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
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Abstract

Nowadays, human identifications are necessary for our routine activities such as entering any secure locations besides many other applications. To that end, higher security levels need with easier user interaction 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 extract 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 Warping. 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 supervisor 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 research 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.

Contents

List of Figures

List of Tables

List of Abbreviations

DTW Dynamic Time Warping

EER Equal Error Rate

EM Expectation Maximization

FAR False Acceptance Rate

FFT Fast Fourier Transform

FN False Negative

FP False Positive

FPR False Positive Rate

FRR False Rejection Rate

GMM Gaussian Mixture Model

HMM Hidden Markov Model

HSV Handwritten Signature Verification

$LCSS$ Longest Common Sub-Sequence

MAP Maximum A Posteriori

$MCYT$ Ministerio de Cienia y Tecnologia

MLE Maximum Likelihood Estimation

MLP Multi Layer Perceptron

NN Neural Networks

ROC Receiver Operation Characteristics

SVM Support Vector Machine

TN True Negative

TP True Positive

TPR True Positive Rate

UBM Universal Background Model

Chapter 1

Introduction

1.1 Motivation

Signature is the most socially and legally accepted means for person authentication and is therefore a modality confronted with high level attacks. Signature verification plays an important role in identification of forgery signature and bio-metric application. Bio-metrics measures individuals unique physical or behavioral 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 expensive 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 technologies.
Handwritten signature is a well know bio-metric attribute. An important advantage 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 unconscious also [2]. HSV is classified into two types online and offline. Offline 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 verification [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 addition to its shape. Dynamic features include the number and order of the strokes,

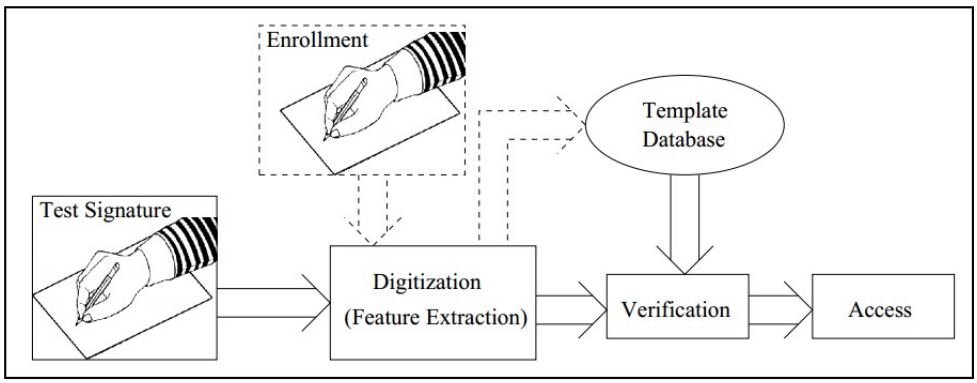


Figure 1.1: Typical Signature Verification System

the overall speed of the signature, the pen pressure at each point, etc. and make the signature more unique and more difficult 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 signature (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 values. 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 signatures. 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 estimated by the Maximum Likelihood method. The Maximum likelihood method

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 signature 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 Handwritten 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 verification?
2. How LCSS algorithm is better when compared to other matching algorithms?
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?

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 understanding 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 diffuse techniques reported are Euclidean distance, Elastic matching, regional correlation, tree matching,relaxation matching, split and merge, string matching, NN, HMM, SVM [2] [6]. 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. Experimental 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 system based on discrete wavelet transforms(DWT) features extraction and feed forward back error neural network classification [7]. To enhance the difference 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 representations 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%.

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 determined 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 genuine 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 approach, GMM into the DTW framework to verify the online signatures [10]. Firstly, they extracted the writer dependent statistical characteristics for signature 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 systems when the number of training samples is small, where the number of available signatures per user is limited. Nine different 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 different 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 decision 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 classification of forgery and genuine signature is done by binary classification first by simple engineered features, then by machine learning techniques as logistic regression, MLP and finally by a deep learning approach with a convolutional neural 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 signature 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 usually 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 attempting 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 difficult when passing from simple to skilled forgery. Currently, there is a growing demand for the processing of individual identification to be faster and more accurate, therefore the design of a signature verification system becomes an important challenge.

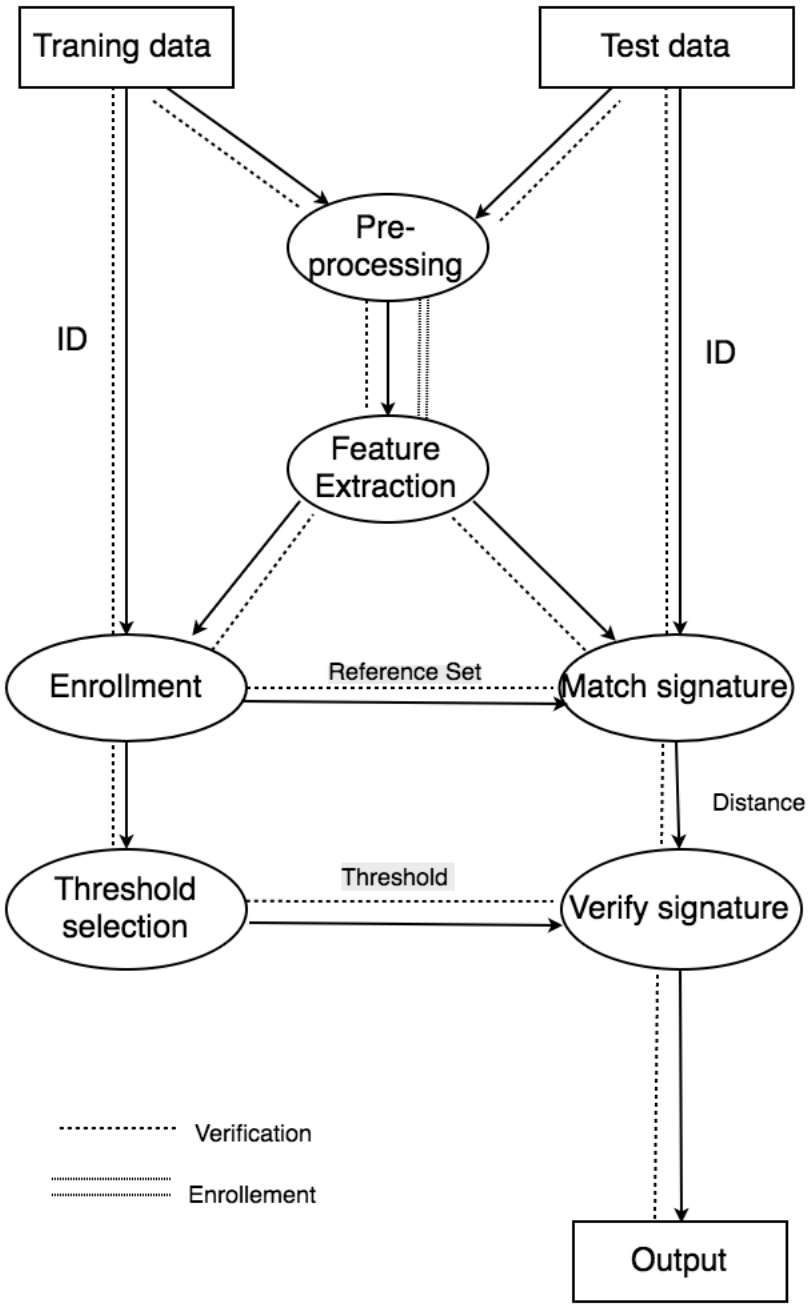


Figure 3.1: Module of Signature Verification System

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 information (pen trajectory, pen pressure and pen azimuth=altitude) and off-line information (image of the written signature) are considered in the database. Therefore, $330 \times (25 + 25) = 16500$ signature samples are considered in the MCYT baseline on-line corpus. Since the acquisition of each on-line signature is accomplished dynamically, a graphics tablet is needed: the acquisition device used is a WACOM pen tablet, model. The sampling frequency of the acquired signals is set to 100 Hz, considering the Nyquist sampling criterion, as the maximum frequencies of the underlying bio-mechanical movements are always under 2030 Hz [17].

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 selection of the important features for recognition and to improve the robustness of features to be extracted. Moreover, Preprocessing steps are performed to reduce noise in the input images, and to remove most of the variability of the handwriting [15].
For online signatures, some important preprocessing algorithms are filtering, noise reduction, and smoothing. They are also other preprocessing steps like the pen-up duration's, and drift and mean removal, time normalization and stroke concatenation before feature extraction.
To compare the spatial of a signature, time dependencies must be eliminated from the representation. Certain points in the signature such as the start points and the end points of a stroke and the points of a trajectory change, carry important information. These points are the critical points and are extracted and remained throughout the process [16].

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)=$\sqrt{x^2(t) + y^2(t)}$
6	Velocity in x $\nu_x(t)$
7	Velocity in y $\nu_y(t)$
8	Absolute Velocity v(t)=$\sqrt{\nu_x^2(t) + \nu_y^2(t)}$
9	Velocity of r(t) $\nu_r(t)$
10	Acceleration in x $a_x(t)$
11	Acceleration in y $a_y(t)$
12	Absolute Acceleration, a(t)= $\sqrt{x^2(t) + y^2(t)}$

3.4 Feature Extraction

Signature verification techniques employ various specifications of a signature. Selecting the features that are to be extracted has an enormous effect on the accuracy of the signature verification system. It is also the most difficult phase of signature verification system due to the different shapes of signatures and different situations of sampling. The feature extraction process represents a major tackle in any signature verification system. Even there is no guarantee that two genuine signatures of a person are accurately the same (intrapersonal variations). Its difficulty also stems from the fact that skilled forgeries follow the genuine pattern (interpersonal variations). This is unlike fingerprints or irises where fingerprints or irises from two different persons vary widely. Ideally interpersonal variations should be much more than the intrapersonal variations. Therefore it is very important to identify and extract those features which minimize intrapersonal variation and maximize interpersonal variations. Table 3.1 shows the list of common features. There is a lot of flexibility in the choice of features for verification of a signature extracting information from a signature is classified into two types:

1. Parameter Function based approach.

2. Function Feature based approach.

Parameter Function based approach
Signature verification systems differ both in their feature selection and their decision methodologies. Features can be classified in two types: global and local.

Global features are features related to the signature for instance the average signing speed, the signature bounding box, and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory 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 different for each of them [15][16].

Common Threshold
Common threshold is more advantageous because it has the optimal threshold for all the writers.This value is selected after computing the dissimilarities of the data signatures and a common threshold is selected based on the minimum error criterion.

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 procedure 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 often want to compare scores or sets of scores obtained on different scales. For example, how do we compare a score of 85 in a cooking contest with a score of 100 on an I.Q. test?. In order to do so, we need to "eliminate" the unit of measurement, this operation is called to normalize the data.

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 normalization is shown in figure 4.2. The formulae that is used for min-max normalization is

$$z = \frac{x - min(x)}{max(x) - min(x)} \tag{4.1}$$

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 computation 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

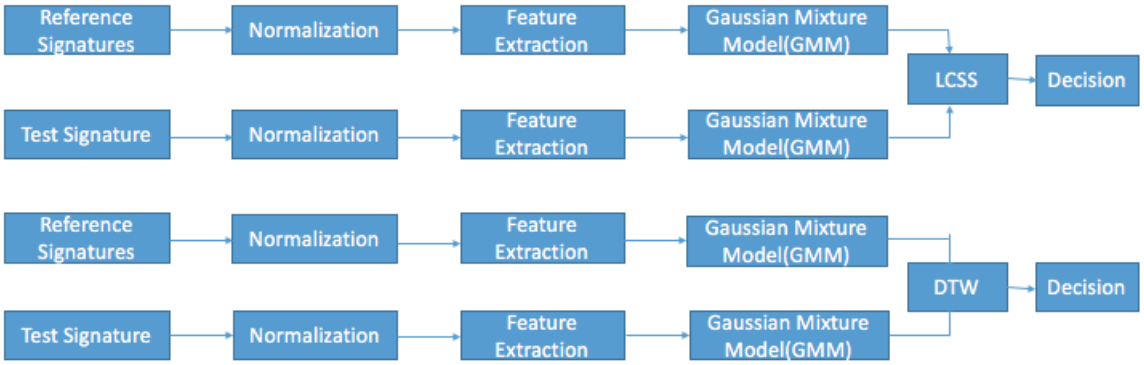


Figure 4.1: Block diagram of implementation of online signature verification system

	1	2	3	4	5
1	2134	5799	70	150	55
2	2108	5765	100	150	55
3	2100	5755	158	152	56
4	2100	5745	216	152	56
5	2100	5736	277	152	56
6	2100	5736	339	151	56
7	2095	5736	392	151	56
8	2095	5736	447	151	56
9	2095	5736	494	151	56
10	2095	5736	538	151	56
11	2100	5745	536	151	56
12	2100	5758	551	151	56
13	2100	5769	565	151	56
14	2100	5775	561	151	56
15	2100	5775	574	151	56

(a)

	1	2	3	4	5
1	0.3725	0.2016	0.0997	0.5200	0.4444
2	0.3641	0.1746	0.1425	0.5200	0.4444
3	0.3615	0.1667	0.2251	0.6000	0.5556
4	0.3615	0.1587	0.3077	0.6000	0.5556
5	0.3615	0.1516	0.3946	0.6000	0.5556
6	0.3615	0.1516	0.4829	0.5600	0.5556
7	0.3599	0.1516	0.5584	0.5600	0.5556
8	0.3599	0.1516	0.6368	0.5600	0.5556
9	0.3599	0.1516	0.7037	0.5600	0.5556
10	0.3599	0.1516	0.7664	0.5600	0.5556
11	0.3615	0.1587	0.7635	0.5600	0.5556
12	0.3615	0.1690	0.7849	0.5600	0.5556
13	0.3615	0.1778	0.8048	0.5600	0.5556
14	0.3615	0.1825	0.7991	0.5600	0.5556
15	0.3615	0.1825	0.8177	0.5600	0.5556

(b)

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

term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient 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 difference of basic features

The most common way to remove non-stationarity is to difference the time series. The first order difference 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, then the first difference of x at period t is equal to x(t)-x(t-1). In Stat-graphics, the first difference of x is expressed as DIFF(x). If the first difference of x is stationary and also completely random (not auto-correlated), then x is described by a random walk model: each value is a random step away from the previous value. If the first difference of x is stationary but not completely random–i.e., if its value at period t is auto-correlated with its value at earlier periods then a more sophisticated forecasting model such as exponential smoothing or may be appropriate. The following $\Delta x(t), \Delta y(t), \Delta z(t), \Delta\phi(t), \Delta\theta(t)$ are the first order difference of x,y,z co-ordinates, angle and azimuthal of signature data

$$\begin{aligned} \Delta x(t) &= x(t) - x(t-1), \\ \Delta y(t) &= y(t) - y(t-1), \\ \Delta z(t) &= z(t) - z(t-1), \\ \Delta\phi(t) &= \phi(t) - \phi(t-1), \\ \Delta\theta(t) &= \theta(t) - \theta(t-1). \end{aligned} \tag{4.2}$$

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

4.2.2 Second order difference of spatial co-ordinates

Sometimes, first order differencing doesn't eliminate all non-stationarity, so a differencing must be performed on the differenced series. This is called second order differencing. Differencing can go on multiple times, but very rarely does an analyst need to go beyond second order differencing to achieve stationarity. $\Delta^2 x(t), \Delta^2 y(t)$ are the second order difference of spatial co-ordinates. The formula for second order differencing is

$$\begin{aligned} \Delta^2 x(t) &= \Delta x(t) - \Delta x(t-1), \\ \Delta^2 y(t) &= \Delta y(t) - \Delta y(t-1). \end{aligned} \tag{4.3}$$

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

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 periods and frequencies. The frequency domain analysis aims to decompose original time series into its cyclic components and to compute their frequencies to study their impact on the observed data. The spectral analysis uses two periodic sinusoidal functions, sine and cosine to represent the original time series. Sine and Cosine measures are calculated as

$$\begin{aligned} \sin(\alpha(t)) &= (\Delta y(t))/\sqrt{((\Delta x(t))^2 + (\Delta y(t))^2)}, \\ \cos(\alpha(t)) &= (\Delta x(t))/\sqrt{((\Delta x(t))^2 + (\Delta y(t))^2)}. \end{aligned} \tag{4.4}$$

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 difference of spatial co-ordinates i.e., x and y co-ordinates. The change in length $\Delta l(t)$ is the square root of sum of squares of second order difference of spatial co-ordinates is calculated as

$$\begin{aligned} l(t) &= \sqrt{(\Delta x(t)^2 + \Delta y(t^2))}, \\ \Delta l(t) &= \sqrt{(\Delta^2 x(t)^2 + \Delta^2 y(t^2))}. \end{aligned} \tag{4.5}$$

The length based features defined for t=1,2,....,n-1. The feature $\Delta l(t)$ 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 generated from a mixture of a finite number of Gaussian distributions with unknown parameters. GMMs are used as a parametric model of the probability distribution of the continuous measurements or features in a bio metric system, such as vocal tract spectral features in a speaker recognition system. GMM parameters are estimated from training data using the iterative EM algorithm or Maximum Likelihood Parameter estimation from a well-trained prior model [15].
A GMM is a weighted sum of M components Gaussian densities as

$$p(x|\lambda) = \sum_{i=1}^{M} \omega_i g(x|\mu_i, \Sigma_i) \tag{4.6}$$

where x is a D-dimensional continuous-valued data vector(i.e., measurement or features), ω_i, i=1,2,....,M, are the mixture weights and $g(x|\mu_i, \Sigma_i)$, i=1,2,....,M, are the component Gaussian densities. Each component density is a D-variate Gaussian function of following

$$g(x|\mu_i, \Sigma_i) = \frac{1}{(2\pi)^{\frac{D}{2}}|\Sigma_i|^{\frac{1}{2}}} exp\{-\frac{1}{2}(x-\mu_i)^T\Sigma_i^{-1}(x-\mu_i)\} \tag{4.7}$$

with mean vector μ_i and co-variance matrix Σ_i. The mixture weights satisfy the constraint that $\sum_{i=1}^{M}\omega_i = 1$. The complete GMM is parametrized by the mean vectors, co-variance matrices and mixture weights from all component densities. These parameters are collectively represented by the following notation

$$\lambda = \{\omega_i, \mu_i, \Sigma_i\} \qquad i = 1, ...M. \tag{4.8}$$

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 given statistic which makes the known likelihood distribution a maximum. Given training vectors and a GMM configuration, we wish to estimate the parameters of the GMM,λ, which in some sense best matches the distribution of the training feature vectors.For a sequence of N training vectors $X = x_1, ...x_N$, the GMM likelihood, assuming independence between the vectors, can be written as

$$p(X|\lambda) = \prod_{t=1}^{N} p(x_t|\lambda). \tag{4.9}$$

4.3.2 EM Algorithm

Unfortunately, the expression (equation 4.9) is a non-linear function of the parameters 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 unobserved latent variables. The basic idea of the EM algorithm is, beginning with an initial model λ, to estimate a new model λ, such that $p(X|\bar{\lambda}) \geq p(X|\lambda)$. The new model then becomes the initial model for the next iteration and the process is repeated until some convergence threshold is reached. The steps involved in estimating parameters of GMM model are as follows

Step1: Initialize weights(ω), mean(μ) and co-variance(Σ) using k-means algorithm.

Step2: Evaluate the initial value of the log likelihood.

Step3: Expectation Step: Evaluating the responsibilities of the current parameters values

$$Pr(i|x_t, \lambda) = \frac{\omega_i g(x_t|\mu_i, \Sigma_i)}{\sum_{k=1}^{M} \omega_k g(x_t|\mu_k, \Sigma_k)}. \tag{4.10}$$

Step4: Maximization Step: Re-estimate the parameters using current responsibilities
Mixture Weights

$$\bar{\omega}_i = \frac{1}{N} \sum_{t=1}^{N} Pr(i|x_t, \lambda) \tag{4.11}$$

and means

$$\bar{\mu}_i = \frac{\sum_{t=1}^{N} Pr(i|x_t, \lambda) x_t}{\sum_{t=1}^{N} Pr(i|x_t, \lambda)} \tag{4.12}$$

with variances(diagonal co-variance)

$$\bar{\Sigma}_i = \frac{\sum_{t=1}^{N} Pr(i|x_t, \lambda)(x_t - \bar{\mu}_i)(x_t - \bar{\mu}_i)^T}{\sum_{t=1}^{N} Pr(i|x_t, \lambda)}. \tag{4.13}$$

Step5: Evaluating Log-likelihood

$$lnPr(x_t|\mu, \omega, \Sigma) = \sum_{t=1}^{N} ln\{Pr(i|x_t, \lambda)\} \tag{4.14}$$

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

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 similarity of two sequences.

4.4.1 Basic Similarity Measure for Time Series

Suppose if we have two uni-variate time series (sequences) $S = (s_1, s_2, ..., s_|S|)$ and $T = (t_1, t_2, ..., t_|T|)$ with $s_i, t_j \in \Re$ and lengths $|S|$ and $|T|$,respectively. Without loss of generality we assume that $|S| \leq |T|$. The values within a sequence origin from equidistant points in time, which is common in many applications. For given values of two parameters $\gamma, \epsilon \in \Re^+$ with $\gamma \leq 1$, the two sequences S and T are called (γ, ϵ)-similar. The distance measure(d) of sample points of two sequences S and T is

$$d(s_i, t_j) \leq \epsilon \tag{4.15}$$

here, d is the euclidean distance and ϵ describes the required similarity of two sequences, γ is the relative length of the so-called common sub-sequence of S and T for a given ϵ [8][9].
For a given ϵ, we need to find maximum length of common sub-sequences. The similarity can be find out by using the following equation,

$$Sim_\epsilon(S,T) = \frac{2.|S|.max\{\gamma|S, Tare(\gamma,\epsilon) - similar\}}{|S| + |T|}. \tag{4.16}$$

From example figure 4.3, one of the parameter value $\epsilon = 0.2$ 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 $Sim_{0.2}(S,T) = 2/3$.

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 $S = (s_1, s_2, ..., s_|S|)$ and $T = (t_1, t_2, ..., t_|T|)$ with $s_i, t_j \in \Re^N (N \in \aleph)$. 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 $Sim_\epsilon\ (S_n, T_n)$ for the uni-variate sequences $S_n^{'}$and T_n [8], then,

$$Sim_\epsilon(S,T) = \frac{1}{N}\sum_{n=1}^{N} Sim_\epsilon(S_n, T_n). \tag{4.17}$$

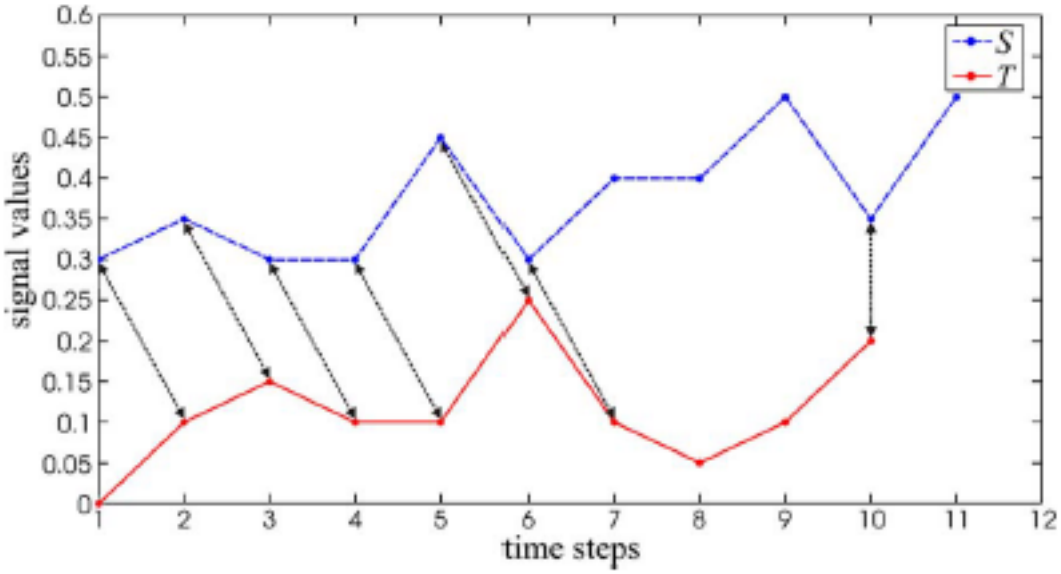


Figure 4.3: Example of how two sequences are compared using LCSS

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 an observation. DTW applications include in speech, speaker, online signature recognition and also in shaping matching.
Suppose, there are two sequences S and T of lengths n_s-2 and n_t-2 , a cost matrix C is constructed with (r,s)th element in C corresponds to dissimilarity value d(r,s) between rth point of T and sth point of S. By utilizing the elements in matrix C, we perform the following recursion to compute the DTW distance between T and S [10],

$$\psi(r,s) = d(r,s) + min \begin{cases} \psi(r,s-1) \\ \psi(r-1,s-1). \\ \psi(r-1,s) \end{cases} \tag{4.18}$$

Here $\psi(r,s)$ is the cumulative distance up to the current element.The sequence of cells in C comprise a 'warping path' denoted by W_p^* . 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 W_p^* are denoted as

$$W_p^* = \{(a_1,b_1),(a_2,b_2),.....,(\mathrm{a}_{l_{W_p^*}},\ b_{l_{W_p^*}}\}\ {}_{i=1}^{l_{W_p^*}} \tag{4.19}$$

the number of aligned pairs along the warping path W_p^* is denoted by $l_{W_p^*}$. The notation (a_i, b_i) indicates that the feature vector corresponding to a_i^{th} sample point of T is aligned to that of b_i^{th} sample point of S_p. Owing to the boundary conditions, we have $(a_1, b_1) = (1, 1)$ and $(a_{l_{W_p^*}}, b_{l_{W_p^*}})$=$(n_t - 2, n_s - 2)$. The continuity and monotonicity conditions necessitate that $a_{i-1} \leq a_i \leq a_{i-1}+1$, $b_{i-1} \leq b_i \leq b_{i-1}+1$, $1 \leq a_i \leq n_t$-2 and $1 \leq b_i \leq n_s$-2. The warping path W_p^*, at times, can give rise to one to many or many to one alignment [10][21][22]. The DTW score or similarity score is denoted as D_{sim} and it is calculated as follows

$$D_{sim} = \frac{\psi(n_t - 2, n_s - 2)}{l_{W_p^*}} = \frac{\sum_{i=1}^{l_{W_p^*}} d(a_i, b_i)}{l_{W_p^*}}. \tag{4.20}$$

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.

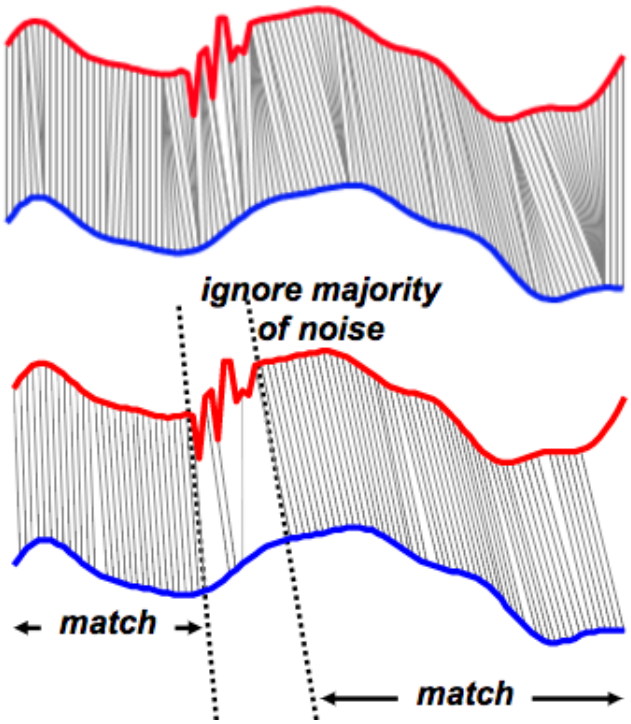


Figure 4.4: Example of how comparison takes place in DTW and LCSS.

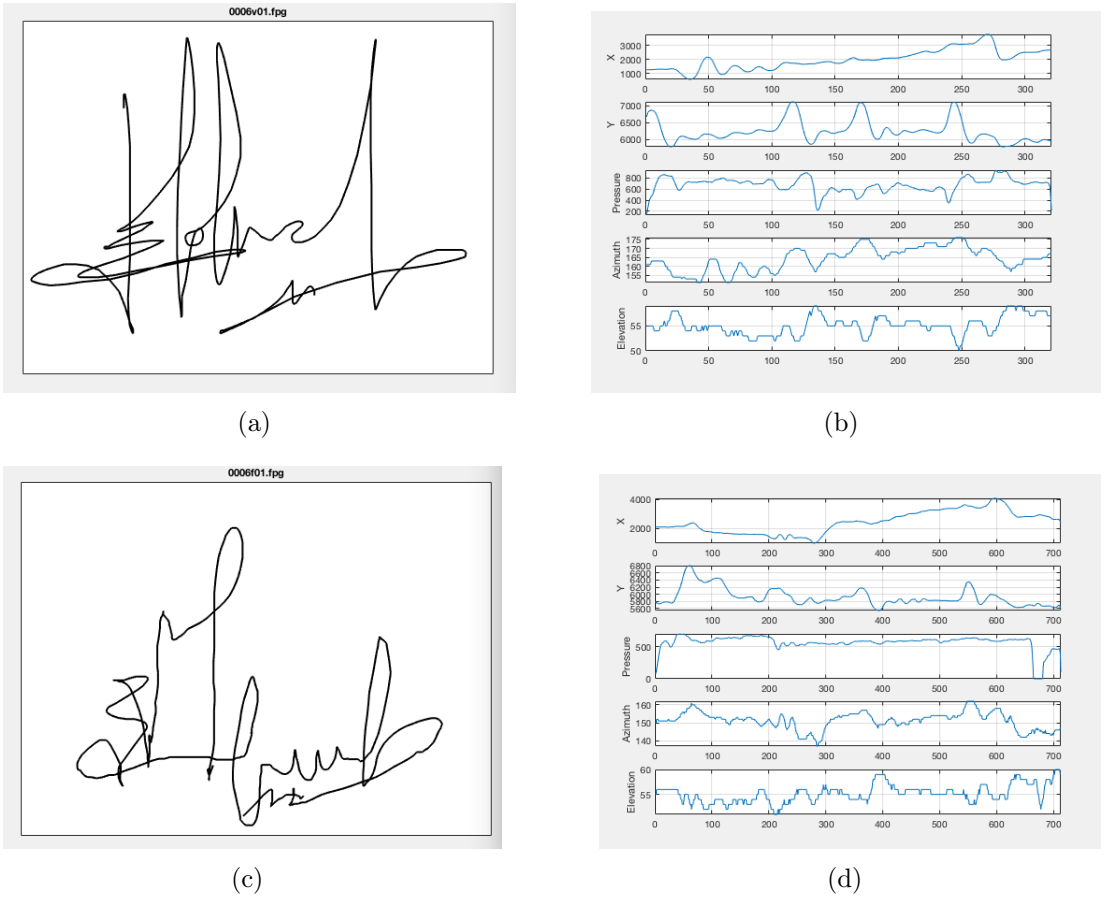
Chapter 5

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 from publicly available database called MCYT-100 from Biometric Recognition Group-ATVS. The database consists of genuine and forgery signatures of 100 users. Each target user produces 25 genuine signatures, and 25 skilled forgeries are also captured for each user. Since the acquisition of each on-line signature is accomplished dynamically, a graphics tablet is needed: the acquisition device used is a WACOM pen tablet, model INTUOS A6 USB. The genuine signatures are represented as reference signatures, how many references signatures we need will depends on the user. For test signature we can use either genuine or forgery signature. The signatures and their features are shown in the figure 5.1. figure 5.1(a) and 5.1(b) is the genuine signature and its features, figure 5.1(c) and 5.1(d) is the forgery signature and its features. After obtaining the reference and test signatures, a set of features are derived from the model based classifier i.e., GMM and similarity is measured using the LCSS and DTW. The similarity scores are used to determine whether the signature is genuine or forgery. The obtained scores are useful for evaluating the performance of the system.



(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.

5.2 Performance Evaluation Factors

The efficiency 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 accepted (match between input and a non-matching template),

$$FAR = \frac{Total\,number\,of\,imposter\,signatures\,accepted\,as\,genuine}{Total\,number\,of\,forgery\,tests\,performed}. \quad (5.1)$$

FRR
The false reject rate is the percentage of valid inputs that are incorrectly rejected (fails to detect a match between input and matching template),

$$FRR = \frac{Total\,number\,of\,genuine\,signatures\,rejected\,as\,imposters}{Total\,number\,of\,Genuinematching\,tests\,performed}. \quad (5.2)$$

EER
The EER indicates the accuracy of the system. The false accept rate and false reject rate intersect at a certain point which is called the EER (the point in which the FAR and FRR have the same value).
In theory, the correct users should always score higher than the impostors. A single threshold could then be used to separate the correct user from the impostors. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the false accept rating but increase the false reject rating.In some cases impostor patterns generate scores that are higher than the patterns from the user.For that reason that however the threshold is chosen, some classification errors occur.

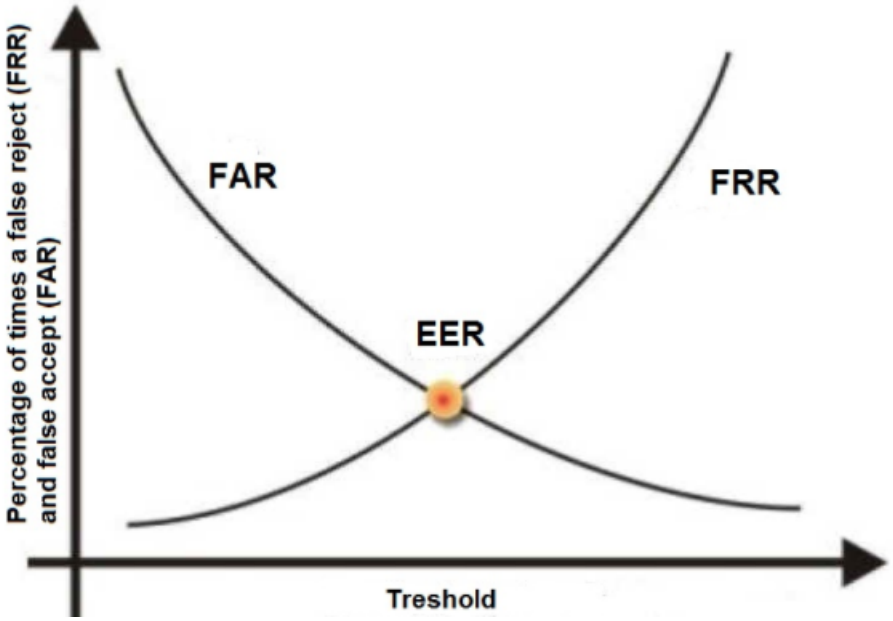


Figure 5.2: FAR and FRR of a bio-metric verification system

ROC Curve
In statistics, a receiver operating characteristic curve, i.e. ROC curve, is a graphical 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 threshold settings. Let us consider a two-class prediction problem (binary classification), in which the outcomes are labeled either as positive (p) or negative (n). There are four possible outcomes from a binary classifier. If the outcome from a prediction is p and the actual value is also p, then it is called a TP; however if the actual value is n then it is said to be a FP. Conversely, a TN has occurred when both the prediction outcome and the actual value are n, and FN is when the prediction outcome is n while the actual value is p.

ROC analysis provides tools to select possibly optimal models and to discard sub-optimal ones independently from (and prior to specifying) the cost context or the class distribution. ROC analysis is related in a direct and natural way to cost/benefit analysis of diagnostic decision making.

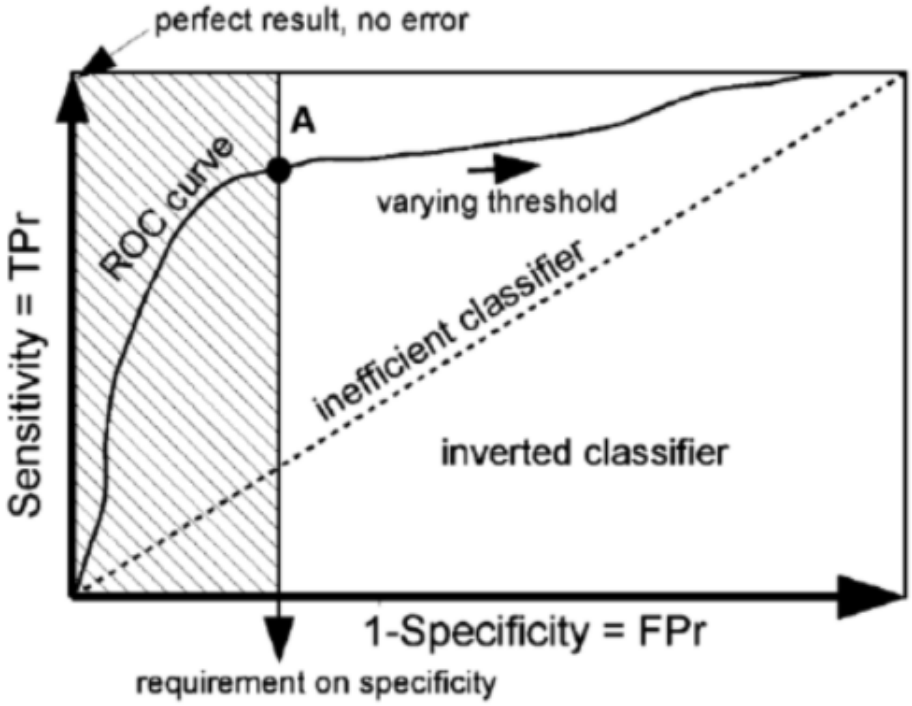


Figure 5.3: ROC Curve created by plotting the TPR against the FPR at various threshold settings

Chapter 6

Results and Discussion

This chapter deals with the results and the effects of the results and also deals with the answers to the research questions and problem faced during the implementation.

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 different threshold values for both combinations of GMM-LCSS and GMM-DTW.

6.1.1 FAR and FRR

The table 6.1 shows the false acceptance rate for both combinations of GMM-LCSS and GMM-DTW. From the table 6.1, it can be shown that percentage of false acceptance that means the system accepts signatures as genuine which actually not genuine. For this case imposter signatures i.e., forgery signatures are given as input to the system. The tables shows the percentages values for different thresholds and for both combinations percentage values are same till 0.6 threshold and after 0.6 the combination GMM-DTW achieved better results with small difference. The table 6.2 shows the FRR for both combinations of GMM-LCSS and GMM-DTW. From the table 6.2, it can be shown that percentage of false rejection that means the system rejects signatures considering not genuine which actually genuine. For this only genuine signatures are given as input to the system. The tables shows the percentages values for different thresholds and by comparing for both the combinations the combination GMM-LCSS achieved better results i.e., it has low FRR when compared to GMM-DTW.

Table 6.1: Table showing FAR percentage values for different 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 different 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 different threshold. The figure 6.1 showing the FAR curve for both combinations GMM-DTW and GMM-LCSS. The two FAR curves are nearly same with small difference.The figure 6.2 showing the FRR curve for both combinations GMM-DTW and GMM-LCSS. For combination GMM-LCSS the system obtained very good curve compared to GMM-DTW.

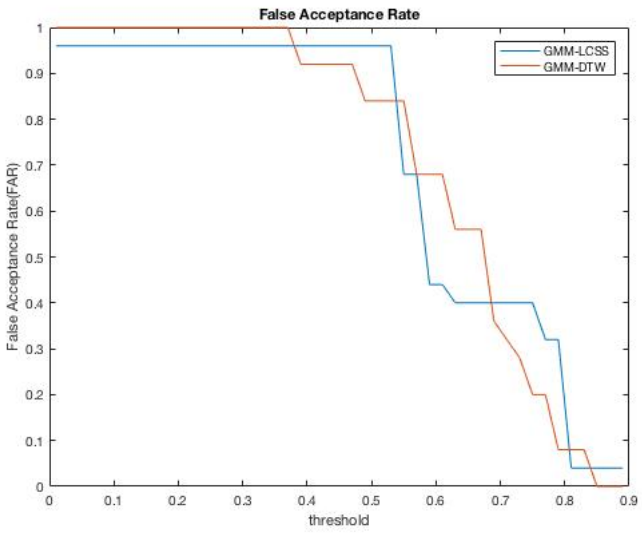


Figure 6.1: Plot showing FAR curves for both combinations GMM-LCSS and GMM-DTW

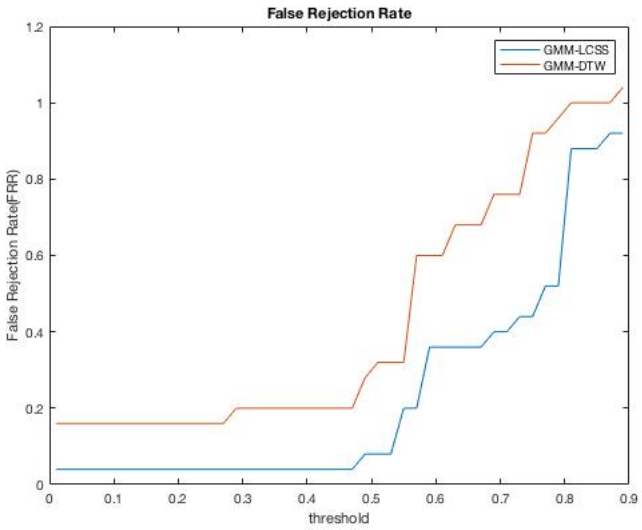


Figure 6.2: Plot showing FRR curves for both combinations GMM-LCSS and GMM-DTW

6.1.2 EER Curves

The performance of system is also evaluated using EER. EER indicates the accuracy 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.

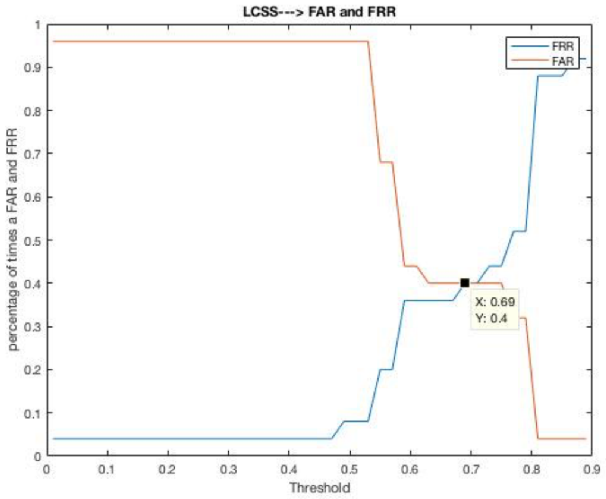


Figure 6.3: Plot showing FAR and FRR curves for combination GMM-LCSS

The figure 6.3 shows the plot for FAR and FRR curves for combination GMM-LCSS. from the plot the two curves intersect at threshold 0.69 where the equal error rate is 0.4. The figure 6.4 shows the plot for FAR and FRR curves for

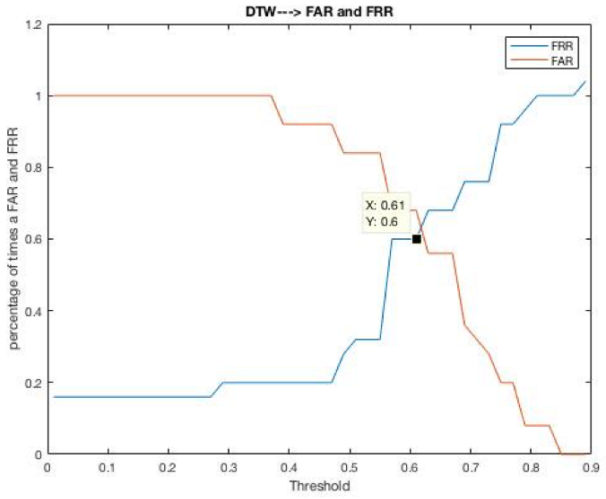


Figure 6.4: Plot showing FAR and FRR curves for combination GMM-DTW

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.

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.

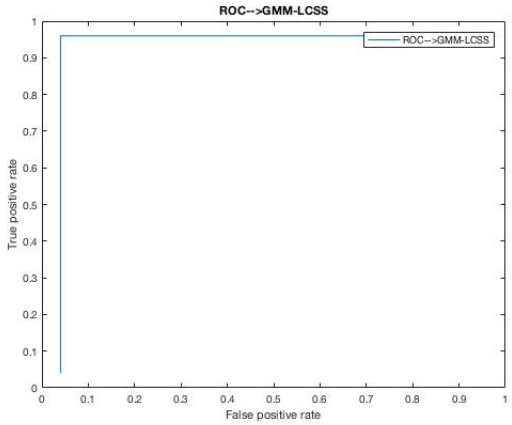


Figure 6.5: Plot showing ROC curve for combination GMM-LCSS

If the input is given a genuine signature and output obtained as positive i.e., signature is genuine, then it's called a TP. If the input is given a forgery signature and output obtained as negative i.e., signature is not genuine, then it's a FP. The example of ROC curve is shown in figure 5.3.

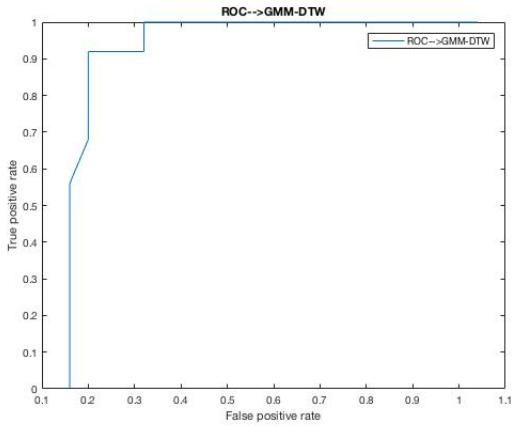


Figure 6.6: Plot showing ROC curve for combination GMM-DTW

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.

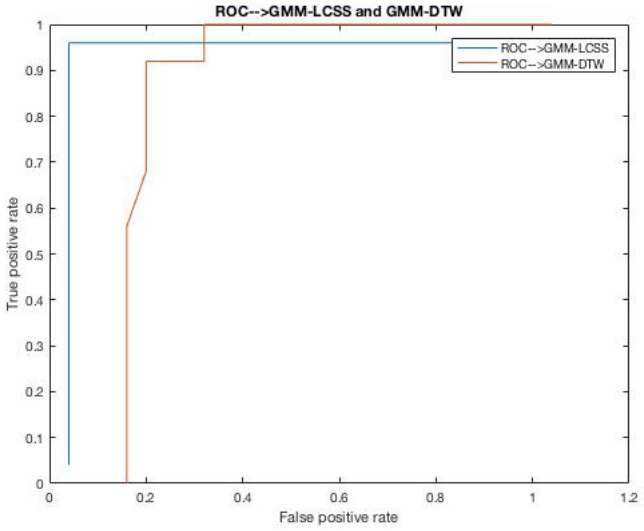


Figure 6.7: Plot showing the comparison of ROC curves for both combinations GMM-LCSS and GMM-DTW

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 verification. 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 different lengths. Other matching algorithms include LCSS, Edit Distance and also classical distance computation techniques like Euclidean and City Block.

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 algorithm is better when compared to DTW matching algorithm. All sample points are matched in DTW where the outlines can distort the distance. In case of LCSS, Outlying values are not matched so, distance/similarity is distorted less i.e., noise is cancelled. The algorithms are discussed in section 4.

Research Question 3: How many genuine signatures are needed to train a reliable GMM-LCSS classifier?
Answer: The classifier model must be trained with certain number of genuine signatures in order to have reliable verification. The number of genuine signatures necessary to train classifier is very important in real world application. Number of signatures depends on specific application, but usually number is expected to be small like starting from three and also choosing the number depends on user. For GMM-LCSS and GMM-DTW, classifier is trained using three to ten number of genuine signatures. If the classifier is trained with more signatures the better is the reliability of the verification.

Research Question 4: Can LCSS be used in combination with other classification models?
Answer: Yes, comparison techniques or distanced based approaches LCSS, DTW can used in combination with the model based approaches or classifier models like HMM, MLP, SVM and other NN models. If more features are extracted which can be separated by classifier model, if the classifier is efficient we can achieve a reliable verification.

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 system is evaluated by calculating FAR, FRR, EER and ROC curves. GMM-LCSS, is able to authenticate persons very reliably even if only five genuine signatures are used for training. It turned out that the LCSS-based similarity assessment of online signature data performance is matching with the DTW-based technique. GMM-LCSS provides more security because its FAR is low compared to GMM-DTW. Equal Error rate is low i.e., 0.4 for GMM-LCSS model when compared Equal Error rate i.e., 0.6 GMM-DTW model. From ROC curve, it is known that GMM-LCSS is efficient classifier compared to GMM-DTW.One main difference of LCSS and DTW is that in LCSS distance is less distorted because outlying values are ignored and in DTW distance is distorted because outlying values are matched. Finally, Our experiments shown that GMM with the LCSS authenticate persons very reliably and with performance better and matching with best comparing technique, DTW with small equal error rate difference.

7.2 Future Work

The future work should address the challenges and issues involved in online signature verification and there is always a scope for new approach which may improve the performance,the future works may involved in exploring new features and new approaches which may be more effective 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,

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 verification: 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 features 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 off-line handwriting recognition: 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 Engineering Journal*, vol. 1, no. 1, pp. 59 – 70, 2010.

[8] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, "Online signature verification 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.

[9] 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.

[10] A. Sharma and S. Sundaram, "A novel online signature verification system based on gmm features in a dtw framework," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 705–718, March 2017.

[11] M. Faundez-Zanuy, "On-line signature recognition based on vq-dtw," *Pattern Recogn.*, vol. 40, no. 3, pp. 981–992, Mar. 2007.

[12] B. Kar, P. K. Dutta, T. K. Basu, C. VielHauer, and J. Dittmann, "Dtw based verification scheme of biometric signatures," in *2006 IEEE International Conference on Industrial Technology*, Dec 2006, pp. 381–386.

[13] 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.

[14] B. Drott and T. Hassan-Reza, "On-line handwritten signature verification using machine learning techniques with a deep learning approach," 2015, student Paper.

[15] S. Z. Li, *Encyclopedia of Biometrics*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[16] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Cir. and Sys. for Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[17] 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 biometric database," *IEE Proceedings - Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, Dec 2003.

[18] D. A. Reynolds and R. C. Rose, "Robust text-independent speaker identification using gaussian mixture speaker models," *IEEE Transactions on Speech and Audio Processing*, vol. 3, no. 1, pp. 72–83, Jan 1995.

[19] 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.

[20] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the em algorithm," *Journal of the Royal Statistical Society, Series B*, vol. 39, no. 1, pp. 1–38, 1977.

[21] A. Fischer, M. Diaz, R. Plamondon, and M. A. Ferrer, "Robust score normalization for dtw-based on-line signature verification," in *2015 13th International Conference on Document Analysis and Recognition (ICDAR)*, Aug 2015, pp. 241–245.

[22] P. Fang, Z. Wu, F. Shen, Y. Ge, and B. Fang, *Improved DTW Algorithm for Online Signature Verification Based on Writing Forces.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 631–640.

[23] V. S. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE*, vol. 85, no. 2, pp. 215–239, Feb 1997.

[24] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, no. 12, pp. 2963 – 2972, 2002, pattern Recognition in Information Systems.

[25] O. Cigdem, T. D. Laet, and J. D. Schutter, "Classical and subsequence dynamic time warping for recognition of rigid body motion trajectories," in *2013 9th Asian Control Conference (ASCC)*, June 2013, pp. 1–6.

[26] Z. Chen, X. Xia, and F. Luan, "Automatic online signature verification based on dynamic function features," in *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Aug 2016, pp. 964–968.

[27] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 609–635, Sept 2008.

[28] J. Richiardi and A. Drygajlo, "Gaussian mixture models for on-line signature verification," in *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, ser. WBMA '03. New York, NY, USA: ACM, 2003, pp. 115–122.

[29] K. Barkoula, G. Economou, and S. Fotopoulos, "Online signature verification based on signatures turning angle representation using longest common subsequence matching," *International Journal on Document Analysis and Recognition (IJDAR)*, vol. 16, no. 3, pp. 261–272, Sep 2013.

[30] S. Garcia-Salicetti, N. Houmani, B. Ly-Van, B. Dorizzi, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, C. Vielhauer, and T. Scheidat, *Online Handwritten Signature Verification.* London: Springer London, 2009, pp. 125–165.

[31] D. S. Guru and H. N. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[32] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "Hmm-based on-line signature verification: Feature extraction and signature modeling," vol. 28, pp. 2325–2334, 12 2007.

[33] D. Cai, C. Zhang, and X. He, "Unsupervised feature selection for multi-cluster data," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '10. New York, NY, USA: ACM, 2010, pp. 333–342.

[34] J. Fierrez-Aguilar, S. Krawczyk, J. Ortega-Garcia, and A. K. Jain, *Fusion of Local and Regional Approaches for On-Line Signature Verification.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 188–196.

[35] M. Alhaddad, D. Mohamad, and A. M. Ahsan, "Online signature verification using probablistic modeling and neural network," in *2012 Spring Congress on Engineering and Technology*, May 2012, pp. 1–5.

[36] K. Wang, Y. Wang, and Z. Zhang, "On-line signature verification using graph representation," in *2011 Sixth International Conference on Image and Graphics*, Aug 2011, pp. 943–948.

[37] D. Z. Lejtman and S. E. George, "On-line handwritten signature verification using wavelets and back-propagation neural networks," in *Proceedings of Sixth International Conference on Document Analysis and Recognition*, 2001, pp. 992–996.

[38] C. Kahindo, S. Garcia-Salicetti, and N. Houmani, "A signature complexity measure to select reference signatures for online signature verification," in *2015 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Sept 2015, pp. 1–8.

[39] Y. Liu, Z. Yang, and L. Yang, "Online signature verification based on dct and sparse representation," *IEEE Transactions on Cybernetics*, vol. 45, no. 11, pp. 2498–2511, Nov 2015.

[40] C. Vivaracho-Pascual, M. Faundez-Zanuy, and J. M. Pascual, "An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances," *Pattern Recognition*, vol. 42, no. 1, pp. 183 – 193, 2009.

[41] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2400 – 2408, 2005.

[42] A. Schlapbach, M. Liwicki, and H. Bunke, "A writer identification system for on-line whiteboard data," *Pattern Recognition*, vol. 41, no. 7, pp. 2381 – 2397, 2008.

[43] A. Kholmatov and B. Yanikoglu, *Biometric Authentication Using Online Signatures*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 373–380.