ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

E-Biometric Authentication for Smart Devices

S.Kannan[1], Dr. C. Nalini[*2]

Assistant Professor, Department of Computer Science & Engineering, Jerusalem College of Engineering, Chennai, Tamil Nadu, India [1]

Associate Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[2]

[*]Corresponding Author

ABSTRACT: The use of biometric person recognition for secure access to restricted data services using a mobile phone with Internet connection have been dealt. Biometrics can be divided into two categories based upon the underlying characteristic they are using: physiological and behavioral. There are three general categories of user authentication: 1) something you know, e.g., passwords and personal-identification numbers (PINs), 2) something you have (e.g., tokens), and 3) something you are (e.g., biometrics). Today, 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 , e-banking, e-commerce (better: m-commerce), etc.). We have, then, a very popular device, with increasing functionality and access to personally and financially sensitive information; therefore, the requirement for additional and/or advanced authentication mechanisms is essential. The problem of capturing and sending the biometrics to the web server via PC is very easy to solve using embedded applications in the web pages. The proposal of this project is to present novel mobile-phone application architecture to capture and send the biometric to the web server based on the use of an embedded web browser. The current mobile technology is not ready for embedded applications in mobile web browsers; however, it is prepared for our solution, which is very easy and effective, as will be seen.

I. INTRODUCTION

Biometric person recognition is the use of unique human characteristic to recognize the user. The mainstay of this project is to present an application that allows a mobile phone to be used as a biometric-capture device. The main contribution of our proposal is that this capture, and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC).

The use of biometric person recognition for secure access to restricted data /services using a mobile phone with Internet connection have been dealt. Biometrics can be divided into two categories based upon the underlying characteristic they are using: physiological and behavioural. There are three general categories of user authentication,

- Something you know, e.g., passwords and personal-identification numbers (PINs)
- Something you have (e.g., tokens)
- Something you are (e.g., biometrics)

Today, 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 , e-banking, e-commerce (better: m-commerce), etc.). We have, then, a very popular device, with increasing functionality and access to personally and financially sensitive information; therefore, the requirement for additional and/or advanced authentication mechanisms is essential.

The problem of capturing and sending the biometrics to the web server via PC is very easy to solve using embedded applications in the web pages. The proposal of this project is to present novel mobile-phone application architecture to capture and send the biometric to the web server based on the use of an embedded web browser[1]. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

current mobile technology is not ready for embedded applications in mobile web browsers; however, it is prepared for our solution, which is very easy and effective, as will be seen.

II. LITERATURE SURVEY

There are various systems that are existing for biometrics in mobile phones. Some of them are discussed below.

In work [2], the application that allows a mobile phone to be used as a biometric-capture device is shown. The main contribution of our proposal is that this capture, 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 (PC, personal digital assistant (PDA), mobile phone, etc.) biometric web access. The review, which is from both an academic and commercial point of view, of the biometry and mobile device state of the art shows that in other related works, the biometric capture and recognition is either performed locally in the mobile or remotely but using special communication protocols and/or connection ports with the server[3]. The second main contribution of this study is an in-depth analysis of the present mobile web-browser limitations; thus, it is concluded that, in general, it is impossible to use the same technologies that can be used to capture biometrics in PC platforms (i.e., Applet Java, ActiveX Control, JavaScript, or Flash); therefore, new solutions, as shown here, are needed.

In work [4], as the security of personal information is becoming more important in mobile phones, we apply iris recognition technology to mobile device. Different from conventional iris recognition system used for access control, user puts the mobile phone by hands in this case. So, optical and motion blurring happens, frequently. In addition, most users have tendencies to use the mobile phone in outdoor and sunlight (which includes much amount of IR(Infra-Red) light) may have much effect on the input iris image in spite of the visible light cut filter attached in front of iris camera lens. To overcome such problems, we propose a new method of extracting the accurate iris code based on AGF (Adaptive Gabor Filter)[5]. The kernel size, frequency and amplitude of Gabor filter are determined by the amount of blurring and sunlight in input image, adaptively. Experimental results show that the EER by our propose method is 0.14 %.

In work [6], the ever-increasing functionality and services accessible via mobile telephones, there is a strong argument that the level of user authentication implemented on the devices should be extended beyond the Personal Identification Number (PIN) that has traditionally been used. This paper presents the results of a survey of 297 mobile subscribers, which attempted to assess their use of mobile devices, their use of current authentication methods, and their attitudes towards future security options.

The findings revealed that the majority of the respondents make significant use of their devices, with clear demands for protection against unauthorized use[7]. However, the use of current PIN-based authentication is problematic, with a third of the respondents indicating that they do not use it at all, and other problems being reported amongst those that do. In view of this, the respondents' opinions in relation to future security options are interesting, with 83% being willing to accept some form of biometric authentication on their device. The discussion considers these findings, and the potential applicability of the preferred techniques to mobile devices.

In work [8], The proliferation of handheld devices such as PDAs and smart phones represents a new scenario for automatic signature verification. Traditionally, research on signature verification has been carried out employing signatures acquired using digitizing tablets or Tablet-PCs. In this paper we study the effects of the mobile acquisition conditions and we analyze the considerations that must be taken in the new handheld scenario.

A signature verification system adapted to handheld devices via feature selection is proposed and a systematic comparison with a traditional pen tablet-based system is performed[9]. The system is combined with another based on hidden Markov models using score fusion. Results confirm increased signature variability in the case of handheld devices.

In work [10], recently many companies have attempted to adopt biometric technology in their mobile phones. In this paper, we propose a new NIR (Near-Infra-Red) lighting face recognition method for mobile phones by using mega-pixel camera image. This paper presents four advantages and contributions over previous research. First, we propose a new eye detection method for face localization for mobile phones based on corneal specular reflections. To detect these

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

SRs (Specular Reflections) (even for users with glasses), we propose successive On/Off activation of the dual NIR illuminators of mobile phone. Second, because the face image is captured by the NIR illuminator, the nose area can be highly saturated, which can degrade face recognition accuracy.

To overcome this problem, we use a simple logarithmic image enhancement method, which is suitable for mobile phones with low processing power. Third, considering the low processing speed of mobile phones, we adopt integer-based PCA (Principal Component Analysis) method for face recognition excluding floating-point operation[11]. Fourth, by comparing the recognition performance using the integer-based PCA to those using LDA (Linear Discriminate Analysis) and ICA (Independent Component Analysis) methods, we could know that the integer-based PCA showed better performance apt for mobile phone with NIR image.

III. EXISTING SYSTEM

The mainstay of this project is to present an application that allows a mobile phone to be used as a biometric-capture device. The main contribution of our proposal is that this capture, and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC).

In existing system, the great amount of particular applications that can be found, the cost of changing or modifying biometric platforms, the lack of normalization in capture-device technology, and communication protocols, as well as social-acceptance drawbacks are all barriers to the popularization of biometric recognition.

The dominant approach on current control access is via password or PIN, but its weaknesses are the most clearly documented: if it is easy to remember, it is usually easy to guess and hack into, but if it is difficult to attack, it is usually difficult to remember; hence, a lot of people write them down and never change them[12]. The problem with tokens is that they authenticate their presence, but not the carrier; they can be easily forgotten, lost, or stolen, and, as it happens with the credit cards, can be fraudulently duplicated. As a result, biometry appears as a good solution, which is generally used, in addition to the previous authentication methods, to increase security levels.

The problem with tokens is that they authenticate their presence, but not the carrier; they can be easily forgotten, lost, or stolen, and, as it happens with the credit cards, can be fraudulently duplicated.

As a result, biometry appears as a good solution, which is generally used, in addition to the previous authentication methods, to increase security levels.

IV. PROPOSED SYSTEM

The main contribution of our proposal is that this capture, and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC). Today, 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.

The main characteristics of our proposal with regard to the state of the art are Simplicity, Low Cost, Multiplatform, Multi biometrics and Secure[13]. A lot of works/applications can be found that focus on the use of biometry with mobile devices; however, as far, none of them show a similar system to the one in this paper: a general proposal to capture biometrics by means of a mobile phone during a standard web session. 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.

Modules

- Server Design
- Client Registration and ID Generation
- User Login and Image Capturing Engine
- Feature Extraction and e-Banking

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

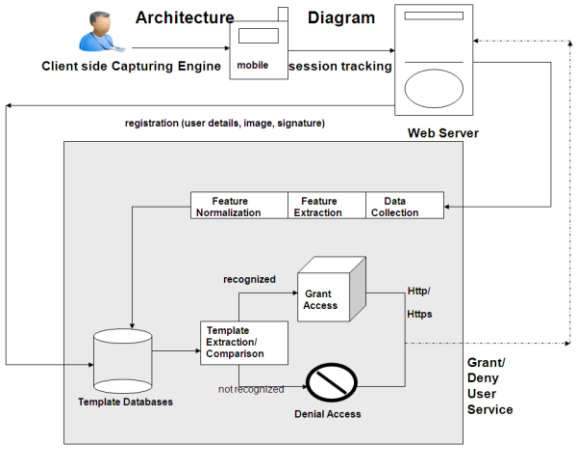

Fig. 1. System Architecture

V. MODULE DESCRIPTION

A. *Server Design*

The server side contains the main parts of the functionality of the proposed architecture. In our first module we deal upon accessing the Server Tier designing part of our project. We deal on working with Tomcat Server and designing our web pages using Struts.

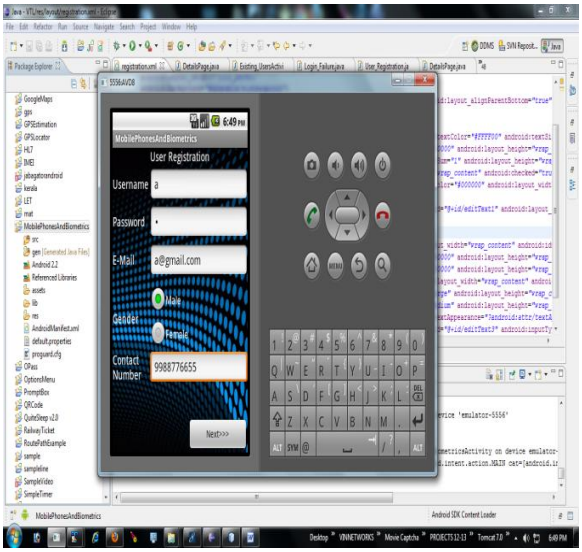

Fig. 2. Registration

B. *Client Registration and Id generation*

On the client side, the biometric acquisition software is deployed. 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[14]. We perform Client Registration from our mobile end to connect it to our server which in turn creates account id and user id for the respective client.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

C. User Login and Image Capturing Engine

Biometric Capturer takes in charge of calling and managing the mobile capture devices and a biometric up loader is in charge of sending the biometric data to the server and managing this uploading. A Client makes a login using his account id and user id, and the server performs a validation using his details. The Biometric Capturer captures the client's image and passes on to the server.

D. Feature Extraction and E-Banking

This module collects the raw biometric data and prepares them for processing by the verification engine. This is based on biometric data supplied by the server-side capturing engine, and it generates the feature vectors.

In addition to obtaining the features vector or sequence of feature vectors, it is usual to perform further geometric transformations[15]. The database contains information from the users of the system (i.e., user's database subsystem) and their biometric templates (i.e., user's templates subsystem). The matcher compares the information received against the template of the client stored in the database, thereby generating a numeric comparison score.

The Score-normalization is to improve the system performance or to use a universal decision threshold. From the comparison of the score with a decision threshold, this determines whether the user is accepted or rejected and is, thus, granted or denied access to the system or protected services and transmits the output back to the client.

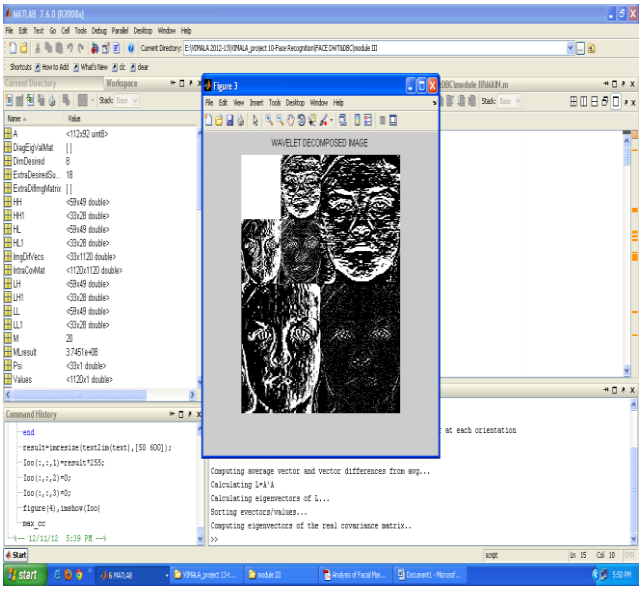

Fig. 3. Feature Extraction

VI. CONCLUSION AND FUTURE WORK

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.

This future line of the work can be divided into technological and basic research. The technological problems to be approached in the future are to implement the proposed solution in other mobile phone platforms and to perform an in-depth study of the communication load and server performance in terms of the number of users. With regard to basic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

research, multichannel (PC, PDA, mobile phone, etc) biometric recognition is an interesting problem. There are studies in biometrics, such as voice or face, but other biometrics, such as signature, is still an open problem.

REFERENCES

[1] N. L. Clarke and A. Mekala,(2007) "The application of signature recognition to transparent handwriting verification for mobile devices," *Inf. Manage. Comput. Secur.*, vol. 15, no. 3, pp. 214–225,.
[2] R. L. Kay. (2003). Protecting mobility, IDC White Paper [Online]. Available at: http://www.tsi.enst.fr/ ~chollet/Biblio/Articles/Domaines/ BIOMET/IDC/Protecting_Mobility.pdf/
[3] Subha Palaneeswari M., Abraham Sam Rajan P.M., Silambanan S., Jothimalar, "Blood lead in end-stage renal disease (ESRD) patients who were on maintainence haemodialysis", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) pp.1633-1635.
[4] R. M. Godbole and A. R. Pais, (2008)"Secure and efficient protocol for mobile payments," in *Proc. 10th Int. Conf. Electron. Commerce*, , pp. 1–10.
[5] Selva Kumar S., Ram Krishna Rao M., Balasubramanian M.P., "Chemopreventive effects of Indigofera aspalathoides on 20-methylcholanthrene induced fibrosarcoma in rats", International Journal of Cancer Research, ISSN : ISSN: 1811-9727, 7(2) (2011) pp.144-151.
[6] D. S. Jeong, H.-A. Park, K. R. Park, and J. Kim,(2005.) "Iris recognition in mobile phone based on adaptive gabor filter," *Lect. Notes Comput. Sci.*, vol. 3832, pp. 457–463,
[7] Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
[8] Q. Zhang, J. N. Moita, K. Mayes, and K.Markantonakis,(2004) "The secure and multiple payment system based on the mobile phone platform," presented at Workshop Inf. Secur. Appl., Jeju Island, Korea,
[9] N. L. Clarke and S. M. Furnell, (2005) "Authentication of users on mobile telephones.A survey of attitudes and practices," *Comput. Secur.*, vol. 24, no. 7, pp. 519–527,.
[10] Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
[11] 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.
[12] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia,(Dec. 2008) "Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation," in *Proc. 19th Int. Conf. Pattern Recogn.*, , pp. 1–5.
[13] Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
[14] D. J. Hurley, B. Arbab-Zabar, and M. S. Nixon, (2008)"The ear as a biometric," in *Handbook on Biometrics*, A. K. Jain, A. A. Ross, and P. Flynn, Eds. New York: Springer-Verlag, , pp. 131–150.
[15] S. yi Han, H.-A. Park,D.H. Cho, K. R. Park, and S. Lee,(2007)"Face recognition based on near-infrared light using mobile phone," in *Proc. ICANNGA, Part II (Lect. Notes Comput. Sci. vol. 4432)*, , pp. 440–448.
[16] Dr. T.Nalini, Dr.K.Manivannan, Vaishnavi Moorthy, Efficient Remote Data Possession CheckingIn Critical Information Infrastructures Ensuring Data Storage Security In Cloud Computing, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 12-18, Vol. 1, Issue 1, March 2013
[17]Dr.K.P.Kaliyamurthie, Cervical Cancer Screening and Classification Using Acoustic Shadowing, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 1659-1662, Volume 1, Issue 8, October 2013
[18] Dr.K.P.Kaliyamurthie, Automated Information Retrieval System Using Correlation Based Multi- Document Summarization Method, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 4328-4335, Vol. 1, Issue 7, September 2014
[19] Dr.K.P.Kaliyamurthie, D.Parameswari, Modelling Cloud Storage, International Journal of Communication Engineering, ISSN: 2249-2651,pp 1-5, Volume1 Issue3 Number2–Dec2011
[20] Dr.K.P.Kaliyamurthie, D.Parameswari, Implementation of Customized Greencall Algorithm for Energy-Efficient Of Wireless LANs, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 15-21, Volume1 Issue 1 Number2-Aug 2011