Available online at www.sciencedirect.com

ScienceDirect

Fuzzy Sets and Systems 305 (2016) 149–159

FUZZY sets and systems

www.elsevier.com/locate/fss

Fuzzy pattern recognition-based approach to biometric score fusion problem

Khalid Fakhar [a,*], Mohamed El Aroussi [a,b], Mohamed Nabil Saidi [a,c], Driss Aboutajdine [a]

[a] *LRIT Research Laboratory (associated unit to CNRST, URAC n° 29), Mohammed V University in Rabat, Faculty of Sciences, Morocco*
[b] *LETI, EHTP, Casablanca, Morocco*
[c] *INSEA, Rabat, Morocco*

Received 8 July 2015; received in revised form 19 February 2016; accepted 1 May 2016

Available online 9 May 2016

Abstract

This paper introduces a novel approach for biometric score fusion problem that can be viewed as a fuzzy pattern recognition one. In this approach, the matching score space is considered as consisting of two fuzzy sets ("genuine" and "impostor"). First, each individual matcher is modeled as a fuzzy set, using an automatic membership function generation method, in order to handle uncertainty and imperfection in matching scores. Then, the new fuzzy matching scores are fused with a fuzzy aggregation operator, and the final decision is given. Experimental results on well-known benchmark databases show that our method significantly improves single best biometric matcher performance, and reaches comparable results to several relevant methods. Moreover, the proposed method exhibits high robustness to small size of client training data.

Keywords: Multi-biometric; Verification; Score level fusion; Fuzzy set theory; Fuzzy pattern recognition

1. Introduction

A biometric system is essentially a pattern recognition system that recognizes a person based on his feature vector [1]. This latter is derived from a specific physiological or behavioral characteristic that the person possesses. Biometric systems based on a single biometric suffer from limitations such as the lack of uniqueness, non-universality of the chosen biometric trait, spoof attacks, and sensitivity to noise [2]. Multi-biometric systems, which fuse information from multiple biometric sources, have been developed in order to overcome these problems and to achieve better recognition performance [3]. The technique implementation of a multi-biometric system requires the information fusion methods. These methods of fusion can be done at various levels [4], such as sensor, feature, matching score and decision levels. In the multi-biometric context, the most used method is the fusion at matching score level. In fact, it provides the best trade-off in terms of the information content and the ease in fusion [5].

* Corresponding author.
E-mail address: kld.fakhar@gmail.com (K. Fakhar).

http://dx.doi.org/10.1016/j.fss.2016.05.005
0165-0114/

Several fusion methods at matching score level have been proposed in the literature [6–9]. These methods can be divided into three major categories [6]. The first category is known as transformation-based. Firstly, all the component matching scores are transformed onto a comparable scale. Then, simple fusion rules are applied on the transformed matching scores. However, this category is data-dependent and requires extensive empirical evaluation [2,10,11]. The second category of fusion scheme is called density-based. It requires explicit joint densities estimation of the genuine and imposter matching scores, and the fusion is carried out by statistical tests, such as the likelihood ratio test [12], that is an optimal fusion method. Indeed, it minimizes the probability of error when a large number of representative training matching scores are available [6,13]. The third category is classifier-based. In such a case, the component matching scores are concatenated into new feature vectors which are used to train a new classifier [8,14,15]. However, a large training set is required to build an optimal classifier.

Among the different fusion approaches proposed in the above categories, statistical pattern recognition is the most successful approach to biometric score fusion problem [5,6,12]. Indeed, it produces a sound methodological background for the treatment of large data sets. Furthermore, its principal advantage over the other methods is clear when the mechanism of matching score generation is stable and identifiable. Nevertheless, the matching scores are never controlled by such mechanisms. This is due to the noise presented in the sensor during the acquisition of the biometric signal and the errors made by the feature extraction and matching processes [2]. The results of the application of statistical pattern recognition methods to such data cannot be interpreted precisely enough. Therefore, there is a need to use more flexible methodology that allows to deal with uncertain and imprecise information. Fuzzy pattern recognition approach [16–18], seems to be an appropriate tool to cope with such problems. This approach based on fuzzy set theory [19], offers problems solving tool between the precision of classical mathematics and the uncertainty of real world.

This paper introduces a novel approach for biometric score fusion that considers the problem as a fuzzy pattern recognition one, where the matching score space is considered as consisting of two fuzzy sets ("genuine" and "impostor"). Indeed, the proposed method models each biometric matcher as a membership function, using an automatic generation method, in order to handle uncertainty and imperfection in matching scores. Furthermore, we exploit the fuzzy aggregation operator in order to improve the final decision.

The rest of the paper is organized as follows. First, we describe the proposed method in the next section. Then, the proposed method is evaluated through simulation results in section 3. Finally, the conclusion ends this paper.

2. Proposed biometric score fusion

2.1. Fuzzy sets in biometric score fusion problem

To formulate the biometric score fusion problem within the fuzzy pattern recognition, we propose to express each biometric matcher n as a mapping:

$$\mathcal{F}_n : \mathbf{V}_n \rightarrow \{\text{genuine, impostor}\}, \tag{1}$$

where $\mathbf{V}_n$ is the feature space and $\mathcal{F}_n$ is formed as follows:

- Let $v_Q^n \in \mathbf{V}_n$ be the query feature vector associated to the claimed identity I, $v_I^n \in \mathbf{V}_n$ is a stored template corresponding to the identity I and x_n is the matching score between v_Q^n and v_I^n. Using the fuzzy if–then rule, we can consider an unique rule of the form:

$$\mathrm{R}_n : \text{ if } v_Q^n \text{ is CLOSE TO } v_I^n \text{ then the user is genuine.} \tag{2}$$

- Using fuzzy set theory, we can associate, with the linguistic term 'CLOSE TO', a fuzzy set A_n^I represented by a membership function $\mu_{A_n^I}$. The membership value $\mu_{A_n^I}(v_Q^n)$ can take values between 0 and 1, where 0 represents the perfect reject and 1 represents the perfect accept. According to [20], it is commonly assumed that the membership value for any vector v_Q^n is related to its similarity with its ideal prototype v_I^n. We can therefore deduce that:

$$\mu_{A_n^I}(v_Q^n) = \mu_{\mathcal{C}}(x_n), \tag{3}$$

where $\mathcal{C}$ is a fuzzy set that represents the "genuine" class and $\mu_{\mathcal{C}}$ is its membership function. The membership value $\mu_{\mathcal{C}}(x_n)$ represents the degree of belonging of x_n to the genuine class.

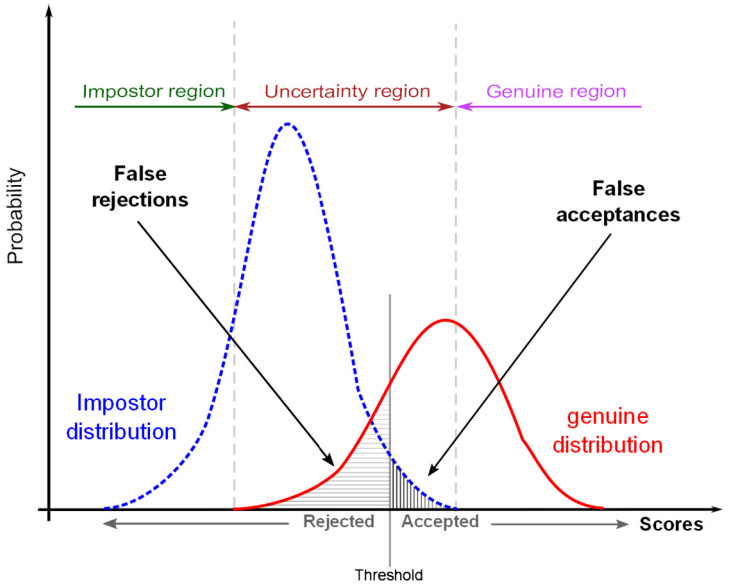

Fig. 1. An example of matching score distribution for a practical biometric system.

- The fuzzy output is regarded as a fuzzy matching score $s_{\mathcal{F}_n} \in [0, 1]$ and it is computed as follows:

$$s_{\mathcal{F}_n} = \mu_{\mathcal{C}}(x_n). \tag{4}$$

Let $[x_1, \cdots, x_N]$ denote the matching scores of N biometric matchers, where x_n is the matching score provided by the nth matcher, $n = 1, \cdots, N$. According to a fuzzy pattern recognition point of view, the matching score space is divided into two fuzzy sets: $\mathcal{C}$ for the genuine class and $\mathcal{I}$ for the impostor class. Therefore, the new output of each biometric matcher is a fuzzy matching score $s_{\mathcal{F}_n}$ that represents the degree of belonging of x_n to the fuzzy set $\mathcal{C}$, i.e., $s_{\mathcal{F}_n} = \mu_{\mathcal{C}}(x_n)$. To find the final membership grade, all fuzzy matching scores $[s_{\mathcal{F}_1}, \cdots, s_{\mathcal{F}_N}]$ must be aggregated. To accept or reject the claimed identity I, the task is to assign the combined membership grade to genuine or impostor class.

The final decision rule for the proposed method is obtained by applying a decision threshold $\theta_{\mathcal{F}}$ as follows:

$$I \in \begin{cases} \text{genuine}, & \text{if } F(s_{\mathcal{F}_1}, \cdots, s_{\mathcal{F}_N}) \geq \theta_{\mathcal{F}}, \\ \text{impostor}, & \textit{otherwise} \end{cases} \tag{5}$$

where F is a fuzzy aggregation operator. The next task is to determine an appropriate fuzzy membership function $\mu_{\mathcal{C}}$ and to choose an effective fuzzy aggregation operator F.

2.2. Determination of the membership function

The determination of membership function is an important step in many applications of fuzzy set theory. Indeed, the success of these applications depends on the membership functions used. Although membership functions can be constructed from (training) data when it is available, the choice of the method depends on the desired application. They are commonly modeled by a parametric representation.

The fuzzy set $\mathcal{C}$ is characterized by its membership function $\mu_{\mathcal{C}}$, which maps each matching score x to the unit interval [0, 1]. This function describes the degree of belonging of x to the fuzzy set $\mathcal{C}$. The membership value $\mu_{\mathcal{C}}(x)$ varies from 0 to 1, where the value of 1 implies that the user is genuine and the value of 0 implies that the user is impostor. A perfect biometric system must always accept genuine users and reject imposter users correctly. In that case, $\mathcal{C}$ is equivalent to a classical set and $\mu_{\mathcal{C}}$ is its characteristic function that is a particular case of the membership function, which has the value 1 for all genuine matching scores and the value 0 for all impostor matching scores.

Unfortunately, a practical biometric system is not perfect and sometimes makes errors. This is due to many factors such as intra-class similarity, inter-class variance, noise and low sampling quality [2,5]. As illustrated in Fig. 1,

a practical biometric system can make two types of errors, namely, false rejection and false acceptance. These errors are caused by the region of overlap between the genuine and impostor matching score distributions. In this case, the matching score space can be divided into three distinct regions (see Fig. 1). The first region is the impostor region which contains only impostor matching scores. The membership values of all matching scores x of this region are equal to zero, i.e., $\mu_{\mathcal{C}}(x) = 0$. The second region is the uncertainty region which contains both genuine and impostor matching scores. In this region, the membership value of each matching score is between 0 and 1, i.e., $\mu_{\mathcal{C}}(x) \in (0, 1)$. The third region is the genuine region which contains only genuine matching scores. The membership values of all matching scores x of this region are equal to one, i.e., $\mu_{\mathcal{C}}(x) = 1$. Therefore, the general formula of the membership function $\mu_{\mathcal{C}}$ can be define as follows:

$$\mu_{\mathcal{C}}(x) = \begin{cases} 0 & \text{if} \quad x \leq \alpha, \\ f(x) & \text{if} \quad \alpha < x < \beta, \\ 1 & \text{if} \quad x \geq \beta, \end{cases} \tag{6}$$

where (α, β) is the uncertainty region, f is a monotonic increasing function defined on (α, β), and bounded between 0 and 1.

In biometric recognition context, the uncertainty region is the region where the false accept rate (FAR) and false reject rate (FRR) are non-zero, i.e., $(\alpha, \beta) = (x_{\mathsf{zeroFAR}}, x_{\mathsf{zeroFRR}})$, where $FAR(x_{\mathsf{zeroFAR}}) = FRR(x_{\mathsf{zeroFRR}}) = 0$. In practice, both x_{zeroFAR} and x_{zeroFRR} are estimated from a training data set. Therefore, in the test data set, we can find genuine matching scores into the impostor region and/or impostor matching scores into the genuine region. Accordingly, we propose to extend this area between x_{oneFAR} and x_{oneFRR}, where x_{oneFAR} and x_{oneFRR} are the points in the matching score space where the FAR and FRR are equal to one, respectively.

In the literature, piecewise-linear membership functions are preferred, because they are simple and easily manipulated by fuzzy operators [21]. Therefore, this work propose to define the function f as a piecewise-linear monotonic increasing function as:

$$f(x) = \begin{cases} a\left(\frac{x - x_{\mathsf{oneFAR}}}{x_{\mathsf{zeroFRR}} - x_{\mathsf{oneFAR}}}\right) & \text{if} \quad x_{\mathsf{oneFAR}} < x \leq x_{\mathsf{zeroFRR}}, \\ a + (c - a)\left(\frac{x - x_{\mathsf{zeroFRR}}}{x_{\mathsf{EER}} - x_{\mathsf{zeroFRR}}}\right) & \text{if} \quad x_{\mathsf{zeroFRR}} < x \leq x_{\mathsf{EER}}, \\ c + (b - c)\left(\frac{x - x_{\mathsf{EER}}}{x_{\mathsf{zeroFAR}} - x_{\mathsf{EER}}}\right) & \text{if} \quad x_{\mathsf{EER}} < x \leq x_{\mathsf{zeroFAR}}, \\ b + (1 - b)\left(\frac{x - x_{\mathsf{zeroFAR}}}{x_{\mathsf{oneFRR}} - x_{\mathsf{zeroFAR}}}\right) & \text{if} \quad x_{\mathsf{zeroFAR}} < x < x_{\mathsf{oneFRR}}, \end{cases} \tag{7}$$

where x is a matching score, x_{EER} is the equal error rate (EER) point, $FAR(x_{\mathsf{zeroFAR}}) = FRR(x_{\mathsf{zeroFRR}}) = 0$, and $FAR(x_{\mathsf{oneFAR}}) = FRR(x_{\mathsf{oneFRR}}) = 1$. Fig. 2 shows the shape of this membership function.

2.3. Estimation of the membership function parameters

The shape of the membership function $\mu_{\mathcal{C}}$ can be determined by three parameters a, b, and c. Therefore, the problem becomes to find a combination of the parameters such that the corresponding biometric matcher has a minimum classification error. The main objective of any biometric system operating at the matching score level, is to reduce the genuine/imposter distribution overlap. A small overlap region between these two distributions tends to produce less classification error. Therefore, the optimum value of parameters a, b, and c can be obtained by minimizing this overlap region.

Although minimizing the overlap region is equivalent to minimizing the classification error, this latter cannot be used to determine the membership function parameters. Indeed, the transformation of the matching scores data set into fuzzy space does not change the classification error of this data set. It is interesting to note that minimizing the overlap region is also equivalent to maximizing the separation between genuine and impostor matching score distributions, e.g., Fisher-ratio for a two-class problem [22], d-prime [23], and F-ratio [24]. Hence, the class separability measure can be used to determine the membership function parameters, especially the F-ratio measure, because it is directly related to the classification error EER [24]. The F-ratio gives an indication of the separation between the genuine and impostor matching score distributions as follows:

$$\text{F-ratio} = \frac{\mu_g - \mu_i}{\sigma_g + \sigma_i}. \tag{8}$$

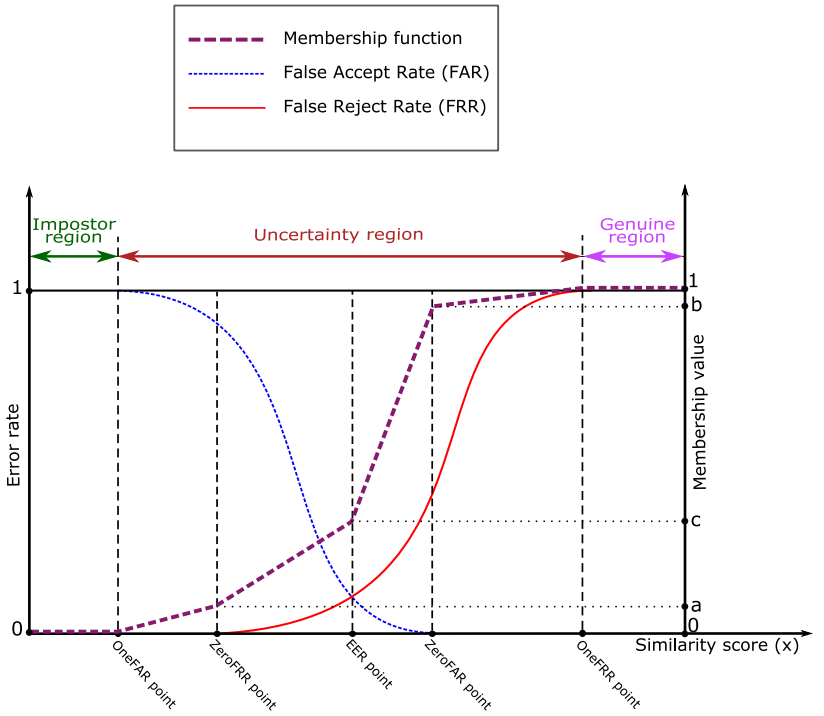

Fig. 2. The membership function $\mu_{\mathcal{C}}$ of the fuzzy set $\mathcal{C}$.

where μ's and σ's are the means and standard deviations, respectively, of the genuine and impostor matching score distributions.

Changing parameter values of the membership function will lead to different fuzzy matching score distributions, thus different values of the F-ratio. Consequently, the F-ratio of Eq. (8) can be regarded as a function of the parameter set $p = (a, c, b)$ and can be written as:

$$\text{F-ratio}\left(\mathcal{X}_{\text{impostor}}; \mathcal{X}_{\text{genuine}}; p\right) = \frac{\mu_g^{fuzzy} - \mu_i^{fuzzy}}{\sigma_g^{fuzzy} + \sigma_i^{fuzzy}} \tag{9}$$

where $\mathcal{X}_{\text{genuine}}$ and $\mathcal{X}_{\text{impostor}}$ are the (training) data set of the genuine and impostor matching scores, respectively, μ^{fuzzy}'s and σ^{fuzzy}'s are the means and standard deviations, respectively, of the genuine and impostor *fuzzy* matching score distributions. The problem becomes to find the best set parameters $p_{\text{best}} = (a_{\text{best}}, c_{\text{best}}, b_{\text{best}})$ that maximize F-ratio of Eq. (9) as follows:

$$p_{\text{best}} = \arg\max_{p} \left\{ \text{F-ratio}(\mathcal{X}_{\text{impostor}}; \mathcal{X}_{\text{genuine}}; p) : \ 0 \le a \le c \le b \le 1 \right\}. \tag{10}$$

There are some heuristic methods that can be used to optimize Eq. (10) efficiently. This paper propose to use the Differential Evolution (DE) algorithm [25], because it is a very simple algorithm, having only a few control parameters, and it is arguably one of the most powerful real parameter optimizers of current interest [26]. The idea in DE algorithm is to start with a randomly generated initial population, which is then improved using mutation, recombination or crossover, and selection operations. Only the last three steps are repeated into the subsequent DE generations. The generations continue until satisfying the termination criterion. A predefined upper limit G_{max} for the number of generations is usually used. The DE algorithm steps can be summarized as follows:

- *Generate initial population:* Let $P^{(g)} = \{p_1^{(g)}, p_2^{(g)}, \ldots, p_{NP}^{(g)}\}$ denote the population after g generations (0 is an initial generation), where NP is the population size and $p_i^{(g)} = (a_i^{(g)}, c_i^{(g)}, b_i^{(g)})$ is a decision vector of the population, $i = 1, 2, \ldots, NP$. The initial population ($g = 0$) is randomly generated from an uniform distribution as follows:

$$p_i^{(g=0)} = \text{sort}\Big(rand_{i,1}[0,1], rand_{i,2}[0,1], rand_{i,3}[0,1]\Big) \quad i = 1, 2, \ldots, NP, \;\; NP \geq 4. \tag{11}$$

where sort() represents a function that sorts the vector elements in ascending order, to verify the property that f of Eq. (6) should be a monotonic increasing function. $rand_{i,j}[0,1]$, $j = 1, 2, 3$, represents an uniformly distributed random variable within the range $[0, 1]$ for each i and j.

- *Mutation process:* In the mutation process, NP mutant vectors $v_i^{(g)}$, $i = 1, 2, \ldots, NP$, is generated from three individuals chosen randomly, with indexes r_1, r_2 and r_3, using a scale factor F, as follows:

$$v_{i,j}^{(g)} = p_{r_1,j}^{(g)} + F\left(p_{r_2,j}^{(g)} - p_{r_3,j}^{(g)}\right), \quad r_1 \neq r_2 \neq r_3 \neq i. \tag{12}$$

Note that indexes have to be randomly generated once for each mutant vector. The scale factor F is a predefined positive control parameter.

- *Recombination or crossover process:* In this process, crossover operation is applied to each pair of the target vector $p_i^{(g)}$ and its corresponding mutant vector $v_i^{(g)}$ to generate a trial vector $u_i^{(g)}$ as follows:

$$u_{i,j}^{(g)} = \begin{cases} v_{i,j}^{(g)} \text{ if } rand_{i,j}[0,1] \leq CR \text{ or } j = j_{\text{rand}} \\ p_{i,j}^{(g)} \text{ if } rand_{i,j}[0,1] > CR \text{ or } j \neq j_{\text{rand}} \end{cases} \tag{13}$$

where CR is the crossover rate constant $\in [0, 1]$ and j_{rand} is a randomly chosen index from $\{1, 2, 3\}$.

- *Selection process:* The target vector $p_i^{(g)}$ or trial vector $u_i^{(g)}$ that generates a better solution will be selected as the target vector of the next generation $p_i^{(g+1)}$. The selection formula is shown in Eq. (14):

$$p_i^{(g+1)} = \begin{cases} u_i^{(g)} \text{ if } h(u_i^{(g)}) \leq h(x_i^{(g)}) \\ p_i^{(g)} \text{ otherwise} \end{cases} \tag{14}$$

where h is the F-ratio function defined in Eq. (9).

The pseudo code of the complete algorithm is summarized in Algorithm 1. Fig. 3 shows an example of the membership function $\mu_{\mathcal{C}}$, which is generated automatically by the proposed algorithm 1, of the Speech matcher (PAC, GMM) in the XM2VTS-Benchmark database [27].

2.4. Fuzzy aggregation operator

Aggregation operations on fuzzy sets [28] are operations by which several fuzzy sets are combined in a desirable way to produce a single fuzzy set. Several studies have proposed deploying the fuzzy aggregation operators in a biometric score fusion problem [29,30]. These operations are mainly based on general concepts such as fuzzy rules and triangular norms (t-norms and t-conorms). However, the main challenge of the methods based on fuzzy rules is the number of rules used because it grows exponentially with the number of biometric matcher, and triangular norms have the same behavior whatever the values of the information to combine (i.e., t-norms are conjunctive in nature and t-conorms are disjunctive in nature). In this work, we use symmetric sums to combine membership functions because they could be conjunctive (if the sources of information have low conflicting evidences) or disjunctive (if the sources of information have high conflicting evidences) depending on the values of the variables involved.

A binary symmetrical sum [31] is defined as an operator σ from $[0, 1] \times [0, 1]$ in $[0, 1]$ such that: σ is commutative, increasing both arguments, continuous, auto-dual, and $\sigma(0, 0) = 0$. Moreover, $\sigma(1, 1) = 1$. According to [31] any symmetric sum has the following form:

$$\sigma(x, y) = \frac{g(x, y)}{g(x, y) + g(1 - x, 1 - y)}, \tag{15}$$

Inputs : $\mathcal{X}_{\text{genuine}},\ \mathcal{X}_{\text{impostor}},\ G_{\max},\ NP \geq 4,\ F \in (0, 1+],\ CR \in [0, 1]$
Output: $(a_{\text{best}}, c_{\text{best}}, b_{\text{best}})$

$D \leftarrow 3,\ g \leftarrow 0$
Create a random initial population
for $i \leftarrow 1$ **to** NP **do**
  $p_i^{(g=0)} \leftarrow \text{sort}\Big(rand_1[0,1], rand_2[0,1], rand_3[0,1]\Big)$
  $h_i^{(g=0)} \leftarrow \text{F-ratio}\left(\mathcal{X}_{\text{impostor}}; \mathcal{X}_{\text{genuine}}; p_i^{(g=0)}\right)$
end
for $g \leftarrow 1$ **to** G_{max} **do**
  for $i \leftarrow 1$ **to** NP **do**
    Mutation and Crossover process
    Select randomly $r_1, r_2, r_3 \in \{1, 2, \ldots, NP\},\ r_1 \neq r_2 \neq r_3 \neq i$
    $j_{\text{rand}} \leftarrow randint(1, D)$ ▷ returns an integer number between 1 and D
    for $j \leftarrow 1$ **to** D **do**
      if $j == j_{rand}$ **or** $rand_j[0,1] \leq CR$ **then**
        $u_{i,j}^{(g)} \leftarrow p_{r_1,j}^{(g)} + F\left(p_{r_2,j}^{(g)} - p_{r_3,j}^{(g)}\right)$
        $u_{i,j}^{(g)} \leftarrow \max(u_{i,j}^{(g)}, 1)$ ▷ verify boundary constraints
        $u_{i,j}^{(g)} \leftarrow \min(u_{i,j}^{(g)}, 0)$
      else
        $u_{i,j}^{(g)} \leftarrow p_{i,j}^{(g)}$
      end
    end
    $u_i^{(g)} \leftarrow \text{sort}\left(u_i^{(g)}\right)$ ▷ $a_i^{(g)} \leq c_i^{(g)} \leq b_i^{(g)}$
    $h_i^{(g)} \leftarrow \text{F-ratio}\left(\mathcal{X}_{\text{impostor}}; \mathcal{X}_{\text{genuine}}; p_i^{(g)}\right)$
    Selection process
    if $h_i^{(g-1)} \leq h_i^{(g)}$ **then**
      $p_i^{(g+1)} \leftarrow u_i^{(g)}$
      $h_i^{(g+1)} \leftarrow h_i^{(g)}$
    else
      $p_i^{(g+1)} \leftarrow p_i^{(g)}$
      $h_i^{(g+1)} \leftarrow h_i^{(g-1)}$
    end
  end
  $i\text{best} \leftarrow \arg\max_i(h_i^{(g+1)})$
  $(a_{\text{best}}, c_{\text{best}}, b_{\text{best}}) \leftarrow p_{i\text{best}}$
end

Algorithm 1. Pseudo code of the complete algorithm.

for some function g such that: g is positive, continuous, increasing, and $g(0, 0) = 0$. The operator σ is commutative if g is symmetric. Moreover, σ is quasi-associative if g is associative. In fact, any function satisfies all properties of the function g could be used. However, it should be able to give a good results. For n sources, $g(x, y)$ has to be changed into $g(x_1, \cdots, x_n)$ [32]. The function g considered in this paper is defined as:

$$g(x_1, \cdots, x_n) = \sum_{i=1}^{n} \left(\sqrt{x_i}\right)^2. \tag{16}$$

It is immediate that g is a positive, continuous and increasing function satisfying $g(0, \cdots, 0) = 0$.

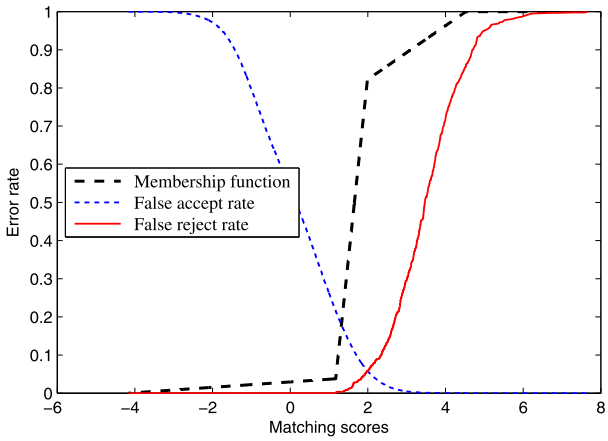

Fig. 3. Example of the membership function $\mu_{\mathcal{C}}$ of the Speech matcher (PAC, GMM) in the XM2VTS-Benchmark database ($G_{\max} = 100$, $NP = 30$, $F = 0.5$, $CR = 0.9$).

3. Experimental results

The performance of the proposed method is evaluated using two publicly available databases. The first database is the XM2VTS-Benchmark database [27], which contains the matching scores from synchronized face video and speech data of 295 subjects. The matching scores are computed from five face matchers and three speech matchers. The experimental protocol for this database is clearly defined according to the Lausanne Protocol-1 (see [27] for details). First, there is an evaluation set, which is used to estimate the parameters, and then there is a test set which is used to evaluate the performance. In total, the evaluation set has 600 genuine and 40 000 impostor scores, and the test set has 400 genuine and 111 800 impostor scores.

The second database used in the experiments is the NIST-BSSR1 [33], which contains three different partitions. The first partition is the NIST-Multimodal database which is composed of two face scores and two fingerprint scores from 517 subjects. This partition consists of 517 genuine and 266 772 imposter scores. The second partition, is the NIST-Fingerprint database which is composed of two fingerprint scores from 6 000 subjects. This database consists of 6 000 genuine and 35 994 000 imposter scores. Finally the third partition is the NIST-Face database which is composed of two face scores from 3 000 subjects. In this partition there are $2 \times 3\,000$ genuine and $2 \times 8\,997\,000$ impostor scores. For these databases there is no experimental protocol defined. In our experiments, half of the impostor and the genuine scores were randomly selected to form the training set and the remaining half is used to form the testing set. Reported results are average values over the 20 trials. To compare the performance of the proposed method with existing ones, we have also implemented three other typical score fusion methods, namely, (i) sum rule-based fusion preceded by min–max normalization, (ii) likelihood ratio-based fusion with Gaussian Mixture Model (LLR-GMM) and (iii) SVM-based fusion.

Fig. 4 shows the receiver operating characteristic (ROC) curves for the three partitions of the NIST-BSSR1 and XM2VTS-Benchmark databases of the proposed method, the individual matchers, and the state of the art methods. By comparing the obtained results, we first notice that the proposed method provides a significantly better rate than the best single modality of all the four databases. Then, we notice that the performance of the proposed method has similar performance compared to likelihood ratio-based fusion and SVM-based fusion. On the other side, we remark that while the performance of sum rule-based fusion is comparable to proposed method on the NIST-Multimodal and the NIST-Fingerprint databases (see Figs. 4b and 4c), it is less efficient than the proposed method on the NIST-Face and XM2VTS-Benchmark databases (see Figs. 4a and 4d). As detailed in [6], those results are due to the fact that the min-max normalization is not effective for these databases. However, if we carefully choose the normalization scheme better fusion performance can be achieved.

As stated before, the size of training data impacts the fusion performance. This is why we further investigated the influence of the size of training data, particularly the client training data, by comparing the results on different sizes, namely, 100%, 50%, 10%, and 1% from the original client training data. In Fig. 5, the mean and the standard deviation of Equal Error Rate (EER) on the NIST-Face database is displayed for the all fusion methods, at different sizes of

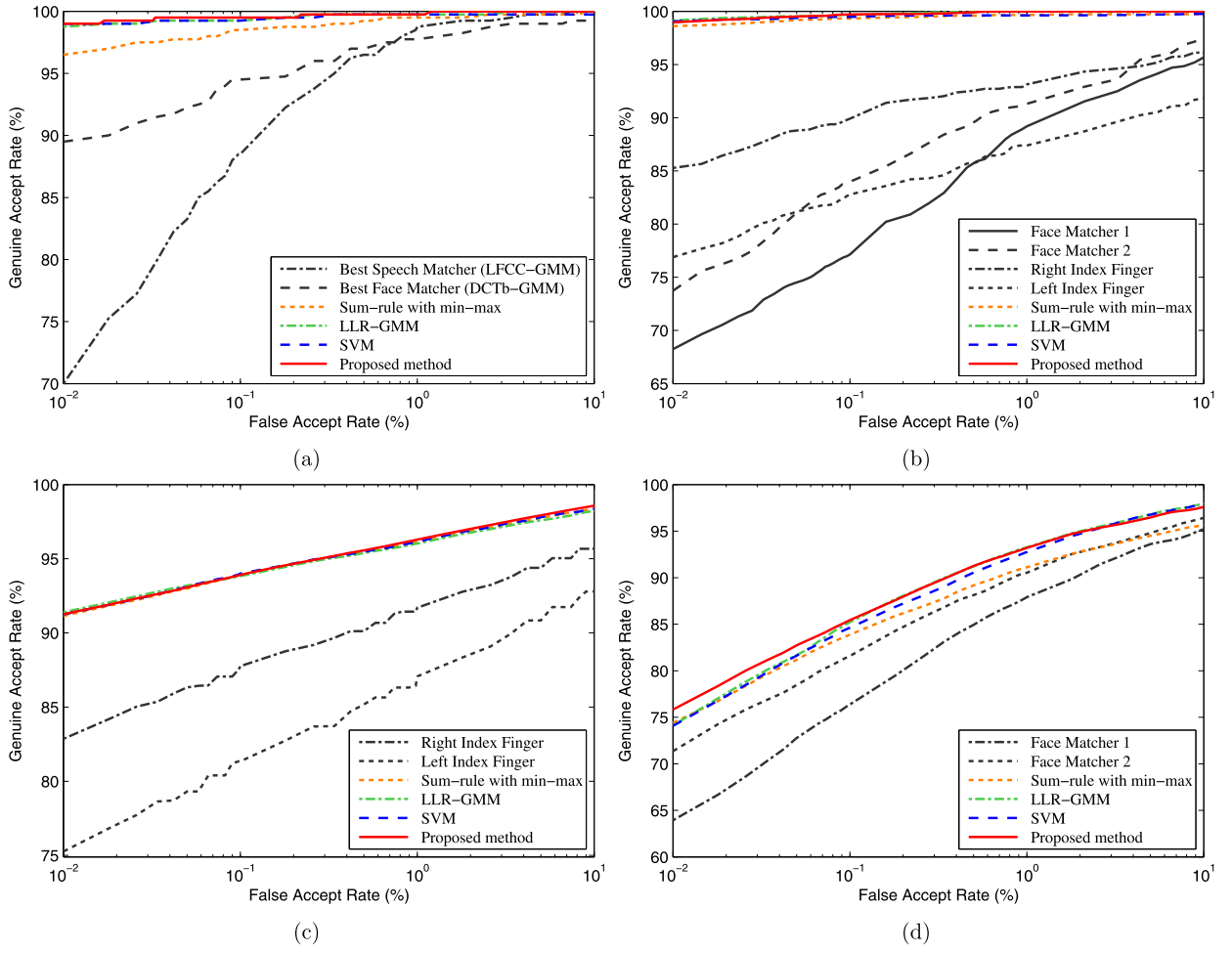

Fig. 4. Comparison of the fusion results in terms of ROC on the (a) XM2VTS-Benchmark (in this database the results are achieved by the fusion of eight available matchers, but we show only the ROC curves of the best face matcher and the best speech matcher for clarity), (b) NIST-Multimodal, (c) NIST-finger, and (d) NIST-face databases. A SVM with radial basis function kernel is used in all databases, and its parameters tuning are done by cross validation and grid search.

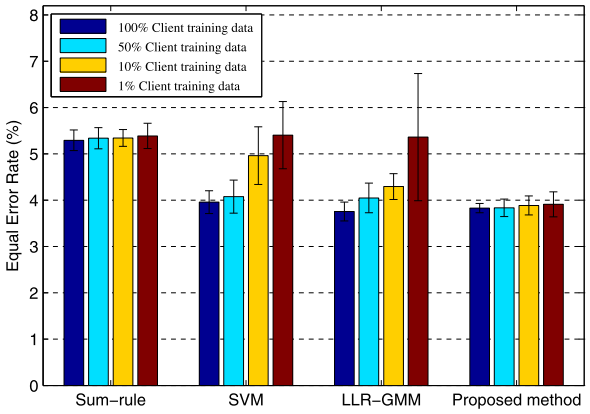

Fig. 5. Comparison of the fusion results in terms of EER on the NIST-face database. The mean and the standard deviation of EER is plotted for four different sizes of the client training data: 100%, 50%, 10% and 1%.

client training data. These results show that EERs for the proposed method and the sum rule-based fusion increase slowly when the size of client training data decreases, in contrast to EERs for the likelihood ratio-based fusion and SVM-based fusion, which increase when the size of client training data decreases. This is due to the fact that both methods require a large number of representative training matching scores, in order to estimate the joint densities of the matching scores (for the likelihood ratio-based fusion), or to train the relevant classification parameters (for the SVM-based fusion).

4. Conclusion

This paper introduces a new method for biometric score fusion problem based on fuzzy set theory. In this method, each individual matcher is modeled as a fuzzy pattern recognition system. We have validated the proposed method on several multi-biometric databases. The method improved single biometric matchers performance significantly, and demonstrated competitive fusion performance compared to more relevant methods. In addition, the method exhibited high robustness to small size of client training data.

References

[1] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Trans. Circuits Syst. Video Technol. 14 (1) (2004) 4–20.
[2] A.K. Jain, K. Nandakumar, A. Ross, Score normalization in multimodal biometric systems, Pattern Recognit. 38 (12) (2005) 2270–2285.
[3] A. Ross, A.K. Jain, Information fusion in biometrics, Pattern Recognit. Lett. 24 (2003) 2115–2125.
[4] A. Ross, A.K. Jain, Multimodal biometrics: an overview, in: Proceedings of 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, 2004, pp. 1221–1224.
[5] A. Ross, K. Nandakumar, A.K. Jain, Handbook of Multibiometrics, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
[6] K. Nandakumar, Y. Chen, S.C. Dass, A.K. Jain, Likelihood ratio based biometric score fusion, IEEE Trans. Pattern Anal. Mach. Intell. 2 (30) (2008) 342–347.
[7] C. Bergamini, L.S. Oliveira, A.L. Koerich, R. Sabourin, Combining different biometric traits with one-class classification, Signal Process. 89 (11) (2009) 2117–2127.
[8] H.F. Liau, D. Isa, Feature selection for support vector machine-based face-iris multimodal biometric system, Expert Syst. Appl. 38 (9) (2011) 11105–11111.
[9] Q. Tao, R. Veldhuis, Robust biometric score fusion by naive likelihood ratio via receiver operating characteristics, IEEE Trans. Inf. Forensics Secur. 8 (2) (2013) 305–313.
[10] K.-A. Toh, X. Jiang, W.-Y. Yau, Exploiting global and local decisions for multimodal biometrics verification, IEEE Trans. Signal Process. 52 (10) (2004) 3059–3072.
[11] R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, Large scale evaluation of multimodal biometric authentication using state-of-the-art systems, IEEE Trans. Pattern Anal. Mach. Recogn. 27 (3) (2005) 450–455.
[12] P. Griffin, Optimal biometric fusion for identity verification, Technical Report RDNJ-03-0064, Identix Research.
[13] S.C. Dass, K. Nandakumar, A.K. Jain, A principled approach to score level fusion in multimodal biometric systems, in: Proc. Audio- and Video-Based Biometric Person Authentication, 2005, pp. 1049–1058.
[14] C. Sanderson, K. Paliwal, Information fusion and person verification using speech and face information, Tech. Rep., IDIAP, Switzerland, 2002.
[15] Y. Wang, T. Tan, A.K. Jain, Combining face and iris biometrics for identity verification, in: Proc. 4th Int. Conf. AVBPA, 2003, pp. 805–813.
[16] L. Kuncheva, Fuzzy Classifier Design, Springer-Verlag, Heidelberg, 2000.
[17] S. Mitra, S.K. Pal, Fuzzy sets in pattern recognition and machine intelligence, Fuzzy Sets Syst. 156 (3) (2005) 381–386.
[18] W. Pedrycz, Fuzzy sets in pattern recognition: accomplishments and challenges, Fuzzy Sets Syst. 90 (2) (1997) 171–176.
[19] L.A. Zadeh, Fuzzy sets, Inf. Control 3 (8) (1965) 338–353.
[20] D. Majumder, Fuzzy sets in pattern recognition, image analysis and automatic speech recognition, Apl. Mat. 30 (4) (1985) 237–254.
[21] S. Medasani, J. Kim, R. Krishnapuram, An overview of membership function generation techniques for pattern recognition, Int. J. Approx. Reason. 19 (3–4) (1998) 391–417.
[22] C. Bishop, Neural Networks for Pattern Recognition, Oxford University Press, 1999.
[23] J. Daugman, Biometric decision landscapes, Tech. Rep. TR482, University of Cambridge Computer Laboratory, 2000.
[24] P. Norman, A. Ross, L. Weifeng, J. Kittler, A user-specific and selective multimodal biometric fusion strategy by ranking subjects, Int. J. Pattern Recognit. Artif. Intell. 46 (12) (2013) 3341–3357.
[25] R. Storn, K.V. Price, Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces, J. Glob. Optim. 11 (1997) 341–359.
[26] S. Das, P. Suganthan, Differential evolution – a survey of the state-of-the-art, IEEE Trans. Evol. Comput. 15 (1) (2011) 4–31.
[27] N. Poh, S. Bengio, Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication, Pattern Recognit. 39 (2) (2006) 223–233.
[28] H.J. Zimmermann, Fuzzy Set Theory and Its Applications, fourth ed., Kluwer Academic Publishers, Dordrecht, 2001.

[29] M. Hanmandlu, J. Grover, A. Gureja, H.M. Gupta, Score level fusion of multimodal biometrics using triangular norms, Pattern Recognit. Lett. 32 (14) (2011) 1843–1850.
[30] R.N. Rodrigues, L.L. Ling, V. Govindaraju, Robustness of multimodal biometric fusion methods against spoof attacks, J. Vis. Lang. Comput. 20 (3) (2009) 169–179.
[31] W. Silvert, Symmetric summation: a class of operations on fuzzy sets, IEEE Trans. Syst. Man Cybern. 9 (10) (1979) 657–659.
[32] I. Bloch, Information combination operators for data fusion: a comparative review with classification, IEEE Trans. Syst. Man Cybern. 26 (1) (1996) 52–67.
[33] National Institute of Standards and Technology: NIST Biometric Scores Set, available at http://www.itl.nist.gov/iad/894.03/biometricscores, 2004.