Three Layered Security System for Bank Locker

Prof.K.D.Mahajan
BVCOEW/E&Tc.,Pune,India
Sharvari Tatwawadi, Ayesha Shaikh, and Rashmi Shewatkar
BVCOEW/E&Tc.,Pune,India

Abstract

The value of biometrics have been realised by security system for two main purposes i.e to identify and to verify users. There are many places where only authorized people can enter and in that situation we need to identify person entering restricted areas like bank lockers, military base stations, R&D labs etc. If process of identification is performed by security guards manually, it will be difficult to identify each person. Also these processes are time consuming and there are chances of many errors. To avoid these problems we are proposing a three layered security system for bank locker based on iris recognition, fingerprint detection and OTP which will recognize the person. This is a biometric system for access control that uses the most unique characteristic of the human body, the iris and the fingerprint, employed in automated border crossings, national ID systems, etc. The proposed system will provide information of recognized person & thus controlling the access of the people into the restricted area.

Index Terms - *Iris recognition and detection, Fingerprint recognition and detection, One Time Password support.*

I. INTRODUCTION

The main aim of the project is development of a system with high level security for restricted areas with the help of iris recognition fingerprint detection and OTP support to display the information of recognized person and to control the access of the person. If process of identification is performed by security guards manually, it will be difficult to identify each person. Also these processes are time consuming and there are chances of many errors.

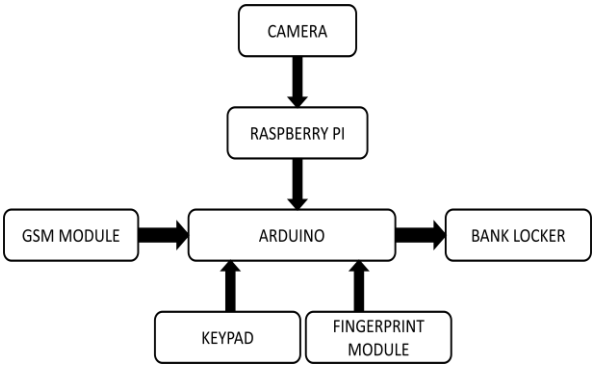
Biometrics is automated methods used for person identification based on physiological and behavioral characteristics. Use of biometric for identification/ verification is increasing because biometric qualities are extremely difficult to replicate, and some do not change for a lifetime. Fingerprints are the most popular biometric characteristic because of several advantages it offers. Other biometrics used for identification includes hand geometry, palm vein patterns, retinas, irises, facial characteristics, signatures, and vocal qualities.

Iris recognition efficacy is rarely impeded by contact lenses or glasses. A key advantage of iris recognition is its stability. Iris recognition method gives better performance than all other image processing system. Iris recognition system can be used to identify individuals or to prevent unauthorized access. When installed,the users are required to register to the system. A distinct iris code is then generated for every iris image enrolled and is saved in the system. Once registered, a user can present his iris to the system and get identified.

Fingerprints (FPs) are basically feature pattern of one finger, this is the most important biometric technology used now a days for personnel identification. Fingerprint is the pattern of ridges and valleys on finger tip, which is also known as furrows. Ridge characteristics and their relationship are unique for any fingerprint. Each fingerprint in this world is unique and so each person of this world has a unique fingerprint with permanent unique characteristics over it. There are two related application areas in this field, Fingerprint verification (FPV) and identification. FPV means one to one matching, in this given fingerprint is verified that whether it is the one which is registered as authenticated one.

Random numbers generated keypad based on one time pad concept was proposed to increase the level of security in common types of security counter measure used in authentication information mentioned above. The OTP is generated by a token which is possessed by the user and it is input to the authentication system. The OTP which is generated is compared with the input OTP. If the input OTP matches the OTP generated by the system, the user is allowed access to the system.

II. USED APPROACH



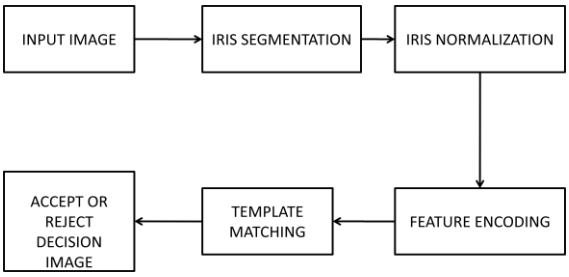
A. Iris Recognition and Detection

Security system using iris works in following two major steps:

1. Iris recognition system to recognize the person.
2. Iris recognition system integrated with microcontroller and LCD.

The iris recognition system is basically a five step process as follows:

1. Iris segmentation
2. Iris normalization
3. Feature encoding
4. Template matching
5. Accept/Reject decision



1. ***Iris segmentation***:
   - Captured eye image will act as input for this stage. It deals with segmenting the iris part from an eye image.
   - Iris segmentation consists of iris outer and inner boundaries localization, detection of lower and upper eyelids, and detection or removal of reflection from the cornea or eyeglasses.

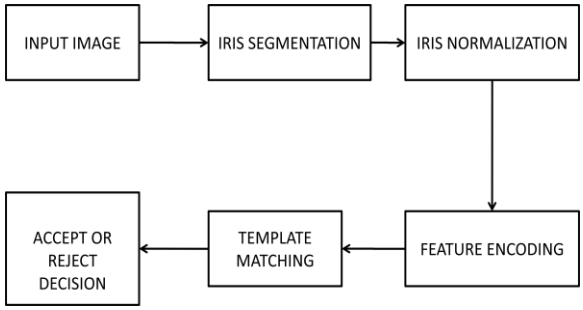
2. ***Iris normalization***:
   - In iris normalization the segmented iris region is remapped to the fixed-size rectangular image by mapping the iris region which is extracted into normalized coordinate system.

3. ***Feature encoding***
   - In the feature encoding step, a template representing iris pattern information is created.
   -

4. ***Template matching***
   - The goal of matching is to evaluate the similarity of two iris representations.
   -

5. ***Accept or Reject decision***
   - In this process, if templates match with each other, then human identification will be accepted otherwise it will be rejected.

B. Fingerprint Recognition and Detection



A. Classification of fingerprint patterns:

There are three types of fingerprint patterns

1. Arches:
   - The patter whose ridges route from one side to the other side lacking any type of location called as arches. Normally, no arch pattern allows the delta.
   - Arches are classified into four types:
     - Radial arches
     - Tented arches
     - Plain arches
     - Ulnar arche

2. Loops:
   - The pattern, whose ridges moves inwards and return in line to the origin is known as loops.

   - There are four types of loops are as follows:
     - Plain loop
     - Lateral pocket loop
     - Twinned loop
     - Central packet loop

3. Whorls:
   - The pattern whose ridge makes a circular formation around a central point is called as whorls.
   - Whorl patterns are classified in following four groups:

- Plain whorls
- Central pocket loop whorls
- Accidental whorls
- Double pocket loop whorls

B. Fingerprint Security Methods

1. ***Minutiae based Approach***
   - This includes four stages and is defined as:
     - Minutiae extraction
     - Orientation field assessment
     - Ridge extraction
     - Post processing

2. ***Pattern recognition Approach***
   - Fingerprints are consisting of a combination of a ridge and valleys named as patterns.
   - These patters utilize for authentication by the pattern identification methods.

3. ***Wavelet based Approach***
   - Wavelet theory is usually utilized in the signal processing.
   - But, then the traditional wavelet transformation displayed some restrictions on the 2-D image processing.
   - Wavelet theory can perform in a better way by holding the information of the image edge.

C. One Time Password (OTP)

- OTP is password authentication scheme where a new password is generated for each authentication session. Once the password is used, it is no longer valid and any attempt to reuse the same password for future authentication sessions would fail . Properties of one time passwords ensure the resistance towards various common attacks and the uniqueness of human perception makes it usable .
- OTP generation algorithms typically make use of pseudo-randomness or true-randomness. This is necessary because future OTP's can be easily predicted by observing previous ones.

III. ALGORITHM

A. Algorithm for RaspberryPi

1) START
2) Initialize iris detection, fingerprint recognition and GSM.
3) Initialize iris database.
4) Scan iris of the person.
5) Compare the scanned image of iris with database.
6) If match is found send the data to arduino else suspend process.
7) STOP

B. Algorithm for Arduino

1) START
2) Check input data from Raspberry PI.
3) Scan fingerprint.
4) Compare database and scanned fingerprint.
5) If match is found, send OTP to registered number.
6) If OTP is correct, open locker else suspend the process.

IV ADVANTAGES

- Iris and fingerprint both are the unique characteristics of human being.
- Biometrics provide accurate identification.
- Easy and safe for use.
- Time saving.
- User friendly system.
- Convenient.
- Versatile and Scalable.
- Use of fingerprint to avoid any fooling involved.
- With the help of this, entry in authorized areas can be prohibited.

V APPLICATIONS

- Bank lockers security.
- Military base station security.
- Security systems in R&D labs.
- Criminal identification
- ATM
- Prison security
- Aviation security
- Border crossing control
- Database access
- Home/office

VI CONCLUSION

- This project should be able to implement three layered security system.
- The main aim of the project is to secure bank lockers but this can also be used for R&D labs and military base stations.
- As the process go, camera first scans the iris of the user and if it matches with his saved database it further scans the fingerprint, verifies it and send OTP after which the user can open his locker.

- If the match is not found at any stage in the process, it gets suspended.
- With the help of this customers will be able to rely on banks for proper service and security.

ACKNOWLEDGEMENT

Working on this project "THREE LAYERED SECURITY SYSTEM FOR BANK LOCKER" was a source of immense knowledge to us. We would like to express our sinciere gratitude to Prof.K.D.Mahajan for her guidance and valuable support throughout the course of this project work. We acknowledge with a deep sense of gratitude, the encouragement and inspiration received from our faculty members and colleagues. We would also like to thank our parents for their love and support.

REFERENCES

[1] IEEE paper on "Iris based human identification" of 2015 by Madhulika Pandey of computer science and engineering department, Amity University, Noida,,India

[2] IEEE paper on "A secure personal identification system based on human retina" of 2013 by Joddat Fatima , Adeel Syed and M. Usman Akram department of Computer and Software Engineering Bahria University, Islamabad, Pakistan.

[3] 3.IEEE Paper on "A security system based on human iris identification " of 1997 by W. W. Boles, School of Electrical and Electronic System Engineering, Queensland, University of Technology , Australia.

[4] IEEE paper on "The human iris structure and its application in security system of car'' by Sreekala.P, Victor Jose, assistant professor, Electrical and Electronics Dept. kanjirapally.

[5] IEEE paper on "A Broad Survey on Fingerprint Recognition Systems" by Subba Reddy Borra and G. Jagadeeswar Reddy .

[6] IEEE paper on "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching" by Mouad.M.H.Ali and Vivek Mahale .

[7] IEEE paper on "Fingerprint Recognition Techniques and its Applications" by Priyanka.

[8] IEEE paper on "Physical Authentication using Random Number Generated (RNG) Keypad based on One Time Pad (OTP) Concept" by Herny Ramadhani Mohd Husny Hamid and Norhaiza Ya Abdullah.

[9] Gorazd Vrcek Peter Peer Computer Vision Laboratory, Faculty of Computer and Information Science, "Iris based human verification system", University of Ljubljana, Slovenia.

[10] A.Mallikarjuna and S. Madhuri, "Biometric security techniques for iris recognition system", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 8, August 2013.