Score Level Fusion Algorithm Using Differential Evolution and Proportional Conflict Redistribution Rule

Lamia Mezai
Faculté des Nouvelles Technologies
de l'Information et de la Communication
Département d'Informatique Fondamentale et ses Applications
Université Constantine 2 Abdelhamid Mehri
Nouvelle Ville Ali Mendjeli, BP, 67A, Constantine, Algeria
Email: lamia.mezai@gmail.com

Fella Hachouf
Faculté des Sciences de la Technologie
Département d'Electronique
Laboratoire d'Automatique et de Robotique
Université des Frères Mentouri
Route Ain El Bey 25000, Constantine, Algeria
Email: hachouf.fella@gmail.com

***Abstract*—In this paper, a new score level fusion approach is proposed. It is based on Differential Evolution (DE) technique and Proportional Conflict Redistribution fusion rule. DE technique is used to find the best confidence factors of the belief assignments of the different modalities. The fusion of the weighted belief assignments is then performed by Proportional Conflict Redistribution combination rule. Experiments are conducted on the scores of BANCA multimodal dataset. A comparative study is achieved using our method, Proportional Conflict Redistribution combination rule and the SVM based fusion. The experimental results show that the proposed approach improves significantly the performance compared to the well established methods.**

I. Introduction

Biometrics is a statistical measurement of human physiological/behavioural traits. It can be used as an alternative of the traditional security systems based on keys, cards, badges, passwords or PIN numbers. Unimodal biometric systems rely on a single modality, so they are limited against accuracy and vulnerability to spoofing. This is mainly due to many reasons such as imperfect sensor, noisy data, intra-class variation and non universality [8]. To overcome these limitations the fusion of biometric systems has been proposed [8]. Multi biometric systems combine various biometric data at different levels like sensor level, feature extraction level, score level or decision level. The fusion at score level is widely used in biometrics as it is simple and efficient. It is based on the combination of similarity scores of the biometric matchers. Fusion methods at score level are divided into three categories [12] statistical, learning and belief functions based methods. Statistical techniques combine the scores of the different unimodal matchers by using various basic statistical rules such as sum, product, Max and Min. Learning techniques classify multimodal scores into one of the two classes: genuine or impostor. The main techniques are support vector machine (SVM), Bayesian inference and neural networks (NN). Belief functions are used to convert the scores into belief assignments which are mixed by a combination rule based on Dempster Shafer and Dezert-Smarandache theories.

The main problem with statistical and learning fusion techniques appears when different unimodal biometric systems produce highly conflicting results. These methods are not able to handle this conflict and the fusion performance is not enhanced. In opposition, belief functions can manage the conflict between many unimodal biometric systems [12]. The integration of evolutionary methods in a multi biometric system for selecting the best fusion rule and estimating its parameters has given promising results [13], [10], [1], [3] and [4]. But, these techniques are focused on using transformation methods like weighted sum rule, product, exponential sum and tanh hyperbolic sum. Other fusion approaches such as learning and belief functions methods have not been used with evolutionary methods. In order to improve the verification performance of several biometric systems, a framework for multi-biometric fusion is proposed. It combines belief functions with evolutionary methods. This choice is justified by the fact that belief functions manage the conflict between several classifiers and the evolutionary techniques like DE allows better parameters estimation.

This paper is composed of four sections. In section 2, the related work is discussed. In section 3, the proposed method is described. In section 4, the experimental results are presented. In section 5, the paper is concluded.

II. Related Work

Recently, the design and the development of a multimodal biometric system which automatically selects the best fusion rule and estimates its parameters has become one of the most active research areas. In literature, some works have been proposed. Most of them use evolutionary methods such as Particle Swarm Optimization (PSO) or Differential Evolution (DE).

An adaptive multimodal biometric fusion algorithm (AMBF) has been proposed by Veeramachaneni et al. [13]. It is based on a Bayesian decision fusion and PSO. A Bayesian framework has been employed to combine the decisions of several biometric classifiers. PSO has been used to search the best decision fusion rule and the threshold at a desired security level. This algorithm has been tested only on simulated data to investigate its performance. The data distribution is assumed to be Gaussian which is not true for several biometric systems.

A method for enhancing the performance of correlated biometric classifiers is suggested by Srinivas et al. [10]. It is based on the weighted sum rule and PSO. PSO has been used to compute the weight for each classifier. A Bayesian risk function is used as a fitness function. This approach has been tested on the NIST BSSR dataset and on a synthetic scores generated by a multivariate normal distribution. The experiments have shown that this method outperforms the classical weighted sum rule.

A Particle Swarm Optimization scheme in the weighted sum rule is proposed by Anzar et al. [1]. In this approach, the d-prime statistics has been used to measure the separation between the genuine and the impostor score distribution. It is calculated for both of fingerprint and voice modalities. The weight of each modality is based on the ratio of these two statistics. The best weights are estimated by PSO. This method has been studied under various noise conditions. It has decreased the FAR (False Acceptance Rate) even at low conditions. The recognition rate is enhanced above 0 dB SNR (Signal to Noise Ratio). However, this method presents poor results under noise conditions (for SNRs <0 dB).

An evolutionary approach for adaptive combination of multiple biometric systems is presented by Kumar et al. [3]. This adaptive combination consists on selecting the optimal fusion strategy and estimating its parameters by using a hybrid PSO. The score level fusion rules used in this work are sum, product, exponential sum and tanh hyperbolic sum. This approach has been tested on real and simulated biometric data. The experiments have illustrated that this approach achieves good and stable performance over the fusion at the decision level based on PSO.

DE has been used by Mukherjee et al. [4]. It is employed to adjust tunable parameters of an adaptive weight and exponent based function which maps the matching scores from different biometric sources into a single matching score. DE is used to minimize the overlapping area of the distribution of the genuine and impostor scores. This method has been tested on two databases of 4 modalities (fingerprint, iris, left ear and right ear). The experiments have shown that this method outperforms the conventional score level fusion rules: sum, product, tanh, exponential. The disadvantage of this technique is the number of parameters to be estimated.

III. Proposed methodology

In the mentioned works [13], [10], [1], [3] and [4], the integration of evolutionary methods in a multi biometric system to choose the best fusion rule or find its parameters has given promising results. These works have only used combination rules such as: or, and, sum, product, exponential sum and tan-hyperbolic sum rules. To our knowledge, there is no work which uses evolutionary methods combined to other fusion techniques such as learning and belief functions methods. So, in this work, we propose the fusion of several unimodal biometric systems for person verification using belief functions and evolutionary method. This choice is justified by the fact that the belief functions can deal with the conflict between the different classifiers and the evolutionary techniques like DE allow the best parameters estimation.

The proposed method consists of two steps: training and testing as depicted on figure 1. In the training step, DE technique is used to find the best parameters on the training dataset. The testing step consists on the several steps. First, the score of each biometric system is transformed into belief assignment by using the best parameters obtained by DE. Next, the fusion is performed by Proportional Conflict Redistribution combination rule. Finally, in the decision step, a person is classified as a genuine or an impostor by using the best decision threshold calculated by DE.

A. Training step

The training step consists on two steps. First, all training scores of the dataset are transformed into belief assignments. Then, DE technique is used to find the best parameters.

1) Transformation of the training scores into masses: Generally, in a verification biometric system, the classification step is formulated as a two class problem. The two classes are genuine θ_{gen} and impostor θ_{imp}. So, $\Theta = \{\theta_{gen}, \theta_{imp}\}$ is used as a frame of discernment.

In this step, each training score of the dataset which is provided by each unimodal biometric system is transformed into three masses: the mass of genuine θ_{gen}, the mass of impostor θ_{imp} and the mass of the uncertainty $\theta_{gen} \cup \theta_{imp}$. This transformation is performed with Appriou [2] model which is defined by:

$$\begin{cases} m_i(\theta_{gen}) & = & \alpha_i \times \psi(s_{ij}) \\ m_i(\theta_{imp}) & = & \alpha_i \times (1 - \psi(s_{ij})) \\ m_i(\Theta) & = & 1 - \alpha_i \end{cases} \tag{1}$$

where

i corresponds to the i^{th} unimodal biometric system.

α_i is a confidence factor of the i^{th} unimodal biometric system such as $0 < \alpha_i < 1$.

s_{ij} is the match score of a person j delivered by the i^{th} unimodal biometric system.

ψ is an increasing function which maps the scores in the range [0, 1]. In the experiment, the logistic sigmoid function is used. It is defined by:

$$\psi(s_{ij}) = logsig(s_{ij}) = \frac{1}{1 + exp(-s_{ij})} \tag{2}$$

In this step, α_1, α_2, ..., α_D are fixed to 1 but they are computed by DE in the next section, where D is the number of modalities.

2) Confidence factors estimation using Differential Evolution (DE): Differential Evolution (DE) is one of the evolutionary algorithms. It was proposed by Storn and Price [11]. DE is similar to genetic algorithm. It has a population which is a set of N trial solutions. The parameters to be optimized are represented by a vector $x_{j,G} = [x_{1,j,G}, x_{2,j,G}, ..., x_{D,j,G}]$ where j = 1, 2, ..., N. G is the generation number such as $G = 0, 1, ..., G_{max}$ and G_{max} is the maximum number of generations and D is the number of parameters to be optimized. At the first generation the population is randomly initialized in the search space constrained by the prescribed minimum and maximum bounds. The Mutation, in the DE, consists on a random perturbation about a vector $x_{j,G}$. It is done by randomly selecting three non overlapping vectors $x_{r1,G}$, $x_{r2,G}$ and $x_{r3,G}$ from the population such as the indices j, $r1$, $r2$ and $r3$ are distinct. The donor vector of the $(G+1)^{th}$ generation is calculated by:

$$v_{j,G+1} = x_{r1,G} + F \times (x_{r2,G} - x_{r3,G}) \tag{3}$$

where F is the scaling factor such as $F \in [0.4, 1]$.

After, the trail vector $u_{j,G+1} = [u_{1,j,G+1}, u_{2,j,G+1}, ..., u_{D,j,G+1}]$ is developed from the elements of the vector $x_{j,G}$ and the elements of the donor vector $v_{j,G+1}$ as follow:

$$u_{k,j,G+1} = \begin{cases} v_{k,j,G+1} \quad if \quad rand_{k,j} \leq Cr \quad or \quad k = J_{rand} \\ x_{k,j,G} \quad otherwise \end{cases} \tag{4}$$

where

k = 1, 2, ..., D.

$rand_{k,j}$ is random number generated in the range [0,1].

J_{rand} is a random integer chosen from [1, 2, ..., D] and ensures that $v_{j,G} \neq x_{j,G}$.

Then, the vector $x_{j,G}$ is compared with the trail vector $u_{j,G+1}$ and the one with the lowest fitness function value is admitted to the next generation. This comparison is given by:

$$x_{j,G+1} = \begin{cases} u_{j,G+1} \quad iff(u_{j,G+1}) \leqslant f(x_{j,G}) \\ x_{j,G} \quad otherwise \end{cases} \tag{5}$$

where f is the fitness function.

The following steps are repeated until some stopping criterion is reached or the maximum number of iteration is achieved.

In our approach, DE is used to estimate the confidence factors (α_1, α_2, ..., α_D) with the constraint $0 < \alpha_i < 1$, for $i = 1, 2, ..., D$. Each solution is formed by D confidence factors where D is the number of the modalities. Confidence factors estimation is done by the following steps:

1) Initialisation of DE parameters (the number of the solutions in the population, the values of all population, the maximum number of iterations and F.
2) The transformed training scores are multiplied by the values (confidence factors) of the population.
3) The weighted scores are fused by PCR5 combination rule (see section III-B2).
4) Evaluation of the fitness function by calculating the weighted error rate (WER) over all the range of the scores.
5) If the maximum number of iterations is reached the solution (confidence factors) and the threshold which minimize the WER are saved in order to use them in the testing step.
6) Otherwise the population is updated using equations (3), (4) and (5) and the steps 2 to 5 are repeated.

The weighted error rate (WER) is defined by [11]:

$$WER(\Delta) = C_{FA} \times FAR(\Delta) + (1 - C_{FA}) \times FRR(\Delta) \tag{6}$$

where

C_{FA} varies from 0 to 1, it balances between the costs of FAR and FRR,

FAR is the false acceptance rate,

FRR is the false rejection rate,

Δ is the decision threshold that minimizes the weighted error rate (WER) on a development set.

B. Testing step

In the testing step, the scores provided by several unimodal biometric systems are transformed into belief assignment by using the best confidence factors obtained by DE. Next, the fusion is performed by Proportional Conflict Redistribution combination rule. Finally, in the decision step, a person is classified as a genuine or an impostor by using the best decision threshold calculated by DE.

1) Transformation of the scores into masses: In this step, the scores of an individual which are provided by the D biometric systems are transformed into belief assignment using equation (1). The confidence factors α_1, α_2, ..., α_D are equal to the values computed in section III-A2.

2) Score level fusion by Proportional Conflict Redistribution: In this step, the theory of evidence is used in order to combine the different modalities. This theory is a generalization of the probability theory. It includes many approaches such as Dempster Shafer theory and Proportional Conflict Redistribution rule [9]. In the proposed method, Proportional Conflict Redistribution rule has been used.

In proportional conflict redistribution (PCR) rules [9], five versions are proposed PCR1 to PCR5. PCR5 is the most efficient and accurate for information fusion under uncertainty and conflict since the redistribution of the partial conflicts is performed only to the elements which are truly involved in each partial conflict. This is done according to the proportion or weight of each source. The PCR5 combination rule of two belief functions $m_1(.)$ and $m_2(.)$ over the power set of Θ (i.e. 2^Θ) is given by [9]:

$$m_{PCR5}(A) = m_{12}(A) + \sum_{A,B \in 2^\Theta, A \cap B = \emptyset} \left[\frac{m_1(A)^2 m_2(B)}{m_1(A) + m_2(B)} + \frac{m_2(A)^2 m_1(B)}{m_2(A) + m_1(B)} \right] \tag{7}$$

where

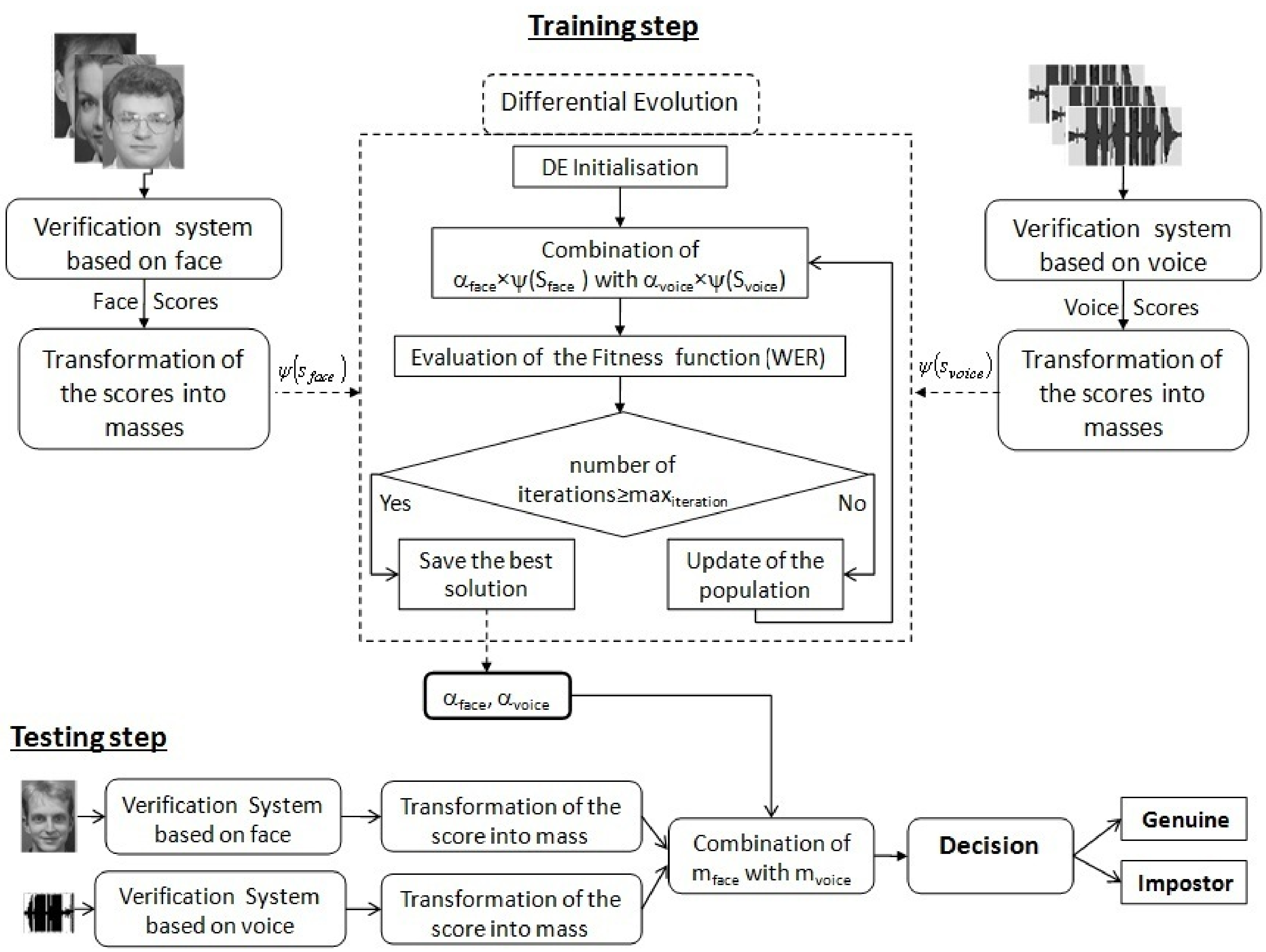


Fig. 1. Flow diagram of the proposed method.

$2^{\Theta} = \{\theta_{gen}, \theta_{imp}, \theta_{gen} \cup \theta_{imp}\}$.

$m_1(.)$, $m_2(.)$ represent the first and the second unimodal biometric system respectively.

$m_{12}(A)$ corresponds to the conjunctive consensus on A between the two sources. It is defined as:

$$m_{12}(A) = \sum_{X,Y \in 2^{\Theta}, X \cap Y = A} m_1(X) m_2(Y) \tag{8}$$

where X and Y are subsets of 2^{Θ}.

Equation (9) is used to combine two modalities. When, there are more then two modalities to be combined, the fusion based on PCR5 is performed pairwise. The first and the second biometric traits are fused and then the obtained belief assignment is fused with the third biometric trait and so on.

3) Decision: In this step, the classification is performed. It consists on classifying a person as a genuine or as an impostor. First, the fused beliefs are transformed into a probability measure by using the pignistic transformation [9] (see (9)). Then, a statistical classification approach such as the likelihood ratio test is employed for computing the final decision (see (10)).

$$betP(X) = \sum_{X \in \Theta, Y \in 2^{\Theta}, Y \neq \emptyset} \frac{|X \cap Y|}{|Y|} \frac{m_{PCR5}(Y)}{1 - m_{PCR5}(\emptyset)} \tag{9}$$

where $|Y|$ denotes the cardinality of Y.

$$Decision = \begin{cases} genuine\ if \dfrac{betP(\theta_{gen})}{betP(\theta_{imp})} \geq \Delta \\ impostor\ otherwise \end{cases} \tag{10}$$

IV. RESULT

To evaluate the performance of the proposed method, the published matching scores of the BANCA benchmark dataset available from [5] are used. This database contains two modalities face and speech. It is captured in four European languages during 12 sessions. In this work, we have only used the English subset because the available free scores are calculated from this subset. The English subset [6] contains 52 subjects which are divided into two sets, called g1 and g2. Each set contains 13 males and 13 females. g1 is used as a development set and g2 is used as an evaluation set.

In the BANCA database, there are 7 different protocols [7]: matched controlled (Mc), matched degraded (Md), matched adverse (Ma), unmatched degraded (Ud), unmatched adverse (Ua), pooled test (P) and grant test (G). The kind of data used in training and testing steps for the seven protocols are described in table I. The scores of the BANCA database [5] are computed using three classifiers: Gaussian Mixture Models (GMMs), Multi-Layer Perceptrons (MLPs) and Support Vector Machines (SVMs).

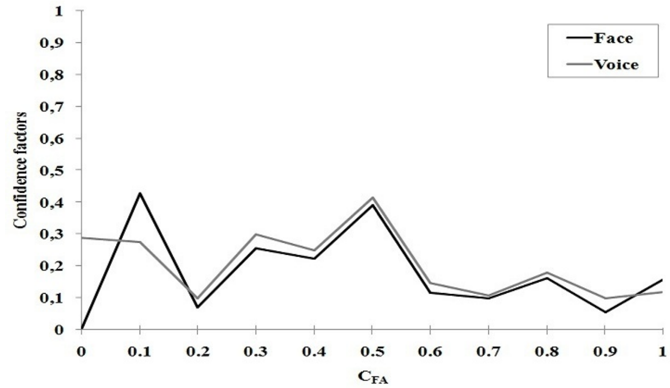
In this experiment, we have used all the combinations of face and speech classifiers. The results are presented in Table II. A comparison is made with the following methods: PCR5 combination rule, SVM based fusion and the method cited in [4]. Since we have compared the proposed method with the approach cited in [4], we have used the same DE parameters as in [4]. So, 20 particles have been used and the DE parameters are fixed with the following values: ($F = 0.8$ and $CR = 0.9$). The DE algorithm is running 10 times with 100 iterations per run. In each run, the HTER is computed on the evaluation set (g2) for each case of the combination of the different classifiers. The average HTER of all combinations are presented in Table II. The HTER is defined as follow [6]:

$$HTER(\Delta^*) = (FAR(\Delta^*) + FRR(\Delta^*))/2 \qquad (11)$$

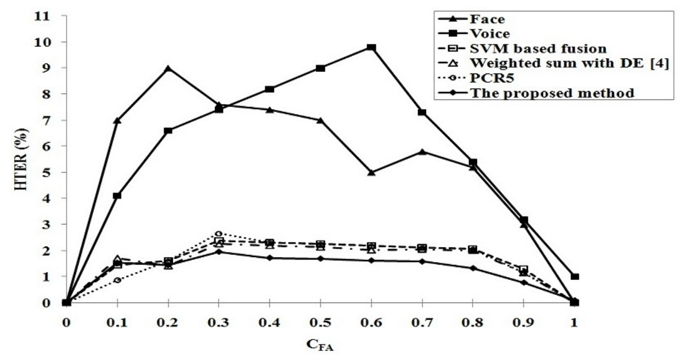
where $\Delta^* = argminWER(\Delta)$

The average HTER of all combinations achieved by the proposed approach and by the individual classifiers are presented in Table II. It is observed that the proposed approach achieves better average HTER than the individual classifiers.

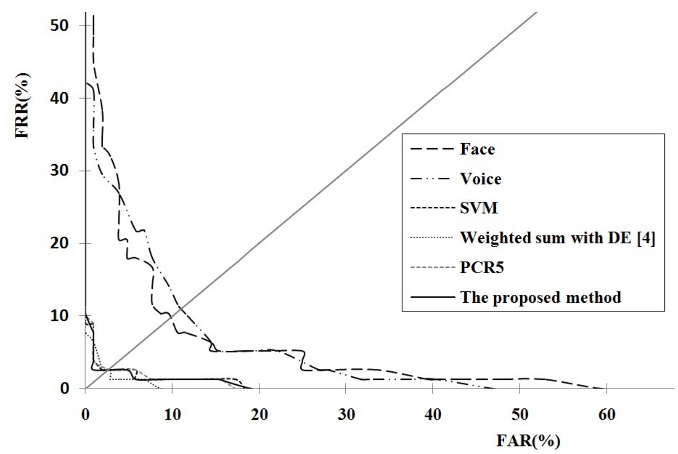
Table II summarizes also a comparative study between the proposed method, PCR5 combination rule, SVM based fusion using RBF kernel and the method cited in [4]. It is seen that the proposed approach reaches a high accuracy when compared to the fusion based on PCR5 combination rule without using DE over all the BANCA protocols because the proposed approach estimate the best confidence factors to weight the belief assignments but the PCR5 combination rule without DE uses the value 1 for all the confidence factors. Moreover, the proposed approach outperforms the fusion based on SVM for all the protocols since the proposed approach is based on PCR5 which deals the conflict between the classifiers but the SVM did not handle such conflict. Furthermore, the proposed approach have the same average HTER as the method cited in [4] on the protocol G in which controlled, regraded and adverse data are used in training and testing steps. However, it achieves higher accuracy than the method cited in [4] on the protocols Ud, Ma, Mc and Md because in these protocols the classifiers have conflict decision and the proposed method is based on PCR5 which manages the conflict between the classifiers .



(a)



(c)



(b)

Fig. 2. (a) Confidence factors achieved by the proposed approach, (b) HTER computed by varying C_{FA}, (c) ROC Curve using Ma Protocol (14^{th} combination).

Figure 2.a presents the confidence factors calculated by the proposed approach by varying C_{FA} for the 14^{th} combination of Ma Protocol. We notice that the confidence factors values change by varying C_{FA}. This proves that the proposed approach estimate the best confidence factors that achieve the best accuracy.

Figure 2.b presents the HTER computed by the different methods against C_{FA} variations for the 14^{th} combination of Ma Protocol. It is noticed that PCR5 combination rule

Protocol	Training data	Testing data	N. of face classifier	N. of voice classifier
G	controlled, degraded, adverse	controlled, degraded, adverse	18	56
P	controlled	controlled, degraded, adverse	18	54
Ua	controlled	adverse	14	27
Ud	controlled	degraded	14	27
Ma	adverse	adverse	14	28
Mc	controlled	controlled	14	27
Md	degraded	degraded	14	29

TABLE I
DESCRIPTION OF THE BANCA DATABASE PROTOCOLS

Protocol	Face	Voice	PCR5	The proposed method	SVM	Method cited in [4]
G	7.146	4.082	1.727	**<u>1.181</u>**	1.325	**<u>1.181</u>**
P	18.480	8.412	7.548	6.104	6.266	**<u>6.051</u>**
Ua	28.171	15.159	14.336	11.518	12.104	**<u>11.345</u>**
Ud	16.564	3.876	4.643	**<u>2.315</u>**	3.095	2.353
Ma	12.706	11.785	6.528	**<u>6.202</u>**	6.459	6.457
Mc	3.835	2.962	1.241	**<u>1.119</u>**	1.334	1.164
Md	8.459	6.244	2.744	**<u>2.639</u>**	2.960	2.736

TABLE II
AVERAGE HTER OF THE INDIVIDUAL CLASSIFIERS, PCR5, THE PROPOSED METHOD, SVM BASED FUSION AND THE METHOD CITED IN [4] (C_{FA} = 0.5)

is the best method for $0 \leq C_{FA} \leq 0.2$. However, the proposed approach yields the minimum values of HTER for $0.2 \leq C_{FA} \leq 1$.

The ROC curve of the 14^{th} combination of Ma Protocol is presented in figure 2.c. We can notice that the proposed method achieves the best performance compared to the other methods.

V. CONCLUSION

In this study, a new multi biometric fusion algorithm is proposed. It is based on PCR5 and DE. The contribution of this research consists on estimating the best confidence factors with DE. Then, they are used to weight the belief assignments of each classifiers. After that, the weighted belief assignments are fused with PCR5 combination rule.

The experimental results have proved that the proposed method outperforms the unimodal biometric systems. Also, it surpasses the fusion based on PCR5 without DE. In addition, the proposed approach outperforms the fusion based on SVM on all the BANCA protocols. However, it surpasses the method cited [4] on four protocols.

REFERENCES

[1] S. M. Anzar and P. S. Sathidevi, An efficient PSO optimized integration weight estimation using d-prime statistics for a multibiometric system, *International Journal on Bioinformatics and Biosciences*, 2(3):1504-1511, 2012.

[2] A. Appriou, Multisensor signal processing in the framework of the theory of evidence, *RTO SCI Lecture Series on Application of Mathematical Signal Processing Techniques to Mission System*, 1999.

[3] A. Kumar and V. Kanhangad and D. Zhang, A new framework for adaptive multimodal biometrics management, *IEEE Transactions on Information Forensics and Security*,5(1):92-102, 2010.

[4] S. Mukherjee and K. Pul and B. P. Majumder and C. Saha and B. K. Panigrahi Shi and S. Das, Differential Evolution Based Score Level Fusion For Multi-modal Biometric Systems, *IEEE Symposium on Computational intelligence in Biometrics an Identity Management*, 39-44, 2014.

[5] N. Poh, BANCA database, http://personal.ee.surrey.ac.uk/Personal/Norman .Poh/web/, 2006.

[6] N. Poh, *Multi-system biometric authentication: optimal fusion and user-specific information*, Faculty of Sciences and Engineering Technology, IDIAP Laboratory, Swiss Federal Institute of Technology in Lausanne, 2006.

[7] N. Poh and S. Bengio, Using chimeric users to construct fusion classifiers in biometric authentication tasks: an investigation, *ICASSP*, 1077-1080, 2006.

[8] A. Ross and K. Nandakumar and A. Jain, *HandBOOK of multibiometrics*, Springer, 2011.

[9] F. Smarandache and J. Dezert, *Advances and applications of DSmT for information fusion: collected works, volume 2*, American Research Press, 2006.

[10] N. Srinivas and K. Veeramachaneni and L. A. Osadciw, Fusing correlated data from multiple classifiers for improved biometric verification, *International Conference on Information Fusion*, 1504-1511, 2009.

[11] R. Storn and K. Price, Differential evolution a simple and efficient heuristic for global optimization over continuous spaces, *Journal of Global Optimization*, 11(4):341359, 1997.

[12] M. Vatsa and R. Singh and A. Noore, *Framework for biometric match score fusion using statistical and belief models Chapter 17 in Advances and Applications of DSmt for Information fusion Collected Works Volume3*, American Research Press, 2009.

[13] K. Veeramachaneni and L. A. Osadciw and P. K.Varshney, An adaptive multimodal biometric management algorithm, *IEEE Trans. Sys. Man and Cybern., Part-C*, 35:344-356, 2005.