**CHAPTER 1**

**INTRODUCTION**

A signature is a special case of handwriting which includes special characters and flourishes. It is a behavioral biometric which is in control of the subject and tend to change over the short and long terms due to various factors such as health, aging and physiological state. Other traits like speaking and walking also come under behavioral biometric. Physiological biometrics on other hand mainly measures the physical features of the subject such as face, figerprint, iris, hand and finger geometry. The physical features mostly remain same unlike the behavioral characteristics. A behavioral biometric generally requires several samples due to their inherent variations. Signature variations depend on fatigue, mental and physical state, and writing position.

Signature recognition and verification is one of the important ways to identify the owner of the signature and also to find whether the signature is genuine or forged. It also holds a particular importance as it the only widely accepted method for endorsing financial transactions. It has been used for decades in civilian applications while other methods still have the stigma of being associated with criminal investigation.

The signature verification can be divided into two methods which are online (dynamic) and off-line (static) verification. In this study, we are going for off-line verification where the subject’s signature is acquired on paper and scanned where biometric system recognizes the unique features and states the genuinely of it.

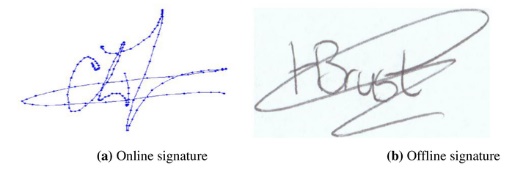
* 1. **Online Signature Recognition & Verification**

Online signature recognition and verification refers to a process where the user’s signature is acquired on a digital device. The signer uses a special pen called stylus to create their signature. Online SVRS track down path and other time-variable sequence variables using specially designed tablets or other devices during the act of signing. As Figure 1.1 shows the process where the user’s signature is acquired on a digital device.



**Figure 1.1** online signature using digital device and stylus

Automatic online SVRS is an interesting intellectual challenge with many practical applications. This technology examines the behavioral components of the signature such as: stroke order, speed, and pressure, as opposed to comparing visual images of signatures. Unlike traditional signature comparison technologies, online SVRS measures the physical activity of signing. Figure 1.2 shows the dynamic/online form of signature which is acquired on digital device by the user.



**Figure 1.2** dynamic form of signature

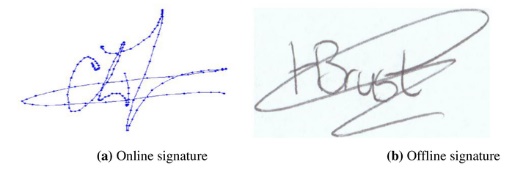
* 1. **Off-line Signature Recognition & Verification**

Off-line signature recognition and verification and recognition are concerned with the verification of signature made by a normal pen. Figure 1.3 shows the process where the user’s signature is acquired on paper using a pen.



**Figure 1.3** off-line signature using pen and paper

Off-line SVRS can be done using two different approaches. One is the writer dependent signature verification, where models for genuine and forgery signatures are constructed for each writer. Then, the test signature sample of a writer is compared to its own training sample. The second approach is as called writer-independent signature verification is used by forensic experts. This approach is considered as the most practical cases, since it is not necessary to generate a model for each writer in order to verify its signature. In this case, a general model is built from some writers chosen randomly. However, the writer-independent signature verification constitutes a more difficult task because of the important morphological variability inter-writers. Figure 1.4 shows the static/off-line form of signature which is acquired on paper using a pen by the user.



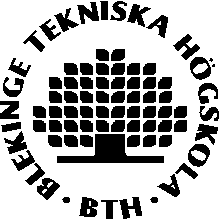
**Figure 1.4** static form of signature

**1.3 Organization of the Report**

This report starts with an overview of different ways of signature recognition and verification. We analyze the impact of different techniques and procedures to be performed on the images before comparison called preprocessing and feature extraction techniques in order to get an accurate output. The report is organized as follows:

Master Thesis

Electrical Engineering



September 2017

Online Handwritten Signature

Verification System

using Gaussian Mixture Model and Longest

Common Sub-Sequences

Shashidhar Sanda

Sravya Amirisetti

Department of Applied Signal Processing

Blekinge Institute of Technology

SE–371 79 Karlskrona, Sweden

This thesis is submitted to the Department of Applied Signal Processing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering with emphasis in Signal Processing.

Contact Information:

Author(s):

Shashidhar Sanda

E-mail: shsa16@student.bth.se

Sravya Amirisetti

E-mail: sram16@student.bth.se

Thesis Superviser:

Dr. Josef Ström Bartunek

Dept. Applied Signal Processing

E-mail:josef.strombartunek@bth.se

University Examiner:

Dr. Sven Johansson

Dept. Applied Signal Processing

E-mail:sven.johansson@bth.se

|  |  |  |  |
| --- | --- | --- | --- |
| Dept.Applied Signal Processing | Internet | : | www.bth.se |
| Blekinge Institute of Technology | Phone | : +46 455 38 50 00 | |
| SE–371 79 Karlskrona, Sweden | Fax | : | +46 455 38 50 57 |

Abstract

Nowadays, human identifications are necessary for our routine activi-ties such as entering any secure locations besides many other applica-tions. To that end, higher security levels need with easier user inter-action which can be achieved using bio-metric verification. Bio-metric verification helps us identify people based on their extracted physical or behavioural features. These features should have certain properties such as uniqueness, permanence, acceptability, collectability, and the cost to employ any bio-metric.

HSV is one of the bio-metric verification which authenticates whether the signature is genuine or forged. In our study a new approach is proposed for online signature verification using classifier model and comparing techniques. The classifier model i.e., GMM is used to ex-tract the physical and behaviour features. The comparison technique i.e., LCSS is used for comparing extracted features.

The publicly available online handwritten signature data(MCYT-100 database) is used for experiments. The results obtained in the form of performance metric curves called FAR, FAR, EER, ROC curves.

To know the performance of the verification system, it is compared with the widely used comparing technique called Dynamic Time Warp-ing. Our experiments show that GMM with the LCSS authenticate persons very reliably and with a performance better and matching with best comparing technique, DTW.

Keywords: Signature Verification,GMM, LCSS, DTW, FAR, FRR, EER, ROC Curves.

Acknowledgments

Firstly, we would like to express my sincere gratitude to our su-pervisor Dr. Josef Ström Bartůněk for the continuous support of our master thesis study and related research, for his patience, motivation, and immense knowledge. His guidance helped us in all the time of re-search and writing of this thesis. we could not have imagined having a better advisor and mentor for our thesis study.

Besides our supervisor, we would like to thank our thesis examiner Dr. Sven Johansson for his insightful comments and encouragement. We would like to express our deepest gratitude to the Department of Applied signal processing for helping us throughout the research.

Last but not the least, I would like to thank our friends, our family: our parents and to our brothers and sister for supporting us spiritually throughout writing this thesis and our life in general.

ii

Contents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Abstract | | |  | i |
| Acknowledgments | | | | ii |
| 1 | Introduction | | | 1 |
|  | 1.1 | Motivation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 1 |
|  | 1.2 | Problem Statement . . . . . . . . . . . . . . . . . . . . . . . . . . | | 1 |
|  | 1.3 | Problem Solution . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 2 |
|  | 1.4 | Aim and Objectives . . . . . . . . . . . . . . . . . . . . . . . . . . | | 3 |
|  | 1.5 | Research Questions . . . . . . . . . . . . . . . . . . . . . . . . . . | | 3 |
|  | 1.6 | Outline of Thesis . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 4 |
| 2 | Literature Study | | | 5 |
| 3 | Background | | | 7 |
|  | 3.1 | Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 7 |
|  | 3.2 | Signature Database . . . . . . . . . . . . . . . . . . . . . . . . . . | | 9 |
|  | 3.3 | Preprocessing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 9 |
|  | 3.4 | Feature Extraction . . . . . . . . . . . . . . . . . . . . . . . . . . | | 10 |
|  | 3.5 | Verification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 11 |
| 4 | Proposed Method | | | 12 |
|  | 4.1 | Pre-processing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 12 |
|  | 4.2 | Feature Extraction . . . . . . . . . . . . . . . . . . . . . . . . . . | | 12 |
|  |  | 4.2.1 | First order di erence of basic features . . . . . . . . . . . . | 14 |
|  |  | 4.2.2 | Second order di erence of spatial co-ordinates . . . . . . . | 14 |
|  |  | 4.2.3 | Sine and Cosine Measures . . . . . . . . . . . . . . . . . . | 15 |
|  |  | 4.2.4 | Length based features . . . . . . . . . . . . . . . . . . . . | 15 |
|  | 4.3 | GMM ................................. | | 15 |
|  |  | 4.3.1 | Maximum Likelihood Parameter Estimation . . . . . . . . | 16 |
|  |  | 4.3.2 | EM Algorithm . . . . . . . . . . . . . . . . . . . . . . . . . | 16 |
|  | 4.4 | LCSS.................................. | | 18 |
|  |  | 4.4.1 | Basic Similarity Measure for Time Series . . . . . . . . . . | 18 |
|  |  | 4.4.2 | Multivariate Time Series . . . . . . . . . . . . . . . . . . . | 18 |

iii

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4.5 | DTW ................................. | | 19 |
|  | 4.6 | LCSS vs DTW . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 20 |
| 5 | Performance Evaluation | | | 22 |
|  | 5.1 | Setup of the Evaluation . . . . . . . . . . . . . . . . . . . . . . . | | 22 |
|  | 5.2 | Performance Evaluation Factors . . . . . . . . . . . . . . . . . . . | | 24 |
| 6 | Results and Discussion | | | 27 |
|  | 6.1 | Results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 27 |
|  |  | 6.1.1 | FAR and FRR . . . . . . . . . . . . . . . . . . . . . . . . | 27 |
|  |  | 6.1.2 | EER Curves . . . . . . . . . . . . . . . . . . . . . . . . . . | 29 |
|  |  | 6.1.3 | ROC Curve . . . . . . . . . . . . . . . . . . . . . . . . . . | 31 |
|  | 6.2 | Discussion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 32 |
|  |  | 6.2.1 | Answers to Research Questions . . . . . . . . . . . . . . . | 32 |
|  |  | 6.2.2 | Problems faced during implementation . . . . . . . . . . . | 33 |
| 7 Conclusion and Future Work | | | | 34 |
|  | 7.1 | Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 34 |
|  | 7.2 | Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 34 |
| References | | |  | 36 |

iv

List of Figures

|  |  |  |
| --- | --- | --- |
| 1.1 | Typical Signature Verification System . . . . . . . . . . . . . . . . | 2 |
| 3.1 | Module of Signature Verification System . . . . . . . . . . . . . . | 8 |
| 4.1 | Block diagram of implementation of online signature verification |  |
|  | system . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 13 |
| 4.2 | Basic features (a) Before Normalization, (b) After Normalization . | 13 |
| 4.3 | Example of how two sequences are compared using LCSS . . . . . | 19 |
| 4.4 | Example of how comparison takes place in DTW and LCSS. . . . | 21 |
| 5.1 | a) Genuine signature b) Features of Genuine signature c) Forgery |  |
|  | signature d) Features of Forgery signature. These signatures are |  |
|  | from MCYT-100 signature database. . . . . . . . . . . . . . . . . | 23 |
| 5.2 | FAR and FRR of a bio-metric verification system . . . . . . . . . | 25 |
| 5.3 | ROC Curve created by plotting the TPR against the FPR at var- |  |
|  | ious threshold settings . . . . . . . . . . . . . . . . . . . . . . . . | 26 |
| 6.1 | Plot showing FAR curves for both combinations GMM-LCSS and |  |
|  | GMM-DTW.............................. | 29 |
| 6.2 | Plot showing FRR curves for both combinations GMM-LCSS and |  |
|  | GMM-DTW.............................. | 29 |
| 6.3 | Plot showing FAR and FRR curves for combination GMM-LCSS . | 30 |
| 6.4 | Plot showing FAR and FRR curves for combination GMM-DTW . | 30 |
| 6.5 | Plot showing ROC curve for combination GMM-LCSS . . . . . . | 31 |
| 6.6 | Plot showing ROC curve for combination GMM-DTW . . . . . . | 31 |
| 6.7 | Plot showing the comparison of ROC curves for both combinations |  |
|  | GMM-LCSS and GMM-DTW . . . . . . . . . . . . . . . . . . . . | 32 |

v

List of Tables

3.1 List of Common Features . . . . . . . . . . . . . . . . . . . . . . . 10

6.1 Table showing FAR percentage values for di erent thresholds for both combinations GMM-LCSS and GMM-DTW . . . . . . . . . 28

6.2 Table showing FRR percentage values for di erent thresholds for both combinations GMM-LCSS and GMM-DTW . . . . . . . . . 28

vi

List of Abbreviations

DT W Dynamic Time Warping

EER Equal Error Rate

EM Expectation Maximization

F AR False Acceptance Rate

F F T Fast Fourier Transform

F N False Negative

F P False Positive

F P R False Positive Rate

F RR False Rejection Rate

GM M Gaussian Mixture Model

HM M Hidden Markov Model

HSV Handwritten Signature Verification

LCSS Longest Common Sub-Sequence

M AP Maximum A Posteriori

M CY T Ministerio de Cienia y Tecnologia

M LE Maximum Likelihood Estimation

M LP Multi Layer Perceptron

N N Neural Networks

ROC Receiver Operation Characteristics

SV M Support Vector Machine

T N True Negative

vii

T P True Positive

T P R True Positive Rate

U BM Universal Background Model

viii

Chapter 1

Introduction

1.1 Motivation

Signature is the most socially and legally accepted means for person authenti-cation and is therefore a modality confronted with high level attacks. Signa-ture verification plays an important role in identification of forgery signature and bio-metric application. Bio-metrics measures individuals unique physical or be-havioral characteristics with the aim of recognizing or authenticating identity. Physical characteristics in a bio-metric attribute include iris, hand geometry, face and fingerprints. Among these iris and fingerprints do not change over time and thus have very small intra-class variation, they require special and relatively ex-pensive hardware to capture the bio-metric image. Behavioral characteristics in a bio-metric attribute include signature, voice, keystroke pattern, and gait [1]. The most developed characteristics among these are the signature and voice technolo-gies.

Handwritten signature is a well know bio-metric attribute. An important advan-tage of hand written signature over other identification verification technologies is that it can only be applied when the person is conscious and willing to write unlike the finger print technology where it can be taken when the person is un-conscious also [2]. HSV is classified into two types online and o ine. O ine signature verification includes a document where the signature is present, it is scanned to obtain digitalized image representation. Online signature verification uses a special hardware, such as a digitalized tablet or a pressure sensitive pen. The shape and the dynamics of writing are captured in the online signature ver-ification [3].

1.2 Problem Statement

Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addi-tion to its shape. Dynamic features include the number and order of the strokes,

1

|  |  |
| --- | --- |
| Chapter 1. Introduction | 2 |

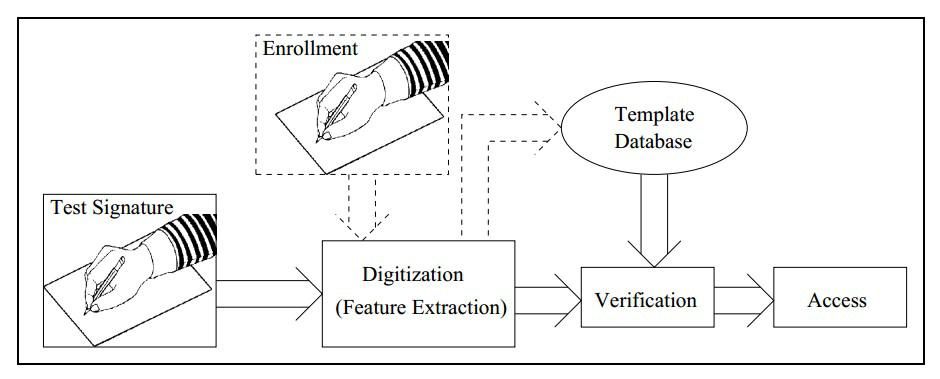


Figure 1.1: Typical Signature Verification System

the overall speed of the signature, the pen pressure at each point, etc. and make the signature more unique and more di cult to forge [4].

In an online signature verification system figure 1.1, the users are first enrolled by providing signature samples (reference signatures). When a user presents a signa-ture (test signature) claiming to be an individual, this test signature is compared with the reference signatures for that individual. If the dissimilarity is above a certain threshold, the user is rejected. During verification, the test signature is compared to all the signatures in the reference set, resulting in several distance values [5]. One must choose a method to combine these distance values into a single value representing the dissimilarity of the test signature to the reference set, and compare it to a threshold to decide. The single dissimilarity value can be obtained from the minimum, maximum or the average of all the distance val-ues. Typically, a verification system chooses one of these and discards the others. In evaluating the performance of a signature verification system, there are two important factors: the FRR of genuine signatures and the FAR of forgery signa-tures. As these two errors are inversely related, th EER where FAR equals FRR is often reported [6].

1.3 Problem Solution

To determine whether signature is genuine or forgery a new approach is proposed in dealing with the online signature verification a combination of two methods GMM and LCSS using publicly available signature database i.e., MCYT-100. Firstly, the signature is normalized and the parameters of the GMM are esti-mated by the Maximum Likelihood method. The Maximum likelihood method

|  |  |
| --- | --- |
| Chapter 1. Introduction | 3 |

estimation technique finds the parameters that maximize the joint likelihood of the data which are supposed to be independent and identically distributed. In the Gaussian mixture, it captures the underlying statistical variability’s of the point based features, being used for describing the online trace of the signatures. Then LCSS detection algorithm which measures the similarity of signature time series. A threshold value is set and a decision is made comparing the test signa-ture values with the database signature values whether the signature is genuine or forgery. To evaluate LCSS performance, it is compared with the most widely used technique called DTW.

1.4 Aim and Objectives

The aim of this thesis is to propose an approach for verification of online Hand-written signatures.

1. Collecting online handwritten signature via a digital tablet or pen based input device can provide very useful dynamic features such as writing speed, pen orientation and pressure in addition static shape information.
2. Deriving set of features from model based classifier i.e., GMM.
3. Measuring the similarity of signature using LCSS Algorithm.
4. Determining FAR, FRR, ERR and ROC curves to know the performance of signature verification.
5. Evaluation of performance by comparing it with most widely used technique called DTW.

1.5 Research Questions

The following are the research questions:

1. What are the former methods used for online handwritten signature verifi-cation?
2. How LCSS algorithm is better when compared to other matching algo-rithms?
3. How many genuine signatures are needed to train a reliable GMM-LCSS classifier?
4. Can LCSS be used in combination with other classification models?

|  |  |
| --- | --- |
| Chapter 1. Introduction | 4 |

1.6 Outline of Thesis

Chapter 1: Here we discuss the main aim for this thesis, motivation, problem statement, aims and objectives, research questions, outline of thesis.

Chapter 2: In this chapter we discuss on the literature study

Chapter 3: In this chapter the background knowledge for good understand-ing of the thesis is defined in detail step by step.

Chapter 4: In this chapter the proposed methodology is explained in detailed.

Chapter 5: In this chapter the performance evaluation factors are explained in detail.

Chapter 6: In this chapter the results obtained and answers to the research questions are discussed in detail.

Chapter 7: In this chapter conclusion and future scope are discussed.

Chapter 2

Literature Study

There are several surveys conducted on the handwritten signature verification systems and the methodologies used. Several approaches have been recently proposed and lot of research has been carried out for both feature extraction and classification using HMM, SVM, FFT, MLP wavelets and NN [4][5]. Several matching strategies employed in signature analysis are holistic matching, regional matching and multiple regional matching. Some of the most di use techniques re-ported are Euclidean distance, Elastic matching, regional correlation, tree match-ing,relaxation matching, split and merge, string matching, NN, HMM, SVM [2]

1. The issues and challenges faced by signature verification system are discussed in the survey reports [1] [3].

Hansheng Lei, Venu Govindaraju conducted a comparative study of features which are commonly used. Generalizing the existing feature-based measure a consistency model is developed to measure the distances-based measure. Experi-mental results shown that the simple features like X -, Y - coordinates, the speed of writing and the angle with the X -axis are among the most consistent and it was found that uniformly re-sampling the sequences does not necessarily increase verification performance [2].

Dr.Maged M.M.Fahmy presented a online handwritten signature verification sys-tem based on discrete wavelet transforms(DWT) features extraction and feed forward back error neural network classification [7]. To enhance the di erence between a genuine signature and its forgery, the signature is verified in DWT domain. A multi-matcher consists of six neural networks which use multiple rep-resentations and matching for the same input bio-metric signal is used to verify signature. The recognition rate for each of these neural network recognizers is discussed and a comparison of those rates is performed. Experiments are carried on signature database for five users each of 20 genuine and 20 skilled forgery signatures. Recognition success rate for genuine signatures obtained is 95%.

5

|  |  |
| --- | --- |
| Chapter 2. Literature Study | 6 |

Christian Gruber, Thiemo Gruber, Sebastian Krinninger proposed a new method to verify online signature verification with support vector machines based on LCSS kernel function [8]. Here the similarities of the two time series are de-termined by the length of an LCSS using a kernel function. This new technique shown that the SVM LCSS, can authenticate persons very reliably if only six gen-uine signatures are used for training. It turned out that the LCSS-based similarity assessment of online signature data is even superior to DTW-based techniques [9].

Abhishek Sharma and Suresh Sundaram has proposed a new model based ap-proach, GMM into the DTW framework to verify the online signatures [10]. Firstly, they extracted the writer dependent statistical characteristics for sig-nature matching. Then the characteristics of a warping path is being analyzed using a derivation in warping path based feature which is useful for verification. Later a fusion of the proposed warping path based feature with the normalize DTW score for enhancing the verification performance of DTW based system is done. This new model based method has been demonstrated successfully on the signature data from the available MCYT data base and is the first one that uses the features derived from a GMM in a DTW matching algorithm for improved verification of online signatures [11] [12].

Gabriel [13] proposed the problem of training on-line signature verification sys-tems when the number of training samples is small, where the number of avail-able signatures per user is limited. Nine di erent classification strategies based on GMM, and the UBM are evaluated. These models are designed to work under small-sample size conditions and tested using three di erent experiments. The performance of these methods degraded faster when the training set included less than 50% of the samples (around 12 signatures per user). The decision was made by estimating the likelihood ratio and comparing it with respect to the EER deci-sion threshold. The accuracy obtained by the GMM-SVM models, is considerable better than the GMM-UBM models when the available training subset is at least 50% of the whole database.

Beatrice drott and Thomas Hassan-Reza proposed an approach where classifi-cation of forgery and genuine signature is done by binary classification first by simple engineered features, then by machine learning techniques as logistic re-gression, MLP and finally by a deep learning approach with a convolutional neu-ral network. The deep learning approach on the signature verification problem showed promising results but there is still need for improvement [14].

Chapter 3

Background

In this chapter, the detailed background about signature verification is discussed.

The module of signature verification system is shown in figure 3.1.

3.1 Introduction

Online hand written signature verification is a process of testing whether a signa-ture is genuine or forgery. A signature can easily be forged. Forgeries of signatures are classified into three types: simple, random and skilled forgery [15] [16].

Random Forgery: It is produced by the forger without knowing the writers name as well as genuine signature.

Simple Forgery: In which the forger has no idea what the signature to be forged looks like. This is the easiest type of forgery to detect because it is usu-ally not close to the appearance of a genuine signature. This type of forgery will sometimes allow an examiner to identify who made the forgery based on the handwriting habits that are present in the forged signature.

Skilled forgery: In which the forger has a sample of the signature to be forged. The quality of a simulation depends on how much the forger practices before at-tempting the actual forgery, the ability of the forger, and the forger’s attention to detail in simulating the signature. A skilled forgery looks more like the genuine signature. The problem of signature verification becomes more and more di -cult when passing from simple to skilled forgery. Currently, there is a growing demand for the processing of individual identification to be faster and more accu-rate, therefore the design of a signature verification system becomes an important challenge.

7

|  |  |
| --- | --- |
| Chapter 3. Background | 8 |

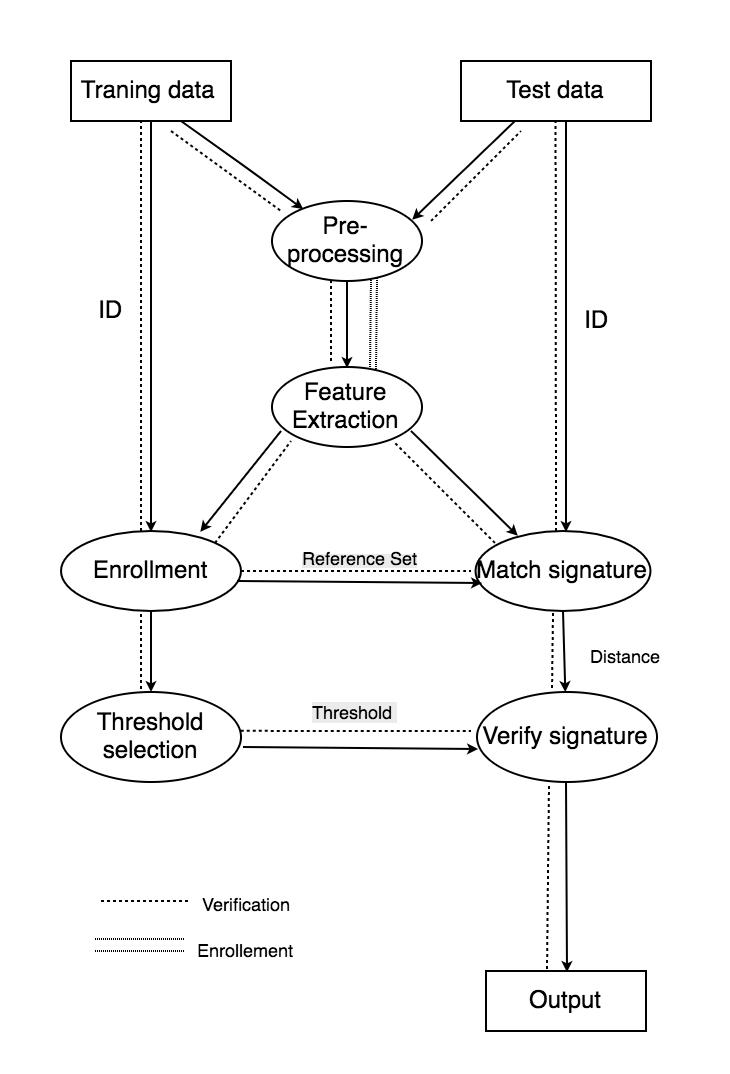


Figure 3.1: Module of Signature Verification System

|  |  |
| --- | --- |
| Chapter 3. Background | 9 |

3.2 Signature Database

The Biometric Research Laboratory, ATVS, of the Universidad Politécnica de Madrid, has promoted the plan of action and the development of the MCYT project, in which the design and acquisition of a large-scale bio-metric bi-modal database, involving fingerprint and signature traits, has been accomplished [17]. Although there are some other commercial and forensic partners within. In the case of the MCYT Signature sub corpus, 25 client signatures and 25 highly skilled forgeries (with natural dynamics) are obtained for everyone. Both on-line infor-mation (pen trajectory, pen pressure and pen azimuth=altitude) and o -line

3.3 Preprocessing

Preprocessing of online signatures is commonly done to remove variations that are thought to be irrelevant to the verification performance. Re-sampling, size, and rotation normalization are among the common preprocessing steps. In the preprocessing phase, the signature is undergone some enhancement process for extracting features. The signature images require some manipulation before the application of any recognition technique. This process prepares the image and improves its quality to eliminate irrelevant information and to enhance the selec-tion of the important features for

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chapter 3. Background | | |  |  | 10 | | | | | |
|  |  | Table 3.1: List of Common Features | | | | | | | | |
|  |  | List of Common Features | | |  |  |  |  |  |  |
|  | S.No: | Description |  |  |  |  |  |  |  |  |
|  | 1 | Coordinate x(t) | | |  |  |  |  |  |  |
|  | 2 | Coordinate y(t) | | |  |  |  |  |  |  |
|  | 3 | Pressure p(t) |  |  |  |  |  |  |  |  |
|  | 4 | Time stamp |  |  |  |  |  |  |  |  |
|  | 5 | Absolute Position, r(t)= |  | x2(t) + y2(t) | | | | | |  |
|  | 6 | Velocity in x νpx(t) | | |  |  |  |  |  |  |
|  | 7 | Velocity in y νy(t) | | |  |  |  |  |  |  |
|  | 8 | Absolute Velocity v(t)= | νx2(t) + νy2(t) | | | | | | |  |
|  | 9 | Velocity of r(t)qr( | | | ) | |  |  |  |  |
|  |  | ν |  | t |  |  |  |  |  |  |
|  | 10 | Acceleration in x ax(t) | | | | | | | |  |
|  | 11 | Acceleration in y ay(t) | | | | | | | |  |
|  | 12 | Absolute Acceleration, a(t)= p | | | | x2(t) + y2(t) | | |  |  |

3.4 Feature Extraction

Signature verification techniques employ various specifications of a signature. Se-lecting the features that are to be extracted has an enormous e ect on the ac-curacy of the signature verification system. It is also the most di cult phase of signature verification system due to the di erent shapes of

Parameter Function based approach

Signature verification systems di er both in their feature selection and their de-cision methodologies. Features can be classified in two types: global and local.

|  |  |
| --- | --- |
| Chapter 3. Background | 11 |

Global features are features related to the signature for instance the average sign-ing speed, the signature bounding box, and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajec-tory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory. Most commonly used online signature acquisition devices are pressure sensitive tablets capable of measuring forces exerted at the pen-tip, in addition to the coordinates of the pen. The pressure information at each point along the signature trajectory is another example of commonly used local feature. In some of these features are compared to find the more robust ones for signature verification purposes. Other systems have used genetic algorithms to find the most useful features [2][15][16]

Function Feature based approach

In Function feature based approach the signature is characterized in terms of a time function whose values constitute the feature set, such as position, velocity, pressure, etc.

3.5 Verification

After applying the feature extraction process the test signature and the reference signature are compared with the minimum of the dissimilarities values,Average of all the dissimilarities and the maximum of all the dissimilarities. Choosing any of the above dissimilarity values the a decision is made whether it is a forgery signature or a genuine signature . this comparison is done using a threshold value for all the reference and test signature. if the value is approximately equal to the reference signal value then it is assumed to be a genuine signature and if the dissimilarities is above that threshold value the signature is rejected. This threshold value is can be identical to all the signature or it can also be di erent

Writer dependent threshold

In this type of threshold the writer is limited to a single person. The data for this threshold should be larger compared to the regular data. Here in this type of threshold selection the writer modifies the value every time after each enrollment.

Chapter 4

Proposed Method

This chapter deals with proposed method for signature verification. The proce-dure of implementation of online handwritten signature is based on GMM, LCSS, DTW is shown in the figure 4.1.

4.1 Pre-processing

The data must be pre-processed before it is analyzed. In data pre-processing we normalize the data using normalization technique. So, what is normalization?, we

Min-Max Normalization

In our case, min-max normalization is used to normalize each of the basic feature data to the range [0,1]. Basic features before normalization and after normaliza-tion is shown in figure 4.2. The formulae that is used for min-max normalization is

|  |  |  |  |
| --- | --- | --- | --- |
| z = | x − min(x) | (4.1) |  |
| max(x) − min(x) |  |
|  |  |  |

where, x is the data vector, min(x) is the minimum of x, max(x) is the maximum of x.

4.2 Feature Extraction

Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of complex data one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and compu-tation power, also it may cause a classification algorithm to over fit to training samples and generalize poorly to new samples. Feature extraction is a general

12

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 13 |

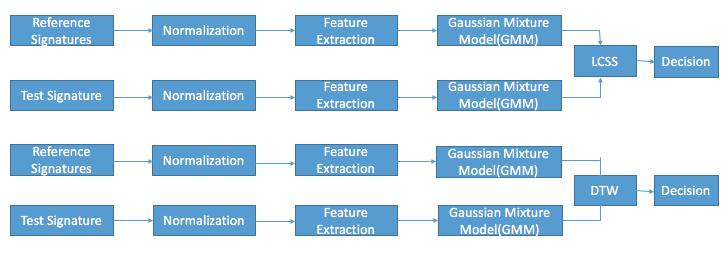
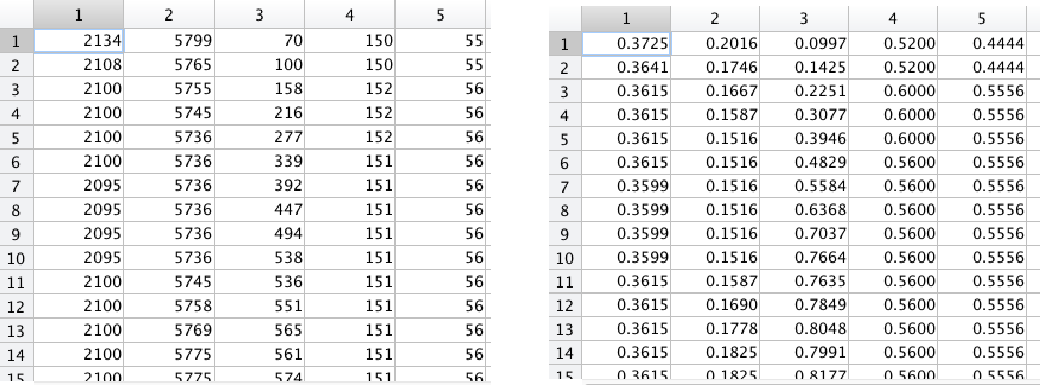


Figure 4.1: Block diagram of implementation of online signature verification sys-tem



(a) (b)

Figure 4.2: Basic features (a) Before Normalization, (b) After Normalization

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 14 |

term for methods of constructing combinations of the variables to get around these problems while still describing the data with su cient accuracy[10]. In feature extraction module, a set of eleven features are extracted from the basic features which are normalized to range [0,1].

4.2.1 First order di erence of basic features

The most common way to remove non-stationarity is to di erence the time series. The first order di erence of a time series is the series of changes from one period to the next. If x(t) denotes the value of the time series(basic feature) x at period t,

Δx(t) = x(t) − x(t − 1),

Δy(t) = y(t) − y(t − 1),

Δz(t) = z(t) − z(t − 1), (4.2)

Δφ(t) = φ(t) − φ(t − 1),

Δθ(t) = θ(t) − θ(t − 1).

The first order di erence is defined, for t=1,2,........,n-1.

4.2.2 Second order di erence of spatial co-ordinates

Sometimes, first order di erencing doesn’t eliminate all non-stationarity, so a di erencing must be performed on the di erenced series. This is called

Δ2x(t) = Δx(t) − Δx(t − 1),

(4.3)

Δ2y(t) = Δy(t) − Δy(t − 1).

The second order di erence of spatial co-ordinates is defined, for t=1,2,........,n-2.

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 15 |

4.2.3 Sine and Cosine Measures

A time series can be viewed as sum of variety of cyclic components. These cyclic components are characterized using there wavelengths as expressed via

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| cos(α(t)) = (Δx(t))/p |  |  |  | (4.4) |  |
| ((Δx(t))2 | + (Δy(t))2). | |  |
| sin(α(t)) = (Δy(t))/ | ((Δx(t))2 | + (Δy(t))2), | |  |  |

p

Sine and Cosine measures of the angle α computed with respect to horizontal axis, defined for t=1,2,...,n-1.

4.2.4 Length based features

The length of the signature l(t) is the square root of sum of squares of first order di erence of spatial co-ordinates i.e., x and y co-ordinates. The change in length Δl(t) is the square root of sum of squares of second order di erence of spatial co-ordinates is calculated as

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | |  |  |  |  |  |
| l(t) = (Δx(t)2 + Δy(t2)), | | | | | (4.5) |  |
| p |  |  |  |  |  |
| Δl(t) = (Δ2x(t)2 + Δ2y(t2)). | | | | |  |  |

The length based features defined for t=1,2,....,n-1. The feature Δl(t) relates to

the change in length obtained between successive pen positions.

4.3 GMM

A GMM [18][19] is a probabilistic model that assumes all the data points are gen-erated from a mixture of a finite number of Gaussian distributions with unknown parameters. GMMs are used as a parametric model of the probability distribu-

|  |  |  |
| --- | --- | --- |
| M |  |  |
| Xi | (4.6) |  |
| p(x|λ) = ωig(x|µi, Σi) |  |
| =1 |  |  |

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 16 |

where x is a D-dimensional continuous-valued data vector(i.e., measurement or features), ωi, i=1,2,....,M, are the mixture weights and g(x|µi, Σi), i=1,2,....,M,

are the component Gaussian densities. Each component density is a D-variate Gaussian function of following

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g(x | µi, Σi) = | 1 | | | |  |  |  | exp | 1 | | (x |  | µi)T Σ−1 | (x |  | µi) |  | (4.7) |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | D | | 1 | | |  |  |  |  |  |  |
| | |  | (2π) | |  |  | |Σi| |  |  |  | {−2 | |  | − | i |  | − |  | } |  |  |
|  | 2 | 2 |  |  |  |  |  |  |

with mean vector µi and co-variance matrix Σi. The mixture weights satisfy

M

the constraint that P ωi = 1. The complete GMM is parametrized by the mean

i=1

vectors, co-variance matrices and mixture weights from all component densities. These parameters are collectively represented by the following notation

λ = {ωi, µi, Σi} i = 1, ....M. (4.8)

4.3.1 Maximum Likelihood Parameter Estimation

MLE [18][19][20] is a method of estimating the parameters of a statistical model given observations,it is used for finding the value of one or more parameters for a

|  |  |  |
| --- | --- | --- |
| =1 |  |  |

4.3.2 EM Algorithm

Unfortunately, the expression (equation 4.9) is a non-linear function of the param-eters λ and direct maximization is not possible. However, EM algorithm[20][18] is an iterative method to find Maximum Likelihood or Maximum A Posteriori estimates of parameters in statistical models, where the model depends on unob-served latent variables. The basic idea of the EM algorithm is,

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 17 |

Step2: Evaluate the initial value of the log likelihood.

Step3: Expectation Step: Evaluating the responsibilities of the current pa-rameters values

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P r(i | x | , λ) = | M | ωig(xt|µi, Σi) | . | (4.10) |  |
| | | t |  |  |  |  |

P

ωkg(xt|µk, Σk)

k=1

Step4: Maximization Step: Re-estimate the parameters using current respon-

sibilities

Mixture Weights

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | | |  |  | N | |  |
|  |  |  |  | Xt | | |  |
| ω¯i = N | | | |  |
|  | P r(i|xt, λ) | |  |
|  |  |  |  |  | =1 |  |  |
| and means | | | |  |  |  |  |
|  |  | N | |  |  |  |  |
| µ¯i = tPN | | | | | P r(i|xt, λ)xt |  |  |
|  | | =1 | | |  |

P

P r(i|xt, λ)

t=1

(4.11)

(4.12)

with variances(diagonal co-variance)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | N |  |  |  |
|  | =1 P r(i|xt, λ)(xt − µ¯i)(xt − µ¯i)T | |  |  |
| Σ¯i = | tP | N | . |  |
|  |  |

P

P r(i|xt, λ)

t=1

Step5: Evaluating Log-likelihood

|  |  |  |
| --- | --- | --- |
|  | N |  |
| lnP r(xt|µ, ω, Σ) = | Xt |  |
| ln{P r(i|xt, λ)} |  |
|  | =1 |  |

If there is no convergence obtained, return to step 2.

(4.13)

(4.14)

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 18 |

4.4 LCSS

LCSS [8][9] is an algorithm for finding the longest sub-sequence common to all sequences in a set of sequences (often just two sequences) or measuring the simi-larity of two sequences.

4.4.1 Basic Similarity Measure for Time Series

Suppose if we have two uni-variate time series (sequences) S = (s1, s2, ......, s|S|)

and T = (t1, t2, ....., t|T |) with si, tj ∈ < and lengths |S| and |T |,respectively.

Without loss of generality we assume that |S| ≤ |T |. The values within a sequence origin from equidistant points in time, which is common in many

|  |  |  |  |
| --- | --- | --- | --- |
| Sim (S, T ) = | 2.|S|.max{γ|S, T are(γ, ) − similar} | . | (4.16) |
|  | |S| + |T| | |  |

From example figure 4.3, one of the parameter value = 0.2 can be known. The length of common sequences is seven and length of shorter sequence is ten. So, from equation 4.16 the similarity score is Sim0.2(S, T ) = 2/3.

4.4.2 Multivariate Time Series

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Multivariate time series must be processed in signature verification and many | | | | | | | |  |  |  |
| other | application fields, i.e., we are given S = (s1, s2, ......, s | | | | | S | ) and T = (t1, t2, ....., t | T | ) |  |
|  | N |  |  | | | | | | | | |  |  |
| with si, tj ∈ < | |  | (N ∈ ℵ). Here, similarity of two sequences is computed in each | | | | |  |  |  |
| dimension separately and obtained results are averaged [8][9]. For each dimension | | | | | | | |  |  |  |
| n = 1, ..., N, we compute Sim (Sn, Tn) for the uni-variate sequences Sn0and Tn | | | | | | | |  |  |  |
| [8], then, | |  |  |  |  |  |  |  |  |  |
|  |  |  | 1 | | N |  |  |  |  |  |
|  |  |  | Sim (S, T ) = |  | XSim (Sn, Tn). |  | (4.17) |  |  |  |
|  |  |  | N |  |  |  |  |

n=1

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 19 |

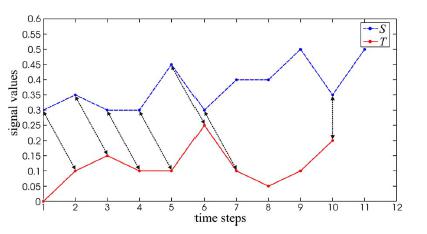


Figure 4.3: Example of how two sequences are compared using LCSS

4.5 DTW

DTW [11][12] is an algorithm for measuring similarity between two temporal sequences, which may vary in speed. For instance, similarities in walking could be detected using DTW, even if one person was walking faster than the other, or if there were accelerations and deceleration’s during the course of

|  |  |  |  |
| --- | --- | --- | --- |
|  | ψ(r, s − 1) |  |  |
|  |  |  |  |
|  | ψ(r − 1, s − 1). | (4.18) |  |
| ψ(r, s) = d(r, s) + min |  |
|  | ψ(r − 1, s) |  |  |
|  |  |  |  |

Here ψ(r, s) is the cumulative distance up to the current element.The sequence of cells in C comprise a ‘warping path’ denoted by Wp∗ . This path defines a mapping between T and S, and satisfies the constraints of boundary conditions, continuity and monotonicity. In this work, the set of cells in the warping path Wp∗ are denoted as

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Wp∗ = | { | (a1, b1), (a2, b2), ....., (alW | ∗ | , blW | ∗ | } | lW p∗ | (4.19) |  |
| i=1 |  |
|  |  | p |  | p |  |  |  |  |

|  |  |
| --- | --- |
| Chapter 4. Proposed Method | 20 |

the number of aligned pairs along the warping path Wp∗ is denoted by lW ∗p. The no-tation (ai, bi) indicates that the feature vector corresponding to atih sample

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Dsim = | | − |  | − | |  | lW p∗ |  |  | . | (4.20) |  |
|  | = iP | | d(ai, bi) | |  |
|  | ψ(nt |  | 2, ns | 2) | |  |  |  |  |  |
|  |  | =1 | |  |  |  |  |  |
|  |  | lW p∗ | |  |  |  |  | lW p∗ |  |  |  |  |

4.6 LCSS vs DTW

LCSS has some advantages over DTW. Example of DTW and LCSS is shown in figure 4.4. LCSS and DTW allows local scaling and LCSS ignores outlines.

Disadvantages of DTW

* All points are matched.
* Outliers can distort distance.
* One to many mapping.

Advantages of LCSS

* Outlying values are not matched.
* Distance/similarity distorted less.

Chapter 4. Proposed Method 21

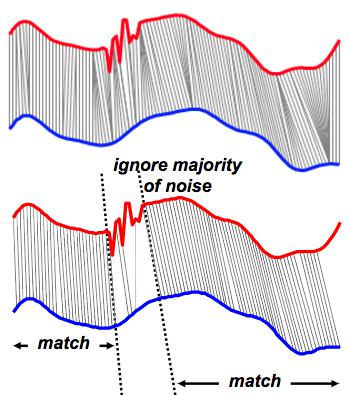


Figure 4.4: Example of how comparison takes place in DTW and LCSS.

Chapter 5

Performance Evaluation

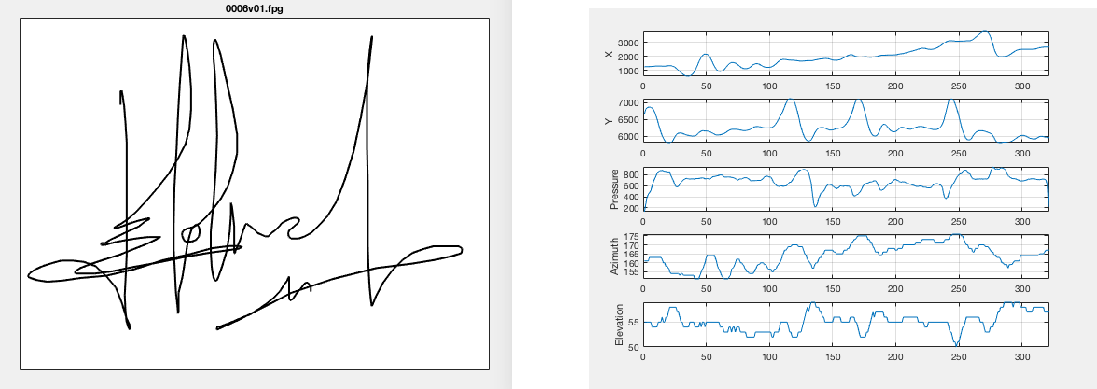
This chapter deals with the setup of the evaluation and the factors used for the evaluating performance of the signature verification system.

5.1 Setup of the Evaluation

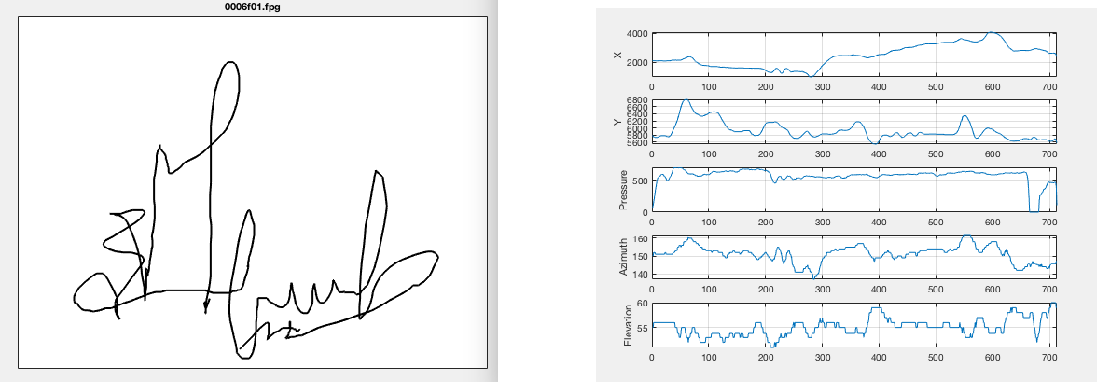
For evaluating the signature verification system a database of genuine and test signatures are required. The database of handwritten signatures are obtained

22

|  |  |
| --- | --- |
| Chapter 5. Performance Evaluation | 23 |



(a) (b)



(c) (d)

Figure 5.1: a) Genuine signature b) Features of Genuine signature c) Forgery signature d) Features of Forgery signature. These signatures are from MCYT-100 signature database.

T otal number of Genuinematching tests perf ormed

T otal number of f orgery tests perf ormed

|  |  |
| --- | --- |
| Chapter 5. Performance Evaluation | 24 |

5.2 Performance Evaluation Factors

The e ciency of a signature verification and recognition system, is expressed in terms of two error rates: the Type I error rate and Type II error rate, which are also known as the FRR and FAR respectively. The performance is also measured in terms of ERR and ROC curves. [15][16]. So, the performance is evaluated using the following factors,

* FAR
* FRR
* EER
* ROC Curve

FAR

The false accept rate is the percentage of invalid inputs that are incorrectly ac-cepted (match between input and a non-matching template),

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FAR = | T otal number of imposter signatures accepted as genuine | . | (5.1) |  |
|  |  |

|  |  |
| --- | --- |
| Chapter 5. Performance Evaluation | 25 |

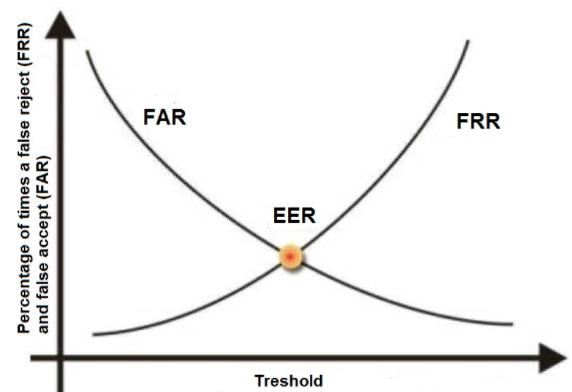


Figure 5.2: FAR and FRR of a bio-metric verification system

ROC Curve

In statistics, a receiver operating characteristic curve, i.e. ROC curve, is a graph-ical plot that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied.

The ROC curve is created by plotting the TPR against the FPR at various

|  |  |
| --- | --- |
| Chapter 5. Performance Evaluation | 26 |

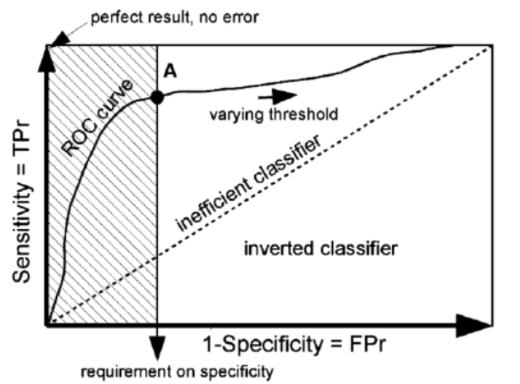


Figure 5.3: ROC Curve created by plotting the TPR against the FPR at various threshold settings

Chapter 6

Results and Discussion

This chapter deals with the results and the e ects of the results and also deals with the answers to the research questions and problem faced during the imple-mentation.

6.1 Results

The experiment is conducted on 25 genuine signatures and 25 forgery signatures with 5 genuine signatures taken as reference signatures. The performance metric curves FAR, FRR and ROC curves are shown in the below figures. There are also tables showing the FAR and FRR percentage values for

27

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 28 |

Table 6.1: Table showing FAR percentage values for di erent thresholds for both combinations GMM-LCSS and GMM-DTW

|  |  |  |
| --- | --- | --- |
| Threshold | using LCSS—>FAR | using DTW—>FAR |
| 0.1 | 0.96 | 1 |
| 0.2 | 0.96 | 1 |
| 0.3 | 0.96 | 1 |
| 0.4 | 0.96 | 0.92 |
| 0.5 | 0.96 | 0.84 |
| 0.6 | 0.68 | 0.68 |
| 0.7 | 0.4 | 0.36 |
| 0.8 | 0.32 | 0.2 |
| 0.9 | 0.04 | 0.08 |

Table 6.2: Table showing FRR percentage values for di erent thresholds for both combinations GMM-LCSS and GMM-DTW

|  |  |  |
| --- | --- | --- |
| Threshold | using LCSS—>FRR | using DTW—>FRR |
| 0.1 | 0.04 | 0.16 |
| 0.2 | 0.04 | 0.16 |
| 0.3 | 0.04 | 0.2 |
| 0.4 | 0.04 | 0.2 |
| 0.5 | 0.08 | 0.28 |
| 0.6 | 0.2 | 0.6 |
| 0.7 | 0.4 | 0.76 |
| 0.8 | 0.52 | 0.92 |
| 0.9 | 0.94 | 1 |

The figure 6.1 and figure 6.2 are FAR and FRR curve plotted for di erent threshold. The figure 6.1 showing the FAR curve for both combinations

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 29 |

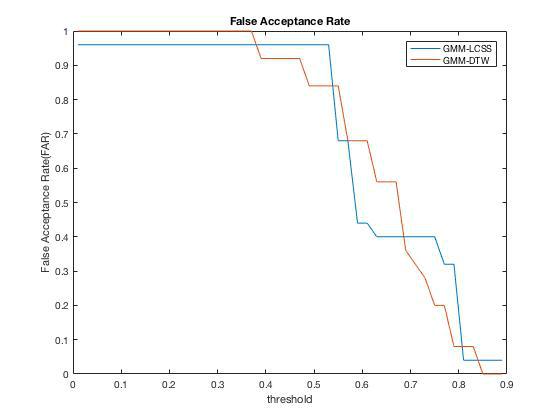


Figure 6.1: Plot showing FAR curves for both combinations GMM-LCSS and GMM-DTW

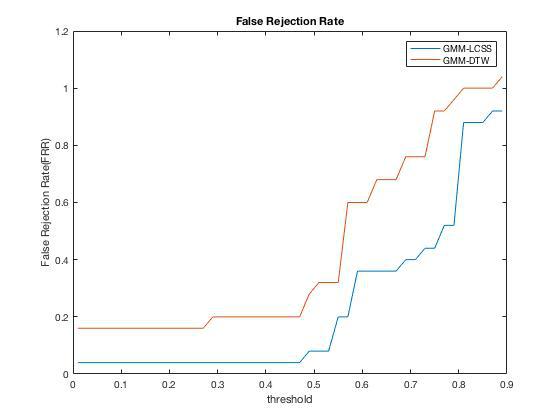


Figure 6.2: Plot showing FRR curves for both combinations GMM-LCSS and GMM-DTW

6.1.2 EER Curves

The performance of system is also evaluated using EER. EER indicates the ac-curacy of the system. A single threshold must be chosen to separate the correct user from the imposters. To know that single threshold we plot both FAR and FRR curves where both intersect at certain point which is called as EER.

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 30 |

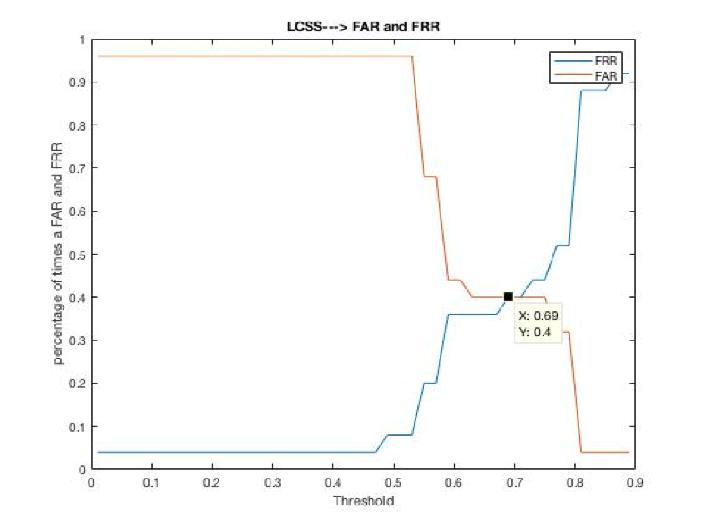


Figure 6.3: Plot showing FAR and FRR curves for combination GMM-LCSS

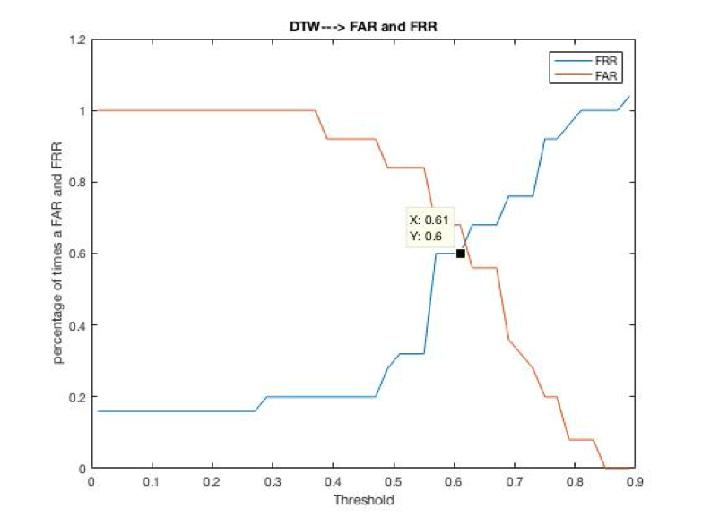


Figure 6.4: Plot showing FAR and FRR curves for combination GMM-DTW

combination GMM-DTW. from the plot the two curves intersect at 0.61 where equal error rate is 0.6.From both EER curves GMM-LCSS has low EER when compared to GMM-DTW.

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 31 |

6.1.3 ROC Curve

To know whether the classifier model is good or bad ROC curve must be created. The ROC curve is created by plotting the TPR against the FPR at various threshold setting.

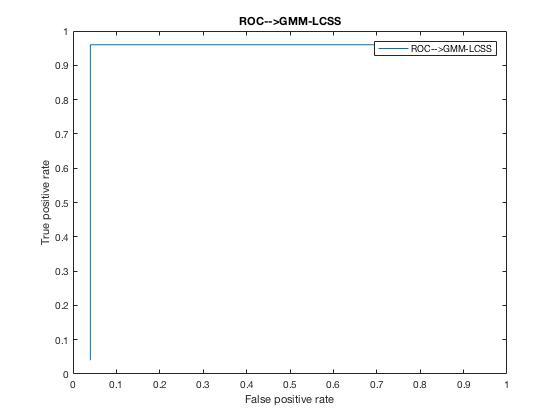


Figure 6.5: Plot showing ROC curve for combination GMM-LCSS

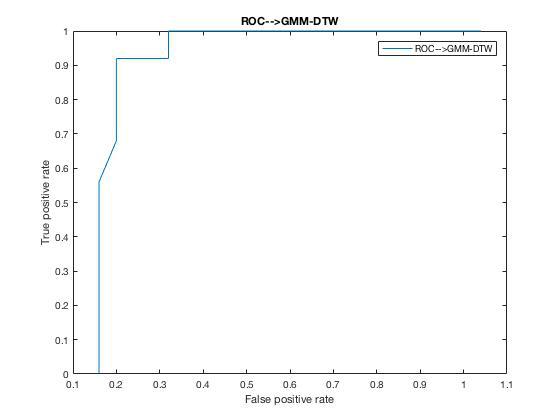


Figure 6.6: Plot showing ROC curve for combination GMM-DTW

The figure 6.5, figure 6.6, are the ROC curves obtained at various threshold levels. To judge whether the classifier model is good or bad the ROC curve must be in straight line and also without any variations.

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 32 |

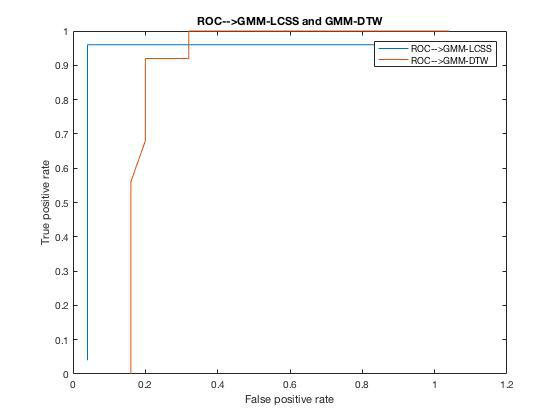


Figure 6.7: Plot showing the comparison of ROC curves for both combinations GMM-LCSS and GMM-DTW

From figure 6.7. the model GMM-LCSS has good curve compared to the model GMM-DTW because GMM-LCSS has straight curve and also the starts early when compared to GMM-DTW.

6.2 Discussion

6.2.1 Answers to Research Questions

Research Question 1: What are the former methods used for Online Signature Verification?

Answer: Many methods are proposed for signature verification since past three decades. Global features based and local features are the two strategies which are used to extract the relevant information/features from the signatures. These features are discussed in section 3.3. Model based approach and distance based approach are the classifier methodologies which are used for signature verifica-tion. In model based approach, HMM, MLP, SVM and other NN models are used to build a statistical profile of signature and evaluate the relation of the features which are used in making decision. In distance based approach, most widely used technique is DTW which aligns the sample points of two signatures having di erent lengths. Other matching algorithms include LCSS, Edit Distance and also classical distance computation techniques like Euclidean and City Block.

|  |  |
| --- | --- |
| Chapter 6. Results and Discussion | 33 |

Research Question 2: How LCSS algorithm is better when compared to DTW matching algorithm?

Answer: The results contain comparing the two classifier models GMM-LCSS and GMM-DTW. From experiments results it can be stated that LCSS algo-

6.2.2 Problems faced during implementation

During implementation of the system, to get the performance curves the system need to be tested with the available 25 genuine and 25 forgery signatures. It took hours of time to test with each test signatures and store the score values. This became a major problem. So, to solve this problem, a Matlab function is created with all the test signatures. After creating it became easy to calculate the performance curves with just one click on the run button. The work was totally implemented in Matlab R2016b software.

Another problem faced during implementation is the time taken for the executing the matlab script. Since the signature data is large and also the testing it with reference signature became a time consuming factor.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

A system for online HSV system is implemented. At various threshold values the performance of verification system is evaluated. The aim of the work is to propose a new approach for online signature verification system and also to evaluate the performance by comparing with the mostly widely used technique for comparison of two sequences i.e., DTW in the bio-metric verification. The performance of sys-tem

7.2 Future Work

The future work should address the challenges and issues involved in online sig-nature verification and there is always a scope for new approach which may im-prove the performance,the future works may involved in exploring new features and new approaches which may be more e ective in distinguishing forgeries from genuine signatures. There is a scope for reducing number of signatures required for training the model for reliable authentication. Comparison techniques LCSS and DTW can be used in combinations with other classifier models like HMM,

34

|  |  |
| --- | --- |
| Chapter 7. Conclusion and Future Work | 35 |

MLP model, SVM and other NN models. These classifier models can also be used in combination with other distance based approaches like edit distance, euclidean, city block distance computation techniques.

References

1. D. Impedovo, G. Pirlo, and R. Plamondon, “Handwritten signature verifica-tion: New advancements and open issues,” in 2012 International Conference on Frontiers in Handwriting Recognition, Sept 2012, pp. 367–372.
2. H. Lei and V. Govindaraju, “A comparative study on the consistency of fea-tures in on-line signature verification,” Pattern Recogn. Lett., vol. 26, no. 15, pp. 2483–2489, Nov. 2005.
3. F. J. Zareen and S. Jabin, “A comparative study of the recent trends in biometric signature verification,” in 2013 Sixth International Conference on Contemporary Computing (IC3), Aug 2013, pp. 354–358.
4. G. Padmajadevi and K. S. Aprameya, “A review of handwritten signature verification systems and methodologies,” in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016, pp. 3896–3901.
5. D. Morocho, J. Hernandez-Ortega, A. Morales, J. Fierrez, and J. Ortega-Garcia, “On the evaluation of human ratings for signature recognition,” in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Oct 2016, pp. 1–5.
6. R. Plamondon and S. N. Srihari, “On-line and o -line handwriting recogni-tion: A comprehensive survey,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 1, pp. 63–84, Jan. 2000.
7. M. M. Fahmy, “Online handwritten signature verification system based on dwt features extraction and neural network classification,” Ain Shams Engi-neering Journal, vol. 1, no. 1, pp. 59 – 70, 2010.
8. C. Gruber, T. Gruber, S. Krinninger, and B. Sick, “Online signature verifi-cation with support vector machines based on lcss kernel functions,” IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 40, no. 4, pp. 1088–1100, Aug 2010.

36

|  |  |
| --- | --- |
| References | 37 |

1. C. Gruber, T. Gruber, and B. Sick, Online Signature Verification with New Time Series Kernels for Support Vector Machines. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 500–508.
2. A. Sharma and S. Sundaram, “A novel online signature verification system based on gmm features in a dtw framework,” IEEE Transactions on Infor-mation Forensics and Security, vol. 12, no. 3, pp. 705–718, March 2017.
3. M. Faundez-Zanuy, “On-line signature recognition based on vq-dtw,” Pattern Recogn., vol. 40, no. 3, pp. 981–992, Mar. 2007.
4. B. Kar, P. K. Dutta, T. K. Basu, C. VielHauer, and J. Dittmann, “Dtw based verification scheme of biometric signatures,” in 2006 IEEE Interna-tional Conference on Industrial Technology, Dec 2006, pp. 381–386.
5. G. Zapata, J. D. Arias-Londoño, J. Vargas-Bonilla, and J. R. Orozco, “On-line signature verification using gaussian mixture models and small-sample learning strategies,” Revista Facultad de Ingeniería, vol. 2016, 06 2016.
6. B. Drott and T. Hassan-Reza, “On-line handwritten signature verification using machine learning techniques with a deep learning approach,” 2015, student Paper.
7. S. Z. Li, Encyclopedia of Biometrics, 1st ed. Springer Publishing Company, Incorporated, 2009.
8. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recog-nition,” IEEE Trans. Cir. and Sys. for Video Technol., vol. 14, no. 1, pp. 4–20, Jan. 2004.
9. J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. I. Moro, “Mcyt baseline corpus: a bimodal biomet-ric database,” IEE Proceedings - Vision, Image and Signal Processing, vol. 150, no. 6, pp. 395–401, Dec 2003.
10. D. A. Reynolds and R. C. Rose, “Robust text-independent speaker identifica-tion using gaussian mixture speaker models,” IEEE Transactions on Speech and Audio Processing, vol. 3, no. 1, pp. 72–83, Jan 1995.
11. D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, “Speaker verification using adapted gaussian mixture models,” Digit. Signal Process., vol. 10, no. 1, pp. 19–41, Jan. 2000.
12. A. P. Dempster, N. M. Laird, and D. B. Rubin, “Maximum likelihood from incomplete data via the em algorithm,” Journal of the Royal Statistical So-ciety, Series B, vol. 39, no. 1, pp. 1–38, 1977.

|  |  |
| --- | --- |
| References | 38 |

1. A. Fischer, M. Diaz, R. Plamondon, and M. A. Ferrer, “Robust score nor-malization for dtw-based on-line signature verification,” in 2015 13th Inter-national Conference on Document Analysis and Recognition (ICDAR), Aug 2015, pp. 241–245.