International Journal of Research in Engineering, Science and Management
Volume-2, Issue-4, April-2019
www.ijresm.com | ISSN (Online): 2581-5792

Smart Banking Machine Embedded with Iris Biometric Controlled System

K. Jeevitha[1], R. Uma[2], R. Sangeetha[3], A. Preethi[4]
[1]*Assistant Professor, Department of ECE, R. M. K. Engineering College, Kavaraipettai, India*
[2,3,4]*UG Scholar, Department of ECE, R. M. K. Engineering College, Kavaraipettai, India*

***Abstract*: Nowadays all ATM card has PIN numbers, so the robbers easily hack the ATM card details. This prompted us to increase the security by including the biometric and security question to the existing system. In this, ATM cards are replaced by Biometrics and Red-tacton module. Moreover, the feature of security question increases privacy to the users in the same way. He/she can be free from recalling the PIN numbers. During the enrollment stage, we store the iris image of the user and the details of the user for the Red-tacton device. If the Iris Image is matched properly, then the next stage of using Red-tacton begins. The secret code stored in the Red-tacton will be passed to the receiver in the ATM machine, then transaction starts. Both the iris and Red-tacton code should be matched for the transaction else the transaction will be blocked.**

***Keywords*: Biometric security, biometric technology, ATM (Automated Teller Machine), Red-tacton, Point of Sale (POS).**

1. Introduction

According to RBI Report, about 25,000 accounts are opened in a day. In early days, transaction cannot be done in emergency situation and it also consumes more time so John Shepherd invented ATM (Automated Teller Machine). Drastic increase in the user account made to change the banking system. As users increased, fraudulent activity also increased equally so banking system gave more importance to security. Hence the need for security is increased rapidly. Biometric system measures the unique characteristics of a person so that no one can break the system. Because of this strong feature of Biometric, this idea evolved in banking sectors. Biometric includes Iris recognition, voice recognition, face recognition and fingerprint recognition. Among the various types of Biometrics used, Iris recognition transaction using ATM card is more convenient and simple, all the account holders rely on card system. But on the other hand cards can be created easily and account can be accessed. It is necessary to maintain the transaction reports. To overcome these disadvantages, card less system is implemented using Red-tacton. Red-tacton uses the surface of the human body as a safe, high speed network transmission path. This proposed system utilizes Red-tacton module instead of the Debit card used in the ATM sector. The Red- tacton module transmit a secret key of the account holder stored inside the Red-tacton transmitter through human body. In the systems, Bankers will collect the customer account details using Red-tacton, Iris and security question and its answer details while opening the accounts, then customer only access ATM machine.

2. Relevant work

Existing banking system gives unique four-digit number to all account holder. Whenever they need to access the ATM they enter the four-digit number. It is the simple method transaction and statistical, so that hackers can easily extract the numbers and access others accounts. Thus this paper [6] focused our attention on security towards banking sector. Biometrics has the feature of unique characteristics so the biometric based banking system emerged. During the creation of the account in the bank, the account holder's image and other details is being saved in the database. During transaction, the image is compared if both the image matches, the transaction permitted else declined. ATM is an Automated Teller Machine is invented in order to make the money transaction work easy and to make the availability to withdraw money in all emergency situation. All the account holder can access their account by giving them the PIN number. The PIN number accessing method is implemented in all devices like car, door, etc. Later it became insecure and easy for the hackers to hack those PINs. So this paper [19] increased security by using face recognition techniques with three different angles at a time. Face recognition starts with face scanning using high resolution camera, workstations, and software and back-end processors. Scanning is to capture the facial characteristics such as distance below the eyes, mouth, or nose and face cut of person. Devising a face grid algorithm and an effective ATM simulator forms is the main focus of future research.

This paper [5] focused on the security over money transaction because of the growing direct or spoofing fraudulent activity of thieves. This proposed system is more secure by providing personal identification by analyzing the biometrics like fingerprint, iris recognition. Since they are uniquely bound to individuals. This idea provides paper less banking environment and a secure ATM access. In this banking sector the samples of the fingerprint and iris along with the mobile number of the customer is saved in the database. Once the customer wants to access their account the image of the customer is captured and compared with the samples saved in

the database. Once the valid customer is found three-digit code will be sent to the registered phone number. This process is done using a GSM modem with the ARM7. The sent OTP and the entered OTP is being checked if it is verified then the system allow for transaction else the account will be blocked.

Because of the rapid growth of bank, everyone demand a transaction should be more secure and faster in ATM (Automated Teller Machine). Since Biometrics has a unique recognizing characteristics the biometric technology used all over for the transaction in ATM. Biometric technology in many different sectors provides a data privacy and a secured transaction. When comparing the features of other biometrics like handwriting, voice, iris, voice and fingerprint, fingerprint authentication is accepted widely.

The paper's [18] proposed System provide a faster and secured transaction by providing fingerprint based transactions. The server will have several samples of user's fingerprint, during transaction the person who tries for transaction fingerprint is taken using fingerprint scanner and the fingerprint will be compared with all the samples in the server and if that fingerprint is present in that database the person will be allowed for transaction else the process will be blocked. This fingerprint module can also added with Point Of Sale (POS) machine to eliminate the purpose of using physical debit cards.

This proposed system is effective if the user has only one account if the user has many accounts in different banks this system cannot deal. So that in future, this system will be enhanced by using the same fingerprint used to detect all the accounts the user holds in different banks.

3. Proposed system

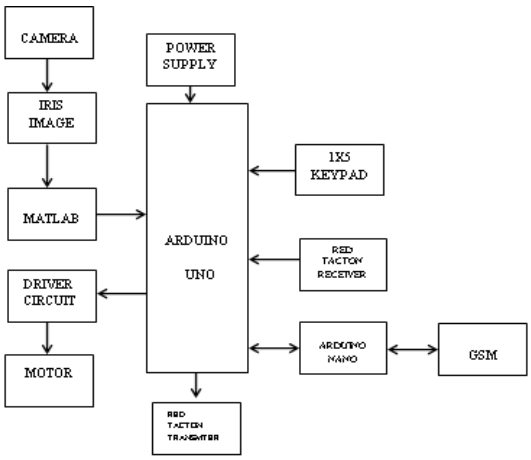

Fig. 1. Block diagram of proposed system

This proposed system utilizes Red-Tacton module instead of the debit card used in the ATM sector. The Red-TACTON module transmits a details of the account holder stored inside the Red-TACTON transmitter through human body. The controller checks the received data of the Red-tacton and waits for the user to match the IRIS details. Now the User will perform IRIS recognition. During the enrollment stage, we store the details of the user for the respected Red-Tacton device. Now the user's IRIS is detected by the MATLAB software. And MATLAB provides the data to the controller indicating the result of the user's IRIS detection process. If the matching of iris recognition is done, then MATLAB gives data to controller. Now the ATM mechanism starts working. The ATM working is indicated with the help of Motor. Once the Matching is performed, the motor is activated. In the case of emergency situation if the user friend went for the ATM behalf of the user then the IRIS is not matched. Then the System prompts the user with an OTP through GSM module to the user and the user can inform the OTP to his friend then the Motor starts to indicate that the User's friend is authenticated to access the ATM. Now the user can type the OTP on keypad.

A. Iris Recognition

Segmentation: Isolate the actual iris region from eyelids and eyelashes. Methods used are:

1. Hough Transform
2. Daughman's Integral differential operator.

Problems in Segmentation:

1. Orientation of eye image.
2. Low Contrast between iris and pupil.

Hough Transform:

1. Used to deduce radius and center coordinated of pupil and iris region.
2. Parabolic Hough Transform used to deduce eyelids.

Normalization:

1. Produces iris region nullifying the effects of dimensional inconsistencies.
2. Algorithm involves polar conversion of iris image.
3. Mapping of each of iris coordinate into polar grid using linear interpolation.
4. Separating only the annular iris ring thus eliminating pupil and other region.

Daughman's Rubber Sheet Model:

1. Model doesn't compensate for rotational inconsistencies.
2. Remaps each point within iris region to a pair of polar coordinates.

Feature Extraction:

1. Generated unique mathematical templates for iris images.
2. There are two widely used methods for feature extraction:
   - Gabor Filters
   - Haar wavelets

Total number of bits in template= 2* normalized image restoration.

Matching:

1. Reads templates and noise mark from database
2. Some design metrics that are available for matching templates
   - Hamming design metric

- Weighted Euclidean distance
- Canberra Distance metric

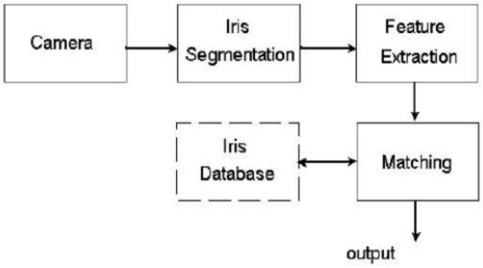

Fig. 2. A basic flow of the iris recognition

B. Red-Tacton

Red-Tacton is a Human Area Networking and Telephone corporation (NTT's). It uses Human body surface as a transmission path because it is completely distinct from wireless and infrared .Red-tacton uses the surfaces of the body because surface of the Human body generates minute electric field other than human body it also uses various other conductors and dielectrics as a transmission media. Red-tacton uses the laser beam to detect the changes in the optical properties of the electro-optic crystal. If the properties of the electro-optic crystal changed then the weak electric field is also changed. Red-tacton relies on this principle. Red-tacton transmitter induces the weak electric field on the surface of the body and the receiver senses the changes in the weak electric field and converts the result to an electric signal to the receiver circuit. It has a world wide applications which induces one-to-one service, marketing applications, Instant private data exchange, Personalization of mobile phone, conferencing system etc.

C. The MATLAB Language

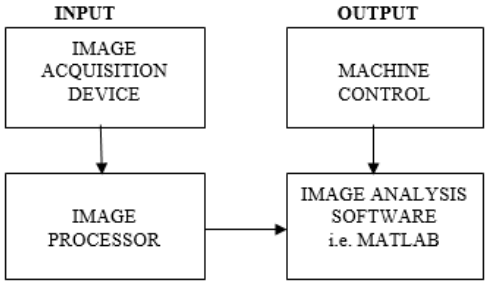

Fig. 3. Block diagram of MATLAB

The MATLAB Language provides native support for the vector and matrix operations that are fundamental to solving engineering and scientific problems, enabling fast development and execution. With the MATLAB Language, you can write programs and develop algorithms faster than with traditional languages because you do not need to perform low-level administrative tasks such as declaring variables, specifying data types, and allocating memory. In many cases, the support for vector and matrix operations eliminates the need for for-loops. As a result, one line of MARLAB code can often replace several lines of C or C++ code. MATLAB provides feature of traditional programming languages, including flow control, error handling, and object-oriented programming (OOP).

Uses of MATLAB:

MATLAB is widely used as a computational tool in science and engineering encompassing the fields of physics, chemistry, math and all engineering streams.

It is used in a range of applications including:

- Signal processing and communications
- Image and video processing
- Control systems
- Test and measurement
- Computational finance
- Computational biology

4. Result

Iris image of the account holders are captured and undergoes filtering then stored in the database.

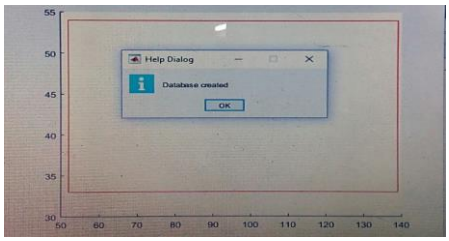

Fig. 4. Card less ATM-Enrolment

The LCD displays whether the accessing person is authorized user or unauthorized user.

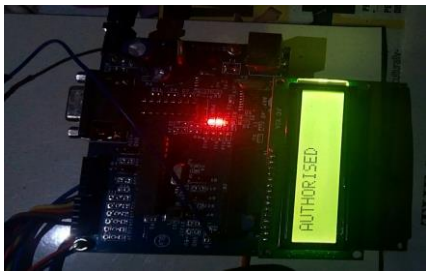

Fig. 5. Card less ATM-Authorized

Secret key is transferred using Red Tacton module from Red Tacton transmitter to Red Tacton receiver.

Fig. 6. Red-Tacton Transfer

Iris image is captured using camera and matched with the database, if the image matches then the user will be authenticated.

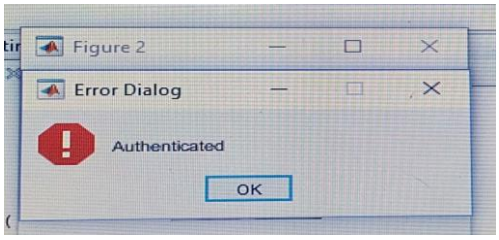

Fig. 7. MATLAB Unit

If the secret key transferred by Red Tacton and the iris image captured belongs to the account holder, then the transaction will be successful.

Fig. 8. Transaction successful

The LCD displays whether the accessing person is authorized user or unauthorized user.

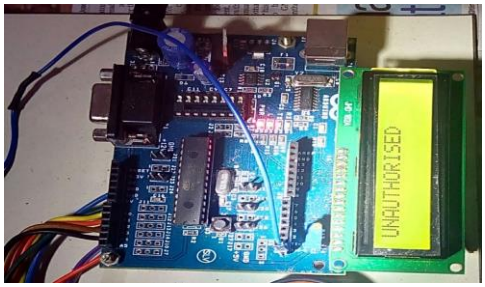

Fig. 9. Card less ATM-Unauthorized

Secret key is transferred using Red Tacton module from Red Tacton transmitter to Red Tacton receiver.

Fig. 10. Red Tacton Transfer

Using GSM Module message will be sent to the registered user.

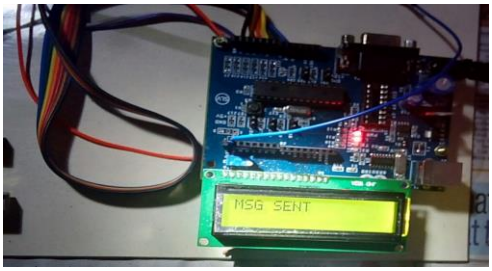

Fig. 11. GSM Module

Registered user answers the Security question.

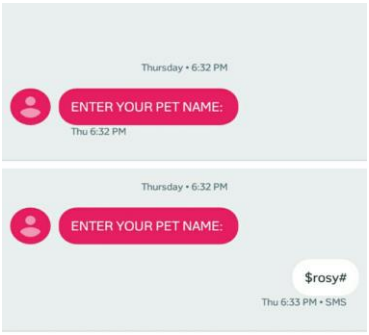

Fig. 12. Security Question

If the secret key transferred by Red Tacton and the answer for the security question belongs to the account holder, then the transaction will be successful.

Fig. 13. Transaction Successful

5. Future scope

In future the image can be captured from few feet far from the camera. ATM technology will be implemented with biometrics not only for the withdrawal of money but also for the deposit by simply scanning the Cheque and depositing. Since the use of biometric in ATM is quite expensive. The system can be added with a limit on amount of cash withdraw. For an Example: the fixed limit is 500. If the customer tries to withdraw money below 500 the biometric scanning is not mandatory they need to enter the security answer for accessing the ATM.

6. Conclusion

From the above model it is clear that it is not mandatory to carry the ATM card with them and they are free from

recollecting the PIN numbers. The level of security is high in the model so the fraudulent activity is reduced in higher level. The efficiency of the system increases gradually.

References

[1] Joyce Soares, A. N. Gaikwad "Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP" 2016.
[2] Mohsin Karovaliya, Saifali Karedia, Sharad Oza, D. R. Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features", International Conference on Advanced Computing Technologies and Applications (ICATA-2015).
[3] Reshma Begum, Basavaraj Gadhay, Veeresh Pujari and Pallavi B, "Security of ATM System Using Biometric and OTP", International journal, vol. 5, No.4 June 2017.
[4] Chavan Jagruti Kailas, Choudhary Kusum Savaram, Gavade Ankita Vijay Kumar, "ATM security based on Iris Recognition", International Research Journal of Engineering and technology, Vol.5, Issue 4, April 2018.
[5] Joyce Soares, A. N.Gaikwad "A Self Banking Biometric Machine with fake Detection Applied to Fingerprint and Iris along with GSM Technology for OTP", 2016.
[6] G. Renee Jebaline, S. Gomathi, "A Novel Method to Enhance the Security of ATM using Biometrics", International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2015.
[7] Ahmad Tasnim Siddiqui, "Biometrics to Conrol ATM Scams: A Study", International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2014.
[8] Prakash Chandra Mondal, Rupan Deb and Md. Nasim Adnan, "On Reinforcing Automatic Teller Machine (ATM) Transaction Authentication Security Process by imposing Behavioral Biometrics", The International Conference on advance in electrical Engineering (ICAEE), September 2017.
[9] Czajka, "Pupil dynamics for iris liveness detection," IEEE Trans. Inf. Forensics Secure., vol. 10, no. 4, pp. 726–735, Feb. 2015.
[10] Deepa Malviya, "Face Recognition Technique: Enhanced Safety Approach for ATM", International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.