



**Repositorio Institucional de la Universidad Autónoma de Madrid**

<https://repositorio.uam.es>

Esta es la **versión de autor** de la comunicación de congreso publicada en:  
This is an **author produced version** of a paper published in:

Biometric ID Management and Multimodal Communication: Joint COST 2101 and 2102 International Conference, BioID\_MultiComm 2009, Madrid, Spain, September 16-18, 2009. Proceedings. Lecture Notes in Computer Science, Volumen 5707. Springer, 2009. 236-243

**DOI:** [http://dx.doi.org/10.1007/978-3-642-04391-8\\_31](http://dx.doi.org/10.1007/978-3-642-04391-8_31)

**Copyright:** © 2009 Springer-Verlag

El acceso a la versión del editor puede requerir la suscripción del recurso  
Access to the published version may require subscription

# Biometric system verification close to “real world” conditions

Aythami Morales<sup>1</sup>, Miguel Ángel Ferrer<sup>1</sup>, Marcos Faundez<sup>2</sup>, Joan Fàbregas<sup>2</sup>, Guillermo Gonzalez<sup>3</sup>, Javier Garrido<sup>3</sup>, Ricardo Ribalda<sup>3</sup>, Javier Ortega<sup>4</sup>, Manuel Freire<sup>4</sup>

<sup>1</sup>GPDS Universidad de Las Palmas de Gran Canaria, <sup>2</sup>Escola Universitària Politècnica de Mataró (Adscrita a la UPC), <sup>3</sup>HCTLab, Universidad Autónoma de Madrid, <sup>4</sup>ATVS, Universidad Autónoma de Madrid

[mferrer@ulpgc.es](mailto:mferrer@ulpgc.es)

**Abstract.** In this paper we present an autonomous biometric device developed in the framework of a national project. This system is able to capture speech, hand-geometry, online signature and face, and can open a door when the user is positively verified. Nevertheless the main purpose is to acquire a database without supervision (normal databases are collected in the presence of a supervisor that tells you what to do in front of the device, which is an unrealistic situation). This system will permit us to explain the main differences between what we call "real conditions" as opposed to "laboratory conditions".

**Keywords:** Biometric, hand-geometry verification, contact-less, online signature verification, face verification, speech verification.

## 1 Introduction



Biometric system developments are usually achieved by means of experimentation with existing biometric databases, such as the ones described in [1]. System performance is usually measured using the identification rate (percentage of users whose identity is correctly assigned) and verification errors: False Acceptance Rate (FAR, percentage of impostors permitted to enter the system), False Rejection Rate (FRR, percentage of genuine users whose access is denied) and combinations of these two basic ratios, such as Equal Error Rate (EER, or adjusting point where FAR=FRR) and Detection Cost Function (DCF) [2].

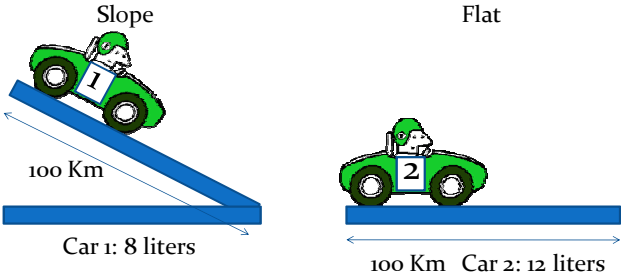
A strong problem in system comparison is that most of the times the experimental conditions of different experiments performed by different teams are not straight forward comparable. In order to illustrate this problem, let us see a simple example in the motoring sector. Imagine two cars with the fuel consumption depicted in table 1. According to this table, looking at the distance (which is equal in both cases) and the

speed (which is also equal) we could conclude that car number 1 is more efficient. Nevertheless, if we look at figure 1, we realize that the experimental conditions are very different and, in fact, nothing can be concluded. This is an unfair comparison.

It is well known that car makers cannot do that. Slope, wind, etc., must be very controlled and it is not up to the car maker. Nevertheless the situation is not the same in biometrics, because there is no “standard” database to measure performance. Each fabricant can use its own database. This can let to unfair comparisons, as we explain next.

**Table 1.** Toy example for car fuel consumption comparison

		
Distance	100 Km	100Km
Speed	100 Km/h	100Km/h
Fuel consumption	8 liters	12 liters

**Fig. 1.** Experimental conditions corresponding to table 1.

We will assume that training and testing of a given biometric system will be done using different training and testing samples, because this is the situation in real operating systems in normal life. Otherwise, this is known as “Testing on the training set”: the test scores are obtained using the training data, which is an optimal and unrealistic situation. This is a trivial problem where the system only needs to memorize the samples, and the generalization capability is not evaluated.

The comparison of different biometric systems is quite straight forward: if a given system shows higher identification rate and lower verification error than its competitor, it will be considered better. Nevertheless, there is a set of facts that must be considered, because they can let to reach a wrong conclusion.

Nevertheless, there is a set of facts that must be considered, because they can let to reach a wrong conclusion. We will describe these situations in the next sections.

#### A. Comparison of results obtained with different databases

When comparing two biometric systems performing over different databases, it must be taken into account that one database can be more trivial than the other one. For instance, it does not have the same difficulty to identify people inside the ORL

database [3] (it contains 40 people) than in the FERET database [4] (around 1000 people). For a study of this situation, see [5]. Thus, as a conclusion, a given system *A* performing better on Database *DB1* than another system *B* performing worse on database *DB2*, is not necessarily better, because the comparison can be unfair.

### *B. Comparison of results obtained with the same database*

When comparing two biometric systems performing over the same database, and following the same protocol (same samples for training both competing systems and the remaining samples for testing), it seems that the comparison is fair. In fact it is, but there is a problem: how can you be sure that these results will hold on when using a different database? Certainly you cannot. For this reason, researchers usually test their systems with different databases acquired by different laboratories. In the automobile example, probably, you will get the fuel consumption in several situations (urban, highway, different speeds, etc.) because one car can be more efficient in a particular scenario but it can be worse in a different one. Of course the car must be the same in all the scenarios. It will be unfair to trim the car design before making the test (one design for urban path, one design for rural path, another one for highway, etc).

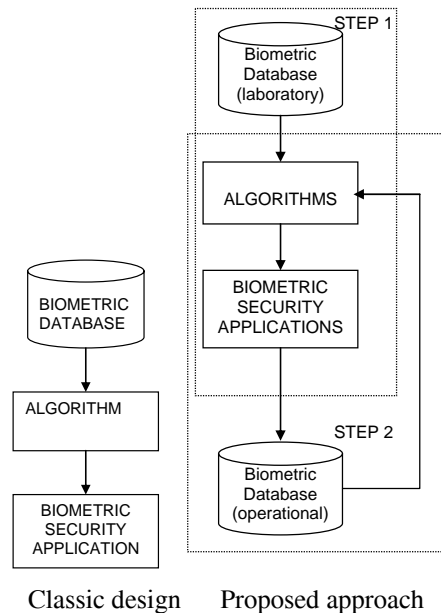
In which comparison is interested the system seller? Probably in the most favorable one for his/her product. In which comparison are we (the buyers) interested? Obviously the best characterization of biometric systems is the one that we achieve with a fully operating system, where users interact with the biometric system in a “normal” and “real” way. For instance, in a door opening system, such as the system described in [6-7].

In this paper we want to emphasize the main differences between databases collected under “real conditions”, as opposed to “laboratory conditions”. This is a milestone to produce applications able to work in civilian applications. Next sections summarize the main differences between our proposed approach and classical approaches.

## **1.1 Classic design (step 1)**

Biometric system design implies the availability of some biometric data to train the classifiers and test the results. Figure 2 on the left summarizes the flow chart of the procedure, which consists on the following steps:

1. A database is acquired in laboratory conditions. There is a human supervisor that tells the user what to do. Alternatively, in some cases, programs exist for creating synthetic databases, such as SFINGE [8] for fingerprints. Another example would be the software Faces 4.0 [10] for synthetic face generation. Nevertheless, synthetic samples have a limited validity to train classifiers when applied to classify real data.
2. After Database acquisition, a subset of the available samples is used for training a classifier, user model, etc. The algorithm is tested and trimmed using some other samples of the database (testing subset).
3. The developed system jumps from the laboratory to real world operation (physical access, web access, etc.).



**Fig. 2.** Classic design (on the left) versus proposed approach (on the right)

This procedure is certainly useful for developing a biometric system, for comparing several different algorithms under the same training and testing conditions, etc., but it suffers a set of drawbacks, such as:

- a) In real world conditions the system will be autonomous.
- b) Laboratory databases have removed those samples with low quality, because if the human supervisor detects a noisy speech recording, blurred face image, etc., will discard the sample and will ask the user for a new one.
- c) Database acquisition with a human supervisor is a time consuming task.
- d) Real systems must manage a heterogeneous number of samples per user. Laboratory system developments will probably ignore this situation and thus, will provide a suboptimal performance due to mismatch between the present conditions during development and normal operation.

## 1.2 Proposed approach (step 2)

A more sophisticated approach involves two main steps (see figure 2 on the right). The operation can be summarized in the next steps:

1. Based on algorithms developed under the “classical approach”, a physical access control system is operated.
2. Simultaneously to system operation, biometric acquired samples are stored in a database.

This procedure provides the following characteristics:

- a) In general, the number of samples per user and the time interval between acquisitions will be different for each user. While this can be seen as a

drawback in fact this is a chance to develop algorithms in conditions similar to “real world” where the user’s accesses are not necessary regular.

- b) While supervised databases contain a limited number of recording sessions, this approach permits to obtain, in an easy way, a long term evolution database.
- c) Biometric samples must be checked and labeled a posteriori, while this task is easier in supervised acquisitions.
- d) While incorrect (noisy, blurred, etc.) samples are discarded in supervised databases, they exhibit a great interest when trying to program an application able to manage the Failure to Acquire rate. In addition, these bad quality samples are obtained in a realistic situation that hardly can be obtained in laboratory conditions.

## 2 Multimodal interface for biometric recognition and database acquisition

In this section we present a multimodal device specially designed to acquire speech, on-line signature, hand-geometry and face. The system is prepared for four biometric traits, the acquisition protocol asks the user to provide his/her identity and two biometric traits (randomly selected). If both biometric traits are positively identified, the user is declared as “genuine”. In case of tilt, a third biometric trait is checked. The core of this system is a hewlett-packard notebook with touch screen (suitable for online signature acquisition). The technological solutions behind each biometric trait are DCT-NN [9] for face recognition, SVM for hand-geometry, HMM for signature and GMM for speaker recognition. Figure 4 shows a physical installation in a wall for door opening system.

Micro: speech   Webcam: face   Webcam: hand



Touch screen: signature

**Fig. 3:** Multimodal interface for biometric database acquisition (hand-geometry, speech, face and on-line signature). Frontal view (top)



**Fig. 4.** Physical installation (at EUPMt) in a wall for door opening system.

### 3 Real world: one step further from laboratory conditions

The goal of research should be to develop applications useful for daily usage. However, nowadays, most of the research is performed in laboratory conditions, which are far from “real world” conditions. While this laboratory conditions are interesting and necessary in the first steps, it is important to jump from laboratory to real world conditions. This implies to find a solution for a large number of problems that never appear inside the laboratory.

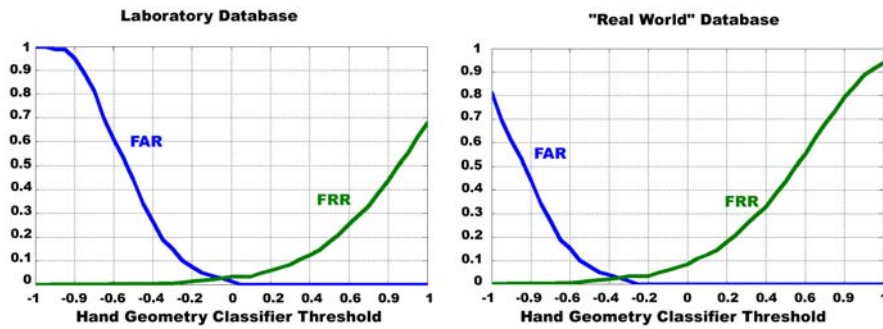
In conclusion, the goal is not a fine trimming that provides a very small error in laboratory conditions. The goal is a system able to generalize (manage new samples not seen in the laboratory). It is important to emphasize that the classical Equal Error Rate (EER) for biometric system adjustment implies that the verification threshold is set up a posteriori (after knowing the whole set of test scores). While this is possible in laboratory conditions, this has no sense in a real world operation system. Thus, system performance measured by means of EER offers a limited utility.

The Table 2 shows the system performance of the multimodal biometric system with two different set up methods. During four months, 102 people (70 genuine and 32 impostors) use the system. More than 900 unsupervised accesses were achieved. In the Laboratory set up method, we process the database acquired in “real world” condition using the set up configuration obtained with previous laboratory conditions experiments. In the “Real world” method we use a posteriori set up configuration to obtain the less EER.

**Table 2.** “Real World” System performance with different set up methods

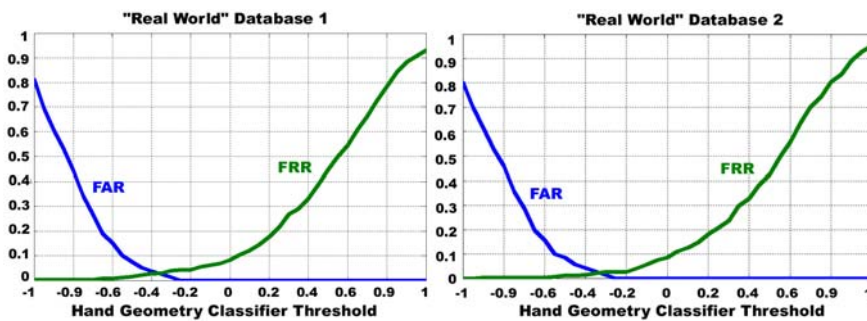
Verification Method	FAR	FRR	EER
Laboratory set up	5.1%	15.3%	10.2%
“Real world” set up	2.5%	2.3%	2.4%

Figure 5 shows an example of difference between laboratory set up and “Real world” set up. In this example we use the Hand Geometry Classifier Threshold versus FAR and FRR curves. On the left we use a 30 people database obtained in laboratory conditions. The best EER is obtained for -0.06 Hand Geometry Classifier Threshold. Working with the “Real World” database used for the Table 2 we observe -0.33 optimum threshold.



**Fig. 5.** Hand Geometry Classifier Threshold versus FRR and FAR, Laboratory Database (on the left) “Real World” database (on the right).

In Figure 6 we divide the “Real World” database in two different databases with the same length. We obtain similar thresholds in both databases. In this case, we can use the database 1 to obtain the set-up of the system.



**Fig. 6.** Hand Geometry Classifier Threshold versus FRR and FAR, “Real World” database 1 (on the left) “Real World” database 2 (on the right).



## 4 Conclusions

In this paper we have presented a multimodal interface for biometric database acquisition. This system makes feasible the acquisition of four different biometric traits: hand-geometry, voice, on-line signature and still face image. The results obtained using the laboratory set up in a “Real World” system shows that we are far from the best set up options. To use set up information obtained from laboratory conditions experiment in “Real World” systems can be not advisable. In this paper we have emphasized the convenience of unsupervised database acquisition.

**Acknowledgments.** This work has been supported by FEDER and MEC, TEC2006-13141-C03/TCM, and COST-2102.

## References

1. M. Faundez-Zanuy, J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez “Multimodal biometric databases: an overview”. IEEE Aerospace and electronic systems magazine. Vol. 21 n° 9, pp. 29-37, August 2006.
2. A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, “The DET curve in assessment of detection performance”, V. 4, pp.1895-1898, European speech Processing Conference Eurospeech 1997
3. F. Samaria & A. Harter "Parameterization of a stochastic model for human face identification". 2nd IEEE Workshop on Applications of Computer Vision December 1994, Sarasota (Florida).
4. “Color FERET. Facial Image Database.”, Image Group, Information Access Division, ITL, National Institute of Standards and Technology. October 2003
5. J. Roure-Alcobé and M. Faundez-Zanuy “Face recognition with small and large size databases”. IEEE 39th International Carnahan Conference on Security Technology ICCST’2005 Las Palmas de Gran Canaria. Pp.153-156. October 2005
6. M. Faundez-Zanuy “Door-opening system using a low-cost fingerprint scanner and a PC” IEEE Aerospace and Electronic Systems Magazine. Vol. 19 n° 8, pp.23-26, August 2004.
7. M. Faundez-Zanuy and J. Fabregas “Testing report of a fingerprint-based door-opening system”. IEEE Aerospace and Electronic Systems Magazine. Vol.20 n° 6, pp 18-20, June 2005.
- 8.<http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111%7C%7C12&>
9. M. Faundez-Zanuy, J. Roure-Alcobé, V. Espinosa-Duró, J. A. Ortega “An efficient face verification method in a transformed domain” Pattern recognition letters. Vol.28/7 May 2007 pp.854-858 Elsevier