Fingerprint based locking system

Ajinkya Kawale

Abstract—Fingerprint recognition technology allows access to only those whose fingerprints that are pre stored in the memory. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since there are no keys or combinations to be copied or stolen, or locks that can be picked.
The fingerprint based lock therefore provides a wonderful solution to conventionally encountered inconveniences. This report focuses on the use of fingerprints to unlock locks, as opposed to the established method of using keys.

Index Terms— Fingerprint, Interfacing, Locking system, Microcontroller

1 Introduction

Biometric systems have overtime served as robust security mechanisms in various domains. Fingerprints are the oldest and most widely used form of biometric identification. The use of fingerprint for identification has been employed in law enforcement for about a century. A much broader application of fingerprint is for personal authentication, for instance to access a computer, a network, an ATM machine, a car or a home.

Electronic lock using fingerprint recognition system is a process of verifying the fingerprint image to open the electronic lock. This project highlights the development of fingerprint verification.Verification is completed by comparing the data of authorized fingerprint image with incoming fingerprint image. Then the information of incoming fingerprint image will undergo the comparison process to compare with authorized fingerprint image.

In this project, digital image processing algorithms is employed to indentify whether the incoming fingerprint image is genuine or forgery**.**

2 Statement of the Problem

The main aim of this project is develop a secure locking system based on fingerprint scanning. In this project, microcontroller accompanied with an interface circuit has been used for opening and closing lock based on finger print which is stored in microcontroller itself so that only authorized person will access the security lock.

3 Definition of Terms

3.1 Fingerprint

Fingerprints are patterns of ridges and valleys on the surface of the finger. Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events.

3.2 Minutiae Based Approach in Fingerprint Recognition

In practice only ridge ending and ridge bifurcation minutiae types are used in fingerprint recognition Fingerprint recognition systems based on minutiae consist mainly of three stages: Image acquisition/pre-processing, locating the minutiae, and comparing the minutiae list of both fingerprints, often solved as a constrained graph matching problem.Minutiae-based matching is highly robust against nonlinear fingerprint distortion, but shows only limited capability for recognizing poor-quality fingerprint images due to unexpected fingertip conditions (e.g., dry fingertips, rough fingertips, allergic-skin fingertips) as well as weak impression of fingerprints.

3.3 Interfacing Microcontroller

Interfacing is a method to establish communication between Microcontroller and the Interface**.** Various interfaces are listed above. These interfaces are generic and can communicate with any microcontroller. Interfacing is a combination of hardware (i.e. the Interface) and Software (i.e. the source code to communicate, also called as the Driver**).** In simple words, to use LED as output device, LED should be connected to a port pin of the microcontroller and there has to be a program running inside the microcontroller to make it On or Off or blink or dim. This program is called as the driver and can be developed using any programming language like Assembly, C, Basic etc.

4 Theoretical Framework

The system can be divided into the following Modules: fingerprint analysis software module that accepts fingerprints images; hardware interface module and the locking system module.Stepwise break-up of execution plan is as follows-

- Study of biometrics literature -specially with reference to fingerprint analysis.
- Study of basics of image processing algorithms so as to compare images with the point of view of uniqueness of fingerprints.
- Cogitation of MATLAB as a programming tool for image processing and comparing .

• *Author name is currently pursuing bachelors degree program in electronic engineering in Nagpur university, PH-+919763195577. E-mail: ajinkya.d.kawale@gmail.com*

- To make a guiding flowchart to enforce the above studied algorithm.
- Translating this flowchart into C embedded code and simulating the software to check
- for expected results.
- Interfacing the Fingerprint scanner module with micro-controller.
- Modifying the control circuit (in the locking system) so as to connect it with above designed hardware.
- Finally testing the circuit for expected results.

5 FUTURE SCOPE

Fingerprint based locks are revolutionary locking systems that open with just the touch of authorised user's finger; their increased use in various locking applications can actuate what would be known as 'Keyless World'.

- A fingerprint mismatch can be conveniently regarded as an attempt of illegal access In the wake of such unratified event, an adjunct siren alarm may be initiated to reveal possible theft.
- For systems demanding more security, such as expensive jewellery items or museum articles, scanning of multiple fingerprints may be employed.

6 CONCLUSION

The prototype system can be divided into the following modules: fingerprint analysis software module (employing digital image recognition algorithms) that accepts fingerprints images; hardware interface module (utilizing a microcontroller and a interface control circuit) and the locking module. In actual implementation, the fingerprint data will be recorded using a fingerprint scanner.

The fingerprint Recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database in the form of stored samples in bmp, tiff, tiff, jpg, jpeg, gif type image files.

So before any user can unlock or ignite the vehicle, his/her fingerprint image is matched against the fingerprints in this database while users with no match in the database are denied access to the system. Biometric method requires the physical presence of the person to be identified.

Thus, biometric recognition systems offer greater security and convenience than traditional methods of personal recognition.

REFERENCES

[1] Koichi I., Ayumi M., Takafumi A., Hiroshi N., Koji Kobayashi, and Tatsuo H. (2005) "A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-BasedMatching", http://www.aoki.ecei.tohoku.ac.jp/~ito/cr2114.pdf -00

[2] Anton S. (2002) "Sorting it out: Machine learning and fingerprints", Paper presented at the seminar on Telematik fingerprint, Siemens Corporate Technology, Munich, Germany.

[3] Graevenitz G.A. (2003) "Introduction to fingerprint technology", A&S International, Vol. 53,pp. 84 – 86.

[4] Thai R. (2003) "Fingerprint Image Enhancement and Minutiae Extraction", Unpublished B.Sc Thesis, School of Computer Science and Software Engineering, The University of Western Australia, Australia

[5] http://www.crimtrac.gov.au/fingerprintanalysis.htm, "Fingerprint Analysis – The Basics"

[6] http://www.biometricinfo.org/fingerprintrecognition.htm,"Biometrics Information Resource"

[7] http://webfealb.fea.aub.edu.lb/dsa/labs/projectv1.1.pdf

[8] http://www.computer-.howstuffworks.com/fingerprintscanner.htm

[9] http://www.computer.howstuffworks.com/fingerprintscanner.htm

[10] http://www.crimtrac.gov.au/fingerprintanalysis.htm