AN APPROACH ON BIMODAL BIOMETRIC SYSTEMS

Eugen LUPU , Simina EMERICH
Technical University of Cluj-Napoca, 26-28 Baritiu str. Cluj-Napoca
phone: +40-264-401-266; fax: +40-264-592-055;
e-mail: Eugen.Lupu @com.utcluj.ro

Abstract: Although unimodal biometric systems have an edge over traditional security methods they have their limits and raise a variety of problems. In order to overcome some inconveniences and limitations of these systems and in order to realize reliable and robust authentication systems, the use of multimodal biometric systems is recommended. The information contained in multiple biometrics can be integrated by using various methods at distinct levels (rank, decision, match-score levels, feature and sensor) and in different contexts. The experiments were made on a bimodal biometric system employing speech and dynamic signature as biometric features. The results show that the score fusion of the two biometric improves the system overall performance.

Keywords: *biometric, speech, dynamic signature, score level fusion, feature selection*

I. INTRODUCTION

Biometric systems consist of recognition systems which are based certain models. They capture biometric features from a person and extract a set of specific vectors which are later compared with a set of models held in a database.

The four important elements met in a common biometric system are the following [5]:

- *Sensor module:* acquires the biometric data of an individual, an example of such an element being the microphone which captures voice utterances.
- *Feature extraction module:* feature values are extracted after processing the acquired data. An example of this is the extraction of MFCC coefficients in the feature extraction module of a speech system.
- *Matching module*: by generating a matching score, the feature values are compared with the values in the template. For instance, the distance between the query sequence of MFCC coefficients extracted from speech signal and the template will be computed and treated as a matching score in this module.
- *Decision module*: establishment of the user's identity takes place or a claimed identity is accepted or rejected based on the matching score generated in the matching module.

The application context determines the mode in which a biometric system must operate: the *verification* mode or the *identification* mode.

Biometric recognition firstly implies the **enrolment of the user** in the system such that a reference model is created in the database.

formation. The following limitations and problems affect

In the verification mode, there can be either acceptance or rejection of the assignation of the test model to the asserted person. Hence, one comparison only is made between the test model and the reference of the claiming user.

In identification mode, the system recognizes whom the tested biometric feature belongs to, by this understanding that it compares the test model with the reference models from the database test vector.

A **screening task** is required in some applications to verify if some persons or suspects are registered in the biometric database [1] [2].

The global performance of a biometric system is appreciated by considering different factors such as precision, speed and storage of the data, easiness of utilization and costs. These factors affect system efficiency. The application determines the features of the architecture of the biometric recognition system.

Enlisting of any user must be performed before he/she can be tested by the system, this meaning that he/she must pass through a stage where the biometric characteristics are captured.

II. MULTIMODAL BIOMETRIC SYSTEMS

A. Unimodal biometrics limitations

Unimodal biometric verification systems are more reliable than classical authentication systems. The essence of unimodal biometric systems is that they perform person recognition based on a single source of biometric in

such systems:

Manuscript received September 3, 2010; Revised November 3, 2010

- Lack of universality of some characteristics; for example, approximately 4% of people cannot enlist because of weak fingerprints, and this figure increases at 7% in the case of the iris [6];
- Noisy signals captured from the sensors due to incorrect usage and due to environmental conditions such as humidity, dirt, dust etc.;
- Lack of safety of the used sensors;
- Limitation of the discrimination of biometric systems due to a high in-class and low inter-class variability;
- The recognition performances of the systems are upper limited;
- In the case of unimodal biometric systems, unacceptable error rates have been accounted for;
- Lack of variability in time and permanence of biometric features;
- Possibility of fraud through the cloning of a biometric characteristic either voluntarily or involuntarily [3].

These practical problems lead to quite high error rates associated with unimodal biometric systems, their being made unacceptable for deployment in security critical applications.

A synthesis of the information above may be found in the following: ***each biometric feature has its limits and no biometric system is perfect.***

B. Multimodal systems overview

Multimodal systems are used in order to overcome the above mentioned limitations and problems. This leads to the improvement of the system's performances and to the increase of the number of enlisted population in the systems. Also, this ensures significant discouragement of fraud. The multibiometric system may be seen as a fault tolerant system which may operate even when some biometric sources become unreliable due to different malfunctions.
The goal of the biometrics systems is to reduce as much as possible of the features below:

- False acceptance rate (FAR)
- False rejection rate (FRR)
- Failure to enroll rate (FTE)
- Failure to acquire rate (FaR)
- Susceptibility to spoofing (SS)

Some drawbacks that belong to this approach are:

- The increase in the complexity of the multimodal system
- Additional costs for the sensors
- Increase of system testing time
- Additional costs and delays for user enrolling
- Need for a priori data.

Multimodal systems architecture

An important role in making the design decisions is played by the application scenario which influences the performance of the system. The architecture of a multimodal biometric system is determined by the sequence in which different biometrics are acquired and processed. The architecture is either of *parallel* or *cascade/serial* nature. **Parallel** functioning involves the processing types operating independently with their outcomes fusing according to a predefined scheme, while functioning in **serial** implies the sequential processing of functions with the result from one modality affecting the next modality.

Advantages and disadvantages occur in both types of architecture: serial systems are more user-friendly because they require less recognition time compared to parallel systems, yet they require complex algorithms in order to achieve the control of the sequence of operations. Hence, a cascaded multimodal biometrics system is recommended for applications that are less security critical (e.g. bank ATMs).

Parallel architecture is recommended for applications which require a high level of security (e.g. access to military installations or sites). **Hierarchical** construction is another possibility, that of combining parallel and serial architecture, by designing a system that preserves the advantages offered by both architectures [3] [4].

Sources of evidence

Different biometric ***sources of evidence*** are used in multimodal biometric systems so as to overcome the limitations of unimodal biometric systems. Multimodal biometric systems may be of the following types (fig.1 adapted from [6]):

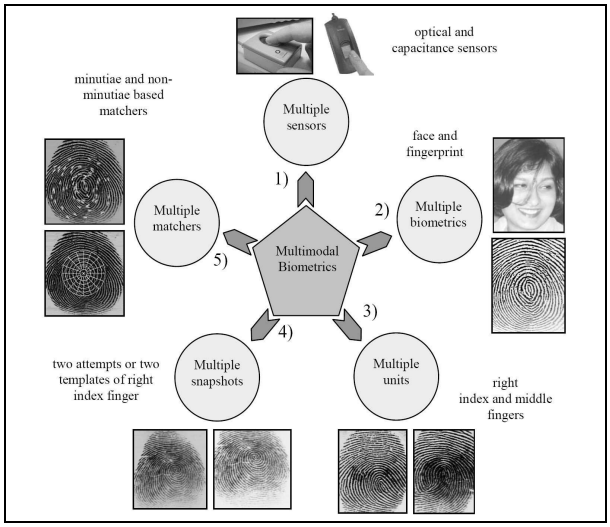


Figure 1. Scenarios in a multimodal biometric system.

1. Single biometric trait, multiple sensors: multiple sensors record the same biometric feature; in this way, raw biometric data obtained from different sensors is attained.

2. Single biometric trait, multiple classifiers: one sensor only is employed in order to obtain raw data; this data is later used by multiple classifiers, each of them operating either on the same feature set extracted from the data or by generating their own feature sets.

3. Single biometric trait, multiple units: in the case of fingerprints or iris, there is the possibility of integrating information from two or more fingers or from both the irises of one user. This consists of a cost effective method of improving system performance as it does not require multiple sensors nor additional feature extraction or matching modules.
4. Multi-capture/instance system: samples are acquired from the same biometric characteristic; for instance, the same fingerprint will be sampled several times;
5. Multiple biometric traits: multiple biometric features (fingerprints, face, hand, voice etc.) are employed when establishing the identity of an individual; multiple sensors are used to acquire data pertaining to different traits; the independence of the traits ensures significant improvement in performance [11].

C. Levels of fusion

In theory, it is possible that **fusion** occurs at any level (sensors, feature extraction, parameters matching or decision module) in the multimodal biometric systems. A variety of scenarios become possible, depending on the number of traits, sensors, and feature sets used (Figure 2).

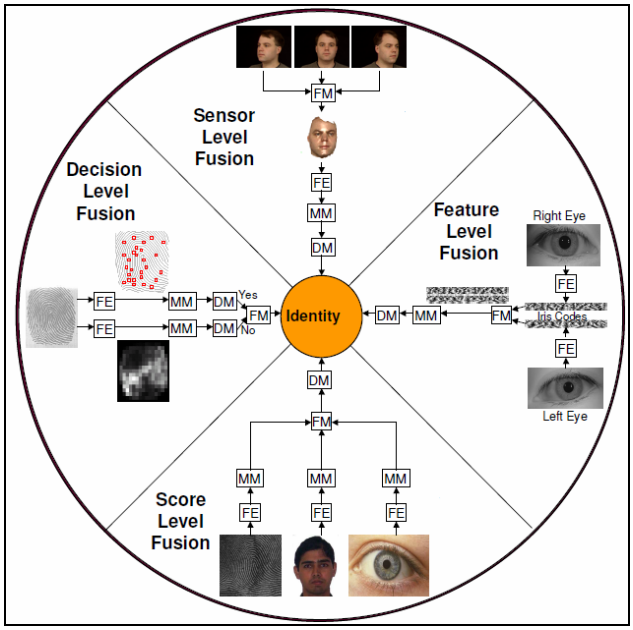


Figure 2. Levels of fusion in multibiometric systems. (adapted from [1])

In general, the fusions at the first two levels are difficult to achieve. For example, fusion at the feature level in practice is difficult to be employed due to the fact that the feature sets of the various modalities may be incompatible (eigen-coefficients of face and minutiae set of finger) and due to the fact that most commercial biometric systems do not provide access to the feature sets used in their products; the decision level is seen as rigid because of availability of limited information. Fusion at the matching score level is preferred in general, as relatively low difficulty is implied by accessing and combining the scores presented by multiple modalities [10].

Decision level fusion. Each biometric device makes its own accept or reject decision, these decisions being then fused together by the multi-modal combiner by voting, a weighted sum or some other way. Its performance is not good enough such that it often gives a combined decision worse than the decision from the best individual biometric device.

Score level fusion. When the match scores provided by different biometric matchers are combined to obtain a final recognition decision, fusion is realized at the match score level or confidence level. The most commonly used approach in multibiometric systems is the information fusion at the match score level as it offers the best trade off in terms of ease in fusion and information content. In the case of a correct approach, the combined performance is guaranteed to be no worse than the best of the individual performances [4].
Many score level fusion techniques have been proposed in the literature, the being grouped into three main categories: density-based, transformation-based and classifier-based schemes. The performance of each scheme depends on the both the amount and the quality of the available training data [7].

Feature level fusion. In the unlikely case that correlation between the features measured by the individual biometric device exists, this level can be better than score fusion. Otherwise, score combination will work, it being simpler as well.

D. Fusion methods

Fusion in biometrics systems can take the different forms and may be realized at more levels [5]. Five fusion methods are presented here, among which the first three are considered classical and the last two are seen as innovative solutions, their employing the importance of individual matchers in analyzing their contributions [8].

The explained notations are the following : n_m^i for the normalized value for the matcher m (m=1,2,…M, M is the number of distinct matchers) and the user i (i=1,2,…I, I is the number of registered individuals). f_i is the fused score.

Simple sum (SS): Sums the scores for an individual:

$$f_i = \sum_{m=1}^{M} n_i^m, \forall i \tag{3}$$

Min Score (MIS): Extracts the minimum from the scores of an individual:

$$f_i = \min(n_i^1, n_i^2, \ldots\ldots n_i^M), \forall i \tag{4}$$

***Max Score (MAS)**:* Extracts the maximum from the scores of an individual:

$$f_i = \max(n_i^1, n_i^2, \ldots\ldots n_i^M), \forall i \quad (5)$$

Matcher Weighting (MW): Fusion based on MW uses the Equal Error Rate (EER). The weight w^m connected to the matcher m is calculated as it follows, provided that the EER of the matcher m is e^m, m=1, 2...M:

$$w^m = \frac{\frac{1}{e^m}}{\sum_{m=1}^{M} \frac{1}{e^m}} \quad (6)$$

One must consider that $0 \le w^m \le 1, \forall m, \sum_{m=1}^{M} w^m = 1$ and that the relationship between weights and their corresponding errors is of inverse proportionality, consequently higher weights are in relation to more accurate matchers. It must be mentioned that EER is used so as to spam the data available to the integrator above, even though the accuracy of a matcher may not be estimated well enough by the EER alone. The fused score (MW) is given by:

$$f_i = \sum_{m=1}^{M} w^m n_i^m, \forall i \quad (7)$$

User Weighting (UW): Applies weights to individual matchers, leading to distinct solutions for distinct users. The fused score will be calculated as follows:

$$f_i = \sum_{m=1}^{M} w_i^m n_i^m, \forall i \quad (8)$$

where w_i^m represents the weight of a matcher m for user i.

E. Normalization techniques

The matching scores output given by the different modalities are heterogeneous (distance or similarity), distributions may be different; hence score normalization is needed so that the scores can be brought to a common domain before combining them. For example, if one matcher is in the interval [100, 500] and another matcher is in the interval [0, 1], the lack of normalization in the fusion of scores leads to the neglecting of the contribution of the second matcher. The most frequently used methods are presented in what follows [8]. Let ***s*** be a raw matcher from the complete set of scores for that matcher, and ***n*** the corresponding normalized score.

Min-Max (MM): Maps the raw scores in the [0, 1] range, max(S) and min(S) being the limits of the score range, generally provided by vendors:

$$n = \frac{s - \min(S)}{\max(S) - \min(S)} \quad (9)$$

Z-score (ZS): Transforms scores to a distribution with mean of 0 and standard deviation of 1. *Mean () and std ()* represent the mean and standard deviation operators:

$$n = \frac{s - mean(S)}{std(S)} \quad (10)$$

Tanh(TH): Robust statistical technique [6], it maps the scores to the [0, 1] range:

$$n = \frac{1}{2}\left[\tanh\left(0.01\frac{s - mean(S)}{std(S)}\right) + 1\right] \quad (11)$$

Adaptive (AD): Errors of individual biometric matchers are given by the overlap of genuine and impostor distributions, this region giving its center *c* and its width *w*. An adaptive normalization procedure which increases the level of separation of genuine and impostor distributions is used, while mapping scores to [0, 1]. It is formulated as

$$n_{AD} = f(n_{MM}) \quad (12)$$

where *f()* is the mapping function used on the matching module normalized scores. These functions may be logistic quadratic-line-quadratic, two-quadratics [8].

Normalization technique	Robustness	Efficiency
Min-max	**No**	**High**
Decimal scaling	**No**	**High**
Z-score	**No**	**High (optimal for Gaussian data)**
Median and MAD	**Yes**	**Moderate**
Double sigmoid	**Yes**	**High**
Tanh estimators	**Yes**	**High**
Biweight estimators	**Yes**	**High**

Table 1. Efficiency and robustness of normalization techniques [7].

III. BIMODAL SPEECH – DYNAMIC SIGNATURE BIOMETRIC SYSTEM

A. Bimodal biometric system architecture

Among the biometrics that has a high user acceptance are the following: face, speech and signature. Although they don't have the best performances (due to repetitions, sessions, channel, and background noise) they provide some important advantages such as:

- user friendliness
- short time required by enrolment session
- capturing does not require special hardware
- difficult to imposture all modalities
- biometric profile remains local, hence guaranteeing privacy
- processing of the biometric data is local (privacy).

In our experiments we chose a system based on speech and dynamic signature as biometrics, due to their similarity to signal level and due to the use of the same feature extraction. In the figure below, a bimodal biometric system architecture employing a score level fusion is presented.

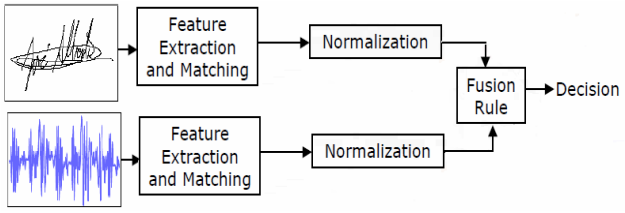


Figure 3. Dynamic signature and speech score level fusion biometric system.

B. Features extraction and selection

The TESPAR DZ coefficients consist of the main features extracted from the signal samples [9]. Also, other additional features based on wavelet analysis are employed. The background of TESPAR method is presented in references [14] [15]. This paper employs a version of this method using TESPAR DZ matrices. Hence, three descriptors will be used for each epoch: D, S and A (Amplitude) which stands for the maximum value among the samples of an epoch. The TESPAR DZ coding procedure ensures that pairs of epochs are compared and then each type of descriptor from each epoch pair is compared and a symbol is produced indicating the differences between the individual D, S and Amplitude descriptors of the two epochs being compared [9].

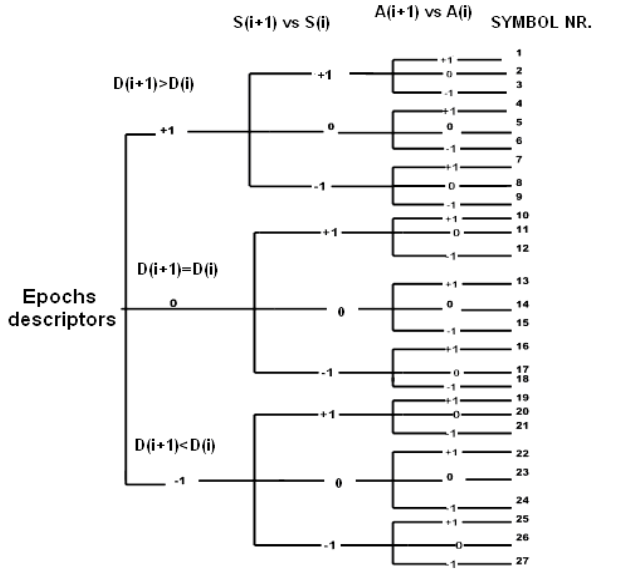


Figure 4. TESPAR DZ symbols assignation.

The comparison between the descriptors of the epochs may be performed for different lags. The mechanism is illustrated in what follows: comparisons will be made between epoch K and epoch K-1 for a lag=1, comparisons will be made between epoch K and epoch K-2 for a lag=2 etc. For each individual epoch pair comparison and for each epoch descriptor a three level vector comparison is made. Consequently, for a lag of 1, when comparing D, S and A, for epochs K1 and K2, the following holds for parameter D: if D2=D1, the resulted value is 0, if D2<D1, the resulted value is -1 and if D2>D1, the resulted value is +1.
Fig. 4 presents the flowchart of the symbol assignation [9].

Fig. 5 shows a histogram resulted in the TESPAR DZ coding process (from the symbols string) for a user utterance and fig. 6 an averaged histogram for Vy (y axe velocity) feature provided by a user signature.

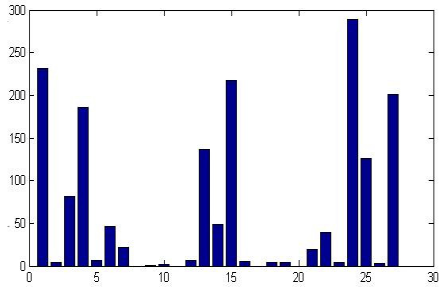


Figure 5. TESPAR DZ histogram for a coded utterance.

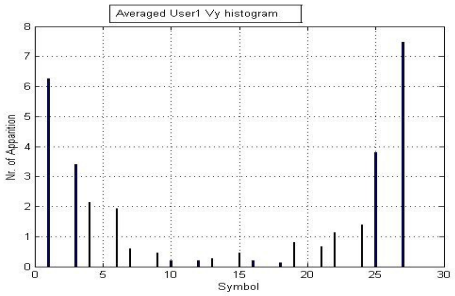


Figure 6. TESPAR DZ histogram for velocity Vy feature.

Wavelets are a recently developed processing tool. The input signal is passed through two complementary filters to obtain *approximations* - high scale and low frequency components and *details* - low scale and high frequency components. The algorithm is iterative, the approximations being successively decomposed. Usually the decomposition level is chosen according to the nature of the signal or on certain criteria. The final set of components characterizes the signal completely.
In our approach, we selected the Haar wavelet function and 4 iterations. Further, the energy of approximation (cA5) and details (cD1, cD2, cD3, cD4) was computed, obtaining 5 additional coefficients for each analyzed signal.

By applying the TESPAR DZ coding procedure 27 coefficients are obtained from each speech signal. Moreover, 5 energy wavelet based coefficients are added, resulting into a 32 length vector - $\mathbf{Speech_{32}}$.
After some previous experiments, we decided to employ the following functions: $y(t)$, $v_x(t)$, $v_y(t)$, $p(t)$ (*y* axis position, the writing velocities *Vx, Vy* and the pressure) to generate the templates for each signature [9]. By applying the same methods, we obtained a vector of 128(4*27+4*5) coefficients – $\mathbf{Sign_{128}}$.

Most methods for feature selection involve searching the space of attributes in order to find a subset of relevant features that is most likely to predict the correct class. To do this, we chose the "Ranker" method from the "ChiSquaredAttributeEval" algorithm of Weka's Attribute Evaluator."ChiSquaredAttributeEval" calculates the intensity of the correlations between attributes, using the ChiSquare (χ^2) test. The "Ranker" method sorts the attributes depending on the evaluation. After the feature

selection step, we retained 20 coefficients for speech (**$Speech_{20}$**) and 42 for each signature (**$Sign_{42}$**). This feature selection brings important vector dimensions reduction; so the speech vector length arrive to 62.5% from the initial dimension, while signature vector length to 32.8% and the results are unchanged.

C. PENTAHO system approach

WEKA (Waikato Environment for Knowledge Analysis) [16] is recognized as a landmark system in data mining and machine learning, it having achieved widespread acceptance within business circles and academia. Free access to the source code has enabled the development of a thriving community and has facilitated the creation of many projects that use WEKA.

Pentaho Data Mining [17] is based on the Weka software and provides a modern environment for building analytical models, it providing a comprehensive suite of data mining tools with more than 200 algorithms for data pre-processing, classification, clustering, regression and attribute selection. Furthermore, Weka's community and strong connections to academia ensure that the toolkit remains up-to-date. User-friendly graphical interfaces and full support for experimental data mining ensure the fast development and validation of predictive models.

Pentaho Data Integration or **Kettle** ensures powerful Extraction, Transformation and Loading (ETL) capabilities using a metadata focused approach. With an intuitive environment and a proven and standards-based architecture, Pentaho Data Integration more and more represents the choice of organizations over other tools.

The Weka scoring plug-in is a tool that ensures classification and clustering models created with Weka to be used to score new data as part of a Kettle transform. "Scoring" stands for attaching a prediction to an incoming set of data. The plug-in is capable of handling all types of classifiers and clusters that can be constructed in Weka. This scoring plug-in allows the attachment of a predicted label (classification/clustering), number (regression) or probability distribution (classification/ clustering) to a row of data [18].

IV. EXPERIMENTS AND RESULTS

Our bimodal database **(BimDB10)** contains 100 signatures and 100 utterances from 10 users, items which were collected during 10 different sessions. Several series of experiments have been carried out by using 2 items from each session, so 20 attempts/user. The fact that there are inherent variations in the patterns written or uttered by the same person during time is well known.

In our study, by using the weighted sum of scores fusion rule after the normalization of each matcher's output, the unimodal match scores have been computed. We considered the minimum and maximum values for the given set of training match scores and then the min-max normalization was applied.

After the feature extraction and selection steps, the relevant coefficients were converted to *''. arff"* (Attribute-Relation File Format) files for both signature and speech and they were given as input to the Weka system. An ARFF file is an ASCII text file describing a list of instances sharing a set of attributes, it having been developed for use with the Weka software. The header of this file contains the name of the relation, a list of attributes and their types. In the data section, every instance is represented on a single line. Attribute values are delimited by commas and must appear in the order in which they were declared in the header part of the file.

These input files must also be converted to *''.csv" (Comma-Separated Variables)* format, so that they become compatible with Kettle.

In these experiments we choose to use two types of classifiers respectively BayesNet (Bayes Network) and IBk (Instance Based of the Nearest k Neighbor). We performed a10-fold cross-validation learning scheme on the training data and the results provided by Weka were further stored into*''. model"* files.

The next step is that of Weka scoring plug-in installation in Kettle, followed by the construction of a simple transform that links a CSV input step to the Weka scoring step. The fields in the incoming data from the .csv file have been matched with the attributes model file. The output is represented by a set of matching scores which stand for the probabilities that one object belongs to different possible classes and is saved in *''.xls"* (Excel file) format, Fig.7. Further, the score level fusion was implemented in Matlab.

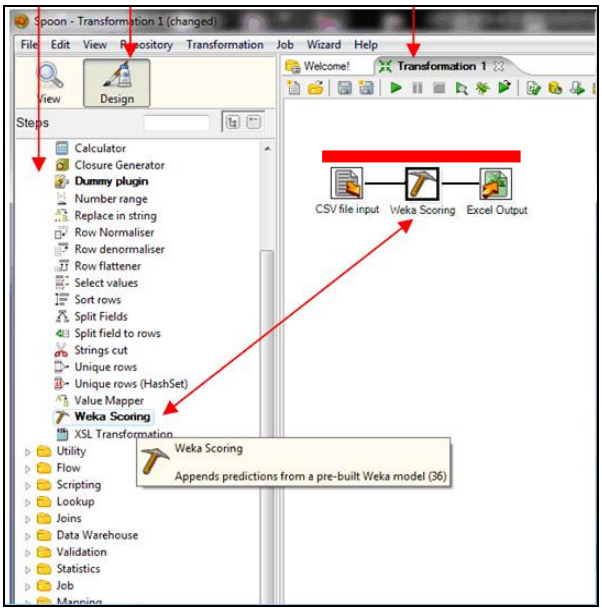


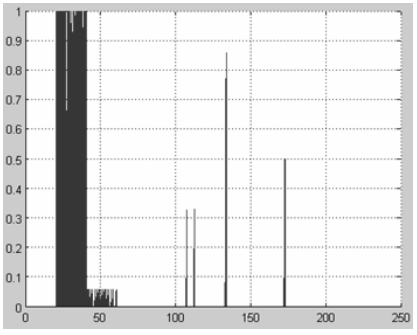
Figure 7. Kettle steps for Weka Scoring.

The matching scores generated by the signature and speech systems for one user were brought together by the weighted parameter α so as to obtain a new match score which is later used to make the final decision:

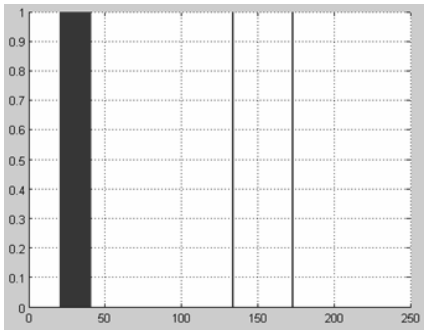
$$score_{fused} = \alpha * speech_{score} + (1-\alpha) * signature_{score} \quad (13)$$

where $\alpha = 0; 0.1; 0.2; 0.3; 0.4; 0.5; 0.6; 0.7; 0.8; 0.9; 1$. There are a total of 11 different possibilities (if $\alpha = 1$ the bimodal system employs only the speech feature and then $\alpha = 0$ only the signature feature is employed).

An example of how the fusion is made is detailed in what follows. Before analyzing the results, we have to specify that in the next figure we intend to represent the probability assigned by the system to every user attempt. For every user, there are a number of 20 attempts; hence the range 1-20 is reserved for user1, the range 21-40 for user2 and so forth. Fig. 8a, 8b shows the probabilities obtained for user2 after the score fusion step ($\alpha = 0.4$). On the x-axis one can see the user2 probabilities attempts distribution (for an ideal system all items should be situated in the 21-40 range; for our real system it can be seen that user2 is sometimes mistaken for other users). The y axis represents the probability of user attempt identification. In order to establish the bimodal system recognition accuracy, the following approximation was made: if probability, p > 0.5 then p=1; else p=0 as shown in Fig. 8b.



a



b

Figure 8. The probabilities obtained for user2 in a bimodal system ($\alpha = 0.4$).

The next figure presents the accuracy of the bimodal system in terms of classification rates for BayesNet and IBk (k=3) classifiers for user 2 for all values of α .

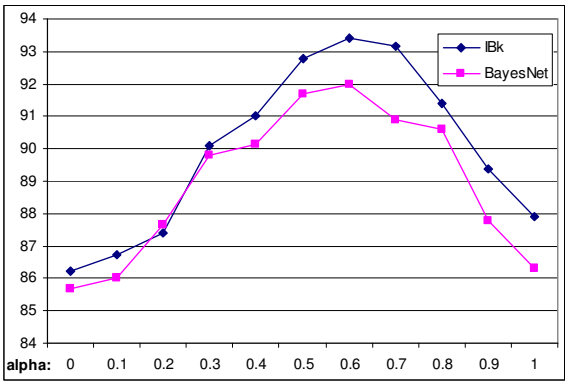


Figure 9. The recognition rates obtained for user2, for the BayesNet and IBk (k=3) classifiers ($\alpha = 0.4$).

An averaged recognition rate provided by the experimental system for all the enrolled users, employing BayesNet and IBk (k=3) classifiers, for all α values may be seen in fig. 10.

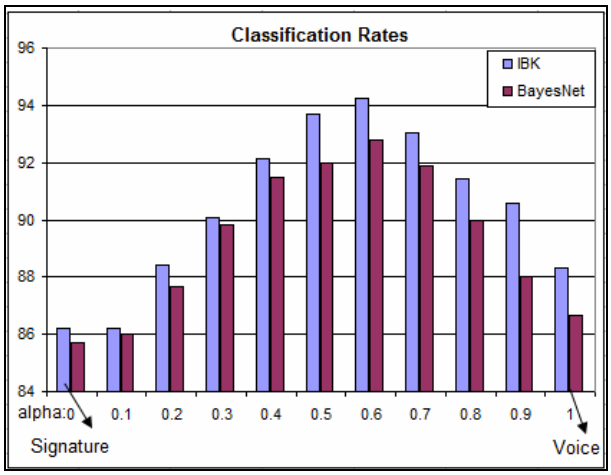


Figure10. Averaged recognition rate provided by the experimental system for all the enrolled users.

By analysing these experimental results, it can be seen that the speech based system ($\alpha = 1$) provides slightly better identification rates for both classifiers than the signature based system ($\alpha = 0$).
As expected the bimodal approach provide better results than unimodal ones. The best suited value for α seems to be 0.6.

It is known that TESPAR DZ methodology provides a low-cost, low-complexity and robust speech recognition solution. The standard 27 symbols from TESPAR DZ alphabet have also provided sufficient accuracy in the case of signatures [9].

As far as we know, this coding procedure was firstly used for on-line signature based signals. In our future work we propose to optimize (to reduce the alphabet dimension) the method for this type of signals. We may justify this attempt by the fact that several TESPAR DZ coefficients of the coded signature are equal with 0, so they are not useful in the recognition task and may be eliminated.

V. CONCLUSIONS AND OUTLOOK

Biometric fusion improves the accuracy of biometric recognition, alleviates problem with noisy data, high failure to enroll and intrusion.

This paper presented an experimental bimodal framework for biometric identification based on dynamic signature and speech, by using two different classifiers. The best accuracy was achieved when the IBk (k=3) classifier was employed. The first purpose was to select several suitable features for the task of user classification. A secondary aim was to analyze the strengths and the limitations of the unimodal systems. The results reveal that the system based on speech gave slightly better performance than the one based on signature, although the vector lenght is lower. It can be observed that even though the system based on signature information had poorer performance than the other one, its features have valuable information and in the case of score fusion the overall accuracy rate is increased. When these two biometrics are fused, the performance and the robustness of the biometric system are improved. Best results for the bimodal system (94.22%) were obtained for the weight $\alpha = 0.6$, the IBk classifier.

Further outlook and attractive challenges for future research lie in several aspects: testing the system on an extended database, extracting more effective features and using the fusion at the match score, rank and decision levels in order to find the best performances foe the bimodal system. Other classifiers (e.g. SVM) are recommended for testing in the classification task.

ACKNOWLEDGMENT

This work has been supported by the grant project CNCSIS PN II 904/2007, "MULTIMODAL BIOMETRICS AUTHENTICATION SYSTEM".

REFERENCES

[1] K. Nandakumar *Integration of multiple cues in biometric systems* Master of science thesis, Michigan State University, 2005

[2] A.K. Jain, A. Ross, S. Prabhkar "An introduction to biometric recognition" *IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image and video-based biometrics,* ***vol.14****, No.1. Jan. 2004*

[3] A.Ross, A.K. Jain "Multimodal Biometrics: an overview" *Proc. of 12th European Signal Processing Conference (EUSIPCO*), (Vienna, Austria), pp. 1221-1224, September 2004.

[4] R. Snelick, U. Uludag, A. Mink, M. Indovina, A.K. Jain "Large Scale Evaluation of Multimodal Biometric Authentication Using Stat of-the-Art Systems", *IEEE Transactions on Pattern Analysis and Machine Intelligence", **vol. 27,*** No. 3, Mar 2005, pp 450-455

[5] A. Ross, A.K. Jain "Information Fusion in Biometrics" *Pattern Recognition Letters, September 2003*

[6] A.K. Jain "Multimodal biometrics systems" 2004, [Online] Available: *http://biometrics.cse.msu.edu* [Accessed: July 1, 2010].

[7] S.Z. Li, A.K. Jain *Encyclopedia of Biometrics* Springer 2009

[8] Jain A., Mink A., Uludag U., Indovina M. "Multimodal Biometric Authentication Methods: A COTS Approach", *Proceedings of Workshop on Multimodal User Authentication*, December, 2003

[9] E.Lupu, S.Emerich, F.Beaufort, "On-Line Signature Recognition Using a Global Features Fusion Approach", *Acta Tehnica Napocensis Electronics and Telecomunications Vol.50,* nr.3/2009, pp. 13-20

[10] A. Ross, A.K. Jain, J.Qian, "Information fusion in biometrics" in *Proceedings AVBPA'01*, Halmstad, Sweden, Jun 2001, pp. 354–359.

[11] A. Ross, K. Nandakumar and A.K. Jain *Handbook of Multibiometrics*, Springer, 2006.

[12]St. Krawczyk *"User authentication using on-line signature and speech"* Master of science thesis, Michigan State University, 2005

[13] A. Jain, K. Nandakumar, A. Ross, *"Score Normalization in Multimodal Biometric Systems",* Pattern Recognition, 2005.

[14] R.A. King, T.C. Phipps "Shannon, TESPAR and Approximation Strategies", *ICSPAT 98,* Toronto, Canada, Sept.1998 Vol. 2, pp. 1204-1212,.

[15] E. Lupu**,** V.V. Moca, P.G. Pop "TESPAR coding study for speaker recognition*" The 30th session of scientific presentations "Modern technologies in the XXI Century"* pp. 214-221, *Bucharest 2003*

[16] http://www.cs.waikato.ac.nz/ml/weka/ [Accessed: August 15, 2010].

[17] http://www.pentaho.com/ [Accessed: August 15, 2010].

[18] http://wiki.pentaho.com/display/datamining/ [Accessed: July 1, 2010].

[19] J.Kittler, M. Hatef, R. P. Duin, J.G. Matas. On Combining Classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3):226–239, March 1998.