ONLINE SIGNATURE VERIFICATION TECHNIQUES

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

In

Telematics and Signal Processing

By

KIRAN KUMAR GURRALA

209EC1103

Under the Guidance of

Dr. Sukadev Meher

Department of Electronics and Communication Engineering

National Institute Of Technology

Rourkela

20010-2011

NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA

CERTIFICATE

This is to certify that the thesis titled "**ONLINE SIGNATURE VERIFICATION TECHNIQUES"** submitted by **Mr. Kiran Kumar Gurrala** in partial fulfillment of the requirements for the award of Master of Technology degree in **Electronics & Communication Engineering** with specialization in "**Telematics and Signal Processing**" during session 20010-2011 at **National Institute Of Technology, Rourkela** (Deemed University) is an authentic work by him under my supervision and guidance.

Dr. Sukadev Meher
Dept.of Electronics and Communication Engg.
National Institute of Technology.
Rourkela-769008.

Acknowledgement

I would like to express my gratitude to my thesis guide **Dr.Sukadev Meher** for his guidance, advice and constant support throughout my thesis work. I would like to thank him for being my advisor here at National Institute of Technology, Rourkela.

Next, I want to express my respects to **Prof. S. K. Patra, Prof. G. S. Rath , Prof. S. K. Behera , Prof. Poonam singh , Prof. U. C. Pati , Prof A. K. Sahoo** and **Prof D. P. Acharya** for teaching me and also helping me how to learn. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would like to thank all faculty members and staff of the Department of Electronics and Communication Engineering, N.I.T. Rourkela for their generous help in various ways for the completion of this thesis.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I've enjoyed their companionship so much during my stay at NIT, Rourkela.

I am especially indebted to my parents for their love, sacrifice, and support. They are my first teachers after I came to this world and have set great examples for me about how to live, study, and work.

Kiran Kumar Gurrala.

Roll No: 209ec1103.

Dept of ECE, NIT, Rourkela.

ABSTRACT

Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones. Signature verification is split into two according to the available data in the input. Offline (static) signature verification takes as input the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape.

The purpose of project is to develop an authentication system based on personal signatures. Signature verification is an important research topic in the area of biometric authentication. In this project the work is done in such a way that the signatures are captured using WEBCAM. A visual-based online signature verification system in which the signer's pen tip is tracked. The data acquisition of the system consists of only low-cost cameras (webcams) and does not need special equipment such as an electronic tablet. Online signature data is obtained from the images captured by the webcams by tracking the pen tip. The pen tip tracking is implemented by the Sequential Monte Carlo method in real time. Then, the distance between the input signature data and reference signature data enrolled in advance is computed using Dynamic Time Warping (DTW). Finally, the input signature is classified as genuine or a forgery by comparing the distance with a threshold.

Contents

ABSTRACT iii

List Of Figures vi

List Of Tables vii

Chapter 1 1

1. Introduction 2

1.1Biometrics: 2

1.1.1 Identification 3

1.1.2 Verification 3

1.1.3Advantages of a biometrics system 3

1.1.4 Disadvantages of a biometric system 3

1.2 Problem Statement 4

1.3 Signature Verification: 5

1.3.1 Types of Signature verification 5

1.3.2 Why Online (Dynamic) 6

1.3.3 Advantages: 7

1.3.4 Applications: 7

1.4 General System Overview: 8

1.4.1 General Diagram: 8

1.4.2 Input: 9

1.4.3 Output: 9

1.4.4 Preprocessing: 10

1.4.5 Feature Extraction: 10

1.4.6 Enrollment 13

1.4.6 Verification: 13

1.4.7 Identification: 13

1.5 Performance Evaluation: 14

1.6 Thesis Outline 15

Chapter 2 16

2. Literature Survey 17

2.1 Using Variable Length Segmentation and Hidden Markov Models: 17

2.2 On-line Handwritten Signature Verification using HMM Features: 19

2.3 Dynamic Signature Verification using Local and Global Features: 21

2.4 New extreme points warping technique: 22

2.5 Wavelet Transform Based Global Features: 24
2.6 Two-Stage Statistical Model: 26
2.7 Biometric Authentication using Online Signatures: 28
2.8 Signature Recognition through Spectral Analysis: 29
2.9 Vision System for Pen Tracking: 30
2.9.1 System description 31
2.9.2 Initialization and Preprocessing 32
2.9.2. Pen tracking 37
Chapter 3 39
3. Implemented Technique 40
3.1 Overview of the system: 40
3.2. Data acquisition 41
3.3. Pen tip tracking 42
3.3.1 Template: 44
3.3.2 Tracking the pen: 44
3.3.3 Estimation 47
3.3.4 Computation of dissimilarity 48
3.4. Preprocessing 49
3.5. Feature extraction 49
3.6. Distance calculation 50
3.7. Decision Making 50
Chapter 4 52
4.Experimental setup and Results 53
4.1 Data collection: 53
4.2 Evaluation Criteria 54
4.3 Evaluation 55
Chapter 5 58
5. Conclusion and Future work 59
References 60

LIST OF FIGURES

FIGURE 1. 1BIOMETRICS AUTHENTICATION SYSTEM 2
FIGURE 1. 2 OFFLINE SIGNATURES.. 5
FIGURE 1. 3 ONLINE SIGNATURES 6
FIGURE 1. 4 GENERAL SYSTEM OVERVIEW.. 9
FIGURE 1. 5 EXAMPLE OF A RECEIVER OPERATING CHARACTERISTIC (ROC) CURVE.......... 14
FIGURE 1. 6 ANGLE OF TANGENT LINE 18
FIGURE 2. 1 ANGLE OF TANGENT AT TWO END POINTS 18
FIGURE 2. 2 SYSTEM OVERVIEW 24
FIGURE 2. 3 REF[15] BLOCK DIAGRAM OF SIGNATURE VERIFICATION SYSTEM.................. 26
FIGURE 2. 4 BLOCK DIAGRAM OF THE SYSTEM 32
FIGURE 2. 5 EXPERIMENTAL SET UP 32
FIGURE 2. 6 INITIALIZATION AND PREPROCESSING 34
FIGURE 2. 7 PEN TIP MODEL ASSUMED FOR THE INITIALIZATION 35
FIGURE 2. 8 GIVEN THE PREDICTED LOCATION OF THE PEN TIP IN THE CURRENT FRAME. 38
FIGURE 3. 1 POSITION OF WEBCAMS... 40
FIGURE 3. 3 DATA ACQUISITION.. 42
FIGURE 3. 2 OVERVIEW OF THE SYSTEM 41
FIGURE 3. 4 TIME SERIES IMAGES.. 42
FIGURE 3. 5ONLINE SIGNATURE DATA ACQUISITION FROM FRAMES. BY TRACKING THE PEN TIP AND OBTAINING PEN TIP POSITIONS FROM THE FRAMES, TRAJECTORIES OF X- AND Y-COORDINATES ARE OBTAINED AS TIME SERIES DATASETS. 43
FIGURE 3. 6 RECTANGULAR FEATURE 44
FIGURE 3. 7 TEMPLATE DATA USED FOR PEN TIP TRACKING 45
FIGURE 3. 8 EXAMPLE OF THE INITIAL SAMPLES USING DATA CAPTURED FROM LEFT HAND CAM. THE SAMPLES ARE GENERATED BY ADDING GAUSSIAN NOISE TO THE CENTER COORDINATES OF THE INITIAL POSITION. 47
FIGURE 4. 1 POSITION OF WEBCAMS... 53
FIGURE 4. 2 SIDE DATA FIGURE 4. 3 FRONT DATA 54
FIGURE 4. 4 EXAMPLES OF SIGNATURE DATA 54
FIGURE 4. 5 ERROR TRADEOFF CURVE OF X-COORDINATE(IX).. 55
FIGURE 4. 6 ERROR TRADE OFF CURVE OF Y-COORDINATE (IY). 55
FIGURE 4. 7 ERROR TRADEOFF CURVE OF VELOCITY (|V|).. 56
FIGURE 4. 8 ERROR TRADEOFF CURVE OF ANGLE (Θ). 56

LIST OF TABLES

TABLE 2. 1USING VARIABLE LENGTH SEGMENTATION AND HMM 19
TABLE 2. 2 ON-LINE HANDWRITTEN SIGNATURE VERIFICATION USING HMM FEATURES..20
TABLE 2. 3 DYNAMIC SIGNATURE VERIFICATION USING LOCAL AND GLOBAL FEATURES .21
TABLE 2. 4 NEW EXTREME POINTS WARPING TECHNIQUE..23
TABLE 2. 5 WAVELET TRANSFORM BASED GLOBAL FEATURES 25
TABLE 2. 6 TWO-STAGE STATISTICAL MODELS 27
TABLE 2. 7 BIOMETRIC AUTHENTICATION USING ONLINE SIGNATURES 29
TABLE 2. 8 SIGNATURE RECOGNITION THROUGH SPECTRAL ANALYSIS.............................30

TABLE 5. 1EER (EQUAL ERROR RATE)..57

Chapter 1

1. Introduction

Humans usually recognize each other based on their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. These characteristics are their identity. To achieve more reliable verification or identification we should use something that really recognizes the given person.

1.1Biometrics:

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics means the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of verification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. These characteristics are measurable and unique. These characteristics should not be duplicable. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system shown in Figure 1-1 can be either a verification (authentication) system or an identification system[18].

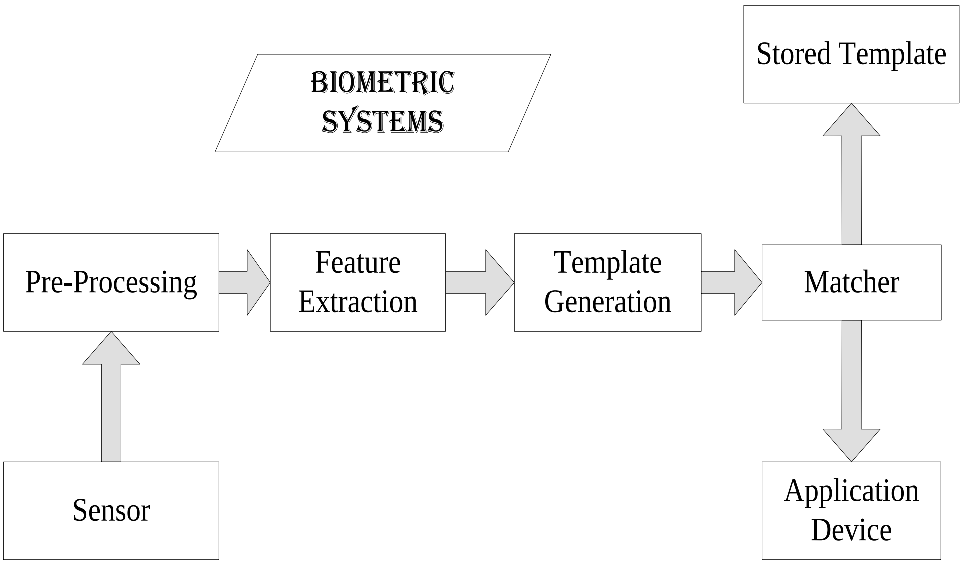


Figure 1. 1Biometrics Authentication System

1.1.1 Identification

Identification can be done using a person's identity based only on biometric measurements. The comparator matches the obtained biometric with the ones enrolled in the database using a 1: N matching algorithm for identification.

1.1.2 Verification

Verification involves the process of confirming or denying a person's claimed identity. When the user claims to be is already enrolled in the system (presents an ID card or login name). The biometric data obtained from the user is compared to the user’s data already stored in the database [18].

1.1.3Advantages of a biometrics system

Finger print or retina of the eyes of one person does not match with any other in the database. Biometrics means Voice, Vein, Eye, Fingerprint, Facial recognition and more.

1.1.4 Disadvantages of a biometric system

Biometric system also has some of disadvantages that can be given as:

- The finger prints of those people, who working in Chemical industries are often affected. Therefore those companies should not use the finger print mode of authentication.
- It is found that with age, the voice of a person changes. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not work correctly. Therefore this method of verification is not workable all situations.
- For those people, who affected with diabetes, the eyes get affected resulting in differences.
- Biometrics is an expensive identification solution.

Despite these disadvantages, biometric systems are nowadays used widely in much kind of industries. If one can gain desired accuracy, than no other thing can take its place [18].

1.2 Problem Statement

Signature verification techniques utilize many different characteristics of an individual’s signature in order to identify that individual. The advantages of using such an authentication techniques are

(i) Signatures are widely accepted by society as a form of identification and verification.

(ii) Information required is not sensitive.

(iii) Forging of one’s signature does not mean a long-life loss of that one’s identity.

The basic idea is to investigate a signature verification technique which is not costly to develop, is reliable even if the individual is under different emotions, user friendly in terms of configuration, and robust against imposters.

In signature verification application, the signatures are processed to extract features that are used for verification. There are two stages called enrollment and verification. In determining the performance of the verification system the selection of features takes main role and it is critical. The features are selected based on certain criterions. Mainly, the features have to be small enough to be stored in a smart card and do not require complex techniques. There are two types of features that validating a signature. They are static and dynamic features.

Static features are those, which are extracted from signatures that are recorded as an image whereas dynamic features are extracted from signatures that are acquired in real time. The features are of two types, function based and parameter based features. The function based features describes a signature in terms of a time-function.

Function based feature examples include position, pressure and velocity. Even though the performance of such features is accurate in verifying signatures, they are not suitable in this case due to the complexity of its matching algorithm. Hence, use of parameter based features is more appropriate.

It is important to take into account external factors when investigating a signature verification technique. Nowadays signature verification applications are used in our daily lives and will be exposed to human emotions. The system has to give reliable accuracy in verifying an individual’s signature even if user is under different emotions.

1.3 Signature Verification:

Signature verification is a common behavioral biometric to identify human beings for purposes of verifying their identity. Signatures are particularly useful for identification of a particular person because each person’s signature is highly unique, especially if the dynamic properties of the signature are considered in addition to the static features of the signature. Even if skilled forgers can accurately reproduce the shape of signatures, but it is unlikely that they can simultaneously reproduce the dynamic properties as well.

1.3.1 Types of Signature verification

Signature verification is split into two according to the available data in the input.

Offline (Static): The input of offline signature verification system is the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Some examples of offline signature shown in Figure 1-2.

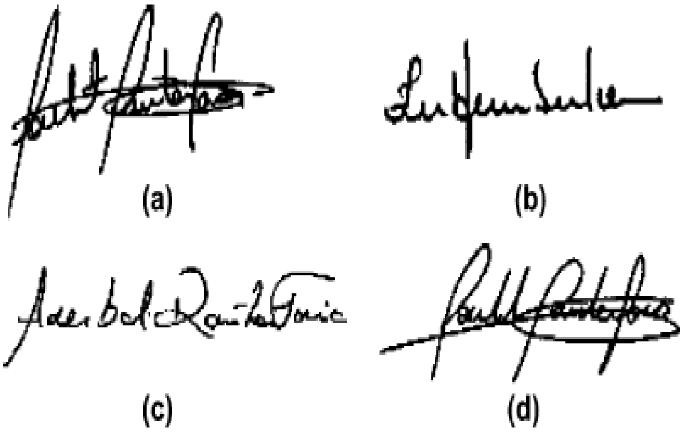


Figure 1. 2 Offline Signatures

Online (Dynamic): Signatures that are captured by data acquisition devices like pressure-sensitive tablets (shown in Figure 1.3) and webcam that extract dynamic features of a signature in addition to its shape (static), and can be used in real time applications like credit card transactions, protection of small personal devices (e.g. PDA), authorization of computer users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings.

Figure 1. 3 Online Signatures

1.3.2 Why Online (Dynamic)

Off-line signatures systems usually may have noise, because of scanning hardware or paper background, and contain less discriminative information since only the image of the signature is the input to the system. While genuine signatures of the same person may slightly change, the differences between a forgery and a genuine signatures may be difficult, which make automatic off-line signature verification be a very challenging pattern recognition problem. In addition, the difference in pen widths and unpredictable change in signature's aspect ratio are other difficulties of the problem. It is worth to notice the fact that even professional forensic examiners perform at about 70% of correct signature classification rate (genuine or forgery).Unlike offline, On-line signatures are more unique and difficult to forge than their counterparts are, since in addition to the shape information, dynamic features like speed, pressure, and capture time of each point on the signature trajectory are available to be involved in the classification. As a result, on-line signature verification is more reliable than the off-line.

Performance Evaluation of Signature vs. System: For evaluating the performance of a signature verification system, there are two important factors: the false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures. As these two are inversely related, lowering one often results in increasing the other. The equal error rate (EER) which is the point where FAR equals FRR.

There are two types of forgeries:

- A skilled forgery is signed by a person who has had practiced a genuine signature.
- A random or zero-effort forgery is signed without having any information and practice about the signature, or even the name, of the person whose signature is forged.

The performance of the available on-line signature verification algorithms give equal error rate between 1% and 10% , while off-line verification performance is still between 70% and 80% equal error rate.

There have been several studies on on-line signature verification algorithms. On-line signature verification systems differ on various issues like data acquisition, preprocessing, and dissimilarity calculation.

1.3.3 Advantages:

In the point of view of adaption in the market place, signature verification presents three likely advantages over other biometrics techniques.

- First nowadays it is a socially accepted verification method already in use in banks and credit card transaction.
- Second, it is useful for most of the new generation of portable computers and personal digital assistants (PDAs) use handwriting as the main input channel.
- Third, a signature may be changed by the user. Similarly to a password while it is not possible to change finger prints iris or retina patterns.

Therefore, automatic signature verification has the unique possibility of becoming the method of choice for identification in many types of electronic transactions, not only electronics but also for other industries.

1.3.4 Applications:

Signature verification has been and is used in many applications ranging from governmental use to commercial level to forensic applications.

A few of them are discussed below:

Security for Commercial Transactions*:* Nowadays signature verification used for commercial use. It can be used for authentication on ATMs, for package delivery companies. The internationally recognized courier service UPS has been using signature verification for many years now for personnel identification.

Secure computer system authentication: Logging on to PCs can be done with a combination of signature verification system and fingerprint identification system to achieve a higher level security in a sensitive area. We can also use a combination of password and signature verification system. This would allow the users to have a higher level of security and confidentiality for their clients and protection of their work.

Cheque Authentication: Signatures have been using for decades for cheque authentication in banking environment. But even experts on forgeries can make mistakes while identifying a signature. In general, Off-line signature verification can be used for cheque authentication in commercial environment.

Forensic Applications: Signature verification techniques have been used for cheque fraud and forensic applications.

1.4 General System Overview:

A dynamic signature verification system gets its input from data acquisition device like a digital tablet or other, dynamic input device. The signature is then represented as time-varying signals. The verification system focuses on how the signature is being written rather than how the signature was written. This provides a better means to grasp the individuality of the writer but fails to recognize the writing itself.

1.4.1 General Diagram:

In general online signature verification system has different phases. These phases are treated as an individual processes. The general system diagram for signature verification is as given below in Figure 1.4:

The Figure 1.4 shows the process used for development of system. Input is taken from a digitizer or such kind of device like webcam. This input is in the form of signal.

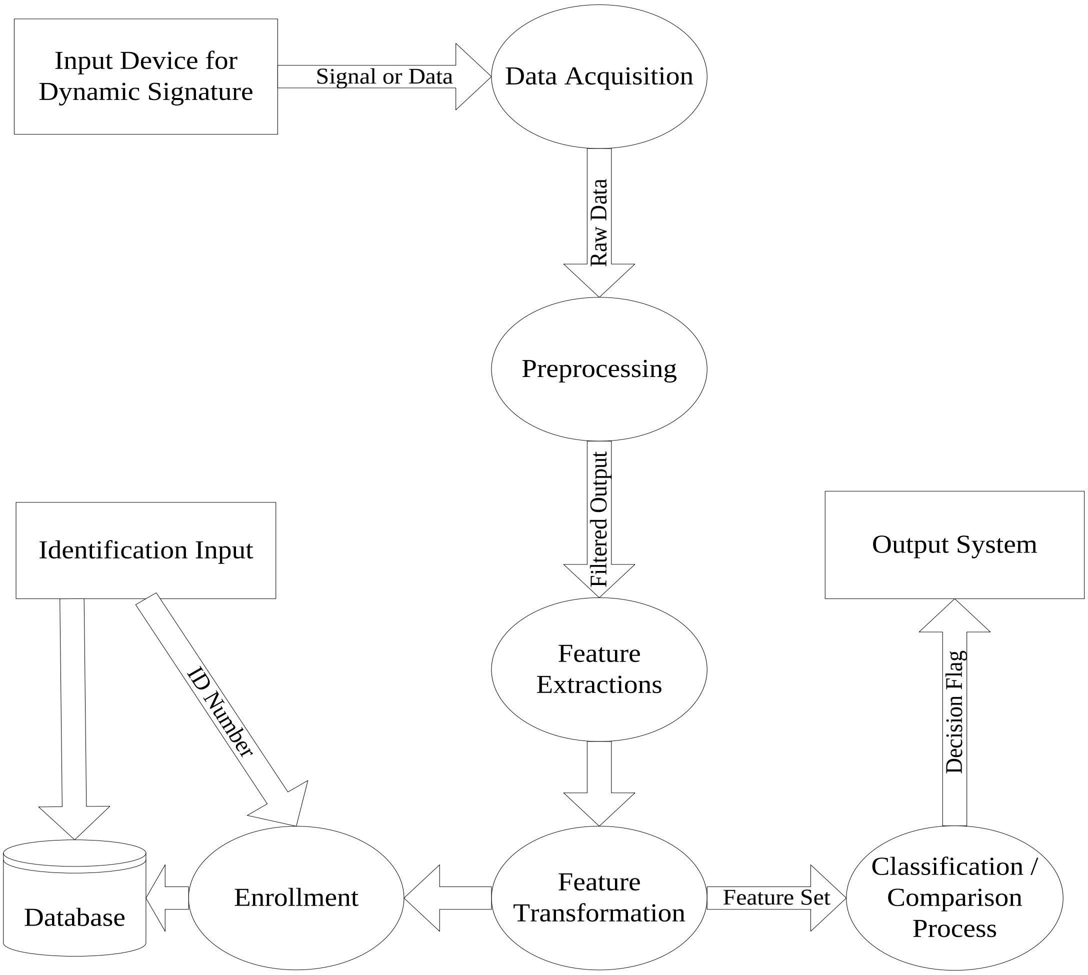


Figure 1. 4 General System Overview

1.4.2 Input:

For an on-line signature verification system, input is dynamic. This input is normally captured through a digital tablet or like other device. This input is digitized and fed for processing. First of all pre-processing is done on the input received and then some features are extracted from the caputerd online data on the basis of which the signature is validated.

1.4.3 Output:

The output obtained from an online signature verification system is a decision if the person providing the signature is authorized or not.

1.4.4 Preprocessing:

There are some common preprocessing steps, aimed to improve the performance of a verification system. These include size normalization, smoothing of the trajectory and re-sampling of the signature data. Low resolution tablet or low sampling rates tablets may give signatures that have jaggedness which is commonly removed using smoothing techniques. In the systems where tablets of different active areas are used, signature size normalization is a frequently used as preprocessing technique. Comparing of two signatures having the same shape but of different sizes would result in low similarity scores. Size normalization is applied to remove that affect. Modern digital tablets have a sampling rate of more than 100 trajectory points per second. In some of the previous methods, re-sampling, as a preprocessing step, was used to remove possibly redundant data. After successful re-sampling, shape related features were reliably extracted

1.4.5 Feature Extraction:

Feature extraction stage is one of the crucial stages of an on-line signature verification system. Features cans be classified as global or local, where global features represents signature's properties as a whole and local ones correspond to properties specific to a sampling point. The global features examples are signature bounding box, trajectory length or average signing speed, and distance or curvature change between consecutive points on the signature trajectory are local features.

Feature Types for Signature Authentication:

It is important to implement identity verification modality which provides high degree in performance and is still acceptable by a majority of users. A signature can be authenticated using either static (off-line) or dynamic (on-line) verification.

- Static (off-line): 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 enrolled (reference) signature. The difficulty with this technique is that a good forger will be able to copy the shape of the signature.

- Dynamic (on-line): The user's signature is acquired in real-time. By using this dynamic data, further feature such as acceleration, velocity, and instantaneous trajectory angles and displacements can be extracted.

The selection of features for extraction is difficult for the performance of a bio-metric authentication system. The features extracted must have able to describe the signature, separable between classes and also invariant within the same class. Two types of features can be extracted are both dynamic and static feature sets. For both dynamic and static feature sets, they are parameter based features and function based features. In general, function based features give better performance than parameters, but they usually time-consuming matching procedures. Parameter based features are easily computed and matched because of its simplicity.

When creating a system, it is important task is to take into account different external factors. For example like a bank or teller application, the retrieval of features and computation of matching has to be fast 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 creating a system is also an issue for certain applications.

Certain criterions have to be established during feature extraction to obtain the suitability of the feature set. The list of the criteria shown below, 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 based on different classes. This allows for low equal error rates during verification.

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

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

4. The amount of features extracted has to be small enough to be stored in a smart card. The number of features should be small,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 users are distinguishable with minimum computational risk.

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

1.4.5.1 Dynamic Feature Set

The dynamic feature set describes how the signature is being signed rather than how it seems. Dynamics of the signature are very difficult to forge because these not only have the information of the overall shape of the signature, but also dynamic information of signature. When the user sign on a data acquisition module, it needs to be scanned at a rate high enough to capture this information, and from this dynamic data, relevant features are extracted.

The dynamic feature set extracted consists of global parameter based features which allows us for easy and quick computing. This feature set requires less computational power and is of more cost efficient although it might not perform as well with compare to function based feature sets. The list of dynamic feature set is as follows:

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

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

3. Total length of the sign (1 digit): The total length of the signature calculated by adding the distance between each of the coordinates.

4. Maximum velocity (1 digit): While signing the maximum velocity found between two consecutive coordinates.

5. Minimum velocity (1 digit): While signing the minimum velocity found between two consecutive coordinates.

6. Duration of Vx : The total time that the pen is moving from left to right is indicated by this feature. It is obtained by adding up the amount of times that the pen is moving from left to right between two consecutive coordinates.

7. Duration of Vy : The total time that the pen is moving from down to up. It is obtained by adding up the amount of times that the pen is moving from down to up between two consecutive coordinates.

10. Length of signature horizontal: This feature describes the width of the signature. It can be found by subtracting the maximum x coordinate value with the minimum x coordinate value.

11. Length of signature vertical: This feature describes the height of the signature. It can be found by subtracting the maximum y coordinate value with the minimum y – coordinate value.

12. Area of signature: It can be found by multiplying both the length of the signature vertically and the length of the signature horizontally.

1.4.6 Enrollment

During enrollment, signature of each user is stored. The Non skilled forgeries and skilled forgeries are also enrolled in the database.

1.4.6 Verification:

During the verification stage, a signature to be tested and an ID of a claimed user are submitted to the system. The test signature is compared with the template of reference signatures enrolled in the data base. A threshold value is defined and the test signature is classified as genuine or forged depending on the threshold value.

1.4.7 Identification:

During the identification stage, only the test signature and no ID are submitted to the system. The unknown test signature is compared with every template signature enrolled in the database. The signature is identified which it belonging to in the database to which it is closest to[18].

1.5 Performance Evaluation:

The performance of biometric verification systems is typically described based on terms, the false accept rate (FAR) and a corresponding false reject rate (FRR). A false acceptance occurs when the system allows an forger’s sign is accepted. A false reject ratio represents a valid user is rejected from gaining access to the system. These two errors are directly correlated, where a change in one of the rates will inversely affect the other. A common alternative to describe the performance of system is to calculate the equal error rate (EER). EER corresponds to the point where the false accept and false reject rates are equal. In order to visually comment the performance of a biometric system, receiver operating characteristic (ROC) curves are drawn. Biometric systems generate matching scores that represent how similar (or dissimilar) the input is compared with the stored template. This score is compared with a threshold to make the decision of rejecting or accepting the user. The threshold value can be changed in order to obtain various FAR and FRR combinations.

The ROC curve represents how the FAR changes with respect to the FRR and vice-versa.

An ROC curve example is shown in Figure 1.4. These curves can also be plotted by using the genuine accept rate versus the false accept rate. The genuine accept rate is obtained by simply one minus the FRR.

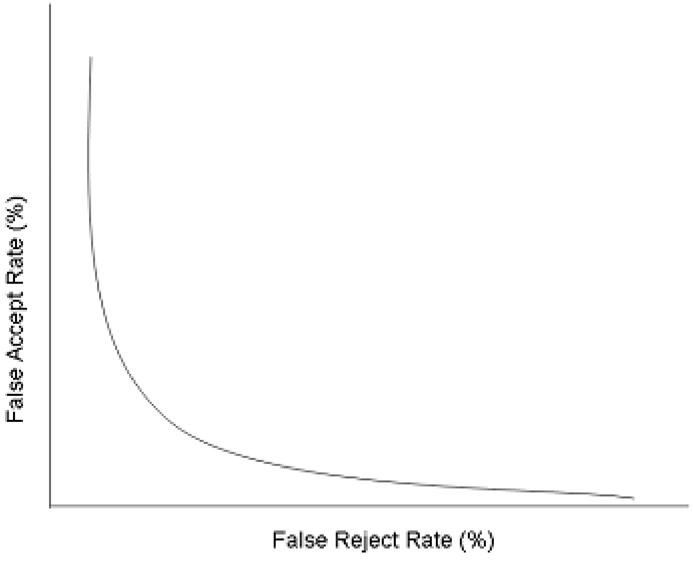


Figure 1. 5 Example of a receiver operating characteristic (ROC) curve

1.6 Thesis Outline

In chapter 2, a comprehensive literature survey of the major techniques implemented in the field of signature verification is presented.

In chapter 3 the implemented technique is discussed along with Database creation.

In chapter 4 the discussion of the results are included.

The references and appendix is at the end of the thesis.

Chapter 2

2. Literature Survey

In human life security takes important role. Nowadays it’s the basic fundamental of all systems developed. For this purpose, biometric authentication system got a lot of importance. Biometric authentication systems are secure, easy to use, easy to develop, uses basic techniques of signal processing and cheap to build. This improves the familiarity of biometric authentication system. Among these techniques signature verification is the most famous one because of cheap data acquisition devices. We can see the use of on-line signature verification in every kind of real time applications, such as credit card transactions, document flow applications, and identity authentication prior to access of sensitive resources. There have been several studies on on-line signature verification algorithms.

Most commonly used on-line signature acquisition devices are pressure sensitive tablets, digitizer and webcam etc. Smart pens are also widely used in signature verification systems, which are capable of measuring forces at the pen-tip, exerted in three directions. Special hand gloves with sensors for finding finger bend and hand position and orientation, and a CCD camera based approaches were also in signature acquisition; however, due to their high cost and impracticality, such devices couldn’t find use in real systems. Depending on the device used, fair amount of preprocessing may be required to a signature data before the feature extraction phase.

This portion of thesis is to describe about the previous work in the field of signature verification. The on-line signature verification techniques can be classified into two broad areas.

1. Using features extracted from the visible parts of the signature.
2. Using features extracted from virtual strokes or invisible parts of the signature (the parts that are not created but are imagined to be created).

2.1 Using Variable Length Segmentation and Hidden Markov Models:

In paper [8], Shafiei introduced a new on-line handwritten signature verification system using Hidden Markov Model (HMM) . The system proposed by him is based on variable length segmentation of signatures in a HMM model for on-line signature verification. To achieve this, he segmented each signature at its perceptually important points. Then after applying some preprocessing, he associated to each segment a scale and displacement invariant feature vector.

The result of segmentation is a number of variable length segments for each signature. Each segment is now characterized by location of its most significant point in the signature. Features to be extracted are average velocity, average acceleration, average pressure, pressure variance and two angles of tangent lines to curve of segment in two segment end points.

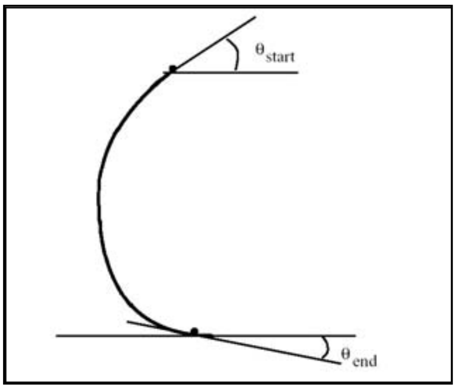


Figure 2. 1 Angle of Tangent at Two End Points

Finally, the resultant sequence is then used for training an HMM to achieve signature verification. For each signer an HMM is trained using 5 genuine signatures. Assuming mixture of 10 Gaussians for emission probabilities for this HMM. The number of states of each HMM model equals to 0.5 times the average number of segments that is computed for each signature in the training set.

He used EM algorithm during enrollment and the Viterbi algorithm during the verification stage to approximate the likelihood of the signature. The overall information of this paper is shown in Table 2-1.

Table 2. 1Using Variable Length Segmentation and HMM

Features used	Database Size				Features Extracted	Results	
	Total Persons	No.of sig/person	Forgeries	Total Sign		FAR	FRR
➢ Left to right HMM with loop ➢ Forward and skip transitions ➢ Density function modeling	69	4-34	1010	622	➢ Location of most significant point in the signature ➢ Average velocity ➢ Average acceleration ➢ Average pressure ➢ Pressure variance ➢ Two angles of tangent lines to curve	4%	12%

In this case he got high FRR, comparing to other works, were caused by the small number of signatures used in training phase. In spite of using Gaussian mixtures for modeling interpersonal variability, the HMM doesn't learn sufficiently these variability when using minimun number of signatures in the training phase [18].

2.2 On-line Handwritten Signature Verification using HMM Features:

In this paper[9], Kashi proposed a method for the automatic verification of on-line handwritten signatures using both global and local features. The global and local features indicate various aspects of signature shape and dynamics of signature production. He expalind that with the addition to the global features of a local feature based on the signature likelihood obtained from Hidden Markov Models (HMM), the performance of signature verification method improved significantly. In this paper, he models the signing process with many states that constitute a Markov chain, each of them corresponding to a segment of signature. The states are not directly observable (hidden); one can only observe the signature local features here as tangent angles. In this signature verification, the handwriting tangent and its derivative as an observation vector in equal length segmentation is used. The HMM likelihood method of the signature verification performed comparable to the Euclidean distance rule for this observation vector. The detailed information of this paper is shown in Table 2.2.

Table 2. 2 On-line Handwritten Signature Verification using HMM Features

Features used	Database Size				Features Extracted	Results	
	Total Persn	No. of sig/persn	Forgrs	Total Sign		FAR %	FRR %
➢ Length-to-width ratio L ➢ Horizontal span ratio ➢ Horizontal centroid ➢ Vertical centroid	59	6	325	542	Total of 23 Global features ➢ Total signature time ➢ Time down ratio ➢ x , y components of velocity and acceleration ➢ Root-mean-square (rms) speed V ➢ Average horizontal speed V. ➢ Integrated centripetal acceleration	13- 5	1

The combination of the HMM local and global feature information improved the performance of the system when compared to either the local or global methods used independently. The equal error rate has decreased from about 4.5% to about 2.5% with the enhanced technique. The addition of the local information reduces the false acceptance at the 1% false rejection (FR) point [18].

2.3 Dynamic Signature Verification using Local and Global Features:

In this paper [10], Pippin proposed two verification filters, each filter employing different techniques commonly used in the literature. The first filter extracts high-level global features of a signature and compares these features with stored signature templates using KNN classification. The second filter uses velocity based stroke segmentation to encode the signature as a series of strokes and then uses dynamic time warping to find the closest distance between test and template signatures. Considering only global features of a signature has advantages that it is simple to compute and addresses privacy concerns.

Table 2. 3 Dynamic Signature Verification using Local and Global Features

Features used	Database Size				Features Extracted	Results	
	Total Persns	No. of sig/persn	Forgrs	Total Sign		1st Filter	2nd Filter
➢ Average Pressure ➢ Pen Tilt. ➢ Average Velocity ➢ Number of Pen Ups ➢ Number of Strokes ➢ Velocity as a function of time	19	10	73	180	➢ Average Pressure ➢ Pen Tilt ➢ Average Velocity ➢ Number of Pen Ups ➢ Number of Strokes	91%	77%

This made this method ideal as an inexpensive technique that can be used to detect a majority of forgeries, without risk to privacy concern. This technique can classify signatures with approximately 89% accuracy with a small number of global features. The main strength of this method is that as an individual’s signature changes over time, each signature need only be added to the reference database, and newer signatures will naturally be closer to more recent reference signatures.

Two techniques for online signature verification using dynamic global and local features were described. It was also shown that specific threshold values improved the performance of the local filter. Moving ahead, further verification on a larger dataset should be performed. However, it is expected that with additional experimentation and adjustment of the feature sets results can be improved [10,18].

2.4 New extreme points warping technique:

In this paper [11], Feng proposed a new warping technique for the functional base approach in signature verification. Dynamic time warping (DTW) is the commonly used warping technique. There are two common methodologies to verify signatures: the functional approach and the parametric approach so the functional based approach was originally used in application speech recognition and has been applied in the field of signature verification with some successful accuracy since two decades ago. The new warping technique he proposed, named as extreme points warping (EPW). It was proved that this method is adaptive in the field of signature verification than DTW in the presence of the forgeries. In the functional approach, a straightforward way to compare two signal functions is to use a linear correlation. It has the following two problems:

- Due to difference of overall signal duration.
- Due to existence of non-linear distortions within signals.

For a signal function, the signal duration is the same for different samples even from the same signer. In addition, distortions occur non-linearly within the signals for different signings. A non-linear warping process needs to be performed before comparison to correct the distortion. An established warping technique used in speech recognition is dynamic time warping (DTW). The use of DTW has also become a major technique in signature verification for the past two decades. Though DTW has been applied to the field with success, it has some drawbacks.

DTW has two main drawbacks when applied in signature verification:

- It has heavy computational load,
- Another is warping of forgeries.

The first drawback is a known problem in case of speech recognition, because DTW performs nonlinear warping on the whole signal. For this method, the execution time is proportional to the square of the signal size; define boundary conditions in the DTW matching matrix to reduce the computation time. The second drawback, however, is not well documented in the past, but still got good accuracy and results as mentioned below in Table 2.4:

A new warping technique called EPW replaced the commonly used DTW. Instead of warping the whole signal as DTW does, EPW warps a set of selective points. We achieve the goal of warping the whole signal through matching the EPs and warping the segments linearly. Since EPW warps only EPs, the local curvatures between the EPs are saved, which prevents forged signals taking advantages from the warping process.

Table 2. 4 New extreme points warping technique

Features used	Database Size				Features Extracted	Results	
	Total Persns	No. of sig/persn	Forgrs	Total Sign		ER EPW)	EER DTW)
➢ Rise distance w.r.t time ➢ Drop distance w.r.t time	25	30	250	1000	Variations ➢ Non-synchronicity for the start point ➢ Existence of ripples ➢ Non-synchronicity for the end point	27.7%	35%

Using EPW, the EER is improved by a factor of 1.3 over using DTW and the computation time is also reduced by a factor of 11. Hence this new technique EPW is quite promising to replace DTW to warp signals in the functional approach, as part of an effective signature verification system.

2.5 Wavelet Transform Based Global Features:

In this paper a system proposed by F.A. Afsar [12], U. Farukh and M Arif. They worked in such a way that first the global features are extracted from the spatial coordinates and these features are obtained during the data acquisition stage. The method used here is one dimensional wavelet transform. Then the results are obtained using K-NN classifier and proved the accuracy of the proposed technique better. It is global feature based approach t signature verification. The signature patterns are matched based on wavelet domain features that are extracted from the normalized spatial coordinates of the signatures obtained during data acquisition. The differences between the spatial coordinates of consecutive points in the signature are also subjected to both wavelet decomposition and feature extraction. The total temporal duration of the signature used as a distinguishing feature during classification. The Figure 2.2 shows the block diagram of the system. The system is described in these stages

- Acquisition
- Preprocessing
- Feature Extraction
- Template Generation
- Feature Matching

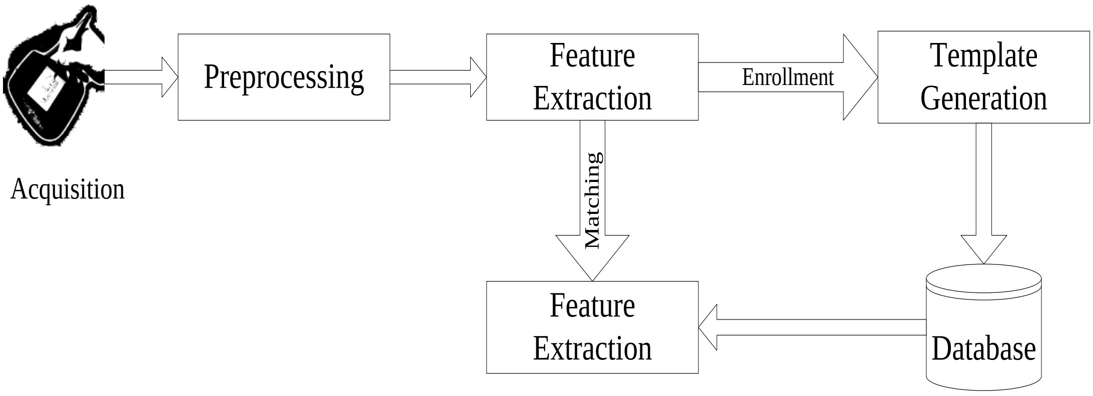


Figure 2. 2 System Overview

Online signatures are generally acquired by using digitizer or pressure sensitive tablets. To improve the reliability and accuracy of the feature extraction process, preprocessing is carried out prior to feature extraction in order. Then the local and global features are extracted. During enrollment phase of an online signature verification system, features from multiple training signatures of a subject are used to create a template. The detailed information is shown in Table 2.5.

Table 2. 5 Wavelet Transform Based Global Features

Features used	Database Size				Features Extracted	Results	
	Total Persns	No. of sig/persn	Forgrs	Total Sign		AR	RR
➢ Pressure ➢ Velocity ➢ Pen Ups ➢ Velocity as a function of time ➢ X-coord ➢ Y-coord	100	15	5	2000	➢ Total time ➢ No of zero crossings in x-velocity ➢ No. of zero crossings in y-velocity ➢ No. of zero crossings in x-acceleration ➢ No. of zero crossings in y-acceleration ➢ No. of zero values in x-acceleration ➢ No. of zero values in y-acceleration ➢ Average pressure ➢ overall path length	Ran 3.21 Skl 6.79	Ran 3.27 Skl 6.61

The template of the subject is stored in a database and is used in the matching phase. In the matching stage of an online signature verification system, features extracted from a given signature are compared with the stored template to generate the matching score, based on which the verification decision is depend. These results very clearly demonstrate the importance of the global features obtained using the Wavelet Transform. The results can be improved further if orientation normalization and re-sampling is carried out during preprocessing and some local features are also used along with the global features.

2.6 Two-Stage Statistical Model:

In this paper [13], Liang Wan proposed a new two-stage statistical system for automatic on-line signature verification. System is consists of a simplified GMM model for global signature features and a discrete HMM model for local signature features. He explained specific simplification strategies for system building and training. The system requires only 5 genuine samples for new users and depends on only 3 global parameters for quick and efficient system tuning. Experiments are conducted to verify the effectiveness of this system. The Figure 2.3 shows the block diagram of signatures verification system.

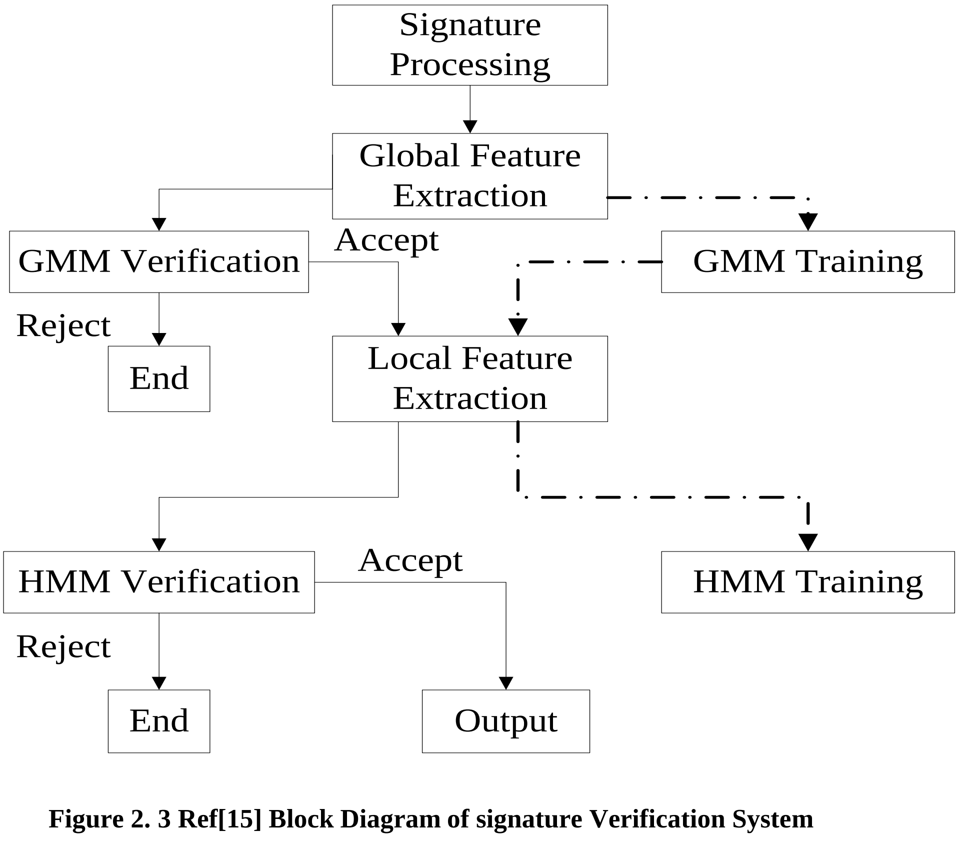


Figure 2. 3 Ref[15] Block Diagram of signature Verification System

It is basically a two-stage statistical system to on-line signature verification. The system is composed of a simplified GMM model built for global signature features and a left-to-right HMM model based on segmental features. The general GMM model and

HMM model are complex for this specific application, so he introduced specific strategies to do model building and initialization.

System depends on 3 global parameters to control its performance. Features are estimated globally for all users such that forgeries are only needed for system.

Table 2. 6 Two-Stage Statistical Models

Features used	Database Size				Features Extracted	Results
	Total Persns	No. of sig/persn	Forgrs	Total Sign		Accuracy
➢ the average speed ➢ maximum speed ➢ average pressure ➢ maximum pressure difference between two sample points, ➢ total duration time ➢ Ratio of pen-down time to total writing time.	NA	5	No	5/person	➢ width and height ➢ total length of signature strokes ➢ stroke count and number of self-intersection points; ➢ segment count ➢ Total curvature.	93.3 % (With Pressure) 89.7% (Without Pressure)

For each signer, two models are processed separately, corresponding to global and local signature information (features). In global modeling, a Gaussian mixture model to estimate the distribution of global features such as time duration and average speed is used. In local modeling, he introduces an HMM model based on both piecewise information and structural relation between strokes.

The signature is accepted as genuine only when it also passes the HMM verification test. The highlights of system are listed below:

- Given the well-established system, it only uses few genuine signatures as training data for a new user. No forgeries are used in the training stage.
- Discriminative local and global features are proposed, respectively.
- This system adopts a two-stage statistical structure, where the global features can rule out obvious forgeries quickly.

The system can be easily modified since there are only three global parameters involved [18].

2.7 Biometric Authentication using Online Signatures:

In his paper [14] Alisher, proposed a system for on-line signature verification. Here approaching the problem as a two-class pattern recognition problem. During enrollment, reference signatures are collected from each registered user and cross aligned to extract featurs about that user's signature. A test signature's authenticity is established by first comparing it with each reference signature for the claimed user. The signature is then classified as genuine or forgery based on the alignment scores which are normalized by reference statistics, using standard pattern classification techniques. He experimented with the Bayes classifier on the original data as well as a linear classifier used in conjunction with Principal Component Analysis (PCA). The system has following phases:

- Data Acquisition
- Feature Extraction
- Signature Alignment
- Enrollment
- Training
- Verification

During the enrollment phase, a set of reference signatures are enrolled, which are used to determine user dependent parameters characterizing the variance within the reference signatures. The reference set of signatures together with these parameters stored with a unique user identifier in the system's database. When a test signature is input to the system for verification, it is compared with each of the reference signatures of the claimed person. The person is authenticated based on the resulting dissimilarity measure.

Table 2. 7 Biometric Authentication using Online Signatures

Features used	Database Size			Features Extracted	Results	
	Genuine Sign	Forgrs	Total Sign		FAR	FRR
➢ X-coordinates ➢ Y-coordinates	182	313	500	➢ x-y coordinates relative to the first point of signature trajectory ➢ x and y coordinate differences between two consecutive points(*¢x;¢y*), ➢ Curvature differences between consecutive points.	Skl **Bayes** 3.51% **PCA** 1.28 %	Gen **Bayes** 2.19% **PCA** 1.65%

2.8 Signature Recognition through Spectral Analysis:

In this paper by CMAN F. LAM [15], the signatures were normalized for size, orientation, etc. After normalization, the X and *Y* coordinates of each sampled point of a signature over time (to capture the dynamics of signature writing) were represented as a complex number and are transformed into the frequency domain via the fast Fourier transform. A Gaussian probabilistic model was introduced to screen and select from the large set of features. The significant harmonics of the signature were sorted according to the chi-square value (equivalent to the signal-to-noise ratio). Fifteen harmonics with the largest signal-to-noise ratios from the true signatures were used in a verification analysis. The Table 2-8 gives the detailed information.

Table 2. 8 Signature Recognition through Spectral Analysis

Features used	Database Size				Features Extracted	Results
	Total Persons	No. of sig/person	Forgeries	Total Signatures		Error
➢ shape, ➢ motion ➢ pressure ➢ timing, ➢ transformation methods	20	8	152	312	➢ Shape ➢ Motion ➢ Pressure ➢ Timing, ➢ Transformation methods	2.5%

Signature data were recorded dynamically as integer values on a digital graphic tablet at intervals of 10 ms for 1024 points**.** The values of X and Y ranges from 0 to 2047. The Z values indicate whether the pen is down (Z = 1) or up (Z = 0). The data were stored on the computer in files of length 1024 lines. To remove noise and minor elements the recorded signature needs to be preprocessed, which include Spike and Minor Element Removal, Ligature, Drift, position, Duration, rotation, connect tails and scaling. After the signature data were normalized the data were then transformed into the frequency domain using the fast Fourier transform [18]**.**

2.9 Vision System for Pen Tracking:

In this paper [20], the author proposed the design of a system that captures both the spatial and temporal aspects of handwriting using a standard quality video camera as input device. Compare to others, cameras are of low cost and advances in manufacturing technology. There would be no need to buy additional hardware for the implementation of online signature verification system.

We captured video while a subject writing on a piece of paper and we manually identified the position of the pen tip in each image of the sequence using a mouse. Author observe that the trajectories are a bit noisy especially the one tracked at 30hz.The pen tip position is collected for all the images of the sequence including frames both cases in which the pen is actually writing on the paper and frames in which the pen is travelling above the paper. After taking away the strokes that correspond to the pen moving above the paper and leaving only the strokes that correspond to the pen down on the paper. The trajectories are clear enough to enable one to easily read what was written.

2.9.1 System description

Figure2.4 shows the block diagram of the system and the experimental setup. The images captured by the camera are shown on the screen of the computer to provide visual feedback for the user. The user has the flexibility of placing the relative positions of the camera and the piece of paper in order to write with comfort as well as to provide the system with a clear sight of the pen tip.

The camera captures a sequence of images to the preprocessing stage. This phase performs initialization of the algorithm, i.e., it finds the initial position of the pen and selects a template (rectangular sub region of the image) corresponding to the pen tip. In subsequent frames, the preprocessing stage has only the function of cutting a piece of image around the predicted position of the pen tip and feeding it to the next block. The task of pen tip tracker has to find the position of the pen tip in each frame of the sequence. The ballpoint detector finds the position of the very end of the tip, i.e., the place where the pen is in contact with the paper when the user is writing. The filter is a recursive estimator that predicts the position of the pen tip in the next frame based on an estimate of the current position, velocity and acceleration of the pen. The filter also estimates the most likely position of the pen tip for missing frames. At last, the last block of system checks the presence of ink on the paper at the ball point detected positions [19].

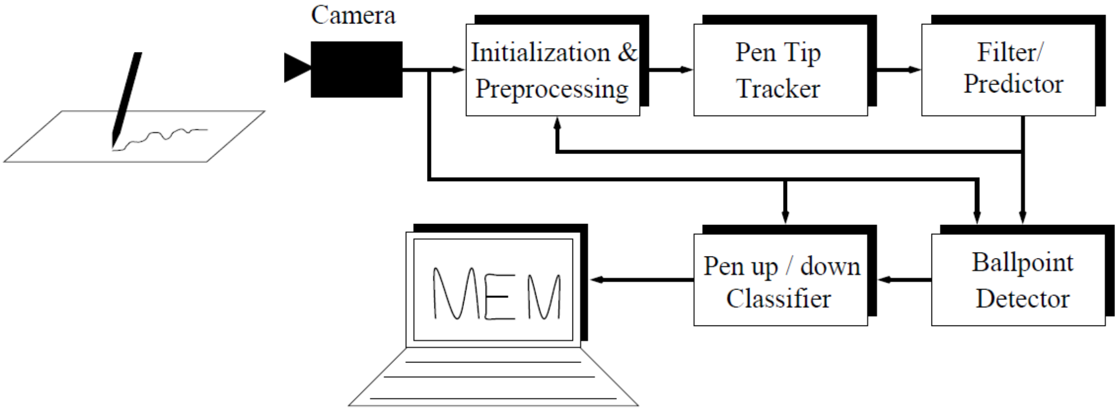


Figure 2. 4 Block diagram of the System

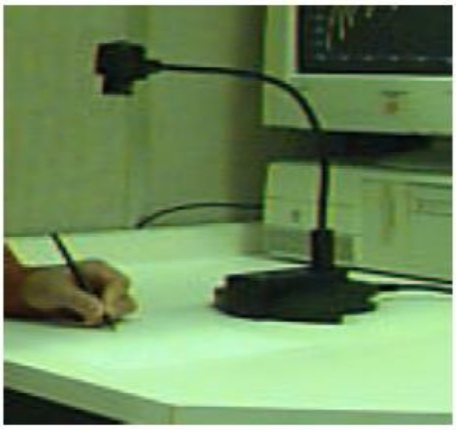


Figure 2. 5 Experimental set up

2.9.2 Initialization and Preprocessing

The first problem to be solved is to detect and locate the position of the pen tip in the first frame and to select the template to be used for detection in subsequent frames. There are two possible situations:

1. The user writes with a pen that is familiar to the system.
2. The user writes with a pen that unknown to system.

The familiar pen case is easy to handle, i.e., the system may use a previously used stored template representing the pen tip and detect its position in the image by using correlation.

There are some of methods to initialize the system when the pen is unknown. Here initialization method is a semi automatic one that requires a small amount of user cooperation.

Let us assume that the user is writing with a dark colored pen on a light colored piece of pen. For template, A rectangular box is over layered on this image as shown in Fig 2.6 (a). The user is requires to place the pen tip inside the displayed box, ready to start writing. The pen tip coordinates obtained by image differencing between frames. When the number of pixels obtained by image differencing is big enough as shown in Fig.2.6 (b), the system assumes that there is an object that entered the box and it then starts a waiting period until the object remains same. The user in this way has the possibility of placing the pen with in the box and taking a comfortable position on paper before starting to write. After the activity within the box has returned to low for a period of time, the system acquires the pen tip template and user starts tracking.

Figure2.6 shows a sketch of the pen tip, which is seems to be roughly conical .Hence, the projection of pixels of the pen tip on to the image plane will be a triangle. Here,one of the borders of this triangle corresponds to the edge between the pen tip and the piece of paper. Detection and extraction of the pen tip template is reduced to finding the boundary points of the pen tip by computing the corresponding centroid and cutting a portion of the image around the centroid. The edges between the pen tip and the paper have bigger contrast than the edge between the pen tip and the finger. Thus, we only look for these two boundaries in the detection and extraction of the template for pentip.

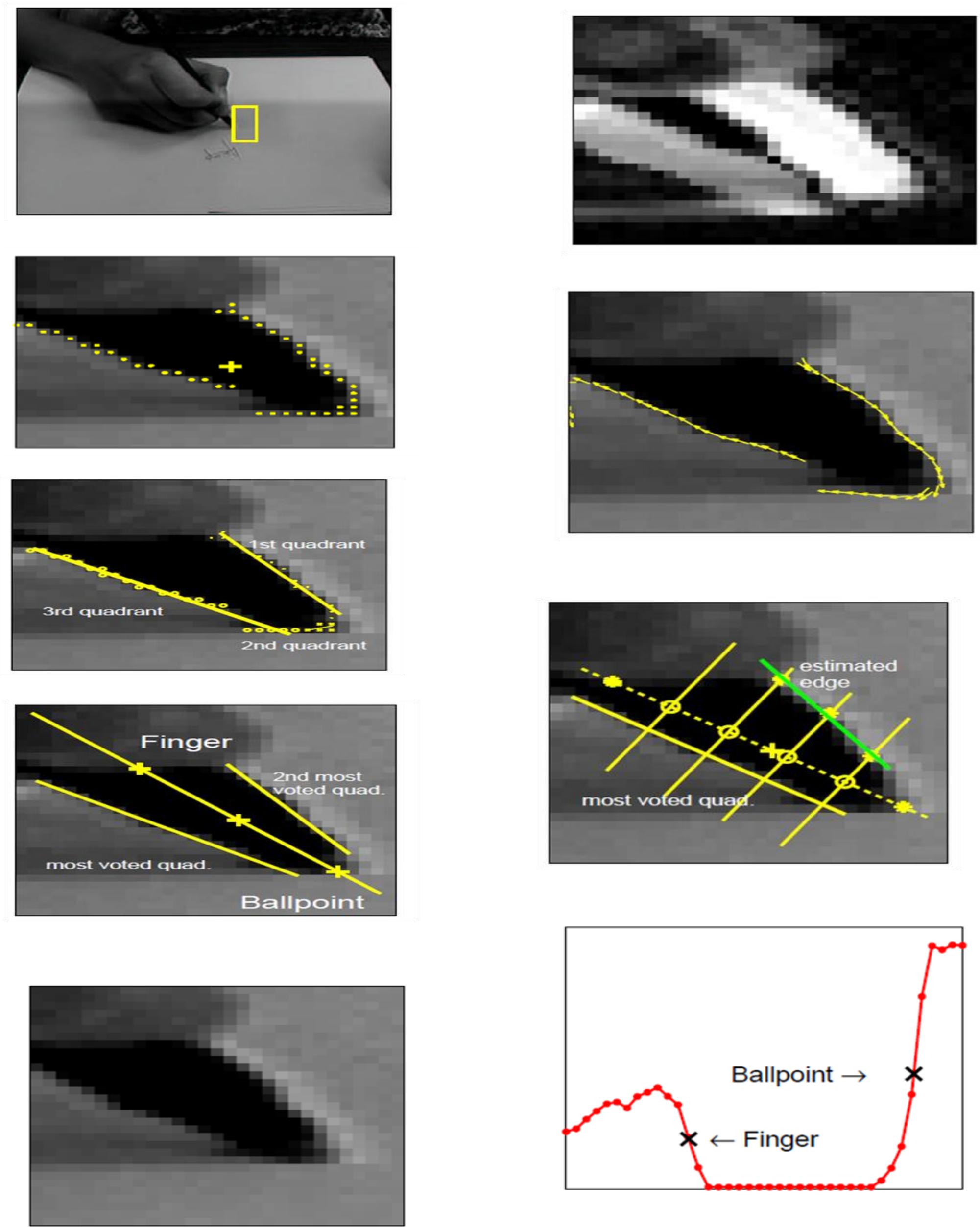


Figure 2. 6 Initialization and Preprocessing

(a) Image provided by the camera with the rectangular box overlaid.

(b)Result of image differencing when the pen enters the pen tip acquisition area.

(c) Output of Canny's edge detector used for extracting the boundary of the pen tip, where the cross indicates the centroid of the boundary points.

(d) Orientation of the edge elements extracted with Canny's detector.

(e) Combining of the edge elements into the four quadrants and lines indicating the mean orientation in each of the quadrants.

(f) Detection of the missing boundary edge using the estimated position of the centroid of the pen tip and the orientation of the other edge.

(g) Boundary lines obtained by combining the information provided by the edge detector across different frames. Here, Pen tip axis extracted as the mean of the boundary lines.

(h) Profile of the image across the estimated pen tip axis is used to find the positions of the ballpoint and the finger by performing a 1D edge detection [19].

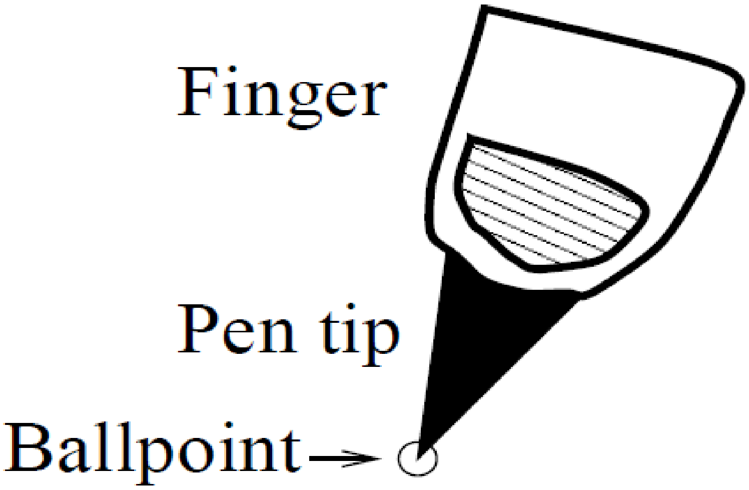


Figure 2. 7 Pen tip model assumed for the initialization

Since detection and extraction of the pen tip from a single frame is not very reliable due to changes in illumination.

The system collects information about the pen tip for a few frames before getting the template. The algorithm is summarized as follows:

1) Compute the difference between current image and previous image within the rectangular box until a sufficient number of pixels have a difference value bigger than a predefined threshold value, then go to step 2.

2) Compute image subtraction between current and previous images within the rectangular box until there is no activation for a sufficient number of frames, then go to step3.

3) Then apply Canny's edge detector to the neighborhood of the image inside the rectangular box.

4) Select only the neighborhood pixels that have sufficient contrast and whose parabolic cylinder has its axis close enough to the center of the pixel.

5) Obtain the centroid of these activated pixels.

6) Accumulate the orientation of the activated pixels in to four quadrants and get the mean orientation and the number of activated pixels per quadrant.

7) Repeat steps 3-6 for several frames and then go to step 8.

8) Compute the mean position of the centroids computed in 5.

9) Consider the most voted quadrant and compute the mean orientation across frames. If the most voted quadrant does not have sufficient votes, abort the extraction of the pen tip and emit a sound signal to let the user know the error condition.

10) Consider the second most voted quadrant, if it does not have enough votes, recompute its position and orientation using the current image and the results of 8 and 9. Obtain the mean centroid position and the estimated orientation of one of the boundaries of the pen tip, the profile of the image is searched perpendicular to this orientation in order to find points with high contrast. These points are used to estimate the location of the other the pen tip boundary.

11) Compute the pen tip's orientation as the mean of the orientations obtained in steps 9 and 10.The mean orientation is computed taking in to consideration the quadrant

information of steps 9 and 10 in order to omit problems with the inherent wrap-around $[0,360^0]$ of angular quantities.

12) Get the profile of the image along a line that passes through the centroid obtained in step 6 with the orientation calculated in step 9.

13) Find the position of the ball point and the finger in thse images by performing 1D edge detection on the image profile. Recompute the position of the centroid as the mean of the locations of the ballpoint.

14) Extract the template of the pen tip by selecting an area of the image of a effective adequate size around the centroid computed in step11.

The acquisition of the pen tip template is performed only at the beginning of the acquisition phase. The function of this module in subsequent frames is only to extract a region of interest in the neighborhood of the predicted position of the pen tip.

2.9.2. Pen tracking

The second module of the system has the task of tracking the position of the pen tip in the current frame of the sequence. The solution of this task is to get the optimal signal detection literature. Assuming that the signal to be detected is known exactly, the optimal detector is a matched filter which is a linear filter that looks like the signal one is trying to detect. In our case, the signal consists of the pixels that represent the pen tip and the noise has two components: one component is due to noise in the acquisition of the images and the other one is because of changes in the apparent size and orientation of the pen tip during the sequence of the images. The acquisition noise is the result of a combination of many factors like changes in illumination due to light flickering or automatic gain of the video camera, quantization noise, changes in gain of the frame grabber, etc. where not all these factors are effective. Changes in the apparent size and orientation of the pen while the user is writing significantly distort the image of the pen tip, as shown in Fig 2.7. The detection of the position of the pen tip is obtained by locating the maximum of the normalized correlation between the pen tip template and an image neighborhood centered on the predicted position of the pen tip.

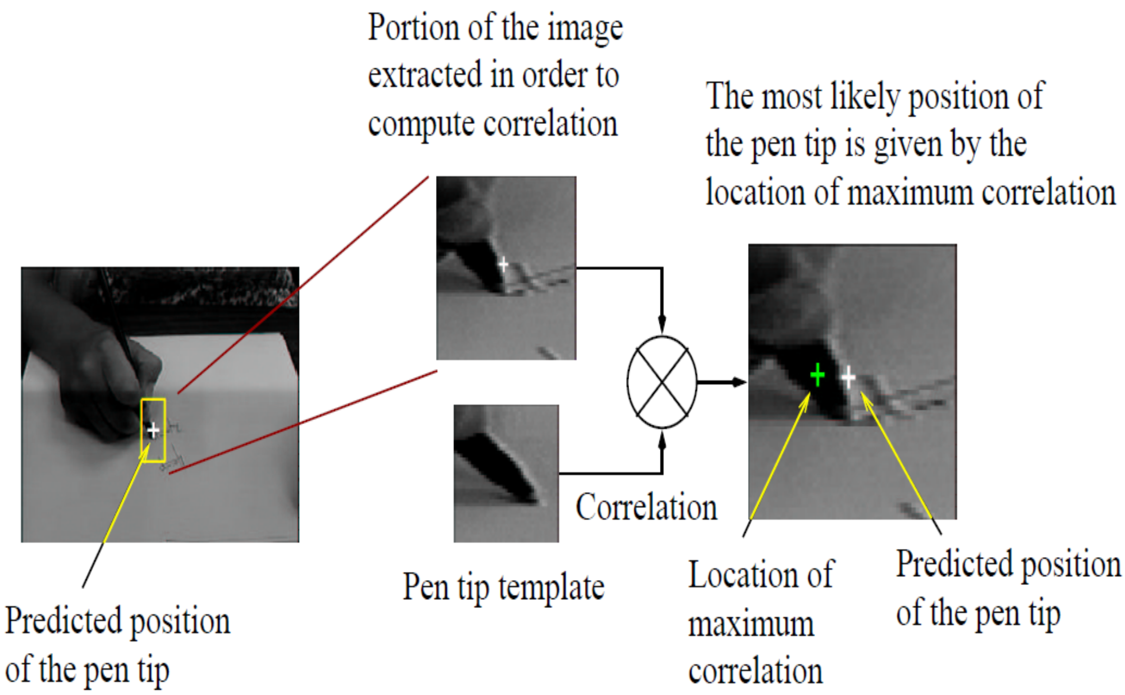

Portion of the image extracted in order to compute correlation
The most likely position of the pen tip is given by the location of maximum correlation
Correlation
Pen tip template
Location of maximum correlation
Predicted position of the pen tip
Predicted position of the pen tip

Figure 2. 8 Given the predicted location of the pen tip in the current frame.

The most likely position of the pen is obtained by finding the place where that has maximum correlation with the previously stored template of the pen tip.

The spatial resolution of the interface is defined by the localization accuracy during the computation of the maximum correlation between template and images. Sub-pixel resolution is achieved by fitting a paraboloid to the correlation surface in the neighborhood of the pixel with maximum correlation.

The system also analyzes the values of maximum normalized correlation to detect whether the pen tip is not within the predicted image neighborhood or not. If the value of maximum correlation is lower than a threshold, the system gives an audible signal and continues to look for the pen tip in the same place, waiting for the user to realize that tracking has been lost and that the pen tip must be returned to the image neighborhood. The system waits for a few frames and if the pen tip does not return to sight, then the tracking stops.

Chapter 3

3. Implemented Technique

We implemented a camera (webcam) based online signature verification system. The system consists of two low cost webcams. The input online signature data obtained by time series images, which are acquired through webcam by pen tip tracking, while the signature is being written. The pen tip tracking is obtained by sequential Monte Carlo method. We are taking two camera positions one at left side and another at front side. The input signature and reference signature data are compared with calculation of distance between them using DTW (dynamic time warping) method. Finally, the input signature is classified as genuine or forgery by comparing the distance with a threshold. We collected signatures from 10 users. We observed that the system was suit for signature verification. We investigated the effects of camera positions on verification accuracy [3,4&6].

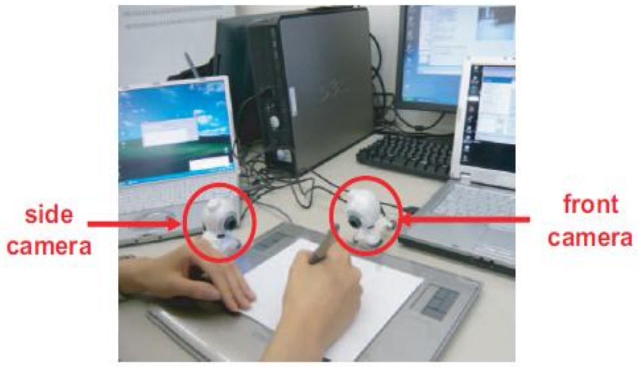


Figure 3. 1 Position of webcams

Side camera: The webcam is placed at the left side of the hand.

Front camera***:*** The webcam is placed at the front of the hand.

3.1 Overview of the system:

There are two stages in algorithm:

Enrollment phase: The user produces several signatures for enrollment. The time series images are obtained by webcam. The online signature data obtained from images captured by webcam by pen trip tacking. Then this data preprocessed and some features are extracted. The extracted features enrolled as reference data.

Verification Phase**:** The test signature given as input for verification. The time series images are obtained from webcam. The online signature data obtained from these time series images by pen trip tracking using sequential Monte Carlo methods. Then the data undergo pre-processing and some features are extracted. The extracted features of test signatures compared with the reference signature enrolled in data base features and dissimilar scores are calculated. A decision is made by comparing the distance with a threshold value .

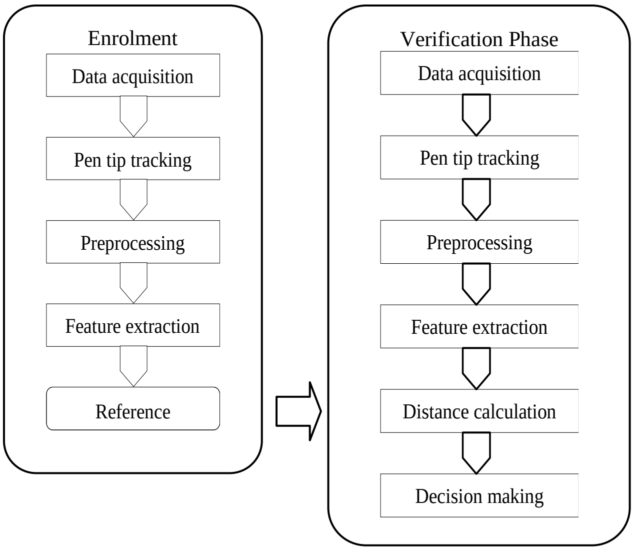


Figure 3. 2 Overview of the System

The Individual phases**:** Data acquisition, pen trip tracking, preprocessing, feature extraction, distance calculation and decision making.

3.2. Data acquisition

We first capture video while the user signing using webcam. Then transform video into frames. The static images are obtained by webcam while a signature being written. We use the images from the side camera and the front camera independently.

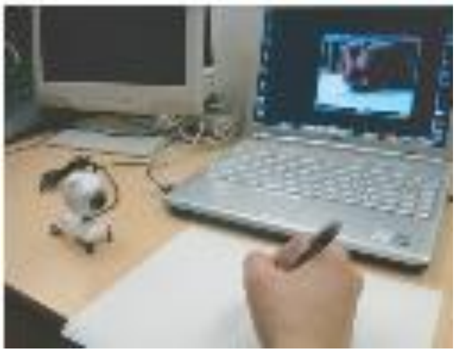


Figure 3. 3 Data acquisition

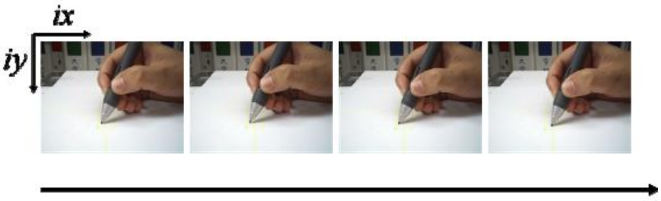
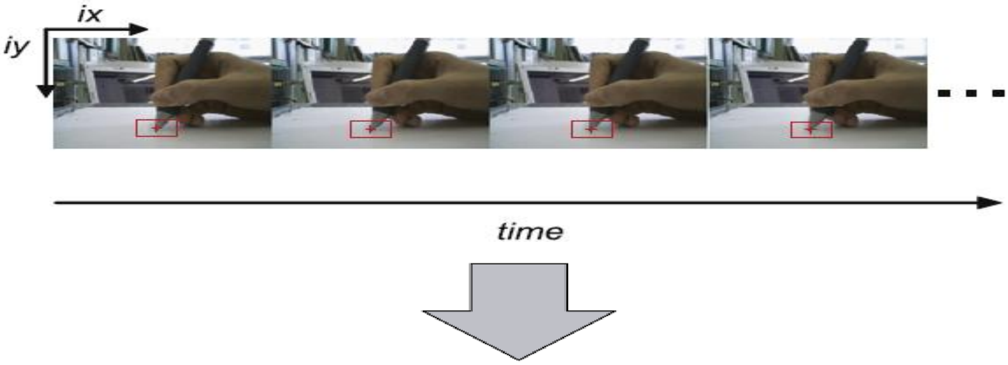


Figure 3. 4 Time series images

3.3. Pen tip tracking

To get the pen tip coordinates, it is to detect repeatedly the position of the pen tip in each frame. The input online signature data consists of two dimensional time series data. The procedure of pen tip tracking here obtained by using Monte Carlo method. It is observed that the y-coordinate information on the image from left hand side cam has decreasing trend with respect to time because a signature moves from left to right in real space and this moment is consistent with the decreasing direction of the y-coordinate in image space. The x-coordinate information on the image from the left hand cam does not show such a effect in a signature [6].



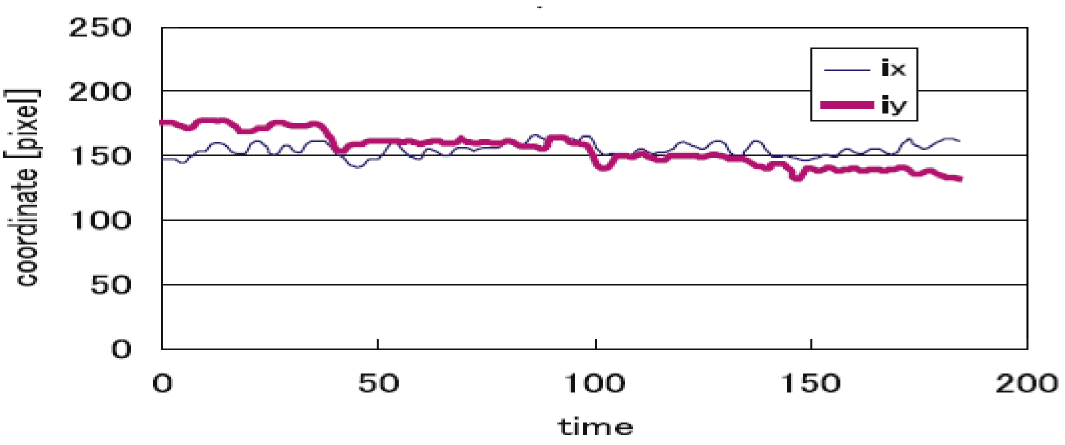


Figure 3. 5Online signature data acquisition from frames. By tracking the pen tip and obtaining pen tip positions from the frames, trajectories of x- and y-coordinates are obtained as time series datasets.

It id to detects repeatedly the position of the pen tip in each frame to get the signature data. The signature data obtained from the static images consists of two dimensional time-series data:

$$signature = \{(x_t, y_t)\}_{t=1}^{T} \qquad \text{.....................(3.1)}$$

where $(x_t, y_t$) are the coordinates of the pen tip detected at time t. The observed thing here that the x-coordinate has an increasing trend with respect to time because a signature typically moves from left to right. On the other hand, the y-co ordinate, on the other hand, does not have such a effect in a typical signature.

SMC is a Bayesian sequential mont carlo technique, which approximates the posterior distribution using a set of weighted samples. In addition to that, since the probability of some samples is negligible, re sampling is necessary to omit degeneracy problems. A brief describe of SMC below, although SMC is now a fairly well known method.

We first convert color images of signature data to grayscale images to re-duce the computation time. Color images are represented by a combination of red, green, and blue (*R*,*G*, *B*). On the other hand, grayscale images are represents as shades of gray by using luminance *Y*, given by:

$$Y = 0.298912 \times R + 0.586611 \times G + 0.114478 \times B. \qquad (3.2)$$

For tracking the pen tip,we use rectangular features. Let (*w*,*h*) be the width and the height of the rectangle box, which are assumed to be constants. More general formulation is possible.

Let

$$\boldsymbol{X}_t = (ix_t\ ,iy_t\ ) \qquad (3.3)$$

be the center coordinates of a rectangle box at time *t* using the respective axes of the images.

3.3.1 Template:

The starting position of the pen tip with in rectangular box considered as template, we store the template of the pen tip in advance. It considered as the rectangular feature of the pen tip. We have to keep the luminance at each pixel within the rectangular box in the first position corresponding to the pen tip. Fig 3.6 shows an example of the template using data captured from left hand cam.

For data acquisition, only one type of pen or one type of camera is used. However it is possible, by changing the template, we can use a different type of pen that satisfies several conditions or a different type of camera with different characteristics.

3.3.2 Tracking the pen:

We define the input image obtained by the webcam captured while the user signing at time t as Y_t, Using the luminance information.

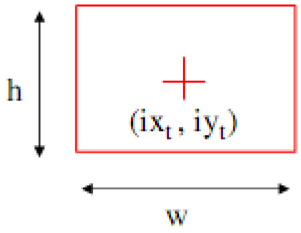


Figure 3. 6 Rectangular feature

The rectangle is centered at (ix_t, iy_t), and the width and the height of the rectangular are w and h, respectively which are constants. Rectangular area centered on pen tip is considered as a template.

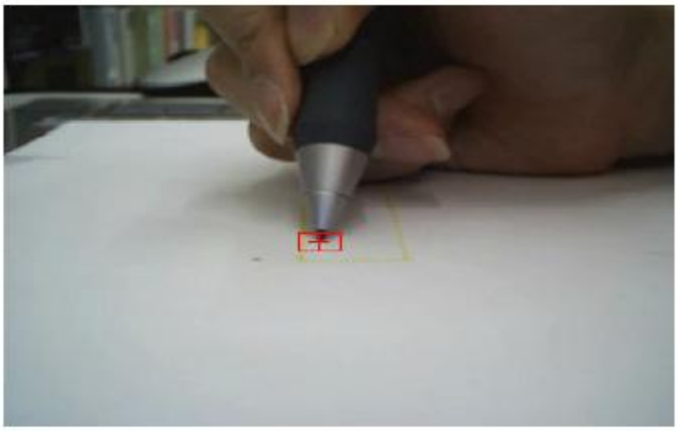


Figure 3. 7 Template data used for pen tip tracking

The likelihood information for pen tip is defined by

$$\text{P }(Y_t/X_t, \lambda_t) = \left(\frac{\lambda_t}{2\pi}\right)^{\frac{hw}{2}} \; exp\left[\frac{-\lambda_t}{2} \times score\right], \qquad (3.4)$$

where score means the dissimilarity measure and λ_t is hyper parameter to be learned online. Consider the following stochastic dynamics for X_t :

$$X_t = X_{t-1} + (X_{t-1} - X_{t-2}) + w_t \qquad (3.5)$$

$$w_t \sim N(0, \frac{1}{\xi_t}) \qquad (3.6)$$

where ξ_t a hyperparameter to be learned online .Thus, the task consists of sequentially estimating (X_t, λ_t, ξ_t) from the available image sequence$Y_{1:t} = \{Y_1, \dots., Y_t\}$. It follows from the Bayes formula that

$$P(X_t, \lambda_t, \xi_t \,|\, Y_{1:t}) = P(X_t, \lambda_t, \xi_t \,|\, Y_{1:t-1}) \frac{P(Y_t \,|\, X_t, \lambda_t)}{P(Y_t \,|\, Y_{1:t-1})} \qquad (3.7)$$

with predictive distribution

$$P\left(X_t, \lambda_t, \xi_t \,\middle|\, Y_{1:t}\right) =$$
$$\int P\left(X_t, \lambda_t, \xi_t \,\middle|\, X_{t-1}, \lambda_{t-1}, \xi_{t-1}\right)\; P\left(X_{t-1}, \lambda_{t-1}, \xi_{t-1} \,\middle|\, Y_{1:t-1}\right)\, d(X_{t-1}, \lambda_{t-1}, \xi_{t-1}), \quad (3.8)$$

Where the first term of the integrand is defined by

$$P\left(X_t, \lambda_t, \xi_t \,\middle|\, X_{t-1}, \lambda_{t-1}, \xi_{t-1}\right) = P\left(X_t \,\middle|\, X_{t-1}, \xi_{t-1}\right) P\left(\xi_t \,\middle|\, \xi_{t-1}\right) P\left(\lambda_t \,\middle|\, \lambda_{t-1}\right). \qquad (3.9)$$

The first factor $P\left(X_t \,\middle|\, X_{t-1}, \xi_{t-1}\right)$ will be the motion dynamics defined by (3.9) and second and third factors are the hyper parameters update dynamics, which will be assumed to be log normal:

$$P\left(\xi_t \,\middle|\, \xi_{t-1}\right) = \frac{1}{\sqrt{2\pi}\sigma_\xi \xi_t}\; exp\left[-\frac{(log\xi_t - log\xi_{t-1})^2}{2\sigma_\xi^2}\right], \qquad (3.10)$$

$$P\left(\lambda_t \,\middle|\, \lambda_{t-1}\right) = \frac{1}{\sqrt{2\pi}\sigma_\xi \lambda_t}\; exp\left[-\frac{(log\lambda_t - log\lambda_{t-1})^2}{2\sigma_\lambda^2}\right], \qquad (3.11)$$

Where σ_λ^2 and σ_ξ^2 are hyper-hyperparameters of hyperparameters λ and ξ, respectively. In the hierarchical Bayesian approach, the quality of estimation is reasonably robust about hyper-hyperparameters. Therefore we set the hyper-hyper parameters to be constant. One of the main reasons for using the log normal distribution is to ensure that the hayperparameters remain positive. This algorithm implements and updates the hyper parameters λ associated with different characteristics.

The SMC attempts to get samples from (3.7) without knowing the denominator $\mathrm{P}\left(Y_t \,\middle|\, Y_{1:t-1}\right)$. More specifically, let$\theta_t = (X_t, \lambda_t, \xi_t)$, let Q($\theta_t$) be a proposal distribution, and let

$$\theta_t^n \sim \mathrm{Q}\ (\theta_t)\ ,\ \mathrm{n}=1,\ldots..\mathrm{N} \qquad (3.12)$$

be a set of N samples from Q(Θ_t). The importance weights are given by

$$\Omega(\theta_t^n) = \frac{P(Y_t \,|\, \theta_t^n)P(\theta_t^n \,|\, Y_{1:t-1})}{Q(\theta_n^n)} \tag{3.13}$$

If the proposal distribution is (3.7) itself with (3.8) ,the denominator $Q(\theta_n^n)$ cancels out with the second factor of the numerator, and the importance weight becomes the likelihood:

$$\Omega(\theta_t^n) = P(Y_t \,|\, \theta_t^n). \tag{3.14}$$

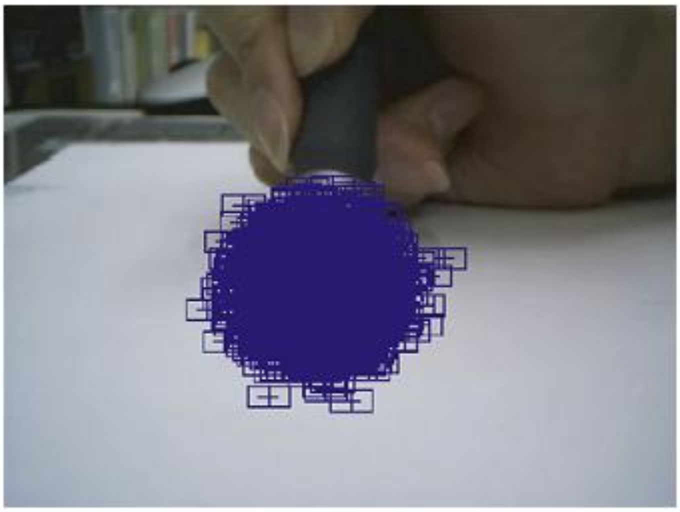


Figure 3. 8 Example of the initial samples using data captured from left hand cam. The samples are generated by adding Gaussian noise to the center coordinates of the initial position.

3.3.3 Estimation

The process of estimating the position of the pen tip by SMC is as follows

1. Initialization: t=0. It is to begin the tracking problem. It starts by generating a set of N samples by adding Gaussian noise to the center coordinates of the initial position (ix_0, iy_o):

$$ix_o^n = ix_0 + w_0^n \tag{3.15}$$

$$iy_o^n = iy_0 + w_0^n. \tag{3.16}$$

Where w_0^n is Gaussian noise with zero mean and unity variance.

Let us assume, at least, that (ix_0, iy_o) is given and the variance of the Gaussian noise is set with observation. One of the reasons for using Gaussian noise is to consider mainly samples close to the initial point and a few samples that are not close to the initial point are also considered.

2. the input image observation: t>0. The system observes the input image Y_t at time t.
3. Predictive distribution of samples: From Given the past data $Y_{1:t-1}$,the system generates a set of N samples Θ_t^n .

4. Computation of normalize weights: The system computes a set of N normalized importance weights by :

$$\bar{\Omega}(\Theta_t^n) = \frac{\Omega(\Theta_t^n)}{\sum_{n=1}^{N} \Omega(\Theta_t^n)} . \qquad (3.17)$$

5. Computation of the pen tip posterior mean: The system computes the estimated position in terms of the normalized importance weights

$$\overline{X_t} = \sum_{n=1}^{N} \bar{\Omega}(\Theta_t^n)\, X_t^n \qquad (3.18)$$

6. Resampling: The samples are resampled to omit degeneracy and extract important samples Θ_t^n according to each normalized weight$\bar{\Omega}(\Theta_t^n)$.

7. The system goes back to step 2.

3.3.4 Computation of dissimilarity

We compute the dissimilarity score between the template and each rectangle centre at each sample of each frame to acquire importance weights$\Omega(\Theta_t^n)$. We compute the sum of square difference (SSD). SSD is the computing the dissimilarity by subtracting the luminance Y at each pixel as is. Given that the size of the template image is h× w, we define the luminance at coordinates (i,j) within the template as $Y_{temp}(i,j)$. Therefore, the dissimilarity score is given by

$$score = \sum_{j=-h/2}^{h/2-1} \sum_{j=-w/2}^{w/2-1} \left(Y_t(i - ix, j - iy) - Y_{temp}\left(i + \frac{w}{2}, j + \frac{h}{2}\right)\right)^2 \qquad (3.19)$$

Even if the input images are small, SSD can express the dissimilarity clearly, because it uses the square difference. The dissimilarity score using SSD becomes zero if the sample corresponds exactly to the template.

3.4. Preprocessing

The following transformation is performed to obtained online signature data:

$$\left(\overline{ix_t}\,, \overline{iy_t}\right) = \left(\frac{ix_t - ix_g}{ix_{max} - ix_{min}}, \frac{iy_t - iy_g}{iy_{max} - iy_{min}}\right) \qquad (3.20)$$

These x and y coordinate information used as features.

where

$$ix_{min} = {}^{min}_{\ \ t}\ ix_t \qquad iy_{min} = {}^{min}_{\ \ t}\ iy_t$$

$$ix_{max} = {}^{max}_{\ \ t}\ ix_t \qquad iy_{max} = {}^{max}_{\ \ t}\ iy_t$$

$$ix_g = \frac{1}{T}\sum_{t=1}^{T} ix_t \qquad iy_g = \frac{1}{T}\sum_{t=1}^{T} iy_t \quad [4] \qquad (3.21)$$

3.5. Feature extraction

The pen movement vector θ and velocity V are calculated from the pen position(ix_t, iy_t) and are considered to features for verification purpose.

$$|v|_t = \sqrt{{v_{ixt}}^2 + {v_{iyt}}^2}$$

$$\theta = \tan^{-1}\left(\frac{v_{iyt}}{v_{ixt}}\right) \qquad (3.22)$$

where

$$v_{ixt} = \overline{ix_{t+1}} - \overline{ix_t} \qquad \text{t=1,2,…..T,}$$

$$v_{iyt} = \overline{iy_{t+1}} - \overline{iy_t} \qquad \text{t=1,2,…..T,} \qquad (3.23)$$

Therefore, the feature vectors that we use consist of the folllowing four-dimensional data elements:

$$\left(\overline{ix_t}\,, \overline{iy_t}, |v|_t\,, \theta_t\right) \qquad \text{t=1,2,…..T} \qquad [3] \qquad (3.24)$$

3.6. Distance calculation

Let us assume there are T number of reference signatures $Rsig^t$ are registered during the enrollement phase, where T stands for t number reference signatures and R stands for reference signature. We compute the distance between test input signatures and enrolled signatures to verify whether they are genuine or not. Two signature time sequences of n^{th} feature to be compared as $Rsig_n^t = \{r_{ni}^t\}_{i=1}^{I_t}$and $Sig_n = \{s_{nj}\}_{j=1}^{J}$where Sig stands for input signature.

1. Initialization

$$dist(0,0) = 0 \qquad (3.25)$$

2. Recursion

$$dist(i,j) = min\begin{cases} dist(i-1,j-1) + d(r_{ni}, s_{nj}) \\ dist(i-1,j) + d(r_{ni}, s_{nj}) \\ dist(i,j-1) + d(r_{ni}, s_{nj}) \end{cases} \qquad (3.26)$$

Where $d(r_{ni}, s_{ni})$ is a function that computes the distance between r_{ni} and s_{ni}

1. Termination

$$D(Rsig_n^m, sig_n) = dist(I,J) \qquad (3.27)$$

The distance of each feature $\{\overline{ix_t}\ , \overline{iy_t}, |v|_t\ , \theta_t\}$ is calculated separately. Distance vector between two time series data $Rsig_n^t$ and sig_n is given by

$$Dist(Rsig_n^m, sig_n) = (Dx, Dy) \qquad [6] \qquad (3.28)$$

3.7. Decision Making

The computed distance between test signature and enrolled signature data compared with the threshold to verify whether the signature is genuine or not. If the distance is smaller than the threshold then the input signature is genuine. The numbers of reference signatures are T. One dimensional distance calculated as

$$\overline{Dist}(sig_n) = \frac{1}{T}\sum_{t=1}^{T} Dist(Rsig_n^m, sig_n) \qquad (3.29)$$

The final decision is based on the following rule:

$$\begin{cases} Accepted\ if\ \overline{Dist}(sig) \leq threshold \\ Rejected\ if\ \overline{Dist}(sig) > threshold \end{cases} \qquad [6] \qquad (3.30)$$

Chapter 4

4. Experimental setup and Results

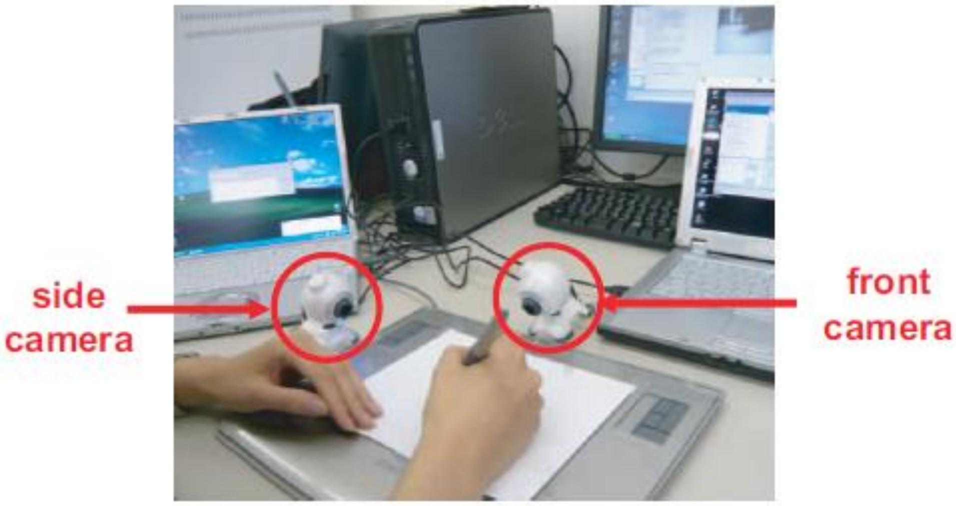


Figure 4. 1 Position of webcams

Side camera: The webcam is placed at the left side of the hand.
Front camera***:*** The webcam is placed at the front of the hand.

The implemented technique tested on a 2.4Ghz Intel Core2 PC with 2012MB memory. The cameras had a resolution of 320 × 240 pixels. The processing time for pen tip tracking was about 0.03s per frame.

4.1 Data collection:

The camera data captured from the side camera can be called as “side data” and the camera data captured from the front camera can be called as “front data”. The pen coordinates using x- and y-coordinates expressed in real space. The x- and y-axes of the fornt data and side data in real space were shown in Fig.4.5.For enrollment phase;We collected 20 signatures for 20 different users. 10 signatures were collected for verification phase.

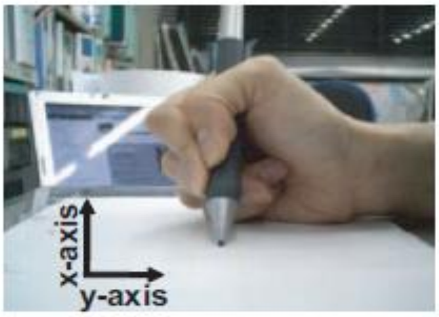


Figure 4. 2 Side data

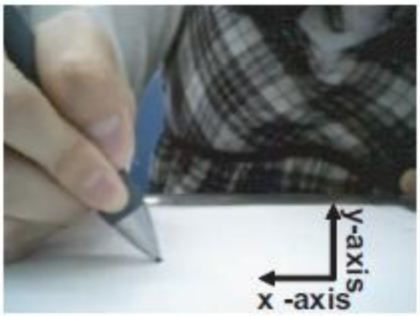


Figure 4. 3 Front data

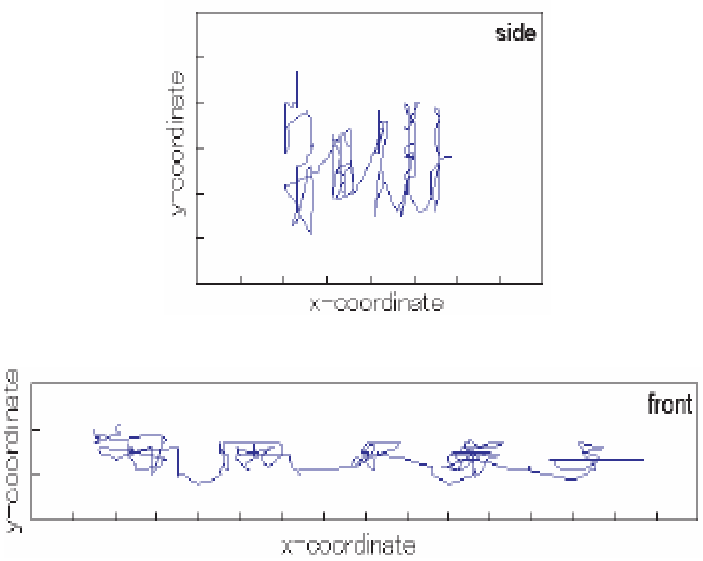


Figure 4. 4 Examples of signature data

4.2 Evaluation Criteria

The evaluation of each feature using the equal error rate (EER) computed as the intersection of the false acceptance rate (FAR) and the false rejection rate (FRR) curves.

FAR (False Acceptance Ratio): A false identity claim is accepted.
FRR (False Rejection Ratio): The error rate that a true user identity claims is falsely rejected.

We computed EER of each feature individually to evaluate the accuracy of each feature.

4.3 Evaluation

The experimental results depended on the fact that the setting of threshold. When feature ix was taken into consideration for verification, left hand cam was the best. This observation is easy, because feature ix in the images from left hand cam is much consistent with the y-coordinate information in real space, whereas feature ix in the images from front hand cam is consistent with the x-coordinate information in real space. Equal Error Rate(EER) tradeoff curves for left hand camera are shown Figures 4.6 – Figure 4.9.

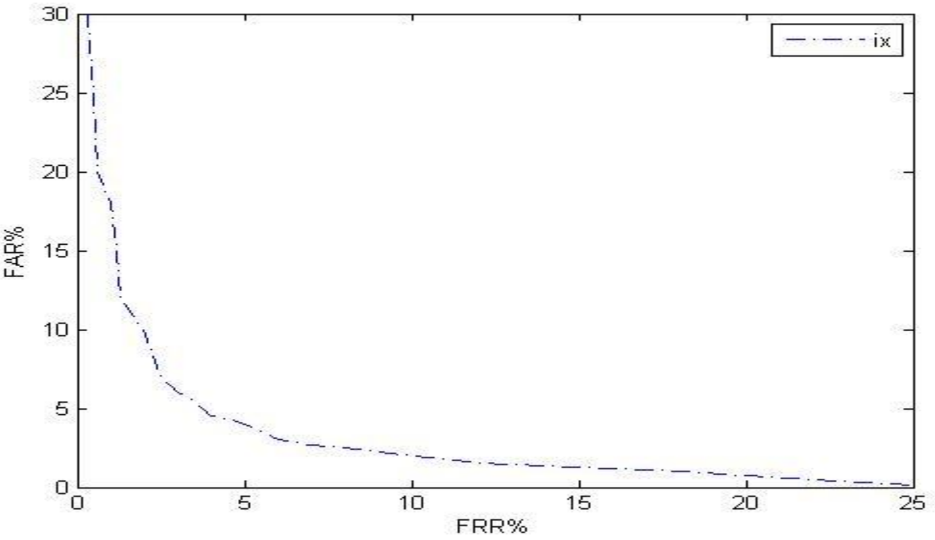


Figure 4. 5 Error tradeoff curve of x-coordinate(ix).

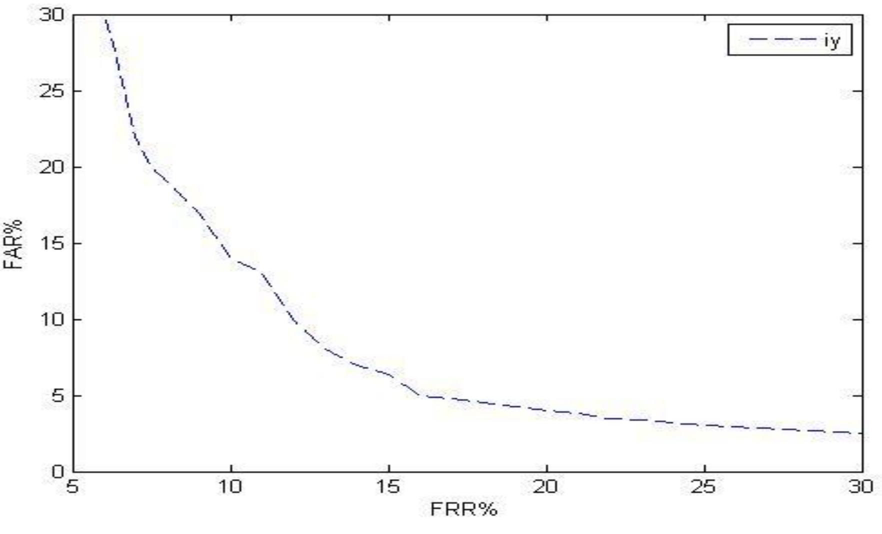


Figure 4. 6 Error trade off curve of y-coordinate (iy).

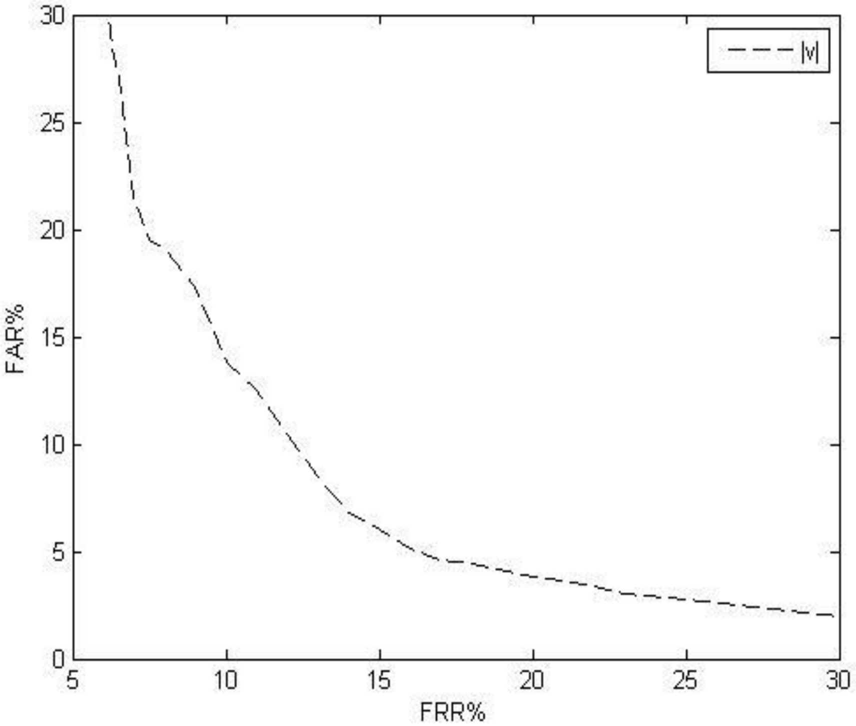


Figure 4. 7 Error tradeoff curve of velocity (|v|).

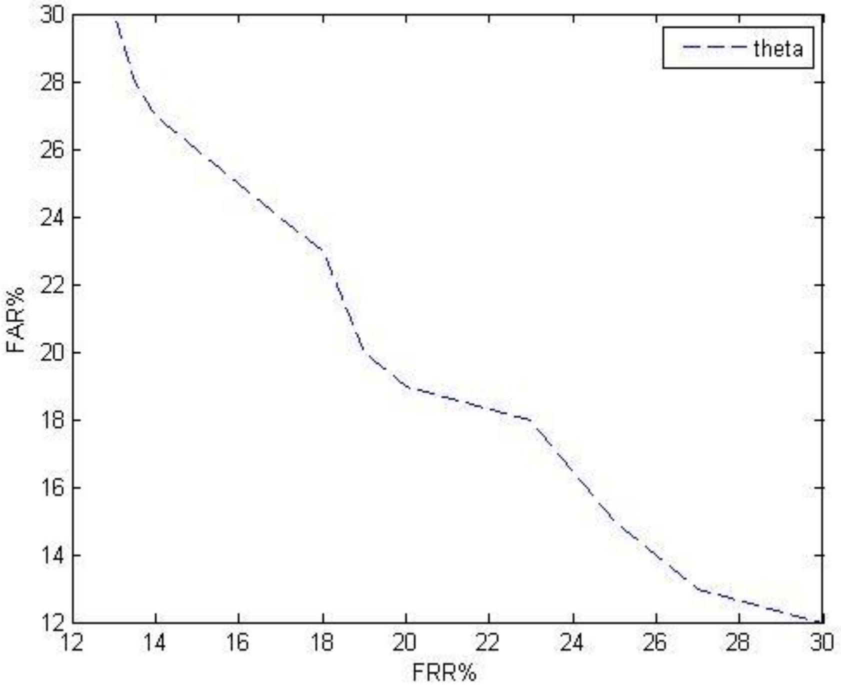


Figure 4. 8 Error tradeoff curve of angle (θ).

When feature iy was taken into consideration, in front cam was the best, because feature iy in the images from front cam is consistent with the y-coordinate information in real space. However, the performance for iy from front cam is worst than that for ix from left hand cam because of compression.

Features	Left hand cam(EER)	In front cam(EER)
ix	0.259	2.0
iy	10.3	7.0
v	3.2	13.5
θ	0.2	0.11

Table 5. 1EER (Equal Error Rate)

The pen tip movement along optical axis of both cameras were compressed. Therefore, it is observed that the features related to the vertical movement in real space are much more compressed by front camera and are less compressed by left hand cam.

Chapter 5

5. Conclusion and Future work

We analyzed online signature verification by tracking the pen tip. The system does not need any special hardware like tablet, unlike fingerprint verification or iris scanning systems. It requires only low cost webcams. We evaluated the best placement for webcams. It was confirmed that the webcam should be placed to the side of the hand for best results.

The data base used for the verification was not large. Thus, this technique should be verified with large data base.

It is observed that several cases where the system lost its track of the pen tip when the user wrote with an extremely fast stroke and the images of the pen tip were blurred at that time. This problem can be solved by an approach that finds blurred images by using sequential marginal likelihood with sequential Monte Carlo marginalization, and re-estimates the pen tip positions.

Only the local features were considered for verification and evaluated independently. Combining these features with global can improve the accuracy. Global features also can be extracted from the signatures obtained by using a camera. Combining the local features and global features can improve the accuracy.

Another interesting future work will be to incorporate a multimodal technique combining other biometric data acquired from webcams or combing the signature data obtained from cameras placed at different positions.

References

[1]. D.Muramatsu, M. Kondo, M. Sasaki, S. Tachibana, and T. Matsumoto. “A markov chain monte carlo algorithm for bayesian dynamic signature verification”. *IEEE Transactionson Information Forensics and Security*, 1(1):22–34, March,2006.

[2]. K. Yasuda, D. Muramatsu, and T. Matsumoto, “Visual-based online signature verification by pen tip tracking”, *Proc. CIMCA 2008, 2008, pp. 175–180.*

[3]. Satoshi Shirato, D. Muramatsu, and T. Matsumoto, “camera-based online signature verification: Effects of camera positions.” *World Automation congress2010 TSI press.*

[4]. D. Muramatsu, K. Yasuda, S. Shirato, and T. Matsumoto. “Visual-based online signature verification using features extracted from video”, *Journal of Network and Computer Applications Volume 33, Issue 3, May 2010, Pages 333-341.*

[5]. R. Plamondon and G. Lorette. Automatic signature verification and writer identification - the state of the art. *Pattern Recognition, 22(2):107–131, 1989.*

[6]. M. E. Munich and P. Perona. “Visual identification by signature tracking.” *IEEE Trans. Pattern Analysis and MachineIntelligence,* 25(2):200–217, February 2003.

[7]. F.A.Afsar, M. Arif and U. Farrukh, “Wavelet Transform Based Global Features for Online Signature Recognition”, Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[8]. Mohammad M. Shafiei, Hamid R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models," Seventh International Conference on Document Analysis and Recognition (ICDAR'03), vol. 1, pp. 443, 2003.

[9]. R. S. Kashi , J. Hu & W. L. Nelson, “On-line Handwritten Signature Verification using Hidden Markov Model Features”, Fourth International Conference Document Analysis and Recognition (ICDAR'97), pp. 253 – 257, 1997.

[10]. Charles E. Pippin, “Dynamic Signature Verification using Local and Global Features”, Georgia Institute of Technology, July 2004.

[11]. Hao Feng and Chan Choong Wah, “Online Signature Verification Using New Extreme Points Warping Technique”, *Pattern Recognition Letters*, vol. 24, pp. 2943-2951, Dec. 2003.

[12]. F.A. Afsar, M. Arif and U. Farrukh, “Wavelet Transform Based Global Features for Online Signature Recognition”, Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[13]. Liang Wan, Bin Wan, Zhou-Chen Lin “On-Line Signature Verification with Two-Stage Statistical Models”, Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 – 286, 2005 .

[14]. Alisher Kholmatov, “Biometric Authentication Using Online Signatures”, MS Thesis, Sabanci University, June 2002.

[15]. Chan F. Lam, David Kamins and Kuno Zimerann, “Signature Recognition through Spectral Analysis”, Pattern Recognition, vol. 22, pp.39-44, Jan.1989.

[16]. Liang Wan, Bin Wan, Zhou-Chen Lin “On-Line Signature Verification with Two-Stage Statistical Models”, Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 – 286, 2005.

[17]. Chan F. Lam, David Kamins and Kuno Zimerann, “Signature Recognition through Spectral Analysis”, Pattern Recognition, vol. 22, pp.39-44, Jan.1989.

[18]. Muhammed Nauman Sajid “Vital Sign: Personal Signature based Biometric Authentication System”,Bs degree thesis,Pakistan Institute of Engineering and Applied sciences,sept 2009.

[19]. Mario Enrique Munich “Visual Input for Pen-Based Computers” Phd thesis, California Institute of technology,Pasadena,California.