Model–View–Controller based Online Face Recognition System

Youssef Elmir[1], Mohmmed Soumer[2]
[1]Department of Mathematics and Computer Science
University Tahri Mohammed of Bechar
Algeria
elmir.youssef@yahoo.fr
[2]Department of Mathematics and Computer Science
University of Adrar
Algeria

ABSTRACT: *Biometric authentication systems are now widely recognized as the strongest authentication technol-ogies available on the market. To incorporate this mechanism as a web service, an alternative of the classical approach constituted of a classifier and a vector of facial biometric features is proposed to be used. In order to make it possible, the adopted methodology based on Model–View–Controller (MVC) architecture is used. This accredited architectural strategy in the proposed system, allowed us by the end to do online authentication based on the facial recognition with good obtained results of experimentation on ORL database.*

Keywords: Face Recognition, MVC architecture, Servlet, Java Web Server, JavaEE, Web Application

Received: 9 September 2018, Revised 15 December 2018, Accepted 10 January 2019

DOI: 10.6025/ijwa/2019/11/2/49-57

1. Introduction

There is a growing interest in identification and online automatic recognition systems. The access control market opened with the proliferation of systems, but none is effective against fraud because all use an external identifier such as badge / card, key, code ... etc. The common fault of all these authentication systems is that we identify an object (code, card ...) and not the person itself. Faced with the constraint of authentication "objects", the biometry brings simplicity and convenience to web users. Biometric means therefore allow a safe and strong authentication because they are based on the presence of the individual itself. However, biometric systems are more complicated compared to traditional schemes of authentication for traditional uses for access to Internet applications. This is due to the nature of data to be processed (non-uniform, variables), to the number and complexity of the processing modules.

Ephraim T. et al [1] developed optimizations to the Viola-Jones face detection method to make it suitable for use in a web browser running on a standard laptop or a desktop equipped with a webcam. In this setting certain assumptions can be made about the number and location of faces to find, and information from a previous frame can help to localize the search. These optimizations lead to an algorithm which performs real-time face detection using a slow scripting language, even on low-end computers.

Specifically, they have implemented the algorithm in Adobe Flash and their implementation can be deployed via a web browser without any extra installation. They emphasized that the most important application of this optimized algorithm is within the realm of mobile and other low-power devices. By simplifying the problem, they have demonstrated that these barriers can be overcome. Perhaps real-time face detection is also possible in other settings where it was previously thought not to be.

Sahani M. et al [2] designed and developed a home security system, based on human face recognition technology and remotely monitoring technology, to confirm visitor identity and to control door accessibility. A wireless network technique ZigBee based and PCA based image processing technique dedicatedly make the security system alive as per the request. ZigBee module and electromagnetic door lock module operate the door accessibility, has been designed and developed. Face detection and recognition algorithms, as well as a wireless interface are used to detect and identify visitors and send an email and/or an alert message about the current home environment status via GSM network automatically to the home owner's mobile phone or any communication devices. Users can monitor visitors and control the door lock on active Web pages enhanced with JavaScript and HTML.

Cotgreave J. [3] invented a social networking system that uses facial recognition software to match members. A first member may choose to search for other members who look like the first member or may search for members who look like a third party. The invention is implemented on the internet and allows members to upload personal information as well as photos to be used in match searches. The system also includes all or most of the features of existing internet Social networking systems.

As presented above, those systems focus on face detection in images acquired from webcams by web browsers or face recognition for remote home monitoring or for matching social networking members. In this paper biometric system is proposed for website access control using face recognition instead of passwords for user's authentication.

In the next section, some theoretical principles of remote biometric solutions and face recognition are presented. The proposed approach is discussed in section 3 and its design and simulation in section 4. We conclude by giving the achievements and future works.

2.Theoretical Context

Biometric solutions are generally used within the enterprise to control the access to the most sensible applications. There are currently no norms applied by internet browsers of the market that would control access from any PC on the internet.

2.1 Families of Biometric Solutions

Storage and management of biometric data clashed with regulations governing the protection of the individual. Some countries, for example, do not allow the establishment of central databases of biometric data. The solutions of biometrics allow implementing three different types of architecture [4].

	Storage of Biometric Data	**Verification of the Authentication**
Server based solution	On the server	By the server
Workstation solution	On the user station	By the workstation
Cryptographic card based solution	On the cryptographic card	By the card or by the workstation

Table 1. Types of architecture used for biometric solutions

2.1.1 Server based Biometrics

This kind of solutions is based on the following components:

- A central server,

• An enrolment module of biometric features,

• A specific authentication module to manage authentication.

2.1.2 Workstation Solution

These solutions avoid the central storage of biometric signatures and store them on user's computer. If this solution is more acceptable from a legal point of view in many countries, it causes a problem of user mobility.

2.1.3 Cryptographic Card based Solution

This solution also avoids the use of a central server, while it gives the user a free mobility possibility. Indeed, the biometric signatures are stored on a smart card and follow the user on all workstations. If this solution is at the same time more secure and better accepted in many countries, it requires the use of a "Card Management System" for deploying of cards and dispose all the necessary peripherals on different workstations.

2.2 Face Recognition

Facial recognition systems use face to identify or check the identity of a person from a digital image or a video sequence. This can be done by comparing the features of requested face with the features of the stored faces. Like any biometric system, such a face recognition system works in one or two of the following modes:

• Face identification

• Face verification

The performance of any face recognition system is largely dependent on a variety of factors such as lighting, face pose, face expression, person age, hair, wear face and movement [5].

2.2.1 Process of a Facial Recognition System

A facial recognition system has usually four modules as shown in Figure 1. Face detection, normalization, feature extraction and matching. These modules are described below [5].

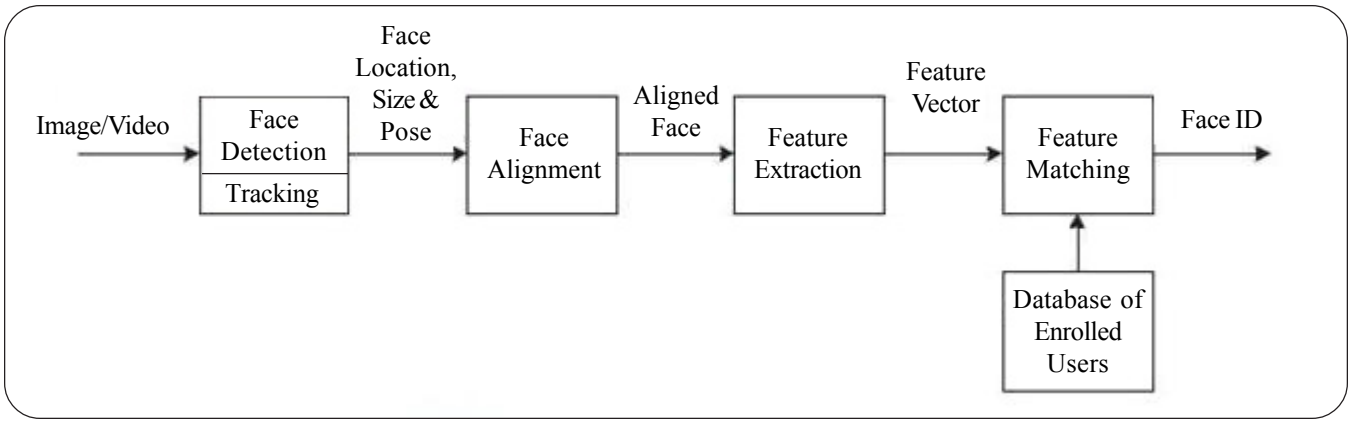

Figure 1. Process of a facial recognition system [5]

• **Face Detection:** Face Detection locates the facial marks (for example, eyes, nose, mouth and facial outline).

• **Facial Normalization:** This phase allows normalizing the face (geometric and photometric) to be ready for recognition by reducing the expressions and any other factors like incidence, change, lighting, which can make some influences on the recognition performance.

• **Extraction of Facial Features:** This phase is performed on the normalized face to extract the useful pertinent information to distinguish faces of people.

• **Comparison:** The extracted features from an input face are compared with one or many faces templates stored in the database. The results of this phase will therefore be "yes" or "no" for verification. For identification, the output is the identity of the input face when there is a correspondence with enough confidence, or unknown when the score of the comparison is below threshold.

3. The Proposed Approach

The proposed approach focuses on the use of facial recognition of an online user to control and secure his access to confidential web data by using a remote biometric platform (internet/local network). The main objective of this system is to capture and identify/verify the identity to ensure the access to a Web site. Thus, this system bases is a web application based on Model-View-Controller (MVC) architecture to send to the web server the captured apprenticeship images of the user face, and his ID instead of password and user ID through recognition module that handles the following tasks:

• Biometric data acquisition in the web session at the client machine. In this step, the system acquires face image of the visitor and send it with his ID to the remote server.

• Biometric data storage at a remote server. Like any website registration phase, in user biometric registration, the remote server extracts face features and stores them as reference to be used for future authentication operations.

• Comparison between extracted features of the requested image and those of reference images (obtained in the registration phase) in the phase of authentication.

• Redirection toward the controlled website in the case of a positive authentication. The remote server sends the decision (result of comparison) to the client.

Each time, this system demand using the same module forms a plug-in for taking facial images:

• Registration of a new user by sending his own information (username, apprenticeship images).

• Authentication of a registered during a web session that leads to a biometric authentication instead of checking a password.

4. Design, Implementation and Results

The general idea is to develop an online biometric authentication system that can authenticate users based on their biometric data, the face for example. The project uses modular technologies of the distributed processing, since the biometric data of users should be stored on a remote server. In addition, such authentication system will be hosted in a web server such manner that directly after the biometric authentication, the connectivity toward the controlled application by this system should also established. In this context, the opted biometric solution will fit with the type of web application. In this regard, it should be emphasized that the architecture that is based on biometric solution with central server is most preferred at this kind of systems [4]. They are based on the following components:

• A central server,

• An acquisition module of biometric data,

• A specific authentication module to manage the authentication.

4.1 System's Modules

To ensure safe access to a website, online system of face recognition is designed to replace the password by the features of the user's face. Two main modules are incorporated into the global system.

4.1.1 Client Side

Another compromise was either to use Java applet or Java Web Start technology which is quite similar to applets, but there are a number of differences. For elaborating a Web page which is able to interact with the webcam of each client for the acquisition step. Java Web Start technology presents the advantage of centralized FaceTrack-er.jnlp [6] acquisition module and makes it

downloadable on client computers. However and since J2EE is used throughout the project, it was preferred not to mix Inter multiple programming languages. So in both phases (registration/authentication), the client module is primordial. Therefore, the use OpenCV and JavaCV is required in order that the module can capture face images. Apprenticeship images are first locally captured, and then they will be sent with their corresponding user ID to the server.

4.1.2 Server Side

In the client side, the client module was checked if it is able to detect and track a face during its movement in front of a webcam. In the server side, the server module tries to recognize the face using Eigen faces as shown in Figure 2.

Figure 2. Eigen faces generated by the server module [7]

4.1.2.1 Eigen Face

To extract the Eigen face, the Build Eigen Faces class generates vectors and proper values from the data of the apprenticeship phase, while Face Recognition class uses the new data of the request emitted by the user, and finds the nearest image in the set of those of the apprenticeship.

4.1.2.2 Reference Data Construction

The set of the apprenticeship images is stored in a folder created automatically for each client, their emplacement (relative URL) will be recorded in MySQL database. The set of these clients folders recorded in a sub-folder called "trainingImages/". There are several results during the execution of the BuildEigenFaces class.java, most crucial being a binary file named eigen.cache. The mask is an object of the FaceBundle class serialized which stores the calculated proper vectors and the proper values, like various information on the apprenticeship images. A new eigenfaces sub-folder, will be generated because it will be useful in the authentication phase later as it contains all the pertinent ones. The sub-folder eigenfaces contains all the proper faces stored in the form of images. The fold-er eigenfaces, and the binary file eigen.cache are stored inside the client folder.

4.1.2.3 Recognition of a New Image

The second important part of the FaceRecognition module, is reading the code of a new image (new data). FaceRecognition decides, which apprenticeship images, is the closest to that in entry. When the user presses on button "send", the selected face is transmitted to the FaceRecognition module where a treatment will be made corresponding to the image and measurement of Euclidian distance to make decision of giving access to the website or not.

4.2 User Authentication

When the user sends a request (user ID, face image) to the server, a servlet invoke to start the process of the authentication (see Figure 3). The input facial image issued by the user is compared with a set of images of the apprenticeship phase. The query image is associated with the closest image of the set of the apprenticeship images that has the smallest calculated Euclidean distance, and after comparing with a studied threshold, the decision determines the degree of similarity for giving a rejection response or acceptance.

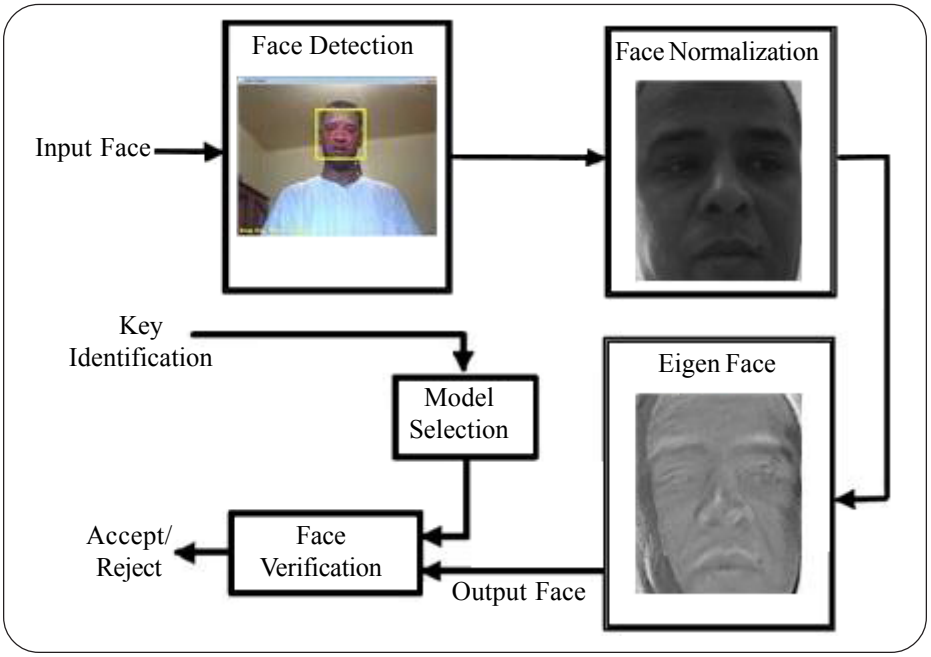

Figure 3. Face authentication process

4.3 Implementation

After developing the design and realize the unitary tests of the main modules, the last component of the project aims to expose the implementation phase of the global web application. This implementation phase is considered to be the final realization of the entire conceptual method of the general system (put the global system online). Acting first the technical study, so the use of software resources to develop this project. In the first place, the choice of the working environment is presented, where the software environment used is specified to carry out this application, and then the architecture is detailed.

The architecture is client-server type, where a computer interacts with others on the Internet. As we have men-tioned above, this system has two parts: one for user management developed with the integration of Java web start technology, and another part for the identity authentication developed using html/servlet/JavaBeans, with the use of libraries such as (opencv, javacv, …etc.).

- *On the application server (Apache Tomcat):* for user management and identity auditor.

- *On the database server MySQL***:** for data storage.

- *The thin client:* a web browser (Internet Explorer, Google Chrome ...etc.).

As mentioned above, MVC architecture is adopted to affirm the maintained insurance, the modularity of the appli-cation and the rapidity of development. MVC is an architecture that organizes the man-machine interface in a way that can develop independent layers. It imposes the separation of data, presentation and treatments, which gives three fundamental parts in the final application: the data model, the controller and the view.

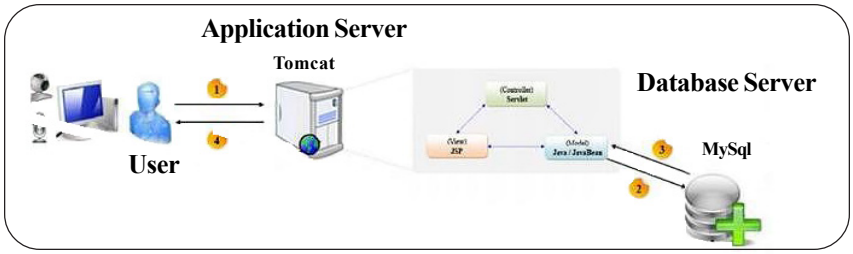

Figure 4. Architecture of the proposed application

1. The web browser sends HTTP requests to the application server.

2. The request is supported by the servlet making office of the controller. The controller processes this re-quest using the model layer (JavaBeans) that sends the request to the database server

3. JavaBeans perform the necessary treatments according to the request and the servlet redirects the re-quest to the HTML page.

4. The HTML page resends the response that is sending again by the application server to the client.

Practically, the mechanism of the proposed system works according to the diagram shown in Figure 5. Consequent-ly, it is necessary that the user sends an HTTP request to the application server. After the validation of this information, the user will be redirected to the website interface.

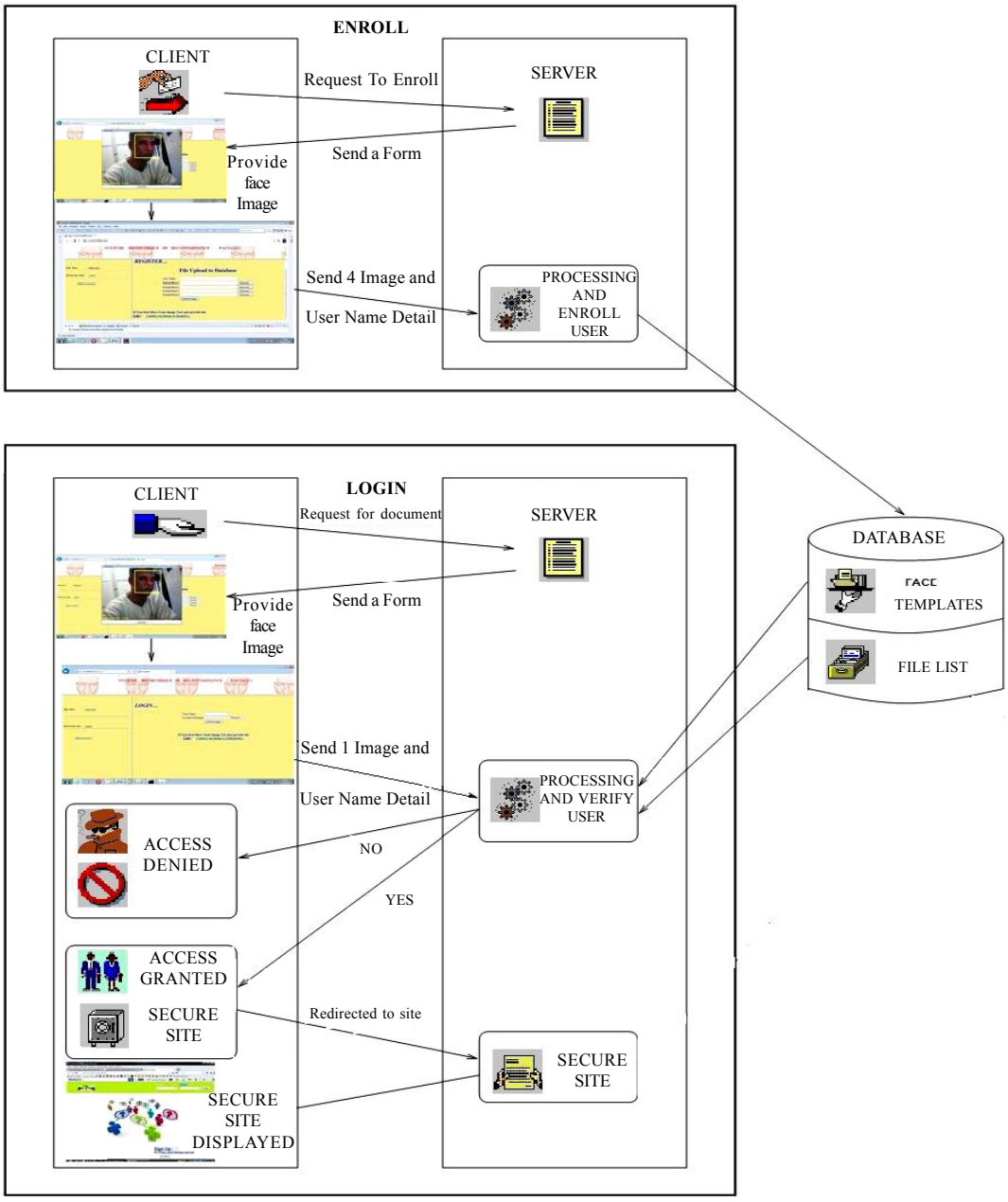

Figure 5. Flow of client-server interaction [7]

4. Results

In order to evaluate the proposed system, a social network website is implemented. The classical login module of this website based on passwords was replaced by the proposed module based on face recognition (Figure 6).

The results of experiments and the achievements of the prototype of online authentication is deployed and tested with samples from ORL database [8] which contains 40 person that each of them provides 10 face images. Four images are used to construct the reference folder of each person, and six other images are used for login tests for each person. Therefore, the system was tested 40x6 = 240 times. The obtained results are very encouraging where the accuracy was 100%.

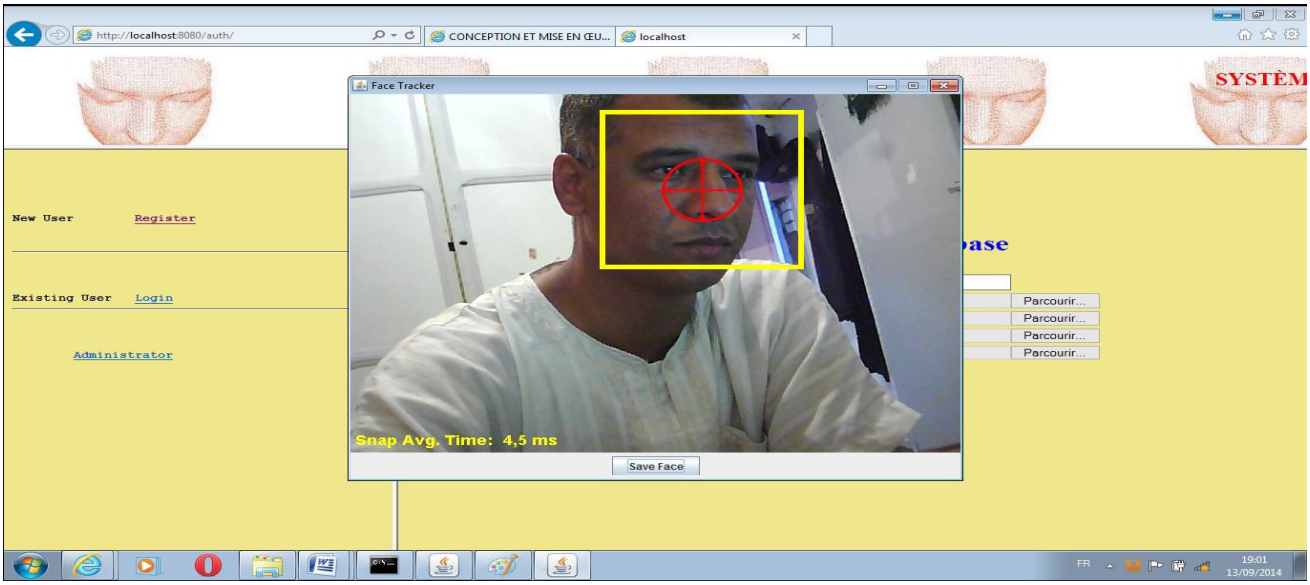

Figure 6. Execution of login attempt [7]

5. Conclusion and Perspectives

A web application is developed throughout this work which its goal is the control of website login of users using biometric authentication instead of classical password. The proposed system allows users to secure their ac-counts using online biometric authentication in centralized manner contrary to the majority of existing works that are limited to the processing of biometric data based on local solution and require considerable configuration for devices used for each workstation. This application has been applied in a social network to check its feasibility. The results are very encouraging after the various tests in a database of 40 persons with 10 apprenticeship images for each person. Practically, the mechanism of this system works according to the client-server approach; all the described features in the introduction, and the functional specifications were developed and validated. Nevertheless, this work can be improved in future by adding more features that can be considered as perspectives of this work, such as:

- Steering system by an administrator,

- Remote intervention by using dynamic threshold dealing with exceptions following new constraints

References

[1] Ephraim, Theo., Tristan, Himmelman., Kaleem, Siddiqi. (2009). Real-time viola-jones face detection in a web browser, in *Canadian Conference on Computer and Robot Vision*.

[2] Sahani, Mrutyunjaya., Chiranjiv, Nanda., Kumar., Sahu Abhijeet., Biswajeet, Pattnaik. (2015). Web-based online embedded

door access control and home security system based on face recognition, *In: I*nternational Conference on Circuits, Power and Computing Technologies, p. 1-6.

[3] Cotgreave, James . (2008). System and Method for Connecting Individuals in a Social Networking Environment Based on Facial Recognition Software, US 2008/0270425 A1, October 30.

[4] MIHI, Abdel Hakim and TERBAGOU, Amina. (2013). Authentification unifiée pour l'accès aux services web de l'université, Université Kasdi Merbah, Ouargla, MSc thesis.

[5] Anil, K., Jain, Z., Li. Stan. (2011). Handbook of face recognition. New York: springer.

[6] Davison, Andrew. (2013). Java Prog. Techniques for Games. NUI Chapter 8. Face Recognition., 2013, Draft #2.

[7] Mohammed, Soumer. (2014). Un Réseau Social Basé sur l'Authentification Biométrique, Université D'Adrar, Adrar, MSc thesis.

[8] Ferdinando, S., Harter, Andy, C. Samaria. (1994). Parameterisation of a stochastic model for human face identification, *In: Workshop on Applications of Computer Vision*, 1994, p. 138-142.