International Journal of Innovative Computing, Information and Control
Volume **7**, Number **5(B)**, May **2011**
ICIC International ©2011 ISSN 1349-4198
pp. 2709–2726

FUSION OF MULTI-CLASSIFIERS FOR ONLINE SIGNATURE VERIFICATION USING FUZZY LOGIC INFERENCE

Marzuki Khalid, Rubiyah Yusof and Hamam Mokayed

Universiti Teknologi Malaysia
Center for Artificial Intelligence and Robotics (CAIRO)
Jalan Semarak, 54100 Kuala Lumpur, Malaysia
rubiyah@ic.utm.my; marzuki@utm.my

Received January 2010; Revised June 2010

Abstract. *Compared to physiologically based biometric systems such as fingerprint, face, palm-vein and retina, behavioral based biometric systems such as signature, voice, gait, etc. are less popular and many of the research in these areas are still in their infancy. One of the reasons is due to the inconsistencies in human behavior which requires more robust algorithms in their developments. In this paper, an online signature verification system is proposed based on fuzzy logic inference. To ensure higher accuracy, the signature verification system is designed to include the fusion of multi classifiers, namely, the back propagation neural network algorithm and the Pearson correlation technique. A fuzzy logic inference engine is also designed to fuse two global features which are the time taken to sign and the length of the signature. The use of the fuzzy logic inference engine is to overcome the boundary limitations of fixed thresholds and overcome the uncertainties of thresholds for various users and to have a more human-like output. The system has been developed with a robust validation module based on Pearson's correlation algorithm in which more consistent sets of signatures are enrolled. In this way, more consistent sets of training patterns are used for training. The results show that the incorporation of multi classifier fusion technique has improved the false rejection rate and false acceptance rate of the system as compared to the individual classifiers and the use of fuzzy logic inference module for the final decision helps to further improved the system performance.*
Keywords: Fuzzy logic, Multi classifiers, Online signature verification, Back propagation neural network, Pearson correlation

1. **Introduction.** Biometrics technology has gained importance in recent years to provide a more secure method of identification based on the physiological and behavioral characteristics of a person [1]. Physiological characteristics such as face, retina, finger prints, palm veins, etc. have been widely researched and many of these biometric based products have been commercialized and used in a wide variety of applications. However, behavioral type biometric systems are still lacking in terms of commercialized products, the main reason being the behavioral type biometric systems such as signature, voice, gait, etc. usually have higher error rates when compared to physiological based biometric products.

The assessment of a biometric trait is strongly dependent on the specific application since it involves not only technical issues but also social and cultural aspects [2,3]. It is also important to realize that no trait is able to completely satisfy all the desirable characteristics of biometrics systems. In this sense, handwritten signatures bear importance in certain applications of biometric systems [4,5], due to the fact that handwritten signatures have long been established as the most widespread means of personal verification. Signatures are generally recognized as a legal means of verifying an individual's identity by administrative and financial institutions. These factors provide the advantage of the signature verification compared to other biometric characteristics in its traditional use in many common commercial fields such as E-business, which includes online banking transactions, electronic payments, access control, etc. Moreover, verification by signature analysis requires no invasive measurements and people are familiar with the use of signatures in their daily life.

With the advancement of the internet technologies and applications in recent years, and the growing needs for personal verification in many daily applications, automatic signature verification is being considered with new interest [6,7]. The creation of specific laws and regulations, pertaining to the standardization of signature data interchange formats [8-11] which have been approved in many countries are testimonies of the renewed attention in this field. Efforts have been made to facilitate the integration of signature verification technologies into other standard equipment to form complete solutions for a wide range of commercial applications such as banking, insurance, health care, ID security, document management, and e-commerce [12-15].The increasing use of low-cost portable devices capable of capturing signature signals such as tablet PCs, mobile telephones or PDAs added to the growing demand of signature-based authentication applications [16-18].

According to [5], signature verification system presents a double challenge. The first is to verify that what has been signed corresponds to the unique characteristics of an individual, without necessarily caring about what was written. A failure in this context, i.e., the rejection of an authentic signature, is referred to as a Type I error or commonly called False Rejection Rate (FRR). The second challenge is more demanding than the first and consists of avoiding the acceptance for forgeries as being authentic. The second type of error is referred to as a Type II error or commonly called False Acceptance Rate (FAR). The design of such an automatic verification system has to be tested with regards to its robustness to accept genuine signatories as well as to reject impostors. A wide range of research which encountered these problems has been reported during the past few years [19-24].;A more recent trend on signature verification research is towards multi classifiers design [25,26]. Many studies have been made which suggested that design using different classifiers offers complementary information about the patterns to be classified and the application of different types of classifiers simultaneously improved the classification accuracy. The research results motivates multi-biometric authentication, where decisions based on individual biometrics are *fused*.

Various fusion techniques which are able to deal with conflicting decisions for multiple classifiers are also developed in recent years, among which include those such as majority voting, sum or product rules, different classifier types like Support Vector Machines (SVM), Bayesian classifier, decision trees and k Nearest Neighbour (k-NN) [27-36].

The use of fuzzy logic as a fusion technique for multiple classifier system has also been explored in recent years [37-41]. In [38], the authors presented a decision-making module based on fuzzy logic for model-based fault diagnosis applications. Fuzzy rules used the concept of fault possibility and knowledge of the sensitivities of the residual equations. A fault detection and isolation system, based on the input–output linear model parity equations approach, and including this decision-making module, had been successfully applied in laboratory equipment, resulting in a reduction of the uncertainty due to disturbances and modeling errors. Furthermore, the experimental sensitivity values of the residual equations allow the fault size to be estimated with sufficient accuracy.

In [39], a multi-biometric verification system that combined speaker verification, fingerprint verification with face identification has been developed. The fusion technique is based on fuzzy logic decision, which is able to account for external conditions that affect verification performance. A multimodal biometric system using two different fingerprints was proposed in [40]. The matching module integrates fuzzy logic methods for matching score fusion. Experimental results showed an improvement using the matching score level fusion rather than a mono-modal authentication system.

In this work we develop an online signature verification system based on two classifiers and a set of fuzzy logic inference decision module. Research on online signature verification system has been carried out over the years [42-47]. In [45], pressure signal is used as the main feature of the signature pattern and neuro-templates were used as classifiers for the online signature verification system. It was also demonstrated that one of the major factors causing instability in the performance accuracy of the signature verification system among different users is due to the non uniformity of the characters used by them.

In this work, we incorporated local features based on x, y and pressure signals as well as two global features to provide a more spoof-free system. In most cases, signatures are forged based on shapes, but the time and length of the signatures are not easy to be determined even by experienced forgers. Therefore, the inclusion of the global features is to ensure that the FAR is lower and, thereby, increasing the performance of the system. We also proposed a dynamic signature validation module in the enrolment stage based on Pearson's statistical method. The objective is to ensure that the signatory's signatures are consistent within a certain margin during the enrolment stage. This is to avoid large variations among the same class of signatures. These data are then used by the classifiers for training. Two classifiers are used which is the multilayer neural network using the back-propagation learning algorithm and another is the Pearson correlation technique.

To ensure higher accuracy, the signature verification system is designed to fuse the classifiers' outputs based on fuzzy inference. Another fuzzy inference engine is also developed for the global features and this output is fused with the two classifiers such that the final decision is not only based on a threshold value but also has a fuzzy human-like interpretation. In this way, the signature verification system can provide results which are more human-like such as "genuine", "genuine with risk", "may-be impostor" or "impostor" which can be interpreted easily by humans.. The results are compared with the conventional threshold based decision module and are found to be better.

This paper has been organized as follows: the main modules of the signature verification system are described after the introduction, the threshold based decision module and the proposed fuzzy logic decision modules are described in the following section. Then, some experimental results using the proposed system are discussed which include comparison made with normal threshold techniques.

2. **Overall System Design.** The signature verification system consists of five modules which are (i) data acquisition, (ii) pre-processing, (iii) dynamic validation, (iv)feature extraction and (v) classification. The system can be divided into two main stages which are the enrollment and verification. In the enrolment stage, the user has to provide a set of signatures and these signatures are pre-processed and the variations of the signatures are checked using the data validation method described in Section 2.3. The features of the signatures are then extracted and are used as inputs to the back propagation neural network (BPNN) module and the Pearson correlation module. The training of these features produced a neuro-template for each of these signatures and the corresponding threshold values for the Pearson correlation .

In the verification phase, the features of the new data will be input to the BPNN and Pearson correlation for the classification process. The proposed sequential fuzzy logic decision module will be used to determine the overall output of the system. Figure 1 shows the process flow of the system in the enrolment and verification stage.

2.1. **Data acquisition module.** The data in the dynamic verification system is acquired using a digital tablet which captures the dynamic information of the signature such as the pen position in the X and Y axes, the pen's pressure and time. In this system, we use a WACOM digital tablet with resolution of 2,032 dpi and a sampling rate of 1000 points/sec.

2.2. **Pre-processing module.** The pre-processing part of the signature verification system consists of two steps.

Step 1. Size Normalization. Signatures are normalized to rectify different sizes of signatures by scaling each signature both horizontally and vertically to get the same scaled signatures. A signature acquisition process on a restricted size frame is assumed. The normalization is done by the following equations:

$$x_i = \frac{x_i^o - x_{\min}}{x_{\max} - x_{\min}} W \tag{1}$$

$$y_i = \frac{y_i^o - y_{\min}}{y_{\max} - y_{\min}} H \tag{2}$$

where (x_i^o, y_i^o) denotes the original point, and (x_i, y_i) is the corresponding point after transformation, and W, H are the width and height of the normalized characters, respectively and the minimum and maximum, x and y coordinates are given by:

$$x_{\min} = \min_i \{x_i^o\}, \quad x_{\max} = \max_i \{x_i^o\}, \quad y_{\min} = \min_i \{y_i^o\}, \quad y_{\max} = \max_i \{y_i^o\}, \tag{3}$$

Step 2. Re-sampling. In our system, the re-sampling process is divided into two categories: re-sampling of the distance and re-sampling of the time. In the case of re-sampling the distance, the signature data points are required to be equidistant with a fixed number of points. This can be done using a simple linear interpolation algorithm as given in (4), (5), and (6). The re-sampling step, ΔS, is a fraction of the total arc length (L) given as:

$$L = \sum_{i=1}^{n-1} d_i \tag{4}$$

$$d_i = \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2} \tag{5}$$

$$\Delta S = LL/n_1 \tag{6}$$

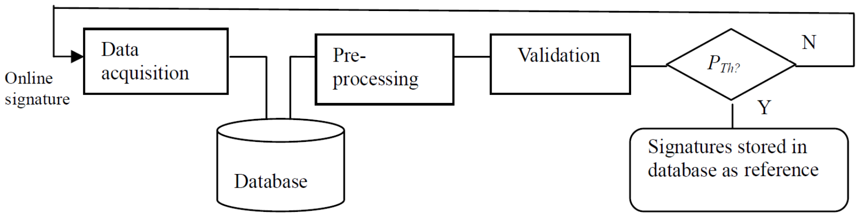
where d_i denotes the distance of point to point and n is the number of points.

After re-sampling, the characters have a fixed number (n_1) of points per character (100 points in our system) which provides a fixed size input to the BPNN. The process of re-sampling the distance from the original data signature is shown in Figure 2.

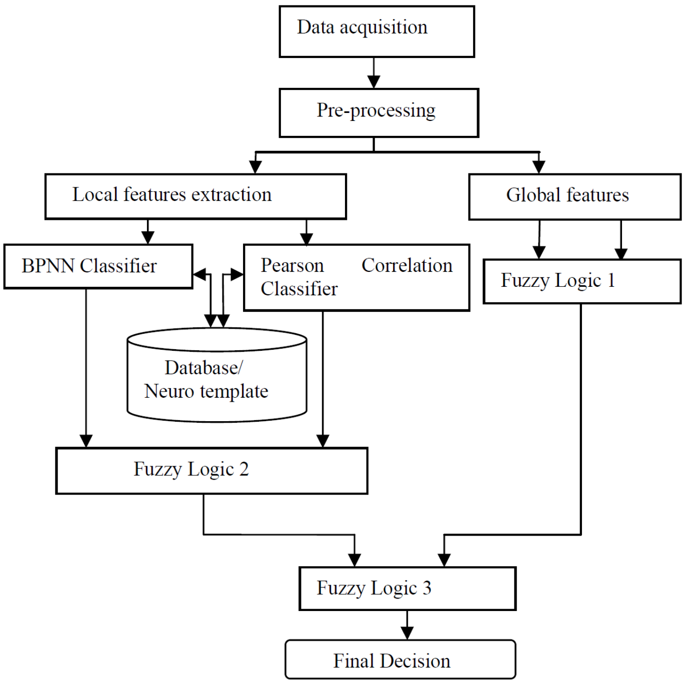
The re-sampling of time is used to ensure the same time interval is used for each sampling point. This is done using linear interpolation algorithm. The re-sampling step ΔT is a fraction of the total time signature $T(n)$ and is given as follows:

$$\Delta T = T(n)/n_2 \tag{7}$$

where n is the total number raw data of signature before re-sampling process. After re-sampling, the signatures have a fixed number (n_2) of points per signature (100 points in our system).

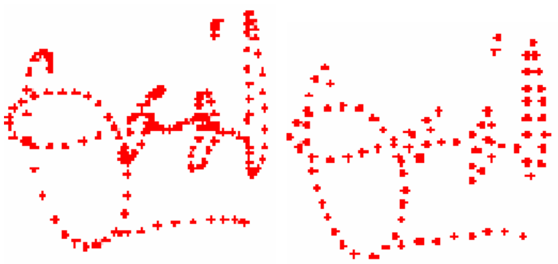


(a)



(b)

Figure 1. The process flow of the overall system design. (a) enrollment stage (b) verification stage



(a) (b)

Figure 2. The process of re-sampling the distance (a) Original (b) After re-sampling

2.3. **Enrolment and signature validation module.** In signature verification problem, the task is a pattern recognition task for discriminating two classes: original and forgeries. It is known that the process does not always result in identical signatures, neither with respect to their state nor to their dynamic characteristics. Although there are many attempts to reduce the distinct variability of the signer's signature, the problems remain due to the physical or psychological reasons. The basic problem of signature verification systems is the allowance of certain variations within the genuine class, while simultaneously detecting significant differences between the genuine and the forgery class forgeries.

In order to overcome this problem, we propose the use of Pearson correlation technique [48] in the enrollment stage of the signature verification system. The use of the technique is to ensure that the signatures' training set of an individual is kept at a certain level of consistencies during the enrolment stage. In the enrollment stage, a set of signatures of an individual will be taken and used as a reference signatures and will be used for training. A consistent signature means that the variation of the signature is not too large and the correlation of the signatures is positive.

The Pearson correlation technique is defined by following formula:

$$r = \frac{\sum (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum (x_i - \overline{x})^2 . \sum (y_i - \overline{y})^2}} \tag{8}$$

Where r is the correlation coefficients of the population of signatures of the individual signer during the enrollment stage, xi, yi are signature data for $i = 1, 2, \ldots n$, x, y are the mean of x and y respectively.

Pearson correlation reflects the degree of linear relationship between two variables. It ranges from $+1$ to -1. A correlation of $+1$ means that there is a perfect positive linear relationship between variables. In this work, we propose the use of a threshold value P_{Th} which is selected to determine the acceptable variations within the reference signatures based on the correlation coefficient r. However, as the degree of the inter-variations in genuine signatures as well as the intra-variations between the genuine signatures and the forgeries are the main issues in the signature verification system, the task of finding the threshold value which represents the allowable variations in the signatures is not an easy one. Having conducted various experiments to determine the acceptable threshold value of the validation module, the threshold value for the validation process is given as follows:

$$P_{Th} = mean(r_1, \ldots r_n) - \alpha_1 \tag{9}$$

where $r_1, \ldots, r_n$ are the Pearson correlation coefficients of the n reference signatures. In this case, the threshold is the mean of the Pearson correlation coefficients among the n signatures of an individual with some adjustment constant α_1.

2.4. **Feature extraction module.** In this paper, we use both the feature-based approaches, in which a holistic vector representation consisting of a set of global features is derived from the signature trajectories and the function-based approaches, in which time sequences describing local properties of the signature are used for recognition. The purpose is to enhance the variability of the system to help discriminate the signatures of the users. In our system, the local features are obtained from the x and y coordinates of the signatures as well as the pressure with respect to time. The local features described the shape of the signatures although the element of pressure features provides additional information not relating to shape. Our online signature verification system is based on the fusion of local and global features as described in the next section.

2.4.1. *Local features.* The local features are divided into two categories namely, local features based on time domain and local features based on writing strokes. The former has 5 dimensions which includes displacement (X, Y), pressure (P), and direction (X, Y). All of the local features based on time and stroke are bounded and varied between 0 and +1 and are given as follows:

$$f_1 = \frac{X}{X_{\max}} \tag{10}$$

$$f_2 = \frac{Y}{Y_{\max}} \tag{11}$$

$$f_3 = \frac{P}{1023} \tag{12}$$

$$f_4 = (\sin\theta_x + 1)/2 \tag{13}$$

$$f_5 = (\sin\theta_y + 1)/2 \tag{14}$$

Where $\sin\theta_X(n) = \frac{\Delta X(n)}{D(n)}$, $D(n) = \sqrt{\Delta X(n)^2 + \Delta T(n)^2}$, $\sin\theta_Y(n) = \frac{\Delta Y(n)}{Q(n)}$, $Q(n) = \sqrt{\Delta Y(n)^2 + \Delta T(n)^2}$ The features based on the stroke are as follows:

$$f_6 = (\cos\theta + 1)/2 \tag{15}$$

$$f_7 = (\sin\theta + 1)/2 \tag{16}$$

$$f_8 = (\cos\phi + 1)/2 \tag{17}$$

$$f_9 = (\sin\phi + 1)/2 \tag{18}$$

where θ, ϕ are calculated as shown in Figure 3.

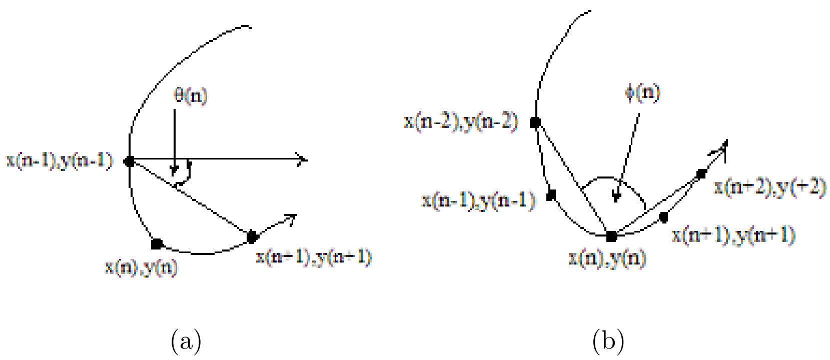


Figure 3. Feature extraction based on strokes showing how the angles are calculated

2.4.2. *Global feature.* The global features in this system are selected to obtain an improved FAR and FRR which includes the total length and total time of the signature. The formulation to calculate the total length is given as in (3), and the total time can be obtained from the time recorded at the end point.

2.5. **The classifier module.**

2.5.1. *Neural network classifier.* A three-layer fully connected BPNN module was trained to recognize the signatures with the 9-dimensional features. Based on a re-sampling of 100 points, a total of 900 points are used as the actual inputs of each neural network model. In this system, the number of hidden layer neurons is judiciously chosen at 100 with 1 output node. Samples of the reference pattern of genuine signatures and samples of random pattern of forgeries are used as input patterns in the training stage. A set of neuro-templates based on sigmoid activation function are obtained for each individual in the training set.

The neural network module is trained to saturate at "1" for genuine input patterns and "0" for impostor input patterns. The training phase includes the offline testing from the samples of genuine reference signatures to get the corresponding output values of individuals in the training set of the BPNN which are then used to determine the threshold of the BPNN.

2.5.2. *Pearson correlation classifier.* The classifier works in the same way as the validation module where the degree of the linear relationship between the signatures based on 9-dimensional features are used as a means of verification. As the number of re-sampling points is 100 points, thus 900 (9*100) points per signature were used as inputs to the Pearson correlation module during the enrolment stage. The algorithm will calculate the correlation factor (r_e) of the input signatures and the respective reference signatures obtained during the enrollment stage. The threshold value Th_2 is determined during the training and testing stage.

2.6. **Majority vote decision module.** In multi classifier system, various strategies have been formulated to enable decisions to be made, among which majority vote is by far the simplest, and yet it has been found to be just as effective as more complicated schemes in improving the decision results taking into consideration that a correct decision by majority is a correct decision by plurality. Majority voting has been used as decision technique when more than one classifier is involved in decision making [49-52]. This simple method depends on counting votes for each class over the input classifiers and selecting the majority class. In this approach, the input features of a person will be assigned to the matcher based on the output from classifier. For example, two out of three classifiers recognized the signature belongs to "A", therefore the decision after fusion is "A". Since all the matchers are assumed to perform equally well, the quality of decision is totally dependent on the competencies of the classifiers. If some of the classifiers have poorer performance, the quality of the decision will also be worse.

In this paper, we use the majority votes as a basis of comparison with our proposed fusion technique. The majority votes are based on the three-classifier modules, namely, BPNN module, Pearson correlation module, and the global features module.

The output result from the BPNN classifier module is

$$BPNN\,Output = \begin{cases} 1 & \text{if } x > Th_1 \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

where x is output value of the BPNN and Th_1 is the threshold value chosen judiciously by experiment in the training stage. Similarly, the output result from the Pearson correlation module is given as:

$$Pearson = \begin{cases} 1 & \text{if } z > Th_2 \\ 0 & \text{otherwise} \end{cases} \tag{20}$$

The output of the Pearson Correlation classifier is based on the Pearson coefficient z_i obtained by correlating the ith input signature with associated genuine reference signatures from the enrollment stage. The threshold value Th_2 is obtained using (9) in the training stage.

In the case of the global features, two threshold values are used to classify the two global features which are Th_3 referring to the total length of the signature and Th_4 referring to the total time of the signature. These thresholds are obtained in the training stage and can be expressed as shown in the following equations:

$$b = mean(L_1 \ldots Lm) - b_1 < Th_3 < b = mean(L_1 \ldots Lm) + b_1 \tag{21}$$

$$c = mean(T_1 \ldots Tm) - c_1 < Th_4 < c = mean(T_1 \ldots Tm) + c_1 \tag{22}$$

where $L_1 \ldots Lm$ are the total length and $T_1 \ldots Tm$ are the total time of signatures from m reference genuine signatures. The constant parameters b and c are values which can be used as adjustment values and they are obtained experimentally. The total length and time of the input signature will be calculated and compared with Th_3 and Th_4 respectively to obtain a "Pass" or "Fail" output.

2.7. **The fuzzy decision modules.** The work using fuzzy logic as the fusion technique is motivated by the fact that biometric verification systems are often affected by external conditions and variables which resulted in degradation of performance. This problem is aggravated for signature verification systems as signatures are very much dependent on a variety of guaranteed absolute reliability, which can reinforce one another when used jointly to maximize verification performance. One example is the mismatched conditions between enrollment and verification.

Moreover, fuzzy logic is one type of artificial intelligence techniques developed to imitate the decision of humans by encoding their knowledge in the form of linguistic rules. So, fuzzy systems are particularly suitable to be implemented as a decision module since fuzzy rules provide a natural framework of deciding and it is able to emulate human thinking capabilities in dealing with uncertainties.

In the majority voting system, the decision is based on the score of the votes which are very binary like and based mainly on the input pattern passing or failing the threshold values which have been selected for each classifiers based on trial and error. In most applications, there are various external conditions affecting the measurement of the input pattern. In signature verification system, the external factors are considered as normal and inherent behaviors and contribute to the diversity of the error. Moreover, in multi classifier design, it has been shown that the sets of patterns misclassified by the different classifiers would not necessarily overlapped, suggesting that the different classifier design offered complimentary information about the patterns to be classified. Therefore, the use of majority voting may result in poor performance or higher FRR and FAR due the poor performance of the classifiers.

The use of threshold values as described in section 2.6 is conservative in the sense that the values are fixed and does not provide flexibility to counter any variations in the input patterns. In order to overcome the limitations of the threshold based decision module which gives a hard output decision of which either "pass" or "fail", we proposed a fuzzy inference decision module for all the classifier as well as the final decision module. With the fuzzy decision module, each classifier has a softer output which is more accurate and easier to be interpreted by humans. Moreover, the total system can be tuned such that the user can select the type of output to be emphasized, whether the output from the fusion of the classifiers which is based on the local features or the output based on the global features which are the time and length of the signature.

In this signature verification system, three fuzzy decision modules are cascaded. Figure 4 shows the block diagram of the proposed fuzzy inference decision module. The fuzzy logic decision modules are used in the verification stage. The inputs to the fuzzy logic 1 are the signature's length and time. Figure 5 shows the input membership function developed by considering the threshold values obtained in the enrolment stage which includes the training and testing process. In this way, the task of making decision based on the global feature classifiers are not dependent on the hard threshold values and offers more flexibility in addressing the variations of the signatures and overcomes the boundary limitations of the threshold values. The output of this fuzzy module is quantized into 3 consequents which are genuine (GE), Risky (RI), and Impostor (IM). The second fuzzy logic module consists of the BPNN classifier output values x and the Pearson correlation classifier output z as the inputs. The input membership function of both the classifiers is developed using the threshold values given in (19) and (20) as references as shown in Figure 6. The output of the second fuzzy module is quantized into 4 consequents which are Fa (Fail), HR (High Risk), LR (Low Risk) and Ac (Accept). Again, the decision making based on the two classifier output is not binary like as given in (20) and (21). The fuzzy logic module allows flexibility in terms of the boundaries of the threshold values and able to leverage on the strength of the classifications results of both classifiers.

In the majority voting implementation discussed in Section 2.6, the final decision of the system is based on the majority votes of the classifiers used, putting the same weightage for all the classifiers. The use of the third fuzzy logic module is to ensure the final decision is made based on the quality information given by the outputs of these classifiers. The outputs of these two fuzzy logic modules are used as inputs to third fuzzy logic, forming a total fuzzy logic decision module. The fuzzy logic rules for the third fuzzy logic module is given in Table 1. The output of the system has the following consequents which are genuine (GE), genuine with risk (GR), maybe an impostor (MI), and impostor (IM).

For each fuzzy module, the appropriate fuzzy rules are required to be developed. These rules can be further fine-tuned in cases where there is a need to emphasize different parameters during the implementation stage. The max-min inference procedure is used in each of the fuzzy modules. Figure 7 shows the membership functions of the output

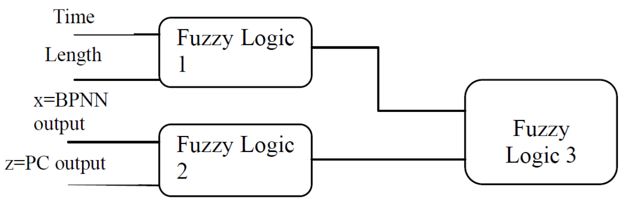


FIGURE 4. Fuzzy decision modules for the signature verification system

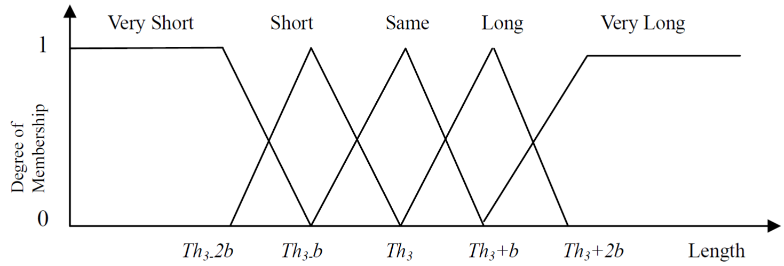
of Fuzzy Module 1 and Fuzzy Module 2 which are the inputs to the Fuzzy Module 3, and Figure 8 shows the output of fuzzy logic 3 which is the final decision of the system. For the defuzzification, the centroid defuzzification strategy is used as given in (23)

$$C = \frac{\sum Mi * Xi}{Area} \tag{23}$$

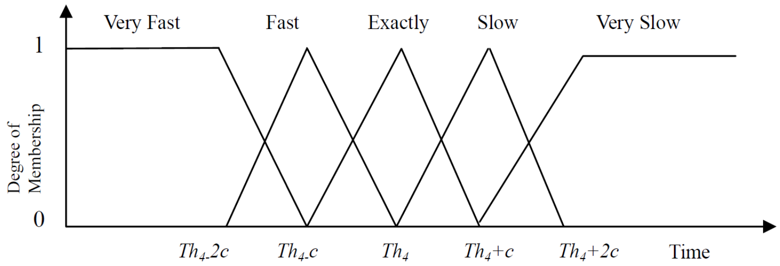
where X_i is the X coordinate at the point in the array, and M_i is the value at that point.

3. Experimental Results and Discussions.

The proposed fuzzy logic decision module uses the fuzzy logic inference to make decisions on the classifications of the signatures, as well as a combination of classifiers forming a concrete decision module design in order to improve the FAR and FRR rate of the signature verification system. In this note, the



(a)



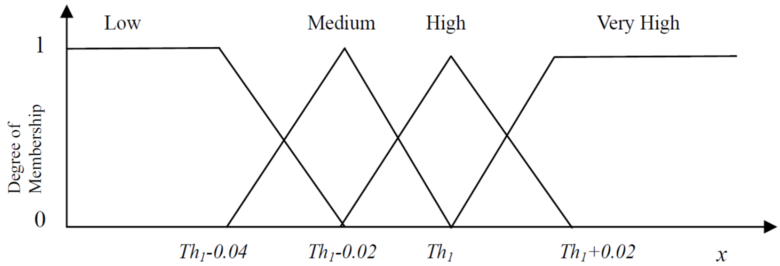
(b)

FIGURE 5. Input membership function of Fuzzy Logic Module 1: (a) Length and (b) Time of signature

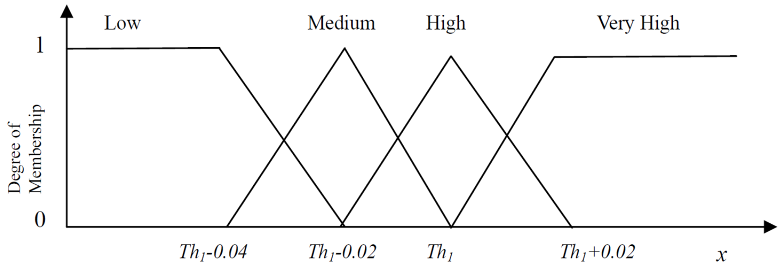
experiments are conducted to evaluate the performance of the proposed system in terms of the FAR and FRR. Two main evaluations are being considered which are the performance of the complete system as compared to the majority voting system discussed in section 2.6 which uses mainly the output of the classifiers based on fixed threshold values and the performances of single classifier and multi classifier systems. The experiments were performed using databases which were collected at the Centre for Artificial Intelligence and Robotics (CAIRO) of Universiti Teknologi Malaysia. The system is currently being used at the center for the purpose of attendance access control. The signature databases were developed based on 20 users. Each user has 20 reference genuine signatures collected during the enrolment stage of which 10 signatures were used for training and the other 10 were used for testing. The testing set was used to obtain the FRR of the system.

The database also consists of 10 skilled forgeries signatures, and 10 simple forgeries signatures for each user. The simple forgeries were developed by copying the signatures based on visual inspection of the signatures. Skilled forgeries are those signatures copied by tracing the genuine signatures as closely as possible. These samples were used to obtain the FAR of the system.

3.1. **Experiment I.** In this experiment, the threshold values of the classifiers, namely, BPNN and Pearson correlation as well as the global features were determined. These threshold values were used to obtain the final decision using the method as described in the previous sections. Based on the local features described in section 2.4, BPNN was trained and tested using different threshold values. The result of the BPNN classifier for the different threshold values is given in Figure 9. It can be seen that, as the threshold of the neural network output is increased, the FRR is also increased, but, on the other

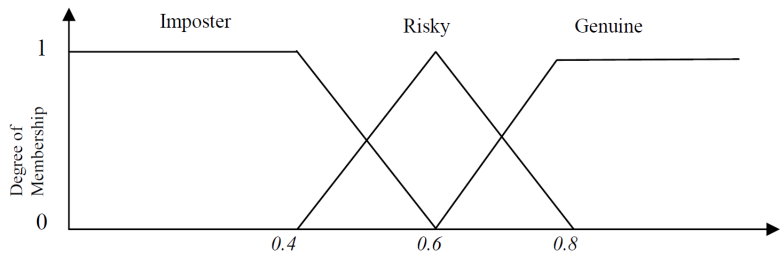


(a)

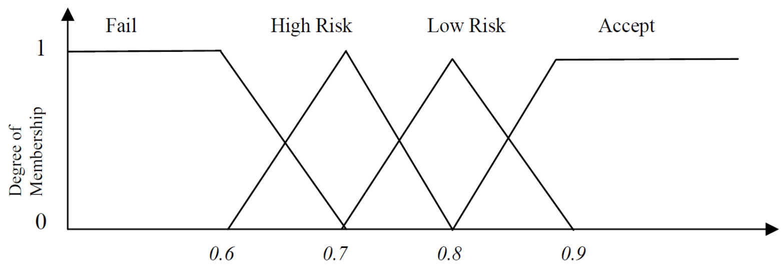


(b)

FIGURE 6. Input membership functions of the Fuzzy Module 2. (a) BPNN output and (b) Pearson correlation output



(a)



(b)

FIGURE 7. Input membership functions of Fuzzy Logic Module 3 (a) Output of Fuzzy Logic Module 1 and (b) Output of Fuzzy Logic Module 2

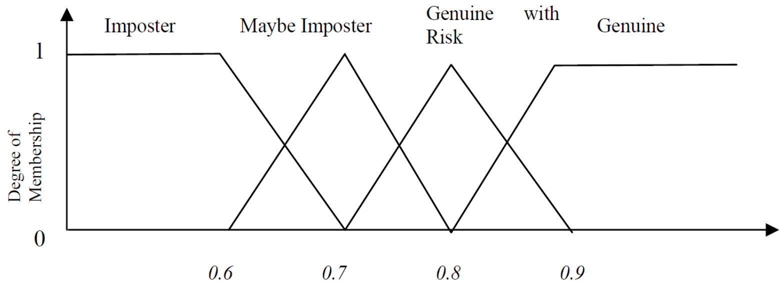


FIGURE 8. The output membership functions of the Fuzzy Module 3

hand, the FAR is decreased. In designing an online system, a compromise has to be made in order to have a good FRR as well as a good FAR, and usually the choice is made based on the requirement of the system application. In this case, based on the result of Figure 9, we can choose the threshold value of 0.93 as this is the point where the FRR and FAR (simple forgeries) are quite low and of the same value. However, we can see that the FAR (skilled) is quite high at about 10.5 %. In order to reduce FAR (skilled forgeries), we need to increase the threshold value, which in turn will increase the FRR of the system.

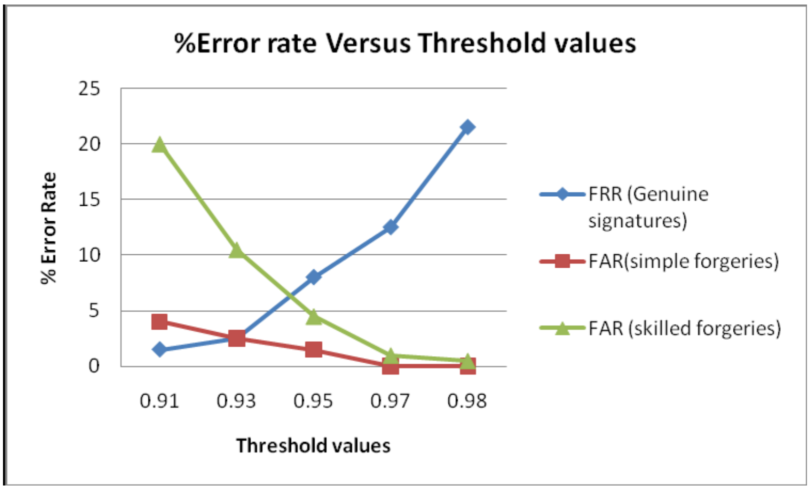


FIGURE 9. Percentage error rate versus threshold values for neural network classifier

Similar experiments were carried out for the Pearson classifier. The value of the constant α which allows for some variations of the signatures of an individual as explained in (9) is determined by having 10 genuine signatures for each α value in the range between 0 – 0.1 in steps of 0.005. The results of FRR for genuine, FAR for simple forgery and FAR for skilled forgery with different threshold values are shown in Figure 10. The threshold for this classifier is chosen to be 0.04 based on the reasonable acceptable FRR and FAR values.

In the case of the global features, 10 genuine signatures are used for different variations of constant values b, c about the mean of the 10 signatures for time and length respectively. The range of values chosen is between 0 – 1000 in steps of 50. The verification results corresponding to various parameters of the threshold values are shown in Figure 11. The system accepts the signature if both length and time values of the input signature are between the allowed range of the length and time values. From Figure 11, we can get an acceptable FRR and FAR for both simple and skilled forgeries for $Th_3 = 200$ and $Th_4 = 300$.

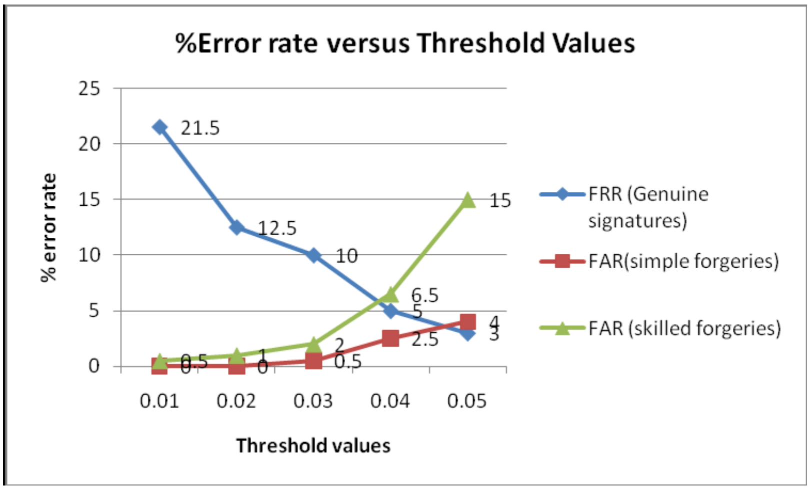


FIGURE 10. Percentage of the error rate versus threshold values for Pearson classifier

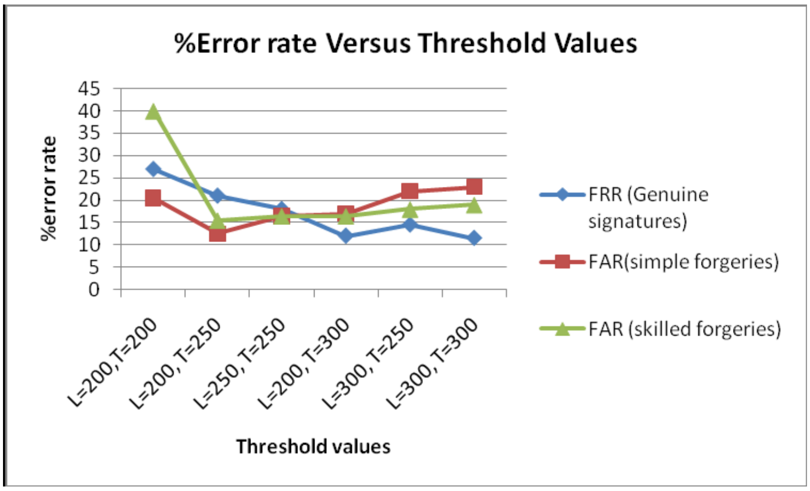


FIGURE 11. Percentage error rate versus threshold values for Global features

3.2. **Experiment II.** One of the main problems in the above technique is the difficulty in choosing the threshold values such that the FRR and FAR are reasonably acceptable. This is because both the FRR and FAR are conflicting in nature, which means that, increasing the threshold would increase the FRR considerably, but on the other hand would reduced the FAR. In order to overcome this problem, fuzzy variables are used as inputs to each of the fuzzy modules to obtain a more human like decisions. This method overcomes the boundary limitations of fixed thresholds and overcome the uncertainties of thresholds for various users. In this case, the threshold values chosen can just be a rough estimates or used as reference values in order to design the fuzzy logic module. The uncertainties and the variations will be addressed by the fuzzy logic module. The same set of training and testing signatures were used for the proposed fuzzy logic decision module and the results for both the majority voting based on fixed threshold and the fuzzy logic systems are shown in Table 1.

3.3. **Discussion.** One of the major observations that can be made in comparing the performance of the proposed fuzzy logic module and the majority voting is the reduction in the FRR and FAR for the online signature verification system. The proposed method is able to reduce the FRR of the majority voting based on fixed threshold from 6.5 %

Table 1. Percentage error rate for both the majority voting based on fixed threshold and the fuzzy inference

Final Decision :Majority Voting		
FRR (Genuine signatures)=6.5	FAR(simple forgeries)=0.5	FAR (skilled forgeries)=0
Final Decision: Sequential Fuzzy Logic		
FRR (Genuine signatures)=3.5	FAR(simple forgeries)=0	FAR (skilled forgeries)=0

to 3.5%, the FAR of simple forgeries from 3.5% to 0% and the FAR for skilled forgeries from 3.5% to 0%. The FRR and FAR for the system are low and acceptable for an online signature verification system. Apart from that, the proposed system reduces the time consuming task of finding the suitable threshold values in order to get an acceptable verification result.

Another major observation is the use of the multi classifiers as proposed in the design has also improved the FAR and FRR of the online signature verification system in comparison to the single classifier. The FAR for both simple and skilled forgeries of the BPNN classifier selected for a threshold value of 0.97 were very low, but the FRR is high at 12.5%. Similarly, in the Pearson correlation case, the threshold value of 0.04 chosen gave a FRR of about 5.0, but the FAR for both simple and skilled forgeries are not as low as those obtained from the BPNN. It can be observed that the FRR and FAR for the global features are higher due to the larger threshold values chosen. The reason for the choice of the threshold values within this range is because, for the global features, the sensitivity range of the threshold values and the FRR and FAR is rather small, and therefore, any reduction or increment of the threshold values would increase the FRR and FAR considerably. The use of the fusion technique of the two classifiers and the global features has improved the results of FRR and FAR considerably as can be seen from Tables 1.

4. **Conclusion.** Signature verification systems are behavioral based biometric systems and have not been widely used in many real world applications. One major drawback is that humans are not consistent in signing their signatures. Thus, more robust signature verification systems are required to be developed before they can be accepted for implementation. In this paper, a robust signature verification system has been proposed based on fuzzy logic inferences. The system incorporates a fusion of multi classifiers namely, BPNN and Pearson correlation, as well as the fusion of global features of time and length of the signatures, both using fuzzy logic inferences. A validation module based on the Pearson's correlation statistical technique is also incorporated in the system. The performance of the proposed multi-classifier fuzzy inference based signature verification system is compared in terms of FRR and FAR for simple and skilled forgeries with the conventional majority voting system based on fixed threhold.

This paper highlights two main results of the system, which are the improvement of FRR and FAR for the system by having the fusion of multi classifiers and the use of the fuzzy inference modules. Moreover, the advantage of the proposed system proposed does not only reduce the error rate but also reduce the tedious process of finding the acceptable threshold values for the classifiers. The fuzzy rules and membership functions of the fuzzy inference modules can be easily tuned to meet different organizational environments which make the system more flexible and easier to be implemented. The fuzzy inference has also improved the output decision of the system to be interpreted in a more human-like manner.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation of this paper.

REFERENCES

[1] A. K. Jain, A. K. Ross and A. Prabhakar, An introduction to biometric recognition, *IEEE Trans. Circ. Sys. Video Technol.*, vol.14, pp.4-20, 2004.
[2] A. K. Jain, L. Hong and S. Pankanti, Biometric identification, *Commun., ACM*, vol.43, no.2, pp.91-98, 2000.
[3] K. Veeramacheneni, L. A. Osadciw and P. K. Varshney, An adaptive multimodal biometric management algorithm, *IEEE Trans. Syst., Man, Cybern. C*, vol.35, no.3, pp.344-356, 2005.
[4] M. C. Fairhurst and E. Kaplani, Perceptual analysis of handwritten signatures for biometric authentication, *Inst. Elect. Eng. Proc. Vis., Image Signal Process*, vol.150, no.6, pp.389-394, 2003.
[5] Plamondon and S. N. Srihari, On-line and off-line handwriting recognition: A comprehensive survey, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.22, no.1, pp.63-81, 2000.
[6] V. S. Nalwa, Automatic on-line signature verification, *Proc. of the IEEE*, vol.85, no.2, pp.215-239, 1997.
[7] S. Nanavati, M. Thieme and R. Nanavati, *Biometrics: Identity Verification in a Networked World*, New York, Wiley, 2002.
[8] W. S. Wijesoma, K. W. Yue, K. L. Chien and T. K. Chow, Online handwritten signature verification for electronic commerce over the internet, *Lecture Notes in Artificial Intelligence 2198*, WI, 2001.
[9] N. Zhong, *Information Technology-Biometric data Interchange Format Signature/Sign Data*, ANSI Standard ANSI INCITS 395-2005, 2001.
[10] *Information Technology – Biometric Data Interchange Formats – Part 7: Signature/Sign Time Series Data*, ISO Standard ISO/IEC FCD 19794-7, 2006.
[11] *Information Technology – Biometric Data Interchange Formats – Part 11: Signature/Sign Processed Dynamic Data*, ISO Standard ISO/IEC WD 19794-11, 2007.
[12] Y. M. Tseng, T. Y. Wu and J. D. Wu, An efficient and provably secure id-based signature scheme with batch verifications, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(A), pp.3911-3922, 2009.
[13] Y. F. Chung and K. H. Huang, Chameleon signature with conditional open verification, *International Journal of Innovative Computing, Information and Control*, vol.5, no.9, pp.2829-2836, 2009.
[14] F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez , Secure access system using signature verification over tablet PC, *IEEE A&E Systems Magazine*, 2007.
[15] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia and A. Neri, Cancelable templates for sequence-based biometrics with application to on-line signature recognition, *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol.40, no.3, 2010.
[16] M. Wang, H. Hu and G. Dai, An identity-based signature scheme for mobile business, *ICIC Express Letters*, vol.4, no.2, pp.565-570, 2010.
[17] M. S. Hwang, S. F. Tzeng and S. F. Chiou, A non-repudiable multi-proxy multisignature scheme, *ICIC Express Letters*, vol.3, no.3(A), pp.259-264, 2009.
[18] F. Chun, W. Chih and S. Wei-Zhe, Fast randomization schemes for chaum blind signatures, *International Journal of Innovative Computing Information and Control*, vol.5, no.11(A), pp.3887-3900, 2009.
[19] D. Wang, Y. Zhang, C. Yao, J. Wu, H. Jiao and M. Liu, Toward force-based signature verification: A pen-type sensor and preliminary validation, *IEEE Transactions on Instrumentation and Measurement*, vol.59, no.4, 2010.
[20] L. Nanni and A. Lumini, Human authentication featuring signatures and tokenized random numbers, *Neurocomputing*, vol.69, no.7-9, pp.858-861, 2006.
[21] C. Y. Chen, H. F. Lin and C. C. Chang, An efficient generalized group-oriented signature scheme, *International Journal of Innovative Computing, Information and Control*, vol.4, no.6, pp.1335-1345, 2008.
[22] C. Vivaracho-Pascual, M. Faundez-Zanuy and J. M. Pascua, An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances, *Pattern Recognition*, vol.42, no.1, pp.183-193, 2008.
[23] M. A. U. Khan, M. K. Niazi and M. Aurangzeb Khan, Velocity-image model for online signature verification, *IEEE Transactions on Image Processing*, vol.15, no.11, 2006.

[24] L. Govindaraju, A comparative study on the consistency of features in on-line signature verification, *Pattern Recognition Letters*, vol.26, no.15, pp.2483-2489, 2005.
[25] G. Fumera and F. Roli, A theoretical and experimental analysis of linear combiners for multiple classifier systems, *IEEE Trans. Pattern Anal. Machine Intelligence*, vol.27, no.6, pp.942-956, 2005.
[26] T. K. Ho, J. J. Hull and S. N. Srihari, Decision combination in multiple classifier systems, *IEEE Trans. Pattern Anal. Mach. Intelligence*, vol.16, no.1, pp.66-75, 1994.
[27] R. P. W. Duin and D. M. J. Taz, Experiments with classifier combining rules, *Lecture Notes in Computer Science*, Gagliari, Italy, pp.16-29, 2000.
[28] C. De Stefano, A. Della Cioppa and A. Marcelli, An adaptive weighted majority vote rule for combining multiple classifiers, *Proc. IEEE ICPR*, vol.2. pp.192-195, 2002.
[29] J. Kittler and F. M. Alkoot, Sum versus vote fusion in multiple classifier systems, *IEEE Trans. Pattern Anal. Machine Intelligence*, vol.25, pp.110-115, 2003.
[30] L. I. Kuncheva, Decision templates for multiple classifier fusion: An experimental comparison, *Pattern Recognition*, vol.34, no.2, pp.299-314, 1999.
[31] J. Y. Zhao, R. Laganiere and Z. Liu, Performance assessment of combinative pixel-level image fusion based on an absolute feature measurement, *International Journal of Innovative Computing, Information and Control*, vol.3, no.6(A), pp.1433-1447, 2007.
[32] X. Gao, X. Wang and S. J. Ovaska, Uni-modal and multi-modal optimization using modified harmony search methods, *International Journal of Innovative Computing, Information and Control*, vol.5, no.10(A), pp.2985-2996, 2009.
[33] L. Lam and C. Y. Suen, Optimal combinations of pattern classifiers, *Pattern Recognition Letters*, vol.16, pp.945-954, 1995.
[34] D. E. Maurer and J. P. Baker , Fusing multimodal biometrics with quality estimates via a Bayesian belief network, *Elsevier Science*, vol.41, no.3, pp.821-832, 2008.
[35] C. Y. Suen and L. Lam, Multiple classifier combination methodologies for different output levels, *Multiple Classifier Systems*, pp.52-56, 2000.
[36] T. Scheidat, C. Vielhauer and J. Dittmann, Single-semantic multi-instance fusion of handwriting based biometric authentication systems, *Proc. of ICIP*, pp.393-396, 2005.
[37] A. Azzini, S. Marrara, R. Sassi and F. Scotti, A fuzzy approach to multimodal biometric authentication, *Proc. of the 11th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, KES'07*, Vietri sul Mare (SA), Italy, pp.801-808, 2007.
[38] L. J. De Miguel and L. F. Blanquez, Fuzzy logic based decision making for fault diagnosis in a dc motor, *International journal on Enginering Applications of Artificial Intelligence*, vol.18, pp.423-450, 2005.
[39] C. W. Lau, M. Bin, H. M. Meng, Y. S. Moon and Y. Yeung, Fuzzy logic decision fusion in a multimodal biometric system, *International Conference on Spoken Language Processing (ICSLP)*, 2004.
[40] T. Ko, Multimodal biometric identification for large user population using fingerprint, face and iris recognition, *Proc. of the 34th Applied Imagery and Pattern Recognition Workshop(AIPR05)*, 2005.
[41] S.-B. Cho and J. H. Kim, Multiple network fusion using fuzzy logic, *IEEE Trans. Neural Networks*, vol.6, no.2, pp.497-501, 1995.
[42] A. Fadlil, M. Khalid, R. Yusof, S. Salleh, N. Omar and A. R. M. Shaari, Higher performance signature verification based on two-classifier modules, *Proc. of the 1st International Symposium on Bio-inspired Computing (BIC'05)*, 2005.
[43] L. Nanni and A. Lumini, A novel local on-line signature verification system, *Pattern Recognition Letters*, vol.29, no.5, pp.559-568, 2008.
[44] L. Nanni and A. Lumini, A supervised method to discriminate between impostors and genuine in biometry, *Expert Systems with Applications*, vol.36, no.7, pp.10401-10407, 2008.
[45] L. Mi and F. Takeda, Analysis on the robustness of the pressure-based individual identification system based on neural networks, *International Journal of Innovative Computing, Information and Control*, vol.3, no.1, 2007.
[46] X. Li and D. Y. Yeung, On-line handwritten alphanumeric character recognition using dominant points in strokes, *Pattern Recognition*, vol.31, no.1, pp.31-44, 1996.
[47] B. Li, D. Zhang and K. Wang, On-line signature verification based on NCA (null component analysis) and PCA (principal component analysis), *Pattern Analysis*, pp.345-356, 2006.
[48] Khazanie, *Statistics in a World of Applications*, Harper Collins College Publishers, 1996.

[49] M. Monwar and M. Gavrilova, Enhancing security through a hybrid multibiometric system, *IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, pp.84-91, 2009.

[50] S. Hassan and B. Verma, Decisions fusion strategy: Towards hybrid cluster ensemble, *The 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, ISSNIP 2007*, pp.377-382, 2007.

[51] A. A. Ross, A. K. Jain and K. Nandakumar, *Levels of Fusion in Biometrics, Handbook of Multibiometrics*, Springer, US, 2006.

[52] A. Rahman and M. Fairhurst, Decision combination of multiple classifiers for pattern classification: hybridisation of majority voting and divide and conquer techniques, *The 5th IEEE Workshop on Applications of Computer Vision*, pp.58-63, 2000.