International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 1, Issue 2, October 2014

Biometric Recognition during Web Accessing Through Mobile Phone

Glory Priyadharshini.J[1], Mrs. C. K. Vijayalakshmi[2]

Student, ME- Embedded System Technologies, ACET, Tirupur, India[1]

Assistant professor, Department of EEE, ACET, Tirupur, India[2]

Abstract: Biometric systems can be used for reliable user authentication. In this study, mobile phone is used as a biometric-capture device and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC), thus allowing a multiplatform (personal computer, personal digital assistant, mobile phone, etc.) biometric web access. The main contribution of our proposal is providing higher security and comfort, by means of combining mobile and PCs/Laptops, which doesn't have any biometric-capturing device, by means of using one time access (OTA) password.

Keywords: Biometric recognition, mobile phones, web-based access.

I. INTRODUCTION

A. Biometrics

Biometrics is the science and technology of measuring and analysing biological data. In information technology, biometrics refers to technologies that measure and analyse human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

B. Biometrics in Mobile Phones

Mobile phones are more and more widely used worldwide, with increasing functionality and access to personally and financially sensitive information; therefore, the requirement for additional and/or advanced authentication mechanisms is essential. With the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services (e.g., secure payment [3], e-banking [4], e-commerce (better: m-commerce [5]), etc.).

C. Web-Based Access through Mobile Phones

It is a standard communication protocol. A lot of remote services are accessible via web (e.g., e-banking, e-commerce, e-mail, etc.). Only a web browser and internet connection are needed, which, at this moment, are available in different platforms: Personal Computers (PCs), Laptops, Net Books, Personal Digital Assistants (PDAs) and Mobile phones.

Mobile phones usually connect to the internet via two different methods: Over a mobile phone operator's network, such as EDGE or HDSPA, or over local Wi-Fi (wireless Internet), like the wireless internet connection you may have at home.

D. Biometrics on Web Access

It was not long ago that system security issues look a back seat to system performance. Today, there is an increased need for network security as our society is becoming more tightly interconnected. There is a huge amount of sensitive commercial, personal, military and governmental information on the Internet that needs to be secured so that only authorized people can gain access to the name service the security based on correlating names and network addresses will fail. The risk of password eavesdropping can be reduced by the use of encryption technologies.

II. PROPOSED SYSTEM

The proposal of this study is to present mobile phone application architecture to capture and send the biometric to the web server based on the use of an embedded web browser. This capture can only be stored in the server or used with remote (i.e., web service) or local (i.e., mobile data or application) restricted access.

The main characteristics of our proposal are:

1) *Simplicity* It took less than 2 months to develop the application (including the web-server modifications),

starting from a PC-based development. Mobile applications based on speech and online signature developed for Android in just weeks.

2) *Low cost:* The same architecture for biometric web applications can be used both in PC and mobile scenarios.

3) *Multiplatform*: There are almost no differences for accessing the server services via PC or via mobile.

4) *Multibiometrics:* The biometric recognition can be monomodal, i.e., using only one biometric or multimodal, i.e., merging several biometrics.

5) *Secure:* Dealing with biometrics, which is a mandatory requirement, is security. However, this issue is overcome in web technology at the communication layer, with the secure version of the hypertext transfer protocol (see http) protocol (e.g., HTTPS).

A. Architecture

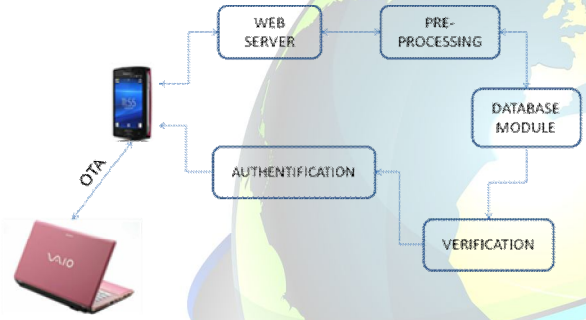

Fig. 1 Proposed Block Diagram

Fig. 2 shows the overall structure of the proposed architecture to implement a biometric system in mobile-acquisition conditions.

The main modules of the proposed architecture are the following:

1) *Client Tier:* On the client side, the biometric acquisition software is used. Since, as noted above, there is no standard software solutions for web browsers to capture biometric data, this part should be distributed "ad hoc" for each type of platform. For this reason, our architecture proposes to leave only the data capturing module on the client side, with the rest of the modules at the server side. This means that the applications developed need no special memory or processing requirements, since the main computer load falls on the execution of a web navigator and standard mobile devices (e.g., touch screen, microphone, camera, etc.) are used to capture the biometrics; then, our proposal can be run in, practically, any current mid-range to high-range mobile devices.

The application at this side controls and communicates with the following three main general components:

a. Embedded browser in charge of the navigation and accessing to the web service,

b. Biometric capturer in charge of calling and managing the mobile capture devices,

c. Biometric uploader in charge of sending the biometric data to the server and managing this uploading.

2) *Server Tier:* The server side contains the main parts of the functionality of the proposed architecture. The components at this tier are the following.

a) *Web Server:* This is responsible to collect the data sent by the data-capturing software on the client side, and passing it to the security module.

b) *Security Module:* Its mission is to ensure that incoming data are consistent and come from reliable sources. Some examples of tasks carried out in this module are checking access lists, usernames, algorithms for checking the validity of HTTP sessions, countermeasure detection of attacks by automated systems, etc.

c) *Server-Side Capture Engine:* This is in charge of collecting the data received by the web server and storing for sub- sequent processing by other components of the system

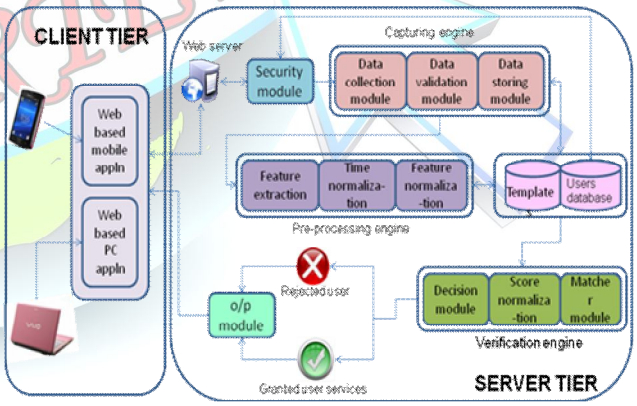

Fig. 2 General Architecture of the System

d) *Pre-processing Engine:* This collects the raw biometric data and prepares them for processing by the verification engine.

e) *Database System:* This contains information from the users of the system (i.e., user's database subsystem) and their biometric templates (i.e., user's templates subsystem).

f) Verification Engine: This module decides whether the access to the system is granted or denied to the user.

g) *Output Module:* This transmits the output back to the client.

B. Face Recognition

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

1) Eigen Faces: Eigen faces are a set of eigenvectors used in the computer vision problem of human face recognition. It is considered the first successful example of facial recognition technology. These eigenvectors are derived from the covariance matrix of the probability distribution of the high-dimensional vector space of possible faces of human beings.

2) Practical implementation: To create a set of eigenfaces, one must: Prepare a training set of face images. The pictures constituting the training set should have been taken under the same lighting conditions, and must be normalized to have the eyes and mouths aligned across all images. They must also be all resample to a common pixel resolution (r × c). Each image is treated as one vector, simply by concatenating the rows of pixels in the original image, resulting in a single row with r × c elements. For this implementation, it is assumed that all images of the training set are stored in a single matrix T, where each row of the matrix is an image. Subtract the mean. The average image a has to be calculated and then subtracted from each original image in T. Calculate the eigenvectors and Eigen values of the covariance matrix S. Each eigenvector has the same dimensionality (number of components) as the original images, and thus can itself be seen as an image. The eigenvectors of this covariance matrix are therefore called Eigen faces. They are the directions in which the images differ from the mean image. Usually this will be a computationally expensive step (if at all possible), but the practical applicability of Eigen faces stems from the possibility to compute the eigenvectors of S efficiently, without ever computing S explicitly, as detailed below.

Choose the principal components. The D x D covariance matrix will result in D eigenvectors, each representing a direction in the r × c-dimensional image space. The eigenvectors (Eigen faces) with largest associated Eigen value are kept.

These eigenfaces can now be used to represent both existing and new faces: we can project a new (mean-subtracted) image on the eigenfaces and thereby record how that new face differs from the mean face. The eigenvalues associated with each eigenfaces represent how much the images in the training set vary from the mean image in that direction. We lose information by projecting the image on a subset of the eigenvectors, but we minimize this loss by keeping those eigenfaces with the largest eigenvalues. For instance, if we are working with a 100 x 100 image, then we will obtain 10,000 eigenvectors. In practical applications, most faces can typically be identified using a projection on between 100 and 150 eigenfaces, so that most of the 10,000 eigenvectors can be discarded.

3) Use in facial recognition: Facial recognition was the source of motivation behind the creation of eigenfaces. For this use, eigenfaces have advantages over other techniques available, such as the system's speed and efficiency. Using eigenfaces is very fast, and able to functionally operate on lots of faces in very little time. Unfortunately, this type of facial recognition does have a drawback to consider: trouble recognizing faces when they are viewed with different levels of light or angles. For the system to work well, the faces need to be seen from a frontal view under similar lighting. Face recognition using eigenfaces has been shown to be quite accurate. The figure 3.3 shows the workflow graph for this algorithm.

III. Results And Discussion

The main functions of the algorithm and functional description are as given below in table I. First, the recognition system is run in the GUI (as shown in the Fig. 3).Then input image is selected by pressing the select image icon in the GUI add the image in the database (Fig. 4) a given a unique number called ID number (positive).

We can add as many faces and correspondingly can assign the ID number for each image (As shown in Fig. 5) so that each image is represented by the Unique ID number. We can perform face recognition (As shown in Fig. 6) as we select a particular face which was previously added in the data base algorithm search for the nearby face as per work flow with reference to class and distance from the face space.

TABLE I
FUNCTION DESCRIPTION

S.No	Function	Description
1.	Select Image	Read the input image
2.	Add selected image to database	The input image was added to database and will be used for training
3.	Database Information	Show information's about the images present in database. Image must have the same size. If this is not this is not true you have to resize them
4.	Face recognition	Face matching. The selected input image is processed
5.	Delete database	Remove database from the current directory
6.	Visualization tool	Show information's
7.	Exit	Quit the procedure

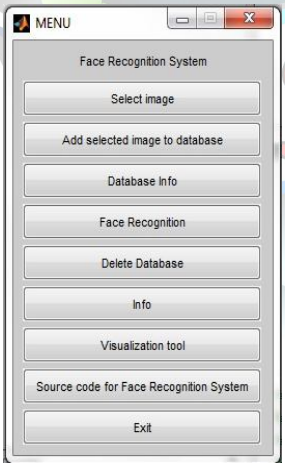

Fig. 3 Running GUI

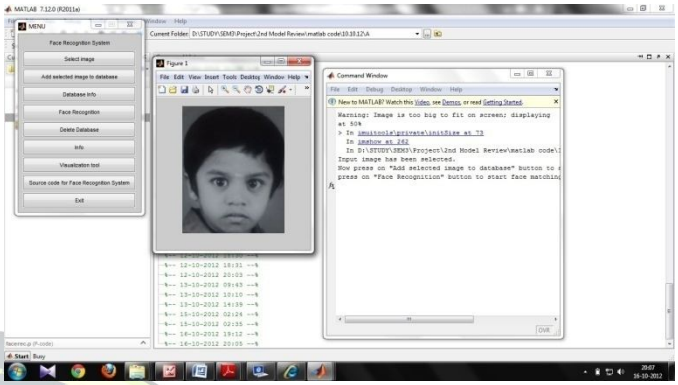

Fig. 4 Selecting input image

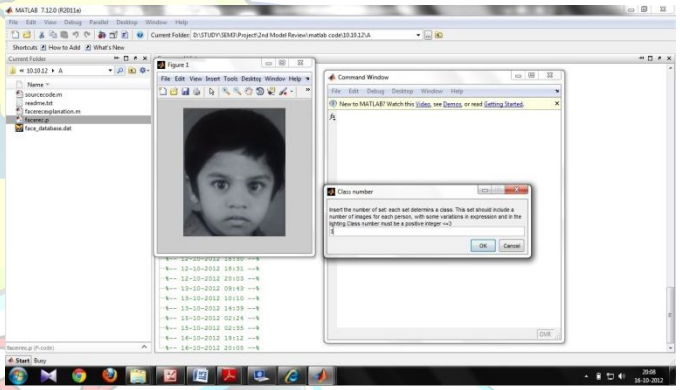

Fig. 5 Assigning ID number

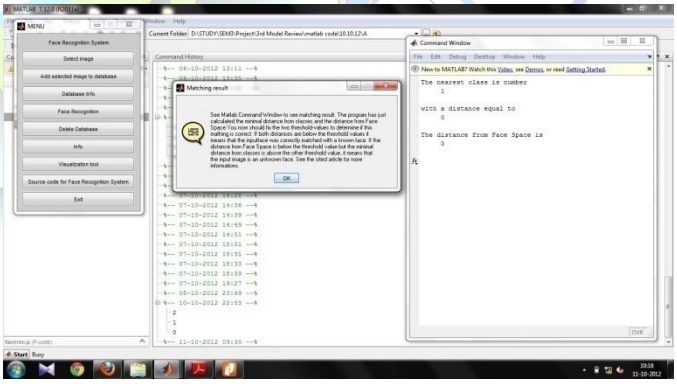

Fig. 6 Performing Face recognition

A. Links and Bookmarks

http://www.secure-phone.info

http://www.mobioproject.org/

http://www.freeband.nl/project.cfm?id=530

http://www.cogentsystems.com/

IV. Conclusion

In this paper, the problem of using biometric user authentication during a standard web session when a mobile phone is used has been successfully approached. We have focused on the technological problem of capturing the biometric with the mobile phone, sending it to the web server, and, after user authentication, allowing or rejecting the user's continuation with the web session in the same way this had been performed using password authentication. We have proved that the standard solutions by face recognition as a biometric system for web access to a restricted services in the mobile phone.

Acknowledgement

I thank my friends everyone who gave me support in all the ways for designing my project with various ideas and also I thank my guide Mrs.C.K.Vijayalakshmi who has been with me in all my steps in this project.

References

[1]. N. L. Clarke and A. Mekala, "The application of signature recognition to transparent handwriting verification for mobile devices," Inf. Manage. Comput. Secur., vol. 15, no. 3, pp. 214–225, 2007.

[2]. R. M. Godbole and A. R. Pais, "Secure and efficient protocol for mobile payments," in Proc. 10th Int. Conf. Electron. Commerce, 2008, pp. 1–10.

[3]. D. S. Jeong, H.-A. Park, K. R. Park, and J. Kim, "Iris recognition in mobile phone based on adaptive gabor filter," Lect. Notes Comput. Sci., vol. 3832, pp. 457–463, 2005.

[4]. Q. Zhang, J. N. Moita, K. Mayes, and K. Markantonakis, "The secure and multiple payment system based on the mobile phone platform," presented at Workshop Inf. Secur. Appl., Jeju Island, Korea, 2004.

[5]. N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones—A survey of attitudes and practices," Comput. Secur., vol.24, no. 7, pp. 519–527, 2005.

[6]. K. R. Park, H.-A. Park, B. J. Kang, E. C. Lee, and D. S. Jeong, "A study on iris localization and recognition on mobile phones," EURASIP J. Adv. Signal Process., vol. 2008, pp. 1–11, 2008.

[7]. M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation," in Proc. 19th Int. Conf. Pattern Recogn., Dec. 2008, pp. 1–5.

[8]. D. J. Hurley, B. Arbab-Zabar, and M. S. Nixon, "The ear as a biometric," in Handbook on Biometrics, A. K. Jain, A. A. Ross, and P. Flynn, Eds. New York: Springer-Verlag, 2008, pp. 131–150.

[9]. S. yi Han, H.-A. Park, D. H. Cho, K. R. Park, and S. Lee, "Face recognition based on near-infrared light using mobile phone," in Proc. ICANNGA, Part II (Lect. Notes Comput. Sci. vol. 4432), 2007, pp. 440–448.

[10]. "Enhancing security for the mobile workforce," Biometric Technol. Today, vol. 16, no. 1, pp. 8–8, 2008.

[11]. N. Clarke, S. Karatzouni, and S. Furnell, "Flexible and transparent user authentication for mobile devices," in Proc. IFIP AICT SEC (Lect. Notes Comput., Sci. vol. 297), 2009, pp. 1–12.

[12]. T. Hazen, E. Weinstein, and A. Park, "Towards robust person recognition on handheld devices using face and speaker identification technologies," in Proc. Int. Conf. Multimodal Interfaces, 2003, pp. 289–292.

[13]. C. C. Broun, W. M. Campbell, D. Pearce, and H. Kelleher, "Distributed speaker recognition using the ETSI distributed speech recognition stan- dard," in Proc. Int. Conf. Artif. Intell., vol. 1, 2001, pp. 244–248.