A Hierarchical Data Fusion and Classification Model for Biometric Identification Systems

Sorin SOVIANY[1], Mariana JURIAN[2]

Rezumat. *Articolul prezintă un model ierarhic de clasificare a datelor biometrice, destinat a asigura îmbunătățirea performanțelor procesului de recunoaştere a persoanelor folosind sisteme de identificare biometrică. Abordarea ierarhică se bazează pe combinarea mai multor clasificatori în cadrul unei ierarhii cu fuziune biometrică multi-nivel. Fuziunea biometrică multi-nivel include atât fuziunea pre-clasificare cu selecția optimă a caracteristicilor, cât şi fuziunea post-clasificare cu aplicarea unei reguli de însumare ponderată a scorurilor de similaritate. Soluția asigură creşterea preciziei procesului de recunoaştere biometrică inclusiv prin aplicarea unei strategii adecvate de selecție a caracteristicilor, deoarece nu toate componentele vectorilor de caracteristici asigură acelaşi grad de îmbunătățirea performanței.*

Cuvinte cheie: *fuziune biometrică multi-nivel, model ierarhic, eroare de generalizare.*

Abstract. *The paper presents a hierarchical biometric data classification model which is designed to provide the performance enhancement for the persons recognition task in biometric identification systems. The hierarchical approach is relying on more classifiers combination within a multi-level biometric fusion hierarchy. The multi-level biometric fusion model includes both of pre-classification fusion with optimal feature selection and the post-classification fusion based on the similarity scores weighted sum. The proposed solution increases biometric recognition accuracy based on a suitable feature selection, as much as not all of the feature vectors components support the performance improvement degree.*

Keywords: *multi-level biometric fusion, hierarchical model, generalization error.*

1. INTRODUCTION

The actual concern in security systems design is focused on issues related to biometrics, as much as they are relying on natural human feature providing a more reliable identity proof. However, the biometric authentication process is inherently pro netomatching errors. Therefore, the main research direction in this field is to fiind out more reliable solutions in order to improve biometric recognition accuracy. One of the approach is to integrate more biometrics within the same access control system, handling issues such as the non-universality of some human physical traits, and to improve the accuracy and security. [1] These improvements are give neither by using more sensors types, more pre-processing algorithms for biometric template generation and/or more classification techniques in order to increase recognition accuracy. [2]

[1] Institutul Național de Studii şi Cercetări pentru Comunicații – I.N.S.C.C.

[2] Universitatea din Piteşti, Facultatea de Electronică şi Calculatoare.

Most of the actual researches on multi-biometric or multimodal biometric systems focuses especially on matching score level-biometric fusion, achieving different degrees of performance improvement. [2][5] However, there is still a significant potential of biometric accuracy enhancement by considering also the feature-level biometric fusion, as much as this could provide more independent discriminant information to final authentication decision.

A novel approach is to apply a hierarchical multi-classifier approach for an individual biometric within a multimodal system, and then combining their outputs, thereby providing an additional optimization level. This could be done by performing classification on carefully selected subset of features, and combining the results.

The remainder of this paper is structured as follows. In section 2 the proposed multimodal architecture is presented. Section 3 describes in more details the hierarchical approach of our model. Section 4 shows the achieved results for the proposed multimodal biometric system based on a hierarchical approach with multi-level biometric fusion and multi-classifiers. Section 5 concludes our research and also provides some future research directions to be further explored in order to improve the biometric recognition accuracy and security.

2. THE SYSTEM ARCHITECTURE WITH HIERARCHICAL APPROACH

Any biometric authentication system is performing the following basic tasks:[3][4][5]

- ***data acquisition***: for each of the biometrics the measurements are performed providing the primary biometric data;
- ***feature extraction***: to find a given number of distinguishing features carrying information;
- ***feature selection***: a further dimensionality reduction stage providing the most discriminatory information, out of all possible features, in order to find out a subset of features achieving the best generalization performance of the classifier when trained on this subset;
- ***data classification***: the essential step of the biometric recognition; [6]
- ***biometric fusion***: the typical task in a multimodal biometric system. The biometric data fusion could be performed at different levels (biometric sensors, features, matching score and final decision), but the most applied fusion schemes are the post-classification ones, meaning that the similarity scores provided by different biometric classifiers are combined according to a mathematical rule in order to provide a global similarity score;
- ***final acceptance/rejection decision***: the global score given S is compared to the system security threshold (θ), and based on the difference between the two values, the final decision will be to accept or to reject the access request. [7]

The proposed multimodal biometric system architecture is depicted in Fig. 1. This architecture is based on a **hierarchical approach** for biometric data fusion and classification. The system includes 2 main identification components:

- *the fingerprint and palmprint identification subsystem*. This component is relying on a feature-level biometric fusion scheme;
- *the hand geometry identification subsystem*;
- *the post-classification fusion scheme,* which combines the two previous components results;
- *the decision module* which provides the final acceptance or rejection decision based on the global score.

The proposedmultimodalapproachisfeaturedby**a multi-levelintegration**, as shown in Figure 1. Also for each biometric identification component the model provides a multi-classifierapproach, in ordertoensure a local optimization.

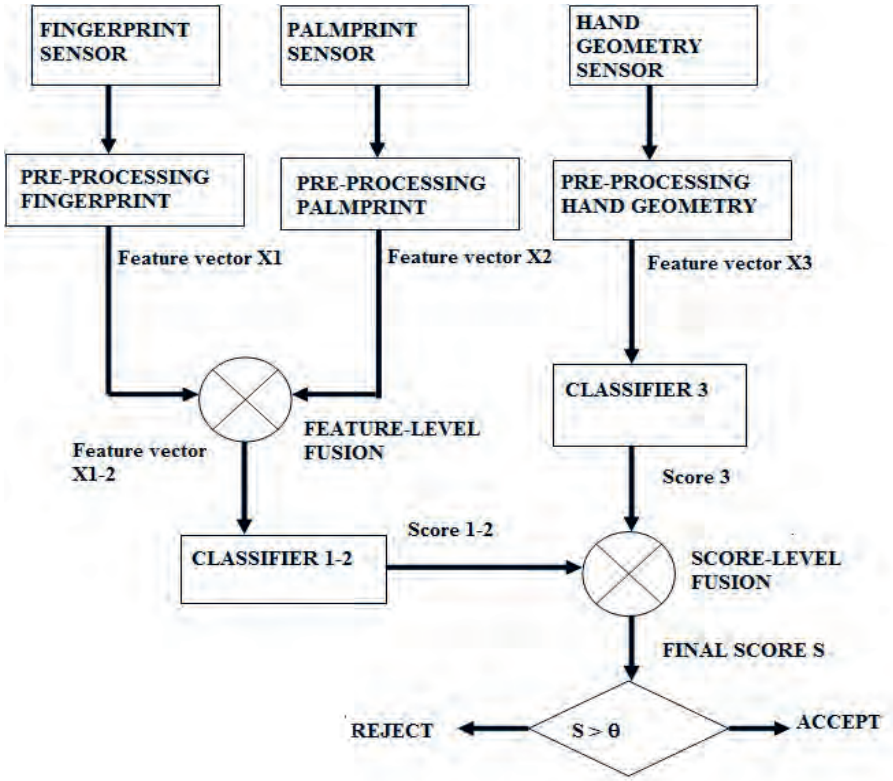

Fig. 1. The multimodal biometric system architecture with hierarchical approach.

Therefore, the **hierarchical** approach is featured by:

- *the two biometric fusion schemes*: a pre-classification-level fusion and a post-classification-level fusion;
- *the multi-classifier model* provided by using more classifiers for each identification component within the biometric system architecture

For testing the proposed model, we used a database containing images of fingerprint, palmprint and hand geometry of 100 persons. On these images we designed for each component a set or relevant features and then we selected the optimal classification algorithms. This is the *training dataset* used to design the classifiers to be used for each of the multimodal biometric system components. The applied classifiers were tested on a validation dataset. The training and validation datasets are independent. The validation dataset includes 10 biometric records, each of them belonging to one person. The biometric system is used for an identification purpose, therefore it deals with a multi-class problem in which every person's biometric data are belonging to one class.

3. THE HIERARCHICAL MODEL COMPONENTS FOR BIOMETRIC DATAFUSIONAND CLASSIFICATION

In the ***hierarchical approach***, after feature extraction performed in order to generate the biometric templates (during the pre-processing stage of the biometric authentication process), the main steps to be performed are the following:

- *the pre-classification fusion*: this is the feature-level biometric fusion between the fingerprint and palmprint biometrics;
- *the data classification tasks*, for each of the two identification subsystems;

• *the post-classification fusion* to combine the individual matching scores into a global one.

3.1. Feature-level fusion scheme (pre-classification fusion)

The feature-level fusion is performed by *concatenation of the two feature vectors* from fingerprint and palmprint, X1 and X2 respectively. Although a procedure from *feature selection* is applied on the concatenated feature vector, in order to decrease the dimensionality of the resulting combined data. The feature selection procedure is a non-exhaustive one, based on an iterative approach with backward searching. Basically the selection feature procedure creates 2 clusters from the features in the concatenated vector (fingerprint and palmprint), and the resulting selected features are given based on the performance of an elementary classifier. The cluster with the best elementary classifier performance is the cluster with the relevant features from the fingerprint and palmprint, to be considered for the next stage of the biometric fusion in the multimodal system. The distances between the clusters are computed relying on *Mahalanobis distance*, which has the following definition:

$$d_M(X,Y) = \sqrt{(X-Y)^T S^{-1}(X-Y)} \qquad (1)$$

where S is the covariance matrix of the two vectors (features sets) X and Y, given by:

$$\Sigma = Cov(X,Y) = E[(X - E[X])(Y - E[Y]^T)] \qquad (2)$$

The ***feature-level fusion rule*** based on concatenation is

$$X_{12} = [X1, X2] \qquad (3)$$

where: $X1$ is the *fingerprint feature vector*, and $X2$ is *the palmprint feature vector*. The physical significance of these feature vectors components are as following [1, 9]:

✓ for *the fingerprint feature vector X1*:minutiae-related features like ridge ending, bifurcation and dots; also some of the features are given as distances between 5 relevant points on a central ridge, and also from the ending point. Basically, the considered features are the minutiae relative positions on a fingerprint (captured from the same source);

✓ *for the palmprint feature vector X2*: distances between the main lines, number of singular points, also fingerprint-like minutiae extracted from the ridges within selected region of interest in the palm

The essential steps of the ***feature selection procedure*** are the following:

Selection-feature(X_{12})

//X_{12} = the concatenation of the feature vectors for the fingerprint and palmprint

BEGIN

1. ***Initialization***

Cluster1=X_{12}*;*

*Cluster2={} //*empty cluster

Relevant_set={}

*H1=Evaluation(Cluster1); //*the performance of a basic classifier for the current feature set

H2=Evaluation(Cluster2);

2. ***Computes the inter-cluster distance*** *for the current feature set, using Mahalanobis distance*

d_inter=d_M*(Cluster1, Cluster2)*

3. ***While H1 ≥ H2***

//one feature extraction improves the current set performance *Cluster1=Cluster1-{feature1};*

Cluster2={feature1};

d_inter= d_M*(Cluster1, Cluster2)*

H1=Evaluation(Cluster1);

H2=Evaluation(Cluster2);

4. ***If d_inter ≥ θ*** //threshold

Relevant_set=Cluster1;

Else

Relevant_set=X_{12};

End

The basic classifier used to evaluate the actual feature set performance is NN (Nearest-Neighbor) rule, as much as its error rate is bounded as following [5, 6]:

$$\varepsilon^* \le \varepsilon_{NN} \le 2\varepsilon^* \cdot (1-\varepsilon^*) \le 2\varepsilon^* \quad (4)$$

where: ε_{NN} is the error rate for the Nearest-Neighbor classsifier; ε^* – the error rate for the optimal Bayesclassifier

The 3rd identification component (hand geometry) is separately processed in this approach. X3 is the *hand geometry feature vector*, and its components are related to geometric features of hand and fingers, such as distances between relevant points and finger widths.

3.2. Classification Models for Biometric Data

For the proposed combined system we developed classification models for each of its two components (fingerprint + palmprint features and hand geometry features) separately. For each of these components we designed a set of meaningful features that depicts the characteristics of the data. These features form the representation space for each component model. Then a set of classification algorithms was applied to classify the data in the given number of classes. For these systems the number of classes is equal to the number of people that needs to be classified or recognized.

For each of the two identification components we used a classifiers combination given by SVM (Support Vector Machine) with the suitable kernel and KNN with the optimal value of k. The local optimization was performed by averaging the results on each component.

3.2.1. The SVM Classifier Model

Support Vector Machine defines a linear non-probabilistic classifier which find out a separation boundary between classes, by maximizing the distances between the separation hyperplanes in the features spaces. [4]

Basically, the SVM classifier could be used in the following approaches:

a) binary classification for completely linear separable data;

b) binary classification for non-completely linear separable data;

c) non-linear classification.

Also we should notice that although the basic SVM classifier is defined and applied for 2-class problems (such as biometric verification with genuine/impostor decision), the results of the applied model could be extended for multi-class problems (such as biometric identification) by averaging their outputs values for data class labeling.

The SVM classifier model applied for biometric data in our case is designed for non-linear classification task by considering a kernel function to perform the inner products in a higher dimensionality feature space, while mapping the input data on this transformed space.

Therefore, ***the applied SVM model*** is the following [4, 6].

For each of the identification components, given *the training dataset Zj* = {zj_i, yj_i}, where zj_i is the biometric template (j = 1 for fingerprint + palmprint and j = 2 for hand geometry, respectively), and yj_i is its known class label, and the *testing dataset Xj* (also for both components, j =1 for fingerprint and

palmprint concatenated feature vector the following tasks are performed [6]:

• *selection of a kernel function*: the mapping $x \to \phi(x)$ between the features spaces and the optimal kernel model:

$$K(x,y) = \phi(x) \cdot \phi(y) \tag{5}$$

where x and y are features data point within the input data space for the classifier:

Actually we needed to directly specify only the kernel model. The available options for the kernels are the following:

o Gaussian radial basis function kernel:

$$K(x,y) = \exp\left(-\frac{\|x-y\|^2}{2\sigma^2}\right) \tag{6}$$

where x and y are the feature vectors to be matched for their similarity, and σ^2 is the variance of the compared features.

o Polynomial kernel function, given by:

$$K(x,y) = \left(\alpha x^T \cdot y + a\right)^b \tag{7}$$

where α, a and b are constant values depending on the application and the data types to be classified. Actually the polynom degree b is the main parameter with the most important impact on the classification accuracy if the polynomial kernel is applied. The operator is the inner (scalar) product of the two vectors. The homogeneous variant of the polynomial kernel is given by

$$K(x,y) = \left(x^T \cdot y\right)^b \tag{8}$$

o Sigmoid kernel given by

$$K(x,y) = \tanh\left(\alpha x^T \cdot y - b\right) \tag{9}$$

The parameters α, a and b reveal the kernel function behavior

• *building the matrix H with its elements provided by the inner products applied pairwise on the training dataset*, both for fingerprint + palmprint feature vectors and for hand geometry feature vector:

$$H_{i,j} = y_i y_j K(z_i, z_j) = y_i y_j \phi(z_i) \cdot \phi(z_j), \quad i,j = \overline{1,N_Z}$$

where: N_Z is the training dataset size for the classifier; z_i, z_j are feature vectors from the training dataset; $K(z_i, z_j)$ is the applied kernel, useful to map a non-linear classifier into a linear high-dimensionality space (which is a space where the input data are linear separable);

• *providing the wrong classification penalty:* η ;

• *computes the coefficients of the linear classifier,* α, by maximizing of the dual Lagrange function:

$$_D(\alpha_i) = \sum_{i=1}^{N_Z} \alpha_i - \frac{1}{2}\alpha^T \cdot H \cdot \alpha \tag{10}$$

according to

$$0 \le \alpha_i \le \eta, \quad \forall i = \overline{1,N_Z} \text{ and } \sum_{i=1}^{N_Z} \alpha_i y_i = 0$$

• *computes the SVM classifier main parameters*:

$$w = \sum_{i=1}^{N_Z} \alpha_i y_i \cdot \phi(z_i) \tag{11}$$

• the *support vector set* (which are the training datapoints having the same maximum distance from the boundary decision given by the hyperplane):

$$VS = \{z_i \in Z \,|\, 0 \le \alpha_i \le \eta, \; i = \overline{1,N_Z} \text{ and } w \cdot \phi(z_i) + c = \pm 1 \mp \delta_i\} \tag{12}$$

where δ_i is also a penalty flag for the wrong classified examples;

• computes the *offset parameter for the decision boundary hyperplane*

$$c = \frac{1}{card(VS)} \sum_{s \in VS} \left[y_s - \sum_{j \in VS} \alpha_j y_j \cdot \phi(z_j) \cdot \phi(z_s) \right] \tag{13}$$

Testing/evaluation for new data classification:

• for each example x belonging to the validation dataset X: perform the classification based on the return of the following discriminant function:

$$y = \text{sgn}(w \cdot \phi(x) + c) \tag{14}$$

The SVM classifier is applied for each of the two feature vectors: X_{12} fingerprint and palmprint, X_3 hand geometry feature vector. Also the classifier will be evaluated for different kernel functions, in order to find out the optimal one.

3.2.2. The KNN Classifier Model

The KNN (K-Nearest Neighbor) algorithm is a discriminative classification rule as it directly models the decision function. Also it is a distance-based classifier, because it requires a distance function on data instances to be classified. Basically, the KNN classifier assigns an object described by a set of relevant features to the class with the highest occurrence frequency among *k* nearest neighbors in the classifier's training dataset [4], [6].

Let us *xj* is the feature vector obtained from fingerprint + palmprint, and from hand geometry respectively. Also the training dataset KNN classifier is $Zj = \{zj_1, zj_2,\ldots, zj_N\}$. Each component of the training dataset is a labeled data instance.

For every instance xj_i, i = 1, 2…., Nv in the validation dataset (where Nv is the validation dataset size) , the KNN algorithm performs essentially in the following steps:

1) Locates the *K* nearest examples in the iris training dataset *Zj*: $\{Zj_1, Zj_2,\ldots, Zj_K\}$. These are the *K* closest training data instances to the instance *xj* to be classified;

2) Label *xj* with the class label that occurs more frequently among the selected *K* training instances for the iris classifier.

In order to compute the distance between a test instance *xj* (fingerprint + palmprint and, respectively, hand geometry feature vectors) and its neighbors from the training dataset, the Mahalanobis distance was applied, according to (15):

$$D_M(x_J - z_J) = \sqrt{(x_J - z_J)^T \cdot S^{-1} \cdot (x_J - z_J)} \qquad (15)$$

where *S* is the covariance matrix between the instances *xj* and *zj*. This option is reasoned by the main properties of Mahalanobis distance i.e. scaling-invariance and exploiting correlation among the features.

The choice of the *K* value is critical for this classifier results. A higher value of the selected neighbors number in KNN classification model provides a smoother, less locally sensitive decision function. On the other hand, the drawback of increasing value of *K* is that as *K* becomes closer to the training dataset size *N*, the classifier performance will approach that of the most statistical classifiers, because the classifier will assign the actual data instance to the most frequent class in the training dataset.

The problem of the distant instances influence is avoided, in our model, by assigning a weight to each neighbor vote. This weight is defined as a function of the distance between the unknown instance (to be classified) and its neighbor in the training dataset. The weight is given as an inversed squared distance between the two instances:

$$w(i) = \frac{1}{d(zj_i xj)^2} \qquad (16)$$

where: $w(i)$ is the weight for the neighbor instance zj_i; *xj* is the unknown instance to be classified.

Also the distance between the training data instance and the testing instance, $d(zj_i, xj)$, is computed using Mahalanobis distance, given by (15).

3.2.3. The local biometric fusion (local multi-classifier approach)

For each of the two components of the multimodal system, we applied a local multi-classifier approach, according to Figure 2.

The local biometric fusion is performed ***by averaging*** the results of the 2 classifiers applied for each of the two identification component of the multimodal system: fingerprint + palmprint and hand

geometry, respectively. The SVM classifiers were evaluated for different kernels, and the KNN classifiers were evaluate for the following values of the selected neighbors number: k = 1,3,5,7,9,11.

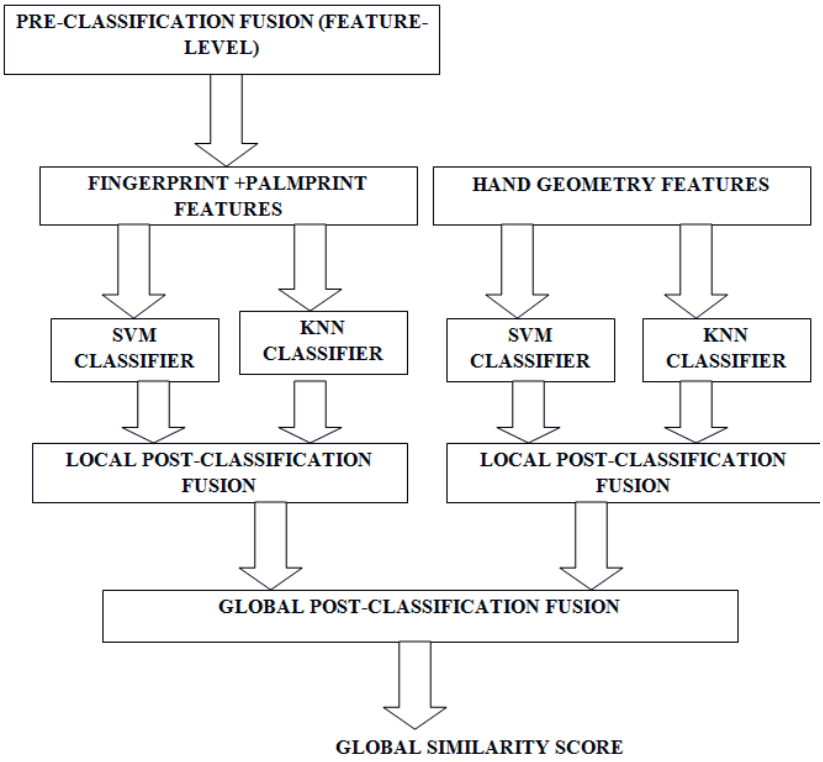

Fig. 2. The multi-level fusion hierarchical model, with local and global biometric fusion.

3.3. Score-level fusion scheme (post-classification fusion)

The fusion method consists on a unique combination of fingerprint+palmprint identification and hand geometru recognition, each subsystem being designed and optimized separately and also entirely, at a global level [9].

Taking the output for each identification subsystem, i.e. $y1$ for fingerprint+palmprint component, $y2$ for hand geometry component, the whole multimodal system output Y is given by the following rule:

$$Y = \sum_{i=1}^{n} w_i \cdot y_i \qquad (17)$$

where: n is the identification components number, here n = 2; w_i – the weight which we assigned to the component i; y_i – the classifier i output.

Basically the weights are taken depending on each identification component performance, so that the more accurate identification subsystem should have the highest contribution on the overall system output. Also the assigned weights have to meet the following normalization condition:

$$\sum_{i=1}^{n} w_i = 1 \qquad (18)$$

Given the training dataset size influence over the classifier performance, a dynamic approach for updating these weights was applied :

- weights initialization

$$w_i \leftarrow w_{i,0} = \frac{1}{n}, \quad i = \overline{1,n} \qquad (19)$$

- weights updating

$$w_i \leftarrow w_i \cdot K_i, \quad i = \overline{1,n}, \quad K_i > 0 \qquad (20)$$

$$K_i = \begin{cases} \dfrac{1}{\max \varepsilon_i - \min \varepsilon_i}, & \varepsilon_i < \varepsilon, \quad i = \overline{1,n} \\ \max_i \varepsilon_i - \min_i \varepsilon_i, & \varepsilon_i > \varepsilon, \quad i = \overline{1,n} \end{cases}$$

where ε_i is the error rate for classifier *i*, and ε is the overall system average error rate.

This dynamic strategy allows for further accuracy improvement for our multimodal biometric system, even by additional biometric fusions such as feature-level fusion or by rejection option for low-quality biometric data.

4. RESULTS AND DISCUSSION

For ***the fingerprint and palmprint classification***, we originally designed 25 fingerprint features and, respectively, 34 palmprint features. After carefully analysis we finally selected 12 fingerprint features and 19 palmprint features. The resulting concatenated fingerprint and palmprint features vector has 31 independent components. Also applying the feature selection procedure, we obtained a final feature vector with 14 components.Therefore, the final **fingerprint and palmprint feature vector** to be classified has containing ***14 features*** selected from the initial fingerprint and palmprint primary data.

Also for the ***hand geometry classification***, from the originally features we selected 10 of them.

For each of the two components, we applied the SVM and KNN classifiers. The SVM classifier was applied for more kernel types (gaussian, linear and polynomial), and the KNN classification rule was applied for the following values of k: 1,3,5,7,9,11.

In all cases, first we looked to find out the optimal size of the training dataset for the best classifier to be applied.

We are depicted the learning curves for each of the classifiers to be used for biometric data, according to the proposed model. The learning curve for a classifier describes its performance versus the training dataset size. Also there are represented the generalization error rates and ther apparent error rates:

- ***the generalization error rates*** refer to the classifier error which are achieved on new data, i.e. data which are not previously seen during the supervised learning step. Essentially for an optimal classifier is to minimize the generalization error rate;
- ***the apparent error rates*** refer to the classification error which are obtained on the training dataset. Actually this error rate is less than the previous one (generalization error). However, one of the main risk in classifier design task is to build a super-trained classifier, for instance by memorizing the training data, but with a high generalization error rate.

Therefore, the learning curves allows us to choose the optimal training dataset size for each classifier, in order to prevent the super-training risk and although to decrease the difference between the generalization error rate and the apparent error rate.

The learning curves for SVM classifier are given in Figure 3. These learning curves allows us to select the best training dataset size.

From fig. 3 we should notice that the best kernel to be applied while using SVM classifies for biometric data seems to be the polynomial kernel, especially the 3rd order polynomial kernel.

Also the learning curves for KNN classifiers are depicted in Figure 4, for different values of the parameter *k* (the selected nearest neighbor numbers from the training dataset).

From these learning curves we should conclude that the smallest generalization error is provided for $K = 5$ if considering training dataset sizes around 50.

Therefore, for our multimodal system we should select the SVM classifier with a 3rd order polynomial kernel and the KNN classifier with $K = 5$. Both classifiers should be trained with a dataset with 50 biometric templates (fingerprint+palmprint and hand geometry, respectively).

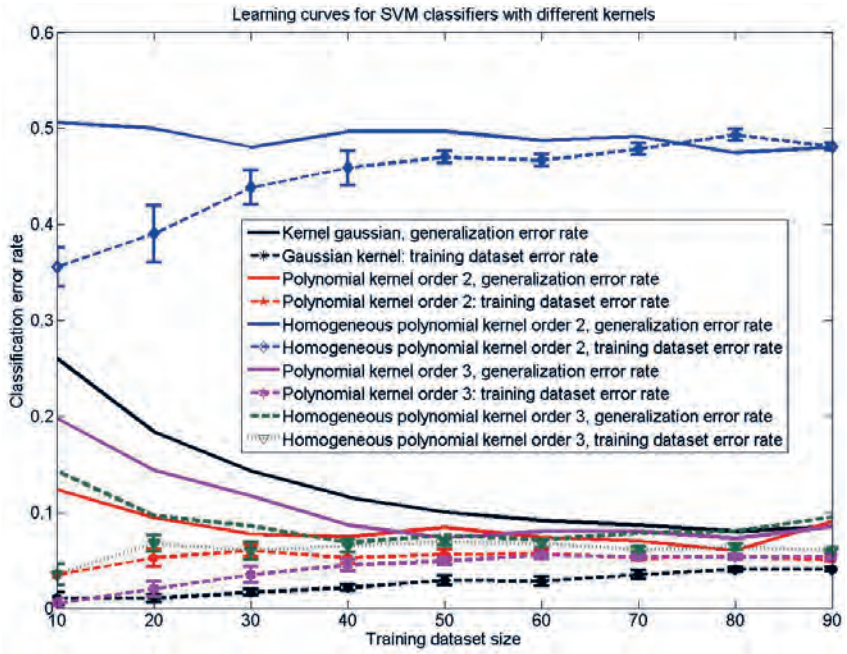

Fig. 3. Learning curves for SVM classifier.

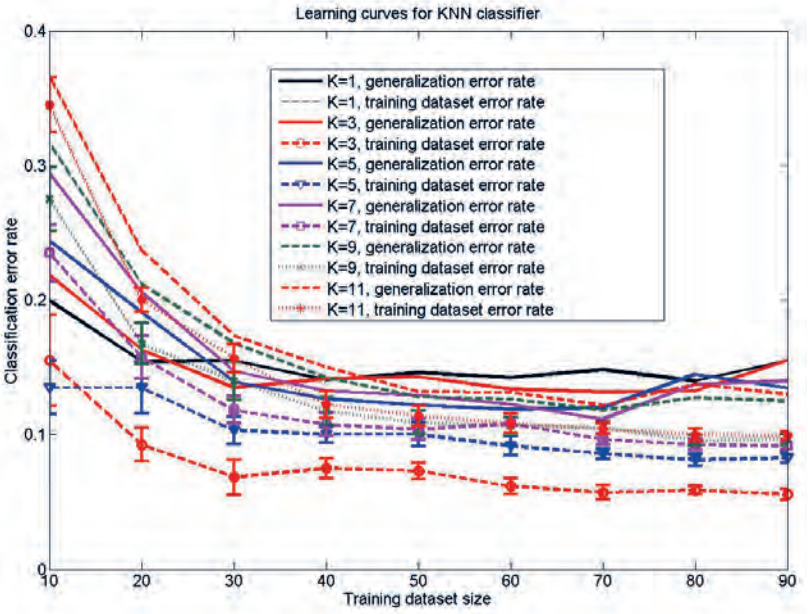

Fig. 4. Learning curves for KNN classifier.

Also, by applying the local fusion rule and the global biometric fusion rule, we obtain the performance depicted in figure 5, for different training dataset sizes. Also the figure 5 shows that the pre-classification fusion rule has an important potential to further improve the multimodal biometric system accuracy. The performance improvement provided by the feature-level biometric fusion is greater than for matching score-level biometric fusion, and this results shows that the earlier-stage biometric fusion could better exploit more discriminant information from the primary biometric data.

Finally, the figure 5 shows that the multimodal or multi-biometric approaches provide an obvious performance improving, by reducing the average global error rate for persons recognition. These results were achieved by performing 10 tests per person, and averaging the corresponding results.

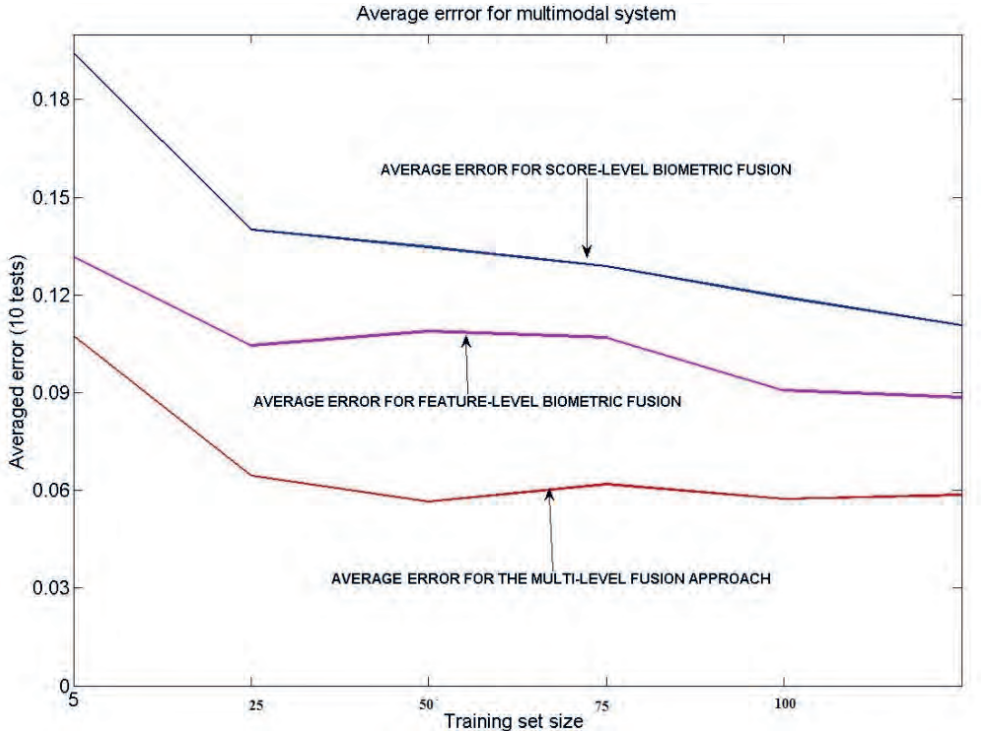

Fig. 5. The performance of the multimodal system with multi-level biometric fusion and multi-classifier approach.

5. CONCLUSIONS

In this paper we introduced a new vision for a highly accurate biometric system which combines fingerprint identification, palmprint identification and hand geometry identification systems in order to optimize the accuracy and performance. The proposed approach is based on a multi-level biometric fusion integration: feature-level fusion and matching score-level fusion. The feature-level biometric fusion provides most of the overall performance improvement for the whole multimodal biometric system.Although we found out the optimal classifier for each biometric component, by finding out the suitable training dataset providing the trade-off between the generalization error rate and the apparent error rate.

Finally, the multi-classifier approach applied for multimodal biometric systems allows to perform not only global optimization but either local optimization, in order to improve the biometric recognition accuracy. Further researches should be performed especially on feature-level biometric fusion, and its impact on biometric recognition accuracy.

REFERENCES

[1] P. Reid, *Biometrics for Network Security*, Prentice Hall, 2004.

[2] R. Snelick, M. Indovina, *Multimodal biometrics: issues in desgin and testing*, Proceedings of 5th International Conference on Multimodal Interface, pp.68-72, 2003.

[3] S. Soviany, M Jurian, *Multimodal biometric securing methods for informatics systems,* 34th International Spring Seminar on Electronics Technology (ISSE2011), Slovakia, 11-15 May 2011.

[4] R. Polikar, *Pattern recognition*, Wiley Encyclopedia of BioMedical Engineering, 2006.

[5] A.K. Jain, A*n Introduction to Biometric Recognition, IEEE Transaction on Circuits and Systems for Video Technology*, Special Issue on Image- and Video-Based Biometrics, vol. 14, no. 1, 2004.

[6] A.K. Jain, R.P.W. Duin, J. Mao, *Statistical Pattern Recognition: A Review*, in IEEE Transactions on

Pattern Analysis and Machine Intellingence, vol. 22, No.1, January 2000.

[7] S. Soviany, M. Jurian, R. Dragomir, S. Puşcoci, *Securing Medical Databases Access by Mixed Authentication Methods*, Proceeding of the 2nd International Conference on e-Health and Bio-engineering Romania, 2009.

[8] S. Soviany, M. Jurian, S. Puşcoci, *Decision Optimization Criteria in Multimodal Biometric Systems*, Proceeding of ECAI 2011-International Conference on Electronics, Computers and Artificial Intelligence, România, July 2011.

[9] S. Soviany, C. Soviany, M. Jurian, *A Multimodal Approach for Biometric Authentication with Multiple Classifiers*, Proceeding of ICCINS 2011-International Conference on Communications, Information and Network Security, Italy, November 2011.