Investigation on Automatic Emotion Recognition Using Deep Learning Based Methods

Tanzeel Khan and Ramesh K. Bhukya

***Abstract*—This work proposes a novel online signature verification system based on the methodology of distance based matching. We use the dynamic time warping (DTW) algorithm for aligning a test signature against the enrolled signatures of an user. The prior works in literature primarily utilize only the DTW scores to authenticate a test signature. To the best of our knowledge, the characteristics of the warping path (used for the alignment) in the cost matrix is hardly exploited for verification of online signatures. Accordingly, we explore a new feature that utilizes the information from the cost matrix and warping path. We subsequently consider its fusion (using a sum rule combiner) with the DTW score for authenticating the veracity of a test signature. Another contribution is with regards to the set of features employed for matching the signatures. We introduce a spacing parameter for feature extraction, and demonstrate its applicability in increasing the separation between the distribution of genuine and forgery signatures, for an user. The proposal, when tested on two publicly available online signature databases - the SVC-2004 Task-2 and MCYT-100, achieves equal error rates at par, with recent methods.**

***Index Terms*—Facial Emotion Recognition, MXNET, Deep Learning, FER2013.**

I. Introduction

In a facial emotion recognition system, we process an image of a person by either taking it directly as an input or by continuously capturing pictures through a video feed and identify the emotion the person is feeling. Based on a matching score, a decision is made to either accept the claimed signature as genuine or to reject it as a forgery [1]. In online signature verification, we make use of the temporal functions of attributes captured during the signing process. The input comprises a set of strokes, each of which in turn are a sequence of points. A stroke starts with a pen-down and ends with the next pen-up status signal. The research area of signature verification falls under the purview of handwriting analysis. In the domain of document processing, it is classified under the 'text-dependent' writer identification framework [2].

The topic of 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 [3]–[5]. 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 global features, derived from the acquired signature trajectories. Examples of such attributes include length, width, height of the signature, 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 sequences 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, the approaches being proposed in literature have been largely focussed on distance and model based techniques [6]. Distance based methods primarily invoke concepts from dynamic programming to match the test signatures with the set of enrolled signatures, subsequent to extraction of local-features at each sample point of the signatures. Model based techniques, on the other hand, employ the use of either generative-based classifiers like Hidden Markov Models (HMMs) [7] and Gaussian Mixture Models (GMMs) [8] or discriminative ones such as Support Vector Machines (SVMs) [9], [10] and Multi Layer Perceptrons (MLPs) [11] for verification.

The research in the area of distance based methods is focussed on the method of Dynamic Time Warping (DTW), an elastic matching scheme. The early explorations of this scheme can be found in the works such as [1], [12], [13], where the idea is to extract a set of features from the shape of the signature and to compute the similarity between an input signature and the reference set using dynamic programming. The score obtained is then subsequently compared to a threshold for authentication. With regards to the decision making process, employing user specific thresholds is found to give improved performance, in comparison to a single global threshold [1].

A variant of the DTW approach is the extreme point warping technique [14], where-in only selective points of the online trace are warped. Yet another modification is the edit-distance based string matching algorithm [15] for comparing the sequence of position extremal points between a test input and the set of enrolled signatures.

In [9], the authors view the signature verification system as a two class pattern recognition problem. The authenticity of test signature is determined by matching it against a set of reference signatures using DTW. Thereafter, a set of three distances of the test signature to the reference signatures are derived and subsequently normalized to form a three-dimensional feature vector. The classification to either genuine or forgery is achieved by using a SVM.

The authors are with the Department of Computer Science and Engineering, Graphic Era Univeristy (Deemed to be University), Dehradun-248002, Uttarakhand, India.
Department of Electronics and Communication Engineering, Indian Institute of Information Technology Allahabad, Prayagraj-211012, India.
e-mail: tanzeyl.khan@gmail.com, rkbhukya@iiita.ac.in
Manuscript received ; revised .

A matching between signatures, based on the concept of Longest Common Sub-Sequence has been used in [16], with turning angle based features, that are derived at each sample point of the online trace. The authors in [17] suggest a verification system, built using a fusion of DTW with Fourier descriptors. In addition, length normalization methods based on three resampling techniques (namely spatial based, temporal based and mean based) are proposed in [18], to allow for an easy computation of the similarity of the test signature with the enrolled reference signatures.

II. Problem Formulation and Contributions

We propose our novel verification strategy in line with the distance based techniques. The DTW algorithms in the literature of online signature verification use only the distance scores, obtained between the test signature and the genuine enrolled signatures, for formulating the decision rule [6]. Either the minimum, maximum or average of scores are utilized in the verification step [19]. We note two important observations from the survey of works on distance based techniques in the literature.

1) The cost matrix is utilized only for getting the DTW score.
2) 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. However, at times, the sole dependence on the DTW score may not be effective enough in discriminating the 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 forgery signature getting accepted.

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. This is the research gap from the literature of online signature verification that we intend to address with our proposal. The main idea, as we shall see in subsections III-C and III-D, is to consider using the alignment obtained from a DTW match together with another alignment, proposed based on a measure analogous to correlation-based matching. The characteristics of each of the alignments on the warping path are analyzed to discriminate between genuine and forgery signatures by proposing a novel feature. Thereafter we fuse the DTW score with that obtained from the proposed warping-path based feature in subsection III-E, to enhance the authentication performance beyond that achieved using DTW score alone.

In addition, we consider evaluating our enhanced DTW system on a set of novel features, that have been modified from the ones popularly used in literature. We propose the notion of a spacing parameter in subsection III-A for feature extraction and demonstrate its utility in increasing the separation between the distribution of genuine and forgery signatures of an user.

The following are the contributions of our work:

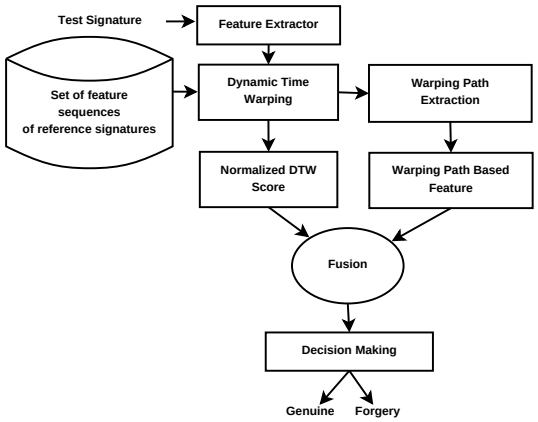


Fig. 1. Block diagram of proposed verification scheme.

- proposal of a novel feature that describes the characteristic of the warping paths of genuine and forgery signatures.
- incorporation of the derived warping-based feature with the DTW score for decision making.
- extraction of features for the DTW algorithm, based on the novel idea of spacing parameter.

III. Proposed Signature Verification System

Figure 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 enrolled signatures using the DTW matching technique. The performance of the verification system is enhanced by taking into consideration, attributes derived from the warping path in the cost matrix. In the following sub-sections, we provide details on the modules.

A. Feature Extractor

We adopt a local-feature based approach, wherein a set of features are derived from each point along the online trace of a signature. The basic raw features captured by the device during data acquisition comprise x and y co-ordinates, pressure p, azimuth ϕ and inclination angle θ. Prior to feature extraction, each of them are separately normalized, by the min-max transformation, to the range $[0, 1]$. This step ensures that all the transformed basic features are mapped to a comparable numeric scale.

Our proposed attributes comprise eleven features, derived from the normalized basic features. These include namely, the first order differences of basic features, second order differences of spatial coordinates and trigonometric representation of angles- which are quite popular from literature. The novelty in the feature extraction module is primarily with regards to the method of computation, as enumerated below:

First order difference of basic features: For $i = 1, 2, ...n-r$,

we have

$$\begin{aligned}\Delta x_r(i) &= x(i+r) - x(i)\\ \Delta y_r(i) &= y(i+r) - y(i)\\ \Delta p_r(i) &= p(i+r) - p(i)\\ \Delta \phi_r(i) &= \phi(i+r) - \phi(i)\\ \Delta \theta_r(i) &= \theta(i+r) - \theta(i)\end{aligned} \tag{1}$$

Here n corresponds to the number of points in the signature. The value of r determines the coordinate with respect to which the first order difference is derived. By varying it, we can come up with different set of features, for describing the trajectory of the online signature. Hereinafter, we refer to r as the spacing parameter.

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

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

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

$$\begin{aligned}\sin(\alpha_r(i)) &= \frac{\Delta y_r(i)}{\sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2}}\\ \cos(\alpha_r(i)) &= \frac{\Delta x_r(i)}{\sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2}}\end{aligned} \tag{3}$$

Length-based features : defined by

$$\begin{aligned}l_r(i) &= \sqrt{(\Delta x_r(i))^2 + (\Delta y_r(i))^2}\\ \Delta l_r(i) &= \sqrt{(\Delta^2 x_r(i))^2 + (\Delta^2 y_r(i))^2}\end{aligned} \tag{4}$$

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 stems from the trend of distributions that is noticed between the genuine and forgery signatures for an user. As an illustration, Figures 2 (a)-(d) depict the normalized histograms of the length feature 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 IV-B is used in obtaining these plots. The distributions for the case when $r = 1$ is not that discriminative, when compared to that from the higher value $r = 6$. In fact, the bin indices corresponding to the genuine and forgery signatures at $r = 1$, have very similar values (Figures 2 (a) and (b)). On the other hand, the values of bin indices are quite different at $r = 6$, thereby suggesting that the features derived at higher spacing parameter ($r > 1$) aim at providing greater discrimination between the genuine and forgery signatures (Figures 2 (c) and (d)). It is however to be noted that the parameter r is chosen empirically based on experimentation. Accordingly, the values considered for the distributions in Figure 2 are for illustrative purpose only.

Let $\{S_1, S_2, ..., S_N\}$ denote the N genuine (reference) signatures of an user, that are enrolled into the verification system. We represent the sequence of point based features, for signature S_p (comprising n_p sample points) as:

$$\mathbf{F}_p = \{\mathbf{f}_p^1, \mathbf{f}_p^2, ..., \mathbf{f}_p^{n_p - r - 1}\} \qquad 1 \le p \le N \tag{5}$$

Here $\mathbf{f}_p^j = [f_p^j(1) \quad f_p^j(2) \quad .... \quad f_p^j(11)]^{\mathbf{T}}$ 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. The symbol $\mathbf{T}$ corresponds to the transpose operation of the row vector.

B. DTW based matching

The Dynamic Time Warping (DTW) algorithm is considered for matching a test signature T, (comprising a feature vector sequence of length $n_T - r - 1$) against a genuine enrolled signature S_p of length $n_p - r - 1$, where $1 \le p \le N$. 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 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:

$$d(m, n) = |\mathbf{f}_T^m - \mathbf{f}_p^n| = \sum_{k=1}^{11} |f_T^m(k) - f_p^n(k)| \tag{6}$$

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.

$$\psi(m, n) = d(m, n) + \min \begin{cases} \psi(m, n-1) \\ \psi(m-1, n-1) \\ \psi(m-1, n) \end{cases} \tag{7}$$

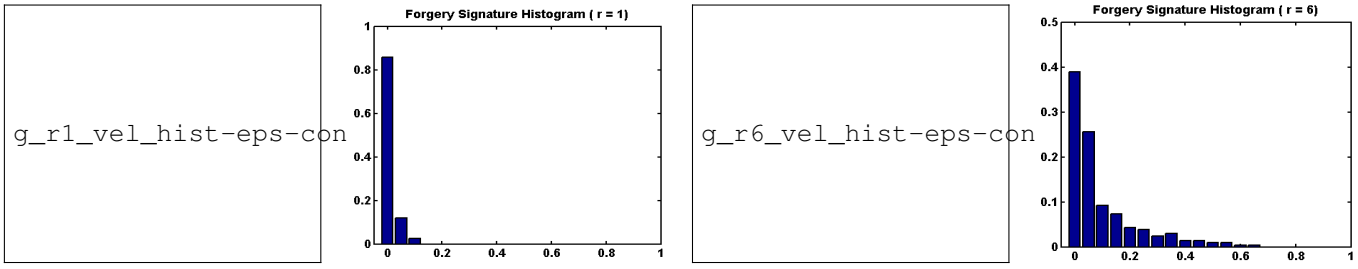
where $\psi(m, n)$ corresponds to the cumulative distance up-to the current element. In order to account for the varying warping paths, obtained during the matching process, with different enrolled signatures, the DTW score is normalized with $l_{\mathcal{W}_p^*}$, the number of aligned pairs on the warping path $\mathcal{W}_p^*$ [20] as:

$$d_1^p = \frac{\psi(n_T - r - 1, n_p - r - 1)}{l_{\mathcal{W}_p^*}} \tag{8}$$

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

$$\mathcal{W}_p^* = \{(a_1, b_1), (a_2, b_2), ..., (a_{l_{\mathcal{W}_p^*}}, b_{l_{\mathcal{W}_p^*}})\} = \{(a_i, b_i)\}_{i=1}^{l_{\mathcal{W}_p^*}} \tag{9}$$

Each of the pairs (a_i, b_i) denote that the feature vector corresponding to the a_i^{th} sample point of 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 cost matrix, corresponding to the a_i^{th} row and b_i^{th} column. Henceforth, in the remainder of the work, we interchangeably refer to the pair (a_i, b_i) as an 'alignment' or 'cell'. Owing to the boundary



(a) (b) (c) (d)

Fig. 2. Plot of the distribution of length feature, from an user in the MCYT-100 database, obtained using 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 $r = 6$ (sub-figures (c) and (d)).

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 features from the warping path in the following sub-section, to improve the verification performance.

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 analogous to correlation-based matching. The characteristics of each of the alignments (a_i, b_i) and (a_i, r_i^*) $\forall i$ $1 \leq i \leq l_{\mathcal{W}_p^*}$ are then analyzed to discriminate between genuine and forgery signatures. The formulation of the same is discussed in the following sub-section, subsequent to the determination of index r_i^*.

C. Extraction of Warping Path Based Feature

With the aim of analyzing the trend of values along the warping path of the cost matrix, we derive a novel warping-path based feature, based on two components - referred to as 'feature distortion' and 'displacement' To start with, we outline the preliminary ideas that will be utilized in deriving these components for the online signature verification problem.

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 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 $1 \leq i \leq l_{\mathcal{W}_p^*}$):

$$r_i^* = \arg \min_{1 \leq r_i \leq n_p - r - 1} \sum_{j=-w}^{w} |\mathbf{f}_T^{a_i+j} - \mathbf{f}_p^{r_i+j}| \qquad (10)$$

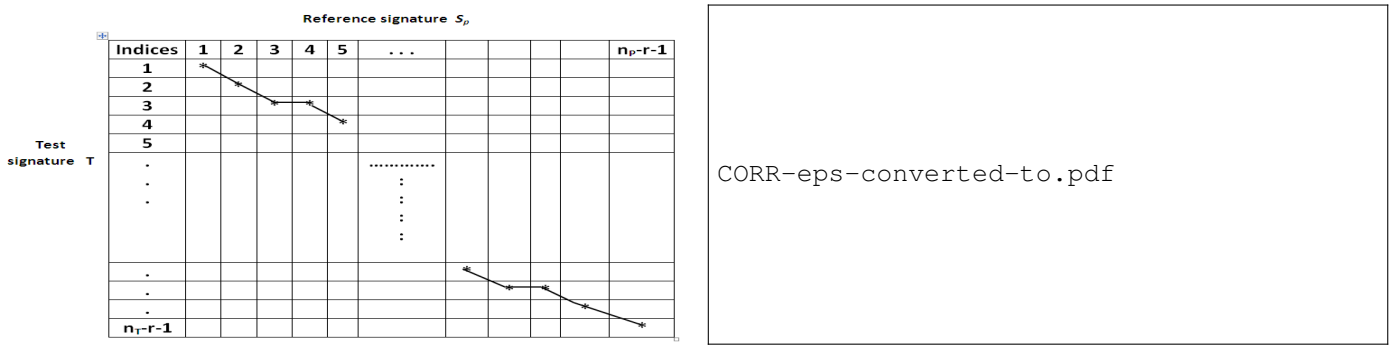
From the definition of Equation 6 on City Block distance, we can rewrite the above equation as

$$r_i^* = \arg \min_{1 \leq r_i \leq n_p - r - 1} \sum_{j=-w}^{w} d(a_i + j, r_i + j) \qquad (11)$$

Corresponding to each segment around a_i^{th} sample point of test signature T, the implementation for obtaining r_i^* in Equation 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 10) corresponds to the index value r_i^*. The computation in Equation 10 is performed for $\forall a_i$ in $\mathcal{W}_p^*$. This scheme of matching is analogous to the correlation-based matching method (based on neighborhood information), that has been successful in the domain of computer vision [21].

However, 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 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 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 T and reference signature S_p, denoted by $\{(a_1, r_1^*), (a_2, r_2^*), ..., (a_{l_{\mathcal{W}_p^*}}, r_{l_{\mathcal{W}_p^*}}^*)\}$, which can be also written in the form $\{(a_i, r_i^*)\}_{i=1}^{l_{\mathcal{W}_p^*}}$. 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 an example for the above matching scheme, let us consider the Figure 3(a), where-in a warping path from a DTW match between two



(a) (b)

Fig. 3. (a) An example 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 discussed in Equation 10

signatures is assumed to pass through the alignments $\{(a_1,b_1),(a_2,b_2),(a_3,b_3),(a_4,b_4),(a_5,b_5),.....,(a_{l_{\mathcal{W}_p^*}},b_{l_{\mathcal{W}_p^*}})\}$ such $\{(1,1),(2,2),(3,3),(3,4),(4,5),.....,(n_T-r-3,n_p-r-4),(n_T-r-3,n_p-r-3),(n_T-r-2,n_p-r-2),(n_T-r-1,n_p-r-1)\}$ on the cost matrix. Let us, as 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^*). To this effect, we consider a window of odd size (say three) around the fourth sample point in T (as shown in Figure 3(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 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 correlation based match.

From the definitions of the alignments / cells (a_i,b_i) and (a_i,r_i^*), we infer that:

- Both b_i and r_i^* refer to the index in the reference signature S_p.
- The warping path of DTW always passes through the alignment / cell (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 (Equation 10) and is analogous to the correlation-based methods. As such, 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 / cell (a_i,r_i^*) $\forall i$, $1\leq i\leq l_{\mathcal{W}_p^*}$.

Based on the preceding discussion, we observe two alignments for the a_i^{th} sample point of the test signature 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 the alignments (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 $1\leq i\leq l_{\mathcal{W}_p^*}$ [1]. We refer to each such term as 'feature distortion' in this work. When matching a genuine test signature T against a reference genuine signature S_p in the enrolled set, 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 difference / 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 an enrolled genuine 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} enrolled signature S_p (by considering the number of aligned pairs falling on the warping path $\mathcal{W}_p^*$), as follows:

$$d_{21}^p=\frac{1}{l_{\mathcal{W}_p^*}}\sum_{i=1}^{l_{\mathcal{W}_p^*}}d(a_i,b_i)-d(a_i,r_i^*) \tag{12}$$

In addition, for a match of genuine test signature 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 12, we average across the 'displacements' (by considering the number of aligned pairs on the warping path $\mathcal{W}_p^*$) as follows:

$$d_{22}^p=\frac{1}{l_{\mathcal{W}_p^*}}\sum_{i=1}^{l_{\mathcal{W}_p^*}}|b_i-r_i^*| \tag{13}$$

It is worth reminding here that both the indexes b_i and r_i^* correspond to the enrolled 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-genuine signature comparison, and higher for a forgery-genuine signature match.

Our proposed feature is the sum of average feature distortion and average displacement , defined as:

$$d_2^p=d_{21}^p+d_{22}^p \tag{14}$$

[1]To handle the case where identical values of r_i^* are obtained for more than one match, we consider that value corresponding to the minimum $d(a_i,r_i^*)$

In order to ensure that the terms d_{21}^p and d_{22}^p are in the same numerical range, each of the feature distortion terms $d(a_i, b_i) - d(a_i, r_i^*)$ in d_{21}^p are divided using a factor D_i defined as

$$D_i = \max_{1 \leq j \leq n_p - r - 1} d(a_i, j) \quad \forall i, 1 \leq i \leq \mathcal{W}_p^* \tag{15}$$

In a similar fashion, 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 14 as:

$$d_2^p = \frac{1}{l_{\mathcal{W}_p^*}} \left(\sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{d(a_i, b_i) - d(a_i, r_i^*)}{D_i} + \sum_{i=1}^{l_{\mathcal{W}_p^*}} \frac{|b_i - r_i^*|}{n_p - r - 1} \right) \tag{16}$$

D. Discussion

For the discussions in this sub-section, we will assume that there is only one reference signature S_1 of an user enrolled to the system, so that $p = 1$. We demonstrate the goodness of the proposed warping-based feature to the process of authentication, by considering the match of a genuine and skilled forgery signature in Figures 4(b) and (c) against a reference genuine signature, shown in Figure 4(a). The signatures presented correspond to an user from the SVC-2004 database. The scores d_1 from the DTW match are very close (0.78 and 0.74), and may not provide adequate discrimination (Figures 4(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 0.74 may falsely reject the genuine signature of Figure 4(b) to a forgery, while the forgery signature of Figure 4(c) can get falsely accepted as genuine, with a higher threshold (greater than 0.78). In addition, any threshold between 0.74 and 0.78 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 distance d_1. Nevertheless, this is alleviated by the proposal of the warping based feature d_2, which is observed to be contrasting for the genuine and forgery signature, respectively (the values being 0.21 and 0.48). Note that in comparison to d_1, the d_2 score for the genuine signature match in Figure 4(d) is lower compared to that of the forgery signature match in Figure 4(e). This trend 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 4(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 7 is used to compute the index r_i^* $\forall i$ along the warping path.

A critical analysis of the warping path (of the genuine to reference signature DTW match) in Figure 4(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 14. 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 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 4(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 4(e), the dissimilarity costs $d(a_i, b_i)$ along the warping path of a genuine to reference signature match in Figure 4(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 d_2 feature.

However, it is to be mentioned that owing to the large size $(n_T - r - 1) \times (n_p - r - 1)$, 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 the cells of the cost matrix. Thus, an alternative, we resort to analyzing the normalized histograms of the dissimilarity values $d(a_i, b_i)$ $\forall i$ along the warping paths. Figures 5(a) and (b) depict the plots for the case of the DTW match between the genuine and skilled forgery signature in Figures 4(b) and (c) with the reference signature in Figure 4 (a) respectively. Similarly, the normalized histograms for the feature distortion and normalized displacement terms, $\frac{d(a_i, b_i) - d(a_i, r_i^*)}{D_i} + \frac{|b_i - r_i^*|}{n_p - r - 1}$ $\forall i$ along the warping paths are shown in Figures 5(c) and (d). Comparing 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 0.28. Relative to this, the histograms in Figures 5(c) and (d) corresponding to the warping based features for the genuine and skilled forgery signature match have a high dissimilarity score of 0.75. This measure in turn suggests the discriminative nature of the warping based feature d_2, with regards to the verification of online signatures. For completion, in the Figures 5(e) to (h), we also present the normalized histograms for the feature distortion, $\frac{d(a_i, b_i) - d(a_i, r_i^*)}{D_i}$ and displacement terms $\frac{|b_i - r_i^*|}{n_p - r - 1}$ $\forall i$ along the warping paths, resulting from the DTW match of the genuine and skilled forgery signature in Figure 4(b) and (c) with the reference signature of Figure 4(a) respectively.

E. Fusion

As a further exploration, we investigate in this sub-section, on whether a conjunction of the warping based feature (d_2) with the DTW distance (d_1) can help improve the verification efficacy of our proposal. Given a set of N enrolled 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 distances as follows:

$$d_1^{mean} = \frac{1}{N} \sum_{i=1}^{N} d_1^i \qquad d_2^{mean} = \frac{1}{N} \sum_{i=1}^{N} d_2^i \tag{17}$$

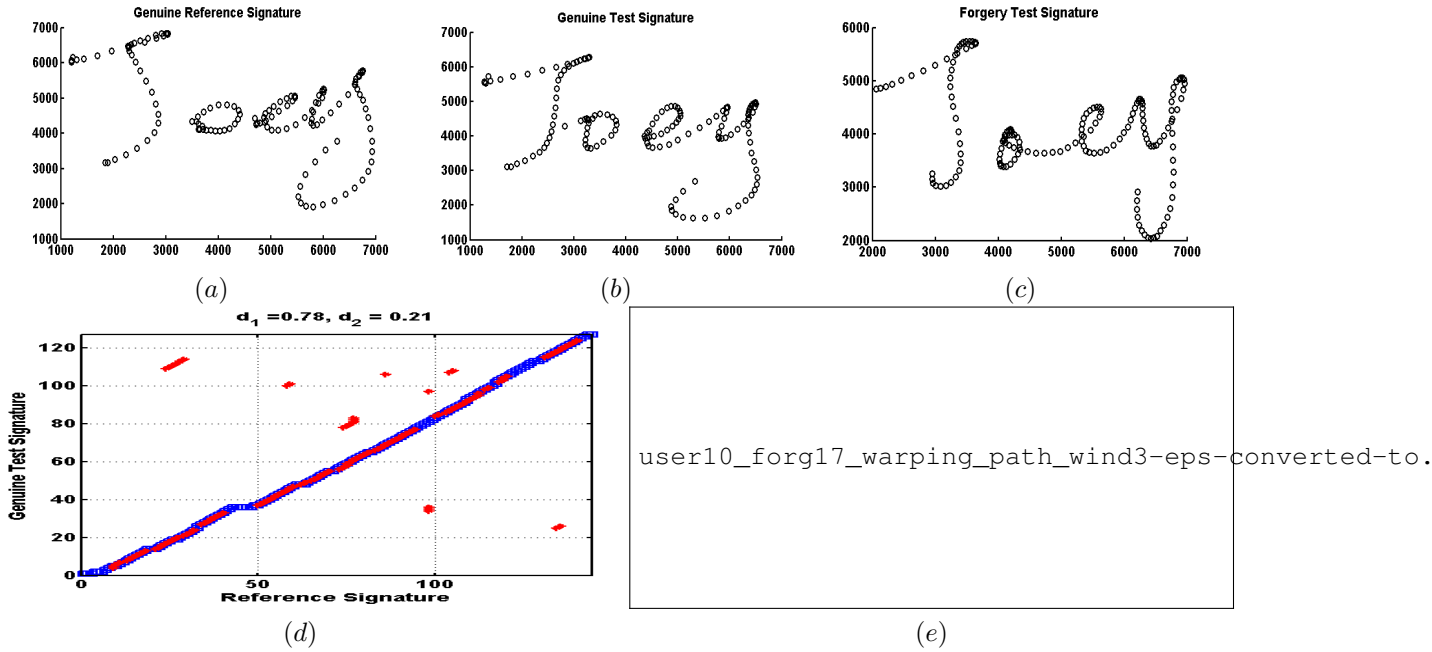


Fig. 4. An illustration of the effectiveness of warping based feature d_2 feature for verification. The sub-figure (a) depicts a sample of genuine reference signature (from an user of the SVC-2004 data-base) enrolled into the system. Sub-figures (b) and (c), correspond to a sample of genuine and skilled 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 are very close, leading to a possible false acceptance of a skilled forgery signature and /or rejection of the genuine signature to the verification system. The warping feature d_2, on the other hand, attempts to discriminate the signatures better. Here, a window of size 7 is employed for calculating r_i^*.

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 6(a) and (b)). The experimental protocol discussed in sub-section IV-B is used in generating these plots, with the values of d_1^{mean} and d_2^{mean} recorded over a set of ten enrolment trials. We see that the scores are indeed complementary in nature. The exclusive use of d_1^{mean} or d_2^{mean} yields a noticeable overlap between the distance values of genuine and forgery signatures. Hence, through a combination of these distances, it is hoped that the extent of overlap be reduced, thereby improving the efficacy of the verification system. A simple choice of combination that we employ is the sum rule, defined by:

$$d_T = d_1^{mean} + d_2^{mean} \tag{18}$$

Prior to combining the scores, they are separately mapped to the range $[0, 1]$ using the sigmoidal function. The verification system accepts the test sample 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 below:

$$d_T = \min_{1 \le i \le N} d_1^i + d_2^i$$
$$d_T = \max_{1 \le i \le N} d_1^i + d_2^i \tag{19}$$

The experimental results on the signature data-bases used in this work suggest that the fusion based on mean of the distance scores outperform the others. This is discussed further in the sub-section IV-D.

IV. Experiments and Discussion

A. Database Description

The signature verification experiments in this paper are reported on the publicly available SVC-2004 Task-2 set and MCYT-100 databases. Hereinafter, we refer to the SVC-2004 Task-2 database as SVC-2004. Here, the signature data is collected from a graphic tablet (WACOM Intuos) with 20 genuine and 20 skilled forgeries for each person. In total, 40 persons have contributed to this data in two separate sessions, spaced apart by at least one week. The data captured include (x, y) co-ordinates, pressure, azimuth, inclination, time stamp and pen up / pen down status [22].

The MCYT-100 [23] is a larger data-base, comprising signature samples of 100 individuals. For each individual, 25 genuine and 25 forgery signatures were collected using the WACOM pen tablet, model-Intuos A6 USB. Each trace of the signature contains the same information, as that of the SVC-2004 database (except for the time-stamp). The skilled forgeries were contributed by five different users, who had access to the static images of the genuine signature. The forgers were requested to sign in a natural way, without artifacts, such as slowdown or breaks.

B. Enrollment Protocol

In most experiments in this paper, the following protocol is used for the SVC-2004 database: for each user, we randomly

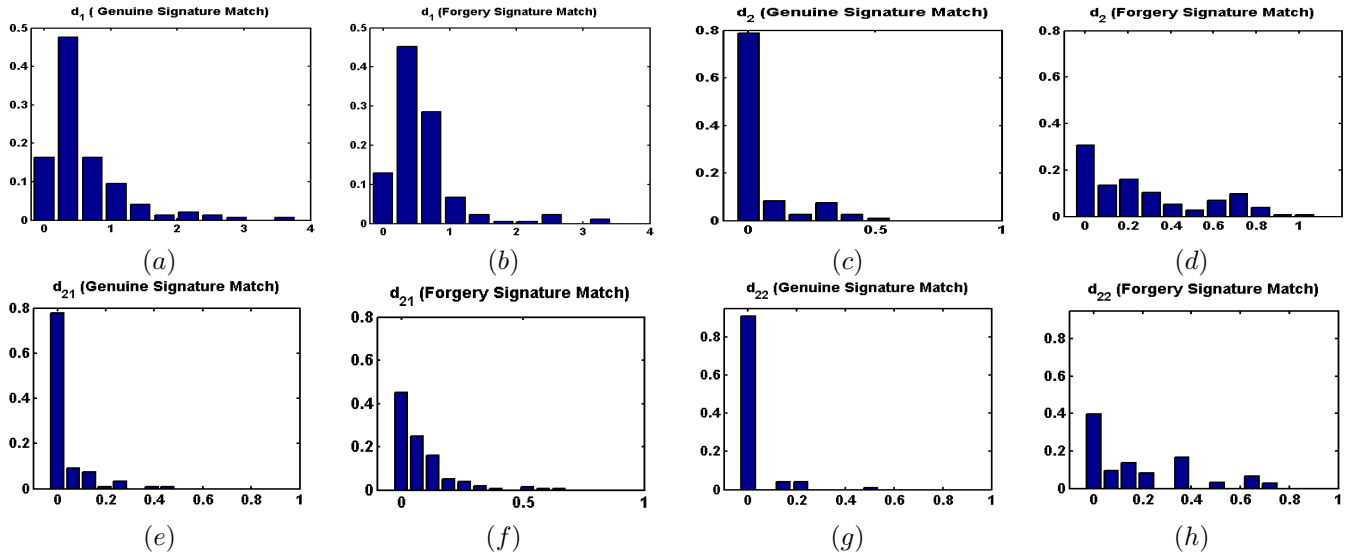


Fig. 5. (a-d): Normalized histograms of the dissimilarity values $d(a_i, b_i)$ (sub-figures (a),(b)) and the feature terms $\frac{d(a_i,b_i)-d(a_i,r_i^*)}{D_i} + \frac{|b_i - r_i^*|}{n_p - r - 1}$ (sub-figures (c),(d)) along the warping path, resulting from DTW match of the genuine and skilled forgery signature in Figure 4(b)-(c) with the reference signature of Figure 4(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))

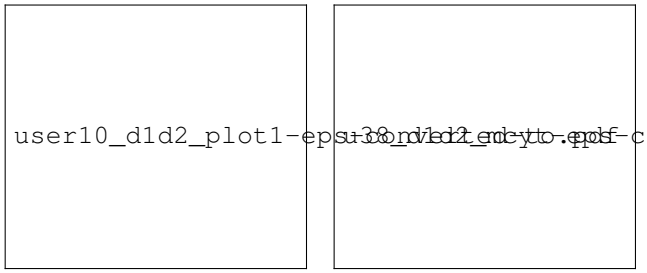


Fig. 6. A two-dimensional distribution of the normalized DTW and warping feature based scores on the genuine and skilled forgery signatures (depicted in blue and red colors respectively) of an user from the (a) SVC-2004 and (b) MCYT-100 database. The experimental protocol discussed in sub-section IV-B is used in generating these plots.

select a set of five of his/her genuine signatures for enrollment. The signatures are chosen from the first session, keeping in line with the set up used in the signature competition [22]. The remaining genuine signatures (not selected for enrollment) and skilled forgeries of this user are used to evaluate the performance of verification system. For computing the false acceptance of the random forgeries, genuine signatures of other users are used. In our set up, we consider one genuine signature per user, resulting in 39 random forgery examples for testing.

For the MCYT-100 database, we consider five genuine signatures per user for enrolment. The remaining 20 genuine signatures and 25 skilled forgeries are used for testing the efficacy of our proposal. In addition, a set of 99 genuine signatures (one each from the other users) is used to measure the performance of the system on random forgeries.

The procedure of selection of the signatures for enrollment (in either database) is performed over a set of ten trials. As each of the databases have limited number of users, we use this cross validation technique to evaluate a reliable average error performance of the proposed system.

C. Evaluation Protocol

While evaluating a 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.

With regards to the decision making process, we have explored using both the *a-posteriori* user-dependent threshold and *a-posteriori* user-independent / common threshold [7], [24]. In a common threshold setting, the matching scores corresponding to all signature data (apart from those used for enrolment) from all the writers are pooled together to compute a global threshold and subsequently the EER. However, prior to obtaining the threshold, a target / user dependent normalization [25] is desired to transform the score distribution of each user to a standard range. In this work, we consider subtracting the matched score from the corresponding mean of the target scores, that are obtained from the set of enrolled signatures, and subsequently apply the sigmoidal function to map the scores to $[0, 1]$ range. In order to compute the mean score from the set of enrolled data, each reference signature is considered as a model of the user. Thereafter, the DTW and warping-path based distances (d_1 and d_2) with regard to the remaining reference signatures is calculated. In this way, for N enrolled signatures, we get $\binom{N}{2}$ scores to compute the mean.

Contrary to common threshold setting, for the user-

TABLE I
PERFORMANCE EVALUATION OF THE BASELINE DTW BASED SYSTEM ON THE PROPOSED FEATURES DERIVED USING VARYING VALUES OF SPACING PARAMETER r. THE MEER (IN %) IS COMPUTED WITH REGARDS TO THE GENUINE AND SKILLED FORGERIES, THAT ARE COMPARED AGAINST THE ENROLLED SIGNATURES IN THE SVC-2004 DATABASE.

* r	Common-threshold			User-threshold		
	BL-DTW system	WP system	Fused system	BL-DTW system	WP system	Fused system
1	20.24	13.72	12.93	13.38	5.96	4.43
2	15.53	12.34	9.98	8.46	4.59	3.83
3	13.05	10.89	9.24	5.86	4.64	2.96
4	11.26	10.24	8.46	4.96	4.45	2.71
5	11.11	10.09	8.13	4.52	4.16	2.58
6	10.98	10.04	8.42	4.16	4.02	2.64
7	10.91	10.17	8.44	4.28	4.05	2.78
8	10.42	10.10	8.31	4.25	4.18	2.71
9	10.37	10.10	8.54	4.30	4.10	2.98
10	10.39	10.05	8.52	4.12	4.05	3.06

TABLE II
PERFORMANCE OF THE SUM RULE COMBINATION ON THE THREE STRATEGIES REFERRED TO IN THE EQUATIONS 18 AND 19 WITH, SPACING PARAMETER $r = 5$ FOR FEATURE EXTRACTION.

* Method	Common Threshold			User Threshold		
	BL-DTW system	WP system	Fused system	BL DTW system	WP system	Fused system
Mean	11.11	10.09	8.13	4.52	4.16	2.58
Minimum	12.08	10.94	9.01	4.83	4.5	3.07
Maximum	14.23	12.98	10.95	7.06	5.71	4.40

dependent threshold setting, we use only the scores corresponding to the claimed user in question to obtain the EER. Accordingly, to test the efficacy of the system, we average the EERs across all the users enrolled in the system, and adopt the MEER (Mean Equal Error Rate) for performance evaluation. The averaged EER / MEER (computed over the trials) is reported for both common / user-independent and user-dependent threshold settings.

D. Performance Evaluation on SVC-2004 Database

The baseline used in this work (abbreviated by BL-DTW system) is the one that employs the DTW scores d_1^{mean} for verification. To begin with, we evaluate its performance on the proposed feature set (discussed in section III-A), that are characterized by using different values of the spacing parameter r. The second and fourth columns of Table I outline the findings of this experiment for r between one to ten in step of one. As expected, the MEER obtained from using user specific threshold (fourth column) is lower to that of the common threshold (second column). Yet, an interesting trend observed is with regards to the MEERs 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.

TABLE III
MEER (IN %) OF THE PROPOSED SYSTEM WHEN DIFFERENT NUMBER OF REFERENCE GENUINE SIGNATURES OF THE SVC-2004 DATABASE ARE ENROLLED TO THE VERIFICATION SYSTEM. IN THIS SET UP, SPACING PARAMETER $r = 5$ IS CONSIDERED FOR FEATURE EXTRACTION.

# of ref sign	Common Threshold		User Threshold	
	BL-DTW system	Fused system	BL-DTW system	Fused system
1	22.97	17.01	6.14	4.4
2	14.28	12.53	4.96	3.23
3	12.25	10.05	4.68	2.91
4	11.25	8.61	4.63	2.87
5	11.11	8.13	4.52	2.58
10	10.69	8.56	4.94	2.74

Coming to the efficacy of the proposed enhanced DTW system, we see that the fusion with the warping path (WP) based score, brings down the MEER of the baseline system. An MEER to as low as 8.13% and 2.58% is obtained with a spacing parameter $r = 5$, for the common and user threshold settings respectively for the fused system. Owing to its good performance, we consider the spacing parameter $r = 5$ for the experiments described hereinafter for this database. It may be noted that the MEER (in %) is computed with regards to the genuine and skilled forgeries of the SVC-2004 database, that are compared against the enrolled signatures.

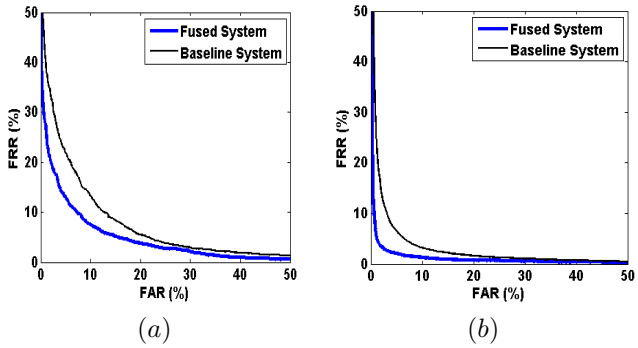
We now explore on the performance of the sum rule on the three strategies referred to in the Equations 18 and 19. The results in Table II, suggest a comparable performance between the mean and minimum based fusion techniques (8.13 % and 9.01 % MEER for common threshold, 2.58% and 3.07% MEER for user threshold set-up respectively). However, owing to the fact that the database comprises a wide intra-class variation between the genuine signatures of an user, we prefer the mean based fusion. This technique in a way, aids in smoothing out the intra-class variability by averaging each of the distances d_1 and d_2, over the set of enrolled reference samples, and then combining them with the simple sum rule (Equations 18 and 19). 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 distances d_1 and d_2 over the set of reference signatures, gives a higher MEER of 10.95 % and 4.40 % for common and user thresholds respectively.

In the results of Tables I and II, we use a window of length 11 to calculate the warping feature (described in Equations 10 to 14). We did experiment using different odd window sizes ranging from one to fifteen. However, across varying lengths, we found very comparable results. The window size of eleven gave the minimum MEERs for the mean-based fusion strategy.

By using the mean based fusion strategy with spacing parameter $r = 5$ (for computation of features) and window

TABLE IV
EFFECTIVENESS OF THE PROPOSED SYSTEM (ON THE SVC-2004 DATABASE) WITH RANDOM FORGERIES, FOR VARYING VALUES OF SPACING PARAMETERS r.

	BL-DTW system	Fused system	BL-DTW system	Fused system
1	1.02	0.39	0.11	0.02
2	0.48	0.32	9.2×10^{-5}	1.16
3	0.30	0.25	0	0
4	0.24	0.19	0	0
5	0.19	0.15	0	0
10	0.14	0.13	0	0



(a) (b)

Fig. 7. The Detection Error Tradeoff (DET) curves corresponding to the SVC-2004 and MCYT-100 databases (using skilled forgeries) for the user-independent threshold scenario.

$2w+1$ of size 11 (for computing d_2), we evaluate our proposal for different number of genuine reference signatures enrolled to the system. It is interesting to note (from Table III) that the fusion step verifies the authenticity of a user quite effectively with as low as three or four reference signatures for user-specific and common threshold setting respectively.

As a next experiment, we consider experimenting our strategy on random forgery signatures. The MEER performance with different spacing values r is shown for both common and user specific thresholds in Table IV. An improvement is noticed for $r = 1$, (using common threshold) with MEER reducing from 1.02% to 0.39%, subsequent to the fusion step. Beyond $r = 3$, user specific threshold provides an MEER of 0%, even for the baseline DTW system. Moreover, for the values of r where the MEER is non zero with the baseline DTW system, there is reduction in its values post fusion step. This improvement in the verification performance further bolsters the efficacy of our methodology.

We conclude the discussion of the experiments on the SVC-2004 database by providing the DET curve obtained from all the tested signatures (using skilled forgery) across all the tested users of a single trial in Figure 7(a). The features used are computed at spacing parameter $r = 5$. An user-independent threshold is used in deriving this curve, which by definition, is a two-dimensional measure of classification performance that plots the rate of false rejection (FRR) against the rate of false acceptance (FAR). It is interesting to note that the fusion outperforms the baseline system in almost all of the points of the DET-curve.

E. Performance Evaluation on MCYT-100 Database

The experiments reported in this subsection are aimed towards suggesting that the proposed methodology does enhance the performance of the DTW based system, irrespective of the database being used. Keeping in perspective, the contributions of our work on proposal of new features (using spacing parameter) and improvement of the DTW system using warping based features, we demonstrate our results in Table V. The MEER (in %) is computed with regards to the genuine and skilled forgeries of the MCYT-100 database, that are compared against the enrolled signatures.

The warping based feature alone (in third and sixth columns) is effective in bringing the MEERs to an average of around 3.07% (common threshold) and 1.23% (user dependent threshold), for values of the spacing parameter r between 4 and 6. In addition, as observed from the fourth and seventh columns, the fusion step helps in further reducing the MEERs. 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 persons (unlike the SVC-2004 database, wherein the persons were asked to 'invent' signatures [22], [26]). 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 feature d_2 effective for discriminating the genuine from the forgery signatures. Nevertheless, perfect separation of warping based feature between genuine and forgery signatures is not guaranteed, and hence fusion of scores helps. For the case of user-dependent threshold, our verification system achieves a lowest MEER of 1.15 % for the spacing parameter $r = 6$. With regards to the common threshold, we achieve a MEER of 2.76%, again for the spacing parameter $r = 6$.

In addition, on experimentation with different ways of fusing the scores (Table VI), we observe a trend similar to that obtained in the SVC-2004 (with the mean strategy outperforming the others). With regards to the performance with different number of genuine reference signatures, we obtain an MEER to as low as 1.56 % (common threshold) and 0.71% (user threshold) with 20 reference signatures, enrolled to the system, thus indicating that the proposed methodology is capable of rejecting skilled forgeries (Table VII). Further, we evaluate our verification strategy on random forgery signatures. The MEER performance with different spacing values r is shown for both common and user specific thresholds in Table VIII. Once again, we observe a reduction in MEER, post the fusion step. Last but not the least, we conclude by providing the DET curves of all the tested signatures (using skilled forgery) across all the users for a single trial in Figure 7(b). The features used are computed at spacing parameter $r = 6$.

F. Comparison to prior works

To corroborate on our contributions, we present a comparison of the proposed technique to recent algorithms from the

TABLE V
PERFORMANCE EVALUATION ON THE GENUINE AND SKILLED FORGERIES OF THE MCYT-100 DATA-BASE, WITH FEATURES PROPOSED USING DIFFERENT VALUES OF SPACING PARAMETER r.

r^*	Common-threshold			User-threshold		
	BL-DTW system	WP system	Fused system	BL-DTW system	WP system	Fused 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

TABLE VI
PERFORMANCE OF THE SUM RULE COMBINATION ON THE THREE STRATEGIES REFERRED TO IN THE EQUATIONS 18 AND 19, WITH SPACING PARAMETER $r = 6$ FOR FEATURE EXTRACTION.

Method*	Common Threshold			User Threshold		
	BL-DTW system	WP system	Fused system	BL DTW system	WP system	Fused 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

TABLE VII
EFFICACY OF THE PROPOSED SYSTEM WHEN DIFFERENT NUMBER OF GENUINE REFERENCE SIGNATURES FROM THE MCYT-100 DATABASE ARE ENROLLED, WITH SPACING PARAMETER $r = 6$ FOR FEATURE EXTRACTION.

# of ref sign	Common Threshold		User Threshold	
	BL-DTW system	Fused system	BL-DTW system	Fused 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

TABLE VIII
EFFECTIVENESS OF THE PROPOSED SYSTEM WITH RANDOM FORGERIES ON THE MCYT-100 DATABASE, FOR VARYING VALUES OF SPACING USED FOR FEATURE EXTRACTION.

r^*	Common Threshold		User Threshold	
	BL-DTW system	Fused system	BL-DTW system	Fused system
1	1.92	1.43	0.71	0.38
2	1.44	1.07	0.49	0.19
3	1.35	0.88	0.46	0.16
4	0.86	0.63	0.39	0.18
5	0.82	0.62	0.37	0.13
6	0.74	0.56	0.31	0.15
10	0.66	0.54	0.33	0.16

literature of online signature verification for the SVC 2004 and MCYT 100 databases. The relevant works are listed in Tables IX and X. It is worth mentioning that each of the systems have been trained and tested differently, with different sets of features employed for the classifiers, and hence a direct one-to-one comparison may not always be possible. Nevertheless, we note that our method, is at the very least, comparable (or even better) in terms of verification performance than a majority of these works (including those based on DTW) for the SVC 2004 database. A special mention is with regards to the MCYT-100 database, where we obtain a very commendable MEER of 2.76 % using common thresholds.

V. CONCLUSION AND FUTURE WORK

In this paper, we presented a novel online signature verification strategy, that extends on the classical DTW framework. Our contributions are (i) exploration of novel features for the DTW algorithm, based on the idea of spacing parameter. (ii) proposal of a novel feature that describes the characteristic of the warping paths of genuine and forgery signatures. (iii) incorporation of the derived warping-based feature with the normalized DTW score for decision making.

The current research leads to possible explorations for the future- Firstly, we can study the effect of concatenating the sets of point-based features, computed at various spacing values on the performance of the DTW algorithm. The current work utilizes the local features derived from only a single value of r. Another direction for exploration is to consider the proposed warping based feature on the variants of DTW that have been used in works from other domains, such as speech [20]. Lastly, one can attempt implementing ideas similar to our proposal on other domains that utilize the DTW algorithm.

REFERENCES

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

[2] A. Namboodiri and S. Gupta, "Text independent writer identification from online handwriting," in *Tenth International Workshop on Frontiers in Handwriting Recognition*, 2006, pp. 287–292.

[3] 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.

[4] 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.

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

[6] 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-Delacrétaz, Gérard Chollet, Ed. Springer Science & Business Media, 2009, pp. 125–165.

[7] 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.

[8] 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.

TABLE IX
SURVEY OF RELATED WORKS ON THE SVC-2004 DATABASE.

Method	Common threshold	User Threshold
DTW + SVM [9]	6.96	-
Feature selection+DTW [27]	-	3.38
LCSS [16]	-	5.33
DTW+HMM [24]	10.91	6.91
Sparse representation [28]	5.61	3.98
Dynamic programming [29]	10.15	3.61
Horizontal partitioning+fuzzy rule based [30]	11.58	-
Vertical partitioning+fuzzy rule based [31]	10.70	-
HMM + Viterbi Path [26]	4.83	-
HMM [7]	6.90	-
Proposed method	**8.13**	**2.58**

TABLE X
SURVEY OF RELATED WORKS ON THE MCYT DATABASE.

Method	Common threshold	User threshold
Dynamic programming [29]	10.15	3.61
VQ+DTW [19]	-	5.42
DTW + Fourier descriptors [17]	-	7.22
Symbolic Representation [32]	6.12	5.84
Histogram Based Analysis [33]	4.02	-
Velocity and pressure based partition [34]	-	1.09
HMM+Parzen Window [35]	5.29	2.12
HMM + Viterbi Path [26]	3.37	-
Ensemble of Parzen Windows [36]	8.4	-
Proposed method	**2.76**	**1.15**

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

[10] 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.

[11] 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.

[12] Y. Sato and K. Kogure, "Online signature verification based on shape, motion and writing pressure," in *Proc. of 6th Intl. Conf. on Pattern Recognition*, 1982, pp. 823–826.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

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

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

[22] 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.

[23] J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, "MCYT baseline corpus: a bimodal biometric database," *IEE Proc. Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 391–401, 2003.

[24] 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.

[25] 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.

[26] 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.

[27] J. Pascual-Gaspar, V. Cardeñoso-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.

[28] Y. Liu, Z. Yang, and L. Yang, "Online signature verification based on DCT and sparse representation," *Cybernetics, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014.

[29] 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.

[30] K. Cpałka, M. Zalasiński, 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.

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

[32] 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.

[33] 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.

[34] 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.

[35] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, 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. K. Ratha, Eds. Springer Berlin Heidelberg, 2005, vol. 3546, pp. 523–532.

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

Abhishek Sharma received the Bachelors degree in Electronics and Telecommunication engineering from the Government Engineering College, Raipur, India, in 2008, and the M.Tech. degree from the Indian Institute of

Technology (IIT) Delhi, India, in 2010. He is currently working toward the Ph.D. degree in the Department of Electrical and Electronics Engineering, IIT Guwahati, India. His research interests include online signature verification, writer identification, character recognition, and pattern recognition.

Suresh Sundaram received his PhD degree from Indian Institute of Science, Bangalore, India in 2012. Between 2012 September to July 2013, he was a research consultant at Hewlett Packard Research Labs, Bangalore, India. He is currently an assistant professor in the department of Electronics and Electrical Engineering at IIT Guwahati, India. His research interests encompass the areas of handwriting recognition, biometrics , document analysis.