# Fingerprint Recoginition for user Authentication to Implement ATM Security

**Krishnendu. S. Nair[1], Shekhar Mane[2]**
[1, 2] Department of Computer Engineering
[1, 2] Mumbai University,India

***Abstract-*** *Fingerprint Based ATM is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction by login using his fingerprint and enter the pin code. The user can withdraw money from his account, transfer money to various accounts by mentioning account number and also view the balance available in his respective account etc. In order to withdraw money user has to enter the amount he want to withdraw and has to mention from which account he want to withdraw (i.e. saving account, current account) provided he has enough balance in his account. The system will provide the user to view last 5 transactions. The main objective of this system is to be used for ATM security applications. Over here, Bankers will collect the customer finger prints, Names by default needed and mobile number when they open their accounts, only after that the customer can access ATM machine. The conventional methods like ID card verification or signature does not provide perfection and reliability. IN this when customer place finger on the finger print Component then it automatically generates a different 4-digit code every time and it sends as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code when received by the customer should be entered by pressing the keys on the screen. Once entered it will check for validity and then allows the customer accessibility for any further transactions. This system can be employed at any application with enhanced security because of the uniqueness of fingerprints.*

***Keywords-*** Fingerprint processing and recognition, Image Enhancement, ATM terminal; ARM9

## I. INTRODUCTION

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. Biometric information can be used to accurately identify people by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on.Using a unique, physical attribute of your body, such as your fingerprint or iris, to effortlessly identify and verify that you are who you claim to be, is the best and easiest solution in the market today. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the sole of the foot can also leave an impression of friction ridges. the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. Nowadays, the algorithm that the fingerprint recognition uses is continuously updated and sending the four digit code has offered new verification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effective. Using an ATM, customers can access their bank accounts in order to make cash withdrawals, debit card cash advances, and check their account balances as well as purchase prepaid cell phone credit. Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to bank where they have their accounts or in the countries where their account are held. Despite the numerous advantages of ATM system, ATM fraud has recently become more widespread.

Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated; hence no misuse of system is possible.

## II. LITERATURE REVIEW

To implement this concept, we have referred different researches done by many research scholars and finally got the following information.

For fingerprint recognition, a system needs to capture fingerprint and then use a certain algorithm for fingerprint matching. The research paper [4] discusses a minutiae detection algorithm and showed key parameters of fingerprint image for identification. The system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required. For solving the bugs of traditional identification methods, the author of designs a new ATM terminal customer recognition system with chip of S3C2440 is used for the core of microprocessor in ARM9 and an upgraded enhancement algorithm of fingerprint image intensify the security of bank account as well as ATM machine. First the system is required the owner's fingerprint. If all the recognition is right, the system would send password to the Account holder and he will enter the same password in on the keypad for accessing the ATM Terminal. If Authentication Failure then it send the alert message to the Account holder and Bank. The overall flow chart of software is shown in figure:

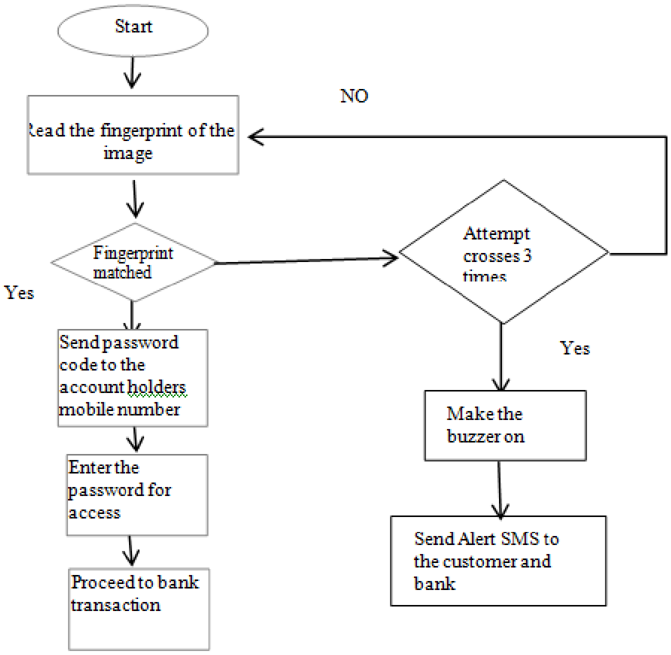
Start
Read the fingerprint of the image
NO
Fingerprint matched
Attempt crosses 3 times
Yes
Yes
Send password code to the account holders mobile number
Make the buzzer on
Enter the password for access
Send Alert SMS to the customer and bank
Proceed to bank transaction

Fig.1 Flowchart of the software

## III. THE CHARACTERISTICS OF THE SYSTEM DESIGN

The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzed existed ATM system. The S3C2440 chip is used as the core of these embedded system which is associated with the technologies of fingerprint recognition and current high speed network communication. The primary functions are shown as follows:

- Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.
- Remote authentication: System can compare current client's fingerprint information with remote fingerprint data server.
- Message alarming: different 4-digit code as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.
- Two discriminate analysis methods: Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

### A. Hardware Design

The S3C2440 chip is used as the core of entire hardware. Furthermore, the modules of LCD, keyboard, alarm, fingerprint recognition are connected with the main chip (S3C2440).The SRAM and FLASH are also embodied in the system. There are some modules consisted of the system as follows:

LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 image of 15 gray-scale or 3375 colours.

- keyboard module: It can be used for inputting passwords.
- SRAM and FLASH: The 16-bit 29LV160BB- 70REC of FLASH chip and the 32-bit HY57V561620CT-6 of SRAM chip are connected with the main chip. Their functions are storing the running code, the information of fingerprint and the algorithm.
- Fingerprint recognition module: Atmel Company's AT77CI04B be used as a fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anticorrosion.
- Ethernet switch controller: RTL8308B can provides eight 10/100 Mbps RMII Ethernet ports, which can connect police network and remote fingerprint data server.

### B. Software design

This system of software is implemented by the steps as follows: first of all, the Linux kernel and the File system are loaded into the main chip. The next, the system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required.

First the system is required the owner's fingerprint. If all the recognition is right, the system would send password to the Account holder and he will enter the same password in touch screen for accessing the ATM Terminal. If Authentication Fails then it send the alert message to the Account holder and Bank. The overall flow chart of how all the procedure works out is given below:

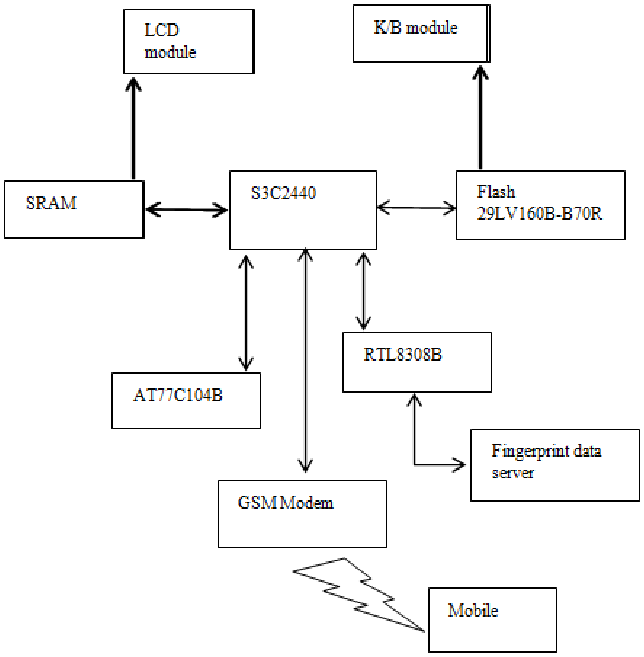

Fig. 2 : Hardware design

### C. The design of fingerprint recognition algorithm

1) The detail of fingerprint recognition process. The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram computing, image enhancement and image binarization. Lastly, the characteristic value was extracted, and the results of the above measures would be compared with the information of owner's fingerprint in the database so as to verify whether the character is matched, and then the system returned the results matched or not.

### Fingerprint Matching

The fingerprint matching process can be represented by the flowing block diagram

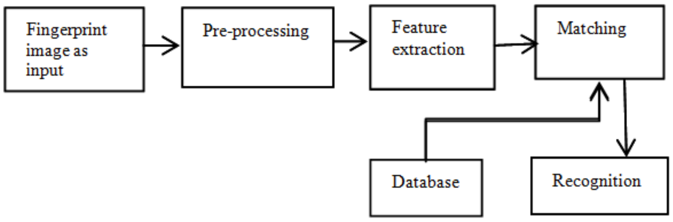

Fig. 3: Matching Block Diagram

The pre-processing aim is to improve the quality of the image. The pre-processing has two tasks: ridge enhancement and restoration and segmentation of fingerprint image. The pre-processing step produces a binary segmented fingerprint ridge image from an input grey scale image. The pre-processing steps involve 1) computation of orientation field 2) foreground/background separation, 3)ridge segmentation , and 4) directional smoothing of ridge [5].

Analysis of the fingerprints shows that the ridges (or the valleys) exhibit different anomalies refered to as ridge ending, ridge bifurcation, short ridge, ridge crossovers etc... There are some eighteen different types of features enumerated and called minutiaes. The most frequently used are the ridge ending and ridge bifurcations, they are as shown in Fig. 3(a) and (b).

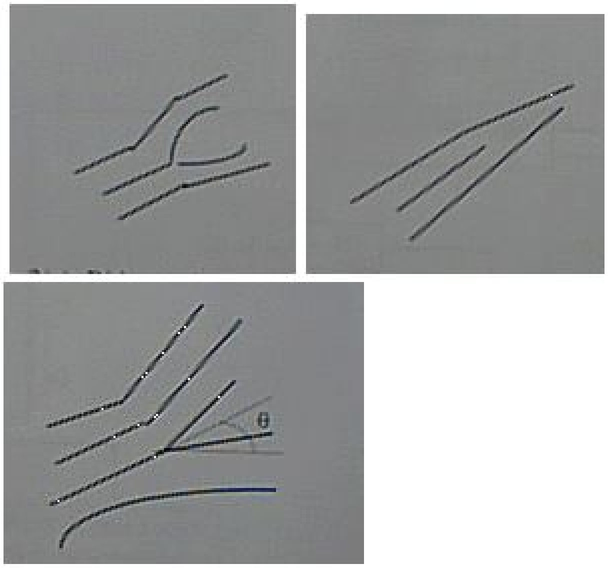

Fig. 3(a): Ridge ending Fig. 3(b): Ridge bifurcation Fig. 3(c): Ridge direction

A typical good finger print has about 70 to 80 minutiae points. Other complex fingerprint features can be expressed as a combination of these two features. The features are normally recorded as a vector with three attributes: the x-co-ordinate, the y-co-ordinate, and the local ridge direction is shown on Fig. 3 (c).

The finger matching is the matching of the minutiae sets. This can done with number of techniques including point set matching , graph matching , and sub-graph isomorphism [2]

## A.FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING AND CROSING NUMBER :

### 1. Fingerprint

A fingerprint is the feature pattern of a finger as shown in figure 4. It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. The two most prominent local ridge characteristics, called minutiae, are 1) Ridge ending and 2) Ridge bifurcation.[3].

A good quality fingerprint contains 25 to 80 minutiae depending on sensor resolution and finger placement on the sensor. The false minutiae are the false ridge breaks due to insufficient amount of ink and cross-connections due to over inking. It is difficult to extract reliably minutia from poor quality fingerprint impressions arising from very dry fingers and fingers mutilated by scars, scratches due to accidents, injuries. The motivation behind the work is growing need to identify a person for security. The fingerprint is one of the popular biometric methods used to authenticate human being.

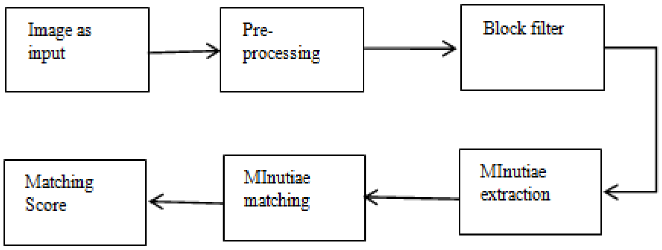

Fig 4.Block Diagram of FRMSM

**A. Binarization:** The pre-processing of FRMSM uses Binarization to convert gray scale image into binary image by fixing the threshold value. The pixel values above and below the threshold are set to ‘1’ and ‘0’ respectively.

**B. Block Filter:** The binarized image is thinned using Block Filter to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning does not change the location and orientation of minutiae points compared to original fingerprint which ensures accurate estimation of minutiae points. Thinning preserves outermost pixels by placing white pixels at the boundary of the image, as a result first five and last five rows, first five and last five columns are assigned value of one. Dilation and erosion are used to thin the ridges.

**C. Minutiae Extraction:** The minutiae location derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively

**D. Minutiae Matching:** To compare the input fingerprint data with the template data Minutiae matching is used. For efficient matching process, the extracted data is stored in the matrix format. The data matrix is as follows. Number of rows: Number of minutiae points. Number of columns: 4
Column 1: Row index of each minutia point.
Column 2: Column index of each minutia point.
Column 3: Orientation angle of each minutia point.
Column 4: Type of minutia. (A value of ‘1’ is assigned for termination, and ‘3’ is assigned for bifurcation).

**Problem definition:** Given the test Fingerprint Image the objectives are,
1. Pre-processing the test Fingerprint.
2. Extract the minutiae points.
3. Matching test Fingerprint with the database.Table 1 gives the algorithm for fingerprint verification, in which input test fingerprint image is compared with template fingerprint with template fingerprint image, for recognition

**E. Matching Score:** it is used to calculate the matching score between the input and template data is given in an equation (3)
Matching score = Matching Minutiae / Max(NT,NI )

Where, NT and NI represent the total number of minutiae in the template and input matrices respectively. By this definition, the matching score takes on a value between 0 and 1. Matching score of 1 and 0 indicates that data matches perfectly and data is completely mismatched respectively

**GSM:** Global System for Mobile Communications ( GSM: originally from Group Special Mobile) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that 82% of the global mobile market uses the standard GSM is used by over 2 billion people across more than 212 countries and territories. GSM differs from its predecessors in that both signalling and speech channels are digital call quality, and thus is considered a second generation (2G) mobile phone system. This has also meant that data communication was built into the system using the 3rd Generation Partnership Project (3GPP). GSM also pioneered a low-cost alternative to voice calls, the Short message service. GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world.

## VI. CONCLUSION

This type of ATM prototype can be efficiently used with fingerprint recognition. Since, password protection is not bypassed in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease for use. Fingerprint images cannot be recreated from templates; hence no one can misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed of execution can be enhanced with the use of more sophisticated microcontroller. The security options were increased for the most part for the stability and dependableness of owner recognition. The whole system was built on the technology of embedded system that makes the system additional safe, reliable and straightforward to use. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

## REFERENCES

[1] Anil K. Jain and Arun Ross, "Multibiometric Systems", Communications Of The ACM, January 2004/Vol. 47,

[2] Ching-Tang Hsieh and Chia-Shing –u, "Humanoid Fingerprint Recognition Based on Fuzzy Neural Network", International Conference on Circuit, Systems, Signal and Telecommunications, pp. 85-90, (2007). 15].

[3] Liu Wei, "Fingerprint Classification using Singularities Detection", International Journal of Mathematics and Computers in Simulation, issue 2, vol. 2, pp. 158-162, (2008).

[4] Bhawna Negi 1 , Varun Sharma"Fingerprint Recognition System", International Journal of Electronics and Computer Science Engineering 872 , www.ijecse.org ISSN- 2277-2011.

[5] Ravi. J, K. B. Raja, Venugopal. K. R,"Fingerprint Recogniti on Using Minutia Score Matching", International Journal of Engineering Science and Technology Vol.1(2), 2009,35-42.(2012)

[6] Pennam Krishnamurthy, Mr. M. Maddhusudhan Redddy," Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 – 071X,(2012)

[7] Bhupesh Gour, T. K. Bandopadhyaya and Sudhir Sharma, "Fingerprint Feature Extraction using Midpoint Ridge Contour Method and Neural Network", International Journal of Computer Science and Network Security, vol. 8, no, 7, pp. 99-109, (2008)

[8] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37: 543-553.

[9] Cheng J, Tian J. Fingerprint enhancement with dyadic scale-space. Pattern Recognition Letters, 2004, 25(11): 1273-1284.