ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9 September, 2014 Page No. 8356-8361

New level of Security in ATM System Using Brain Fingerprinting

N.Geethanjali,
Assistant Professor,
Department of Computer Science and Engineering,
SNS College of Engineering,
Coimbatore
anjali.ckec@gmail.com

ABSTRACT

Security plays a vital role in all fields and in various applications. The existing computer security systems used at various places like banking, passport, credit cards, smart cards, PIN (Personal Identification Number), access control and network security are using username and passwords for person identification. In distributed system like ATM (Automated Teller Machine) the security is a main issue. The security level has been grown from providing PIN to Smart Card to Biometrics. Even though the security has been increased at the same time fraudulent activities have been grown to equal level. In the existing approaches different biometric technologies, multibiometrics, multimodal biometrics and two tier security is introduced in ATM to provide higher level of security. The proposed work is to enhance the security using brain fingerprinting technology which acts as an uncrackable password. A brain computer interaction has been developed to record the brain signal through Digital Electroencephalography. Brain fingerprinting is a technique used to find the unique brain-wave pattern generated by brain when a person encounters a familiar stimulus.

Keywords

ATM (Automated Teller Machine), Security, Biometrics, Multimodal biometrics, Multibiometrics, Brain fingerprinting

1. INTRODUCTION

In this era, world is bounded with technology. Every day comes up with different technologies which make the human more sophisticated and at the same time they are facing more problems. Rapid development of banking technology has changed the way how the banking activity is carried out which has both positive and negative impact in automated teller machine (ATM). ATM was first used in 1939. There are two important aspects that need to considered in ATM. First one is the idea about the communication with ATMs and the second thing is the security in ATM [1]. According to various researches there are more than 2.2 million ATMs deployed worldwide. It is suspected that there will be 3 million ATM by 2016. As the number of ATMs usage increases, the frequency and sophistication of security threats also increases. ATM crime is not limited to the theft of cash in ATM. Many ATM attacks seek to obtain a user's personal information, such as their card number and personal identification number (PIN).

ATM threats can be segmented into three types of attack:

- Card and currency fraud
- Logical Attacks
- Physical Attacks

CARD AND CURENCY FRAUD:

It involves both direct attacks to steel cash from the ATM and indirect attacks to steal a consumer's identity (in the form of consumer card data and PIN theft).

1) **ATM card skimming** is the most prevalent and well known attack against ATM. Card skimmers are devices used by perpetrators to capture cardholder data from the magnetic stripe on the back of an ATM card.

2) **Card Trapping/ Fishing** attempt to seal consumers' cards as they are inserted into the card reader during a transaction. The purpose of this type of attack is to steel the card and use it at a later time

3) **Currency Trapping/Fishing** is an attempt by perpetrators to capture currency that is dispensed by the ATM during a transaction.

LOGICAL / DATA ATTACKS:

It is the most difficult attacks to detect logical attacks that target an ATM's software, operating system and communication systems.

1) **Malware and Hacking** is done by installing malicious software to violate the confidentiality, integrity and/or authenticity of data on the computer system.

PHYSICIAL ATTACKS:

Physical attacks on an ATM include any type of assault that physically damages the components of the ATM in an attempt to obtain cash. While the entire ATM can be a target for a physical attack, specific components of the ATM are often targeted.

The rest of the paper is organized as follows: The **section 2** presents the existing security measures taken in ATM and **section 3** explains the proposed approach of brain fingerprinting and how it works in ATM. In **section 4** conclusion and future work has been presented.

2. RESEARCH BACKGROUND

The PIN protection in ATM can be easily hacked by trying out various probabilities. Once user's bank card is lost or password is stolen, the users account is vulnerable to attack. Despite warning many people continue to choose easily guessed PIN's and passwords- birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem.

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Biometrics refers to the physiological or behavioural characteristics of a person to authenticate his/her identity[2]. Biometric systems based on single source of information are called Unimodal systems. Multimodal biometrics is an integration of two or more types of biometric system and it provides a secondary means of identification. The integration of two or more types of biometric verification systems helps to meet stringent performance requirements set by security conscious customers. The biometric system is a combination of various unimodal biometrics; it aims to fuse two or more physical or behavioural traits. After determining which biometric sources are to be integrated, then the next step is to build the system architecture[3].

Physical biometrics is a static biometrics and the data is derived from the measurement of an action performed by an individual. It includes fingerprint, Iris, Retina, Hand geometry, Palm print, Face recognition, DNA and Vascular Pattern Recognition. Behavioural biometrics is a dynamic biometrics and the data is derived from the measurement of an action performed by an individual and the parameter considered over here is time; the measures action has a beginning, middle and end. It includes signature, keystroke, Handwriting, Voice recognition and Gait. Soft biometrics also known as chemical biometrics is a human characteristic that provide some information about the individual. It includes height, weight and color of hair [4].

2.1 UNIMODAL IN ATM SYTEM

The oldest and successful technology which is implemented in ATM is fingerprint recognition **[5].**The algorithms used for fingerprint recognition are minutiae extraction and singular point detection. After the user inserts the card in the ATM system and enters the PIN number, if the PIN number is valid, then the user needs to print his/her fingerprint for authentication purpose. If the fingerprint template matches with the template which is stored in the database during enrollment, then the user is authenticated and he/she can access their account which is shown in figure1. The reason behind the popularity of fingerprint-based recognition among the biometric-based security systems is the unchangeability of fingerprints during the human life span and their uniqueness. This type of system provides the basic level of security and the error rates is high**.**

LIMITATIONS OF UNIMODAL BIOMETRICS:

Biometric system is essentially pattern recognition system that operates by acquiring biometric data from an individual. Biometric systems are often affected by the following problems **[4]:**

- **Noise in sensed data**- The accuracy play a major role in recognition of biometrics. The accuracy of the biometric system is very sensitive to the quality of the biometric input and the noise present in the data will result in a significant reduction in the accuracy.
- **Non-Universality**- If every individual is able to present the biometric trait for recognition, then the trait is said to be universal. Non-universality leads to Failure to Enroll (FTE) error in a biometric system.
- **Lack of individuality**- Feature extracted from different individuals may be similar. This lack of uniqueness increases the False Accept Rate (FAR) of a biometric system.
- **Intra-class variations**- The data acquired for verification will not match to the data used for generating template during enrollment. For example the face biometric is captured under different angle. Large intra-class variations increase the False Reject Rate (FRR) of a biometric system.
- **Inter-class variations**- It occurs mainly between twins. It refers to the overlap of feature spaces corresponding to multiple individuals. Large inter-class variations increase the False Acceptance Rate (FAR) of a biometric system.
- **Spoofing**- A biometric system may be circumvented by presenting a fake biometric trait to the sensor.

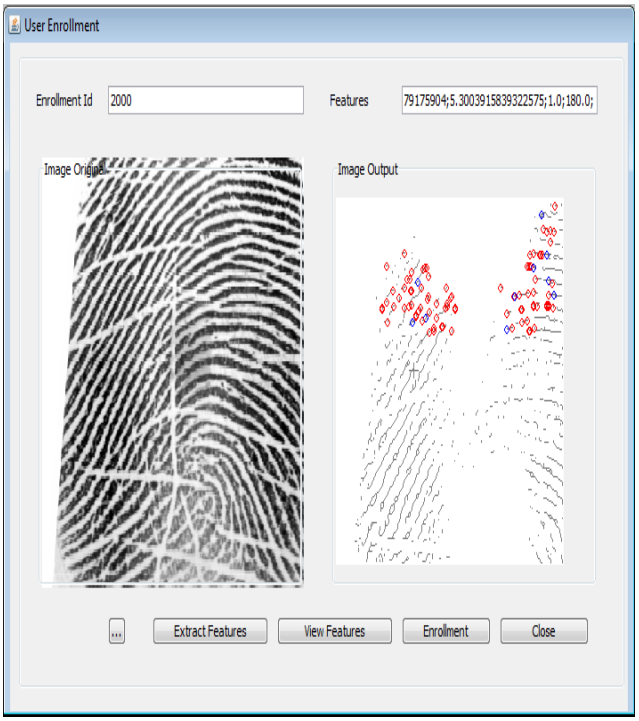

Figure 1: Unimodal biometrics implemented in ATM

2.2 MULTIBIOMETRICS IN ATM SYSTEM

Multibiometrics is a combination of one or more biometrics. It can be any physical or behavioral biometrics. Multibiometrics overcomes the problem of unimodal biometrics **[5].** These systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. This system

mainly addresses the problem of non-universality and provides anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple traits of a legitimate user. There are variety of factors that need to be considered while designing the multibiometric system, these include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated. Based on the multiple sources multibiometric systems are classified as Multi-sensor systems, Multi-algorithm systems, Multi-instance systems and Multi-sample systems. There are various level of fusion like Sensor level fusion, Score level fusion, Matching level fusion and feature level fusion **[6][7].**

Multibiometrics is mainly used to provide security in the server side. The fingerprint, Iris and Face recognition is used to provide security. The features are extracted from biometrics using feature level fusion and the features are combined into single biometric and biometric cryptosystem scheme is used to protect the template. In figure 2 the system flows like the person needs to insert the ATM card and enter the PIN number. If it is valid, it undergoes the fingerprint, Iris and Face scan and all the biometrics are verified. If all the template query matches with the template stored in the database during enrollment, the user will be authenticated as authorized person and he will be able to access his/her account.

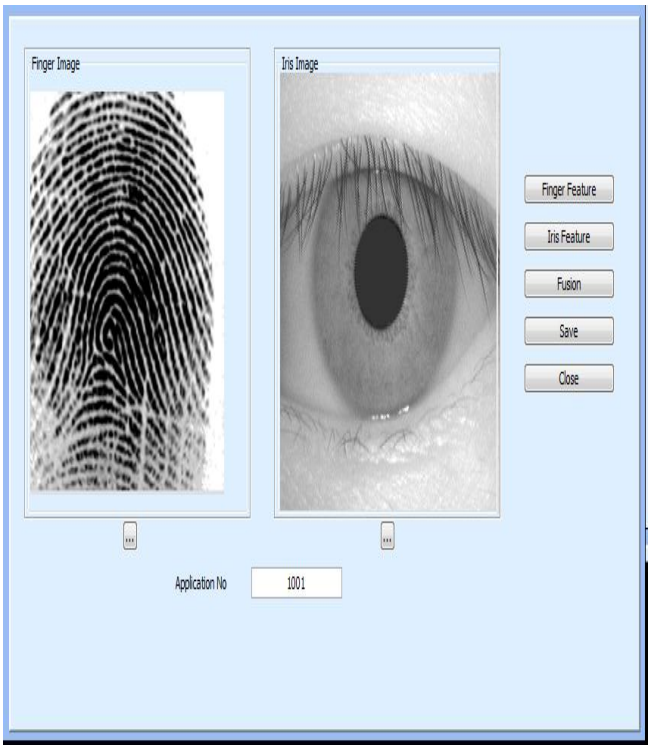

Figure 2: Multibiometrics Security in ATM System

LIMITATIONS OF MULTIBIOMETRICS SYSTEM:

- The accuracy of the biometric enrollment and biometric identification need to be improved.
- Noise in the biometrics like scratches in the fingerprint and lens mark in iris will lead to false rejection rate (FRR).
- In multibiometrics, failure of one biometrics will make the whole system to fail.

2.3 MULTIMODAL BIOMETRICS AND TWO TIER SECURITY IN ATM

The multimodal biometrics is to enhance the security of biometrics in ATM system [8][9][10]. From the past work, it has been highlighted that even though the security has been improved, the error rates has to consider for improvement of the performance of system. By considering all those drawbacks, the higher level of security can be provided by implementing multimodal biometrics and two level security in ATM system. In multimodal biometrics, different biometrics like Fingerprint, Iris and Face is considered. The biometric systems are designed in the way as integration of different biometrics. The three different biometric systems are Fingerprint and Iris, Iris and Face, Face and Fingerprint. Based on the user choice, the biometric system is selected. The choice of user depends on the biometrics he needs to enroll for verification and it should not be affected by external factors and it should prove him as an authenticated person. In case of unavoided failure, the user can undergo secondary means of verification by making other two biometric systems.

If due to unavoidable reason the user was not able to prove him as a genuine person with the help of multimodal biometrics, he cannot able to access his account. But this situation happen soo rarely. In that situation, if and only if he prove him as authorized person the ATM system will allow user to access his account to avoid hacking activities. Even though the security has been increased at the same time fraudulent activities have grown to equal level, so the security in ATM is an essential one and the two level security has been introduced [11]

Figure 2 explains the proposed concept system flow diagram of multimodal biometrics system and Two-tier security in ATM system. The user needs to insert the card in the ATM system and enter the PIN number; if it is valid the options will be displayed. The user needs to select the biometric system which he needs. In case if he has wound in the finger, he can select option 2 to prove he is an authenticated user. In case of environmental factors, if the user is not identified as authenticated person, he can make use of other biometric system and make a secondary enrollment by selecting other biometric system. Likewise it reduces the False Reject Rate. Two tier security is provided, when all the biometric system fails. In the two-tier security, the verification code will be send to the user email id. He needs to enter that verification code correctly to prove him as authenticated user and only three attempts are provided and if the hacker try to guess out the code by trying more than 3 attempts, that account will be locked and he cannot able to access the system.

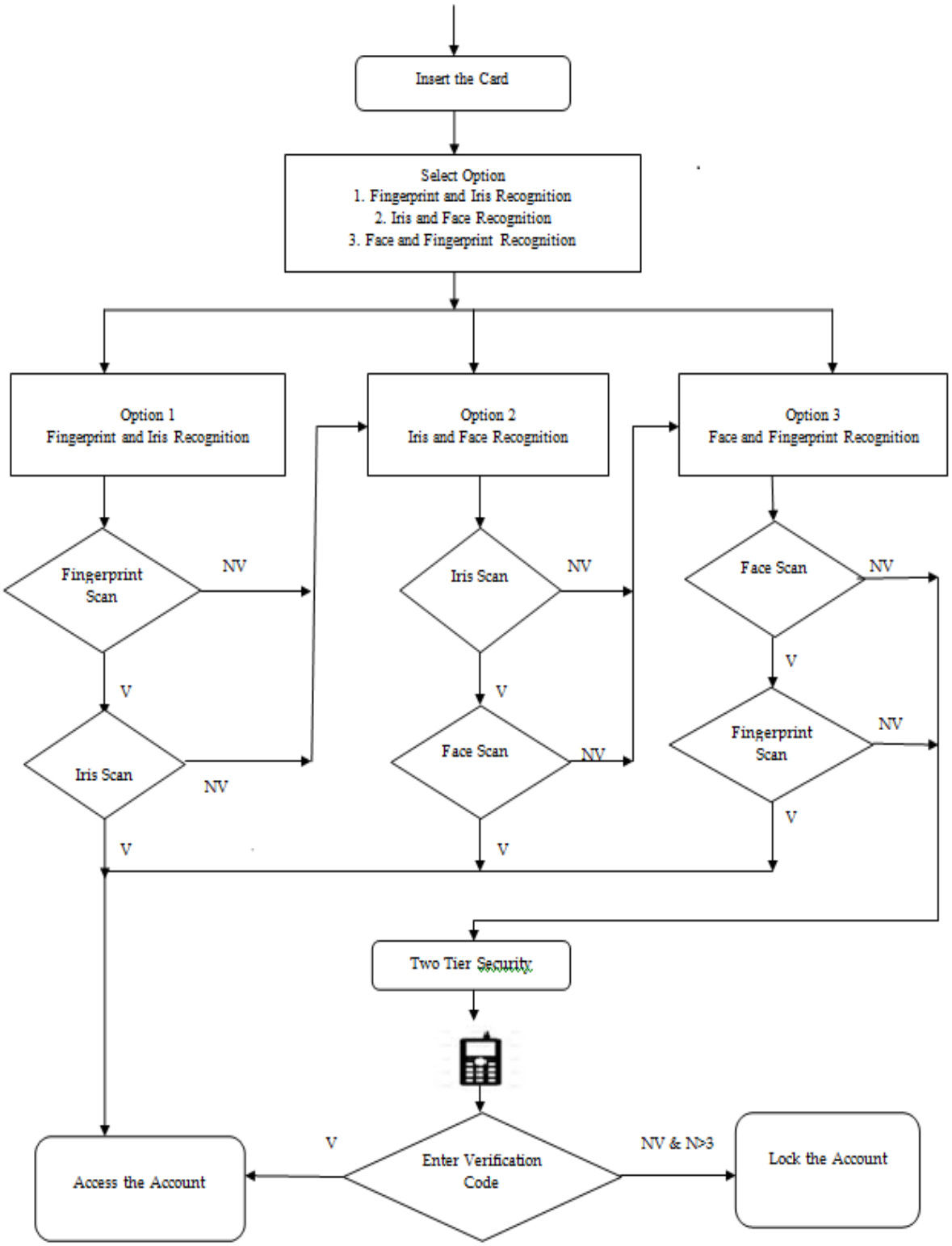

Figure 3: System Flow Diagram for Multimodal Biometrics and Two-Tier Security in ATM System

3. BRAIN FINGERPRINTING TECHNOLOGY

In the existing approaches different biometrics are used to provide security but hackers can able to hack every biometric techniques which are being employed. In multibiometrics, features of different

biometrics are extracted and combined using feature level fusion and biometric cryptosystem is used to protect the template. But if anyone of the biometrics fails then authenticated user cannot be identified as legitimate user. so the idea of multimodal biometrics along with two tier security was introduced. It solved all the problems of unimodal biometrics and multibiometrics but it was the complex task and it was not cost effective and it takes more time. So my proposed approach to use brain fingerprinting technique which will be an uncrackable password authentication.

Figure 4 Brain Fingerprinting

Brain Fingerprinting is a scientific technique to determine whether specific information is stored in an individual's brain or not by measuring an electrical brain wave response to word, phrases or picture that are presented on computer screen.[12] Brain fingerprinting is an advanced computer-based technology. The primary application of the brain computer interface is to map the brain signal of human being through digital EEG. Basically human brain will record the incidents happened in our life into our mind.

Brain Fingerprinting was invented by Lawrence Farwell [13]. The theory is that the suspect's reaction to the details of an event or activity will reflect if the suspect had prior knowledge of the event or activity. This test is called as MERMER (Memory and Encoding Related Multifaceted Electroencephalographic Response).

3.1 MERMER METHODOLOGY

The procedure used is similar to the Guilty Knowledge Test; a series of words, sounds or pictures are presented via computer to the subject for a fraction of second and record the stimuli of "Target", "Irrelevant" or a "probe". A target stimulus is chosen for relevant information. Most of the non-Target stimuli are irrelevant. The probe stimuli is relevant to test.

How it works?

A suspect is tested by looking at three kinds of information represented by different colored lines:

- **Red color** line denotes the information the suspect is expected to know.
- **Green color** line denotes the information not known to suspect.
- **Blue color** denotes the information of the crime that only perpetrator would know.

As the blue and green lines closely correlate, suspect does not have critical knowledge of the crime and hence it is not guilty. As the blue and green lines are apart from each other and they are closely correlate, suspect has the critical knowledge of the crime and hence it is guilty[14].

4. BRAIN FINGERPRINTING IN ATM PROVIDES SECURITY

The person is asked to wear the head band with electronic sensors that measure the Electroencephalography from several locations on the scalp. As we know that human brain is central to human acts everything what we see is stored in brain in the form of music, video or text. As per the brain fingerprinting technology unique brain wave will be created by individual brain when they see the things which is displayed on the screen and this brain wave can be used as password to access his/her account by inserting ATM card. The brain wave which is generated will be stored in a computer controlled device and when the person need to use the ATM this brain wave can be used to prove him as a authenticated person [15].

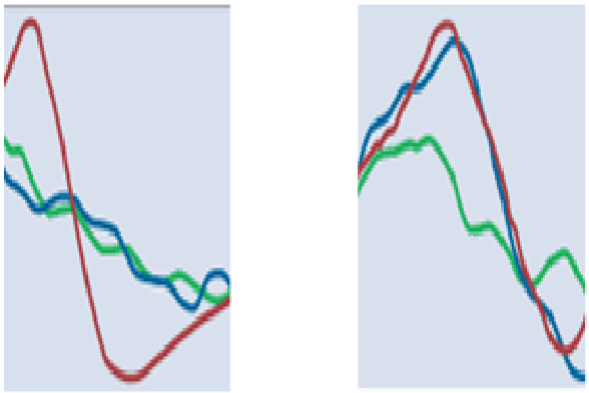

Figure 5 (a) Not Guilty (b) Guilty

In this type of password authentication, it is very difficult for hackers to know the password and even if they try to know they cannot regenerate the same brain wave using brain fingerprinting because brain wave is unique to the individual person. This type of security provides the highest level of security in ATM.

5. CONCLUSION AND FUTURE WORK

Brain fingerprinting technique in ATM will be a new level of security. Biometrics like fingerprint, face and iris template can be generated by using fake biometric trait and the error rates like FAR and FRR will be more which will decrease the performance of the system. Brain fingerprinting is mainly used in applications like criminal cases, counter-terrorism, advertisements and security testing. In criminal cases it has been proved that there will be 100% accuracy and this brain fingerprinting is not yet implemented in distributed system applications like ATM and Passport but it is implementable.

6. REFERENCES

[1] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani "ATM Security Using Fingerprint Biometric Identifier: An Investigate Study", IJACSA, Volume.3, no.4, 2012.

[2] A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multibiometrics" NewYork: Springer,2006.

[3] Harbi AlMahafzah and Maen Zaid AlRwashdeh "A Survey of Multibiometric Systems", International Journal of Computer Applications, Volume 43, no.15, 2012.

[4] Karthik Nandakumar, "Integration of Multiple Cues in Biometric Systems", Thesis for Master of Science in Michigan State University. 2005.

[5] Roli Bansal, Priti Sehgal and Punam Bedi "Effective Morphological Extraction of True Fingerprint Minutiae based on the Hit or Miss Transform*", IJBB*, Volume 4, Issue 2, 2010.

[6] Abhishek Nagar, Karthik Nandakumar and AnilK. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion", IEEE transactions on information forensics and security, vol. 7, no. 1255-268, February, 2012.

[7] B. Yanikoglu and Kholmatov, "Combining multiple biometrics to protect privacy", in Proc. ICPR-BCTP Workshop, Cambridge, August, England.

[8] Santhi.B and Ramkumar.K "Novel Hybrid Technology in ATM Security Using Biometrics", JATIT, Volume.37, no 2, 2012.

[9] S.R. Agarwal, D.R. Kokadwar, Zareen Kauser and Gouri Apte "Multimodal Biometrics System-Applications, Challenges and Research Areas", BIOINFO Human-Computer Interaction, Volume 1, Issue 1, 2011.

[10] S. Pravinthraja and K. Umamaheswari"Multimodal Biometrics for Improving Automatic Teller Machine Security", Bonfring International Journal of Advances in Image Processing, Volume 1, December, 2011.

[11] N.Geethanjali and K.Thamaraiselvi "Feature level fusion of Multimodal Biometrics and Two Tier Security in ATM System", International Journal of Computer Applications Volume 70– No.14, May 2013.

[12] Prof. Dinesh Chandra Jain and Dr. V.P. Pawar, The Brain Fingerprinting Through Digital. Electroencephalography Signal Technique, International Journal on Computer Science and Engineering, IJCSE11-03-03-047.

[13] Dr. Farwell and Smith SS, Brain Fingerprinting, Journal of Forensic Sciences, 2001.

[14] Farwell LA and Smith SS, Using Brain MERMER Testing To Detect Concealed Knowledge Despite Efforts To Conceal Journal of Forensic Sciences 2001.

[15] Nikhil M. Palekar1, Vaishnavi P. Rakhunde, "Uncrackable Password Authentication Using Brain Fingerprinting", IOSR Journal of Computer Science (IOSR-JCE) PP 29-32