International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:11, 2011

A Multimodal Approach for Biometric Authentication with Multiple Classifiers

Sorin Soviany, Cristina Soviany, Mariana Jurian

***Abstract*—**The paper presents a multimodal approach for biometric authentication, based on multiple classifiers. The proposed solution uses a post-classification biometric fusion method in which the biometric data classifiers outputs are combined in order to improve the overall biometric system performance by decreasing the classification error rates. The paper shows also the biometric recognition task improvement by means of a carefully feature selection, as much as not all of the feature vectors components support the accuracy improvement.

***Keywords*—**biometric fusion, multiple classifiers

I. Introduction

THE multimodal biometric systems integrate more technologies to perform people recognition by exploiting their individual physiological and/or behavioral traits. The increasing focus on the multimodal modern approach is justified by the unimodal biometric recognition systems limitations. The following main issues were encountered in the actual practice of unimodal biometric methods: security issues, accuracy issues and non-universality issues.

Most of the actual researches on multimodal biometrics focused on similarity matching score-level fusion schemes, but without further considering the statistical classification approaches and the classifiers combinations. The biometric fusion was only performed by combining the individual distance-based scores.

A novel approach is to apply the multi-classifier approach for an individual biometric within a multimodal system, and then combining their outputs (i.e. by averaging), thereby providing an additional local optimization level. This could be done by performing classification on carefully selected subset of features, and combining the results. The purpose is to increase the biometric recognition accuracy.

The main applications of the multimodal biometric authentication solutions are physical (i.e. border control) and logical (local and remote) access control (i.e. local or remote database access securing) [1].

The remainder of this paper is structured as follows. *Section II* presents the proposed multimodal biometric system architecture. *Section III* specifies the classification models applied for each of the integrated biometrics . The biometric fusion method is presented in *section IV*. *Section V* presents the achieved results (error rates) for the proposed multimodal biometric system (multi-classifier approach); these results are given on the ROC (Receiver Operating Characteristic) curves for each of the model component and for the overall multimodal system, respectively. *Section VI* concludes our research and also provides future research directions to be explored in order to improve the multimodal biometric recognition accuracy.

Sorin Soviany is scientific researcher at National Communications Research Institute, Bucharest, Romania.(phone: +40-21-3000011; fax: 021-318-9575; e-mail: sorin_soviany@co.cnscc.ro).

Cristina Soviany is founder and Managing Director at IDES Technologies, Bruxelles, Belgium (e-mail: cristina.soviany@ides-technologies.com).

Mariana Jurian is professor at Electronic and Computers Department, Pitesti University, Romania (e-mail: m_jurian@yahoo.com).

II. The Multimodal Biometric System Architecture

The multimodal biometric system is a biometric system which integrates more biometric technologies to perform the authentication process.

The multimodal biometric authentication is based on a typical pattern recognition application which is performed in the following stages [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. The multimodal biometric system architecture includes a feature extraction function for each of the integrated biometrics;
- *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; its performance provides also the system security and accuracy[6];
- *post-classification biometric fusion*: within this step, biometric data pre-processed (i.e. by feature extraction and selection tasks) and/or processed (by classification and/or matching tasks) are combined in a score-level approach;
- *final acceptance/rejection decision:* the global score given as a result of post-classification biometric fusion (S) is compared to the system security threshold (θ).

The proposed multimodal biometric system architecture is depicted in fig. 1[3].

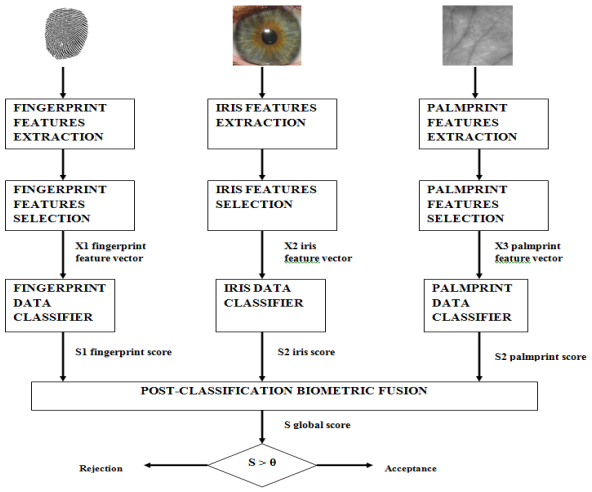

Fig. 1 The multimodal biometric system architecture

This structural-functional model integrates the following biometric methods:

- fingerprint recognition;
- iris recognition;
- palmprint recognition

It was used a database containing images of iris, fingerprint and palmprint of 20 persons. On these images it was 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.

III. Classification Models For Biometric Data

For the proposed combined system we developed classification models for each of its three components (fingerprint, iris and palmprint) separately. For each of these components it was 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. Moreover, after choosing the best classifier (or combination of classifiers) for each component, it was optimized the chosen representation space and classification algorithms using the ROC analysis by fixing the operating point in such a way to obtain the best accuracy tradeoff not only per component but also for the entire multi-modal system as a whole.

A. The classification model for fingerprint identification:

Parzen classifier

Let us consider the first system component, i.e. the fingerprint identification. For this subsystem, there were originally designed 25 fingerprint features and after careful analysis we finally selected 7 relevant features. Also it was considered 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).

The optimum classifier found for this set of 7 features was the Parzen classifier.

Parzen classifier is based on a non-parametric estimate of the class-conditional probability density function (p.d.f.).

The main components of any *probabilistic classifier model* (i.e. Naïve-Bayes classifier and also Parzen classifier) are the following[4][5]:

- $P(\omega_i)$ is the prior probability for class ω_i, $i = \overline{1, C}$
- $P\left(x \middle| \omega_i\right)$ is the class-conditional probability density function.

The probabilistic model assumes that both $P(\omega_i)$ and $P\left(x \middle| \omega_i\right)$ are known. The posterior probability is computed based on Bayes theorem, according to (1):

$$P\left(\omega_i \middle| x\right) = \frac{P\left(\omega_i\right) \cdot P\left(x \middle| \omega_i\right)}{P\left(x\right)} \quad (1)$$

where P(x) is given by

$$P\left(x\right) = \sum_{j=i}^{C} P\left(\omega_j\right) P\left(x \middle| \omega_j\right) \quad (2)$$

Within this probabilistic framework, the optimal classifier is one that performs assignation of the feature vector x to the class with the highest posterior probability, i.e.:

$$\omega = \arg\max_{\omega_k} P\left(\omega_k \middle| x\right) \quad (3)$$

Parzen classifier uses this probabilistic model and a kernel function in order to get the class-conditional probability density estimate and finally to estimate the posterior probability for each class [5].

As for all biometric data classifiers considered for the proposed multimodal system, the training dataset is relying on biometric records from a number of persons N=20. The validation dataset includes 10 records, which should be independent from the training set. These datasets are denoted as it follows:

$Z1=\{z1_1, z1_2, .., z1_N\}$ the fingerprint classifier training dataset;
n1 is the selected features number (n1 = 7);
X1 denotes the validation dataset, with size(X1)=10

The Parzen classifier model uses a *kernel function* (*Parzen window function*), denoted K(x1); for fingerprint identification subsystem, x1 is the fingerprint feature vector resulted from the feature extraction and selection steps.

K(x1) denotes a multi-dimensional function centered around the component $Z1_j$ of the training dataset, and it is usually given in the following form:

$$\frac{1}{h^{n1}}K\left(\frac{x1-zl_j}{h}\right)$$

where h is the *smoothing parameter* for the *Parzen window*. According to the Parzen classifier model, the class-conditional probability density function is estimated based on the samples set Z1 (for fingerprint biometric data, in this case) by:

$$\hat{P}\left(x1|\omega_i\right)=\frac{1}{N_i}\sum_{j=1}^{N}\frac{1}{h^{n1}}K\left(\frac{x1-zl_j}{h}\right) \quad (4)$$

$$zl_j \in Z1$$

In equation (4), N_i is the number of training samples (from the dataset Z1) belonging to the class ω_1.

Also the prior probability estimators are given by

$$\hat{P}\left(\omega_i\right)=\frac{N_i}{N} \quad (5)$$

Therefore the posterior probability estimate for the fingerprint feature vector x1 is given by Bayes theorem, (1), in which the prior probability estimates and the class-conditional p.d.f. estimates are given by (4) and (5):

$$\hat{P}\left(\omega_i|x1\right)=\frac{1}{Np\left(x1\right)}\sum_{j=1}^{N}\frac{1}{h^{n1}}K\left(\frac{x1-zl_j}{h}\right) \quad (6)$$

If using the following indicator function:

$$I(i,j)=\begin{cases}1, & \text{if } zl_j \in \text{class}\left(\omega_i\right)\\ 0, & \text{otherwise}\end{cases}$$

then the posterior probability for the fingerprint feature vector x1 is estimated by:

$$\hat{P}\left(\omega_i|x1\right)=\frac{1}{N}C_1\left(x1\right)\sum_{j=1}^{N}I(i,j)K\left(\frac{x1-zl_j}{h}\right) \quad (7)$$

The equation (7) includes a generic term $C_1\left(x1\right)$ which is dependent on the feature vector x1 and also on the samples number N of the dataset.

The assumed kernel function (Parzen window) for the fingerprint classification model was the multi-variate Gaussian kernel function, as much as the data distribution follows the normal law as resulting from our experiments. The Gaussian kernel is expressed by (8):

$$\frac{1}{h^{n1}}K_G\left(\frac{x1-zl_j}{h}\right)=\frac{1}{h^{n1}\cdot\sqrt{(2\pi)^{n1}}\sqrt{\det\left(S_1\right)}}\cdot \exp\left(-\frac{1}{2h^2}\left(x1-zl_j\right)^T S_1^{-1}\left(x1-zl_j\right)\right) \quad (8)$$

where S_1 is the covariance matrix expressed by

$$S_1=E\left[\left(x1-E\left[x1\right]\right)\left(x1-E\left[x1\right]\right)^T\right] \quad (9)$$

Finally the posterior probability estimates for fingerprint feature vector x1 are given by the following equation in the Parzen classifier model with multidimensional Gaussian kernel:

$$\hat{P}\left(\omega_i|x1\right)=\frac{1}{N}C_2\left(x1\right)\sum_{j=1}^{N}I(i,j)K_G\left(\frac{x1-zl_j}{h}\right);\quad i=1,...,C \quad (10)$$

C_2 is also a coefficient dependent on the feature vector x1. For the biometric identification, the overall classes number C is the number of the genuine users which were previously enrolled in the biometric system database.

B. The classification model for iris identification: KNN classifier

For the second component, i.e. the iris recognition subsystem there were generated 41 relevant features from which there were finally selected 13 features (i.e. the normalized distance between the inner and the outer boundary iris, spatial location, orientation and frequency for typical iris patterns or texture details, spots, furrows, stripes and so on). The optimal found classifier was a KNN classifier with a kernel of 7.

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 x2 is the iris feature vector obtained from this biometric. Also the training dataset for iris data KNN classifier is $Z2=\{z2_1, z2_2,\ldots,z2_N\}$. Each component of the iris training dataset is a labeled data instance.

For every instance $X2_i$, 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 Z2: $\{Z2_1, Z2_2,\ldots,Z2_K\}$. These are the K closest training data instances to the instance x2 to be classified;
2. Label x2 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 x2 (iris feature vectors) and its neighbors from the training

dataset, the Mahalanobis distance was applied, according to (11):

$$D_M(x2,z2)=\sqrt{(x2-z2)^{\tau}\cdot S^{-1}\cdot(x2-z2)} \quad (11)$$

where S is the covariance matrix between the instances x2 and z2. 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:

$$w(i)=\frac{1}{d(z2_i,x2)^2} \quad (12)$$

where:

w(i) is the weight for the neighbor instance $z2_i$;

x2 is the unknown instance to be classified.

Also the distance between the training data instance and the testing instance, *d(z2i, x2)*, is computed using Mahalanobis distance, given by (11).

C. The classification model for palmprint identification: combined classifier (Fisher and KNN)

For the third component, i.e. the palmprint recognition subsystem 34 features were designed from which there were selected 19 features (such as 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) as representation space for this data. As a final classifier for this subsystem, a combined classifier was applied, consisting on a Fisher (on a subset of 9 from the selected 19 features) and a KNN with a kernel of 5 (on a subset of 10 from the 19 selected features).

Actually a multi-class extension of the Fisher linear discriminant analysis (LDA) was applied to classify the first subset of the palmprint features.

This linear discriminant gives a separation by finding out of a linear transformation w in the F-dimensional representation space in order to maximize the ratio between the inter-class scatter matrix determinant and the intra-class scatter matrix determinant, actually the following function [4]:

$$J(w)=\frac{\text{Inter}-\text{class variance}}{\text{Intra}-\text{class variance}} \quad (13)$$

For a training dataset consisting in N F-dimensional labeled samples $z1,z2,\ldots,z_N$, belonging to N classes (as much as the biometric application has to perform persons identification), the intra-class scatter matrix is given by

$$S_{within}=\sum_{i=1}^{N}\sum_{z\in class(\omega_i)}(z-\overline{z1})(z-\overline{z1})^T \quad (14)$$

where

$$\overline{z1}=\frac{1}{Ni}\sum_{z\in class(\omega_i)} z \quad (15)$$

and Ni is the number of training samples belonging to class i.

Also the inter-class scatter matrix is given by (16):

$$S_{between}=\sum_{i=1}^{N} Ni(\overline{z1}-\bar{z})(\overline{z1}-\bar{z})^T \quad (16)$$

where $\overline{z1}$ is the mean for each class, computed with (15), and $\bar{z}$ is the total mean vector given by

$$\bar{z}=\frac{1}{N}\sum_{i=1}^{N} Ni\overline{z1} \quad (17)$$

The total number of classes is assumed to be the same as the total number of the training dataset records. This assumption is valid for a biometric identification process, in which each person's biometric data are belonging to a separate class.

After obtaining the intra- and inter-class scatter matrix, the Fisher criterion states that the desired linear transformation w should maximize the following ratio:

$$J(w)=\frac{|w^T S_{between} w|}{|w^T S_{within} w|} \quad (18)$$

This linear transformation could result from the generalized eigenvalues equation:

$$S_{between} w=\lambda S_{within} w \quad (19)$$

where λ is the eigenvalue for the matrix $S_{within}^{-1}S_{between}$

Finally, once having the linear transformation w, the classification is performed in the transformed palmprint features representation space based on a distance metric. Again, the Mahalanobis distance between the samples was used, for the same reasons as for the iris data classifier.

The second feature subset of the palmprint biometric is classified using the KNN classifier (k=5), with the same distance metric as for KNN-based iris classifier (Mahalanobis).

Finally the two classifiers output were average to obtain the decision function value for the palmprint biometric.

IV. The Biometric Fusion Method

The fusion method consists on a unique combination of fingerprint identification, iris recognition an hand recognition,

each subsystem being designed and optimized separately and also entirely, at a global level [2][7][8].

Taking the output for each identification subsystem, i.e. y1 for fingerprint component, y2 for iris component and y3 for palmprint component, the whole multimodal system output Y is given by the following rule:

$$Y = \sum_{i=1}^{n} w_i \cdot y_i \quad (20)$$

where:

n is the identification components number. Here n = 3;

w_i is the weight which we assigned to the component i.

y_i is 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:

$$\sum_{i=1}^{n} w_i = 1 \quad (21)$$

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

- weights initialization

$$w_i \leftarrow w_{i,0} = \frac{1}{n}, \quad i=\overline{1,n} \quad (22)$$

- weights updating

$$w_i \leftarrow w_i \cdot K_i, \quad i=\overline{1,n}, \quad K_i > 0 \quad (23)$$

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

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.

V. Results And Discussion

This optimization method is focused first locally, at the component level and finally global, at the system level. All optimizations were done using a thorough fully analysis of the ROC curves on error per component and then global.

Fig. 2 presents the ROC curve with error rates on 2 data samples from our database: A (which stands for person A) and B (which stands for person B) for the fingerprint identification component. The optimal selected model for this fingerprint identification component had an average error of 0.14. This is a tradeoff for the fingerprint identification subsystem.

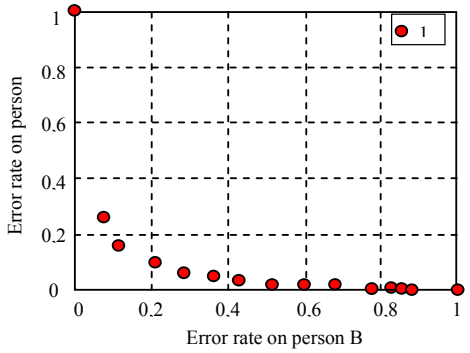

Fig. 2 The ROC curve with error rates for fingerprint identification subsystem

Similarly, fig. 3 depicts the ROC curve for the iris identification subsystem. The best performance obtained for this component corresponds to an average error of 0,15, again as a tradeoff for the 2 classes (persons) A and B. This value is close to the average error rate obtained for fingerprint identification. Like for the previous identification subsystem, the global error rate for all classes could be evaluated by averaging on each persons pairs. Also these tradeoffs were obtained for certain security thresholds fixed for the identification process.

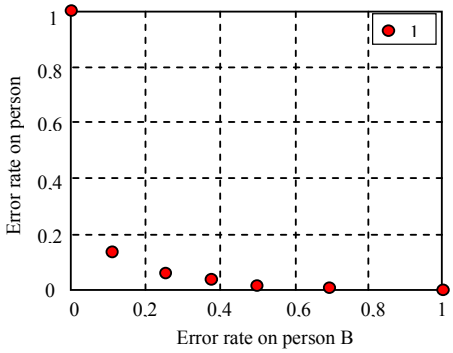

Fig. 3 The ROC curve with error rates for iris identification subsystem

Fig. 4 shows that for palmprint identification subsystem, the operation point (defined by the tradeoff for the average rate) provides an average error rate of 0,17.

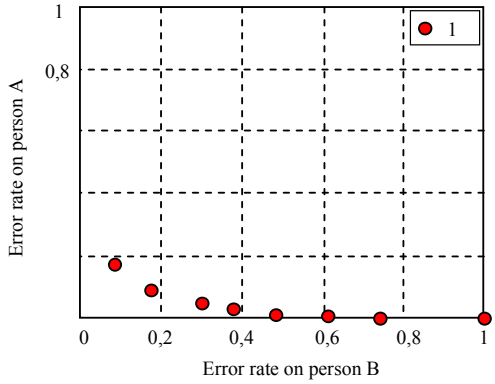

Fig. 4 The ROC curve with error rates for palmprint identification subsystem

The final solution was achieved by combining the separate 3 models and, in fig. 5 below, we give again the ROC on error rates for the same 2 data samples A and B. For the same threshold as for each identification subsystem, the achieved average error rate of 0,07 is less than the average error per person for each of the system components (fingerprint, iris and palmprint recognition subsystems, respectively).

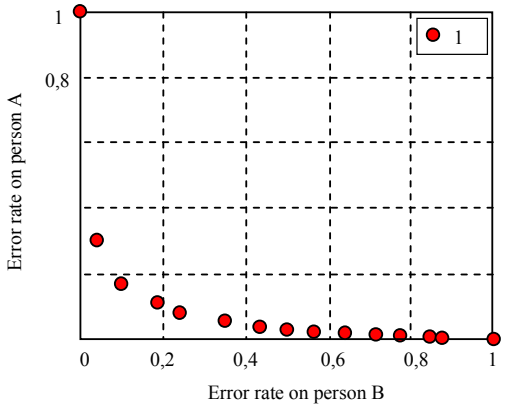

Fig. 5 The ROC curve with error rates for the multimodal system (multi-classifier approach)

VI. Conclusions

In this paper it was introduced a new vision for of a highly accurate biometric system which combines fingerprint identification, iris identification and palmprint identification systems in order to optimize the accuracy and performance. This approach optimized the performance of each component independently and then as a combination of the whole system. As it was presented, using this combined approach it is possible to obtain a very accurate biometric identification with global errors on each class (person to be identifies) less than 0,08. This global error rate was obtained for a fixed security threshold of the biometric system.

However, there are still opportunities for further improvement as much as it is still possible to decrease the classification error rate by increasing the training dataset size for each biometric classifier. Another improvement possibility is to make a more efficient feature selection and to include an additional biometric fusion (i.e. feature-level fusion). Therefore, a multimodal biometric system with multi-level fusion schemes is an option to be further researched.

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. This approach also supports designing the multimodal system with multi-level biometric fusion, as previously mentioned.

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 „An 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 Bioengineering, 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 Intellingence, România, July 2011