International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Implementation of Enhanced Finger Print based Door Locking System

Alfakhri M.Murshed*[1], K. Lokesh Krishna[2], Hussam Alqubati[3], Noordin Ali[4]
*[1]Department of ECE, SVCET, Chittoor, Andhra Pradesh, India
[2]Department of ECE, S.V.College of Engineering, Tirupati, Andhra Pradesh, India
[3]Department of Computer Applications, Nizam's College, Hyderabad, India
[4] Department of CSE, SVCET, Chittoor, Andhra Pradesh, India

ABSTRACT

Security has continuously been a foremost apprehension for industrial applications, various households and across different office environments. The important parameters considered are security and safety. In this paper an enhanced fingerprint biometric system for controlling the door movement in a highly confidential area is presented. At present, the majority of door locking security systems installed across various environments suffers from various lapses. Taking this into consideration, the design and prototype of a biometric fingerprint based door locking system is demonstrated in this paper. The fingerprints of the authorized individual persons are registered separately one by one and licensed to provide access to a facility that is used by multiple users. The program is written such that any number of individual fingerprints can be added or deleted from the database based on the memory incorporated in the system. If the individual's fingerprint is matched, then the door will be opened, otherwise the GSM module gets activated automatically and a SMS message is sent to the registered user, while simultaneously the alarm also gets activated to alert the people or the security official in the surroundings. The microcontroller used in the present work is Arduino UNO R3 board. The proposed enhanced fingerprint security system is tested in real time and provides a comprehensive security solution and unauthorized individuals are prohibited from entering through the door. In contrast to the other authentication methods such as using RFI and passwords security, the proposed method has proven to be most efficient and reliable.

Keywords: Wireless, Authorization, Sensor, Speaker, Microcontroller and Switches.

I. INTRODUCTION

Recent advancements in every phase of modern living and the world around us progressively digitized, it becomes very difficult for protecting the one's confidential information. Old-fashioned passwords and keys are originally considered to be sufficient to provide secure data transactions or for any other purpose. However, in the current scenario, they became weak because of sophisticated hacker attacks and unauthorized users across the internet. With more and more number of electronic gadgets such as tablets, multiple sensors, smartphones and cloud-based services etc interconnected to internet, and with simultaneous sending and receiving of data, there arises a need to keep the data unavailable to hackers and unauthorized individuals. To prevent this, passwords can be used. However, the problem is that the user may use same password for multiple devices. In addition, these passwords are sometimes shareable and persons with strong technical knowledge can use variety of methods to crack these passwords. The latest reports of identity thefts and network security breaches assert the need for a strong authentication in the current situation [1]-[2]. Therefore, to address the need for tough, reliable and false proof personal identification, every authentication system must require a biometric component. The biometric authentication security system has become the only effective way to prove an individual's identity.

The term biometric is derived from the greek word with "bio" means life and "metric" means to measure. A biometric system is a pattern recognition system that validates an individual based on his biometric behaviors. The biometric behaviors are inborn and unique to each individual person and comprise various behaviors such as face, fingerprints, iris, voice, retina and palm vein etc. This technology fits flawlessly because it is less prone to hacking and also cannot be replicated or stolen. Moreover, it offers a lot of convenience to individuals by completely eliminating the need of typing in a password repeatedly into each device. Therefore, the biometrics is the measurement and statistical analysis of person's physical and behavior characteristics as mentioned above. So the biometric security systems can validate an individual's identity with utmost accuracy and reliability since biometric behaviors are part of the individual's being [3]-[4]. The biometric security system technology consists of four main modules: (i) a sensor that captures the samples of a biometric trait, (ii) a feature extraction module that extracts definite salient features of the biometric sample captured by the sensor, (iii) a database that stores the features extracted by the feature extraction module, and (iv) a matcher module that equalizes the features extracted from the biometric samples with the features stored in the system database.

At present, there are six major biometric technologies available in today's market. They are Fingerprint recognition, Hand geometry recognition, Iris and Retina recognition, Voice recognition, Signature recognition and Facial recognition. Of these recognition technologies, the facial recognition, finger print recognition and iris recognition are the most dominantly used for numerous applications. In this work, fingerprint recognition technology is considered.

Fingerprint recognition technology is a technique of identification based on the different patterns of human fingers, which is actually unique among each person. It is the best common way of obtaining details of any individual person and is the most easy and convenient way of identifying an individual person [5]-[6]. The scientific study of fingerprints as a means of identification of an individual person is called Dactylography. The main advantage of fingerprint recognition method is that the fingerprints pattern remains the same for an individual person throughout his/her life, making it an unfailing method of human identification.

The skin surface of any individual human finger consists of a pattern of dark lines of ridges along with white lines or valleys between them. Figure 1, shows a typical view of an individual fingerprint pattern. The structure of ridges changes at points known as minutiae and can be either split or of short length or two ridges can end on a single point. These details or patterns are unique in every individual human being. The flow of these ridges, their features, the intricate details of ridges and their sequence is what defines the information for fingerprint identification.

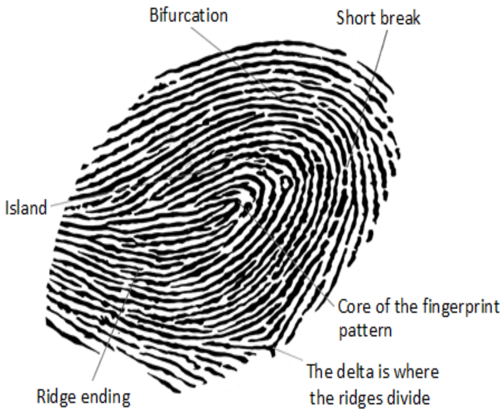
Bifurcation
Short break
Island
Core of the fingerprint pattern
The delta is where the ridges divide
Ridge ending

Figure 1. Typical view of fingerprint pattern

This paper is organized as follows. Section II discusses the design and implementation of the proposed biometric based door locking system using Arduino UNO R3. Section III explains the flowchart of the entire working process. The hardware results and prototype are presented in Section IV. Finally, conclusions are drawn in Section V.

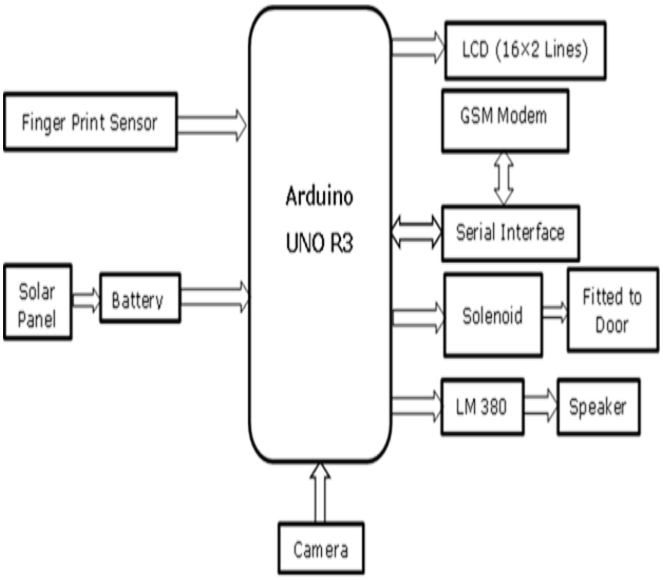

Figure 2. Block diagram of biometric based fingerprint door locking system

II. DESIGN AND IMPLEMENTATION USING ARDUINO UNO R3

The block diagram of the proposed biometric based fingerprint door locking system is shown in figure 2. In this proposed work, Arduino UNO R3 board is the main microcontroller board. Based on the written program, Independent automatic operations are carried out without human intervention.

III. FLOW CHART

When the complete system is powered ON, a welcome message is displayed on the LCD screen (16X2 lines). The flowchart of the entire process is shown in figure 3.

When an individual person put his/her, finger on the fingerprint scanner it creates an image of the ridges and valleys of the finger and distinguishes whether the individual person is authorized or unauthorized. If ridges and valleys present in the finger print matches, then the system permits the user to access next process. In the next level the system will ask for two options namely open the door and modify the user input. If option 1 is selected, the system asks for a password. So the user needs to type his/her password and the system will check whether the password given is correct or wrong. If the typed password is correct, then the solenoid valve on the door will be opened and the individual may be permitted to enter through the door. After doing this, by pressing any key, the door will automatically get closed. This entire operation of opening the door is recorded by a camera and an SMS message will be sent to the registered mobile number through GSM technology. In case if the typed password is incorrect, then a signal is sent to an alarm circuit through the LM380 power amplifier. This will alert the nearby people to get noticed. An enhanced feature is included in this proposed system in which there are options such as new individual registration, user id to be deleted, and change password which make the entire system more flexible and reliable. When option 1 is pressed, a new individual is asked to scan his finger. When option 2 is pressed, any used id will be deleted. Similarly when option 3 is pressed, the current password will be changed to a newer one. Besides these, a camera is placed in front of the door for live streaming. The stored images will be notified to the concerned individuals operating the system.

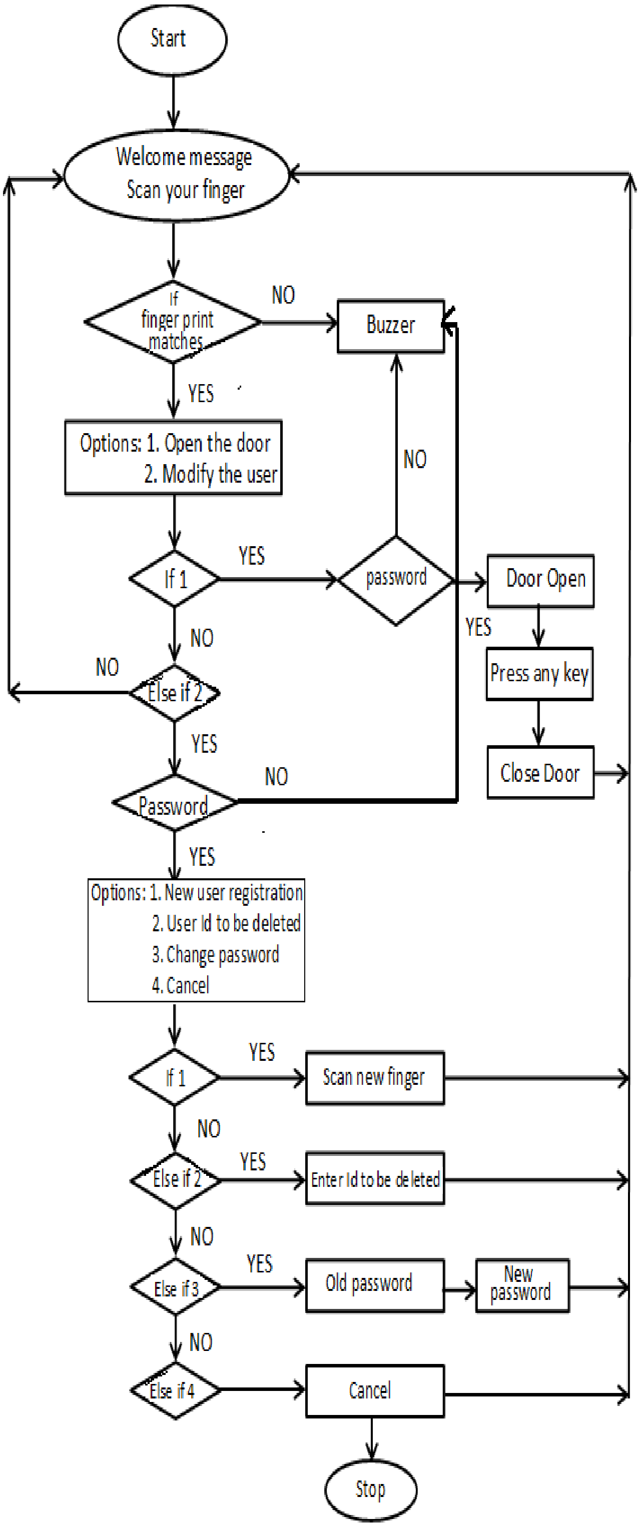

Figure 3. Flowchart of the entire process

IV. HARDWARE IMPLEMENTATION

In this proposed work, Arduino Uno R3 is the main controller. The key sensor used in this work is the optical fingerprint recognition module fingerprint reader R305. This sensor is scratch resistant with an image resolution of 500 pixels per inch. The solenoid valve is connected to the door. When the door is in locked position, no power is drawn by the solenoid valve make it power efficient. Only when authorization takes place, the solenoid valve operates and power is drawn from the supply. In case if any unauthorized individual places a finger, the system alerts through a very big sound generated by means of LM380 power connected to a speaker. Figure 4 shows a complete prototype of the biometric based fingerprint door locking system connected to permanent door, while figure 5 and figure 6 shows when the door is closed and opened.

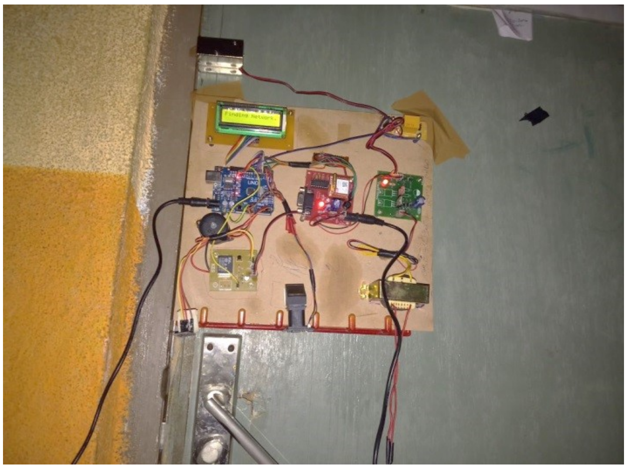

Figure 4. Prototype of the entire system

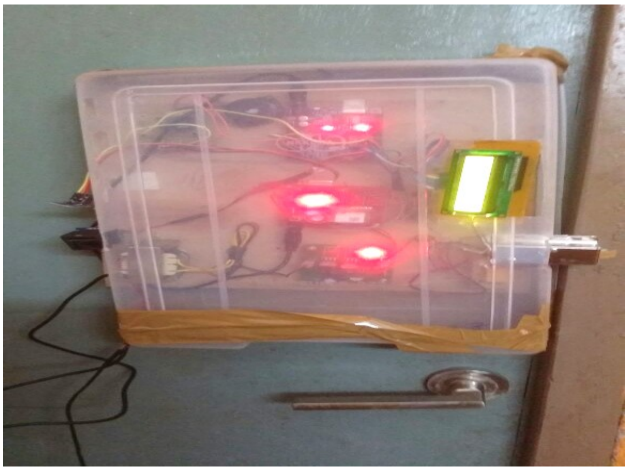

Figure 5. Door closed

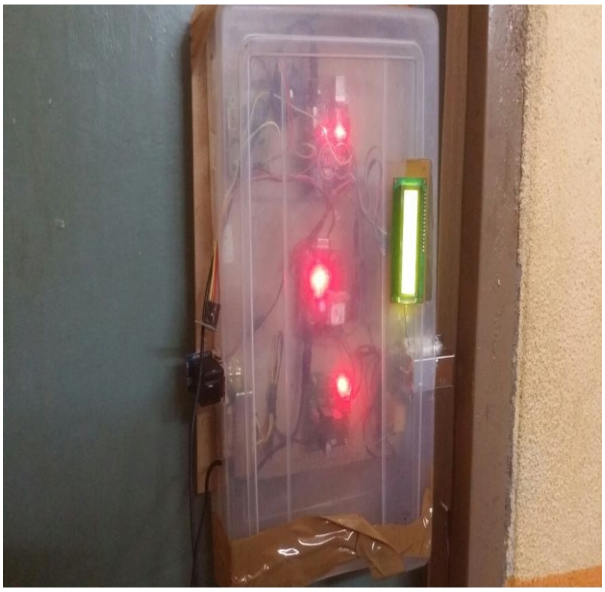

Figure 6. Door opened

V. CONCLUSION

The design and prototype of a biometric based fingerprint door locking system is presented in this paper. The proposed system is customizable and flexible. Biometrics fingerprint authorization demonstrates to be one of the best traits because the skin on our palms exhibits a flow like pattern of ridges on each fingertip which is unique and unchanged over time. This makes biometric fingerprint technology a unique identification for everyone. The proposed enhanced fingerprint security system is tested in real time, produced accurate results and further the implemented system is power efficient, flexible, highly consistent and cost effective.

VI. REFERENCES

[1]. J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6.

[2]. Y. Zhao and Z. Ye, "A low cost GSM/GPRS based wireless home security system," in IEEE Transactions on Consumer Electronics, vol. 54, no. 2, pp. 567-572, May 2008.

[3]. W. Dongdong, "Introduction of capacitive fingerprint sensor packaging technology," 2017 18th International Conference on Electronic Packaging Technology (ICEPT), Harbin, 2017, pp. 130-134.

[4]. R. Lazarick and P. Wolfhope, "Evaluation of 'non-traditional' fingerprint sensor performance," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016, pp. 1-7.

[5]. S. Palka and H. Wechsler, "Fingerprint Readers: Vulnerabilities to Front- and Back- end Attacks," 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, Crystal City, VA, 2007, pp. 1-5.

[6]. T. Ogane and I. Echizen, "Biometric Jammer: Preventing surreptitious fingerprint photography without inconveniencing users," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, 2017, pp. 253-260.

[7]. K. L. Krishna, J. Madhuri and K. Anuradha, "A ZigBee based energy efficient environmental monitoring alerting and controlling system," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-7.

[8]. C. Lin and A. Kumar, "Matching Contactless and Contact-Based Conventional Fingerprint Images for Biometrics Identification," in IEEE Transactions on Image Processing, vol. 27, no. 4, pp. 2008-2021, April 2018.