International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Secure Flash Drive (using Fingerprint Sensor)

Ashish Kumar Gupta[1], Dr. Anshuman Tyagi[2]
[1]*Electrical & Electronics Engg. Student, PSIT, Kanpur, India*
[2] *Electrical & Electronics Engg, Asso. Prof, PSIT Kanpur*

Abstract: The study demands the user to submit his Finger print to access the pen drive. This uses the Finger print technology and Embedded Systems to design this application. The main objective of this is to design a system that asks the user to show his Finger print as identity proof. The system reads the data from the Finger print and verifies this data with the already stored data in its database. If the details present in the data base it matches with the stored data, the system allows the person to enter into and access the information from drive. If the details of the Finger do not match with the stored data, the system cannot be able to access the pen drive.
This is a device that collects data from the tag and codes the data into a format that can be understood by the controlling section. This system also collects information from the master device and implements commands that are directed by the master.
The objective of the project is to develop a microcontroller based security system. It consists of a Finger print reader, microcontroller, the interfacing unit to allow the communication between the microcontroller and Finger print module, and the LCD.

I. INTRODUCTION

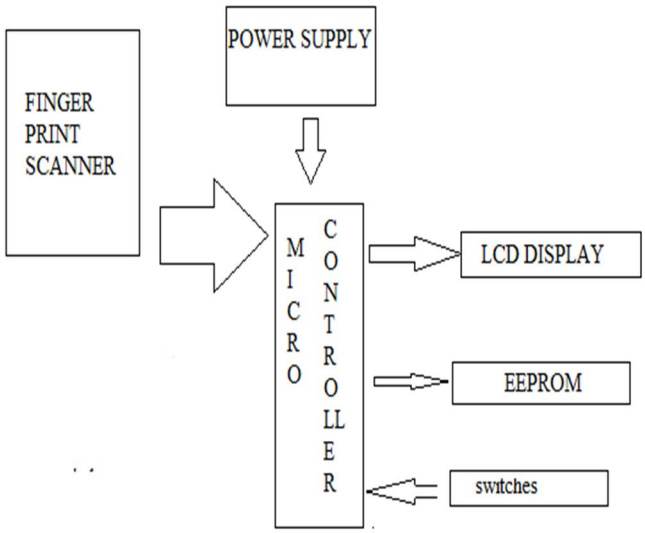
This demands the user to submit his finger on sensor to sure that person is authorized to start the data transfer.
This examines policy regarding the electronic approaches and developments towards electronic data storage and transmission. This Finger print reader reads the details from the tag. This data is passed to the controlling unit for the verification. The controller reads the data from the reader and compares this data with the already existing data. If the data matches with the already stored information, the person is allowed to access the pen drive. If not, a message is displayed on LCD and the person is not allowed to access the pen drive.
The software application and the hardware implementation help the microcontroller read the data from the Finger print verify the data with the already stored data and take the next action. The system is totally designed using Finger print module and embedded systems technology.
The Controlling unit has an application program to allow the microcontroller interface with the Finger print module, the reader eads the data from the tag, passes the data to the microcontroller and the controller verifies this data with the already existing data in the controller's memory and then implement the commands directed by the controller section. The performance of the design is maintained by controlling unit.

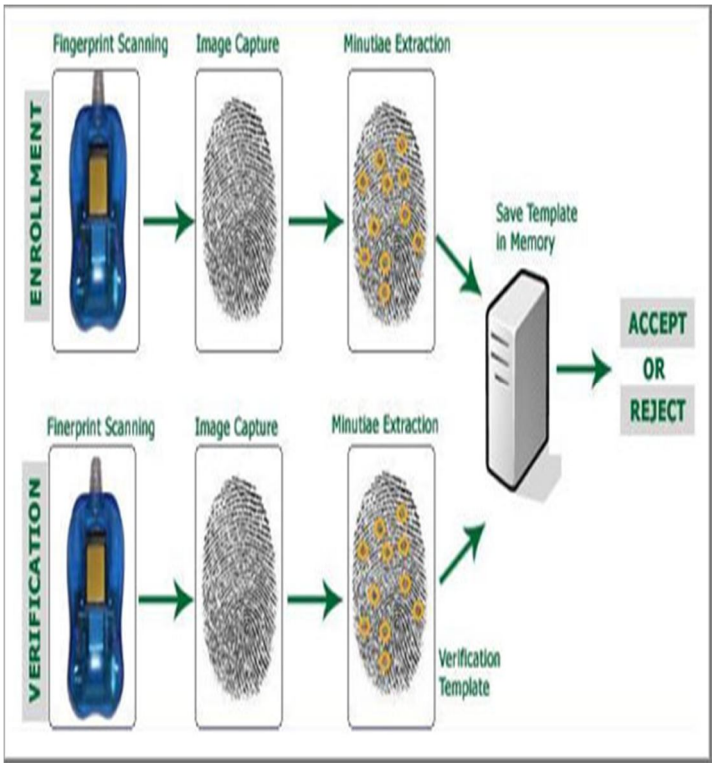
II. OVERVIEW OF THE TECHNOLOGIES

The implementation of the project design can be divided in two parts.

A. Hardware implementation
B. Firmware implementation

Hardware implementation deals in drawing the schematic on the plane paper according to the application, testing the schematic design over the breadboard using the various IC's to find if the design meets the objective, carrying out the PCB layout of the schematic tested on breadboard, finally preparing the board and testing the designed hardware.
The firmware part deals in programming the microcontroller so that it can control the operation of the IC's used in the implementation. In the present work, we have used the Or-cad design software for PCB circuit design, the Keil µv3 software development tool to write and compile the source code, which has been written in the C language. The Flash main programmer has been used to write this compile code into the microcontroller.
The project design and principle are explained using the block diagram and circuit diagram. The block diagram discusses about the required components of the design and working condition is explained using circuit diagram and system wiring diagram.





Working can be explained further, This system operates by given a input by the finger print sensor and the matching is done by the finger print module if the input is matched ,the microcontroller generates a signal and it allows the transferring the data from the host computer and the data traveler .

C. This system has two modes

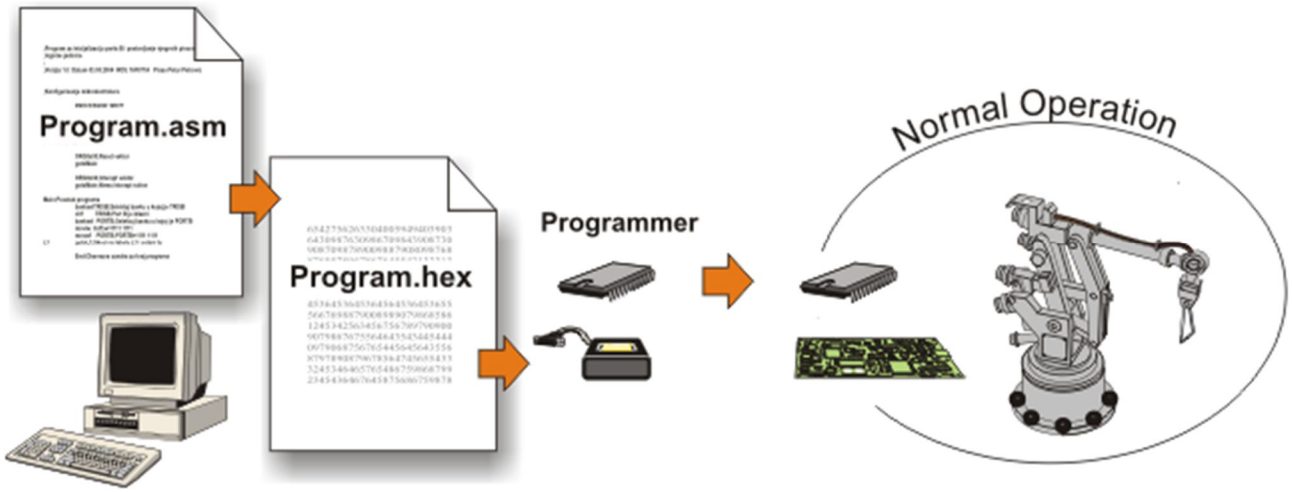
1) Add mode

2) Search mode

In add mode the finger print is added (up to 6) In search mode the i/p finger print is search in the stored data (template). And if it is matched the signal is generated by the microcontroller and allows the data transfer and display on LCD i.e. FINGER PRINT IS MATCHED If not matched then display on LCD finger print not matched

D. Programming A Microcontroller

Microcontrollers and humans communicate through the medium of the programming language called Assembly language. The word Assembler itself does not have any deeper meaning, it corresponds to the names of other languages such as English or French. More precisely, assembly language is only a passing solution. In order that the microcontroller can understand a program written in assembly language, it must be compiled into a language of zeros and ones. Assembly language and Assembler do not have the same meaning. The first one refers to the set of rules used for writing program for the microcontroller, while the later refers to a program on a personal computer used to translate assembly language statements into the language of zeros and ones. A compiled program is also called Machine Code. A "Program" is a data file stored on a computer hard disc (or in memory of the microcontroller, if loaded) and written according to the rules of assembly or some other programming language. Assembly language is understandable for humans because it consists of meaningful words and symbols of the alphabet. Let us take, for example the command "RETURN" which is, as its name indicates, used to return the microcontroller from a subroutine. In machine code, the same command is represented by a 14-bit array of zeros and ones understandable by the microcontroller. All assembly language commands are similarly compiled into the corresponding array of zeros and ones. A data file used for storing compiled program is called an "executive file", i.e. "HEX data file". The name comes from the hexadecimal presentation of a data file and has a suffix of "hex" as well, for example "probe.hex". After has been generated, the data file is loaded into the microcontroller using a programmer. Assembly language programs may be written in any program for text processing (editor) able to create ASCII data files on a hard disc or in a specialized work environment such as MPLAB described later.



III. CONCLUSION AND DISCUSSION

The information that can be transfer and which is an important that cannot be accessed by any other person it can be accessed by only authenticated person. Hence the data is secure. I make the system which is used for the purpose of secure the data transfer using flash drives by the authentication of authorized person bio-metric.

REFERENCES

[1] "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Archived from the original on 7 January 2012. Retrieved 2012-06-10.

[2] "What is Biometrics?". Biometrics Research Group. Michigan State University. Retrieved 10 November 2017.

[3] Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91–98. doi:10.1145/328236.328110

[4] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[5] Damaševičius, R.; Maskeliūnas, R.; Venčkauskas, A.; Woźniak, M. Smartphone User Identity Verification Using Gait Characteristics, Symmetry 2016, 8, 100.

[6] "Biometrics for Secure Authentication" (PDF). Archived from the original (PDF) on 25 March 2012. Retrieved 29 July 2012.

[7] Weaver, A. C. (2006). "Biometric Authentication". Computer, 39 (2), p. 96–97. DOI 10.1109/MC.2006.47

[8] Jain, A. K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.

[9] Bleicher, Paul (2005). "Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity". Applied Clinical Trials.

[10] Sahoo, SoyujKumar; Mahadeva Prasanna, SR (1 January 2012). Mahadeva Prasanna, SR, Choubisa, Tarun. "Multimodal Biometric Person Authentication : A Review". IETE Technical Review. 29 (1): 54. doi:10.4103/0256-4602.93139. Archived from the original on 17 September 2013. Retrieved 23 February 2012.Missing |last2= in Authors list (help)

[11] Zahid Akhtar, "Security of Multimodal Biometric Systems against Spoof Attacks", Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6 March 2012.

[12] "Characteristics of Biometric Systems". Cernet. Archived from the original on 17 October 2008.

[13] The History of Fingerprints.

[14] Josh Ellenbogen, Reasoned and Unreasoned Images: The Photography of Bertillon, Galton, and Marey (University Park, PA, 2012)

[15] Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in Critical Inquiry 41:4 (Summer, 2015), 841–868.

[16] Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in Critical Inquiry 41:4 (Summer, 2015), p. 853.

[17] David Lyon, Surveillance Society: Monitoring Everyday Life(Philadelphia, 2001).

[18] A. Rattani, "Adaptive Biometric System based on Template Update Procedures", PhD thesis, University of Cagliari, Italy, 2010

[19] R. Palaniappan, "Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population", published in E. Corchado et al. (eds): Intelligent Data Engineering and Automated Learning – IDEAL 2006, Lecture Notes in Computer Science, vol. 4224, pp. 604–611, Springer-Verlag, Berlin Heidelberg, 2006. DOI:10.1007/11875581_73]

[20] R. Palaniappan, and S. M. Krishnan, "Identifying individuals using ECG signals", Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp. 569–572, 11–14 December 2004. DOI:10.1109/SPCOM.2004.1458524]

[21] Langston, Jennifer (8 May 2015). "Researchers hack Tele operated Surgical Robot to Reveal Security Flaws". Scientific Computing. New Jersey. Retrieved 17 May 2015.