ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

BIOMETRIC ENHANCED AUTHENTICATION AND RESULT UPDATION USING RASPBERRY PI AND LINUX

AVADANAM HARITHA, D. SHEKAR GOUD

AvadanamHaritha, M.Tech Student, DeptOf ECE, Ellenki InstituteofEngineering&Technology, Patelguda,Patancheru,Sangareddy(dist),Telangana-India.

D.ShekarGoud, M.Tech,Asst. Professor, Dept Of ECE, Ellenki Group of Institutions,Patelguda,Patancheru,Sangareddy(dist),Telangana- India.

Abstract:

Biometrics can be defined as the natural characteristics that are unique to an individual such as fingerprint, voice, face, IRIS, ear patterns, DNA etc. In this technology driven world, biometric authentication systems are playing a vital role in information security. Biometric entities have profoundly revamped individual recognition and verification process. The main motive of this paper is to implement a cost effective, compact, flexible multimodal biometric identification system. The proposed authentication node sends SMS and E-mail to the remote server with status of authentication. After completing every authentication, the result is sent to the remote server via SMS. In case of failed authentication, this model of implementation has the capability to send the image of the malicious user to the server via E-mail.

The Raspberry-pi board is used as authentication node which is a powerful system with several features and available at low cost. The proposed architecture is having buzzer interfaced to raspberry-pi to give alert out in case of authentication failure. This system uses the combination of advanced Local Binary Patterns (LBP) algorithm and Eigen faces for face and iris detection. The system uses OpenCV framework for the software development and equipped with Wifi to support IOT features such as E-mail.

Keywords: multimodal biometric authentication, Local Binary Patterns, Eigen faces, Raspberry-Pi, buzzer, OpenCV, fingerprint module.

I.INTRODUCTION

Biometric systems play vital role in physical identity control systems. An individual's biometric entities are real characteristics that are required in figuring out someone. Conventional techniques for authentication rely upon outer things like tokens, passwords and keys which can be easily stolen or duplicated. Clients can have numerous private records. The client may require various passwords on numerous number of Sites. At the core of all security frameworks is the impression of verification confirming that the individual is legitimate user. Biometric entities are used to safeguard that a service or system can be accessed by a legitimate user. The biometric authentication systems can be deployed in numerous purposes like mobile internet banking, Indian aadhar card, electronic voting system, ATMs, attendance executive system, civil supply management, inventory management etc. The biometric system's use is flourishing every day.

A. Basic Design:

The biometric authentication section has two phases, enrollment and identification. The initial point when a particular person uses a biometric multimodal system for registering is called enrollment. During the enrollment state, biometric characteristics from the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

specific person is abstracted and saved in a database. In this procedure, a smartcard can be generated with ID number or username to designate Threshold values for every individual is produced and saved in the exemplary directory. Second is the identification mode. The biometric entity establishes a one to multiple correlations across a database of biometric vectors. This procedure is established to constitute the distinctiveness of an anonymous personality. The framework succeeds in distinguishing the person within the database comes within a formerly set threshold. The enrolment phase is very crucial as the legitimate features should be extracted. To generate template using OpenCV algorithms, photo with specific qualities or a vectored array of integers could be utilized. A template is an extraction of the relevant characteristics from the source. Components that are not required for the biometric calculation and matching algorithm are scrapped to minimize size of the template file and to safeguard the characteristics of the enroller.

B. Motivation:

Multimodal biometric entities can acquire set of characteristics from various biometric assets of the same user. Multimodal biometric entities are generally more vigorous to pirated attacks. The suggested biometric model makes use of multimodal authentication using fingerprint and face detection.Updating results to remote server improves scalability and flexibility needed by real time program of biometric identification system. The use of Local Binary Patterns(LBP) framework in OpenCV accelerates the system to get very fast response time compared to other frameworks like haar cascade. LBP algorithm produces accurate results with lesser turnaround time. In the LBP procedure, during enrolment phase, the image of the individual is converted to grayscale. In every pixel of image, the centre pixel and specific surrounding size is selected and LBP value is generated. The LBP arrays are generated by using LBP class entities and a vector value is calculated. During the face identification process, the Individual's face LBP vector is generated. The generated vector is compared with the vectors of existing list of users.

what template must be passed down for comparing the traits.

C. Existing System:

There are currently two existing methods for authenticating a person's identity. First is by using passwords. User saves the password initially and he has to remember it when accessing the system. Internet sites which require a username and login passwordcomposition are also increasing exponentially. To overcome this shortage, users deploy analogous or similar passwords for various objectives, which scalesdown the security of the password to that of the weakest possibility.Second mode of identification system useunimodal authentication like fingerprint. They suffer byidentical limitations. For example iris identificationentities could be duplicated by aged and stale irises and fingerprint capturing system by worn-out fingerprint called spoof attack.

D. Scope:

The Raspberry Pi evaluation board framework consists of BCM2835 System-on-Chip processor which has an ARM11 controller and Image capturing device consists of a USB webcam which is Linux compliant. The software codes for both identification and perception of faces are developed by employing OpenCV framework and C++ language. The scope of this paper covers below objectives:

1. Configuring the USB-serial camera interface and fingerprint interface, buzzer interface, Wifi and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

GSM.

2. Develop code with LBP algorithm APIS to take 15 snapshots of user face and two fingerprints, sort and store them in YAML format and generate vectors. Compare the user face vector with existing database of photos and produce results.
3. Making use of QT tool for cross compiling biometric code to run on Linux, and to validate the biometric recognition on Raspberry-pi.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

II. PROPOSED METHODOLOGY AND DISCUSSION

The suggested biometric model consists of multimodal biometric-based identification method which can detect bogus identities, those can be deployed in multiple biometric models with different applications. It uses person's fingerprint and face to identify multiple methods of fraudulent access approaches. . In this project, the USB camera is interfaced to Raspberry Pi (an ARM11 based development board). The USB camera obtains face image of a person and send it to controller. The RPi controller will identify the face of the specific individual from the image. The raspberry-pi is also connected to PC via USB-VGA interface to see the images getting captured. The fingerprint section will get the fingerprint from the individual and send to RPi controller. The RPi controller will identify the fingerprint of specific individual from the database. If they are similar then it will display the result on display section.Otherwise the buzzer will be blown to indicate failed authentication.

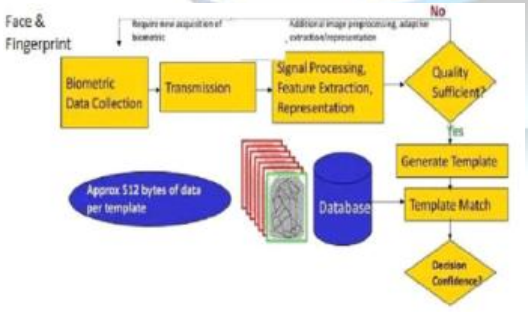


Fig 1:Multimodal biometric authentication system

The other output of Raspberry-pi is connected to GSM/GPRS SIMS hardware and Wi-Fi module. An SMS will be sent to smartphone at every time of authentication to indicate the status. In case of failed authentication, the image of suspicious user will be sent via E-mail.

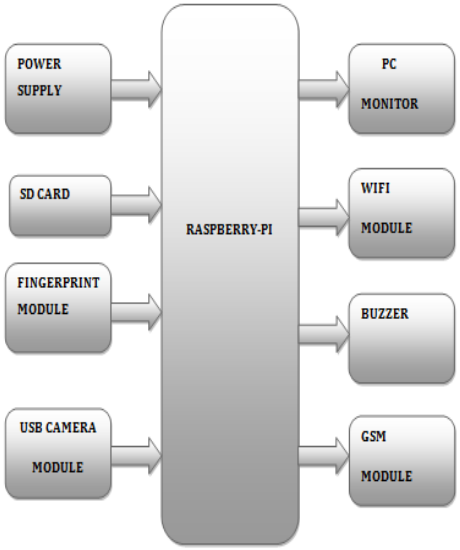
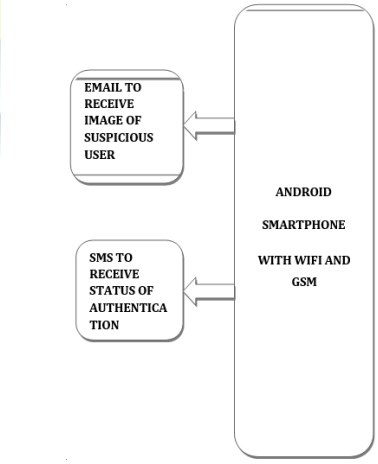


Fig 2: Block diagram of authentication section

The entire system consists of two sections, one is Raspberry-pi controller with fingerprint, camera, GPRS, inbuilt Wi-Fi,monitor connections and the other section is android smartphone to display result in email. There are two stagesinvolved in fingerprint and face detection, enrolment phase and identification phase respectively.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

Fig 3: Smartphone used as server to receive status

During the enrolment phase, fingerprint and image of a person is acquired and saved. This process uses username, ID number to attach to fingerprint and face. A database is created to maintain username, ID, fingerprint and face image details. Second is the identification proof mode, the framework plays out aone-to-numerous examination across a biometric template directory trying to set up the character of an unknown person.OpenCVframework LBP face algorithm libraries are used to compare the face images and will produce the result as matching or not matching. OpenCV framework in Raspbian is used to compare the fingerprint and produce the result. The OpenCV Mat class is employed to compare the fingerprints. The class Mat illustrates n-dimensional arithmetic one-channel or multiple-channel array. The stored vectors are compared with input fingerprint vector and the result is produced as matching or not matching.TheOpenCV LBP algorithm is used to compare the face image with existing images and produce the result. Object identification by employing LBP and Eigen faces is an efficient object identification method.

III. HARDWARE SETUP AND CONNECTIONS

The proposed IOT based biometric system uses below hardware components:

1. Raspberry Pi SoC controller booted with Linux based Raspbian OS with all the required libraries of OpenCV, Libusb, and serial interface, Wifi support.
2. R303A fingerprint scanner connected via USB interface
3. Quantum USB camera connected via USB interface.
4. SIM800 GPRS/GSM Modem with antenna connected via USB
5. Buzzer connected via serial interface,
6. PC Monitor connected via HDMI/VGA interface,
7. Smart Phone equipped with Android /IOS with Wifi connection,
8. QT creator for compiling and flashing the code on SD card.

Raspberry Pi 3: The Raspberry Pi system on chip device is equipped with a BCM2835, Broadcom processor. This ARM 1176JZFS processor runs at 700MHz frequency, contains internal memory of 512 MB, equipped with video core IV GPU. It helps to understand how to do programming in Python and C++ languages.

Fig 4: Raspberry-pi 3

R303A fingerprint scanner: Processing of fingerprint depends on two factors: first is the enrollment of fingerprint and second is comparing of the fingerprint. While enrolling, user desires to take up to 2 instances. The machine will technique the 2 time fingerprint, generates atemplate of the fingerprint on

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

processing consequences and save the updated template. At the time of comparison, the consumer enters the fingerprint through an optical sensor. The device will generate a template of the fingerprint and match it with the saved fingerprint library templates.

Fig 5: R303A fingerprint module

SIM800 GSM Modem:

SIM800 is a GSM modem which can be readily connected to Raspberry-pi. AT instructions can be sent through the serial port on Raspberry Pi. Due to this reason the device supports dialing and answering calls, sending and receiving messages through serial port in real time may be found out. Moreover, the module helps powering-on and resetting via software program application. Sim800 is interfaced with Raspberry-pi on i2c serial interface.

Quantum USB camera:

The Quantum USB camera is connected to Raspberry-pi USB port, to capture the face of user and transfer it to the board for processing. The UVC driver is very crucial in providing plug and play functionality to webcam. The UVC driver is to be built as part of vraspbian OS image and should be loaded while booting the image on Raspberry-pi.

IV RESULT ANALYSIS REPORT:

This section covers the snapshot of the biometric entity implementation, the process of collecting faces and storing in database for training, Process of authenticating the person whose biometrics are already stored. This section also talks about unauthorized user access and sending email with photo of unauthorized user. The performance improvement gained by using the LBP algorithm API's is also discussed.

Fig 6: Snapshot of multimodal biometric entity

During the phase of collecting faces, the system takes15 images of the user and store them. During the Training Recognizer phase, the system does noise filtering of the images and templates are generated and vector array is generated. Every user record contains the username, ID, face templates and fingerprint template. [4] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder.

Fig 7: Sample fingerprint image

In the authentication section the user image and fingerprint will be captured and compared with the user registers present in a database. The system will validate if there is enough similarity to the stored datato the current user data to match with a certain confidence. If so it shows the result as successful authentication. In case of authentication failure the Buzzer in the setup will blow horn.

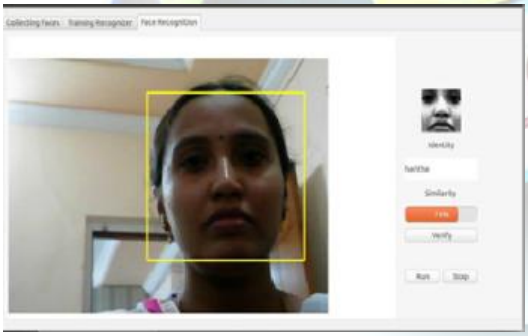


Fig 8: Face recognition using LBP algorithm

The IOT section handles transmission of authentication status to smart-phone server. In case of successful authentication, the user ID, name and status will be sent to the administrator mobile via SMS. In case of failed authentication, from the IOT section, an email will be sent with the photograph of the individual with status indicating failed authentication. An SMS also would be dispatched to the administrator mobile with status as authentication failure.

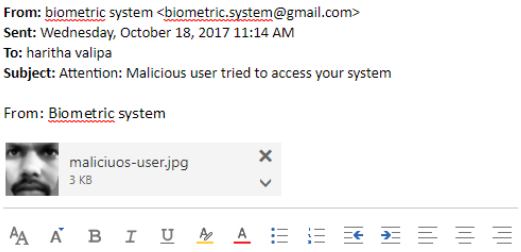


Fig9 : Email with photo of suspicious user

Performance characteristics ofLBP:

The traditional methods of face recognition used Haar cascade. We can find many implementations which uses Haar cascade for object recognition.

The Haar cascade has the disadvantage of slower processing times.Haar cascade uses complex floating point operations to generate vectors which makes it slower in real time applications. The Local Binary Pattern cascade uses histogram approach and uses integer operations to obtain good turnaround time but with less accuracy.

Platform	Algorithm	Vector generation time(msec)		
		1 Face	2 Faces	3 Faces
Raspberry-pi	Haar Cascade	33	37	46
Raspberry-pi	LBP Cascade	29	32	38

Table 1: Comparison of cascade algorithms performance

V CONCLUSION:

Reliable personal recognition is critical to many business processes. Biometrics refer to spontaneous identification of a person according to his physiologicaland/or behavioral attributes.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 2, January 2017

In reality, a legitimate device layout will often entail incorporation of many biometric and non-biometric components (constructing blocks) to offer trustworthy individual identification.The degree of securityof a biometric device relies upon on the necessities (threat model) of the software and the price-advantage evaluation. As the biometric generation matures, there might be a growing collaboration among themarket, technology, and the packages. This collaboration can be encouraged through the brought exposure of the technology, customer attractiveness, and the credibility of the service vendor. It is very much troublesome to predict the path and which biometric inventions could evolve and get embedded in which programs. But it's far sure that biometric-based identification may have a profound impact on the manner we continue our everyday affairs.

FUTURE SCOPE:

1. The accuracy of biometric systems can still be improved by using other high speed processors, complex DSP algorithms and expanding storage to store more images.
2. While using IOT techniques, In order to protect a person's data, various encryption/decryption techniques can be employed to protect user's confidential information.
3. Other biometric techniques can be added to existing system such as speech recognition,ear pattern recognition.

REFERENCES:

[1]. Real time face recognition system(RTFRS) by Suad Haji College of Technology Firat University Elazig, Turkey, AsafVarol Software Engineering Department College of Technology, Firat University Elazig, Turkey

[2]. OmarAbdulwahabeMohamad, RashaTalal Hameed, NicolaeTapus, " Access Control Using Biometrics Features with Arduino Galileo", International Journal of Advanced Research in Computer Science and Software Engineering, vol 4, issue 8, Aug 2014.

[3]. Biometric Authentication, Available: http://www.computer world.com/article/2556908/security0/biometric-authentication .html. [3] DhavalChheda, DivyeshDarde, ShraddhaChitalia: "Smart Projectors using Remote Controlled Raspberry Pi", International Journal of Computer Applications (0975 – 8887) vol. 82 – No 16, Nov 2013.

[4]. Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07

[5]. DebnathBhattacharyya,Rahulranjan,PoulamiDas,TaiHoon Kim, Samir KumarBandyopadhyay,Biometric Verification approach and Its future conceivable outcomes.

[6]. IEEE Trans Int. conf. On portable PC and electrical Engineering,pp. 652-655, 2009. A. k. Jain, A. Ross and S. Pankanti, "Biometrics: An instrument for

certainties security," IEEE Exchanges on insights Crime scene investigation and security.

[7]. IEEE paper "End to End encryption based biometric Saas" by Dhvani. K. Shah, Dr. Vinayak A. Bharadi, V. J. Kaul,Sameer, Information Technology Department, Thakur College of Engineering and Technology.

[8]. Biometrics of Next Generation: An Overview. SPRINGER, 2010. Debnath Bhattacharyya, Rahul Ranjan, FarkhodAlisherovA.,andMinkyu Choi. Biometric Authentication: A Review, International Journal.

[9]. A. Gaszczaka, T. Breckon, and J. Hana, Real-time people and vehicle detection from UAV imagery, SPIE Conference Intelligent Robots and Computer Vision, 2011. doi:10.1117/12.876663

[10]. T. Ahonen, A. Hadid, and M. Pietik¨ainen, Face recognition with local binary patterns, IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(12):2037-2041, 2004. doi:10.1109/TPAMI.2006.244

AUTHORS PROFILE:

1. **Mrs. AVADANAM HARITHA** has received her Bachelor of Engineering degree in Electronics and Communications Engineering from Rajiv Gandhi Memorial college of Engineering and Technology, Nandyal in the year 2005. At present she is pursuing M.Tech with the specialization of Embedded SystemsatEllenki Institute of Engineering and Technology, Hyderabad.Her area of interest is in the study of biometricsensors, precision agriculture and water resources management.

Email:haritha.valipa@hotmail.com

2. **D.SHEKARGOUD,**

M.TECH(EMBEDDED SYSTEMS) he is currently working as Assistant Professor in department of Electronic and communication of Engineering inEllenki Group of Institutions, Hyderabad. He guided for more than 35 projects to final year B.Tech students and guided for M.Tech students with good teaching experience.His Areas of interest in Embedded System R & D, DSP, Microprocessors and Microcontrollers.

Email: shekar.embedded@gmail.com