

Wireless Fingerprint Based Security System Using Zigbee Technology

Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar

Abstract - Among the huge requirements, the one and only one requirement which has a vital importance in our daily life is "Security". It may be for application, information, data, network, home, financial, and national security like parliament etc. In this present day we have already several type of security system like CCTV, barcode, identity card etc. which is based on the various type of technology and has tedious processing, which is long time taking, highly expensive, less percentage of securing, not widely used, chance of hacking and destroy or altered easily. Due to this dearth the present security system is unable to fulfil our best security. In this paper we propose a wireless fingerprint security system based on Zigbee technology to overcome above dearth. This system is based on the taking fingerprint of a user with the help of a fingerprint sensor module and matching it with the database details corresponding to the user fingerprint and displays it on the computer screen. This security system has a better percentage of security with respect to other security system available. Apart from this it is fast processing, less expensive, better portability and a little bit chance of hacking, alter and copy of information between source and database.

INDEX TERMS- Database, Fingerprints Sensor Module, Fingerprints Verification, Zigbee Technology.

I. INTRODUCTION

A Fingerprint, as the name suggests is the print or the impression made by our finger because of the patterns formed on the skin of our palms and fingers. It is fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual. Each of our ten fingerprints is different from one another and from those of every other person. Even identical twins have unique finger-prints. That makes them ideal for personal identification. With age, these marks get prominent but the pattern and the structures present in those fine lines do not undergo any change. For their permanence and unique nature, they have been used for not only in identification but also in the field of security as criminal and forensic investigation for a long time. Every fingerprint consists ridges and furrows where the ridges are thick lines while the furrows are space between two ridges. But we can't distinguish the fingerprints of two persons on the basis of ridges and furrows because it has some similarities between the fingerprints of different persons.

Manuscript received April, 2013.

Mukesh Kumar Thakur, Electronics and Communication Engineering, Bengal College of Engineering and Technology, Durgapur, India.

Ravi Shankar Kumar, Electronics and Communication Engineering, Bengal College of Engineering and Technology, Durgapur, India.

Mohit Kumar, Applied Electronics and Instrumentation Engineering, Bengal College of Engineering and Technology, Durgapur, India.

Raju Kumar, Electronics and Communication Engineering, Bengal College of Engineering and Technology, Durgapur, India.

To overcome these things we use minutiae extraction method, a minutiae have some abnormalities in a ridge and furrow.

Minutiae are an unique points on the ridge usually they are the termination and bifurcation of ridges and also the other minutiae points which are combination of these two, like crossover, core, island, delta and pore . The whole information about the fingerprint is obtained by the location of minutiae points present in the fingerprint. For getting details about fingerprints these minutiae points are converted into the digital codes and it is matched with the code of relevant fingerprint in required database.



Fig .1: Image of a Fingerprint

We are going to represent an example of this wireless fingerprint based security system for the national security like parliament security of a nation to prevent an unauthorised person to enter into the parliament house because an unauthorised person may enter by easily manipulating the security guard or any other manual security system. For entering, a person can scan their finger on the fingerprint sensor module at the important entry place of the parliament house in perfect manner. If their fingerprint matched with the fingerprints of the database which has made for parliament authorised person, then the person can enter otherwise they will be denied. The matching process of the fingerprint of a person to the database is done automatically using biometric architecture as shown below.

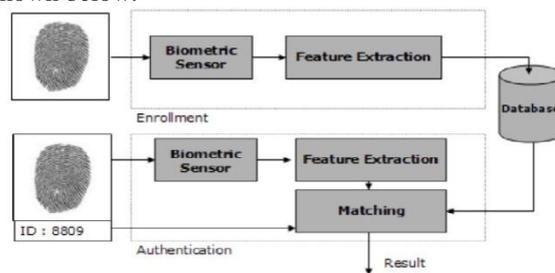


Fig 2: General architecture of biometric system

II. PREVIOUS WORK

Generally the previous security systems use the manual based security system like CCTV (closed circuit television camera), alarm, security lighting, security card, security code and security guard. These manual methods are more expensive and can be easily altered or manipulated. In the case of security code and card it can be forgotten, hacked and altered by another person.

III. SYSTEM OUTLINE

A. Hardware Architecture

A fingerprint scanner, LCD display, Zigbee device and a Personal Computer will be used as hardware in this project. Where the finger print scanner scan a finger of a person and sends its image to the Zigbee device through a USB connection while the Personal Computer(PC) houses the database and runs some relevant application to compare and matching the database fingerprints to the scanned fingerprint. LCD display will be displaying accurate all database details information about the relevant person with the help of a connection to the PC. After matching the database is updated automatically.



Fig.3: USB Fingerprint Scanner Module

B. Software Architecture

In this system we are using software architecture as Database and Application Program.

Database:The database consists of tables that stores records implemented in Microsoft SQLServer database. However, this can be migrated to any other relational database of choice. SQLServer is fast and easy, it can store a very large record and requires little configuration.

Application Program:The application program is developed with Microsoft C# programming language using Microsoft Visual Studio framework and it provides a user interface for the security system. The advantages of Microsoft C# programming language are its robustness, easy to program, has an excellent database connectivity, runs on the two most common operating system platforms (Windows and Unix) and it has a larger user community that provides online support.

C. Zigbee Technology

In this project we are using Zigbee Technology for the purpose of wireless communication between fingerprint sensor module and the PC. This technology was developed for a wireless personal area networks (PAN), aimed to control low data rate and low power consumption. In this technology we can use application of both WI-FI and Bluetooth. It relies upon IEEE 802.15.4, which has excellent performance in low SNR environments. It is a specification for a suite of high level communication protocols. Using small, low-power digital radios based on an IEEE 802 standard for personal. Its devices are often used

in mesh network form to transmit data over longer distances, passing data through intermediate devices to reach more distant ones and also device can be tasked with running network. It is targeted at applications that require a low data rate, long battery life and secure networking. It has a defined rate of 250kbit/s, best suited for single signal transmission from a sensor or input device.

IV. AUTOMATIC SECURITY SYSTEM AND DATABASE MANAGEMENT

Figure 4: shows the synopsis of automatic security system which is implemented at important entry places. Database storage contains the fingerprint templates of persons along with their all details information (e.g. – photo, fingerprint, name, age, sex, identification mark, permanent address etc.). When a person scans their finger over the fingerprint sensor module then fingerprint verifying machine verify the fingerprint and it is send to wireless communication module which is already connected with pc workstation through Zigbee wireless device. Now the fingerprint is analysed with database at pc workstation. After analysing process the workstation sends both the information matched and denied which is depends on analysing result, to the fingerprint sensor module screen through the same wireless communication path, hence the identification takes place. Database is designed in such a manner that it can be updated manually and automatically for a period of time and also we can add new entry and remove previous information of a person when it needed.

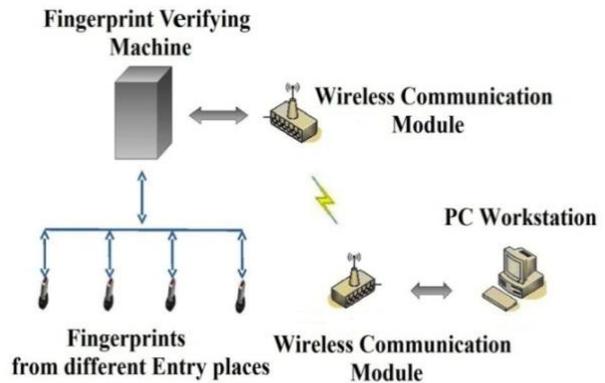


Fig 4: Synopsis of Automatic Security System

V. RESULT

This system has been verified to observe the 251 authorised and 10 unauthorised people for entry into the parliament. In case of authorised, 250 identification have been identified successfully and only one identification didn't recognize due to their wrong manner of giving fingerprint and in case of unauthorised person all person have been successfully denied. Accuracy in both situations is shown below (Table. 1&2).

A. For Authorised Person

Table No.1

No. of person	Successful Identification	Unsuccessful Identification	Accuracy
251	250	001	99.6%

B. For Unauthorised Person

Table No.2

No. of person	Successful Identification as Denied	Unsuccessful Identification	Accuracy
10	10	00	100%

Here an example of Database result for an authorised and unauthorised person is shown.

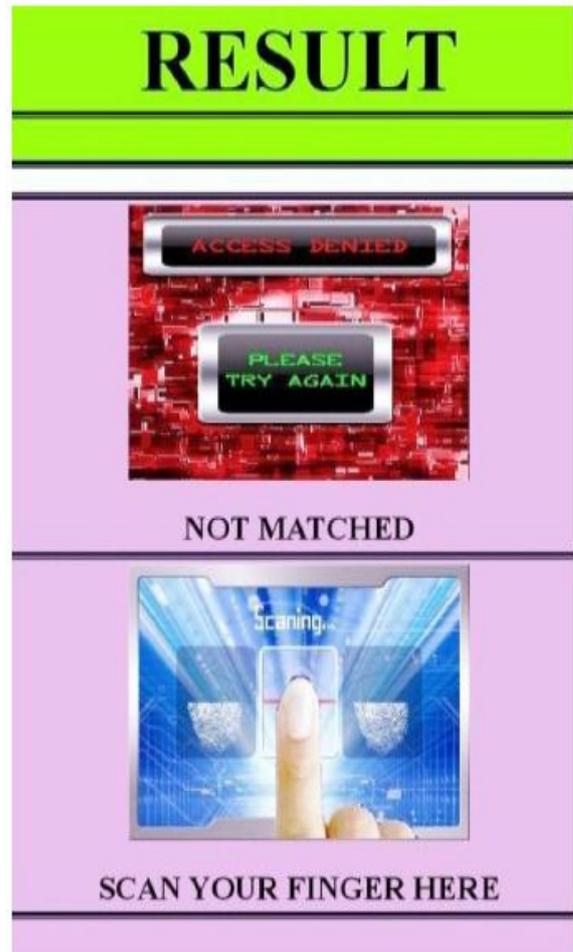
A. In matching condition



The above database details of an authorised person is shown on a LCD display at the main control room of the parliament

house that may be used for other purpose as sending this details to the important place through internet connection.

B. In not matching condition



VI. CONCLUSION

The proposed approach uses the technique which combines a unique biometrics and the concept of wireless communication. Fingerprint provides a solution for protecting the privacy of the user; since the user's true biometric feature is never changed in the whole life. Fingerprint is used for the better security and accuracy. In the privacy and security domains, the proposed method fulfils all requirements as to reject a forged person. The proposed technique makes it computationally hard to invert the transformed template without presenting the unique personal key as input fingerprint. From the results obtained it is clear that the proposed approach provides very high accuracy. Thus the approach is very much secured. Thus the system provides a substantive improvement over recognition of a person based purely on biometric feature. This approach can be enhanced to higher level in order to further improve the security. This common wireless security system can be extended in future by using several different types of required database that will be very hard to break by the attackers and thus it can provide better security.

VII. ACKNOWLEDGMENT

The authors are thankful to IJEAT for giving them the opportunity to present their research work.

REFERENCES

- [1] M. Lourde R, D. Khosla, "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.
- [2] G.Sambasiva Rao, C. NagaRaju, L. S. S. Reddy and E. V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", International Journal of Computer Science and Network Security.
- [3] International Journal of Engineering and Advanced Technology (IJEAT). ISSN: 2249 – 8958, Volume-2, Issue 3, February 2013. 201. "Wireless Fingerprint Based College Attendance System using Zigbee Technology"
- [4] www.ijecse.org/wp-content/.../08/Volume-1Number-3PP-872-878.pdf
- [5] www.iiste.org/Journals/index.php/CEIS/article/download/580/469
- [6] A. K. Jain, U. Uludag and A. Ross, "Biometric Template Selection: A Case Study in Fingerprints", *Proc. 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pp. 335-342, Guildford, UK, June 9-11, 2003.
- [7] L. Hong and A. K. Jain, "Classification of Fingerprint Images", *Proc. 11th Scandinavian Conference on Image Analysis*, June 7-11, Kangerlussuaq, Greenland, 1999
- [8] "Design of Zigbee Transceiver for IEEE 802.15.4 Using MATLAB/SIMULINK"] Prof. Sarat Kumar Patra (Supervisor) Head of Department, Dept. of Electronics & Communication Engg. National Institute of Technology Rourkela-769008.
- [9] thesis.nitrkl.ac.in/995/1/neeta.pdf
- [10] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic Fingerprint-Database Generation," in *Proc. 16th International Conf. on Pattern Recognition*, August 2002, pp. 744-747.
- [11] https://en.wikipedia.org/wiki/IEEE_802.15.4
- [12] Nandakumar K, Jain AK, Pankanti S. Fingerprint-base Fuzzy Vault: Implementation and Performance, IEEE Transactions on Informatics Forensics and Security, vol. 2, no. 4, pp. 744-757, December 2007.



Mukesh Kumar Thakur, B.Tech. 3rd year Student, Department of Electronics and Communication Engineering, Bengal College of Engineering and Technology.



Ravi Shankarkumar, B.Tech. 3rd year Student, Department of Electronics and Communication Engineering, Bengal College of Engineering and Technology.



Mohit Kumar, B.Tech. 3rd year Student, Department of Applied Electronic and Instrumentation Engineering, Bengal College of Engineering and Technology.



Raju Kumar, B.Tech. 3rd year Student, Department of Electronics and Communication Engineering, Bengal College of Engineering and Technology.