SAFE BIOMETRIC DOOR ACCESS SYSTEM USING IRIS AND FINGERPRINT

Balu Chandar K N
Master of Computer Application (MCA)
(Information Security and Management Services)
Jain University, Bangalore, Karnataka, India

Prof. Feon Jaison
MCA
Department of Computer Science and Information Technology
Jain University, Jayanagar, Bangalore

Abstract: Access is very important security aspect; access can be in the form of Physical access or access to System and Application. Securing the data plays a vital role in everyone's life. Data can be in the form of Softcopy (Stored in System and Applications) and in Physical Format (Hardcopy). This system is basically designed keeping securing the data in physical format and stop unauthenticated access to cabins and rooms in office and home. This system has two layers of Biometric Authentication i.e. Iris and Fingerprint. The system is designed in such a way that no intruders can hack the system and spoofing is completely stopped because this system used Biometrics as an authentication mechanism.

Keywords: Iris, Fingerprint, Biometric, Security, Access Control

I. INTRODUCTION

Security is the most important aspect. The data stored in the office or home can be stolen by the intruder. Data plays an important role in day to day life; most of them lost their business and also life due to data breach, important data or valuable things stored in your home or office gets stolen, it will lead to financial loss and also sometimes loss of life. This project is basically designed in such a way to secure the valuable things and data stored in the physical format in home and office. Hackers and intruders and finding new ways to steal data from home and office premises.

This project is designed using biometric authentication. Biometrics authentication methods are fingerprint, iris, face recognition, and voice recognition. Biometric authentication methods used in this project is fingerprint and iris. This project is a door authentication model which has two layer of security in it. The first level is fingerprint authentication and second level is iris recognition. When the user needs to get access to their room or cupboard they need to verify their identity. First users fingerprint is recognized and verified, and then the user's iris is scanned and if it matches, then the door or cupboard will be opened.

II. EXISTING SYSTEM

Mainly used access system in day to day life is Traditional Lock and Key, this is widely used in every office and homes. Apart from this, now a day in few places, they have implemented unimodal Authentication for Physical Access, commonly used Authentication methods are Fingerprint and RFID.

Disadvantages of existing system

The Main Disadvantage of Existing System is:

- Keys can be duplicated if it gets into hackers and thief's hand.
- RFID tags can be easily stolen and by keeping it an intruder can easily get access to the Cabin and stole the data he requires.
- Unimodal Biometric Authentication produces more noise and the False Negative Ratios are more.
- Fingerprint Authentication used in some of the places are very old.
- Biometric Door access control in current Market is Very Costly.

III. PROPOSED SYSTEM

As there is need of new authentication method to keep the data safe. This System will allow users to access their door and cupboards in more secured way. Users can store their valuable data and information, without fear of hackers.
This Project is basically an authentication method, where users need to authenticate themselves to access it.
There are two levels of authentication embedded in the system, they are:-

- Fingerprint Recognition
- IRIS recognition

These two are biometric authentication where the access will be more secured than the currently available authentication methods.

Fingerprint Recognition

Fingerprints are generally used biometric identification. Fingerprint of every person is unique. The ridges and valley present in the fingers provides the uniqueness in every individual. To differentiate fingerprints, Minutiae points are used. With the help of Optical scanner, Fingerprint image is captured and then it is enhanced and converted into a template. Few factors like image noise, distortions and skin condition makes fingerprint matching difficult. Most of them use fingerprint as a common biometric feature, because of its reliability and accuracy. Whenever the fingers are too wet or too dry, system has a chance of returning false match or mismatch.

Iris Recognition System

As a biometric feature, Iris plays an important and vital role, Iris for each user will be unique and there is no similar iris can be found in two different users. Iris is a part of eye, and this biometric feature is used because, no duplication can be taken easily without your reference. Fingerprints can be easily captured with help of some items, whereas iris cannot be easily captured. In this Project we use hamming distance vector to Match Iris.

Advantages of Proposed System

- Two Layer of Authentication
- Reduces Noise
- More secured compare to Traditional Access System and More Secured than Unimodal Authentication
- Biometric Encryption – IRIS and Fingerprint both are unique and can’t be broken easily.
- Cost Efficient

IV. MODULE DESCRIPTION

This is an authentication project, where when the user needs to get access to their cabin or cupboards, they need to authenticate themselves, this is implementing to block unauthorised access to the cabins and secure the data.

This System has two Layers of Authentication, this is implemented to protect and provide a very strong access controller for a cabin or cupboard. This system uses Biometric as a basic Authentication Mechanism, this helps to protect the data and system from hackers and intruders.

The Biometric Authentication used in this system is:-

- Fingerprint
- Iris

As both are biometric and unique for individuals, this makes system to be more secure and provides maximum security and best access control.

System Working Mechanism

There are two Stages in this system

- Enrolment
- Identification

Enrolment:

At the time of enrolment user are first requested to enter the required data, once it’s done system will prompt user to go for Fingerprint Enrolment. User has to Place their finger and Enrol for Fingerprint. Once fingerprint enrolment is done, user will be then requested to place their iris for iris enrolment, if both fingerprint and iris is enrolled, data of the user will be stored in Database

Identification:

When the user wants to access the cabin or cupboard, first they should authenticate themselves. At the time of identification, user will be asked to authenticate their fingerprint at first, once the fingerprint is authenticated, system will prompt user for Iris Authentication, once the Iris is authenticated, and System will send the signal to servo motor for unlocking the door.

The Flow Diagram from Enrolment and Identification Stages are as follows:

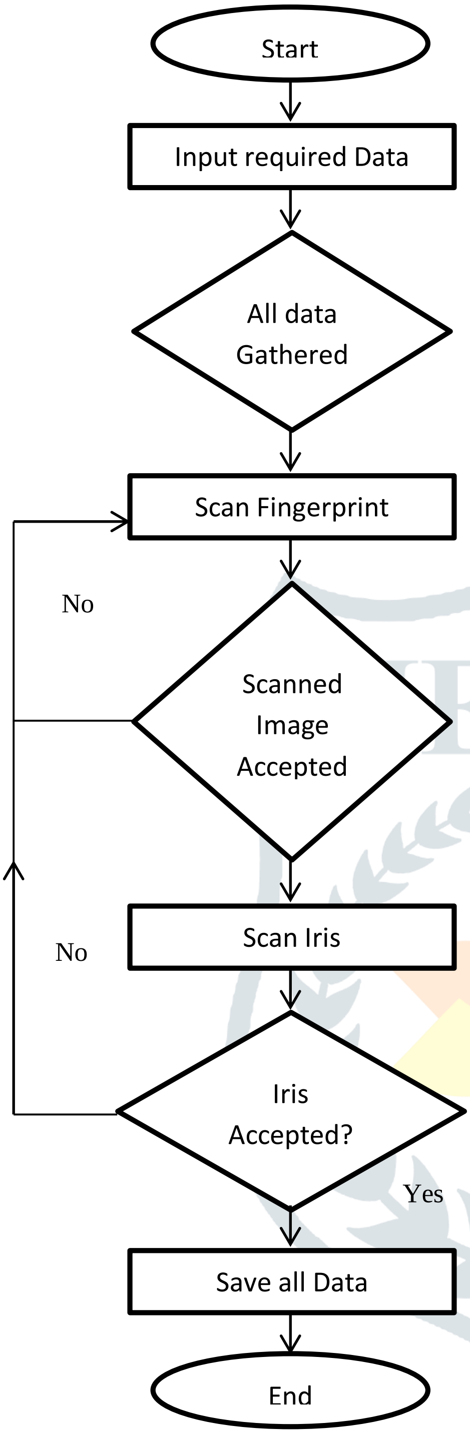

Figure 4.1 Flow Diagrams for Enrolment Stage

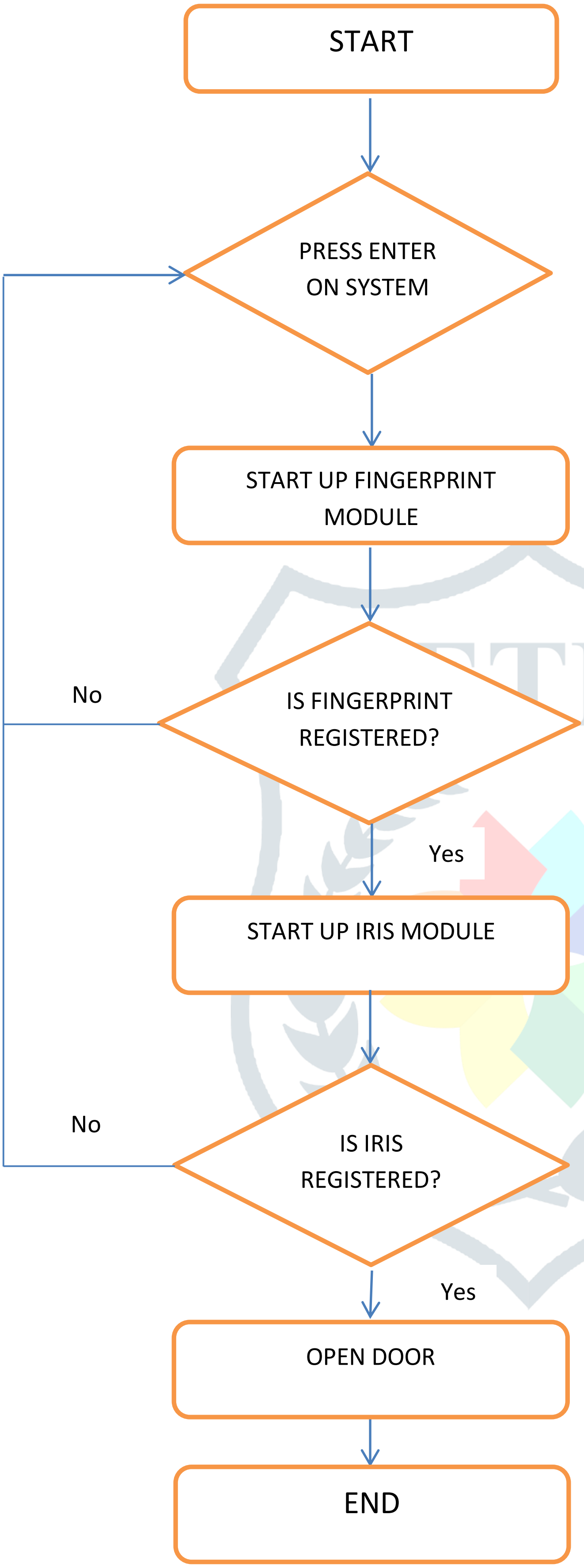

FIGURE 4.2 Flow Diagrams for Identification Stage

V. CONCLUSION

This Paper has presented the Safe Biometric Access Control System using Fingerprint and Iris. This is implemented using hardware and software. This project is mainly implemented to protect access and implement it with low cost components. Project is completely built using Low cost components and main aim is to provide security which is more secure and cost effective. Bimodal Authentication helps to protect the data more securely than most of the other techniques.

VI. FUTURE ENHANCEMENT

Future Enhancement of the Project is as follows:

- Implement Multi Modal Authentication
- OTP Based Authentication for Another secure layer
- Buzzers need to be implemented for wrong authentication and breakage

VII. REFERENCES

[1] D. Maltoni, D. Maio, A.k. jain, S. Prabhakar, Handbook of Fingerprint Recognition, second ed, Springer Publishing Company, Incorporated, 2009.

[2] K. Okokpujie, N.-O. Etinosa, S. John, and E. Joy, "Comparative Analysis of Fingerprint Preprocessing Algorithms for Electronic Voting Processes," in International Conference on Information Theoretic Security, 2017, pp. 212-219.

[3] Ogbanufe, O. and Kim, D.J., 2017. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems.

[4] Addy, D. and Bala, P., 2016, September. Physical access control based on biometrics and GSM. In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 1995-2001). IEEE.

[5] KO Okokpujie, A Abayomi-Alli, O Abayomi-Alli, M Odusami, IP Okokpujie, OA Akinola. An automated energy meter reading system using GSM technology.

[6] Jain, A. Ross, K. Nandakumar, “Introduction to Biometrics”, Springer Science & Business Media, 2011.

[7] K Okokpujie, E Noma-Osaghae, O Okesola, O Omoruyi, C Okereke, S John, IP Okokpujie. Fingerprint Biometric Authentication Based Point of Sale Terminal. InInternational Conference on Information Science and Applications 2018 Jun 25 (pp. 229-237). Springer, Singapore.