Fingerprint Identification in LMS and its Empirical Analysis of Engineer Students' Views

Charo Gil
Electrical and Computer Department
UNED – Spanish University for Distance Education
Madrid, Spain
rgil@ieec.uned.es

Gabriel Díaz and Manuel Castro
Electrical and Computer Department
UNED – Spanish University for Distance Education
Madrid, Spain
gdiaz@ieec.uned.es; mcastro@ieec.uned.es

Abstract— **This paper describes a fingerprint identification system (FIS) developed to be integrated in learning management system (LMS). Hence, a middleware is necessary to connect any LMS with our own FIS, which will provide us a scalable, robust, easy integration in any LMS. This project aims to solve the problems of identity authentication of users in remote or virtual environments whose use has spread both in distance education and traditional universities. It seeks its integration into traditional and remote environments, and in the remote environment in exams as well as virtual labs. The project aims to cover all the weaknesses that traditionally have the password or user name. The implementation starts from the own fingerprint identification system developed to its final integration in the LMS.**

Keywords-evaluation; fingerprint identification system; learning management system; middleware; virtual labs)

I. INTRODUCTION

Nowadays, there are many precise solutions for the security in physical access and even in processes online. Into the higher education is becoming a need using new security systems. Student cards with just bar code are not enough to assure the identity. In the same way, new virtual communities manage different courses, contents and tools such as: forum, chat, calendar, etc. but what refers to identification still uses user name and password to let enter to the system. Hence, it can see the necessity of developing new application that complement and intensify the learning management systems.

In higher education there are several systems and utilities that provide robustness for both teachers and students. One example is smart cards that give access to both physical buildings and specific applications of a college. However such systems do not guarantee the identity of the person in the building, in the lab or using resources of a subject. So, we need a solution for the identity of the people that access to physical building or Web applications.

The starting point of the research is to develop a biometric system [1] which has the requirements that are demanded today in higher education. The initial challenge is to deal with a branching structure, which is our university case. As a distance Education University has different centers throughout the country and even beyond our borders. This branching structure is completely transparent to the student. The student attends at his nearest center for tutoring or exams. The documentation or logistics behind a subject are hidden.

Our university has made great changes, automating the entire process, leading to what we call "virtual package". A barcode reader identifies students who access an examination room. After checking if the student is allowed to do an exam, it prints in real time a customized exam for that student, indicating the place in the classroom where the student must sit.

The new assessment model aims to use the resources of educational communities and add a new identification module. As advantages are:

- Use of resources and applications that offer the learning management systems
- Structure applicable to any LMS
- Elimination of the process of sorting and delivery of exams
- Biometrics [2] could resolve the problem of identification

Therefore this new model instead of printing the test, the test will be done by computers in the examination room. The prints just only will indicate on a label where a student must sit. Every post will have a computer along with a USB biometric reader which will identify the student and then will show his test, Fig. 1.

II. NEW EVALUATION APPROACH IN LOCAL ENVIRONMENT

A. Biometric Technology

The new assessment model aims mainly to verify the identity of all students in both local and remote access. The choice of technology should be based on something that characterizes each individual from the rest; therefore biometrics can provide a reliable answer to our problem.

However, a 100% secure system [3] is impossible. While biometrics can minimize the risks involved in an examination, these cannot disappear altogether. Graphically the reliability [4] of a biometrics system could watch in what is called The

Biometric Solution Matrix [5] that is based on five key points: urgency, effectiveness, exclusivity, receptivity and reach. A study of biometrics in our application and our specifications required obtained two matrices: one for local environments and another for the remote, Fig. 2.

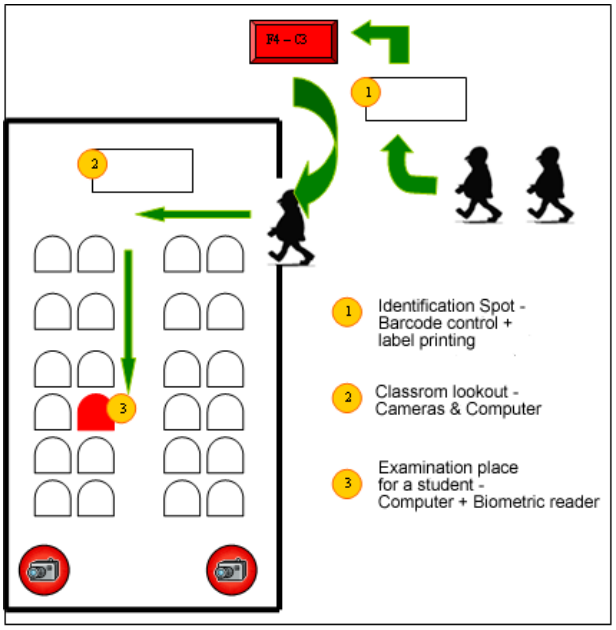

Figure 1. Schematic of the new local examination environment

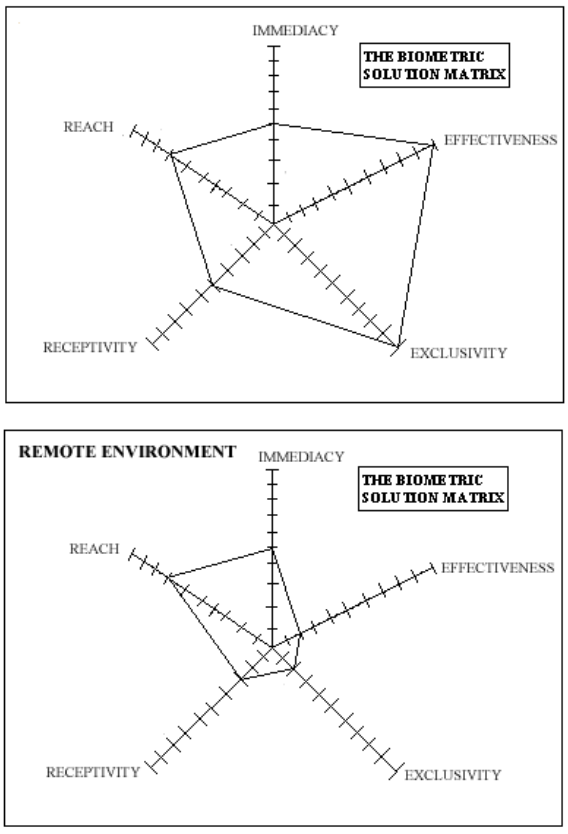

Figure 2. The Biometric Solution Matrix: Local and Remote Environment

As shown both matrices have the same levels of immediacy and reach. The immediacy show us how important are the data and whether development is needed immediately or not. In local enclosure, there is already a manual version to verify identities by ID card and in remote enclosures as they are not yet developed, hence the immediacy should have a moderate value either because there is a workaround or because data are not so important for endanger human life. The reach defines the amount of people where the biometric solution must be implemented. An application of verification for a small group would not make sense in relation use-cost, biometric systems take place in medium-high groups of students. Our university is of this kind, it handles a large volume of students every year.

The effectiveness, exclusivity and receptivity take different values in both environments. The effectiveness show us how well the system solves a problem of authentication, in local enclosure through the use of biometrics can solve perfectly the problem of identification. In remote enclosure, it is true that biometrics will give some support to the implementation, but these uncontrolled environments will have many problems to be covered.

The exclusivity present to biometrics as the only solution for an application with the need to verify identities. In local environment to our current design, the biometrics technology is presented as the best applicable technology and unique to these enclosures. In the remote environment, having a not very high effectiveness and needing other devices to control the enclosure, it is presented as a not exclusive solution needing some other methods for identification to take place at the same time.

The receptivity of students using biometrics has a moderate value in local environment, as it presents a new control that could have malfunction or give an excessive feeling of data collection. In the remote environment, the situation even worse since the implementation of biometrics must be done in a room that usually use students; the perception of intrusive technology becomes more noticeable.

Following this study we see that biometrics is a solution that fits better into the local environment, since it gets a better solution improving the current model. But in the remote environment it is insufficient and requires additional technology. Regardless of this matrix widely used to define solutions, our two environment demand greater emphasis on feasibility and costs relationship.

B. Phases in the implementation

The access to a class in the LMS with open permissions is done by a user name and password, which are data that can be easily acquired by others. Which puts into discussion the resources and content that must be shared with this ambiguous security.

The new service stems from the challenge of ensuring that identification. In other words ensure that the person is really the person access to such rights. This is done for a double identification using the username and password along with a new biometric application that interacts with the LMS and contents such as web exams, virtual labs, and so on.

As shown in the Fig. 3, an LMS provides the following services basically for the identification:

- Login (user/password)
- Access to Management Groups and Profiles, which gives a specific role
- Access to the resources for that role

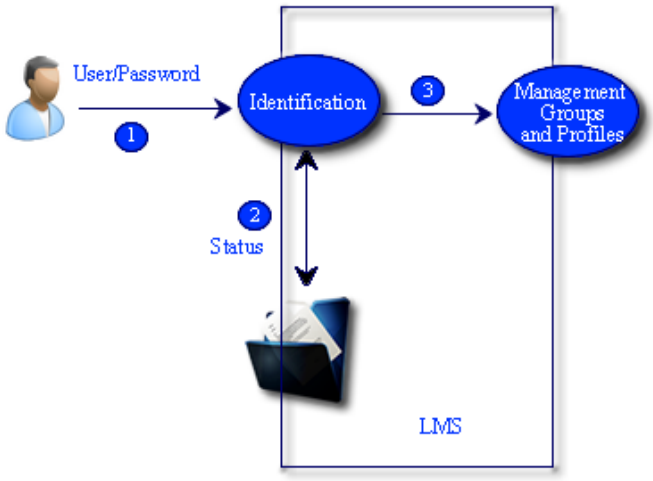

Figure 3. Basic Identification in the LMS

The new model, Fig. 4, involves adding resources that do not exist in the learning management systems. Our project should design a module applicable to any LMS, such as dotLRN, Moodle, Sakai, etc.

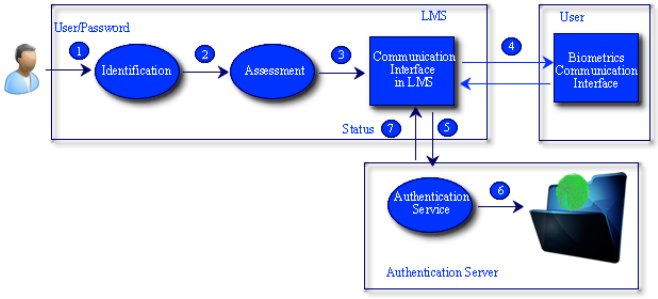

Figure 4. Block diagram of the new security model

The learning management system offers range of services among which is the option to do tests. When a student accesses to the assessment package in LMS it will start the communication between the LMS and the biometric device on the user.

The communications interface in LMS will request the capture of a biometric sample. Then, the biometric interface will send a captured sample. The next step will be to communication between the LMS interface and the authentication server.

The captured sample will be verified in the database of the Authentication server. This database will contain all the samples of students with personal data, so that the biometric matching [6] will be 1:1 from a password.

The methodology of the double identification will be:

1) The user is identified in the LMS by user name and password, which is the basic and general identification of any LMS.

2) Access to the Assessment portlet

3) As a result, it starts the communication between the LMS interface and Biometrics interface.

4) The biometric communication interface will capture the fingerprint's user and return it to the LMS interface.

5) The communication interface of the LMS provides the fingerprint captured to the authentication server.

6) In the authentication server the new sample is compared with the fingerprint database.

7) It returns the approval (status) to continue the evaluation process.

Transparent manner could envisage a repeat steps 4 to 7 during the test. This would ensure that the user does not change during the test. This check can load the system and would only be done if the examination is conducted on-line remotely, that is not performed in specialized classrooms of the UNED.

III. Design of the Fingerprint Identification System (FIS)

The fingerprint identification was the first identification system that was developed, is widely introduced in the market and consequently there is great availability and variety of devices and prices. For the implementation of an automatic fingerprint recognition system in learning managements systems, it was developed a priori in a standalone environment in order to move into LMS after some test.

This system involves an image processing, study and extraction of useful information from the fingerprints. Therefore it requires a previous phases before the extraction of information, these will be a pre-processing phase and an enhancement of the image phase. The total phases generated are as follows [7]:

- Image acquisition: Firstly, it used a database of fingerprints of free distribution accessible from the website of "Fingerprint Verification Competition, FVC". Therefore we used the database FVC2002. In this database for each user was taken 8 different samples, which was enough to test false acceptance and false rejection.
- Enhancement the image. The possible noise introduced in the capture can cause distortions in the information in the fingerprint. It is therefore important to undertake a phase of enhancement [8] of the image.
- Minutiae extraction and post-processing. This is the study of discontinuities in the fingerprint, such discontinuities are called minutiae. In this phase these points are extracted and are verified that they are not spurious points.
- Comparison of data. In the last phase of the identification system compares the new captured sample with the stored samples in a database.

The block diagram of the automatic fingerprint identification system is shown in Fig. 5.

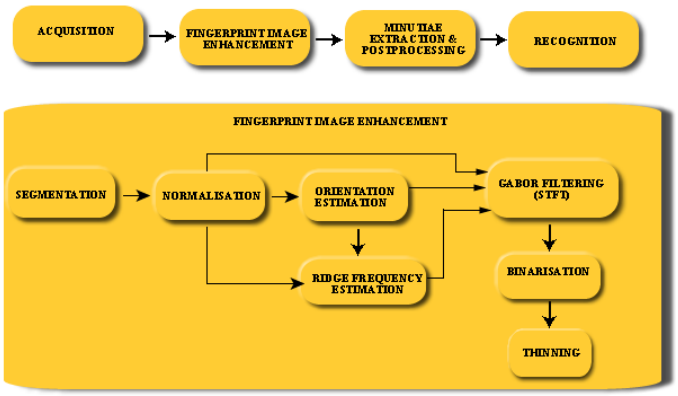

Figure 5. Block diagram of the fingerprint identification system

A. Enhancement of the Image

Some basic concepts that will be used are: ridges, valleys and minutiae. The ridges are simply the present lines in the fingerprint, so the valleys are the groove between adjacent two lines or ridges. The useful information will be the discontinuities in the pattern of ridges in a fingerprint, which are called minutiae.

Within the minutiae are different but the most general classification is to discriminate between ridge endings and bifurcations. The endings, as its name suggests the line simple simply ends and bifurcations will be a line divided into two. The minutiae points are the targets for the next phase, but the elimination of false information will do in this phase.

The enhancement phase includes various blocks, there are: segmentation, normalization, orientation and frequency of the ridges, filtering using Gabor filters, conversion to binary image and thinning. Following, it explains each block to obtain an overview of the achievements in this phase.

1) Segmentation. It selects the image area where there is useful information, also called area of interest. The result is an image with only the foregrpund of the fingerprint. It uses a variance method [9].

2) Standardization. It adjusts the intensity values in grayscale in a certain range, mean and variance desired. This does not change the structure of the image. This phase facilitate the implementation of the successive stages in the identification process

3) Orientation of the ridges. This phase is necessary because of the type of filtering is done in the following stages. Gabor filters or also known as STFT (Short-Time Fourier Transform) are selective in frequency and orientation. For the calculation of the orientation, the image is divided into blocks and each block is calculated gradients using the Sobel operators for the direction x and y. Then we calculate the local orientation of a block centered on pixel (i,j), $\theta(i,j)$.

4) Local frequency ridges. The calculation of frequency follows the same methodology as in previous stages. It divides the image into blocks projecting all pixel values in the direction orthogonal to the orientation of the ridges, which has been calculated in previous step. Such projection has almost sinusoidal shape, which minimum points correspond to the crest of the fingerprint. Thus we can calculate the distance between the first and last peak obtaining the frequency of a block.

5) Gabor filters. Gabor filters (Fig. 6) [10-11] consist of a sinusoidal waveform to a particular frequency and orientation modulated by a Gaussian envelope (1-2). As it is selective in frequency and orientation, works effectively on the ridges without affecting its structure while reducing the noise level.

$$G(x,y;\theta,f)=\exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2}+\frac{y_\theta^2}{\sigma_y^2}\right]\right\}\cos(2\pi f x_\theta) \quad (1)$$

$$x_\theta = x\cos\theta + y\sin\theta,\ \ y_\theta = -x\sin\theta + y\cos\theta, \quad (2)$$

Where: θ is the orientation of the Gabor filters; f is the frequency of the cosine; σ_x^2 and σ_y^2 are the standard deviation of the Gaussian envelope along the x and y axis respectively; x_θ and y_θ define the axes of the filter x and y.

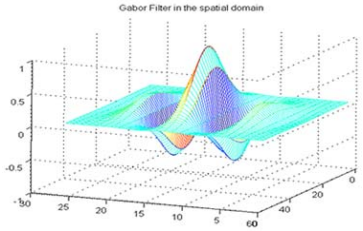

Figure 6. Gabor Filter in the spatial domain

The enhanced image is obtained from the convolution of the Gabor filter and the normalized input image. Applying this filter results an image with noise reduction, smoothing and reconstruction of the ridges.

6) Conversion to binary image. Because of most algorithms for extraction of minutiae operate with binary images, it requires the conversion of binary from grayscale. This process provides a greater contrast between ridges and valleys, where the pixels 1 are ridges.

7) Thinning of the image. In this last phase, which will be the input of the successive blocks in the fingerprint identification process, consists of thinning the width of the lines. Iteratively [12], the width of the lines will be reduced lines until one pixel width lines. As a result we have the skeleton of the input image without affecting the structure of it.

B. Minutiae and post-processing

In order to extract the minutiae point it uses the Crossing Number (*CN*) [13-14] algorithm. Such algorithm consists of

scanning the values of neighboring pixels to a particular pixel P. It takes a window of 3×3 and calculates the sum of the differences of a pixel value minus the value of next pixel counterclockwise. As a result of this algorithm yields a value of *CN* which corresponds to a pixel type (Table I).

TABLE I. CLASSIFICATION OF PIXELS ACCORDING TO THE VALUE OBTAINED CN

CN	Property
0	Isolated point
1	Ending ridge
2	Continues point
3	Bifurcation
4	A crossing point

Only the ending and bifurcation ridge will be interesting to discriminate fingerprint. So the pixels with values of *CN* 1 or 3 will be stored in a database. For each minutia will be important to keep: the coordinates (*x, y*) point, local orientation and its distance to the next distance to the next minutia. Such information will be required in the matching phase.

After using this algorithm it gets some false minutiae points, which are not real information of the user, Fig. 7. This false information can be introduced by noise on the image that has not been eliminated at earlier stages and by the thinning process that could generate some random points. Then a post-processing stage is implemented, where the extracted information is analyzed. In our project was carried out following the algorithm of Tico & Kuosmanen [15], which has a common initialization phase for both the analysis of bifurcations and endings, then two alternatives: for false bifurcations or false endings.

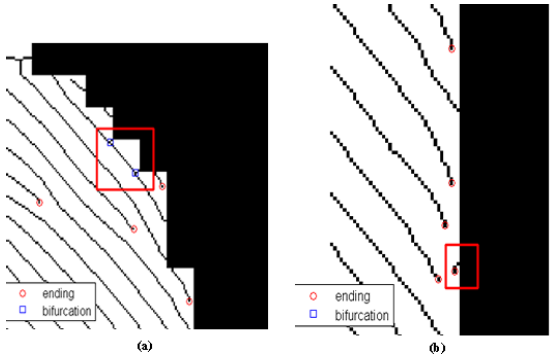

Figure 7. Results of the extraction of minutiae points: (a) Detail of the false bifurcations extracted; (b) Detail of false ending extracted.

C. *Fingerprint matching*

In this last phase of the identification algorithm is comparing an input fingerprint against the database. As we said, in the database there is local information which was extracted in the previous phases. Comparing local information [16] we will observe the relationships between points will not change. So any shift or rotation will be proportional in the both images.

Graphically all the phases of the design of our FIS can be appreciated in Fig. 8.

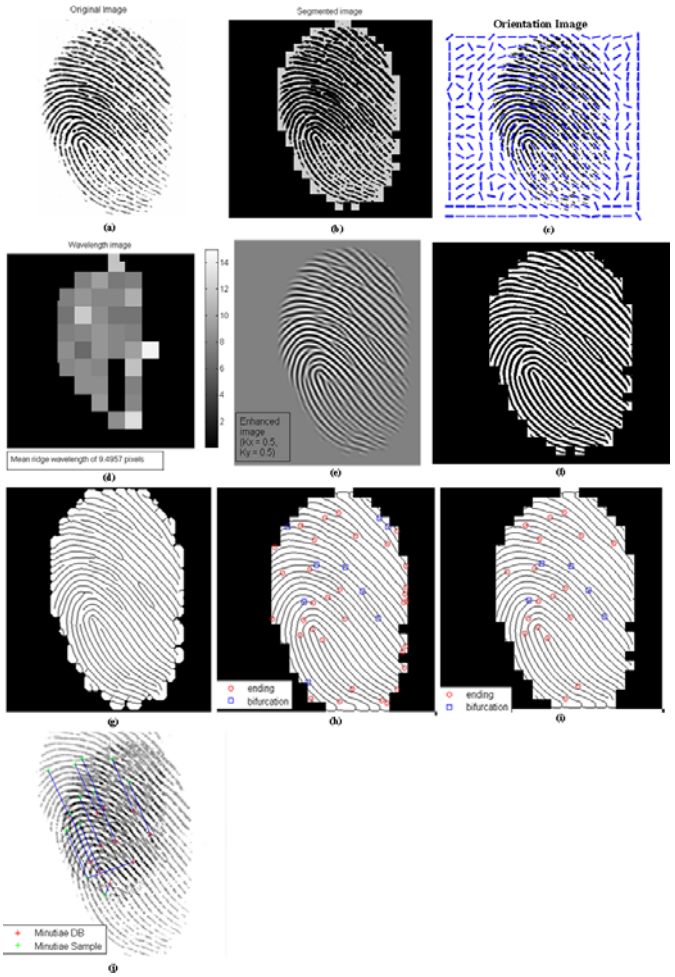

Figure 8. Fingerprint Identification System. Results: (a) Original image; (b) Segmented image; (c) Orientation image; (d) Wavelength image; (e) Enhanced image; (f) Binary image; (g) Thinning image; (h) Minutiae extraction; (i) Post processing image; (i) Matching.

IV. FIS IN ALF

The UNED uses an educational community, called aLF, to develop different contents of their courses, offers a range of services that allow a living relationship between students and teachers. It's a friendly environment. It is also an intuitive environment that requires no prior training course at the user level. That means UNED uses dotLRN as the LMS, which is an application of OpenACS, and in which aLF is based on.

OpenACS, Open Architecture Community System, is a free Toolkit, open source, which provides a fast Web application development with GPL. OpenACS architecture is based on a Web server AOLserver and as database Oracle and PostgreSQL. OpenACS provides a large set of applications that can be used to develop Web sites and is particularly useful for those who are collaborative. Some of the most important applications are dotLRN, dotFolio, Workflow, CMS, Blogging, e-commerce, forums.

It has a great set of APIs and services to rapidly develop new applications. Its data model follows the philosophy of

object-oriented with standard SQL and methods with PL/SQL and support different databases (PostgreSQL and Oracle).

OpenACS is developed by TCL code and is widely used in a number of universities, institutions, companies and freelance developers.

DotLRN is a fully featured LMS-type software, open source and has a sophisticated portal system that integrates tools for managing courses, content and collaboration tools. As we said dotLRN is a system that is based on OpenACS. OpenACS is the Web Framework and dotLRN is its e-learning system and management of communities. It is scalable, robust, extensible, and with the SCORM standard. OpenACS data model implements an object-oriented that developers can modify. Users or system administrators have a Web interface that allows them to create departments and schools within which the courses are distributed.

Figure 9 shows the home screen of a course "*Pruebas del CSI"* in aLF. This is the screen to find any student in a subject.

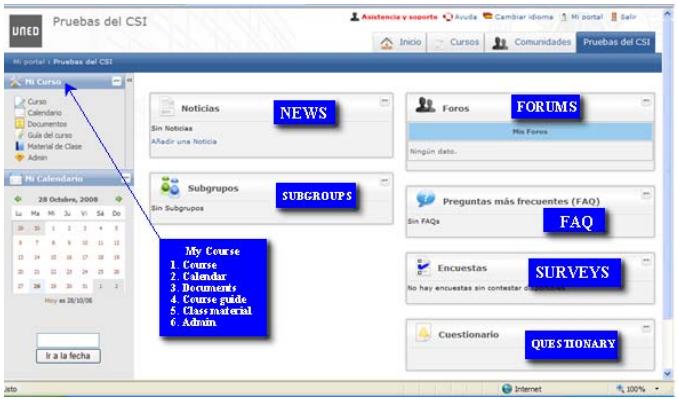

Figure 9. Start Menu for a Course in aLF

As shown on page layout is three columns with the first column narrower. In this column we present the tools, clicking on *"Material de Clase"* (Class material) one can find different exercises to be performed or documentation, subsumed under *"Tareas, Proyectos and Exámenes"* (Tasks, Projects and Exams). In this example there is an exam, called *"Prueba 1"*, see Fig. 10. At this point, the LMS Communication Interface requests the capture of the fingerprint to provide access to screen or Web site of the exam.

The creation of a test by the teacher of that subject is simple; it can create a multiple-choice test or submit a URL to another page.

V. STUDY: REAL CASE IN LABS EXAMS

Evaluation is a necessary process in any training activity. If no assessment, the potential for improvement of the learning processes are not significant. The assessment helps to know the strengths and weaknesses of the training activities developed. It allows us to implement mechanisms of correction.

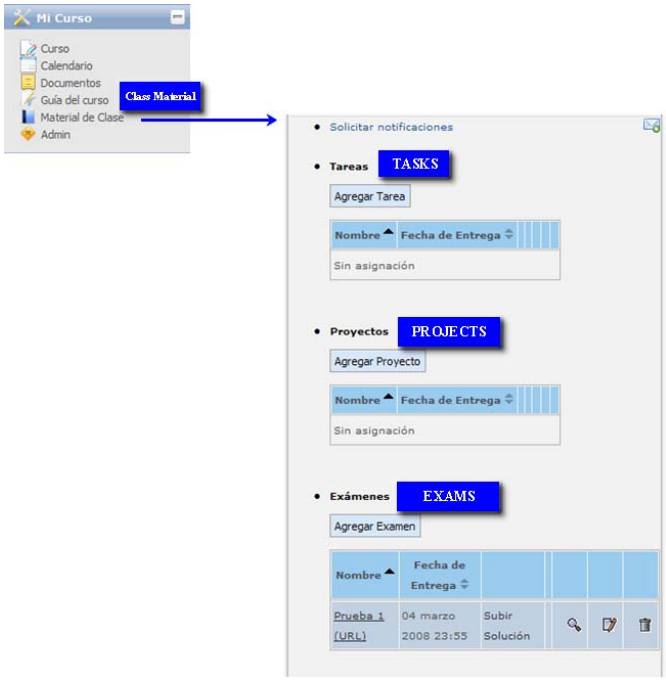

Figure 10. Class Material Options: Tasks, Projects and Exams in ALF

Three moments must be evaluated in this project:

- The design, content and strategies
- The development of the system during tests or access to virtual or remote laboratories
- The results once exams or practices in labs are over

Then, we seek a pedagogical evaluation covering the educational aspects of introducing our FIS into the LMS, including its planning, development and results.

It should be noted that levels of reaction generates the new model. Referring to the assessment that students make the quality of the new model, based on their impressions. This is an assessment of the degree of user satisfaction. Notwithstanding the evaluation results will also be important, i.e. the consequences of the new model at the level of quality for students.

So, on one side is to assess the application itself, technological, and on the other side the educational impact on student learning [17]. Table II can be seen these two lines of assessment based on the three occasions, already cited, where one must evaluate the project.

Once the module Fingerprint Identification System is created, the next step is to test its real utility in higher education. The student profile in these tests will be engineering careers. This is an advantage at the technical level, as the acceptability of introducing new technologies and ease of use is high. Users are familiar to new emerging technologies, and the use of different devices is common in their day to day. This causes the learning of another new application is fast and reduces the associated training failures.

TABLE II. EVALUATION MODEL

DESIGN	
Technological	**Pedagogical**
-Accessibility -Usability -Technical functionality of the module	-Organization (student orientation) -Objectives -Contents -Training strategies -Learning activities -Resources -Evaluation
DEVELOPMENT	
-Information / Introduction -Resolution of technical problems -Synchronous communication -Asynchronous communication	-Tutoring -Task-Management -Evaluation / feedback -Combination local / Online
FINAL	
-Acquisition of new knowledge and skills -Usefulness	

Our university has both profiles of students, sciences and arts. But the FIS module tests are intended for use in the department of Electrical, Electronics and Control engineering for industrial engineering students. At first this module is designed to apply in the subject *"Digital Electronic"* for local environments in real labs. This subject handle around of 80 students and the tests are conducted over 5 days, which means an average of 16 students per day.

After the tests of this new module to see its advantages over a traditional model is important to get values of the false acceptance rate (FAR) and the false rejection rate (FRR) as well as the measured of acceptability of users. That is the perception that they were inspired by this new module.

A questionnaire [18-19] example of parameters to be measured and which depend on the response and opinion of the students are shown in the Table III.

TABLE III. SURVEY ON THE EFFECTIVENESS OF FIS IN THE LMS

Item	1	2	3	4	5
1. Use only passwords and user name					
2. Use of biometrics in college					
3. Fingerprint is a technique intrusive					
4. Suitability of biometrics in college					
5. Improvements in the conduct of examinations Web from the traditional					
6. Integration of Web tests in the LMS					
7. Ease of online examinations					
8. Delayed LMS resource usage by FIS					
9. Improved identification after integrating FIS					
10. The identification can be faked even after FIS					
11. Enrollment difficult for biometrics					

Where: 1. Very Inappropriate, 2. Some Inappropriate, 3. Neutral, 4. Some Suitable, 5. Very appropriate

Similarly it must keep in mind that the results of the questionnaires are based on:

- Sample of 80 students
- Advanced technical knowledge
- Average age: 30 years
- Second career or professional experience for over 3 years
- Degree: Industrial Engineering

VI. CONCLUSION

The integration and testing of fingerprint identification system in the learning management system and its development during online test is the line of research that we want to continue and evaluate the advantages and disadvantages in platforms increasingly extensive and highly diverse. As well as studying the responses of students to new technologies in learning platforms.

This new module is targeted for technical profiles with advanced knowledge in emerging technologies. This provides initially greater acceptability and low skepticism about its value. After the test of the module in real exams must do a deep study about the results, producing a feedback and improving to achieve low failure rates as well as a broad acceptance and a possible extension to other technical areas within the university. As the initial approach is oriented to conduct tests online, it is intended that this resource can be integrated as middleware between protected resources, so it is attractive to think of integration in access to virtual and remote labs.

ACKNOWLEDGMENT

The authors wish to thank the Ministry of Science and Innovation Spanish and the National Plan R+D+I 2004-2007 by the support at the project TSI2005-08225-C07-03 "MOSAICLearning: Mobile and electronic learning, open source, based on standards, secure, contextual, personalized and collaborative" and TIN2008-06083-C01/TSI "s-labs: Integration of open services for remote and distributed virtual laboratories, reusable and safe".

REFERENCES

[1] Reid, P. Biometrics for Network Security. Ed. Prentice Hall- PTR, Indianapolis, 2004.

[2] J. Chirillo & S. Blaul, Implementing Biometric Security, Editorial Wiley, Nueva York, (2003).

[3] J.M. Huidobro & D. Roldán, Seguridad en Redes y Sistemas Informáticos, Editorial Thomson Paraninfo, Madrid, (2005).

[4] S. Nanavati, M. Thieme and R. Nanavati, Biometrics: Identity Verification in a Networked World, Editorial Wiley, Nueva York, (2002).

[5] P. Reid, Biometrics for Network Security, Editorial Prentice hall-PTR, Indianapolis, (2004).

[6] S. Liu y M. Silverman, "A Practical Guide to Biometric Security Technology", Revista IEEE Computer Society, (2001).

[7] Raymond Thai. "Fingerprint Image Enhancement and Minutiae Extraction". School of Computer Science and Software Engineering, The University of Western Australia, 2003

[8] Hong, L., Wan, Y., and Jain, A.K. Fingerprint image enhancement: Algorithm and performance evaluation. IEEE Transactions on Pattern Analusis and Machine Intelligence 20, 8 (1998), 777-789

[9] Mehtre, B. M. Fingerprint image análisis for automatic identification. Machine Vision and Application 6, 2(1993), 124-139

[10] Daugman, J.G. Uncertainty relation for resolution in space, spatial frequency and orientation optimizad by two-dimensional visual cortical

filtres. Journal of the Optical Society of America (A) 2, 7 (July 1985), 1160-1169.

[11] Jain, A. K, and Farrokhnia, F. Unsupervised texturesegmentation using Gabor filtres. Pattern Recognition 24, 12 (1991), 167-186

[12] Guo, Z., and Hall, R. W. Parallel thinning with two-subiteration algorithms. Communications of the ACM 32, 3 (march 1989), 359-373.

[13] Amengual, J.C., Juan, A, A., Prez, J.C., Prat, F., Sez, S., and Vilar, J.M. real-time minutiae extraction in fingerprint images. In Proc. Of the 6th Int. Conf. On Image Processing and its Applications (July 1997), pp.871-875.

[14] S. Kasaei, M.D., and Boashash, B. Fingerprint feature extraction using block-direction on reconstructed images. In IEEE region TEN Conf., digital signal Processing applications, TENCON (December 1997), pp. 303-306.

[15] Tico, M., and Kuosmanen, P. An algorithm for fingerprint image postprocessing. In Proceeding of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers (November 2000), vol. 2, pp. 1735-1739.

[16] Aching Jorge L., Rojas David A. Algoritmos para el reconocimiento de imágenes de huellas dactilares. Facultad de Ingeniería de la Electrónica de la Universidad Nacional Mayor de San Marcos. 2004, Lima, Perú.

[17] Martínez J., Marcelo C, and others. Prácticas de e-learning. Ed. Octaedro Andalucía, 2006.

[18] Galina, S. La protección jurídica de los datos biométricos en la Comunidad Europea. Revista de Derecho Informático, No. 084. Ed. Alfa-Redi. Julio de 2005.

[19] King, C., Guyette Jr., R.W. y Piotrowski, C. Online Exams and Cheating: An Empirical Analysis of Business Students' Views. The Journal of Educators Online, Vol. 6, Nº 1. Enero 2009.