An Automatic Offline Signature Verification and Forgery Detection System

Vamsi Krishna Madasu

School of Engineering Systems
Queensland University of Technology
Brisbane, QLD 4000, Australia
Phone: +61 7 3138 1623
Fax: +61 7 3138 1469
E-mail: v.madasu@qut.edu.au

&

Brian C. Lovell

NICTA Limited (Queensland Laboratory)
Level 19 & 20, 300 Adelaide Street, Brisbane, QLD 4000
and
School of ITEE, University of Queensland
Phone: +61 7 3000 0481
Fax: +61 7 3000 0480
E-mail: brian.lovell@nicta.com.au

An Automatic Offline Signature Verification and Forgery Detection System

Abstract

This chapter presents an offline signature verification and forgery detection system based on fuzzy modelling. The various handwritten signature characteristics and features are first studied and encapsulated to devise a robust verification system. The verification of genuine signatures and detection of forgeries is achieved via angle features extracted using a grid method. The derived features are fuzzified by an exponential membership function, which is modified to include two structural parameters. The structural parameters are devised to take account of possible variations due to handwriting styles and to reflect other factors affecting the scripting of a signature. The efficacy of the proposed system is tested on a large database of signatures comprising over 1200 signature images obtained from 40 volunteers.

Keywords: Signature Verification, Forgery Detection, Grid Method, Fuzzy Modelling,

1 Introduction

A handwritten signature can be defined as the scripted name or legal mark of an individual, executed by hand for the purpose of authenticating writing in a permanent form. The acts of signing with a writing or marking instrument such as a pen or stylus is sealed on the paper. The scripted name or legal mark, while conventionally applied on paper, may also be accomplished using other devices that capture the signature process in digital format.

Hilton (1992) discusses what a signature is and how it is produced. He notes that the signature has at least three attributes, form, movement and variation. Since the signatures are produced by moving a pen on a paper, movement perhaps is the most important aspect of a signature. Movement is produced by muscles of the fingers, hand, wrist, and for some writers, the arm; and these muscles are controlled by nerve impulses. Once a person is used to signing his signature, these nerve impulses are controlled by the brain without any particular attention to detail.

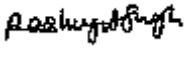
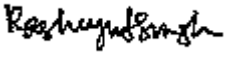
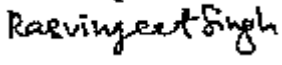
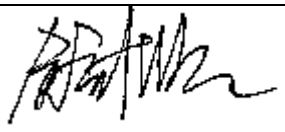
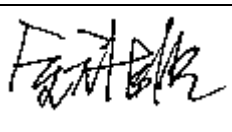
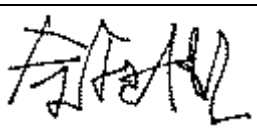
Type	Genuine	Skilled forgery	Unskilled forgery
Simple			
Cursive			
Graphical			

Figure 1: Types of signatures

The variations in handwritten signatures are quite immense, both within samples from the same individual and to an even larger degree across the population of individuals. The susceptibility of a signature to false imitation is clearly a function of the nature of the signature itself. In a broad sense, signatures can be classified as simple, cursive or graphical based on their form and content as shown in Fig. 1.

Simple signatures are the ones where the person just scripts his or her name in a stylish manner. In this type of signatures, it is very easy to interpret all the characters in the name. Cursive signatures on the other hand are more complex. Though the signatures still contain all the individual characters within the name, they are however drafted in a cursive manner, usually in a single stroke. Lastly, the signatures are classified as graphical when they portray complex geometric patterns. It is very difficult to deduce the name of the person from a graphical signature as it is more of a sketch of the name of the signer.

2 Handwritten Signatures

It is a well known fact that no two signatures, even if signed by the same person, are ever the same. However, if two signatures are *exactly* alike, then one of them is not a genuine signature but is a copy of the other – either a machine copy, such as one produced by a computer or photocopier, or a manually produced copy, such as tracing. In addition, simulation must be taken into account, where an individual copies the signature of another, using a genuine signature as a model. In these cases, the simulated writing usually exhibits an incorrect interpretation of inconspicuous characteristics of a genuine signature which are quite hard to recognize by a non-expert.

Osborn (1929), one of the earliest experts in the field of document examination observed that the variations in handwriting are themselves habitual. This is clearly seen in any collection of genuine signatures produced at different times and under a great variety of conditions. When carefully examined these signatures show that running through them is a marked, unmistakable individuality even in the manner in which the signatures vary as compared with one another. He further notes that unusual conditions under which signatures are written may affect the signature. For example, hastily written, careless signatures, cannot always be used unless one has sample signatures that have been written under similar conditions. Furthermore, signatures written with a strange pen and in an unaccustomed place are likely to be different than the normal signatures of a person.

Locard (1936), another expert document analyst, surveyed graphometric techniques used for the authentication of questioned documents. Locard categorizes the characteristics of genuine handwritten signatures into two broad classes. The first class is related to those characteristics of genuine signatures which are quite difficult to imitate such as the rhythmic line of the signature consisting of the positional variation of the maximum coordinate of each character in the signature; the local variation in the width of the signature line which is closely related to the dynamics of the writing process; and the variation in the aspect ratio of the complete signature followed by other local features like the difference in orientation and relative position, etc. The characteristics of the second class are the ones that are very easily perceived by a casual forger and are therefore easier to imitate. These are usually the general shape of the signature like the signature's overall orientation and its position on the document.

Osborn states that the successful forging of a signature or simulating another person's writing by a forger involves not only copying the features of the genuine signature but also hiding his own personal handwriting characteristics.

The forgeries in handwritten signatures have been categorized based on their characteristic features (Suen *et al.*, 1999). The three major types of forgeries are:

- *Random forgery* - The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery. These forgeries represent almost 95% of all the cases generally encountered in fraudulent cases although they are very easy to detect even by the naked eye (Harrison, 1958).
- *Unskilled forgery* - The signer imitates the signature in his own style without any knowledge of the spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for a while.
- *Skilled Forgery* - undubtedly the most difficult of all forgeries is created by professional impostors or persons who have experience in copying the signature. For achieving this one could either trace or imitate the signature by hard way.

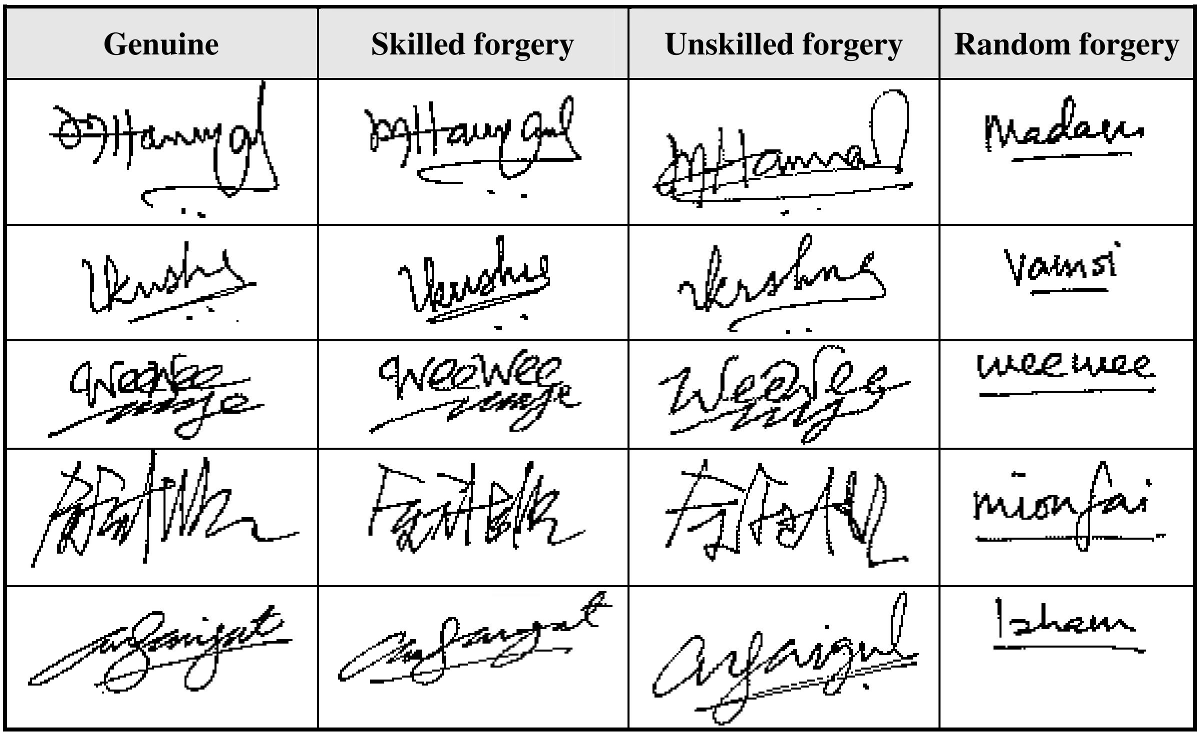


Figure 2: Types of forgeries

We now list some of the most important characteristics of genuine signatures and forgeries as outlined by several document examiners in the past. The understanding of these characteristics is important for determining those aspects or features of the signatures which are most important for automatic signature verification. Once the unique features have been selected, a knowledge base of all the feature values of the reference signature can be built so that when a test signature comes across the system, only the feature values are needed. This will eliminate the need for storage of all the signature images.

- **Enlargement of characters:** A forgery is usually larger than the original signature. This is due to the fact that a forger carefully observes the genuine signature before imitating it at the same time. The feedback mechanism in the brain of the forger is slower than the process taking place in the mind of the original writer, and consequently more time is spent drawing each letter. This makes a forgery larger than the original both in terms of the size of letters and the size of the entire signature. Similarly, the complete signature can also be larger than the original so enlargement does not just apply to individual letters.
- **Tendency of curves to become angles:** Curved letters are often observed in the forgery as being more angular. The forger takes care to obtain the correct letter shape by using a slower speed to produce the curve accurately. Ironically this results in more angular letters as greater time elapses on the making of the curves. In the same way, angled letters in the original signature can become smooth curves.
- **Retouching:** results when the imitation has been done already but an addition is made to it at a later stage. Lines may appear to be thicker at these points or there may be lines that do not follow the continual flow of the pen as in the original signature.
- **Poor line quality:** The ink reveals variation in light and shade; pressure and speed, with either more or less ink appearing on the page. It is more usual to find that the pressure used for the questioned signature is harder than that of the real signature. However, a lighter pressure can sometimes be detected. This may be due to a tremor which is caused by trembling of the hand; poor line quality or by writing too slowly.
- **Hesitation:** In the process of creating a forgery, the forger may pause to consult the genuine signature and then continue duplicating it. This can often create blobs (when the pen leaves an ink mark on the page) which may not be obvious.
- **Punctuation:** Full stops, dots on small letter "i" in wrong place, missing or added.
- **Differing pressure:** refers to the differences in pen pressure applied while signing. The pen pressure may be too heavy or too light depending on the style of the forger. Pressure differences occur at different places from the genuine signature as identical pen pressure is difficult to achieve. Most of the forgeries come out too dark or too light as everyone has a different pen style, but it is also hard to vary pressure in the same way as a genuine signer.
- **Sudden Endings:** Usually the original signature just trails off whereas the forgery just stops. Sudden endings are a characteristic feature of a forgery as it is very difficult to trail off in the same way as the genuine signature. Most often it is simply easier to end more definitely rather than trailing off in a particular pattern.
- **Forger's Characteristics:** The forger unconsciously reveals characteristics of his own handwriting when doing the forgery. Basic letter shapes, spacing, position of letters in relation to base line are very similar to forger's own. However, this is difficult to detect if the forger is unknown or in other words, only possible when the forger's characteristics are definitely known.
- **Baseline Error:** The forger, in an attempt to correctly imitate the size and shape of a signature, often neglects to ensure that the imaginary line which runs across the base of the signature is similar in the forged signature as in the genuine signature. The baseline in a signature is not horizontal and any notable variances in the baseline are almost sure signs of forgery.
- **Spacing:** Spacing may be larger or smaller spaces between individual letters, between whole words, and between punctuation and letters cannot be copied by tracing a signature.

- **Bad line quality:** Bad line quality is apparent by hesitant or shaky pen strokes and occurs when the forgery has been done too slowly.
- **Forming characters not appearing in signatures*:*** Unintelligible signatures are rationalised by a forger so that individual letters can be discerned in the forgery, whereas they are not apparent in the genuine signature. A characteristic of poor forgers is often caused by them knowing the name they are trying to forge and by unconsciously including letters which do not appear in the genuine signature. If the forger is unsure of the name then incorrect letters may appear clearly in the forgery.

These characteristics demonstrate that human signature verification is far from trivial but clearly most of these points cannot be applied to computerized signature verification. The aim of this study is therefore to investigate the intrinsic properties of signatures which are repeated again and again so as to increase the reliability of uniquely identifying a person on the basis of his handwritten signature.

3 Handwritten Signature Features

The handwritten signature is a behavioural biometric which means that the biometric measurement is not based on any physiological characteristic of the individual, but on behaviour that can change over time. The process of determining the legitimacy of a handwritten signature is termed as signature verification. Since an individual's signature alters over time, the use of signature verification for authenticating sensitive financial transactions over a long period may lead to high error rates. Enrolment to a signature verification system requires the collection of an exclusive set of signature samples that are similar in nature so as to locate an adequate number of common characteristics. Inconsistent signatures lead to high false rejection rates and high enrolment failure rates for individuals who do not sign in a consistent way. However, the positive aspect of signature verification technology is that unlike other physiological biometrics like face, fingerprint or iris, if the signature biometrics of an individual is compromised, the individuals can simply change their signatures.

In the recent past, many questions have been raised about the scientific basis of the expert opinion offered by forensic document examiners. In order for forensic document examination to retain its credibility and legal acceptability as a science there must be some statistically sound basis for the decision. In addition, such scientific information is also useful for the efficient development of automatic signature verification systems. This research is concerned with the automatic analysis of perceptible features in handwritten signatures to determine the features which distinguish a forgery from a genuine signature. In static or offline signature verification systems, the signature image is characterized as a vector of elements, each one representative of the value of a feature. The careful selection of this feature vector is crucial for the success of any signature verification system.

3.1 Types of Features

Features extracted for offline signature verification can be broadly divided into three main types (Fang et al., 2003; Lee & Pan, 1992):

(i) *Global features* depict or categorize the signature as a whole. These features are usually extracted from all the pixels that lie within the region circumscribing the signature image such as the length, width or baseline of the signature. Although global

features are easily extractable and less sensitive to noise as small distortions in isolated regions of the signature do not cause a major impact on the global feature vector. They are however dependent upon the overall position alignment and therefore highly susceptible to distortion and style variations.

(ii) *Local features* represent a segment or limited region of the signature image such as critical junctions and gradients. These features are generally derived from the distribution of pixels of a signature such as local pixel density or slant. Local features are more sensitive to noise within the region under consideration but unaffected by other regions of the signature. Although, they are computationally expensive but are much more accurate than global features.

(iii) *Geometric features* describe the characteristic geometry and topology of a signature thereby preserving both their global as well as local properties. These features have a high tolerance to alterations and style variations, and they can also tolerate a certain degree of translation and rotation variations.

3.2 General Overview of Signature Features

Many different types of features have been proposed for offline signature verification systems with varying degrees of success. Since dynamic information is not available in static signatures, features can only be extracted from the geometric analysis of signatures. Some of the most widely used parameters are the signature image area, the signature height and width, the ratio between the signature height and its width, the ratio between middle zone width and signature width, global and local slant, the number of characteristics points (end-points, cross-points, cusps, etc.), number of loops, the presence of the lower zone parts and the number of elements in the signature (Amaar, 1990, 1991; Blatzakis & Papamarkos, 2001; Plamondon & Lorette, 1989).

The coefficients obtained from Fourier, Hadamard and Wavelet transforms, have also been used as parameters for off-line signature verification (Deng *et al*. 1999; Fadhel & Bhattacharya, 1999; Murshed *et al*. 1997; Nagel & Rosenfeld, 1977). Projections–based features include the number of vertical and horizontal projection peaks, maximum vertical and horizontal projections (Ammar, 1990, 1991). The main contour-based features are concerned with the use of parameters extracted from signature envelope and outlines (Bajaj & Chaudhury, 1997; Cardot *et al*. 1994). Furthermore, texture based features derived from the co-occurrence matrices of the signature image have also been considered by Blatzakis & Papamarkos, 2001.

Many of the local features are of the same character as the global ones. The difference is that they are applied either to the cells of a grid covering the signature, or to the specific elements obtained after signature segmentation. They include: slant of the element, density factor, and length ratio of two consecutive parts, position relation between the global baseline and the local one; upper, central and corner line features and critical points (Ismail & Gad, 2000; Qi & Hunt, 1994; Quek & Zhou, 2002). In grid-based features, the signature image is divided into rectangular regions and ink distribution in each region is evaluated (Blatzakis & Papamarkos, 2001; Drouhard *et al*. 1996; Sabourin *et al*. 1997).

The features based on geometrical properties of a signature image are useful for the detection of random and simple forgeries, but they fail to recognize skilled forgeries which are almost identical to the genuine signatures in terms of global shape and orientation. There have been attempts to extract dynamic information from static images. Parameters like stroke direction,

length, width and curvature variation are estimated with these techniques. Different levels of pressure features have also been extracted from the signature images (Ammar, 1990, 1991; el-Yacoubi *et al*. 2000; Justino *et a*l. 2001; Rigoll and Kosmala, 1998). It is assumed that they are connected with varying speeds at various parts of the signature (Quek & Zhou, 2002).

Qi and Hunt (1994) discuss a static signature verification based on global and local features of a signature image. The global features are: height and width of a signature image, width of the signature image with blank spaces between horizontal elements removed, slant angle of the signature, vertical centre-of-gravity of black pixels, maximum horizontal projection, area of black pixels, and baseline shift of the signature image. The local (or grid) features include the structural information of image elements, for example, angle of a corner, curvature of an arc, intersection between the line strokes and number of pixels within each grid. These features are found to give good results as compared to structural features.

From the above discussion, it is understood that an appropriate combination of global and local features will produce more distinctive and efficient features. This is because by localizing global features, the system will be able to avoid major shortcomings of both the approaches and at the same time benefit from their combined advantages.

4 Data Acquisition

The first step in the design of a static signature verification system is data acquisition. Handwritten signatures are collected from different individuals and some unique features are extracted from them to create a knowledge base for each individual. The features stored in the knowledge base are then learned by the system and used as a reference for comparing with those of the test signature in the recognition phase. A standard database of signature samples is thus needed for calculating the performance of the signature verification system and also for comparison with the results obtained using other techniques on the same database. Unfortunately, no such standard benchmark database exists in the field of signature verification due to the confidentiality and privacy issues associated with handwritten signatures.

The proposed signature verification system is trained and tested on a database consisting of a total of 1200 handwritten signature images. Out of these, 600 are authentic signatures and the other 600 are forgeries. These signatures are obtained from 40 volunteers with each person contributing 15 signature samples, among which 10 are used for learning purposes and the rest for testing (See Table 1).

Table 1: Signature Database

Type of Signatures	**Training set**	**Test set**	**TOTAL**
Genuine signatures	40 × 10	40 × 5	**600**
Skilled forgeries	-	40 × 5	**200**
Unskilled forgeries	-	40 × 5	**200**
Random forgeries	**-**	40 × 5	**200**

The selection of an optimum number of samples for training is a critical point during the construction of the signature databases. To investigate signatures, Osborn recommends that several genuine signatures should always be obtained, if possible, and five signatures always provide a more satisfactory basis for an opinion than one just signature and ten signatures being better than five. Hence after much consideration, we have fixed the size of the training set to 10 samples for each person to reflect their signature variations optimally. In addition, the system is trained with only genuine signatures, i.e., none of the forgeries are used for training the system. Most of the signature verification systems trained with both genuine and forged signatures have been subject to errors. For example, the automatic off-line signature verification of Pender (1991) has a false acceptance rate (FAR) of 100% when trained with only genuine signatures. This means that it could not distinguish even a single forgery from genuine signatures when the system is not trained with the samples of forged signatures.

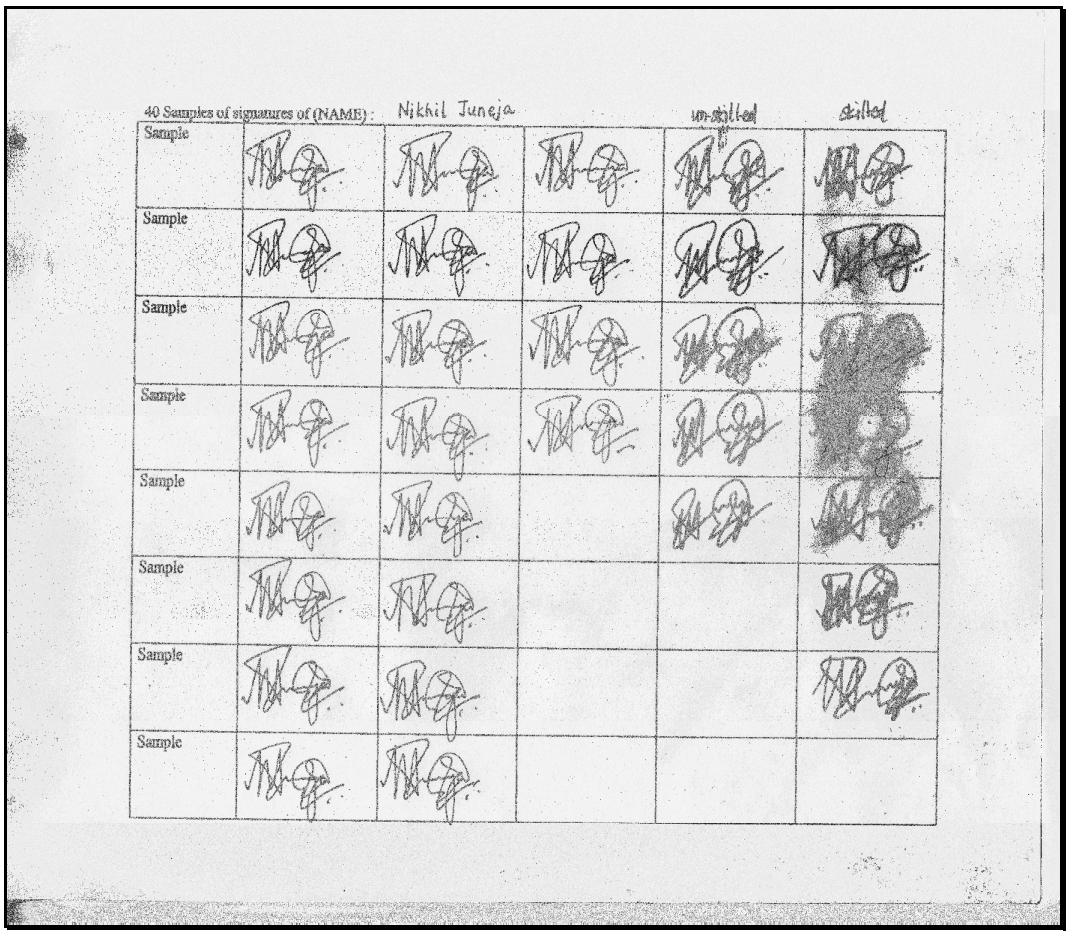


Figure 3: Signature Data Acquisition

The signatures are handwritten on a white sheet of paper, using any type of pen or pencil, and are scanned at a resolution of 300 *dpi*. A scanned image of the special sheet designed for collecting signatures is shown in Fig. 4.3. The signatures are collected over a period of four weeks to account for the variations in signature style with time. The forgeries are also collected over the same time frame. The random forgeries are obtained by supplying only the names of the individuals to the casual forgers who never had any access to the actual genuine signatures. The unskilled forgeries in turn, are obtained by providing sample genuine signatures to the forgers who are then allowed to practise for a while before imitating them to create the forgeries. Each volunteer had to provide five imitations of any one of the genuine

signatures, apart from his or her own signatures. These samples constitute the set of unskilled forged signatures for the set of genuine signatures. We have then requisitioned the services of two expert forgers to provide five forgeries of each genuine signature in the test set so as to create the skilled forged samples of all the persons.

5 Pre-processing

The signature images scanned during the data acquisition phase are extracted and pre-processed in this module. The steps of pre-processing are briefly discussed in the following sections.

5.1 Binarization

Binarization is the first step in pre-processing of signature images. In this process, the input gray scale image is converted into a two tone image format, i.e., black and white pixels (commonly represented by 1 and 0 respectively).

5.2 Slant Normalization

A practical signature verification system must be able to maintain high performance regardless of the size and slant of a given signature. For handwritten signatures, one of the major variations in writing styles is caused by slant, which is defined as the slope of the general writing trend with respect to the vertical line. It is important that the system be insensitive to slant hence need for slant correction in the signature image.

The image matrix is divided into upper and lower halves. The centres of gravity of the lower and upper halves are computed and connected. The slope of the connecting line defines the slope β of the window (image matrix). The slant-corrected image is obtained by applying the following transformation to all black pixels with coordinate points x, y in the original image:

$$x' = (x - y) \times \tan(\beta - \beta_0), \quad y' = y \tag{1}$$

where

x' and y' are slant corrected coordinates and

β_0 is a parameter specifying the default (normal) slant.

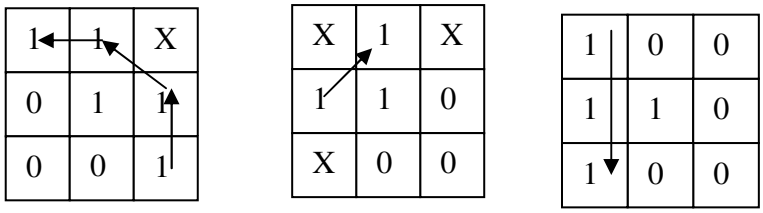
Slant correction needs to precede other pre-processing tasks, i.e. it is applied before smoothing. This is because smoothing tends to change the image topology and the correction operation usually creates rough contours to the character.

5.3 Skeleletonization

A two-tone digitized image is defined by a matrix A, whose element $a_{i,j}$ is either 1 if character is present or 0 otherwise. Iterative transformations are applied on A to obtain a thinned image which is of one pixel thickness. This process is termed as ‘Skeletonization’ as the output image is a skeleton of the original image. The modified safe point thinning algorithm (SPTA) (Shih and Wong, 1995) is used in this work for the task of skeletonization.

5.4 Smoothing

Because of the excessive processing performed during the slant correction and thinning stage, we find that a signature often contains barbs and some redundant dark pixels that are not relevant in maintaining the connectivity of the image. Some such points have been identified and Boolean expressions developed to rid the image of points such as those described below. In the following depictions, "1" represents a dark pixel, "0" represents a white pixel while X represents a 'don't care' condition. The central pixel is not relevant in maintaining the connectivity of the image, as path depicted by the arrows connects the remaining pixels. Points of similar configuration but different orientations (three other possible) are identified and removed (converted to white). Another set of points, termed as extra corners is also identified and deleted as shown in Fig. 4.4 (b). Again, seeing the connectivity we remove the central dark pixel. Three other orientations can be easily identified and the corresponding points deleted. Finally, the following set of points is identified in Fig. 4.4 (c). Here again, the central point is deleted.



(a) (b) (c)

Figure 4: Smoothing using maintenance of connectivity

End Point Smoothing

Another novel approach has been devised to smoothing and removal of spurious tails of signature images that are distorted initially or during the pre-processing. Two types of points in sinatures are considered for this process:

- *End points :* Dark points with only one dark neighbour out of eight closest neighbours.
- *Junction Points:* Dark points with more than two dark neighbours out of eight closest neighbours.

The approach essentially involves identification of all end points in the pre-processed image. Starting with each end point, a path is traced till we either reach a junction point or exceed a heuristically determined path length. If we reach a junction point, within the length specified, the path of dark pixels starting from that end-point to the junction point is determined as a spurious tail and deleted. If during traversal the path length is exceeded, we retain the branch and divert our search to the next end-point, until all points are covered. A bottleneck faced in the performance of this approach is the size of the heuristically determined path length. If correctly chosen, it gives some spectacular results. However, incorrectly chosen lengths would either leave the image unaffected or may delete branches that should not be deleted otherwise.

5.5 Size Normalization

After the binarization process, there would be extra zeros on all four sides of the signature image as zero padding is applied during binarization. To standardize the size of the signatures, extra rows and columns containing only zeros are removed from all four sides of the image.

Normalization is thus the process of equating the size of all signature samples so as to extract features on the same footing. To achieve this, we use standard bilinear transformation, by which, every input bitmap P, of size $m \times n$, is transformed into a normalized bitmap Q, of size $p \times q$. Both p and q are quadrilateral regions. All the signature images are standardized to a fixed window of size 120 × 60 pixels.

6 Feature Extraction

The success of a pattern recognition system depends largely on the type of features extracted from the dataset. The chief objective of this process is to extract those features which will enable the system to correctly discriminate one class from the other. In this section, we will present our 'Signature Grid' method which has been devised for extracting innovative angle and distance features. The motivation behind the design of the grid is illustrated to prove its efficacy. Edge based direction features adopted from handwriting recognition are also discussed.

6.1 Grid based approaches

The structural information contained in a handwritten signature is obtained using a grid that is superimposed on the size-normalized signature image. The feature vector of each grid element includes the boundary code and the total number of pixels inside the grid. The boundary grid is a binary vector that is defined as,

$$b_i = \begin{cases} 1 & \text{pixel at i}^{\text{th}}\text{ position} > 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where

b_i is the distance from the upper-left corner of each grid when moving counter-clockwise on the boundary.

The length of the boundary code is equal to four times the side of each square grid. This boundary code is an incomplete, linear approximation to the structure within each grid when the size of the grid is relatively small, because there are multiple ways to linearly connect a given set of boundary locations within a grid. To alleviate this ambiguity, the intersection between the line stroke and the grid is thinned so that each intersection is represented by only one code element b_i. The total grid feature is thus represented as,

$$v_g = (n, b_1, b_2, ..., b_{4l}) \qquad b_i \in (0,1) \forall i \tag{3}$$

where

n is the total number of pixels within each grid.
l is the side length (in pixels) of the squared grid.

Murshed *et al*. (1997) perform a local analysis of the shape of a signature within a predefined search region called the identity grid which is designed for each writer in the system. The signature image is centralised on the identity grid which is divided into nine regions which are further divided into squares of size 16 × 16 pixels. The *xy*-coordinates of each 16 × 16-pixel square indicate a location of a graphical segment in the identity grid of a particular writer. Feature extraction is performed on each of the 16 × 16-pixel squares that contain a graphical

segment by first calculating the centre of the square and then extracting the graphical segment enclosed within 32 × 32-pixel square.

A signature image of 512×128 pixels is centred on a grid of rectangular retinas which are excited by local portions of the image (Refer to Fig. 5). Each retina has only a local perception of the entire scene and granulometric size distributions are used for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of the attention grid.

Figure 5: A signature image centred on a grid of rectangular retinas

In (Quek & Zhou, 2002), the skeletonized image is divided into 96 rectangular segments and for each segment; area (the sum of foreground pixels) is calculated. The results are normalized so that the lowest value (for the rectangle with the smallest number of black pixels) would be zero and the highest value (for the rectangle with the highest number of black pixels) would be one. The resulting 96 values form the grid feature vector. A representation of a signature image and the corresponding grid feature vector is shown in Fig. 6. A black rectangle indicates that for the corresponding area of the skeletonized image, there would be the maximum number of black pixels. On the contrary, a white rectangle indicates the smallest number of black pixels.

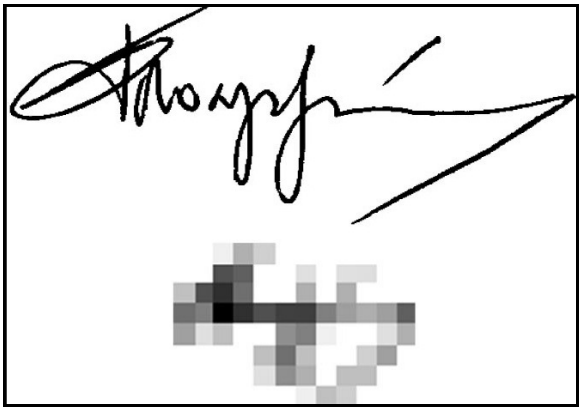


Figure 6: The grid feature vector for a signature

6.2 Signature Grid Method

The signature grid is defined as the *region of interest*, within which the signature image is enclosed. The size of the grid therefore depends on the signature being enclosed within it. The grid is divided into eight partitions which in turn are subdivided into 12 equal boxes.

The chief motivation behind the use of a signature grid is to divide the signature into local regions or boxes which over a set of all samples of a writer form a fuzzy set. In this way, we are able to capture the global behaviour through the local features, which form an intelligent knowledge base of unique features for a particular individual. The other motivation for designing the grid is to reduce the area of focus to just the signature image.

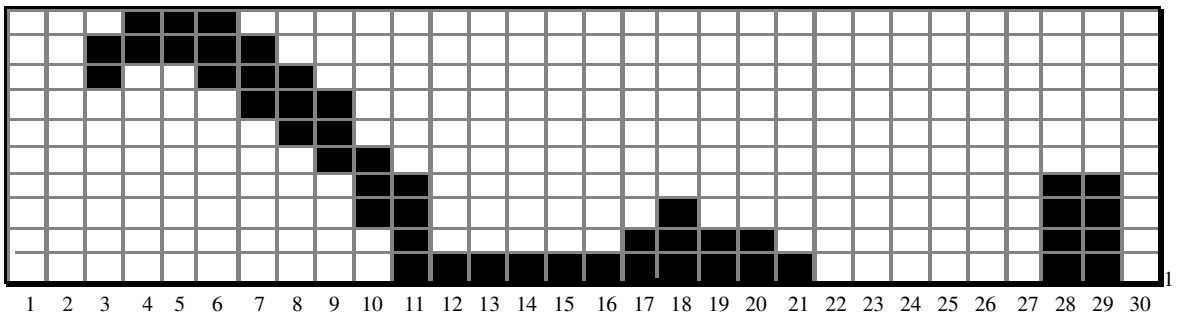


Figure 7: Partition using horizontal density approximation method

The pre-processed image is partitioned into eight portions using the equal horizontal density method. In this method, the binarized image is scanned horizontally from left to right and then from right to left and the total number of dark pixels is obtained over the entire image. The pixels are clustered into eight regions such that approximately equal number of dark pixels falls in each region. This process known as the horizontal density approximation method is illustrated in Fig.7.

From Fig.7, we note that the total number of points (dark pixels) is 48. If we divide the total pixels by four, we obtain 12 pixels per partition. Since the partition is done column wise, obtaining exactly 12 points in each partition is difficult. Therefore, we take approximately 12 points in each partition using two-way scanning approach. In this method we scan the image from left to right till we reach the column where the number of points in a particular partition is 12 or more. We repeat the same procedure while scanning the image from right to left direction. Then we partition the image in both directions: from left to right and right to left. Next, we take the average of two column numbers in each partition. Each partition is now resized to a fixed window of size 38 $\times$ 60 pixels and is thinned again. This partition is again sub-divided into 4 rows and 3 columns, constituting 12 boxes. In total we have 96 boxes for a single signature. This approach is termed the 'Signature Grid Method'. The idea behind this method is to collect the local information contained in the box.

6.2 Signature Grid Features

Signature Grid Features are extracted using the signature grid method which is based on the spatial division of the signature image. The signature is initially pre-processed and the partitioned using the signature grid, as explained in the previous sections. The signature grid is divided into 96 (12×8) equal boxes which are superimposed on the signature image. The bottom left corner of each box is taken as the absolute origin (0,0) and distance and angle features are computed with reference to the origin of the box. The vector distance for k th pixel in b th box at location (i, j) is calculated as,

$$d_k^b = \sqrt{\left(i^2 + j^2\right)} \tag{4}$$

The above vector distances constitute a set of features based on distance. Similarly, for each k th black pixel in a box at location (i, j), the corresponding angle is computed in a similar manner.

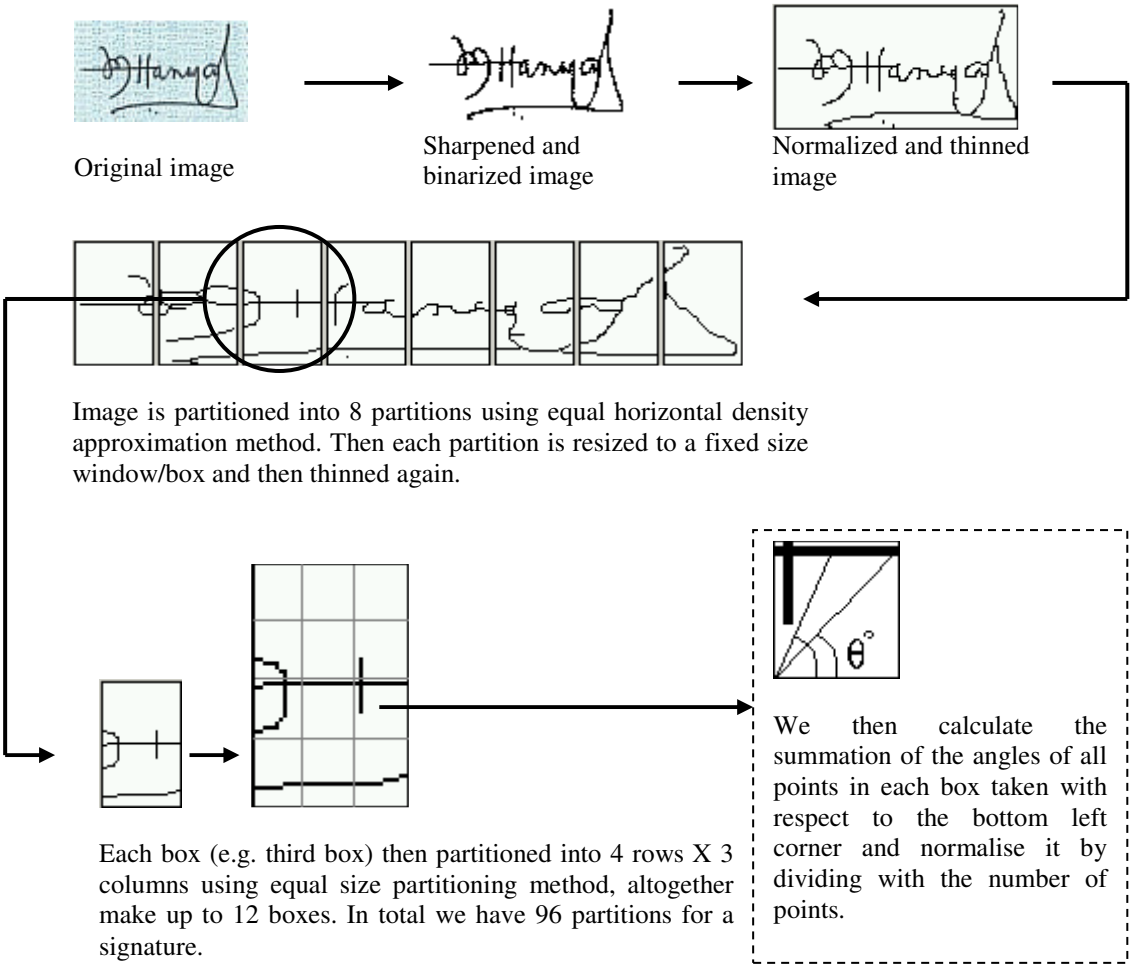


Figure 8: Pre-processing and Feature Extraction

By dividing the sum of distances of all black pixels (having value '1') present in a box with their total number, a normalized vector distance, γ_b, for each box is obtained as,

$$\gamma_b = \frac{1}{n_b} \sum_{k=1}^{n_b} d_k^b \tag{6}$$

where, n_b is number of pixels in b^{th} box.

Then the sum of all angles in a box b is divided by the number of 'l' pixels present in that box to yield a normalized angle γ_b.

$$\gamma_b = \frac{1}{n_b} \sum_{k=1}^{n_b} \theta_k^b \tag{7}$$

where, n_b is number of pixels in b th box.

The angle and distance features obtained from all the 96 boxes constitute the complete feature set of a particular signature sample. For the present problem of signature verification and forgery detection, we have experimented with both distance and angle distributions. However, it is found that the angle distribution is better than distance distribution due to its non-linearity (Refer to Fig. 9).

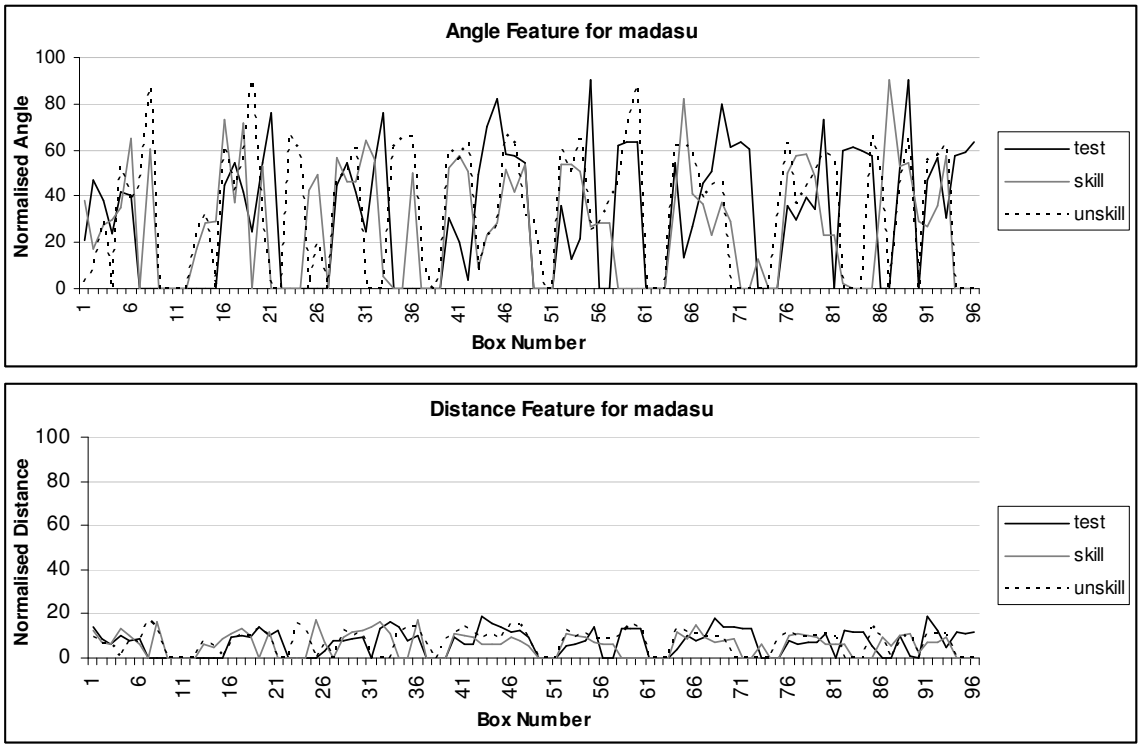


Figure 9: Distance and angle feature distributions for signatures

Hence the choice fell on extracting angle information from the boxes. We now discuss the computational aspects. Table 2 gives the angle features of one of the signatures used for training. The eight rows stand for the eight partitions of the signature while the columns symbolize the further divisions within each partition.

Table 2: Angle features of one of the signatures used for training

Partition / Cluster	1	2	3	4	5	6	7	8	9	10	11	12
1	21.1	46.8	38.1	23.9	41.6	40.1	0	0	0	0	0	0
2	0	0	0	44.8	54.8	41.7	24.7	54.5	76.1	0	0	0
3	0	0	40.1	46.9	39.8	0	72.4	60.2	21.0	46.1	56.4	0
4	0	0	30.5	20.5	3.7	49.4	70.2	81.9	58.0	57.5	54.2	0
5	0	0	35.6	12.7	21.3	90	0	0	61.6	63.3	63.3	0
6	0	0	54.7	13.6	26.9	45.6	50.6	79.9	60.9	63.3	60.5	0
7	0	0	36.1	30.1	39.4	33.9	73.4	0	59.6	61.3	59.6	57.4
8	0	0	52.1	90	0	47.1	56.6	30.7	57.4	59.1	63.3	0

7 Verification system

Automatic verification of handwritten signatures on bank checks is integral to the success of a bank check processing and authentication system. The focus of this paper is hence on the development of an automatic system for verification and forgery detection of handwritten signatures extracted from paper documents. The features considered in the recognition system are angle and distance features.

The verification system is based on the Takagi-Sugeno (TS) fuzzy model (Takagi & Sugeno, 1985). A Takagi-Sugeno fuzzy inference system is well suited to the task of smoothly interpolating the linear gains that would be applied across the input space; it is a natural and efficient gain scheduler. It is also suitable for modelling nonlinear systems by interpolating multiple linear models. A graphical representation of a TS model is illustrated in Fig. 10.

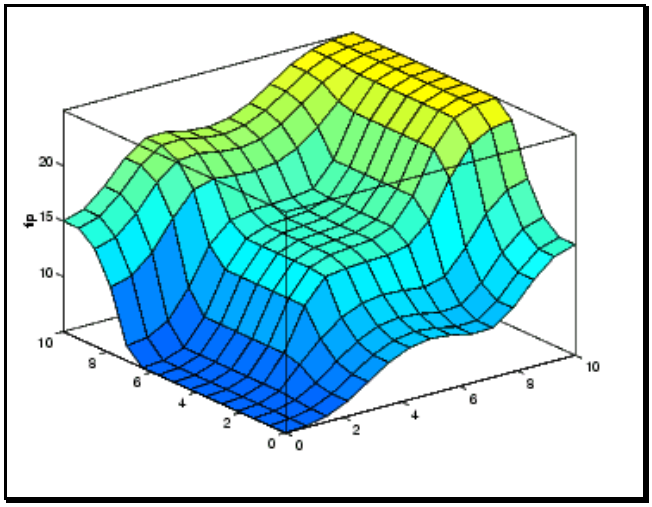


Figure 10: Takagi-Sugeno Fuzzy Model

Signature verification and forgery detection are carried out using angle features extracted from the signature grid. Each feature corresponds to a fuzzy set over all the samples of the training set. The features are fuzzified by an exponential membership function involved in the TS model, which is modified to include structural parameters to account for variations in signing styles. The membership functions constitute weights in the TS model. The optimization of the output of the TS model with respect to the structural parameters yields the solution for the parameters. The simplified form of TS model is derived by fixing the coefficients of consequent parts of the rules made up of all input features and also by considering a single rule for all input features.

7.1 System design

The proposed system includes both signature verification and forgery detection modules. The difference between them is that verification is based on inherent characteristics of a signer whereas the detection is based on specification of a limit, which exceeds the inherent variation in the genuine signatures of a signer. Different categories of forgery arise depending on the limit of variation allowed over the inherent variation. The various phases of the verification and detection are discussed in the following sections.

7.1.1 Model Formulation

Since the main thrust here is to establish the genuineness of the signature thereby detecting the forgeries, we have employed the TS fuzzy model for this purpose. In this study, we consider each feature as forming a fuzzy set over large samples. This is because the same feature exhibits variation in different samples giving rise to a fuzzy set. So, our attempt is to model the uncertainty through a fuzzy model such as the TS model. The overall system organization is depicted in Fig. 11.

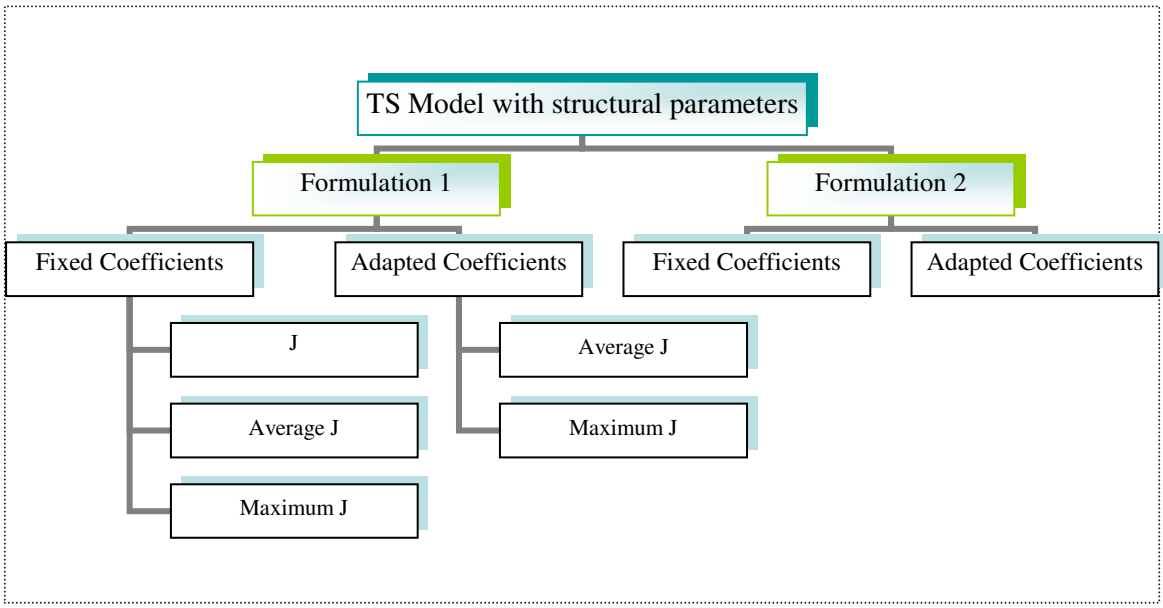


Figure 11: System Organization

The First Formulation: Let x_k be the k^{th} feature in a fuzzy set A_k, so the k^{th} IF THEN fuzzy rule in TS model has the following form

$$\begin{aligned} &\textit{Rule k:} \quad \text{IF } x_k \text{ is } A_k \\ &\qquad\quad \text{THEN } y_k = c_{k0} + c_{k1} x_k \end{aligned} \tag{8}$$

Each feature will have a rule so we have as many rules as the number of features. The fuzzy set A_k is represented by an exponential membership function (MF) that includes two structural parameters s_k and t_k. This membership function is expressed as,

$$\mu_k(x_k) = \exp - \left[\frac{(1-s_k) + s_k^2 \left| x_k - \overline{x_k} \right|}{(1+t_k) + t_k^2 \sigma_k^2} \right] \tag{9}$$

where,

$\overline{x_k}$ is the mean

σ_k^2 is the variance of k^{th} fuzzy set

The structural parameters are included in the TS model so as to track the intra-class variations in the different samples of signatures obtained from the same individual. A special condition of the above function occurs when $s_k = 1$ and $t_k = -1$. In that case, the MF becomes devoid of the structural parameters and is solely dependent on means and variances. The significance of this condition is that the reference signature and the signatures under investigation will have the same statistics. This choice is guided by the consideration of no role for parameters if the signatures of a person don't change. The justification for the modified MF is two-fold: (i) Easy to track variations in means and variances, and (ii) no need for any sophisticated learning technique.

The strength of the rule in Eqn. 8 is obtained as,

$$w_k = \mu_k(x_k) \tag{10}$$

The output is expressed as

$$Y = \sum_{k=1}^{L} w_k y_k \tag{11}$$

where,

L is the number of rules.

We define the performance function as

$$J = (Y_r - Y)^2 \tag{12}$$

where,

Y and Y_r denote the output of the fuzzy model and of the real system respectively.

Since the output of a verification system Y_r is not available, it can be safely assumed to be unity. In order to learn the parameters involved in the membership function (i.e., s_k and t_k) and the consequent parameters c_{k0} and c_{k1}, Eq. (12) is partially differentiated with respect to each of these parameters. Accordingly, we have

$$\frac{\partial J}{\partial c_{k1}} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial y_k} \cdot \frac{\partial y_k}{\partial c_{k1}} = 2\left(Y - Y_r\right) w_k x_k \tag{13}$$

$$\frac{\partial J}{\partial c_{k0}} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial y_k} \cdot \frac{\partial y_k}{\partial c_{k0}} = 2\left[Y - Y_r\right] w_k = 2\delta w_k \tag{14}$$

$$\begin{aligned} \frac{\partial J}{\partial s_k} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial w_k} \cdot \frac{\partial w_k}{\partial t_k} &= 2(Y - Y_r) \cdot y_k \cdot \frac{\mu_k \left\{1 - 2s_k \left| x_k - \overline{x_k} \right|\right\}}{\left\{(1 + t_k) + t_k^2 \sigma_k^2\right\}} \\ &= 2\delta y_k \mu_k \left[\left\{1 - 2s_k \left| x_k - \overline{x_k} \right|\right\} \Big/ T \right] \end{aligned} \tag{15}$$

$$\frac{\partial J}{\partial t_k} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial w_k} \cdot \frac{\partial w_k}{\partial t_k} = 2(Y - Y_r)\, y_k \mu_k \frac{\left\{(1-s_k) + s_k^2 \left| x_k - \overline{x_k} \right| \right\} \left\{1 + 2t_k \sigma_k^2\right\}}{\left\{(1+t_k) + t_k^2 \sigma_k^2\right\}^2}$$
$$= 2\delta y_k \mu_k \left\{(1-s_k) + s_k^2 \left| x_k - \overline{x_k} \right| \right\} \left\{1 + 2t_k \sigma_k^2\right\} \Big/ T^2 \tag{16}$$

where,

$\delta = Y - Y_r$, $T = (1+t_k) + t_k^2 \sigma_k^2$ and

$k = 1,..,L$ denotes the rule number.

The gradient descent learning technique is applied to learn the parameters as follows:

$$c_{ki}^{new} = c_{ki}^{old} - \in_1 \frac{\partial J}{\partial c_{ki}}, i = 0,1 \tag{17}$$

$$s_k^{new} = s_k^{old} - \in_2 \frac{\partial J}{\partial s_k} \tag{18}$$

$$t_k^{new} = t_k^{old} - \in_3 \frac{\partial J}{\partial t_k} \tag{19}$$

where,

$\in_1, \in_2, \in_3$ are the learning coefficients such that $\in_1, \in_2 \; and \in_3 \in \Re^+$.

Global gradient descent learning of parameters

We can make use of global learning when we have large datasets, say, M . This is known as a batch learning scheme, in which change in any parameter is governed by the following equation:

$$\Delta w(q) = \sum_{j=1}^{M} \Delta_j w(q) + \alpha_m \Delta w(q-1) - \gamma w(q) \tag{20}$$

The parametric update equation is,

$$w(q+1) = w(q) + \Delta w(q) \tag{21}$$

where,

w in (21) may stand for any of the parameters c_{ki}, s_k, t_k .

q is the q^{th} epoch.

α_m is a momentum coefficient in the limits $0 \le \alpha_m < 1$ (typically $\alpha_m = 0.9$).

γ is a decay factor (typically in the range of 10^{-3} to 10^{-6}).

We can obtain initial $\Delta w(q)$ from Eqns. (17) - (19) by computing the partial derivatives of J . We will now show that the recognition approach explained above is a special case of TS

model. For this, assume $c_{k0} = 1/L$ and $c_{k1} = 0$ so that $y_k = 1/L$ in Eq. (8). Substituting this in (11) yields,

$$Y = \frac{1}{L}\sum_{i=1}^{L}\mu_i \tag{22}$$

In the above Eqn. (22), Y is given by the average of the membership functions (MFs) and we will now prove that this average MF is a special case of TS model. The recursive equations, Eqns. (17) to (19), are iterated until the summation of δ for all feature values is small enough. The initial values of the structural parameters are obtained from:

$$\frac{\partial J}{\partial s_k} = 0 \Rightarrow 1 - 2s_k\left|x_k - \overline{x_k}\right| = 0 \Rightarrow s_k = \frac{1}{2\left|x_k - \bar{x}_k\right|} \tag{23}$$

$$\frac{\partial J}{\partial t_k} = 0 \Rightarrow 1 + 2t_k\sigma_k^2 = 0 \Rightarrow t_k = -\frac{1}{2\sigma_k^2} \tag{24}$$

Note that the above initial values do not yield satisfactory results. We have to fine tune these values to obtain an efficient set of values.

The Second Formulation: Alternatively, it is possible to use only a single rule for all input features. The corresponding TS model will have the fuzzy rule of the form

$$\begin{array}{lll} \textit{Rule:} & \text{IF} & x_1 \text{ is } A_1, x_2 \text{ is } A_2, .., x_n \text{ is } A_n \\ & \text{THEN} & y = c_0 + \sum_{i=1}^{n} c_i x_i \end{array} \tag{25}$$

The performance function now becomes,

$$J = \{Y_r - wy\}^2 \quad \text{with } w = \Pi_{j=1}^{n}\mu_j \tag{26}$$

The derivatives of J with respect to c_0, c_i, s_i, t_i are given by the following equations:

$$\frac{\partial J}{\partial c_0} = -2\{Y_r - wy\}\Pi_{j=1}^{n}\mu_j \tag{27}$$

$$\frac{\partial J}{\partial c_i} = -2\{Y_r - wy\}x_i\Pi_{j=1}^{n}\mu_j \tag{28}$$

$$\frac{\partial J}{\partial s_i} = -2\{Y_r - wy\}y\mu_i\frac{\left\{1 - 2s_i(x_i - \overline{x_i})\right\}}{\left\{(1+t_i) + t_i^2\sigma_i^2\right\}} \tag{29}$$

$$\frac{\partial J}{\partial t_i} = -2\{Y_r - wy\} y \mu_i \frac{\{(1-s_i) + s_i^2 (x_i - \overline{x_i})\}\{1 + 2t_i \sigma_i^2\}}{\{(1+t_i) + t_i^2 \sigma_i^2\}^2} \tag{30}$$

The parameters can be found by the gradient descent technique. We will now derive the simplified version of the performance function. For this, assume $c_0 = 0$ and $\forall c_i = 0$ in Eqn. (24). This results in the equation,

$$y = w = \Pi_{j=1}^{n} \mu_j \tag{31}$$

From Eqns. (22) and (31), we observe that if we have a rule for each input feature, the simplified performance function is given by the average MF whereas if all input features are linked by a single rule, the simplified performance function corresponds to the multiplication of all MFs. We find that Eqn. (31) is more stringent than Eqn. (22) as it requires that all membership values must be nonzero. The recognition using Eqn. (22) is bound to be better in view of a large number of rules and parameters involved. So, our implementation follows this recognition strategy but by making subtle changes to suit the real world problems.

7.2 Implementation

The proposed system is applied on the Signature Database described in detail in Section 4. For implementation, we will consider two cases: In the first case, we use the simplified TS model in which the coefficients of the THEN part (Consequent) are fixed whereas in the second case we adapt the coefficients.

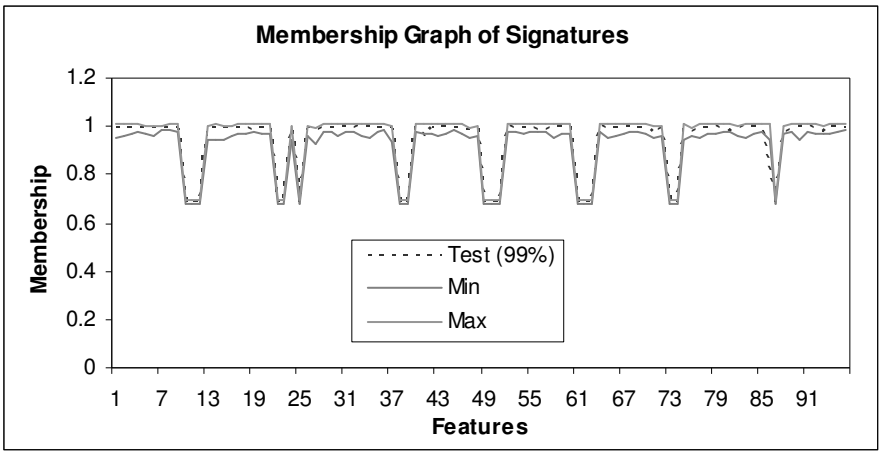
Case 1: TS model with consequent coefficients fixed

In view of Eqn. (22) and taking $Y_r = 1$, Eqn. (12) becomes

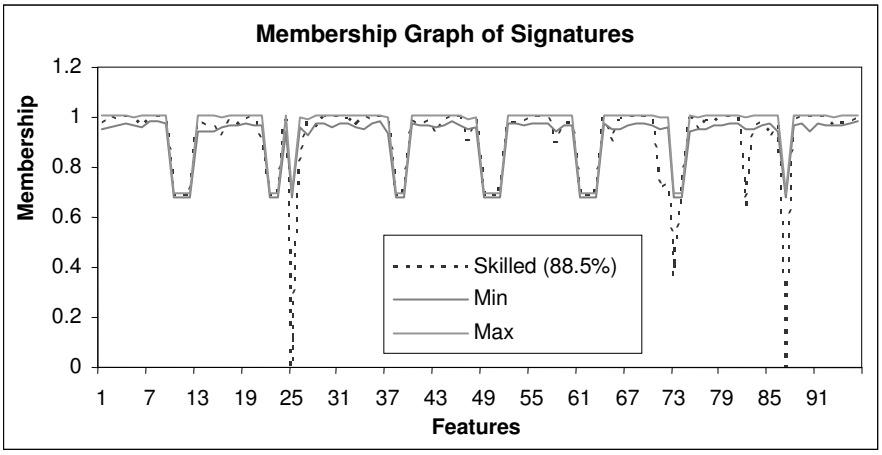
$$J = (1 - \frac{1}{L} \sum_{i=1}^{L} \mu_i)^2 \tag{32}$$

With the above performance index, we compute $\frac{\partial J}{\partial s_i}$ and $\frac{\partial J}{\partial t_i}$ in order to update the structural parameters s_i and t_i; $i = 1,..,96$. Using these values, we compute the membership functions for all the features. This process is repeated for all the training samples of a person. Here, we have devised an innovative approach for the classification of all signatures (i.e., test signatures and random, skilled and unskilled forgeries) of a person.

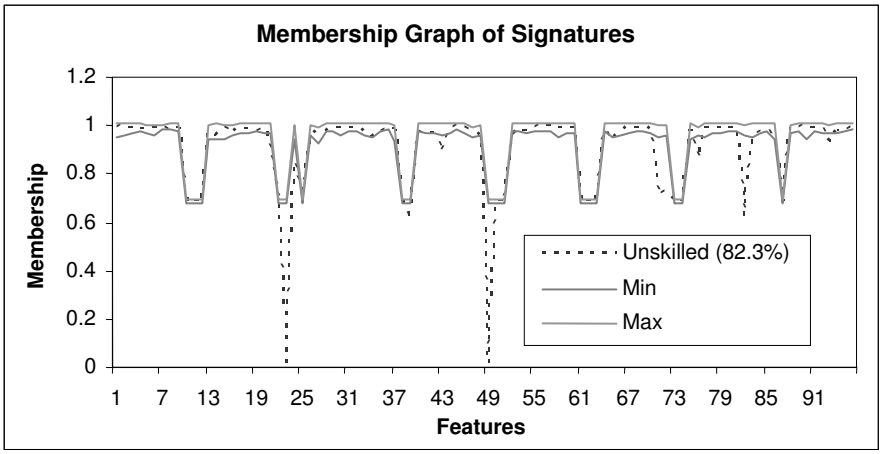
Innovative Approach using variation in MF: In order to know the extent of variation in the genuine signatures, we determine the maximum and minimum membership functions for each feature over all signatures in the training set. The difference between these two gives the inherent variation in the signatures of a person. We add some tolerance to the maximum and delete the same from the minimum so as to increase the range of variation in the different signatures. This tolerance is meant for possible increase in the inherent variation over a time.



(a)



(b)



(c)

Figure 12: Membership graph of (a) genuine (b) skilled forgery and (c) unskilled forgery

We now use the inherent variation to judge the test signatures. We will also explain its utility in the testing phase. For a particular feature, if the membership value lies within the range of variation which is given by the difference of minimum and maximum thresholds, it is counted as 'true'. The total number of 'true' cases for a particular signature is divided by the total number of features (i.e., 96) to get the percentage. For example, in Fig.12a, the test signature has 99% of its features lying well within the threshold as can be seen from the membership

function (i.e., 95 out of 96 features are within the range of inherent variation). The skill-forged and unskilled-forged signatures have corresponding figures of 88.5% (Fig.12b) and 82.3% (Fig.12c) respectively. We set the minimum limit or acceptable percentage for genuine signature at 91% referring to the output result of signature of one particular individual. Signatures that have percentage less than 91% are treated as forged signatures. Table 3 gives the initial values of learning and structure parameters.

Table 3: Initial values of the structural and learning parameters

Parameter	Simplified TS model Initial Values	TS model Initial Values
s	0.1	1
t	1.4	2
c_0	1/96	1/96
c_1	0	0
ε_1	-	0.00000001
ε_2	0.01	0.01
ε_3	0.01	0.01
Precision	**0.01**	**0.01**

Intuitive Approaches taking the average and max of J: Next, we have used the performance index given by Eqn. (12) and its derivatives to adapt the structural parameters during the training phase. These are used to determine the extent of inherent variation in terms of J in the training phase. We have tried two intuitive approaches. In the first case we have taken average J and in the second case we have taken maximum J, both serving as thresholds. The samples in the testing phase are judged by comparing their J values against the thresholds. Table 4(a) summarizes the results of forgery detection using this innovative approach. Tables 4(b) and 4(c) provide the results of forgery detection using the average J and max of J respectively. Comparing these results, we find that the innovative approach yields the best performance.

Table 4 Results using Formulation 1 with fixed consequent coefficients

Signature Type	Total	Accepted	Rejected
(a) J			
Genuine	200	200 (100%)	0 (0%)
Skilled forgery	200	0 (0%)	200 (100%)
Unskilled forgery	200	0 (0%)	200 (100%)
Random forgery	200	0 (0%)	200 (100%)
(b) *Average J*			
Genuine	200	184 (92%)	16 (8%)
Skilled forgery	200	44 (22%)	156 (78%)
Unskilled forgery	200	8 (4%)	192 (96%)
Random forgery	200	0 (0%)	200 (100%)
(c) *Maximum J*			

Genuine	200	200 (100%)	0 (0%)
Skilled forgery	200	42 (21%)	158 (79%)
Unskilled forgery	200	6 (3%)	194 (97%)
Random forgery	200	0 (0%)	200 (100%)

Case 2: TS model with adaptive consequent coefficients

Next, we have used the performance index given in Eqn. (12) and its derivatives to adapt the both consequent coefficients and the structural parameters during the training phase. As mentioned above, we have used both the average and maximum values of J for the detection of forgeries. Tables 5(a) and 5(b) show results using these two thresholds.

Table 5 Results using Formulation 1 with coefficients adapted

Signature Type	Total	Accepted	Rejected
(a) Average J			
Genuine	200	172 (86.0%)	28 (14%)
Skilled forgery	200	47 (23.5%)	153 (76.5%)
Unskilled forgery	200	8 (4%)	192 (96.0%)
Random forgery	200	0 (0%)	200 (100%)
(b) Maximum J			
Genuine	200	200 (100.0%)	0 (0%)
Skilled forgery	200	44 (22%)	156 (78%)
Unskilled forgery	200	6 (3%)	194 (97.0%)
Random forgery	200	0 (0%)	200 (100%)

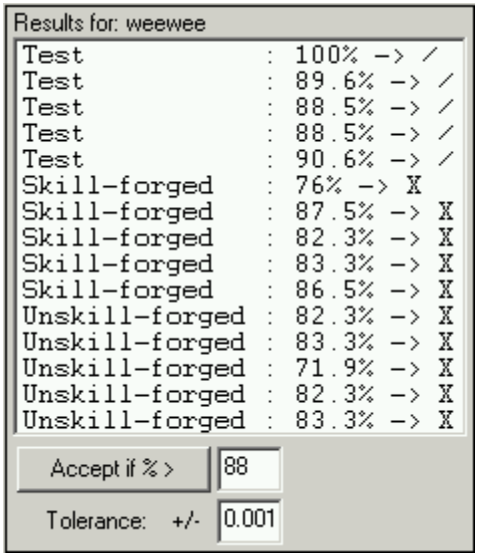
The trained features and structural parameters for one signature set are enumerated in Table 7. For the second formulation involving a single TS rule, the results with consequents fixed are shown in Table 6(a) and results with coefficients adapted are shown in Table 6(b). As compared to the results of the first formulation, these results are not promising for the reasons cited above. Here, we have not made use of the average and maximum values of J.

Table 6 Results using Formulation 2

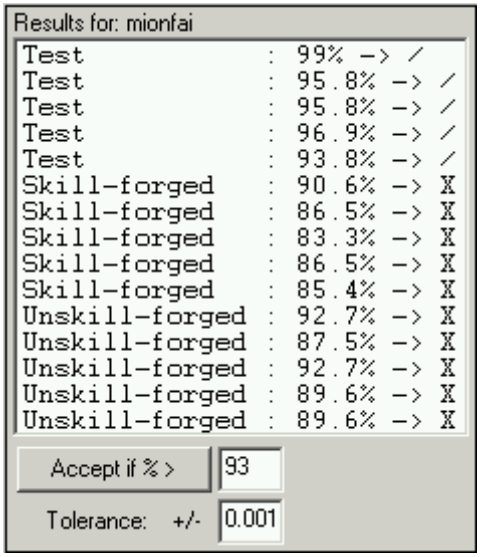
Signature Type	Total	Accepted	Rejected
(a) *Fixed Consequent coefficients*			
Genuine	200	125 (62.5%)	75 (37.5%)
Skilled forgery	200	68 (34%)	132 (66%)
Unskilled forgery	200	51 (25.5%)	149 (74.5)
Random forgery	200	50 (25%)	150 (75%)
(b) *Adapted Consequent coefficients*			
Genuine	200	107 (53.5%)	93 (46.5%)
Skilled forgery	200	84 (42%)	116 (58%)
Unskilled forgery	200	68 (34%)	132 (66%)
Random forgery	200	45 (22.5%)	155 (77.5%)

Table 7 Trained Features and Structural Parameters of one particular signature set

Partition	**Cluster**											
	1	3	3	4	5	6	7	8	9	10	11	12
(a) ***Features of a trained signature sample***												
1	21.1	46.8	38.1	23.9	41.6	40.1	0	0	0	0	0	0
2	0	0	0	44.8	54.8	41.7	24.7	54.5	76.1	0	0	0
3	0	0	40.1	46.9	39.8	0	72.4	60.2	21.0	46.1	56.4	0
4	0	0	30.5	20.5	3.7	49.4	70.2	81.9	58.0	57.5	54.2	0
5	0	0	35.6	12.7	21.3	90	0	0	61.6	63.3	63.3	0
6	0	0	54.7	13.6	26.9	45.6	50.6	79.9	60.9	63.3	60.5	0
7	0	0	36.1	30.1	39.4	33.9	73.4	0	59.6	61.3	59.6	57.4
8	0	0	52.1	90	0	47.1	56.6	30.7	57.4	59.1	63.3	0
(b) ***Parameter 'S'***												
1	0.100523	0.100618	0.100621	0.100581	0.100226	0.100256	0.100698	0.10075	0.10076	0.09998	0.09998	0.09998
2	0.100412	0.10046	0.100436	0.10023	0.100368	0.100492	0.100734	0.100624	0.100479	0.09998	0.09998	0.100392
3	0.09998	0.100263	0.10047	0.100406	0.100626	0.100601	0.10074	0.100735	0.100683	0.100607	0.100696	0.100721
4	0.100365	0.09998	0.09998	0.100569	0.100606	0.100577	0.100444	0.100705	0.100749	0.100417	0.100089	0.100256
5	0.09998	0.09998	0.09998	0.100607	0.100532	0.100555	0.1007	0.100719	0.100721	0.100423	0.10069	0.100703
6	0.09998	0.09998	0.09998	0.10063	0.100585	0.100408	0.100603	0.100619	0.100588	0.10068	0.100156	0.100155
7	0.09998	0.09998	0.100517	0.100134	0.100374	0.100572	0.100638	0.100705	0.100681	0.100157	0.100641	0.100699
8	0.100473	0.100544	0.09998	0.100307	0.100693	0.100689	0.100683	0.100505	0.100149	0.100703	0.100735	0.100764
(c) ***Parameter 'T'***												
1	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.39953	1.39908	1.39911
2	1.38695	1.399945	1.391186	1.4	1.4	1.4	1.4	1.4	1.4	1.39934	1.39932	1.39989
3	1.38929	1.399922	1.399964	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
4	1.39922	1.39908	1.39972	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
5	1.39461	1.39921	1.39989	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
6	1.39558	1.39567	1.39945	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
7	1.39115	1.39229	1.39939	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
8	1.4	1.399631	1.39906	1.4	1.4	1.399985	1.4	1.4	1.4	1.4	1.4	1.4



Genuine signature if 88% and above



Genuine signature if 93% and above

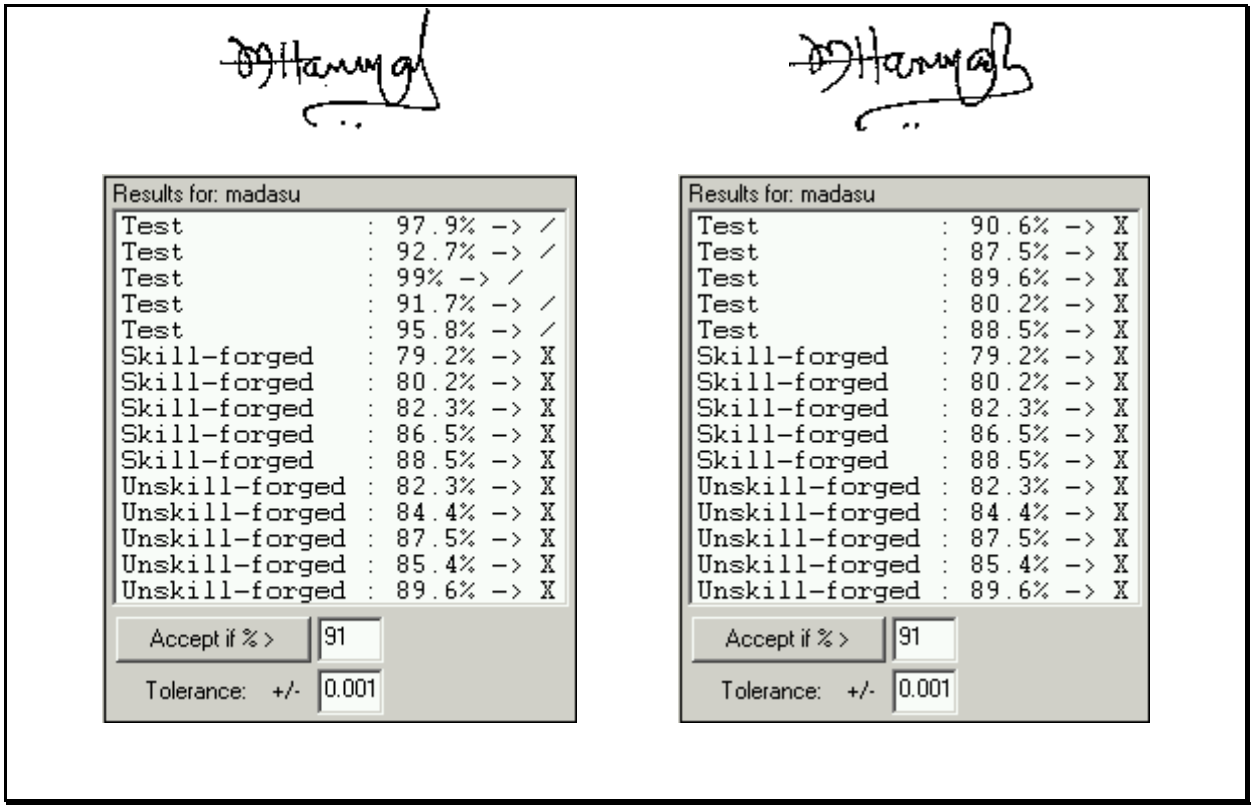
Figure 12: Sample outputs from the program for the signer (a) Weewee (b) Mionfai

Figure 12 shows the sample output of the program for two authors. All the experiments have been carried on a Pentium III, 1.1 GHz Celeron processor having 256MB SDRAM with Windows XP operating system. With this configuration, the system takes about 19 seconds to train 10 signature images while it takes about two seconds to test one signature. Surprisingly, only a single iteration is required to achieve the convergence as the learning parameters and initial structure parameters have been selected optimally.

7.3 Experiments

In this section, we will describe a few experiments which we conducted on the Signature Database using the grid method to test its robustness with respect to scale invariance, continuity and stability.

In the first experiment to test the efficacy of the proposed signature verification system, we have subjected it to a typical assessment. The current signatures of a particular signer, who had changed his signature a few years ago, have been used to train the parameters and thresholds for testing the old signatures. As the old signatures have a slight change at their ends, the verification system declared the old signatures as forged. The sample outputs for the typical case are shown in Fig. 13. This test demonstrates the capability of the system in detecting even the slightest changes in the signature samples, even if they are acquired from the same person who has changed his signature style. This is because of the change in the *s* and *t* parameters which are crucial to the success of the system. It is therefore important to adapt these parameters according to the new reference signatures as the previous values were computed using the old reference signatures.



(a) Current signature of the signer (b) Old signature of the same signer

Figure 13: Sample outputs from system showing that the old signatures are treated as forged when the thresholds of the current signatures are applied

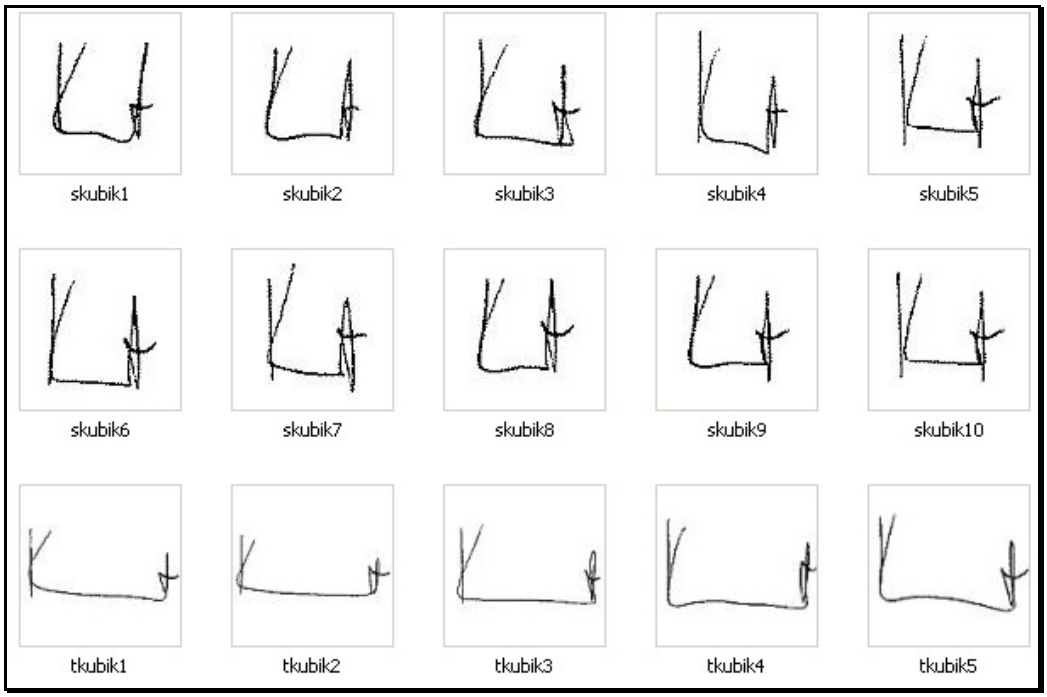


Figure 14: Signature samples of an individual of varying sizes and stroke widths

In the second experiment, we have taken signatures of different sizes of the same person to test the effectiveness of the signature grid which encompasses the signature samples (See Fig. 14). We have also analysed the effect of an elongated signature grid whenever the width of the signature strokes extends beyond the normal signing style. This can easily happen as some of the extreme features of the signature may alter from time to time depending on the width of the signature strokes. For this purpose we have taken signature samples of varying stroke widths and used them as test signatures for computing the recognition accuracies. It has been observed that even after size normalization; the inherent features of a person's signature are preserved, as the recognition rates come out to be near perfect. This particular characteristic of the system is vital for the success of a commercial signature verification system because of the tendency of signers to sign their names with varying stroke widths depending on the availability of space for putting the signature.

8 Conclusions

In this chapter, an offline signature verification and forgery system based on additive fuzzy modelling is presented. The handwritten signatures images are pre-processed and angle features extracted from them via a novel grid method. These features are then modelled using the Takagi-Sugeno fuzzy model, which involves two structural parameters in its exponential membership function. Each angle feature yields a fuzzy set when its values are gathered from all samples because of the variations in handwritten signatures. Two cases are considered. In the first case, the coefficients of the consequent part of the rule are fixed so as to yield a simple form of TS model and in the second case the coefficients are adapted. In this formulation, each rule is constituted by a single feature. In the second formulation, we consider only one rule encompassing all the features. Here again, we have derived two models depending on whether coefficients of the consequent part are fixed or adapted. However, this formulation is not implemented as the membership values are found to be very small for some fuzzy sets. The efficacy of this system has been tested on a large database of signatures. The verification system achieved 100% success in verifying genuine signatures and detecting all types of forgeries: random, unskilled and skilled on a signature database consisting 1200 signature samples. Simple form of TS model in the first formulation is found to be better than that with coefficients adapted. We have also demonstrated the effectiveness of the intuitive approach for signature verification over other approaches using the performance index.

References

[1] Ammar M., Yoshida, Y., &. Fukumura, T. (1990). Structural description and classification of signature images. *Pattern Recognition*, *23*, 697-710.

[2] Ammar, M. (1991). Progress in verification of skilfully simulated handwritten signatures. *International Journal of Pattern Recognition and Artificial Intelligence*, *5*(1-2), 337-351.

[3] Bajaj, R., & Chaudhury, S. (1997). Signature verification system using multiple neural classifiers. *Pattern Recognition*, *30*(1), 1-7.

[4] Blatzakis, H., & Papamarkos, N. (2001). A new signature verification technique based on a two-stage neural network classifier. *Engineering Applications of Artificial Intelligence*, *14*, 95-103.

[5] Cardot, H., Revenu, M., Victorri, B., & Revillet, M.J. (1994). A Static Signature Verification System based on a Cooperating Neural Networks Architecture. *International Journal of Pattern Recognition and Artificial Intelligence*, *8*(3), 679-692.

[6] Deng, P.S., Liao, H-Y.M., Ho, C.W. & Tyan, H-R. (1999). Wavelet based Off-line Handwritten Signature Verification. *Computer Vision and Image Understanding*, *76*(3), 173-190.

[7] Drouhard, J.P., Sabourin, R., & Godbout, M. (1996). A Neural Network Approach to Off-line Signature Verification using Directional PDF. *Pattern Recognition*, *29*(3), 415-424.

[8] el-Yacoubi, A., Justino, E.J.R., Sabourin, R., & Bortolozzi, F. (2000). Off-line signature verification using HMMS and cross-validation. In *Proceedings of Ninth IEEE Workshop on Neural Networks for Signal Processing* (pp. 859-868).

[9] Fadhel, E.A., &. Bhattacharyya, P. (1999). Application of a steerable Wavelet Transform using Neural Network for Signature Verification. *Pattern Analysis and Applications*, *2*, 184-195.

[10] Fang, B., Leung, C.H., Tang, Y.Y., Tse, K.W., Kwok, P.C.K., & Wong, Y.K. (2003). Offline signature verification by tracking of feature and stroke positions," *Pattern Recognition*, *36*, 91-101.

[11] Harrison, W.R. (1958). *Suspect Documents: Their Scientific Examination*. Sweet & Maxwell Ltd., London.

[12] Hilton, O. (1992). Signatures - Review and a New View. *Journal of Forensic Sciences*, *37*(1), 125-129.

[13] Ismail, M.A. & Gad, S. (2000). Off-line Arabic signature recognition and verification. *Pattern Recognition*, *33*(10), 1727-1740.

[14] Justino, E.J.R., Bortolozzi, F. & Sabourin, R. (2001). Offline signature verification using HMM for random, simple and skilled forgeries. In *Proceedings of sixth IEEE International Conference on Pattern Recognition*, (pp. 450-453).

[15] Lee, S. & Pan, J.C. (1992). Offline tracing and representation of signatures. *IEEE Transactions on Systems, Man and Cybernetics*, *22*(4), 755-771.

[16] Locard, E. (1936). *Traité de Criminalistique*. Payoy, Lyon.

[17] Murshed, N.A., Sabourin, R., & Bortolozzi, F. (1997). A cognitive approach to offline signature verification. In H. Bunke and P.S.P. Wang (Ed.), *Automatic Bankcheck Processing*, (pp. 339-364). Singapore: World Scientific Publishing.

[18] Nagel, R.N. & Rosenfeld, A. (1977). Computer Recognition of freehand forgeries. *IEEE Transactions on Computers*, *26*(9), 895-905.

[19] Nemcek, W.F., & Lin, W.C. (1974). Experimental investigation of Automatic Signature Verification. *IEEE Transactions on Systems, Man and Cybernetics*, *4*, 121-126.

[20] Osborn, A.S. (1929). *Questioned Documents*, New York: Boyd Printing.

[21] Plamondon, R., & Lorette, G. (1989). Designing automatic signature verification and writer identification – The state of the art. *Pattern Recognition*, *2*(2), 107-131.

[22] Pender, D.A. (1991). *Neural Networks and Handwritten Signature Verification*. Doctoral dissertation, Stanford University.

[23] Qi, Y. & Hunt, B.R. (1994). Signature verification using global and grid features. *Pattern Recognition*, *27*(12), 1621-1629.

[24] Quek, C., & Zhou, R.W. (2002). Antiforgery: a novel pseudo-outer product based fuzzy neural network driven signature verification system. *Pattern Recognition Letters*, *23*(14), 1795-1816.

[25] Rigoll, G., & Kosmala, A. (1998). A Systematic Comparison between On-line and Off-line Methods for Signature Verification with Hidden Markov Models. In *Proceedings of the 14th International Conference on Pattern Recognition*, (pp.1755-1757).

[26] Sabourin, R., Genest, G., & Prêteux, F.J. (1997). Off-Line Signature Verification by Local Granulometric Size Distributions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *19*(9), 976-988.

[27] Shih, F.Y. & Wong, W-T. (1995). A new safe-point thinning algorithm based on the mid-crack code tracing. *IEEE Transactions on Systems, Man and Cybernetics*, *25*(2), 370 – 378.

[28] Suen, C.Y., Xu, Q., & Lam, L. (1999). Automatic recognition of handwritten data on cheques – Fact or Fiction? *Pattern Recognition Letters*, *20*, 1287-1295.

[29] Takagi, T. & Sugeno, M. (1985). Fuzzy identification of systems and its application to modeling and control. *IEEE Transactions on System, Man and Cybernetics*, *15*, 116-132.

[30] Xiao, X., & Leedham, G. (2002). Signature verification using a modified Bayesian network. *Pattern Recognition*, *35*(5), 983-995.