International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fingerprint Enhanced Security System

[1]Harsh Sinha, [2]Ankit Gupta, [3]Anil Maurya

[1,2] U.G Students, Electronics & Communication,
Buddha Institute of Technology, Gorakhpur, Uttar Pradesh, India
[3] Asst Prof, Electronics & Communication,
Buddha Institute of Technology, Gorakhpur, Uttar Pradesh, (India)

ABSTRACT

Security has been assuming a key part in lots of places like workplaces, foundations, libraries, research centers and so on so as to keep our information secretly so that no other unapproved individual could have an entrance on them. These days we require security frameworks for protection of profitable information and even cash. This paper displays a finger print based entryway opening system which gives security and which can be utilized for some banks, establishments and different associations etc..,. There are different techniques for validating authentication through password, RFID however this strategy is most productive and solid. To give culminate security to the bank lockers and to make the work simpler, this project is taking help of two unique innovations viz. Embedded systems and Biometrics.

Keywords- Security, Recognition, Alarm, Biometrics, Authentication, Finger print, embedded system.

I. INTRODUCTION

Individual safes are progressive locking storing cases that open with simply the touch of your finger. These items are planned as secure storing for solutions, ornamentations, weapons, reports, and other important or possibly destructive things .These use unique finger impression acknowledgment innovation to permit access to just those whose fingerprints you pick. It contains all the fundamental hardware to permit you to store, erase, and check fingerprints with simply the touch of a button. Stored fingerprints are held even in case of power failure or complete battery drain .These allocates with the requirement for monitoring keys or recalling a combination secret word, or PIN. It must be opened when an approved client is available, since there are no keys or combinations to be replicated or stolen, or bolts that can be picked. For the most part passwords, distinguishing proof cards and PIN confirmation strategies are being utilized yet the burden is that the passwords could be hacked and a card might be stolen or lost. The most secured framework is the fingerprint recognition on the grounds that a unique finger impression of one individual never coordinates the other. Biometrics normally includes fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Numerous different modalities are in different phases of advancement and evaluation. Among these accessible biometric attributes fingerprint turns out to be one of the best method for authentication.

Biometric authentication theory

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Fig1. Biometric Based Solutions

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives.

II. LITERATURE REVIEW

Individual safes are progressive locking storing cases that open with simply the touch of your finger. These items are planned as secure storing for solutions, ornamentations, weapons, reports, and other important or possibly destructive things .These use unique finger impression acknowledgment innovation to permit access to just those whose fingerprints you pick. It contains all the fundamental hardware to permit you to store, erase, and check fingerprints with simply the touch of a button. Stored fingerprints are held even in case of power failure or complete battery drain .These allocates with the requirement for monitoring keys or recalling a combination secret word, or PIN. It must be opened when an approved client is available, since there are no keys or combinations to be replicated or stolen, or bolts that can be picked.

For the most part passwords, distinguishing proof cards and PIN confirmation strategies are being utilized yet the burden is that the passwords could be hacked and a card might be stolen or lost. The most secured framework is the fingerprint recognition on the grounds that a unique finger impression of one individual never coordinates the other. Biometrics normally includes fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Numerous different modalities are in different phases of advancement and

evaluation. Among these accessible biometric attributes fingerprint turns out to be one of the best method for authentication.

III. SYSTEM DESCRIPTION

Instruction code is burned into the microcontroller using serial cable by sliding the switch in programming mode. After burning the code supply and serial cable are disconnected. Now connection is done as shown in (figure 2). LCD will display "1. Welcome, 2.User Name, 3. Add Fingerprint, 4. Clear".

Now the entries are done by a keypad, press '1' to ADD fingerprint, and press'2' to CLEAR, press'3' to SAVE and press'4' to RE CHECK.

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 fingerprint 3 to 4 times. System will process the 3 to 4 times 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.

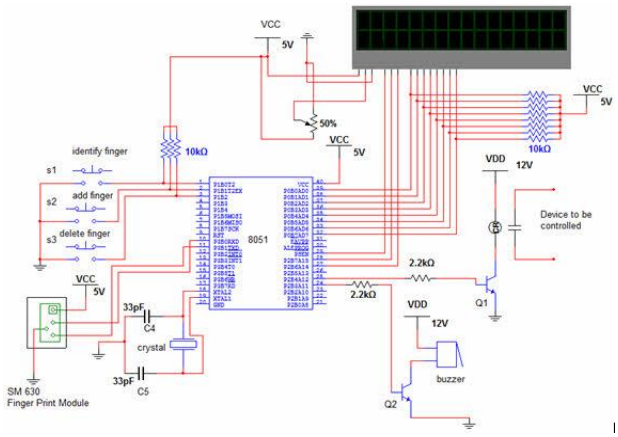

Fig-2. System Model

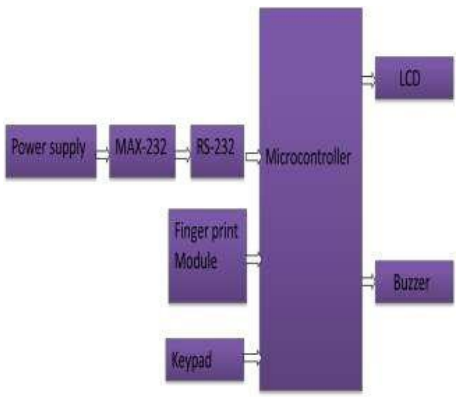

Fig.3. Block diagram

IV. DESIGN METHODOLOGY

Our proposed system overcomes all the security problems in existing system and provides high security and efficiency. This is a perfect/optimal solution for saving/protecting one from the hassle of stolen/lost key or an unauthorized entry. Fingerprint is a boon solution for these problems which provides high level of recognition accuracy. The skin on our palms and soles exhibits a flow like pattern of ridges called friction ridges. The pattern of friction ridges on each finger is unique and immutable. This makes fingerprint a unique identification for everyone. Fingerprint door lock incorporates the proven technology. Fingerprint scanner scans the fingerprints of users and used for ensuring authentication. Fingerprint scanning is more accurate and cost effective method and duplication is virtually impossible. A Fingerprint recognition system can easily perform verification. In verification, the system compares an input fingerprint to the enrolled fingerprint of a specific user to determine if they are from the same finger. Now the security of our home/office is literally in our hands or rather on our fingertips.

Microcontroller AT89S52 (figure 4)

The AT89S52 is a low power, high performance CMOS 8 bit microcontroller with 8k bytes of in-system programmable flash memory. The device is manufactured using Atmel's high density non-volatile memory technology and is compatible with the industry standard 80C51 instruction set and pin out. The on-chip flash allows the program memory to be reprogramed in-system or by a conventional non-volatile memory programmer.

Fig.4. Microcontroller AT89S52

LCD Display (16*2) (figure 5)

It has 16 columns and two rows. There are lots of combination available like 8*1, 8*2, 16*1, etc. but the most used one is the 16*2 LCD. So, it will have (16*2=32) 32 characters in total and each character will be made of 5*8 pixel dots.

Fig.5. LCD (16*2) Display

Buzzer (Security Alarm)

A buzzer or beeper is a signaling device, usually electronics, typically used in automobiles and household appliances such as microwave and gaming devices. The word "buzzer" comes from the rasping noise that buzzers made when they were electromechanical devices, operated from step down AC lines voltage at 50 or 60 cycles. Others sound commonly used to indicate the button has been pressed are a ring or a beep.

Final Design (figure 6)

The components of our fingerprint enhanced system are placed together on the PCB. The components are mounted on PCB by some spacing to avoid short circuiting with proper wiring as shown in (figure6).

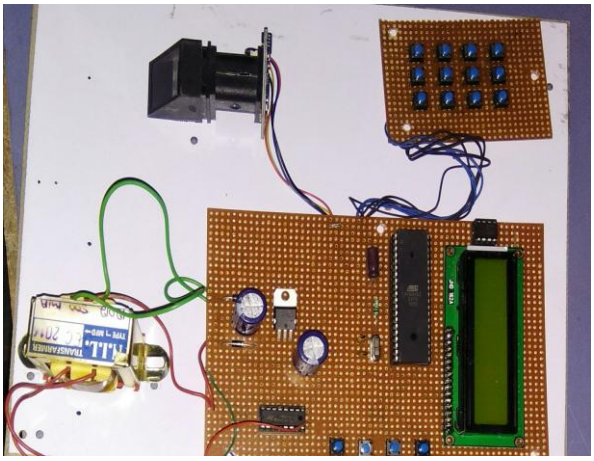

Fig.6. Final Design

V. CONCLUSION

Biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities. We have short listed a few highly popular applications of biometrics technology. Although this list is no way complete it is simply an effort to list a few of the more popular biometric applications.

- Biometrics is an emerging area with many opportunities for growth.
- Not to remember passwords.
- User friendliness.
- A new way to interact with devices.
- Biometrics can only be limited by limiting one's imagination.
- Biometric technology is now being used in almost every area.

In order to achieve desired accuracy and system performance, it is essential to fully understand all specifications and then implement a combination of existing algorithms (or a modification of them).

REFERENCES

[1]. Dey S, Samanta D. Improved feature processing for iris biometric authentication system. Inter. journal of comp. system science and engg, world academy of science.2008; 4(1):127-134.

[2]. Jain A. K., Ross A, Prabhakar S. An introduction to biometric recognition, IEEE trans. on circuits and systems for video tech., special issue on image and video-based biometrics.2004; 14(1):1-29.

[3]. NSTC Subcommittee on Biometrics, Iris Recognition, http://biometrics.gov/ documents/irisrec.pdf/. 2006. (Apr. 11, 2015).

[4]. Daugman J. How iris recognition works, IEEE trans. on circuits and systems for video tech.2004; 14(1): 21–30.

[5]. VangieBeal,http://www.webopedia.com/TERM/A/authentication.html (Apr. 12, 2015).

[6]. MargaretRouse,http://searchsecurity.techtarget.com/definition/authentication (Apr. 12, 2015).

[7]. Sullivan, Clare. Digital identity-The legal person, Computer law & security review.2009; 25(3):227-36.

[8]. http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf (Apr. 12, 2015).