Design and Implementation of a Fingerprint Based Lock System for Shared Access

Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit
Department of Electrical and Computer Engineering
North South University, Dhaka - 1229
{jayasree.baidya, trina.saha, ryad.moyashir, rajesh.palit}@northsouth.edu

***Abstract*—Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. Most of the major door lock security systems have several loopholes which could be broken down to gain access to the desired places, and it creates a concern for a secure lifestyle and proper working environment. Additionally, terrorism and unauthorized access to places have become a major issue now-a-days, and there is a need for a secure system to prevent unauthorized access especially in shared access environment. With this consideration, a design and prototype of a biometric fingerprint based door lock system has been presented in this paper. Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy. The RFID or password based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or stolen, thus for facilities with shared access require biometric-based secure system. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system. We have implemented a centralized control system from where we can control who can enter in which rooms and who cannot. This is an Arduino UNO device based flexible working device that provides physical security using the fingerprint sensor technology.**

***Index Terms*—Bio-metrics; Fingerprint sensor; Security System; Authorization;**

I. Introduction

These days office/corporate environment security is a major threat faced by every individual when away from home or at the home. When it comes to security systems, it is one of the primary concerns in this busy competitive world, where human cannot find ways to provide security to his confidential belongings manually. Instead, He finds an alternative solution which provides better, reliable and atomized security. This is an era where everything is connected through network, where anyone can get hold of information from anywhere around the world. Thus chances of one's info being hacked are a serious issue. Due to these risks it's very important to have some kind of personal identification to access one's own info. Now a day's personal identification is becoming an important issue all around. Among mainstream personal identification methods we mostly see password and identification cards techniques. But it is easy to hack password now and identification cards may get lost, thus making these methods quite unreliable.

978-1-5090-4228-9/17/$31.00 ©2017 IEEE

There are certain situations which are very annoying like when a person locks himself out of his house or office or he leaves his key inside or sometimes when a thief just breaks the lock and steals everything. These kinds of situations always trouble people who use manual door lock with keys. Although in some places people use smart cards, there might arise a situation when someone loses the card or keeps the card inside. Then in other scenarios there are caretakers for locking houses or offices and keeping the keys safe. But then again there are times when a person in charge of the keys might not be available or has gone to some emergency routine, which can cause unwanted delay for people who need the key straightaway. These are some of the hassles that people might face when using keys or smart cards. That is when our system, fingerprint based lock system comes into play. Our design is implemented to provide better securities as users don't need to remember passwords and don't need any sort of keys or cards that often get lost. If someone's fingerprint is authorized in the system he would not face any sort of delays to enter a room.

Fingerprint recognition is one of the most secure systems because a fingerprint of one person never matches with the others. Therefore unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users and unlock the system when a match is found. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone. The popularity and reliability on fingerprint scanner can be easily guessed from its use in recent hand-held devices like mobile phones and laptops.

In this paper, we discuss the background in Section II where the bio-metric based lock systems have been discussed, proposed solution and finger print method are given in Section III. Then we describe the design and implementation of the proposed lock system in Section IV. The implementation details includes circuit diagram, software implementation, enrollment and deletion of fingerprints, function of the complete system. Section V contains the results and discussions on the testing and people feedback of the implemented system. This paper is concluded in Section VII following a section on future work.

II. Background

This study has analyzed current lock systems that are used in houses and offices at present. It has been found that although these methods are helpful in the initial days, eventually they become outdated and pose much threat to security issues. They have also been identified as quiet expensive. Below is a discussion on the pros and cons of the existing systems.

A. Deadbolt System

Security protocol followed in this system was “Single key for a single lock”. For a few days, it was satisfactory but at one time it was proved wrong by the fact that multiple keys can be easily made for a single lock. Hence this system is considered vulnerable and outdated in current times.

B. Password-Authentication

This system stores the password of authenticated users for the purpose of validation which provides considerable security to the users. Power consumption is efficient and usage is user-friendly. However, unauthorized users can easily acquire passwords through different methods (hacking, guessing and so on.).

C. RFID reader authentication

Radio Frequency Identification (RFID) is a fundamental and inexpensive technology that enables wireless data transmission [9]]. With RFID, wireless automatic identification takes a very specific form: the object, location, or individual is marked with a unique identifier code contained with an RFID tag, which is in some way attached to or embedded in the target [10]. This system has some advantage like the data on a RFID card is readable only with special equipment, keeping the data recorded on the chip secure. RFID systems can be easily duplicated or cards can fall into the wrong hands.

D. Face detector lock

These systems have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [7].

E. Retinal scanner

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. The image acquisition requires a person to peep into an eyepiece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged [1]. This device is frequently used for security purpose. The false acceptance and rejection rates are lower in this device. But the problem of this device is, it is not user- friendly and the equipment cost is very high.

F. Iris scanner

Iris recognition is a method of biometric authentication, based on extraction features of the iris of an individual’s eyes. Each individual has a unique iris; the variation even exists between identical twins and between the left and right eye of the same person [6]. The advantage of using iris scanner is, it has very high accuracy and the accuracy of iris scanners can be affected by changes in lighting. As iris is a small target and a scanner cannot be performed properly for multiple people of different heights. The main shortcomings with iris recognition technology, is that the iris scanners are very expensive and requires a lot of memory to store data.

G. Voice recognition

Voice recognition or speaker recognition is the problem of identifying a speaker from a short utterance [8]. This biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style) [9]. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise [1].

III. Proposed Lock System

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [11]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about USD 20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities [1]. This is a perfect solution for protecting one from the hassle of stolen/lost key or an unauthorized entry.

A. Fingerprint based Door Lock

Our proposed fingerprint based lock system is a reliable and very secure lock that will not only ensure safer environment but also ease lifestyle. This system can prove very useful in housing buildings, large offices, universities and so on. Because it offers the flexibility to add more features to the system. Users do not need to implement many systems from scratch. They can simply use our fingerprint lock system because fingerprint scanning is more accurate and cost effective method. It is also secure because fingerprint duplication is virtually impossible. Additionally, we have also used password authentication system for security purposes to ensure access to not enrolled people.

B. Fingerprint Identification

Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies [2]. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical [8]. The three basic patterns of fingerprint ridges are the arch, loop, and whorl.

- Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger. In the whorl pattern, ridges form circularly around a finger.

A fingerprint recognition system can be used for both verification and identification. 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 (1:1 match). In identification, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:N match). Detecting multiple enrollments, in which the same person obtains multiple credentials such as a passport under different names, requires the negative identification functionality of fingerprints.

When it came to designing the lock, we wanted to achieve simplicity in terms of the entire lock itself as well as in the internal components. The lock will be hanging on the wall beside the doorway that will include a fingerprint sensor. We have added a buzzer system to notify the usage of the device and a keypad that can be used to enter a password to allow access in case of the fingerprint bearer is not present. As shown in Fig. 1, an additional switch is added to the system so that people from the inside can unlock the door. We are using an optical fingerprint sensor. Optical fingerprint sensors use reflective light to scan the surface of the finger with almost 100% accuracy. The sensor we are using is called FPM10A Fingerprint Sensor.

For this project the main components are:

- Arduino Uno, fingerprint sensor
- Electronic lock, push button, Buzzer
- 4X4 Matrix keypad
- Channel relay module

Additionally, we used a breadboard, male-to-male connecting wires, plastic glue, a 12V power adaptor, hard plastic for casing and a door.

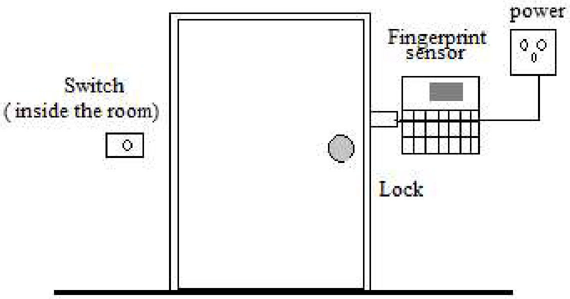

Fig. 1. Schematic diagram of the fingerprint based door lock.

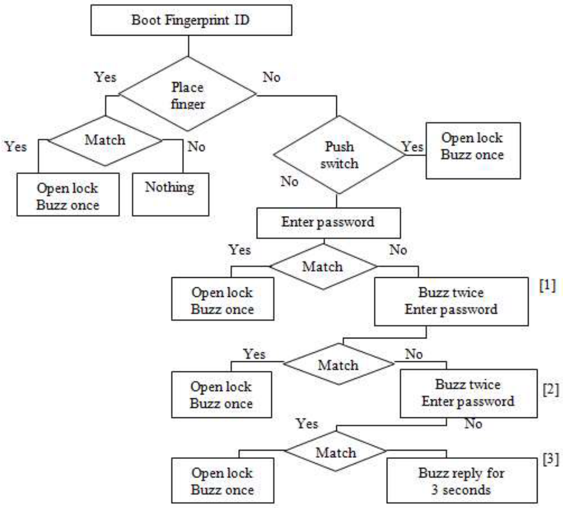

Fig. 2. Flowchart of entire system.

- As shown in Fig. 2, when a finger is placed on the sensor, it will read the print and match it with the fingerprints saved inside it. If no match is found, the device will not do anything. If a match is found, it will play one buzz and trigger the electronic lock to unlock the doorway.
- In addition to the fingerprints saved in the device, a 4-digit password will be saved.
- The keypad can be used to enter the password for access. Each key pressed will make a low beeping sound, upon entering the code; if right code is entered the door will open with a single buzz. If wrong code is entered, the door will remain locked and beep twice. Upon 3 failed attempts the door will buzz continuously for 3 seconds.
- A switch will be installed inside the doorway. Upon pressing it the door will unlock with a single buzz.

The total cost for this project is 7,790 BDT only. Mass manufacture of this project will yield in lower cost.

IV. Design and Implementation

The detail of hardware and software implementations are described in this section.

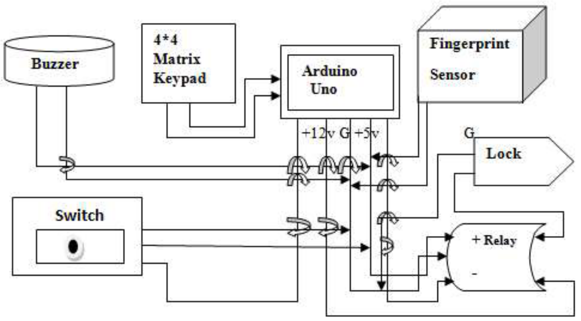

Fig. 3. Block diagram of the whole system.

A. Hardware implementation

As shown in Fig. 3 we set the devices then connect them according to the block diagram. Tx-out and Rx-in of the sensor are connected to the pin 2 and pin 3 of the Arduino Uno respectively. The electronic lock is connected with one of the output ports of the Uno. Making a network with the relay allows switching between the 5V and the 12V electrical components. Now we have attached the Arduino Uno to the laptop for registering fingerprints. We require the connection with the computer for assigning the ID to the prints. This can be done through Smartphone with Arduino application as well. We save the ID into the sensor and upload the code to the Uno. We disconnect the Uno with the computer and turn on the power adaptor. Once it gains power, the system boots up the fingerprint IDs saved inside and waits for a print to be matched. If no match is found, the keypad and the switch remain active. Once a match is found, the buzzer will buzz once and the lock will open. If no match is found, the system will not take any action at all. The scanner can perform over 100 scans per second, so when someone places a finger, it will respond instantly if the prints match. This system can store up to 126 fingerprint IDs. So, it can control the access of 126 different people. Review of the whole system

- 126 different fingerprints can be enrolled into the system to open door/doors.
- On placing a registered finger, the lock unlocks for 5 seconds with no noise or buzz.
- A 4-digit password can be entered through the keypad.
- Each key pressed results in a beeping sound. A successful code opens the door with a single buzz.
- An incorrect input will not open the door; the system will buzz shortly twice.
- 3 failed attempts on the keypad will make the system buzz continuously for 3 seconds notifying an intrusion attempt.
- On pressing the switch from inside, the lock unlocks for 5 seconds with a single buzz.

B. Software implementation

First of all, we download the Adafruit Fingerprint sensor library from net. For enrolling a new finger, we put together a simple sketch and upload it to the Arduino. Then follow this process which is shown below in Fig. 4.

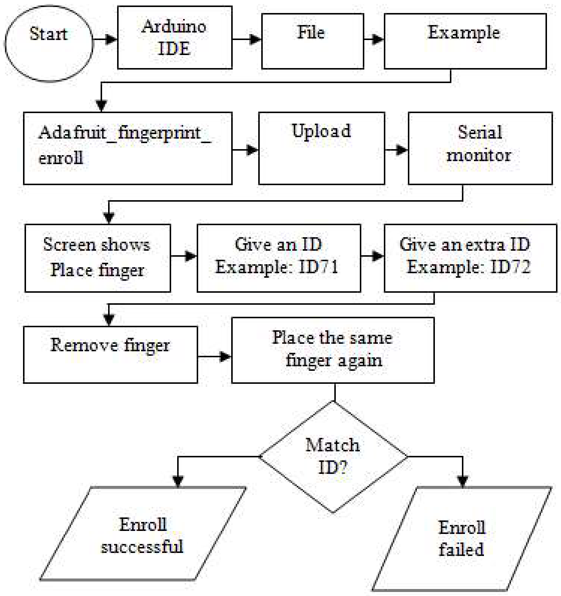

Fig. 4. Finger print enrollment steps.

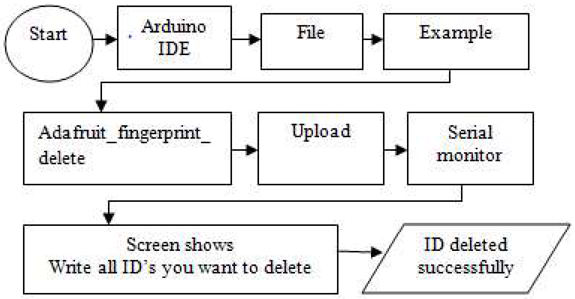
Start
Arduino IDE
File
Example
Adafruit_fingerprint_ delete
Upload
Serial monitor
Screen shows Write all ID's you want to delete
ID deleted successfully

Fig. 5. Finger print deletion steps.

1) Fingerprint verification process: For verifying an enrolled finger, we placed finger against that was already enrolled. If arduino recognize that fingerprint, the door will unlock, otherwise the door remains locked.

2) Fingerprint deletion process: To delete any fingerprint, type the IDs in the serial monitor and it will delete that fingerprint. The steps is shown in Fig. 5. A picture of developed prototype of the fingerprint sensor based lock system is given in Fig. 6.

V. Results and Discussion

In this section, we discuss how the system behaved upon completion. We devised various tests to see if the individual functions are performing accordingly. After implementation of the tests, we have collected the results to verify the functionalities of the individual components. Then the system was tested as a whole for any error. After carrying out the tests, the system was given to engineers so that they can try to break the system and use their own fingerprints in the system. They

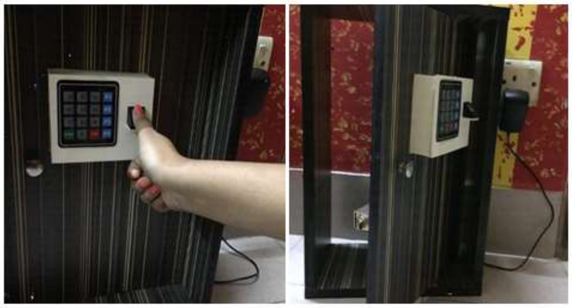

Fig. 6. Fingerprint sensor based door lock.

TABLE I
RESULTS OF FINGERPRINT TESTING.

Print ID	Finger Bearer	Attempts	case I	case II
100	Trina	20	20	18
500	Joya	20	20	19
600	Ryad	20	20	15

were also asked to give us feedback of the system through a survey.

Fingerprint testing: After saving a fingerprint, we wanted to test the accuracy of it. We tried placing the finger partially, inverted, in wet conditions etc. and the sensor was able to match the prints. It failed when the finger was muddy or very oily as shown in Table. I in case II. These are the conditions to avoid. But in normal cases, the sensor is able to detect saved prints almost all the times (case I). In our rigorous testing, the success ratio is more than 95%.

When the finger is extremely dirty or oily, it did fail. But the sensor seems to get the reading right when the finger is less dirty or oily. However, it did not fail when the finger was wet. Marks were present on the sensor lens but that was easily wiped away. Those marks were water particles left after the finger was replaced.

The sensor claims to have 99% accuracy rate and it seems to be living up to its promise.

- Keypad testing: We have entered the password once. Entered wrong code three times in a row. Expected results achieved. But in practice, the fingerprint is much more secure; this feature is kept for an extreme case of emergencies.
- Switch testing: Upon pressing the switch, the door was unlocked every time it was pressed. It did not fail once.

After successfully completing the goal and experimenting with the system, we can conclude that we have created a very reliable and secure lock.

To test the accuracy and the functionality of the system we have devised various finger conditions to test the scanner, tested the keypad with test codes and test runs for the switch. The scanner was able to detect over 90% of the fingerprint scans after we have deliberately tested it with extreme finger conditions (dirty, oily, wet, etc.) The keypad and the switch have performed accordingly with 100% accuracy. We have later given the system on the hands of a group of young engineers for testing and review. They also found that the functions of the system were working well and reviewed the system through a survey. They wanted more functions to be added which is possible with this system, for that we will require the requirement specific hardware and a few modification of code.

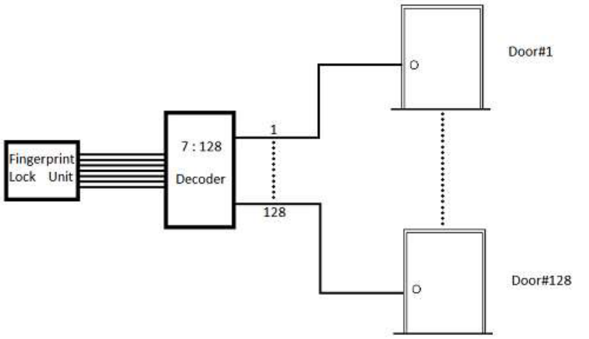

Fig. 7. Decoder network fingerprint lock system.

VI. Future Work

The developed system is very much flexible. The system we have created operates on only one lock, but in our current state, we can add more electronic locks, where each lock can be unlocked with specified print IDs. All it will need is more electronic locks and code modifications. There can be some other implementations to this system as well, some of them are given below.

A. Multi-lock/ Decoder network system

As mentioned earlier, this system currently has one lock connected to, and we can add up to 5 more. In fact, by using a network of decoders, we can connect as many locks as we want and provide access to up to 126 different individuals. As shown in Fig. 7 a decoder network can be used with this system. Additionally, 6 different locks can be added. Instead of using those output pins from the no for locks, we can create a system using 7: 128 decoders. In that way, all the memory space of the fingerprint sensor (126 capacity), connect them to individual doorway or doorways with just one system.

B. Computerized Fingerprint lock system

This system can be installed on a PC, which will act as the brain behind the system. It can add new IDs and delete old ones and can even unlock doors through the computer. This will require the computer to be in the security control room or somewhere secure. In particular a log system can be easily implemented with the use of a computer with this system.

C. Smartphone based fingerprint security system

Smartphones with latest features use fingerprint ID system to allow access to the phone. This system can be made to connect with those phones and use their print ID and

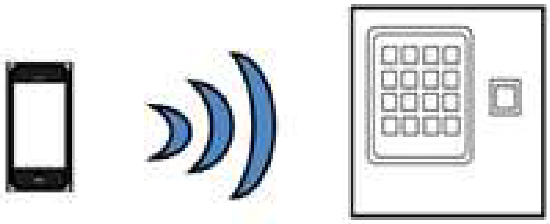

Fig. 8. Smartphone connectivity with the fingerprint lock.

their sensor on the phone to open doors. The system can be connected to the phone via Bluetooth or WiFi, and an application can be made for the phone (Fig. 8, allowing them to interact. Fingerprint ID is being used in most new phones now-a-days and soon the fingerprint ID based phone will be everywhere, almost everyone will have them and then this security system will be very helpful.

D. Improvements

More locks can be added to the system, *i.e.*, we do not need to spend so much for just one lock. A system to save prints without the use of a computer could have been made, but it will require more parts than the ones we used.

E. Limitations

It may not be able to detect fingers if they are exposed to certain chemicals and it can make errors with the dryness or dirty fingers or cuts and bruises on the finger. It is not appropriate for children, because of the size of their fingerprint changes quickly.

F. Challenges

Since this lock needs electricity to run, a power failure can make it totally useless. Thus an UPS or battery is needed. We used relay module, which is sensitive to power it gets. If it does not get sufficient power then relay switching sometimes malfunctions. So we had to give constant power to the relay module. The optical sensor we used is prone to scratches, dirt. As a result it may sometimes give inaccurate result.

VII. Conclusion

The design and implementation of fingerprint based lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our fingerprint based lock system has high accuracy rate and is also quick to recognize fingerprints which enable seamless integration with the users and provides tighter security. In our country, private and government organizations are very much concerned about security. Many companies are interested in using this type of locking mechanism but the system which is available have very high installation cost. Due to this excessive cost, many small firms cannot afford such systems. Keeping the installation cost in mind we planned to develop a system that should be affordable to both large and small firms. This design can be improved by more intensive development and additional features such as more locks can be added to the system. Thus we do not need to spend so much for just one lock if this can be used to control several doorways. A system to save prints without the use of a computer could have been made, but it will require more parts than the ones we used. In order to maintain security properly, the keypad should be placed inside the security room. A system for batteries could also be made or even solar powered. One of the main advantages of this system is its flexibility. Several other systems can be implemented with this system. The system is very secure. Fingerprints are unique and the sensor is able to identify most of the prints during testing. It provides greater control for access to restricted places. There are some drawbacks of this system such as this system is expensive for a single door and also that it depends on electricity. A power failure will make it unworkable. In that case, we can, connect the system with an IPS or add rechargeable batteries to the system.

References

[1] Anil K. Jain, Arun Ross and Salil Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14(1), January, 2004.

[2] R. P. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, vol. 85, no. 9, pp. 1348-1363, September, 1997.

[3] Anil K. Jain, Jianjiang Feng and Karthik Nandakumar. Matching Fingerprints. IEEE Computer, 43(2), pp. 36-44, February, 2010.

[4] Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), October, 2010.

[5] Zevdin Pala and Nihat Inanc. Smart Parking Applications Using RFID Technology. 1st Annual RFID Eurasia, Istanbul, 2007, pp. 1-3.

[6] D. Vinod kumar and M R K Murthy. Fingerprint Based ATM Security by using ARM7. IOSR Journal of Electronics and Communication Engineering(IOSRJECE), Volume 2(5), October 2012, PP 26-28.

[7] Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni. Fingerprint Image Reconstruction from Standard Templates. IEEE Trans. Pattern Analysis and Machine Intelligence, 29(9), pp. 1489-1503. September 2007.

[8] Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition, 2008. John Wiley & Sons, Inc., New York, NY, USA.

[9] Fernando L. Podio. Personal authentication through biometric technologies. Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525), Gaithersburg, MD, 2002, pp. 57-66.

[10] Yu-Chih Huang. Secure Access Control Scheme of RFID System Application. Fifth International Conference on Information Assurance and Security, China, 2009.

[11] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2002: Fingerprint Verification Competition. Proceedings of International Conference on Pattern Recognition (ICPR), pp.744-747, Quebec City, Canada, August 2002.