IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Smart ATM Access and Security System using IRIS Recognition

Madhura Raju Lakhe[1], **Prof. S.S. Savkare**[2]

Dept of Electronics and Telecommunication, JSPM Technical Campus, Pune, India[1,2]

Abstract: The main aim of this paper is to provide security for ATM Centers by using IRIS Recognition. For the traditional ATM terminal, customer recognition systems rely only on bank cards, passwords and such identity verification methods which measures are not perfect and functions are too single. For solving the bugs of traditional ones, there is need to designs new ATM terminal recognition systems to verify the IRIS of the Acc holder of the bank at ATM Center. The use of Biometric ATM's based on IRIS recognition technology providing a safe and paperless banking environment. The iris recognition system completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. This project will detect the iris of the user and allows the person to make transactions, by using matlab it detects the human IRIS and allows person for the transaction and sends the message automatically. Once we receive the OTP we need to enter that key and then it allows the transactions, plus when the attacker try to damage the ATM machine vibration detection sensors gets activated. A message is passed to the nearby police stations with the help of GSM modem and door will get lock. We can remotely monitor the user accounts for Authorized or unauthorized Access by using Internet of Things (IOT).

Keywords: IRIS recognition, One-Time Password (OTP), ATM Security, Biometric, GSM, Vibration sensor.

1. INTRODUCTION

Automated teller machines (ATM) were first started to used in year of 1939. Nowadays, about 1.5 million are installed worldwide. ATMs are now found in many locations. For e:g ATMs are typically found in restaurants, Convenience stores, malls, supermarkets schools, gas stations, hotels, work locations, banking centers, airports, and entertainment. There are different aspects that should be considered. One of the paramount consideration issues is security because all over the world is an increasing use of ATMs and it mean that risks of hacking turn to be a reality more than before. Automated teller machine well known as the ATM is a computerized telecommunication device and it enables its customers to access their bank deposits or credit accounts in order to make a variety of transactions such as cash withdraws, check balances etc without any need for a cashier or human clerk. In conventional ATMs the identification of the customer is done using a PIN number .Here there is a possibility of hacking of passwords more over memorizing a password (PIN) and carrying smartcards in a significant overhead to users. Nowadays there are many persons which uses technological progress in circumvention of humans to steal their money, like Skimming Attack, Card trapping, PIN Cracking, ATM Malware and ATM hacking. So there is need to make framework with more secure and make unenlightened people able to use ATMs with quick secure way, it lead us to use biometrics which use human traits. [2]
Now a days, Government of India has taken up Digital Payment mode Across all sectors Related to billing and Transactions with development in the banking sector, security implementation has become priority to check the Authentication of the Account Holder. ATMs and Various Digital Payment modes are found in many locations.

2. PROBLEMS IN EXISTING SYSTEM

1] Card Theft:
In some ATM Machines Hooks are attached to the probes preventing the card from being returned to the consumer at the end of the transaction.

2] Skimming Devices:
Skimming method is the most frequently used method of illegally obtaining card track data. Skimmers are devices used by criminals to capture the data stored in the magnetic strip of the card.

3] Shoulder Surfing:
Shoulder Surfing method is the act of direct observation, watching what number that person taps onto the keypad.

4] Utilizing a Fake PIN Pad Overlay:
In this case, a fake Pin pad is placed over the original keypad. This overlay of PIN pad captures the PIN data and stores the information into its memory. The Duplicate PIN pad is then removed, and recorded PINs are downloaded. [13]

DOI10.17148/IJARCCE.2017.6762

3. LITERATURE SURVEY

Frauds in ATM's are increases day by day. So we need to give security to the ATM machine to prevent these frauds. The following are the different technology used to solve the ATM Frauds.
A. GSM based Technology
B. RFID Technology
C. Biometric Technology

The brief discussions about these technologies are as follows.

A. GSM based Technology

The researchers Suraj Kumar, Arjun Kumar Mistry, and Vicky Prasa proposed a system, i,e Secured Atm Transaction Using GSM, in which they provide security to ATM transaction. In this system whenever a user wants to make transaction user have to enter the pin number, if the password matches then a message will be send to corresponding account holder through GSM. The machine also gets acceptance message from an account holder. If acceptance message is delivered to the machine then machine allow doing further transaction else machine denies the transaction.[11]

B. RFID Technology

RFID Technology mostly used for a security purpose. It is also used in a library, for antitheft security, E-passport etc. Radio Frequency Identification (RFID) Technology is used for security purpose. RFID technology is used to identify a particular person is authorized or not.[11]

The drawbacks of RFID are as follow:
1] RFID card can be track easily.
2] The communication between tag & reader can eavesdrop; it occurs when unauthorized reader intercepts the tag.

C. Biometric Technology

The biometric system is a pattern recognition system which is operated by acquiring the biometric data from users and then extracting this feature of biometric data, after extracting this feature compare with the stored set of the database. Biometric technology is used for security purpose; it is more secure than RFID & GSM technology. There are various techniques that are used in ATM security:[11]
i. Fingerprint Recognition
ii. Face Recognition
iii. IRIS Recognition

4. PROPOSED SYSTEM

In the previous technology which is used for ATM security, there are some limitations, so there is a need to add some extra features in ATM security. The following diagram gives the proposed system which is used to enhance a security of ATM.

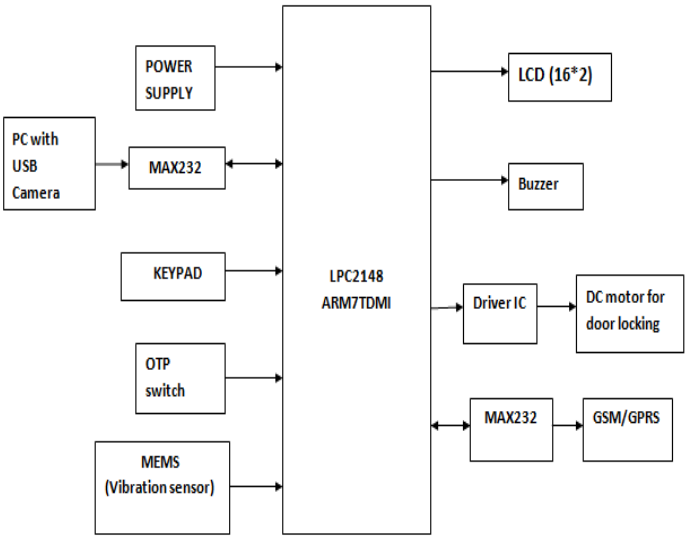


Figure 1.Block diagram of system

DOI10.17148/IJARCCE.2017.6762

Here we are interfacing the camera to the ARM controller. The USB camera will capture IRIS image of the person and send it to the PC Database, comparison will be done. Controller will recognize the iris of the particular person from the image. If they match then it will display the data on the display unit, and then a 6 digit code is messaged (OTP) to the customers' registered mobile number through GSM module connected to the ARM. It is only after entering this valid OTP that the user is allowed for making further transactions. For providing security to the ATM terminal from thieves we include a vibration sensor in the system. The vibration sensor will sense the position of ATM, in case of robbery the position of the ATM is changed then the sensor will automatically generate an alarm signal and will shut down the shutter of the ATM center. The turn off of the shutter will be done using a DC motor.

5. METHODOLOGY

IRIS Recognition:
The human Iris is an internal organ of the eye, protected by the eyelid, cornea. The iris is the colored portion of the eye that surrounds the pupil .It controls light levels inside the eye similar to the aperture of a camera. The round shape in the center of the iris is called the pupil. Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits like fingerprint, Face.

Iris Recognition System:
A typical iris recognition system in involves three main modules:

a. Image acquisition:
It is to capture a sequence of iris images from the subject
Using a specifically designed sensor. To capture a high quality image of the iris with using cameras and sensors with High resolution and good sharpness.

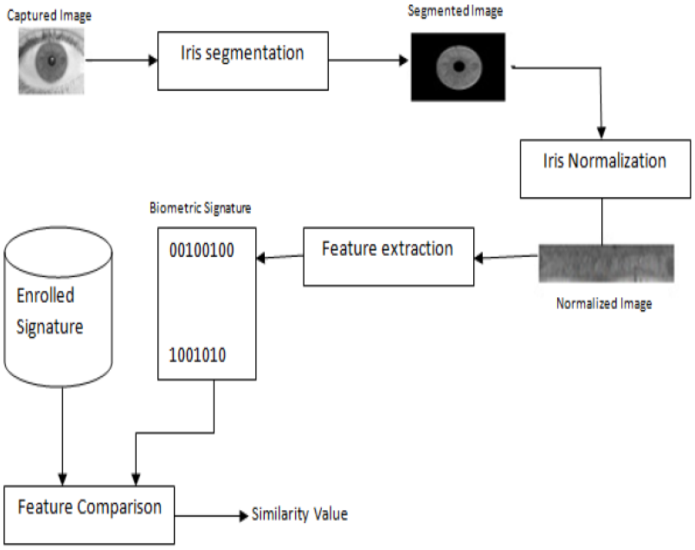


Figure 2 .IRIS Recognition System

b. Preprocessing Stage:
Preprocessing includes various stages such as:
1. Image Enhancement
2. Iris Segmentation
3. Iris Normalization

1. Image Enhancement:
In image enhancement we convert the colour image into the grayscale and resize the image. Processing on image to convert Colored image to black and white image for accurate comparison. Image enhancement technique. image processing that uses in preparing an image for a particular application.

2. Iris Segmentation:
The first step of iris recognition system is to isolate the actual iris region from the captured digital eye.

DOI10.17148/IJARCCE.2017.6762

In segmentation process Iris are approximated by two circles, one for the iris/sclera boundary and another for interior of the iris pupil boundary. The eyelids and eyelashes normally obstruct the upper and lower parts of the iris region.

3. Iris Normalization:

Normalization of Iris in this iris of different people may be captured in different size, for the same person also size may vary because of the variation in illumination and other factors. After both the inner and outer boundaries of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size.

c. Feature extraction and Encoding:

Feature Extraction is based on Euclidian distance. This is the most key component of an iris Recognition system and determines the system's performance to a large extent. it compare with input images and matching these features with known patterns in the feature database.

Hough Transform

The Hough Transform is an algorithm presented by Paul Hough in 1962 for the detection of features of a particular shape like lines or circles in digitalized images. it is used to detect the parameters of simple geometric objects, such as lines and circles, present in an image. The number of HT peaks obtained by the application of HT to an entire image varies for each image and this leads to redundancy during feature extraction. To overcome this, the image is divided into a number of blocks, causing a part of the image to be present in each block. The block size depends on the number of blocks the image is segmented into. The aspect ratio of the original image and the block image is maintained constant. After applying HT, the number of peaks obtained again varies for different blocks of the image.[10]

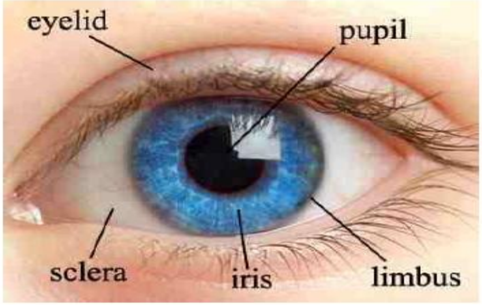


Figure 3. IRIS Image

Benefits of using IRIS Technology

1. Very high accuracy.
2. Uniqueness
3. Stability
4. Artificial duplication is virtually impossible
5. Probability of matching of two irises is 1:1078
6. Unique patterns.
7. Living Password cannot be forgotten or copied.
8. Works on blind person.
9. Accurate, faster, and supports large data base.

6. EXPERIMENTAL SETUP

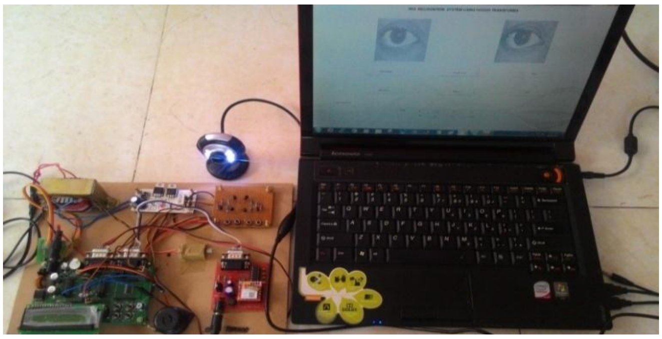


Figure 4. Experimental Setup

DOI10.17148/IJARCCE.2017.6762

7. FLOWCHART

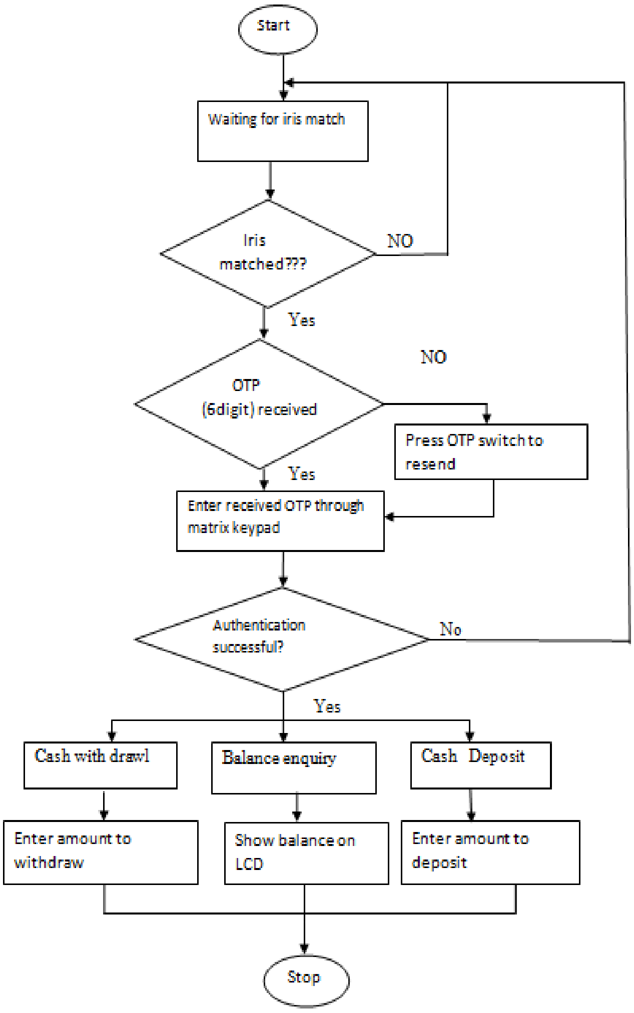


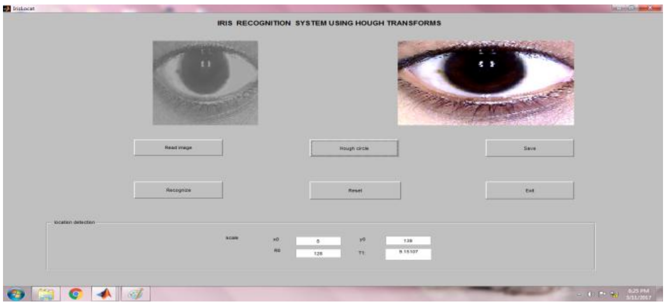
Figure 5. System Flow Diagram

1. Capture user iris image using USB Camera.
2. Compare captured iris with database
3. If iris matched with database image, send OTP(6 digit OTP) automatically to user, if it fails to send OTP automatically even if iris is matched then user has to press OTP generator key.
4. Matrix keypad to enter received OTP. OTP should be displayed on screen when user is entering received OTP.
5. After authentication successful Display options on LCD, as follow,
(a) Cash with drawl.
(b) Balance Enquiry.
(c) Deposit Cash.
6. Change in ATM transaction should be seen on Web server page (IOT).
(a) User Account number, Name
(b) Current Balance
20
(c) Last 5 transactions details

8. RESULTS

IRIS Acquisition Image:
In this stage IRIS image is get captured and enhancement process is done on it. Image enhancement means captured colored image is convert into black and white image.

DOI10.17148/IJARCCE.2017.6762

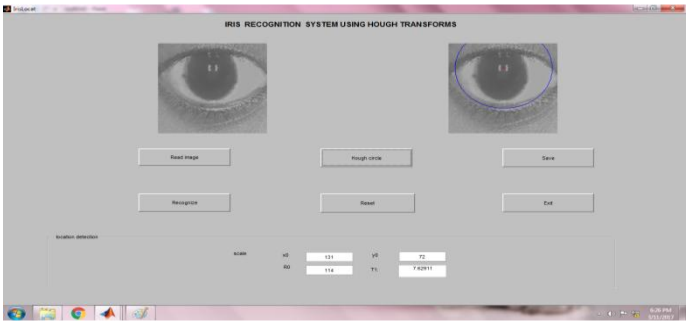


scale
x0 5
y0 139
R0 128
T1 9.15107

Figure 6.IRIS Capture Image

Hough Transform:

When we click on Hough circle option circular Hough transform is get applied only to the Part of IRIS.



scale
x0 131
y0 72
R0 114
T1 7.62911

Figure 7.Hough Transform applied Image

Edge Detection:

In Edge Detection Process, The points where the variation in the brightness of the image is abrupt are organized into a set of curved segments called edges.

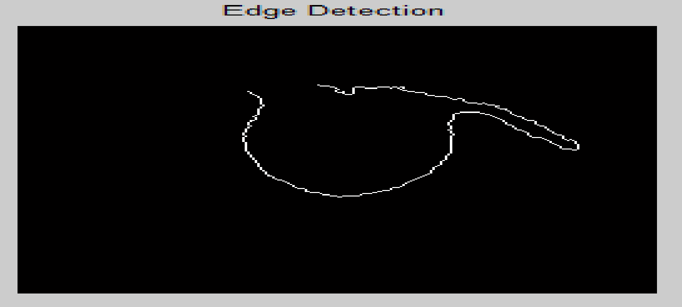


Figure 8.Edge Detection Image

Normalization:

In Normalization process, both the inner and outer boundaries of the iris have been detected; it is easy to map the iris ring to a rectangular block of texture of a fixed size.

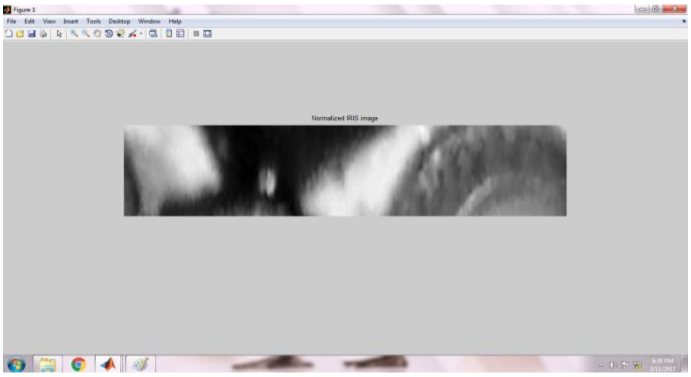


Figure 9.Normalized Image

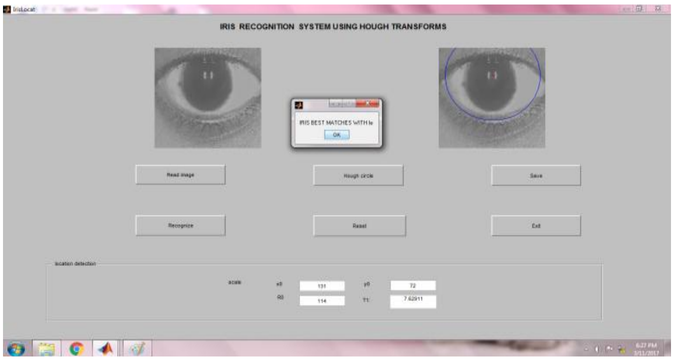
DOI10.17148/IJARCCE.2017.6762

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Recognition:
It will compare currently captured IRIS image with the image saved in database.



IRIS RECOGNITION SYSTEM USING HOUGH TRANSFORMS

IRIS BEST MATCHES WITH Ie

location detection

scale x0: 131 y0: 72

R0: 114 T1: 7.62911

Figure 10. Recognition Result Image

9. CONCLUSION

Biometric technology is more secure than RFID and GSM technology. In the biometric method, rather than fingerprint, face recognition IRIS recognition gives high performance. This concept will be very much useful in providing advanced high end Authentication and also problems such as carrying card etc will be avoided. As it offers high security, the unauthorized entry is restricted to maximum extent.

REFERENCES

[1] David Menotti, Member, IEEE, Giovani Chiachia, “Deep Representations for Iris, Face, and Fingerprint Spoofing Detection”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015

[2] Mohamed A. Kassem, Nagham E. Mekky, Rasheed M. EL-Awady, “An Enhanced ATM Security System Using Multimodal Biometric Strategy”, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:14 No:04,August 2014

[3] K. MAHESH, HARI HARA BRAHMAL, DR. G. KODANDA RAMAIAH, “ATM Based Recognition Technique on IRIS Technology with GSM Module”, International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04, Issue51, December-2015

[4] Raj M, Anitha Julian, “Design and Implementation of Anti-theft ATM Machine using Embedded Systems”, International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015 IEEE

[5] Pradnya M. Shende, Dr.Milind V. Sarode, “A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric”, International Journal of Computer Science Engineering and Technology, IJCSET, April 2014, Vol 4, Issue 4,129-132

[6] Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr.D.R.Kalbanded, “Enhanced security for ATM machine with OTP and Facial recognition features”, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[7] Shahrukh N. Maniyar, Swapnil A. Adsule, Purushottam A. Ekkaldevi, Rahul Bhivare, “Biometric Recognition Technique for ATM System”, International Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 4 Issue III, March 2016.

[8] Khattab M. Ali Alheeti, “Biometric Iris Recognition Based on Hybrid Technique”, International Journal on Soft Computing, IJSC November 2011 Vol.2, No.4

[9] Richa Singh,Mayank Vatsa,P. Gupta “Comparison of iris Recognition Algorithms”, IEEE, 2004.

[10] Mr C Raghavendra , Dr S. Sivasubramanian, Dr A M Sameeullah, “ HIGH PROTECTION HUMAN IRIS AUTHENTICATION IN NEW ATM TERMINAL DESIGN USING BIOMETRICS MECHANISM”, RESEARCH PAPER, Volume 3, No. 11, November 2012

[11] Prachi More1, Dr. S.D.Markande, “ Survey of Security of ATM Machine”, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 5, Issue 4, April 2016

[12] Diptadeep Addy, Poulami Bala,“ Physical Access Control Based on Biometrics and GSM”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 5, May 2016

[13] Lusekelo Kibona, “Face Recognition as a Biometric Security for Secondary Password for ATM Users: A Comprehensive Review”, 2015 IJSRST, Volume 1, Issue 2.

Copyright to IJARCCE

DOI10.17148/IJARCCE.2017.6762