Validation of Dynamic Signature for Identity Verification

A thesis submitted in fulfilment
of the requirements for the degree of

Doctor of Philosophy

Shern Cheng Yau

M. Eng.(Telecommunication Engineering), RMIT University,
Melbourne, Australia

School of Electrical and Computer Engineering
Science, Engineering and Technology Portfolio
RMIT University
August 2008

Declaration

I certify that except where due acknowledgements has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; and, any editorial work, paid or unpaid, conducted by a third party is acknowledged.

Shern Cheng Yau

Acknowledgements

My first thanks to the all mighty Lord and saviour for always being by my side through any situations and guiding me through good and bad times.

I would like to thank my supervisor, Associate Prof. Dr. Dinesh Kant Kumar for his constant support and excellent guidance during the course of this research. His valuable advices in conducting scientific research are essential for this research. It has been a great pleasure and privilege to work with him and to benefit from his rich knowledge and experience. I would also like to thank him for his encouragement throughout this research when morale was low.

I would like to express my deepest gratitude to my parents for constantly supporting me throughout this work. Their unconditional love has always been a source of strength for me to overcome obstacles in life.

Many thanks to Sridhar, Wai and Jonathan who have critically read drafts of this thesis and provided valuable comments. I would also like to thank my officemates, Ganesh, Vijay, and Thara for providing me with a fun and inspiring environment to work in. I would like to thank all my friends for their support and voluntary participation in the experiments.

Last but not least, I would like to thank the staff at the School of Electrical and Computer Engineering, RMIT University for their help and coorperation.

Abstract

Machine based identity validation is extremely important to determine the authenticity of documents, for financial transactions, and for e-communication. Recent explosion of frauds have demonstrated the ineffectiveness of password, personal identification numbers and biometrics. This thesis presents a signature verification technique which is inexpensive, user friendly, robust against impostors and is reliable, and insensitive to factors such as users' exposure to emotional stimuli.

This work has addressed three important issues which are:

- the selection of appropriate features for dynamic and static signatures.
- the suitable classifier for classification of the features.
- the impact of emotional stimuli on the natural handwriting and signatures of the subjects.

The thesis reports a comparison of the dynamic and static signatures and demonstrates that while the dynamic signature technique has a small increase in the rejection of the authentic user (92% compared with 94%), the system is far more discerning regarding the acceptance of the impostors (1% compared with 21%). The work also demonstrates that the use of 'unknown' as a class reduces the rejection to

zero, by putting those into a class who would be asked to repeat the experiment.

This thesis has also studied the impact of emotional stimuli on peoples' handwriting and signatures and has determined that while the signatures are insensitive to these stimuli, the handwriting is affected by these stimuli. This outcome may be of importance for people who conduct graphology analysis on people because this suggests that while general handwriting is affected by short term emotional changes of people, signatures are a more robust indicator of the person and hence their personality.

Publications Arising From This Thesis

Fully Refereed Conference Proceedings

1. Yau, S. C., & Kumar, D. K. (2007). Recognition of dynamic signatures for people verification. *Int. Workshop on Pattern Recognition in Information Systems (PRIS)* , (pp. 189-198), June 12-16, Funchal, Portugal.

2. Yau, S. C., & Kumar, D. K. (2007). Dynamic signature for identity validation. *in Proceedings of 13th Conference of the International Graphonomics Society,* , November, Melbourne, Australia.

International Journals

1. Yau, S. C., & Kumar, D. K. (2008). Unpenned Signature Verifier - Comparison of Static and Dynamic Features. *International Journal of Pattern Recognition and Artificial Intelligence (IJPRAI), World Scientific* Under Review

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

We are currently living in a society that is extremely conscious of security. There is need for securing building space, data, and transactions. For this purpose, it is important to verify the identity and authenticate an individual. There are three major means of verifying the identity of an individual- what they have (identity card), what they know (password) or what they are (biometrics).

Personal Identification Number (PIN) and use of password have evolved over the past 3 decades to provide means of authentication of people for accessing funds, database or buildings. These are being used at banks and ATM, for telephonic access to financial information, for accessing computers and database. While this technique has the advantage of being easily automated, there are several shortcomings. Authentic users may forget their PIN, and it has been demonstrated repeatedly that it is possible to deduce the PIN and password from other seemingly unrelated information of the user.

Unlike PIN and passwords, which are easily forgotten or deduced by impostors, and identity cards, which are easily stolen or lost, biometrics is a part of us. Biometrics is the utilization of physiological characteristics or behavioural traits for identity validation of an individual. Biometric authentication has become one of the more popular and trustable security system that has become an alternative to password based security system. In the recent past, biometric techniques have been developed for machine based verification of the identity of a person (Prabhakar et al., 2003). There are two types of biometric authentication; (i) anatomical, which uses human physiology, and (ii) non-anatomical, which is behavioural based.

While the use of the anatomical measurements of the individual has often been considered to be extremely robust for identifying an individual, they have their own limitation. All traditional biometrics measures have certain limitations associated to them. For example:

- DNA can't be used in certain applications due to issues of contamination, sensitivity, cumbersomeness and privacy.
- Ear-shape as a biometric measure has a problem of non unique features.
- Facial biometrics have problems with aging, face disguise and variable imaging conditions.
- Hand and finger geometry has limited applications, although fingerprints are very unique but they also have the problem of fake fingers, storage and imaging conditions problems.
- Iris biometrics is intrusive and has issues of unreliability.

- Speech biometrics has the limitation of mechanical variance due to the microphone and dependence on subjects' health (Prabhakar et al., 2003).

One other major concern with the anatomical based biometrics is that if these can be copied by the impostor using deceit or force, the authentic user would be faced with life-long loss of identity (Woodward, 1997).

To overcome some of the above mentioned shortcomings, researchers have attempted to develop non-anatomical biometrics. Biometrics such as keystroke and gait analysis are based on the behaviour of the individual but the reliability is highly questionable (Prabhakar et al., 2003).

One of the most commonly used non-anatomical biometric authentications is based on the person's penned signature. Unlike other biometrics, signature authentication is widely accepted by nearly every society as a form of secure authentication. It overcomes most of the setbacks of anatomical biometrics as well as its flexibility in comparison to the other non-anatomical biometrics. Signature has been used in our daily lives to identify ourselves. The validation of the signature is routinely conducted by people at the retail outlets' check-out counter or teller of a bank or the sentry of the building for less sensitive applications such as small payments or entry into domestic and office buildings. Often the signatures are verified based on the visual comparison with the sample of the authentic signature that is either kept on the back of the card (credit card) or other similar instrument.

While the use of penned signatures in the traditional banks is not free from frauds, the number of frauds is few because the bank executives are trained to be able to spot forgery. But with the explosion of the use of credit cards, and with the database of the authentic signature being available at the back of the

card itself, and the check-out cashier not trained to spot forgeries, there has been an explosion of signature related frauds. While graphic-analysis experts are able to spot the differences between authentic signatures and frauds, a lay person at the counter of a departmental store is unable to see such subtleties. In order to prevent lay people from falsely accepting an individual, a computerized authentication system can be used in their place. There is need for a system that is easy to use, does not intrude on the privacy of the individual, is robust against imposters, and is reliable for the individual even under different external factors such as emotions.

1.2 Problem Statement

Signature verification techniques utilize many different characteristics of an individual's signature in order to authenticate that individual (Vacca, 2007). The advantages of using such an authentication technique are; (i) signatures are widely accepted by society as a form of verification (Kung et al., 2004), (ii) information required is not sensitive and (iii) forging of an individual's signature does not mean a long-life loss of that individual's identity. The general idea of this research is to investigate a signature verification technique which is not costly to built, user friendly in terms of configuration, robust against imposters and is reliable even if the individual is under different emotions.

In signature verification application, the signatures are processed to extract features that are later fed into a classifier. The task of the classifier is to assign the signature features to classes of individuals. The selection of signature features is critical in determining the performance of a signature verification system. In

this research, the features were selected according to certain criterions. Mainly, the features have to be small enough to be stored in a smart card and does not require complex classification techniques.

There are two ways of validating a signature. They are static and dynamic. Static features are comprised of features which are extracted from signatures that are recorded as an image whereas dynamic features are extracted from signatures that are acquired in real-time (Faundez-Zanuy, 2005; Plamondon and Srihari, 2000). These feature types can be broken down into two types which are function based and parameter based features.

The function based features describes a signature in terms of a time-function. Examples of function based features include position, pressure and velocity (Dimauro et al., 2004). While the performance of such features is well known to researchers in accurately verifying signatures, they are not suitable in this case due to the complexity of its matching algorithm. Hence, the use of parameter based features is more appropriate.

Even though it is critical to select a suitable set of features to be extracted, emphasis has to be put into selecting an appropriate classifier for the features selected. Some classifiers do not work for certain type of features, for example Hidden Markov Model (HMM). The HMM classification technique for signature verification has been proposed by many researches such as Igarza et. al. (Igarza et al., 2003) and Muramatsu et. al. (Muramatsu and Matsumoto, 2003). The main issue in using HMM is modeling the extracted features in Markov Model. Moreover, the larger the amount of features, the more complex the HMM would be. There are many other classification techniques available that have been proposed by Srihari et. al. (Srihari et al., 2004), Rioja et. al. (Rioja et al., 2004)

and Sakamoto et. al. (Sakamoto et al., 2001). These would be discussed in detail in chapter 2.

It is important to take into account external factors when investigating a signature verification technique. Signature verification applications are used in our daily lives and will be exposed to human emotions. The system has to be reliable in accurately verifying an individual's signature even if he/she is under different emotions. Sackheim (Sackheim, 1990), Gardner (Gardner, 2002), Lange et. al (Lange et al., 2006) and Yank (Yank, 1991) have shown that handwriting of a person is affected by their emotions. Most of the techniques which have been proposed by researchers have not been tested against people's emotions.

1.3 Research Aim and Objectives

The general idea of this research is to investigate a signature verification technique which is not costly to build, user friendly in terms of configuration, robust against imposters and is reliable even if the individual is under different emotions. The main aim of this research is to:

- Choose a suitable features required for a robust signature verification technique, yet inexpensive to build and user friendly in terms of configuration. The features are chosen according to certain criterions listed in chapter 3.
- Investigate the performance of selected classifiers which are suitable for classifying the chosen features.
- Examine the robustness of the feature set against variations in human emotions.

1.4 Research Definition

This research aims to select a set of suitable features, which is small and concise, for signature verification from the available state-of the art features. The features have to be suitable for a robust signature verification technique, yet inexpensive to build and user friendly in terms of configuration. The features used in this research are dynamic global parameter based features. The main advantages of this type of features are; (i) they are computationally inexpensive to extract and classify and (ii) they cannot be reverse engineered to obtain the original image of the individual's signature.

This research also investigates the performance between two classifiers which are the ANN and the statistical analysis classifier. Although ANN is a good and easy to use classification tool, there are still many setbacks, which will be discussed in the later chapters. Hence, a more suitable and less complex classifier, the statistical analysis classifier, was needed.

In this research, the performance comparison between the chosen feature set and the static Hu moment feature set was done as well. The Hu moment was chosen as the static feature set because of its ability to concisely describe an image and its simplicity in extracting it from signatures.

Emotions play a big part in our daily lives and studies have shown that it affects the handwriting of an individual. The scope of this thesis also extends to investigating whether emotions have any effect on the chosen feature set, extracted from both the handwritten words and signature of an individual. For this research, the four basic emotions, happy, sad, fear and anger, are used.

1.5 Outline of the Thesis

This thesis is organized into 7 chapters. The first chapter provides an introduction of the research. Chapter 2 describes the previous work and background studies which have been done on signature verification.

Chapter 3 presents the theory behind the original contribution of this research. This chapter reports on the criterions needed to select the suitable features required. Chapter 3 also gives a brief description on the static Hu moments and the classifier ANN. Other than that, this chapter also reports on the theory of a new method for a simple yet efficient statistical analysis classifier.

Chapters 4 and 5 present the experiments done in this research. Chapter 4 describes the experimental set up used to determine the performance of both the ANN and statistical analysis classifier, using the chosen set of features.

Chapter 5 reports on the experiment done to compare the performance of the dynamic signature and static signature, using the statistical analysis classifier.

Chapter 6 reports the experimental study of the effects of emotions on the chosen feature set and also the handwriting of an individual.

Finally, chapter 7 summarizes all the discussion and results obtained from the experiments done during this research. This chapter concludes this thesis and provides recommendations for future studies in this research topic.

Chapter 2

Background

2.1 Introduction

For this research, the first important issue is the understanding of current state of people identity authentication technology. This is essential for identifying the weakness of these technologies. There are three main issues related to signature authentication at hand which need to be addressed. The first issue is the selection of suitable signature features. Second is the choice of having a suitable classifier for the chosen feature set and finally, the issue of emotions affecting the selected feature set. In this chapter, a brief description on biometric authentication and a generalized model for a signature verification system is reported, followed by a review on various studies based on the three main issue stated above. This chapter also gives a literature review of emotions on handwriting and also graphology at the end.

2.2 Biometric Authentication

Biometric authentication is the use of a unique, non-duplicable or transferable and measurable human physiological or behavioural characteristic to identify or verify a certain user (Delac and Grgic, 2004; Dugelay et al., 2002; Matyas and Riha, 2003; Wayman, 1997).

Biometric technologies can be divided into two different types; (i) anatomical biometrics and (ii) non-anatomical biometrics. Anatomical biometrics involves the use of physical human body parts for the purpose of authentication. This includes finger prints, DNA, face, iris, hand geometry and etc. As previously discussed in chapter 1, the downside of anatomical biometrics is the delicateness of its required information. The success of forging such biometrics will result in a life-long loss of an identity (Woodward, 1997).

Non-anatomical biometrics is the use of human behavioural characteristics for the purpose of authentication. The use of human speech, handwritten signature and keystrokes for authentication are the few examples of non-anatomical biometrics authentication. Compared to anatomical biometrics, the use of non-anatomical biometrics for authentication is more acceptable to society (Kung et al., 2004) as its information is less intrusive.

In reality, there are many kinds of biometric characteristics which can be used to authenticate a user. Each of these methods has their own distinctive way of operating. Although biometric technologies differ in many ways, their basic operation model is the same. The biometric system can basically be modeled in 2 layers which are enrolling users and verifying users (Matyas and Riha, 2003).

Authentication can be done in two modes. They are:

- Verification: a user claims to be enrolled in the database by presenting an ID card or login and the computer compares the user's biometrics to the biometrics characteristics stored in its database. The matching done in this mode is one to one (Jain et al., 2004; Matyas and Riha, 2003; Moon et al., 1999; Phillips et al., 2000).

- Identification: the system matches the biometric characteristic of the user to all records in the database, not knowing whether the user is on the database or not. Basically, the system searches through a database of enrolled biometrics characteristics to find a template which matches the user's. The matching done in this mode is one to many (Jain et al., 2004; Matyas and Riha, 2003; Phillips et al., 2000).

2.3 Signature Authentication

A signature of an individual is very consistent although there might be slight variations every time an individual signs. However, its consistency makes it natural for biometric authentication (Lee, 1992). Signature authentication is the biometric process of using an individual's signature to authenticate a particular individual. Handwritten signatures offer high degree in performance and are "yet a known and established legal status, acceptability by the public, the elimination of common concerns about unwelcome connotations or health factors associated with some other modalities, and the convenience in execution afforded to users". Handwritten signatures are dependent on the user, unlike anatomical biometric measures, allowing the users to be able to change their signatures according to the application it is needed for (Fairhurst and Kaplani, 2003).

Like any other biometric system, the signature authentication system can basically be modeled in 2 layers which are enrolment and matching. During enrolment, an individual enrolls himself into the system by providing signatures to the system. This allows the system to learn that individual's signature. During matching, a sample of the individual's signature is obtained and matched with the already enrolled signatures in the system. The basic steps are illustrated in Figure 2.1.

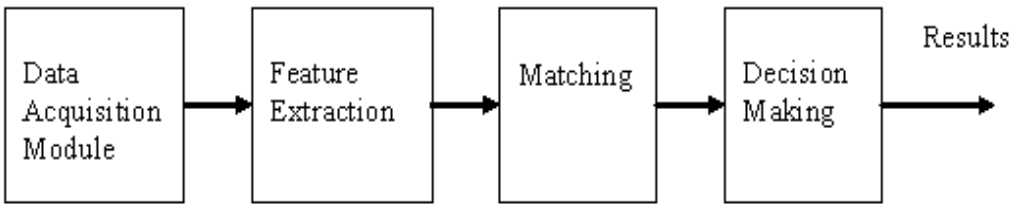

Figure 2.1: General Scheme for signature authentication

- *Data acquisition* - This is a process to obtain signatures from individuals for the purpose of both training and authentication purpose for the system.
- *Feature extraction* - In this process, certain features are extracted to concisely describe a signature. For some signature authentication techniques, preprocessing and normalization of data is done before the features are extracted.
- *Matching* - A sample signature of an individual is provided and its features are then extracted. The features of an individual's signature are matched with other features of signatures in the system's database.

- *Decision Making* - The system makes a decision whether the sample signature matches the signatures in the system's database based on the output of the matching algorithm (Faundez-Zanuy, 2005; Rioja et al., 2004; Zhu et al., 2000).

Figure 2.2 shows the data flow diagram of a dynamic signature verification system, one of the early works of Plamondon (Plamondon, 1995). The diagram shows a detailed model of steps used for dynamic signature verification system.

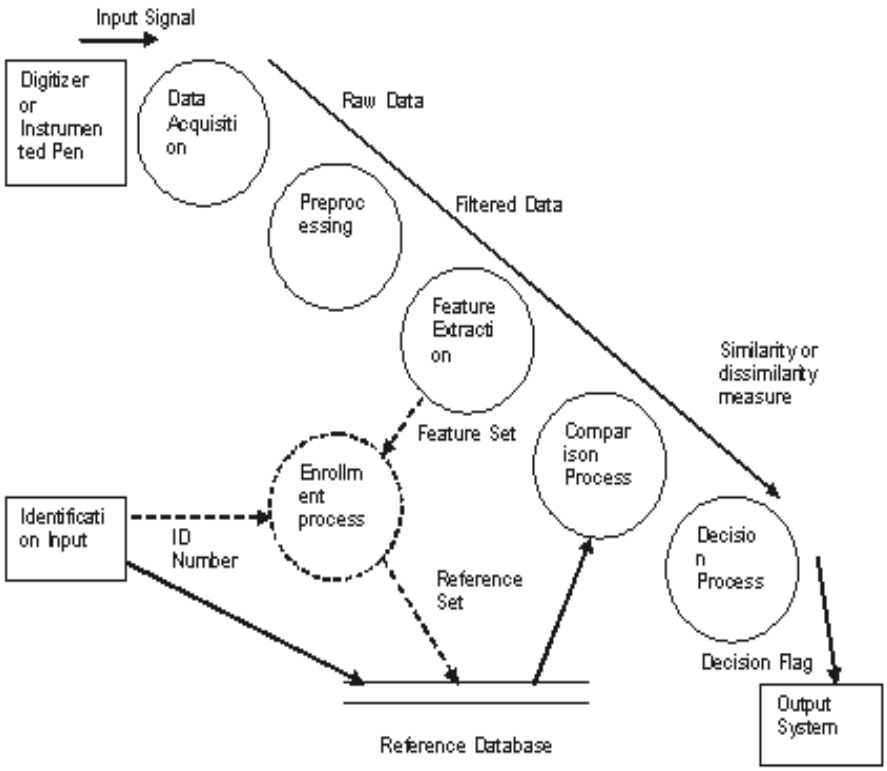

Figure 2.2: Data flow diagram of a dynamic signature verification system

2.4 Feature Types for Signature Authentication

Fairhurst & Kaplani (Fairhurst and Kaplani, 2003) state that it is important to seek identity verification modality which provides high degree in performance and yet is still acceptable by a majority of users. A signature can be authenticated either through static (off-line) or dynamic (on-line) verification.

- Static (off-line): In this mode, the signature is written, either on a piece of paper and then scanned or directly on the computer using devices such as the digital pad. The shape of the signature is then compared with the authentic signature (Faundez-Zanuy, 2005; Plamondon and Srihari, 2000). The difficulty with such a technique is that a good forger will be able to copy the shape of the signature.

- Dynamic (on-line): In this mode, the user writes his or her signature which is acquired in real-time. By using this set of dynamic data, further information such as acceleration, velocity, and instantaneous trajectory angles and displacements can be extracted (Faundez-Zanuy, 2005; Plamondon and Srihari, 2000).

Two types of features can be used for signature verification: parameters or functions (Plamondon and Lorette, 1989). For parameter based features, the features extracted from a signature forms a vector of elements, each one representative of the value of a feature. As for function based features, the signature is described in terms of a time-function, whose values constitute the feature set (Dimauro et al., 2004).

2.4.1 Function based Features

Table 2.1 presents some of the most commonly used function based features. Velocity is generally considered to be more informative than position and acceleration for dynamic signature authentication. The velocity profile can be used to classify a specific signature with great accuracy. It is one of the most widely used characteristics in describing a handwritten signature. Pressure and force functions have also been used frequently and specific devices have been developed to capture them directly during the signing process. The problem with the force and pressure features lies in the capture devices. Over time, pressure sensitive tablets can change and as a result affect the accuracy of authentication. In general, the advantage of having function based features is that it performs much better compared to parameter based features. The downside to it is the required complexity and large amount of time consumption in the classification stage (Dimauro et al., 2004).

Table 2.1: Function based features for signature verification

Feature	Type	References
Position	dynamic/static	(Sato and Kogure, 1982) (Mizukami et al., 2002)
Velocity	dynamic	(Wu et al., 1998) (Lorette and Plamondon, 1984)
Acceleration	dynamic	(Herbst and Liu, 1977) (Liu et al., 1979)
Direction of pen movement	dynamic	(Hangai et al., 2000) (Faundez-Zanuy, 2005)
Pressure	dynamic	(Sato and Kogure, 1982) (Rioja et al., 2004)
Forces	dynamic	(Crane and Ostrem, 1983)

2.4.2 Parameter based Features

Table 2.2 reports some of the popular parameter based features available. The average (AVE), the root mean square (RMS), the maximum (MAX) and minimum (MIN) values are derived from the position, displacement, speed and acceleration time-functions of a signature (Lee et al., 1996; Nelson et al., 1994). Parameters such as, Fourier, Hadamard and Wavelet transforms are determined from mathematical transforms (Castellano et al., 1990, 1988; Dimauro et al., 1997; Lam and Kamins, 1989; Letjman and George, 2001; Nemcek and Lin, 1974; Wu et al., 1998). Other typical parameters for on-line signature verification describe the signature apposition process, total signature time duration, pen-down time ratio, number of pen-lifts (pen-down, pen-up) etc (Lee et al., 1996; Nelson et al., 1994). Most of the parameter based features are useful when speed is a concern. Feature extraction and classification time is much lower in most cases when parameter based features are used. The downside to using parameter based features is that they might not be able to describe the signature as accurately as function based features will (Dimauro et al., 2004).

2.5 Review of Classification Models for Signature Verifier

Classification of the data involves assigning of new inputs to one of a number of predefined discrete classes. Classification is performed by partitioning the multi-dimensional feature space using statistical techniques or iterative learning algorithms. In some situations the separation may be linear but most real-world pat-

Table 2.2: Parameter based features for signature verification

Feature	Type	References
Position, Speed Acceleration and its AVE/RMS/MAX/MIN	dynamic/static	(Rioja et al., 2004) (Nelson et al., 1994) (Lee et al., 1996)
Positive/Negative Time duration of Acceleratio and Speed	dynamic	(Nelson et al., 1994) (Lee et al., 1996)
Mathematical Transforms	dynamic	(Lam and Kamins, 1989) (Castellano et al., 1988)
Total sig. time duration	dynamic	(Lee et al., 1996)
Pen down time ratio	dynamic	(Nelson et al., 1994)
Number of pen ups	dynamic	(Lee et al., 1996)

tern recognition applications involve non-linear partitioning of the feature space (Theodoridis and Koutroumbas, 1999). Examples of linear and nonlinear classification techniques are:

- Hidden Markov Models (HMM)
- Artificial Neural Networks (ANN)
- Naive Bayesian classifier
- Support Vector Machines (SVM)

Classifiers can be broadly categorized into two types; supervised and unsupervised classifiers. Supervised classifiers are provided with training patterns with known class labels and exploit the a-priori information of the training data.

The unsupervised classifiers are not given any training data with class labels. For such classifiers, the classification algorithms attempt to find the underlying 'similarities' and group the 'similar' feature vectors in one class.

There are a number of classifiers that are available. The selection of the suitable classifier is very important to ensure the success of the system. The next section describes some of the important classifiers.

2.5.1 Hidden Markov Models (HMM)

Standard HMM has been proven to be a useful tool for sequence pattern recognition (signature classification). HMM technique assumes that the input signals can be well characterized as a parametric random process known as Markov processes (Theodoridis and Koutroumbas, 1999). Many researchers have incorporated HMM as a classifier for their proposed signature verification system. Camino et al. (Camino et al., 1999) proposed a signature authentication system that incorporates HMM as their pattern recognition method. The recognition rates obtained decreased significantly as their sample sizes increased. Later, many other systems were designed and implemented using the HMM Model classification (Ferrer et al., 2005; Igarza et al., 2003; Muramatsu and Matsumoto, 2003; Zou et al., 2003). One of the systems proposed had a hybrid classification algorithm which consists of a Kohonen self-organizing map which find cluster centers in the training data and Hidden Markov Models which are trained to model the dynamics of signatures (Wessels and Omlin, 2000). The difficulty with using HMM as a classifier is the complexity of the sketch, leading to a level of HMM that would be computationally impossible (Theodoridis and Koutroumbas,

1999). Moreover, HMM is only suitable if the features can be characterized as a Markov process.

2.5.2 Artificial Neural Network

Artificial Neural Network (ANN) is a bioinspired iterative learning technique that learns from examples provided during training after which it is configured for the application. The major advantage of using ANN is the non parametric nature of the network and its suitability to be reconfigured for a user by a lay user (Theodoridis and Koutroumbas, 1999). This allows it to be one of the simpler tools for classification, provided sufficient amount of data is supplied to train the ANN. Studies have been done implementing ANN as the matching algorithm for signature verification purposes. In the early 90's, Lucas and Damper proposed a technique that can perform signature verification with high reliability using non-stochastic syntactic neural networks (Lucas and Damper, 1990). Early works from Lee (Lee, 1996) proposed three different neural network approaches for human signature verification, which were the Bayes multilayer perceptron, time delay neural networks and input-oriented neural network. The implementation of ANN as a classifier for signature verification were later proposed by many, such as, Rioja et. al.(Rioja et al., 2004), Martens and Claesen (Martens and Claesen, 1997), and, Pacut and Czajka (Pacut and Czajka, 2001). Although it is easy to configure an ANN for classification purposes, the major disadvantage of ANN is its time consuming training capabilities as well as its need for a large amount of sample data (Theodoridis and Koutroumbas, 1999).

2.5.3 Naive Bayesian

This classifier is considered one of the simplest probabilistic classifier due to the fact that it is based on probabilistic models which incorporate strong independence assumptions which often have no bearing in reality. However that is not always the case. Bayesian classifier relies on the assumption that the underlying probability values of the input data are known (Theodoridis and Koutroumbas, 1999). The advantage of this classifier is its simplicity and speed in computing the matching output. The disadvantage of this classifier is to determine the suitable probability function for the features. It may be possible to determine the probability function if the error of misclassification was random, but when attempting to identify a fraud who is attempting to forge the signature, it is not possible to estimate this probability. Srihari et al. (Srihari et al., 2004) used the Naive Bayesian classifier as a comparison to SVM and distance measures for signature classification.

2.5.4 Examples of other Classifiers

There are many other classifiers which have been proposed for the purpose of signature verification. Sakamoto et. al. (Sakamoto et al., 2001) used Dynamic Programming (DP) matching as the classifier for their techinique for the verification of signatures. DTW (Faundez-Zanuy, 2005; Hangai et al., 2000; Parizeau and Plamondon, 1990; Plamondon and Parizeau, 1988; Sato and Kogure, 1982) and tree-based matching (Parizeau and Plamondon, 1990; Plamondon and Parizeau, 1988) are some of the algorithms which have been used for the classification of signatures . DTW is an application of the DP techniques developed by Bellman in

the 50's (Bellman and Dreyfus, 1962). Tree-based matching is a method which estimates the distance between two signals by comparing the distance between their corresponding trees (Plamondon and Parizeau, 1988). Other statistical tools, such as kernel methods, have also been used, complementing the linear SVM in the classification of signatures. In the SVM, the kernel method replaces the scalar product used to calculate the distance between the input and the seperating hyperplane. This avoids the need of computing the transformed feature space which can be impossible for large-dimensional data (Kung et al., 2004; Webb, 2003). Ferrer et. al. (Ferrer et al., 2005) and Martinez et. al. (Martinez et al., 2004) have proposed a technique which uses SVM as its classifier.

Parizeau and Plamondon (Parizeau and Plamondon, 1990) have done a comparison between tree-based matching and DTW algorithm for signature classification. DTW matching algorithm, although less time consuming and requires less sensitivity in configuration, should only be used on y(t) based signal features whereas tree-based matching is time consuming (Parizeau and Plamondon, 1990).

A comparison between SVM and other classifiers have been done by Srihari et. al. SVM performed very well as a supervised classifier (trained with both genuine and forged signatures), whereas with a one-class SVM trained with only genuine signatures, its performance was very poor (Srihari et al., 2004). For real world application, it is not possible to obtain forged signatures for the training of classifiers.

2.6 Emotions on Handwriting and Signatures

Studies have shown that emotions do affect handwriting of a person (Gardner, 2002; Lange et al., 2006; Sackheim, 1990; Yank, 1991).Signature authentication is done often in our daily lives especially in banks, post offices, for credit cards and for access control. One of the main issues in choosing features to be extracted from signatures is determining whether the features extracted are able to withstand external factors which often affect our daily lives especially human emotions.

As stated before, part of this thesis is to investigate whether emotions have an effect on the selected features extracted from both a person's handwritten words and also his or her signature. Many studies have been conducted which shows that there is a variability in a person's handwriting when emotions are in play. The question would be whether signatures, just like any other form of handwriting, are affected by emotions. This study proposes to determine whether emotions have an impact on the dynamic signature of an individual.

Studies on handwriting and the human brain had been done since a long time ago, dating back to the 70's. Levy and Reid (Levy and Reid, 1976, 1978) proposed that there is a relation between handwriting posture and the cerebral organization. This had later been reconfirmed by Smith and Moscovitch (Smith and Moscovitch, 1979) and McKeever (McKeever, 1979). The question would be to what extent is the relationship between handwriting, in general, and the brain. The topic of interest now is whether handwriting and signature of a person would be affected by emotions.

There are many definitions and models in scientific literature on emotions. The part of emotions that is used in this thesis is the feelings component. In folk

psychology, feelings basically make up an important part of the overall complex phenomenon of emotion, and are most strongly associated with the term emotion.

Many studies have been conducted which shows that there is a variability in a person's handwriting when emotions are in play. Yank (Yank, 1991) has done studies on handwriting of people with multiple personality disorder (MPD). According to one of her research, Yank did studies on eleven women which were diagnosed with MPD and samples of handwriting were taken from alternate identities or personalities. Four inconspicuous handwriting characteristics were measured with electronic calipers under magnification. Yank (Yank, 1991) stated that writings of MPD patient often contain information specific to a particular alter who may express emotions repressed by other alters or provide information for which other alters are amnesic. She found that there was a significant variability in the handwriting samples produced by different alters but no consistent pattern was found.

Depue (Depue et al., 1994) have linked dopamine to a person's personality, emotion and temperament. From the study done by Lange, Mecklinger, Walitza, Becker, Gerlach, Naumann and Tucha (Lange et al., 2006) on the effects of dopamine on handwriting, it is shown that alterations of the dopamine system in a person's body adversely affect movement execution during handwriting. Their experiments showed that the number of inversions of the direction of the velocity profile increased in the subjects, irrespective of whether the subject was healthy or the subject was suffering from Parkinson's disease. The number of inversions in velocity represents a measure of the degree of movement automisation.

Based on the studies outlined in this section, it is known that emotions have an impact on handwritings (Gardner, 2002; Lange et al., 2006; Sackheim, 1990;

Yank, 1991). In literature, there does not appear any study that has analysed the impact of emotions on signature.

2.6.1 Graphology and Handwriting Analysis

Gardner (Gardner, 2002) once said that "The movements and corresponding levels of muscular tension in writing are mostly outside of conscious control and subject to the ideomotor effect. Therefore, emotion, mental state, and biomechanical factors such as muscle stiffness and elasticity are reflected in a person's handwriting." This is the basis of graphology.

Graphology can be defined as the study and analysis of handwriting that has strong connections or relations with human psychology or a person's behaviour. Many have sometimes incorrectly related graphology to forensic document examination. Just like forensic document examination, graphology uses the characteristics of a handwriting to determine a person but the difference is that graphologists believe that such handwriting minutiae are physical manifestation of the unconscious mental functions (Driver et al., 1996).

Graphology have longed been used in the field of handwriting analysis in order to determine the characteristics of a person. Graphology is useful for everything from understanding health issues and mental problems(Ludewig et al., 1992).

According to a book written by Sackheim (Sackheim, 1990), she claims that handwriting analysis is a behavioral study. Furthermore, she explains the relation between the characteristics of handwriting and mental processes. Sackheim also wrote on fear traits and ego defenses and its relation to handwriting samples. Moreover, she also explains in the book that handwriting of a person can reflect

the person's mood. In her conclusions, she also talks about how messiness of handwriting correlates with hysteria and how other handwriting traits project different personality of a person.

The question at hand is that if the dynamics of signatures are not affected by emotions, unlike handwriting, wouldn't the inclusion of an individual's signatures in the graphological process more accurately profile an individual? The study of whether emotions have an impact on the dynamics of signature would determine if signatures are useful in the field of graphology.

2.7 Summary

This chapter has talked about the different work and research done previously by different academicians on biometric authentication and signature authentication. It reports on biometric authentication in general, the basic signature authentication model, different types of features proposed by researches for extraction from an individual's signature and the different types of classifier algorithms which has been implemented through the years. The chapter further describes a little on the background graphology and handwriting analysis as well as the studies done which has shown how human emotions have affected people's normal handwriting.

Chapter 3

Feature Extraction and Classifiers for Signature Verifier

3.1 Introduction

This chapter describes the theory underpinning the research reported in this thesis. The emphasis of this chapter is on the feature extraction technique used for both dynamic and static features as well as the classifier used. It describes how the features were selected for the dynamic set and the theory behind the computation of the seven Hu moments for the static signature. This chapter also describes the theory of the Artificial Neural Network (ANN) and the statistical analysis classifier, the two classifiers which have been used for the experiments described in the later chapters.

3.2 Signature Authentication System

Any signature authentication system requires an underlying data feature extraction combined with pattern recognition. The role of pattern recognition is to identify the pattern class with minimum average risk (Wang and Chen, 2003). The system takes the features of the unknown subject and determines the class membership. This is done by selecting the class which is closest to the sample, which can be determined through highest probability or shortest distance.

A Pattern recognition system can be considered to have two aspects:

1. enrolment (training)
2. matching (Matyas and Riha, 2003)

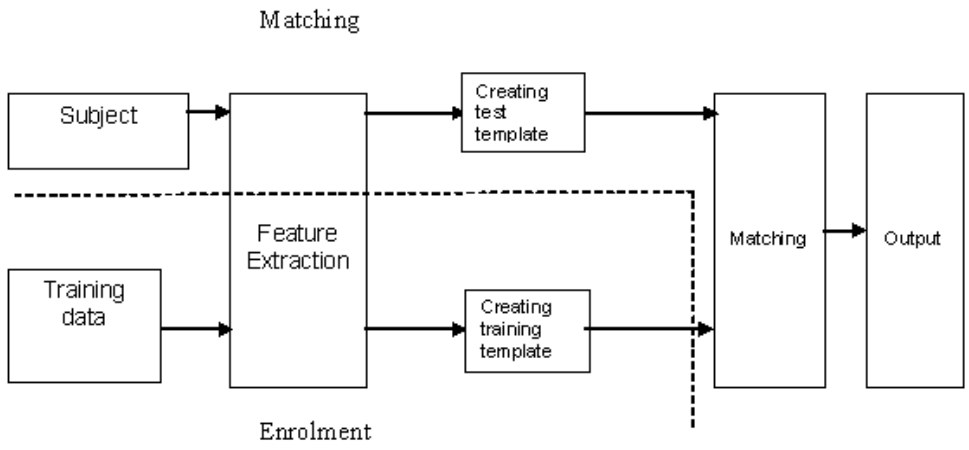

Figure 3.1: Signature Authentication Model

The Figure 3.1 is a diagram depicting the signature authentication model on which the experiments performed during this research are based. The bottom half of the diagram shows the steps for enrolment while the rest of the diagram

shows the process of feature matching to generate the output of the system. Each of these has been detailed below.

The enrolment process is a combination of the following:

1. *Acquiring samples*: In this step of the experiment, the necessary data that represents the individual's identity is acquired. This data is to be used to train the system for the purpose of matching.

2. *Feature Extraction*: In this step the relevant features are extracted that can be best used to represent the uniqueness of the authentic individual. It is important that irrelevant features are discarded while the suitable features that provide the maximum distinguishing between the individuals are selected.

3. *Storing master template*: The features of the sample are stored as a template in a database and this represents the authentic individual to be verified. The template is later used to compare against the live signature of an individual during matching.

The matching process is to match the signature of the unknown person with that of the authentic user and confirm or negate the identity. The data acquisition step is similar to the one during enrolment. The steps for matching process is as follows:

1. *Creation*: This step extracts the same set of features from the sample signature of the individual. This set of features are made into a template similar to the template stored during the training process. Normalisation may be required at this stage.

2. *Comparison*: In this step, the newly created template is compared against a specific template or all the other templates stored in the database, depending on its application. The verification of identity would typically require the comparison of this template with the template of the authentic user, while the identification of the individual would require the comparison with all the templates stored. For a neural network, the newly created template is input into a neural network which is trained using all the master templates stored.

3. *Decision*: The final step is to decide the class membership of the the newly created template (Matyas and Riha, 2003). This decision may be one to many, such as for the identity of an individual from a pool of known users or one to one, such as to validate the identity of the unknown against claimed identity.

3.3 Feature Extraction

The selection of features for extraction is critical to the performance of a biometric authentication system. The features extracted have to be able to describe the signature, separable between classes and also invariant within the same class. As described in chapter 2, two types of features can be extracted for both dynamic and static feature sets. They are parameter based features and function based features. In general, function based features allow better performance than parameters, but they usually require time-consuming matching procedures (Dimauro et al., 2004). Parameter based features are both easily computed and matched due to its simplicity.

When creating a system, it is important to take into account many different external factors. For example, for a bank or teller application, the retrieval of features and computation of matching has to be quick as well as accurate for feasibility for such an application. For daily access control, depending on the level of security, speed is an issue. The cost of building a system is also an issue for certain applications. While many people have tried to incorporate biometric features into smart cards or digital memory, recent studies show that one of the main issues concerning the reliability is the need to suitably encrypt the data to be stored for the security of sensitive information (Panotopoulos and Psaltis, 2001) and need for real time analysis (Nixon et al., 1999).

Certain criterions have to be established during feature extraction to ensure the suitability of the feature set. Below is the list of the criteria which act as a guideline to obtain the appropriate features.

1. Selected features must have a high inter-personal variance to ensure that the signatures are separable between different classes. This allows for low error rates during classification.

2. Selected features must have a low intra-personal variance. This will allow for the same type of signatures to group together, enabling better performance for the system.

3. The features set should be fast, simple and easy to compute in order to have a system which requires low computational power.

4. The amount of features chosen has to be small enough to be stored in a smart card. The smaller number of features will in turn allow for quicker and faster computation.

5. The number of features should be large enough to ensure that the signatures of different subjects are distinguishable with minimum risk.

6. Selected features cannot be reverse-engineered to obtain the original sketch of the signature. This is to ensure that even if the features were to be obtained, although encrypted, the original sketch of the signature is still unknown.

The two different sets of features, dynamic and static features, are described in the next section. The dynamic feature set consists of 10 different global parameter based features whereas the static feature set consists of the seven moments of Hu.

3.3.1 Dynamic Feature Set

The dynamic feature set describes how the signature is signed rather than how it looks. Dynamics of the signature are very difficult to imitate (Li et al., 2001) because these not only have the information of the overall shape of the signature, but also information of the individual strokes and the speed of the different strokes. When the user signs on a digital tablet, the tablet needs to be scanned at a rate high enough to capture this information, and from this dynamic data, relevant features are extracted.

For this research, the dynamic feature set chosen consists of global parameter based features which allows for easy and quick computing. This feature set requires less computational power and is more cost efficient although it might not perform as well comparatively to function based feature sets. This paper reports a choice of 12 features that provide the required information related to the dynamics of signing. The list of dynamic feature set is as follows:

1. *Total time to sign (1 digit)* This feature describes the time taken to sign the signature. This is obtained by counting the number of coordinates recorded while the individual is signing. Each coordinate is sampled at a constant rate.

2. *Number of pen-ups (1 digit)* The feature recorded shows the number of times the pen leaves the screen during signing. While recording, a ";" is recorded every time the pen is up and the number of ";" is the number of pen-ups occurred during signing.

3. *Total length (1 digit)* This is the total length of the signature calculated by adding the distance between each of the coordinates.

4. *Max velocity (1 digit)* This is the maximum velocity found during signing between two consecutive coordinates.

5. *Min velocity (1 digit)* This is the minimum velocity found during signing between two consecutive coordinates.

6. *Duration of $Vx \geqq 0$ (1 digit)* This feature describes the total time that the pen is moving from left to right. This feature is obtained by adding up the amount of times it is found that the pen is moving from left to right between two consecutive coordinates.

7. *Duration of $Vy \geqq 0$ (1 digit)* This feature describes the total time that the pen is moving from down to up. This feature is obtained by adding up the amount of times it is found that the pen is moving from down to up between two consecutive coordinates.

8. *Duration of $Vx \leqq 0$ (1 digit)* This feature describes the total time that the pen is moving from right to left. This feature is obtained by adding up the amount of times it is found that the pen is moving from right to left between two consecutive coordinates.

9. *Duration of $Vy \leqq 0$ (1 digit)* This feature describes the total time that the pen is moving from up to down. This feature is obtained by adding up the amount of times it is found that the pen is moving from up to down between two consecutive coordinates.

10. *Length of signature horizontal (1 digit)* It describes the width of the signature. This feature can be found by subtracting the maximum x coordinate with the minimum x coordinate.

11. *Length of signature vertical (1digit)* It describes the height of the signature. This feature can be found by subtracting the maximum y coordinate with the minimum y coordinate.

12. *Area of signature (1 digit)* This feature can be found by multiplying both the length of the signature vertically and the length of the signature horizontally.

Figure 3.2 below shows the statistical analysis of the features for 3 subjects. The mean and standard deviation of the features of 3 subjects have been derived from the training data of these 3 subjects. The training data consists of 10 signatures from each of the subjects.

The histogram plots in Figure 3.2 shows the mean and standard deviation of each feature extracted from three different subjects. The line plot from Figure 3.3

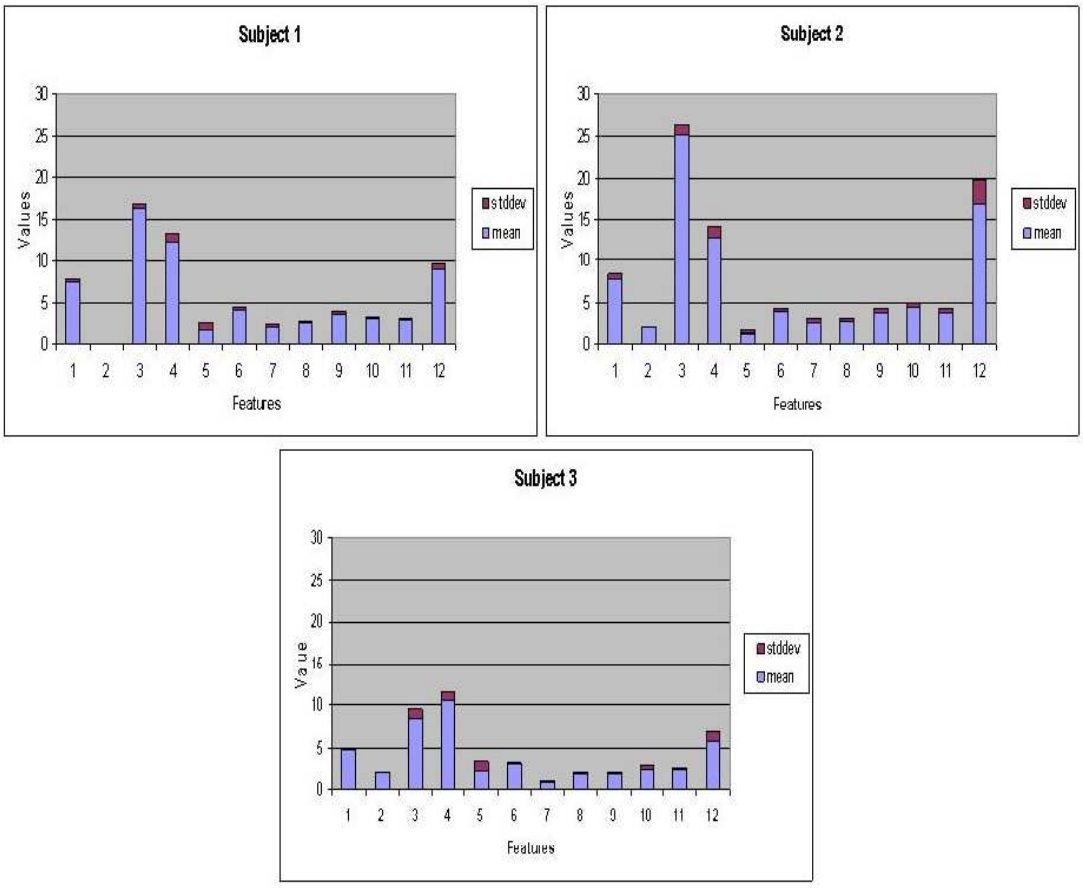

Figure 3.2: Histogram plot of mean and standard deviation of features (Feature Value vs Feature No.) for subjects 1, 2 & 3

shows the difference in the mean between each of the three subjects. The features are numbered according to the list compiled previously. It is observed from the histogram plots that the ratio of each feature's standard deviation to its mean is very small. From the observation of the line plot, the means of each feature obtained from subjects are different. From visual analysis of the histogram plots and the line plot of the three subjects, it is confirmed that the features extracted are suitable for describing an individual's signature as well as differentiating it between different types of signatures.

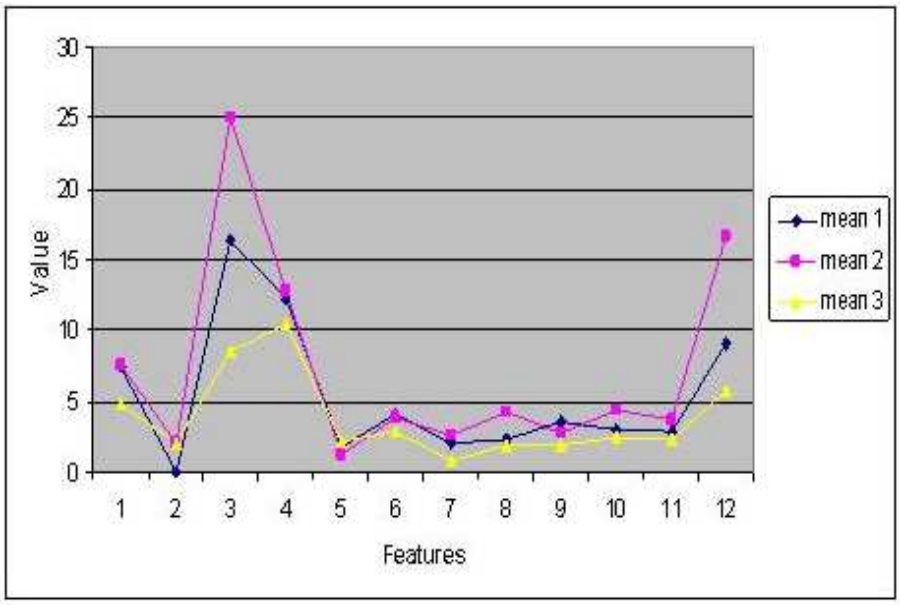

Figure 3.3: Comparison of mean for each feature (Mean Value vs Feature No.) of subjects 1, 2 & 3

Numerous preliminary experiments were done using the ANN. After the preliminary experiments, 10 out of the 12 features were selected. The two features that were dropped were (i) min velocity (feature 5) and (ii) the area of signature (feature 12). By observation from the line plot and from the preliminary experiments done, the subject's feature 5 is quite close to each other. Although the area of signature feature (feature 12) has a very good inter-personal, its standard deviation to mean ratio is one of the largest compared to the rest of the features. Based on the guidelines in Section 3.3, these features are not suitable. The rationale for this is:

- The min velocity (feature 5) has a low inter-personal variance. This may be because, at one point of each person's signature, the person's signing velocity slows down to a minimum. The minimum velocity at that point

would be the same for many people. This would make it hard for the system to differentiate between different people (in terms of that particular feature alone), which in turn, would affect the performance of the system.

- The area of signature is calculated from the length of signature horizontally multiplied by the length of signature vertically. Since the area of signature consists of these two variables, the variance of this feature will naturally be the multiplication of both the variance of the two variables. Its variance will be amplified, which makes it hard for the system to accept genuine signatures of a person. This feature will have a high intra-personal variance.

3.3.2 Static Feature Set

Static signature of an individual when read by a machine is the image of the signature. The verification of the static signature requires automated classification of the image. Some of the challenges associated with the signature of the person are the high variation among the signatures of the authentic user. These are largely associated due to rotation, translation and scaling. The issue with the classification of the image of the signature is the need to identify suitable features that best represent the shape of the signature and are small enough for easy storage and classification.

Hu moments are statistical moments that can be used to describe the image of a signature. Hu moment are derived from geometric moments. Moments computed from the images are very concise and can represent the global characteristics of the objects' shapes within the image (Zhang and Lu, 2004). In this context, Hu moments can be considered to be translation, rotation and scale in-

variant, and descriptors of the shape of the image, thus suitable for representing the image of a signature.

Geometric moments are computed by projecting an image function onto a set monomial function $\{X^p, Y^q\}$. Let the image function be denoted as $f(x, y)$, where, $f(x, y) = 1$ for each recorded coordinate
else = 0

For the image function of a signature, $f(x, y)$ of size $N * M$, the geometric moments are defined as

$$m_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} x^p y^q f(x, y) \tag{3.1}$$

where m_{pq} is the $(p+q)^{th}$ order moment of the continuous image function $f(x, y)$ and p,q = 0,1,2...

Geometric moments defined in Eq.3.1 are not invariant to rotation, translation and scaling. Translation invariance of the features can be achieved by placing the centroid of the image at the origin of the coordinate system (x, y). This results in the central moments to be:

$$m_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (x - \bar{x})^p (y - \bar{y})^q f(x, y) \tag{3.2}$$

where

$$\bar{x} = \frac{m_{10}}{m_{00}}; \bar{y} = \frac{m_{01}}{m_{00}} \tag{3.3}$$

The central moments can be further normalized to achieve scale invariant as

defined by

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\sigma}} \tag{3.4}$$

where

$$\eta_{pq} = \frac{p+q}{2} + 1 \tag{3.5}$$

The low order geometric moments represent the fundamental geometric properties of the image distribution function $f(x, y)$. The zeroth order moment m_{00} which is the mean of the distribution function represents the total mass of the image. Thus, the m_{00} computed for a silhouette image of a segmented object indicates the total object area. The first order moments (m_{01}, m_{10}) are used to compute the centroid of the image as shown in Eq.3.3 above. On the other hand, the second order moments (m_{11}, m_{02}, m_{20}) are also known as the moments of inertia and can be used to determine useful image properties such as the image ellipse, principal axes and the radii of gyration of an image. The higher order moments describe the finer details of the shape of the image.

The normalized central moments are invariant to changes in position and scale of the mouth within the image. Therefore, normalized geometric moments computed using Eq.3.4 are invariant to translation and scaling. Nevertheless, the normalized geometric moments are not invariant to the rotational changes.

Hu (Hu, 1962) introduced seven nonlinear combinations of normalized central moments that are invariant to translational, scale and rotational differences of the image patterns. These seven moments are known as the Hu moments. Hu moments are derived based on theory of algebraic invariants. The seven Hu

moments from 0^{th} up to 3^{rd} order are defined as

$$M_1 = \eta_{20} + \eta_{02} \tag{3.6}$$

$$M_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2 \tag{3.7}$$

$$M_3 = (\eta_{30} - \eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \tag{3.8}$$

$$M_4 = (\eta_{30} - \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \tag{3.9}$$

$$\begin{aligned} M_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} - \eta_{12})[(\eta_{30} + \eta_{12})^2 - (3\eta_{21} + \eta_{03})^2] \\ + (3\eta_{21} + \eta_{03})(\eta_{21} + \eta_{03})[3(\eta_{30} - \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \end{aligned} \tag{3.10}$$

$$M_6 = (\eta_{30} - 3\eta_{12})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \tag{3.11}$$

$$\begin{aligned} M_7 = (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(3\eta_{21} + \eta_{03})^2] \\ + (\eta_{21} - 3\eta_{12})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - \eta_{21} - \eta_{03}^2] \end{aligned} \tag{3.12}$$

The functions $M1$ to $M6$ remain invariant under rotation, reflection and also a combination of rotation and reflection. The seventh moment invariant is skew

invariant defined to differentiate mirror images and is only invariant to rotation and changes sign under reflection. The scale and translation invariance of $M1$ to $M7$ is provided by the normalized central moments μ_{pq}. The higher order (>3) Hu moments are difficult to be derived from geometric moments. These seven Hu moments are used in this paper as static features to represent the image of a signature.

Static Hu moments were chosen as the static feature for this research because of its ability to concisely represent the global characteristics of the image of a signature. Moreover, these moments are quick, easily derived and require little computational power. They are also small enough for easy storage and classification.

The purpose for the static feature in this thesis is to compare the performance of a static feature based verifier against a dynamic feature based verifier. In order to obtain the optimum set of features for extraction which fit all the criterions stated, both static and dynamic features have to be looked into and compared.

3.4 Classifiers

The complexity of a classification task is dependent on the variability of the feature values of the observations of the same class relative to the difference between feature values of the observations of different classes. The variability of the feature values for inputs in the same class may be due to the underlying model of the features or noise (Duda et al., 2001). In a signature validation system, the noise associated with classification of visual speech features is due to device, while the variation in the signature of the authentic user is the underlying

model variation. It is impossible for classifiers to yield perfect performance due to presence of noise and variability in the data such as signature features. This misclassification is measured as the error rate. It is desirable to keep this error rate as low as possible to ensure the robustness of the applications.

There are two types of learning for different classifiers which can be used. They are:

- *Supervised learning* In supervised learning, the training data provided consists of a pair of input data and its targeted class. This method is similar to "informing the classifier that this data belongs to this class and asking it to learn." Learning of such a classifier requires training with substantial examples (input and target pairs) to learn the patterns of each class.

- *Unsupervised learning* In unsupervised learning, the training data is not provided in a form of input-class pair. Input data is provided but its target class is not known. These classifiers are self-learning and involve the partitioning of the data in the feature space into subgroups without predefined input and target pairs. Most applications fall within the domain of estimation problems such as statistical modelling, compression, filtering, blind source separation and clustering.

In this research, two different classifiers; ANN and statistical analysis classifier, have been used to conduct the experiments. As stated earlier, this thesis investigates the performance of the ANN and the statistical analysis classifier. The reason behind using these two classifiers will be discussed in the folowing sections, which describes both the ANN and the statistical classifier.

3.4.1 Artificial Neural Network

The Artificial Neural Networks (ANN) is inspired by the functionality of human brain's neurons (Hagan et al., 1996). A plexus of connected or functionally related neurons in the peripheral nervous system or the central nervous system is known as biological neural network. Artificial neural networks were designed to model some properties of biological neural networks, though most of the applications are of technical nature as opposed to cognitive models.

The major advantage of using ANN is the non parametric nature of the network and also the ability of ANN to classify data, without making assumptions on the underlying statistical distribution of the data (Lippmann, 1987). Another major advantage is its suitability for being used with high dimensional data set. The ability of ANN to adapt and learn is important when designing a reconfigurable system due to the presence of authentic signature variability (Theodoridis and Koutroumbas, 1999). The disadvantage of ANN is that while ANN is simple to use, it does not provide the user with information about the closeness of the data making it difficult to optimise it. Moreover, a rather large number of training samples is required to properly train the neural network before it can classify any inputs. In this research, the ANN used is fully supervised. For application in the real world, it is not possible to obtain a set of training data which consists of both genuine and forged signatures or a combination of both an individual's or other user's signatures. Therefore, it is more feasible to have a semi-supervised classifier, where only a small amount of data of one class is needed to accurately classify the signatures. Hence a second classifier, statistical analysis classifier, is used (discussed in section 3.4.2). As a starters tool, ANN is very useful as it is

easily configured with enough data, making it one of the simpler classification tools.

The type of neural network that was used during this research is known as a feed forward multilayer perceptron which consists of 2 hidden layers. The nodes of the 2 hidden layers are configured to the logsig transfer function. MLP ANN was selected due to its ability to work with complex data compared with a single layer network. Due to the multilayer construction, such a network can be used to approximate any continuous functional mapping (Bishop, 1995).The network is trained by back-propagation algorithm. The data is arranged in such a way that backward propagation finds the minimum mean squared error approximation to the Bayes discriminant function which minimizes the misclassification error probability.

3.4.1.1 A Brief Description of Neural Network

(This section may be skipped by the reader familiar with the topic.)
Neural networks are made of units known as neurons, where their states can be described by single numbers, their "activation" values. Each unit generates an output signal based on its activation. Units are connected to each other very specifically, each connection having an individual "weight". Each unit sends its output value to all other units to which they have an outgoing connection. Through these connections, the output of one unit can influence the activations of other units. The unit receiving the connections calculates its activation by taking a weighted sum of the input signals. The output is determined by the activation or also known as transfer function. Networks learn by changing the weights of the connections.

Neural networks have a remarkable ability to derive meaning from complicated or imprecise data. With this, it is able to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques.

3.4.1.2 Neuron

In an engineering approach, an artificial neuron is a device with many inputs and one output. The model of an artificial neuron is shown in the Figure 3.4. There are two adjustable parameters here in a neuron which are the weights, W, and the bias value, b. The inputs are 'weighted' and the effect that each input has at decision making is dependent on the weight of the particular input. The weight of an input is a number which when multiplied with the input gives the weighted input. These weighted inputs are then added together with the bias value, b, and put through a transfer (activation) function, f. The transfer function acts as a thresholding function to produce an output if the accumulated input reaches a certain value.

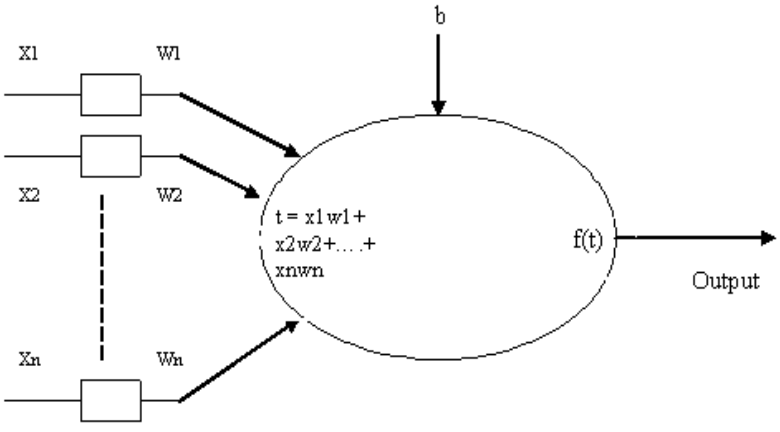

Figure 3.4: General model of a neuron

There are several types of transfer functions that can be used in ANN. The choice of thresholding function is depending on the type of the application. The most commonly found transfer function is the Log-Sigmoid (logsig) function. t is used mainly when back propagation algorithm is used for training. The mathematical formula is as stated in Eq.3.13, where a is the gradient of the slope and v is the net input. The plot of the logsig function is shown in Figure 3.5.

$$\phi(v) = \frac{1}{1 + e^{-av}} \tag{3.13}$$

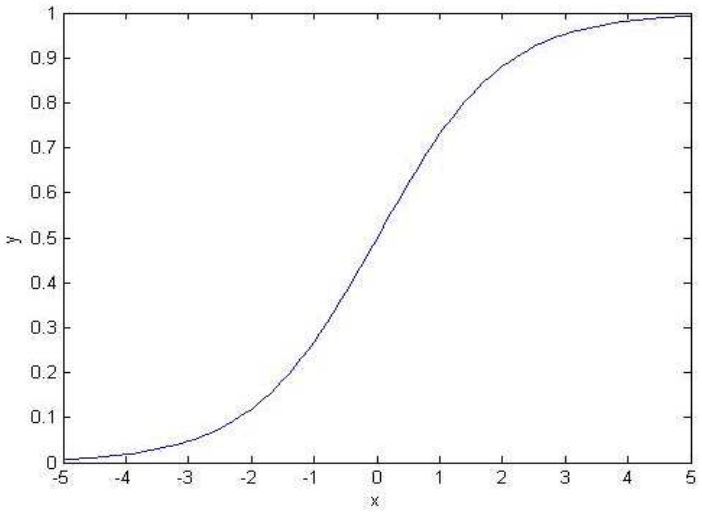

Figure 3.5: Logsig

3.4.1.3 Architecture

In general, a neural network is composed of a group or groups of physically connected or functionally associated neurons. A single neuron can be connected to many other neurons and the total number of neurons and connections in a net-

work can be extremely large.

Feed Forward Multilayer Perceptron Network

The simplest form of neural network is called a perceptron which consists of a single neuron. The multilayer perceptron consists of a set of input nodes (input layer), one or more hidden layers and a set of output nodes (output layer). The hidden layers are defined as the layers of nodes in between the input layer and the output layer. The nodes within the hidden layers do all the computation. The hidden layers enable the network to learn complex task.

A feed forward neural network is an ANN where connections between units do not form a directed cycle. Feed forward ANNs only allow signals to travel one way only from input to output, through the hidden layers if any. There are no feedbacks or loops within this network. Feed forward ANNs tend to be straight forward networks that associate inputs with outputs. They are extensively used in pattern recognition.

Figure 3.6 on the next page shows a feed forward multilayer perceptron network which consists of a single layer of hidden node. As observed in the figure, the arrow signifies the route of information which travels from the input layer through the hidden layer and on to the output layer. There are no loops within the network which allows information to be fed back. The information only travels from left to right. The level of complexity of this network is dependant on the number of nodes and hidden layers within the network.

For the hidden layers in a multilayer perceptron to function properly, the nodes in the hidden layers must have a non-linear transfer function. One of the most commonly used non-linear transfer function is the logsig function.

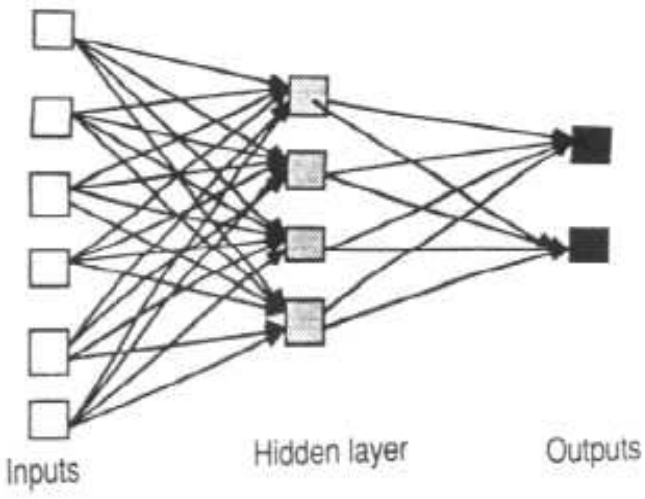

Figure 3.6: Feed forward multilayer perceptron network

Back Propagation Learning Algorithm

The back propagation learning algorithm is the most commonly used algorithm in training a feed forward neural network. It uses an iterative gradient descent algorithm designed to minimize the mean squared error between the output of the neural network and the desired output or target provided by a supervised training data.

The back propagation process requires two passes through the network which are the forward pass and the backward pass. During the initial forward pass, the weights are assigned randomly. The signal is pass forward to obtain an output. The output of the network is then subtracted from the desired output to obtain an error signal which is then propagated back through the network during the backward pass. During this pass, the weights are adjusted accordingly to make the actual output closer to the desired target. The process is repeated until

the minimum error rate is achieved. Back propagation usually allows for quick convergence on satisfactory local minima for error.

Figure 3.7 shows the schematic of information flow of the back propagation learning algorithm. The diagram shows the weights change according to the error signal propagating backwards.

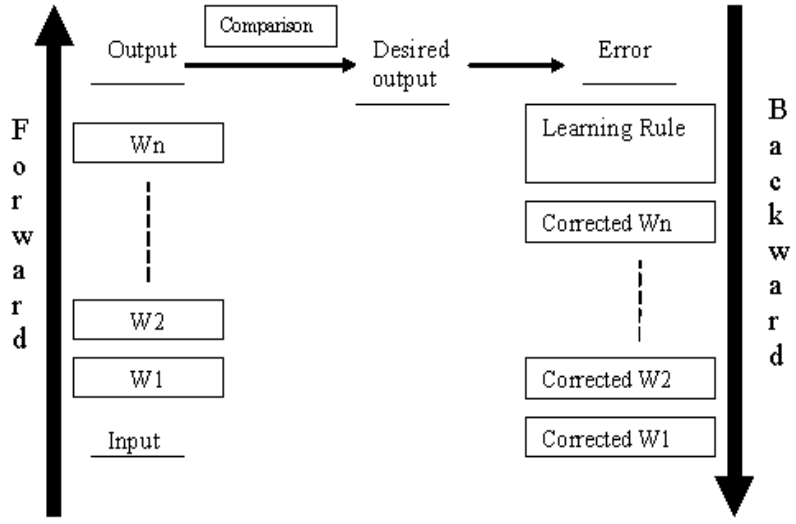

Figure 3.7: Schematic of information flow for back propagation algorithm

3.4.2 Statistical Analysis Classifier

This classifier was built based on the purpose of overcoming the shortcomings of the ANN classifier. The statistical classifier takes the probability of each of the feature of an individual's signature being equal to its respective feature of a signature enrolled in the database and computes the total score by combining the probabilities, following certain rules, in order to decide whether that signature matches the enrolled signature it is being compared to. If the score is higher than the threshold, the signature matches the enrolled template.

There were assumptions that were made in order for the classifier to work properly.

- The probability distribution of each of the features was needed to be estimated. It is observed earlier at the start of the chapter that the features of an individual's signatures are all centered on a mean and varied very little. Therefore, if a feature extracted from a signature is very close to the mean, it has a high probability of it being in the same feature category, else, it will have a low probability. Hence, it was assumed that the features were normally distributed.
- Each feature was assumed to be independent of one another.

3.4.2.1 Training of Classifier and Template Creation

The training of the classifier involves obtaining the estimated mean and variance of each of the features of an individual's signature. The equations for estimating the mean and variance of a feature are as follows.

Mean: Given a random sample X1, , XN (N independent variables with the same distribution as X), the sample mean is calculated as follows.

$$\hat{x} = \frac{1}{N}\sum_{k=1}^{N} x_k \tag{3.14}$$

Variance: For a given sample y1, , yn (n number of samples), the equation for the sample variance is shown below.

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{N} (y_i - \hat{y})^2 \tag{3.15}$$

The equation can be further simplified to,

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{N}(y_i)^2 - \frac{n}{n-1}(\hat{y})^2 \tag{3.16}$$

Each of the features' estimated mean and variance is obtained and this forms a template belonging to that particular individual. The template also consists of a matching threshold which will be discussed later on.

3.4.2.2 Statistical Testing of an Individual Feature

By assuming that the features are normally distributed around its mean, a p-value can be obtained for each of the sample features. The p-values indicates how close each of the features are to its mean. For each sample feature, a sample score can be computed using the p-value. For a sample feature x distributed on N(0,1), if x is positive, the sample score = 1 - p-value. If x is negative, the sample score = p-value (interested in only one half of the graph).

Figure 3.8 shows the probability density plot of a normal distribution with mean of 0 and variance of 1. Consider an example with three samples, X1, X2 and X3 (X distributed on N(0,1)). If X1 value is the closest to the mean and X3 value is the farthest from the mean, then X1 will have the largest sample score, followed by X2, and X3 having the smallest sample score.

The equation below shows the probability density function of a normal distribution on mean μ and variance s^2. The function shown below is a Gaussian function.

$$\rho_{(\mu,\sigma^2)} = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{3.17}$$

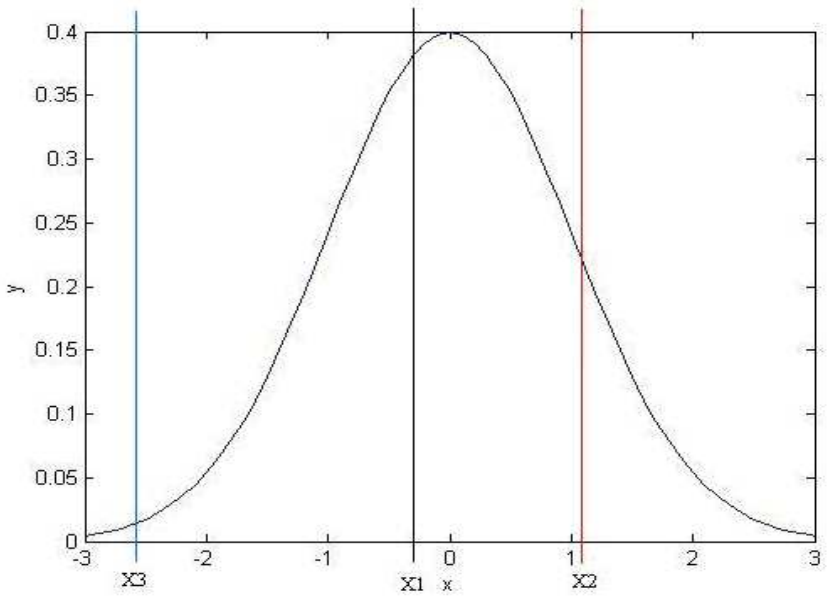

Figure 3.8: Normal distribution plot mean = 0, variance = 1

For $\mu = 0$ and s2 = 1, the probability density function can be simplified as,

$$\rho_{(0,1)(x)} = \frac{1}{\sqrt{2\pi}} e^{-\frac{(x)^2}{2}} \tag{3.18}$$

Therefore using the equation above, the p-value can be obtained as follows.

$$p - value = Pr(x \leqq X) = \int_{-\infty}^{x} e^{-\frac{(x)^2}{2}} \tag{3.19}$$

The sample score is obtained through the following:

If x=0, Sample score = p-value

Else, Sample score = 1 - p-value

The steps of obtaining p-value for a feature are listed below.

1. The estimated mean and standard deviation of the feature is obtained, μ and σ respectively.

2. Since it is assumed that a feature is normally distributed on N (μ, σ), the respective sample feature is also naturally distributed on N (μ, σ).

3. The sample feature, f, has to be normalized to normal distribution N(0,1). Using the formula Eq.3.20, f can be normalized on N (0, 1).

$$Y = \frac{(f - \mu)}{\sigma} \tag{3.20}$$

4. With the newly found sample feature, Y, the p-value can be found by using the equation Eq. 3.19.

5. Since we are only interested in one half of the normal distribution N (0, 1), if Y is positive, the sample score = 1 - p-value. If Y is negative, the sample score = p-value.

6. In the case where $\sigma = 0$, if f = μ, the sample for that sample feature is 0.5 (maximum value). If not, the sample score is 0.

3.4.2.3 Matching and Threshold

With each of the features' sample score obtained, the next step is to compute the final score for the signature. The sample scores are then added up to obtain the final score. The larger the final score, the closer the sample data is to the template it is compared to.

As for the threshold, it is obtained by inputting the training data into the matching algorithm stated. The training data used for enrolment is used as the

testing data in order to find the threshold. The training signature that has the lowest final score is used as the threshold.

There are rules which need to be followed for both matching and obtaining the threshold. The rules are listed as follows.

1. Threshold has to be greater than 1. If the lowest final score is less than 1, the next lowest score is used.

2. If 3 or more of the features does not lie within +- 1.5σ of its mean, the sample data is rejected without even computing the final score.

3. A sample data is only classified in that class if the sample data complies with rule (2) and its final score is greater than the threshold of the class it is compared to.

3.5 Summary

This chapter has briefly described the theory for feature extraction of signature authentication. It also described how the features were chosen for the dynamic set and the theory behind the seven Hu moments for static features. This chapter has also described the feed forward back propagation-trained multilayer perceptron ANN model and its advantages and disadvantages in using it as a classifier. The statistical classifier, which uses probability models to describe the features, is also described. The performance of both the classifier is later analysed in chapter 4.

Chapter 4

Performance Analysis of Dynamic Signature Verifier - ANN and Statistical Analysis

4.1 Introduction

This chapter reports on the experiments conducted to analyse the performance of the dynamic signature verifier based on the ten selected features. Two sets of experiments were conducted. The purpose of the first set of experiments was to validate the choice of the features and confirm if the dynamic features selected were separable between classes as well as whether they are sufficient for signature classification. This experiment was conducted by classifying the data using Artificial Neural Network (ANN). The same set of features was then used in the second set where a statistical analysis classifier was used instead. The purpose of the second set of experiment was to study the distances between the different

features to determine the robustness and to compare the performance of the dynamic signature verifier based on two different classifiers. The results from the first set of experiments (ANN) were compared with the results obtained from the second experiment (statistical analysis). This was done to determine which of the two classifier was most suitable.

The experimental protocol was approved by the Human Experiments Ethics Committee of RMIT University. The participants were verbally and in writing informed of the experimental details in plain language and signed the consent forms. The experiments consisted of two sections:

1. The first set of experiments (Section 4.2) validates the choice of the features and confirms if the dynamic features selected were separable between classes as well as evaluates the performance of the ANN for the dynamic signature verifier. In this section, three experiments were done. The first experiment was done using 4 subjects, with each of them signing 15 times. The purpose of the first experiment is to examine the ability of the verifier to identify the signature of a user in a small sample population. The second experiment was done with 5 subjects trying to imitate a signature given by a user. This experiment was to determine if the verifier was able to successfully reject a forger. The first 2 sets of experiments acted as preliminary experiments to show that the features chosen were able separate signatures of different individuals as well as differentiate genuine signatures from forgeries. Therefore, a small group of subjects were used. The third experiment was conducted in a similar way as the first experiment. Unlike the first experiment, the third experiment used a much larger subject database. The results of these experiments were then tabulated, discussed

and compared with the statistical analysis classifier.

2. The second section of this chapter (Section 4.3) evaluates the accuracy of the dynamic signature verifier which uses statistical analysis as its matching algorithm. This experiment firstly tested the system's ability in verifying the user correctly. Secondly, it determined if the system was able to successfully reject an imposter who is actively trying to forge a signature. A total amount of 20 subjects were gathered to conduct this experiment. The results were then tabulated, discussed and compared with the results from the first set of experiments conducted using the Artificial Neural Network.

For the 2 types of experiments decribed earlier, users were not put under different conditions, such as when they were standing up or sitting down, exposed to different weather or whether they were indoor or outdoor. The reason for this is that most real life applications of a signature verification system are used indoors. Therefore, the experiments were not done under different weather conditions. Furthermore, the situation of whether the users were standing up or sitting down was not noted and was random throughout the whole database of signatures. The same pen was used throughout the experiments because it is assumed that pens for signature capture in real life situations do not differ much.

As for the forgery database, obtaining professional forgers was very difficult. Therefore in order to mimic as close as possible to professional forgers, all of the forgers in the experiments had been trained using the genuine sample signatures given. They were given time to practice forging a sample signature. A tracing guide of the sample signature was also provided during sampling test forged signatures.

The criterion for the performance of the system was measured by the ability of the system to identify the authentic user and to reject an impostor. As with any security system, given that the subject is, or is not, a true instance of the enrolled subject, there are four possible outcomes of the errors (Duda et al., 2001). These measures of accuracy are:

- Acceptance of Authentic Enrolled Subject (AA) or Genuine Accept Rate (GAR)
- Acceptance of Impostor Subject (IA) or False Accept Rate (FAR)
- Rejection of Authentic Subject (RA) or False Reject Rate (FRR)
- Rejection of Impostor Subject (RI) or Genuine Impostor Rejection (GRR)

The biometric system accuracy requirements depend greatly on the application. In forensic applications, such as in criminal identification, FRR rate (and not FAR) is the critical design issue, because we do not want to miss a criminal even at the risk of manually examining a large number of potentially incorrect matches that the biometric system identifies. Many civilian applications such as digital signatures for electronic document authentication require the performance requirements to lie between these two extreme limits of both the FAR and the FRR. The application of the current system ensures that the impostor is rejected, while minimising the rejection of the authentic user. It was thus desirable to have FAR as close as possible to zero. In a performance analysis of a biometric system, it is also important to consider trained and target-selected forgers in order to accurately assess the true security afforded by the system (Boyer et al., 2007).

4.2 Validation of Selected Features and Performance Analysis of ANN

4.2.1 Data Acquisition

For this section of experiments, a WACOM tablet connected to a PC was used. The tablet was used to capture the person's signature. A program was created using "FLASH" to track the movements of a pen on the tablet when one was signing. The tablet was scanned at a fixed frequency rate. The output of this was a series of coordinates where the pen ran and also included sampling of all the times when the pen was up. From the series of coordinates obtained, the selected dynamic features were computed. These features were stored as a vector whenever a signature was saved. Figure 4.1 shows the tablet and pen movement tracking program used to obtain the signatures of subjects.

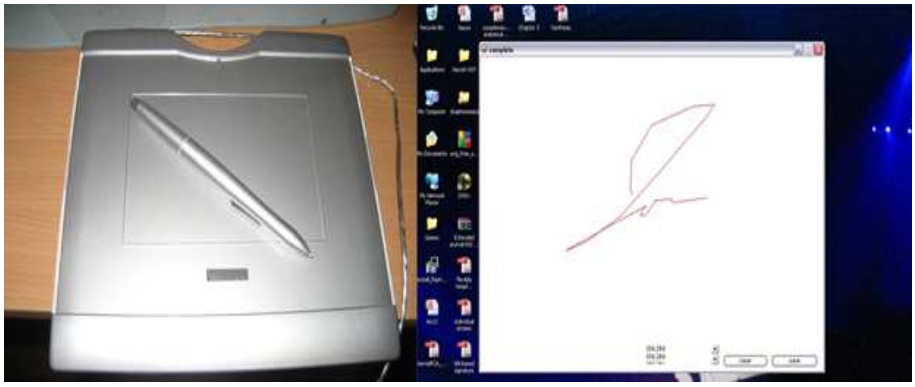

Figure 4.1: The tablet and tracking program used in this experiment

4.2.2 Methodology

The method of person identification is logically divided into two separate modules: (1) enrolment (or training) module and a (2) recognition (or testing) module. The enrolment module is responsible for enrolling new individuals in the system database. During the enrolment phase, an individual supplies a number of samples of his/ her signature. A model (developed iteratively) of the individual is built based on the features extracted from the signature. During the recognition phase, the individual supplies test sample of his/her signature, and a measure of similarity is computed between the features of the test signature with the available model to establish the identity of the individual, using back propagation neural network approach. A multilayer perceptron (MLP) of size 90*50 was used for this purpose. The size was determined iteratively. The efficacy of the technique is determined by computing the GAR, GRR, FAR and FRR.

Three sets of experiments (Experiment 1, 2 and 3) were performed using ANN; (i) identifying if a non-authentic user could be classified as the user, when the signatures of the user are not known for a small sample population, (ii) identifying the ability of the system to detect a forgery, when the fraud attempts to copy the signature of the user and (iii) identifying the system's ability to identify a signature when a larger number of sample population is used.

The type of neural network that was used is known as the feed forward multilayer perceptron, which uses back propagation as its learning algorithm. The network consists of 2 hidden layers where the nodes are configured to the logsig transfer function.

4.2.2.1 Experiment 1: Identification of Signatures (small population, preliminary)

The purpose of this experiment was to show the system's efficiency in classifying signatures of different people. The data of this classification experiment consisted of 60 signature samples, which were signed by 4 different users. Each user was required to sign their own signature 15 times and the features of each signature were then extracted. The users were labeled as A, B, C, and D. 10 signatures from each user A, B, C and D were used as training data for the neural network while the remaining 5 signatures each were used as test signatures for the trained neural network. In this experiment, user A would be classified as "0, 0", user B as "0, 1", user C as "1, 0" and user D as "1, 1".

4.2.2.2 Experiment 2: Rejection of Forged Signatures (preliminary)

The data of this classification experiment consisted of 60 signature samples. 30 of them were signed by one person - the authentic user, and the other 30 are signed by 5 other people. The non-authentic people were asked to copy the signature of the authentic person. These 5 people were shown the signatures of the authentic user, were given a trace of the signature and were requested to learn to copy the authentic signature. They were then asked to forge the user's signature 6 times each to create a total of 30 forged signatures. The purpose of giving the trace of the signature and asking them to learn to copy the authentic signature was such that they were able to forge a signature that was as close as possible to the authentic signature. From the pool of 30 samples belonging to each class, 20 out of 30 genuine and forged signatures were chosen at random to be used as training

data for the neural network classifier. The remaining 10 signatures of each class were used as test samples. The MLP output was given a threshold of 0.4 and 0.8. If the output was less than 0.4, it would classify as 0 while an output greater than 0.8 would classify as 1. An output between 0.4 and 0.8 would be classified as 'unknown'. The reason for choosing such a threshold rather than having it at just 0.5 was to avoid the system from being "too harsh" in determining whether to reject a signature or to accept it. Having a class "unknown" provides a small grey area which reduces the false acceptance as well as the false rejection.

4.2.2.3 Experiment 3: Identification of Signatures (large population)

17 subjects were required to sign their own signature 15 times each. 10 of each were used to train the neural network and the remaining 5 were used to test the trained neural network. The training signatures were signed first by the user and the test signatures were then obtained 1-2 hours later from the users. A total of 255 signatures were obtained where 170 of the signatures were used to create the training database for the ANN and the remaining 85 signatures were used to test the trained ANN.

Each user had a lower and upper threshold. For instance, if the output of the neural net was below the lower threshold, the output would be classified as a "0" whereas if the output was higher than the upper threshold, then it would be classified as a "1". Anything which falls between the lower and upper threshold would be classified as unknown, "u". In order to obtain the threshold of each user, the training data was inputted into the trained neural network. The threshold was obtained from the output of the neural network. The lower threshold would be the highest number a "0" can go up to and the upper threshold would be the

lowest number a "1" can go down to. Each user was numbered from 0-16 and the classification output consisted of the binary version of their respective number.

The class "unknown" was used to calculate the FAR and the FRR of the system. If a test signature was classified as unknown, the system would not reject the signature totally but also would not accept the signature as genuine. In this case, the user may have a choice of signing in again, according to the application. This was used to avoid signatures from being too easily rejected by the system.

4.2.3 Results and Discussion

4.2.3.1 Experiment 1: Identification of Signatures (small population)

Table 4.1 shows the tabulated results of Experiment 1. The number of test samples which were accepted correctly by the system was recorded.

Table 4.1: Table of classification for experiment 1.

	Classification threshold: 0.5	
Subject	no. of test samples	no. of samples correctly classified
Subject A	5	5
Subject B	5	5
Subject C	5	5
Subject D	5	5

From table 4.1, it is observed that the system classified the signatures by 4 different users correctly. Table 4.2 shows that the GAR and FAR for Experiment 1 is 100% and 0% respectively. The results of this experiment demonstrate that the system is suitable for security application in a small population since the

Table 4.2: Table of Genuine Acceptance Rate and False Acceptance Rate for Experiment 1.

Type	Accuracy (%)
FRR	0
GAR	100

GAR and FAR is shown to be perfect.

4.2.3.2 Experiment 2: Rejection of Forged Signatures

From table 4.3, it can be observed that the system does not classify any forger as the authentic user, nor does it classify any authentic user as a forger. However the system does classify 2 forgers and 2 authentic users' signatures as Unknown. The output for sample 6 and 8 were observed to be close to the threshold. This maybe due to the low amount of samples used for the training of the ANN.

Table 4.3: Results of Experiment 2 - Authentic user and Forger user (10 examples)

	Identification Output		Classification Accuracy, Threshold = 0.4, 0.8	
Sample no.	Genuine	Forgery	Genuine	Forgery
1	0.941	0.0029	Y	Y
2	0.829	0.004	Y	Y
3	0.936	0.0029	Y	Y
4	0.574	0.119	Unknown	Y
5	0.975	0.787	Y	Unknown
6	0.5337	0.0729	Unknown	Y
7	0.9917	0.3322	Y	Y
8	0.89	0.7943	Y	Unknown
9	0.9585	0.0849	Y	Y
10	0.9505	0.0099	Y	Y

The False Acceptance Rate and False Rejection rate is perfect (0%), the Genuine Acceptance Rate and Genuine Rejection Rate is at 80% (shown in table 4.4). A statistical analysis, non-parametric KS test, was used on the database of signatures. 10 genuine signatures and 10 forgery samples were picked at random from the database. The test showed that all but one of the features had a low p-value at much less than 0.05. The H_0 hypothesis, which states that the 2 groups are of the same distribution, is therefore rejected. It is shown that there is a clear separation between the genuine and forged signatures, even with low amount of training and test samples. The results of the second experiment demonstrate that the system is suitable for high level security applications where it is essential that FAR and FRR is 0, while the GAR and GRR are 'reasonable'.

Table 4.4: Table of Genuine Acceptance Rate, False Acceptance Rate, False Reject Rate and Genuine Reject Rate for Experiment 2.

Type	Accuracy (%)
GAR	80
FAR	0
FRR	0
GRR	80

4.2.3.3 Experiment 3: Identification of Signatures (large population)

It is observed from the results that the ANN was able to classify the majority of the signature test samples. Table 4.5 shows that 75 out of 85 total test samples were correctly classified, which comprised of 89% of the total sample population (table 4.5). However, 3% of them were wrongly classified and 8% of the total samples were not able to be classified.

Table 4.5: Table of the classification of signatures for ANN and the recognition rates.

	Number of samples	Recognition rate (%)
Total test samples	85	-
Correct classification	75	89 (GAR)
Wrong classification	3	3 (FAR)
Unknown classification	7	8 (FRR)

4.3 Comparison of Classifiers for Dynamic Signature Verifier - ANN vs Statistical Analysis

In this section, the same number of dynamic features was fed into the statistical analysis classifier to compare the performance of the two different classification techniques. This section reports on the experimental verification of the dynamic signature verifier for the application of verification of the authenticity of the user. The purpose of the experiment done in this section is to analyse the performance of the statistical analysis classifier in separating the different classes. The results from this were then used to compare with the previous results obtained from the ANN in section 4.2. These experiments were conducted to compare the performance of the ANN and the Statistical Analysis classifier. The system was optimised by selecting the value of the threshold based on the distances of the different classes for each of the features.

4.3.1 Performance Analysis of Dynamic Signature Verifier using Statistical Analysis

4.3.1.1 Data Acquisition

The use of signature capture device evolved from a WACOM tablet connected to a PC (section 4.2) to a hand held PDA. This provided greater flexibility for the user. It overcame the shortcoming of the previous method of signature capture, its portability. With the PDA, obtaining signatures were made easier. The program which was responsible for the tracking the pen movements and feature extraction was inputted directly into the PDA. The templates were stored in the PDA for easy access. Figure 4.2 illustrates the PDA used in this experiment.

Figure 4.2: The PDA used in aquiring signatures for experimental verification in this section

4.3.1.2 Methodology

The experiment was conducted in two phases; the enrolment phase and the testing phase. In the enrolment phase, the participant made their sample signatures and the dynamic features from these were saved. In the second phase, the user

signed their normal signature and the system responded to this input based on its dynamic features and declared whether the signature was authentic or a forgery.

To determine the ability of the system to validate the authentic user, each participant signed 5 times for enrolment (training). 10 more samples of the signature were recorded after a break of approximately 1 hour and these were used for testing purposes. To determine the ability of the USV to identify the forgery, people other than the genuine user were asked to copy the genuine signature. They were provided with a trace of the genuine signature that could be mounted on the USV and were given time to practice forging the signatures. Based on the response of the USV and knowledge of the actual, the FAR, and GRR was computed.

4.3.1.3 Experimental Setup

20 people were gathered to sign their signatures 15 times where 5 of them were used as training data and the other 10 were used as testing data (testing data signed 1 hour after the user signed for training). After the users signed, their templates were created from the 5 training data each. The users were later asked to choose a template at random other than their own and actively try to forge it. The person was asked to forge the signature 20 times. This is to test the system's robustness against attempted forgery. Each person is shown the signature of the template of his or her choice. They were then given a trace of the signature and asked to learn about the genuine signature so that they were able to sign as close as possible to the authentic signature. For this experiment, a total of 300 genuine signatures were obtained, where 100 of these signatures were used to train the system and the remaining 200 signatures were then used to test the

system. Another 400 forged signatures were then obtained to test the system's ability in detecting forgeries.

4.3.1.4 Results and Observations

Table 4.6: Table of the classification of signatures for Statistical Analysis Classifier and the recognition rates.

	Number of samples	Recognition rate (%)
Total test samples	600	-
Total genuine samples	200	-
Total forgery samples	400	-
Correct acceptance	183	92 (GAR)
Wrong rejects	17	8 (FRR)
Wrong accepts	3	1 (FAR)
Correct rejection	397	99 (GRR)

It is observed that the statistical classifier produced a very good recognition rate in a fairly large population sample size. Table 4.6 shows the classification of the test signatures and their recognition rates. 17 out of 200 genuine signatures were rejected and 3 out of 400 attempted signature forgeries were accepted. This computes the recognition rate GAR, FAR, FRR and GRR; 92%, 1%, 8% and 99% respectively.

4.3.2 Comparing ANN and Statistical Analysis

Experiments in section 4.2 have studied the performance of the ANN as the classifier for the dynamic signature verifier. For a small sample, the ANN works very well with a perfect GAR shown in the results of experiment 1. The results

in experiment 2 shows that there was no false acceptance rate but not all the forgeries were rejected. 2 out of the 10 forged samples were classified as unknown. However, as the sample size increases, it can be seen that it is harder for the ANN to properly identify the signatures correctly. It is shown that 3 signatures were classified incorrectly and 7 signatures were not able to be classified.

The experiment in section 4.3.1, shows the performance of the statistical analysis as the classifier for the dynamic signature verifier. The results obtained from this section are very promising. For a large subject base of 20 people, it is shown that only 1% of the total forged signature of 400, from subjects' attempt to forge each other's signatures, was accepted. The genuine acceptance rate shown in these results was 92%. Table 4.7 summarizes the recognition rates obtained from the experiments conducted in this chapter.

Table 4.7: Comparison of recognition rates obtained from experiments in chapter 4.

	Section 4.2: ANN			Section 4.3.1: Stat. Analysis
Type	Exp. 1	Exp. 2	Exp. 3	-
GAR	100%	80%	89%	92%
FAR	-	0%	3%	1%
FRR	0%	0%	8%	8%
GRR	-	80%	-	99%

By comparing both the results obtained from the ANN and statistical analysis, it can therefore be said that the statistical analysis classifier performs much better compared to the ANN classifier. Before analysing further into this topic, a breakdown of the difference between the experiments done in section 4.2 and 4.3.1 are shown as follows:

1. In the experiments conducted using ANN (section 4.2), the training data is fully supervised, where the training data consists of signatures of all classes. On the other hand, in the experiment done using statistical analysis (section 4.3.1), the training data only consists of genuine signatures (semi-supervised) from a single class or user.

2. During experiment 2 done in section 4.2, the 5 people were actively forging just 1 signature which belonged to 1 user whereas during the experiment done in section 4.3.1, each participant's signature was used in determining the system's performance against forgery.

3. In the experiment done in section 4.3.1, a break of one hour is implemented between enrolment and obtaining testing data for authenticity. All signatures were obtained together during the experiments done in section 4.2.

4. The threshold in the experiment done in section 4.3.1 is determined by the training data of the user during enrolment unlike the experiments done in section 4.2, which was already preset.

5. The experiment done in section 4.2 is in a more controlled environment whereas the experiment done in section 4.3.1 is done in manner which is closely related to real world conditions.

The purpose of the experiment conducted in section 4.2 was to determine if the features selected were separable and sufficient enough to separate signatures of different classes as well as to recognise signatures of the same classes. Therefore it was done in a controlled environment. Also, the purpose of the experiment done in section 4.3.1 was to see if the features chosen can actually be used in real

world conditions. Therefore, the conditions for the second experiment were made "harsher" compared to the one used earlier for the ANN (section 4.2).

Comparing both the results obtained from section 4.2 and 4.3.1, the statistical analysis method produced much better results although the experiment was exposed to much "harsher" conditions. From the above observations, it can thus be concluded that the performance of the dynamic signature verifier is more optimal when using the statistical analysis as compared to using the ANN.

4.4 Summary

In conclusion, the features selected for the dynamic signature verifier is separable and suitable for signature verification. The dynamic feature set used is sufficient for separating signatures of different classes as well as recognising signatures of the same classes. According to the results found in section 4.2 and 4.3.1, it can be observed that the system is able to efficiently recognise signatures as well as rejecting a forged signature when detected. Therefore, the feature set chosen is suitable for a high level security system.

Moreover observing the results obtained from section 4.3.1, it was found that the system which incorporates the statistical analysis method produced better recognition and rejection rates compared to the system which uses ANN. Hence, the dynamic signature verifier which uses the statistical analysis as the classifier performs significantly better, since it is exposed to "harsher" conditions, compared to the system which uses the ANN as the classifier.

Chapter 5

Performance Analysis of Different Feature sets for signature verification - Dynamic vs Static

5.1 Introduction

The experiment conducted in this chapter were to compare the performance of the static and dynamic signature verifier, each with appropriate feature sets. The difference between these 2 feature sets have already been discussed earlier in chapter 3.

For the dynamic feature set, the list of features was the same as the ones originally selected for the previous experiments conducted in chapter 4. As for the static feature set, the Hu moments of the signature were used. Earlier in chapter 3, the computation and image features of the seven Hu moments was described. The purpose of this chapter was to compare the difference in the

performance of the dynamic feature set and static feature set when used in an unpenned signature verification system

The performance of the dynamic feature set has already been analysed previously in Chapter 4. The experiment done in this chapter was to obtain a comparative performance analysis of the static feature set. The statistical analysis based classifier method described earlier in chapter 3 was used in this experiment.

5.2 Comparison of Performance Analysis of Dynamic Feature Set VS Static Feature Set for Signature Verification

The performance analysis which was done in this chapter is similar to the criterion used in the previous chapter. As stated before, the performance of a biometric authentication system is based on its ability to reject an intruder while accepting a genuine user. Based on this, the performance of the static feature set signature verifier is compared to the performance of the dynamic feature set which was obtained in chapter 4.

5.2.1 Performance Analysis of Static Feature Set Signature Verifier

5.2.1.1 Data Acquisition

The same PDA used in the experiment conducted in section 4.3.1 previously was also used here in this experiment. A new program was developed to extract the

Hu moments directly from the signature on the PDA. The static Hu moments were stored seperately from the dynamic features.

5.2.1.2 Experimental Setup

Similar to the experimental setup described in Section 4.3.1, the experiment was conducted in two phases; enrolment phase and testing phase. The same people who participated in the experiment done in section 4.3.1 were enrollled for this experiment. A total of 20 subjects were used in this experiment. During the enrolment phase, the participants made their sample signatures and the static Hu moments of each of their signatures were then extracted and saved. Each participant was asked to sign 5 times for this phase. The data collected from each subject was used to create a template which represented the subject's signature. A total of 20 templates were created during the duration of this experiment. In the testing phase, 10 more samples of the signature were recorded from each of the subjects after a break of approximately 1 hour and these were used for testing purposes. Each user signed their normal signature and the signature verifier responded to this input based on the static Hu moments features recorded in the template and verifying the autheticity of the signature.

To determine the ability of the signature verifier to identify a forgery, the participants other than a authentic user were asked to copy the genuine signature. Before forging the signature, they were asked to observe how the signature was signed as well as given time to practice signing the signature. A trace of the signature was mounted on the signature verifier as a guideline for the subjects to forge.

Based on the response of the signature verifier, the results obtained were then

tabulated and analysed. The GAR, GRR, FAR and FRR were later computed and compared with the recognition rates obtained when the dynamic feature sets were used.

5.2.1.3 Results and Discussion

Table 5.1: Table of the classification of signatures through Static Hu moments and the recognition rates.

	Number of samples	Recognition rate (%)
Total test samples	600	-
Total genuine samples	200	-
Total forgery samples	400	-
Correct acceptance	188	94 (GAR)
Wrong rejects	12	6 (FRR)
Wrong accepts	85	21 (FAR)
Correct rejection	315	79 (GRR)

Table 5.1 shows the total number of genuine and forged signatures used to evaluate the performance of the signature verifier using static features. From table 5.1, it can be observed that 12 out of 200 genuine samples were rejected and 85 out of 400 forged signatures were accepted when signed for authentication. From this, the recognition rates can be computed. The false acceptance rate obtained in this experiment was 21% whereas the false rejection rate computed for this experiment was 6%. The rest of the recognition rates are also shown in table 5.1.

From the observations, the static feature signature verifier performed very well in terms of recognising and authenticating genuine signatures. In the case of rejecting forged signatures, the performance of the static feature classifier is below par. This is due to the static features describing a signature as a still picture.

When forging a signature, the subjects learnt how the signature was signed and a trace of the genuine signature was mounted on the signature verifier. This makes it is easier to copy a signature as a picture, which causes a rise in the false acceptance rate. This aptly demonstrates the downside of having only static features in a set of features.

5.2.2 Comparison of Performance - Dynamic vs Static

Table 5.2 below shows the comparison of recognition rates between the dynamic features signature verifier and the static features signature verifier.

Table 5.2: Table of GAR, FAR, FRR and GRR, comparing Dynamic to Static features (Statistical Analysis classifier)

Type	Dynamic Signature	Static Signature
GAR	92%	94%
FAR	1%	21%
FRR	8%	6%
GRR	99%	79%

The results of the classification of the static signature using Hu moments shows that such a system produces a better GAR of 94% as compared to the classification of the dynamic signature that produces a GAR of 92%. Hence, the static feature signature verifier is able to accept more genuine signatures compared to the dynamic feature signature verifier. Unfortunately, such a system allows a large number of false positives, with a FAR being 21%. This has shown that the static signature verifier has allowed a very large amount of forged signatures to be classified as genuine signatures as compared to dynamic signature verifier which only has a 1% false acceptance rate. The results indicate that static signatures

may be suitable for low level of security where forgers are not expected to be much of a concern. Where a higher level of security is expected, a system employing dynamic signatures has a much better chance at detecting forgers.

Based on the results obtained from the experiments, it can be concluded that the dynamic feature set performs much better than the static feature set. Hence it can be seen that even though the static feature set performs slightly better in accepting a genuine signature, the dynamic feature set outperforms the static feature set in rejecting a forgery. When building a biometric system, it is more important to be able to reject an impostor although a certain level of acceptance rate is necessary. Hence the conclusion that a dynamic feature set performing much better than a static feature set.

5.3 Summary

From the results of the experiment, it is observed that Hu moments of a static signature are only suitable for validating the identity of an individual where the level of security is low and expert forgeries are not expected because of the system's high acceptance rate (21%). Such a system may be suitable only where it is implemented along with other security systems such as PIN, or where the required level of security is very low. While other measures of shape were not tried, based on this work, it is observed that the shortcoming of the static signatures is the case with which non-authentic user can copy a signature.

Additionally, the results indicate that the dynamic signature verification system has a higher rejection of authentic users (9%) but is very good at identifying forgeries. Comparing both different sets of features, the dynamic signature tech-

nique has a much lower false acceptance rate of 1%. This is because the dynamic signature technique measures the speed and number of strokes, making it extremely difficult for another person to copy (Li et al., 2001), even when they were provided with a tracing of the signature. Taking the dynamic features of a signature for verification of a user is like using the signature of the user to describe the handwriting behaviour of that person. As it is difficult to copy the behaviour of a person's handwriting, even for an expert forger, thus the dynamic signature based system is a preferable signature verifier for a high levelsecrity system as opposed to a static based system since the dynamic signature based system has comparatively lower false positives.

It is also possible to have a system which incorporates both dynamic and static features but in this thesis, the system used only incorporates dynamic features. This is because:

1. Static features are easier to copy compared to dynamic features by professional forgers. They are excluded because this system is a score-based system which is dependent on the amount of features accepted by the system. Having static features which are easily copied would make features be easily accepted, which in turn cause the system to be more susceptible to forgers.

2. Most static features are function based features and therefore incorporating static features would dramatically increase the computational power of the system which is one of the main criteria in building this system.

Chapter 6

Emotions on the Dynamic Feature Set Extracted from Handwritten Words and Signatures

6.1 Introduction

Based on the earlier studies outlined in chapter 2, the handwriting of a person is affected by his or her emotions. Chapter 2 also describes how graphology can be used to determine the personality of a person through his or her handwriting. The purpose of the experiment conducted in this chapter is to determine whether the 4 basic human emotions; happy, sad, fear and anger, effects the dynamic feature set of both the handwriting of normal words and the signature of a person. This chapter also describes and discusses the results of this experiment towards

application related to signature verifier as well as a personality profile done on a person using graphology.

This experiment was done by inducing the 4 basic emotions on a subject through emotion-specified videos provided by the department of psychology from The University of Melbourne. Experts from the psychology department of The University of Melbourne have claimed that the emotion-specified videos are able to induce the specific emotion on the subject who watches them. Immediately after a subject was induced with an emotion, he or she was asked to write the words "happy', "sad", "fear" and "anger", as well as sign his or her signature twice. The data was then statistically analysed to determine if there was any effect of the emotion on the dynamics of the handwritten words and signature.

A detailed report of the methodology of the experiment is described below, followed by a brief report on multi-variate analysis of variance (MANOVA) used to analyse the data and this is followed by a discussion of the results obtained. Lastly, this chapter ends with a conclusion stating how the results of this experiment will affect the signature verifier and graphology.

6.2 Experiments to Evaluate the Effects of Emotion on the Dynamic Feature Set

6.2.1 Data Capture

The subjects were asked to write the words and sign their signatures on the same PDA used in the experiments conducted in previous chapters. The extracted dynamic features were then exported to a desktop computer for further analysis.

6.2.2 Methodology

The experiment was done over a span of three days involving 9 volunteered participants. Four types of videos were used in this experiment, with each video stimulating a state of emotion when watched. The states of emotion used were happy, sad, fear and anger. A neutral video was shown before each one of the emotional inducing videos was shown to a subject so that the previous emotion would not effect the emotional state of a subject while watching the current video. It was also a requirement that a subject does not watch the same video more than once.

The purpose of this experiment was to study the impact of the different emotional stimuli of subject's handwriting and signature. After watching a type of video, a subject was required to write the words "happy", "sad", "fear" and "anger" followed by two signatures of the subject on the PDA. The subject was also required to write all the four words and sign their signature twice after watching each neutral video to obtain the reference. Figure 6.1 shows examples of the words "happy", "sad", "fear" and "anger" written by subject X.

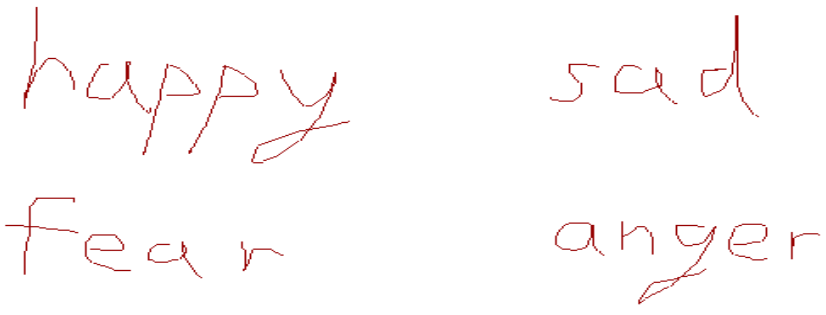

Figure 6.1: Words written by subject X used for analysis in this section

The features extracted were the same features used in the dynamic signa-

ture verifier described and tested in chapter 4. These features have already been discussed and listed in section chapter 3. This experiment was not designed to identify whether an emotion causes an increase or decrease in a certain feature but only to determine whether there was any changes in the feature set. The experiment was repeated for 3 days to overcome error due to experimental variation.

6.2.3 Statistical Analysis of Data Using MANOVA

Multi-variate analysis of variance (MANOVA) is a statistical tool used to analyse the means of multiple variables and determine whether the mean of these variables differ significantly between classes. Based on the One-Way Analysis of Variance (ANOVA), MANOVA is designed to analyse more than one dependent variable. MANOVA measures the differences for two or more metric dependent variables based on a set of categorical variables acting as independent variables (Hair et al., 2006).

Canonical variables are linear combinations of the mean-centered original variables. With canonical analysis, the linear combination of the original variables with the largest separation between the groups can be found. By using a grouped scatter plot of the first two canonical variables, it shows more separation between groups than a grouped scatter plot of any pair of original variables of the features.

MANOVA was used on the feature sets extracted from the handwritten words and signatures of the subjects to investigate the separation of classes between 5 different states of emotions (including neutral state). If a grouping of that particular state (class) of emotion is seen in a group scatter plot of its first two

canonical variables, that emotion has impacted on the subject when that word or signature is written. The results of the number of subjects affected by an emotion while writing the four words and signing are recorded and tabulated (Table 6.1 and 6.2).

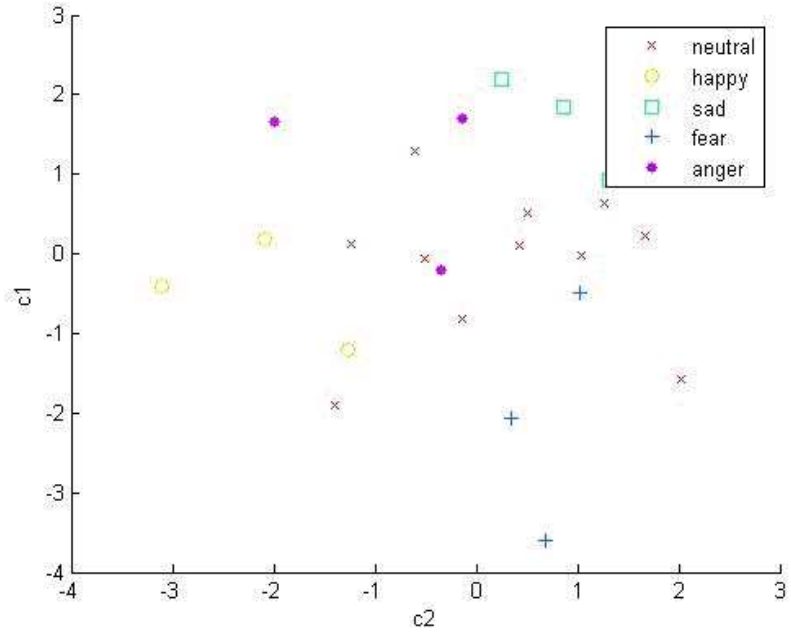

Figure 6.2: Grouped scatter plot of the first two canonical variables, c2 vs c1, for subject 9 writing "happy" in 5 different emotional states (including neutral)

Fig 6.2 shows the plot of the second canonical variable (c2) vs the first canonical variable (c1) of subject 9 writing the word "happy" after being shown the emotion stimulating video over the span of 3 days. Fig 6.3 shows the plot of the second canonical variable (c2) vs the first canonical variable (c1) of subject 2 writing the word "sad". Figure 6.2 shows that there is no clear separation between each of the emotional states whereas Figure 6.3, (the circled areas) shows a clear grouping of the writing for each of the emotional states. For example, sub-

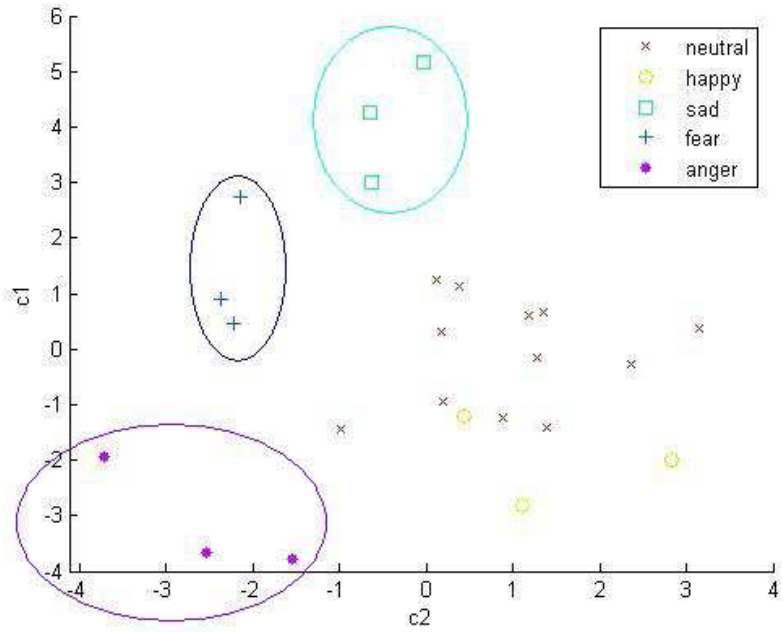

Figure 6.3: Grouped scatter plot of the first two canonical variables, c2 vs c1, for subject 2 writing "sad" in 5 different emotional states (including neutral)

ject 9 shows no clear effects of emotions on his or her handwriting when writing "happy". Subject 2 exhibits variations in his or her handwriting when writing "sad" after being emotionally induced.

6.2.4 Results and Discussion

Tables 6.1 and 6.2 show which which of the written words or signature signed by which subject is affected by which emotion. The "1" symbol means that the particular word written by that subject was affected by that emotion. Table 6.3 shows the total number of subjects when writing that word or signing was affected by a particular emotion. Overall through table 6.3, it was observed that the dynamics of handwritten words such as "happy", "sad", "fear" and "anger"

were affected after the subjects were emotionally stimulated. The signature of a person does not appear to be effected by the person's emotion. There is no significant impact of overall emotions on a person's signature. From tables 6.1 and 6.2, it can be seen that only 2 subjects were affected by the emotions "sad" and "fear" while signing and only 1 subject was affected by the "fear" emotion. The rest of the 6 subjects' signature features did not change after being induced with the four emotions. From the results, it can be observed that (1) there is no significant impact of emotional stimuli on people's dynamic signature and (2) if any of the emotions were to effect the way people sign, it would most likely be the "fear" emotion.

Table 6.1: Words and signature of subjects 1 - 4 affected by emotional states

Sub.	1					2				
emo.		happy	sad	fear	anger		happy	sad	fear	anger
word	happy			1		happy		1	1	1
	sad		1			sad		1	1	1
	fear			1		fear	1	1		1
	anger	1	1	1	1	anger	1		1	1
	sig.					sig.				
Sub.	3					4				
emo.		happy	sad	fear	anger		happy	sad	fear	anger
word	happy		1		1	happy	1			
	sad		1	1		sad			1	
	fear		1	1	1	fear			1	
	anger	1	1		1	anger				
	sig.			1		sig.				

According to table 6.1 and 6.2, 66 out of the 144 words written are affected by emotions. That is nearly half of the words written being affected by emotions. Subject 4 and subject 5 show that their handwriting is hardly affected by emotions

Table 6.2: Words and signature of subjects 5 - 9 affected by emotional states

Sub.	5					6				
emo.		happy	sad	fear	anger		happy	sad	fear	anger
word	happy	1				happy			1	1
	sad	1				sad	1	1		
	fear					fear		1	1	
	anger	1			1	anger		1		1
	sig.					sig.				
Sub.	7					8				
emo.		happy	sad	fear	anger		happy	sad	fear	anger
word	happy	1	1	1		happy			1	1
	sad	1	1			sad				
	fear		1	1		fear		1	1	1
	anger		1			anger			1	
	sig.		1	1		sig.				
Sub.	9									
emo.		happy	sad	fear	anger					
word	happy									
	sad	1	1	1	1					
	fear		1	1						
	anger	1		1	1					
	sig.		1	1						

and their signatures were totally unaffected by the 4 emotions.

It can thus be concluded that though there is a large inter-subject variability in the impact of emotional stimuli on people's handwriting. While there appears to be a measurable impact of the stimuli on all people, the extent is very different. The results from table 6.1 and 6.2 show that all the subjects' handwritings are affected dynamically by emotions to a certain extent. Nearly 46% of the words recorded were affected dynamically by the four emotions.

This raises a fundamental question for graphology. Is it sufficient to just take a person's normal handwriting and get his or her personality profiled? From the

results, we observe that which a signature is unaffected by emotions, handwriting is. Therefore, the use of signatures for graphology might yield a more accurate result compared to only using the normal handwriting of a person.

Table 6.3: Number of subjects affected by the emotional state while writing the word and signing.

		happy	sad	fear	anger	emotion
word	happy	3	3	5	4	
	sad	4	6	4	2	
	fear	1	6	7	3	
	anger	5	4	4	7	
	signature	0	2	3	0	

6.3 Summary

In conclusion, this chapter has studied the impact of emotions on the selected dynamic features of a person's handwriting and signature. From the results, it is observed that a person's handwriting is more susceptible to the four main emotions compared to a person's signature. It is shown that nearly half of the words recorded are affected by the subjects' emotions. If a subject was to be asked to write more words, the changes in their handwriting may have been more distinct. The results also show that only 3 subjects' signatures were affected by the emotions of sad and fear. While it cannot be said that a person's signature is totally immune from all of emotions, the impact appears to be less than for handwriting.

From this study, it is also concluded that in the field of graphology, it is not appropriate to only take a person's handwriting and do a personality profile.

From the results, it is observed that the four main emotions do affect a person's handwriting and this might produce an inaccurate result when conducting a graphology on a person's normal handwriting. Unlike handwriting, the set of features extracted from a person's signature can be said to be less sensitive to the four emotional stimuli. Thus, if a person's signature is studied for graphology, the results might be more accurate than using a person's normal handwriting. This might be due to a person's signing being more habitual compared to their normal handwriting.

Chapter 7

Summary and Conclusion

7.1 Summary and Discussion

This thesis has examined the efficacy of the signature verification using a dynamic feature set chosen according to the required specification as a biometric authentication tool. The thesis has also shown the simplicity of the system by just using a standard PDA installed with a self made program which captures the dynamics of the signature and a simple matching program which incorporates basic statistical analysis. The classification method evolved from using the Artificial Neural Network to using a simpler statistical analysis method. The key point in the high success rate in identifying the correct user while rejecting an imposter is in selecting the correct set of dynamic features that make it hard to imitate, even for an expert forger. On the basis of the experimental results, it can be concluded that:

- The selected dynamic features are suitable for applications of high level security. From the results obtained from the experiments conducted, it can be concluded that the selected features are sufficient to classify different

signatures. Moreover, it is observed that with the right classification tool, the selected global parameter based dynamic features can seperate a forgery from an authentic signature, even if it is signed by a trained forger.

- The statistical classifier which works as a verifier produces a better recognition rate compared to the ANN which works as an identifier. For a real world application, it is computationally less expensive to create a system for verification where users sign their own signature and it is matched against their own signature which has already been stored in a template held by them (smart cards for example). The results (section 4.2.3 Experiment 3) show that the system using ANN has a recognition rate of GAR 89%, FAR 3% and FRR 8%. The subjects did not actively try to forge other subjects' signature and the false acceptance rate was already at 3%. As for the system which implements statistical classifier (section 4.3.3), the recognition rate was GAR 92%, FAR 1%, FRR 8% and GRR of 99%. This shows that the system which uses the statistical classifier produced a better recognition rate than the system which uses the ANN, especially when the subjects were asked to actively forge one another's signature. Therefore, the rest of the experiments were done using the statistical analysis as the classifier.

- The unpenned signature system is suitable for digital verification of the authetic user's identity. The system demonstrates robustness even when a forgery is attempted with the help of tracing guides. The results show that the system using the chosen dynamic feature set and the statistical analysis classifier has a very low false acceptance rate and a high genuine acceptance rate. This system is also suitable for the application in the real world due

to its simplicity. The feature template of a signature is easily computed, irreversible and small enough to be stored in a smartcard which is kept by the user.

- For biometric authentication systems, it is a priority to actively reject imposters from accessing the system. It is shown that the dynamic feature set chosen works better than the Hu moments static feature set, in this sense. From the results of the experiments, it is observed that the Hu moments of the static signature are sufficient for validating the identity of an individual where the level of security is low and expert forgeries are not expected due to the system's high (21%) acceptance of the forger as the authentic user. Alternatively, such a system may be suitable only where there are multiple levels of security, such as using it along with PIN. The results (section 5.2.2) also indicate that though dynamic signature verification system does have a higher rejection rate of authentic users (9%), it is still very good at identifying forgeries. The dynamic signature technique measures the speed and number of the strokes, making it extremely difficult for another person to copy, even when the subjects were provided with a trace of the signature. Thus the dynamic signature based system has a very low false positives compared with the static signature based system.

- A signature verification tool is a widely used biometric authentication tool in the real world. However, its application can be affected by many factors. One such factor is human emotions. For a signature verifier that uses the selected dynamic feature set, it would be "safe" from the 4 main emotions, happy, sad, fear and anger. It can be seen from the results in chapter 6 that 5

out of the 36 signatures recorded were affected by emotional stimuli. These comprises of 14% of the total sample population of signatures. Majority of the subjects showed no signs of being affected by the emotional stimuli while signing their own signature. This maybe due to the signing of a person's signature being habitual. Most people maybe used to signing their own signature, irrespective of whether they are feeling happy, sad, fearful or angry.

- A person's handwriting is more susceptible to the 4 main emotions compared to a person's signature. It is shown in the results (chapter 6) that nearly half of the words recorded from subjects after watching emotionally stimulating videos were affected by the subjects' emotions. In the field of graphology, it is concluded that rather than to analyse a person's handwriting and do a personality profile based on that, signature of a person should be studied.

7.2 Conclusions

From the experimental results presented in this thesis, it is concluded that dynamic signature based system using the statistical analysis based classifier can be used for verifying the identity of an individual. The system provides security against imposters and trained forgers while it is able to verify the authentic user even when under emotional stress. Such a system is easy to implement, inexpensive and does not intrude on the privacy of an individual. It may be used for number of applications including behind a bank teller, automatic verification for credit cards, access control for entry to objects ranging from secured information

to actual physical entry into secured places. Unlike anatomical biometrics where identity theft can result in life-long compromise, this is under the control of the user and can be changed if an identity theft happens.

In conclusion, this thesis has shown the suitability of the dynamic features chosen for signature verification. Through the experiments done, the chosen dynamic features produced good recognition results. Comparing the results from both classifiers, the statistical analysis produced better recognition rates compared to the ANN. This thesis has also compared the performance of the chosen dynamic features with the static Hu moments feature set. Although the static Hu moments feature set signature verifier produced a better genuine acceptance rate compared to the dynamic feature set, it has a significantly higher false acceptance rate. For higher level security, the chosen dynamic feature set is more suitable with a much lower false acceptance rate and acceptable genuine acceptance rate. This is to prevent forgers from being able to access to personal and sensitive information.

This thesis has also shown that the chosen dynamic features of a signature are less sensitive to the four main emotional stimuli; happy, sad, fear and anger. For real world application, it is not only important to just have a good recognition rate but it is also important to take into consideration many such external factors. The dynamic feature set of a signature is easily computed, irreversible, unaffected by human emotions which occurs in our daily lives and small enough to be stored in a smartcard which can be kept on the user. The statistical analysis matching algorithm requires very little computational power and time to provide an output. The system shown in this thesis which incorporates the chosen dynamic feature set and statistical analysis as its classifier does not only have good recognition

rates but is also flexible, user friendly, easily configured and efficient.

This study has also shown that the dynamics of handwriting, but not the dynamics of signatures, are affected by the four emotional stimuli. In this case, if a person's signature were to be studied for the graphology of a person, the results might be more accurate than using a person's normal handwriting.

7.3 Future Studies

This study has demonstrated the efficacy of the use of dynamic and static signatures for people identity validation. The study has also done a comparative between the two techniques and determined the ability of these techniques to identify the forgers and the authentic users. The system developed for this research is a portable and easy to use device. The study has also tested the impact of emotional stimuli on the efficacy of the system. The work has determined that while signatures of the person appear to be insensitive to the emotional stimuli, general handwriting appears to be impacted by these stimuli.

For the realisation of the outcomes of thesis work for real world applications, it is important that this study should be extended for a bigger population including people from different demographics. While 20 is a good size for testing, all the participants were of similar age groups and educational qualifications and the new study should test the system beyond such a limitation. Further, the future studies should include testing of this system beyond English language and should consider languages such as Chinese and Hindi.

One of the important outcomes of this work is the determination that while signatures of people appear to be insensitive to the emotional stimuli, there is an

impact of these stimuli on people's general handwriting. This study needs to be expanded to include a bigger and more diverse population and larger number of words.

References

Bellman, R. E. and Dreyfus, S. E. (1962), *Applied Dynamic Programming*, Princeton University Press. 21

Bishop, C. M. (1995), *Neural Networks for Pattern Recognition*, Birmingham: Oxford University Press. 43

Boyer, K., Govindaraju, V. and (Eds.), N. R. (2007), Special issue on recent advances in biometric systems, *in* 'IEEE Trans. on Syst., Man and Cybernetics - Part B', Vol. 35. 57

Camino, J. L., Travieso, C. M., Morales, C. R. and Ferrer, M. A. (1999), Signature classification by hidden markov model, *in* 'Security Technology, EEE 33rd Annual 1999 International Carnahan Conference', pp. 481–484. 18

Castellano, M., Dimauro, G., Impedovo, S. and Pirlo, G. (1990), Online signature verification system through stroke analysis, *in* 'Proc. AFCET', Vol. 1, pp. 47–53. 16

Castellano, M., Impedovo, S., Mingolla, A. and Pirlo, G. (1988), A spectral analysis based signature verification system, *in* 'Lecture Notes in Computer

Science:Recent Issues in Pattern Analysis and Recognition', pp. 316–323. 16, 17

Crane, H. D. and Ostrem, J. S. (1983), 'Automatic signature verification using a three-axis force-sensitive pen', *IEEE T-SMC* **13**, 329–337. 15

Delac, K. and Grgic, M. (2004), A survey of biometric recognition methods, *in* 'Electronics in Marine, Proceedings Elmar 2004 46th International Symposium', pp. 184–193. 10

Depue, R. A., Monica, L., Arbisi, P., Collins, P. and Leon, A. (1994), 'Dopamine and the structure of personality: Relation of agonist-induced dopamine activity to positive emotionality', *Journal of Personality and Social Psychology* **67**, 485–498. 23

Dimauro, G., Impedovo, S., Modugno, M. G. and Pirlo, G. (2004), Recent advancements in automatic signature verification, *in* 'Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition', pp. 179–184. 5, 14, 15, 16, 29

Dimauro, G., Impedovo, S., Pirlo, G. and Salzo, A. (1997), 'A multi-expert signature verification system for bankcheck processing', **11**, 827–844. 16

Driver, R., Buckley, M. R. and Frink, D. D. (1996), 'Should we write off graphology?', *International Journal of Selection and Assessment* **4**, 78–86. 24

Duda, R. O., Hart, P. E. and D.G.Stork (2001), *Pattern Classification*, Wiley. 40, 57

Dugelay, J. L., Junqua, J. C., Kotropoulos, C., Kuhn, R., Perronnin, F. and Pitas, I. (2002), Recent advances in biometric person authentication, *in* 'Acoustics, Speech, and Signal Processing, IEEE International Conference', Vol. 4, pp. 4060–4063. 10

Fairhurst, M. and Kaplani, E. (2003), 'Perceptual analysis of handwritten signatures for biometric authentication', *Vision, Image and Signal Processing* **150**, 389–394. 11, 14

Faundez-Zanuy, M. (2005), 'Signature recognition state-of-the-art', *Aerospace and Electronic Systems Magazine, IEEE* **20**, 28–32. 5, 13, 14, 15, 20

Ferrer, M. A., Alonso, J. B. and Travieso, C. M. (2005), 'Offline geometric parameters for automatic signature verification using fixed-point arithmetic', **27**, 993–997. 18, 21

Gardner, R. (2002), *Instant Handwriting Analysis: A Key to Personal Success*, Llewellyn Publications. 6, 22, 23, 24

Hagan, M. T., Demuth, H. and Beale, M. (1996), *Neural Network Design*, Boston: PWS Publishing Company. 42

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. and L.Tatham, R. (2006), *Multivariate Data Analysis*, Prentice Hall. 82

Hangai, S., Yamanaka, S. and Hamamoto, T. (2000), On-line signature verification based an altitude and direction of pen movement, *in* 'Multimedia and Expo, IEEE International Conference', Vol. 1, pp. 489–492. 15, 20

Herbst, N. M. and Liu, C. N. (1977), 'Automatic signature verification based on accelerometry', *IBM J. Res. and Dev 1977* pp. 245–253. 15

Hu, M. K. (1962), 'Visual pattern recognition by moment invariants', *IEEE Trans. on Information Theory* **8**, 179–187. 38

Igarza, J. J., Goirizelaia, I., Espinosa, K., Hernaez, I., Mendez, R. and Sanchez, J. (2003), Online handwritten signature verification using hidden markov models, *in* 'CIARP', pp. 391–399. 5, 18

Jain, A. K., Ross, A. and Prabhakar, S. (2004), 'An introduction to biometric recognition', *Circuits and Systems for Video Technology, IEEE Transactions* **14**, 4–20. 11

Kung, S. Y., Mak, M. W. and Lin, S. H. (2004), *Biometric Authentication: A Machine Learning Approach*, Prentice Hall. 4, 10, 21

Lam, C. F. and Kamins, D. (1989), 'Signature recognition through spectral analysis', **22**, 39–44. 16, 17

Lange, K. W., Mecklinger, L., Walitza, S., Becker, G., Gerlach, M., Naumann, M. and Tucha, O. (2006), 'Brain dopamine and kinematics of graphomotor functions', *Human Movement Science* **25**, 492–509. 6, 22, 23

Lee, L. L. (1992), On-Line Systems for Human Signature Verification, PhD thesis, Cornell Univ. School of Electrical Engineering. 11

Lee, L. L. (1996), Neural approaches for human signature verification, *in* 'Signal Processing, 3rd International Conference', Vol. 2, pp. 1346–1349. 19

Lee, L. L., Berger, T. and Aviczer, E. (1996), 'Reliable on-line human signature verification systems', *IEEE T-PAMI* **18**, 643–647. 16, 17

Letjman, D. and George, S. (2001), On-line handwritten signature verification using wavelets and back-propagation neural networks, *in* 'Proc. of ICDAR 01, Seattle', pp. 596–598. 16

Levy, J. and Reid, M. (1976), 'Variations in writing posture and cerebral organization', *Science* **194**, 337–339. 22

Levy, J. and Reid, M. (1978), 'Variations in cerebral organization as a function of handedness, hand posture in writing, and sex', *Journal of Experimental Psychology: General* **107**, 119–144. 22

Li, B., Wang, K. and Zhang., D. (2001), 'On-line signature verification for e-finance and e-commerce security system', *Machine Learning and Cybernetics* **5**, 3002–3007. 31, 78

Lippmann, R. P. (1987), An introduction to computing with neural nets, *in* 'IEEE ASSP Magazine'. 42

Liu, C. N., Herbst, N. M. and Anthony, N. (1979), 'Automatic segnature verification: System description and field test results', *IEEE T-SMC* **9**, 35–38. 15

Lorette, G. and Plamondon, R. (1984), On-line handwritten signature recognition based on data analysis and clustering, *in* 'Proc. 7th ICPR, Montreal', Vol. 2, pp. 1284–1287. 15

Lucas, S. M. and Damper, R. I. (1990), Signature verification with a syntactic neural net, *in* 'Neural Networks, IJCNN International Joint Conference', Vol. 1, pp. 373–378. 19

Ludewig, R., Dettweiler, C. and Lewinson, T. S. (1992), 'Possibilities and limits of medical graphology: Determination of current status and perspectives', *Z Gesamte Inn Med.* **47**, 549–557. 24

Martens, R. and Claesen, L. (1997), On-line signature verification: discrimination emphasised, *in* 'Document Analysis and Recognition, Proceedings of the Fourth International Conference', Vol. 2, pp. 657–660. 19

Martinez, L. E., Travieso, C. M., Alonso, J. B. and Ferrer, M. A. (2004), Parameterization of a forgery handwritten signature verification system using svm, *in* 'Security Technology, 38th Annual 2004 International Carnahan Conference', pp. 193–196. 21

Matyas, V. J. and Riha, Z. (2003), 'Toward reliable user authentication through biometrics', *IEEE Security and Privacy* **1**, 45–49. 10, 11, 27, 29

McKeever, W. F. (1979), 'Handwriting posture in left-handers: Sex, familial sinistrality, and language laterality correlates', *Neuropsychologia* **17**, 429–444. 22

Mizukami, Y., Yoshimura, M., Miike, H. and I.Yoshimura (2002), 'An off-line signature verification system using an extracted displacement function', *Pattern Recognition Letters* **23**, 1569–1577. 15

Moon, Y. S., Ho, H. C. and Ng, K. L. (1999), A secure card system with biometrics capability, *in* 'Electrical and Computer Engineering, 1999 IEEE Canadian Conference on', Vol. 1, pp. 261–266. 11

Muramatsu, D. and Matsumoto, T. (2003), An hmm on-line signature verifier incorporating signature trajectories, *in* 'Document Analysis and Recognition, Seventh International Conference', Vol. 1, pp. 438–442. 5, 18

Nelson, W., Turin, W. and Hastie, T. (1994), 'Statistical methods for online signature verification', *IJPRAI* **8**, 749–770. 16, 17

Nemcek, W. F. and Lin, W. C. (1974), 'Experimental investigation of automatic signature verification', **4**, 121–126. 16

Nixon, M., Carter, J., Cunado, D., Huang, P. S. and Stevenage, S. V. (1999), Automatic gait recognition, *in* 'A. Jain and R. Bolle and S. Pankanti(Ed.), BIOMETRICS: Personal Identification in Networked Society', Springer, pp. 231–249. 30

Pacut, A. and Czajka, A. (2001), Recognition of human signatures, *in* 'Neural Networks, Proceedings IJCNN '01 International Joint Conference', Vol. 2, pp. 1560–1564. 19

Panotopoulos, G. and Psaltis, P. (2001), 'Hand gesture biometrics', *Caltech Centre for Neuromorphic Systems Engineering* . 30

Parizeau, M. and Plamondon, R. (1990), 'A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification', **12**, 710–718. 20, 21

Phillips, P. J., Martin, A., Wilson, C. L. and Przybocki, M. (2000), An introduction evaluating biometric systems, *in* 'IEEE Computer', Vol. 33, pp. 56–63. 11

Plamondon, R. (1995), The handwritten signature as a biometric identifier: psychophysical model and system design, *in* 'Security and Detection, European Convention', pp. 23–27. 13

Plamondon, R. and Lorette, G. (1989), 'Automatic signature verification and writer identification: The state of the art', *Pattern Recognition* **22**, 107–131. 14

Plamondon, R. and Parizeau, M. (1988), Signature verification from position, velocity and acceleration signals: a comparative study, *in* 'Pattern Recognition, 9th International Conference', Vol. 1, pp. 260–265. 20, 21

Plamondon, R. and Srihari, S. N. (2000), 'Online and off-line handwriting recognition: a comprehensive survey', *Pattern Analysis and Machine Intelligence, IEEE Transactions* **22**, 63–84. 5, 14

Prabhakar, S., Pankanti, S. and Jain, A. K. (2003), 'Biometric recognition: Security and privacy concerns', *IEEE Security and Privacy* **1**, 33–42. 2, 3

Rioja, F. R., Miyatake, M. N., Prez, M. H. and Toscano, M. K. (2004), Dynamics features extraction for on-line signature verification, *in* 'Proceedings of the 14th International Conference on Electronics, Communications and Computers', pp. 156–161. 5, 13, 15, 17, 19

Sackheim, K. K. (1990), *Handwriting Analysis and the Employee Selection Process*, CT: Quorum Books. 6, 22, 23, 24

Sakamoto, D., Morita, H., Ohishi, T., Komiya, Y. and Matsumoto, T. (2001), Online signature verification algorithm incorporating pen position, pen pressure and pen inclination trajectories, *in* 'Acoustics, Speech, and Signal Processing, IEEE International Conference', Vol. 2, pp. 993–996. 6, 20

Sato, Y. and Kogure, K. (1982), Online signature verification based on shape, motion, and writing pressure, *in* 'Proceedings of the Sixth International Conference on Pattern Recognition', pp. 823–826. 15, 20

Smith, L. C. and Moscovitch, M. (1979), 'Writing posture, hemispheric control of movement, and cerebral dominance in individuals with inverted and noninverted hand postures during writing', *Neuropsychologia* **17**, 637–644. 22

Srihari, S. N., Xu, A. and Kalera, M. K. (2004), Learning strategies and classification methods for off-line signature verification, *in* 'Proceedings of the 9th Intl Workshop on Frontiers in Handwriting Recognition', pp. 161–166. 5, 20, 21

Theodoridis, S. and Koutroumbas, K. (1999), *Pattern Recognition*, Academic Press. 17, 18, 19, 20, 42

Vacca, J. R. (2007), *Biometric Technologies and Verification Systems*, Butterworth-Heinemann. 4

Wang, S. J. and Chen, X. (2003), Biomimetic (topological) pattern recognition - a new model of pattern recognition theory and its application, *in* 'Proceedings of

the International Joint Conference on Neural Networks', Vol. 3, pp. 2258–2262. 27

Wayman, J. L. (1997), A generalized biometric identification system model, *in* 'Signals, Systems and Computers, Conference Record of the Thirty-First Asilomar Conference', Vol. 1, pp. 291–295. 10

Webb, A. (2003), *Statistical Pattern Recognition*, Wiley. 21

Wessels, T. and Omlin, C. W. (2000), A hybrid system for signature verification, *in* 'Neural Networks, IJCNN 2000, Proceedings of the IEEE-INNS-ENNS International Joint Conference', Vol. 5, pp. 509–514. 18

Woodward, J. D. (1997), Biometrics: Privacy's foe or privacy's friend?, *in* 'Proc. IEEE', Vol. 85, pp. 1480–1492. 3, 10

Wu, Q. Z., Lee, S. Y. and Jou, I. C. (1998), 'On-line signature verification based on logarithmic spectrum', **31**, 1865–1871. 15, 16

Yank, J. R. (1991), 'Handwriting variations in individuals with mpd', *Dissociation* **4**, 2–12. 6, 22, 23, 24

Zhang, D. and Lu, G. (2004), 'Review of shape representation and description techniques', *Pattern Recognition Letters* **37**, 1–19. 36

Zhu, Y., Tan, T. and Wang, Y. (2000), Biometric personal identification based on handwriting, *in* 'Pattern Recognition, 15th International Conference', Vol. 2, pp. 797–800. 13

Zou, M., Tong, J., Liu, C. and Lou, Z. (2003), On-line signature verification using local shape analysis, *in* 'Proceedings of the Seventh International Conference on Document Analysis and Recognition', Vol. 1, pp. 314–318. 18