Published in IET Biometrics
Received on 9th February 2012
Revised on 11th June 2013
Accepted on 14th June 2013
doi: 10.1049/iet-bmt.2012.0048

ISSN 2047-4938

Online signature verification using segment-level fuzzy modelling

Abdul Quaiyum Ansari[1], Madasu Hanmandlu[2], Jaspreet Kour[1], Abhineet Kumar Singh[3]

[1]*Department of Electrical Engineering, JMI, New Delhi, India*
[2]*Department of Electrical Engineering, IIT, New Delhi, India*
[3]*Department of Information Technology, IIIT, Allahabad, UP, India*
E-mail: tojaspreet@gmail.com

Abstract: This study presents a new online signature verification system based on fuzzy modelling of shape and dynamic features extracted from online signature data. Instead of extracting these features from a signature, it is segmented at the points of geometric extrema followed by the feature extraction and fuzzy modelling of each segment thus obtained. A minimum distance alignment between the two samples is made using dynamic time warping technique that provides a segment to segment correspondence. Fuzzy modelling of the extracted features is carried out in the next step. A user-dependent threshold is used to classify a test sample as either genuine or forged. The accuracy of the proposed system is evaluated using both skilled and random forgeries. For this, several experiments are carried out on two publicly available benchmark databases, SVC2004 and SUSIG. The experimental results obtained on these databases demonstrate the effectiveness of this system.

1 Introduction

Biometrics is an emerging field of technology for the enforcement of security. Several biometric modalities have been proposed in the last decades [1]. These can be divided into two main classes, depending on whether they are based on physical called physiological or behavioural traits of an individual. Physical traits are related to anatomical characteristics of a person and include fingerprint, face, iris and hand geometry among others. Behavioural traits refer to how an individual performs an action, and include voice, signature and gait among the most popular ones.

Signatures have been used for centuries to validate documents and transactions. Therefore, signature is one of the most socially accepted biometric traits, thus making it the most natural and established way of confirming an identity. It is non-invasive in nature and has no undesirable health connotations [2]. In the past few decades, digitising devices have made machine-based signature verification possible. Despite its wide acceptance, automatic signature verification is still a challenging task. One of the main challenges in signature verification is posed by the signature variability. While signatures from the same user taken at different times show considerable differences (high intra-class variability), skilled forgers can imitate signatures with high resemblance (low inter-class variability). An experimental study of human perception of handwritten signatures covering genuine and the forged samples is reported in [3]. The human strategies for signature checking influence the automatic signature verification. Moreover, factors like the number of reference samples available, signature sample variability and complexity of signature patterns also affect the verification process.

Signature verification can be split up into two modes – online and offline – depending on the type of available data. Online or dynamic signatures are captured by special hardware (e.g. smart pens or pressure sensitive tablets), which is capable of measuring dynamic properties of a signature in addition to its shape. Offline signatures, on the other hand, are drawn on paper with ordinary pens and thus have shape as the only available information. Online signatures are typically considered more reliable than offline ones since dynamic properties like pen pressure and writing speed make the signature more unique and difficult to forge. Each online signature is represented by a discrete time sequence of data points with each point containing the x, y coordinates, time stamp and button status. Additional information like pen pressure, altitude angle and azimuth angle may also be present.

Applications of online signature verification include identity verification during electronic payments (e.g. using a credit card), authorisation of computer users for accessing the sensitive data or programs, authentication of individuals for accessing physical devices or buildings and protection of small personal devices (e.g. PDA, laptop) from unauthorised usage [4].

The remainder of this paper is organised as follows: Section 2 presents a brief review of the existing literature along with showcasing the novelty of this work over an existing method [5]. Section 3 details the proposed methodology involving preprocessing, segmentation, segment alignment, feature extraction and fuzzy modelling. Section 4 presents the details of databases and methodologies used in the performance evaluation along with the obtained results and their comparison with several

state-of-the-art methods. Section 5 gives the conclusions and the future scope.

2 Background

2.1 Related work

An extensive literature exists in the field of online signature verification. A review of some of the more recent approaches has been carried out in [6]. Signature segmentation is considered mostly as the first step in the verification process. Segmentation is defined as the detection of perceptually important points in [7] at which to divide the signature into segments. The work presented in [8] measures the perceptual importance of each point by the change of writing angle between the selected point and its neighbour. A modified version of this method appears in [9], where the end points of pen-down strokes are considered as the significant splitting points. The method proposed in [10] uses the points of geometric extrema, both horizontal and vertical, as the segmenting points and carries out segment-to-segment matching through a set of rules based on the properties of the extremum specific to each such point. Three different segmentation methods, using equal partitioning, strokes and local extrema, are implemented in [11].

Since different signatures may have different lengths, a method is needed to equalise them before they can be compared on a point-to-point or segment-to-segment basis. Dynamic time warping (DTW) is a technique that employs compression or expansion of the time axis of two time sequences, representing two signatures with possibly different number of points, to obtain a correspondence that minimises some measure of distance between them. DTW has been employed widely in the literatures [10, 12–16] to aid the signature matching process.

Most of the existing methods extract a set of features either from the signature or from the individual segments before verification. A comparative study of features commonly used in online signature verification is presented in [17]. Owing to a large number of the available features, we need a method to select a subset of features with the maximum discriminative ability. Genetic algorithm (GA) has been used for this purpose in [5, 18–20]. The approaches such as velocity image model [21], fast Fourier transform [22], Rough sets [23] and Mellin transform [24] necessitate complex feature extraction procedures.

Fuzzy logic is a powerful tool for solving complex problems because of its ability to handle uncertainties in the inputs and it also incorporates the heuristics devised by a human expert to arrive at the most likely solution. Fuzzy inference is used for both offline and online signature verification. Methods in the former category include those based on modular neural network [25], snake algorithm [26], box method [27, 28] and confidence fuzzy intervals [29]. Most of these methods employ the relatively simpler Takagi-Sugeno (TS) model. There are several examples in the latter category, such as [30] that employs a neural network classifier with fuzzy inference decision module; [20] that uses fuzzy network; [31] that employs neural network-driven fuzzy reasoning; and [5] that uses a rule-based Mamdani system for fuzzy modelling of optimal features selected using GA.

2.2 Novelty of the proposed method

The present work can be regarded as an extension of the work in [5], where fuzzy modelling is carried out on features extracted from a whole signature. In this work, however, a signature is first divided into segments which are then aligned with the segments of a reference signature before applying an adapted version of the same fuzzy model at the level of individual segments. This extra step of segmentation can significantly improve the detection accuracy for reasons stated in Section 3.2. In addition, a novel adaptive segmentation improves the quality of segments and produces more accurate segment-to-segment correspondence.

Another significant difference arises with regard to the use of a threshold. A single global threshold is used in [5] to classify a test signature as genuine or forged whereas we use a different threshold for each user. A user-dependent threshold captures the inherent variability in a particular user's signatures and thus helps to reduce both false acceptances and false rejections. For example, a user who is not very precise about the way he writes his signatures will exhibit greater variability among his genuine signatures as compared to a user who is always extremely specific about the way his signatures are made. This difference in writing habit necessitates the use of a higher threshold for the second user than the first one to obtain optimal results. Thus, using a single threshold for both these users may lead to an increased rate of false rejections for the first user and false acceptances for the second one. Another advantage of user-dependent threshold is that the use of global threshold requires the entire system to be trained again to obtain an updated threshold whenever a new user is added to the database whereas with user-specific threshold, however, only the new user's signature samples are needed in the training process The time required for this process is therefore independent of the number of users already present in the database and does not increase as the database grows larger, which is not the case with the global threshold. Also, the user-specific threshold is found to be more appropriate than the global threshold in behavioural biometrics because of comparatively larger variations in genuine samples of a person than in physiological biometrics where global thresholds might make more sense.

3 Proposed system

A block diagram of the proposed system is shown in Fig. 1. All the tasks mentioned therein are performed independently for each user. The preprocessing of each signature sample is followed by segmentation along the points of geometric extrema. Next, all the training samples of the same user are pair-wise segment-aligned with each other. One of the training samples is then chosen as the prototype genuine sample for that user and all the test samples of that user are segment-aligned with this sample. This is followed by the feature extraction where both static (shape) and dynamic features are extracted for each segment for all the samples (training and testing). The extracted features are subjected to fuzzy modelling using a combination of TS and Mamdani approaches to obtain a single match score for each segment. The scores of all the segments of each sample are then combined to obtain an overall score for that sample. This score is compared with a user-dependent threshold at the decision stage to classify the sample as either genuine or forged.

3.1 Preprocessing

The signing process is considered as a ballistic movement that causes variation among the genuine signatures of the same

doi: 10.1049/iet-bmt.2012.0048

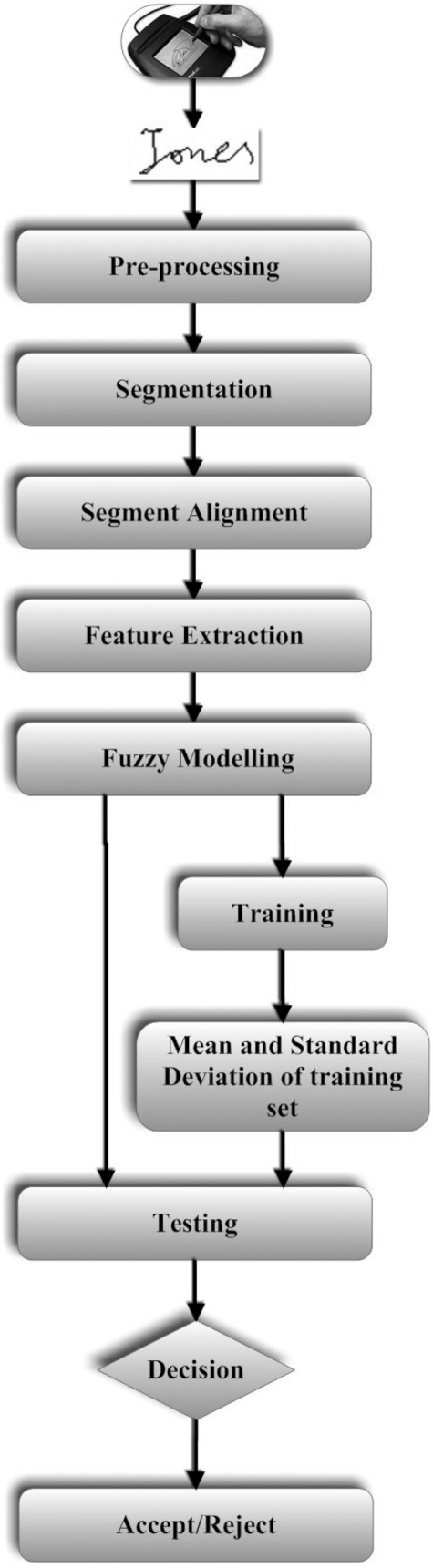

Fig. 1 *Block diagram of the proposed system*

person. As the variations in different signatures have different dynamic ranges, min–max normalisation is applied on their x and y coordinates. The normalisation process used here shifts the minimum and maximum scores to 0 and 1000, respectively; but it does not change the underlying distribution of the data except for a scaling factor.

$$x_n = \frac{x - \min(x)}{\max(x) - \min(x)} \times 1000 \tag{1}$$

$$y_n = \frac{y - \min(y)}{\max(y) - \min(y)} \times 1000 \tag{2}$$

where x and y are the original coordinates and x_n and y_n are the normalised coordinates. The remaining components of each data point, viz., pressure and angle information (both altitude and azimuth) are not changed since they are fairly resistant to noise and also contain crucial clues to the way a person holds the pen and writes with it. These characteristics are typically specific to a person and are practically impossible to forge without detailed knowledge of the person's writing manner. Thus retaining their original values is necessary for deriving maximum discriminative ability.

3.2 Segmentation

When features are extracted from the whole signature sample, they are subjected to an averaging effect [10] due to which finer information present in localised regions of the sample is lost, thus reducing the discriminative capability of the features. This is particularly true for online signatures – since dynamic information present in specific parts of a signature is crucial in identifying the writer and it is difficult to be forged. For example, many people have a specific pattern in the speed with which they typically generate their signatures, for instance, slow in the beginning and at the end of the signature but with the maximum speed in the middle. This is why the samples are segmented before the feature extraction step.

A good segmentation method should meet two main requirements [10]: the segments generated should be consistent across all the genuine samples and the correspondence between matching segments of any two samples should be easy to find. Based on these requirements, the points of geometric extrema are chosen to segment the signatures since they constitute the corner points of the frame of the pattern and are thus reproduced reliably in different samples of the same user. They also have specific properties that help in determining segment-to-segment correspondence [10]. Points of vertical and horizontal extrema are detected by finding the zero crossings of the derivatives of x and y sequences, respectively. The ith point in a signature sequence is taken as a point of vertical extremum, if the following condition holds true

$$(y_{i+1} - y_i)(y_i - y_{i-1}) \leq 0 \tag{3}$$

Here, y_i denotes the y coordinate value in the ith data point where $i = 2, 3, \ldots, k-1$ for a sample with k data points. A similar expression is used for the points of horizontal extrema too. In order to deal with the presence of noise in the time sequence, which may lead to several invalid segments, a certain threshold (δ) is taken as the minimum number of points in an acceptable segment. If a segment is having number of points $<\delta$, it is merged with the next segment if possible or with the previous one if it happens to

be too close to the end of the signature. Experiments are conducted by considering each of the x and y derivatives separately and the best results are obtained using the latter. Fig. 2 shows a few genuine and skilled forgery samples for the same user from SVC2004 database.

During experimentation δ is fixed at 5 and 10 and the former value was found to give better results than the latter value on SVC2004 while the opposite is true for SUSIG. Further investigation into this has revealed that signatures in SUSIG are on average 50% longer than those in SVC2004 in terms of the number of points in the signature sequence (300 points against 208 points). This suggests that higher values of δ should be used for longer signatures to obtain the best results. This in turn has led us to the concept of adaptive segmentation where, instead of using a fixed value of δ for all samples, a different δ is used for each sample. A certain fraction (min_fraction) of the total number of points in a sample is taken as the value of δ for that sample subject to a global minimum (global_min). Thus, the value of δ for a sample with n points is evaluated as follows

$$\text{min\_points} = \text{floor}(\text{min\_fraction} \times n) \tag{4a}$$

$$\delta = \max(\text{global\_min}, \ \text{min\_points}) \tag{4b}$$

Here floor(x) returns the largest integer not greater than x. This method constrains the total number of segments in a sample to be less than a specific value irrespective of the length of that sample and is quite effective at dealing with spurious extrema generated due to shaky hands or instrument noise. In addition, it also makes the task of finding segment-to-segment correspondence easier and more accurate since the number of segments obtained for different samples is likely to be roughly equal even if the samples are of widely differing sizes.

We have experimented with several values of min_fraction between 0.01 and 0.2 and global_min between 5 and 15 and optimal results were obtained using min_fraction = 0.03 for SVC2004 and min_fraction = 0.04 for SUSIG, with global_min = 5 for both databases. A comparison of the results obtained for various values of min_fraction is presented in Fig. 3.

3.3 Alignment of segments

Since any two signature samples may have different number of segments, a non-trivial method is needed to find the correspondence between the segments of the two samples. Through the process of alignment, segments of a sample are matched with those of another sample to obtain this correspondence. This matching may involve mapping in which a single segment of either sample matches with multiple segments of the other. To make it more clear, consider two samples, sample1 and sample2, then a single segment of sample1 may match with multiple segments of sample2 or a single segment of sample2 may match with multiple segments of sample1, as in Fig. 4.

For this purpose, a DTW-based method is used, as detailed in [32]. It employs a dynamic programming-based approach to obtain a many-to-many mapping between the segments of two samples so as to minimise the accumulated distance between the matched segments, as given by some distance function (e.g. Euclidean distance). Let us call this minimum accumulated distance between two samples (or segments) as the DTW distance between them.

The mapping produced by this method is subject to the following constraints:

1. There is always a mapping between the starting and the ending pairs of segments of the two samples.
2. The mapping is strictly non-decreasing in time from the perspective of either sample. This means that, while matching two samples, samples_1 and samples_2, if segment m of samples_1 (Seg_{1m}) has been matched to segment j of samples_2 (Seg_{2j}), then any other segment Seg_{1n}, where $n \geq m$, can match to a segment Seg_{2k} only if $k \geq j$.
3. Each segment of either sample must be a part of exactly one mapping which may be one-to-one, many-to-one or one-to-many. A particular segment cannot be a part of two different types of mappings at the same time. For instance, in the example of Fig. 4*a*, segments 3 and 4 of sample (iii) are paired with segment 4 of sample (i) and are thus involved in a many-to-one mapping. Now it would be invalid for either of these two segments to be a part of another mapping with segments of sample (i) (e.g. segment 3 of sample (iii) cannot have a one-to-one mapping with segment 3 of sample (i) even though such a mapping would not violate the other two constraints). This constraint also implies that each segment of either sample must match with at least one segment of the other sample.

Following are the main steps involved in the matching process:

1. First, a measure of distance needs to be defined between two segments, each belonging to one of the two samples being aligned, where each segment is represented by a sequence of data points. We have used the mean Euclidean distance between the x and y coordinates of the corresponding data points in the two segments as the measure. Two cases may arise here:

i. If the two segments have equal number of data points, then the distance between them is given by the following equation:

$$\text{dist}_{ij} = \frac{1}{n}\sum_{k=1}^{n}\sqrt{\left(x_{ik} - x_{jk}\right)^2 + \left(y_{ik} - y_{jk}\right)^2} \tag{5}$$

Here, dist_{ij} is the DTW distance between seg_i and seg_j, belonging, respectively, to samples_1 and samples_2 and each having n data points. The x, y coordinates of seg_i and seg_j are (x_{ik}, y_{ik}) and (x_{jk}, y_{jk}), respectively, for $k = 1, 2, \ldots, n$.
ii. If, on the other hand, they have different number of data points, we find the minimum-distance-matching between the two sets of data points by recursively applying the same DTW-based method of finding a correspondence between two sets of segments except that here we assume that each segment has only one data point. Thus, the DTW distance between two such single-point-segments is simply the Euclidean distance between the points. The overall DTW distance dist_{ij} between seg_i and seg_j is then the mean accumulated Euclidean distance between the matched points.

2. The distance obtained in Step 1 is used in a dynamic programming-based algorithm to find a path from the first pair to the last pair of segments with the minimum accumulated cost. This is the optimal DTW path and the accumulated cost divided by the number of steps in this path is the corresponding DTW distance between the two samples. More details of this algorithm can be found in [32].

doi: 10.1049/iet-bmt.2012.0048

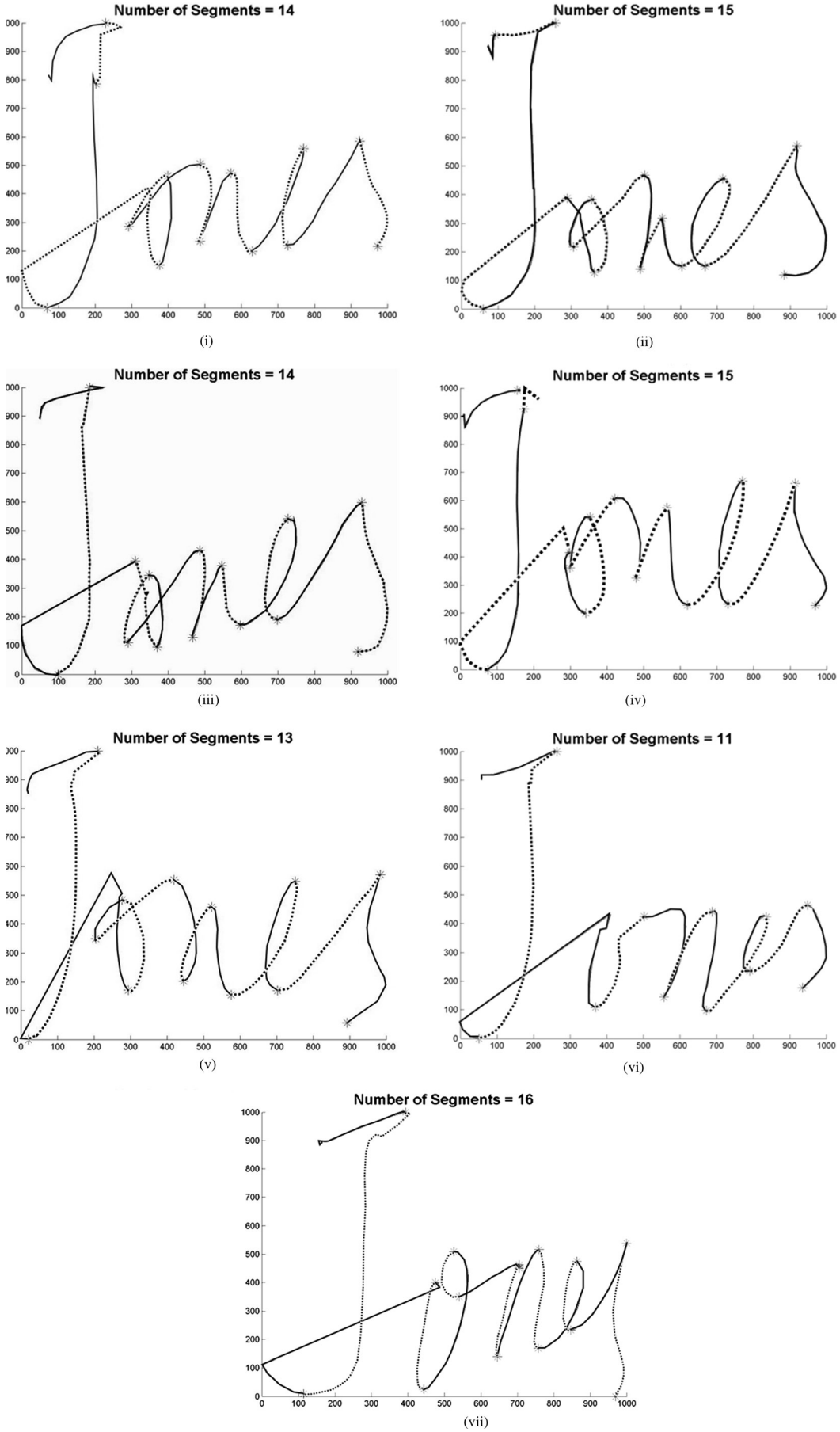

Fig. 2 *Sample signatures of a user from SVC2004 database segmented along points of vertical extrema (min_fraction = 0.03 global_min = 5)*

The segmentation points are marked by an asterisk and consecutive segments are shown by solid and dotted lines
The unmarked end is the starting point of the signature
(i) Prototype sample; (ii) and (iii) training genuine samples; (iv) and (v) test genuine samples; (vi) and (vii) skilled forgery samples

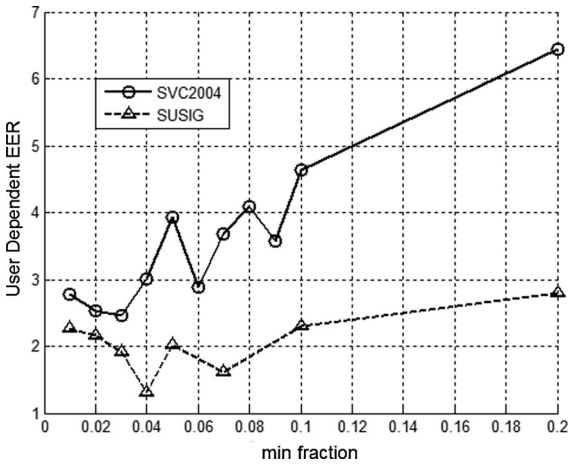

Fig. 3 *Results obtained in terms of user-dependent EER for different values of min_fraction using both SVC2004 and SUSIG databases*

$N = 5$ and global_min = 5 were used for all runs

3. The method outlined in the previous two steps is applied pair wise to all the training samples of the same user, thus obtaining the distance of each training sample from each of the other training samples. Hence if there are n training samples, there will be a total of $((n(n-1))/2)$ pairings. The training sample with the least mean distance from all others is then chosen as the prototype (or reference) genuine sample for that user.
4. Finally, Steps 1 and 2 are applied to find the segment correspondence between the prototype sample and each of the test samples, both genuine and forged.

Since the DTW matching process produces a many-to-many mapping between the segments of the two samples, a method of resolution is needed for cases where one segment of the prototype sample gets paired with multiple segments of the other sample. The properties of the multiple matching segments need to be combined so that they can be compared to the corresponding property of the single prototype segment. Three alternative methods are tried to carry out this combination

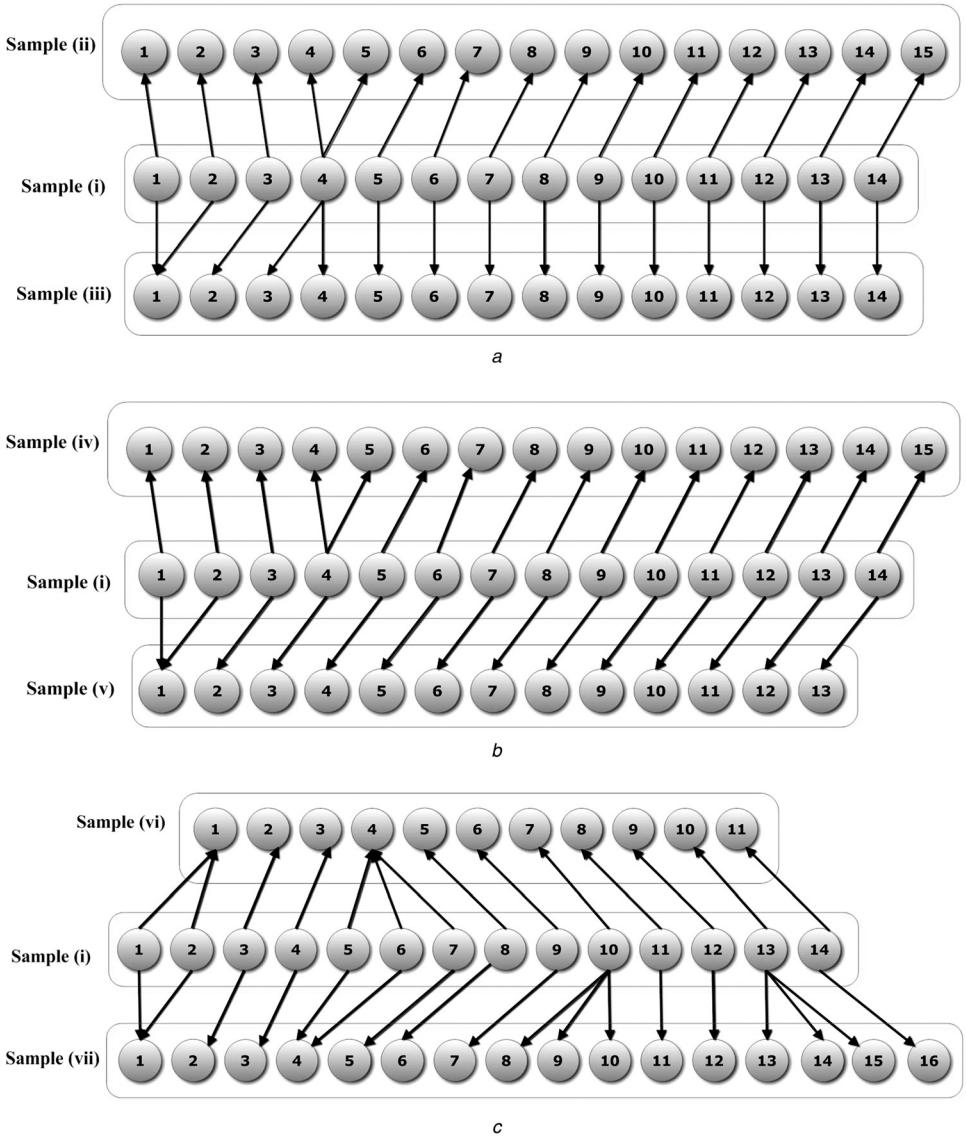

Fig. 4 *Pairings obtained by the DTW method between the prototype sample and a few other samples*

a Pairings of sample (i) with samples (ii) and (iii) of Fig. 2
b Pairings of sample (i) with samples (iv) and (v) of Fig. 2
c Pairings of sample (i) with samples (vi) and (vii) of Fig. 2

doi: 10.1049/iet-bmt.2012.0048

1. Extract the features of each matching segment as detailed in Section 3.4 and take the mean over all the segments to obtain a single value for each feature which is then used for further processing. This is the case of feature-level combination.
2. Extract features and carry out the first two steps of fuzzy modelling (Section 3.5) to obtain the degree of match (DOM) for each of the segments independently and then take the mean of these DOMs as the single DOM representing these segments. This is the case of DOM level combination.
3. As a consequence of the second constraint in the matching process specified earlier, if multiple segments of one sample match with a single segment of the other sample, they will necessarily be consecutive segments. Thus, another way to combine them is to consider all the data points from the first point of the first segment to the last point of the last segment as belonging to a single segment and then extract features from this composite segment. This is the case of combination at the level of data points.

Experiments are carried out using each of these methods and the second one is found to give the best results probably because of least incidence of the averaging effect mentioned in Section 3.2. Thus, only the results of DOM level combination are mentioned in Section 4.

To clarify the segment alignment process, the segment pairs that were obtained between the prototype sample and the other samples shown in Fig. 2 are given in Fig. 4.

3.4 Feature extraction

Two types of features, viz., shape and dynamic features are extracted from each segment at this stage. Shape features are useful for detecting random forgery but may fail for skilled forgeries because of the relative ease of copying the overall shape of a signature. Dynamic features, on the other hand, have much better discriminative power because they are much harder to imitate [33].

Several features are experimented and out of which only those having valid values for any segment are used in this work. Although the main inspiration for this work is [5], but many of its features cannot be used here because of either divide-by-zero problems or their irrelevance at the level of individual segments. For example, features like height-to-width ratio and length-to-width ratio used in [5] cannot be used here because of the possibility of the width becoming zero for some segments, a problem that does not occur when these features are extracted for the whole signature. Moreover, some complex features like RMS centripetal acceleration, RMS tangential acceleration and RMS acceleration [5] could not be used here since they are expensive to compute, leading to unacceptable performance when this computation has to be repeated for each segment. Thus, only a few relatively simple features are used in this work. These are listed in Table 1.

Table 1 Features used in the proposed system

Shape features	Dynamic features
mean of *x* coordinate	total signature time
mean of *y* coordinate	mean velocity in *x* direction
height	mean velocity in *y* direction
width	mean acceleration in *x* direction
length	mean acceleration in *y* direction
	mean of pressure
	mean of azimuth angle
	mean of altitude angle

3.5 Fuzzy modelling

Fuzzy modelling of each feature of each segment of the prototype sample signature, which forms a fuzzy set as explained below, is used in the verification of an unknown signature. This decision is made on the basis of the fuzzy membership values of the features extracted from this signature using the fuzzy sets that are learned during the training stage. In fact, these fuzzy sets constitute the fuzzy rules framed. The concept of a fuzzy set arising from a set of features is explained as follows. A fuzzy set is formed from each feature of each segment of the prototype sample gathered over all the training samples. Suppose there are m training samples and the prototype sample has n segments with i features extracted from each of these. Then there would be a total of $n \times i$ fuzzy sets with each one having m values since each training sample would contribute one value to each fuzzy set. The variation in the feature values over the training sample space gives rise to fuzziness.

Whenever multiple segments of a sample match with a single segment of the prototype sample during the DTW alignment process, their features will be combined and will either be compared with (a test sample) or contribute to (a training sample) the single fuzzy set corresponding to that segment of the prototype sample. For instance, in the example of Fig. 4*a*, segments 3 and 4 of training sample (iii) would contribute only to the fuzzy set corresponding to segment 4 of prototype sample (i). Along the same lines, when the test sample (iv) of Fig. 4*b* is passed through this system, the properties of its segments 4 and 5 would be combined and compared to the values in the fuzzy set corresponding to segment 4 of the prototype sample (i). Conversely, it is also possible for one segment to contribute to multiple fuzzy sets, as demonstrated by segment 1 of sample (iii) that contributes to the fuzzy sets corresponding to both segments 1 and 2 of sample (i).

This work uses the rule-based Mamdani approach to fuzzy modelling, which is adapted from [5]. This approach involves the following steps for each segment:

1. Calculate the normalised difference for each feature from its reference set by

$$\mathrm{Dist}_i = \frac{f_i - \mu_i}{\sqrt{1 + \sigma_i^2}} \tag{6}$$

Here, f_i is the value of the ith feature, μ_i and σ_i are the mean and standard deviation of this feature over the training samples.
2. Compute the DOM. This is a measure of the degree of similarity of the test signature's specific feature value for a particular segment against the reference, expressed as a percentage. This is the output of single-input, single-output and single rule TS model whose input is Dist_i from Step 1 and output is the corresponding DOM, as shown in Fig. 5. This model uses two parameters $\mathrm{Dist}_{\min}$ and $\mathrm{Dist}_{\max}$ such that $\mathrm{DOM}_i = 100$ for $\mathrm{Dist}_i \leq \mathrm{Dist}_{\min}$ and $\mathrm{DOM}_i = 0$ for $\mathrm{Dist}_i \geq \mathrm{Dist}_{\max}$. After experimenting with several combinations of these parameters, the values of 1 and 7 for $\mathrm{Dist}_{\min}$ and $\mathrm{Dist}_{\max}$, respectively, are found to give optimal results.

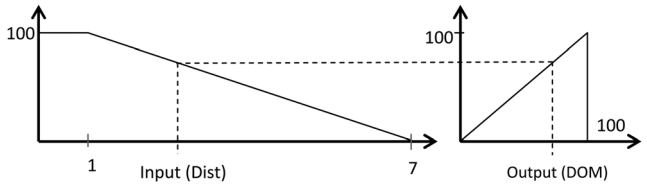

Fig. 5 *Single-input, single-output, single-rule TS fuzzy system*

The above two steps are repeated to obtain the DOM for each feature.

3. Compute the total degree of match (TDOM) for each of the two feature sets: static/shape-based features and dynamic features. For each set, a weighted mean of all the features in the set is called the TDOM for that set. The weighting factors reflect the relative importance of features and are taken to be inversely proportional to the respective standard deviations. This is based on the reasoning that lesser the standard deviation of a feature over the training set, more is its relative importance in discriminating the user's genuine signatures from the forged ones. Thus, a feature's relative importance (RIM) may be expressed as

$$\mathrm{RIM}_i = \frac{1}{\sqrt{1+\sigma_i^2}} \tag{7}$$

The variances between RIMs of different features are very large, making them unsuitable for direct use as weighting factors. A sigmoid function is therefore used to normalise the RIM into the range from 0 to 1. This provides us a measure of the feature's normalised relative importance (NRIM) given by

$$\mathrm{NRIM}_i = \frac{1}{1+\exp\left(-\mathrm{RIM}_i\right)} \tag{8}$$

The weight of the ith feature is then obtained as

$$W_i = \frac{\mathrm{NRIM}_i}{\sum_{j=1}^{n} \mathrm{NRIM}j} \tag{9}$$

These weights are used to obtain two values of TDOM, one each for the shape and dynamic features. These TDOMs are computed as

$$\mathrm{TDOM} = \sum_{i=1}^{n} \left(W_i \times \mathrm{DOM}_i\right) \tag{10}$$

The summations in (9) and (10) are done over all the n features in the respective feature set.

4. Find the degree of authentication (DOA) for each segment expressed as a percentage: The overall DOA of each segment is obtained as the output of a two-input, single-output and multiple-rules Mamdani fuzzy system for which the TDOMs of shape and dynamics are the two inputs. This gives an overall measure of authenticity for each segment of the test signature.

The two input linguistic variables used are 'TDOM of shape' and 'TDOM of dynamics' whereas the output linguistic fuzzy variable is 'DOA of segment'. The number of linguistic terms partitioning the input and output spaces is set to 11 each so that there is one term whose triangular membership function is centred at each of the multiples of ten from 0 to 100 (both inclusive). For the sake of convenience, these linguistic terms are assigned integers (called linguistic IDs or LIDs) from 1 to 11 rather than names. It should be noted from Fig. 6 that higher numbers denote lower degrees of match. The associated functions are identical for each of the two inputs as well as the output, as shown in Fig. 6. The rule base used in this work is given in Table 2.

To further elucidate the meaning of the membership functions and the rule base, the rules that are fired for the example of Fig. 7, with TDOM values of 92 and 87%, respectively, for dynamic and shape feature sets, are given in the conventional If–Then rule form as follows:

i. *If* Shape TDOM has LID 1 *and* Dynamic TDOM has LID 2 *Then* segment DOA has LID 2
ii. *If* Shape TDOM has LID 1 *and* Dynamic TDOM has LID 3 *Then* segment DOA has LID 3
iii. *If* Shape TDOM has LID 2 *and* Dynamic TDOM has LID 2 *Then* segment DOA has LID 3

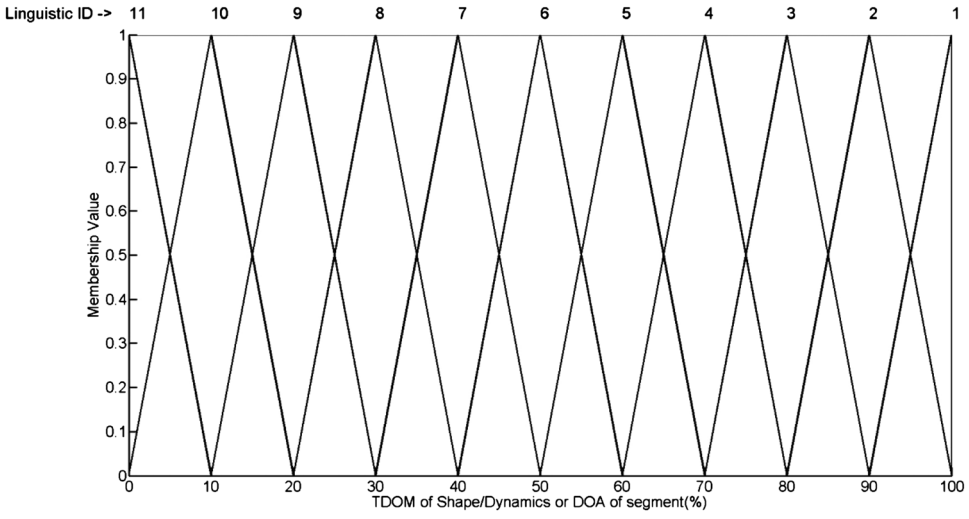

Fig. 6 *Triangular membership functions for the inputs as well as the output*

doi: 10.1049/iet-bmt.2012.0048

Table 2 Rule base for fuzzy inference

	S. No.	TDOM of dynamics										
		1	2	3	4	5	6	7	8	9	10	11
TDOM of shape	1	1	2	3	4	5	6	7	8	9	10	11
	2	2	3	4	5	6	7	8	9	10	11	11
	3	3	4	5	6	7	8	9	10	11	11	11
	4	4	5	6	7	8	9	10	11	11	11	11
	5	5	6	7	8	9	10	11	11	11	11	11
	6	6	7	8	9	10	11	11	11	11	11	11
	7	7	8	9	10	11	11	11	11	11	11	11
	8	8	9	10	11	11	11	11	11	11	11	11
	9	9	10	11	11	11	11	11	11	11	11	11
	10	10	11	11	11	11	11	11	11	11	11	11
	11	11	11	11	11	11	11	11	11	11	11	11

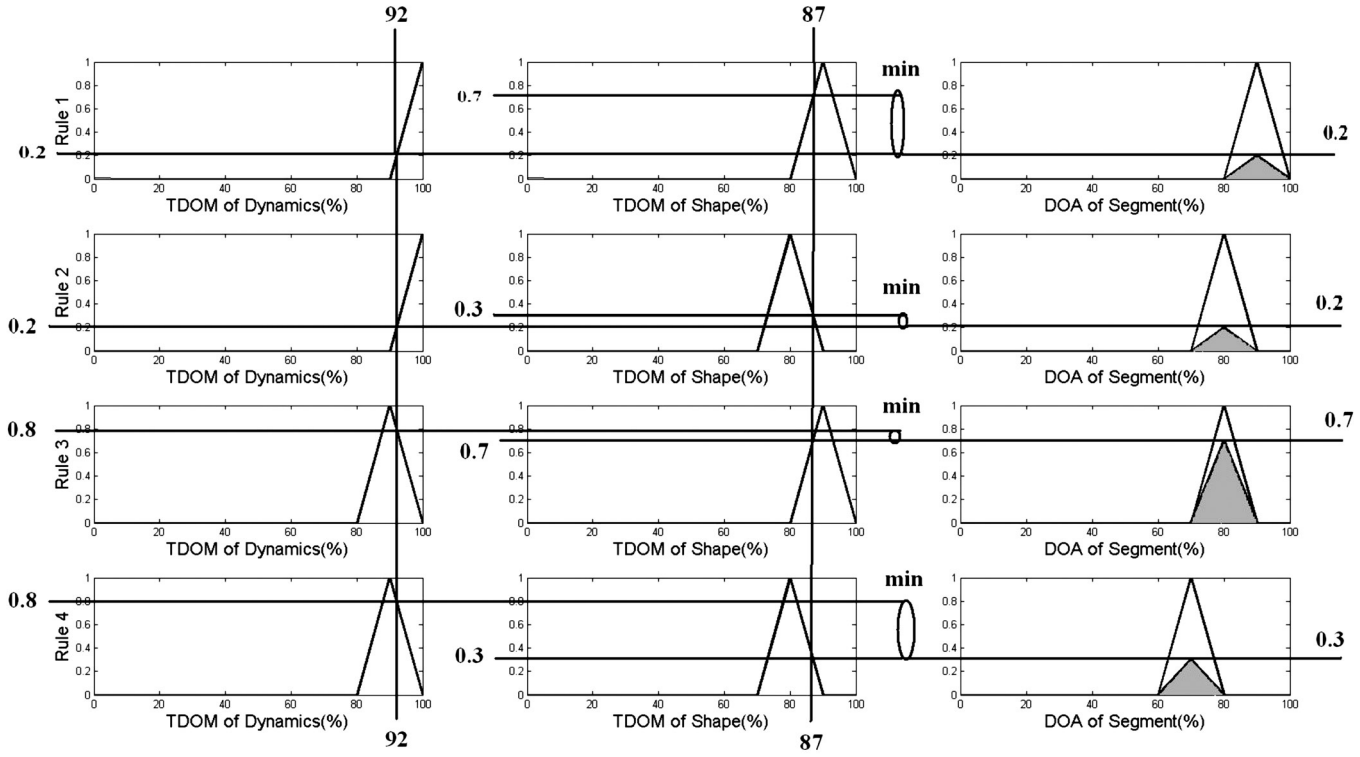

Fig. 7 *Graphical representation of Larson's method*

iv. *If* Shape TDOM has LID 2 *and* Dynamic TDOM has LID 3 *Then* segment DOA has LID 4

Larson's method is used to combine the rule base and the membership functions to obtain a single crisp value for each segment. A graphical representation of Larson's method is shown in Fig. 7, where singleton fuzzification and mean of maximum (MOM) defuzzification methods are employed. The defuzzified percentage DOA of the segment is given by (refer to Fig. 7)

$$\text{DOA(segment\%)} = \frac{0.2 \times 90 + 0.2 \times 80 + 0.7 \times 80 + 0.3 \times 70}{0.2 + 0.2 + 0.7 + 0.3} = 79.28\%$$

5. *Classify the test signature based on its TDOA*: The total degree of authentication (TDOA) of a signature sample is defined as the arithmetic mean of the DOAs of all of its segments. This value is compared with a user-dependent threshold to classify the sample as either genuine or forged. The expression for calculating the TDOA of a sample having k segments is

$$\text{TDOA} = \frac{1}{k}\sum_{i=1}^{k} \text{DOA}_i \tag{11}$$

4 Performance evaluation

For verifying a test signature, it must be given as the input to the fuzzy model, learned during the training stage to obtain a single similarity score (TDOA). This is then compared with a threshold, selected during the training stage, to classify the signature as genuine or forged. For identifying an unknown signature, it must be passed through the models of all users

in the database and the user whose model gives the maximum TDOA relative to his/her genuine training samples subject to the condition that it is above the threshold specific to the same user is identified with the unknown signature. If a signature sample fails to cross the threshold for any of the users in the database, it is classified as unknown.

Automatic signature verification can produce two types of errors: Type I error, which is concerned with the false rejections of genuine signatures called the false rejection rate (FRR); and Type II error, which is concerned with the false acceptance of forged signatures called the false acceptance rate (FAR). Typically, FAR decreases while FRR increases as the threshold is increased. The equal error rate (EER), which is another measure of the overall accuracy of a system, arises when FRR is made equal to the FAR by adjusting the threshold [34]. The forgeries used in the verification process are categorised as random and skilled. In the case of a random forgery, the forger has either no knowledge of the original signature or does not try to imitate it. A skilled forgery, on the other hand, is attempted by a professional imposter who traces over or imitates the signature as best as he can. Skilled forgeries already exist in the two databases whereas random signatures of other users serve as random forgeries.

4.1 Databases

Two publicly available databases used in this work are described now.

4.1.1 SVC2004: This database [35] has two sets of signatures, namely, Task 1 and Task 2; out of which only Task 2 signatures have been used in this work. This set contains signatures of 40 users with 40 samples for each user. Out of 40 samples, 20 are genuine and the rest are skilled forgeries. Each signature in Task 2 is represented as a sequence of points, containing x coordinate, y coordinate, time stamp and pen status (pen-up or pen-down), azimuth, altitude and pressure. Some sample signatures from this database are shown in Fig. 8.

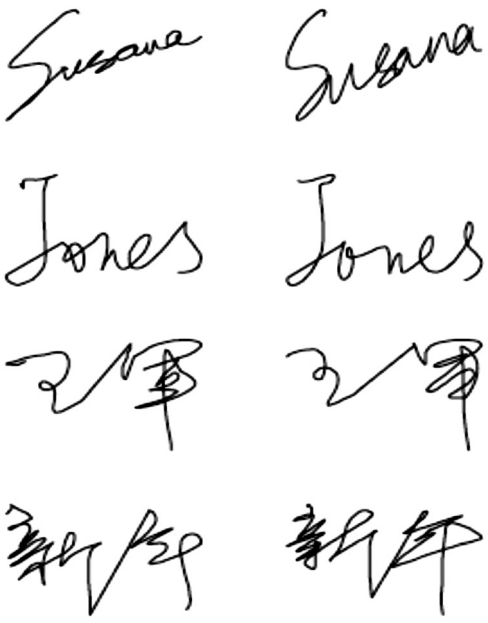

Fig. 8 *Sample signatures from SVC2004*

4.1.2 SUSIG: This database [36] has two sets, viz., blind and visual sub corpus. We have used the second set. This set contains signature data of 100 users; but we have used the data of only 94 users with each having 20 genuine and 10 skilled forgery signatures because the remaining six users have one or more signatures missing. The representation of signature data is similar to that of SVC2004 except that the data on azimuth, altitude and pen status is not available in SUSIG. A few sample signatures from this database are shown in Fig. 9.

4.2 Experiments and results

4.2.1 Performance evaluation methodology: Two sets of experiments are conducted to evaluate the system performance, with the first one using only skilled forgeries while the second one including random forgeries in addition to skilled forgeries. Each set of experiments takes the training samples of 5 and 10, with the remaining genuine samples being used for testing along with the forgeries. To increase the reliability of the results, cross validation is done with five trials on each user. A different set of genuine samples, selected randomly, comprises the training set in each of these trials. The random forgeries in the second set of experiments are obtained by randomly selecting 10 samples belonging to other users in the database. Note that the experiments are conducted on each database separately.

The overall system performance is evaluated using two measures: accuracy and EER. Here, accuracy is defined as the percentage of forgery samples whose TDOA is less than the TDOA of the genuine sample with the minimum TDOA. It is calculated independently for each user and then averaged over all users in the database to obtain the system accuracy. EER is obtained at the point where the FAR equals the FRR, where FAR is the percent of forgery samples whose TDOA $\geq$ threshold, whereas FRR is the percent of genuine samples whose TDOA $<$ threshold. Two different methods are used in this work to evaluate EER.

User-dependent threshold: As stated in Section 1, this work emphasises the user-dependent thresholds at the verification stage. In this approach, the values of FAR and FRR are obtained for each user for a range of thresholds and these are used to draw plots of FAR against threshold and FRR against threshold. The point of intersection of these two plots gives EER for that user. In the case of cross validation with multiple trials, EER is evaluated independently for each trial and mean is taken over all trials for a user to obtain EER for that user. Finally, the overall EER of the system for a particular database is computed as the mean of EERs of all the users in the database. A few

Fig. 9 *Sample signatures from SUSIG*

doi: 10.1049/iet-bmt.2012.0048

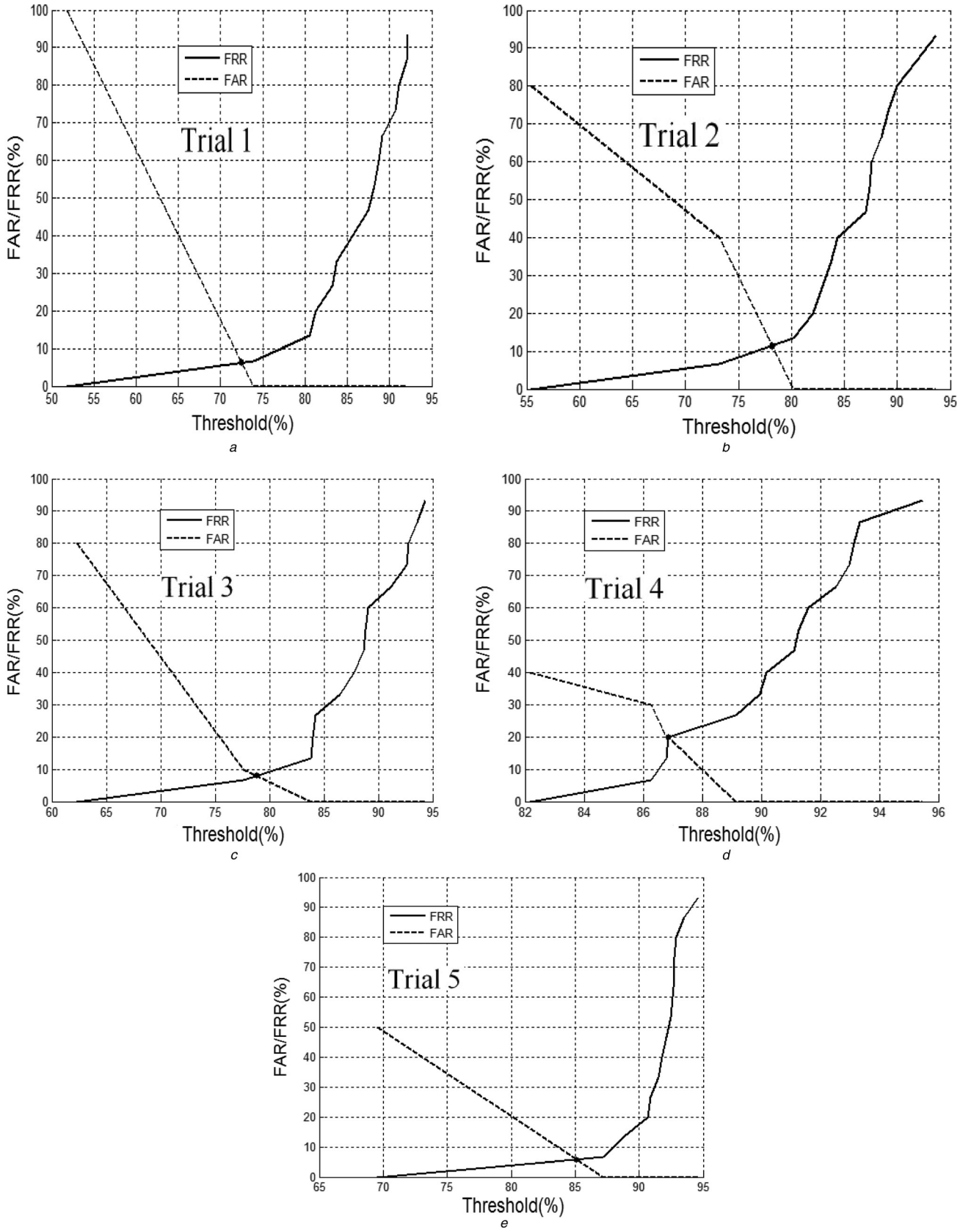

Fig. 10 *User-dependent threshold-based FAR/FRR curves for the same user from SUSIG database*
a) Trial 1 b) Trial 2 c) Trial 3 d) Trial 4 e) Trial 5

sample FAR/FRR curves for the same user are shown in Fig. 10.

Global threshold: Even though this system relies on user-dependent threshold, results are obtained using both global threshold and user-dependent threshold for the sake of comparison. TDOAs obtained for all the users in the database are combined and subjected to a single threshold, varying from 0 to 100, to obtain FAR and FRR values for

each threshold. These values are used to obtain a plot of FAR against FRR and its intersection with the line $x = y$ gives the global EER. The curves due to the proposed method and the method of [5] are shown in Fig. 11.

As expected, EER obtained with the global approach proved to be significantly higher than the mean EER obtained using user-dependent thresholds for both databases (Tables 3 and 4).

4.2.2 Comparison with signature-level fuzzy modelling: To evaluate the effectiveness of segment-level fuzzy modelling over signature-level fuzzy modelling, we have also implemented the method in [5] and conducted the above experiments on this system too. Since no details about preprocessing are mentioned in [5], experiments using this method are conducted on the original data. Although the results of SVC2004 are as expected, with our system outperforming that of [5] by a large margin (Table 3), the results of SUSIG are very similar on both methods (Table 4), with [5] having a slight advantage.

Table 3 Results of the first set of experiments (only skilled forgeries) on SVC2004 database where N = no. of training samples

SVC2004 (only skilled forgeries)		Accuracy, %	EER, %	
			User-dependent threshold	Global threshold
$N = 5$	proposed method	93.525	2.458	7.571
	method of [5]	55.050	14.930	19.088
$N = 10$	proposed method	96.175	1.781	5.250
	method of [5]	65.975	11.538	15.277

It may be noted that genuine signatures in SVC2004 are not real signatures, unlike those in SUSIG, because people who provided signatures have made up signatures for the sake of contribution leading to more variation within genuine

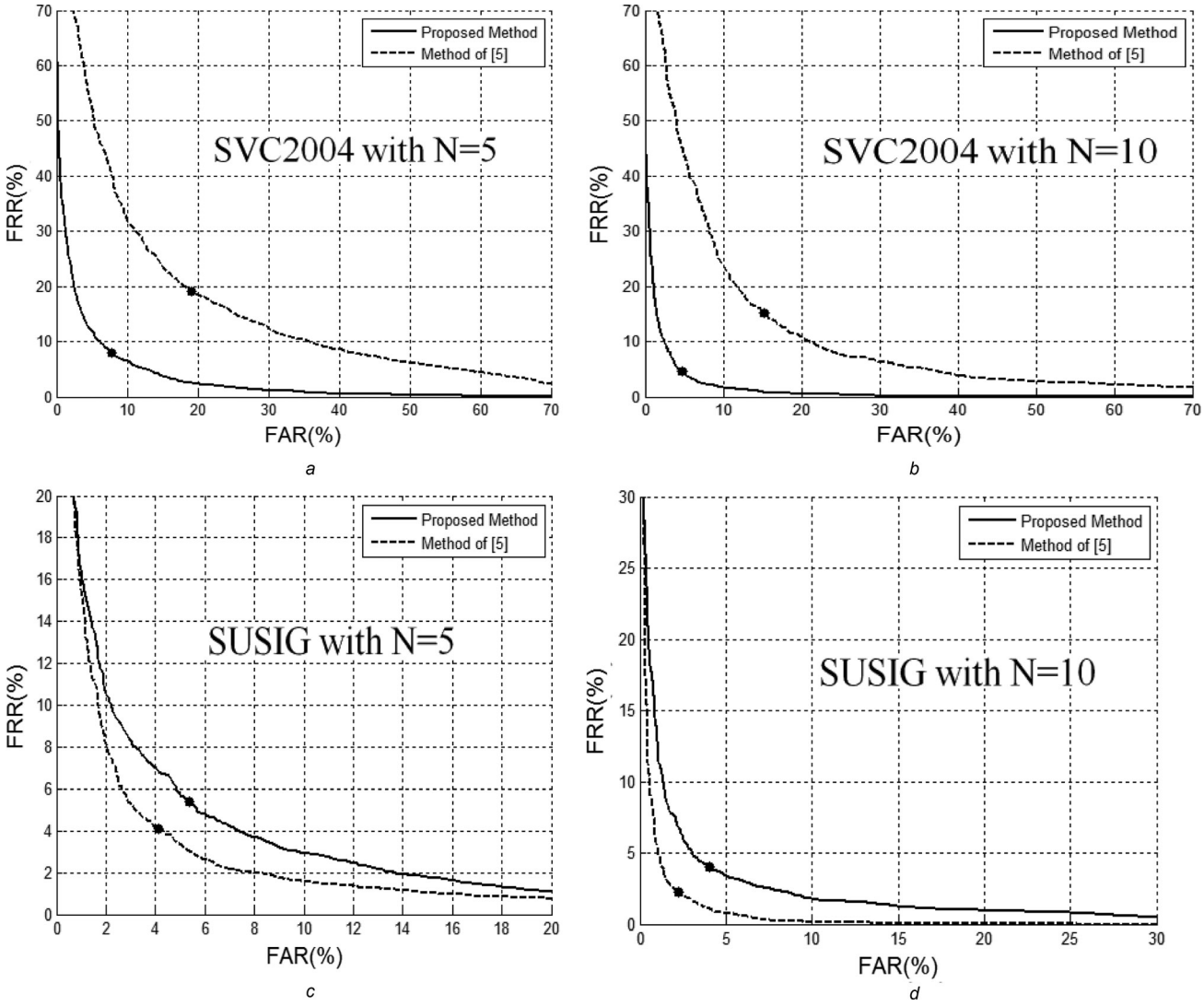

Fig. 11 *Error tradeoff curves with global threshold using only skilled forgeries (Set 1)*

The curves corresponding to the proposed method are shown with solid lines whereas those of [5] are shown with dotted lines
The point of EER is marked with a black dot on each curve
a SVC2004 with 5 training samples
b SVC2004 with 10 training samples
c SUSIG with 5 training samples
d SUSIG with 10 training samples

doi: 10.1049/iet-bmt.2012.0048

Table 4 Results of the first set of experiments (only skilled forgeries) on SUSIG database where N = no. of training samples

SUSIG (only skilled forgeries)		Accuracy, %	EER, %	
			User-dependent threshold	Global threshold
$N = 5$	proposed method	94.660	1.303	5.386
	method of [5]	95.340	1.319	4.116
$N = 10$	proposed method	96.064	1.037	4.021
	method of [5]	98.638	0.684	2.234

samples than would be possible in the real signature, thus making the task of separating the genuine and forged signatures more difficult. To verify this, we have calculated the mean difference between the TDOA of genuine samples and that of skilled forgery samples using our method and that in [5] on both databases and found this difference to be significantly larger for SUSIG indicating a greater ease of separation than in SVC2004 (Table 5).

To the best of our knowledge, the approach in [11] is the only other existing method in the literature, apart from ours, that has been tested on both SVC and SUSIG databases. The results obtained there too are consistent with our observation since the EER obtained on SVC database (7.02) is nearly three times the EER on SUSIG (2.46). Owing to this difference, SVC2004 database benefits greatly from the additional fine information captured by segmentation level modelling, while the benefits are minimal for SUSIG where signatures differ enough for even signature-level modelling to be able to separate them with ease. In fact, the additional information provided by segmentation even appears to have a slight negative impact on the results. Thus, we conclude that our method is more suitable for situations where the forgery has been executed with great skill.

Since random forgeries are easier to detect than skilled ones, we expected the results to improve when 10 random forgeries were added to the testing set. The results of the proposed method indeed show a marginal improvement for both SVC2004 and SUSIG databases. The results of [5], however, show an increasing trend in results only on SVC2004 (Table 6) but exhibits a significant decline in results on SUSIG (Table 7). This could be due to the fact that the features extracted from a genuine signature match with those extracted from a completely different signature (i.e. random forgery). This unexpected behaviour is observed more with the signature-level feature extraction method of [5] than with the proposed segment-level feature extraction method. Thus, the method of [5] is more likely to confuse with a genuine signature as a random signature than the proposed method.

4.2.3 Comparison with other methods: In order to compare the performance of our method with other contemporary methods, we have considered EER based on the user-dependent threshold to represent our system's accuracy. All results are the outcome of using five training samples with no random forgeries.

A comparison of the results is given in Table 8 and Table 9 for SVC2004 and SUSIG databases, respectively. Results of the proposed method have been obtained using min_fraction = 0.03 for SVC2004 and min_fraction = 0.04 for SUSIG, with global_min = 5 for both the databases.

Table 5 Mean difference between the TDOAs of genuine and skilled forgery samples using five training samples

	SUSIG	SVC2004
proposed method	34.171	25.457
method of [5]	45.561	15.432

Table 6 Results of the second set of experiments (both skilled and random forgeries) on SVC2004 database where N = no. of training samples

SVC2004 (skilled and random forgeries)		Accuracy, %	EER, %	
			User-dependent threshold	Global threshold
$N = 5$	proposed method	95.783	1.653	5.493
	method of [5]	64.783	13.468	16.754
$N = 10$	proposed method	98.300	0.906	3.466
	method of [5]	73.550	10.701	13.615

Table 7 Results of the second set of experiments (both skilled and random forgeries) on SUSIG database where N = no. of training samples

SUSIG (skilled and random forgeries)		Accuracy, %	EER, %	
			User-dependent threshold	Global threshold
$N = 5$	proposed method	95.904	1.234	4.567
	method of [5]	92.585	3.731	6.304
$N = 10$	proposed method	97.447	0.911	3.394
	method of [5]	95.574	2.712	4.733

Table 8 Comparison with other methods using SVC2004 database

Authors	Year	Method	EER, %
Ong *et al.* [37]	2009	statistical quantisation mechanism (SQM), user-dependent threshold	5.32
Fierrez-Aguilar *et al.* [38]	2005	fusion of local (DTW) and regional (HMM) approach, user-dependent threshold	6.91
SVC 2004 [35]	2004	team 219b	6.90
Mohammadi *et al.* [39]	2012	extended regression and DTW, user-dependent threshold	6.33
Wang *et al.* [11]	2011	segmentation and graph matching, user-dependent threshold	7.02
Fallaha *et al.* [24]	2011	Mellin transform and MFCC, neural network	3.00
proposed method	2013	segment-level fuzzy modelling, user-dependent threshold	2.46

Table 9 Comparison with other methods using SUSIG database

Method	Year	Method	EER, %
Khalil *et al.* [40]	2009	multiple feature set and DTW, user dependent threshold	3.06
Khomatov *et al.* [36]	2009	Fourier descriptor and DTW	2.10
Ibrahim *et al.* [41]	2009	Fisher linear discriminant (FLD) analysis, user-dependent threshold	1.57
Wang *et al.* [11]	2011	segmentation and graph matching, user-dependent threshold	2.46
proposed method	2013	segment-level fuzzy modelling, user-dependent threshold	1.30

5 Conclusions

A novel online signature verification method is developed using segment-level fuzzy modelling of features. The fuzzy modelling requires a simple rule-base and a few simple features. The matching of the features of a test signature with the training features is done using a similarity score called the TDOA which is based on the TDOM of individual segments. The results obtained by our method are either comparable to or better than the existing methods even though some of them are complex and computationally intensive. This is an indication of the potential underlying the concept of the localised fuzzy modelling. The use of segment-specific features coupled with a sophisticated rule base with some additional computation may improve the results.

6 Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions, which have helped a lot in improving this paper.

7 References

1 Jain, A.K., Ross, A., Parbhakar, S.: 'An introduction to biometric recognition', *IEEE Trans. Circuits Syst. Video Technol. Special Issue on Image- and Video-Based Biometrics*, 2004, **14**, (1), pp. 4–20
2 Fairhurst, M.C.: 'Signature verification revisited: promoting practical exploitation of biometric technology', *Inst. Electr. Eng. Electron. Commun. Eng. J. (ECEJ)*, 1997, **9**, (6), pp. 273–280
3 Fairhurst, M.C., Kaplani, E.: 'Perceptual analysis of handwritten signatures for biometric authentication', *Inst. Electr. Eng. Proc. Vis. Image Signal Process.*, 2003, **150**, (6), pp. 389–394
4 Khalmatov, A., Yanikoglu, B.: 'Identity authentication using improved on-line signature verification method', *Patt. Recogn. Lett.*, 2005, **26**, (15), pp. 2400–2408
5 Wijesoma, W.S., Mingming, M., Yue, K.W.: 'On-line signature verification using a computational intelligence approach', in: Reusch, B. (Ed.): 'Fuzzy days' (Springer, Berlin, Germany, 2001), vol. 2206, pp. 699–711
6 Zhang, Z., Wang, K., Wang, Y.: 'A survey of on-line signature verification'. CCBR 2011, 2011 (*LNCS*, **7098**), pp. 141–149
7 Schmidt, C., Kraiss, K.F.: 'Establishment of personalized templates for automatic signature verification'. Proc. Fourth Int. Conf. Document Analysis Recognition (ICDAR-4), IEEE Computer Society, Ulm, Germany, August 1997, vol. 1, pp. 263–267
8 Brault, J.J., Plamondon, R.: 'Segmenting handwritten signatures at their perceptually important points', *IEEE Trans. Patt. Anal. Mach. Intell.*, 1993, **15**, (9), pp. 953–957
9 Shafiei, M.M., Rabiee, H.R.: 'A new on-line signature verification algorithm using variable length segmentation and Hidden Markov models'. Seventh Int. Conf. Document Analysis and Recognition (ICDAR-7), IEEE Computer Society, Edinburgh, UK, August 2003, vol. 1, pp. 443–446
10 Lee, J., Yoon, H.S., Soh, J., Chun, B.T., Chung, Y.K.: 'Using geometric extrema for segment-to-segment characteristics comparison in online signature verification', *Patt. Recogn.*, 2004, **37**, (1), pp. 93–103
11 Wang, K., Wang, Y., Zhang, Z.: 'On-line signature verification using segment-to-segment graph matching'. Int. Conf. Document Analysis and Recognition (ICDAR), 2011, School of Computer Science & Engineering, Beihang University, Beijing, China, 18–21 September 2011, pp. 804–808
12 Yue, K.W., Wijesoma, W.S.: 'Improved segmentation and segment association for on-line signature verification'. IEEE Int. Conf. System Man Cybernetics, 2000, vol. 4, pp. 2752–2756
13 Zhang, J., Kamata, S.: 'Online signature verification using segment-to-segment matching'. Int. Conf. Frontiers in Handwriting Recognition ICFHR (2008), Montréal, Québec, 19–21 August 2008
14 Lee, W.S., Mohankrishnan, N., Paulik, M.J.: 'Improved segmentation through dynamic time warping for signature verification using a neural network classifier'. Proc. IEEE Int. Conf. Image Processing (ICIP), Chicago, IL, October 1998, vol. 2, pp. 929–933
15 Rhee, T.H., Cho, S.J., Kim, J.H.: 'On-line signature verification using model-guided segmentation and discriminative feature selection for skilled forgeries'. Proc. Sixth Int. Conf. Document Analysis and Recognition (ICDAR-6), Seattle, WA, September 2001, pp. 645–649
16 Martens, R., Claesen, L.: 'On-line signature verification by dynamic time-warping'. Proc. 13th Int. Conf. Pattern Recognition (ICPR96), Vienna, Austria, 1996, pp. 38–42
17 Lei, H., Govindaraju, V.: 'A comparative study on the consistency of features in on-line signature verification', *Patt. Recogn. Lett.*, 2005, **26**, pp. 2483–2489
18 Aguilar, J.F., Nanni, L., Penalba, J.L., Garcia, J.O., Maltoni, D.: 'An online signature verification system based on fusion of local and global information'. IAPR Int. Conf. Audio – and Video-Based Biometric Person Authentication, AVBPA, 2005a (*LNCS*, **3546**), pp. 523–532
19 Kour, J., Hammandlu, M., Ansari, A.Q.: 'Online signature verification using GA-SVM'. Proc. Int. Conf. Image Information Processing, ICIIP, 3–5 November 2011, pp. 1–4
20 Xuhua, Y., Furuhashi, T., Obata, K., Uchikawa, Y.: 'Selection of features for signature verification using the genetic algorithm', *J. Comput. Ind. Eng. Archive*, 1996, **30**, (4), pp. 1037–1045
21 Khan, M.A.U., Khan, M.K., Khan, M.A.: 'Velocity-image model for online signature verification', *IEEE Trans. Image Process.*, 2006, **15**, (11), pp. 3540–3549
22 Yanikoglu, B., Khalmatov, A.: 'Online signature verification using Fourier descriptors', *Hindawi Publ. Corp., EURASIP J. Adv. Signal Process.*, 2009, article id 260516. DOI: 10.1155/2009/260516
23 Al-Mayyan, W., Own, H.S., Zedan, H.: 'Rough set approach to online signature identification', *Digit. Signal Process.*, 2011, **21**, (3), pp. 477–485
24 Fallaha, A., Jamaatib, M., Soleamanic, A.: 'A new online signature verification system based on combining Mellin transform, MFCC and neural network', *Digit. Signal Process.*, 2011, **21**, pp. 404–416
25 Mirzaei, O., Irani, H., Pourreza, H.R.: 'Offline signature recognition using modular neural networks with fuzzy response integration'. Int. Conf. Network and Electronics Engineering, 2011, (IPCSIT), vol. 11
26 Velez, J., Sanchez, A., Moreno, A.B., Esteban, J.L.: 'A hybrid approach using snakes and fuzzy modelling for offline signature verification'. Proc. Eleventh Int. Conf. Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU 2006), 2006, Editions EDK, vol. I, pp. 882–889
27 Madasu, V.K., Lovell Brian, C., Kubik, K.: 'Automatic handwritten signature verification system for Australian passports'. Science, Engineering and Technology Summit on Counter-Terrorism Technology, Canberra, 2005, pp. 53–66
28 Hanmandlu, M., Mohammed, M.H., Madasu, V.K.: 'Off-line signature verification and forgery detection using fuzzy modeling', *Patt. Recogn.*, 2005, **38**, (3), pp. 341–356
29 Zakaria, R., Waheb, A.F., Ali, J.M.: 'Confidence fuzzy interval in verification of offline handwriting signature', *Eur. J. Sci. Res. ISSN 1450-216X*, 2010, **47**, (3), pp. 455–463
30 Khalid, M., Yusof, R., Mokayed, H.: 'Fusion of multi classifiers for online signature verification using fuzzy logic inference', *Int. J. Innov. Comput. Inf. Control*, 2011, **7**, (5B), pp. 2709–2726
31 Martínez-R, J., Alcántara-S, R.: 'On-line signature verification based on optimal feature representation and neural-network-driven fuzzy reasoning'. Proc. Fifth Int. Conf. Advances in Infrastructure for

doi: 10.1049/iet-bmt.2012.0048

e-Business, e-Education, e-Science, e-Medicine on the Internet, L'Auila, Italy, 2003
32 Muller, M.: 'Information retrieval for music and motion' (Springer, 2007), Ch. 4 (available at http://www.springer.com/cda/content/document/cda_downloaddocument/9783540740476-c1.pdf?SGWID=0-0-45-452103-p173751818)
33 Yang, L., Widjaja, B., Prasad, R.: 'Application of hidden Markov models for signature verification', *Patt. Recogn.*, 1995, **28**, (2), pp. 161–170
34 Impedovo, D., Pirlo, G.: 'Automatic signature verification: the state of the art', *IEEE Trans. Syst. Man Cybern.*, 2008, **38**, pp. 609–635
35 www.cse.ust.hk/svc2004
36 Khomatov, A., Yanikoglu, B.: 'SUSIG: an online signature database, associated protocols and benchmark results', *Patt. Anal. Appl.*, 2009, **12**, (3), pp. 227–236
37 Ong, T.S., Khoh, W.H., Teoh, A.: 'Dynamic handwritten signature verification based on statistical quantization mechanism'. Int. Conf. Computer Engineering and Technology, 2009, vol. 2, pp. 312–316
38 Fierrez-Aguilar, J., Krawczyk, S., Ortega-Garcia, J., Jain, A.K.: 'Fusion of local and regional approaches for online signature verification'. Proc. IWBRS, 2005 (*LNCS*, **3617**), pp. 188–196
39 Mohammadi, M.H., Faez, K.: 'Matching between important points using dynamic time warping for online signature verification', *Cyber J.: Multidiscip. J. Sci. Technol., J. Sel. Areas Bioinf.*, 2012 Jan, pp. 1–7
40 Khalil, M.I., Moustafa, M., Abbas, H.M.: 'Enhanced DTW based online signature verification'. 16th IEEE Int. Conf. Image Processing (ICIP), 2009, pp. 2713–2716
41 Ibrahim, M.T., Kyan, M., Guan, L.: 'Online signature verification using Global features'. Canadian Conf. Electrical and Computer Engineering, 2009, pp. 682–685