Smart Locker System Using Biometrics Authentication

Shital P. Chavan[1], Tejaswini G. Pagare[2], Sweety K. Sapkal[3], Gauri S. Shimpi[4]

[1,2,3,4]*Department of Information Technology, Engineering, MCOERC, Nashik, Maharashtra, India*

Abstract- **Security and Authentication of individuals is necessary for our daily lives especially in Bank lockers. A smart digital door lock system for bank automation is equipment that uses the digital information such as a user's data, voice detection, and face recognition as the method for authentication in the system. In this system bank will collect the biometric data of each person for accessing the lockers. Only authenticated person can recover the money, documents from the lockers as biometric is stored for individual identity of a person. A bank locker system proposed here consists of Node MCU, motor module for opening and closing of the door, communication module for giving the notification. As the locker is the safest place, the bank automation function in digital locker system enables user to conveniently control and monitor digital locker environment.**

Index Terms- **Node MCU, Face Recognition, Voice Detection, IOT.**

1. INTRODUCTION

Now a day's, people are concern about the safety of their valuable things like Money, Jewelry and Documents etc. Therefore, the bank lockers are the safest place to protect them. Because in day by day life we need to seek new security system because there are some problems in the traditional bank lockers like loss of key, duplicate key could be generated. Therefore, we will develop biometric based security system to improve maximum level security. There are many types of sensors available in the market for providing different facilities. The sensor can detect different types of changes occur in the surrounding and the data will be process according to the pre-set value. In this paper, we have implemented safety of the valuable things in the bank locker, house, and office (treasury) by using Node MCU, Biometric and Notification to each user which will be more secure than other systems. In this system only, authentic person can be recovered valuable things from bank locker with biometric protection method.

A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological characteristic for identify a person. Physiological characteristic includes face and voice. This character is remaining unchanged through life of person. Biometric system operates as verification mode or identification mode depending upon on the requirement of application. In verification mode, the system validates a person's identity by comparing the captured biometric characteristic with the actual individual's biometric template, which is already stored in the system database. This model will be a major contribution to the field of Home Security and for banking sectors.

2. TYPES OF BIOMETRIC AUTHNETICATION

Each of the different methods of biometric identification have something to recommend them. Some are less invasive, some can be without the knowledge of the subject, and some are very difficult to fake.

1. Face recognition

Of the various biometric identification methods, face recognition is one of the most flexible. It also shows promise as a way to search through masses of people who spent only seconds in front of a "scanner" - that is, an ordinary digital camera. Face recognition systems work by systematically analyzing specific features that are common to everyone's face - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin and so forth. These numerical quantities are then combine in a single code that uniquely identifies each person.

2. Fingerprint identification

Fingerprints remain constant throughout life. In over 140 years of fingerprint comparison worldwide, no two fingerprints ever been found to be alike, not even those of identical twins. Good fingerprint scanners are install in PDAs like the iPAQ Pocket PC; so scanner technology is also easy. Might not work in industrial applications since it requires clean hands. Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file.

3. Hand geometry biometrics

Hand geometry readers work in harsh environments, do not require clean conditions, and forms a very small dataset. It is not regarded as an intrusive kind of test. It is often the authentication method of choice in industrial environments.

4. Retina scan

There is no known way to replicate a retina. As far as anyone knows, the pattern of the blood vessels at the back of the eye is unique and stays the same for a lifetime. However, it requires about 15 seconds of careful concentration to take a good scan. Retina scan remains a standard in military and government installations.

5. Iris scan

Like a retina scan, an iris scan also provides unique biometric data that is very difficult to duplicate and remains the same for a lifetime. The scan is similarly difficult to make (may be difficult for children or the infirm). However, there are ways of encoding the iris scan biometric data in a way that it can be carried around securely in a "barcode" format. (See the SF in the News article Biometric Identification Finally Gets Started for some detailed information about how to perform an iris scan.)

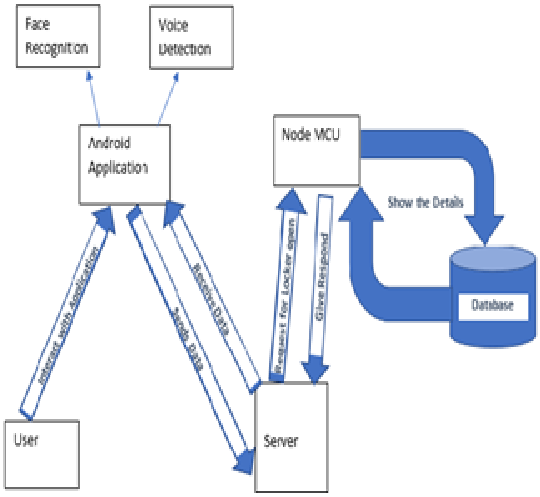
6. Signature

A signature is another example of biometric data that is easy to gather and is not physically intrusive. Digitized signatures are sometimes used, but usually have insufficient resolution to ensure authentication.

7. Voice analysis

Like face recognition, voice biometrics provide a way to authenticate identity without the subject's knowledge. It is easier to fake (using a tape recording); it is not possible to fool an analyst by imitating another person's voice.

3. PROPOSED SYSTEM



The above figure 1 shows the block diagram of proposed smart locker system. The brief explanation of the operating principle of the smart locker is narrated, here the biometric scanner is used to scan the person whoever utilize the smart locker and this will be stored in the Node MCU whenever the locker has to be opened or closed the Face has to be recognized. If the unknown face is identified the lock will not open. If the locker is open then notification will be send to the authenticated person

Android: Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets. As of May 2017, Android has two billion monthly active users, and it has the largest installed base of any operating system. Hence, we have decided to build an Android application which is used for interacting with user and accessing the locker by specific user.

Android Studio: Android Studio is the official integrated development environment (IDE) for Google’s Android operating system, built on Jet Brains’ IntelliJ IDEA software and designed specifically for Android development [8]. We use Android Studio to build an Android Application.

4. SYSTEM REQUIREMENTS

To develop this smart locker system the following components are required:

a. Node MCU
Node MCU is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.. You can tinker with your UNO without worring too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again. "Uno" means one in Italian and was chosen to mark the release of Node MCU Software (IDE) 1.0. The Uno board and version 1.0 of Node MCU Software (IDE) were the reference versions of Node MCU now evolved to newer releases. The Uno board is the first in a series of USB Node MCU, and the reference model for the Node MCU platform; for an extensive list of current, past or outdated boards see the Node MCU index of boards.

b. Camera
A camera is an optical instrument for recording or capturing images, which may be stored locally, transmitted to another location, or both. The images may be individual still photographs or sequences of images constituting videos or movies. The camera is a remote sensing device as it senses subjects without any contact.

c. Servo Motor
A servomotor is a rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity and acceleration.[1] It consists of a suitable motor coupled to a sensor for position feedback. It also requires a relatively sophisticated controller, often a dedicated module designed specifically for use with servomotors. Servomotors are not a specific class of motor although the term servomotor is often used to refer to a motor suitable for use in a closed-loop control system.

d. 5V Battery
A medium-sized rechargeable battery pack for your Raspberry Pi (or Node MCU, or Propeller, or anything else that uses 5V!). This pack is intended for providing a lot of power to an iPhone, cell phone, tablet, etc but we found it does a really good job of powering other miniature computers and micro-controllers. If you want even more power, we have a 10,000mAh power pack with two USB ports that can provide up to 2A! We tested it with an iPhone 5 & 5s so we know it will charge those models. It isn't good for charging large tablets that need 2A charging current such as the iPad.

5. CONCLUSION

In this system, we have introduced a Smart locker security system using Biometric authentication system. It is a low cost, low in power conception, compact in size and standalone system. We will use face recognition And voice control technique for open the locker. This system provides high security for bank.

REFERENCES

[1] P. Sugapriya, K. Amsavalli "Smart Banking Security System Using Pattern Analyzer" Vol.3, Special Issue 8, October 2015.

[2] M.Naveen Kumar and K.Usha, "Voice based Guidance and location indication system for blind using GSM,GPS and Optical Device Indicator," IJETT, vol. 4, pp. 1-3, July 2013.

[3] C.Vigneshwari, V.Vimala and G.Sumithra, "Sensor based Assistance System for Visually Impaired," IJETT, vol. 4, pp. 2-4, Oct 2013.

[4] K.Yelamarthi, Haas.D, Neilson.D and Mothersell.S, "RFID and GPS integrated navigation system for the visually impaired," IEEE Trans on Circuits and Systems(MWCAS), pp. 1149-1152, Aug 2010.

[5] Sagar S. Palsodkar, Prof S.B. Patil "Biometric and GSM Security for Lockers" Vol. 4, Issue 12(Part 6), December 2014, pp.237-239.

[6] L Huang and Y Xu, "Design and Implementation of Location Based Mobile Health System," IEEE International Conference on Computational and Information Sciences (ICCIS),pp.919920,Aug 2012. Micropik, "Ultrasonic Ranging Module

[7] Mary Lourde R and DushyantKhosla, ”Fingerprint Identification in Biometric Security Systems” ,International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.