Enhancing Security System using Finger Print based Authentication

Lalit Negi
M.Tech. (Student)
Dept. of Electronics Engg
YMCA University, Faridabad

Anju Gupta
Associate Professor
Dept. of Electrical Engg.
YMCA University, Faridabad

Pooja Khurana
Assistant Professor
Faculty of Engg..& Tech.
Manav Rachna International University, Faridabad

ABSTRACT
Security has been assuming a key part in lots of places like workplaces, foundations, libraries, research centres 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

1. 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 include 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.

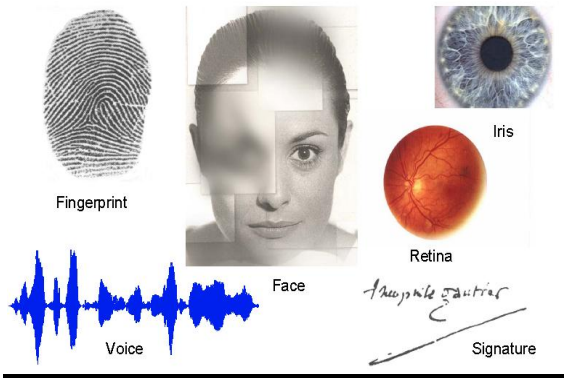

Fig. 1.Different Types of Authentication Techniques

2. BIOMETRICS
The term biometrics is derived from the Greek words bio (life) and metric (to measure).Biometrics can be defined as recognising and identifying a person based on physiological or behavioural characteristics. Biometrics is becoming an interesting topic now in regards to computer and network security. However the ideas of biometrics have been around for many years.

3. SIGNATURE IDENTIFICATION
Signature recognizable proof is the examinations of the way a client signs his or her name. The procedure utilized by a biometric framework to check a mark is called dynamic mark confirmation (DMC) [1]. The edge at which the pen is held, the quantity of times the pen is lifted, the time it takes to compose the whole signature, the weight applied by the individual while marking, the varieties in the speed with which diverse parts of the mark are composed. Favorable circumstances are, Unique for each person and client himself can choose the personality, lesser false acknowledgment rate, moderately shoddy innovation, No master preparing required.

Detriments are mark of a man may change after quite a while like if a client experienced an mishap and he can't utilize his hand and afterward he signs after quite a while, his sign and weight focuses may change, High false dismissal rate Pressure focuses may change on account of climate or some sickness. Framework can be tricked by copying Profile Database.

Fig. 2.Signature Identification

4. VOICE RECOGNISATION

Voice acknowledgement is the Identification utilizing the acoustic elements of discourse that have been found to vary between people. Focal points are Easy to utilize also, require no uncommon preparing or hardware, generally cheap contrasted with different biometrics and Purchasers like to utilize voiceprints over other biometric innovation for ID as indicated by a Pursue bank's exploration ponder. Drawbacks are When handling a man's voice over various channels such a receiver and afterward over a phone decreases the acknowledgment rate, Physical states of the voice for example, those because of infection, influence the voice confirmation handle, Environment clamor lessens the general precision and adequacy of the acknowledgment [2].The capacity necessity for voiceprint database can be huge, a man's voice changes after some time.

5. FACE RECOGNISATION

Face recognition uses the visible physical structure of the face and analyses the spatial geometry of distinguishing features in it identify an individual. Facial recognition systems have a higher relative unit cost, they do offer increased accuracy levels. Inherently the technology has a number of advantages, most notably, that it is readily acceptable by the public and relatively easy to integrate with other security systems, particularly CCTV. But development work still needs to be done to improve its performance. It needs to make allowance for the changes that occur to the human face over time - aging, facial hair, skin tone, glasses, etc. All of which could impede the recognition. Software. And technically, the affect of prevailing light conditions and the angle of the image need to be reduced, thereby allowing faster and more accurate Processing.

Fig. 3. Face Recognisation

6. IRIS SCAN

The iris is the colored ring of textured tissue that surrounds the pupil of the eye.Advantages are very high accuracy, verification timeIs generally less than 5 seconds, the eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. Disadvantages are Intrusive, a lot of memory for the data to be stored, Very expensive, difficult to use because of positioning eye requires more time for matching with database stored.

Fig. 4. Iris Scan

7. FINGRPRINT TECHNOLOGY

In the 1890s, an anthropologist named Alphonse Bertillon tried to settle the issue of distinguishing sentenced offenders and transformed biometrics into an unmistakable field of study. He created 'Bertillon age', a technique for substantial estimation which got named after him. The issue with distinguishing rehashed guilty parties was that the offenders frequently gave diverse nom de plumes each time they were capture [3]. Bertillon understood that regardless of the possibility that names changed, regardless of the possibility that a man trim his hair or put on weight, certain components of the body stayed settled, for example, the extent of the skull or the length of their fingers. His framework was utilized by police specialists all through the world, until it immediately blurred when it was found that a few people had the same estimations and in light of the estimations alone, two individuals could get regarded as one. After this, the police utilized finger printing, which was created by Richard Edward Henry of Scotland Yard. Basically returning to similar strategies utilized by the Chinese for quite a long time. There are many strides in the history of fingerprinting as an approach to recognize lawbreakers. Bertillon included fingerprinting in his framework, yet not as a critical component. An Argentine police official was the primary individual to keep unique finger impression documents [5]. He ordered fingerprints as per a framework built up by Sir Francis Galton, an anthropologist identified with Charles Darwin. Galton later distributed a book, Fingerprints that contained an order framework. In this innovation one's finger is the key i.e., one's fingerprints are utilized as the "Secret word" for ID and confirmation. Unique finger impression innovation was created by Fujitsu to help battle the expanding rate of budgetary misrepresentation and fabrication. Among these accessible biometric qualities, unique mark ends up being one of the best characteristics giving great confound proportion, high precise as far as security and additionally solid. To give idealize security and to make the work less demanding we are taking the assistance of two diverse advancements viz. installed frameworks and unique finger impression biometrics in our venture.

Fig. 5. Finger Print

8. PROPOSED 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.

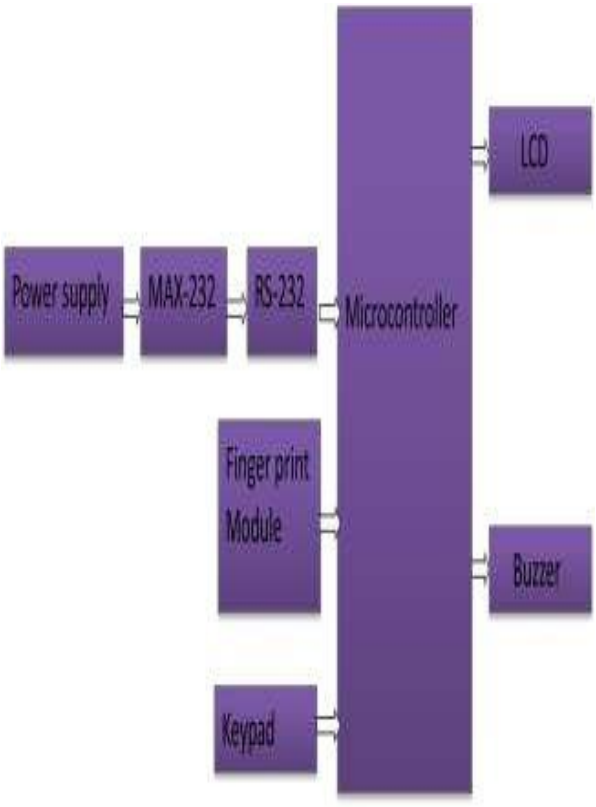

Fig.6. Proposed model of the system

9. RESULTS

Fig.7. Hardware Implementation

Fig.8. Initial display on LCD when power is on

Fig.9. Indication to scan the Finger

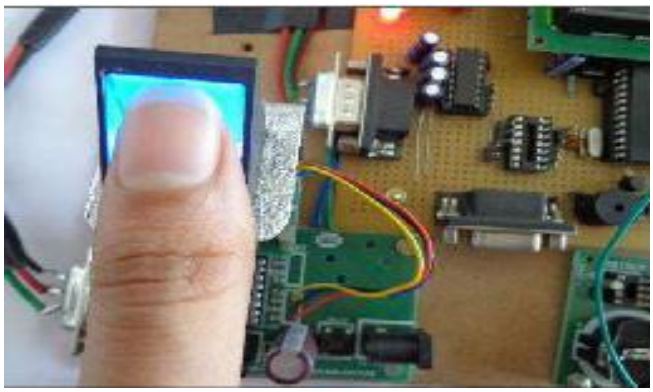

Fig.10. Scanning the Finger

10. REFERENCES

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[2] International Journal of Advanced Research in ComputerScience and Software Engineering, Volume 2, Issue 10,October 2012.

[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).

[4] R. A. Fisher Biometrics, Vol. 20, No. 2, In Memoriam: Ronald Aylmer Fisher, 1890-1962 (Jun., 1964), pp. 261-264.

[5] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[6] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[7] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar "Wireless Fingerprint Based Security System using Zigbee" , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.

[8] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[9] "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, Department of Computer Science and Enginnering, Michign State University Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[10] John Wharton: An Introduction to the Intel MCS-51TM Single-Chip Microcomputer Family, Application Note AP-69, May 1980