Novel strategies for online signature verification using Dynamic Time Warping

A THESIS

submitted for the award of the degree of

DOCTOR OF PHILOSOPHY

By

Abhishek Sharma

DEPARTMENT OF ELECTRONICS AND ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781 039, INDIA

July 2017

To

My guide **Dr. Suresh Sundaram**

for his guidance and inspiration

&

My **parents**

for their blessings, love and support

Certificate

This is to certify that the thesis entitled "**Novel strategies for online signature verification using Dynamic Time Warping**", submitted by **Abhishek Sharma**, a research scholar in the *Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati*, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by him under my supervision and guidance. The thesis has fulfilled all requirements as per the regulations of the institute and has reached the standard needed for submission. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Dated:

Guwahati.

Dr. Suresh Sundaram
Assistant Professor
Dept. of Electronics and Electrical Engg.
Indian Institute of Technology Guwahati
Guwahati - 781 039, Assam, India.

Acknowledgements

I would like to express my whole hearted and deep sense of gratitude to my guide Dr. Suresh Sundaram for his guidance, help and encouragement throughout my research work. I am greatly inspired by his attitude towards research, creative thinking, hard work and dedication in work. I am highly grateful to him for patiently checking all my manuscripts and thesis. This thesis would not have been possible without his bounteous effort.

I also owe my profound gratitude to doctoral committee members Prof. S. R. M. Prasanna, Dr. Prithwijit Guha and Prof. Rohit Sinha for their support in all respects. Special thanks also goes to Prof. P. K. Bora and Prof. Vijaya Saradhi for clarifying many of the concepts during my Comprehensive Examination. I would like to acknowledge faculty members and the office staffs of the Department of Electronics and Electrical Engineering, IIT Guwahati, for their help in carrying out this research work. I am thankful to Rajesh, Suman, Subhashish, Balaji, Ramesh and Rohan for their comradeship and for being there during both the highs and lows.

Finally, I attribute this achievement to my guide for his constant support and constructive criticism for my success and moreover, making me stand in this position.

Abhishek Sharma

Abstract

The basic methodology in a signature verification system is to contrast features of a test signature against those from a set of enrolled genuine signatures of an user whose identity is to be authenticated. There are two possible outcomes : either the claimed signature is accepted as genuine or it is rejected as forgery. The area of on-line signature verification has caught attention among researchers in recent times. This is primarily owing to the release of devices offering a pen based interface to input handwritten data. The pen captures the trajectory information and the dynamic characteristics of the handwritten trace, such as (x, y) coordinates, pressure, azimuth, altitude, time stamp and number of contacts of pen with the surface. The input to an online signature verification system consists of a set of strokes - that are a temporal sequence of points.

In this thesis, we propose novel online signature verification systems, in line with the distance based methods. The traditional Dynamic Time Warping (DTW) algorithms for online signature employ only the scores between the test signature and the genuine enrolled signatures, in formulating the decision rule. The scores obtained correspond to the distance values / distortions, accumulated along the warping path. The warping path, as such, is generated by placing constraints on the alignments between pair of sample points of the two signatures being compared. However, at times, the sole dependence on the DTW score may not be sufficient in discriminating the forgery signatures from the genuine. This is quite likely, when the signature patterns belonging to genuine and forgery, exhibit values, that are quite close to each other. As an alleviation to this issue, we propose strategies to characterize the warping path, that in a way, provide additional cues to enhance

the verification capabilities of the DTW based system.

In the first part of the thesis, we utilize the alignment obtained from a DTW match together with another, proposed based on a measure inspired from correlation-based neighborhood matching for formulating a warping-path based score. The derived score comprises two components - feature distortion and displacement, each of which are found to empirically aid the verification step. As a second contributing chapter of the thesis, we derive a score that determines the proportion of the aligned pairs that provide a low distortion value, relative to the length of the warping path, obtained from DTW. For computing this proportion, we consider utilizing a codebook of appropriate size, built from a Vector Quantization (VQ) model. Lastly, we explore the characteristics of warping path by a combination of distance with model based approach. We encode the local features extracted at each sample of the online trace of a user's signature by a set of descriptors, that are obtained from a Gaussian Mixture Model (GMM). The resulting descriptors are then aligned using DTW and subsequently utilized for deriving the warping path score.

The work reported in this thesis is the first of its kind that uses strategies to propose interesting scores that evaluate the well-ness of the warping path associated with DTW. This score in conjunction with that of DTW is shown to give reduced error rates for online signature verification. In order to demonstrate the efficacy of our proposals, the signature verification experiments are conducted on the publicly available SVC-2004 and MCYT-100 databases with promising results to prior works.

Contents

List of Figures

List of Tables

List of Common Abbreviations

EER	Equal Error Rate
MEER	Mean Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
DET	Detection Error Trade-off
DTW	Dynamic Time Warping
VQ	Vector Quantization
GMM	Gaussian Mixture Model
BL-DTW	A DTW based verification system, wherein the alignment of signatures being compared is based on the feature set discussed in Section 3.3.
WP	A verification system that utilizes the warping path score discussed in sub-section 3.5.2.
FUS1	A verification system resulting from the fusion of the scores of *BL-DTW* and *WP*.
CTX-DTW	A DTW based verification system, that utilizes the contextual information for the matching of signatures.
FUS2	A system resulting from fusing the warping path score (derived using the *VQ* based codebook) and the *CTX-DTW*.
GMM-DTW	A DTW system that utilizes the GMM-based membership feature vectors for matching
FUS3	A system resulting from fusing the warping path score (derived using the GMM based descriptors) and the *GMM-DTW*.

HMM	Hidden Markov Model
SVM	Support Vector Machine
PCA	Principal Component Analysis
MLP	Multi Layer Perceptron
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
LCSS	Longest common subsequence

List of Symbols

$\{x(i), y(i), p(i), \phi(i), \theta(i)\}$	Attributes of (x, y) coordinate, pressure, azimuth and inclination as captured at i^{th} sample point of an online signature
N	Number of enrolled reference signatures per user
S_p	p^{th} enrolled reference signature
S_T	Test signature whose veracity is to be established.
n_p	Number of sample points in enrolled signature S_p
n_T	Number of sample points in test signature S_T
$\mathbf{f}_p^i$	Feature vector extracted at the i^{th} sample point of p^{th} reference signature
$\mathbf{f}_T^i$	Feature vector extracted at i^{th} sample point of the test signature S_T
d	Dimension of a feature vector
$\mathbf{F}_p$	Feature vector sequence for reference signature S_p
r	Spacing parameter used for feature extraction
$\{\Delta x_r(i), \Delta y_r(i), \Delta p_r(i), \Delta\phi_r(i), \Delta\theta_r(i)\}$	First order difference of attributes computed at i^{th} sample point of the trace with spacing parameter r.
$\{\Delta^2 x_r(i), \Delta^2 y_r(i)\}$	Second order difference of spatial coordinate attributes computed at i^{th} sample point of the trace with spacing parameter r.

$\alpha_r(i)$	Angle computed with respect to horizontal axis at i^{th} sample point of the trace with spacing parameter r.
$l_r(i)$	Length based feature at i^{th} sample point calculated along the trace with spacing parameter r.
$\Delta l_r(i)$	Change in length feature at i^{th} sample point calculated along the trace with spacing parameter r.
$d(m,n)$	Distance between m^{th} sample point of test signature S_T and n^{th} sample point of enrolled signature S_p
C	Cost matrix
ψ	Cumulative cost matrix
$\mathcal{W}_p^*$	Warping path obtained by DTW matching of test signature S_T with enrolled signature S_p
$l_{\mathcal{W}_p^*}$	The number of aligned pairs of sample points on $\mathcal{W}_p^*$
(a_i, b_i)	Indicates that the a_i^{th} sample point of test signature S_T is aligned to b_i^{th} sample point of an enrolled signature by using DTW
(a_i, r_i^*)	Indicates that the a_i^{th} sample point of test signature S_T is aligned to $(r_i^*)^{th}$ sample point of an enrolled signature by correlation match
$\ominus_p^*$	Set of aligned pairs obtained from the correlation based matching scheme between test signature S_T and enrolled signature S_p
W	Width of the window (of odd size $2w+1$) centred around a sample point of the trace.
d_1^p	Normalized DTW score obtained by matching the test signature S_T with enrolled signature S_p
d_2^p	Normalized warping path score obtained subsequent to the DTW match of test signature S_T and enrolled signature S_p
d_{21}^p	Normalized feature distortion component of d_2^p score obtained subsequent to the DTW match of test signature S_T and enrolled signature S_p
d_{22}^p	Normalized displacement component of d_2^p score obtained subsequent to

	the DTW match of test signature S_T and enrolled signature S_p
d_1^{mean}	Average DTW score obtained by matching the test signature S_T with the N enrolled signatures
d_2^{mean}	Average warping path score obtained by matching signature S_T with the N enrolled signatures
d_T	Fused score for verifying the authenticity of the test signature S_T
$\mathcal{O}$	Big-O notation used in mentioning the computational complexity of algorithms.
K	Code-book size
$\{\mathbf{c}_u^j\}_{j=1}^K$	Set of code vectors obtained from feature vectors of the enrolled signatures of an user u
$l_T^{a_i}$	Index of codevector assigned to a_i^{th} sample point of signature S_T
$l_p^{b_i}$	Index of codevector assigned to b_i^{th} sample point of signature S_p
$I(.)$	Indicator variable
$d_V(a_i, b_i)$	Average number of votes from the points in the neighborhood of (a_i, b_i), based on whether their feature vectors get assigned to the same code-vector
β	Weighting factor used for implementation of the *FUS2* system
M	Number of Gaussian components in GMM
$\{\pi_k, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k\}$	Mixing coefficient, mean vector and co-variance matrix of the k^{th} Gaussian component of the GMM
L	Log-likelihood score
L_{avg}	Average log-likelihood score obtained from the enrolled reference signatures of an user
D_L	Mean subtracted log-likelihood score used for verification.
n_{tr}	Number of feature vectors for learning the GMM parameters.
$g_p^i(k)$	The membership value of the feature vector $\mathbf{f}_p^i$ to the k^{th} Gaussian component

$\mathbf{g}_p^i$	GMM membership feature vector representation corresponding to the i^{th} sample point of signature S_p
$\mathcal{H}_{\mathcal{W}_p^*}$	Histogram obtained by considering the GMM descriptors along the aligned pairs of warping path $\mathcal{W}_p^*$
$\mathcal{H}_{\ominus_p^*}$	Histogram obtained by considering the GMM descriptors along the aligned pairs of $\ominus_p^*$

1

Introduction

Contents

1.1 Bio-metric Systems : an overview

In recent times, owing to security reasons, authentication of a person has become the need of the hour. The traditional means of authentication include the use of password and/or PIN number. These have a disadvantage that they can be either forgotten or stolen. Bio-metrics refers to identification of a person based on their physical or behavioral characteristics [1]. It is inherently, more reliable than traditional knowledge-based (such as a password) or token-based (such as an access card) systems. A physical or behavioral trait that has universality, distinctiveness, permanence, acceptability and accessibility (such as fingerprint, iris, voice, face to state a few) may be regarded as a candidate bio-metric for designing an automatic authentication system [2].

From the works in literature, the field of bio-metrics is categorized to one of two types, namely (i) physiological and (ii) behavioral [3]. The physiological bio-metrics employ direct measurements of a part of the human body, such as fingerprint [4], face [5], iris [6] and hand-scan [7] for identification. On the other hand, behavioral bio-metrics operate on features derived from data obtained from an action performed by the user. Examples of the same include signature [3], keystroke dynamics [8] and gait [9].

The design of a bio-metric system follows a pipeline closely related to that of a pattern recognition framework. The first step is in the capture of data from an individual, based on which his / her identity is to be established. This is followed by a suitable technique to extract discriminative or salient features from the data. Subsequent to this, the matching is performed by comparing the extracted feature sets to those stored in the database. As a final step, on the basis of the comparison, a decision is made with regards to the authenticity of the data.

In general, it is worth noting that a bio-metric system can be operated in one of the two modes, namely identification or verification. The distinguishing characteristics between them are highlighted below:

Verification: In this mode, the bio-metric system authenticates the veracity of an individual's claim by comparing the provided data with their corresponding templates stored in the database. Without loss of generality, verification systems may be regarded as a one class problem, wherein the positive samples correspond to those enrolled from the user, whose claim is to established. The decision being made at the output either confirms or denies a person's claimed identity

Identification: In this mode, the system recognizes the identity by matching the captured data to the templates of all users stored in the database. Contrary to the verification scheme, a one to many comparison is made with the use of a classifier designed in a multi-category setting.

An important consideration for the development of a biometric system is in the use of discriminative features. In particular, different samples of the same individual do exhibit variabilities of the feature set - which in the literature is referred to as 'intra-class' variation. Likewise, the variability observed between feature sets originating from two different individuals is known as 'inter-class' variation. Accordingly, an appropriate feature set, capturing the information of the biometric data is to be employed - one that provides a small intra-class but large inter-class variation.

The crux of the present dissertation, as we shall see in the subsequent Chapters, is in the exploration of strategies for authenticating the identity of the user with his / her signature. Accordingly, with the preceding succinct introduction to biometric systems, we shift our focus to the problem of signature verification in the remainder of this thesis.

1.2 Introduction to signature verification systems

Amongst the several bio-metric characteristics being explored for identity verification, the handwritten signature has been in use for quite a long time. The authentication through the medium of signature is commonly found in applications of commerce and banking transactions as well as in credit card payments. As a matter of fact, signature verification has become a well accepted biometric trait for all types of legal documents. In addition, the process of data acquisition of a signature has an advantage - in that it is considered to be non-invasive.

A handwritten signature may be regarded as a complex process - one that relies on factors such as the psychophysical state of the signer. Despite theories being suggested in the literature in [10–12] to model handwriting, signature verification till date remains an open research problem. This is primarily owing to the fact that the veracity needs to be determined by only a few available samples of the user that are enrolled to the system.

In a signature verification system, features of a test signature are contrasted against those from a set of enrolled genuine signatures of an user whose identity is to be authenticated. This leads to one of two possible outcomes : either the claimed signature is accepted as genuine or rejected as forgery. The research area of signature verification falls under the purview of handwriting analysis. Moreover, in the domain of document processing, it is classified under the 'text-dependent' writer identification framework [13].

Based on the mode of data acquisition, signature verification techniques can be categorized into one of the two systems: off-line and on-line.

Off-line verification system : In this approach, the ink of the signature from the user are captured on paper, subsequently scanned and saved as digital bit map images. The data being employed for processing contain gray-level information of the strokes corresponding to the pixels occupied by the ink. Accordingly, off-line signature verification system make use of techniques from the area of image analysis to verify the identity of the claimed person [14–16].

Online verification system : The recent trend in technology has led to the release of devices offering a pen based interface to input handwritten data. Such devices, referred to as hand-held devices are manufactured small, portable and are easy to use. They primarily utilize an electronic pen (referred to as stylus) to capture data on a pressure-sensitive screen. The pen records the trajectory information of the handwriting, such as (x, y) spatial location, pressure, azimuth, altitude, time of signing act and number of contacts of pen with the surface. In the literature, the processing of such dynamic data of signatures is referred to as 'online'.

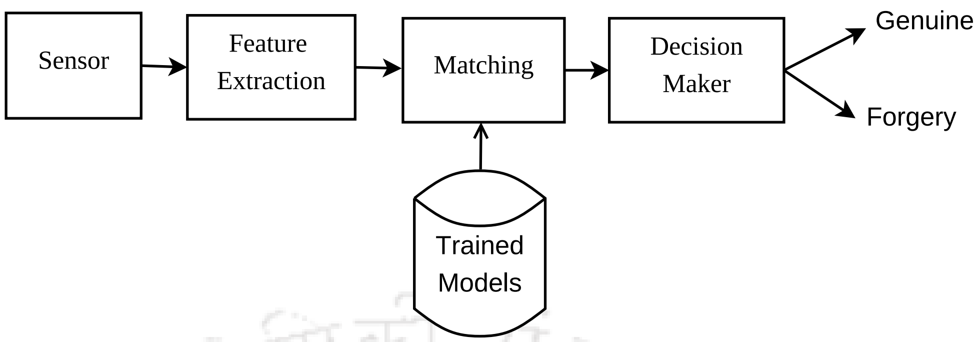


Figure 1.1: Block diagram representation of an online signature verification system.

The incorporation of dynamic features that uniquely characterize an user during the act of signing can provide additional verification mechanisms to be embedded into modern ID documents. In this regard, online signatures can be considered as a viable verification option for users of processes such as e-banking and e-commerce. It thus comes as no surprise that in recent times, these are increasingly getting more attention in e-shopping and e-delivery systems (e.g., Amazon and Flipkart) as a substitution of paper-based signatures. Moreover, with the availability of electronic signature acquisition device, the methodology of the identity verification techniques has emerged. Secondly, when a person wants to bypass a system, he / she will have to forge the signature of another person by trying to reproduce as close as possible the target signature. As such, one has to replicate more information than that provided using the static image of the signature in an off-line verification setting - thus making the process of imitation more challenging.

1.3 A schematic of an online signature verification system

Figure 1.1 illustrate a block diagram of an online signature verification system - comprising the sensor, feature extraction, matching and decision module. In the following subsections, we present a high level description of these various blocks.

1.3.1 Sensor Module

Thanks to technology, online signatures are straightforward to obtain with relatively inexpensive electronic devices the so-called 'tablets'. These devices capture the pen trace in real time by measuring many dynamic features such as pressure of a pen on the tablet surface, position of a pen, and so on. During signing, as a result of the sampling process, the continuous signature of a person is reduced to a set of discrete points.

It may be mentioned that for research explorations of verification algorithms, a number of online signature databases have been made publicly available for evaluation. The signatures have been collected with pen tablets and/or digitizing tablets [17] [18]. The dynamic information being captured for analysis include:

(i) Position in x-axis.

(ii) Position in y-axis.

(iii) Pressure applied by the pen.

(iv) Azimuth angle of the pen with respect to the tablet.

(v) Inclination of the pen with respect to the tablet.

Figure 1.2 (a) and (b) presents an illustration of an online signature from the SVC-2004 and MCYT-100 databases respectively [1], along with the dynamic information captured by the pen.

Thus, to summarize, the input to any online signature verification system comprises a set of strokes, each of which in turn are a sequence of points. A stroke starts with a pen-down movement and ends with the next pen-up movement. It is presented by its duration and a sequence of x and y coordinates, along with other dynamic information. Without loss of generality, in this thesis, we refer the dynamic information captured by the pen on the tablet as 'attributes'.

[1]The signatures from these databases will be used for the experimentations in the thesis. A detailed description of the same are provided in Section 3.2

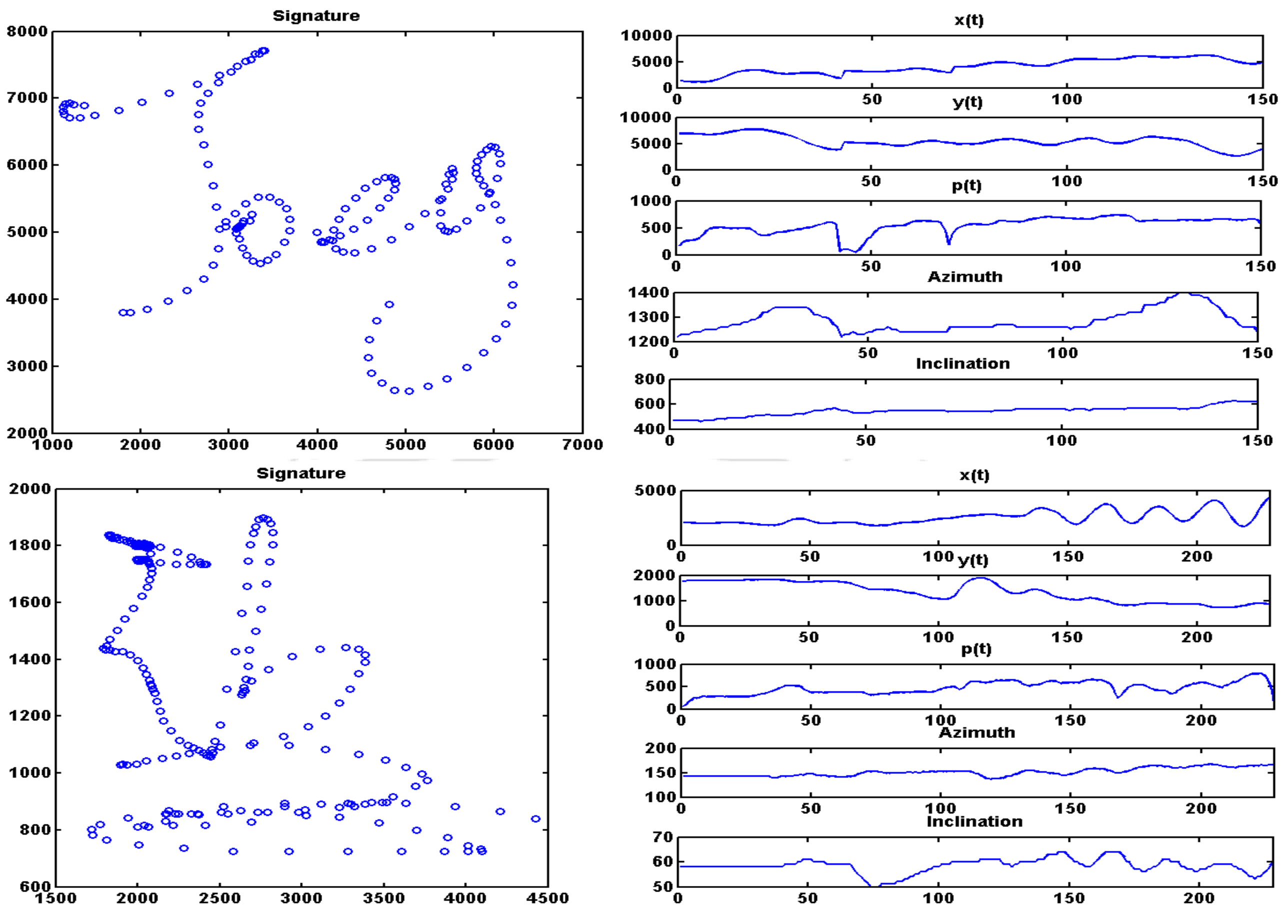


Figure 1.2: Representation of an online signature from SVC-2004 (top panel) and MCYT-100 database (bottom panel) with its dynamic information.

1.3.2 Feature Extraction Module

In this module, salient discriminatory features are extracted from the raw data / attributes obtained from the tablet. Prior to feature extraction, the data may be subjected to pre-processing to reduce the effect of sensor generated noise, pen-jitters and inconsistencies caused by variations due to size and location of the captured signatures. With regards to noise reduction, common filtering approaches include the use of the Gaussian [3] and cubic spline smoothing techniques [19,20]. In order to address the issue of location / translation invariance, a popular preprocessing step is to subtract the horizontal and vertical trajectories of the trace with respect to their corresponding centroids. Rotational invariance of signatures as such is achieved by using techniques such as PCA [19] and moment of inertia [21, 22]. Size normalization strategies are also adopted as a preprocessing step - the common ones being that of min-max [23–25] and z-score methods [26–29]. In general, the idea is to separately scale the horizontal and vertical trajectories of the signatures in a way that their aspect ratio is preserved. Another common preprocessing step adopted in the work [19] is to remove spatial areas of a signature, that have become part of a signature, mainly due to low pressure values recorded by the stylus during data capture. Such points are eliminated by selecting a suitable threshold.

Subsequent to preprocessing, a set of discriminative features are derived from the raw attributes in the feature extractor module. Based on the choice of features selected for signature representation, we can categorize them to either global or local-based approach.

Global based approach: In this technique, features like trajectory length, aspect ratio, number of pens ups and so on are derived to describe the whole signature or a segment of the trace. This method requires that all signatures be represented by a fixed length vector, so that traditional metrics such as Euclidean, City block and L_p norm can be used to calculate the dissimilarity between them. Global feature based techniques have the advantage of (i) compact representation and (ii) low computational complexity while matching the signatures.

There are many works available in literature which use global feature based methods for representing the signatures. In particular, mathematical tools from the area of signal processing such as Fourier transform (DFT), Discrete Wavelet transform (DWT) and Discrete Cosine Transform (DCT) have been used in [30–34]. In the work [35], the authors propose a set of hundred global features for representation.

Local based approach: In this method, multivariate time series / attributes describing the trace of signature captured by the tablet is used for representation [26]. The time functions are converted to a temporal sequence of vectors that exploit the locality properties. Some of the commonly used temporal features for signature representation are (i) velocity, (ii) acceleration, (iii) pressure difference between sample points, (iv) direction of pen movement captured using curvature, (v) azimuth difference between sample points, (vi) inclination angle difference between sample points - to state a few.

In general, features derived locally along the temporal trace require larger storage space for signature representation. This makes the process of matching using elastic based methods (discussed in the following subsection) time-consuming.

1.3.3 Matching Module

In this module, the derived features of a test signature are contrasted against those from the enrolled genuine signatures of an user to be authenticated. The prominent approaches being adopted in literature with regards to the matching strategy are the distance and model based techniques.

Distance based methods: In this scheme, we match the test signature against the enrolled training signatures stored as reference templates. When a signature is represented by global features, the dimensions of feature representation between all the signatures are the same. The metrics such as Euclidean and City-block are used to measure the dissimilarity scores. In case of multiple template signatures, the mean, minimum, maximum or median of distance values are used as a dissimilarity value for a test signature [36].

On the other hand, when a signature is represented by local features or point based features, traditional distance measures such as Euclidean or City-block can not be used directly for matching. This is owing to the fact that the length of training signatures are not necessarily the same. To overcome this problem, elastic matching techniques such as Dynamic Time Warping (DTW) [3, 37, 38] and Longest Common Sub-sequence (LCSS) are used [23]. All these methods employ a dynamic programming strategy to manage the variability of length between the signatures.

Model based methods: The model based technique builds the statistical profile of the signature with generative models Hidden Markov Models (HMMs) [26] and Gaussian Mixture Models (GMMs) [39] or discriminative ones such as Support Vector Machines (SVMs) [38], [40] and Multi Layer Perceptrons (MLPs) [41]. The generative model based approaches evaluate the relation of the features of the signature to be verified with regards to their statistical characterization. In general, the outcome of the verification system is a likelihood measure - that quantifies how probable a test signature belongs to the claimed client's model. Contrary to this, with the discriminative model, the verification score is based on the distance of the claimed signature of the user to their corresponding decision boundary of separation from the other users.

1.3.4 Decision Making Module

Once a similarity or dissimilarity score is obtained, the decision making module calculates the decision threshold. If the similarity score of a signature is greater than or equal to the computed threshold, it is accepted as a genuine otherwise it is rejected as a forgery. In case of dissimilarity score, any signature is accepted as genuine if its value is less than or equal to the threshold.

We now provide the definitions of the performance measures adopted in the online signature verification research community to judge the effectiveness of any strategy.

False Acceptance Rate (FAR): False acceptance of a forgery signature occurs when the similarity score obtained by comparing the forger's test sample with template samples of the claimed user exceeds a specified threshold. In other words, the FAR indicates the proportion of the forgery signatures that get falsely accepted as genuine by the verification system. In particular, lower value of FAR indicates better performance of the algorithm.

False Rejection Rate (FRR): False rejection of a genuine signature occurs when the similarity score obtained by comparing the genuine test sample with template samples of the claimed user falls below a specified threshold. As such, the FRR indicates the proportion of the genuine signature samples that get falsely rejected as forgery.

Detection Error Trade-off (DET) curve: This represents a two dimensional plot of FAR and FRR values at various values of threshold used in the verification process.

Equal Error Rate (EER): The EER refers to that point in the DET curve where the FAR and FRR values are equal. It is thus evident that an algorithm with a lower value of EER is better in authenticating a signature, compared to the one with a higher value.

1.4 Summary

In this Chapter, we first presented a brief introduction of biometric systems - that are used for authenticating the identity of an individual. Thereafter, we mentioned that our emphasis in this thesis is on developing algorithms for the problem of online signature verification. Keeping this in perspective, we provided a block schematic description of the same.

In the next Chapter, we delve into the literature of online signature verification from the point of view of development of classifier structures. This is followed by an outline of the objective of the thesis with a road map to the subsequent contributing Chapters.

2

Literature Survey

Contents

2.1 Introduction

The topic of online signature verification has been a very active area for research exploration, since the past three decades, with the survey of works being well documented in [42–48]. As mentioned in the previous Chapter, the strategies adopted to extract relevant information from an on-line signature data are the global and the local based approaches. In the former, a representation of the signature is built using features, derived from the acquired signature trajectories such as trace length, aspect ratio, number of strokes, number of local extremals (minima and maxima in x, y), number of pen-ups/downs to state a few. Contrast to that, in the local-based approach, the temporal sequence describing the local properties of the signature trace are used for verification. In particular, features like position trajectory, velocity, acceleration, curvature angles and many more, are derived at each sample point of the online trace.

With regards to the classifier structures, there have been various approaches being proposed, primarily based on distance and model based techniques. Distance based methods utilize concepts of edit distance and dynamic programming (from the area of computer science) to match the test signatures with the set of enrolled signatures [3, 49, 50]. Model based approaches, on the other hand, employ the use of either generative-based classifiers like Hidden Markov Models (HMMs) [26, 29, 51–55] and Gaussian Mixture Models (GMMs) or discriminative ones such as Support Vector Machines (SVMs) and Multi Layer Perceptrons (MLPs) for verification.

The main contribution of the thesis (to be detailed in Section 2.4) is on reducing the error rate of online signature verification systems with novel strategies that enhance the utility of distance and model based methods. Keeping this into perspective, we focus our survey primarily with regards to these approaches.

We begin the survey by detailing the strategies that employ distance based methods in Section 2.2. This is followed by a description of systems adopting the model based approach for verification in Section 2.3.

2.2 Distance Based Approaches

The online signature verification works that adopt the distance based approach can be classified into one of two categories - non-elastic and elastic based methods. The former use traditional similarity / dissimilarity measures such as City Block, Euclidean (or in general a L_p- norm) for matching. Accordingly, prior to the similarity computation, a fixed length vector representation for the signature is to be obtained. On the contrary, the elastic distance methods temporally align the sequence of feature vectors describing the local characteristics of the online signature trace with dynamic programming algorithms. Example of the same include the Dynamic Time Warping (DTW), Longest Common Sub-sequence (LCSS) and Edit Distance techniques. As such, elastic distance techniques have the capability to match signatures represented with feature vector sequences of varying lengths.

The details of prior research work from literature utilizing these methods is given under the following two subsections - 2.2.1 and 2.2.2 respectively.

2.2.1 Non-elastic Distance Based Methods

In the work [56], the authors propose a verification scheme based on spectrum analysis, where the Short Time Fourier Transform is employed for analyzing the characteristics of a signature. The trace of the signature is partitioned to a number of segments - subsequent to which, a Fast Fourier transformation is applied on each of them. The distance between the Fourier coefficients within the corresponding segments of the test and reference signatures are computed and the verification is achieved with a Mahalanobis distance criterion.

In another work, Yanikoglu *et al.* extract the Fourier descriptors to represent the signature by a fixed length sequence [30]. Subsequent to extraction, appropriate normalization is done to make the extracted features translation, rotation and scale invariant. Besides normalization, zero padding is done prior to Fourier Transformation to get the same length of feature vector across all the signatures. In the matching stage, the Euclidean metric is used as a dissimilarity measure to compare the Fourier descriptors of the query signature to the reference signatures of the claimed user in the database.

A verification strategy using the concept of wavelet packets is proposed in [57]. Signatures are first normalized and re-sampled, so that they have the same number of sample points. Thereafter, several popular local features are extracted on which the one dimensional Discrete Wavelet Transform is applied. The choice of the optimum number of local features, wavelet bases and wavelet packet settings are studied empirically through experimentation.

An interval-valued symbolic feature representation for signatures is proposed in [58] and [59]. The authors begin by extracting a set of hundred global features, that were suggested in an earlier work by Fierrez-Aguilar *et al* [35]. Thereafter, the lower and upper limit of each interval is set for each of the features on the basis of their statistical characterisation of mean and variance. In order to verify the authenticity of the query signature, the authors propose a measure termed as 'acceptance count'. In addition to this, the concept of writer dependent and feature dependent thresholds have been explored for verification.

The use of the Mellin transform in combination with the Mel Frequency Cepstral Coefficient is presented by the authors of the work in [60]. One of the salient property of Mellin transform is that of scale invariance which makes the extracted features insensitive to different signature scales. Subsequent to the feature generation, the authors borrow the idea from [38] and represent the signature as a three dimensional feature vector comprising distance values. This vector is then fed to a classifier for verification.

The authors of the work [61] use attributes of several histograms, derived from the online signature to construct a discriminative feature vector for signature verification. Their system comprises three stages: feature extractor, template generator and template matching. In the feature extraction stage, a vector consisting of derivatives of a set of features is constructed. In template generator stage, using the enrolled samples of an user, the variances of each of the feature components in a vector are calculated and thereafter an user-specific uniform quantizer is constructed. The resulting quantization step size vector is used to quantize each of the features in a feature vector derived from the enrolled samples. Finally, the average of the quantized feature vectors is regarded as the template for the user under consideration. In the template matching stage, given a test signature, a dissimilarity score is calculated between its quantized feature vector with that of the stored template. Based on this score, a decision is made to authenticate the signature.

In a recent work [34], an online signature verification technique based on Discrete Cosine Transform (DCT) and sparse representation is proposed. The authors investigate on a property termed 'temporal dilation' to obtain a compact and fixed length representation for online signatures. This in a way provides an effective and alternative way to deal with the problem of variable length time series - that is quite common in online signature data. Moreover, a task-specific method of building an over-complete dictionary for sparse representation is used to describe the signature. The verification is achieved using a SVM that considers two sets of attributes - (i) the energy features (computed from DCT coefficients) and (ii) sparsity features (from the sparse framework paradigm).

2.2.2 Elastic Distance Based Methods

These methods employ the temporal sequence describing the local properties of the signature trace for verification. In particular, features such as position trajectory, velocity, acceleration and curvature angles are derived at each sample point of the online trace. In order to capture the similarity of two signatures, one needs to come up with a distance score between their corresponding sequences of the point based features. The number of sample points between any pair of signature samples may not be necessarily the same. In such cases, elastic matching techniques are useful to compare patterns in which rate of progression varies non-linearly. There are a number of such techniques proposed in literature, thanks to the dynamic programming approaches in the area of computer science. Typical examples of the same include the Dynamic Time Warping (DTW) borrowed from speech recognition [62] and Edit-Distance methods used in string matching applications [63].

One of the early works in the DTW approach for authenticating the veracity of signatures was proposed in [3]. Here, a set of local features are extracted from the shape of the signature. The similarity between an input signature and the reference set is then computed by a dynamic programming technique. The signature verification system is evaluated both in terms of a global as well as an user specific threshold. The authors claim that employing user specific thresholds is better, giving improved performance in comparison to a single global threshold. A variant of this work has been addressed in [64], wherein a warping technique termed extreme point warping is proposed. Different from the traditional DTW, the extreme point warping technique operates on only selective points of the online trace. Another work on the same lines utilizes a string matching algorithm to match the sequence of position extremal points between a test input and the set of enrolled signatures [65]. Likewise, the exploration in [66] is based on strategies that select only a subset of sample points for matching with DTW.

In the work [67], the idea is on first dividing the time functions into several segments, that in a way, describe the regional properties. Thereafter, a segment-to-segment mapping is obtained by a variant of the DTW matching algorithm, which is then utilized for verification. Likewise, the work presented in [68] make use of geometric extremals for segmenting the signature trace. Subsequent to this, their properties are exploited to obtain the segment-to-segment correspondence by applying the edit distance strategy.

The authors in [30] suggest a verification scheme, built using a fusion of the DTW system with that of a global feature based system employing Fourier descriptors. Owing to the complementary nature of the two obtained scores, the fused system is shown to outperform the individual ones. In [38], the authors use the x and y co-ordinate difference between consecutive points as local features for signature representation. A modified DTW algorithm is then used to align a test signature with the reference signatures of the user. During the training stage, all the reference signatures are pairwise aligned. Thereafter, the signature that has the lowest average DTW distance to the other reference signatures is taken as the template signature. Given a test signature, its distance to the nearest, farthest and template reference signatures are normalized by the corresponding mean values obtained from the reference set (during training) to form a three dimensional feature vector. This resulting feature vector is then used to verify the authenticity of the signature with a Support Vector Machine (SVM) classifier.

In the work [69], the reference signatures are employed to suggest parameters for each signer, that in a way, ensures the system to cover the intra signer variations. The parameter values are estimated based on matching the signatures using DTW and considering the distances obtained thereof. During the verification step, the estimated parameters of a specific user are used to authenticate the veracity of his / her signature. In addition to this contribution, the authors explore on several feature sets for verification.

The on-line signature verification system proposed in [70] employ a sequential forward selection algorithm to obtain an optimal feature set, so that the verification system can be adapted to environments with different levels of security. The matching of the signatures using the selected feature set is thereafter achieved with a DTW. On a similar note, as an exploration of the effectiveness of azimuth and altitude features for online signature verification, the authors of the work [71] consider a DTW based framework in their empirical study.

In the exploration of [72], the elastic distances between the test signature and the reference signatures are computed on coordinates, pressure and pen-inclination angles (azimuth and altitude) separately. Thereafter, the weighted sum of the three resulting scores are used for verification. Likewise, a strategy of fusing elastic distance scores based on these three measures, namely - spherical coordinates associated to the two pen inclination angles, the pressure time function and the coordinates time functions is proposed in [73].

A two stage score normalization technique is employed on the score obtained from the DTW algorithm in [74]. This scheme detects the simple forgeries in a first stage and copes with more skilled forgeries in a second stage. In addition, the performance of traditional normalization strategies (such as standard min-max, z-score, division by length of questioned signature and average length of reference signature) on the verification performance are also empirically studied.

In order to reduce the computational complexity of the DTW algorithm, a set of length normalization methods based on three re-sampling techniques namely spatial based, temporal based and mean based are proposed in [20]. These techniques equalize the signature length and hence avoid the use of dynamic programming. The authors report an increase in processing speed compared to the DTW-based systems while maintaining comparable performance to prior works. Added to this advantage, a fractional distance measure is employed for dissimilarity computation between the signatures, thus overcoming the concentration phenomenon that appears with high dimensional matching of data using the traditional Euclidean distance measure.

The idea of turning angle sequence and subsequently the turning angle scale space for representing the sample points of the online signatures is considered in [23]. However, for matching the temporal sequences, a variant of longest common sub-sequence (LCSS) matching is employed. The dynamic programming scheme used for calculating the LCSS employs one threshold parameter to reject the matching of sample points with higher distortion values - thus in a way, avoiding the match of outliers. In yet another work, Gruber *et al.* [40] adopt the idea of the longest common subsequences (LCSS) algorithm to a kernel function for Support Vector Machines (SVM). The derived kernel makes it possible to classify the trace of the online signatures of different lengths. As such, the similarity of the two temporal sequences is determined very accurately since outliers are ignored.

A combination of Vector Quantization (VQ) approach with DTW has been presented in [36], wherein the quantized feature vectors of the test signature of a claimed user is matched against that of the enrolled genuine signatures. To further enhance verification performance of the verification system, score level fusion of these two systems using sum rule is employed. It is to be however noted that the main focus for quantization of the feature vector is from the viewpoint of enhancing the privacy of the signature verification system, so that hackers find it difficult to replicate the data from the extracted features transmitted. The subsequent works by [75] and [76] consider using separate code-books across multiple sections of the signature, obtained by partitioning the online trace into equal number of segments for signature recognition. In a way, the separate code-book for each section incorporates the writer specific temporal characteristics and hence provide an improved performance when compared to a single code-book based VQ system.

A simple modified variant with signature curves constraint - abbreviated as 'DTW-SCC' is proposed to solve the problem of heavy computation of DTW in [77]. In addition, an analysis pertaining to the stability of spectral information (inherent in a signature) is performed with the Discrete Wavelet Transform. The stable spectral information is selected dynamically to reconstruct the stable spectral features for each specific user, that are then matched using the DTW-SCC for authentication. In a recent work, to reduce the inconsistencies among genuine signatures due to various size, location and rotation at different inputs, X. Xia *et al.* propose a GMM based alignment method [78]. The resulting aligned signatures are then used for verification by adapting the DTW-SCC scheme of [77].

The utility of DTW for the extraction of a stable and discriminative segment from the online trace of the signature has been explored in [79]. This work employs the user specific velocity profile of the user's signature for segmentation. In particular, the velocity signal is employed for finding the correspondence / alignments among signatures of the same person by using the DTW algorithm. Subsequent to the alignment, velocity values along the trajectory of signature are divided into three velocity bands namely high, low and medium. The authors analyse the different bands and suggest the medium velocity segment to be empirically stable and discriminative for template generation. In their later work, the same authors use features derived from partitioning the horizontal and vertical trajectories of the online signature, on the basis of pressure and velocity profiles to authenticate a test signature [19]. In the verification stage, a signature is partitioned according to the most stable feature selected during training and the two distance values corresponding to horizontal and vertical trajectories are calculated. These scores are then used for authentication by constructing a decision boundary between the genuine and forgery signatures.

Keeping in line with the above works, there has been few recent explorations for partitioning the trace of signatures, depending on the values of attributes such as speed of signature and pen pressure [80], [81] and [82]. Thereafter, the partitions are used for the classification step, which is achieved using flexible neuro-fuzzy one class classifier. Prior to partitioning, the alignment of the signatures are obtained by employing the DTW algorithm so that only the one-to-one correspondences between sample points of the signatures being matched are considered.

We also make a mention of a recent approach adopted in the works [83, 84], wherein a signature is verified using a multi-domain strategy. Based on the stability model of each signer, the signature is split into different segments. Thereafter, for each segment the most profitable domain of representation useful for verification is detected. At the time of verification, DTW is employed to evaluate the authenticity of each segment of the unknown signature by using the specific domain of representation.

2.3 Model Based Methods

In this subsection, we discuss proposals from the literature that pertain to the category of model based approach:

The authors in [85] use a verification system that exploits the global information of signature. A set of 100 global features described in [35] is utilized for signature representation and the matching is performed using an ensemble of Parzen Window classifiers. In another work [86], the same authors explore the performance of one class classifiers such as Mixture of Gaussian descriptor, Principal Component Analysis descriptor and Linear Programming descriptor. In addition, a combination of several systems that treat the verification process as a bi-class pattern recognition problem (genuine or impostor) is shown to give significant reduction of EER in [87]. Likewise, in [88] a multi-matcher scheme is suggested that employs an ensemble of bi-class and one class classifiers for signature verification.

M. Parodi *et al.* explore the concept of consistency to quantify the discrimination capability of features in [25, 89]. In particular, feature combinations associated with the most commonly used time functions related to the signing process are analyzed. A fixed length Legendre polynomial series expansion based representation for modelling the online signature trace is proposed with the expansion coefficients being considered as features [25, 90, 91]. Two state-of-the-art classifiers, namely, SVM and Random Forests are used for verification. It may be noted that this work builds from the idea described in [92], that evaluates on the consistency of individual features employed for signature representation.

The work in [93] proposes a set of similarity measures using the different features obtained during the signing process. These are then reduced to a lower number in the Hotelling reduction process [94], wherein the the most distinctive similarity measures are determined for each user. Subsequently, classifiers such as Perceptron, k-Nearest Neighbor, Random trees, Random forests are used for verification. In a later work by the same authors [95], the preceding idea is experimented using a Probabilistic Neural Network in conjunction with Particle Swarm Optimization algorithm.

In the work [26], a set of time sequences and their first and second order derivatives are calculated from the online signature data. The features are normalized and modeled by a left to right HMM with continuous probability density functions. In the verification step, likelihood scores are considered as relative values with respect to a reference population and are normalized by an appropriate technique [96]. A fusion of HMM likelihood values with segmentation score calculated from the Viterbi path information has been exploited cleverly to discriminate the forgeries from the genuine signatures in [29]. The segmentation score is obtained by computing the average City Block distance between the segmentation vectors, corresponding to Viterbi path of the genuine signatures with that of the test signature.

The use of local and global information present in an online signature has been successfully employed in [35]. The global information is extracted with a feature-based representation that is then subsequently learnt with a Parzen Window Classifier. The local information, on the other hand, is extracted as time functions of various dynamic properties modelled by using HMM. The above two systems are shown to give complementary recognition information and hence fused with the sum rule.

The idea of GMMs for online signature verification has been proposed by several authors [39, 97, 98]. Here, the log-likelihood scores obtained are compared to a threshold for authentication. A two-stage statistical system comprising a simplified GMM model for global signature features, and a discrete HMM model for local signature features is adopted by the authors in [99]. In the works [100–102], the test signature is first aligned with its template by applying a DTW algorithm. Subsequent to this, the most salient features are extracted and used as input to a GMM model for authentication.

Argones Rua and Alba Castro *et al.* [27] use a HMM model in two different modes namely, the User Specific HMM (US-HMM) and the User Adapted Universal Background Model (UA-

UBM). The effectiveness of log-likelihood scores and City Block distance between segmentation vectors obtained from the Viterbi path are studied. In addition to this, the impact that a feature selection set has on the performance of the US-HMM and UA-HMM systems is also investigated.

In yet another exploration, the authors in [103] propose an approach that considers the utility of user dependent features for decision making. The choice of the features as well as the classifier to be adopted per user is made based on the error rate obtained on the training samples. Likewise, the same authors employed features in the work [104] - the selection of which was made on the value of a score computed for each user. Last but not the least, in a recently published work [105], they utilize the idea of interval based symbolic feature description to represent the user dependent features.

2.4 Overview of Thesis

In this thesis, we propose a number of online signature verification systems, in line with DTW based approach. From the review material so far on elastic distance based methods (Section 2.2.2), we see that the systems based on DTW in literature perform a temporal alignment between the feature vectors that are derived at each sample point of the online trace of the signatures being compared. The resulting scores after the accumulation of distance values along the warping path are used to verify the authenticity of the signature. The DTW score reflect in a way the similarity of the test signature with the reference genuine signature of an user, enrolled to the system. Either the minimum or average of scores are compared to a threshold, for authenticating the signatures.

From the survey of works, we note that the warping path, leading to the DTW score, is rarely exploited for verification. The warping path is obtained by placing constraints on the alignments between pair of sample points of the two signatures being compared. In this thesis we demonstrate that, at times, the sole dependence on the DTW score may not be effective enough in discriminating the skilled forgery signatures from the genuine. This is the case, especially, when the signature patterns exhibit values, that are quite close to each other. The verification decision (based on the threshold), may lead to either a genuine signature getting rejected and/or a skilled forgery signature getting accepted. Thus there arises a need to improve the verification capability of the traditional DTW system.

We believe that the analysis of the characteristics of the warping path in the cost matrix may provide us additional cues, that can be possibly exploited for reducing the false acceptance of forgeries and rejection of genuine signatures. We explore in this direction by proposing three different strategies as enumerated below.

Strategy 1: In this novel method, we utilize the alignment obtained from a DTW match together with another, proposed based on a measure inspired from correlation-based neighborhood matching [106] for formulating a warping-path based score. The derived score comprises two components - feature distortion and displacement, each of which are found to empirically aid the verification step.

Strategy 2: In this new technique, we derive a score that determines the proportion of the aligned pairs that provide a low distortion value, relative to the length of the warping path, obtained from DTW. For computing this proportion, we consider utilizing a code-book of appropriate size, built from a Vector Quantization (VQ) model.

Strategy 3: In this novel scheme, we explore the characteristics of warping path by a combination of distance with model based approach. We encode the local features extracted at each sample of the online trace of a user's signature by a set of descriptors, that are obtained from a Gaussian Mixture Model (GMM) - a model based approach. The resulting descriptors are then aligned using DTW and subsequently utilized for deriving the warping path score.

Subsequent to the derivation of the warping score from each of the above strategies, we fuse it to that of the DTW for performance enhancement.

In addition to the above three **major** contributions, the thesis presents novel ideas on other fronts as well:

- We consider evaluating the DTW based signature verification system on a set of features modified from the ones popularly used in literature. In particular, we suggest the notion of a spacing parameter value for feature extraction and demonstrate its utility in increasing the separation between the distribution of genuine and skilled forgery signatures of an user.

- We propose on capturing the contextual information in the formulation of the traditional DTW strategy and show improvement to the verification system.

- An important aspect that has hardly been sought after in the literature is on considering the sequence of feature vectors, being matched, from a probabilistic viewpoint. This representation can help capture the user dependent characteristics of a signature, thereby improving the discrimination between the genuine and skilled forgery signatures. The main premise comes from the notion that feature vectors corresponding to parts of the online trace of the genuine signatures of an user reside in specic regions of the feature space. Thus, it would be interesting, to explore out on a probabilistic representation for the feature vector corresponding to each sample point of the online trace, with regards to their degree of association to each of these regions.

  As a step in this direction, we consider in this proposal, to encode the local features extracted at each sample of the online trace of a users signature by a set of descriptors, that are obtained from a GMM (Gaussian Mixture Model). The resulting descriptor representation of the signatures are then temporally matched using the DTW algorithm.

The novel signature verification algorithms reported in the thesis are validated on the publicly available SVC-2004 and MCYT-100 databases. We demonstrate several experiments, that reflect the various aspects of the proposals, being explored for improving the verification capabilities of the baseline DTW system. Needless to mention, we report a reduced error rate (EER).

2.5 A glimpse of the contributing Chapters

In this thesis, we propose strategies to characterize the warping path, that in a way, provide additional cues to enhance the verification capabilities of DTW based system. Accordingly, in the following subsections, we present the outline pertaining to the three working Chapters.

2.5.1 Chapter 3:: Exploration of novel information from the DTW cost matrix for verification

In this Chapter, we seek to derive additional information from the cost matrix of the DTW algorithm for verifying online signatures. We present illustrative examples that suggest that there is a need to explore cues other than the DTW score to verify the authenticity of an online signature. Our strategy of formulating a warping-path based score makes use of the alignment obtained from a DTW match together with another, proposed based on a measure inspired from correlation-based neighborhood matching [106]. The derived score comprises two terms, namely 'feature distortion' and 'displacement'- the definitions of which are discussed in the Chapter. In particular, we also depict via a histogram based approach, the impact of these individual components to the verification step. Finally, we show through empirical validation that there is a need to fuse both the DTW and warping path scores through a combination scheme for improvement of error rates. This is owing to the fact that the scores behave in a complementary fashion, with the sole reliance of each of them separately presenting an overlap with the genuine and skilled forgery signatures of an user. We also present results to demonstrate that our proposal improves over DTW verification systems implemented using different recursion functions as well as distance measures for the cost matrix computation.

Apart from the analysis of the warping path for verification, we also consider evaluating the verification system on a set of features modified from the ones commonly used in literature. We suggest the notion of the spacing parameter value for feature extraction and illustrate its utility in reducing the error rates in the DTW system.

2.5.2 Chapter 4:: An Enhanced Contextual DTW System using Vector Quantization

In this Chapter, we modify the traditional DTW algorithm to incorporate the neighborhood / contextual information, while matching the test with the reference signature. The entries in the cost matrix in DTW algorithm is calculated by considering the neighborhood of the sample points being matched. The computation of the modified values as such aids in smoothing out any drastic changes in the distance computations, that may occur whenever there is a break in signature. Thus, we get reduced error rates over the conventional DTW that relies on point-to-point matching of sample points (without context).

Further, as an analysis of the warping path to alleviate on the issue of the DTW algorithm discussed in the Section 2.4, we derive a score that quantifies the proportion of the aligned pairs having a low distortion value, with regards to the length of the warping path in the DTW cost matrix. For computing this proportion, we make use of the code-vectors of a code-book of appropriate size, built from a Vector Quantization (VQ) model. Thereafter, owing to the complementing nature, we fuse the derived warping path score with that of the DTW, (by combination strategies), for authenticating the veracity of a test signature. In addition, we also explore on incorporating contextual information into the derivation of the warping path score and use the same for verification.

To the best of our knowledge, this work is the first of its kind that utilizes the use of the codebook from a VQ to describe the characteristics of the warping path. It may be mentioned that the prior work of using VQ for online signature verification reported in [36] was based from the viewpoint of enhancing the privacy of the biometric system.

2.5.3 Chapter 5:: A system based on GMM descriptors in a DTW framework

This part of the thesis explores on the incorporation of GMM into the DTW framework. We begin by a discussion on the GMM likelihood system that has been traditionally employed for online signature verification. Thereafter, we motivate the need to capture the user dependent characteristics of a signature by exploring on a probabilistic representation for the point based feature vectors. We propose on encoding the point-based feature vectors of the online trace of a user's signature by a set of descriptors, obtained from a GMM. This strategy is shown to improve the performance of the traditional DTW verification system - the reason being that we are utilizing the statistical variability of different features for the alignment between online signatures.

As a further step, we propose a score to encapsulate the characteristics of the warping path in the DTW cost matrix. The score is obtained as a match between two histograms that are generated by considering the GMM based descriptors. Finally, owing to the complementary nature, we explore a fusion of the warping path score and DTW to authenticate the veracity of the test signature.

It is worth mentioning here that the proposal detailed in this Chapter is the first of its kind that incorporates descriptors from the GMM into the DTW framework. Previous works on GMM and DTW combined systems [107] have separately considered the outputs of each of them, followed by a fusion using a sum rule.

2.6 Summary

To summarize, we provided a detailed review of works from the perspective of authentication of online signatures. We focussed our survey primarily on classifier structures namely distance and model based approaches. Thereafter, we provided the road map to the dissertation, by addressing an issue of the DTW approach to online signature verification with strategies for improving its verification capabilities. Lastly, a brief overview of the ideas being elaborated in the following three contributing Chapters is provided.

3

Exploration of novel information from the DTW cost matrix for verification

Contents

3.1 Introduction

This Chapter explores the utility of information derived from the Dynamic Time Warping (DTW) cost matrix for the problem of online signature verification. It may be recalled from Section 2.4 that the prior works in literature primarily utilize only the DTW scores to authenticate a test signature. Moreover, the characteristics of the warping path (used for the alignment) in the cost matrix is hardly exploited for verification of online signatures. Hence, as our first strategy, we devise in this work, a score that utilizes the information from the cost matrix and warping path alignments.

Figure 3.1 presents the block diagram representation of the proposed system. The input test signature is first passed through a feature extractor module. Subsequent to this step, we compare it against those of the reference signatures using the DTW matching technique. The performance of the verification system is enhanced by taking into consideration, a score that describes the characteristics of the warping path in the cost matrix. This score is fused to that obtained from the DTW by the sum rule. The combined score obtained is then used to verify the authenticity of the signature.

With regards to formulating a warping-path based score, we utilize the alignment obtained from a DTW match together with another, proposed based on a measure inspired from correlation-based neighborhood matching [106]. This score, we show through an illustrative example in this Chapter, can help discriminate between genuine and skilled forgery signatures of an user. In addition, we consider evaluating the verification system on a set of features modified from the ones popularly used in literature. We suggest the notion of the spacing parameter value for feature extraction and demonstrate its utility in increasing the separation between the distribution of genuine and skilled forgery signatures of an user with illustrative examples.

The following are the highlights of our work in this Chapter:

- Modification of features for an online signature based on the idea of spacing parameter value.
- Exploration of a score that describes the characteristic of the warping path in a DTW

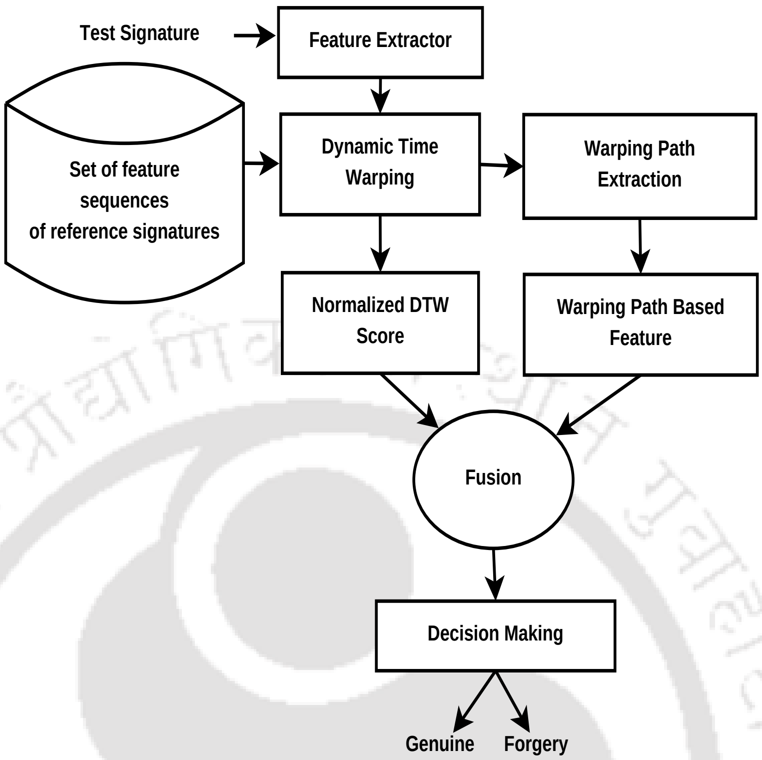


Figure 3.1: Block diagram of the proposed online signature verification scheme.

cost matrix.

- Establishing the utility of the above score for online signature verification, with illustrative examples.
- Proposal of combining the derived warping path score with that of the DTW for decision making.
- Experiments conducted with our strategy present error rates lower to those of the traditional DTW algorithm.

3.1.1 Organization of the Chapter

The contents of the Chapter are organized as follows. We first provide a description of the databases that will be used for the different experimentations of this thesis in Section 3.2. Thereafter, we outline the details of the feature extractor module in Section 3.3. Here, the idea of the spacing parameter value used for modifying the conventional features is discussed with pictorial illustrations. An overview of the traditional DTW algorithm is presented in Section 3.4. As mentioned in Section 3.1, the main crux of the proposal is in coming up with a strategy to characterise the warping path by a score. This is described with complete details in Section 3.5, which for better clarity is subdivided to three subsections - 3.5.1, 3.5.2 and 3.5.3. A pseudo-code is also provided (Algorithm 1) to encapsulate the ideas used for deriving the warping path score. Thereafter, illustrative examples for the application of this score to the problem of online signature verification is presented in Section 3.6. Section 3.7 outlines the protocols used for the experiments in this thesis. This is followed by the details of the experimental results in Section 3.8 obtained with our proposal, that show improvements over the traditional DTW algorithm.

3.2 Dataset description

In this Section, we describe the details of the two freely available databases namely SVC-2004 [17] and MCYT-100 [18]. The signatures of these databases will be employed for the experiments outlined in the thesis as well for the analysis of the different proposals.

SVC-2004: The SVC-2004 development set [17] contains the signature of 40 persons. Each person contributed a total of 20 genuine signatures in two sessions - with 10 genuine signatures per session. The time separation between the two sessions was at least one week. For privacy reasons, signers were advised not to use their real signatures used in daily life. However all the contributors were asked to try to keep consistency of the image and dynamics of their signature. For each person, 20 skilled forgeries were contributed by at least 4 other people. To get the skilled forgeries, writing sequences of each person were made available to the forgers / impostors. A set of genuine and skilled forgery signatures of an user from the SVC-2004 database is illustrated in Figure 3.2.

The signatures were acquired by digitizing tablet (WACOM Intuos tablet) at a sampling rate of 100Hz. Each sample point of a signature is characterized by five attributes: x and y coordinates, pressure and pen orientation (azimuth and altitude). However, all

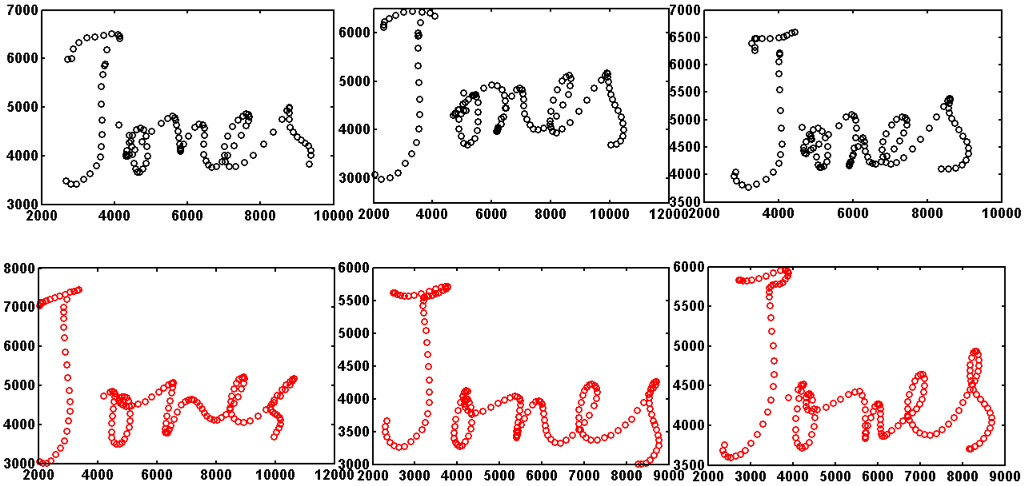


Figure 3.2: Genuine (1st row) and skilled forgery (2nd row) signatures of an user from the SVC-2004 data-base

the sample points of the signature corresponding to zero pressure were removed. The sampling time was recorded for all the captured points along with the pen to tablet contact status.

MCYT-100: This database [18] is provided by the Biometric Recognition Group-ATVC at Escuela Politecnica Superior of the Universidad Autonoma de Madrid. It comprises signature samples of 100 individuals. For each individual, 25 genuine and 25 skilled forgery signatures were collected using the WACOM pen tablet, model-Intuos A6 USB. Each sample point of the trace of the signature contains the following information: (i) Position in x-axis (ii) Position in y-axis (iii) Pressure applied by pen (iv) Azimuth angle of the pen with respect to the tablet (v) Altitude angle of pen with respect to tablet.

The skilled forgery were contributed by five different users, who had access to the static images of genuine signature. Each of the forgers were requested to sign in a natural way, without artifacts, such as slowdown or breaks. As an illustration, the genuine and skilled forgery signatures of an user from this database are presented in Figure 3.3.

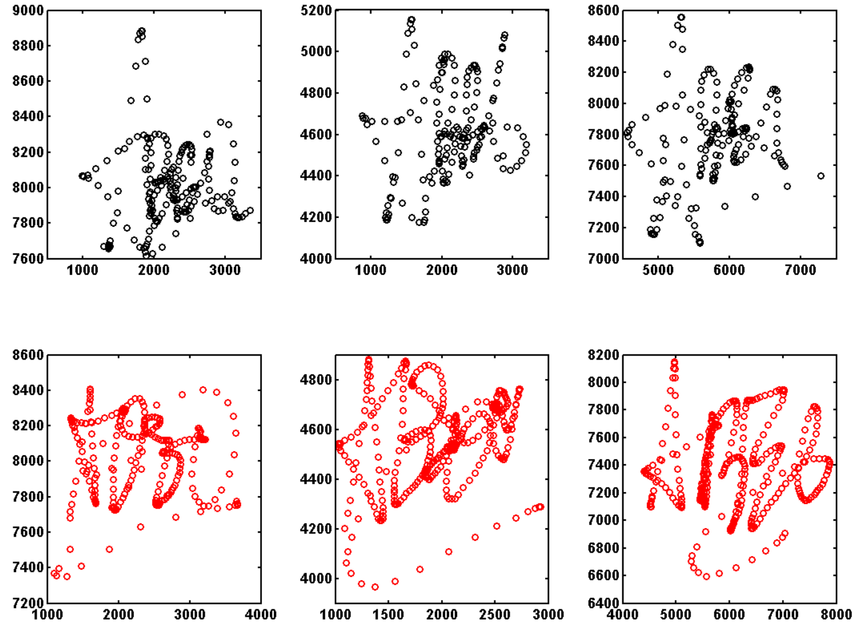


Figure 3.3: Genuine (1st row) and skilled forgery (2nd row) signatures of an user from the MCYT-100 Database

3.3 Feature Extractor

In this work, we adopt a local-feature based approach, wherein a set of features are derived from each point along the online trace of a signature. As mentioned in the preceding Section on data-set description, the dynamic information of the trace as captured by the device used for collecting the signatures comprise a time sequence of attributes such as x and y co-ordinates, pressure p, azimuth ϕ and inclination angle θ. Accordingly, we represent the set of attributes at the i^{th} sample point q_i of the signature by $\{x(i), y(i), p(i), \phi(i), \theta(i)\}$. Prior to feature extraction, each of the sequence of attributes are separately normalized by the min-max transformation to a comparable range $[0, 1]$.

Given a signature comprising n sample points, the feature extractor module constructs a set of eleven features for each sample point from the normalized attributes captured from the device. The features used are quite popular from literature - but for the slight modification with regards to their method of computation as enumerated below:

First order difference: For $i = 1, 2, ...n - r$, we have

$$\begin{aligned}
\Delta x_r(i) &= x(i + r) - x(i) \\
\Delta y_r(i) &= y(i + r) - y(i) \\
\Delta p_r(i) &= p(i + r) - p(i) \\
\Delta \phi_r(i) &= \phi(i + r) - \phi(i) \\
\Delta \theta_r(i) &= \theta(i + r) - \theta(i)
\end{aligned} \tag{3.1}$$

The value of r suggests that the above features are derived between a pair of discrete sample points (q_i, q_{i+r}) of the trace. In other words, the computation is based on the values of the normalized attribute between the sample points whose indices are spaced by value r. In particular, the value $r = 1$ implies that we use consecutive sample points for computing the features. As we shall see shortly, we consider a higher value of r for feature extraction and justify the usage of the same. Hereinafter, in this discussion, we refer to r as the spacing parameter value.

Second order difference of spatial coordinates: For $i = 1, 2, ...n - r - 1$, we define

$$\begin{aligned}
\Delta^2 x_r(i) &= \Delta x_r(i + 1) - \Delta x_r(i) \\
\Delta^2 y_r(i) &= \Delta y_r(i + 1) - \Delta y_r(i)
\end{aligned} \tag{3.2}$$

Sine and cosine : of the angle computed with respect to horizontal axis, defined for $i = 1, 2, ...n - r$, as

$$\begin{aligned}
\sin(\alpha_r(i)) &= \frac{\Delta y_r(i)}{\sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2}} \\
\cos(\alpha_r(i)) &= \frac{\Delta x_r(i)}{\sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2}}
\end{aligned} \tag{3.3}$$

Length-based features : defined by

$$\begin{aligned} l_r(i) &= \sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2} \\ \Delta l_r(i) &= \sqrt{(\Delta^2 x_r(i))^2 + (\Delta^2 y_r(i))^2} \end{aligned} \tag{3.4}$$

The above feature $\Delta l_r(i)$ relates to the change in length obtained between successive pen positions.

Our motivation to suggest features based on the spacing parameter value stems from the trend of distributions that is noticed between the genuine and the skilled forgery signatures for an user. As an illustration, Figures 3.4(a)-(d) depict the normalized histograms of the length feature l_r computed using two values, namely $r = 1$ and $r = 6$, for the genuine and skilled forgery signatures of an user from the MCYT-100 database. The enrollment protocol described in sub-section 3.7.1 is used in obtaining these plots. We note that the distribution of the feature for the value $r = 1$ is not that discriminative, when compared to $r = 6$. In fact, the bin indices corresponding to the genuine and forgery signatures at $r = 1$, have very similar values (Figures 3.4(a) and (b)). On the other hand, the values of bin indices are quite different at $r = 6$, thereby suggesting that the feature derived at higher spacing parameter value ($r > 1$) aim at providing greater discrimination between the genuine and forgery signatures (Figures 3.4 (c) and (d)). It is however to be noted that the value of the parameter r is chosen empirically based on experimentation. Accordingly, the values considered for the distributions in Figure 3.4(a)-(d) are for illustrative purpose only.

Likewise, we can consider the distribution of the length feature with regards to the spacing parameter values $r = 1$ and $r = 6$ for an user from the SVC-2004 database and come up with a similar observation (Figure 3.4 (e)-(h)).

To further generalize on the applicability of the spacing parameter value across another feature, we depict the distribution obtained using the first order difference values of pressure Δp_r for values $r = 1$ and $r = 6$. This is shown in Figures 3.5(a) - (h) for an user from the two databases. Once again, we clearly see a better separation in the normalized distribution of the genuine from the skilled forgery signatures for the higher value of r, namely $r = 6$.

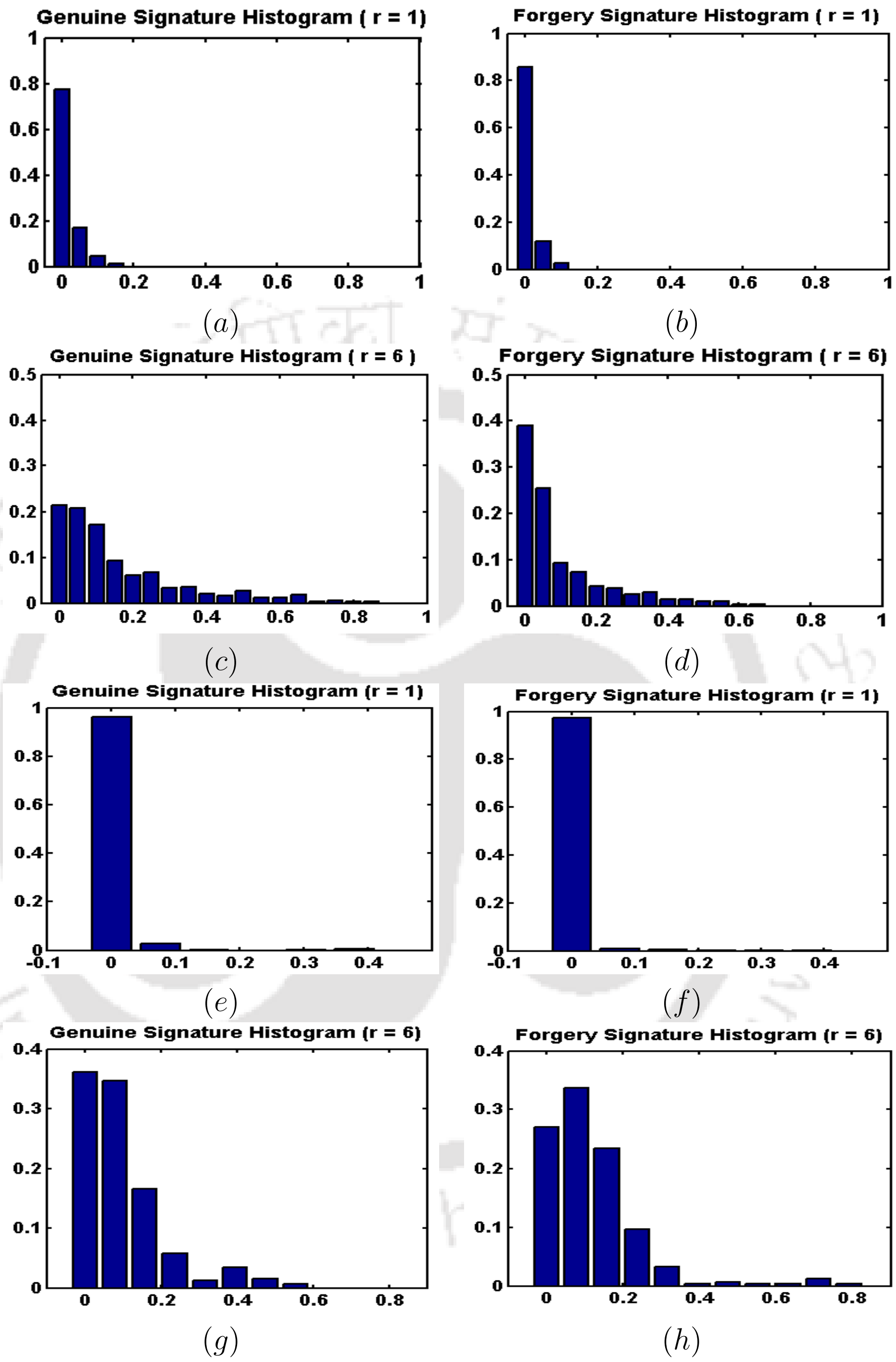


Figure 3.4: These plots illustrate the distribution of length feature as obtained from an user in the MCYT-100 (sub figures (a)-(d)) and SVC-2004 database (sub figures (e)-(h)) respectively for two spacing parameter values $r = 1$ and $r = 6$. We note that between the genuine and skilled forgery signatures, the discrimination is much greater for the higher value, with the corresponding values of bin indices quite different for $r = 6$.

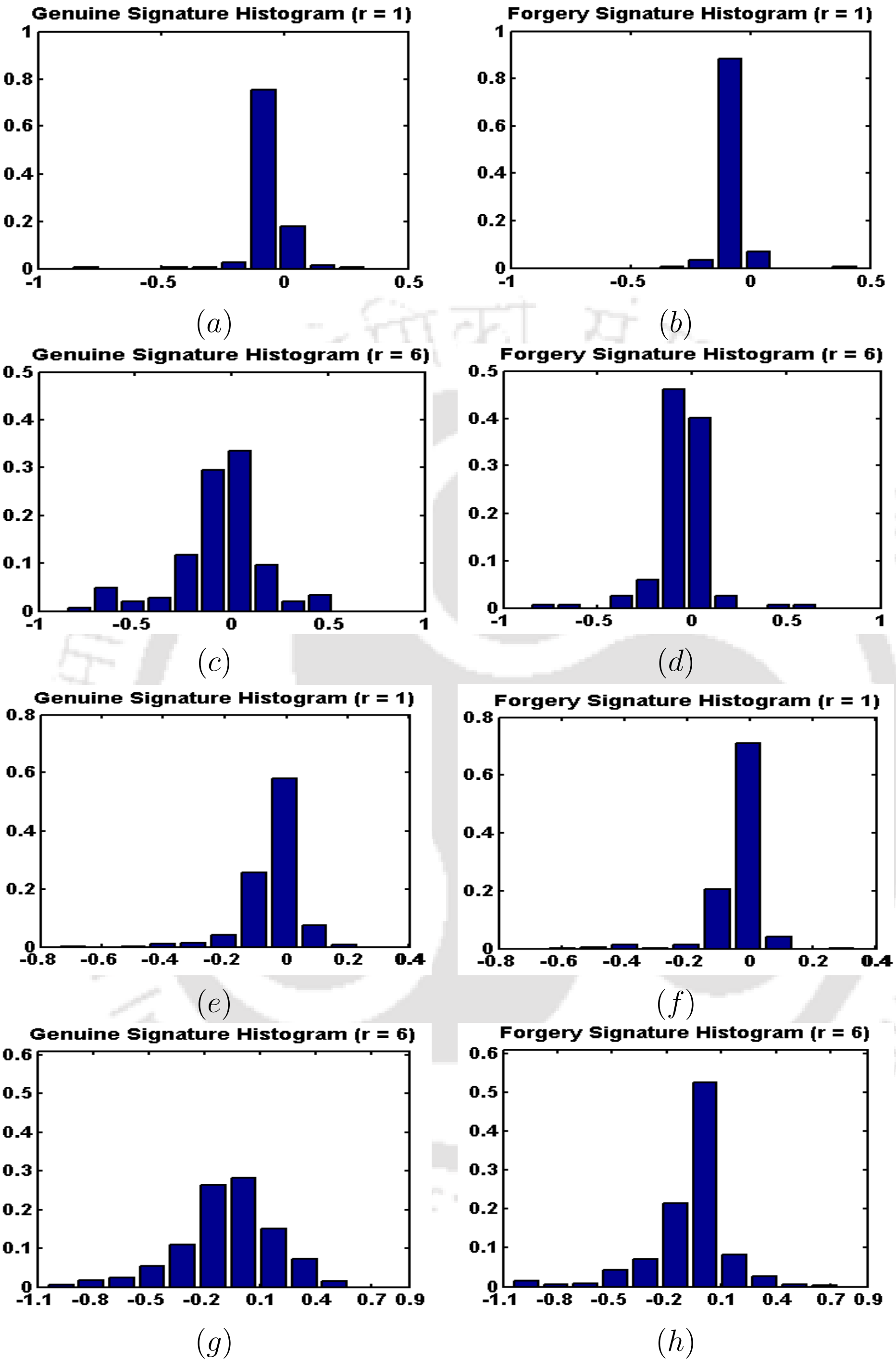


Figure 3.5: These plots illustrate the distribution of the first order difference values of pressure for an user in the MCYT-100 (sub figures (a)-(d)) and SVC-2004 database (sub figures (e)-(h)) respectively for two spacing parameter values $r = 1$ and $r = 6$. Here also it is observed that the discrimination between genuine and skilled forgery signatures is much greater for the higher value, with the corresponding values of bin indices quite different for $r = 6$.

Let $\{S_1, S_2, ..., S_N\}$ denote the N genuine signatures of an user, that are enrolled into the verification system. These will be referred to as 'reference' signatures in this thesis. A reference signature S_p (comprising n_p sample points) is represented as a sequence of point based feature vectors defined by:

$$\mathbf{F}_p = \{\mathbf{f}_p^1, \mathbf{f}_p^2, ..., \mathbf{f}_p^{n_p-r-1}\} \qquad 1 \leq p \leq N \tag{3.5}$$

Here $\mathbf{f}_p^j = [f_p^j(1) \;\; f_p^j(2) \;\; .... \;\; f_p^j(11)]^{\mathbf{T}}$ denotes the eleven dimensional feature vector extracted at the j^{th} sample point of the online trace of the reference signature S_p for a given value of r. Note that the elements in the vector $\mathbf{f}_p^j$ are computed from Equations 3.1 to 3.4. The symbol $\mathbf{T}$ corresponds to the transpose operation of the row vector.

3.4 DTW based matching

The Dynamic Time Warping (DTW) algorithm is considered for matching a test signature S_T, (comprising a feature vector sequence of length $n_T - r - 1$) against a reference signature S_p of length $n_p - r - 1$, where $1 \leq p \leq N$. We construct a $(n_T - r - 1) \times (n_p - r - 1)$ matrix, whose $(m, n)^{th}$ cell contains the measure of dissimilarity (denoted by $d(m, n)$) between the m^{th} point of S_T with the n^{th} point of S_p. Accordingly, we refer to this matrix as the "cost matrix". The measure of dissimilarity used is the City Block distance defined by

$$d(m, n) = |\mathbf{f}_T^m - \mathbf{f}_p^n| = \sum_{k=1}^{11} |f_T^m(k) - f_p^n(k)| \tag{3.6}$$

It is to be noted that the City Block distance is just a choice being made in this work. In lieu of it, one could as well consider any other norm (Euclidean or the like) for the computation of the cost matrix.

Using the cost matrix, an optimal warping path $\mathcal{W}_p^*$ is selected, comprising a contiguous set of matrix elements that define a mapping between the feature vectors of the signatures being compared. The warping path is subjected to the constraints of boundary conditions, continuity and monotonicity. The following recursion relation is used for computing the DTW score.

$$\psi(m,n) = d(m,n) + \min \begin{cases} \psi(m,n-1) \\ \psi(m-1,n-1) \\ \psi(m-1,n) \end{cases} \tag{3.7}$$

where $\psi(m,n)$ corresponds to the cumulative distance up-to the current element. In order to account for the varying warping paths obtained during the matching process with different reference signatures, the DTW score is normalized with $l_{\mathcal{W}_p^*}$, the number of aligned pairs on the warping path $\mathcal{W}_p^*$ [62] as:

$$d_1^p = \frac{\psi(n_T - r - 1, n_p - r - 1)}{l_{\mathcal{W}_p^*}} \tag{3.8}$$

As a notation, we denote d_1^p as the normalized DTW score, obtained when the signature S_T is matched against S_p. For a genuine to reference signature match, the value of d_1^p is low. The contrary is true when a forgery is matched to a reference signature. The optimal warping path, obtained by back tracing the sequence of cells in the warping matrix ψ, is written as:

$$\mathcal{W}_p^* = \{(a_1, b_1), (a_2, b_2), ..., (a_{l_{\mathcal{W}_p^*}}, b_{l_{\mathcal{W}_p^*}})\} = \{(a_i, b_i)\}_{i=1}^{l_{\mathcal{W}_p^*}} \tag{3.9}$$

Each of the pairs (a_i, b_i) denote that the feature vector corresponding to the a_i^{th} sample point of S_T is aligned to that of the b_i^{th} sample point of S_p. Also, with regards to the implementation, (a_i, b_i) refers to the cell in the a_i^{th} row and b_i^{th} column of the cost matrix. Henceforth, in the remainder of the discussion, we interchangeably refer to the pair (a_i, b_i) as an 'alignment' or 'cell'.

Owing to the boundary conditions of the DTW algorithm, we have $(a_1, b_1) = (1, 1)$ and $(a_{l_{\mathcal{W}_p^*}}, b_{l_{\mathcal{W}_p^*}}) = (n_T - r - 1, n_p - r - 1)$. Continuity and monotonicity ensure that $a_{i-1} \leq a_i \leq a_{i-1} + 1$, $b_{i-1} \leq b_i \leq b_{i-1} + 1$, $1 \leq a_i \leq n_T - r - 1$ and $1 \leq b_i \leq n_p - r - 1$. The warping path can, at times, give rise to one to many or many to one alignments, so that the indices in the sets $\{a_i\}_{i=1}^{l_{\mathcal{W}_p^*}}$ and $\{b_i\}_{i=1}^{l_{\mathcal{W}_p^*}}$ may not be necessarily unique.

A close analysis of the dissimilarity costs $d(a_i, b_i)$ along the warping path indicate certain cells with low values, corresponding to parts of the trace between the signatures being matched, for which an impostor is likely to find a difficulty in forging. On the contrary, high values pertain to segments of trace that are distinct between the signatures being compared. An important aspect that the traditional DTW does not adequately capture is the trend in the values of the dissimilarity costs $d(a_i, b_i)$, accumulated along the warping path. We explore in this direction and suggest a score from the warping path in the following Section to improve the verification performance. In doing so, we exploit additional information from the elements of the cost matrix (apart from the DTW score alone).

The idea is to consider using the alignment (a_i, b_i) obtained from a DTW match together with another alignment (a_i, r_i^*) proposed based on a measure motivated using a correlation-based match [106]. The characteristics of each of the alignments (a_i, b_i) and (a_i, r_i^*) $\forall i, 1 \le i \le l_{\mathcal{W}_p^*}$ are then analyzed to devise a warping path score that can help discriminate between the genuine and forgery signatures.

3.5 Utility of additional information from the cost matrix

The proposed warping-path score in this Chapter comprises two components - referred to as 'feature distortion' and 'displacement'. To start with, we outline in subsection 3.5.1 the computation of the alignment pair (a_i, r_i^*) - that will be utilized along with the warping path (a_i, b_i) for deriving these components. Subsequent to its derivation in subsection 3.5.2, the warping path score is combined to that of the normalized DTW in subsection 3.5.3.

3.5.1 Computation of (a_i, r_i^*)

Corresponding to each alignment (a_i, b_i) along the warping path $\mathcal{W}_p^*$, we consider a window segment of odd size $(2w + 1)$ centered on the a_i^{th} sample point of test signature S_T and search for a segment of equal size in the reference signature S_p, whose feature vectors provide the closest match. The window size is empirically chosen and a value greater than one captures the neighborhood information around the centered sample. Accordingly, we can formulate the following criterion (for $1 \leq i \leq l_{\mathcal{W}_p^*}$):

$$r_i^* = \arg \min_{1 \leq r_i \leq n_p - r - 1} \sum_{j=-w}^{w} |\mathbf{f}_T^{a_i+j} - \mathbf{f}_p^{r_i+j}| \tag{3.10}$$

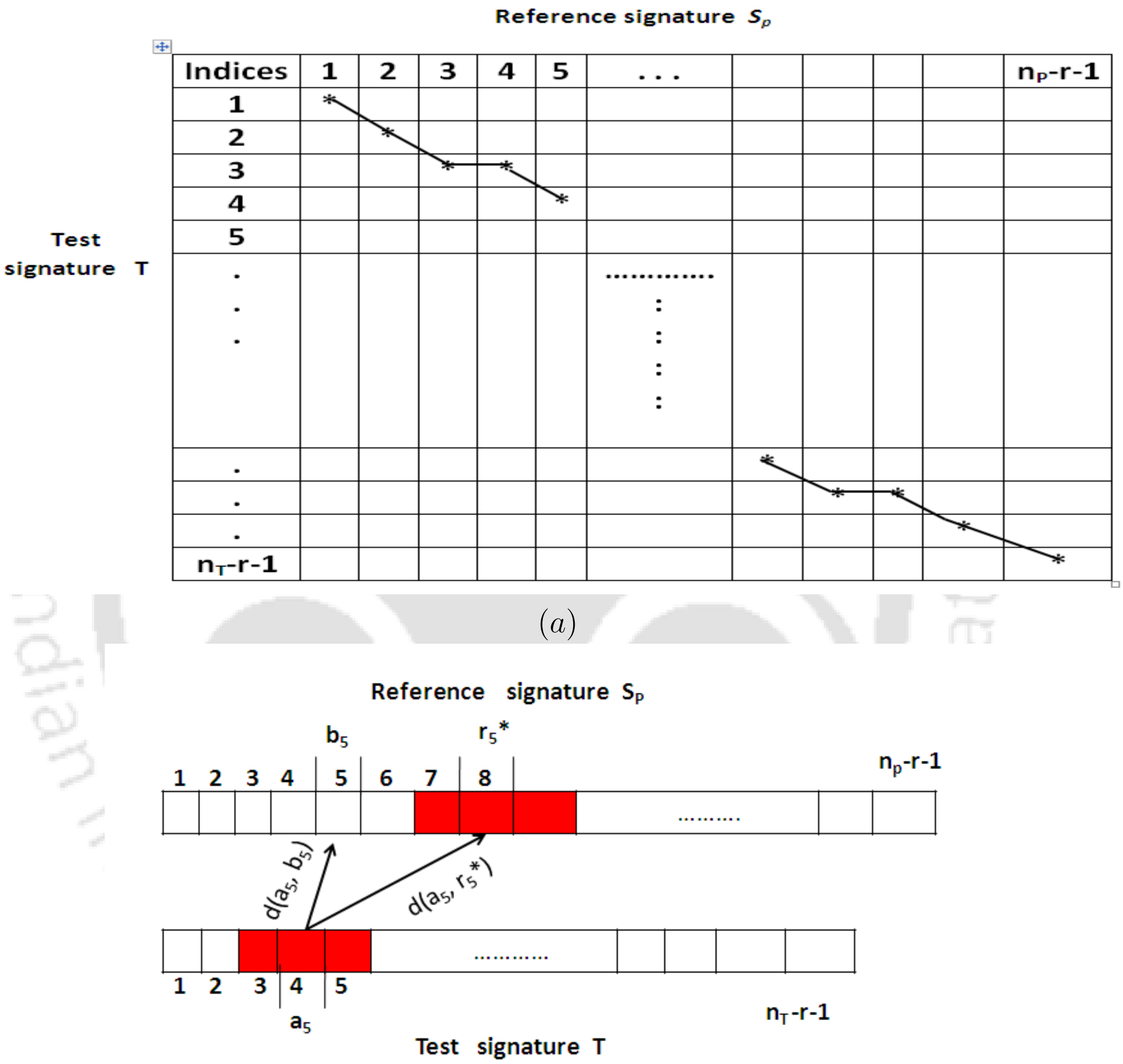
From the definition of Equation 3.6 on City Block distance, we can rewrite the above equation as

$$r_i^* = \arg \min_{1 \leq r_i \leq n_p - r - 1} \sum_{j=-w}^{w} d(a_i + j, r_i + j) \tag{3.11}$$

Corresponding to each segment around a_i^{th} sample point of test signature S_T, the implementation for obtaining r_i^* in Equation 3.10 requires us to compare it against windows of size $(2w+1)$ that are slid across the entire trace of the reference signature S_p. The sum of absolute differences between the feature vectors contained across the window segments being compared is used for computing the matching similarity. The centre index of the segment in S_p providing the closest match (by minimizing the summation terms in Equation 3.10) corresponds to the index value r_i^*. The computation in Equation 3.10 is performed for $\forall a_i$ in $\mathcal{W}_p^*$. This scheme of matching is inspired thanks to the correlation-based technique (based on neighborhood information), that has been promising in the domain of computer vision [106]. To handle the infrequent case where more than one match can give rise to multiple values of r_i^*, we consider the value corresponding to the minimum $d(a_i, r_i^*)$.

Moreover, for values of indices a_i and r_i outside their respective ranges $(w+1, n_T - r - w - 1)$ and $(w+1, n_p - r - w - 1)$, we see that the windows / segments do not completely encompass $2w+1$ sample points. In such cases, we consider padding the first and last sample points of the signatures S_p and S_T, with w repetitions of their corresponding feature vectors. In this way, we ensure matching of segments around each a_i^{th} sample point of test signature S_T along the warping path $\mathcal{W}_p^*$. The end result of the above process is another set of $l_{\mathcal{W}_p^*}$ alignments between test signature S_T and reference signature S_p, denoted by $\{(a_1, r_1^*), (a_2, r_2^*), ..., (a_{l_{\mathcal{W}_p^*}}, r_{l_{\mathcal{W}_p^*}}^*)\}$. On similar lines to (a_i, b_i), the pair (a_i, r_i^*) refers to the cell in the cost matrix, corresponding to the a_i^{th} row and $(r_i^*)^{th}$ column.

As a toy-example for the computation of r_i^*, let us consider the Figure 3.6(a) where-in the



(a)

(b)

Figure 3.6: A toy example for computation of r_i^*. (a) Depiction of a warping path, subsequent to a DTW match between signatures. The alignments are assumed to go through the contiguous cells $\{(1,1),(2,2),(3,3),(3,4),(4,5)......(n_T-r-1,n_p-r-1)\}$. (b) Illustration of the matching scheme formulated in Equation 3.10

warping path from a DTW match between two signatures is assumed to pass through the alignments $\{(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4), ..., (a_{l_{\mathcal{W}_p^*}}, b_{l_{\mathcal{W}_p^*}})\} = \{(1, 1), (2, 2), (3, 3), (3, 4), ..., (n_T - r - 3, n_p - r - 4), (n_T - r - 3, n_p - r - 3), (n_T - r - 2, n_p - r - 2), (n_T - r - 1, n_p - r - 1)\}$ on the cost matrix.

Let us for an illustration, refer to the DTW based alignment $(a_5, b_5) = (4, 5)$. Our goal now is to compute the index r_5^* corresponding to the alignment (a_5, r_5^*) [1] To this effect, we assume a window of odd size (say three) around the fourth sample point in S_T (as shown in Figure 3.6(b)) and search for the most similar window segment of same size in S_p. For illustration, let us presume that out of all possible window segments of size three, the segment around the eighth sample point in S_p provide the closest match (as obtained from Equation 3.10). Accordingly, we get the value of index $r_5^* = 8$, so that $(a_5, r_5^*) = (4, 8)$, corresponds to the alignment obtained from the match in Equation 3.11 based on neighborhood information. Note that, for this toy example illustration, $(a_5, r_5^*) \neq (a_5, b_5)$.

In general, based on the definitions of the alignments (a_i, b_i) and (a_i, r_i^*), we can infer the following:

- Both b_i and r_i^* refer to the index in S_p.
- The warping path of DTW always passes through the alignment (a_i, b_i) $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$ in the cost matrix and is obtained by using dynamic programming.
- The index r_i^* in reference signature S_p is obtained from a match based on neighborhood information. Its value may not always correspond to the index b_i in S_p, so that the relation $d(a_i, b_i) = d(a_i, r_i^*)$ $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$, is not always true.
- It is not mandatory for the warping path of DTW to always pass through the alignment (a_i, r_i^*).

[1] For the present discussion, we are assuming $i = 5$, so that $(a_i, b_i) = (a_5, b_5)$ and $(a_i, r_i^*) = (a_5, r_5^*)$.

3.5.2 Derivation of warping path score

Based on the preceding discussion, we observe two alignments for the a_i^{th} sample point of the test signature S_T, namely (a_i, b_i) and (a_i, r_i^*). The question we wish to address at this juncture is on how to utilize them, together with their respective dissimilarity costs $d(a_i, b_i)$ and $d(a_i, r_i^*)$ for the problem of verifying online signatures. Accordingly, we propose a measure based on (a_i, b_i) and (a_i, r_i^*) for $1 \leq i \leq l_{\mathcal{W}_p^*}$ to separate the genuine signatures from the forgery better.

To begin with, we consider the absolute value of the differences $d(a_i, b_i) - d(a_i, r_i^*)$, for $1 \leq i \leq l_{\mathcal{W}_p^*}$. We refer to each such term as 'feature distortion' in this work. When matching a genuine test signature S_T against a reference signature S_p, owing to the high degree of similarity, the values $d(a_i, b_i)$, $d(a_i, r_i^*)$ of the alignments (a_i, b_i) and (a_i, r_i^*) are close to each other for most parts of the trace. This in turn suggests most of the feature distortion terms $|d(a_i, b_i) - d(a_i, r_i^*)|$ to be low. The contrary is true when a forgery test signature is compared against a reference signature. In this case, each of the feature distortion terms are likely to be higher. Accordingly, we define the average feature distortion for the p^{th} reference signature S_p (by considering the number of aligned pairs falling on the warping path $\mathcal{W}_p^*$), as follows:

$$d_{21}^p = \frac{1}{l_{\mathcal{W}_p^*}} \sum_{i=1}^{l_{\mathcal{W}_p^*}} |d(a_i, b_i) - d(a_i, r_i^*)| \tag{3.12}$$

In addition, for a match of genuine test signature S_T against the reference signature S_p, the index r_i^* in S_p is likely to be in the vicinity of index b_i, for $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$. We define the absolute value of the deviation of r_i^* from b_i (namely, $|b_i - r_i^*|$) as the 'displacement' term in this proposal. Analogous to Equation 3.12, we average across the 'displacements' as follows:

$$d_{22}^p = \frac{1}{l_{\mathcal{W}_p^*}} \sum_{i=1}^{l_{\mathcal{W}_p^*}} |b_i - r_i^*| \tag{3.13}$$

It is worth reminding here that both the indexes b_i and r_i^* correspond to the reference signature S_p under consideration. Coming to the trend of d_{22}^p, its value in general is likely to be low for a genuine-to-reference signature comparison and higher for a forgery-to-reference signature match.

Our proposed warping path score is the sum of average feature distortion and average displacement defined as:

$$d_2^p = d_{21}^p + d_{22}^p \tag{3.14}$$

However, we need to ensure that the values d_{21}^p and d_{22}^p are in comparable numerical range. For this, we normalize each of the feature distortion terms $|d(a_i, b_i) - d(a_i, r_i^*)|$ in d_{21}^p using a factor D_i defined as

$$D_i = \max_{1 \leq j \leq n_p - r - 1} d(a_i, j) \quad \forall i, 1 \leq i \leq \mathcal{W}_p^* \tag{3.15}$$

Likewise, the displacement terms $|b_i - r_i^*|$ in d_{22}^p are normalized with $n_p - r - 1$, the number of sample points in reference signature S_p. We accordingly rewrite Equation 3.14 as:

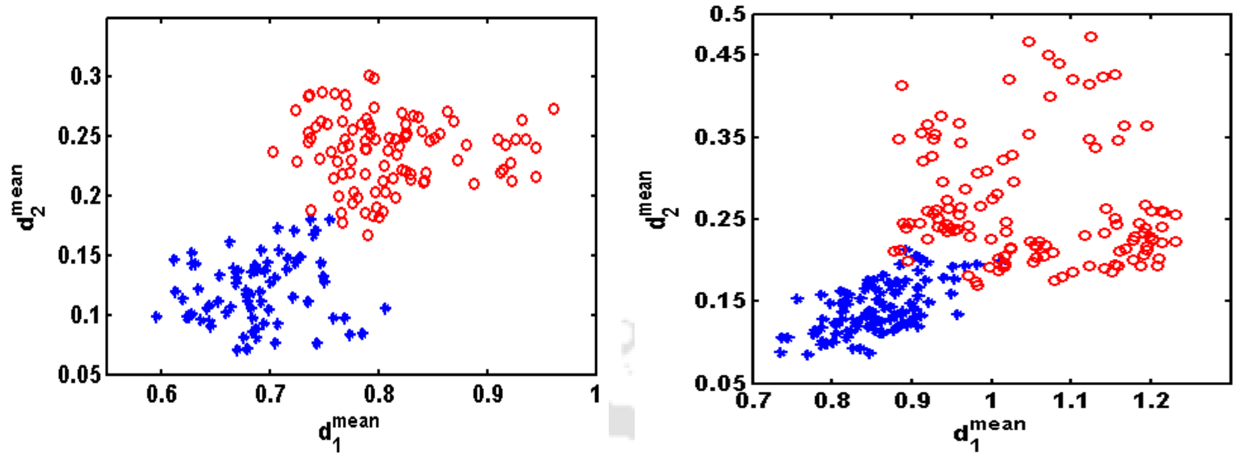
$$d_2^p = \frac{1}{l_{\mathcal{W}_p^*}} \left(\sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{|d(a_i, b_i) - d(a_i, r_i^*)|}{D_i} + \sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{|b_i - r_i^*|}{n_p - r - 1} \right) \tag{3.16}$$

3.5.3 Fusion

We investigate in this sub-section on whether a conjunction of the warping path score (d_2) with that of the DTW (d_1) can help improve the verification efficacy of our proposal. Given a set of N reference signatures of a user, we get values of d_1 and d_2 denoted by $\{d_1^1, d_1^2, ..., d_1^N\}$ and $\{d_2^1, d_2^2, ..., d_2^N\}$ respectively. We first average the scores as follows:

$$d_1^{mean} = \frac{1}{N} \sum_{p=1}^{N} d_1^p$$
$$d_2^{mean} = \frac{1}{N} \sum_{p=1}^{N} d_2^p \tag{3.17}$$

In order to analyze the trend of values of d_1^{mean} and d_2^{mean}, we represent it as a two dimensional plot for the genuine and skilled forgery test signatures of a user from the SVC-2004 and MCYT-100 database respectively (refer Figures 3.7(a) and (b)). The experimental protocol discussed in sub-section 3.7.1 is used in generating these plots, with the values of d_1^{mean} and d_2^{mean}



(a) (b)

Figure 3.7: A two-dimensional distribution of the normalized DTW and warping path scores on the genuine and skilled forgery signatures (depicted in blue and red colors respectively) of an user from the (a) SVC-2004 and (b) MCYT-100 database. The experimental protocol discussed in sub-section 3.7.1 is used in generating these plots.

recorded over a set of ten enrolment trials. We see that the exclusive use of either of the scores present a noticeable overlap between the genuine and skilled forgery signatures. Nevertheless, we can consider exploring out on utilizing the contributions of both of them for authentication, through a combination scheme. In such cases, we say the scores are complementary [2]. The main idea behind the score combination is to reduce the extent of overlap between the genuine and skilled forgery signatures, thus improving the verification system. A simple choice of combination that we employ is the sum rule, defined by:

$$d_T = d_1^{mean} + d_2^{mean} \tag{3.18}$$

Prior to combining the scores, they are separately mapped to a similarity value in the range $[0, 1]$ using the sigmoidal function. The verification system accepts the test sample S_T if d_T is less than a threshold. Otherwise, it rejects it as a forgery.

Apart from using the average, we experimented on other strategies of using the sum rule for fusion (namely by considering the minimum and maximum of the combined scores), as outlined

[2]It may be mentioned in passing that when the distribution of d_2^{mean} scores between the genuine and skilled forgery signatures do not overlap, the use of d_2^{mean} alone would suffice for verification. In such cases, information of d_1^{mean} does not complement to that of d_2^{mean} .

below:

$$
\begin{aligned}
d_T &= \min_{1 \leq p \leq N} d_1^p + d_2^p \\
d_T &= \max_{1 \leq p \leq N} d_1^p + d_2^p
\end{aligned} \tag{3.19}
$$

The experimental results on these schemes are presented in the Section 3.8.

For better clarity, a pseudo-code is presented that summarizes the derivation of the warping path score in the proposed signature verification system for a test signature S_T (refer Algorithm 1).

3.6 Demonstration of the warping path score for verification

In this Section, we demonstrate the use of the proposed warping path score derived in subsection 3.5.2 to the process of authentication. We consider the match of a genuine and skilled forgery signature in Figures 3.8(b) and (c) against a reference genuine signature shown in Figure 3.8(a). To simplify the discussion, we consider only one reference signature S_1 of an user to be enrolled to the system, so that $p = 1$. The signatures presented in the illustrations correspond to an user from the SVC-2004 database.

The scores d_1 from the DTW match are very close (0.70 and 0.65), and may not provide adequate discrimination (Figures 3.8(d) and (e)). Moreover, the genuine to reference signature score match is higher than that of the skilled forgery signature - contradicting to what we should expect! Based on the empirical threshold, it is very likely for the genuine signature to be falsely rejected as forgery and / or vice-versa. A threshold less than 0.65 may falsely reject the genuine signature of Figure 3.8(b) to a forgery, while the forgery signature of Figure 3.8(c) can get falsely accepted as genuine, with a higher threshold (greater than 0.70). In addition, any threshold between 0.65 and 0.70 will lead to an incorrect authentication of both signatures. Hence, irrespective of the threshold set, there will be an erroneous decision made by solely relying on the score d_1.

Algorithm 1 Proposed signature verification algorithm

Input: Test signature S_T ; a set of N enrolled reference signatures of an user denoted as $\{S_1, S_2, ..., S_N\}$

For $p = 1 : N$

- Derive the sequence of point based feature vectors in Section 3.3 corresponding to S_T and S_p

- Perform the DTW match of the test signature S_T with the p^{th} reference signature, S_p of an user to get d_1^p score. (Refer Section 3.4.)

- Extract the cells (a_i, b_i) in the warping path $\mathcal{W}_p^*$ from the DTW cost matrix by back-tracing.

- **For** $i = 1 : l_{\mathcal{W}_p^*}$ % $l_{\mathcal{W}_p^*}$ is the number of aligned pairs on $\mathcal{W}_p^*$ %
  Compute the alignment (a_i, r_i^*) using Equation 3.10 described in sub-section 3.5.1.
  End

  % Computation of the warping path score discussed in sub-section 3.5.2

- Compute the normalized average distortion term: $d_{21}^p = \frac{1}{l_{\mathcal{W}_p^*}} \sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i}$ where $D_i = \max\limits_{1 \le j \le n_p - r - 1} d(a_i, j)$

- Compute the normalized average displacement term: $d_{22}^p = \frac{1}{l_{\mathcal{W}_p^*}} \sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{|b_i - r_i^*|}{n_p - r - 1}$

- **Warping path score** : $d_2^p = d_{21}^p + d_{22}^p$

End

- Fuse the N scores $\{d_1^p\}_{p=1}^N$ and $\{d_2^p\}_{p=1}^N$ with a combination scheme (refer subsection 3.5.3).

- Use the fused score for authentication.

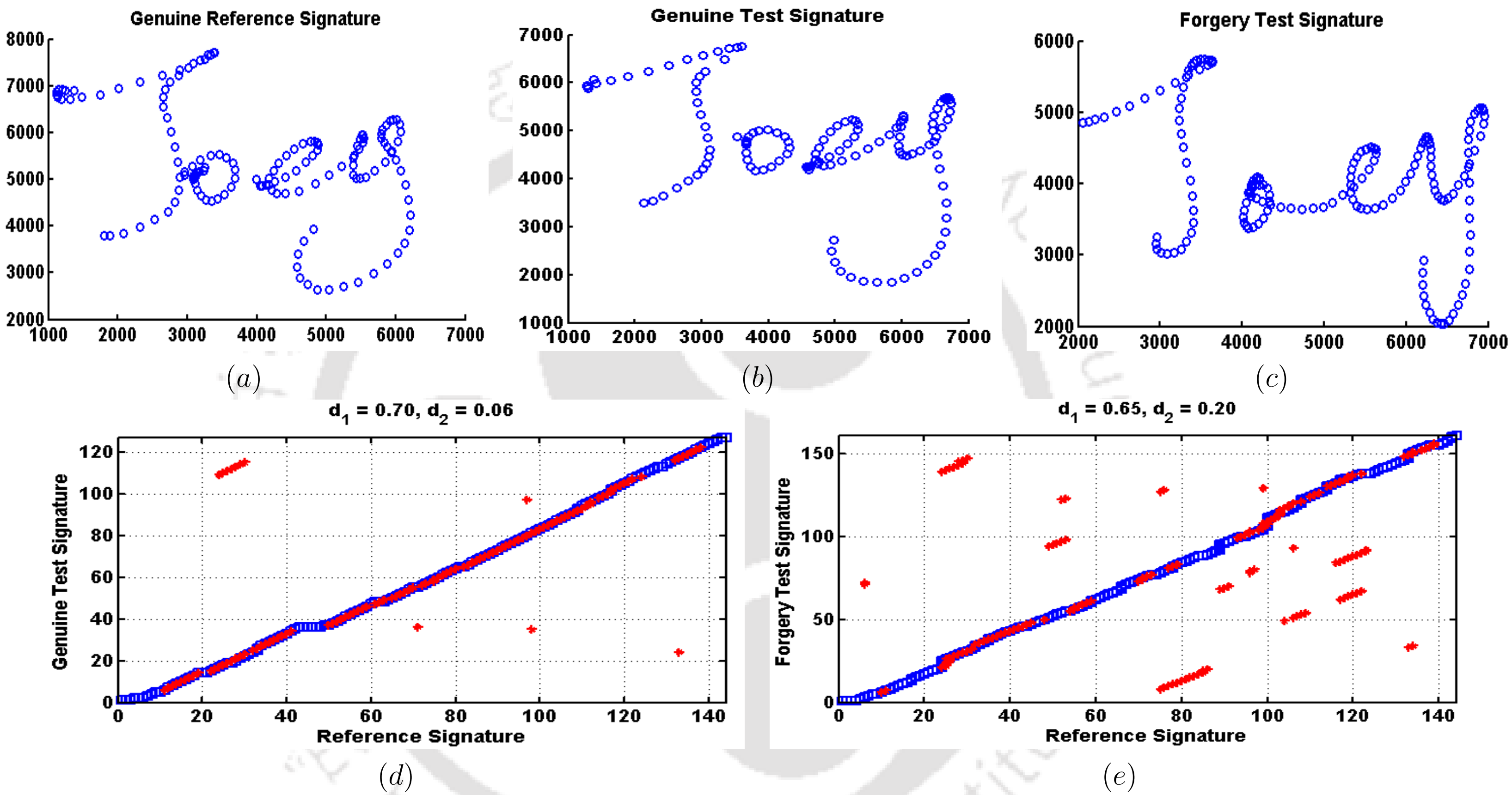


Figure 3.8: An illustration of the effectiveness of warping path score d_2 for verification. The sub-figure (a) depicts a sample of reference signature (from an user of the SVC-2004 data-base) enrolled into the system. Sub-figures (b) and (c), correspond to a sample of genuine and skilled forgery signature, that are matched against this reference signature. In sub-figures (d) and (e) we present a snapshot of the warping path alignments (a_i, b_i) (shown in 'blue') along with the alignments (a_i, r_i^*) (depicted in 'red'), for the case when the signature patterns (b) and (c) are matched to (a) respectively. It can be noted that the DTW scores d_1 of the genuine-reference signature match (sub-figure (d)) are higher to that forgery-reference signature match (sub-figure (e)), contradicting to what we expect!. The warping score d_2, on the other hand, attempts to discriminate the signatures better. Note that in comparison to d_1, the d_2 score for the genuine signature match in sub-figure (d) is lower compared to that of the forgery signature match in sub-figure (e). Here, a window of size 11 is employed for calculating r_i^*.

The above issue is alleviated by the proposed warping path score d_2, which is observed to be contrasting for the genuine and forgery signature respectively (their values being 0.06 and 0.20). Note that in comparison to d_1, the d_2 score for the genuine signature match in Figure 3.8(d) is lower compared to that of the forgery signature match in Figure 3.8(e). In addition, the application of the sum rule combiner on the scores provide values of 0.76 and 0.85 for the genuine and forgery signature match with the reference signature.

The trend in the value of d_2 is attributed to the distribution of the alignments (a_i, r_i^*), (depicted using 'red'), with respect to the warping path alignments (a_i, b_i) (shown in 'blue'). In case of a genuine signature match against a reference signature, we note from the Figure 3.8(d) that the alignments (a_i, r_i^*) either coincide or lie very close to the DTW-based path alignments (a_i, b_i) at most parts of the trace. A window of size 11 is used to compute the index r_i^* $\forall i$.

A critical analysis of the warping path (of the genuine to reference signature DTW match) in Figure 3.8(d) suggest that 63.71 % of the alignments (a_i, b_i) (corresponding to 79 out of 124 aligned pairs) do not contribute to the summations in Equation 3.16. This implies that for those parts of the trace, both alignments (a_i, b_i) and (a_i, r_i^*) coincide, and are exactly matched, so that $b_i = r_i^*$ and $d(a_i, b_i) = d(a_i, r_i^*)$. Subsequently, on accumulating terms of the type $|b_i - r_i^*|$ along the entire warping path in Equation 3.13, we get a low value for the average displacement d_{22}. This trend is however, not predominant in the warping path of the skilled forgery to reference signature DTW match shown in Figure 3.8(e). Here, a lower percentage of 27.85 % of the alignments (a_i, b_i) (44 out of 158 aligned points) along the warping path provide an exact match for the alignment (a_i, r_i^*), thus leading to a high value for d_{22}.

In addition compared to Figure 3.8(e), the dissimilarity costs $d(a_i, b_i)$ along the warping path of a genuine to reference signature match in Figure 3.8(d) either coincide with or are closer to the values $d(a_i, r_i^*)$, thus contributing to lower feature distortion values d_{21} in the computation of the warping score d_2 . However with the large size of the cost matrix in Figures 3.8(d) and (e), the alignments (a_i, b_i) and (a_i, r_i^*) with their corresponding dissimilarity values $d(a_i, b_i)$ and $d(a_i, r_i^*)$ cannot be explicitly shown in their respective cells.

As another illustration, we demonstrate the usefulness of the warping path score by considering signatures from an user of the MCYT-100 database (refer Figure 3.9). Here again, with regards to DTW, a similar trend is noted - with the genuine to reference signature match ($d_1 = 1.1$) being higher to that of the forgery to reference signature match ($d_1 = 0.98$). Hence we rely on the warping path characteristics for ensuring that the signatures get correctly verified. Empirically, we observe that 47.37% of the alignments (a_i, b_i) (corresponding to 72 out of 152 aligned pairs) in the warping path (of the genuine to reference signature DTW match) in Figure 3.9(d) do not contribute to the summations in Equation 3.16. This in turn leads to a low value for the average displacement d_{22}. Contrary to this, the warping path of the skilled forgery to reference signature DTW match shown in Figure 3.9(e) has a relatively lower percentage (19.57 %) of the alignments, thus leading to a high value for d_{22}. On a similar note, the dissimilarity costs $d(a_i, b_i)$ along the warping path of a genuine to reference signature match in Figure 3.9(d) either coincide with or are closer to the values $d(a_i, r_i^*)$, resulting in lower values of d_{21} component in the warping score d_2. The sum rule combiner on the d_1 and d_2 scores provide values of 1.31 and 1.46 for the genuine and forgery signature match with the reference signature - thus leading to a correct decision for the signatures of Figure 3.9(b) and (c).

To validate further on the preceding discussions pertaining to the illustrations, we depict the discriminative nature of the warping path score by representing their components separately through a histogram based approach in the following subsection.

3.6.1 Histogram based analysis of values contributing to DTW and warping path score

To begin with, we plot the normalized histograms of the dissimilarity values $d(a_i, b_i)$ $\forall i$ along the warping paths for the illustration in Figure 3.8. Figures 3.10(a) and (b) depict the plots for the case of the DTW match between the genuine and skilled forgery signature (in Figures 3.8(b) and (c)) with the reference signature in Figure 3.8(a) respectively. Similarly, the normalized histograms of the sum of the feature distortion and displacement terms, $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i} + \frac{|b_i-r_i^*|}{n_p-r-1}$ $\forall i$ (contributing to the warping path score d_2) are shown in Figures 3.10(c) and (d). Comparing

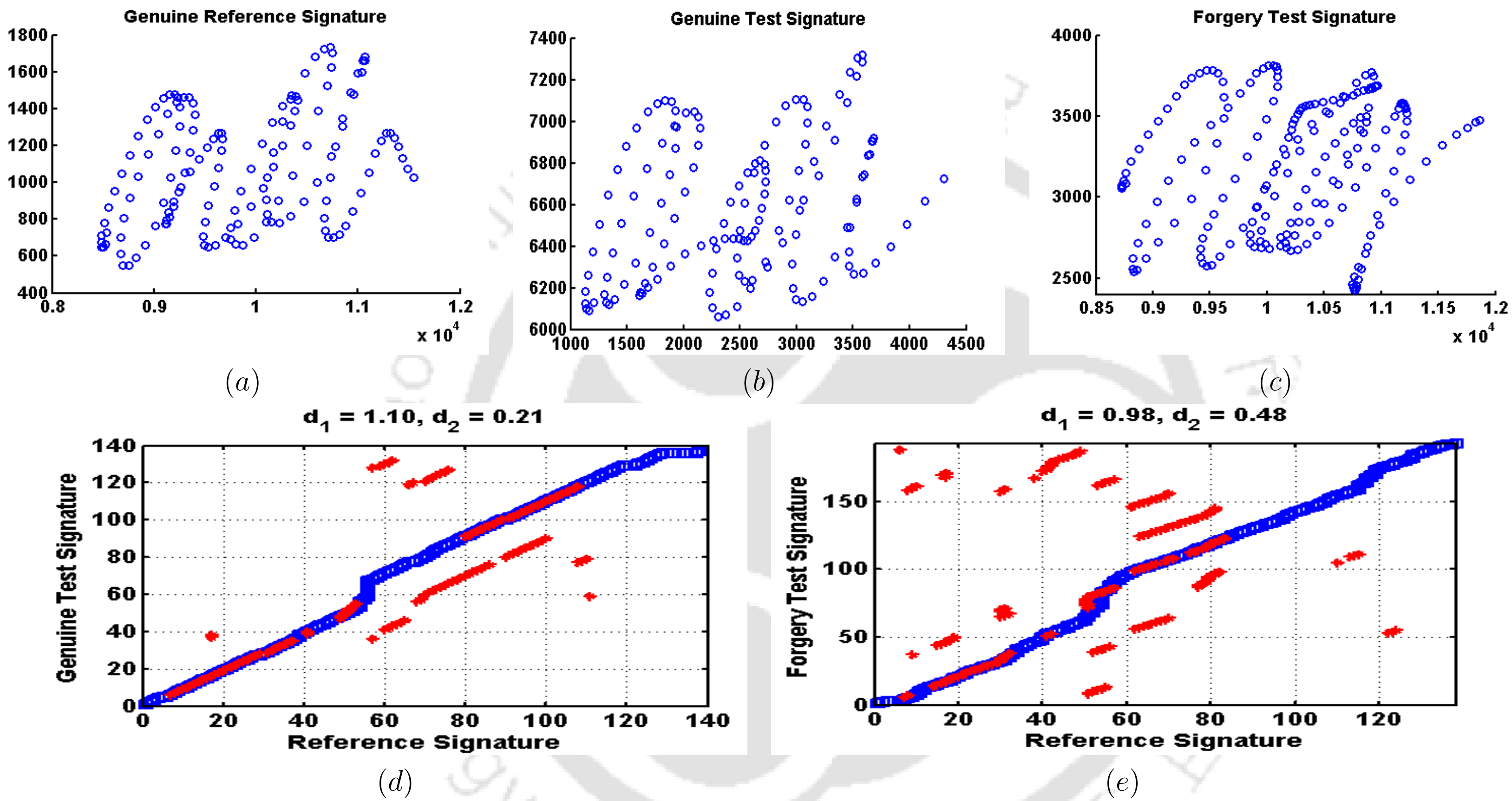


Figure 3.9: An illustration of the effectiveness of warping path score d_2 for verification. The sub-figure (a) depicts a sample of reference signature (from an user of the MCYT-100 Database) enrolled into the system. Sub-figures (b) and (c), correspond to a sample of genuine and skilled forgery signature, that are matched against this reference signature. In sub-figures (d) and (e) we present a snapshot of the warping path alignments (a_i, b_i) (shown in 'blue') along with the alignments (a_i, r_i^*) (depicted in 'red'), for the case when the signature patterns (b) and (c) are matched to (a) respectively. It can be noted that the DTW scores d_1 of the genuine-reference signature match (sub-figure (d)) are higher to that forgery-reference signature match (sub-figure (e)), contradicting to what we expect!. The warping score d_2, on the other hand, attempts to discriminate the signatures better. Note that in comparison to d_1, the d_2 score for the genuine signature match in sub-figure (d) is lower compared to that of the forgery signature match in sub-figure (e). Here, a window of size 11 is employed for calculating r_i^*.

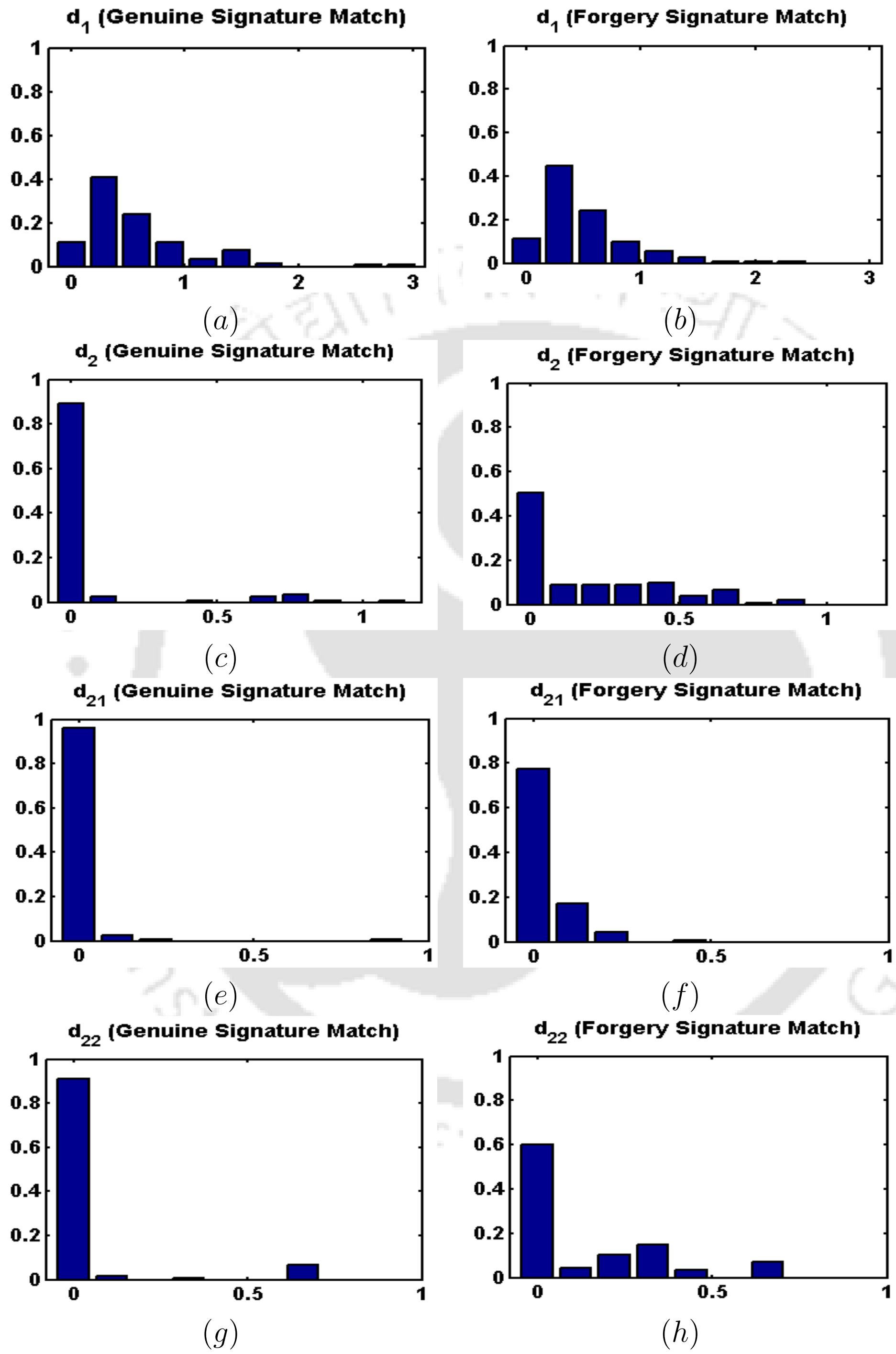


Figure 3.10: (a-d): Normalized histograms of the dissimilarity values $d(a_i, b_i)$ (sub-figures (a),(b)) and the terms $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i} + \frac{|b_i-r_i^*|}{n_p-r-1}$ (sub-figures (c),(d)) along the warping path, resulting from DTW match of the genuine and skilled forgery signature in Figure 3.8(b)-(c) with the reference signature of Figure 3.8(a). The sub-figures (e)-(h) depict the normalized histograms of the feature distortion values $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i}$ (sub-figures (e),(f)) and the displacement $\frac{|b_i-r_i^*|}{n_p-r-1}$ (sub-figures (g),(h))

the sub-figures (a) and (b), the bin indices are observed to be quite similar - with the computed dissimilarity of the two histograms using City block distance being a low value of 0.16. Relative to this, the histograms in Figures 3.10(c) and (d) corresponding to the warping path scores for the genuine and skilled forgery signature match have a high dissimilarity score of 0.82. This measure in turn suggests its discriminative nature with regards to the verification problem.

In the Figures 3.10(e) to (h), we present the normalized histograms separately for the feature distortion, $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i}$ and displacement terms $\frac{|b_i-r_i^*|}{n_p-r-1}$ $\forall i$, resulting from the DTW match of the genuine and skilled forgery signature in Figure 3.8(b) and (c) with the reference signature of Figure 3.8(a) respectively. These plots provide us information on the impact that the individual scores d_{21} and d_{22} have on the verification process. In particular, we empirically note that the histograms in Figure 3.10(e) and (f) corresponding to the d_{21} component have a dissimilarity score of 0.45 while those of Figure 3.10(g) and (h) pertaining to the d_{22} component have a score of 0.66. Clearly, these distances are higher than 0.16 - the value from the histogram match of Figure 3.10(a) and (b) based on the DTW score d_1. This in turn bolsters the utility of our devised scores for verification.

We now consider a similar histogram based analysis for the illustration of Figure 3.9, that employs signatures from an user of the MCYT-100 database. Accordingly, Figures 3.11(a) and (b) depict the plots for the case of the DTW match between the genuine and skilled forgery signature (in Figures 3.9(b) and (c)) with the reference signature in Figure 3.9(a) respectively. The bin indices corresponding to these histograms is similar with a City Block distance of 0.23. Nonetheless, we see that visually, the histogram of the values contributing to the scores d_2, d_{21} and d_{22} (refer Figures 3.11(c)-(h)), enhance the discrimination between genuine and forgery signature. In particular, compared to 0.23, the histograms of the distance values in the Figures 3.11(c) and (d) contributing to the warping path scores d_2 of the genuine and skilled forgery signature match have a high dissimilarity score of 0.59.

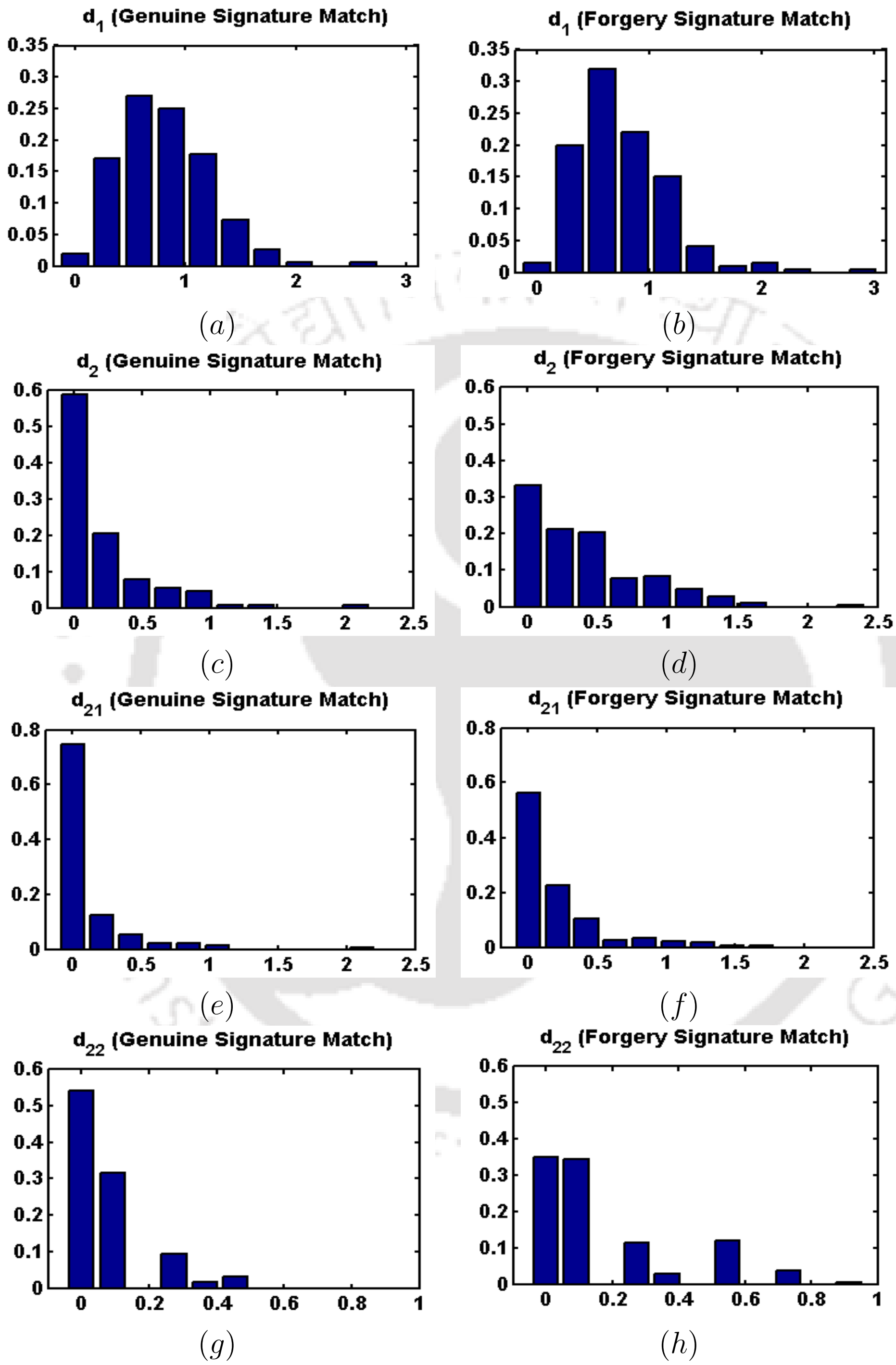


Figure 3.11: (a-d): Normalized histograms of the dissimilarity values $d(a_i, b_i)$ (sub-figures (a),(b)) and the terms $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i} + \frac{|b_i-r_i^*|}{n_p-r-1}$ (sub-figures (c),(d)) along the warping path, resulting from DTW match of the genuine and skilled forgery signature in Figure 3.9(b)-(c) with the reference signature of Figure 3.9(a). The sub-figures (e)-(h) depict the normalized histograms of the feature distortion values $\frac{|d(a_i,b_i)-d(a_i,r_i^*)|}{D_i}$ (sub-figures (e),(f)) and the displacement $\frac{|b_i-r_i^*|}{n_p-r-1}$ (sub-figures (g),(h))

Database	# samples enrolled	# samples to be verified
SVC-2004	200	1400
MCYT-100	500	4500

Table 3.1: Illustration of the number of samples used for each repetition of experiments of the SVC-2004 and MCYT-100 database.

3.7 Experimental framework

In this Section, we present an outline of the enrollment and evaluation protocol adopted in our experiments (subsections 3.7.1 and 3.7.2).

3.7.1 Enrollment Protocol

In most experiments in this thesis, the following protocol is used for the SVC-2004 database - from each of the 40 users, we randomly select a set of five of his / her genuine signatures for enrollment as reference signatures. The signatures are chosen from the first session, keeping in line with the set up used in the signature competition [17]. The remaining 15 genuine signatures (not selected for enrollment) and 20 skilled forgeries of the users are considered for evaluating the performance of the verification system. Likewise, for the MCYT-100 database, we randomly select five genuine signatures from each of the 100 users for enrolment as reference signatures. The remaining 20 genuine signatures and 25 skilled forgeries of these users are employed for testing the efficacy of our proposal.

The procedure of selection of the signatures for enrollment (in either database) is performed over a set of ten trials. The error rates (obtained over the trials) are averaged and reported for the experiments described. For sake of clarity, Table 3.1 presents an illustration of the number of samples used for each trial / repetition of experiments of the SVC-2004 and MCYT-100 database.

3.7.2 Evaluation Protocol

As mentioned in subsection 1.3.4 of the thesis, while evaluating an online signature verification system, we come across two types of errors. The percentage of genuine signature that get rejected by the system constitute the false rejection rate (FRR). The percentage of forgeries that get access to the system is the false acceptance rate (FAR). In signature verification, the system performance is evaluated with the Equal Error Rate (EER) corresponding to the point at which the FAR and FRR are equal.

In this work, we provide EER values for both user and common threshold settings. In the former, we use only the matching scores corresponding to the test signatures of the claimed user in question to compute the error. Thereafter, the EERs obtained across all the users enrolled in the system are averaged for performance evaluation.

Contrary to the above, in the common threshold set-up, the matching scores corresponding to the signatures being tested from all the users are pooled together to compute the EER. However, a normalization of scores is done to ensure that their values are in a comparable range across the enrolled users. Accordingly, corresponding to an user, we consider subtracting the matched score of a test signature from that of the mean obtained from the set of his / her enrolled signatures. Assuming N enrolled reference signatures, we compute the mean from the set of $\binom{N}{2}$ scores. Thereafter, the mean subtracted score is mapped to a similarity value in the range $[0, 1]$ by a sigmoidal function and used for computing the EER.

3.8 Results and Discussion

For the results outlined in this thesis, we denote the average of the EERs computed over the set of ten trials (denoted as MEER) as the measure of performance. The baseline system used is the one that employs the normalized DTW score in Section 3.4 for verification (abbreviated as $BL-DTW$ system). It is with respect to this system that efficacy of our proposal (the WP and $FUS1$ systems) is demonstrated.

3.8.1 Influence of spacing parameter value r

To begin with, we evaluate the performance of the $BL - DTW$ system on the modified features characterized by different values of the spacing parameter r. The second and fifth column of Table 3.2 outline the findings for r between one to ten in step of one for the SVC-2004

Table 3.2: MEER (in %) on the genuine and skilled forgeries of the SVC-2004 data-base, with features modified using different values of spacing parameter r. For this experiment, the City Block distance (L_1 norm) is used to compute the entries of the DTW cost matrix.

r	Common-threshold			User-threshold		
	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
1	20.33	10.54	11.39	13.28	5.29	4.38
2	15.53	10.2	9.45	8.46	4.78	3.15
3	13.05	10.03	8.72	5.86	4.91	2.78
4	11.66	10.08	8.08	4.96	4.93	2.66
5	11.11	9.95	7.80	4.41	4.32	2.53
6	10.71	10.29	7.99	4.16	4.26	2.58
7	10.71	10.29	8.15	4.28	4.14	2.63
8	10.60	10.15	8.24	4.25	4.30	2.69
9	10.35	10.52	8.30	4.30	4.18	2.85
10	10.17	10.10	8.09	4.12	4.19	2.74

database. The MEER (in %) is computed with regards to the genuine and skilled forgeries, that are compared against the reference signatures. As expected, the MEER obtained from using user threshold (fifth column) is lower to that of the common threshold (second column). Yet, an interesting trend observed is with regards to the MEERs of $BL-DTW$ for varying values of r, with both common and user threshold setting. For $r = 1$, the verification efficacy is low. Here, we use consecutive sample data points for deriving the features, which many a times, may be noisy due to the possibility of unintentional trembling of hand / jitter during the writing process. However, the improvement in verification performance is observed at higher values of r. In particular beyond $r = 4$, the MEERs are quite comparable to one another.

For the MCYT-100 database, a similar trend of reduced MEERs of the $BL-DTW$ system with increased value in spacing parameter r can be noted from the results in the second and fifth column of Table 3.3.

Table 3.3: MEER (in %) on the genuine and skilled forgeries of the MCYT-100 data-base, with features modified using different values of spacing parameter r. For this experiment, the City Block distance (L_1 norm) is used to compute the entries of the DTW cost matrix.

	Common-threshold			User-threshold		
r	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
1	10.94	4.45	4.29	7.40	1.84	1.79
2	8.23	3.65	3.44	4.96	1.39	1.36
3	6.91	3.28	3.19	3.95	1.31	1.26
4	6.23	3.10	2.91	3.44	1.20	1.16
5	5.87	3.08	2.84	3.11	1.22	1.18
6	5.61	3.04	2.76	2.79	1.28	1.15
7	5.39	3.26	2.82	2.64	1.33	1.18
8	5.28	3.25	2.88	2.54	1.38	1.20
9	5.09	3.25	2.92	2.44	1.41	1.20
10	5.03	3.34	2.95	2.44	1.45	1.26

3.8.2 Influence of the warping path score

The efficacy of the proposed system for the SVC-2004 database is presented in Table 3.2. Here, we see that the fusion with the warping path score using the sum rule combiner ($FUS1$ system), brings down the MEER (as seen from fourth and seventh columns). The Equation 3.18 is used to implement the sum rule. In particular, an MEER to as low as 7.80% and 2.53% is obtained with a spacing parameter value of $r = 5$ for the common and user threshold settings respectively. We hereinafter consider this value of the spacing parameter for the experiments described for the SVC-2004 database.

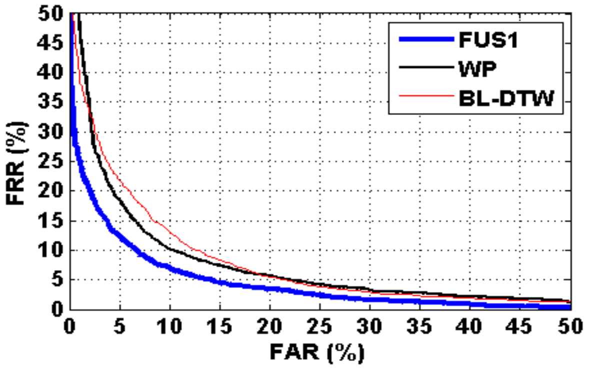
With regards to the MCYT-100 database (Table 3.3), we again see that the warping path score (WP system) is effective in bringing the MEERs to an average of around 3.07% (common threshold) and 1.23% (user threshold) for values of the spacing parameter r between 4 and 6. In addition, from the fourth and seventh columns, the $FUS1$ system helps in further reducing the MEERs. For the case of user threshold, our verification system achieves a lowest MEER of 1.15 % for the spacing parameter value $r = 6$. A similar trend applies to the common threshold scenario as well - with a MEER of 2.76% for $r = 6$.

The relatively higher reduction in MEERs (compared to SVC-2004 database) is owing to the characteristics of the MCYT-100 database. This database has been collected using real signatures of users (unlike the SVC-2004 database, wherein the users were asked to 'invent' signatures [17, 29]). Therefore, across genuine signatures of an user, there is less amount of intra-class variations. This in turn enables the cost matrix and associated warping paths to have a similar structure, thus making the score d_2 effective for discriminating the genuine from the forgery signatures. Nevertheless, perfect separation of warping path score between genuine and forgery signatures is not guaranteed and hence fusion of scores helps.

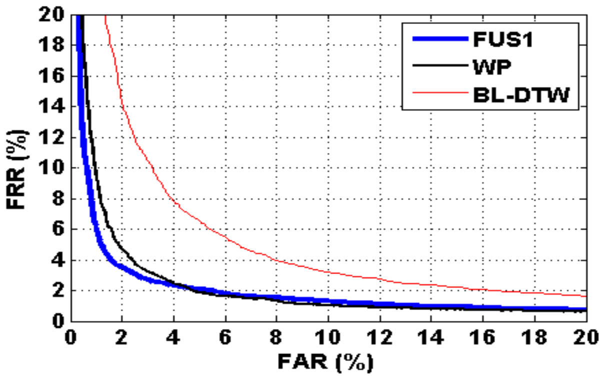
In the results of Tables 3.2 and 3.3, we chose a window of length 11 to compute Equation 3.10. We did experiment using different odd window sizes ranging from one to fifteen. However, across varying sizes, we found very comparable results with the $FUS1$ system outperforming the $BL - DTW$. Empirically, the window size of eleven gave the lowest MEER for the values of the spacing parameter r enumerated in the Tables 3.2 and 3.3. Keeping this in perspective, for the experiments outlined hereinafter in this Chapter, we utilize the same window size.

3.8.3 DET Curves

As a further demonstration to the effectiveness of our proposal, Figure 3.12(a) and (b) provide the DET curves obtained from the tested signatures (using skilled forgery) across all the users of a single trial for the SVC-2004 and MCYT-100 database respectively. A common threshold is used in deriving this curve, which by definition is a two-dimensional measure of verification performance that plots the rate of false rejection (FRR) against the rate of false acceptance (FAR). It is interesting to note that the $FUS1$ system outperforms the $BL-DTW$ in almost all of the points of the DET-curve for both the databases. In addition, for these plots, the value of the spacing parameter being considered for the SVC-2004 and MCYT-100 database are $r = 5$ and $r = 6$ respectively. This choice is made, considering that empirically, they provided the minimum MEER performance with the proposed $FUS1$ system.



(a)



(b)

Figure 3.12: DET curves corresponding to the (a) SVC-2004 and (b) MCYT-100 database, using skilled forgeries, for the common threshold scenario. The plots are obtained from the tested signatures (using skilled forgery) across all the users of a single trial. The number of reference signatures considered is 5.

3.8.4 Influence of the fusion strategies

In this experiment, we explore on the performance of the combination strategies referred to in the Equations 3.18 and 3.19. The results in Table 3.4 for the SVC-2004 database suggest a comparable performance between the mean and minimum based fusion techniques (7.80 % and 9.12% MEER for common threshold, 2.53% and 2.76% MEER for user threshold respectively). Owing to the fact that this database comprises a wide intra-class variation between the genuine signatures of an user, the mean based fusion in a way, aids in smoothing out the intra-class variability by averaging each of the scores d_1 and d_2, over the set of reference signatures and then combining them with the simple sum rule (Equations 3.17 and 3.18). This explains the slight improvement of its verification performance over the minimum based fusion strategy. Also when contrasted with the minimum and mean, the fusion based on the maximum of sum of scores d_1 and d_2 over the set of reference signatures gives a higher MEER of 12.20 % and 4.24 % for common and user thresholds respectively.

Likewise with the MCYT-100 database (Table 3.5), we note a trend similar to that obtained in the SVC-2004 - with the mean strategy outperforming the others.

Table 3.4: MEER (in %) of the sum-rule combination strategies referred to in Equations 3.18 and 3.19 (for the SVC-2004 database) with, spacing parameter value $r = 5$ for feature extraction.

Method	Common Threshold			User Threshold		
	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
Mean	11.11	9.95	7.80	4.41	4.32	2.53
Minimum	12.37	11.33	9.12	4.89	4.45	2.76
Maximum	16.23	13.22	12.20	7.02	6.41	4.24

Table 3.5: MEER (in %) of the combination strategies referred to in Equations 3.18 and 3.19 (for the MCYT-100 database), with spacing parameter value $r = 6$ for feature extraction.

Method	Common Threshold			User Threshold		
	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
Mean	5.61	3.09	2.76	2.79	1.28	1.15
Minimum	6.4	3.75	3.42	2.80	1.49	1.22
Maximum	8.68	5.33	4.47	4.98	2.19	2.12

3.8.5 Influence of Number of Reference signatures

By using the mean based fusion strategy with spacing parameter value $r = 5$ for computation of the features, we evaluate our proposal for different number of reference signatures enrolled to the system for the SVC-2004 database. From Table 3.6, it may be inferred that the $FUS1$ system verifies the authenticity of a user quite effectively with as low as three or four reference signatures for user and common threshold setting respectively. Likewise, for the MCYT-100 database with the mean based fusion strategy and $r = 6$, an MEER to as low as 1.56 % (common threshold) and 0.71% (user threshold) is obtained with 20 reference signatures [3] enrolled to the system (refer Table 3.7). This observation indicates that the proposed methodology is capable of rejecting skilled forgeries better than $BL-DTW$ system.

[3] The results merely suggest the trend of MEER with increasing number of reference signatures. It is to be noted otherwise that having 20 reference signatures for comparison is unrealistic in a large public implementation scenario.

Table 3.6: MEER (in %) of the proposed system when different number of reference signatures from the SVC-2004 database are enrolled, with spacing parameter value $r = 5$ for feature extraction.

# of ref sign	Common Threshold		User Threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
1	22.97	17.23	6.44	4.6
2	14.28	12.83	4.72	3.29
3	12.25	9.34	4.38	2.95
4	11.25	8.48	4.23	2.81
5	11.11	7.80	4.41	2.53
10	10.39	8.02	4.84	2.79

Table 3.7: MEER (in %) of the proposed system when different number of reference signatures from the MCYT-100 database are enrolled, with spacing parameter value $r = 6$ for feature extraction.

# of ref sign	Common Threshold		User Threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
5	5.61	2.76	2.79	1.15
10	4.54	2.35	2.56	1.08
15	4.31	1.77	2.12	0.84
20	4.15	1.56	1.85	0.71

3.8.6 Influence of warping path score on various recursion relation

The dynamic programming recursion relation stated in Equation 3.7 is a basic one. It is quite established from literature that the performance of the DTW verification system according to the function of dynamic programming recursion relation is different from each other [62]. Hence, as an exploration, we demonstrate the efficacy of our approach with two more recursion relations of the DTW as follows:

$$\psi(m,n) = d(m,n) + \min \begin{cases} \psi(m, n-2) \\ \psi(m-1, n-1) \\ \psi(m-2, n) \end{cases} \tag{3.20}$$

Table 3.8: MEER (in %) on the genuine and skilled forgeries of the SVC-2004 data-base - with features proposed using different values of spacing parameter r. The DTW recursive relation in Equation 3.20 is used.

r	Common-threshold		User-threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
1	14.22	10.66	6.49	4.20
2	12.01	9.31	5.12	3.20
3	11.02	9.05	4.47	3.01
4	10.82	8.93	4.28	2.89
5	10.62	8.83	4.29	2.80
6	10.84	9.22	4.44	2.82
7	10.82	9.29	4.52	2.83
8	10.99	9.92	4.57	2.88
9	11.45	10.58	4.78	3.05
10	11.68	10.91	5.01	3.19

$$\psi(m,n) = \min \begin{cases} \psi(m,n-1) + d(m,n) \\ \psi(m-1,n-1) + 2d(m,n) \\ \psi(m-1,n) + d(m,n) \end{cases} \tag{3.21}$$

Recall from Section 3.4 that $d(m,n)$ is the City Block distance between the m^{th} point of test signature S_T with the n^{th} point of reference signature S_p. Also $\psi(m,n)$ corresponds to the cumulative distance up-to the current element in the warping matrix ψ.

The results pertaining to the above mentioned recursions are presented for the SVC-2004 and MCYT-100 databases (refer Tables 3.8 to 3.11). It may be observed that the performance of DTW depends on the recursion function being used. However, our proposal of using the derived score of the warping path does present an improvement over the performance of DTW irrespective of the recursion framework. This is the key take home message from our experimentation.

Table 3.9: MEER (in %) on the genuine and skilled forgeries of the MCYT-100 data-base - with features proposed using different values of spacing parameter r. The DTW recursive relation in Equation 3.20 is used.

r	Common-threshold		User-threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
1	6.87	3.44	2.01	1.30
2	4.82	3.11	1.68	1.18
3	4.12	3.03	1.66	1.08
4	3.59	2.99	1.57	1.04
5	3.55	2.97	1.53	1.05
6	3.47	2.98	1.52	1.07
7	3.34	3.09	1.57	1.08
8	3.44	3.12	1.57	1.12
9	3.80	3.18	1.59	1.15
10	4.28	3.31	1.61	1.16

Table 3.10: MEER (in %) on the genuine and skilled forgeries of the SVC-2004 data-base - with features proposed using different values of spacing parameter r. The DTW recursive relation in Equation 3.21 is used.

r	Common-threshold		User-threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
1	28.57	10.68	22.48	5.32
2	23.45	10.13	16.62	4.67
3	20.38	9.97	13.35	4.24
4	18.38	9.94	11.65	4.18
5	17.07	9.86	10.05	4.16
6	16.65	10.30	8.76	4.28
7	15.82	10.35	8.23	4.35
8	15.59	10.92	8.17	4.38
9	16.45	11.68	8.38	4.45
10	16.68	11.81	8.51	4.49

Table 3.11: MEER (in %) on the genuine and skilled forgeries of the MCYT-100 data-base - with features proposed using different values of spacing parameter r. The DTW recursive relation in Equation 3.21 used.

r	Common-threshold		User-threshold	
	$BL-DTW$ system	$FUS1$ system	$BL-DTW$ system	$FUS1$ system
1	17.71	5.32	13.62	2.19
2	16.42	4.37	12.24	1.68
3	15.64	3.98	11.56	1.42
4	15.18	3.69	11	1.35
5	14.40	3.58	10.34	1.27
6	13.78	3.61	9.9	1.26
7	14.31	3.64	9.41	1.31
8	14.47	3.80	9.46	1.36
9	14.61	4.06	9.51	1.37
10	15.18	4.32	9.62	1.43

3.8.7 Influence of dissimilarity measure

It may be recalled from our description of the DTW algorithm in Section 3.4 that the City Block distance for the computation of the cost matrix was just a choice being made in this work. Stated in another way, in lieu of it, we could have as well considered any other norm (such as Euclidean or the like). Accordingly, the experiments in this subsection aim at demonstrating the impact of the L_2-norm on the verification performance of $BL-DTW$ and $FUS1$ systems. By definition, the L_2-norm or the Euclidean distance can be written as :

$$d(m,n) = \sum_{k=1}^{11} (f_T^m(k) - f_p^n(k))^2 \tag{3.22}$$

Tables 3.12 and 3.13 presents the results of this experiment for the SVC-2004 and MCYT-100 databases respectively. Clearly, we see improvement in the $FUS1$ system over the $BL-DTW$ across all values of the spacing parameter r. As a matter of fact, the results obtained are quite comparable to that using the City Block distance in Tables 3.2 and 3.3 for the SVC-2004 and MCYT-100 databases.

Table 3.12: MEER (in %) on the genuine and skilled forgeries of the SVC-2004 data-base, with features modified using different values of spacing parameter r. Note, that for this experiment, the Euclidean distance (L_2 norm) is used to compute the entries of the DTW cost matrix.

r	Common-threshold			User-threshold		
	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
1	22.10	11.41	11.57	14.95	5.68	5.05
2	17.25	10.12	9.78	10.01	4.90	3.85
3	15.38	10.19	9.13	7.57	5.03	3.53
4	13.16	10.11	8.62	6.51	4.68	3.02
5	12.54	10.25	8.31	5.95	4.87	3.06
6	12.52	10.28	8.32	5.90	4.86	2.95
7	12.29	10.25	8.80	5.90	5.06	3.18
8	12.47	10.15	8.72	5.86	5.22	3.36
9	12.65	10.39	8.86	5.86	5.09	3.29
10	12.07	10.73	8.64	5.62	4.97	3.09

Table 3.13: MEER (in %) on the genuine and skilled forgeries of the MCYT-100 data-base, with features modified using different values of spacing parameter r. Note, that for this experiment, the Euclidean distance (L_2 norm) is used to compute the entries of the DTW cost matrix.

r	Common-threshold			User-threshold		
	$BL-DTW$ system	WP system	$FUS1$ system	$BL-DTW$ system	WP system	$FUS1$ system
1	11.36	4.93	4.66	7.70	1.69	1.85
2	9.39	4.13	3.79	5.85	1.40	1.47
3	8.21	3.51	3.37	4.99	1.30	1.37
4	7.80	3.27	3.16	4.62	1.22	1.31
5	7.64	3.32	3.21	4.39	1.23	1.32
6	7.42	3.35	3.28	4.19	1.32	1.30
7	7.35	3.37	3.37	4.12	1.36	1.41
8	7.34	3.47	3.47	4.05	1.36	1.47
9	7.22	3.48	3.64	3.99	1.43	1.49
10	7.15	3.43	3.67	3.97	1.48	1.55

3.8.8 Statistical Significance of results

In this subsection, we demonstrate that the results of the proposed methodology ($FUS1$ system) is statistically significant compared to that of the $BL - DTW$. The statistical check has been performed using the Student t-test for the significance level of 0.05.

The modified features with spacing parameter value $r = 5$ were employed for the SVC-2004 database - as they provide the lowest MEER with the City Block distance being used for the cost matrix computation. In addition, the evaluation of the systems were performed using common threshold setting. With this configuration for the $BL - DTW$ and $FUS1$ system, the value of p is empirically found to be 4.90×10^{-5}. This indicates that results in our proposed system is statistically significant to that of $BL - DTW$. Likewise, we observed that for each of the results corresponding to the values of the spacing parameter enumerated in Table 3.2 with common threshold setting, the trend in the values of p are lower than the significance level.

On performing the statistical significance test on the best result of the MCYT-100 database, we obtained the value of p as 2.54×10^{-6} which is less than the significance level. This system is based on modified features computed at spacing parameter value $r = 6$ with common threshold setting and City Block distance for the DTW cost matrix. In addition, a similar trend of low values for p was empirically observed across each of the results enumerated for the values of the spacing parameter r in Table 3.3. Hence it may thus be verified that results of our method is statistically significant to that of the $BL - DTW$.

3.8.9 Computational complexity

We now address on the computation complexity of our proposal by presenting it with regards to each step for a test signature S_T of an user, whose N reference signatures $\{S_1, S_2, ..., S_N\}$ are enrolled in the system (refer Table 3.14). The DTW matching between S_T and the p^{th} reference signature S_p involves a complexity of $\mathcal{O}(n_T n_p)$. Subsequently, the comparison against N reference signatures will yield $\mathcal{O}(n_T \max_{1 \le p \le N} n_p)$ (as mentioned under Step 1).

With regards to the match of the p^{th} reference signature, the computation of r_i involves finding the index of the minimum corresponding to the $W = 2w + 1$ summation terms in

Table 3.14: Computation Complexity of the proposed algorithm for a test signature S_T.

Step	Description	Computation Complexity
1	DTW system / d_1 calculation	$\mathcal{O}(n_T \max\limits_{1\leq p\leq N} n_p)$
2	Computation of (a_i, r_i) aligned pairs	$\mathcal{O}(\max\limits_{1\leq p\leq N} W n_p l_{\mathcal{W}_p^*})$
3	Computation of d_{21}	$\mathcal{O}(\max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$
4	Computation of d_{22}	$\mathcal{O}(\max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$
5	Computation of d_2	$\mathcal{O}(1)$
6	Fusion of Scores	$\mathcal{O}(N)$

Equation 3.10. Considering the fact that this operation is done across the length of the warping path $l_{\mathcal{W}_p^*}$, the complexity of this step using the N reference signatures will be $\mathcal{O}(\max\limits_{1\leq p\leq N} W n_p l_{\mathcal{W}_p^*})$.

The computation of d_{21} and d_{22} is carried out along the warping path $\mathcal{W}_p^*$ - with both the calculations having a computational complexity of $\mathcal{O}(\max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$ respectively. Likewise, the warping path score d_2 as the sum of d_{21} and d_{22} has complexity of $\mathcal{O}(1)$. Lastly, the final step of fusing the scores d_1 and d_2 using the sum rule incurs a complexity of $\mathcal{O}(N)$.

Despite the higher computational complexity than traditional DTW system, our proposal achieves significantly better verification performance.

3.9 Summary

In this Chapter, we presented a novel online signature verification strategy that augments complementary information from the cost matrix to the classical DTW framework. The proposal dealt with devising a novel score that describes the characteristic of the warping paths of genuine and forgery signatures. Thereafter, incorporation of the derived warping path score with that of the DTW was suggested for decision making. In addition, the sequence of point-based feature vectors to be matched between the signatures by the DTW algorithm were modified by introducing the spacing parameter value.

4 An enhanced contextual DTW based system using Vector Quantization

Contents

4.1 Introduction

As discussed in Section 2.4, the traditional DTW algorithms for online signature employ only the distance scores, obtained between the test signature and the genuine enrolled signatures, in formulating the decision rule [46]. We believe that the analysis of the characterization of the distortions on the warping path in the cost matrix may provide us additional cues, that can be possibly exploited for reducing the false acceptance of forgery and rejection of genuine signatures. Accordingly, as our contribution in this Chapter, we derive a score that determines the proportion of the aligned pairs that provide a low distortion value, relative to the length of the warping path, obtained from DTW. For computing this proportion, we consider utilizing a code-book of appropriate size, built from a Vector Quantization (VQ) model. We subsequently fuse this score with that of the DTW, (by score combination strategies), for authenticating the veracity of a test signature. In addition, we attempt capturing the contextual information in the formulation of the proposed 'DTW-VQ' strategy and show improvement of the verification system.

To our knowledge, the application of VQ in literature has been devoted to the problem of signature recognition. In [36], the quantized feature vector of the test signature, of a claimed user, is matched against those of the enrolled reference signatures. The main focus for quantization of the feature vector was from the viewpoint of enhancing the privacy of the biometric system, so that hackers find it difficult to replicate the biometric data from the extracted features transmitted. Our proposal on DTW-VQ strategy differs from this work, in that the VQ step is used to enhance the efficacy of the DTW based system.

Figure 4.1 illustrates the overview of our proposal. The input test signature is first passed through a feature extractor module. Subsequent to that, we use the DTW matching technique to compare it against those of the enrolled reference signatures of an user. The feature vectors corresponding to the warping path indices are then voted, based on the code vectors to which they are assigned. The code vectors are obtained from a code book, generated through a VQ model. The score from the votes are then combined with that of DTW, and compared to a

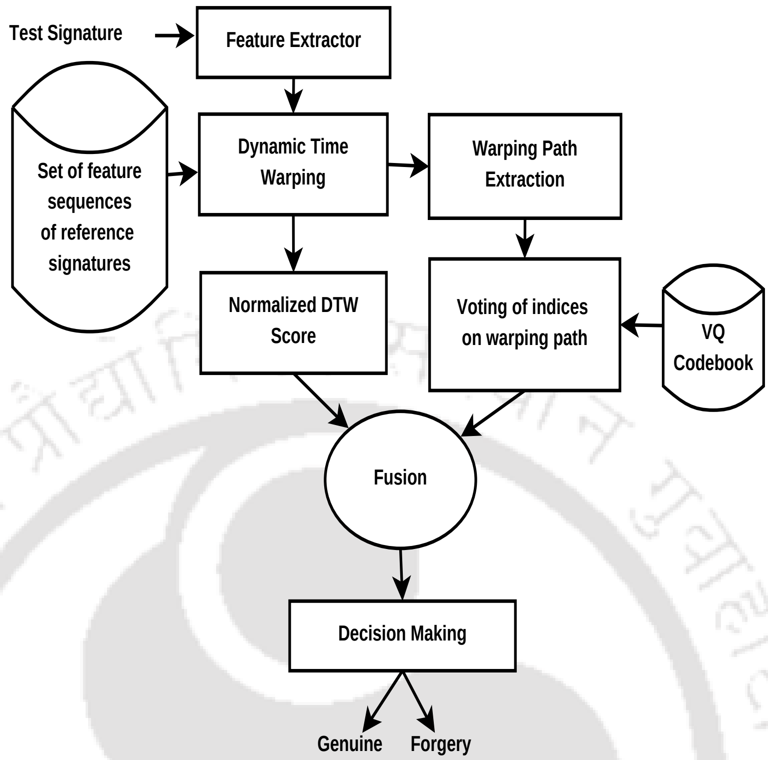


Figure 4.1: Block diagram of the proposed online signature verification scheme.

threshold for determining the veracity of the test signature.

In the context of the present proposal, the following points are to be noted:

- The signatures from the SVC-2004 and MCYT-100 databases will be used for analysis of the strategy and subsequent experimentations.
- The features being employed for the DTW matching of signatures correspond to those discussed in Section 3.3 with spacing parameter $r = 1$.
- For sake of continuity, the same notations as those used for the discussion of the DTW algorithm in Section 3.4 will be adopted.

The rest of this Chapter is organized as follows: we first provide an outline of Vector Quantization in the subsequent Section. This is followed by a detailed description of our 'DTW-VQ' proposal with the derivation of the warping path score in Section 4.3. The idea of incorporating contextual knowledge to our formulation is presented in Section 4.4. We also demonstrate the need of fusing the warping score to that of DTW for verifying signatures in Section 4.5. The experiments demonstrating the efficacy of our proposal is presented in Section 4.6, followed by a brief summary in Section 4.7.

4.2 Vector Quantization

We generate a model based on Vector Quantization [36] for each user. The Linde, Buzo and Gray (LBG) algorithm [108] is used to generate the code-book of size K, where K is a power of 2. A simplified explanation for the same is as follows:

To begin with, the feature vector sequences corresponding to the N enrolled genuine signatures of an user are pooled together and averaged to generate a single code-vector. This code-vector is split into two close vectors, that are then used as input to the k means algorithm with $k = 2$. The pooled feature vectors are employed to refine these code-vectors at each successive iteration of the clustering step. Upon convergence, an updated code-book comprising 2 code-vectors is obtained. Thereafter, these code-vectors are again split to give four seed vectors for the k-means algorithm with $k = 4$. The alternating steps of splitting [1] and clustering are repeated till the code-book of desired size K is obtained.

We denote the resulting final code-vectors of user u by $\{\mathbf{c}_u^1, \mathbf{c}_u^2, \mathbf{c}_u^3, ..., \mathbf{c}_u^K\}$.

4.3 Proposed DTW-VQ based system

For the discussion of our proposal, we consider that the test signature S_T is temporally matched with the p^{th} enrolled signature S_p, using the DTW algorithm detailed in Section 3.4. Accordingly, the cells $(a_i, b_i)_{i=1}^{l_{\mathcal{W}_p^*}}$ of the warping path (denoted by $\mathcal{W}_p^*$) are assumed to be known

[1]Without loss of generality, the splitting step of the LBG algorithm doubles the size of the current code-book with each code-vector $\mathbf{c}_i$ being represented by close vectors defined by:

$$\begin{aligned} \mathbf{c}^{2i-1} &= \mathbf{c}^i(1-\epsilon) \\ \mathbf{c}^{2i} &= \mathbf{c}^i(1+\epsilon) \end{aligned} \qquad 1 \le i \le \tilde{K}$$

Here $\tilde{K}$ represents the size of the current code-book that is to be split and satisfies $\tilde{K} < K$. The value of ϵ used for perturbing the code-vector is very small.

to us by back-tracing through the cost matrix.

For every aligned pair (a_i, b_i) along the warping path $\mathcal{W}_p^*$, we assign its corresponding feature vectors $\mathbf{f}_T^{a_i}$ (from signature S_T) and $\mathbf{f}_p^{bi}$ (from signature S_p) to their respective nearest code vectors. If $l_T^{a_i}$ and $l_p^{b_i}$ denote the indices of code-vectors assigned, we can write :

$$\begin{aligned} l_T^{a_i} &= \arg\min_{1 \le j \le K} |\mathbf{f}_T^{a_i} - \mathbf{c}_u^j| \\ l_p^{b_i} &= \arg\min_{1 \le j \le K} |\mathbf{f}_p^{b_i} - \mathbf{c}_u^j| \end{aligned} \tag{4.1}$$

Subsequent to the assignments of feature vectors $\{\mathbf{f}_T^{a_i}\}_{i=1}^{l_{\mathcal{W}_p^*}}$ and $\{\mathbf{f}_p^{b_i}\}_{i=1}^{l_{\mathcal{W}_p^*}}$ to the code-vectors, we place a vote of 1, on each cell (a_i, b_i), based on the indices $l_T^{a_i}$ and $l_p^{b_i}$. To this effect, we define an indicator variable:

$$I(a_i, b_i) = \begin{cases} 1, & l_T^{a_i} \neq l_p^{b_i} \\ 0, & \text{otherwise} \end{cases}$$

The total number of votes received by cells along the warping path $\mathcal{W}_p^*$, is normalized with the length $l_{\mathcal{W}_p^*}$ as,

$$d_2^p = \frac{\sum_{i=1}^{l_{\mathcal{W}_p^*}} I(a_i, b_i)}{l_{\mathcal{W}_p^*}} \tag{4.2}$$

The above measure can be interpreted as the average degree of mismatch, that occurs between a pair of aligned points (a_i, b_i), along $\mathcal{W}_p^*$, with a VQ code-book of size K.

Consider the matching of a test genuine signature against that from the enrolled set. Due to the high degree of similarity between parts of the trace, the distortion $d(a_i, b_i)$ between feature vectors $\mathbf{f}_T^{a_i}$ and $\mathbf{f}_p^{b_i}$ is low for considerable number of cells along the warping path. It is thus likely that with an appropriate code-vector of size K, the feature vectors fall in the same cluster. By definition, the score d_2^p represents the fraction of cells along $\mathcal{W}_p^*$, whose feature vectors get assigned to different code-vector indices. Accordingly, its value can serve as an indicator as to how dissimilar the trace of the two signatures being compared are. For the case of a genuine to genuine signature match, d_2^p will be low, while the contrary is true when forgery test signature is used to match against a genuine signature in the enrolled set.

To demonstrate the ability of the aforementioned d_2 score to the process of verification, consider the DTW matching of two signatures (one genuine and one skilled forgery) in Figures 4.2 (b) and (c) against a genuine reference signature, shown in Figure 4.2 (a). As with the illustrations in the previous Chapter, to simplify the discussion, we consider only one reference signature S_1 of an user to be enrolled to the system, so that $p = 1$. The depicted signatures are from the SVC-2004 database. Figures 4.2 (d) and (e) indicate the warping paths obtained from the two DTW matches.

The scores from the DTW algorithm d_1 differ by only 0.02 (0.61 and 0.59) and may not provide enough discrimination. It is very likely for the genuine signature to be falsely rejected as forgery and vice-versa. However, on analyzing the trend obtained by assigning the features vectors of the aligned sample points (along the warping path) to their nearest code vectors, we achieve discrimination. This is also suggested by the values of d_2 for the genuine and skilled forgery signature respectively (being 0.60 and 0.77). The contrasting nature of scores is owing to the fact that with a genuine to genuine signature match, more number of points along the warping path have lower distortion values, with their feature vectors getting assigned to the same code-vector (as depicted in Figure 4.2 (f) with the symbol *). This trend is however not predominant for the warping path shown in Figure 4.2 (g). Accordingly, based on Equation 4.2, we obtain a lower value of d_2 for the case where a genuine signature is matched against a genuine reference signature and vice-versa for a skilled forgery match. A code-book size of 32 is used to generate the d_2 score.

As another illustration, we demonstrate the efficacy of the warping path score by considering signatures from an user of the MCYT-100 database (refer Figure 4.3). Here again, the DTW score resulting from the genuine to reference signature match ($d_1 = 1.32$) is higher to that of the skilled forgery to reference signature match ($d_1 = 1.31$). However, the warping path of Figure 4.3 (f) for the genuine signature match presents a high number of feature vectors corresponding to the aligned pairs (depicted by the symbol *) sharing the same code-vector indices. Note that, here again a contrary trend is observed for the warping path of skilled forgery match in Figure 4.3 (g). This differing characteristics in turn leads to the warping path scores 0.72 and 0.92. If further, the sum rule combiner is applied on the scores d_1 and d_2, we

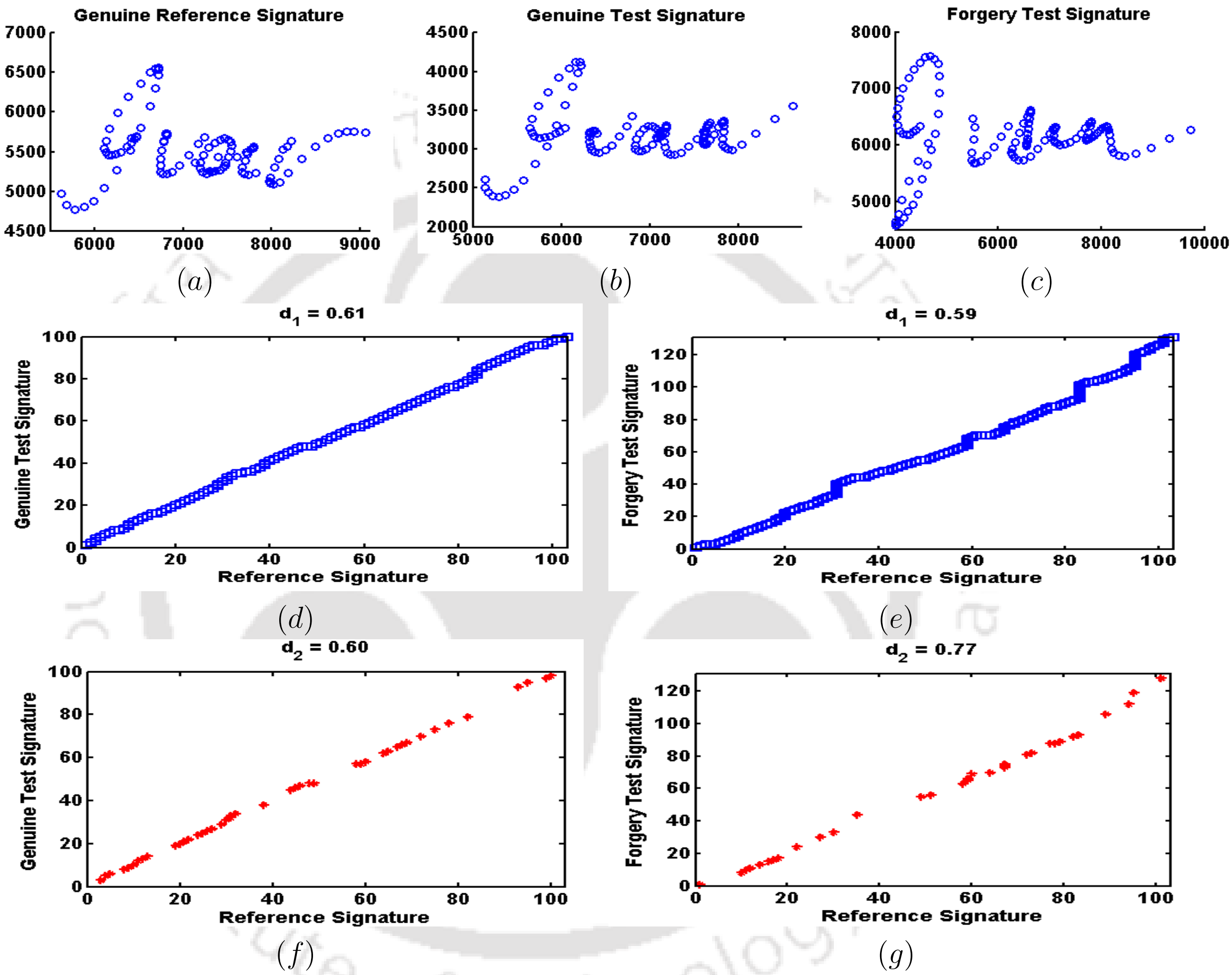


Figure 4.2: A depiction of the warping path score d_2 for verification. The sub-figure (a) shows a sample of genuine signature of an user of SVC-2004 database enrolled into the system. The signatures (b) and (c), correspond to a sample of genuine and skilled forgery signature, that is matched against this signature using DTW algorithm. The scores obtained are very close (sub-figures (d) and (e)), leading to a possible false acceptance of forgery / rejection of the genuine signature. The value of the warping path score d_2, on the other hand, attempts to discriminate the signatures better. The symbol '*' in sub-figures (f) and (g) depict aligned points along the warping path whose corresponding feature vectors get assigned to the same code-vector. The size of code-book = 32.

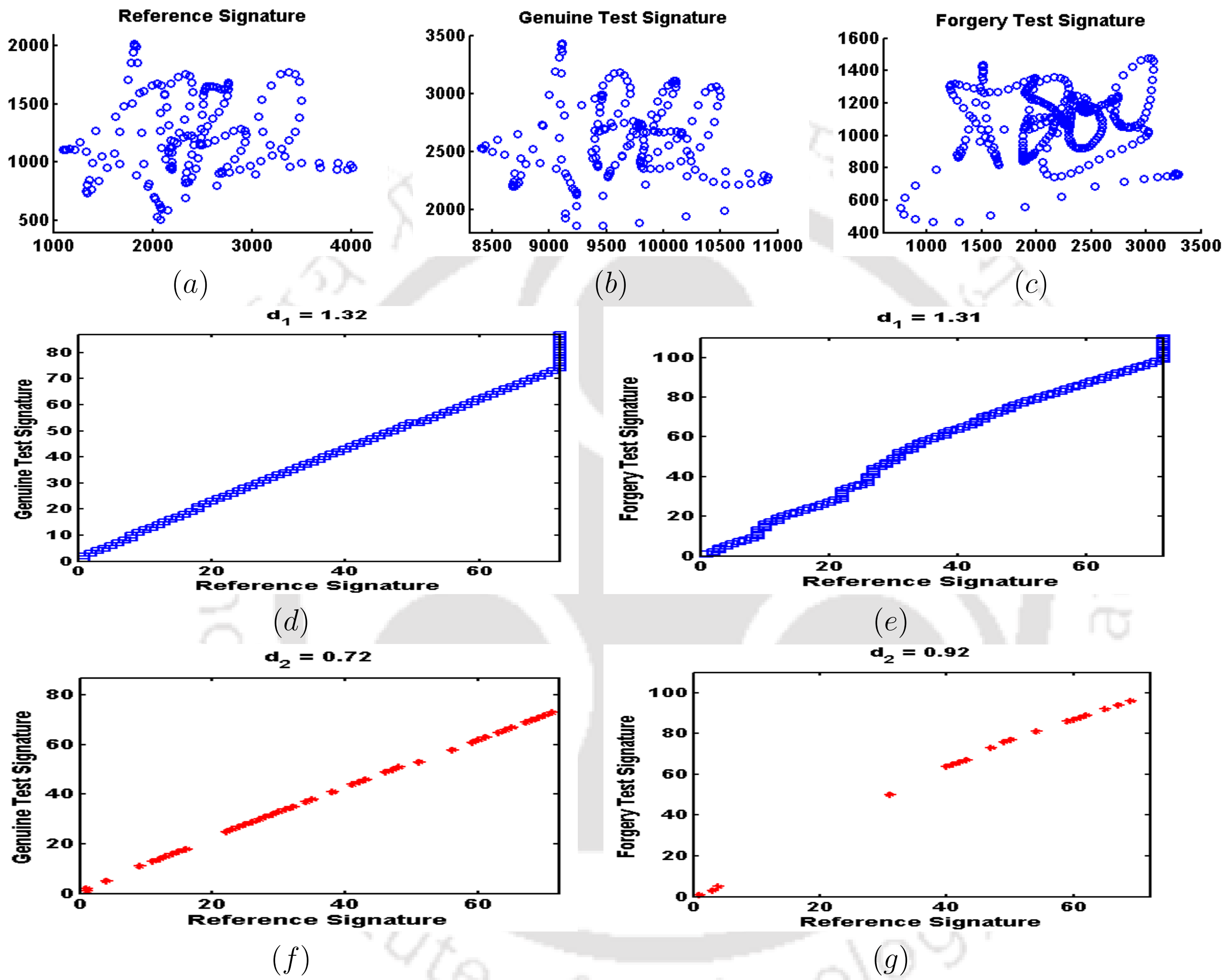


Figure 4.3: A depiction of the warping path score d_2 for verification. The sub-figure (a) shows a sample of genuine signature of an user of MCYT-100 database enrolled into the system. The signatures (b) and (c), correspond to a sample of genuine and skilled forgery signature, that is matched against this signature using DTW algorithm. The scores obtained are very close (sub-figures (d) and (e)), leading to a possible false acceptance of forgery / rejection of the genuine signature. The value of the warping path score d_2, on the other hand, attempts to discriminate the signatures better. The symbol '*' in sub-figures (f) and (g) depict aligned points along the warping path whose corresponding feature vectors get assigned to the same code-vector. The size of code-book = 32.

get values of 2.04 and 2.23 for the genuine and skilled forgery signature match - thus leading to a correct verification decision.

4.4 Incorporation of contextual information

We now consider the aspect of integrating the contextual information to the aforementioned formulation. The benefits of utilizing context for performance enhancement is well known in research domains of image processing and computer vision [106]. To start with, we modify the DTW matching strategy as follows: for every sample point of S_T, along the trace, we consider a window of width $W = 2w + 1$ centered on it, and attempt to align it with a segment of same window length from the signature S_p. The alignment is achieved with the DTW algorithm, by applying the recursion relation of Equation 3.7, on the modified cost matrix, whose cells $d(i, j)$ correspond to:

$$d(i, j) = \frac{1}{2w + 1} \sum_{k=-w}^{w} |\mathbf{f}_T^{i+k} - \mathbf{f}_p^{j+k}| \tag{4.3}$$

The sum of absolute differences between feature vectors is used for the computation. We can interpret Equation 4.3 as the filtering of the distance measures by averaging them in the time window of width W. The process of averaging aids in smoothing out any drastic changes in the distance computations, that may occur whenever there is a break in signature. For values of i and j outside their respective ranges $(w + 1, n_T - w - 1)$ and $(w + 1, n_p - w - 1)$, we see that the windows/segments do not encompass $2w + 1$ sample points. In such cases, we consider padding the first and last sample points of the signatures S_p and S_T, with w repetitions of their corresponding feature vectors.

Subsequent to DTW matching using the modified cost matrix, we obtain a score d_1^p and its associated optimal path $l_{\mathcal{W}_p^*}$. Each of the indices (a_i, b_i) in $l_{\mathcal{W}_p^*}$ indicate that the segment of points (of length $W = 2w + 1$) centered about the a_i^{th} sample point of S_T is aligned to a segment of same length around the b_i^{th} sample point of S_p.

A similar idea of incorporating contextual information is used for the VQ algorithm as well:

for every aligned pair (a_i, b_i), we vote each of the points contained in their neighborhoods (of size $2w + 1$), by determining whether their corresponding feature vectors get assigned to the same code-vector. Let $d_V(a_i, b_i)$ denote the average number of votes received by the $(2w + 1)$ points. We can now write:

$$\begin{aligned} d_V(a_i, b_i) &= \tfrac{1}{2w+1} \textstyle\sum_{j=-w}^{w} I(a_i + j, b_i + j) \\ &= \tfrac{1}{2w+1} \textstyle\sum_{j=-w}^{w} I(l_T^{a_i+j} \neq l_p^{b_i+j}) \end{aligned} \tag{4.4}$$

As can be seen the value $d_V(a_i, b_i)$ is bounded between 0 and 1. The above computation is computed $\forall (a_i, b_i) \in \mathcal{W}_p^*$. Thereafter, the averaged votes are accumulated and normalized with the length of the warping path $l_{\mathcal{W}_p^*}$ to give:

$$d_2^p = \frac{\sum_{i=1}^{l_{\mathcal{W}_p^*}} d_V(a_i, b_i)}{l_{\mathcal{W}_p^*}} \tag{4.5}$$

For the case where only point-based matching is considered (without the incorporation of context), the value of d_2^p reduces to Equation 4.2

4.5 Fusion

Given N enrolled signatures of a user, we get N values of d_1 and d_2 - the average of which are d_1^{mean} and d_2^{mean} respectively. To motivate the need for fusion, we analyze the trend of these values for the genuine and skilled forgery signatures of an user, as a two dimensional plot (Figure 4.4). By empirically noting that the scores are complementary, we consider fusing them with popular score combination techniques. In this work, we explore four such strategies : namely, sum rule, weighted sum rule, weighted product and weighted minimum strategies [108]. The overview of these strategies are enumerated in Table 4.1.

Lastly, to summarize our proposal, we present a pseudo-code of the 'VQ-DTW' strategy in Algorithm 2.

Algorithm 2 Proposed signature verification algorithm

Input: Test signature S_T ; a set of N enrolled reference signatures of an user denoted as $\{S_1, S_2, ..., S_N\}$
User specific code-book of size K comprising code vectors: $\{\mathbf{c}_u^1, \mathbf{c}_u^2, \mathbf{c}_u^3, ..., \mathbf{c}_u^K\}$.

For $p = 1 : N$

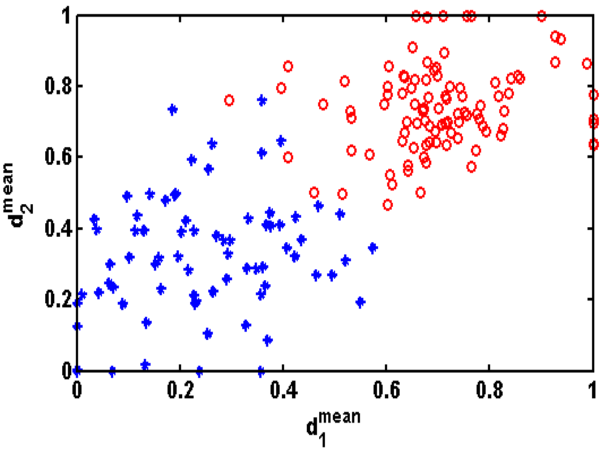
- Derive the sequence of point based feature vectors (discussed in Section 3.3) corresponding to S_T and S_p.
- Perform the contextual DTW match of S_T with S_p to get d_1^p score (refer Section 4.4.)
- Extract the cells (a_i, b_i) in the warping path $\mathcal{W}_p^*$ from the DTW cost matrix by back-tracing.

`% Computation of the warping path score`

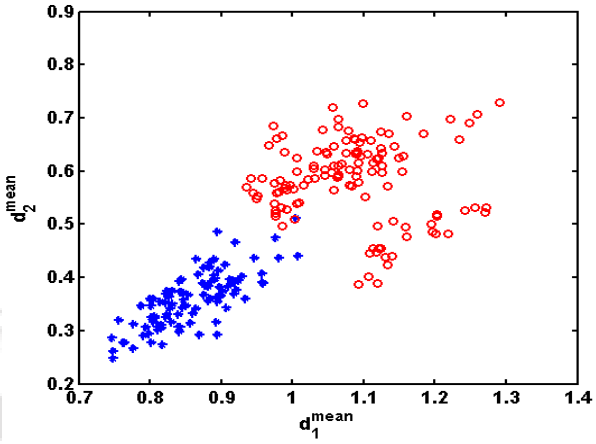
- For every aligned pair (a_i, b_i) along the warping path $\mathcal{W}_p^*$, compute the indicator variable $I(a_i, b_i)$
- For every aligned pair (a_i, b_i) compute $d_V(a_i, b_i)$ (using the Equation 4.4).
- Compute the warping path score $d_2^p = \frac{\sum_{i=1}^{l_{\mathcal{W}_p^*}} d_V(a_i,b_i)}{l_{\mathcal{W}_p^*}}$.

End

- Fuse the N scores $\{d_1^p\}_{p=1}^N$ and $\{d_2^p\}_{p=1}^N$ with a combination scheme from Table 4.1.
- Use the fused score for authentication.



(a)



(b)

Figure 4.4: Two dimensional distance plot (d_1^{mean}, d_2^{mean}) of a user's genuine and skilled forgery signatures (depicted by blue and red color respectively) from the (a) SVC-2004 and (b) MCYT-100 database. The number of reference signatures employed=5 and size of K=32. The experimental set-up discussed in sub-section 3.7.1 is used in generating this plot.

Table 4.1: Overview of the score combination strategies for d_1^{mean} and d_2^{mean}.

Sum rule	$d_T = d_1^{mean} + d_2^{mean}$	
Weighed sum	$d_T = (\beta - 1)d_1^{mean} + (2 - \beta)d_2^{mean}$	
Weighed minimum	$d_T = \min(\beta d_1^{mean}, d_2^{mean})$	
Weighed product rule	$d_T = d_1^{mean} \times (d_2^{mean})^{\beta-1}$	$1 \leq \beta \leq 2$

4.6 Results and Discussion

We start this Section by outlining the systems implemented, together with their abbreviations.

- *BL-DTW*: corresponds to the baseline system, that employs the normalized DTW score d_1 (discussed in Section 3.4) for verification.
- *CTX-DTW*: corresponds to the DTW system, that utilizes the contextual information for the generation of the cost matrix. In other words, the values of each of the cells in the cost matrix are computed using Equation 4.3.
- *FUS2*: A system wherein the normalized DTW score d_1 from the *CTX-DTW* system is fused to that of the warping path score d_2 defined in Equation 4.5. The score combination

Table 4.2: MEER (in %) of the *CTX-DTW* based system with varying window widths for the SVC-2004 database.

Width W	1	3	5	7	9	11
Common Threshold	20.33	18.14	16.80	15.94	15.32	15.59
User Threshold	13.28	10.82	9.32	8.20	7.46	7.53

scheme employed in the *FUS2* system corresponds to one of the strategies presented in Table 4.1.

With regards to the enrolment and evaluation protocol, we use the same as discussed in Section 3.7 for the SVC-2004 and MCYT-100 databases respectively.

4.6.1 Performance Evaluation on SVC-2004 Database

We begin by exploring the performance of the *CTX-DTW* system in Table 4.2 for different odd window sizes varying from 1 to 11. The segment of width one corresponds to the matching between pairs of points of the two signatures being compared and as such reduces to the $BL-DTW$ system - with an MEER of 13.28 % and 20.33% for the user and common threshold respectively. With increase in the number of sample points in the neighborhood for matching, the performance of the *CTX-DTW* system improves. We obtain an MEER to as low as 15.32% (leading to a 24.6% improvement over the $BL - DTW$) for a window size 9 with common threshold.

Table 4.3 (a) and (b) presents the common and user thresholds MEERs on the $FUS2$ system, that takes in to account the score, from voting the aligned points on the warping path in conjunction to that obtained from the *CTX-DTW* system. The sum rule is used for this evaluation. We have experimented over varying code-book sizes (2 to 128 code-vectors) and window widths. To begin, we consider the trend of MEER obtained for $W = 1$, (corresponding to 'without context'). Compared to the *BL-DTW*, with code-books of one to four bits, there is increase in the MEER (21.02%, 21.54%, 22.45% and 21.33%) in Table 4.3 (a) (common threshold set-up), resulting from the coarse quantization process. A small-sized code-book does not adequately capture the finer nuances that discriminate the genuine and skilled forgery

Table 4.3: MEER (in %) of the *FUS2* based system after fusion of the scores d_1^{mean} and d_2^{mean}, using the sum-rule combiner. The sub tables (a) and (b) present the results on the common threshold and user threshold scenario for the SVC-2004 database.

Code-book	Window Width					
Size K	1	3	5	7	9	11
2	21.02	19.15	18.10	17.15	16.40	16.02
4	21.54	18.47	17.40	16.58	15.85	15.15
8	22.45	18.97	17.58	16.44	15.43	14.82
16	21.33	17.95	16.14	15.35	14.68	14.17
32	19.68	17.30	15.72	14.69	13.91	13.41
64	18.40	15.91	14.23	13.28	12.69	13.52
128	17.56	14.82	13.87	13.43	14.09	14.43

(a)

Code-book	Window Width					
Size K	1	3	5	7	9	11
2	14.25	11.41	9.73	8.70	7.81	7.52
4	14.55	11.21	9.50	8.02	7.39	7.11
8	15.01	11.00	8.83	7.58	6.92	6.61
16	14.04	10.06	8.04	6.96	6.41	6.16
32	13.07	9.14	7.50	6.71	6.24	6.11
64	11.40	8.14	6.84	6.16	5.73	5.92
128	10.46	7.51	6.39	5.91	5.83	5.89

(b)

signatures. This is due to their corresponding feature vectors having a tendency to get assigned to the same code-vector that has a very large Voronoi cell around it. Hence, a higher number of false positives are likely to occur. However, with increasing number of bits in the VQ modeling, the number of code-vectors increase, thus alleviating this problem. Accordingly, for selective choices of K (the code-book size) the MEER reduces. We see improvements in verification performance for K beyond 32. A MEER of 17.56% is obtained for a code-book of size 128.

In general, for a given code-book size, we see a reduction in MEER with increasing window widths, thus indicating the usefulness of incorporating the contextual information in the DTW formulation. A similar trend of lower values of MEER with increasing code-book size for a given

Table 4.4: Trend of distortion values for different code-book sizes K of a user of SVC-2004 database, obtained from the VQ step.

K	2	4	8	16	32	64	128
Distortion Value	1160	1010	741.08	122.07	74.13	29.17	9.55

window width can also be inferred. A combination of window width of 9 with code-book size 64 gives the lowest MEER of 12.69 % and 5.73% for the common and user threshold respectively (refer Table 4.3 (a) and (b)).

To validate on the aforementioned trends, we analyze the mean square distortion values of feature vectors, corresponding to varying number of bits in the VQ model (refer Table 4.4). The feature vectors employed are from the five randomly selected enrolled genuine signatures of a user. For small code-book sizes (corresponding to coarse quantization), the mean square error is quite high. However, with finer quantization, achieved with higher-bit / large-sized code-books, the error drops. This in turn could explain the increase in MEER, when d_2^{mean} scores obtained with small code-book sizes, are fused with the normalized DTW score d_1^{mean} from the $CTX - DTW$.

Though the results of Table 4.3 pertain to the sum rule combiner in the $FUS2$ system, it is worth noting that a similar trend of MEERs (with regards to varying code-book size and window widths) is observed for each of the strategies in Table 4.1. That being said, we present only the best MEERs obtained (in Table 4.5), along with their corresponding values of weight parameter β, code-book size K and window width W. The verification results are quite comparable, with the Weighted Product rule for the parameters $(\beta, K, W) = (1.4, 32, 9)$ giving the lowest MEER of 10.85% and 3.89% for common and user threshold scenario.

We also evaluate the performance of the $FUS2$ system for varying number of reference signature samples enrolled to the system. The size of the code-book K and window width W providing the lowest MEER are denoted in the last column of Table 4.6 for each reference set. Clearly, we see reduction of error rates over the $BL - DTW$ system.

Table 4.5: The MEER (in %) for the SVC-2004 database using different combination strategies in the $FUS2$ system. The corresponding values of weight parameter β, code-book size K and window width W are also presented in fourth column.

Combination Scheme	MEER (in %)		(β, K, W)
	Common Threshold	User Threshold	
Sum rule	12.69	5.73	$(1.5, 64, 9)$
Weighted sum rule	11.74	4.92	$(1.2, 64, 9)$
Weighted minimum rule	13.12	6.12	$(1, 32, 7)$
Weighted product rule	10.85	3.89	$(1.4, 32, 9)$

Table 4.6: Performance evaluation of the proposed *FUS2* system for varying number of reference signatures of the SVC-2004 database. The numbers shown in the third and fifth column indicate the MEER (in %) for the sum rule combiner.

# of reference signatures	Common Threshold		User Threshold		(K, W)
	$BL-DTW$ system	$FUS2$ system	$BL-DTW$ system	$FUS2$ system	
2	23.93	16.45	14.31	7.12	(32,7)
5	20.33	12.69	13.28	5.73	(64,9)
10	19.95	14.42	11.83	7.23	(32,9)

4.6.2 Performance Evaluation on MCYT-100 Database

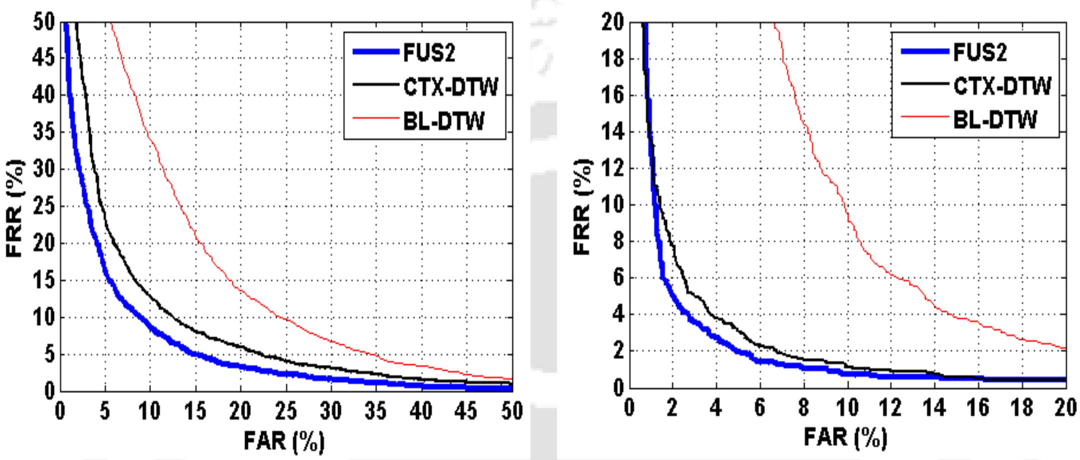
Table 4.7 depicts the result of *CTX-DTW* system for different odd window sizes varying from 1 to 11. Here again, we see reduced MEERs over the *BL-DTW* system, that corresponds to the width W=1. For illustration, we also present the results on the $FUS2$ system using the sum rule for varying code-book sizes K in Table 4.8 (a) and (b). Clearly, the incorporation of the warping path score brings down the MEER to as low as 3.24 % and 1.36% with the parameters $K = 64$ and $W = 9$ for common and user threshold set-up respectively.

We now validate the effectiveness of the proposed *FUS2* system by using the combination strategies presented in Table 4.1. From the results of Table 4.9, we see the Weighted Product rule to give the lowest MEER of 2.53 % for the parameters $(\beta, K, W) = (1.4, 64, 9)$ using common threshold. Likewise, a comparable performance is noted across all the schemes.

The relatively higher verification performance is owing to the fact that samples are collected

Table 4.7: MEER (in %) of *CTX-DTW* system with varying window width values for the MCYT-100 database.

Width W	1	3	5	7	9	11
Common Threshold	10.94	7.36	6.78	5.47	4.49	4.86
User Threshold	7.40	5.01	3.82	3.19	2.46	2.49



(a) (b)

Figure 4.5: DET curves corresponding to the (a) SVC-2004 and (b) MCYT-100 database, using skilled forgeries, for the common threshold scenario. The plots are obtained from the tested signatures (using skilled forgery) across all the users of a single trial. The number of reference signatures considered is 5.

using real signatures of persons, unlike the SVC-2004 database, wherein the persons were asked to 'invent' signatures [17, 29]. As a further demonstration for the efficacy of the proposal, we tabulate in Table 4.10 the MEERs for varying number of reference signature samples enrolled to the $FUS2$ system. We see that a user's signature is authenticated effectively with even few samples.

4.6.3 DET Curves

In this subsection, we provide the DET curves corresponding to the SVC-2004 and MCYT-100 database obtained on a single trial, for the common threshold scenario in Figure 4.5(a) and (b). For generating these plots, the value of the code-book size and window length being considered are $K = 64$ and $W = 7$ respectively. Clearly, the $FUS2$ system outperforms the

Table 4.8: MEER (in %) of the $FUS2$ based system after the sum-rule based fusion of the scores d_1^{mean} and d_2^{mean}. The sub tables (a) and (b) present the results on the common threshold and user threshold scenario respectively for the MCYT-100 database.

Code-book	Window Width					
Size K	1	3	5	7	9	11
2	10.29	7.36	5.73	4.88	4.29	3.69
4	11.46	7.72	6.11	5.17	4.35	3.73
8	11.11	7.56	5.64	4.77	4.21	3.69
16	11.72	7.36	5.59	4.68	3.97	3.38
32	11.78	7.21	5.33	4.59	4.04	3.54
64	11.68	6.98	5.07	4.22	3.24	3.48
128	12.02	6.66	5.07	4.33	3.69	3.75

(a)

Code-book	Window Width					
Size K	1	3	5	7	9	11
2	7.42	4.40	2.98	2.27	1.81	1.55
4	7.73	4.48	3.18	2.48	1.95	1.60
8	8.24	4.44	3.06	2.35	1.80	1.59
16	8.36	4.35	2.87	2.19	1.85	1.55
32	8.53	4.04	2.79	2.03	1.67	1.56
64	8.55	4.04	2.51	1.84	1.36	1.48
128	8.68	3.57	2.36	1.92	1.52	1.70

(b)

Table 4.9: MEER (in %) of the $FUS2$ based system after fusion of d_1^{mean} and d_2^{mean}, using different combination strategies for the MCYT-100 database. The corresponding values of weight parameter β, code-book size K and window width W are also presented in fourth column.

Combination Scheme	MEER (in %)		(β, K, W)
	Common Threshold	User Threshold	
Sum rule	3.24	1.36	$(1.5, 64, 9)$
Weighted sum rule	2.84	1.21	$(1.2, 64, 11)$
Weighted minimum rule	3.01	1.43	$(1, 32, 11)$
Weighted product rule	2.53	1.03	$(1.4, 64, 9)$

$BL-DTW$ and $CTX-DTW$ in almost all of the points for both the databases.

Table 4.10: Performance evaluation of the $FUS2$ system for varying number of reference signatures of the MCYT-100 database. The numbers shown in the third and fifth column indicate the MEER (in %) for the sum rule combiner.

# of reference signatures	Common Threshold		User Threshold		(K, W)
	$BL-DTW$ system	$FUS2$ system	$BL-DTW$ system	$FUS2$ system	
2	14.43	7.08	8.22	2.11	(64,11)
5	10.94	3.24	7.40	1.36	(64,9)
10	9.72	3.58	6.84	1.62	(32,9)

Table 4.11: Computation Complexity of the proposed algorithm for a test signature S_T.

Step	**Description**	**Computation Complexity**
1	DTW system	$\mathcal{O}(n_T \max\limits_{1\leq p\leq N} n_p)$
2	Assignment of code book indices	$\mathcal{O}(K \max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$
3	Computation of indicator variable	$\mathcal{O}(\max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$
4	Computation of d_2	$\mathcal{O}(W \max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$
5	Fusion of Scores	$\mathcal{O}(N)$

4.6.4 Computational complexity

With regards to the computation complexity of our proposal (refer Table 4.11), recall that for a DTW match between a signature S_T to those of the N reference signatures $\{S_1, S_2....., S_N\}$ we incur $\mathcal{O}(n_T \max\limits_{1\leq p\leq N} n_p)$. Thereafter, the assignment of the code-book indices involves computation of distance between feature vectors of aligned sample points on the warping path to each of the K code vectors in the codebook. Thus, the time complexity of this step with regards to the reference signatures is $\mathcal{O}(K \max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$. Likewise, the computation of the indicator variable $I(a_i, b_i)$ for all aligned pairs in the warping path has $\mathcal{O}(\max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$ complexity. From Equations 4.4 and 4.5, we note that the warping path score d_2 is an averaging of votes received over a window size of $W = 2w+1$ along the aligned pairs of feature vectors of the warping path. This operation, as such, gives a complexity $\mathcal{O}(W \max\limits_{1\leq p\leq N} l_{\mathcal{W}_p^*})$. Lastly, the fusion of the scores d_1 and d_2 using a combination strategy incurs a complexity of $\mathcal{O}(N)$.

4.7 Summary

In short, our contributions in this Chapter are: (i) proposal of a score using Vector Quantization (VQ) to describe the trend of the distortion values along the warping paths of genuine and forgery signatures. (ii) incorporation of the derived score with the normalized DTW score for decision making. (iii) inclusion of contextual information to the formulation.

5

A system based on GMM descriptors in a DTW framework

Contents

5.1 Introduction

In this Chapter, we propose an online signature verification system that exploits on cues from a model based approach to improve the performance of the DTW matching scheme. Prior works on the combinations of model based and distance based approach in literature include that of the HMM and DTW based system as described in [107]. It may be noted that the two systems are separately modeled and their scores combined using the sum rule, after appropriate normalization. Likewise, in place of the HMM, the combination is done with the score from the Parzen Window classifier in [35]. Contrast to these works, in this proposal, we consider the incorporation of a model-based technique (GMM) with the distance based method (DTW), from a different view, as will be discussed in the the remainder of this Chapter.

As mentioned in Section 2.2.2 of the thesis, the systems based on DTW in literature perform a temporal alignment between the feature vectors that are derived at each sample point of the online trace of the signatures being compared. The resulting scores after the accumulation of distance values along the warping path are used to verify the authenticity of the signature. The DTW score reflect in a way the similarity of the test signature with the reference genuine signature of an user, enrolled to the system. One aspect that has hardly been sought after in the literature is on considering the sequence of feature vectors, being matched, from a probabilistic viewpoint. This representation, we demonstrate in this Chapter, can help capture the user dependent characteristics of a signature, thereby improving the discrimination between the genuine and skilled forgery signatures. The main premise comes from the notion that feature vectors corresponding to parts of the online trace of the genuine signatures of an user reside in specific regions of the feature space. Thus, it would be interesting, to explore out on a probabilistic representation for the feature vector corresponding to each sample point of the online trace, with regards to their degree of association to each of these regions.

As a step in this direction, we consider in this proposal, to encode the local features extracted at each sample of the online trace of a user's signature by a set of descriptors, that are obtained from a GMM (Gaussian Mixture Model). The resulting descriptors from the GMM obtained at each sample point of the signatures being compared are temporally aligned using the DTW algorithm and matched.

It is worth mentioning here that the present work is the first of its kind that takes into consideration the features derived from the model based approach into the computation of the distance based technique of DTW for signature verification. This makes our proposal different from the other works on combining model-based with distance-based techniques [35, 107] - wherein, as mentioned earlier, the emphasis has been to separately consider the outputs of each of them, followed by a fusion using a sum rule.

Furthermore, we seek to exploit the information from the warping path of the DTW cost matrix for verification, so that the shortcoming of DTW based matching as highlighted in Section 3.4 can be alleviated. Keeping this in perspective, we propose, in this work, a scoring that encapsulates the characteristics of the warping path in the cost matrix. The score is obtained by considering a match between two histograms that are generated from the cost matrix. The striking highlight of our strategy is in the use of the GMM based descriptors itself to derive the histogram, and there-of, the warping path score. Finally, owing to the complementary nature of the warping path score, to that of DTW score, we explore a fusion of the two scores using the sum rule combiner. The combined score is then used to authenticate the veracity of the test signature. We show that the fusion of scores improves the verification performance, beyond that provided by the DTW score alone. It is also worth noting that both the scores are generated from analyzing the DTW cost matrix.

Based on the preceding discussions, the following may be regarded as the main points of this Chapter.

(i) Consideration of the point based feature vectors of the online trace of signatures, from a probabilistic view, by encoding them using GMM based descriptors, prior to DTW matching.

(ii) Exploring the utility of the descriptors from the GMM for scoring the characteristics of the warping path.

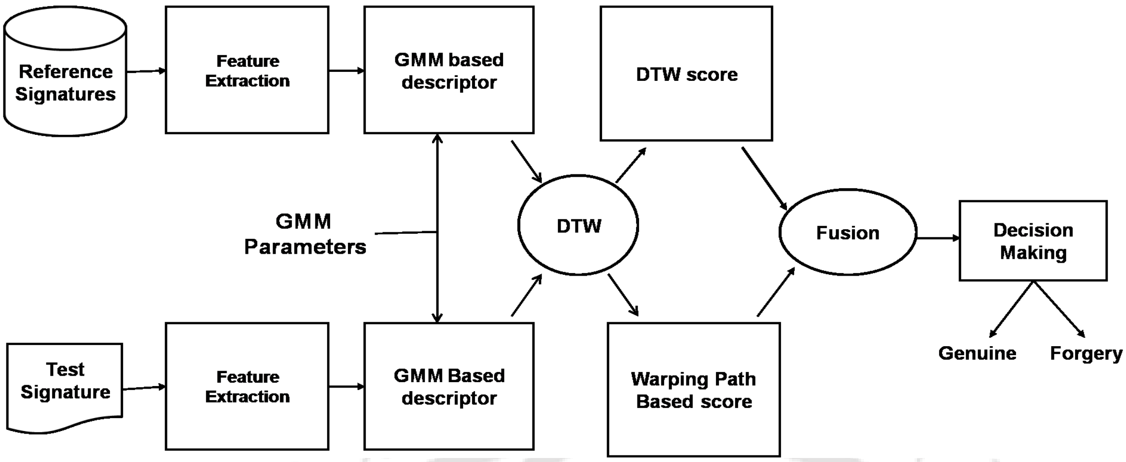


Figure 5.1: Schematic representation of the proposed signature verification system

(iii) Fusion of the warping path score with that of DTW for performance enhancement of the online signature verification system.

5.2 System Architecture

Figure 5.1 presents the block schematic of our proposal. The signature to be verified is passed through a feature extractor module, that operates on each local point of the online trace to derive a set of attributes. The resulting feature vectors are encoded probabilistically by using the parameters of the GMM, that has been learnt from a set of enrolled signatures of an user. The resulting feature descriptors are then aligned, with DTW, against those of the enrolled signatures, that are also encoded using a GMM. Subsequent to the generation of the warping path, we analyze its trend to help discriminate the genuine signatures from the skilled forgery much better. Here again, we use the GMM descriptors for scoring the warping path. Thereafter, for verification of the signature, we consider a fusion of the warping path score, to that of DTW score.

To begin with, we provide a background of the GMM for the context of online signature verification in the following Section. This is followed by a detailed description of our proposal termed as ‘GMM-DTW’ in Section 5.4.

5.3 Gaussian Mixture Models

A Gaussian Mixture Model (GMM) is parametric probability density function that is used to capture the underlying statistical variabilities of the point based features, being considered for describing the online trace of the signatures. Mathematically, for a d-dimensional feature vector $\mathbf{x}$, the GMM comprising M Gaussian components is given by

$$p(\mathbf{x}) = \sum_{k=1}^{M} \pi_k \mathcal{N}(\mathbf{x} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) \tag{5.1}$$

where $\{\pi_k\}_{k=1}^{M}$ represent the mixing coefficients of each Gaussian and sum up to unity. Each of the M Gaussian components are parameterized by a $d \times 1$ mean vector $\boldsymbol{\mu}_k$ and a $d \times d$ co-variance matrix $\boldsymbol{\Sigma}_k$

$$\mathcal{N}(\mathbf{x} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) = \frac{1}{(2\pi)^{\frac{d}{2}} |\boldsymbol{\Sigma}_k|^{\frac{1}{2}}} e^{-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k{}^{-1}(\mathbf{x}-\boldsymbol{\mu}_k)} \tag{5.2}$$

The parameters of the Gaussian components are learnt from the set of enrolled signatures of an user via the Expectation Maximization (EM) algorithm [109]. This algorithm, through iterations, ensures that the optimal parameters maximize the log-likelihood function, computed from the training feature vectors. Considering that feature vectors corresponding to similar parts of the trace of genuine signatures reside in specific regions in the feature space, the statistical characterization regarding the same are obtained from the learnt GMM parameters. While the general framework considers the full covariance matrix for each Gaussian density, in this work, however, we use a diagonal matrix.

In order to learn the parameters of the GMM, we consider a data-set $\mathbf{X}$ comprising $n_{tr} = \sum_{p=1}^{N} n_p$ feature vectors derived from the online trace of the N enrolled signatures of a user. Using the independence and identically distributed (i.i.d) assumption between these vectors, the log-likelihood function can be written as:

$$\ln p(\mathbf{X} | \ \pi_k, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) = \sum_{j=1}^{n_{tr}} \ln\{\sum_{k=1}^{M} \pi_k \mathcal{N}(\mathbf{x}^{(j)} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)\} \tag{5.3}$$

The notation $\mathbf{x}^{(j)}$ refers to a feature vector in $\mathbf{X}$, implying that $\mathbf{x}^{(j)} \in \mathbf{X}$. It may be noted that the features being employed correspond to those discussed in Section 3.3 with spacing parameter $r = 1$.

The objective of the EM algorithm is to estimate the parameters of Gaussian components in a way that the value of the log-likelihood expression is maximized subject to the constraint that the M mixing coefficients $\{\pi_k\}_{k=1}^{M}$ sum up to one [110]. A general iterative procedure for achieving this is presented in Algorithm 3.

In this work, the initialization of the M mean vectors is done using random selections of the training data. Moreover, the M co-variance matrices are considered to be diagonal in each iteration [1] and hence, these are initialized to the identity matrix at the start of the algorithm. Such an assumption is made owing to (i) the small size of samples available for training and (ii) the faster estimation it offers over a non-diagonal matrix.

Each mixing coefficient $\{\pi_k\}_{k=1}^{M}$ to start with, was set to $\frac{1}{M}$. Subsequent to these initializations, the EM iterative algorithm is run until the fulfillment of a specified convergence / stopping criterion. For our case, we used a threshold on the difference between the mean vectors obtained from consecutive iterations. We also mention in passing that we avoid an over-fit of the variance parameters during the EM algorithm estimation by flooring the variance parameters in the co-variance matrix to a minimum value [111].

We now provide an overview of the verification strategy using the likelihood score of the GMM system. During the process of authentication, each of the feature vectors of a test signature S_T, $\{\mathbf{f}_T^j\}_{j=1}^{n_T-2}$ are assumed to be independent and identically distributed. Using this, the log-likelihood function can be written as :

$$L = \frac{1}{n_T - 2}\Big(\sum_{j=1}^{n_T-2} \ln(\sum_{i=1}^{M} \pi_i \mathcal{N}(\mathbf{f}_T^j \mid \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i))\Big) \tag{5.4}$$

Let L_{avg} denote the average normalized log-likelihood scores computed from the set of enrolled signatures of an user whose claim is to be authenticated. For the purpose of verification,

[1] To enforce a diagonal covariance matrix, we set to zero the off-diagonal entries of the M estimates $\{\boldsymbol{\Sigma}_k\}_{k=1}^{M}$ at each iteration in the GMM learning framework of Algorithm 3 and compute only the variances.

Algorithm 3 Estimation of the GMM parameters

(i) Initialize the M mean vectors $\{\boldsymbol{\mu}_k\}_{k=1}^{M}$, co-variance matrices $\{\boldsymbol{\Sigma}_k\}_{k=1}^{M}$ and mixing coefficients $\{\pi_k\}_{k=1}^{M}$.

(ii) Compute the initial value of the log-likelihood function from Equation 5.3.

(iii) `Expectation Step:` Compute the membership value of each component of the GMM with regards to a feature vector $\mathbf{x}^{(j)} \in \mathbf{X}$:

$$g^{(j)}(k) = \frac{\pi_k \mathcal{N}(\mathbf{x}^{(j)} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)}{\sum_{c=1}^{M} \pi_c \mathcal{N}(\mathbf{x}^{(j)} \mid \boldsymbol{\mu}_c, \boldsymbol{\Sigma}_c)}$$

$$1 \leq j \leq n_{tr}, 1 \leq k \leq M$$

(iv) `Maximization Step:` Compute the revised estimates of the parameters as follows:

$$\pi_k = \frac{1}{n_{tr}} \sum_{j=1}^{n_{tr}} g^{(j)}(k)$$

$$\boldsymbol{\mu}_k = \frac{\sum_{j=1}^{n_{tr}} g^{(j)}(k)\mathbf{x}^{(j)}}{\sum_{j=1}^{n_{tr}} g^{(j)}(k)}$$

$$\boldsymbol{\Sigma}_k = \frac{\sum_{j=1}^{n_{tr}} g^{(j)}(k)(\mathbf{x}^{(j)} - \boldsymbol{\mu}_k)(\mathbf{x}^{(j)} - \boldsymbol{\mu}_k)^T}{\sum_{j=1}^{n_{tr}} g^{(j)}(k)}$$

$$1 \leq k \leq M$$

(v) Re-evaluate the log-likelihood function value from Equation 5.3 by using the revised parameters.

(vi) Check for convergence using either the parameters or the log-likelihood value. If convergence criteria is not satisfied, repeat steps (iii) onwards using the revised estimates.

we consider the difference of likelihood score D_L defined by:

$$D_L = L - L_{avg} \tag{5.5}$$

A low value of D_L indicates a genuine signature while the converse is true for a forgery signature. Prior to authenticating, the difference D_L is mapped to $[0, 1]$ by a sigmoidal function. A block schematic of the GMM based likelihood system is presented in Figure 5.2.

A careful analysis of the log-likelihood function in Equations 5.3 and 5.4 indicate that the terms inside the log function reflect the accumulation of contributions of each of the M Gaussian components for each point based feature-vector. As a result of this accumulation, the explicit contributions of each of the Gaussians with regards to the features of the genuine and forgery signature gets ignored at the time of verification. The incorporation of such information we believe can help in enhancing the verification capabilities of the system thus discriminating better the genuine from the forgery signatures. In order to circumvent this issue of the GMM, we propose to encode the feature vector sequence derived at each sample point of the online trace probabilistically with the parameters pre-learnt from the enrolled training signatures of an user.

A second aspect that is not adequately captured from the expression of log-likelihood function is on the incorporation of temporal information - an important cue for the verification of an online signature. We seek to exploit on the same by aligning the temporal trace of the signatures to be matched with our proposed GMM encoded descriptors using the DTW algorithm. The details pertaining to our approach are described in the following Section.

5.4 Details of the GMM-DTW proposal

We present a novel signature verification scheme, that makes use of the GMM descriptors in a DTW framework [2]. For sake of clarity, we divide this Section into three parts and present the algorithm in sequence.

[2]We wish to remind that the the DTW algorithm was presented in sufficient detail in Section 3.4 of the thesis. Accordingly, for consistency, we maintain the same notations used in that discussion for the description of the present proposal.

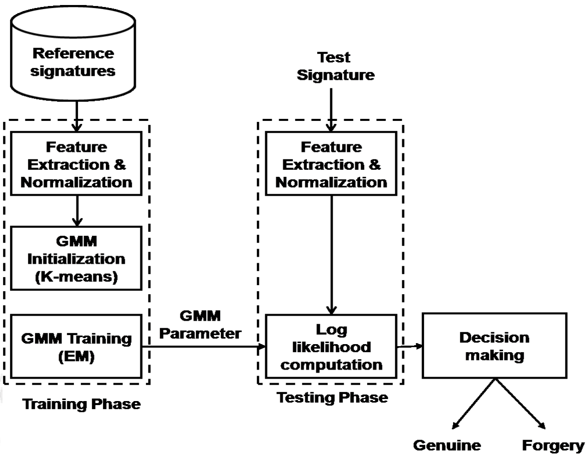


Figure 5.2: Block schematic of GMM based likelihood system

5.4.1 GMM Based Descriptor Representation

The main idea, as mentioned in Section 5.1, is to encode the feature vector sequence derived at each sample point of the online trace probabilistically. The solution to this is straightforward, thanks to the GMM that has been trained a-priori using the enrolled training signatures of an user. Each user is modelled by a specific GMM of M Gaussian components, with parameters $\{\pi_k, \mathbf{\Sigma}_k, \boldsymbol{\mu}_k\}_{k=1}^{M}$. The membership of the feature $\mathbf{f}_p^j$ (corresponding to the j^{th} sample point of signature S_p of an user), to the k^{th} Gaussian component is a scalar value denoted by $g_p^j(k)$ and is given by:

$$g_p^j(k) = \frac{\pi_k \mathcal{N}(\mathbf{f}_p^j \mid \boldsymbol{\mu}_k, \mathbf{\Sigma}_k)}{\sum_{c=1}^{M} \pi_c \mathcal{N}(\mathbf{f}_p^j \mid \boldsymbol{\mu}_c, \mathbf{\Sigma}_c)} \tag{5.6}$$

The membership value $g_p^j(k)$ is a probability measure, bounded between 0 and 1. Likewise, using the above equation, we can evaluate the membership values of the feature $\mathbf{f}_p^j$ to each of the M Gaussian components. This results in a set of M probabilities, which can then be stacked into a M dimensional feature vector, of the form:

$$\mathbf{g}_p^j = [g_p^j(1) \;\; g_p^j(2) \;\; .... \;\; g_p^j(M)]^{\mathbf{T}} \tag{5.7}$$

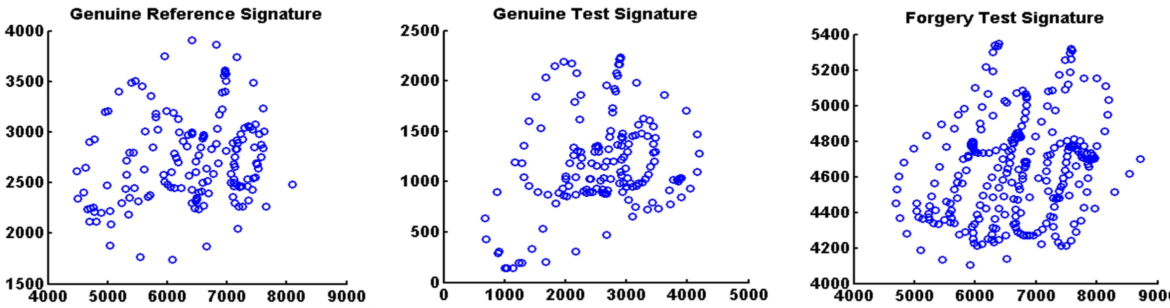
Any feature vector can thus be represented probabilistically in terms of membership values to different Gaussian components. We hereinafter refer to $\mathbf{g}_p^j$ as the membership feature vector / GMM based descriptor corresponding to the point based feature vector $\mathbf{f}_p^j$, derived from the temporal trace of the signature. For authentication, we encode each of the feature vectors of the signatures to be compared by their membership vectors, and then align them using the DTW algorithm, described in Section 3.4. The resulting matching score is then compared to a threshold for decision-making.

Owing to the fact that each of the values in the membership feature vector being matched is a number between 0 and 1, it can be inferred from Equation 3.8, the value of d_1^p will be bounded between 0 and 2 (with City Block distance as a dissimilarity measure in the cost matrix C).

It may be stated in passing that our methodology of obtaining membership vectors is closely related to the ideas presented in speech processing using the so 'Gaussian posterior-grams'. Such features have recently caught attention in applications such as keyword spotting [112] and speaker verification using short phrase utterance [113].

To demonstrate the utility of the proposed GMM based membership feature vectors for signature verification, we present in Figures 5.3(b) and (c), sample of a genuine and skilled forgery test signature, that is matched separately against the enrolled reference signature of an user in Figure 5.3(a). The signatures being depicted are from a user of the MCYT-100 database. For sake of illustration, we assume that there is only one signature of an user enrolled to the system. When the signatures are matched using the set of local features presented in Section 3.3, the DTW matching scores of the genuine and skilled forgery signature with the enrolled signature are found to be 0.55 and 0.52 respectively. We observe that the DTW score of genuine signature is higher than that of the skilled forgery signature, and hence, as discussed in Section 3.6, the decision making process will result in a wrong classification of these signatures.

This erroneous decision is alleviated with the use of GMM based membership feature description for the signature representation. When DTW is performed on the signatures, the d_1 scores of the genuine and forgery signature with the enrolled signature turns out to be 0.81 and 1.05 respectively. Considering that the genuine signature match has a DTW score lower than that of the skilled forgery signature, the decision making process will result in the correct verification of the signatures. For this illustration, we derive the membership feature vectors from a GMM comprising 32 Gaussian components.



(a) (b) (c)

Figure 5.3: Sub-figures (a), (b) and (c) depict the genuine reference signature, genuine test signature and skilled forgery test signature respectively from an user of the MCYT-100 database.

Table 5.1: Illustration of the DTW scores obtained using the proposed membership feature vectors, as compared to the feature vectors outlined in Section 3.3. The signatures mentioned in the first column refer to those of the MCYT-100 presented in Figure 5.3. A GMM comprising $M = 32$ Gaussian components is used for the extraction of member-ship feature vectors.

DTW Match	Feature vector in Section 3.3	GMM-based Membership feature vector
Genuine test signature - reference signature	0.55	0.81
Forgery test signature - reference signature	0.52	1.05

For better clarity, the preceding discussion with regards to the DTW scores obtained using the proposed membership feature vector is summarized in Table 5.1.

To further corroborate on our analysis, we present the histograms of the distance values accumulated along the length of the warping path for the genuine and skilled forgery signature match in Figures 5.4 (a)-(d). The bins in the first two sub-figures (namely (a) and (b)) are based on the distances in the cells of the warping path obtained by matching the signatures in Figure 5.3 (b) and (c) with Figure 5.3 (a) using the set of features described in Section 3.3. Clearly, we see that many of the bin indices have similar values with the computed City-Block distance between these histograms being 0.18. Contrast to that, if the signatures are matched using the GMM based membership feature vectors, we get the histograms shown in Figure 5.4 (c)-(d), that are more discriminating with a City Block distance of 0.37 between them. The high dissimilarity value obtained justifies empirically, our notion of considering the GMM based membership feature vectors in the DTW framework for enhancing the discrimination between the genuine and skilled forgery signatures.

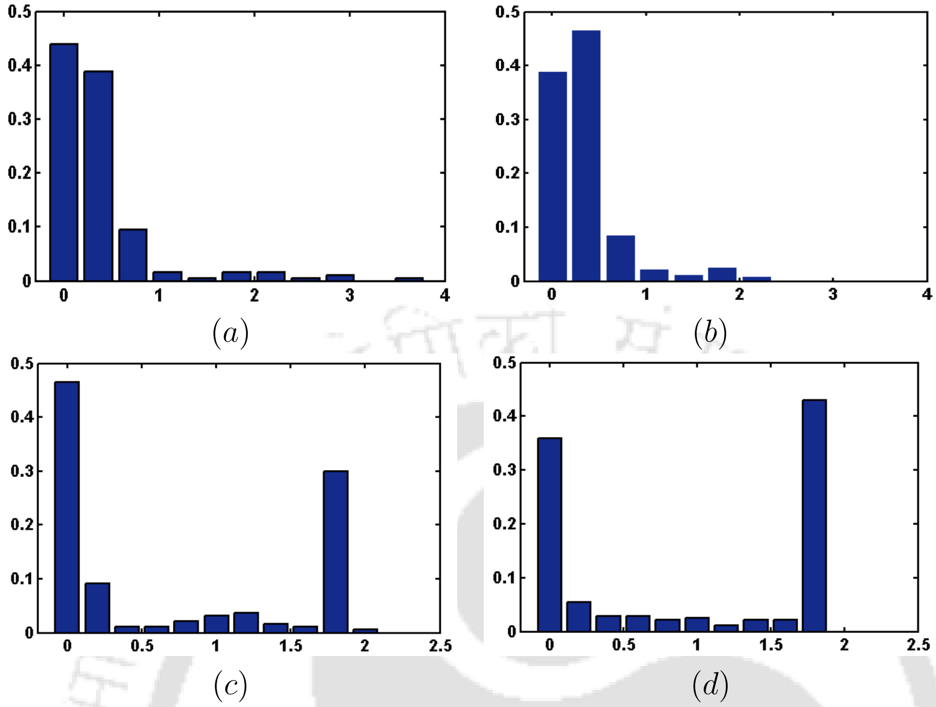


Figure 5.4: Illustration of the histograms of distance values falling on the warping path, resulting from a DTW match of a genuine and skilled forgery signature of Figure 5.3 (b)-(c) with the enrolled signature of Figure 5.3 (a). The sub-figures (a) and (b) represent histograms constructed using the set of features suggested in Section 3.3, while those in sub-figures (c) and (d) correspond to the GMM based descriptors - the membership feature vectors. For this illustration, we derive the membership feature vectors from a GMM comprising 32 Gaussian components.

As a follow-up to this discussion, we attempt at depicting the distribution of the values of the GMM based encoded features in their corresponding feature space. To begin with, we employ a subset of three features from the eleven dimensional feature vector (discussed in Section 3.3) and represent their values as a 3D-plot. The features being considered are Δx, Δy, Δp - first order differences of the x-coordinate, y coordinate and pressure p in Figure 5.5 (a) and (b). The genuine reference as well as genuine and forgery test signatures for this example correspond to those shown in Figure 5.3. Clearly, the feature value of the genuine reference and forgery test signatures are seen to overlap - thereby indicating that the forgery signature is likely to get falsely accepted as genuine. This issue can however be alleviated by referring to the 2-D plot of Figure 5.5 (c) and (d), that represents the membership value of two Gaussian components of the GMM. The selection of Gaussian components g_1 and g_2 correspond to those for which the membership value (averaged across the sample points of the reference signature)

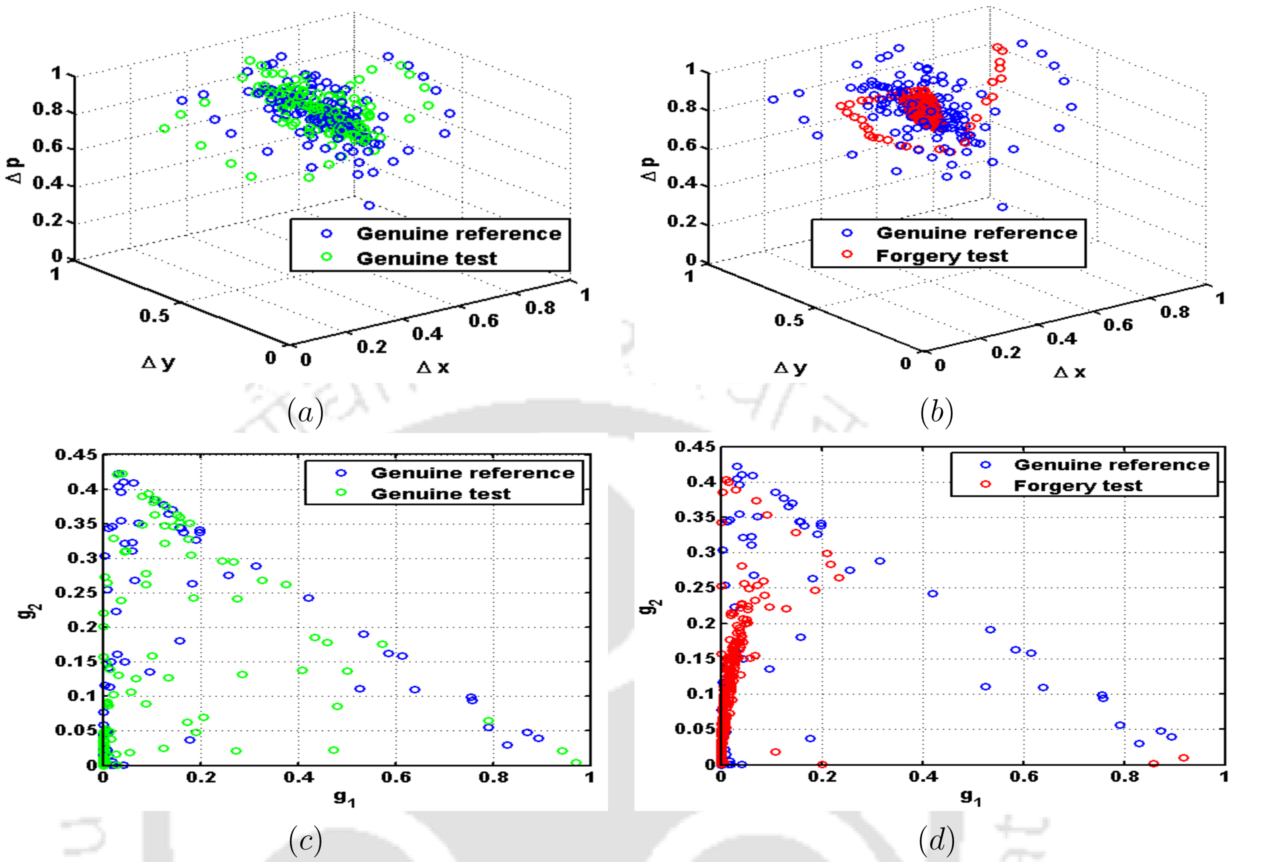
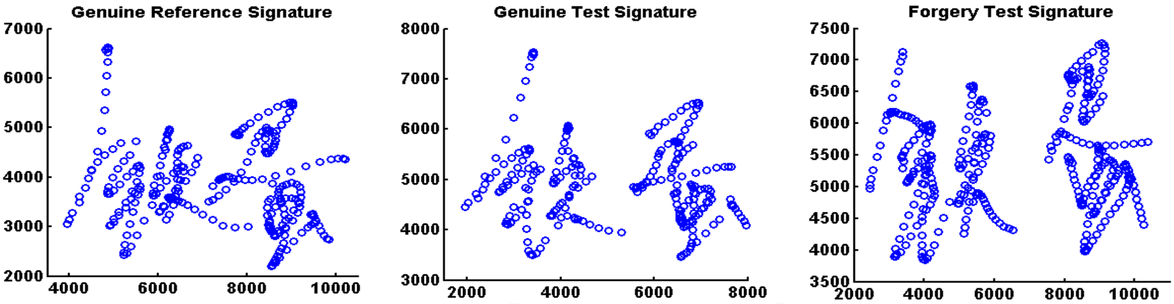


Figure 5.5: Illustration of discrimination capability of GMM descriptors over the set of temporal features for genuine and skilled forgery signature of an user from MCYT-100 database. The signatures being mentioned correspond to those presented in Figure 5.3.

is the first and second largest. Clearly, we see a better separation of the genuine reference signature and skilled forgery test signature in this representation.

Figure 5.6 presents another illustration to demonstrate the utility of the GMM descriptor representation for signature verification. In this case, we consider the DTW match of the genuine and skilled forgery test signatures (Figure 5.6 (b) and (c) respectively) with the genuine reference signature (Figure 5.6 (a)) of an user from the SVC-2004 database. With regards to the feature set presented in Section 3.3, the DTW scores for genuine and skilled forgery test signatures are 0.46 and 0.45 respectively. Clearly, with the score for the genuine test signature being higher to that of the skilled forgery test signature, we are faced with an incorrect decision. These signatures are however authenticated correctly with the proposed GMM based membership feature vectors that provide DTW scores of 1.24 and 1.39 respectively (refer Table



(a) (b) (c)

Figure 5.6: Illustration of genuine reference signature, genuine test signature and skilled forgery test signature in sub-figures (a), (b) and (c) respectively from a user of SVC-2004 database.

Table 5.2: The score obtained by DTW matching, among the signatures of Figure 5.6 using the proposed membership feature vectors and the feature vectors discussed in Section 3.3. A GMM comprising $M = 32$ Gaussian components is used for the extraction of member-ship feature vectors.

DTW Match	Feature vector in subsection 3.3	GMM-based Membership feature vector
Genuine test signature - reference signature	0.46	1.24
Forgery test signature - reference signature	0.45	1.39

5.2). Here again, the GMM based descriptor is derived with number of Gaussian components $M = 32$.

The preceding discussion is bolstered further by considering the histograms of distance values accumulated along the length of the warping path in the DTW cost matrix. The histograms of Figures 5.7 (a) and (b), corresponding to the match of the genuine and skilled forgery test signatures with the reference signature respectively, is constructed from the feature set described in Section 3.3. Likewise, for the Figures 5.7 (c) and (d), the histograms are based on the GMM membership feature vectors. Empirically, we see that the City-Block distance of dissimilarity between histograms of Figures 5.7 (a) and (b) is found to be 0.07. This is lower than 0.32 - the value obtained from the histograms of Figures 5.7 (c) and (d). This trend in a way demonstrates the improved discrimination between genuine and skilled forgery signatures by using the GMM based descriptor.

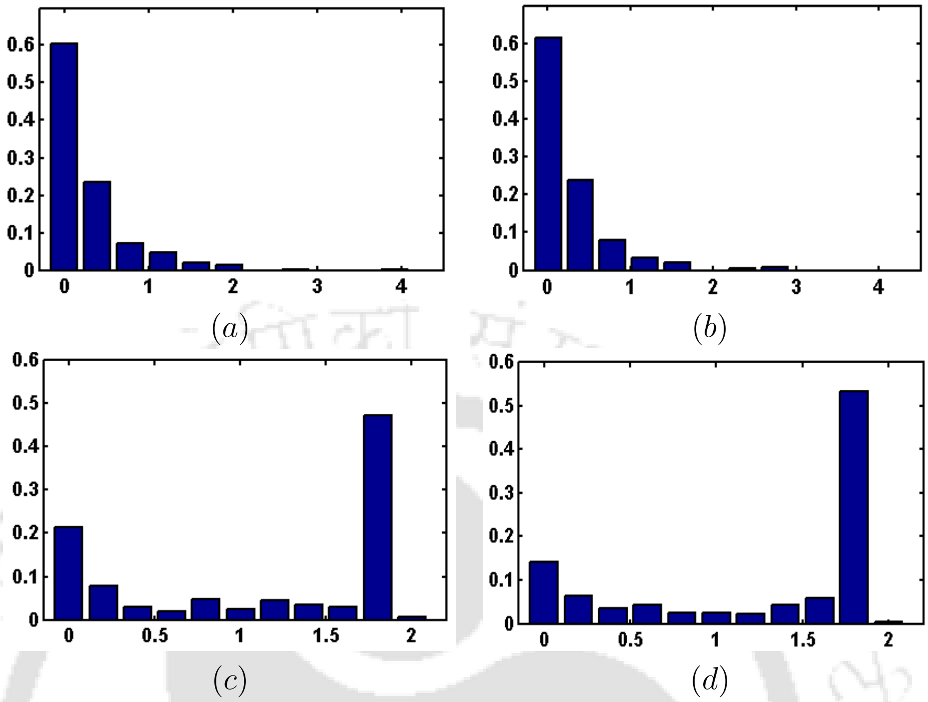


Figure 5.7: The histograms of distance values falling on the warping path, obtained by DTW match of a genuine and skilled forgery signature of Figure 5.6 (b)-(c) with the enrolled signature of Figure 5.6 (a). The sub-figures (a) and (b) corresponds to the histograms constructed using the set of features described in Section 3.3, while those in sub-figures (c) and (d) correspond to the GMM based descriptors - the membership feature vectors. For this illustration, we derive the membership feature vectors from a GMM comprising 32 Gaussian components.

5.4.2 Warping Path Score Derivation

We now outline our strategy that utilizes the characteristics of the warping path in the DTW cost matrix for the verification of online signatures. The idea is to consider the DTW alignment (a_i, b_i), together with another alignment (a_i, r_i^*) - the computation of which is described in the following paragraph. The characteristics of each of the alignments are captured with the aid of separate histograms, whose corresponding bin indices are voted, based on the GMM based membership vectors. Thereafter, the two obtained histograms are matched, and the resulting score obtained is fused with that of the DTW score. This score combination is shown to improve the discrimination between the genuine and skilled forgery signatures.

5.4.2.1 Computation of (a_i, r_i^*)

For the textual presentation in this subsection, we consider that the test signature S_T is temporally aligned with the p^{th} enrolled signature S_p, using the DTW algorithm discussed in Section 3.4. Also the cells $(a_i, b_i)_{i=1}^{l_{\mathcal{W}_p^*}}$ of the warping path (denoted by $\mathcal{W}_p^*$) are presumed to be known to us. Corresponding to each alignment (a_i, b_i), along the warping path $\mathcal{W}_p^*$, we consider another alignment (a_i, r_i^*). The mathematical formulation for obtaining the index r_i^* of the sample point in the reference signature S_p is as follows:

$$r_i^* = \arg \min_{1 \leq s \leq n_p - 2} |\mathbf{g}_T^{a_i} - \mathbf{g}_p^s| \qquad 1 \leq i \leq l_{\mathcal{W}_p^*} \tag{5.8}$$

Here $\mathbf{g}_T^{a_i}$ corresponds to the GMM based membership feature vector for the a_i^{th} sample point in test signature S_T. The above equation suggests us to search along the a_i^{th} row of the cost matrix C and then assign the index of the sample point, whose GMM based membership feature vector provides the closest City Block distance match to $\mathbf{g}_T^{a_i}$. Accordingly, we can rewrite Equation 5.8 as:

$$r_i^* = \arg \min_{1 \leq s \leq n_p - 2} d(a_i, s) \qquad 1 \leq i \leq l_{\mathcal{W}_p^*} \tag{5.9}$$

The above computation can be performed $\forall a_i$ in the warping path $\mathcal{W}_p^*$, thus leading to another set of alignments of the form:

$$\ominus_p^* = \{(a_1, r_1^*), (a_2, r_2^*), ..., (a_{l_{\mathcal{W}_p^*}}, r_{l_{\mathcal{W}_p^*}}^*)\} \tag{5.10}$$

To handle the infrequent case, where more than one match can give rise to multiple values of r_i^*, we consider the value corresponding to the minimum $d(a_i, r_i^*)$. Note that the pair (a_i, r_i^*) refers to the cell in the a_i^{th} row and $(r_i^*)^{th}$ column in cost matrix C. From the definitions of the alignments (a_i, b_i) and (a_i, r_i^*) , we can make the following inferences:

(i) Both b_i and r_i^* correspond to an index in the enrolled reference signature S_p.

(ii) The warping path of DTW always passes through the alignment (a_i, b_i) $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$ in the cost matrix. As mentioned in Section 3.4, (a_i, b_i) represent the indices of the warping path, obtained from back tracing the sequence of cells in the cost matrix, whose corresponding dissimilarity values contributed to making up the DTW score.

(iii) However, it is not mandatory for the warping path of DTW to always pass through the alignment (a_i, r_i^*) $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$. This is owing to the fact that r_i^* is obtained via a nearest match, along the a_i^{th} row of the cost matrix C, as described in Equation 5.9.

(iv) It is important to mention that (a_i, r_i^*) is not related to the warping path, as such. Accordingly, the continuity and monotonicity condition as required in a DTW framework do not apply.

5.4.2.2 Generation of the histograms

Given the set of alignments in $\mathcal{W}_p^*$ and $\ominus_p^*$, we construct histograms, denoted as $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ respectively. It may be stated here that the description of the histogram generation process outlined below as such seem to bear some resemblance to the concept of Bag-of-Words [114,115] popularly used for object detection and retrieval in computer vision applications.

Each of the histograms comprise M bins, corresponding to the number of Gaussian components in the GMM. Initially, the votes in each of the indices are set to zero. Corresponding to each b_i, such that $(a_i, b_i) \in \mathcal{W}_p^*$, the indices in the histogram $\mathcal{H}_{\mathcal{W}_p^*}$ are voted in accordance to the GMM membership feature vectors $\mathbf{g}_p^{b_i}$. In other words, the k^{th} bin of $\mathcal{H}_{\mathcal{W}_p^*}$ is accumulated with a vote of magnitude $g_p^{b_i}(k)$, namely, the k^{th} feature value in the membership vector $\mathbf{g}_p^{b_i}$. For a given M dimensional membership vector, the above accumulation of votes is performed across all the M indices in $\mathcal{H}_{\mathcal{W}_p^*}$. Likewise, the process is continued for all values of sample points b_i in S_p, $\forall i \in \{1, 2, ..., l_{\mathcal{W}_p^*}\}$. The resulting votes of the histogram indices are then normalized with the length of the warping path $l_{\mathcal{W}_p^*}$, to ensure that they are in the numeric range $[0, 1]$.

A similar voting procedure is performed to generate the histogram $\mathcal{H}_{\ominus_p^*}$. However here, the accumulation of votes is done using the membership vectors $\mathbf{g}_p^{r_i^*}$ in S_p, $\forall i \in \{1, 2, ..., l_{\mathcal{W}_p^*}\}$. It is worth reminding that both b_i and r_i^* correspond to an index in the enrolled reference signature S_p. As in the case of $\mathcal{H}_{\mathcal{W}_p^*}$, normalization of votes in $\mathcal{H}_{\ominus_p^*}$ is performed using $l_{\mathcal{W}_p^*}$. For better clarity, the generation of the histograms is summarized in Algorithm 4.

We now present on how the characteristics of the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ can be exploited

Algorithm 4 Histogram Generation : $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$

(i) Perform the DTW match of the test signature S_T with the p^{th} enrolled signature, S_p of an user. The membership feature vectors corresponding to S_T and S_p, (as derived from a pre-trained GMM of M Gaussian components) is used for the alignment of the online traces.

(ii) Extract the cells (a_i, b_i) in the warping path $\mathcal{W}_p^*$ from the DTW cost matrix by back-tracing.

(iii) Corresponding to each cell $(a_i, b_i) \in \mathcal{W}_p^*$, compute the alignment (a_i, r_i^*) using Equation 5.9

(iv) Initialize two histograms, $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$, with zero votes for each of the M bins.

(v) **For** every $(a_i, b_i) \in \mathcal{W}_p^*$ and $(a_i, r_i^*) \in \ominus_p^*$, $\forall i \in \{1, 2, ..., l_{\mathcal{W}_p^*}\}$
For every $k = 1 : M$
Accumulate the k^{th} bin of $\mathcal{H}_{\mathcal{W}_p^*}$ with the vote of magnitude $g_p^{b_i}(k)$
Accumulate the k^{th} bin of $\mathcal{H}_{\ominus_p^*}$ with the vote of magnitude $g_p^{r_i^*}(k)$
End
End

(vi) Normalize the votes of the indices of $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$, with the length of the warping path $l_{\mathcal{W}_p^*}$.

to propose a novel score, that can aid in verifying online signatures. To begin with, consider the matching of a genuine test signature S_T against a reference genuine signature S_p in the enrolled set. Owing to the high degree of similarity between parts of the trace, one should expect, the feature vectors $\mathbf{g}_p^{b_i}$ and $\mathbf{g}_p^{r_i^*}$, to be close to each other for most values of i, $1 \leq i \leq l_{\mathcal{W}_p^*}$. The limiting scenario occurs when a genuine test signature S_T is perfectly matched against S_p, wherein, the cost matrix obtained is a square matrix, whose diagonal elements are zero, with non-negative values in the off-diagonal entries. In this case, the DTW score is zero and $\mathbf{g}_p^{b_i} = \mathbf{g}_p^{r_i^*}$, $\forall i$, $1 \leq i \leq l_{\mathcal{W}_p^*}$. Accordingly, the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ are perfectly matched with a dissimilarity value of zero. Coming now, for the non-ideal case of a genuine match with a reference signature, we expect to see the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ exhibit a high degree of similarity.

The contrary is true when a skilled forgery test signature is compared against an enrolled genuine signature. In this case, each of the feature vectors $\mathbf{g}_p^{b_i}$ and $\mathbf{g}_p^{r_i^*}$ are not that likely to be close, as compared to a genuine-to-reference signature match. Hence, one can expect the normalized values of the bins of the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ to exhibit a lesser degree of similarity. Based on this discussion, we suggest using the degree of dissimilarity between the histograms under consideration as a measure to characterize the warping path. We denote the warping path score, obtained from a match of a test signature with the p^{th} enrolled signature, S_p of an user by d_2^p.

Let $\{h_{\mathcal{W}_p^*}(k)\}_{k=1}^{M}$ and $\{h_{\ominus_p^*}(k)\}_{k=1}^{M}$ correspond to the votes in the M bins of the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ respectively. The proposed warping feature d_2^p is the City Block distance between these histograms, defined as:

$$d_2^p = \sum_{k=1}^{M} |h_{\mathcal{W}_p^*}(k) - h_{\ominus_p^*}(k)| \tag{5.11}$$

It may also be inferred from the expression above, that the value of d_2^p would be bounded between 0 and 2 - this being the case, since the votes of the histogram bins has been normalized with the length of the warping path $l_{\mathcal{W}_p^*}$ during its generation (refer Algorithm 4).

5.4.2.3 An illustrative example

To demonstrate the usefulness of the warping path score for signature verification in MCYT-100 database, we present a DTW matching of a genuine and skilled forgery signature in Figures 5.8(b) and (c) with the genuine reference signature of Figure 5.8(a). The DTW is performed on the membership feature vectors, derived from the GMM, as discussed in sub-section 5.4.1. Figures 5.8 (d) and (e) depict the histograms $\mathcal{H}_{\mathcal{W}^*}$ and $\mathcal{H}_{\ominus^*}$, corresponding to a genuine-signature match. The same histograms, as obtained from the skilled forgery signature match, is shown in Figures 5.8 (f) and (g). Clearly, the City Block distance between the histograms of Figures 5.8 (d) and (e) are lower compared to those between the Figures 5.8 (f) and (g) - their values being 0.49 and 0.98 respectively.

Likewise to the above, we perform a similar analysis on the match of a genuine and skilled forgery test signature with the genuine reference signature of an user from the SVC-2004 database (refer Figure 5.9). The City-Block distance between the histogram $\mathcal{H}_{\mathcal{W}^*}$ and $\mathcal{H}_{\ominus^*}$ (Figure 5.9(d) and (e)) resulting from the genuine signature match is observed to be 0.43 , while it is 0.60 for skilled forgery test signature (Figure 5.9(f) and (g)).

5.4.3 Fusion

Given a test signature S_T, we obtain values of d_1 and d_2 scores corresponding to N enrolled signatures of a user and average them respectively. Thereafter, the sum rule based score fusion scheme as discussed in Section 3.5.3 is utilized for authentication. The need of fusion is motivated by the complementary nature of d_1^{mean} and d_2^{mean} - as presented on a two dimensional plot in Figure 5.10 (a) and (b) for the MCYT-100 and SVC-2004 database respectively.

As a summary to our proposal, we present a pseudo-code in Algorithm 5.

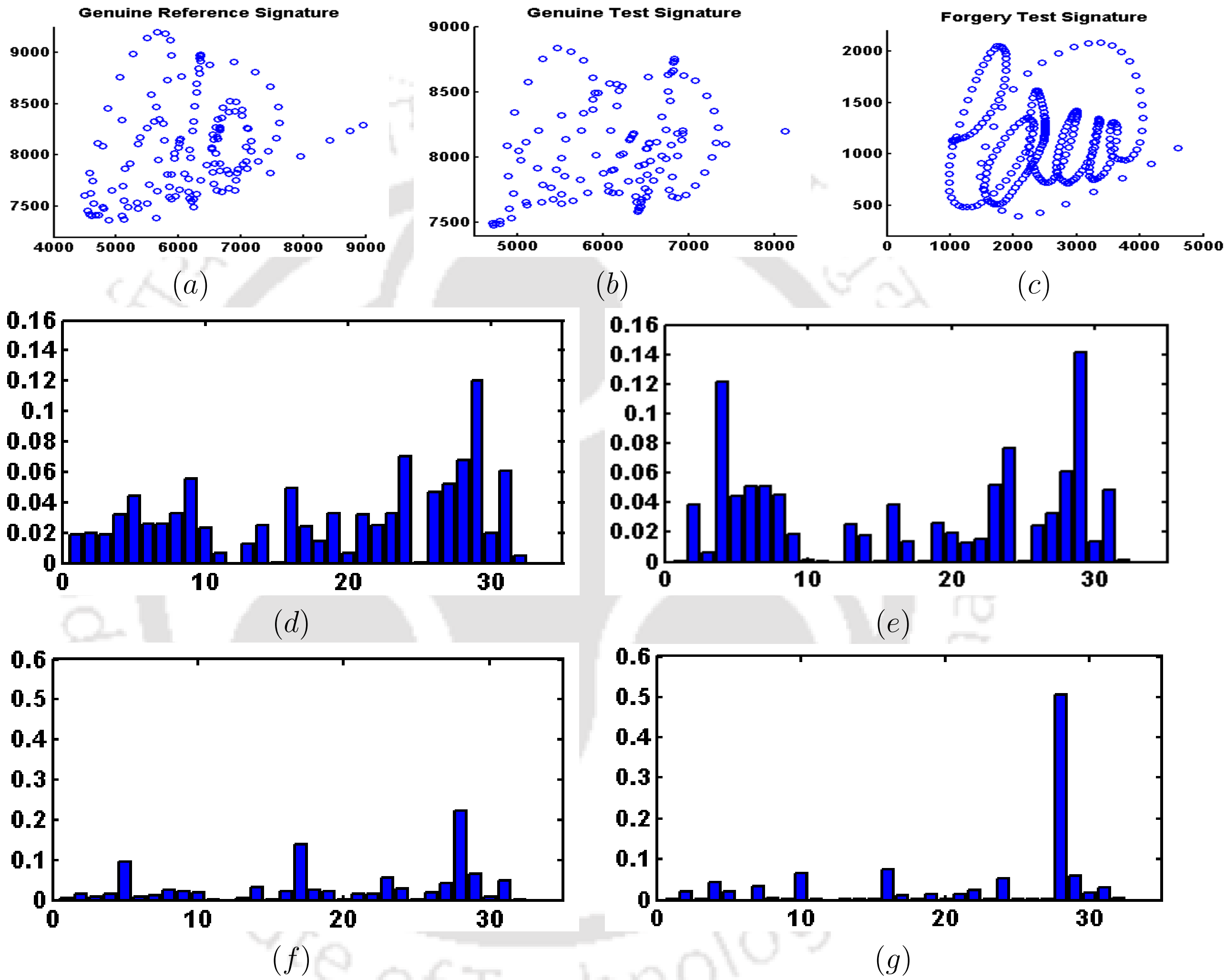


Figure 5.8: Sub-figures (a), (b) and (c) depict the genuine reference signature, genuine test signature and skilled forgery test signature respectively from an user of the MCYT-100 database. The histograms $\mathcal{H}_{\mathcal{W}^*}$ and $\mathcal{H}_{\ominus^*}$, corresponding to a genuine-signature match to the reference signature is shown in sub-figures (d) and (e). On the other hand, the histograms $\mathcal{H}_{\mathcal{W}^*}$ and $\mathcal{H}_{\ominus^*}$, corresponding to a skilled forgery-signature match to the reference signature is presented in sub-figures (f) and (g). For this illustration, we derive the membership feature vectors from a GMM comprising 32 Gaussian components.

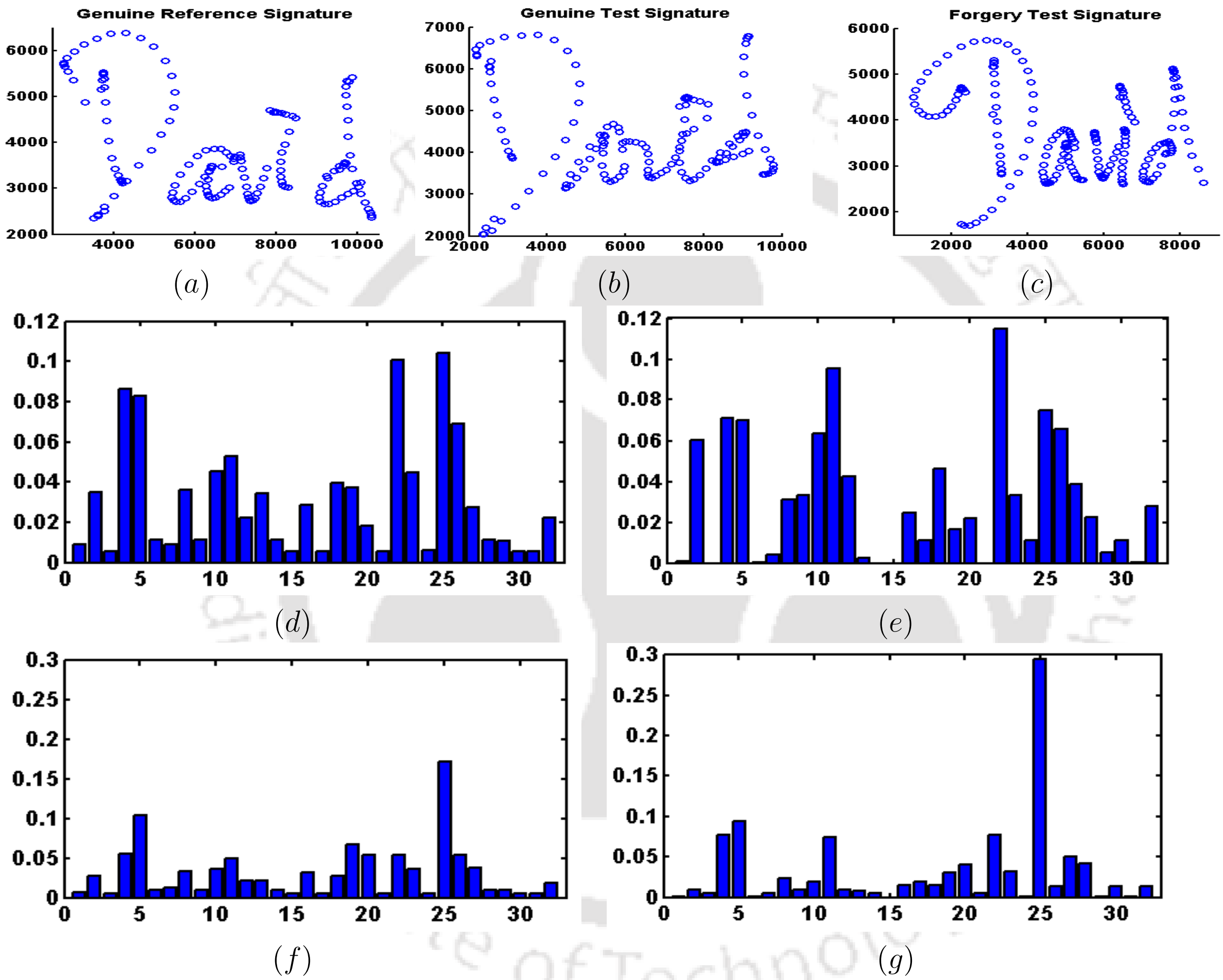


Figure 5.9: Illustration of the genuine reference signature, genuine test signature and skilled forgery test signature in sub-figures (a), (b) and (c) respectively from a user of the SVC-2004 database. The histograms $\mathcal{H}_{\mathcal{W}^*}$ and $\mathcal{H}_{\ominus^*}$, corresponding to a genuine test signature with the reference signature and forgery test signature with the reference signature match is shown in sub-figures (d)-(e) and (f)-(g) respectively. Here the membership feature vectors are derived from a GMM comprising 32 Gaussian components.

Algorithm 5 Proposed signature verification algorithm

Input: Test signature S_T ; a set of N enrolled reference signatures of an user denoted as $\{S_1, S_2, ..., S_N\}$
User specific pre-trained GMM with M number of Gaussian components parameterized with π_k, $\boldsymbol{\mu}_k$, and $\boldsymbol{\Sigma}_k$ $\quad 1 \leq k \leq M$.

For $p = 1 : N$

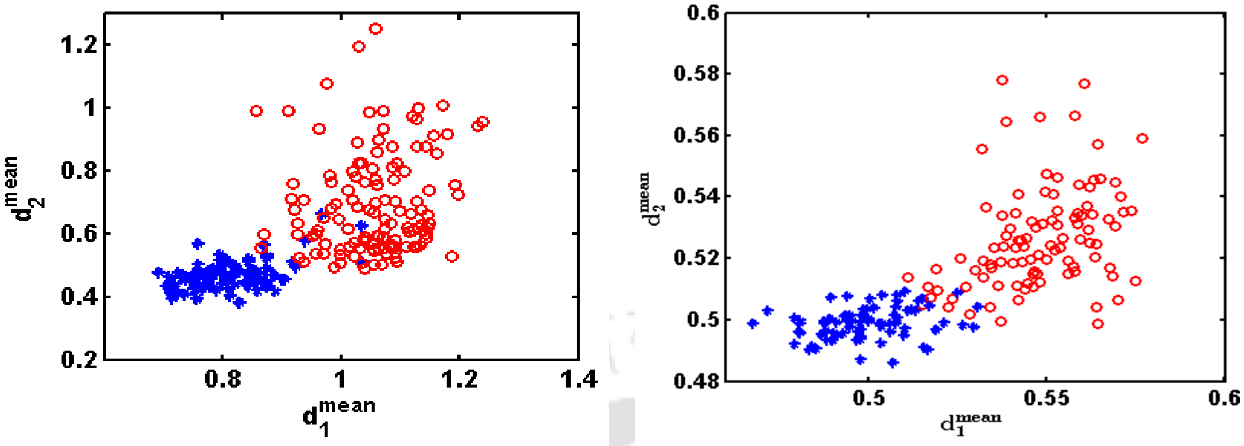
- Derive the sequence of point based feature vectors from Section 3.3 for the signature S_T and S_p.
- Compute the GMM based descriptor corresponding to each feature vector on the trace of S_T and S_p. (refer sub-section 5.4.1)
- Perform the DTW match of S_T and S_p using the GMM descriptors to obtain d_1^p score (refer Section 3.4)
- Extract the cells (a_i, b_i) along the warping path $\mathcal{W}_p^*$ from the DTW cost matrix by back-tracing.

`% Computation of the warping path score`

- Compute the histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ as enumerated in steps (iii)-(vi) of Algorithm 4.
- Compute the City-Block distance between the above two histograms to obtain the warping path score d_2^p.

End

- Fuse the N scores $\{d_1^p\}_{p=1}^N$ and $\{d_2^p\}_{p=1}^N$ using the sum rule. (refer sub-section 5.4.3)
- Use the fused score for authentication.



(*a*) (*b*)

Figure 5.10: Two dimensional distance plot of a user's genuine and skilled forgery signatures (depicted by blue and red color respectively) taken from MCYT-100 and SVC-2004 databases in sub-figure 5.10(a) and (b) respectively. The number of reference signatures employed=5. The experimental set-up discussed in sub-section 3.7 is used in generating this plot. For this illustration, we derive the membership feature vectors from a GMM comprising 32 Gaussian components in MCYT-100 and SVC-2004 databases respectively.

5.5 Results and Discussion

With regards to the enrollment and evaluation protocol, we use the same as discussed in Section 3.7 for the SVC-2004 and MCYT-100 databases respectively.

Prior to outlining the results of the experiments, demonstrating our proposal, we provide details of the systems being implemented, together with their abbreviations, for the discussions in this Section. It may be noted that both *GMM-DTW* and *FUS3* systems are the proposals of this work.

- *BL-DTW*: A DTW system, wherein the alignment of signatures being compared is based on the point based feature set discussed in Section 3.3.
- *GMM-LIKE*: A verification system that relies on the GMM likelihood function (described in Section 5.3) to authenticate the signature [3].
- *GMM-DTW*: A DTW system, wherein the alignment of signatures being compared is

[3] The performance of the *GMM-LIKE* system on the MCYT-100 and SVC-2004 databases has been incorporated, merely for sake of completion, in Tables 5.3 and 5.9 respectively.

Table 5.3: Performance evaluation of the proposal - *GMM-DTW* and *FUS3* systems on the MCYT-100 Database for different number of Gaussian components M in the GMM.

M	User Threshold				Common Threshold			
	GMM-LIKE system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system	*GMM-LIKE* system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system
-	-	7.40	-	-	-	10.94	-	-
2	15.94	-	26.23	31.12	20.42	-	32.97	39.27
4	14.49	-	11.44	13.80	18.69	-	15.09	18.47
8	13.13	-	9.70	6.49	16.94	-	13.63	10.90
16	11.42	-	6.80	3.59	14.94	-	9.98	6.68
32	8.82	-	4.44	1.93	12.82	-	7.18	3.94
64	6.53	-	5.54	1.99	11.61	-	8.61	4.17
128	7.63	-	7.12	2.65	12.94	-	11.49	5.37

based on the proposed GMM-based membership feature vectors discussed in subsection 5.4.1.

- *FUS3*: A system wherein the proposed warping path feature (discussed in subsection 5.4.2) is fused to that of the DTW score of the *GMM-DTW* system.

5.5.1 Performance Evaluation on MCYT-100 Database

As a first exploration, we outline in Table 5.3, the performance of the proposed *GMM-DTW* and *FUS3* systems for the number of Gaussian components M in the GMM, varying from 2 to 128. The results of the *BL-DTW* are also noted for comparison. For this experiment, we choose the values of M in powers of 2. It can be observed from the fourth and eighth columns, that the *GMM-DTW* system provides reduced MEER results over the *BL-DTW* for number of Gaussian components M= 16, 32 and 64 in the GMM. The lowest MEER of 7.18% is obtained using 32 Gaussian components - this corresponds to a performance improvement of 34.37% over the *BL-DTW* of 10.94%, using common threshold. Also, a reduction of MEER by 40% can be inferred for the user threshold case - with the MEER reducing from 7.40% (*BL-DTW*) to 4.44% (*GMM-DTW*). The improved performance can be attributed to the fact that the signature representation using the GMM based membership feature vectors encapsulates the statistical characteristics of the parts of the trace, apart from the temporal information, that is taken into consideration by the DTW. However, with fewer number of Gaussian components M in the GMM, the finer nuances useful for the discrimination of genuine and forgery signature are not adequately captured. This is primarily, due to the problem of under-fitting, wherein the number of model parameters learnt by the GMM are not sufficient to characterise all the variabilities in the feature vectors, specific to an user. This trend is evident for the case of M = 2, 4 and 8. With the increase in number of Gaussian components, this problem is alleviated with the GMM based membership feature vector providing an increased discrimination between genuine and forgery signature in the *GMM-DTW* system. However, with very large values of M, the problem of over-fitting begins to reduce the verification capability, due to the lack in the number of the feature vectors for modeling the large number of the GMM parameters. Hence, for $M = 128$, we see an increase in MEER to 11.49% for the case of common threshold - this value being higher than the MEER of 10.94% of the *BL-DTW* system.

Coming, now to the *FUS3* system, we again see further reductions in MEER for Gaussian components greater than 4 in the GMM. The sum rule, described by the Equation 3.18 is used for implementing this system. We obtain the lowest MEER of 3.94% at $M = 32$ for the common threshold setting. When compared to the baseline *BL-DTW* system of MEER 10.94%, the efficacy of the *FUS3* system is commendable, with an improvement of 63.99 %. Another noteworthy point here is with regards to the performance of the *FUS3* system at high number of Gaussian components. We see an improvement over the *BL-DTW*, even at $M = 128$ - with MEERs of 5.37 % and 2.65% for common and user threshold setting respectively. Considering that $M = 32$ provides the lowest MEER for the performance of the *FUS3* system, for the following next three experiments described, we choose a GMM comprising same number of Gaussian components for further evaluation of the proposal.

Apart from using the mean of distance scores d_1^{mean} and d_2^{mean} between reference and test signature for the sum rule based fusion (Equation 3.18), we experimented on the combination schemes presented in Equation 3.19. Table 5.4 outlines the results of the *BL-DTW*, *GMM-DTW* and *FUS3* systems on these strategies. The sum rule based on mean of distance values outperforms the other, with the MEER of 3.94% for the *FUS3* system with common threshold

Table 5.4: Performance of the combination strategies (referred to in Equations 3.18 and 3.19) on the MCYT-100 Database. The number of Gaussian components $M = 32$ is used for the extraction of the GMM based membership feature vector.

Method	User Threshold			Common Threshold		
	BL-DTW system	*GMM-DTW* system	*FUS3* system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system
Mean	7.40	4.44	1.99	10.94	7.18	3.94
Minimum	7.65	4.51	2.35	11.23	7.41	4.12
Maximum	9.05	6.12	4.14	13.32	9.43	5.87

Table 5.5: The MEER (in %) for the MCYT-100 database using different combination strategies outlined in Table 4.1 for the $FUS3$ system. The corresponding values of weight parameter β is presented in fourth column. The number of Gaussian components $M = 32$ is used for the extraction of the GMM based membership feature vector.

Combination Scheme	MEER (in %)		β
	User Threshold	Common Threshold	
Sum rule	1.99	3.94	1.5
Weighted sum rule	1.36	3.35	1.4
Weighted minimum rule	1.78	3.46	1
Weighted product rule	1.12	3.19	1.5

setting. The minimum and maximum based strategies of sum rule, on the other hand, achieves MEERs of 4.12% and 5.87% respectively. The mean-based technique in a way, achieves better performance by smoothing out the intra-user variations by averaging the scores d_1 and d_2 over the set of reference signatures, prior to combining them. This explains its improvement in verification over the other two strategies. Nevertheless, we see that our proposed *GMM-DTW* and *FUS3* systems outperform the *BL-DTW* system across all the three strategies.

An empirical study using strategies such as weighted sum, minimum and product on the *FUS3* system is presented in Table 5.5, resulting in an MEER to as low as 3.19% and 1.12% with common and user thresholds for the weighted product.

We next consider evaluating the performance of proposed system with varying number of reference signature samples. From Table 5.6, we infer a reduction in MEER with increase in the number of reference signatures. In particular, the *FUS3* system achieves an error rate to as low as 2.71% and 0.86%, with 20 enrolled samples, for common and user thresholds respectively. However, this reduction comes with a trade-off of comparisons against more number of enrolled signatures in the DTW process.

It may be noted that the *BL-DTW* system considered in the preceding discussions was implemented using the point-based features in Section 3.3. Thereafter, reduction in MEER based on our proposal were cited with regards to this system. We believe that the proposed GMM based membership feature vectors in the DTW alignment for verification is quite generic. The reasoning to the same is that the underlying statistical variability of the different features is used for the alignment between signatures in the proposed *GMM-DTW*, rather than the feature value itself.

As a empirical validation to our claim, we experiment the different systems - the *BL-DTW*, *GMM-DTW*, *FUS3* on subsets of features from Section 3.3. In total, six subsets of features were chosen. For notational convenience, we provide in Table 5.7, abbreviations for these sets, together with their definitions. It may be noted that the eleven dimensional feature vector used for the preceding experiments corresponds to the set D_6. We wish to state that the choice of feature subsets in Table 5.7 is not based on any selection algorithm - rather that the main goal here is to only validate the effectiveness of the proposal to multiple feature sets. As before, we experiment with five enrolled signatures per user, using both common and user threshold settings.

Table 5.8 summarizes the results on the different feature sets. The optimal number of Gaussian components M in the GMM, corresponding to the best MEER obtained is also provided for each set separately. Based on the entries in the Table, one can clearly infer an improvement in the verification performance by adopting the proposed *GMM-DTW* and *FUS3* systems, in place of the *BL-DTW*.

Table 5.6: Efficacy of the proposed *GMM-DTW* and *FUS3* system when different number of genuine reference signatures from the MCYT-100 database are enrolled to the verification system. A GMM comprising $M = 32$ Gaussian components is used for the extraction of member-ship feature vectors.

# of enrolled signatures	User Threshold			Common Threshold		
	BL-DTW system	*GMM-DTW* system	*FUS3* system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system
5	7.40	4.44	1.99	10.94	7.18	3.94
10	6.84	4.43	1.72	9.72	6.05	3.04
15	6.20	3.93	1.17	8.94	5.60	2.92
20	5.51	3.64	0.86	8.81	5.96	2.71

Table 5.7: Overview of the different feature subsets used for demonstrating the efficacy of our proposal in Table 5.8.

Notation	Feature sub-set
D_1	$[\Delta x, \Delta y]$
D_2	$[\Delta x, \Delta y, \Delta p]$
D_3	$[\Delta x, \Delta y, \Delta p, \sin\alpha, \cos\alpha]$
D_4	$[\Delta x, \Delta y, \Delta p, \Delta\theta, \Delta\phi, \sin\alpha, \cos\alpha]$
D_5	$[\Delta x, \Delta y, \Delta p, \Delta^2 x, \Delta^2 y, l, \Delta l, \sin\alpha, \cos\alpha]$
D_6	$[\Delta x, \Delta y, \Delta p, \Delta\theta, \Delta\phi, \Delta^2 x, \Delta^2 y, l, \Delta l, \sin\alpha, \cos\alpha]$

5.5.2 Performance Evaluation on SVC-2004 Database

With regards to the SVC-2004 database, the performance of the proposed $GMM-DTW$ and $FUS3$ systems for different number of Gaussian components M is shown in Table 5.9. It may be noted that the trend with regards to the variation of the MEERs are similar to those obtained for the MCYT-100 database. To start with, the *BL-DTW* provides MEER values of 13.28% and 20.33% with user and common threshold set-up respectively. The enhancement in the verification capability can be observed with the $GMM-DTW$ and $FUS3$ systems for number of Gaussian components M greater than 16 in the GMM. In particular, the $FUS3$ system with value of $M = 64$ provides the least MEER value of 12.12% for the common threshold - an improvement of 40.38 % over that of the *BL-DTW*. As with the MCYT-100 database, we observe an increase in the MEERs at small values of M (specifically less than 16) due to the problem of under-fitting. Likewise, at $M = 128$, with the insufficiency of data

Table 5.8: Performance evaluation of the *BL-DTW*, *GMM-DTW* and *FUS3* system on MCYT-100 database with different subsets of features. The optimized number of Gaussian components M used for the extraction of member-ship feature vectors in each case is also presented.

Feature subset	# of Gaussians M	User Threshold *BL-DTW* system	User Threshold *GMM-DTW* system	User Threshold *FUS3* system	Common Threshold *BL DTW* system	Common Threshold *GMM-DTW* system	Common Threshold *FUS3* system
D_1	8	10.30	3.64	2.62	13.65	6.65	5.62
D_2	16	13.87	3.74	1.40	17.32	6.87	3.63
D_3	32	6.16	8.12	2.97	9.60	11.26	5.88
D_4	32	8.57	7.62	2.78	12.43	10.69	5.93
D_5	32	5.04	4.58	1.68	8.47	6.67	4.11
D_6	32	7.40	4.44	1.99	10.94	7.18	3.94

Table 5.9: Performance of *GMM-DTW* and *FUS3* systems on the SVC-2004 Database with varying number of Gaussian components M employed for GMM.

M	User Threshold *GMM-LIKE* system	User Threshold *BL-DTW* system	User Threshold *GMM-DTW* system	User Threshold *FUS3* system	Common Threshold *GMM-LIKE* system	Common Threshold *BL-DTW* system	Common Threshold *GMM-DTW* system	Common Threshold *FUS3* system
-	-	13.28	-	-	-	20.33	-	-
2	16.95	-	39.27	44.68	23.95	-	46.98	49.85
4	16.91	-	25.29	29.67	23.61	-	32.24	37.35
8	15.05	-	18.80	19.45	21.68	-	25.24	26.30
16	13.71	-	15.32	14.07	19.53	-	22.06	20.86
32	12.10	-	9.53	7.82	18.62	-	18.14	16.04
64	15.50	-	7.35	5.52	20.80	-	14.96	12.12
128	13.80	-	7.87	6.41	20.35	-	16.14	13.78

to model the high number of Gaussian components, we once again encounter a decrease in performance - when compared to $M = 64$. Nonetheless, with regards to the $BL - DTW$ system, there is still significant reduction in MEER with the *FUS3* system. By noting that 64 Gaussian components in the GMM resulted in the lowest MEER for the *FUS3* system, we use the same number for the following three experiments.

The performance of our strategy with the combination schemes, given in Equation 3.19 are presented in Table 5.10. Similar to MCYT-100 database, we observe that the strategy based on the mean of scores fares better amongst the other two for both the *GMM-DTW* and *FUS3* systems. An evaluation of score fusion techniques with weighted sum, minimum and product is presented in Table 5.11.

Table 5.10: Performance of the combination strategies (given in Equations 3.18 and 3.19) on the SVC-2004 database. The number of Gaussian components used for the extraction of the GMM based membership feature vector is $M = 64$.

Method	User Threshold			Common Threshold		
	BL-DTW system	*GMM-DTW* system	*FUS3* system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system
Mean	13.28	7.35	5.52	20.33	14.96	12.12
Minimum	13.62	7.58	5.74	20.45	15.12	12.45
Maximum	14.01	8.60	6.25	21.43	16.25	14.01

Table 5.11: The MEER (in %) for the SVC-2004 database using different combination strategies outlined in Table 4.1 for the $FUS3$ system. The corresponding values of weight parameter β is presented in fourth column. The number of Gaussian components used for the extraction of the GMM based membership feature vector is $M = 64$.

Combination Scheme	MEER (in %)		β
	User Threshold	Common Threshold	
Sum rule	5.52	12.12	1.5
Weighted sum rule	5.18	11.84	1.3
Weighted minimum rule	6.74	13.07	1
Weighted product rule	3.52	10.31	1.4

As a following experiment, we consider judging the proposals with varying number of genuine signatures used as the reference set in Table 5.12. The *FUS3* systems achieves the lowest MEER of 11.95% and 4.96% with common and user threshold setting for the case of ten enrolled signatures. On the whole, there is reduction of MEER across *BL-DTW*, *GMM-DTW* and *FUS3* systems with increasing number of reference signature samples.

Lastly, we evaluated the performance of our proposal with different feature sets given in Table 5.7. The MEER results obtained in Table 5.13 do corroborate on the efficacy of the GMM based descriptor over the temporal feature sets D_1 to D_6. In particular, the *FUS3* outperforms the performance of *BL-DTW* and *GMM-DTW* systems across all the sets.

Table 5.12: Efficacy of the proposed *GMM-DTW* and *FUS3* system for varying number of genuine enrolled signatures from the SVC-2004 database. The GMM membership feature vector is derived using $M = 64$ Gaussian components.

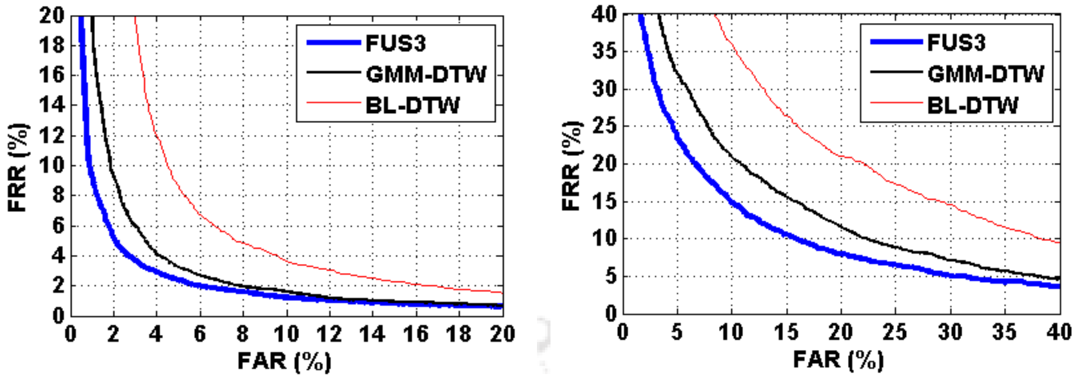
# of enrolled signatures	User Threshold			Common Threshold		
	BL-DTW system	*GMM-DTW* system	*FUS3* system	*BL-DTW* system	*GMM-DTW* system	*FUS3* system
3	13.53	7.49	5.69	20.79	16.40	13.81
5	13.28	7.35	5.52	20.33	14.96	12.12
7	12.90	7.14	5.16	20.19	14.75	12.06
10	11.83	6.97	4.93	19.95	14.52	11.82

Table 5.13: Performance evaluation of the *BL-DTW*, *GMM-DTW* and *FUS3* system on SVC-2004 database with different subsets of features. For *GMM-DTW* and *FUS3* system the number of Gaussian components M has been optimized to obtain lowest MEER.

Feature subset	# of Gaussians M	User Threshold			Common Threshold		
		BL-DTW system	*GMM-DTW* system	*FUS3* system	*BL DTW* system	*GMM-DTW* system	*FUS3* system
D_1	16	15.37	9.93	9.02	21.68	18.11	17.29
D_2	16	17.97	5.80	4.63	25.05	12.76	11.34
D_3	16	14.73	12.92	11.14	22.21	20.62	18.53
D_4	64	14.40	11.92	8.84	21.49	20.46	16.58
D_5	32	13.39	7.99	6.14	20.56	16.68	14.00
D_6	64	13.28	7.35	5.52	20.33	14.96	12.12

5.5.3 DET Curves

Figure 5.11 illustrates the DET curves, a two dimensional plot of False Acceptance Rate (FAR) against the False Rejection Rate (FRR) for varying values of decision threshold, corresponding to the MCYT-100 and SVC-2004 databases. The plots are obtained from the tested signatures (using skilled forgery) across all the users of a single trial. Clearly, the *FUS3* system (in blue) outperforms the *BL-DTW* (in red) and *GMM-DTW* (in black) over all the points on the curves of both databases. The GMM comprising $M = 32$ and 64 Gaussian components is used for the extraction of the membership feature vectors for the MCYT-100 and SVC-2004 databases respectively.



(*a*) (*b*)

Figure 5.11: The Detection Error Trade-off (DET) curves obtained on the test signatures of the MCYT-100 and SVC-2004 database for the common threshold scenario is illustrated for a single trial in sub-figures (a) and (b) respectively. The number of reference signatures considered is 5. The curves corresponding to *BL-DTW*, *GMM-DTW* and *FUS3* systems are depicted in red, black and blue colors respectively. The GMMs comprising $M = 32$ and 64 Gaussian components are used for the extraction of the membership feature vectors in MCYT-100 and SVC-2004 databases respectively.

5.5.4 Computational Complexity

The computation complexity of our proposal in Table 5.14 is presented with regards to each step for a test signature S_T. To start with, the d dimensional feature vector sequence derived from the online trace of S_T is used to compute the GMM based descriptor. This requires the calculation of membership values of the M Gaussians for each of the feature vectors along the online trace, thus leading to a complexity of $\mathcal{O}(n_T d^2 M)$. The subsequent step of matching the sequence of GMM descriptors with DTW algorithm has a computational complexity - $\mathcal{O}(M n_T \max\limits_{1 \leq p \leq N} n_p)$.

With regards to the extraction of the warping path score, we note that the set of alignments $\ominus_p^* = \{(a_i, r_i^*)\}_{i=1}^{l_{\mathcal{W}_p^*}}$ computed based on the nearest neighbor match along the warping path $\mathcal{W}_p^*$ using Equations 5.8 and 5.9 presents a computation complexity of $\mathcal{O}(\max\limits_{1 \leq p \leq N} n_p l_{\mathcal{W}_p^*})$. Thereafter, the generation of histograms $\mathcal{H}_{\mathcal{W}_p^*}$ and $\mathcal{H}_{\ominus_p^*}$ as described in Algorithm 4 has a complexity of $\mathcal{O}(M \max\limits_{1 \leq p \leq N} l_{\mathcal{W}_p^*})$. The process of matching these histograms for the set of N reference signatures gives a complexity of $\mathcal{O}(MN)$. Finally, the fusion of scores d_1 and d_2 using the sum rule will incur $\mathcal{O}(N)$.

Table 5.14: Computation Complexity of the proposed algorithm for a test signature S_T.

Step	Description	Computation Complexity
1	GMM membership value computation for S_T	$\mathcal{O}(n_T d^2 M)$
2	GMM-DTW system	$\mathcal{O}(M n_T \max_{1 \leq p \leq N} n_p)$
3	Computation of (a_i, r_i^*) aligned pairs	$\mathcal{O}(\max_{1 \leq p \leq N} n_p l_{\mathcal{W}_p^*})$
4	Generation of $\mathcal{H}_{\mathcal{W}_p^*}$	$\mathcal{O}(M \max_{1 \leq p \leq N} l_{\mathcal{W}_p^*})$
5	Generation of $\mathcal{H}_{\ominus_p^*}$	$\mathcal{O}(M \max_{1 \leq p \leq N} l_{\mathcal{W}_p^*})$
6	Histogram Matching	$\mathcal{O}(MN)$
7	Fusion of Scores	$\mathcal{O}(N)$

5.6 Summary

In this research, we presented a novel utility of GMM - a model based approach into the DTW framework for signature verification. Our contributions are: (i) Proposal of GMM based descriptors, that captures the writer dependent statistical characteristics for signature matching. (ii) Incorporation of the descriptors in deriving a novel score that characterizes the warping path (iii) Fusion of the proposed warping path score with normalized DTW score for enhancing the verification performance of DTW based system. The method has been demonstrated successfully on the signature data from the SVC-2004 and MCYT-100 databases respectively.

6

Summary and Conclusions

Contents

6.1 List of contributions

The different contributions made in this thesis are enumerated as follows:

- Demonstration of illustrative examples that suggest that there is a need to explore cues other than the DTW score to verify the authenticity of an online signature.
- Proposal to study the trend of the warping path and utilization of the same for signature verification. To the best of our knowledge, this idea has not been explored so far in literature.
- Incorporation of the alignment obtained from a DTW match together with another, proposed based on a measure inspired from correlation-based neighborhood matching to study the characteristics of the warping path.
- Derivation of two components to the warping path score - namely feature distortion and displacement. Thereafter, we demonstrated the impact of these individual components to the verification step.
- Fusion of the warping path score to that of DTW for reduction of the error rates.
- Demonstration of the efficacy of the proposal with different recursive DTW functions.
- Demonstration of the use of the proposal with different distances used for the DTW cost matrix computation.
- Proposal to incorporate contextual information in the computation of DTW score.
- Utilization of a VQ based codebook to study the trend of the warping path. The idea, as such, was to come up with a strategy of voting the aligned pairs of feature vectors along the warping path with the codevectors of the codebook.
- Proposal to incorporate contextual information in the computation of the votes mentioned above.

Table 6.1: Summary of results from proposals of the thesis on the SVC-2004 and MCYT-100 database.

Proposals	Database	Common threshold	User Threshold
Chapter 3	SVC-2004	**7.8**	2.53
Chapter 4	SVC-2004	10.85	3.89
Chapter 5	SVC-2004	10.31	3.52
Chapter 3	MCYT-100	2.76	1.15
Chapter 4	MCYT-100	**2.53**	**1.03**
Chapter 5	MCYT-100	3.19	1.12

- Consideration of the point based feature vectors of the online trace of signatures, from a probabilistic view, by encoding them using GMM based descriptors, prior to DTW matching.
- Exploring the utility of the descriptors from the GMM for scoring the characteristics of the warping path.
- Suggestion of the notion of the spacing parameter value for feature extraction and demonstration of the same in reducing the error rates of the DTW system.

6.2 Discussion to prior works

The goal of this Section is to see on how our proposed strategies described in the thesis fares with several prior works from the literature that use the SVC-2004 and MCYT-100 databases. We summarize on the MEERs obtained by our proposals of the three contributing chapters on the databases in Table 6.1.

An enumeration of the previous systems are thereafter presented in Table 6.2. It is to be noted that each of these have been trained and tested differently, with different sets of features employed for the classifiers and hence a direct one-to-one comparison with the proposals in Table 6.1 is not fair and possible. Nonetheless, the values being reported are the best EERs from employing five genuine reference signature of an user for enrollment, that has more or less

Table 6.2: EER from different signature systems on the SVC-2004 and MCYT-100 database.

Method	Database	Common threshold	User Threshold
LCSS+SVM Kernel [40]	SVC-2004	-	6.84
LCSS [23]		-	5.33
DTW + SVM [38]		6.96	-
Feature selection+DTW [70]		-	3.38
Dynamic programming [71]		10.15	3.61
DTW+HMM [107]		10.91	6.91
HMM [26]		6.90	-
DWT+ FFT+ SVM [116]		7.17	-
Velocity and pressure based partition [19]		12.40	-
Horizontal partition+neuro-fuzzy classifier [80]		11.58	-
Vertical partition+neuro-fuzzy classifier [81]		10.70	-
Segment based matching with DTW [67]		7.83	-
Function based + HMM [96]		7.14	-
Fuzzy Modeling [117]		7.57	2.46
DTW + Fourier descriptors [30]	MCYT-100	7.22	-
VQ+DTW [36]		5.42	-
Dynamic programming [71]		3.72	1.57
Velocity and pressure based partition [19]		1.09	-
Wavelet coefficients [24]		3.21	-
UBM-HMM + fuzzy cryptography [28]		5.87	-
HMM + Viterbi Path [29]		3.37	-
HMM+Parzen Window [35]		5.29	2.12
Symbolic Representation [58]		6.12	5.84
Histogram Based Analysis [61]		4.02	-
Two stage normalization+DTW [74]		3.94	-
One class neuro-fuzzy classifier [82]		3.33	-
Ensemble of Parzen Windows [85]		8.4	-
Fusion of local, regional and global matchers [87]		3.81	-
User dependent features + classifiers [103]		19.4	-
User dependent features + symbol interval feature [105]		2.2	-
Information Divergence based matching [118]		3.16	-

become a standard protocol for performance evaluation in works on online signature verification [34].

The different DTW based systems proposed in this thesis are the first of their kind that mathematically score the warping path for verification of online signatures. With the combination of this score to that of the DTW, we can get an EER to as low as 7.8 % and 2.53% (using common threshold), 2.53% and 1.03% (with user threshold) for the SVC-2004 and MCYT-100 database. With regards to the error rates obtained from the proposals of the three contributing chapters, we see that they are almost at par or better to most of the previous verification systems being proposed for these databases reported in Table 6.2.

6.3 Possible pointers for the future

The different strategies outlined in the thesis so far as well as their evaluation on the SVC-2004 and MCYT-100 databases suggest that they are worth to receive further exploration. Keep this in mind, we now present aspects, that may regarded as research pointers for the future.

- Recall from Chapter 3 that the use of the spacing parameter r on the components of the feature vectors improved the verification capabilities in the performance of the DTW based system. However, it may noted that for the present work, we have applied the same parameter value across all the components. An interesting exploration that can be possibly taken up is on adapting its value according to different features of a given user for further enhancing the discrimination between genuine and skilled forgery signature.

- The proposed warping path score d_2 obtained from the exploration of DTW cost matrix in Chapter 3 constitutes two components, namely - the feature distortion and displacement terms. In this thesis, this score is computed merely as an average of these components and used for verification, thereof. An interesting avenue to look forward to in the future is to model the distribution of the trend of these two components probabilistically, that in a way, can generalize across any genuine signature of an user.

- It may be recalled from Chapter 4 of the thesis, that we explored on the applicability of the VQ scheme for studying the trend of the warping path of the DTW cost matrix. Likewise, in Chapter 5, we considered the descriptors from a GMM classifier to address the same problem. A recent development aligned to this area is that of the sparse representation framework - the application of which has been explored and validated in [34] for the online signature verification. In that work, the authors propose the use of sparsity based feature for verification. As a future extension to analyzing the DTW warping path for verification, a possible investigation could thus be towards considering the atoms of the dictionary being learnt for deriving the score.

- Though the thesis threw light on strategies for extracting scores from the warping path, one can explore out on an alternate approach as well to improve the DTW based verification system. In the following, we outline one such idea from the area of image processing with regards to its application of object retrieval. Recent techniques in this domain (post year 2010) have focussed on descriptors obtained from a codebook [119, 120]. We can possibly consider notions from such methods to motivate the study of online signature verification.

  The idea behind the same comes from the intuition that the feature vectors corresponding to the online trace of the genuine signatures would be aligned in a similar relative location with respect to the nearest codevector to which they are assigned in the feature space. This trend may however not be prevalent across the feature vectors from the online signature of a skilled forger. We can perhaps capture explicitly this idea of relative location by proposing a descriptor with regards to each of the codevectors in the codebook and employ the same for signature verification. Finally, we can explore on whether the score obtained by matching the descriptors of the signatures being matched can provide information that is complementary to DTW for performance improvement.

- Last but not the least, the ideas explored in the three contributing chapters of this thesis may be attempted for the application of verifying off-line signatures as well. The data being employed for processing such data contain gray-level information of the strokes corresponding to the pixels occupied by the ink. Accordingly, this entails the extraction of a different set of features, that are suited for matching the signature images.

Notwithstanding these possible extensions, we believe the work reported in this thesis to be the first of its kind that uses strategies to propose a interesting score for evaluating the well-ness of the warping path associated with DTW. This score in conjunction with that of DTW does provide reduced error rates for the online signature verification.

As a final note, we conclude with a terse discussion on how the proposals of this thesis can be extended for the area of speaker recognition. The road-map of steps would be to first segment out the temporal signal to frames and then describe each frame thereof with features such as Mel Frequency Cepstral Coefficients (MFCC) [62]. The extracted features can then matched using the DTW algorithm between the reference and test speech signals, following which their enhancement can be attempted by scoring the warping path with the methods outlined in this thesis.

References

[1] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, no. 1, pp. 4–20, Jan 2004.

[2] B. Zhang, W. Li, P. Qing, and D. Zhang, "Palm-print classification by global features," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 2, pp. 370–378, 2013.

[3] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, pp. 2963 – 2972, 2002.

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. Springer Publishing Company, 2009.

[5] A. K. Jain and S. Z. Li, *Handbook of Face Recognition*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[6] J. Daugman, "Recognizing people by their iris patterns," *Information Security Technical Report*, vol. 3, no. 1, pp. 33–39, 1998.

[7] D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041–1050, Sept 2003.

[8] F. Monrose and A. Rubin, "Authentication via keystroke dynamics," in *Proceedings of the 4th ACM Conference on Computer and Communications Security*, ser. CCS '97. New York, NY, USA: ACM, 1997, pp. 48–56.

[9] M. S. Nixon, J. N. Carter, D. Cunado, P. S. Huang, and S. Stevenage, "Automatic gait recognition," in *Biometrics*. Springer, 1996, pp. 231–249.

[10] J. Galbally, J. Fiérrez-Aguilar, M. Martinez-Diaz, and R. Plamondon, "Quality analysis of dynamic signature based on the sigma log-normal model," in *Document Analysis and Recognition (ICDAR), 2011 International Conference on*, 2011, pp. 633–637.

[11] M. Gomez-Barrero, J. Galbally, J. Fiérrez, J. Ortega-Garcia, and R. Plamondon, "Variations of handwritten signatures with time: A sigma log-normal analysis," in *International Conference on Biometrics, ICB 2013, 4-7 June, 2013, Madrid, Spain*, 2013, pp. 1–6.

[12] C. O'Reilly and R. Plamondon, "Development of a sigma log-normal representation for on-line signatures," *Pattern Recogn.*, vol. 42, no. 12, pp. 3324–3337, Dec. 2009.

[13] A. Namboodiri and S. Gupta, "Text independent writer identification from online handwriting," in *Tenth International Workshop on Frontiers in Handwriting Recognition*, 2006.

[14] M. A. Ferrer, F. V. Bonilla, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 3, pp. 966–977, 2012.

[15] R. Kumar, J. D. Sharma, and B. Chanda, "Writer-independent off-line signature verification using surroundedness feature," *Pattern Recognition Letters*, vol. 33, no. 3, pp. 301–308, 2012.

[16] S. Pal, A. Alaei, U. Pal, and M. Blumenstein, "SVM and NN based offline signature verification," *International Journal of Computational Intelligence and Applications*, vol. 12, no. 4, 2013.

[17] D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First International Signature Verification Competition," in *Biometric Authentication*, ser. Lecture Notes in Computer Science, D. Zhang and A. Jain, Eds. Springer Berlin Heidelberg, 2004, vol. 3072, pp. 16–22.

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

[19] M. T. Ibrahim, M. A. Khan, K. S. Alimgeer, M. K. Khan, I. A. Taj, and L. Guan, "Velocity and pressure-based partitions of horizontal and vertical trajectories for on-line signature verification," *Pattern Recognition*, vol. 43, no. 8, pp. 2817 – 2832, 2010.

[20] 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.

[21] J. Igarza, L. Gmez, I. Hernez, and I. Goirizelaia, "Searching for an optimal reference system for on-line signature verification based on (x, y) alignment," in *Biometric Authentication*, ser. Lecture Notes in Computer Science, D. Zhang and A. Jain, Eds. Springer Berlin Heidelberg, 2004, vol. 3072, pp. 519–525.

[22] M. E. Munich and P. Perona, "Continuous Dynamic Time Warping for translation-invariant curve alignment with applications to signature verification," in *Proceedings of the Seventh IEEE International Conference on Computer Vision*, vol. 1, Sep. 1999, pp. 108–115 vol.1.

[23] 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, 2013.

[24] P. Thumwarin, J. Pernwong, and T. Matsuura, "FIR signature verification system characterizing dynamics of handwriting features," *EURASIP Journal on Advances in Signal Processing*, vol. 2013, no. 1, 2013.

[25] M. Parodi and J. C. Gmez, "Legendre polynomials based feature extraction for online signature verification. consistency analysis of feature combinations," *Pattern Recognition*, vol. 47, no. 1, pp. 128 – 140, 2014.

[26] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2325 – 2334, 2007.

[27] E. Argones Rua and J. Alba Castro, "Online signature verification based on Generative models," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 42, no. 4, pp. 1231–1242, Aug 2012.

[28] E. A. Rua, E. Maiorana, J. L. A. Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 269–282, 2012.

[29] B. L. Van, S. Garcia-Salicetti, and B. Dorizzi, "On using the Viterbi path along with HMM likelihood information for online signature verification," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 37, no. 5, pp. 1237–1247, Oct 2007.

[30] B. Yanikoglu and A. Kholmatov, "Online signature verification using Fourier descriptors," *EURASIP J. Adv. Signal Process*, vol. 2009, pp. 12:1–12:1, Jan. 2009.

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

[32] L. Nanni and A. Lumini, "A novel local on-line signature verification system," *Pattern Recognition Letters*, vol. 29, no. 5, pp. 559 – 568, 2008.

[33] S. Rashidi, A. Fallah, and F. Towhidkhah, "Feature extraction based DCT on dynamic signature verification," *Scientia Iranica*, vol. 19, no. 6, pp. 1810 – 1819, 2012.

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

[35] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Pealba, J. Ortega-Garcia, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in *Audio- and Video-Based Biometric Person Authentication*, ser. Lecture Notes in Computer Science, T. Kanade, A. Jain, and N. Ratha, Eds. Springer Berlin Heidelberg, 2005, vol. 3546, pp. 523–532.

[36] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognition*, vol. 40, no. 3, pp. 981–992, Mar. 2007.

[37] R. Martens and L. Claesen, "On-line signature verification by Dynamic Time Warping," in *Pattern Recognition, 1996., Proceedings of the 13th International Conference on*, vol. 3. IEEE, 1996, pp. 38–42.

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

[39] M. Liwicki, "Evaluation of novel features and different models for online signature verification in a real-world scenario," in *Proc. 14th Conf. of the Int. Graphonomics Society*, 2009, pp. 22–25.

[40] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, "Online signature verification with Support Vector Machines based on LCSS kernel functions," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 4, pp. 1088–1100, Aug 2010.

[41] M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On line signature verification: fusion of a Hidden Markov Model and a neural network via a Support Vector Machine," in *Frontiers in Handwriting Recognition, 2002. Proceedings. Eighth International Workshop on*, 2002, pp. 253–258.

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

[43] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification - the state of the art," *Pattern recognition*, vol. 22, no. 2, pp. 107–131, 1989.

[44] F. Leclerc and R. Plamondon, "Automatic signature verification: The state of the art- 1989–1993," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 8, no. 3, pp. 643–660, 1994.

[45] R. Plamondon and M. Parizeau, "Signature verification from position, velocity and acceleration signals: a comparative study," in *Proc. of 9th Intl. Conf. on Pattern Recognition, ICPR*, vol. 1, 1988, pp. 260–265.

[46] S. Garcia-Salicetti, N. Houmani, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, C. V. Uer, and T. Scheidat, "On-line handwritten signature verification," in *Guide to Biometric Reference Systems and Performance Evaluation*, B. D. Dijana Petrovska-Delacrtaz, Grard Chollet, Ed. Springer Science & Business Media, 2009, pp. 125–165.

[47] D. Impedovo, "Automatic signature verification: the state of the art," *IEEE Transactions on SMC, Part C: Applications and Reviews*, pp. 609–635, 2008.

[48] T. Wilkin and O. S. Yin, "State of the art: Signature verification system," in *2011 7th International Conference on Information Assurance and Security (IAS)*, Dec 2011, pp. 110–115.

[49] M. Parizeau and R. Plamondon, "A comparative analysis of regional correlation, Dynamic Time Warping, and skeletal tree matching for signature verification," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 12, no. 7, pp. 710–717, 1990.

[50] S. Schimke, C. Vielhauer, and J. Dittmann, "Using adapted Levenshtein distance for on-line signature authentication," in *Proceedings of the Pattern Recognition, 17th International Conference on (ICPR'04) Volume 2 - Volume 02*, ser. ICPR '04, 2004, pp. 931–934.

[51] L. Yang, B. Widjaja, and R. Prasad, "Application of Hidden Markov Models for signature verification," *Pattern Recognition*, vol. 28, no. 2, pp. 161 – 170, 1995.

[52] R. S. Kashi, J. Hu, W. L. Nelson, and W. Turin, "On-line handwritten signature verification using Hidden Markov Model features," in *Proceedings of the Fourth International Conference on Document Analysis and Recognition*, vol. 1, Aug 1997, pp. 253–257 vol.1.

[53] M. Zou, J. Tong, C. Liu, and Z. Lou, "On-line signature verification using local shape analysis," in *Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings.*, Aug 2003, pp. 314–318 vol.1.

[54] J. J. Igarza, Goirizelaia, and J. Sánchez, "Online handwritten signature verification using Hidden Markov Models," in *Progress in Pattern Recognition, Speech and Image Analysis: 8th Iberoamerican Congress on Pattern Recognition, CIARP 2003, Havana, Cuba, November 26-29, 2003 Proceedings*, A. Sanfeliu and J. Ruiz-Shulcloper, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 391–399.

[55] D. Muramatsu and T. Matsumoto, "An HMM on-line signature verification algorithm," in *Proceedings of the 4th International Conference on Audio- and Video-based Biometric Person Authentication*, ser. AVBPA'03. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 233–241.

[56] Z. hua Quan, D. shuang Huang, X. lei Xia, M. R. Lyu, and T.-M. Lok, "Spectrum analysis based on windows with variable widths for online signature verification," in *18th International Conference on Pattern Recognition (ICPR'06)*, vol. 2, August 2006, pp. 1122–1125.

[57] K. Wang, Y. Wang, and Z. Zhang, "On-line signature verification using wavelet packet," in *2011 International Joint Conference on Biometrics (IJCB)*, Oct 2011, pp. 1–6.

[58] D. Guru and H. Prakash, "Online signature verification and recognition: an approach based on symbolic representation," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 31, no. 6, pp. 1059–1073, June 2009.

[59] D. Guru, H. Prakash, and S. Manjunath, "On-line signature verification: An approach based on cluster representations of global features," in *Advances in Pattern Recognition, 2009. ICAPR '09. Seventh International Conference on*, Feb 2009, pp. 209–212.

[60] A. Fallah, M. Jamaati, and A. Soleamani, "A new online signature verification system based on combining Mellin Transform, MFCC and neural network," *Digital Signal Processing*, vol. 21, no. 2, pp. 404 – 416, 2011.

[61] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 6, pp. 933–947, June 2014.

[62] L. Rabiner and B.-H. Juang, *Fundamentals of Speech Recognition*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[63] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*. John Wiley & Sons, 2012.

[64] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," *Pattern Recognition Letters*, vol. 24, no. 16, pp. 2943 – 2951, 2003.

[65] G. Gupta and R. Joyce, "Using position extrema points to capture shape in on-line handwritten signature verification," *Pattern Recognition*, vol. 40, no. 10, pp. 2811 – 2817, 2007.

[66] J.-Y. R. M. Wirotius and N. Vincent, "Selection of points for on-line signature comparison," in *Proceedings of the 9th Intl Workshop on Frontiers in Handwriting Recognition (IWFHR)*, 2004.

[67] J. Zhang and S. Kamata, "Online signature verification using segment-to-segment matching," in *Int. Conf. Frontiers in Handwriting Recognition*, 2008.

[68] J. Lee, H.-S. Yoon, J. Soh, B. T. Chun, and Y. K. Chung, "Using geometric extrema for segment-to-segment characteristics comparison in online signature verification," *Pattern Recognition*, vol. 37, no. 1, pp. 93 – 103, 2004.

[69] M. I. Khalil, M. Moustafa, and H. M. Abbas, "Enhanced DTW based on-line signature verification," in *Proceedings of the 16th IEEE International Conference on Image Processing*, 2009, pp. 2685–2688.

[70] J. Pascual-Gaspar, V. Cardeoso-Payo, and C. Vivaracho-Pascual, "Practical on-line signature verification," in *Advances in Biometrics*, ser. Lecture Notes in Computer Science, M. Tistarelli and M. Nixon, Eds. Springer Berlin Heidelberg, 2009, vol. 5558, pp. 1180–1189.

[71] D. Muramatsu and T. Matsumoto, "Effectiveness of pen pressure, azimuth, and altitude features for online signature verification," in *Proceedings of the 2007 International Conference on Advances in Biometrics*. Springer-Verlag, 2007, pp. 503–512.

[72] Y. Komiya and T. Matsumoto, "On-line pen input signature verification ppi (pen-position/pen-pressure/pen-inclination)," in *Proc. IEEE International Conference on SMC*, 1996, pp. 41–46.

[73] S. Y. S. Hangai and T. Hamamoto, "Writer verification using altitude and direction of pen movement," in *Int. Conf. Pattern Recognition*, 2000, pp. 3843 – 3846.

[74] 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.

[75] M. Faundez-Zanuy and J. Pascual-Gaspar, "Efficient on-line signature recognition based on multi-section Vector Quantization," *Pattern Analysis and Applications*, vol. 14, no. 1, pp. 37–45, 2011.

[76] J. M. Pascual-Gaspar, M. Faundez-Zanuy, and C. Vivaracho, "Fast on-line signature recognition based on VQ with time modeling," *Engineering Applications of Artificial Intelligence*, vol. 24, no. 2, pp. 368 – 377, 2011.

[77] X. Song, X. Xia, and F. Luan, "Online signature verification based on stable features extracted dynamically," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2016.

[78] X. Xia, Z. Chen, F. Luan, and X. Song, "Signature alignment based on GMM for on-line signature verification," *Pattern Recognition*, vol. 65, pp. 188 – 196, 2017.

[79] M. Khan, M. Niazi, and M. Khan, "Velocity-image model for online signature verification," *Image Processing, IEEE Transactions on*, vol. 15, no. 11, pp. 3540–3549, Nov 2006.

[80] K. Cpaka, M. Zalasiski, and L. Rutkowski, "New method for the on-line signature verification based on horizontal partitioning," *Pattern Recognition*, vol. 47, no. 8, pp. 2652 – 2661, 2014.

[81] K. Cpaka and M. Zalasiski, "On-line signature verification using vertical signature partitioning," *Expert Systems with Applications*, vol. 41, no. 9, pp. 4170 – 4180, 2014.

[82] K. Cpaka, M. Zalasiski, and L. Rutkowski, "A new algorithm for identity verification based on the analysis of a handwritten dynamic signature," *Applied Soft Computing*, vol. 43, pp. 47 – 56, 2016.

[83] G. Pirlo, V. Cuccovillo, D. Impedovo, and P. Mignone, "On-line signature verification by multi-domain classification," in *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*. IEEE, 2014, pp. 67–72.

[84] G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo, and P. Mignone, "Multidomain verification of dynamic signatures using local stability analysis," *IEEE Transactions on Human-Machine Systems*, vol. 45, no. 6, pp. 805–810, 2015.

[85] L. Nanni and A. Lumini, "Ensemble of Parzen window classifiers for on-line signature verification," *Neurocomputing*, vol. 68, pp. 217 – 224, 2005.

[86] L. Nanni, "Experimental comparison of one-class classifiers for online signature verification," *Neurocomputing*, vol. 69, no. 7, pp. 869–873, 2006.

[87] L. Nanni and A. Lumini, "Advanced methods for two-class problem formulation for on-line signature verification," *Neurocomputing*, vol. 69, no. 7, pp. 854–857, 2006.

[88] L. Nanni, "An advanced multi-matcher method for on-line signature verification featuring global features and tokenised random numbers," *Neurocomputing*, vol. 69, no. 16, pp. 2402–2406, 2006.

[89] M. Parodi and J. C. Gómez, "Online signature verification based on Legendre series representation. consistency analysis of different feature combinations," in *Iberoamerican Congress on Pattern Recognition*. Springer, 2012, pp. 715–723.

[90] M. Parodi, J. C. Gomez, and M. Liwicki, "Online signature verification based on Legendre series representation: Robustness assessment of different feature combinations," in *Proceedings of the 2012 International Conference on Frontiers in Handwriting Recognition*, ser. ICFHR '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 379–384.

[91] M. Parodi, J. C. Gómez, M. Liwicki, and L. Alewijnse, "Orthogonal function representation for online signature verification: which features should be looked at?" *IET biometrics*, vol. 2, no. 4, pp. 137–150, 2013.

[92] H. Lei and V. Govindaraju, "A comparative study on the consistency of features in on-line signature verification," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2483–2489, 2005.

[93] R. Doroz, P. Porwik, and T. Orczyk, "Dynamic signature verification method based on association of features with similarity measures," *Neurocomputing*, vol. 171, pp. 921–931, 2016.

[94] P. Porwik, R. Doroz, and T. Orczyk, "The k-NN classifier and self-adaptive Hotelling data reduction technique in handwritten signatures recognition," *Pattern Analysis and Applications*, vol. 18, no. 4, pp. 983–1001, 2015.

[95] T. Orczyk, P. Porwik, and R. Doroz, "Signatures verification based on PNN classifier optimised by PSO algorithm," *Pattern Recognition*, vol. 60, pp. 998–1014, 2016.

[96] J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Target dependent score normalization techniques and their application to signature verification," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 35, no. 3, pp. 418–425, Aug 2005.

[97] 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*. New York, NY, USA: ACM, 2003, pp. 115–122.

[98] M. I. Malik, S. Ahmed, A. Dengel, and M. Liwicki, "A signature verification framework for digital pen applications," in *Document Analysis Systems (DAS), 2012 10th IAPR International Workshop on*. IEEE, 2012, pp. 419–423.

[99] L. Wan, B. Wan, and Z.-C. Lin, "On-line signature verification with two-stage statistical models," in *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)*. IEEE, 2005, pp. 282–286.

[100] O. Miguel-Hurtado, L. Mengibar-Pozo, M. G. Lorenz, and J. Liu-Jimenez, "On-line signature verification by Dynamic Time Warping and Gaussian Mixture Models," in *2007 41st Annual IEEE International Carnahan Conference on Security Technology*, Oct 2007, pp. 23–29.

[101] O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in *2008 42nd Annual IEEE International Carnahan Conference on Security Technology*, Oct 2008, pp. 206–213.

[102] M. Lpez-Garca, R. Ramos-Lara, O. Miguel-Hurtado, and E. Cant-Navarro, "Embedded system for biometric online signature verification," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 491–501, Feb 2014.

[103] K. Manjunatha, S. Manjunath, D. Guru, and M. Somashekara, "Online signature verification based on writer dependent features and classifiers," *Pattern Recognition Letters*, vol. 80, pp. 129 – 136, 2016.

[104] D. S. Guru, K. S. Manjunatha, and S. Manjunath, "Online signature verification based on recursive subset training," in *Mining Intelligence and Knowledge Exploration, First International Conference, MIKE 2013, Tamil Nadu, India, December 18-20, 2013*, 2013, pp. 350–361.

[105] D. Guru, K. Manjunatha, S. Manjunath, and M. Somashekara, "Interval valued symbolic representation of writer dependent features for online signature verification," *Expert Systems with Applications*, vol. 80, pp. 232 – 243, Sep 2017.

[106] R. Szeliski, *Computer vision: algorithms and applications.* Springer Science & Business Media, 2010.

[107] J. Fierrez-Aguilar, S. Krawczyk, J. Ortega-Garcia, and A. K. Jain, "Fusion of local and regional approaches for on-line signature verification," in *Proceedings of the 2005 International Conference on Advances in Biometric Person Authentication*, 2005, pp. 188–196.

[108] A. Kumar and C. Wu, "Automated human identification using ear imaging," *Pattern Recognition*, vol. 45, no. 3, pp. 956–968, 2012.

[109] D. A. Reynolds, "Speaker identification and verification using Gaussian mixture speaker models," *Speech Communication*, vol. 17, no. 1, pp. 91–108, 1995.

[110] C. M. Bishop, *Pattern Recognition and Machine Learning (Information Science and Statistics).* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[111] 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.

[112] Y. Zhang and J. R. Glass, "Unsupervised spoken keyword spotting via segmental DTW on Gaussian posteriorgrams," in *Automatic Speech Recognition & Understanding, 2009. ASRU 2009. IEEE Workshop on.* IEEE, 2009, pp. 398–403.

[113] S. Jelil, R. K. Das, R. Sinha, and S. M. Prasanna, "Speaker verification using Gaussian posteriorgrams on fixed phrase short utterances," in *Sixteenth Annual Conference of the International Speech Communication Association*, 2015.

[114] Q. Sun, H. Liu, L. Ma, and T. Zhang, "A novel hierarchical bag-of-words model for compact action representation," *Neurocomputing*, vol. 174, pp. 722–732, 2016.

[115] G. Csurka, C. R. Dance, L. Fan, J. Willamowski, and C. Bray, "Visual categorization with bags of keypoints," in *In Workshop on Statistical Learning in Computer Vision, ECCV*, 2004, pp. 1–22.

[116] W. H. Khoh, T. S. Ong, Y. Pang, and A. B. J. Teoh, "Score level fusion approach in dynamic signature verification based on hybrid wavelet-fourier transform," *Security and Communication Networks*, vol. 7, no. 7, pp. 1067–1078, 2014.

[117] A. Ansari, M. Hanmandlu, J. Kour, and A. Singh, "Online signature verification using segment-level fuzzy modelling," *Biometrics, IET*, vol. 3, no. 3, pp. 113–127, Sept 2014.

[118] L. Tang, W. Kang, and Y. Fang, "Information divergence-based matching strategy for online signature verification," *IEEE Transactions on Information Forensics and Security*, 2017.

[119] R. Arandjelović and A. Zisserman, "All about VLAD," in *IEEE Conference on Computer Vision and Pattern Recognition*, 2013.

[120] H. Jegou, F. Perronnin, M. Douze, J. Sanchez, P. Perez, and C. Schmid, "Aggregating local image descriptors into compact codes," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 9, pp. 1704–1716, 2012.

LIST OF PUBLICATIONS

Journal Publications:

1. **A. Sharma** and S. Sundaram, "On the exploration of information from the DTW cost matrix for online signature verification," *IEEE Trans. Cybernetics*, vol. 48, no.2, pp. 611-624, Feb 2018.

2. **A. Sharma** and S. Sundaram, "A novel online signature verification system based on GMM features in a DTW framework," *IEEE Trans. Information Forensics and Security*, vol. 12, no. 3, pp. 705-718, Mar. 2017.

3. **A. Sharma** and S. Sundaram, "An enhanced contextual DTW based system for online signature verification using Vector Quantization," *Pattern Recognition Letters*, vol. 84, pp. 22-28, Dec. 2016.