Anti-Spoofing Authentication

V.Lalitha , Divya Dharshini A , Divya B,Desu Sravya

Abstract: ***Biometrics,One Among the existing security authentication schemes, involves parts of body for identification, hence used in various fields. Due to the level of its simplicity fingerprint recognition remains popular. But the introduction of many technologies has made to lose its uniqueness by just taking a finger print scan, print it on special paper and then swipe. This project is mainly designed to new optical method, which is based on liveness detection on fingers. Infrared pulse sensor which is a new method is employed to enhance image contrast of the finger vein and to know the pattern of blood flow for liveness detection.***

Index Terms : Biometrics, Infrared pulse sensor, Android Application.

I. INTRODUCTION

Biometrics is a term for body calculations and measurements .It is the metrics relating to human characteristics. Realistic authentication or Biometrics authentication is used as a form of access control and identification .It is used as an identification for individuals in groups that are under surveillance.

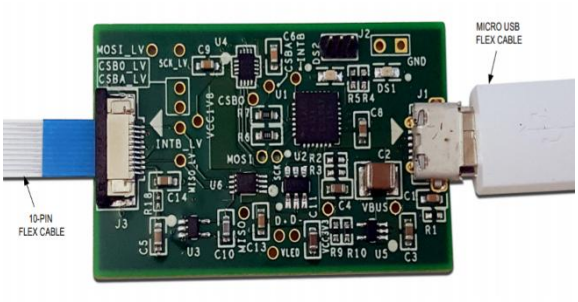
Fingerprint scanners on smartphones are not magic and certainly do not make a determination as to whether the source of the fingerprint is from a live or dead person. Fingerprint scanners on smartphones are nowhere near perfect or failsafe. The technology has been exploited, hacked and bypassed on multiple occasions. One of the first hacks, in fact, was successfully accomplished by a nine year old Chinese kid. Even after the death of the person their mobile phones can be unlocked using their fingerprint which remains intact until 2 hours from the time of their death. So the main objective is to stop recognizing the fingerprint of those persons which remains active for 2 hours after their death

Spoofing of fingerprints in android:

Apple divulged thebiometric locking and iPhone 5s with Touch ID that hackers at Chaos Computer Club (CCC) penetrated its aura of security by making the sensor using a “stolen” fingerprint.

Revised Manuscript Received on October 12, 2019.

V.Lalitha, Associate Professor in Sri Sairam Engineering College, Chennai
Divya Dharshini A, BE Computer Science,Engineering, at Sri Sairam Engineering College.
Divya B, completed BE Computer Science and Engineering, at Sri Sairam Engineering College.
Desu Sravya, completed BE Computer Science and Engineering, at Sri Sairam Engineering College.



MAX30110 :

The MAX30110 is a complete heart rate detection integrated analog front-end and optical pulse oximetry. With external LED(s) and photo diode(s), the MAX30110 offers the lowest power, highest performance heart rate detection solution for wrist applications.

II. LITERATURE SURVEY

[1] Liveness Detection On Fingers Using New Optical Methods

Various methods used for liveness detection using optical technique are discussed here.initially it gives the details about artificial or fake finger used in fingerprint recognition process and the chances of liveness detection.

Then it also comes with the details of three new methods for liveness detection—The first method is related to pulse measurement , next is related to optical characteristics variation by pressure change, the last one is based on reaction of skin to different wavelengths illumination. The last method is related to skin diseases influence in liveness detection using finger print recognition.

[2] Imaging Of Blood Flow And Finger Vein For Anti-Spoofing Authentication Using A Mems Scanner And A Laser

Trans missive vein images were captured, and then compared with those of an LED. perfusion and occlusion were used to determine blood flow patterns.the high repeatability of this scheme was due to Curvature ratios of the blood flow and finger vein intensities detection which were found to be nearly constant, regardless of the vein size.

[3] Biometrics-Technology, Application, Challenge, And Computational Intelligence Solutions

Fingerprint,Signature,Voice or combination of these Traits were used in various biometric technologies for identifying or verifying an individual. Therefore it is measurement of most unique human characteristics like both physical and behavioural. This paper mainly focuses to assist readers as they consider biometric solutions by examining common biometric technologies, introducing different biometric applications, and reviewing recent CI solutions.

[4]Finger-Vein Verification Using Multi-Features Fusion

Biometrics because of its security-related applications and the current world political scenarios, it is most important subject of deep research by academic institutions. Fingerprints are the most common biometric for identification.this paper deals with the details about last three decades research done over this topic. particularly it describes the fingerprint features that are useful for distinguishing various methods of classification that have been in to the problem. Atlastthe results from NIST special database of fingerprint classification system are presented.

[5] Finger Vein Patterns For Personal Identification Using Near-Infrared.

This demonstrates finger vein pattern as identification system which is obtained using near-infrared. Patterns of Finger vein are obtained by passing near-infrared light through a finger of 678 persons and then imaged were captured with CCD camera. then background-reduction filter are used to enhance Finger print pattern. The Similarities between the patterns are identified using Cross Correlation and tilt angle. hence finger vein pattern of 678 persons are identified successfully.

III. EXISTING SYSTEM

The iPhone scanner and other fingerprint scanners that use a similar system that is as soon as you die it would be useless. The scanner does not detect warmth; it detect electrical signals that die when you do. So in that case your fingerprint would stop working at most minutes after your death. Scanners that don't work that way would work until the integrity of your fingerprint was compromised by decomposition.

A. Constraints

Apple's Touch ID is using the following methods for identification of your fingerprint:

1) **Capacitive** – Micro magnitude voltage will pass through the Human body ,which is used by the capacitive sensor. Hence,capacitive sensor is based on the little electrical charge running through the human body. iPhone's touch screen uses this technology to detect input.

2) **Radio frequency** – Radio frequency sensor reads only the living tissue rather than responding to the dead layer of the skin.The Image of your fingerprint will be produced by the Radio frequency sensor, which means that the dead finger is useless. For dead tissues, there will be no flow of electrical charges,hence capacitive sensor cannot respond.The Radio frequency sensor will also fail because no living tissues, hence the phone cannot be unlocked.

IV. PROPOSED SYSTEM

The proposed system is using a new authentication technique where IR pulse sensor is used in combination with fingerprint sensor. The main idea is that using IR pulse sensor the pulse rate of the human is detected by passing infrared rays into blood veins. So the working of the system starts with the Enrolment of fingerprint using a button embedded on fingerprint sensor module R307.Followed by Checking for the liveness of a person using IR pulse sensor.max30100 IR pulse sensor checks the pulse rate by passing IR rays through blood veins which cannot be duplicated or created artificially, so this is the main core part of the proposed system. This is followed by registered fingerprint authentication using R307.These inputs are controlled and verified by NanoArduino.Nano Arduino sends the signal through Bluetooth module HC05 to the android mobile only if authentication is successful. If the authentication is not successful then message will not be passed via Bluetooth.so once the application developed and installed in mobile as wrapper receives the message it unlocks the mobile, else mobile remains in locked state.

Thus, using bloodflow for the detection of live veins can be considered one of the necessary steps for anti-spoofing of finger print recognition.

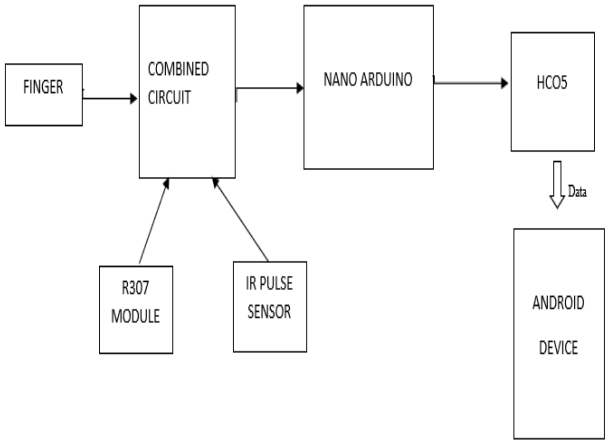
MODIFICATION

- In addition to checking fingerprints, pulse rate is also verified.
- Detects the aliveness of person.
- Stops recognizing the fingerprint of dead person completely.

V. SYSTEM ARCHITECTURE

System Architecture is the conceptual modal ,which describes the structure and behavior of the system. the architectural description of the system is the description and representation of the system,which is organized in such z way that it supports structure reasoning. The architecture diagram of a system is represented using blocks for primary functions which is then connected with the link for representing the relation ship. This implementation represents the higher level description rather than the detailed concept. It shows the relationship between different components of a system.

system components,Externally visible properties of the system components and the relation ship between them can be comprised by the System architecture.



Plan for the product production and systems development is developed by the system's architecture, which work together to implement the overall system.

VI. SYSTEM DESCRIPTION

An application software is generally implemented after complete lifecycle of project. The life cycle process include requirement analysis phase, designing phase, verification of the system, testing of the modules and finally the implementation phase of the entire system. When theoretical design is turned into practical system then implementation is an important stage of the project. Most critical stage in achieving a successful new system and to givig the confidence to the users that the system will be effective and work properly is Implementation phase. The stage include planning, Investigation, implementation, designing and evaluation. At the time of development each program is tested individually using the data and is verified that the computer system and its environment is tested to the satisfaction of the user.

The system is developed and accepted by user. the users can understand the functions clearly because of the operational procedures. The last stage involves documenting the entire system which includes the operating procedures and components of the system.

A. Modules

A modular design reduces complexity and makes the implementation easier by encouraging parallel development for different parts of system. Software which has effective modularity can be developed easily because function can be divided into compartments and interfaces are simplified. Software architecture develops modularity that is software is divided and named separately. Thus the only attribute of software that makes a program to be intellectually manageable is modularity the important novelties that make us design a method in concern with its ability to make an effective modular design are modular decomposability, composability, understandability, continuity, modular protection.

The following are the modules of the project

- Liveness detection
- Authentication procedure
- Configuring Bluetooth module
- Android application for screen lock system
- Anti-spoofing implementation

B. Module Description

Aliveness detection

- Used for detecting whether authentication is done for a live person or dead person
- Detects pulse rate by passing ir rays through blood veins
- In addition to it this also detects oxygen saturation levels.

Authentication procedure

- Checks for the registered fingerprint and pulse rate data
- Authenticates using Nano Arduino.

Configuring Bluetooth module

- After successful authentication a message is passed using hco5 Bluetooth module to mobile
- Aids in sending an input for unlocking screen to mobile

Android applications for screen lock system

- Used for development of a wrapper in mobile for unlocking the screen.
- Provides high level security.

Ant spoofing implementation

- Used for showing that the proposed system does not Work for dead persons
- Proved by artificial mould creation.

C. Module Implementation

Aliveness detection

In this module, the liveness of a person is detected by using a sensor called IR pulse sensor or pulse oximeter or max30100.This is used for detecting the pulse rate of a person by passing infrared rays into the blood vein through the finger. This show the pulse rate so we can easily conclude whether the person is alive or dead person which cannot be created artificially. This is the core part of the proposed system.

Authentication Procedure

This module is for interfacing the max30100 and R307 combined unit with Nano Arduino for authentication procedure. It is used for checking whether the pulse rate obtained is a registered person's or not using Nano Arduino which is the microcontroller. The purpose of using Nano Arduino is that it is microcontroller which is compact and has its own memory unit like ROM,RAM etc. so external

memory requirement is reduced.

Configuring Bluetooth Module

Once authentication is done Nano Arduino sends a message to mobile for

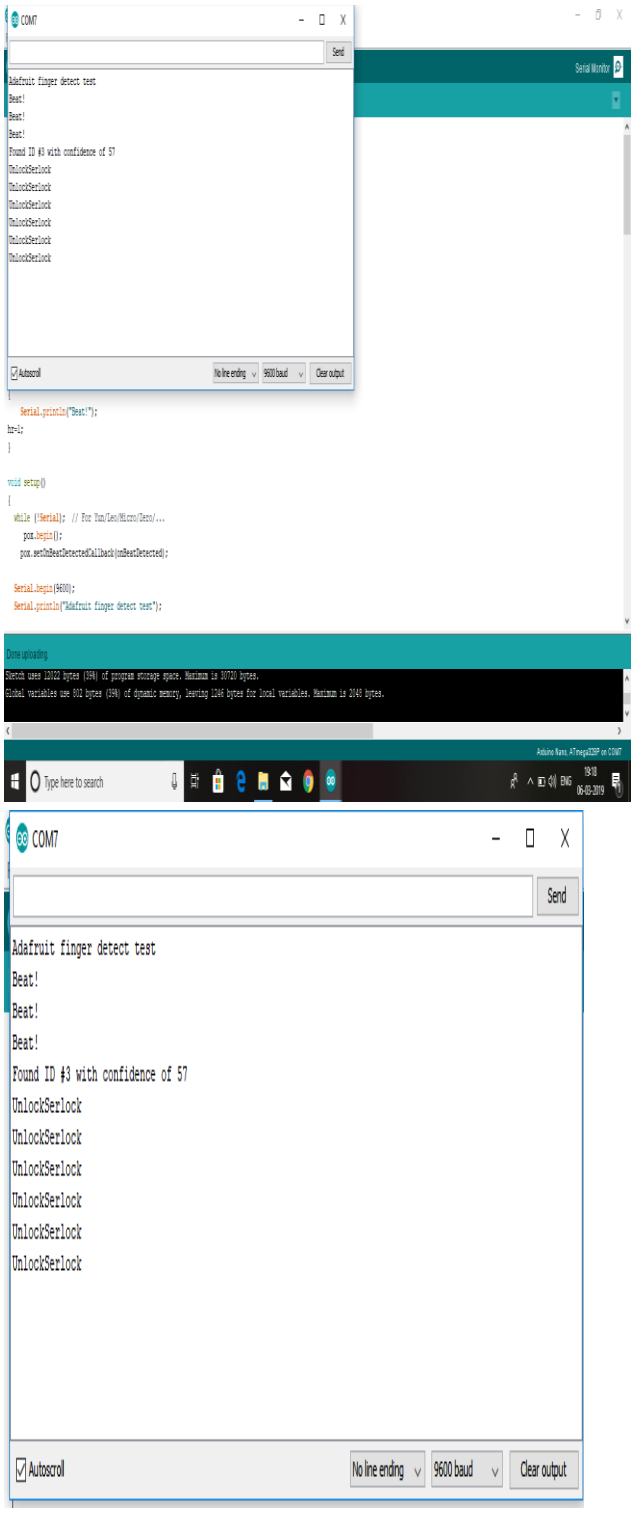
unlocking the screen. Therefore a medium is required to pass the message, sohco5 Bluetooth module is used. Hco5 is wireless serial communication network. This helps in transferring the message without delays as it used serial communication and also avoids usage of wiring since it is a wireless communication.

Android Application for Screen Lock System

This module helps Android device receiving the message via Bluetooth module by using an android application deployed in device. This application is developed in android studio which acts as a wrapper for android device to unlock the screen on receiving the message from Bluetooth module. Unless a successful authentication happens, the message won't be passed via Bluetooth module to android device. So only if authentication is successful a message is received via hco5 by the wrapper which unlocks the screen of android device.

Ant spoofing Implementation

The final module for this system is the one used in proving the difference between existing system and proposed system. Here an artificial mould is created where we print the creases of the finger. In the existing system these creases are enough to unlock the screen but in our proposed system pulse rate must also be satisfied, otherwise the screen will not get unlocked. This differentiation is proved in this module.



VII. EVALUATION OF SYSTEM

A. Advantages

1. Liveness of person is considered.
2. Prevents hacking of private details of dead person.
3. Security levels are higher.
4. Pulse rate is detected which cannot be created artificially.
5. Cheaper compared to other biometrics.
6. User friendly authentication scheme.

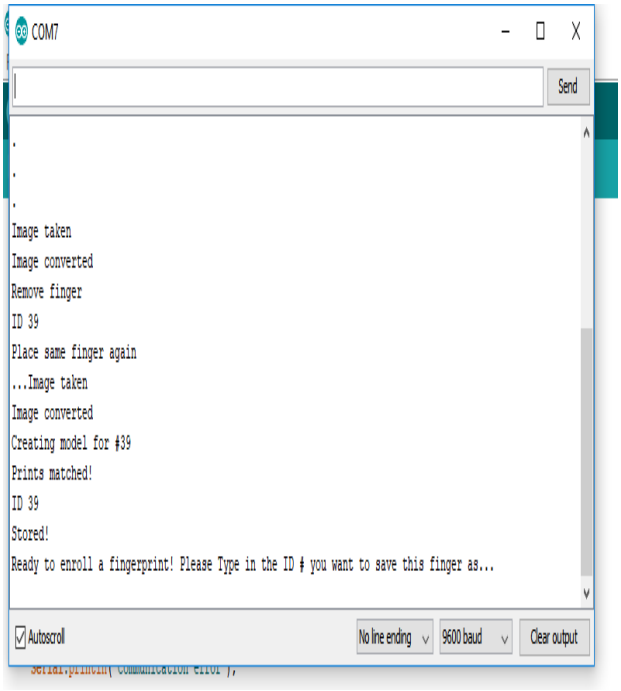
B. Disadvantages

Modification of code in Arduino editor is little difficult than other editors.

C. Applications

This idea can be used extensively in android mobiles to stop recognizing the fingerprints of dead persons.

VIII. SCREENSHOTS



IX. CONCLUSION & FUTURE WORK

Thus the project provides secure authentication using fingerprint in android devices by using IR pulse sensor. Nano Arduino, R307 Module, HC05 and mobile device application providing significant advantages like protecting information of users, unique way of authentication, easy to use and set up application. Although, this approach comes with a disadvantage like lack of integrated device for IR Pulse sensor and fingerprint module but the developed project will be useful for all the versions of android devices up to version 8.1. In future the project can be extended by the additional setup of integrated device which senses the fingerprint and checks the aliveness of fingers in a single sensor. Currently there is no such method for the integration methods so the systems will a single integrated one in future.

REFERENCES

1. Yuan, J.; Jiang, H.; Yan, W.; Cintron-Colón, H.R.; V.L.; Debauch, D.C. W.J.; Wang, J. Vessel sampling and blood flow velocity distribution with vessel diameter for characterizing the human bulbar conjunctival microvasculature. Eye Contact Lens Sci. Clin. Pract. 2016
2. Conlon, S.P , Goldman, R.; Hunt, D.; Mock, M.;.; Roth, B. Micro vein enhancer. U.S. Patent 8,255,040 B2, 28 August 2012
3. Czerniecki, B.J Choe, R.; Konecky, S.D.; Corlu, A.; Lee, K.; Durduran, T.; Busch, D.R.; Pathak, S.;.; Tchou, J.; Fraker, D.L.; et al. Differentiation of benign and malignant breast tumors by In Vivo three-dimensional parallel-plate diffuse optical tomography.
4. M. Suresh Anand, N.Mohankumar,A.Kumaresan,"An Efficient Framework for Indian Sign Language Recognition Using Wavelet Transform",Circuits and Systems, Scientific Research Publishing, Volume 7, Issue no. 8, Jun 2016
5. Kim, K.S.,Moon, S.; Lee, J.; Yun, J.; Lim, J.; Gwak, M.-J.;; Lee, J.-H. Two-Axis electrostatic gimbaled mirror scanner with self-aligned tilted stationary combs. IEEE Photonics Technol. Lett. 2016
6. Park, K.R. Pham, T.D.; Park, Y.H.; Nguyen, Kwon, S.Y.; Nonintrusive finger vein recognition system using nir image sensor and accuracy analyses according to various factors. Sensors 2015

AUTHORS PROFILE

V.Lalitha, completed Bachelor degree (B.E) in Computer Science from Madras University and Masters in Computer Science from Sathyabama University. Working as Associate Professor in Sri Sairam Engineering College, Chennai with 16 years of Experience. Area of Research is network Security and Image Processing. Life member of CSI, ISTE and IAENG.

ivya Dharshini A has completed BE Computer cience and Engineering, at Sri Sairam Engineering ollege. Her area of interest are Cyber Security, rtificial Intelligence and Virtual Reality.

Divya B has completed BE Computer Science and Engineering, at Sri Sairam Engineering College. Her area of interest are Programming in Data structures, Cyber Security.

Desu Sravya has completed BE Computer Science and Engineering, at Sri Sairam Engineering College. Her area of interest are Cyber Security, Data Analytics and Internet Of Things