Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 577-581

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Face Recognition for Mobile Application using Viola-Jones and Principal Component Analysis

[1]Silviya Nancy J, and [2]Udhayakumar Shanmugam

[1]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai - 602105, India.*
[2]*Department of Information Technology, B.S.Abdur Rahman University, Chennai- 600048, India.*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Biometric face recognition, Authentication, smart phones, Feature extraction and normalization.

ABSTRACT

The aim of the proposed work is to present a biometric application in mobile phones for secure banking (M-Banking). The chief contribution of this paper is to use the handheld devices as the biometric capturer, which would be the initial step then later the recognition will be done during every access. The biometric face recognition is employed because of its secure pathway that ensures authentication and confidentiality. It is refined security arrangement for the users who are highly dependent on the smart phones that provides high end authorization for all the personal details. The proposed system of this research paper includes the implementation of facial recognition in smart phone for banking application with the local server (offline environment).

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Silviya Nancy J, and 2Udhayakumar Shanmugam., Face Recognition for Mobile Application using Viola-Jones and Principal Component Analysis. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 577-581, 2015*

INTRODUCTION

Mobile devices of these days inculcate a variety of applications which attracts the users to adapt to its changeable and eminent functionalities. With the initiation of innovative up gradation in mobile technologies the way of communication is been changed. The era of wireless communication paves a renowned way for wide usage of smartphones. The high-end features and provision makes the smartphones to be the crucial part of the daily lives of the people. In early times the mobile phones were only preferred for voice communication, but now the innovation in technology has provided us to grab everything with a second. The mobile applications are growing rapidly in different perspectives like business, education, health care, etc. These applications are offered by many vendors along with the software and hardware configurations by extending its services to all platforms including Android, iPhones, Blackberry, and many others. The purpose of contributing these applications in low power handheld gadgets is to avail the users with necessary functionalities within the reach. In addition to that, wireless networking also plays a vital role with easy network capability and computing. This facilitates wide range of diverse functions in various domains like commerce, shopping, banking, and many more.

There are many security strategies that still exist today. People are advocated with different types of identity recognition by entering passwords or PINs was delivered by Y. Ijiri *et al*. (2006). These methodologies have become very common and the hackers are efficiently breaking the passwords and credential systems easily. With the emergence of various security issues, and to overcome the previously existing models, a new system called biometric face recognition is implemented for the improvement of security patterns. The biometric can be recognized into two types such as, physiological and behavioral analysis. Taking the mobile considerations in mind, all the details are stored in the server to prevent storage and battery crisis and theft of mobile devices. This results in perfect client-server architecture. The state-of-art for introducing the system is because of its simplicity N. L. Clarke and S. M. Furnell (2007) low cost, biometric oriented and secure predicted by Carlos Vivaracho-Pascual and Juan Pascual-Gaspar (2011).

In this work, novel mobile application architecture is designed to capture the images of the users and send to the web server with the registration details. When the user login for the next usage, the image will be captured again for verification which is done with algorithms such as Viola-Jones and PCA and then they will be guided with the banking application.

Related Work:
Mobile Computing:

Corresponding Author: Silviya Nancy J, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, India.
Tel: +91 9487752343; E-mail: jsilviyanancy@gmail.com

The facility to share information from corner to corner is becoming vital reality in our day to day lives. The focus towards the wireless communication has reached a milestone with its impeccable capabilities. The future of mobile computing lies in its mobility and network access. It has the potential to renovate learning perspectives. Its connectedness and interoperability plays an important phase in their wide mission. The mobile computing and its communication aspects has become the major part for the underpinning of wireless LAN applications. It is an endearing technology that advocates the physical links for the transmission of data. This is probably been defined as Personal Communication services (PCS), which enhances its functionalities by inculcating various features of communication like voice and message services, now their added escalation fuelled the wireless access too, where the needed information can be got at anywhere and anytime.

Characteristics:

The mobile computing can be broadly classified with the help of three domains whose applications are mentioned here: When we take hardware into consideration a lot of portable devices are taken onto account. They can be listed as laptops, smartphones and various other components. In the view of software classification there are many vendors fulfilling the hardware with eminent application functionalities with varieties of application infrastructure providing different usable features. Next favorable part is communication where a number of network interface and their protocols offer wireless access.

Features:

The features of mobile computing are discussed below: Mobility refers to permanent access that is been provided for the resource inheritance. It can be clearly defined with user and device mobility features. User mobility takes up the part of explaining the scenario where the users having access to similar telecommunication systems. Device mobility looks out for the mechanism of connectivity when the device moves to different regions. (Connectivity) The diverse network connection plays a mighty role in the deliverance of information. The device mobility feature discussed above employs the interface for the network providers and helps them to keep them in intact with their networks and duties. It keeps the mobile nodes in connected mode with the help of wireless network. The limitation and challenges are: Frequent disconnections, Limited communication bandwidth, draining of battery, Roaming distractions and disconnections, Disruptions in features of mobility, Scarcity of resources and storage, Security risks.

Biometric Authentication:

Carlos Vivaracho-Pascual and Juan Pascual-Gaspar (2011) state the purpose of using biometric for security of the applications in various domains. The authors also have explained about the password management and its flaws when used for high-end systems.

K. R. Park *et al*. (2008) explains the study on corneal specular reflections and the use of Iris as the biometric. The presenters have discussed on various aspects of the eyes, with normal and glasses using Adaboost eye detector.

S. yi Han *et al*. (2007) speaks on the face recognition with near infra-red light on mobile devices. They have proposed NIR illuminator for errorless recognition using Principle Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Independent Component Analysis (ICA).

Y. Ijiri *et al*. (2006) expresses the security enhancement in using face recognition for mobile devices in high-end applications.

Recommended System Model:

We propose novel mobile-phone application architecture to capture and send the biometric to the web server based on the use of an embedded web browser. We exploit two different algorithms (Viola-Jones and PCA) in MATLAB to prove our face detection and face recognition successfully.

The server maintains an interaction session between client and its credential storage. At first the user id is created with an account number for user. Compared the user captured images at the backend and passes the output to the client.

The client registers his information and makes a login using his identity. Captures an image and passes it to the server for further validation. Access the mobile bank's services after biometrical validations.

Most of the works/applications are adaptations of biometric recognition systems to mobile device limitations, which usually suppose a performance loss and a high cost of development when the mobile platform or the recognition systems are changed. The ease of modifying the server side and adapting the client side to different mobile platforms with our proposal has been dealt with.

System Design:

The proposal of the new system is to enhance the security for user authentication. This involves usage of biometric images for authentication. Here the face is been used as the biometric. At the client side the registration and image capturing is done. The image is captured in the mobile and it is sent to the server side for verification.

The sever collects the data, compares the features and normalizes it whereas the comparison is done using two algorithms Viola-Jones and principal component analysis(PCA).Then the face is

compared, if the registered image matches the captured image, the access is been granted to the user. At the same time user's mobile number is been monitored at the backend. Once the face recognition task is been carried out correctly, the users will be directed to the m-banking web page for further processing and transactions.

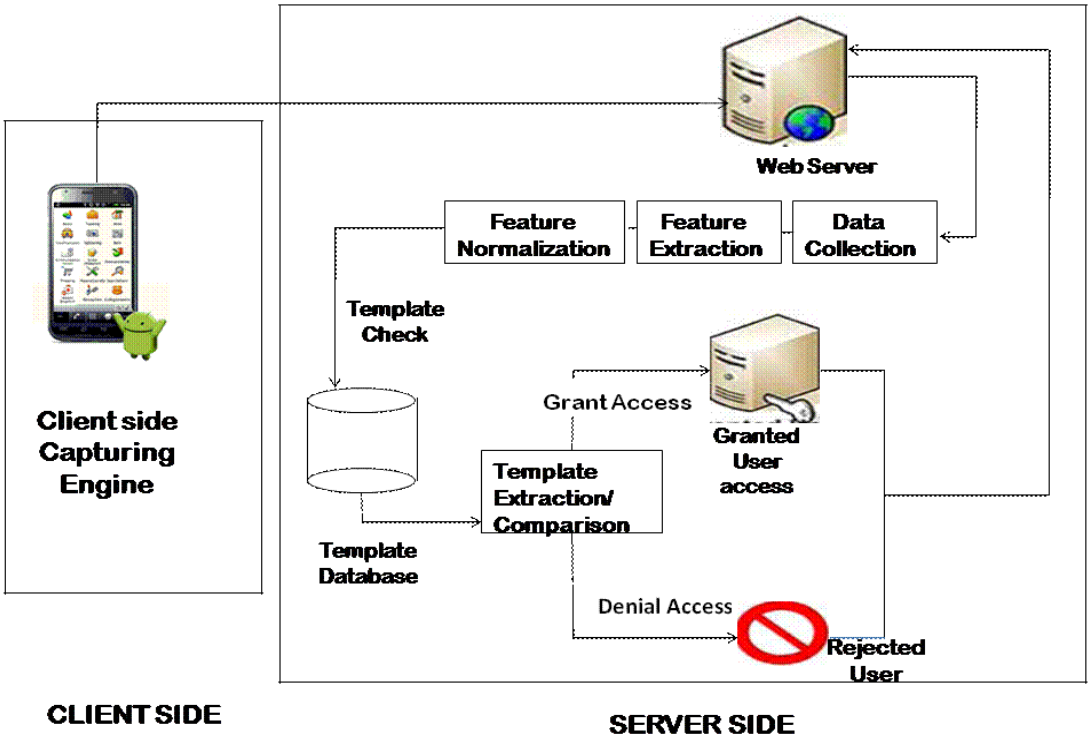

Fig. 1: Proposed System Design

RESULTS AND DISCUSSIONS

The proposed work consists of the following sections;

Client Registration and Identity Generation:

At the client side, only the image authorizing and capturing units are embedded. It obviously defines that there is no need of additional memory requirements for mobile devices. Firstly, the user will register his details with his image to the server. Then the server validates the image with generation of private account number and user id for every particular user.

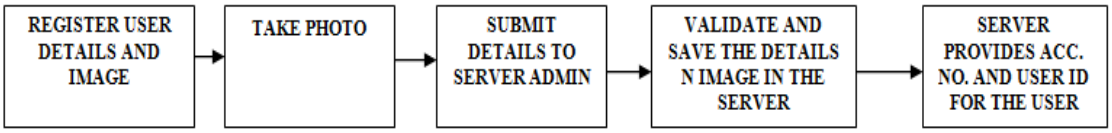

Fig. 2: Registration sequence

Fig. 3: Registration and account generation process with image

User Login and Image Capturing Engine:

With the provided ID and account number, the user can sign in by logging into the system. Again the capturer requests for the image of the user for verification and passes it to the server where the server verifies the images and grants access to M-Banking with OTP or denies the user.

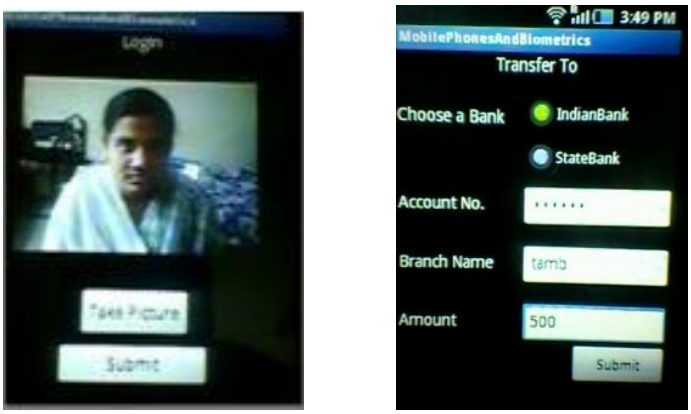

Fig. 4: Login and M-Banking access

Server Design:

The server side contains the main parts of the functionality of the proposed architecture. In the first part, we deal upon accessing the Server Tier as the designing part of our proposal.

The face recognition and face detection is done in this module using two algorithms Viola-Jones and Principal Component Analysis (PCA) [3]. Viola–Jones is an object detection framework, it provide competitive object detection rates in real-time. The basic principle of the Viola-Jones algorithm is to scan a sub-window capable of detecting faces across a given input image. The Viola-Jones face detector analyzes a given sub-window using features consisting of two or more rectangles. The face detection is done by finding the negative and positive in the image where the face is the positive, the detected face by is converted into a covariance matrix data file. The Principal Component Analysis (PCA) is a classical technique it is used in prediction, redundancy removal, feature extraction and data compression.PCA exactly recognizes the data patterns and expressions and point out with differences and identical patterns. The comparison is made the collected images from the client and from already stored images from the server [1].

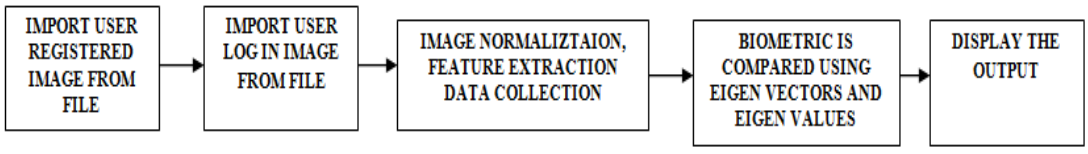

Fig. 5: Server side – Feature Extraction and comparison

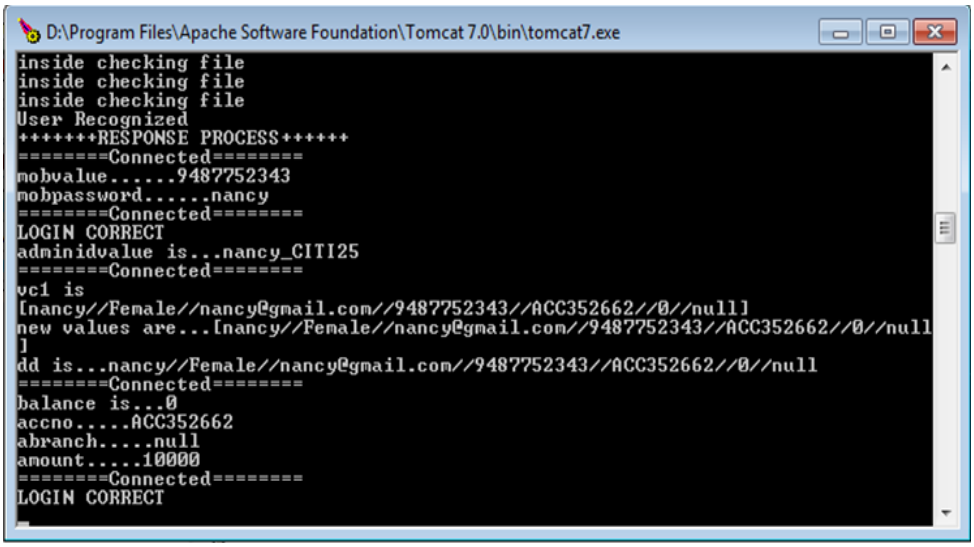

Fig. 6: Monitoring of logs by the local server

Conclusion:

In this paper work, a security model is been developed by using the face as a biometric to overcome the security issues with passwords and PINs. The key features of this system are low cost and simple to use, since the mobile devices are portable and user interfaces are easy to understand. As the first step, it is executed with offline local server system. As a future implementation, it can be implemented with the cloud storage systems.

REFERENCES

Carlos Vivaracho-Pascual and Juan Pascual-Gaspar, 2011. "On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services", pp: 1-10.

Bigun, J., J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, 2003. "Multimodal biometric authentication using quality signals in mobile communications", in Proc. Int. Conf. Image Anal. Process, pp: 2-11.

yi Han, S., 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, PartII (Lect. Notes Comput. Sci. 4432: 440-448.

Clarke, N.L. and S. M. Furnell, 2007. "Advanced user authentication for mobile devices", Comput. Secur., 26(2): 109-119.

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

Ijiri, Y., M. Sakuragi and S. Lao, 2006. "Security management for mobile devices by face recognition", in Proc. IEEE Int. Conf. Mobile Data Manage., pp: 49-53.

Tao, Q. and R.N.J. Veldhuis, 2006. "Biometric Authentication for a Mobile Personal Device", in Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Serv., pp: 1-3.