IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

ADVANCE ATM SECURITY USING FINGERPRINT,IRIS WITH GSM TECHNOLOGY FOR OTP

Dinesh S. Chaudhari[1], Aditya S. Malvi[2], Pradnya K.Kadu[3], Pratiksha S.Potnurwar[4]

[1]*Student, C.S.E.Dept, J.D.I.E.T.Yavatmal, Maharashtra, India,***dineshchaudhari388@gmail.com**

[2] *Student, C.S.E.Dept, J.D.I.E.T.Yavatmal, Maharashtra, India,***aditya.malvi192@gmail.com**

[3] *Student, C.S.E.Dept, J.D.I.E.T.Yavatmal, Maharashtra, India,***pradnyakadu0202@gmail.com**

[4]*Student C.S.E. Dept, J.D.I.E.T. Yavatmal, Maharashtra, India,* **pratikshapotnurwar676@gmail.com**

Abstract

A fraud attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy this paper describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. Moreover, the feature of one time password (OTP) imparts privacy to the users and informs him/her from recalling PINs. Additionally the system provides protection to the ATM terminal from fire and thief attacks by making provisions of pump motor and a DC motor for rolling the shutter. In this system during registration the user's fingerprint and iris samples are retained in the database. The process of transaction begins by capturing and matching fingerprints and iris patterns. The system will automatically distinguish between real legitimate trait and fake samples. A GSM module attached to the ARM7 LPC2148 will message a 3-digit code generated by the system to the registered mobile number. After the valid OTP is entered the user can either withdraw or deposit cash or check his/her balance. In any kind of fake access attempts the account is blocked.

Keywords*—Authentication, Biometrics, Circular Hough Transform, Enrollment, Global System for Mobile Communication (GSM), Minutiae Based Algorithm, One Time Password (OTP).*

--- *** ---

I. INTRODUCTION

In modern era people are very much sensible about security issues in banking applications, like we go to the ATM to withdraw money, so every time we need to carry ATM card for that purpose and need to remember password i.e. 4-digit ATM pin to authenticate successfully. But, now the technology has been changed and people don't want to carry ATM card and keep remembering password given by bank every time to withdraw money from ATM (Automated Teller Machine). The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure).

The biometrics technologies used to measure and analyze personal characteristics. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security. Personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft. This paper will discuss the recent history of biometrics, benefits of biometrics over traditional authentication methods and how IRIS scan is so effective compare to other technology in banking industry for ATM purpose.

II.WHAT IS BIOMETRICS?

The expression "biometrics" is derived from the Greek words "bio" (life) and "measurements" (to quantify).Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. .Biometrics refers to programmed framework that utilises quantifiable physiological attributes or behavioural characteristics to perceive the personality or confirm the guaranteed character of a person. The personality of a personcan be recognized by three approaches, and these are: something you know (e.g., secret key, PIN), something you convey (e.g., ID card, keen card) and something you are (biometrics). 'Something you know' gives the first level of security, 'something you convey' and 'something you are' gives the second level of security. In savvy card, the unique finger impression layouts are encoded into a brilliant card memory, to recognize a person, his/her fingerprints are looked against the computerized formats, put away in the card memory. Personal administration framework is to locate the individual's character. Customary techniques for setting up a person’s character incorporate information based and token-based instruments, which can be effectively lost, shared or stolen.

Features of Biometric

1. Universality
2. Distinctiveness
3. Permanence
4. Collectability
5. Performance
6. Acceptability

A.FINGERPRINT BIOMETRICS

Every single person has his own unique fingerprint. So fingerprint is used for identification and forensic investigation since long time. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

Following are the steps for fingerprint scanning

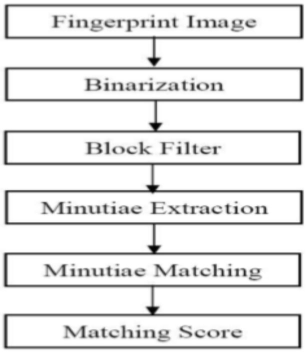

Fig-1: Steps for fingerprint scanning

B. Iris Biometrics

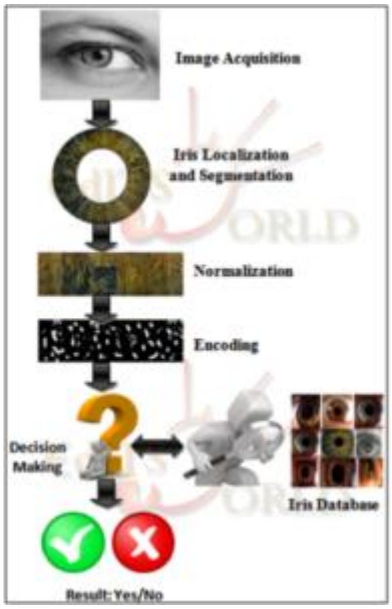

Fig 2: Steps for Iris scanning

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Each iris is a unique structure featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. The iris pattern is taken by a special gray-scale camera in the distance of 10-45 cm from the camera. Once the eye is stable and the camera has focused properly the image of the eye is captured. The iris scanning technology is not intrusive and thus acceptable by most users. Steps for Iris Scanning as follows:

1. Image Acquisition: Captures high quality image of the iris with good contrast and sufficient illumination.

2. Iris localization: the captured eye image is pre-processed and the iris region is isolated from it which consists of iris/sclera boundary and iris/pupil boundary.

3. Iris Normalization: It produces iris images of constant dimensions so that number of iris images being captured will have same features under different conditions.

4. Feature Extraction: canny detection is used for detecting the edges after applying circular Hough Transform for calculating radius and canter coordinates.

5. Storage and Matching: stores iris codes in the database where hamming distance algorithm is used for the recognition of the two samples.

III.PROPOSED SYSTEM

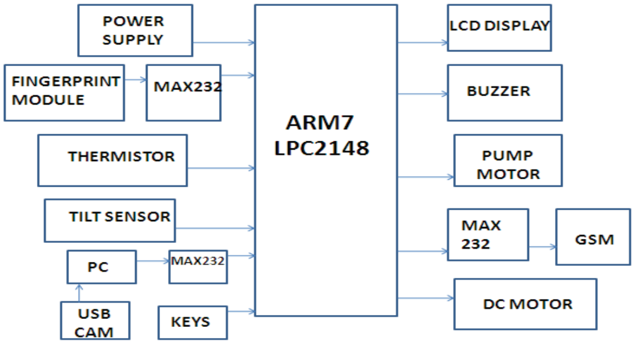

Fig 3:Block Diagram of ATM security

In the proposed system we present a method for detection of fraud access attempts made in an ATM transaction. Transaction security is enhanced by using biometric recognition. In this system ARM7 based LPC2148 controller in used for smart ATM access. The camera will capture the eye image of the person and send it to the controller. The controller will recognize the iris of the particular person from the image. The finger print module will take the finger print from the person and send it to the controller; the controller will recognize the finger print of a particular person from the database. If they match then it will display the data on the display unit, after which a 3 digit code is received by the customer on his/her registered mobile via a message.

GSM technology is used in this system for OTP generation. It is only after entering this valid OTP that the user is allowed for making further transactions. The thermistor continuously monitors the temperature of the ATM terminal which is indicated on the LCD display. No sooner the temperature rises above the threshold limit the alarm sound is indicated by the buzzer and the pump motor will be turned on. The tilt sensor will show the positions of the ATM. When the robber tries to change the position i.e. he shakes it ,a buzzing sound is heard and the DC motor will be started indicating the rolling down of the shutter of the ATM center.

A. Operation flow and implementation

1. **Fingerprint Scanning:** Customer's identity using fingerprints was checked by capturing real time fingerprint images of individuals using the optical sensor of the fingerprint module and storing256*288pixel images in bitmap format as real images during enrollment. During authentication both real and a fake user fingerprints were checked.

2.Iris Identification: Quality of the system developed for recognition of a person's iris was examined by means of a test which was conducted by capturing real time eye images of individuals using USB camera. The iris recognition was done using Hough transform. The iris image of each individual was captured and stored in a 640*480pixel bitmap format. During authentication both real and fake users were checked.

3. GSM technology for OTP generation: Global System for Mobile Communication is a digital cellular technology with the help of which we are able to transmit both voice and data services operating at 800MHz, 900 MHz,1800 MHz and 1900MHz frequency bands. It uses Time division multiple for communication and can carry 64kbps to 120Mbps of data rate.

IV. ALGORITHM AND FLOWCHART FOR PROPOSED SYSTEM

1. Start
2. Ask for finger print and iris scanning.
3. If fingerprint and iris is matched then Goto steps no. 4 else Goto to steps no.1
4. Send OTP on registered mobile number
5. Ask for OTP
6. If OTP is valid then goto steps no.7 else goto steps no. 1
7. Open user account for transaction.

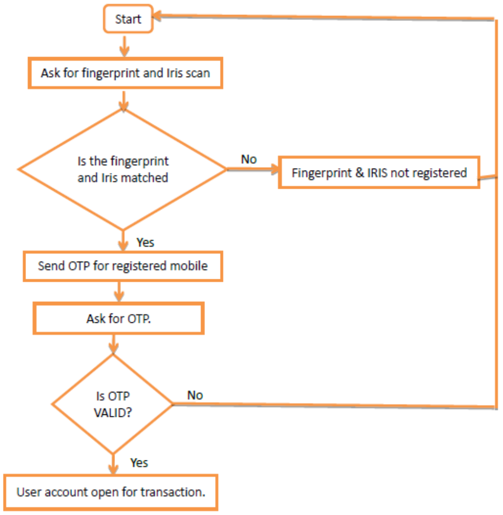
Start
Ask for fingerprint and Iris scan
Is the fingerprint and Iris matched
No
Fingerprint & IRIS not registered
Yes
Send OTP for registered mobile
Ask for OTP.
Is OTP VALID?
No
Yes
User account open for transaction.

Fig 4:Flowchart for proposed system

V. ADVANTAGES:

1. Robust system,
2. Low power management.
3. Quick response time.
4. Fully automated system.
5. Biometrics has no risk of.
   a. Forgetting it
   b. Getting copied
   c. Getting stolen
   d. Being used by anyone else

VI. LIMITATIONS:

1. This process is more costly as compare to current process.
2. A bit more time taken in all verification process.

VII. FUTURE SCOPE:

1. Performance can be increased in term of speed and memory.
2. Speaking voice alarm can be used to indicate unauthorized person accessing the ATM.
3. The system can be made to communicate with modem or mobile phone

VIII. CONCLUSION:

The use of the biometric as a password has made the ATM transaction system more reliable and secured. The OTP concept added to the system further enhances the security and avoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it user friendly and non-invasive. Using this system the ATM terminal is secured from fire and thief attacks.

ACKNOWLEDGEMENT

We would like to thank the anonymous references whose help and technical ideas have improved the quality of this paper.

REFERENCES

[1] Joyce soares and Arungaikwad (2016) fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP. 2016 international conference on Automatic and Dynamic optimization techniques (ICACDOT).international institute of information technology(IIIT) pune.

[2] Kandearchana (2015) Enhanced the security in the ATM System with Multimodal Biometrics and Two-Tier Security.. International Journal of Advance Research in Computer Science and Management Studies , 2. www.ijarcsms.com

[3] Kale, A.S. and Nanda, S.K. (2014) A Review Paper on Design of Highly Secured AutomaticTeller Machine System by Using Aadhaar Card and Fingerprint. International Journal ofAdvance Research in Computer Science and Management Studies , 2. www.ijarcsms.com

[4] Ghodke, S.S., Kolhe, H., Chaudhari, S., Deshpande, K. and Athavle, S. (2014) ATM TransactionSecurity System Using Biometric Palm Print Recognition and

Transaction Confirmation System. International Journal of Engineering and Computer Science. www.ijecs.in

[5] Karthik Nandakumar and Anil K. Jain, "Biometric Template Protection", *IEEE Signal Processing Magazine* September 2015.

[6] MohsinKarovaliya,SaifaliKaredia,SharadOza,Dr.D. R.Kalbande,"Enhanced Security for ATM machine with OTP and facial recognition features",InternationalConferenceon Advanced Computing Technologies and Applications(ICATA-2015).

[7] KhatmodeRanjit P, KulkarniRamchandra V, "ARM7 Based Smart ATM Accesss and Security System Using Fingerprint Recognition and GSM Technology", International Journal of Emerging Technology and Advanced Engineering, Vol.4, Issue 2,Feb. 2014.