International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-5, June 2021

Fingerprint Authentication

J Paul Rajasingh, D Sai Yaswanth

***Abstract:** Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics for authentication purpose. Among the existing biometric technologies are the face recognisation, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice recognition and signature recognition, Biometric method requires the physical presence of the person to be identified. This emphasizes its preference over the traditional method of identifying what you have such as, the use of password, a smartcard etc. Also, it potentially prevents unauthorized admittance to access control systems or fraudulent use of ATMs, Time Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, vehicles and computer networks. Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition.*

***Keywords**: This emphasizes its preference over the traditional method of identifying what you have such as, the use of password, a smartcard etc.*

I. INTRODUCTION

Security is the serious issue looked by everybody when we are far from our family unit. In the present situation acceptable answer for the above issue isn't yet found. Introduced here is an electronic securing framework which Arduino assumes the job of the preparing unit. Arduino which is a microcontroller board has a place with at uber family. It is an open source straight forward instrument. It can detect, screen, store and control application. Access control for the entryway is accomplished utilizing Arduino Mega 2560 board. This task displays a keyless framework for locking and opening purposes utilizing a predefined PICTURE secret key and OTP. Unauthorized person access is ensured by sending OTP and PICTURE password to ADMIN to get OTP and PICTURE password where the person needs to contact the ADMIN to get OTP and PICTURE password. It is entered through the 2.8" TFT touch display, which display all the UI messages and takes inputs from user. In case of authorized user, the system allows fingerprint sensor to validate the person followed by sending either PICTURE password or OTP via SIM using GSM module to the user registered mobile number saved in database (local SD card) in order to access the door. If the entered password matches, door will be opened automatically otherwise a message showing incorrect password will be displayed on TFT display and a notification will be sent to the owner that the security was tried to be breached.

This hardware project achieves 3 levels of security with commonly available component and also consumes less power. This system also has an option to unlock the door through SMS in case of emergency by the ADMIN.

Existing Method

A biometric system can operate in the two modes: verification and identification. In verification mode, the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be (Jain et al., 2004). Three steps are involved in personal verification. In the first step, reference models for all the users are generated and stored in the model data base. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is testing step. This process may use a smart card, user name or ID number (e.g., PIN) to indicate which template should be used for comparison. Positive recognition’ is a common use of verification mode, ‘where the aim is to prevent multiple people from using same identity’ In identification mode, the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual; the system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for ‘positive recognition’ (so that the user does not have to provide any information about the template to be used) or for ‘negative recognition’ of the person ‘where the system establishes identity’. In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for ‘positive recognition’ (so that the user does not have to provide any information about the template to be used) or for ‘negative recognition’, whether the person is he/she (implicitly or explicitly) denies to be. The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, pins or keys are ineffective (Kumar and Ryu, 2009).

Manuscript received on May 18, 2021.
Revised Manuscript received on May 24, 2021.
Manuscript published on June 30, 2021.
* Corresponding Author

J. Paul Rajasingh, Assistant Professor, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India. Email: paulrajj@srmist.edu.in

D. Sai Yaswanth*, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India. Email: saidarur@gmail.com

Retrieval Number: 100.1/ijeat.E26510610521
DOI:10.35940/ijeat.E2651.0610521
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

Proposed Method

Finger print based Authentication lock system. The core part of our project is the micro controller Arduino uno. A fingerprint sensor is interfaced to the micro controller. One motor is used for operating the door and LCD is interfaced for display. It helps to make troubleshooting easier. An alarm circuitry is provided to warn about an unauthorized use. the buttons are provided to select the mode for the fingerprint sensor.

Finger print Sensor

This is a fingure print sensor module with TTL UART interface. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC.

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template.

When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

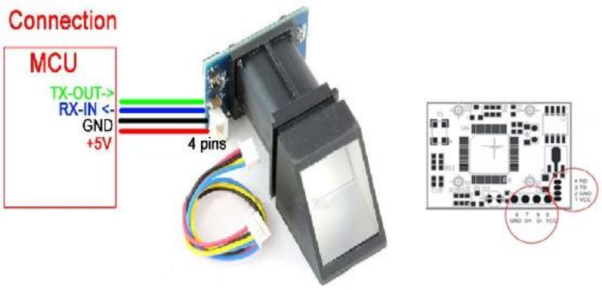

Fig: Finger print sensor

Abbreviations and Acronyms

LED : Light Emitting Diode.
VIN : The input voltage to the Arduino/Genuino board.
IOREF: Pin on the Arduino/Genuino board.
PWM : Pulse-Width Modulation.
SPI : Serial Peripheral Interface.
TWI : Two-Wire Interface.
AREF : Analog Reference.
GND: Ground pins.

Advantages & Applications

1) This system reduces the man power for the verification
2) The fraudulent which is all done automatically
3) This system can widely be used in the time of elections which can be helpful for the purpose of finding fraudulent and to count the number of people and displays
4) The user can also enroll for using the same system.
5) Immediate results
6) Highly secured

II. RESULT AND DISCUSSION

The first step is collecting the finger print using a special sensing device. This process is referred to as enrolment. In this step, the finger print is acquired for authentication. The captured image (called the finger print template) can be stored directly as an image or can be stored as a biometric algorithm. In the case of a biometric algorithm, several data points on the finger print template are scientifically measured and stored, thereby leading to discarding of the actual finger print.

III. CONCLUSION

Biometrics is a means of verifying personal identity by measuring and analyzing unique physical or behavioural characteristics like finger prints or voice patterns. It is becoming widely accepted and is slowly replacing traditional identification methods using password (Kumar and Ryu, 2009). We have designed a simple model of smart door access system using biometric finger print recognition technique. The finger print sensor, R305 uses unique biological features to take images and can store up to 128 images which reduces fraud and saves time. This device provides better security by raising alarm and indication for an emergency condition. This system can be installed in defence offices, intensive care units (ICUs), child care units (CCUs) and research laboratories, etc., where it will offer increased levels of computer user authentication security needed to protect access to sensitive information and to help identify authorised system users in the highly secured environment.

REFERENCES

1. A Review paper on biometrics implementation based on internet of things using raspberry pi Trupti Rajendra Ingale, 2017
2. A literature survey on micro-controller based smart electronic voting machine system S.V.Prasath, R.Mekala M.E. (Ph.D.), 2014
3. P. S. Pandey, P. Ranjan, M. K. Aghwariya, "The Real-Time Hardware Design and Simulation of Thermoelectric Refrigerator System Based on Peltier Effect" ICICCD 2016 DOI 10.1007/978-981-10-1708-7_66, vol. 7, pp. 581- 589, (2016). International Journal on Human and Smart Device Interaction Vol. 2, No. 1 (2015) 6 Copyright ©2015 GV School Publication
4. G. Rani, P. S. Pandey , M. K. Aghwariya ,P. Ranjan, "LASER as a Medium for Data" Transmission Proceeding of International conference on ICARE MIT-2016, Organized by Department of Mechanical Engineering, M.J.P. Rohilkhand University, Bareilly-. ISBN No.: 978-93-82972-19-8, pp. 9-11, December (2016).
5. P. Ranjan, G. S. Tomar, R. Gowri, "Metamaterial Loaded Shorted Post Circular Patch Antenna" International Journal of Signal Processing Image Processing and Pattern Recognition(IJSIP) SERSC Publication, ISSN 2005-4254, vol. 9, no.10, pp. 217-226, (2016).
6. K. Ghatak, K. Thyagarajan, "Optical Electronic", Cambridge University Press, 20 July (1989).
7. N. Q. Ngo, "A new approach for the design of wideband digital differentiator and integrator", IEEE Transactions on Circuits Systems. II: Express briefs, vol. 53, no. 9, pp. 936-940, (2006).

AUTHORS PROFILE

J Paul Rajasingh, is currently working as Assistant Professor (Senior Grade) in SRM Institute of Science and Technology, Ramapuram, Chennai. He completed his B.E(Computer Science and Engineering) from Thiagarajar college of Engineering, Madurai and M.E.(Software Engineering) from College of Engineering Guindy, Anna University, Chennai. He is currently doing Ph.D in Anna University. Having over 10 years of teaching experience, he has published papers in International Journals and Conference and handled various courses including Software Engineering, Data Structures, Operating Systems, Python Programming, Database Management Systems and Service Oriented Architecture. His area of interest includes Software Engineering, Data Analytics and Internet of Things.

D Sai Yaswanth, is currently doing with graduation final year in Computer Science engineering at SRM Institute of Science and Technology, Ramapuram, Chennai. He is good at handling front end and back end languages(python, javascript, css). His area of interest includes software developing.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.