Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Access Control Using Biometrics Features with Arduino Galileo

Omar Abdulwahabe Mohamad*, Rasha Talal Hameed*, Nicolae Ţăpuş
Faculty of Automatic Control and Computers
University of Politehnica in Bucharest
Bucharest, Romania
Computer Science Department, College of Education, AL-Iraqia University, Baghdad, Iraq

Abstract—In this paper, we propose a new efficient home automation security based on multimodal biometrics. The multimodal biometrics there is a combination of different biometric modalities into a single system. The proposed system used the fingerprint and voice as a biometrics features for authentication to access control to the home. This system consist of two parts: first part is the hardware system components and the second part is the proposed system method. The hardware section includes the Arduino Galileo form Intel, fingerprint shield, EasyVR 2.0 voice recognition shield, GPRS/GSM shield. The goal of this project is to increase the security access control by using multimodal biometrics.

Keywords— Biometric, Arduino Galileo, Fingerprint, Voice, GPRS/GSM.

I. INTRODUCTION

Security over the years has been a source of concern to organizations and companies. This has caused quite a significant amount of capital being budgeted for improvements on security systems, simply because it has been discovered that the access control system mechanism is an important part of an organization. One of the important security systems in building security is door access control. The door access control is a physical security that assures the security of a building by limiting access to the building to specific people and by keeping records of such entries [1].

Biometrics is physiological or behavioral characteristics of human such as fingerprint, hand geometry, face, retina, iris, palm print, voice, signature, ADN [2] those usually used in automated person recognition system. A numerous researchers have studied and developed strong combinations of the two emerging technologies: biometrics and embedded system technology in security applications. Specifically, the combination of biometrics and automation into a framework is called home automation system. [3]. Home automation is automation of the home, housework or household activity. Home automation may include centralized control of lighting, HVAC (heating, ventilation and air conditioning), appliances, and other systems, to provide improved convenience, comfort, energy efficiency and security [4]. Some work on multimodal biometric systems has already been reported in the literature. Youssef ELMIR [5] has proposed approach which integrates fingerprint and voice to identify a person. Hong and Jain [6] have developed a multimodal identification system which used two different biometric fingerprint and face. Slobodan Ribaric and Ivan Fratric [7] used different multimodal biometrics property using Bayesian framework. Rozeha A. Rashid, Nur H. [8] has proposed to biometric data (voice) for security system.

However, there are still many challenges to home automation security. Although we use biometrics – a secure way to authenticate access control, how we can be use these biometrics data in efficient way to give authority to access control.

In fact, there are many drawbacks when using unimodal biometric system as a personal identification. In case of voice recognition the noisy sensor data, non-distinctiveness, easy spoof attacks may create problem for determining the identity of the user and the reliability of the voice recognition system in low matching score level (50%). [5]

To solve that problem, in this paper we propose a solution that uses Biometrics data for both (fingerprint and voice) to protect the home or office enter. The fingerprint recognition is secure and more reliability than the voice recognition according to the matching score level in the previous work [9]. The multimodal biometric system overcomes the limitations of unimodal biometric system, reduces fraudulent access and also more accuracy. The proposed algorithm used the two human biometrics (fingerprint and voice) of user to give the authority for access control. The additional feature of this system the home owner or office manager will be known all the events occur at the place by using the cell phone.

This paper is organized as follows. Section II describes the hardware system components. Section III explains proposed system method. The experimental results are shown in Section IV. Finally, Section V contains conclusion.

II. THE HARDWARE SYSTEM COMPONENTS

The system consists of the following components:

A. Arduino Galileo

There are many different types of electronics hardware development boards featuring embedded processors and the most famous species like Raspberry pi, BeagleBone, Arduino Galileo. The embedded world evolved very differently there were too many choices for processors, which were mainly chosen for price and features. The devices like Raspberry pi and BeagleBoard are best for handling media such as video. They are designed to function on a much higher level with already integrated hardware that takes care of things like Ethernet, video processing, large quantities of RAM and an almost unlimited amount of storage space. The Raspberry pi is cheap price (about $35) but without an analog-to-digital converter, analog sensors would not be easy to implement. The BeagleBone board costs almost twice as much as the Raspberry Pi model B, with software license agreement and better work with video processing. [10]

In the other side the Arduino is an excellent choice if we have a project requiring sensors (and decent memory and processing power), monitoring, or have productivity-related applications (Galileo has a real time clock.) Galileo could be used to develop smart everyday "things" with lots of sensors, such as health monitoring, security system ,home automation, fitness devices, or simply be an inexpensive personal computer running Linux sans all things Arduino. The Arduino Galileo price is near the price of BeagleBone board, but the source code is available for download with no software license agreement other than open source licenses, PCI Express (PCIe), a Real Time Clock (RTC) ,small in size (highly integrated), low power. Galileo has an I2C-controlled I/O expander that runs at 200Hz. I/O that runs through the any of the three "GPIO PWM" blocks on the Galileo schematic is going to be limited to only 200 updates per second. IO13 avoids the limitations of the expander, as well as the UARTs, SPI, I2C, and the ADC. Galileo boots from on-board memory. [11]

They each have their purpose since the choice should be based upon the goal of the project, so in this project used two biometrics sensors to the home security access control. The best choice in this project is the Arduino Galileo when compare with other electronics board.

In this project we used the new version of arduino that called Galileo from Intel. The main part of this project is the arduino, so it makes the decisions about control the system by processing the data comes from fingerprint shield, voice shield and GPRS/GSM shield. The arduino Galileo that have been used in this work have some properties like the microcontroller board based on the Intel Quark SoC X1000 Application Processor, a 32-bit Intel Pentium-class system on a chip. Digital pins 0 to 13 (and the adjacent AREF and GND pins), Analog inputs 0 to 5, the power header, ICSP header, and the UART port pins (0 and 1). [12]

B. Fingerprint Shield

There are basically two requirements for using the optical fingerprint sensor. First we need to enroll fingerprints - which mean assigning ID #'s to each print so we can query them later. Second we can enroll using the windows software (easiest and neat because it shows you the photograph of the print) or with the Arduino sketch (good for when you don't have a windows machine handy or for on-the-road enrolling). This shield was used to take the fingerprint for the user and then send it to the arduino to check it for the authority to access control. The technical specifications show in the table I. [13]

TABLE I. FINGERPRINT SHIELD SPECIFICATIONS

Item	**Value**
CPU	ARM Cortex M3 Core (Holtek HT32F2755)
Sensor	Optical Sensor
Effective area of the Sensor	14*12.5(mm)
Image Size	202*258 Pixels
Resolution	450 dpi
Matching Mode	1:1,1:N
The size of template	496 Bytes(template) + 2 Bytes (checksum)
Communication interface	UART, default baud rate = 9600bps after power on , USB 1.1,Full speed
False Acceptance Rate (FAR)	< 0.001%
False Rejection Rate(FRR)	< 0.1%
Enrollment time	< 3 sec (3 fingerprints)
Identification time	< 1.0 sec (200 fingerprint)
Operating voltage	DC 3.3~6 V
Operating current	< 130mA

C. EasyVR 2.0 Voice Recognition Shield

EasyVR 2.0 is a multi-purpose speech recognition module designed to easily add versatile, robust and cost effective speech recognition capabilities to almost any application. In this project, the purpose of used this shield is to take a voice from the authority user and save it in a data base as the user ID. The technical specifications show in the table II. The microphone provided with the EasyVR module is an omnidirectional electret condenser microphone (Horn EM9745P-382): [14]

- Sensitivity -38dB (0dB=1V/Pa @1KHz).
- Load Impedance 2.2K.
- Operating Voltage 3V
- Almost flat frequency response in the range 100Hz – 20 kHz.

D. GPRS/GSM Shield

In this project we used the SIMCOM SIM900 Quad-band GPRS shield development board for Arduino. The shield specifications show in the table III. The purpose of this shield is to make the owner of the house on the lookout if someone not authorized tried to enter to the house through the use of his voice or his fingerprint. [15]

The proposed system used additional hardware components like servo motor, LCD, breadboard, button, jumper wires, resistors, power supply.

TABLE II. EASYVR 2.0 VOICE RECOGNATION SHIELD SPECIFICATIONS

Item	Value
Frame	8 Data bits, No parity, 1 Stop bit
Baud Rate	9600(default),19200,38700,57600,115200
Languages	English(US),Italian, German, French, Spanish, Japanese
Communication interface	UART interface(powered at 3.3V – 5V)
Operating current	180 mA
Operation voltage	DC 3.3~5 V

TABLE III. GPRS/GSM SHIELD SPECIFICATIONS

Item	Value
Power consumption	1.5mA (sleep mode)
Temperature range	-40 °C to +85°C
Quad-Band	850,900,1800,1900 MHZ
GPRS	Multi-slot class 10/8
Services	SMS,MMS,GPRS and Audio via UART
Type of class	Class 4 (2W (AT) 850/900 MHZ), Class 1 (1W (AT) 1800/1900 MHZ)

III. THE PROPOSED SYSTEM METHOD

The complete system architecture with block diagram (Fig.1) is explained in this section. In this system there are four basic models: enrollment and verification models, database model, actions model, and GSM model, as discussed below:

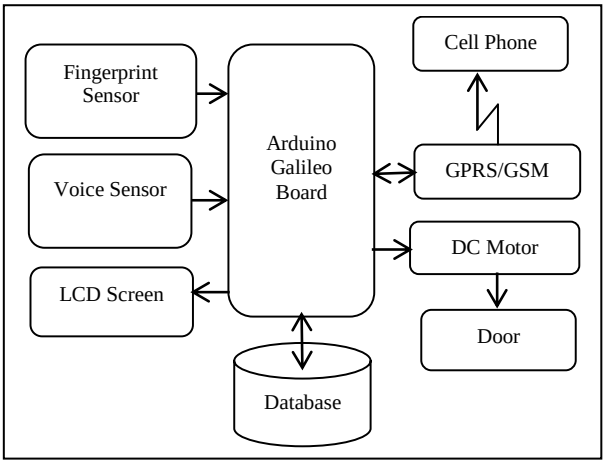

Fig.1 System proposed block diagram.

A. Erollment and Verification Models

The purpose of the enrollment model is to register all the authority users to access control and save the biometrics features in a database. The verification (or authentication) model used for veryify the claimed identify of person.This model consist of two stage : the first one for the fingerprint and the second for the voice ,as expalain below:

1) Fingerprint stage

This system registerd the users that consider as authority to access control in the enrollment model as shown in the (Fig.2). Each user in this stage will take the ID number that save in the database.

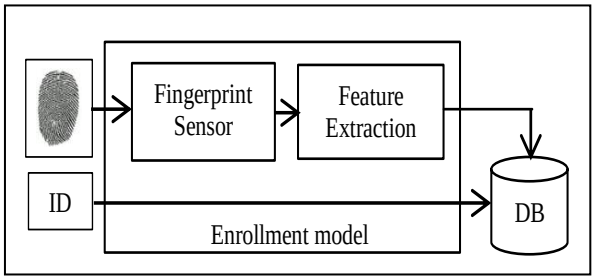

Fig.2 The fingerprint enrollment block diagram

In (Fig.3) shows the blok daigram of the fingerprint verification model.

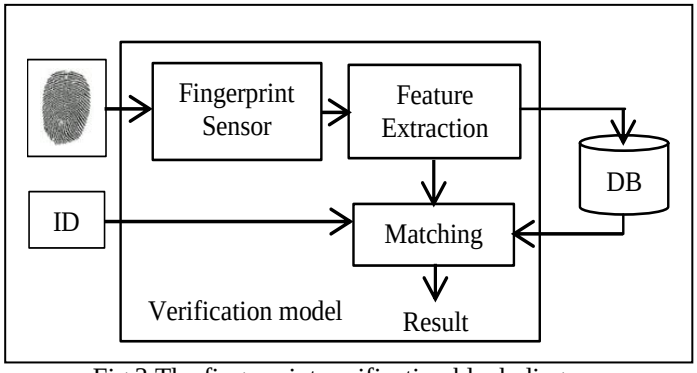

Fig.3 The fingerprint verification block diagram

In fingerprint stage we used two important functions: feature extraction and the matching function. The brief description of these functions as follow:

- Feature Extraction

The feature extraction is responsible for expressing fingerprint's unique characteristics adequately such as directions of the lines, terminals of lines, bifurcation and so on. To ensure the accuracy of comparison, the method of feature extraction must extract useful features as much as possible; meanwhile, filter false features for various reasons. There are two kinds of features in fingerprint images: global feature and local feature. Global feature can reflect overall shaper of fingerprint, which usually applies to fingerprints' classification, the process of extract global feature frequently belongs to procedure of fingerprint classification. The Local feature can reflect minutiae of fingerprint, usually applies to fingerprints' comparison. [16]

Strict feature extraction means local features' extraction. Two fingerprints often have the same global features, but their local features can not be exactly the same. The important information of fingerprints' local feature is following: terminals, bifurcations, branch points, isolated points, enclosures, short lines and so on. In fact, not all the fingerprints have these two features, it often be used as fingerprints' sub-matches [17].This system uses terminals and bifurcations in feature extraction and matching algorithm.

- Feature Matching

The matching function, features extracted from the input fingerprint is compared against those in a database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image. A large number of approaches to fingerprint matching can be found in previous work [17, 18]. In this proposed work we used the matching algorithm that support the optical fingerprint reader module SFG algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction &tolerance to deformed and poor-quality fingerprint and work with both 1:1 and 1:N.

2) Voice stage

In the (Fig. 4), we present the voice enrollment model for the authorized user.

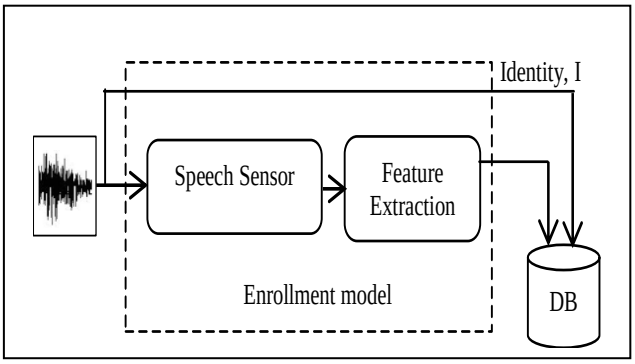

Fig. 4 The voice enrollment block diagram.

The proposed system used the voice verification model to check if the user authorized to access control or not as shown in the (Fig.5).

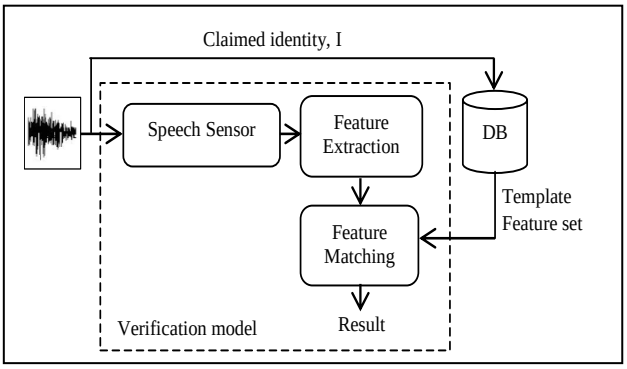

Fig. 5 The voice verification block diagram.

In the voice verification model we used the feature extraction and the feature matching, each of them explain in below:

- Feature Extraction

The Feature extraction is the most important part of speech recognition as it distinguishes one speech from other.[19] There are many feature extraction techniques available such as: Linear predictive analysis (LPC), Linear predictive cepstral coefficients (LPCC), Mel-frequency cepstral coefficients (MFCC), Power spectral analysis (FFT), Mel scale cepstral analysis (MEL), etc. In this work uses the easyVR 2.0 voice recognition shield that supports the following features: custom speaker independent commands, sonicNet, DTMF tone generation. Also the purpose of the work is to using the speech biometric to access control we used the speaker independent commands feature and the Mel-frequency cepstral coefficients (MFCC) feature extraction techniques that the EasyVR 2.0 supports this technique.

The MFCC is the most popular feature extraction technique for speech recognition. It approximates the human system response more closely than any other system because frequency bands are placed logarithmically here. They are obtained from a Mel-frequency cepstrum where frequency bands are equally spaced on the Mel scale. Computation technique of MFCC is based on the short-term analysis and thus from each frame MFCC vector is computed. MFCC can be computed by using the formula: [20, 21]

$$\text{Mel}(f) = 2595 * \log_{10}(1 + f/700) \quad (1)$$

- Feature Matching

There are many techniques used for the speech feature matching such as frequency estimation, hidden Markov models, Gaussian mixture models, template matching , neural networks, matrix representation, Vector Quantization, decision trees etc. The sensor shield (EasyVR 2.0) support the quick synthesis tool with the template matching technique for speech feature matching. [21]

The template matching is the simplest technique and has the highest accuracy when used properly. The first step of this approach is for the user to speak a word or phrase into a microphone. The electrical signal from the microphone is digitized by an "analog-to-digital (A/D) converter", and is stored in database. To determine the "meaning" of this voice input, the computer attempts to match the input with a digitized voice sample, or template that has a known meaning [22]. This technique is attempts to matching the input speech with the speech store in database using a simple condition statement. The proposed work using the template matching technique because it is work properly with the speech recognition EasyVR 2.0 shield ,highest accuracy and simplest.

After these two stages (fingerprint and voice) each user has the personal biometric ID that can be used to access control as authorized person.

B. Database model

The database of the system contains a total of 100 fingerprint images captured from 50 users. For each user it contains fingerprint image from right hand thumb. The database contains the 100 triggers or command as well as voice passwords in English language. For increase the size of memory in this system we used the external SD memory card.

C. Actitons model

This model controlled by the Arduino board to do some events. In this system, we assign the events as follow:

- If the user biometrics ID (fingerprint, voice) accepted form the microcontroller then, the arduino give the order to open the door and wait 30 sec. then close the door.
- If the user biometrics ID rejected, the arduino give the order to send SMS to the owner and display rejected message in the LCD screen.

D. GSM model

The system used GSM shield to makes the owner of the house on the lookout for event that occurs in the house. In this work we used the command send as SMS from system to the owner or receive a SMS from owner to control the system.

The flow chart in the (Fig.6) shows the main system steps.

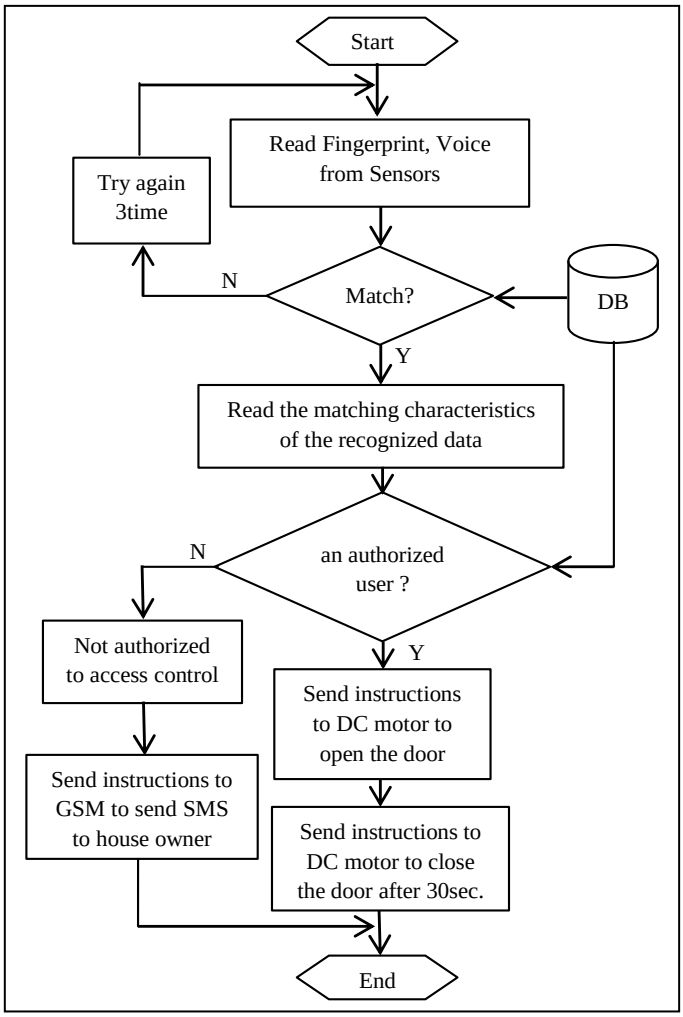

Fig.6 The proposed system flow chart.

IV. THE EXPERIMENTAL RESULTS

We have implemented the proposed system using the C language. The experimental result with the fingerprints that were acquired by the device optical fingerprint reader sensor SFG that has following specifications: "TTL serial interface, template file 512 bytes, signature file 256 bytes, baud rate 57600 bps, and window area 14mm×18mm, resolution 363 DPI". The system experimental result with the voice that used EasyVR 2.0 voice recognition shield with UART interface, baud rate 57600 bps, frame (8 data bits, no parity, 1 stop bit) and the password voice in English language.

The experimental result is collect as the following:

- 50 users were asked to scan fingerprint with register speech and consider as authority users.
- 50 users were asked only to scan the fingerprint.
- 50 users to register the speech password only.

The performance of the system is to estimate accept or reject access control authentication. Each authority user have fingerprint and speech password can used to access control. We used the threshold level (t) for accept or reject user depending on the average matching score of the user fingerprint and speech password.
The threshold in this system is set Equal Error Rate (ERR) and has two scenarios: [2, 8, and 9]

- If the matching score is greater than the threshold (ERR) the user authorized to access control.
- If the matching score is less than the threshold the user is rejecting (not authorized) to access control.

In the table IV shows the performance of the proposed system based on the seven different factors (universality, distinctiveness, permanence, collectability, performance, acceptability, circumvention. [23]

TABLE IV. PERFORMANCE OF THE PROPOSED SYSTEM BASED UPON SEVEN FACTORS (H = HIGH, M = MEDIUM, L = LOW)

Biometric Traits	Voice	Fingerprint	Voice +Fingerprint
Universality	M	M	H
Distinctiveness	L	H	H
Permanence	L	H	H
Collectability	M	M	M
Performance	L	H	H
Acceptability	H	M	H
Circumvention	H	M	H

In the (Fig.7) shows the comparison between multimodal biometrics features with single modal biometrics features when using False Accept Rate (FAR) and False Reject Rate (FRR) to plot the relation between FAR and Genuine Accept Rate (GAR).

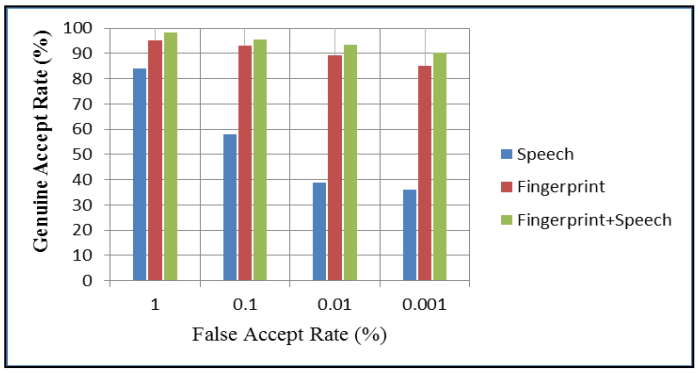

Fig.7 The comparison between multimodal and single modal features.

V. CONCLUSION

In this paper, we proposed an approach to access control based on the multimodal biometrics. The main contribution of this work is to the usage of the two biometrics data collected by sensors and controlled by arduino Galileo. In future, we can use the neural network or fuzzy logic to choose the best matching for the system more secure.

ACKNOWLEDGMENT

We would like to thank University of POLITEHNICA of Bucharest, Faculty of Automatic Control and Computers for many useful help.

REFERENCES

[1] A.O. Oke, O.M. Olaniyi, O.T. Arulogun1, and O.M. Olaniyan "Development of a Microcontroller-Controlled Security Door System ", *the Pacific Journal of Science and Technology*, Volume 10, Number 2. 2009.

[2] NGUYEN T. H. L. and NGUYEN T. T. Hang "An Approach to Protect Private Key using Fingerprint Biometric Encryption Keyin BioPKI based Security System", *IEEE 10th Intl. Conf. on Control, Automation, Robotics and Vision Hanoi*, Vietnam, 17 December 2008.

[3] Yoshifumi Ueshige, "A Study on Biometrics Authentication in BioPKI", Institute of Systems & Information Technologies, KYUSHU, 2005.

[4] Deepali Javale and Mohd. Mohsin, "Home Automation and Security System Using Android ADK", *International Journal of Electronics Communication and Computer Technology (IJECCT)*, Volume 3, Issue 2, 2013.

[5] Youssef ELMIR, Zakaria E and Reda ADJOUDJ, "Score Level Fusion Based Multimodal Biometric Identification (Fingerprint & Voice)", *6th IEEE International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012.

[6] L.Hong and A.Jain "integrating face and fingerprints for personal identification", *in proc.3rd Asian Conference on Computer Vision*, pages16-23, Hong Kong, China, 1998.

[7] Slobodan Ribaric and Ivan Fratric "Experimental Evaluation of Matching-Score Normalization Techniques on Different Multimodal Biometric Systems", *IEEE MELECON*, Benalmádena (Málaga), Spain, 16 May 2006.

[8] Rozeha A. Rashid, Nur H. "Security System Using Biometric Technology: Design and Implementation of Voice Recognition System (VRS)", *International Conference on Computer and Communication Engineering*, Kuala Lumpur, Malaysia, 2008.

[9] Sheetal Choudhary, Rajendra Nath "A multimodal biometric recognition system based on fusion of palmprint, fingerprint and face", *IEEE International Conference on Advances in Recent Technologies in Communication and Computing*, 2009.

[10] A Comparison of Open Source Hardware. [Online]. Available: http://ro.mouser.com/applications/open-source-hardware

[11] The differences between Arduino, raspberry pi and beagleboard. [Online]. Available: http://www.adafruit.com/

[12] Intel Galileo Getting Started. [Online]. Available: https://communities.intel.Com/community/makers

[13] Optical fingerprint reader for Arduino locks. [Online]. Available: https://www.adafruit.com /product/751

[14] EasyVR 2.0 Tutorial. [Online]. Available: https://www.sparkfun.com/products/12656

[15] GPRS/GSM shield for Arduino. [Online]. Available: http://www.ebay.com/itm/SIMCOM-SIM900.

[16] Kaisheng Zhang, Jiao She and Mingxing Gao and Wenbo Ma "Study on the Embedded Fingerprint Image Recognition System", *IEEE International Conference of Information Science and Management Engineering, 2010.*

[17] Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, New York (2003)

[18] F. Alonso-Fernandez, J. Bigun, J. Fierrez: Handbook of Fingerprint Recognition.

[19] Shivam Jain, Preeti Jha and Suresh. R, "Design and Implementation of an Automatic Speaker Recognition System using neural and fuzzy logic In Matlab", Proc. IEEE, 2013.

[20] Urmila Shrawankar and Vilas Thakare, "Techniques for Feature Extraction in Speech Recognition System : A Comparative Study",
Dept. of Computer Science, SGB Amravati University, Amravati, 2013.

[21] Nidhi Desai, Prof.Kinnal Dhameliya, Prof.Vijayendra Desai, "Feature Extraction and Classification Techniques for Speech Recognition: A Review", *International Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 12, December 2013.

[22] Luqman Gbadamosi,"Voice Recognition System Using Template Matching ", *International Journal of Research in Computer Science* Volume 3 Issue 5 pp. 13-17, 2013.

[23] Anil K. Jain, Fellow, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuit and SYSTEMS for Video Technology*, Vol.14, No.1, January 2004.

