

# Automatic Handwritten Signature Verification system for Australian Passports

Vamsi K. Madasu, Brian C. Lovell & Kurt Kubik  
*School of ITEE, University of Queensland, Australia*

**ABSTRACT:** We present an automatic handwritten signature verification system to prevent identity fraud by verifying the authenticity of signatures on Australian passports. In this work, fuzzy modeling has been employed for developing a robust recognition system. The knowledge base consists of unique angle features extracted using the box method. These features are fuzzified by an exponential membership function, consisting of two structural parameters which have been devised to track even the minutest variations in a person's signature. The membership functions in turn constitute the weights in the Takagi-Sugeno (TS) model. The optimization of the output of the TS model with respect to the structural parameters yields the solution for the parameters. The efficacy of the proposed system has been tested on a large database of over 1200 signature images obtained from 40 volunteers achieving a recognition rate of more than 99%.

## 1 INTRODUCTION

### 1.1 Problem Background

The trade in the illegal movement of people, the threat of international terrorism, and the ready availability of high tech equipment, underscore the need for close attention to the questions of identity integrity and security in the Australian passport issuing and scanning process. Identity fraud is a growing threat world-wide, posing risks of an increasing level and range of criminal activity. According to the Passports Australia-Achievements and Challenges yearbook (2001-2002), forgery alone accounted for 31% of the total cases detected which posed a threat to the integrity of the Australian passport. Fraud threats to the Australian passport fall into two main areas:

- Abuse in the application stage, for example, through the production of false identity documents or the assumption of another person's identity by forging the signature or consent of a legal resident.
- Abuse of the document after issue, such as substitution of the photograph, alteration of the bio data page, or forgery of the genuine signature by an impostor.

We wish to combat this kind of fraudulent activity and assist in the prevention of fraud against the Australian passport system by designing fool proof signature verification and forgery detection systems. This system can be used for verification of signatures on Australian passports, provided that a database of sample signatures of all legal Australian citizens is available. Once developed, it can be employed at Australian sea and air ports for scanning travel documents which then could be checked against databases to determine whether the individual should be detained or questioned concerning possible terrorist or criminal involvement.

Signature verification and forgery detection relate to the process of verifying signatures automatically and instantly to determine whether the signature is genuine or forged. There are two main types of signature verification: static and dynamic. Static or off-line verification is the process of verifying an electronic or paper signature after it has been made, while dynamic or on-line verification takes place as a subject creates his signature on a digital tablet or a similar device. The signature in question is then compared to previous samples of the signer's signature, which constitute the database or knowledge base. In the case of an ink signature on paper, the computer requires the sample to be scanned for analysis, whereas a digital signature is already stored in a data format that signature verification can use.

As compared to on-line signature verification systems, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature image only. Although difficult to design, off-line signature verification is crucial for determining the identification of the writer as most of the signatures are still signed on the paper. Therefore, it is very important to verify paper based signatures in security systems.

### 1.2 Literature Review

Automated recognition of handwritten signatures became imperative when it was difficult to distinguish genuine signatures from simulated forgeries on the basis of visual assessment. This led to computer recognition of handwritten signatures which although not perfect, is quite reliable and efficient. Automatic examination of questioned signatures did not come into being until the advent of computers in

the 1960s. As computer systems became more powerful and more affordable, designing an automatic signature verification and forgery detection system became an active research subject.

The design of any signature verification system generally requires the solution of five sub-problems: data acquisition, pre-processing, feature extraction, comparison process and performance evaluation (Plamondon & Lorette 1989). Surveys of the state of the art off-line signature verification systems designed up to 1993 appear in Plamondon & Leclerc 1994 and Sabourin et al. 1992. Another survey article (Plamondon & Srihari 2000) has summarized the approaches used for off-line signature verification from 1993-2000. Most of the work in off-line forgery detection, however, has been on random or simple forgeries and less on skilled or simulated forgeries. Before looking into the landmark contributions in the area of signature verification & forgery detection, we briefly enumerate the types of forgeries as follows:

- 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. This forgery accounts for the majority of the forgery cases although they are very easy to detect even by the naked eye.
- 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 – undoubtedly 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.

In the 1980's, Ammar et al. 1986 started the work on the detection of different kinds of forgeries. Apart from introducing a method for separation of signatures from noisy backgrounds, this paper was one of the first of its kind which tried to solve the problem of simulated or skilled forgeries based on the shape and density features of the signatures. They calculated the statistics of dark pixels and used them to identify changes in the global flow of the writing. The later work of Ammar et al. 1990 is based on reference patterns, namely the horizontal and vertical positions of the signature image. The projection of the questioned signature and the reference are compared using Euclidean distance. They also compared the performances of parametric and reference pattern based features in the verification of skillfully simulated handwritten signatures.

Over the next few years, many researchers used neural networks and their variants for static signature verification. For example, Sabourin and Drouhard 1992, employed neural networks to classify signature images with the probability density func-

tion of the stroke directions serving as a global characteristics vector. Neural networks offers an advantage over other techniques as the system is trained to perform class separation through a continuous process of learning but this requires a large number of signature samples for training which may not be possible in a commercial environment. Guo et al. 2002 on the other hand, presented an algorithm for the detection of skilled forgeries based on a local correspondence between a questioned signature and a model obtained a priori. Writer-dependent properties are measured at the sub-stroke level and a cost function is trained for each writer.

Hidden Markov Models were also explored in the field of signature verification. El-Yacoubi et al. 2000 presented a HMM based approach to dynamically and automatically derive the author dependent parameters in order to set up an optimal decision rule for off-line verification process. The cross validation principle is used to obtain not only the best HMM models, but also an optimal acceptance/ rejection threshold for each author. This threshold led to a high discrimination between the authors and impostors in the context of random forgeries but was not successful for other kind of forgeries.

In the latter half of 1990s, fuzzy modeling started becoming popular among document processing researchers owing to its ability to classify uncertain and fuzzy data. Ismail & Gad 2000 proposed an off-line signature verification system based on fuzzy concepts for the verification of Arabic signatures. Signature verification was also attempted using the Pseudo- Bacterial Genetic Algorithm (Xuhua et al. 1995) which was applied for the discovery of fuzzy rules. The rules are units themselves and they are constituted by several parameters to be optimized, however, the performance of a fuzzy system is obtained synergistically as a sum of the outputs of several rules. The PBGA was then applied for the extraction of personal features for signature verification.

Fuzzy Modeling techniques were further used in conjunction with neural networks for achieving higher recognition rates. A pseudo-outer product based fuzzy neural network drives the signature verification system of Quek & Zhou 2000 which was primarily developed for verifying skilled forgeries. Signature verification using Takagi-Sugeno fuzzy-model is reported in Hanmandlu et al. 2001 and features for this model are drawn from the box approach of Hanmandlu et al. 2003. In the present work, we adapt the same methodology with major modifications. We also consider the TS model for recognition but have modified it with the addition of structural parameters to enhance its capability in the detection of skilled forgeries.

### 1.3 Overview of the paper

In the following sections, we will describe in detail each module of the signature verification & forgery detection system which we have designed. In the initial phase, acquired signatures are pre-processed involving size normalization, binarization and thinning before features are extracted from each of them. These features constitute the knowledge base, which is then used for verifying the genuine signatures and detecting the forgeries. Next is the crucial step of verification where we compare the features of the extracted signature with the features of the reference signatures. But since we all know that no two signatures of the same person are same, we formulate a recognition mechanism which allows for some inter-signature variation but rejects intra-signature variations. Section five tabulates the experimental results on the database of signature images. Finally, the conclusions are presented in section six.

## 2 SYSTEM DESCRIPTION

### 2.1 Data Acquisition

The proposed fuzzy modeling based technique discussed above has been applied on a signature database, developed in our school. The signature database consists of a total of 1200 handwritten signature images. Out of these, 600 were authentic signatures and others were forged ones. These signatures were obtained from 40 volunteers with each of them contributing 15 signatures. This set of 40 individuals represented a fair sample of the general population with volunteers coming from different age-groups, genders and ethnicities.

The signatures were handwritten on a sheet of paper having 25 boxes of fixed size so as to create a uniform database of signatures of different subjects. The signature images were then scanned at a resolution of 200 dpi and re-sampled/resized by 50% using a B-Spline filter in IrfanView. IrfanView is a very fast, small, compact and innovative freeware graphic viewer for Windows 9x/ME/NT/2000/XP. A few signatures and their forgeries are shown in Figure 1.

The signatures were collected in multiple sessions which were spaced over a period of a few weeks to account for variations in the signature with time. The forgeries of these signatures were collected over a similar time frame. The random forgeries were obtained by supplying only the names of the individuals to the casual forgers who did not have any access to the actual genuine signatures. The unskilled forgeries, in turn, were obtained by providing sample genuine signatures to the forgers who were then allowed to practice for a while before imitating them to create the forged signatures. Each volunteer had to provide five imitations of any one of the genuine signatures, apart from his or her own signatures.

These samples constituted the set of unskilled forged signatures for the set of genuine signatures. We then requisitioned the services of a few expert forgers who provided five forgeries of each genuine signature in the test set to create the skilled forged samples of all the persons. These people who wished to remain anonymous have previously been involved in signature forgery cases.

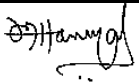
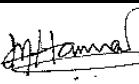
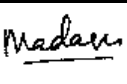
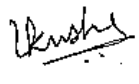

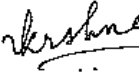
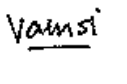

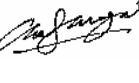

GENUINE	SKILLED FORGERY	UNSKILLED FORGERY	RANDOM FORGERY
			
			
			

Figure 1. Some examples of signatures and their forgeries

### 2.2 Pre-processing of Signatures

Pre-processing of scanned signatures is necessary before feature extraction. In the present system, all the signature images are first resized to a fixed window of size (120 × 60 pixels), then binarized and thinned using the modified SPTA thinning algorithm (Hanmandlu et al. 2001). Features are then extracted from this pre-processed signature image for the creation of the knowledge base.

### 2.3 Feature Extraction

The pre-processed image is then 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 is illustrated in Figure 2 and explained in the following paragraphs.

For example, let the total number of dark pixels in a signature be 48. If we partition the signature into four parts, we should get 12 pixels per partition. However, since the partitioning is done column wise, getting exactly 12 points in each partition is not possible. Therefore, we will take approximately 12 points in each partition using a two-way scanning approach as described below. 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 and then take the average of the two column numbers in each partition to get almost equal partitions.

Each partition is now resized to a fixed window or box of  $38 \times 60$  pixels size and is thinned again. Each box is again divided into 4 rows  $\times$  3 columns, constituting 12 boxes. In total we have 96 partitions for a single signature. The idea behind this method is to collect the local information contained in the box. This method evolved from the earlier ring and sector techniques which were fraught with the problem of revolving centroid. The centroid was treated as the reference point with respect to which the local information contained in a ring or a sector was collected. In the box method any corner point can be chosen as the reference point. The information can be gathered in the form of normalized distances and angles. For the present problem of signature verification and forgery detection, we have experimented with both distance distributions and angle distributions. We have found that the angle distribution has gives better results as compared to distance distribution which is more linear in nature. Hence, the choice fell on extracting angle information from the boxes. For this, we calculate the summation of the angles of all points in each box with respect to the bottom left corner of the box, which is taken as the reference. The summation of angles is normalized with the number of pixels in the box. These angles constitute the feature database for a given signature

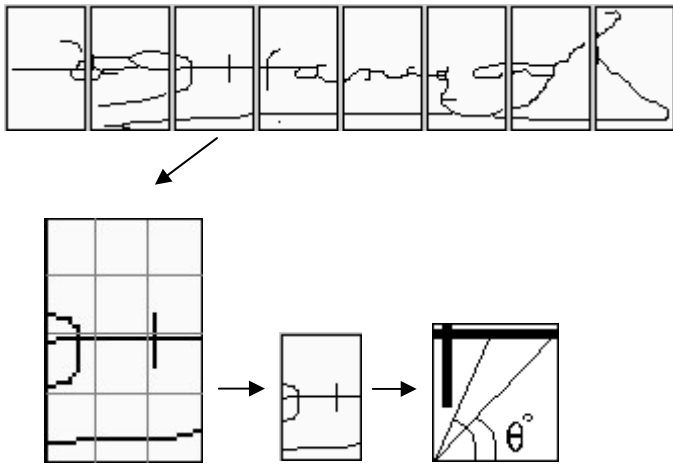


Figure 2. Feature Extraction Procedure

### 3 SIGNATURE VERIFICATION

#### 3.1 Problem Formulation

Since the main aim of this research is to establish the authenticity of handwritten signatures by verifying the genuine signatures and rejecting the forged ones, we opt for fuzzy modeling of the angle features. For this purpose, we have added two structural parameters to the Takagi-Sugeno (TS) fuzzy model. These parameters are quite helpful in tracking the varia-

tions in a person's handwriting style thereby leading to better rejection of skilled forgeries. We also consider that each feature forms a fuzzy set over large samples as the same feature exhibits variation in different samples giving rise to a fuzzy set. So, our attempt is to model this uncertainty through a fuzzy model such as the TS model.

Let  $x_k$  be the  $k^{\text{th}}$  feature in a fuzzy set  $A_k$ , so the  $k^{\text{th}}$  fuzzy rule IF THEN rule in TS model has the following form

$$\begin{aligned} \text{Rule } k: \quad & \text{IF } x_k \text{ is } A_k \\ & \text{THEN } y_k = c_{k0} + c_{k1}x_k \end{aligned} \quad (1)$$

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

$$\mu_k(x_k) = \exp\left[-\frac{(1-s_k) + s_k^2 |x_k - \bar{x}_k|}{(1+t_k) + t_k^2 \sigma_k^2}\right] \quad (2)$$

where  $\bar{x}_k$  is the mean &  $\sigma_k^2$  is the variance of  $k^{\text{th}}$  fuzzy set.

Note that the inclusion of these parameters will help track the variations in the handwriting of signatures. When,  $s_k = 1$  and  $t_k = -1$ , the MF is devoid of structural parameters and hence it is solely governed by the mean and variance. The justification for the modified MF is two-fold: Easy to track variations over mean and variance, and no need of sophisticated learning technique. The numerator and denominator of exponential function in Equation 2 contains a constant term (i.e., 1) plus a function of parameter and the known variation (i.e., either change in mean or in variance). This choice is guided by the consideration of no role for parameters if the signatures of a person don't change. But this need not be the case for other applications. The strength of the rule in Equation 1 is obtained as,

$$w_k = \mu_k(x_k) \quad (3)$$

The output is expressed as,

$$Y = \sum_{k=1}^L w_k y_k \quad (4)$$

where, L is the number of rules.

We define the performance function as

$$J = (Y_r - Y)^2 \quad (5)$$

where Y &  $Y_r$  denote the output of the fuzzy model and of the real system respectively. If  $Y_r$  not available, it can be assumed to be unity.

### 3.2 Parameter Learning

In order to learn the parameters involved in the membership function (i.e.,  $s_k$  &  $t_k$ ) and the consequent parameters  $c_{k0}$  &  $c_{k1}$ . Equation 5 is partially differentiated with respect to each of these parameters. Accordingly, we have

$$\frac{\partial J}{\partial c_{k1}} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial y_k} \cdot \frac{\partial y_k}{\partial c_{k1}} = 2(Y - Y_r) w_k x_k \quad (6)$$

$$\frac{\partial J}{\partial c_{k0}} = \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial y_k} \cdot \frac{\partial y_k}{\partial c_{k0}} = 2[Y - Y_r] w_k = 2\delta w_k \quad (7)$$

$$\begin{aligned} \frac{\partial J}{\partial s_k} &= \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial w_k} \cdot \frac{\partial w_k}{\partial t_k} \\ &= 2(Y - Y_r) \cdot y_k \cdot \frac{\mu_k \left\{ 1 - 2s_k \left| x_k - \bar{x}_k \right| \right\}}{\left\{ (1 + t_k) + t_k^2 \sigma_k^2 \right\}} \\ &= 2\delta y_k \mu_k \left[ \left\{ 1 - 2s_k \left| x_k - \bar{x}_k \right| \right\} / T \right] \end{aligned} \quad (8)$$

$$\begin{aligned} \frac{\partial J}{\partial t_k} &= \frac{\partial J}{\partial Y} \cdot \frac{\partial Y}{\partial w_k} \cdot \frac{\partial w_k}{\partial t_k} \\ &= 2(Y - Y_r) y_k \mu_k \frac{\left\{ (1 - s_k) + s_k^2 \left| x_k - \bar{x}_k \right| \right\} \left\{ 1 + 2t_k \sigma_k^2 \right\}}{\left\{ (1 + t_k) + t_k^2 \sigma_k^2 \right\}^2} \\ &= 2\delta y_k \mu_k \left\{ (1 - s_k) + s_k^2 \left| x_k - \bar{x}_k \right| \right\} \left\{ 1 + 2t_k \sigma_k^2 \right\} / T^2 \end{aligned} \quad (9)$$

where  $\delta = Y - Y_r$ ,  $T = (1 + t_k) + t_k^2 \sigma_k^2$  &  $k = 1, \dots, L$  denotes the rule number.

We use the gradient descent learning for the parameters as follows:

$$c_{ki}^{new} = c_{ki}^{old} - \epsilon_1 \frac{\partial J}{\partial c_{ki}} \quad i = 0, 1 \quad (10)$$

$$s_k^{new} = s_k^{old} - \epsilon_2 \frac{\partial J}{\partial s_k} \quad (11)$$

$$t_k^{new} = t_k^{old} - \epsilon_3 \frac{\partial J}{\partial t_k} \quad (12)$$

where  $\epsilon_1, \epsilon_2, \epsilon_3$  are the learning coefficients such that  $\epsilon_1, \epsilon_2$  and  $\epsilon_3 > 0$ .

### 3.3 Parameter Updating

We can go for global learning when we have large sets of data, say,  $M$ . This is known as the batch learning scheme, in which change in any parameter is governed by the equation:

$$\Delta w(q) = \sum_{j=1}^M \Delta_j w(q) + \alpha_m \Delta w(q-1) - \gamma w(q) \quad (13)$$

and the parametric update equation is;

$$w(q+1) = w(q) + \Delta w(q) \quad (14)$$

where  $w$  in Equation 13 may stand for any of the parameters  $c_{ki}, s_k, t_k$  and  $q$  is the  $q^{\text{th}}$  epoch,  $\alpha_m$  is a momentum coefficient in the limits  $0 \leq \alpha_m < 1$  (typically  $\alpha_m = 0.9$ ),  $\gamma$  is a decay factor (typically in the range of  $10^{-3}$  to  $10^{-6}$ ).

We can obtain initial  $\Delta w(q)$  from Equations 10-12 by computing the partial derivatives of  $J$ . For this, assume  $c_{k0} = 1/L$  and  $c_{k1} = 0$  so that  $y_k = 1/L$  in Equation 1. Substituting this in Equation 4 yields

$$Y = \frac{1}{L} \sum_{i=1}^L \mu_i \quad (15)$$

In the above equation,  $Y$  is given by the average of the membership functions. It is now proved that the average membership function (MF) is a special case of TS model. The recursive Equations 10-12 have to be iterated until the summation of  $\delta$  for all feature values is small enough. The initial values of the structural parameters are obtained from:

$$\frac{\partial J}{\partial s_k} = 0 \Rightarrow 1 - 2s_k \left| x_k - \bar{x}_k \right| = 0 \Rightarrow s_k = \frac{1}{2 \left| x_k - \bar{x}_k \right|} \quad (16)$$

$$\frac{\partial J}{\partial t_k} = 0 \Rightarrow 1 + 2t_k \sigma_k^2 = 0 \Rightarrow t_k = -\frac{1}{2\sigma_k^2} \quad (17)$$

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

## 4 RECOGNITION APPROACH

It is a well known fact that any automatic signature verification system requires a very small training set of signatures. For this reason, we have set the number of training signatures for each individual at ten.

*TS model with consequent coefficients fixed:* If we take,  $Y_r = 1$ , then Equation 5 becomes

$$J = \left( 1 - \frac{1}{L} \sum_{i=1}^L \mu_i \right)^2 \quad (18)$$

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  $t_i$ ;  $i=1,\dots,96$ . Using these values, we compute the membership functions for all the features. This process is repeated for all training samples 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.

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 Figure 3(a), 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 un-skill forged signatures have corresponding figures of 88.5% (Figure 3b) and 82.3% (Figure 3c) respectively. We set the minimum limit or acceptable percentage for genuine signature at 91% referring to the output result of signature of a signer. Signatures that have percentage less than 91% are treated as forged signatures. Table 2 summarizes the results of forgery detection using this innovative approach.

## 5 EXPERIMENTAL RESULTS

The proposed fuzzy modeling techniques were implemented on the signature database described in section 2. The system was trained with only genuine signatures as forged samples of a genuine signature are readily available in the real-world scenario, i.e. the system learned only from the training data for a specific individual. The number of training signatures for each individual was set at ten. The signature database with the number of samples considered from different classes is detailed in Table 1.

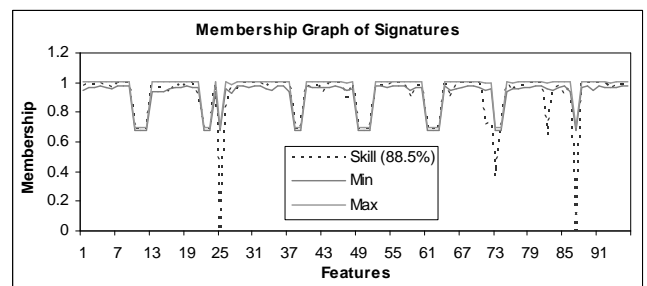
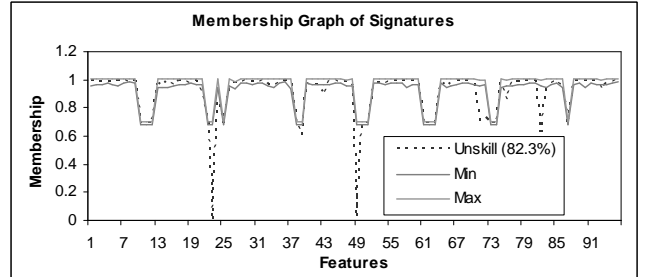
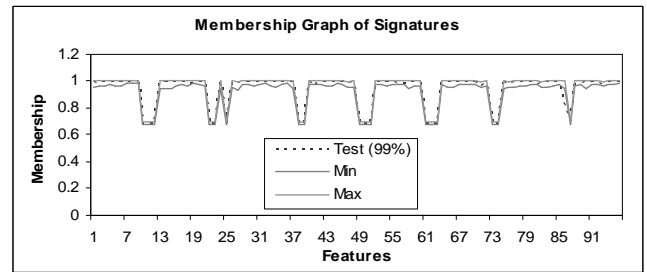


Figure 3 a-c. Membership Graphs of Different Samples

Table 1. Signature Database

Type	Training Set	Testing Set	Total
<i>Genuine</i>	40 × 10	40 × 5	600
<i>Skilled forgeries</i>	-	40 × 5	200
<i>Unskilled forgeries</i>	-	40 × 5	200
<i>Random forgeries</i>	-	40 × 5	200

All the experiments were conducted on a Pentium IV, 1.1GHz processor having 256MB SDRAM with Windows XP operating system. With this configuration, the system takes about 19 seconds to train 10 signature images and around 2 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.

Our system achieved a recognition rate of 99.84% on a database of 1200 signatures with just 2 skilled forgeries being accepted as genuine signatures. All other forgeries were correctly classified. The choice of initial parameters is important in the recognition phase but not crucial. Presently, we have fixed the initial values which are applicable to all types of signatures.

Table 2. Results of Verification

	Total	Accepted	Rejected
<b>Genuine Signatures</b>	200	200	0
<b>Skilled forgery</b>	200	2	198
<b>Unskilled forgery</b>	200	0	200
<b>Random forgery</b>	200	0	200

In the field of off-line signature verification, no standard international database is available due to confidentiality and privacy issues thus making the process of comparative analysis very difficult. We have tried to demonstrate the superiority of our method in contrast to other systems given in the literature by implementing three other methods on our signature database. It can be clearly observed from Table 3 that our method achieves the best results amongst all others thereby proving the superiority of our signature verification system.

Table 3. Comparative Analysis of different off-line signature verification systems

Authors	Method	Results
Ammar, M. 1991	Distance Threshold	85.94%
Ammar et al., 1990	Distance Statistics	88.15%
Quek & Zhou, 2002	Neuro-Fuzzy Network	96%
Madasu et al., 2005	Modified TS Model	99.84%

## 6 CONCLUSIONS

An automatic handwritten signature verification and forgery detection system for authenticating signatures is presented. The system is based on Takagi-Sugeno fuzzy model and involves structural parameters in its exponential membership function. The features consisting of angles are extracted using box approach. Each feature yields a fuzzy set when all the training samples are considered because of the variations in a person's signatures. We have also devised an innovative formulation where a single feature constitutes one rule. We have also demonstrated the effectiveness of an innovative approach using variation in the membership function and incorporation of the values of performance index  $J$  in the decision making.

The efficacy of this system has been tested on a large database of signatures. The verification system is not only able to verify genuine signatures but also detects all types of forgeries: random, unskilled and skilled with utmost precision. Such a system can be integrated with present security systems for verifying signatures obtained from Australian passports thus preventing identity fraud and protecting the integrity of the Australian passport system.

## 7 REFERENCES

- Ammar, M., Yoshida, Y. & Fukumura, T. 1986. A new effective approach for off-line verification of signatures by using pressure features. In: *Proceedings of the International Conference on Pattern recognition*.
- Ammar, M., Yoshida, Y. & Fukumura, T. 1990. Structural Description & Classification of Images. *Pattern Recognition*, 23(7): 697-710.
- Ammar, M. 1991. Progress in verification of skillfully simulated handwritten signatures. *International Journal of Pattern Recognition and Artificial Intelligence*, 5: 337-351.
- El-Yacoubi, A., Justino, E.J.R., Sabourin, R. & Bortolozzi, F. 2000. Off-line signature verification using HMMS and cross-validation. In: *Proceedings of IEEE Workshop on Neural Networks for Signal Processing*.
- Guo, J.K., Doermann, D. & Rosenfeld, A. 2000. Off-line skilled forgery detection using stroke and sub-stroke properties. In: *Proceedings of the International Conference on Pattern Recognition*.
- Hanmandlu, M., Mohan, K.R.M., Chakraborty, S., Goel, S. & Roy Choudhury, D. 2003. Unconstrained handwritten character recognition based on fuzzy logic. *Pattern Recognition*, 36(3): 603-623.
- Hanmandlu, M., Mohan, K.R.M., Chakraborty, S. & Garg, G. 2001. Fuzzy modeling based signature verification system. In: *Proceedings of Sixth International Conference on Document Analysis and Recognition*.
- Hanmandlu, M., Mohan, K.R.M. & Gupta, V. 1997. Fuzzy logic based character recognition. In: *Proceedings of the International Conference on Image Processing*, Santa Barbara, USA.
- Ismail, M.A. & Gad, S. 2000. Off-line Arabic signature recognition and verification. *Pattern Recognition*, 33(10):1727-1740.
- Plamondon, R. & Leclerc, F. 1994. Automatic signature verification: the state of the art 1989-1993. *International Journal of Pattern Recognition and Artificial Intelligence*, 8(3): 643-660.
- Plamondon, R. & Lorette, G. 1989. Automatic signature verification and writer Identification: the state of the art. *Pattern Recognition*, 22(3): 107-131.
- Plamondon, R. & Srihari, S.N. 2000. On-line and off-line Handwriting Recognition: A Comprehensive Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 22(1) : 63-84.
- Sabourin, R., Plamondon, R. & Lorette, G. 1992. Off-line identification with handwritten signature images: Survey and Perspectives. In *Structured Image Analysis*: 219-234, New York: Springer-Verlag.
- Sabourin, R. & Drouhard, J.P. 1992. Off-Line Signature Verification using Directional PDF and Neural Networks, In: *Proceedings of the 11<sup>th</sup> International Conference on Pattern Recognition*.
- Quek, C. & Zhou, R.W. 2002. Antiforgery: a novel pseudo-outer product based fuzzy neural network driven signature verification system. *Pattern Recognition Letters*, 23: 1795-1816.
- Xuhua, Y., Furuhashi, T., Obata, K. & Uchikawa, Y. 1995. Study on signature verification using a new approach to genetic based machine learning. In: *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, USA.