, and K. Odaka, "On-Line Handwriting Recognition", *Proceedings of the IEEE*, vol. 80, no. 7, pp. 1,181-1,194, 1992.

[Wayman03] J. Wayman et. al., "*National Biometrics Test Center Collected Works 1997-2000*", J. Wayman ed., ver. 1.3, San Jose State University, USA, http://www.engr.sjsu.edu/biometrics/nbtccw.pdf, 2003.

[Wessels00] T. Wessels and C. W. Omlin, "A Hybrid System for Signature Verification", *South African Telecommunications Networks and Applications Conference*, pp. 509-513, 2000.