Biometric based Fingerprint Verification System for ATM machines

T Sangeetha 1, M Kumaraguru 1, S Akshay 1 and M Kanishka 1
1Department of Information Technology, Sri Krishna College of Technology, Coimbatore, India
t.sangeetha@skct.edu.in, tokumaraguru.m@gmail.com, 17tuit003@skct.edu.in, 17tuit030@skct.edu.in

Abstract. In this modern world, almost everyone uses ATM machines which allow people to transfer and withdraw cash. This study is based on executing a fingerprint method in the ATM System. We chose this field to improve safety and security for people to make the transaction easier. The fingerprints are unique for each person. There is no insecurity of losing an ATM card and no requirement to carry an ATM card with you every time. On comparison of different technologies for ATM security, the fingerprint technology operates better and safer than others. These reasons make this mechanism an effortless and secure way of transaction and also maintains a coherent ambience with users and ATM machines. This is the most latest technology in electronic cash transactions.

Keywords: Enhancing ATM, biometric based ATM, security system for ATM, and fingerprint based ATM.

1. INTRODUCTION
Our aim is to evolve a far better guarding system by the usage of fingerprint based ATMs. Biometrics may be a technology that aids to form your data extremely securely, unique to each and everyone by way of their unique physical characteristics. Biometric data is employed to spot the person perfectly by using his/her fingerprint, iris, face, speech, hand geometry, or handwriting, etc... Tokens like mag tape cards, physical keys and smart cards, are often stolen, misplaced, replicated, or vanished; passwords are often failed to remember, shared, hacked or fortuitously seen by a third party.

The two key functions given by a biometric system are identification and therefore the other is verification. Fingerprint processing is widely accepted these days and may be a fully developed biometric technology and is effortless to develop for an advanced stage of security and safety at the fingertips. It's uncomplicated to execute and it might take very less time and energy to get a person's fingerprint recorded with an identification device.

Thus, the recognition of fingerprint is taken into account between the minimum disruption and annoyance of all biometric verification procedures. Old time's authorities utilized thumbprints to seal documents, and law firms have been using identification of fingerprints from the 1800s. We here bring an equivalent technology on electronic platforms. Though fingerprint images are captured at first, the pictures aren't stored anywhere in the system. On the other hand, the fingerprints are changed into templates from the initial images. Not regenerate it. Hence, mishandling of the system is not possible[1].
Nowadays, the automatic self-banking has widely spread with the trademark benefaction 24 hours’ service for patrons. Usage of ATM (Automatic Teller Machine) might give people with appropriate banknote dealing is extremely common. However, the monetary crime has risen frequently in these years. Many criminals’ interfere with the ATM depot and steal the person's master card and word of identification by unlawful ways. A person’s credit card is misplaced and therefore the password is theft, the culprit extracts and takes advantage of less time which can lead to lots of monetary losses to people. The way of keeping up is the authentic distinction to the client as it gets the main target in the present financial situation.

Already established ATM mechanisms work usually by the aid of mastercard and password, the tactic has some mistakes. Employing a master card and word of identification alone can’t really verify the customer's identity correctly. Within past few years, the algorithms that are used have fingerprint identification regularly updated and generating the four-digit code by the authority has given the new verification method for people, the first password processing is connected with the biometric system verify the customer’s identity and succeed the use of ATM. Devices improve the security fruitfully[2].

2. RELATED WORKS

2.1. Fingerprint Image For Identification

“Biometrics” evolved from the Greek term “bios” and “metric” that suggests existence and quantification[3]. To execute this, we have brought in the data below based on the studies of different investigated works. Many finger-scan equipment are based on trivial details. The drawback of image matching is, it’s delicate to trueness of the finger while verifying and generating the template is very large. For identifying fingerprints, a device must capture a fingerprint then go through an algorithm for matching. This study talks on precise details of detection algorithms to bring out key stipulations of fingerprint pictures for recognition. The fully developed biometric methods and typically the unexpected enhancement of the recorded devices have given way to the introduction of fingerprinting in various applications only within the recent years, the trivial details are the ruling quiet algorithm[4]. Biometric information parted and clear-cut from personal data.

2.2. Replace Traditional Identification Methods

They’re going to not be theft and accustomed ingress personal data to resolving the bugs of established recognition ways the maker of designs a replacement ATM depot client identification system is availed for an upgraded enhancement algorithm of fingerprint image and the core of microprocessor develop the bank accounts’ security as well as ATM machines[5]. Miaoetal introduced the Gabor filters (GFs) take a significant role within the production of Gabor features and thus the intensification of various sorts of images. Fingerprint and voice operations have the minuscule relative sizes with eye systems presently the most important [6]. If pictures of fingerprints are poor-quality images, they end in unaccounted features, giving way to the bad performance of the fingerprint mechanism. Hence, it is significant for a fingerprint identification system to gauge the standard and viability of the recorded fingerprint pictures[7].

2.3. Biometric Payment

To get a better process of mechanism for fingerprint matching, in counting on the spectral details attributes two feature reduction algorithms provided the Line Discrete Fourier Transform feature
reductions and the Column Principal Component Analysis. Biometric templates may not be reverse-engineered to regenerate personal data which cannot be stolen and accustomed to ingress personal data [8]. Fingerprint information generally reaches impressions on the last joint of the thumb and fingers, to the level that fingerprint cards usually capture parts of the lower finger areas of the fingers [9]. In those recent technologies for operating cash processing, biometric payment mechanisms have recently grabbed more attention as an operable solution to reduce identity heist[10]. It’s visiting be of yore, present or conceptual.

2.4. Electronic money transfer

Samples of digital money are deposits, digital cash transfer, deposit directly, processing of payment, and electronic currencies. A digital currency is often seen as a way of collecting and transferring usual cash through digital mechanism or as electronic currency, which differs in standard and is exchangeable as a currency in its title. Digital cash transfer at an ATM is additionally a certificate of indebtedness machine that’s collected on an digital or remote system within the protection of the server. Alternately, digital security is any instrument, way or operation accustomed to guard system data assets. Data could even be a standard tactical asset that’s maintained and guarded. This protection could even be a venture governing or risk alleviation instrument, and protection steps relieve the risk of transactions proportionate with its worth.

3. EXISTING SYSTEM
In modern days, Everyone used to do banking like storing cash and withdrawing cash. The clients will be in line to extract cash from the bank. The clients felt like biding one’s time to withdraw money. That bank proposes an ATM (Automated teller machine) to aid the client extract cash quickly. In such an ATM, they propose CARDS (Visa, Credit, master, Debit) to the client to extract money through their usage. Major merit is fast money provided by the ATM. The customers feel joyful and they shall not throw away time to take out money being in queue. Still it has a main limitation like, physical keys and smart cards, may be theft, misplaced, duplicated, or forgotten; passwords may get distributed, unremembered, hacked or seen by some third party. Banks needed a good mechanism to manage protection for the clients to make the transaction in the banks. To get rid of issues, we have brought this fingerprint based ATM system Figure1.

![Figure 1. Diagram for Fingerprint based ATM](image)

4. PROPOSED SYSTEM
The introduced mechanism to increase safety and protection by proposing a fingerprint system. The merit of finger scanning technology is accuracy. By using this system multiple limitations are reduced fastly. They do not have the need to take an ATM card in wallets and no thought of losing the card. CARD can be theft, password can be distributed or, hacking all clients are satisfied by our system because of fast and good service. At first, Fingerprint is converted into string values that are collected in the EC2 database. Every user's fingerprint is stored as a string. Which means every string is unique. All
the strings are stored in a vast cloud memory. When a user withdraws his money he places his fingerprint, then that unique string is being searched in the cloud and the authentication process takes place Figure 2.

![Flowchart for ATM fingerprint](image)

**Figure 2.** Flowchart for ATM fingerprint

5. **OBJECTIVES**

The ideology is to propose validation and confirmation measures on the current, ATM machine and to make a fruitful and secure exchange. The fundamental goal of this undertaking is to give a unique mark as approved character and to plan a safer ATM framework. In this, the ATM machine fills in as when the client places his/her finger on the biometric scanner of the ATM and if the finger coordinate is discovered it will show the name of the client on the ATM machine. If by chance, that Fingerprint coordinate is not discovered, it doesn't permit any exchange. Our remarkable development in our venture is, in prior days if the client has his/her verified unique mark connected with the one bank in which he/she has opened his/her record, he/she would need to look for that bank's ATM if there should be an occurrence of crisis or any such circumstance. Be that as it may, by means of our venture the client approaches his/her financial balance through any ATM which underpins our Innovative procedure to pull out cash. This is finished with the assistance of banks co-working with one another to assist clients with pulling out their cash with no entanglements in looking through their specific ATM.

The objective of this research is as below:-

- To introduce the confirmation framework on the current ATM measure for withdrawal after the passage of a right pin.
- To introduce a second level verification framework in a situation where the client indicated withdrawal limit.

6. **METHODOLOGY**

Unique mark confirmation is to check the realness of one individual by his finger impression and Fingerprint and PIN code distinguishing proof is by coordinating the data of the client, for example, pin code and unique mark coordinating. Essentially we can clarify total Fingerprint based ATM framework in two stages:

- Enrollment Phase
- Authentication phase
6.1. Enrollment phase

In the robust fingerprint application, up to 3-4 fingers have to be registered. This makes the mechanism to give protection threshold and also be capable of going with usual life issues like wet dry, skewed finger placement, dirty, cut or worn fingers. The biometric reference information is stored for enrollment and collected in a database or in a data portable carrier that the Enrollment is significant as the once captured reference information will usually be available over the lifetime of the user or their biometric hardware system.

6.2. Enroll Multiple Finger enrollment

It is highly recommended to enroll many fingers. In everyday life harms can occur which turn a recorded fingerprint presently impractical while small cuts do not bring any change to a robust sized sensor mechanism.

6.3. Authentication Phase

In this phase users shall make transactions by using one’s fingers. A person shall place one finger on the Biometric scanner and that person’s finger scan shall be matched through a database in which all authenticated user’s fingerprints are collected. If any person wants to do any banking he/she just places their finger on a scanner and gets their cash in a short span. If a person's fingerprint cannot match by database as some incidental cuts on his/her fingers then he/she shall avail his/her other finger and we shall also give a 4-pin code option, people shall also avail this option with their conveniences. Feature extraction: This process from a fingerprint picture is usually divided into three. Feature shall be availed to divide into leading pattern types such as whorl or loop.

7. ALGORITHM

- User wants to enter the corresponding bank name and pincode of that bank.
- Scan the fingerprint value and pass along with the bank name and pincode.
- Check whether the user is valid or not by using ajax with mysql database.
- If the user is valid then it moves to the transaction page else it moves back to the index page.
- If the user enters the valid password and valid amount the amount will be debited or else it shows the error message.
- Check whether user given data is valid or not by using ajax with mysql database.
- If all the data is correct, the user can debit the amount.

8. EQUIPMENT AND METHODOLOGY

8.2. Fingerprint sensor

For the development of the ATM, R307 Fingerprint Module consists of optical fingerprint sensor, high-performance fingerprint alignment algorithm, high-speed DSP processor, high-capacity FLASH chips and other hardware and software compositions, simple structures, stable performances, with fingerprint entry, fingerprint matching, image processing, search and template storage and other functions.

8.2. Raspberry Pi 3RPig

Low cost, Small credit-card sized computer. RPi3 is faster than Arduino.

8.3. Cloud server and Fingerprint processing
Host server is AWS EC2. Date, time, message status, ID, sensor value and also Fingerprint is converted into string value and collected in the EC2 database. All user's fingerprints are stored as a string. Which means every string is unique. All the strings are stored in a vast cloud memory. When a user withdraws his money he places his fingerprint, then that unique string is being searched in the cloud and the authentication process takes place.

8.4. Software Role

The authentication process is done by a few simple steps for all users. First the basic details which comprises State, district and branch are being selected to make it fast and easy for the software to search the desired string (to verify the fingerprint). Then the verification takes place within a few seconds and the money can be withdrawn.

9. RESULTS AND DISCUSSIONS

In this study, our main concentration is on the end user and people with poor literacy. Using this method we generated a simple login sheet. In this login sheet, we got two options: He/She is going to avail fingerprint and the option card. The client has to avail the card choice he/she should choose one option. Else, they want to choose another option. After choosing the fingerprint, the person has to keep his/her finger in the scanner for recognition. During this, the fingerprint shall be recognized with the aid of a scanner. After the second step, the third step is the significant step. In the third step the client has to give the pin code properly. All the client has a protection number pin provided by the bank. If the client enters the pin number properly and gives a submit, the client shall perform banking services. If the client gives the incorrect number, it shall allow entering thrice only. The below portion is as a regular banking mechanism account transaction selection and selection portion. During this, his/her transaction shall be on his/her choice. We got three options. The person has to check his/her balance. Then, he/she has to extract money from the account, and in the end, he/she has to transfer money from an account to another account and the transaction is completed successfully.

Figure 3. Survey of fingerprint with other Biometrics

The merits of improving ATM protection availing fingerprints are people with less literacy shall ingress it effortlessly. During ATM card misplacement nobody shall use or access it, it can block automatically, nobody shall hack pin code. The hackers might easily guess the 4-digit pin code. Felonies that are
occurring in ATMs become a big problem which affects clients and operators at banks. Many people are dubious about availing ATMs due to the problems it has. Fingerprint mechanism is the very approved and fully developed biometric way and is always effortless to access and for a bigger extent of protection at people’s fingertips. The (Figure.3) depicts the survey of fingerprints with some other biometrics. Among every biometrics system, gain a great response and success as per the survey.

10. CONCLUSION
The execution of ATM protection by availing fingerprint also has the traditional verifying methods that were inputting the client's fingerprints, that is sent by the administrator and checked correctly. The protection feature was improved highly for the firmness and solidity of the client's identity. The complete system was constructed on a fingerprint system that makes the mechanism safe, dependable and effortless to avail. This shall be the most favourable technology in electronic or digital money transactions.

REFERENCES
[1] Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp 1-9, 2013.
[2] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, Available at: https://www.sans.org/readingroom/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning-1177.
[3] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37:543-553.
[4] N. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM banking industry using AES Algorithm, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.
[5] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/j.compeleceng.2020.106784
[6] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3
[7] J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang A Fingerprint Recognition Scheme supported Assembling Invariant Moments for Cloud Computing Communications, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.
[8] J. Leon G. Sanchez G. Aguilar, L. Toscano, H. Perez and J.M. Ramirez, Fingerprint Verification Applying Invariant Moments, Proceedings of IEEE International Midwest Symposium on Circuits and Systems, pp. 751-757, 2009.
[9] LO Gorman Overview of Fingerprint Verification Technologies, Information Security Technical Report, Vol. 3, No. 1, p. 21-32, 1998.
[10] G.B. Iwalokun O.C. Akindoyin, B.K. Alese and O. Olabode Fingerprint Image Enhancement: Segmentation to Thinning, International Journal of Advanced computing and Applications, Vol. 3, No. 1, pp. 15-24., 2012.