International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# ATM WITH AN EYE

*[1]Bhargavi K,[2]Veena S*

SJC Institute of Technology

ABSTRACT:

The technique proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account *and* the live image and stored image match would a user be considered fully verified. We will also look into an automatic teller machine security model providing the customers a card less, password-free way to get their money out of an ATM. Just step up to the camera while your eye is scanned. The iris the colored part of the eye the camera will be checking is unique to every person, more so than fingerprints.

Keywords: ATM, Iris, Facial Recognition.

## INTRODUCTION:

ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share. Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account.

The model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure. The paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account and the live image and stored image match would a user be considered fully verified.

When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for use in fraud transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions.

## LITRETURE SURVEY:

Face Recognition Application for Automatic Teller Machines (ATM): by Abdul-Hay Akbar Pandor[1]

In the article about biometric systems the general idea is to use facial recognition to reinforce security on one of the oldest and most secure piece of technology that is still in use to date thus an Automatic Teller Machine. The main use for any biometric system is to authenticate an input by Identifying and verifying it in an existing database. Security in ATM's has changed little since their introduction in the late 70's. This puts them in a very vulnerable state as technology has brought in a new breed of thieves who use the advancement of technology to their advantage. With this in mind it is high time something should be done about the security of this technology beside there cannot be too much security when it comes to people's money. High Protection Human Iris Authentication

In New ATM Terminal Design Using Biometrics Mechanism: by Mr C. Raghavendra[2]

For the traditional ATM terminal customer recognition systems only rely 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, using a Biological Technology in new ATM terminal customer recognition systems i.e., IRIS Biometrics Mechanism. A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Using iris recognition in ATM a customer simply walks up to the ATM and looks in a sensor camera to access their accounts. The camera instantly photographs the iris of the customer. If the customers iris data matches the record stored a database access is granted.

## BLOCK DAIGRAM:

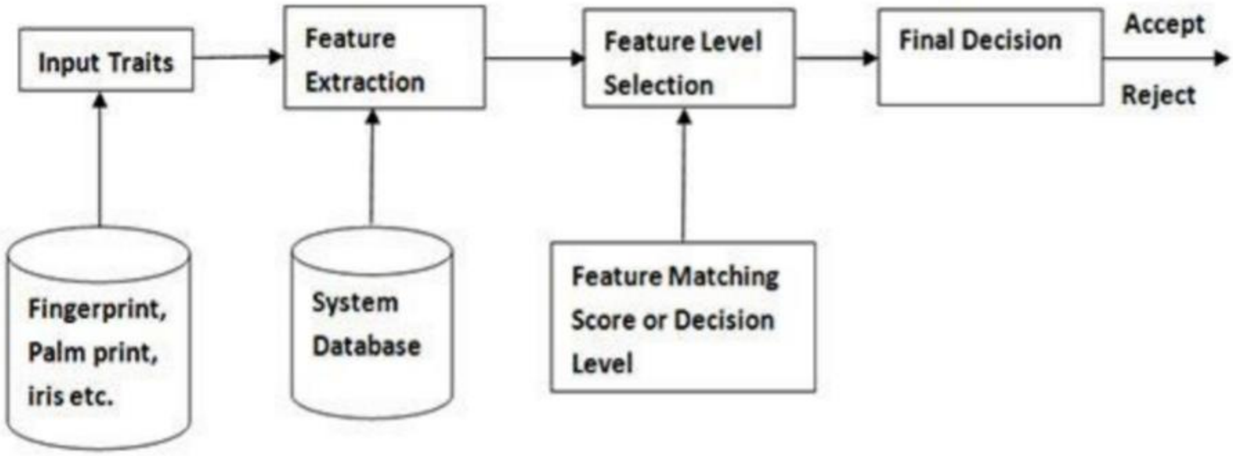


Fig: Block Diagram of the System

The figure shows the Block Diagram of the system. The working of the system is explained by the above figure. The person who want to withdraw the money from the ATM will insert the card and enter the pincode. For the security reason the next step is to verify the persons fingerprint, palm print, iris etc. these are taken as the input trials and sent for feature extraction. In the feature extraction the extracted input data is matched to the data present in the system database. Next the feature level selection will be checked. Then the feature matching score will be detected. Depending upon the feature matching score final decision will be taken whether the person can withdraw the money or not.

## TECHNOLOGY:

The technology used in the project ATM with an eye is Biometric Identification Techniques

1. Fingerprint Verification
2. Retina Scanning
3. Facial Recognition
4. Iris Recognition

### *1. Fingerprint Verification:*

One kind of biometrics technology is fingerprint scanning. We are using our fingers to access the ATM machine and make a transaction. We utilise this method since it's simple to line up. We don't need to get obviate the present ATM machine. The verification module is split into three sub-modules:

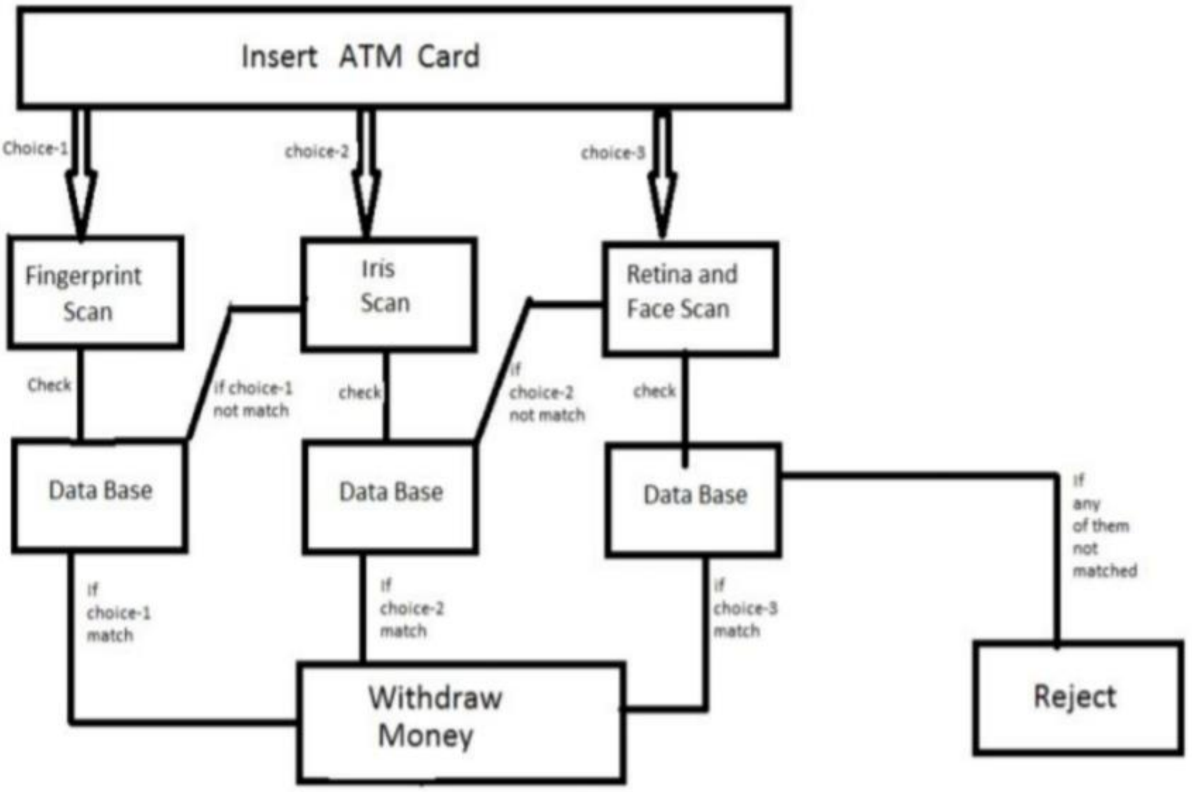
1. Fingerprint Enhancement
2. Feature Extraction
3. Matching

The ATM fingerprint functioning procedure involves obtaining data from a server. We must first get authentication from the bank before proceeding with the method. A biometric machine is employed by a bank employee to scan his or her fingerprint. Enrolment is that the process by which a biometric equipment extracts the features of a fingerprint and stores them during a database. When a client wants to use an ATM that has been biometrically scanned, he must first place his finger at the sensor. First, the biometric scanner will scan it and compare it to the stored feature and If the feature match then the person is allowed for transaction otherwise it not process.

### *2. Retina Scanning:*

Retinal scan is a highly dependable technology because it is highly accurate and difficult to spoof, in terms of identification. The technology, however, has notable disadvantages including difficult image acquisition and limited user applications. Often enrollment in a retinal scan biometric system is lengthy due to requirement of multiple image capture, which can cause user discomfort. However, once user is acclimated to the process, an enrolled person can be identified with a retinal scan process in seconds. Retinal scan technology has robust matching capabilities and is typically configured to do one-to-many identification against a database of users. However, because quality image acquisition is so difficult, many attempts are often required to get to the point where a match can take place. While the algorithms themselves are robust, it can be a difficult process to provide sufficient data for matching to take place. In many cases, a user may be falsely rejected because of an inability to provide adequate data to generate a match template. Because retinal blood vessels are more absorbent of log-energy infrared light than the rest of the eye, the amount of reflection varies during the scan. The pattern of variations is converted to computer code and stored in a database.

## FLOW CHART:



ATM UID operation starts when the account older shows their UID card, unique for each person, to the UID reader for scanning. The account related to the unique UID number will be opened. The next step involves scanning of the iris using a camera that will take an image of the iris pattern and after various methods, will generate a code for the iris pattern. If the code matches the iris pattern code of the account being accessed, stored in the database, then the transaction will be allowed. Otherwise, the account information will not be displayed and further activity will not occurs. The iris is the colour ring surrounds the code matches the iris pattern code of the account being accessed, stored in the database, then the transaction will be allowed. Otherwise, the account information will not be displayed and further activity will not occurs. The iris is the colour ring 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, strings, spots, pits.

## CONCLUSION AND FUTURE SCOPE

### *Conclusion:*

We thus develop an ATM model that is more reliable in providing security by using facial recognition software. By keeping the time elapsed in the verification process to a negligible amount we even try to maintain the efficiency of this ATM system to a greater degree. One could argue that having the image compromised by a third party would have far less dire consequences than the account information itself. Furthermore, since nearly all ATMs videotape customers engaging in transactions, it is no broad leap to realize that banks already build an archive of their customer images, even if they are not necessarily grouped with account information.

### *Future Scope:*

Iris technique finds a wide range of applications in fields involving high security concerns. It is use of your body as a security measure. This biometric technique can be used in many fields like shipping, medical sciences, computer sciences, home security. It is progression in the field of technology there by giving a great push to the technology industry. Many projects related to security and control can be implemented by this biometric technique. There is problem, if anyone eye damage then he cannot withdrawal his/her own money. So, if we use various biometric then this problem solve sometimes.

**References:**

1) Abdul-Hay Akbar Pandor, Face Recognition Application for Automatic Teller Machines (ATM), International Conference on Information A Review on an ATM with an Eye Koushik S at Eureka Journals, Vol. 45, Issue 268, 2018, pp 91-95.
2) Mr C. Raghavendra., High Protection Human Iris Authentication In New ATM Terminal Design Using Biometrics Mechanism, Journal of Global Research in Computer Science, Vol. 3, Issue11, 2012, pp 15-36
3) K. Laxmi Narshima Rao, Recognition Technique for ATM based on IRIS Technology, International Journal of Engineering Research and Development, Vol. 3, Issue 11, 2012, pp 39-45.
4) B. Sundar Raj, A Third Generation Automated Teller Machine Using Universal Subscriber Module with Iris Recognition, International Journal of Innovative Research in Computer and Communication Engineering, Vol.1, Issue 3, 2013, pp 90-106.
5) Aru, Facial Verification Technology for Use inAtm Transactions, American Journal of Engineering Research (AJER), Vol. 02, Issue-05,2017, pp-188-193.
6) Divyarajsinh N. Parmar, Face Recognition Methods & Applications, Divyarajsinh N Parmar et al, Int. J. Computer Technology & Applications, Vol 4, Issue 1, 2019, pp 84-86.
7) GazalBetab and Ranjeet, Fingerprints in Automated Teller Machine-A Survey, International Journal of Engineering and Advanced Technology (IJEAT), Vol. 3, Issue 4, 2014, pp 1287-1393
8) Deepa Malviya, Face Recognition Technique: Enhanced Safety Approach for ATM, International Journal of Scientific and Research Publications, Vol. 4, Issue 12, 2016, pp 308-390
9) https://youtu.be/gRL--Ciol-k
10) https://youtu.be/WeSS3PLWnVM