Accessing the bank account without card and password in ATM using biometric technology

Mini Agarwal [1] and Lavesh Agarwal [2]

Teerthankar Mahaveer University
Email: miniagarwal21@gmail.com[1], lavesh_1071985@yahoo.com[2]

Abstract: Now a day's everyone uses ATM (Automated Teller Machine) for secure transaction but always carrying the ATM card is very difficult. Many times we forget to carry ATM card and sometimes forget the password. Hackers can easily hack the password in the current era. In this paper we introduce the biometric technology in ATM and we also use the extra feature i.e. cell number that easily describe the user identity. Many users have account on same bank so consuming the less time in searching process because each user has its personal cell number , firstly we type the cell number and then can use the biometric technology as an ATM card and biometric password so that without card user can withdraw the cash. We can secure the person's identification and card from thief and hackers through biometric system because each person has unique iris, finger print voice etc.
[Mini Agarwal and Lavesh Agarwal. **Accessing the bank account without card and password in ATM using biometric technology.** Researcher. 2012;4(3):33-37]. (ISSN: 1553-9865). http://www.sciencepub.net. 7

Keywords: hackers, thief, PIN, connectors, withdraw.

Introduction:

In a past days withdraw, saving cash and detail of bank account through bank was very tough work but now a days every used the ATM because it's the most easiest way for withdraw the cash and check the any type of details of their accounts. Many banks open its many ATMs on various places so every one easily withdrawal the cash and check the any type of details of their accounts through any bank ATM. But in today life we have many passwords like lock, email, car radio, mobile phones, computers, bank lockers ATM card etc and users have many cards like Credit card , Debit card, Identity card, PAN Card etc, so the many problems face by user related to ATM card and its passwords some are given below:

1. Tough work to remembering lots of passwords many times user forgets its passwords through forgetting password some times it creates the big problem like user didn't withdraw the cash any details of account and some times ATM card was hacked.
2. The problem comes around when we forget to carry its ATM card. If he has no cash at that time than it create the big problem.
3. Some times user only choose the one password of all things like email , mobile phones etc but it has also deficiencies like if any one knows the his password then the thief or any relative easily use the ATM card.

So removing these types of deficiencies we introduced the ATM machine with biometric system. Various biometric technologies are introduced in current era like iris, finger, voice, wrist and so forth. Each user has its unique identity it's based on physical or behavioral attributes. These attributes are never stolen by any person. But if we only use the biometric technology for opening the account instead of ATM card than it is very time consuming process because millions users use the ATM card then users biometric id checked to million users biometric id . This process consumes the many hours. So, we add the extra feature mobile cell number with biometric system. In the ATM firstly we enter the mobile number with human's biometric id like iris, finger, voice etc. So through mobile number firstly we search the persons account then through biometric matching it open's the account and then again need the biometric id as a password for confirmation of withdraw because sometimes user doesn't close the account for security purpose again match the biometric id.

Working of Biometric technology:

Biometric devices depend on the humans physical and behavioral attributes like figure prints, eye recognition, voice recognition, signature etc. working or operation is similar in all biometric devices. In these devices at the time of human enrollment biometric attributes stored on the in database and at the time of matching input attributes of human matched to the already stored attributes.

The performance or total time of biometric devices is depending upon the acceptance and rejection time. If the acceptance time is high means it takes the several minutes in accepting the user and if the rejection time is high it means it's not the correct user. So, if any time means acceptance or rejection time is high then the performance of the biometric is worst. If both acceptance and rejection process takes the less time minutes some seconds then the performance of the biometric process are excellent. So

the working of biometric is depending upon the enrollment, identification or verification.

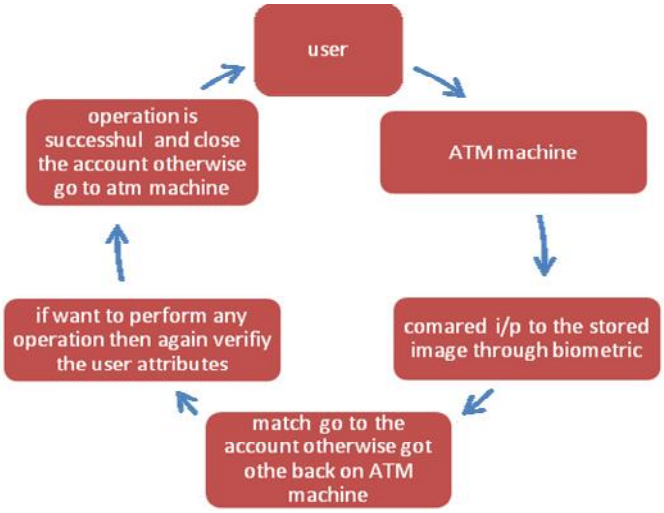

Fig (1): working of ATM with biometric technology.

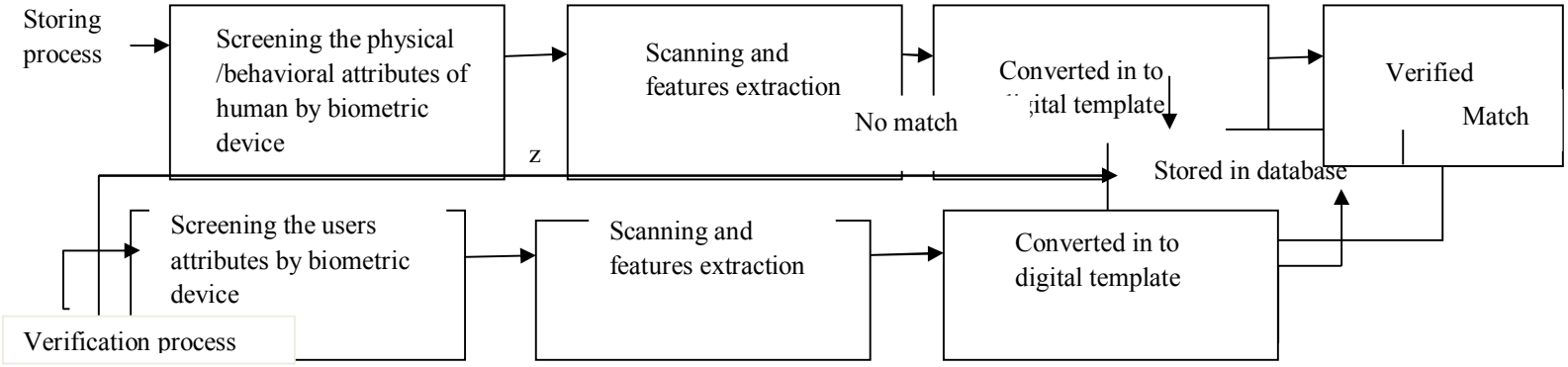

Fig (2): working of biometric device Comparison between password, ATM Card and Biometric system

ATM Card	Password	Biometric
Always need for carrying the card	Password always need for remembering in memory	In this no need for any type of remembering the password
Easily hack by other persons	Its easily hack by other persons	Every human has unique attributes so if any person no this he is nothing doing
No need for user identification	No need for user identification	Need for human identification
It doesn't provide any type of security	It doesn't provide any type of security	It provides high level security

So biometric technology are more secured then ATM card and password. And every one easily handle this because in this no need for carryinging and recalling the card and password.

Verification through biometric devices in ATM:

Now time we used various types of biometric devices but we describe here verification through two or more biometric devices that are described below:

1. Iris technology:

In iris technology verification is totally depend upon the users eye at the time of opening the bank account the humans iris enrollment has done in this a large mega-pixel camera taken the iris picture but it concentrate on the

some specific points see in fig (1) and converted in to a useful or digital template and saved in to the database with cell number of the user because for speeding the process we use the cell number as the temporary identity. At the time of verification current input compared to the stored template. If the match found it means he is a correct user otherwise he is not the authenticated user. When user want to access the account through ATM at that time ATM firstly display the message enter yours cell number. After entering the cell number if cell number is correct then through biometric machine in ATM user gives his physical attributes means iris then attached camera in the ATM machine takes the images of iris and converts the specific points in to digital form these digital template compared to the stored image if match found then the user is correct user otherwise he is fraud. When account is opened if user wants to withdraw the money at that time for security purpose ATM machine with biometric technology again do the verification because some times users forget to close their accounts.

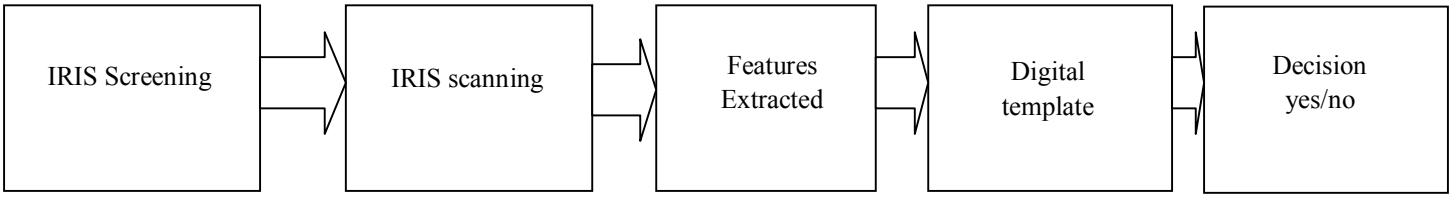

Fig (3): Iris verification process

2. Finger print technology:

Finger print technology is same to the iris technology. This technology totally depends upon the prints of finger. At the time of opening the bank account in enrolled process bank take the finger print of the user and extract the extra features from the finger and then these extra features converted in to the digital template this digital template stored in the database with cell number of the user because for speeding the process we use the cell number as the temporary identity. When user want to access the account through ATM at that time ATM firstly display the message enter yours cell number. After entering the cell number if cell number is correct then through biometric machine in ATM user gives his physical attributes means finger prints then these current finger prints and converted to the digital template and then compared to the user finger print template that stored with cell number if it matches then user go to his account. Otherwise machine display wrong user. At the time of performing any operation user again takes the finger print and check it for security purpose.

Fig (4): Finger prints verification process [2].

3. Voice recognition:

Voice recognition is a simple and easiest method of biometric. This technology totally depends upon the user voice. At the time of opening the account in the bank in enrolled process bank captures the word or a sentence of a user to voice recorder. This word or sentence converted in to the spectrogram. Spectrogram is a graph that represents on the basis of sound frequency and the time this graph store on the database with cell number of the user because for speeding the process we use the cell number as the temporary identity. When user want to access the account through ATM at that time ATM firstly display the message enter yours cell number. After entering the cell number if cell number is correct then through biometric machine in ATM user gives his voice then this voice converts in to the spectrogram. This spectrogram compared to the stored spectrogram if both are matches then account is open

otherwise it shows the message try again. At the time of performing any operation like withdraw etc ATM machine again verify the voice for security purpose.

4. Facial recognition:

Facial recognition in biometric is very simple technology. This technology totally depends on the humans face. At the time of enrolling process bank captures the user image. This user image divides in to several grids these several grids have human features these human extracted features stored on the database with cell number of the user because for speeding the process we use the cell number as the temporary identity. When user want to access the account through ATM at that time ATM firstly display the message enter yours cell number. After entering the cell number if cell number is correct then through biometric machine in ATM user scan his face as an input. Extra features extracted in to the users face scan and compared to the stored database. If both are matches then account is open otherwise it shows the message try again. At the time of performing any operation like withdraw etc ATM machine again verify the voice for security purpose.

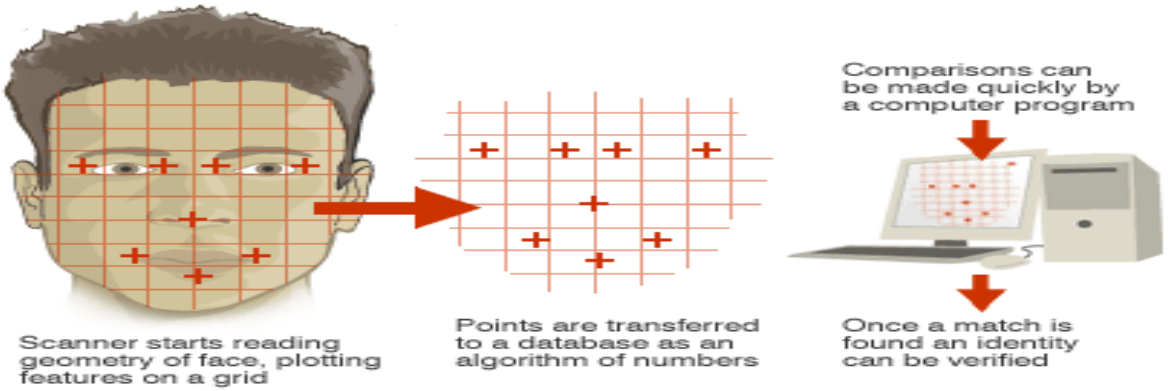

Fig (5): Steps in facial recognition

Requirements for ATM with biometric technology:

Some of the requirements are given below:

- Automated teller machine (ATM)
- Voice, iris, finger facial biometric scanner
- Cables, connectors, usb ports, ups, recorder
- Any operating system like windows, Linux etc
- Database storage like oracle, sql etc
- Any application software like c#, java, .net etc
- Biometric software, drivers and experts
- ATM operator
- Software engineers
- Tester engineers
- Users

Comparison between Iris, facial, finger and voice recognition:

	Iris	**Finger**	**Voice**	**facial**
Specific requirement	camera	Finger scanner	Voice recorder	camera
Input conversion	Feature extraction	Feature extraction	spectrogram	points
cost	Costly	Medium	cheap	medium
Reliability	high	medium	low	medium
Accuracy	high	medium	low	medium
Processing	slow	fast	fast	slow
Interferences	Irritations , glasses	Dust , injury	Cold, noise	Swelling, injury, surgery

Survey:

In a survey of biometric technology we saw that 85% people trust on the iris technology because they said hackers hack the finger prints, voice, facial recognition but them can't change or got the same eye. Each person have unique eye. But 10% users said that finger print is the easy method for biometric because only in this we scan our finger. And 5% people likes voice recognition because only in this we say a one word or sentence and last 5% people likes the facial recognition because this like a click a picture through camera.

Conclusion:

In this paper only we represent that if we have no ATM card or no password then we also access the our account through ATM. We only want to secure our transaction because each person has their unique physical or behavioral attributes that can't be stolen by any one. We remove the password and card forgetting problem. Through biometric technology verification process is done easily and also increasing the account security.

References:

1/21/2012

1. Lynne Coventry, Antonella De Angeli and Graham Johnson "Usability and Biometric Verification at the ATM Interface "Ft. Lauderdale, Florida, USA • April 5-10, 2003.
2. Emuoyibofarhe , Fajuyigbe O., Emuoyibofarhe O.N , Alamu F.O. "A Framework for the Integration of Biometric Into Nigerian Banking ATM System" International Journal of Computer Applications (0975 – 8887) Volume 34– No.4, November 2011.
3. Deane, F.P., Henderson R.D., Mahar D.P. and Saliba A.J. Theoretical examination of the effects of anxiety and electronic performance monitoring on biometric security systems, interacting with Computers, 7.
4. Ashbourn, J. Biometrics. Advanced Identity Verification. Springer Verlag, London, 2000.
5. Automated Teller Machine (2007) http://en.wikipedia.org/wiki/Automated_teller_machine .
6. Fig (4) http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn2page1.stm.