Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Biometric Identification System in Higher Education Exams: Test in Laboratory Practices

Rosario GIL, Sergio MARTIN, Gabriel DIAZ,
Elio SANCRISTOBAL, Manuel CASTRO, Juan PEIRE
ETSI Industrial, Electrical and Computer Department, Spanish University for Distance Education (UNED), C/Juan del Rosal 12, Madrid, 28040, Spain
Tel: +34 91 3987795, Fax: + 34 91 3987785,
Email: {rgil, smartin, gdiaz, elio, mcastro, jpeire}@ieec.uned.es

Abstract: This paper outlines a way to identify users in a branched institution with a high number of users mainly devoted to secure and evaluation applications. In broad lines it starts from a distance model of education with traditional exams, the scope will be to archive a full distance education equipped with tools to control and assure the identity of every user.

Keywords: Distance Education, Learning Management Systems, Biometric, Lab Test, legal protection.

1. Introduction

The Spanish University of Distance Education is headquartered in Madrid, which coordinates all activities. Its distance model results in it having specific characteristics.

How subjects are taught depends on the characteristics of the subject, i.e. whether it is technical or arts. For technical subjects the structure of activities is as follows:

- Study a subject for oneself
- Ask questions by phone, email, etc.
- Attend physical laboratories
- Evaluation at university

For arts subjects the same structure is followed except there is no laboratory work. This study focuses on subjects taught in the Industrial, Electrical and Computer Department.

2. Objectives

Our main aim is to streamline the entire administrative process associated with a subject in its annual cycle. The administrative load that a teacher may have, results in time being spent on non-teaching related tasks. Our national university handles nearly 200,000 students a year, although this burden is distributed across all faculties and specialties. Since most of them are arts degrees, this high volume causes many management problems.

There are a number of issues that need to be reviewed:

- Quantity of questions that a teacher can manage
- Management of laboratories and devices for the volume of people
- Teachers available to supervise during exams and correction of all exams

The department has developed these three lines of investigation to try to solve or streamline these three key points in the development of a course. This paper provides focuses on the last point, items related to evaluation.

3. Studying the Environment: Assessment at the Centre

Until very recently each student had a student card received at enrolment and kept for all studies. Along with their ID number, each student had to identify themselves before entering the examination room. Using the student code on the card an exam form was printed with a header on the top describing the characteristics of that exam:

- Personal detail of that student
- Classroom places allocated. All seats were numbered so as to distribute appropriately.
- Restrictions during the exam, namely whether to permit the use of documentation

It thought new applications much faster for access control so they could coexist perfectly with those already implemented. In addition to this new solution raised it intended to go a step further in administrative management. To save on printed documentation, classification of the subjects after an exam and their corresponding distribution to the teacher, could delay the correction of examinations. It raised the examination Web. In this way teachers could have the exams immediately and the degree of dissatisfaction or insistent calls by students asking for their marks would be dramatically diminished.

So it had two objectives:

- Access Control fast and reliable
- Web design exams

The decision taken was to merge these two concepts into one, so that the student entered the classroom and had his own computer. He could identity and carry out his own exam.

4. Design of Identification Applications

At present there are many technologies used for secure transmission of data over the Internet but it is necessary to know that the person sending the data is not an imposter. Username and Password is inadequate for the rigours of identification now required.

The methods of identification are:

- Something the user knows - password
- Something that the user owns - smart cards
- Something that the user is - quantitative data identifying a person, biometric characteristics

The use of biometric techniques eliminates having to memorize or carry a card because it is something that is always available. The preference of the selection of an identification method was to test the strengths and weaknesses of the available biometric security tools.

Like any technical security in an environment, appear at the same time or almost in parallel ways how to break it or find its weaknesses. Therefore impersonation of people is a fact that this will continue in this technique.

For the characteristics that have such data and information that can shed it becomes necessary to the delimitation of what is seen as biometric data, the treatment being given, as well as legal protection that should have.

As is well known, biometrics is the technique used to measure physical and biological features of the human body. It is worth noting that these biological and physical characteristics are different for each person and that by being able to distinguish certain peculiarities, it is always possible to identify the individual concerned [1].

Biometric data [2] is so named because certain elements distinguish it from other categories of data. Therefore biometric data should be universal, unique and permanent.

Physiological and genetic traits as well as the environment influence the development of a human's personality, with social behaviour acquired through conditioning [3].

Given these influences both hereditary as environmental, biometric data can be obtained on the basis not only in the physical and biological constitution of the individual, but also in specific actions and behaviours taken by that person in achieving their place in society.

According to the class sample is collected, physical-biological or social action, the biometric data may be static or dynamic in nature.

Dynamic biometrics refers to how behavioural aspects relate to the person. Examples include handwritten signature, pressing on keys, analysis of gait and gesture analysis. The problem, is that it is unclear how reliable such biometric data is, as the individual can change how they use a keyboard or how they walk. However, it is possible that with high-tech tools that a person's identity can be reliably confirmed through a combination of variables such as body weight, tilt, force and pressure point.

Static biometric data is based on human anatomy. Physiological aspects are permanent and cannot easily be changed by the individual. Examples include static biometric fingerprints, hand geometry, iris or retina analysis, facial recognition and DNA analysis.

In the use of this new identification technology today, greater priority is given to static biometric data as it margin of error is almost zero.

Static fingerprint biometrics is used to identify persons. Fingerprints are formed by some grooves or ridges on the surface of the phalanx of finger. Their unique position makes it is different and distinctive in each person. The main varieties, which generally have ridges papillary, by their morphology, branching, address and interruptions are commonly known as "minutiae" or points characteristic [4]. These characteristics are different points and are in a different percentage for each person and among the most common are the abrupt, fork, convergence, fragment, eyelet, and point, among others.

In the Table 1 describes different characteristics of some biometric technologies.

Table 1: Comparison of different kinds of Biometrics techniques

Feature	**Fingerprint**	**Geometry of the hand**	**Retina**	**Iris**	**Face**	**Signature**	**Voice**
Easy to use	High	High	Low	Medium	Medium	High	High
Errors associated	Dryness, dirt, age	Damage in hand, age	Glasses	Poor quality of light	Light, age, glasses, hair	Change the signature	Noise, cold climate
Accuracy	High	High	Very High	Very High	High	High	High
Acceptability of use	Medium	Medium	Medium	Medium	Medium	Very High	High
Security Level	High	Medium	High	Very High	Medium	Medium	Medium
Stability in Long-term	High	Medium	High	High	Medium	Medium	Medium

Figure 1 [5] shows also the percentage of each technique on the market, data collected by International Biometric Group in 2006. Finally another comparison between each technique with the ideal behaviour is shown in Figure 2.

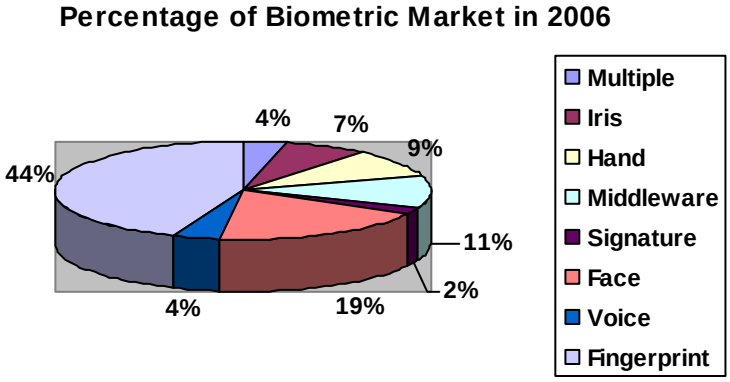

Figure 1: Percentage of Biometric Market in 2006 by International Biometric Group

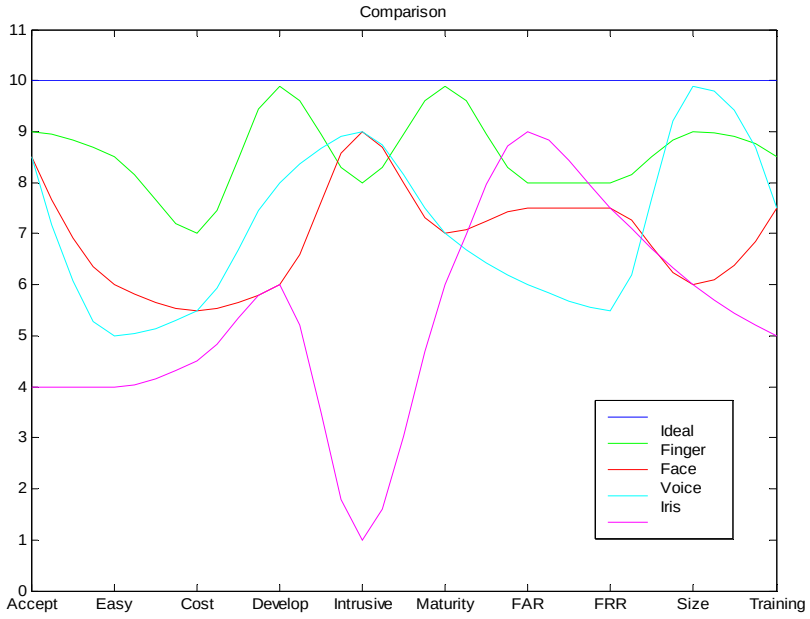

Figure 2: Comparison of Various Biometric Technologies Vs. the Ideal Line One That Would Like to Obtain

Because of its medium-high behaviour to the basic features required in a system, and for its proximity to the line biometric ideal in any environment (Figure 2), fingerprints were selected for integration into our application. The advantages [6] of the fingerprint include:

- Subjects have multiple fingers
- Easy to use, with some training
- Some systems require little space
- Large amounts of existing data to allow background and / or checks watchlist
- You have proven effective in many large scale systems over years of use
- Fingerprints are unique to each finger of each individual and the ridge remains permanent arrangement during one's lifetime

And their handicaps or weaknesses:

- Public Perceptions
- Privacy concerns of criminal implications
- Health or societal concerns with touching a sensor used by countless individuals
- Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust
- An individual's age and occupation sensors may cause some difficulty in capturing a complete and accurate fingerprint image

5. Development in a Controlled Environment

The goal of this test was to create an application that integrates identification and conducting examinations in a learning platform. It was implemented in two phases, the first of which involves registration of personal user details, subjects enrolled and fingerprint. The second phase at exam time, captures a new sample to compare against the database.

Our department (DIEEC Electrical and Computer Engineering Department) of UNED (Spanish University for Distance Education) uses aLF to manage courses. aLF is based on dotLRN and this last one on OpenACS. aLF let us several facilities to develop a course, not just only contents, it can create new forum, surveys and so on. As it is based on OpenACS, it inherited its permissions and associated restrictions. With these permissions we will be able to generate new applications or modify content. However, this does not establish the

true identification of the user behind an e-mail account and password. To improve this situation we have developed a new identification package.

The tool used for identification uses the pattern of the fingerprint to verify a person's identity. As it is difficult to manipulate it and is unique for each student, there will be no problems such as lost or exchange as there may be with password or smart cards.

For the first part, a system was designed that enrols a student in subjects related to our department, storing his personal information along with his fingerprint. The development environment was C++ (MFC, Microsoft Foundation Class) and MySQL database. The capture of the fingerprint was carried out through an optical scanner incorporated into a mouse, requiring no prior training and making fingerprint capture easy (Figure 3).

Figure 3: Enrolment Screen

As a result of this first phase, we obtained three tables in MySQL: personal information and biometric student; subjects available in the department and finally permissions allowed students in the form of subjects enrolled (Figure 4). Thus was controlled identification and the proper access that person to do exam.

For the second phase: verification, dotLRN offers the possibility of doing exams. These can be of different kinds, like multiple choices, large explanation, etc. For the pilot of our application we decided to implement in a laboratory practices where students had to write down the results of different experiments. This choice let us have a small-medium number of students and a medium place to perform experiments but it was big enough to get conclusions of our identification module.

We developed a web service, which receives several input data such as username, fingerprint, etc. from an authentication page that is displayed on the student's browser when he is going to access his exam. This input data is compared with the database tables which contain the data stored in the phase of collection of personal information. In the case of this data matches, an xml file is sent containing the exams elements from the assessment database model and the exam will be displayed on the student's browser. Of course this xml file will be able to be managed by the assessment service, if it is needed. In any other case

the access to exam will be denied. Also we want to mention the importance of using standards as IMS QTI.

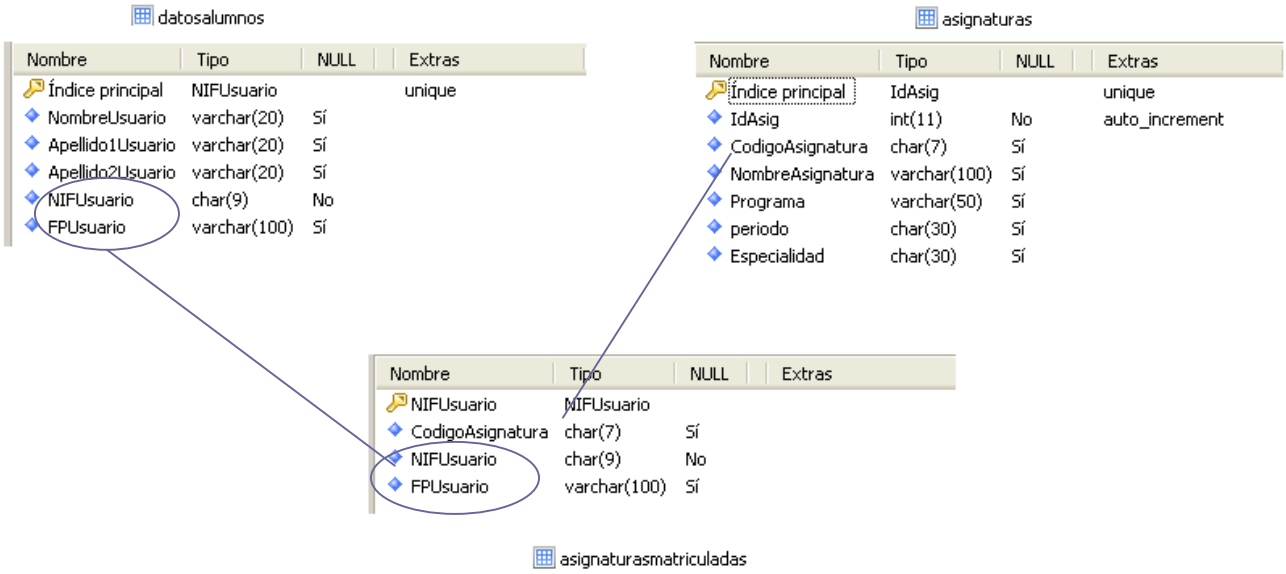

Figure 4: Relationships Between Tables

6. Business Case Description: Real Environment Tests

Since incorporation and changes in the assessment process at a university can carry risks and errors that previously did not exist, we integrated an early version at the departmental level, doing a first test in a laboratory practice, where it was easier for us to monitor the number of people involved, place and the importance of content to be validated was minor.

At the test time in a laboratory, errors were identified and could be solved in real-time. The common error was the false rejection [7] by no training users or by our own module error. In any case, our implementation return rates from other closest samples.

- Dirty finger, wrong orientation
- Weak template stored

The fingerprint usually remains very stable over time, except for those who perform manual work where the fingerprint can become worn or there is a danger of losing a finger. Errors are focused on the quality of the sensor capturing the traces, and cleaning the sensor.

In this first study we also tested with staff without the permission to access the exam, and such people were rejected. For the first test, the level of participation was high and there was a high acceptability. The errors were more related to the use and understanding of the application than the module itself. The application was tried in “Digital Electronic Lab” over five days. As Distance University it was reserved 3 days for students out of Madrid and 2 days for students from Madrid. 80 students were included, around 16 students a day. In figure 5 shows some data extracted from this first experiment as the false rejection rate (FRR); the false acceptance rate (FAR) [8]; the failure to enroll rate (FTER) [9]; and so on.

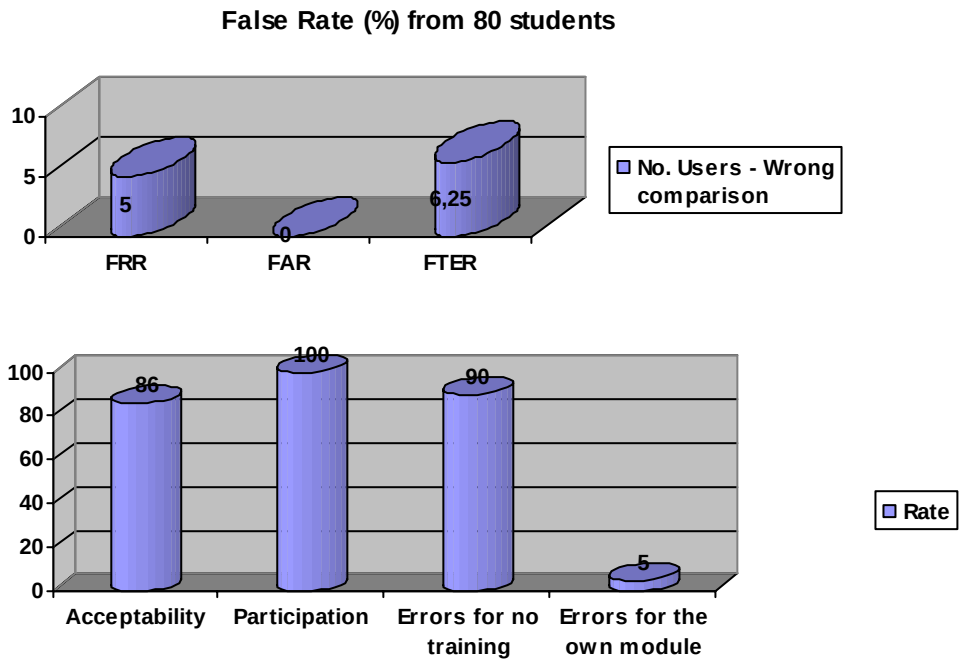

Figure 5: Results from the First Experiments

7. Conclusions and Summary Recommendations

The first real test in a controllable environment achieved an acceptable rating, both by student and by the person assigned. As a non-intrusive technology there were no comments from the students. Likewise, the false rejection occurred in a minority.

The result to integrate a biometric identification in communities such as aLF or other learning systems can give greater freedom to introduce content or create spaces in adequately controlled way.

After this first test in laboratory, it intends to broaden theoretical courses and exams in classrooms equipped with computers for all students. Likewise remote activities where the support of teachers would be no longer necessary, in such case it would have to cope with the false rejection rates, trying to diminish as much as possible.

It is increasingly common to use biometric data as a mechanism for unambiguous identification of individuals. The definition of what is meant by biometric data is important for the nature of these data and the level and content of such information such data should have greater legal protection. This is the case of facial recognition or the use of DNA.

In a general sense the legal protection of biometric data at the community level is covered at first by the Directive 46/95 on the protection of personal data. It says in principle because, the provisions of this Directive 46/95 is limited in its scope if the use of biometric systems geared to issues related to the security of the Member States of the Union.

We must find the right balance [10] between security and freedom for the sake of respecting the dignity and fundamental rights of everyone.

Acknowledgement

The authors would like to acknowledge the Spanish Science and Education Ministry and the Spanish National Plan I+D+I 2004-2007 the support for this paper as the project TSI2005-08225-C07-03 "MOSAICLearning: Mobile and electronic learning, of open source, based on standards, secure, contextual, personalized and collaborative".

References

[1] Aparicio, J.; Estudio Sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Ed. Aranzadi, Navarra, 2000, pp. 54.
[2] 29th Article European Union Working Group referring to computerized biometric data. Working document about biometrics adopted on August, 1st, 2003, pp. 4.
[3] Garcia-Pablos, A; Manual de Criminología, Ed. Espasa-Calpe, Madrid, 1998, pp. 427.
[4] De Diego Diez, L.A.; La Prueba Dactiloscópica, E. Bosch, Barcelona, 2001, pp. 30. Connected to Anton, F.; Iniciación a la Dactiloscopía y otras Técnicas Policiales, 2nd ed., Ed. Tirant Lo Blanch, Valencia, 1998, pp. 33 and more.
[5] Galvis, C.M.; Introducción a la biometria. Bogotá D.C., February 2007. Accessed in June 2008, http://www.monografias.com/.
[6] Biometrics Frequently Asked Questions. National Science & Technology Council Subcommittee on Biometrics. http://www.biometricscatalog.org/NSTCSubcommittee/. Accessed in July 2006.
[7] Wayman, J.L.; A Generalizad Biometric Identification System Model. Proc. IEEE Asilomar Conference on Signals, Systems, and Computers. November 1997
[8] Uludag, U. and Jain, A.K.; Attacks on Biometric Systems: A Case Study in Fingerprints. Proc. SPIE-EI 2004, pp. 622-633, San Jose, CA, January 18-22, 2004.
[9] Wayman, J., Jain, A., Maltoni, D. and Maio, D.; Biometric Systems: Technology, Design and Performance Evaluation. Ed. Springer, 2005.
[10] Tapia, S.G.; La Protección Jurídica de los Datos Biométricos en la Comunidad Europea. Revista de Derecho Informático. Ed. Alfa-Redi.