A Biometric Security Model with Identities Detection and Local Feature-level Fusion

S. Soviany[1], **C. Soviany**[2]
[1]T.C.T. Department, National Communication Research Institute (I.N.S.C.C), Bucharest, Romania
[2]IDES Technologies, Bruxelles, Belgium

Abstract - *The paper presents an innovative solution for biometric security systems design in order to enhance the identification applications performance and also to reduce their complexity. The proposed model is relying on a special kind of classifiers called detectors and it is suitable especially for various security requirements applications. The model also includes a local feature-level fusion for each of the integrated biometrics. The designed system is useful especially for medical database remote access control in which different users have different authorization levels, and their precise identification need more optimized solution (either from the execution time and recognition accuracy points of view).*

Keywords: detectors, hierarchical classifier, identification

1 Introduction

The modern approach in security system design is to integrate biometrics for preventing the unauthorized accesses to the critical resources such as medical databases or banking applications servers. However many of these applications have different performance and implementation costs requirements. On the other hand, although biometrics based applications are reliable security solutions for persons authentication, there are still challenges to be solved. One of the most critical issues is the identification accuracy. Many biometric security systems are better performing especially for the verification operational mode (in which the system is designed to validate the association between the pretended identity and the biometric credential) and not for the identification mode (in which the system has to guess who is a real person before accepting or rejecting his/her access, without any additional identification) [1][2].

We proposed an innovative approach for a more accurate identification system in which for the biometric data matching we applied special classifiers called detectors. They are trained for a few persons identification, and so the proposed method is more suitable for applications in which not all the enrolled users present the same misidentification risk. An example of application domain is the medical database remote access control, for users with different authorization levels.

The remainder of this paper is structured as follows. Section II presents the biometric system architecture. Section III describes the 1st stage in biometric data processing. The data classification stage is detailed in section IV. Experimental results which we achieved on the available data are presented in section V. Finally section VI concludes our paper and also proposes some further research areas to be explored on more biometric data sets.

2 The System Architecture

The biometric security system architecture is depicted in fig. 1.

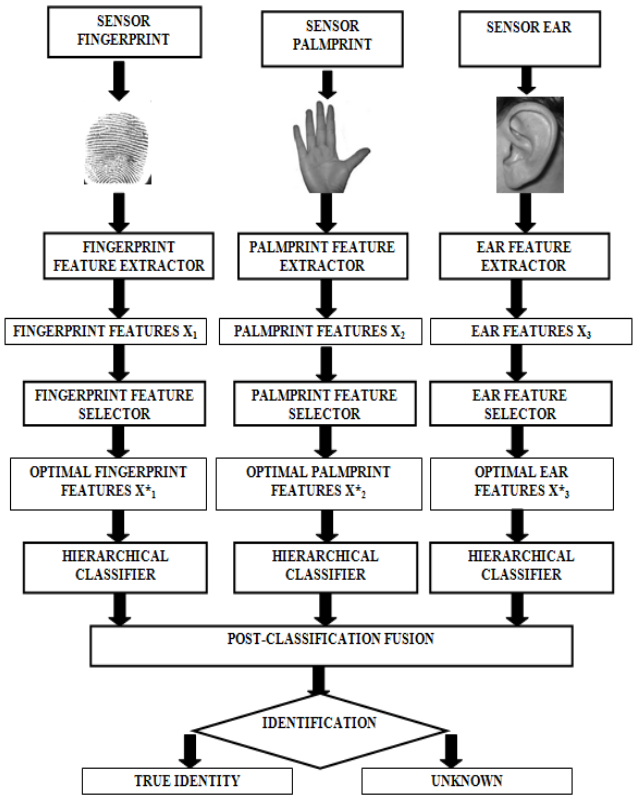

Figure 1: The biometric security system architecture

The biometric security system is relying on a multimodal architecture which integrates 3 biometric measures (fingerprint, palm print and ear). The basic systems functions, further detailed in the next sections, are the following: feature extraction, feature selection for dimensionality reduction and hierarchical classification. The final stage is the post-classification fusion which provides the identification decision for the real biometric system application.

The biometric data comes from 30 users of a medical database. We use 5 images per person per biometric measure (fingerprint, palm print and ear) leading to an overall biometric database which contains 450 images. From these images we generate the biometric templates datasets for the enrolled users within the feature generation and selection stage (Section III). In order to perform the biometric data classification providing the final identification decision (Section IV) we randomly divide the generated biometric datasets into 2 independent subsets: the 1st one is used for system training and the 2nd is used for system performance evaluation.

3 Feature Generation and Selection stage

3.1 Feature Extraction

For the feature extraction we apply a regional approach and also exploit the textural statistical properties of the acquired images (for fingerprint, palm print and ear, respectively). The overall process is depicted in fig. 2.

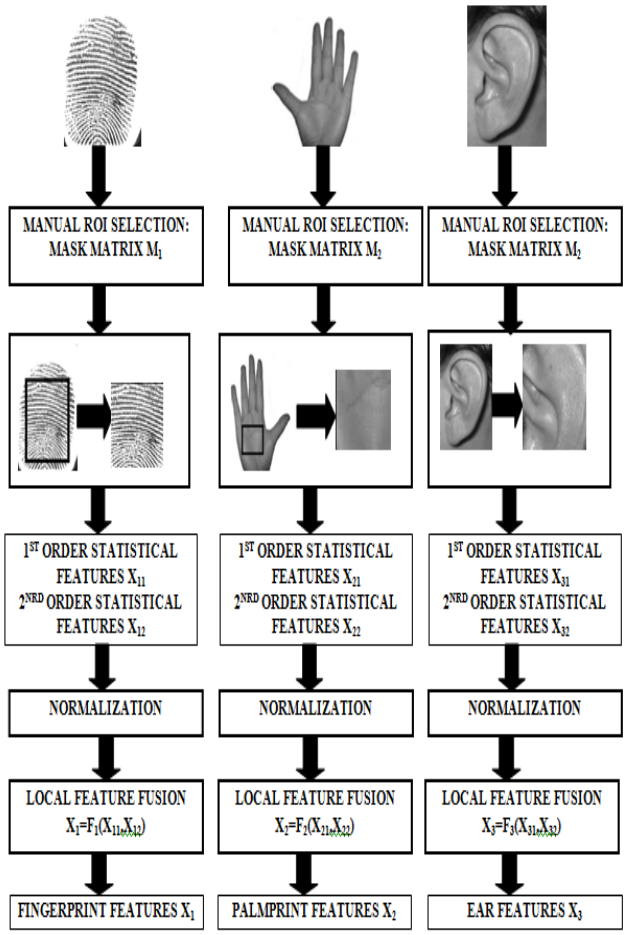

Figure 2: The feature generation step

Before proceeding in feature extraction step, we convert the color images in black-and-white images applying the procedure proposed by Bhattacharyya for iris texture analysis in [3].

Then we perform the manual Region of Interest (ROI) selection on each image, in order to further feature extract only from the regions containing the most useful information for the biometric identification. For each of the 3 biometrics we apply a mask matrix covering a rectangular region selected in the original images, according to:

$$M_k(i_k, j_k) = \begin{cases} 1, x_k \le i_k \le x_k + \Delta x_k, y_k \le j_k \le y_k + \Delta y_k \\ 0, \ otherwise \end{cases} \quad (1)$$

where x_k, $x_k + \Delta x_k$, y_k, $y_k + \Delta y_k$ are the rectangular area coordinates for the selected ROI (k=1 for fingerprint ROI selection, k=2 for palm print ROI selection and k=3 for ear ROI selection). The mask matrix has the same size like the original image (for fingerprint, palm print and ear, respectively).

In the main sub-step of this process we compute 2 sets of statistical textural features from the input ROIs. These features are related to the gray-levels distributions over the selected regions pixels [4]. We generate 2 feature vectors for each biometric containing the 1st and respectively the 2nd order statistical features:

- for fingerprint ROI: X_{11} (the 1st order statistical features) and X_{12} (the 2nd order statistical features);
- for palm print ROI: X_{21} (the 1st order statistical features) and X_{22} (the 2nd order statistical features);
- for ear ROI: X_{31} (the 1st order statistical features) and X_{32} (the 2nd order statistical features).

The 1st order statistical features evaluate the gray-level distribution in the input image [4]. They are relying on the 1st order histogram $P(I_k)$ for the fraction of pixels with gray-level I_k [4]. If N_k is the number of the possible gray levels for fingerprint, palm print and ear ROI images, then the 1st order statistical features derive from the following measures [4]:

- *moments:*

$$m_{j_k} = E\left[I_k^{j_k}\right] = \sum_{I_k=0}^{N_k-1} I_k^{j_k} \cdot P(I_k), \quad j_k = 1,2,\dots, k = \overline{1,3} \quad (2)$$

- *central moments*:

$$\mu_{j_k} = E[(I_k - E[I_k])^{j_k}] = \sum_{I_k=0}^{N_k-1} \left(I_k - m_{1_k}\right)^{j_k} \cdot P(I_k),\ j_k = 1,2,\dots, k = \overline{1,3} \quad (3)$$

- *absolute moments*:

$$\widehat{\mu_{j_k}} = E[|I_k - E[I_k]|^{j_k}] =$$

$$\sum_{I_k=0}^{N_k-1} |I_k - E[I_k]|^{j_k} \cdot P(I_k), j_k = 1,2,\dots, k = \overline{1,3} \quad (4)$$

- *entropy*:

$$H_k = -E[\log_2 P(I_k)] = -\sum_{I_k=0}^{N_k-1} P(I_k) \cdot \log_2 P(I_k), k = \overline{1,3} \quad (5)$$

The feature vectors X_{k1} (for the 3 integrated biometrics in our multimodal architecture) contain the following 1st order feature statistics computed from the previously selected ROIs: *mean* (m1), *variance* (the 2nd central moment μ_2), *skewness* (the 3rd central moment μ3), *kurtosis* (the 4th central moment μ4), the *first 4 absolute moments* ($\widehat{\mu_{j_k,j}}$, $j = \overline{1,4}$, $k = \overline{1,3}$) and *entropy*; therefore each of the 1st feature vectors will have 9 components representing the 1st order statistical features derived from the selected ROI image histograms.

The 2nd order statistical features are pixel-pairwise derived and are provided based on the co-occurrence matrix. Each element in a co-occurrence matrix C contains the probability of a certain gray-level for one pixel in the original image Im_k while another displaced pixel exhibit another gray-level, according to [5][6][7]:

$$C_{\Delta x_k,\Delta y_k,}(i_k, j_k) = P\{Im_k(x_k, y_k) = i_k, Im_k(x_k + \Delta x_k, y_k + \Delta y_k) = j_k\}, k = \overline{1,3} (6)$$

where the pixels displacements are Δx_k and Δy_k. We applied 6 gray-levels for the fingerprint data, 5 gray-levels for the palm print data and 4 gray-levels for the ear data resulting in 36 components for the fingerprint 2nd feature vector, 25 components for palm print and 16 components for ear.

The co-occurrence matrices allow to compute the following additional features [4]:

- *angular second moment:*

$$ASM_k = \sum_{i_k=0}^{N_k-1} \sum_{j_k=0}^{N_k-1} (P(i_k, j_k))^2, k = \overline{1,3} \quad (7)$$

- *contrast:*

$$CON_k = \sum_{n_k=0}^{N_k-1} n_k^2 \cdot \left\{ \sum_{i_k=0}^{N_k-1} \sum_{\substack{j_k=0 \\ |i_k-j_k|=n_k}}^{N_k-1} P(i_k, j_k) \right\}, k = \overline{1,3} \quad (8)$$

- *inverse difference moment:*

$$IDF_k = \sum_{i_k=0}^{N_k-1} \sum_{j_k=0}^{N_k-1} \frac{P(i_k, j_k)}{1 + (i_k - j_k)^2}, k = \overline{1,3} \quad (9)$$

- *entropy:*

$$H_{k,xy} = -\sum_{i_k=0}^{N_k-1} \sum_{j_k=0}^{N_k-1} P(i_k, j_k) \cdot \log_2 P(i_k, j_k), k = \overline{1,3} \quad (10)$$

So far the 2nd feature vectors X_{k2} have the following sizes: 40 for fingerprint, 29 for palm print and 20 for ear biometrics, respectively.

From the 2nd feature vectors X_{k2} we retain only the features which exhibit the lowest absolute values of the Pearson correlation coefficient in order to get **the least-correlated statistical features**: 10 features for fingerprint, 11 features for palm print and 9 features for ear. The apply correlation measure is given for the pixels pair (x_k,y_k) according to [4]

$$r_k(x_k, y_k) = \frac{\left[\sum_{i_k=0}^{N_k-1} \sum_{j_k=0}^{N_k-1} (i_k \cdot j_k) \cdot P(i_k, j_k)\right] - \mu_{x_k} \cdot \mu_{y_k}}{\sigma_{x_k} \cdot \sigma_{y_k}}, k = \overline{1,3} \quad (11)$$

where μ_{x_k}, μ_{y_k} and σ_{x_k}, σ_{y_k} are the mean and standard deviations, respectively, for the 2 pixels intensities. The new vectors are $X_{k2}^*, k = \overline{1,3}$.

The resulting feature sizes for all the integrated biometrics are given in table 1.

TABLE 1. FEATURE SPACES SIZES

Features sets for each biometric			
Biometric	***Size(X_{k1})***	***Size(X_{k2})***	***Size(X_{k2}^*)***
Fingerprint	9	40	10
Palm print	9	29	11
Ear	9	20	9

We **normalize** the X_{k1} and X_{k2}^* components using the sigmoid function to provide a common numerical range for the statistical features:

$$f_{k,i}(X_{ki}) = \frac{1}{1 + exp(-A_{k,i} \cdot X_{ki} - B_{k.i})}, k = \overline{1,3}, i = \overline{1,2} \quad (12)$$

The provided experimental data allowed us to use the following coefficients ranges:

- for fingerprint feature normalization: $A_{1,i} \in [2, 2.5], B_{1,i} \in [1,1.5]$;

- for palm print feature normalization:
  $A_{2,i} \in [2, 3.5], B_{2,i} \in [1.5, 2]$
- for ear feature normalization:
  $A_{3,i} \in [1.5, 2.5], B_{3,i} \in [1, 2]$

Finally we applied a **local feature-level biometric fusion** by concatenating the 2 feature sets for each biometric (fingerprint, palm print and ear). The concatenation-based feature-level fusion needs more homogenous features, according to Jain and Ross [8] and this is why we previously normalized the features. The resulting feature vectors are X_1 (fingerprint biometric template with 19 components), X_2 (palm print template with 20 components) and X_3 (ear template with 18 components). This sub-step is shown in fig. 3.

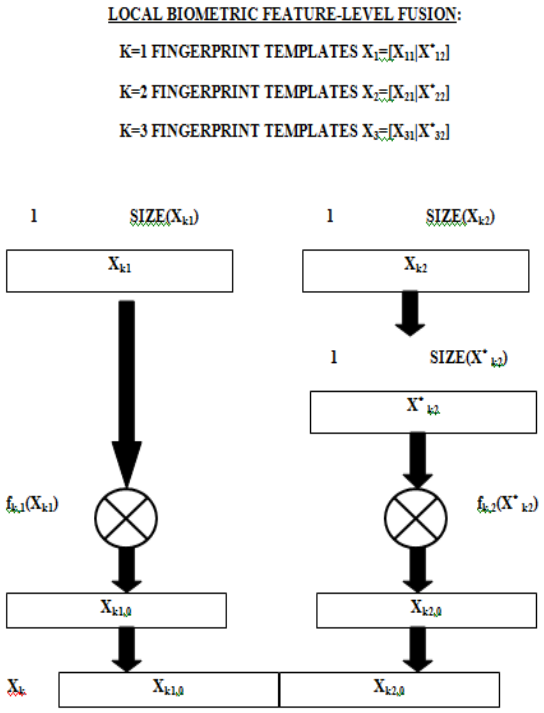

Figure 3: Local feature-level fusion

3.2 Feature Selection

We further apply a feature selection strategy because the biometric templates sizes are still too large. Our purpose is to reduce the feature space dimensionality to at most 10 features per biometric. Less features means less complexity classifiers for the biometric data, less training samples and also a reduced response time which is often an important requirement for the large-scale identification systems.

For feature selection step we apply the **forward-searching feature (sequential) selection** (FSFS) [4] and also we use as the performance criterion *1-NN (nearest-neighbor rule) classification error rate* because of its property to limit the classification error rate [10]:

$$\varepsilon^* \le \varepsilon_{1-NN} \le 2\varepsilon^* \cdot (1 - \varepsilon^*) \le 2\varepsilon^* \qquad (13)$$

where ε_{1-NN} is the error rate for the 1-NN classifier and ε^* is the optimal Bayesian classifier error rate.

The resulting optimal feature sets for each biometric are as following:

- for fingerprint data: 8 features instead of 19;
- for palm print data: 9 features instead of 20;
- for ear data: 10 features instead of 18.

4. Data Classification Stage

The classification stage is based on a hierarchical approach in which each of the 3 biometric data is processed within a multi-stage classifier (fig. 4).

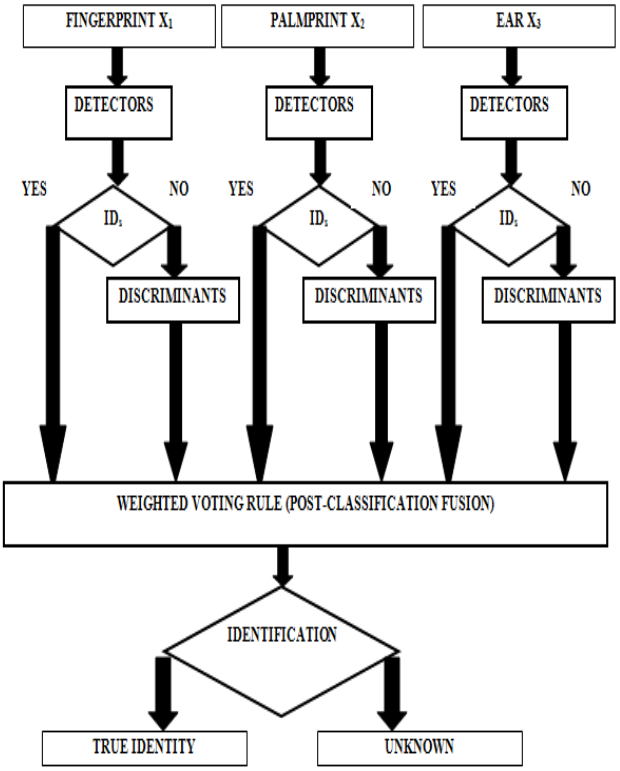

Figure 4: The classification stage

The 2 classification steps for each biometric are: *the detection step* providing decisions only on a few target identities and *the discrimination step* in which all the other identities have to be recognized if the detection failed on the first focused identities. Finally a *weighted voting rule* is applied to provide the most accurate identification decision.

4.1 Detection

In our biometric security application not all the medical database users have the same authorization level

and also not all of them exhibit the same security risk in case of an identification error. This is the reason of applying a special kind of classifiers which are trained only for a few target identities. There are 3 most important users and therefore we trained 3 classifiers for their identities detections. Based on the available biometric data we found *that the Gaussian mixture models* fit very well to the identity detection goal. The basic model for each biometric detector is given by

$$p_k(X_k|I_i) = \sum_{j_{I_i}=1}^{n_k} p_k\left(X_k\middle|j_{I_i}\right) \cdot P_{j_{I_i}}, i = \overline{1,3}, k = \overline{1,3} \quad (14)$$

where P_j are the mixture weights. We designed 3x3 detectors (one for each identity I_i and for each biometric (k=1 for fingerprint, k=2 for palm print and k=3 for ear biometric data, respectively). Also n_k is the mixture component numbers for each biometric detector. The unknown parameters of each Gaussian component are resulting from EM Algorithm (Expectation Maximization) [4][9][11][12].

The identification decision is relying on the following underlying function based on the Bayes rule:

$$g_k(X_k) = P(I_i) \cdot p_k(X_k|I_i) =$$

$$\frac{n_{Z,i}}{n_Z} \cdot \sum_{j_{I_i}=1}^{n_k} p_k\left(X_k\middle|j_{I_i}\right) \cdot P_{j_{I_i}}, i = \overline{1,3}, k = \overline{1,3} \quad (15)$$

where $n_{Z,i}$ is the number of training biometric samples belonging to the person with identity I_i and n_Z is the overall training set size. The biometric detection rule becomes:

$$g_k(X_k) \geq \theta_{I_i} \Rightarrow Identity(X_k) = I_i i = \overline{1,3}, k = \overline{1,3} \quad (16)$$

no matter the other non-target identities.

4.2 Discrimination

The discrimination stage is performed if the 1st detection stage failed on their target identities. We trained the discriminant models only on the other N-3 enrolled identities (because at this point we already have decisions on the 1st 3 identities).

For our available biometric data we choose the following multi-class discrimination models: Naïve-Bayes, Parzen (with Laplace kernel instead of the Gaussian which was most used so far) and Quadratic, according to their behavior on the training datasets. Their learning curves are represented in figures 5 (for fingerprint data), 6 (for palm print data) and 7 (for ear data).

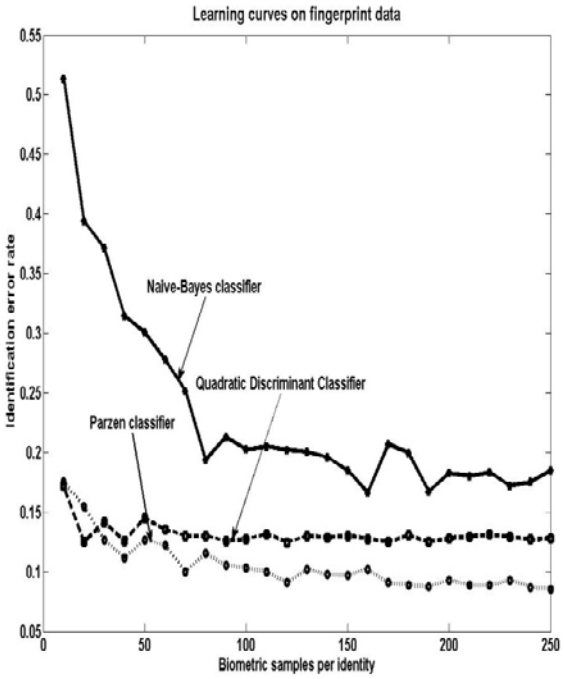

Figure 5: Learning curves for NBayes, Parzen and QDC classifiers on fingerprint data

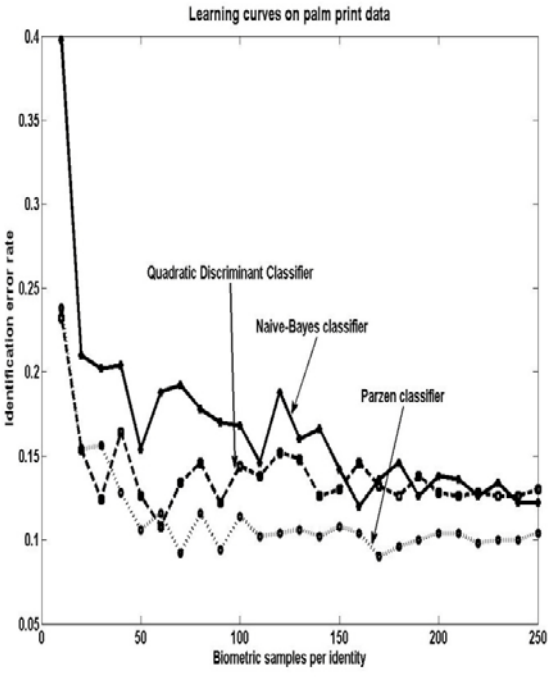

Figure 6: Learning curves for NBayes, Parzen and QDC classifiers on palm print data

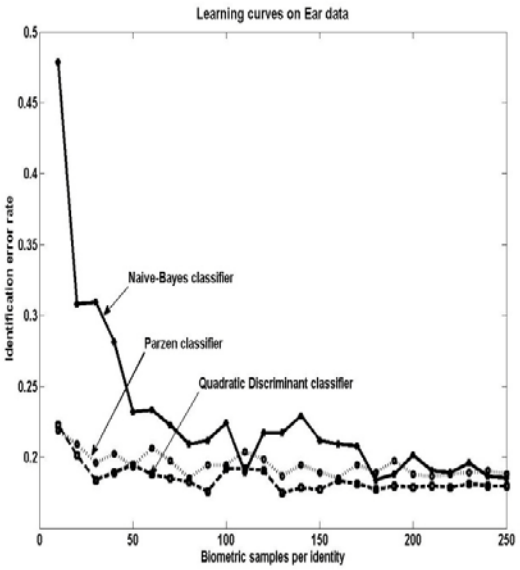

Figure 7: Learning curves for NBayes, Parzen and QDC classifiers on ear data

Parzen and QDC models exhibit the best behavior. We represented the classification (identification) error rate vs. the training biometric data set size. According to these learning curves, we finally choose Parzen classifier for fingerprint and palm print data and QDC model for ear biometric data.

4.3 The post-classification fusion rule

The final post-classification fusion rule is relying on a weighted voting scheme in which we maximize the best hierarchical classifiers contributions with the following weights updating iterative rule:

$$w(i+1) \leftarrow w(i) \cdot \eta(i) \qquad (17)$$

in which $\eta(i)$ is the ratio between the detectors and discriminants performances (measured by their TPr, True Positive Rates) for each of the identification subsystems (fingerprint, palm print and ear).

5 Experimental Results

We evaluate the system performance on 10 experiments and averaging the achieved results. Each of the performed experiments consists in 2 persons authentication attempts for the remote medical database also using the 3 biometrics. The designed biometric security system performance is resulting from the ROC analysis while fixing the classifier operating points in order to provide an optimal trade-off for the 2 persons identification; one of these persons (identity I_1) has the highest authorization degree for using the medical database within the telemedicine application and the other is less authorized (identity I_2). Actually we compare the optimal operating points in 2 cases: with and without identities detection stage (figures 8 and 9, respectively). The classification system is trained with 50 samples per class (identity). Also for all classifiers we apply a rejection threshold of 5%. This rejection option reduces the influence of low-quality biometric templates on the overall biometric security system accuracy.

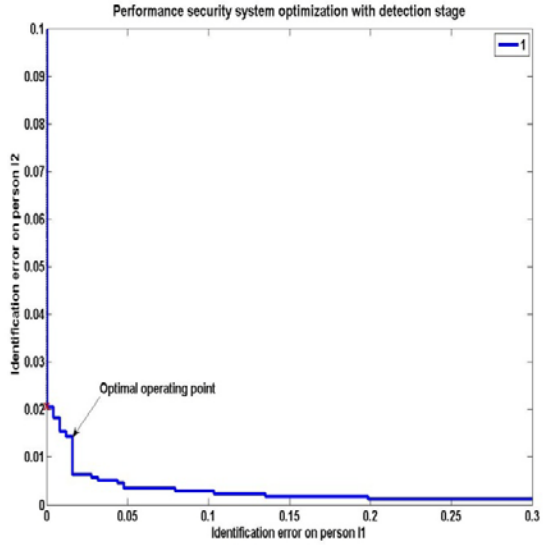

Figure 8: Optimal op.point fixing for the overall security system with detection stage

In Figure 8 one can see that the optimal op. point of the overall system provides an average identification error rate of 0.015 on 2 authenticating persons. Actually this performance indicator reveals the system capacity to find out the real identity, not the acceptance/rejection decisions correctness. In this evaluation we did not focus on the typical FAR (False Acceptance Rate) or FRR (False Rejection Rate) performance indicators. The values are already suggesting the detectors capabilities to improve the overall identification performance of the biometric systems.

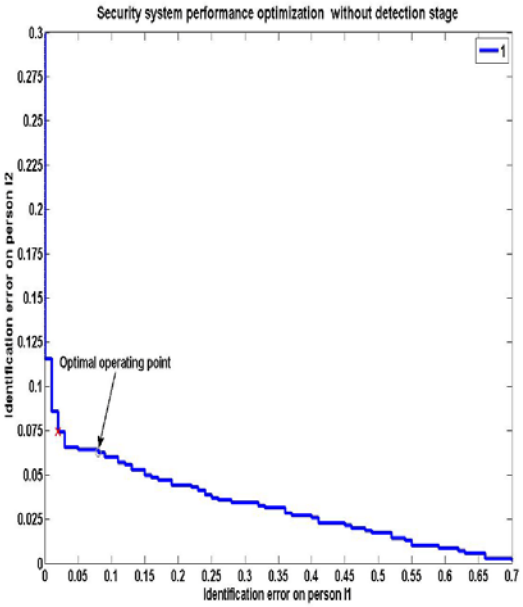

Figure 9: Optimal op.point fixing for the overall security system without detection stage

Without detection stage, the optimal operating point provides an average identification error rate of 0.067 on the same persons. This shows that the detection stage improved the identification process accuracy by almost 4 times. This improvement results from the detector basic principle, which is more focused to target class recognition (in this case, a certain person to be identified).

These results are achieved for a reduced feature number (between 8 and 10 features for the 3 integrated biometrics). Also the local feature-level fusion has a significant contribution to the identification performance.

6 Conclusions

The identification accuracy still remains an important challenge in biometric systems design. This is due to the computational complexity in exploring a huge searching space of possible identities (in large-scale identification). The multimodal biometric systems integrate more biometrics in order to enhance the accuracy and security, but there are still open issues regarding the integration levels, more specifically on the biometric fusion scheme (pre- or post-classification).

We approached these challenges for biometric identification systems through a multi-classifier hierarchical approach in which the biometric data matching is performed in 2 stages, detection and discrimination. This decision hierarchy significantly improves the identification accuracy although the users behavior has a non-neglecting influence on the overall system performance. On the other hand, the execution time should be considered while designing such biometric data classification systems.

Also we included a local feature-level biometric data fusion. So far the pre-classification or feature-level fusion was not implemented in many biometric systems because the different features sets are often incompatible. Also the biometric templates format is usually proprietary from security reasons. However, the pre-classification fusion should be considered for accurate biometric systems design because of its performance improvement. Combining the biometric data at an earlier processing stage enhances the identification accuracy by exploring more independent features sources from the same person.

Further research should be focused on the pre-classification fusion and its potential for performance improvement.

7 References

[1] Soviany S., Puşcoci S., Jurian M.: "A Detector-Discriminant Model for Biometric Security Systems", International Conference on Information Technology and Computer Networks (ITCN 2012), Viena, 10-12 november 2012.

[2] Soviany S., Soviany C., Jurian M.: "A Multimodal Approach for Biometric Authentication with Multiple Classifiers", International Conference on Communications, Information and Network Security (ICCINS 2011), Venetia, 28-30 november 2011

[3] Bhattacharyya D., Das P., Bandyopadhyay S.K., Kim T.: "IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition", International Journal of Database Theory and Application, vol. 1, nr. 1, pp. 53-60, december 2008

[4] Theodoridis S., Koutroumbas K.: "Pattern Recognition" 4th edition, Academic Press Elsevier, 2009

[5] Eleyan A., Demirel H.: "Co-occurrence matrix and its statistical features as a new approach for face recognition", Turk J Elec Eng & Comp Sci, Vol.19, Nr.1, 2011

[6] Zucker S.W., Terzopoulos D.: "Finding Structure in Co-Occurence Matrices for Texture Analysis", Computer Graphics and Image Processing nr. 12, 1980

[7] Bino S. V, A. Unnikrishnan and Kannan B.: "Gray level Co-Occurrence Matrices: Generalisation and some new features", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.2, April 2012

[8] Jain A., Nandakumar K., Ross A.: Score Normalization in multimodal biometric systems, Pattern Recognition, The Journal of the Pattern Recognition Society, 38 (2005)

[9] Zhang David, Song Fengxi, Xu Yong, Liang Zhizhen: "Advanced Pattern Recognition Technologies with Applications to Biometrics", Medical Information Science Reference, IGI Global, 2009

[10] Devroye L., Gyorfy L., Lugosi G.: "A Probabilistic Theory of Pattern Recognition", Springer, 1997

[11] PerClass Training Course: Machine Learning for R&D Specialists, Delft, Netherlands

[12] Borman S.: "The Expectation-Maximization Algorithm. A short Tutorial", 2004