ISSN: 2278 – 7798
*International Journal of Science, Engineering and Technology Research (IJSETR)*
*Volume 6, Issue 1, January 2017*

# High Security Person Authentication And Spoofing Detection With Multimodal Recognition Techniques

**MD. Azeema Sulthana[1],B.J.Prem Prasanna Kumar[2], P. Raja shekhar[3]**

[1]M.Tech Student, Department of Electronics and Communication Engineering,
Sridevi Women's Engineering College, V.N. Pally, R.R District
[2] Professor in ECE, Department of Electronics and Communication Engineering,
Sridevi Women's Engineering College, V.N. Pally, R.R District
3Assistant Professor in ECE, Department of Electronics and Communication Engineering
Sridevi Women's Engineering College, V.N. Pally, R.R District

***Abstract— Now a days, Fake biometrics means by using the real images like iris images captured from a printed paper or fingerprint captured from a dummy finger of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication. There is no such technology to provide security for fake users. , we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment.We have proposed a novel and efficient multi-server authentication protocol using biometric-based fingerprint detection ,image and iris recognition. The controller will recognize the details of particular person from the data base.If all the details get matched,the details will be opened or output will be accessed.Otherwise it will send the message to police or authorized one about wrong accessing.***

*Key Words*: **ARM7 LPC2148 controller, GSM, Finger print module, EEPROM, USB camera, PC**

## 1. INTRODUCTION

Hardware-based selective unlocking schemes have been proposed previously. These include: Blocker Tag, RFID Enhancer Proxy, RFID Guardian, and Vibrate-to-Unlock. A Faraday cage can also be used to prevent an RFID tag from responding promiscuously by shielding its transmission. Cryptographic protocols, Distance bounding protocols, Context-aware selective unlocking, Motion detection has been proposed as another selective unlocking scheme. All of these approaches, however, require the users to carry an auxiliary device.

## 2 OBJECTIVE

The main aim of this project is to provide High Security for Fake Authentication and to provide an auxiliary device for processing
1. There is an Hardware device to process the person identification.
2. High security is possible with the face,iris and fingerprint accessing for fake attempts
3. Fraudulent attempts can be identified by the authorized person

## 3. PROPOSED SYSTEM

In this paper, we have first reviewed the recently proposed scheme and then shown that their scheme is vulnerable to the known session-specific temporary information attack and thus, their scheme fails to prevent reply attack and cannot provide strong user anonymity. Also, we have demonstrated the drawbacks in existing method while distributing the static authentication parameters and with the wrong password entry. To withstand these drawbacks, we have proposed a novel and efficient multi-server authentication protocol using biometric-based fingerprint detection ,image and iris recognition. When all these parameters are authorized the locker will be opened and transactions are done .

*A. Requirements*

The system can be implemented by using hardware modules and software modules. Hardware modules are ARM7 LPC2148 controller GSM, Finger print module, EEPROM, USB camera, PC

Software modules are Keil µvision and flash magic,Matlab software

*B. System Architecture*

Here we are interfacing camera to ARM controller. The camera will capture face image of a person and send to controller. The controller will recognize the face and iris of the particular person from the image. The finger print module will take the finger print from the person and send to controller. The controller will recognize the finger print of particular person from the data base. If they are matched then it will send the OTP to the person personal mobile number.Once the password is matched,the details will be opened or output will be accessed.Otherwise it will send the message to police or authorized one about wrong accessing.Here we are using banklocker as output.When face,iris and Fingerprint matched locker will be opened with the help of a motor and also we do the money transactions.For every module matches the speaker will be activated and tells us whether matched or not

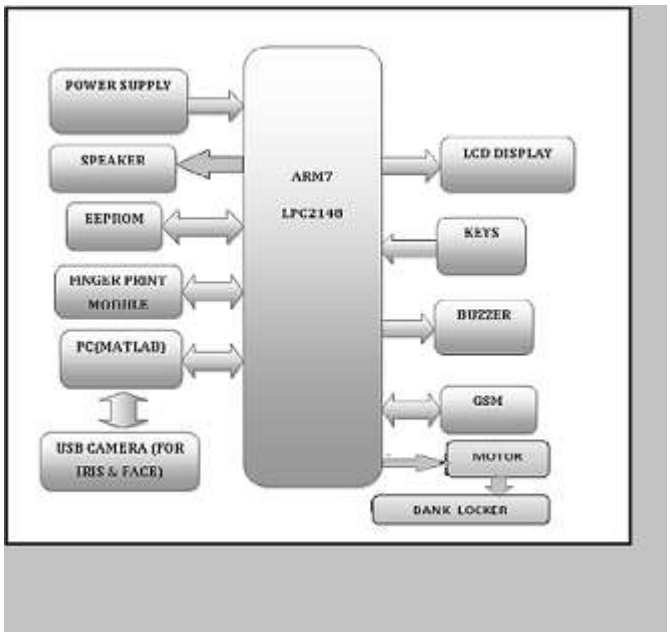



Fig 1:Block diagram of a system architecture

**a)Finger Print Recognition:**

Finger print recognition will be done in module i.e. in module users finger print images are enrolled and even unnecessary finger prints can be deleted also so it has more accessibility in adding new users also.

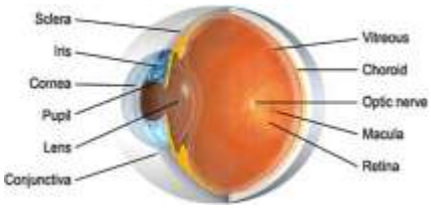
A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.


Fig 2: LCD display showing waiting for thumb print

Fig.3: Fingerprint module

**b) Iris Recognition:**

The purpose of 'Iris Recognition', a biometrical based technology for personal identification and verification, is to recognize a person from his/her iris prints. In fact, iris patterns are characterized by high level of stability and distinctiveness. Each individual has a unique iris. The difference even exists between identical twins and between the left and right eye of the same person



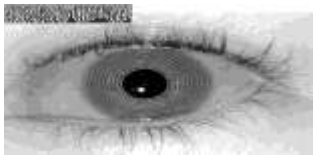



Fig 4:Human eye for recognition

Fig.5**:** Matching the person iris with the existing iris

**c)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. Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances

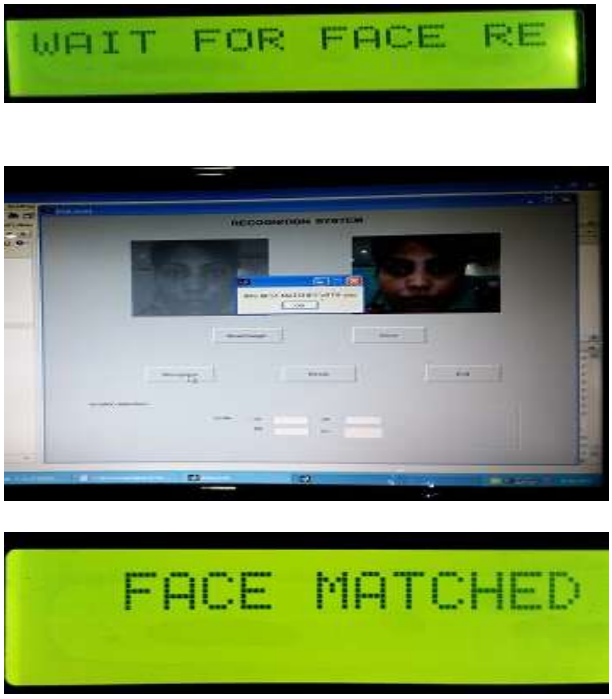



Fig 6:Recognizing the person face

## 4. HARDWARE DESIGN

*1) ARM7 LPC2148 Controller*

The ARM7 is a general purpose 32-bit microprocessor, which offers high performance and very low power consumption. The ARM architecture is based on Reduced Instruction Set Computer(RISC) principles, and the instruction set and related decode mechanism are much simpler than those of micro programmed Complex Instruction Set Computers (CISC).This simplicity results in a high instruction throughput and impressive real time interrupt response from a small and cost-effective processor core. Pipeline techniques are employed so that all parts of the processing and memory systems can operate continuously. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory. The ARM7TDMIS processor also employs a unique architectural strategy known as Thumb, which makes it ideally suited to high volume applications with memory restrictions, or applications where code density is an issue. The key idea behind Thumb is that of a super reduced instruction set. Essentially, the ARM7TDMIS processor has two instruction sets:

• The standard 32-bit ARM set.
• A 16-bit Thumb set.

Fig .8: ARM7 LPC2148 board

*2)Liquid Crystal Display*

Liquid crystal displays (LCDs) have materials, which combine the properties of both liquids and crystals. Rather than having a melting point, they have a temperature range within which the molecules are almost as mobile as they would be in a liquid, but are grouped together in an ordered form similar to a crystal

*3) USB Camera*

Image acquisition is considered the most critical step in our project since all subsequent stages depend highly on the image quality. In order to accomplish this, we used a CCD camera. We set the resolution to 640x480, the type of the image to jpeg, and the mode to white and black for greater details. Furthermore, we took the eye pictures while trying to maintain appropriate settings such as lighting and distance to camera. The camera is situated normally between half a meter to one meter from the subject. (3"to 10 inches)

The CCD-cameras job is to take the image from the optical system and convert it into electronic data. Find the iris image by a monochrome CCD (Charged couple Device) camera transfer the value of the different pixels out of the CCD chip. Read out the voltages from the CCD-chip. Thereafter the signals of each data are amplified and sent to an ADC (Analog to Digital Converter).

Fig.8: USB Camera

*4) GSM*

Here, a GSM modem is connected with the microcontroller. This allows the computer to use the GSM modem to communicate over the mobile network. These GSM modems are most frequently used to provide mobile Internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages. GSM modem must support an "extended AT command set" for sending/receiving SMS messages. GSM modems are a cost effective solution for receiving SMS messages, because the sender is paying for the message delivery.SIM 300 is designed for global market and it is a tri-band GSM engine. It works on frequencies EGSM 900 MHz, DCS 1800 MHz and PCS 1900 MHz . SIM300 features GPRS multi-slot class 10/ class 8 (optional) and supports the GPRS coding schemes. This GSM modem is a highly flexible plug and play quad band GSM modem, interface to RS232, it supports features like voice, data, SMS, GPRS and integrated TCP/IP stack. It is controlled via AT commands. It uses AC – DC power adaptor with following ratings DC Voltage: 12V/1A.

Fig.9 **:** GSM modem

## 5. SOFTWARE DESIGN

The software design includes the ARM7 programming code. In this project, keil µ vision and flash magic is used. Keil µ vision is used to compile the program and flash magic is used to dump the program in to microcontroller.

Matlab software is used to process Face and Iris processing

## 6.RESULT

.

Fig 10;Prototype for the project

Initially the required person information i.e.,image of thumb,iris ,face data details should be store in the memory of the controllers. Whenever ,inorder to access the output data or attendence of a particular person in the required area ,where the information of a person is predefined in the device ,need to go through the four procedure

## 7. CONCLUSION

Image quality assessment for liveness detection technique is used to detect the fake biometrics. Due to Image quality measurements it is easy to find out real and fake users because fake identities always have some different features than original it always contain different color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. Multi-Biometric system is challenging system. It is more secure than unibiometric system. In this paper studied about the three biometric systems that are face recognition, iris recognition, fingerprint recognition, and the attack on these three systems. Multi biometric system is used for various applications. And in future for making this system more secures adding the one more biometric system into this system and trying to improve the system.

## 8.FUTURE SCOPE

**I**n the proposed method, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. For future work, we intend to evaluate suchdatasets using the proposed approaches here and also consider other biometric modalities such as palm, vein, and gait.

## REFERENCES

[1]. ARM7TDMI datasheet ARM
[2]. LPC2119/2129/2194/2292/2294 User Manual Philips
[3]. ARM System on chip architecture Steve Furber
[4]. Architecture Reference Manual David Seal
[5]. ARM System developers guide Andrew N. Sloss, Domonic Symes,
[6]. Chris Wright
[7]. Micro C/OS-II Jean J. Labrosse
GCC The complete reference Arthur Griffith

**Websites**

[1]. http://www.arm.com
[2]. http://www.philips.com
[3]. http://www.lpc2000.com
[4]. http://www.semiconductors.philips.com/
[5]. http://ieeexplore.ieee.org
[6]. http://ww.hitex.co.uk
[7]. http://www.keil.co.uk
[8]. http://www.ucos-ii.com
[9]. http://www.ristancase.com
[10]. http://gcc.gnu.org/onlinedocs/gcc/Evaluation Boards And Modules
[11]. http://www.knox.com

## BIOGRAPHIES

MD. Azeema Sulthana is an M.Tech Student in Digital Electronics and Communication in Department of Electronics and Communication Engineering from SWEC (Hyderabad). Earlier she has completed her under graduation in the field of Electronics and Communication Engineering from CVSR College of Engineering (R.R District)

Shri B.J.Prem Prasanna Kumar, presently working as Associate Professor in SWEC Hyderabad (Telangana) .He has completed B.Tech degree in Electronics & communications From SV University and M.Tech degree from JNTU, He has 15 years experience.Area of interest in Communication

P.Raja Shekhar working as assistant professor in SWEC done M.Tech in JBIET(2013) Published paper on Low Power and Low Voltage Approximation Adders Implementation for Digital Signal Processing in International journal of engineering science and research