ISSN 1870-4069

JaguarEye: Facial Recognition Web Service for Student Access to ITSCH

Yotziri Paloma Pérez Rios, Marco Julio Franco Mora,
José Iraic Alcántar Alcántar, Mariela Chávez Marcial

Instituto Tecnológico Superior de Ciudad Hidalgo,
Mexico

{ypelekai, darkmarksdoe}@gmail.com,
jiraic@itsch.edu.mx, marielawiroma@hotmail.com

Abstract. Biometric systems play a fundamental role in the processes of recognition of people, on which public security policies are based [5], so within the institutions, security is part of the main point to be addressed for improvement in the quality of services than they offer. The educational institutions of the State of Michoacán, México, nowadays have systems focused on treating this problem through methods that may be ineffective, which presents a clear disadvantage to institutions that handle biometric technologies. The use of biometric systems makes it easier for educational institutions to compete on innovation issues, while creating a better user experience, giving rise to a set of data that can determine the behavior of customers and the institutions itself. JaguarEye emerges as a tool that provides solutions focused on security, when allowing access to students belonging to the ITSCH, making a facial recognition to them, thus avoiding the procedures of generation of student credentials.

Keywords: Machine learning, biometric systems, security, openCV.

1 Introduction

Our society is connected electronically and is increasingly mobile. Representations of our identity as secret codes and cards are not completely reliable to establish the identity of people. During the last years.

Facial recognition has become one of the most studied applications in fields such as biometrics, image processing or pattern recognition.

The main reasons for its use is to promote the creation of systems or applications focused on security and surveillance since they form a very powerful tool for identity management. This is because the biometric features cannot be shared or lost and intrinsically represent the bodily forms of the individual it identifies.

The most important markets for this application are financial, health and government, although in principle any business sector is capable of using it. As for physical access to facilities, the objective is to control the identity of the individuals who access, leave or remain in an area, typically a building or a room. Biometric

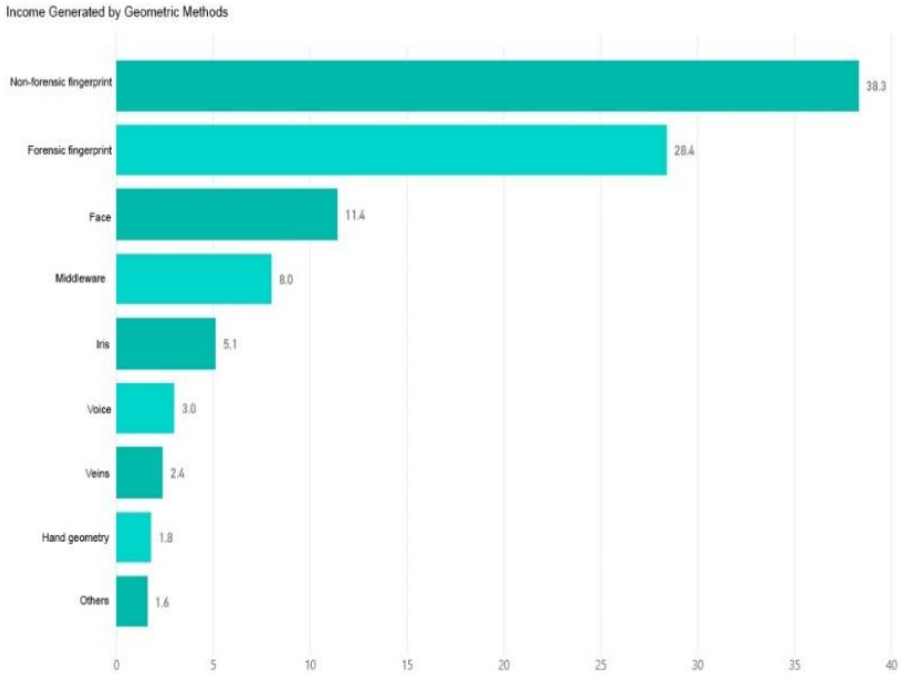

Fig. 1. Percentage of income generated by the different biometric methods.

recognition complements or replaces keys and identification cards, and is often used in certain sensitive rooms or facilities [11], thus indicating the magnitude of the impulse to be used by public and private companies.

2 Analysis and Diagnosis of the Current Situation

The implementation of systems that apply this technology are currently booming with the intention of replacing or optimizing ambiguous tasks related to the identification of people for physical entry to establishments, specifying the above, it should be noted that making use of this type of technology facilitates the manipulation of data in a dynamic way. These types of systems can be used in educational institutions in order to expedite the process of identifying students belonging to it at the time of entry, as a result, the objective of offering more comfortable, safer and faster systems can be achieved.

The increasingly widespread use of biometric technologies has meant that system prices have fallen, components have been miniaturized and more reliable.

And all these facts cause this technology to be used even more (see Figure 1). Figure 1 shows the distribution of biometric features with respect to the income they generate.

The fingerprint is the oldest biometric feature and remains the one that generates the most income. The next biometric feature is the face, which is already a long distance away.

Every day we ask ourselves many questions related to the identity of people. Is this person authorized to enter this building or institution? Can this person be given this information? Is this person wanted for a crime?

In addition to our teams face and solve the same problem: verify if you are who you say you are. The most used tool to get it is the password. However, this is a method that can be stolen or forgotten. Due to the problems that arise with the access codes, it has been essential to develop other systems to verify the identity of the users. The biggest difference between an ordinary password system and a biometric system is that the original sample and the sample to verify never match perfectly. To solve the problem, biometric systems attempt to clean the scanned samples of any element that interferes with the verification process, using only easily recognizable features. However, this "skeleton" must match the original according to mathematical parameters. For a medium security system, a margin of error of a stranger for every 10,000 attempts and the blocking of the legitimate user every 50 cases is assumed as normal. In unstable external environments, light and vibration increase the margin of error and, for this reason, Android's facial recognition, for example, fails in 30 or 40% of cases.

Facial recognition systems can rarely distinguish a real face from a photo. On the other hand, when we use a mechanism with these characteristics, it is really demanding with the lighting conditions and the environment in general, so it will not be necessary to configure additional systems.

In response to providing an agile tool for educational institutions, a web service system called JaguarEye was created, which on this occasion fulfills the specific task of optimizing physical access control for ITSCH students using facial recognition technology, replacing in this way the traditional method of presenting student credentials at the time of entry, in addition to discarding the fact of loss, theft or lost of this and with it the process and properly the payment to generate it again.

3 Research Methodology

3.1 Methodology for Specification of Requirements

Biometric technology is a system that consists of six subsystems: data collection, data transmission, signal processing, data storage, decision making, evaluation and performance [13].

For a certain reason, the development of a web service system integrated to this technology requires an in-depth study of the What? and for what?, it is desired to carry out, with this considered as the principle of innovation the CMMI quality model [2].

To comply with the aforementioned, it was decided to use the agile development model SCRUM [1], since this type of model allows the option of collaborating within reduced development teams (4 members in this case) responsible for development, algorithm, system software logic and engineering, together with a team outside the

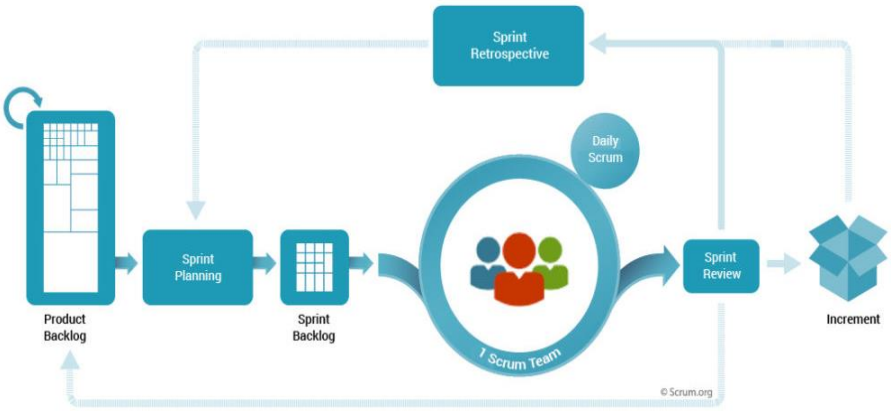

Fig. 2. SCRUM methodology [1].

development area, made up of professionals in the areas of graphic design, user experience and system analysis, with both teams approved in one, the system could be successfully developed without major inconvenience (see Figure 2).

The CMMI Dev v1.3 Model explains the following: "In Agile Environments, the needs and ideas of the client are iteratively educated, elaborated, analyzed and validated. The requirements are documented on forms such as; user history, scenarios, use cases, product backlog and iteration results (code in development in the case of software). What requirements will be addressed in a given iteration are determined by a risk assessment and by the priorities associated with the requirements that are left in the Product Backlog of the product. What details of the requirements (and other artifacts) to be documented are determined by the need for coordination (between team members, teams and subsequent iterations) and the risk of losing what has been learned. When the customer is on the team, there may still be a need to wait for customer and product documentation to allow multiple solutions to be explored.

While the solution arises, the responsibilities of the derived requirements are assigned to the appropriate teams" [3], for this reason, the implementation of agile and simple acquisition techniques is recommended for those development teams that require it.

3.2 Software Requirement Survey Techniques

The Obtaining or Collection of Requirements, is characterized by the identification of Stakeholders, who are all persons interested in the system or in any of its processes for a particular need. The needs of the users with the systems and their expectations are also known.

In the same way, the requirements found from the analyst's perspectives are identified and formalized based on the information collected [9].

In order to provide a quality system focused on security when entering the ITSCH and generate a more user-friendly user experience, it is suggested to use the techniques

listed below, with the objective of achieving results based on creativity and the conceptualization of ideas that generate added value in technological models for modern security systems.

3.2.1 Workshops

It is an effective technique to obtain information quickly between different points of view:

1. It is advisable to have an agenda of activities already predefined of the points to be dealt with in each workshop, in addition to the preselected list of the participants, which will influence in obtaining effective meetings.
2. Make use of a neutral facilitator that performs the function of ensuring that the objectives of the session are met, directing and guiding the participants through proposed dynamics and activities [8].
3. Use visual management (panels, posters, diagrams), and available spaces. Which will help to maintain interest in the session [8].

This technique can be combined in turn with others such as interviews and questionnaires.

3.2.2 Observation

This technique can be combined in turn with others such as interviews and questionnaires:

1. The observation is based on directly identifying the tasks that users usually perform in the organization. The practices of the organization that are carried out with high frequency or that present some complexity in its execution must be selected [10].
2. This technique is based on the observation of physical information of documents in which only specific explanations of the Stakeholders will be requested by the analyst [9].
3. It can be of two types, passive or active.
4. In passive observation, the observer does not ask questions, being limited only to taking notes and not interfering with the normal performance of operations.
5. In active observation, the observer can talk with the user [4].

3.2.3 Brainstorming

It is a group technique to generate original ideas within a relaxed environment:

1. Technique used in various areas and basically based on stimulating the creativity of the team participating in a project.

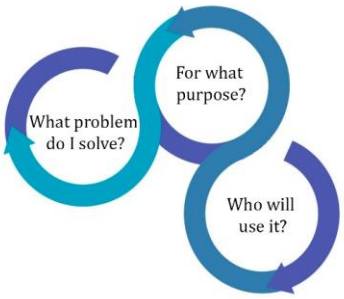

Fig. 3. Purpose delimitation model.

2. Everyone must contribute ideas, which should not be prosecuted until the end of the process, when no one else brings new ideas [7].
3. The technique allows generating different views of the problem, especially at the beginning of the phase of taking requirements, where the views of the problem are still diffuse [6].

3.2.4 Existing Systems

It is a technique used in requirements management. It consists in the search and analysis of systems that have been developed and that have characteristics similar to those of the proposed system:

1. From the documents of requirements of old systems, information can be obtained regarding the domain of the problem, characteristics, turn, nature of the institution, the type of user interfaces can be defined. It is also useful for validating new information that is extracted, information that has probably been omitted [6].

3.3 Proposed Model

In previous lines, the axes that supported the development of the system were mentioned: What? and for what? Which represents a challenge when generating the means for the development and training of requirements, especially in a security system focused on facial recognition that is sought to be implemented within a community where this type of technology is not the determining factor in business models, representing the challenge when generating a new level of innovation, creativity, disruptivity and that they are optimal candidates to generate a new experience scheme in addition to facilitating the observation of the behavior of the agents that are part of the user experience. In the case of the system, the following models were generated that met the expectations of the project see Figure 3.

The fulfillment of the For what?, was given by implementing a model where the needs of the institution are functional and satisfied through the use of the student security system. The points to be resolved by using this method are the validity and verification of the end user, as well as the capacity for technological adoption by the

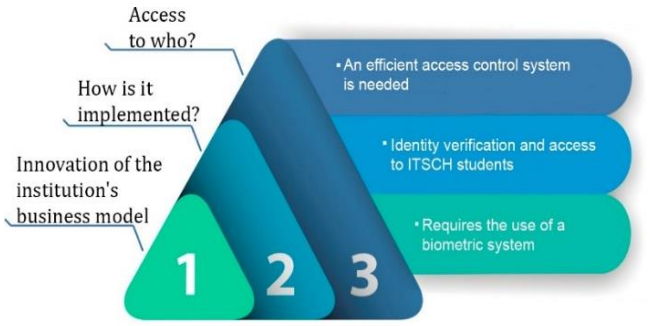

Fig. 4. Model for what? (Verification and Validation).

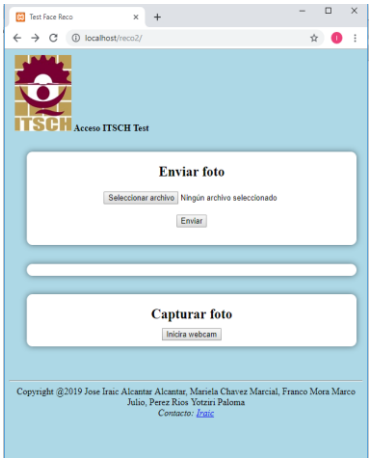

Fig. 5. Web test interface.

institution; where the safety factor plays the most important role in order to assimilate the idea that a profitable, sustainable and scalable facial recognition system to new technologies facilitate the empowerment and quality of service of the institution (see Figure 4).

The key in this product is to ask if the objective set by the users, institution and the development team is satisfactory for all those involved, generating a harmony between the security, technological and commercial aspects.

When talking about the development of the system, technologies were used for the creation of the web service that allowed to speed up the process in order to be able to focus on the conceptualization and engineering of project requirements, therefore technologies such as OpenCV (open source library owned by Intel), PyCharm and Visual Studio Code for the coding of the project, with respect to programming languages Python was used.

MySQL was adopted as a backend system, which is a real-time relational database system, multi-threaded work, API's availability, great level of security, among other services that were not used at the moment.

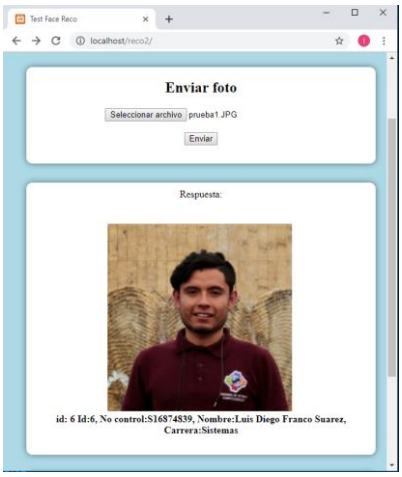

Fig. 6. Recognized face.

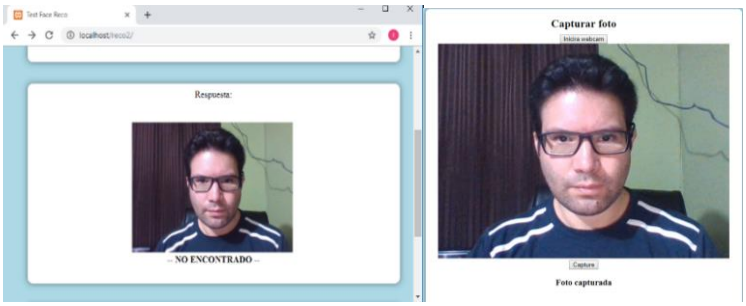

Fig. 7. Unrecognized face.

4 Results

To carry out the tests, a simple web interface was developed, which allows both uploading photographs and capturing from the webcam, which is shown in the following figure (see Figure 5).

The initial tests were carried out with 17 photographs of different students, of which a training was carried out and the characteristics (sample points of the face) were uploaded to a file, subsequently tests were carried out with photos in different positions.

The detection was successfully detected in approximately seventy percent, however, in some situations the faces were not recognized, mainly due to the amount of light on the face and the direction of the shot, which must be front to increase accuracy (see Figure 6-7).

The recognition time is very fast, because the most relevant data of the faces are in a single file, so when applying it to the identification for access the times will be relatively short, however, training will have to be done every time it is required to allow recognition of new people.

Fig. 8. Haar type features.

4.1 Biometric System Performance

By using the Viola-Jones algorithm we focus on performing facial recognition; algorithm that is based on three concepts:

The first of these is the "integral image" [15] that allows the "haar" characteristics used by this detector to be calculated very quickly. This facial detection algorithm will look for specific characteristics that are common in a human face. These "features" are basically black and white rectangles (see Figure 8).

Paul Viola and Michael Jones used the term "Integral Image" within their object detection structure, to refer to a fast and efficient method to calculate the sum of pixel values in any rectangular area of a given image.

The second is a machine learning algorithm, "Adaboost", which selects only the important characteristics of the whole set. The main idea is to combine the output of some weak classifiers in a weighted sum, thus creating a strong final classifier, whose error is exponentially zero.

The third concept is the creation of a “cascade” structure, that is, the combination of complex classifiers, which rejects the background of the input image by spending more calculation time in the areas that may contain the object of interest. The Viola-Jones detector uses the Adaboost technique, but organize the classifiers as a cascade of rejection nodes. Only the candidate who manages to cross the entire waterfall will be classified as a face. In this way the computational cost is significantly reduced [14].

4.2 Algorithm Used for Facial Recognition

The LBPH (Local Binary Patterns Histograms) algorithm was used, where the main idea of the LBPH is not to look at the entire image as a vector, but to describe only local characteristics of an object. The basic idea of local binary patterns is to summarize the local structure in an image by comparing each pixel with its neighbors.

Taking a pixel as the center, if the intensity of the central pixel is greater than or equal to its neighbor, then it will be denoted with 1 and 0 if not. In the end we will end with a binary number for each pixel. So with 8 surrounding pixels we will have 2^8 possible combinations, called local binary patterns or LBP codes (see Figure 9) [16].

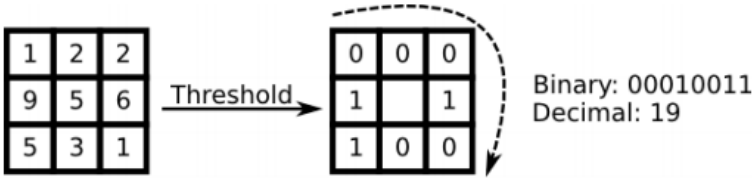

Fig. 9. LBP code.

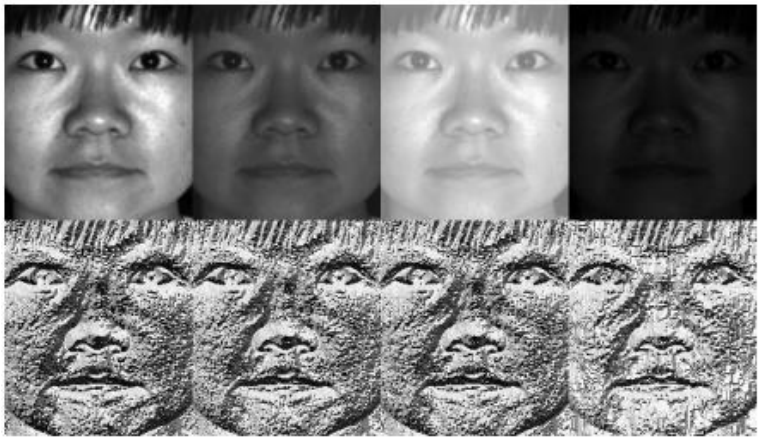

Fig. 10. LBP transformations.

By definition, the LBP operator is robust against monotonic grayscale transformations. An image can be represented in different ways, be it grayscale, filters such as cyan, magenta. In the case of grayscale, each pixel in the image is represented as a number from 0 to 255, the number is saved in one byte, where 0 represents the color black and 255 the color white. Grayscale is used in computational vision to facilitate the treatment of images, when color is not relevant. We can easily verify this by looking at the LBP image of an artificially modified image (see Figure 10).

4.3 Machine Learning Performance

At the beginning there was a series of sample images taken from The Yale Face Database [17] to later use photographs of students belonging to the ITSCH, which had to be the same size to match the dimensional spaces.

That is, for facial recognition to work, it must be divided into two phases, one for training and one for recognition. In the first phase, the training phase, images were collected and their data was extracted in order to apply the algorithms.

To do this every time an image is collected, we will detect the face in it, and a new image containing the face will be saved in a grayscale and resized to a specific size so that they are all the same.

But you don't have to analyze all the images every time you want to make the recognition. When we apply the algorithm to the images, the eigenvalues and the eigenvectors of each one.

They can be saved in an XML / YML file. We will change this file when there are new images. In the second phase, the one corresponding to the recognition phase, a new image will be collected, the face will be detected and it will be grayscale.

Then with the methods that OpenCV provides us, the data extracted from this new image will be compared with those saved in the XML / YML file and you must tell us which image of the training has the greatest coincidence, once this is confirmed, take the id assigned during the training and link to the database to obtain the student's data [14].

5 Discussion

With the development of the system, it allowed, among other things, the following:

1. Identification of students and ITSCH staff.
2. Precave in waste of time for the end user when entering the institution.
3. Bypass procedures in the generation of new student credentials in case of theft or loss.

6 Future Work

With the advantage of mastery of facial recognition and its background, it is suggested to expand the system to new areas within the institution, for example, in order to contemplate a vehicle entry and exit registration by both students and teachers and managers, take the initiative to propose and carry out a security system focused on the aforementioned, preventing any incidents, theft or unauthorized entry of vehicles to the Higher Technological Institute of Ciudad Hidalgo, thus contributing to the community by offering a comfortable system, stable and reliable for the end user.

In the final idea we have the proposal to mount the system on the physical server of the institution that runs on a Linux distribution (Cent Os) offering an expert system for the analysis of user behavior (inputs, outputs, schedules).

Likewise, parallel coding will be analyzed and compared by implementing libraries such as TensorFlow + Keras, CUDA, OpenCL, to look for the best performance when doing facial recognition.

If necessary, to avoid server stress, it’s planned to mount it on hardware architectures such as Intel *Movidius* Neural Compute Stick *(NCS),* Nvidia Jetson, including RaspBerry Pie, always looking for the best possible performance.

References

1. Schwaber, K., Sutherland, J.: The Scrum Guide™ (2017)

2. International Institute of Business Analysis: Babok a guide to the business analysis body of knowledge, IIBA (2015)
3. Equipo del Producto CMMI: CMMI para Desarrollo, Versión 1.3 CMMI DEV, V1.3, Software Engineering Institute (2010)
4. Sarmiento, P., Hernández, D.C.: Metodología para la optimización de los procesos de recolección de información y análisis en la etapa de especificación de requerimientos de software (2017)
5. Etchart, G., Luna, L., Leal, C., Benedetto, M., Alvez, C.: Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales. Facultad de Ciencias de la Administración (2011)
6. Gallardo, J.A., Meneses, C.J.: Un modelo de proceso para educación de requisitos en proyectos de data mining. In: VI Jornadas Iberoamericanas de Ingeniería del Software e Ingeniería del Conocimiento (JIISIC'07) (2007)
7. Gause, D.C., Weinberg, G.M.: Exploring requirements: quality before design. Dorset House (1989)
8. Rodríguez, M.: Inception workshop: Cómo abordar un proyecto ágil (2016)
9. Mera, C.A.: Guía para estructurar con stakeholders en el proceso de ingeniería. Pontificia Universidad Javeriana (2010)
10. Atará, C.A., Liberato, M.C., Sierra, D.A., Vargas, A.J.: Key concepts for the management of technological projects (2016)
11. Ortega, J., Fernández, F.A.: Biometría y seguridad. Grupo de Reconocimiento Biométrico-ATVS (2008)
12. Serratosa, F.: La biometría para la identificación de personas. Universidad Oberta de Catalunya (2012)
13. Luzmilla, M.G., Gonzáles, J.C., Contreras W., Yañez, C.: Tecnologías biométricas aplicadas a la seguridad en las organizaciones. Revista de Ingeniería de Sistemas e Informática, 6(2) (2009)
14. Santamaria, F.J.: Módulo biométrico de imágenes para reconocimiento facial de los usuarios. Universidad de Rioja (2017)
15. Viola, P., Jones, M.: Robust real-time object detection. In: International Workshop on Statistical and Computational Theories of Vision, Modeling Learning, Computing and Sampling (2001)
16. Delbiaggio, N.: A comparison of facial recognition's algorithms. Haaga-Helia University of Applied Sciences (2017)
17. Yale University: Computer Science. https://cvc.cs.yale.edu (2006)