International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2015 Volume 2, Issue-3
Email: editor@ijermt.org www.ijermt.org

Use of Biometrics and Image Processing in ATM Security

Mrinal Paliwal
Department of Computer Science & Engineering
P.K. Group of Institutions Mathura, India

Saddam Hussain
Department of Computer Science & Engineering
P.K. Group of Institutions Mathura, India

ABSTRACT:
Today, ATM has turn into an essential correspondence and administration channel in the middle of banks and cardholders and because of its quick, accommodation and human asset sparing focal points, you can undoubtedly discover ATMs in branches, comfort stores, airplane terminals, and shopping centers. In any case, with the thriving of introduced ATM, the issue of security is too of foremost significance, which requires extremely touchy treatment of the transmitted information. The present era security issue considers the fundamental TCP/IP encryptions and different elements that are given by the system, yet there was absence of reliable ID of people. For this reason the recently created innovation Biometrics, came into picture.
The fundamental target of this paper is to build up an implanted framework, which is utilized for ATM security applications. Accordingly it encases the presentation with respect to the 'IMAGE PROCESSING' and spotlights on one of its significant application i.e. 'BIOMETRICS. Biometrics is any consequently quantifiable, strong and unmistakable physical trademark or individual attribute that can be utilized to recognize an individual or confirm the guaranteed ID of a person. Essentially, it transforms your body into your secret word, which can't be mimicked by others. The two level security calculation has been proposed considering biometric strategies and PII (Personal Identification Image) idea to verify an ATM account holder, empowering a safe utilization of ATM by picture preparing. This paper proposes the most suitable procedure of Biometric Technology with a specific end goal to execute ATM Security utilizing Image Processing. Doubtlessly, biometrics will be cutting edge's intense security apparatus.

KEY WORDS:-Security of ATM, Biometric Verification, PII Verification, Algorithm, Flowchart**.**

I. INTRODUCTION

DIGITAL IMAGE PROCESSING

An Image may be characterized as a two dimensional capacity f (x, y) where x and y are spatial (plane) coordinates, and the sufficiency of f at any pair of coordinates (x, y) is known as the power or dim level of the image by then. At the point when x, y and sufficiency estimations of f are all limited, discrete amounts, we call the image a Digital Image. The field of Digital Image Processing alludes to processing of Digital Images by method for Digital Computer. The whole procedure of Image Processing, beginning from the accepting of visual data to the giving out of depiction of the scene, may be isolated into three noteworthy stages which are likewise considered as significant sub zones, and are given underneath-

(i) Discretion and representation: Converting the visual information took into a discrete form suitable for computer processing, approximating visual information to save storage space as well as time requirement in subsequent processing.

(ii) Processing: Improving image quality by filtering etc, compressing data to save storage and channel capacity during transmission.

(iii) Analysis: Extracting image features, qualifying shape, registration and recognition.

II. OVERVIEW

Presently a-days, the self-administration saving money framework has got broad promotion with the normal for offering excellent 24 hours administration for clients. Notwithstanding, the money related wrongdoing case rises more than once as of late, as heaps of lawbreakers mess around with the ATM terminals yet the security that is by and large right now utilized for ATM in fact has a couple of indirect accesses and it can be enhanced further. In this way, with the expanding necessities of ATM and the accommodations it offers genuine security concerns additionally emerges. Commonly, in the conventional security framework ATMs utilize a blend of "something that you have" (ATM card) and "something that you know" (PIN) to build up an character. The issue with the conventional methodologies of recognizable proof utilizing ownership as a method for character is that the belonging could be lost, stolen, overlooked, or lost.

Then again, the ATM terminals are powerless against gatecrashers who are continually snooping to discover open chances to take client's credit card and passwords by illicit implies. The misfortune of these individual records can be obliterating and can convey colossal monetary misfortunes to the clients. Step by step instructions to bear on the substantial character to the client turns into the concentrate in current budgetary circle. Goal of this paper is to give improved security to ATM by improving the effectively proposed biometric framework and making regardless it secured by PII [Personal Identification Image] process.

III. INTRODUCTION TO BIOMETRICS:

Image Processing, fundamentally is the processing of image in order to uncover the internal points of interest of the image for further examination. Since the mid 1970's, the field of Image Processing proceeds on a way of element development regarding mainstream and logical intrigue and number of business applications. Considering the advances in most recent 30 years bringing about routine use of Image Processing, Image Processing has altered in different fields. Illustrations incorporate mapping inside organs in pharmaceutical utilizing different examining innovations (image remaking from projection), programmed unique mark acknowledgment (design acknowledgment and image coding), and HDTV (feature coding). Among the above samples, Biometric use of Image Processing is a standout amongst the most critical one for security point of perspective, the innovation which permits determination and check of one's character through physical attributes.

Biometrics is gotten from the conjunction of the Greek words bios and measurements that mean life and to gauge individually. It is the investigation of strategies for particularly perceiving people based upon one or more characteristic physical or behavioral qualities. When all is said in done terms, a biometric is watched information of a human that permits the character of that individual to be resolved. Cases of biometrics effectively being explored are DNA, state of the ear, confronts, fingerprints, hand geometry, irises, design of keystrokes on a console, mark, and discourse. These components are utilized to give a verification to PC based security frameworks.

The biometric frameworks offer a few preferences over conventional confirmation frameworks. The issue of data security gives the insurance of data guaranteeing just approved clients have the capacity to get to the data. Here, it is obliged that the individual being confirmed ought to be available at the purpose of validation. Accordingly biometric-based verification technique gives propelled security of the framework.

1. Classification of Biometrics

The two categories of biometric techniques are:

Physiological based Techniques:

It measures the physiological qualities of a man. It incorporates unique mark check, iris investigation, facial examination, hand geometry-vein designs, ear acknowledgment, scent location and DNA design examination. The fundamental point of preference of utilizing these physiological characteristics is that however different sorts of validation like passwords and tokens can be introduced by anyone, physiological attributes can't be imitated and hence structure the principle reason why these Biometrics

frameworks are utilized.

Behavioral based Techniques –

It gauges the conduct of the individual. It incorporates written by hand signature confirmation and discourse investigation. This method takes a shot at taking after standards. Firstly, Authentication which checks whether we are who we guarantee we are i.e. it sets of to check our character. Second, Identification which tries to discover who we are i.e. it sets of to set up a character. Accordingly, Biometric goes a long way from the conventional frameworks and aides in fixing the security of the framework. No single biometrics is anticipated that would adequately fulfill the needs of all recognizable proof applications. Various biometrics have been proposed, examined, and assessed for distinguishing proof (confirmation) applications. A portion of the fields of inclusion of Biometric Analysis are as per the following:

1) **Fingerprints –** Biometric identification from the print made by the pattern of rids and valley on the surface of a finger tip. Even the finger prints of the identical twins are different. This method is traditional, affordable and gives accuracy as well.

2) **Hand Geometry –** This method is based on a number of measurements taken from the human hand, including its shape, size of palm, length and width of fingers. This method is simple and easy to use but the hand geometry may not be invariant during the growth period of children.

3) **Face Recognition:** Biometric identification by scanning the person's face and matching it to the library of known faces. As this technique involves many facial elements, it becomes difficult to match the face images.

4) **Voice Print –** This system goes in for the voice analysis of the person to be authenticated. Voice is the combination of physical and behavioral biometrics. The features of the voice are based on vocal tracts, nasal activities, mouth and lip movement which are invariant for individuals. While the behavioral part of the speech of person changes over time due to age, medical condition and emotional state. This method has many flaws compared to the other methods.

5) **Iris Scanning –** It is the unique structure of human which remains stable over a person for lifetime. It is accurate, cost effective and has very low false accept rate. Iris is believed to be unique and is even different for two identical twins.

6) **Signature Recognition –** It is one of the behavior based technique of biometric analysis which identifies a person by automatically scanning the person's signature and matching it electronically against the library of known signatures.

7) **DNA Pattern Analysis –** Biometric identification obtained by examining the person's unique sequence of DNA base pairs.

Each biometric trait has both advantages and limitations and accordingly, each biometric appeal for a particular identification (authentication) application. Which biometric is suitable for the given application is determined by the match between a biometrics and an application on the basis of the requirements of the given application, the characteristics of the application, and properties of the biometrics.

2. COMPARISON OF BIOMETRICS:

The comparison of various biometric methodologies is based on various factors. The biometric features of fingerprint, face, hand geometry, voice etc. should have some defined characteristics in order to be effective for implementation in any system. These characteristics are universality, uniqueness, permanence, performance and measurability. These characteristics are different for each biometric type. The comparison of different biometric features based on various factors is stated below in the Table 1.

Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the following requirements, which means for a biometric to be effective it should have the following five properties:

(1) Universality - All members of population being identified should possess the biometric.

(2) Uniqueness - Biometric signature should be different for all members of the population which means no two people should be same in terms of characteristics.

(3) Invariance - The signature should be invariant under the conditions that it will be collected, i.e. the biometric should be permanent and not variant with time.

(4) Performance - It should have accuracy which is measured on the basis of False Accept Rate (FAR) and False Reject Rate (FRR).

(5) Measurability - It must be easy to measure quantitatively.

Table 1: The comparison of different biometric characteristics

Biometric Characteristic	Universality	Uniqueness	Invariance	Performance	Measurability
Signatur	Low	Low	Low	Low	High
DNA-	High	High	High	High	Low

IV. ATM SECURITY USING BIOMETRICS:

This biometric methodology has diminished the issue of recognizable proof to the issue of recognizing physical qualities of the individual. The attributes could be either a man's physiological characteristics, e.g., fingerprints, hand geometry etc.or his/her behavioral characteristics,e.g. voice and mark. This system for ID of a man taking into account his/her physiological or behavioral attributes is called biometrics. The essential point of preference of such an ID system over the systems for distinguishing proof using "something that you have" or "something that you know" methodology is that a biometrics can't be lost or overlooked; it speaks to an unmistakable part of "something that you are".

Every system has its own upsides and downsides and is utilized relying upon the level of security wanted and the different ranges where they must be actualized. Unique mark check, Iris filtering, facial acknowledgment, and voice confirmation are the systems for consolidating biometric frameworks with ATM machine. Among the above image-based Biometrics that are in effect effectively considered, the two most encouraging one's are, confronts and fingerprints in light of the fact that utilizing biometrics, for example, Iris ID, Voice confirmation costs much and the upkeep will be troublesome. This makes the framework all the more unreasonable and confounded. Another biometric strategy for supplanting the disappointment of one biometric makes the machine more confounded and expense element is likewise influenced. Also they have not specified the case if the framework falls flat. Biometric strategies, particularly when joined with alternate systems for distinguishing proof, are starting to give capable instruments to issues obliging positive ID. Subsequently, keeping in mind the end goal to stay away from the confinement of making the framework untrustworthy if the biometric falls flat or making the framework complex by consolidating more than one biometric framework, we should accentuation on

utilizing PII (Personal Identification Image) idea as a reinforcement philosophy on the disappointment of biometric framework to improve the security. The reason because of which the different biometric procedures can come up short is the physical harm in which the client can get harmed coming about into the biometric disappointment. This paper proposes a novel system to meet out the challenges and reinforce the security component. Subsequently, the most proper philosophy is Implementation of ATM Security utilizing Fingerprint Recognition and PII idea all the while.

1. BIOMETRIC PATTERN RECOGNITION SYSTEM:

The Biometric Recognition Systems are utilized to distinguish the individual in light of the elements of any of the biometric that the individual has. These frameworks are individual approved frameworks consequently offer more secure and helpful procedure of distinguishing proof contrasted with option routines for ID. The biometric framework utilizes the individual's physical qualities like unique finger impression, hand geometry, face, voice or iris. They are more dependable and secure as they gives the entrance to approved clients in their physical vicinity. A straightforward biometric framework comprises of four modules which have the capacity to gather the biometric (unique mark), to perform preprocessing on unique information, to encode the data to get highlight vector, to match the components to perceive the individual.

(1) Acquisition Module: The decision of significant information for the biometrics is the basic procedure which needs most extreme consideration on the grounds that the measure of consideration taken to secure information decides the execution of the whole framework. In the event that if the boisterous data estimation is acquired then the info image is improved if there is no decision of dismissing the low quality information taken.

(2) Representation or Pre-processing Module: The issue of representation is to totally catch the invariant and biased data in the information estimation. This implies it decides the notable elements of the information estimations which does both, separates between the personalities as well as stay invariant for the given person.

(3) Feature Extraction Module: Through given crude info estimations, consequently removing the given representation will be an greatly troublesome issue, particularly where information estimations are loud. Deciding the elements that were not doable to fuse into the completely programmed unique mark framework. This implies extraction of those elements which have not got much consideration in PC vision but rather is particularly vital for separating the biometrics of a person concerning others.

(4) Matching or Recognition Module: It decides the likeness between the two representations of the biometric estimations. The coordinating is performed by contrasting the arrangement of details present on the unique mark design. Coordinating results where the layout details and its correspondence in data particulars set is associated.

2. IMPLEMENTATION OF 2-TIER SECURITY FOR ATM USING FINGERPRINT RECOGNITION AND PII CONCEPT:

The expanded need of protection and security in our every day life has conceived this new range of science. Fingerprints are a standout amongst the most adult biometric advances utilized as a part of scientific divisions overall for criminal examinations. Commonly, a finger impression picture is caught in one of two ways:

(i) Scanning an inked impression of a finger, or

(ii) Using a live-scan fingerprint scanner.

To make this procedure straightforward, secure and practical than the current PIN confirmation technique, this paper proposes the use of biometric strategy Along with Personal Image Identification which gives advanced Security to the ATM frameworks and an easy to understand and secured administration.

In the proposed security calculation two stages are characterized to verify an ATM account holder, empowering the security of ATM by Image Processing. These two stages give two level securities and there by improves the security of ATM machine. The PII idea will empower the approved individual to get to the ATM machine utilizing the versatile check regardless of the possibility that the biometric falls flat. Utilizing PII idea the client can even protect himself as the card gets blocked when it is constrained by any outsider in light of the fact that just 3 endeavors for PII is given. The proposed system promisingly permits little false acknowledgement and false dismissal rates, as it is in light of particular finger impression division. The finger impression acknowledgment is more precise and effective in light of the distinguishing proof taking into account a few fine and remarkable elements of the unique mark designs which are delegated curve, tented curve, right circle, left circle and whorl (see figure 1).

(a) **(b)** **(c)**

Figure 1: Example of different features of fingerprint pattern (a) right loop (b) whorl and (c) arch

3. Advantages of Using Fingerprint Recognition

(1) Fairly small storage space is required for biometric template, thereby reducing the size of database required.

(2) It is one of the most developed biometric with more details, research and design.

(3) Each and every fingerprint including all the fingers are unique, even identical twins have different fingerprints.

(4) Relatively inexpensive and offers very high level of accuracy.

Thus considering these advantages, this particular methodology can said to be one of the most appropriate biometric technology that can be used in banks for authorization at ATMS and credit card.

V. WORKING AND PERFORMANCE:

In the typical IT biometric system, the person registers within the system when one or more of his physiological or behavioural traits are obtained. The information is then processed by the numerical algorithm and entered into the database. The algorithm creates a digital representation of the obtained biometric and if the user is new to the system, he/she enrols which means the digital template of biometric is entered and saved to the database along with the registered mobile number.

When the user inserts the ATM card again, each subsequent attempt to use the system requires the biometric of the user to be captured again. So the machine asks for a fingerprint and checks for the match of the provide fingerprint in database. The comparison process involves the use of Hamming Distance, which measures the percentage of dissimilar bits out of the total number of comparisons made.
After the above phase two possibilities arises:

Fingerprint matches – If the fingerprint matches with the database the user is automatically directed to next phase.

Fingerprint doesn't matches – In case the fingerprint doesn't matches, every time the different 4-digit code is automatically generated as a message to the registered mobile number of the authorised customer in order to access the terminal.
If the user is authorised user then he/she will enter the received verification code by pressing the keys on the touch screen and the entered code is checked whether it is valid one or not, if valid then the user is directed to the next phase. In case, the user is unauthorised and is trying to access other's account then the person will not receive the verification code and hence can't be directed to next phase.
In the next phase, user enters the PII (Personal Identification Image) which can be anything such as user's full name (if not common), IP address, Credit cards number, Driver's license number etc. The PII is mapped with the position of image stored in the database for that particular transaction.
The user has to be identified through his/her PII image and if authorised, the user should find a PIN number after PII verification. The PIN number found here will be reset after the transaction.
Thus, the user gets authenticated and can execute his/her transactions at the ATM terminal in safe and secured manner.
The performance of biometric is usually referred in terms of False Accept Rate (FAR), False non-match or Reject Rate (FRR) and the Failure to Enroll Rate (FER or FTR). The FAR measures the percentage of invalid users who are incorrectly accepted as genuine users. On the other hand, FRR measures the percentage of valid users who are incorrectly rejected as imposters. In the real-world biometric system, one of the most common measures is the rate at which both accept and reject errors are equal i.e. the Equal Error Rate (EER) which is also known as Cross-over Error Rate (CER). Lower is the value of CER or EER, more accurate the system is considered.
The proposed algorithm therefore provides 2-phase security and act as a two tier security. According to this work flow an unauthorised person can't access other's account just by having users ATM card and knowing user's PII image, he needs user's mobile phone and the fingerprint too. This makes the process more secured than the existing mechanism in which user enters the ATM, inserts the ATM card, enters the PIN and is ready to execute transactions. The proposed algorithm increases the security and efficiency, at the same time decreases the possibility of misusing others account. Thus this provides the two tier security mechanism.

1. Algorithm

STEP 2: User inserts the ATM card in the ATM machine as well as provides his/her fingerprint as an input through the finger scan pad.

STEP 2: The received biometric (fingerprint) of the user is compared with the existing biometric in the database. This means the fingerprint is verified.

STEP 3: If scanned fingerprint is valid, then
GOTO STEP 6
ELSE
GOTO STEP4

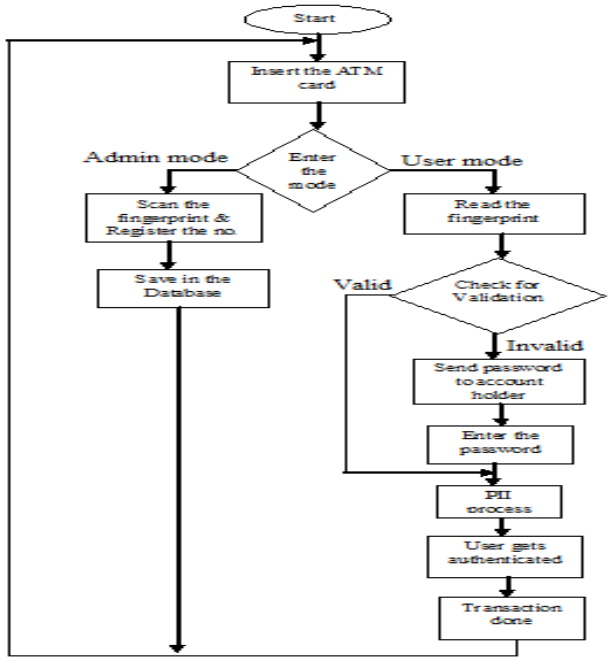
STEP 4: If the scanned fingerprint is invalid, then the 4 digit verification code is automatically generated and sent to the registered mobile number.

STEP 5: If the person accessing the ATM terminal is authorised, he/she will receive the verification code and will enter the code by pressing the keys on the touch screen.

STEP 6: PII process is performed.

STEP 7: User gets authenticated and founds a PIN number fromPII verification.

STEP 8: User can now execute transactions at the ATM terminal



2. Flowchart

Figure 2: Flowchart for implementation of ATM Security

VI. CONCLUSION:

From the first ATM being installed in the world till now, ATM has gradually become a target of crimes due to it providing direct access to safe and cash. While with the constant evolution of reported ATM crime, ATM industry has begun to pay attention to the safety of ATM and even cardholders. The Implementation of ATM security by using fingerprint recognition and PII concept took advantages of the stability and reliability of fingerprint characteristics. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

The proposed method overcomes the limitations that exists in other methods and provides a secured and safe environment that saves the hard earned money of the user. The user when gets hurt in finger can be authenticated via mobile after code verification and when forced can block the account's transaction with PII and even if the stranger tries trial and error, maximum of 3 times PII will function and gets blocked for 24 hrs thereby providing the two tier security.

The increased need of privacy and security in our daily life has given birth to this new concept of generating PIN number through PII process which enhances the security. Even if the biometric system fails due to injury and other reason this proposed PII process allows the user to do

transaction in a secure way. We believe under the joint and sustained effort of ATM suppliers, banks, and related organization, a more safe and convenient transaction platform and channel will be built up eventually.

VII. REFRENCES:

1. Santhi.B; Ram Kumar.K; "Novel Hybrid Technology in ATM Security Using Biometrics", Journal and Theorotical Applied Information Technology on 31st March,2012, Publication Year: 2012, Volume: 37.
2. Pennam Krishnamurthy, Mr. M. Maddhusudhan Redddy, " Implementation of ATM Security by Using Fingerprint recognition and GSM", National Conference on Research Trends in Computer Science and Technology – 2012, International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X
3. Ruud Bolle, Sharath Pankanti and Anil Jain, "Introduction to Biometrics".
4. Sulochana Sonkamble, Dr. Ravindra Thool and Balwant Sonkamble, "Survey of Biometric Recognition System and Their Application", Journal of Theoretical and Applied Information Technology from 2005 - 2010 JATIT.
5. R.Michael McCabe, P. Jonathon Phillips and Rama Chellappa, "Biometric Image Processing and Recognition".
6. A.Hrechak and J. McHugh. Automated Fingerprint Identification using structured m atching.Pattern Recognition, 23:893-904, 1990.
7. Jyothi Shilpa Akelle, Prathik Gadde, Sravani Konidala, " Biometrics, Creating-a-Safer Workplace"