International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 2, Issue 6

ATM Transaction Using Biometric Fingerprint Technology

Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari

***Abstract*- The main objective of this system is to develop an system, which is used for ATM security applications. In these systems, Bankers will collect the customer finger prints and mobile number while opening the accounts then customer only access ATM machine. The working of these ATM machine is when customer place finger on the finger print module when it access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the screen. After entering it checks whether it is a valid one or not and allows the customer further access.**

***Keywords*- ATM, biometric , fingerprint, PIN, security ,.**

I. INTRODUCTION

Now-a-days, in the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Using the ATM (Automatic Teller Machine) which provide customers with the convenient banknote trading is very common. However, 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. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated and sending the four digit code by the controller which 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 effectively.

II. SOFTWARE DESIGN

This software is implemented by the steps as follows: first of all. 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.

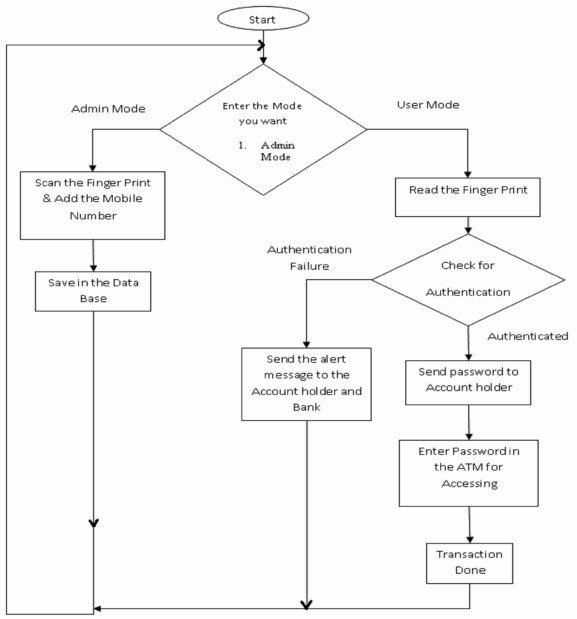


Fig 1. The overall flow chart of software

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 [1].[23]

III. WHY BIOMETRICS FINGERPRINT

A.Advantages

- Uniqueness
- Surety over the Cards and Keypads
- Against to Cards Duplication, misplacement and improper disclosure of password
- No excuses for RF/Magnetic Cards forget ness
- No need to further invest on the Cards Cost

B.comparison between all biometrics

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and

the most prevalent in use today . In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on . The result of the survey conducted by the International Biometric Group (IBG) in 2012 on comparative analysis of fingerprint with other biometrics is presented in Figure. 2.

The result shows that a substantial margin exists between the uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature and middleware .

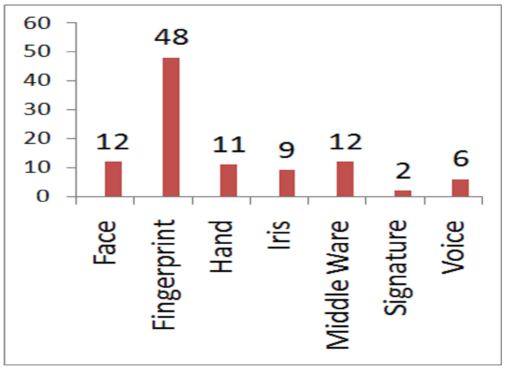


Fig.2. Comparative survey of fingerprint with other biometrics

The row for the eye biometric describes features applying to either iris or retinal scanning technologies.

- All technologies are appropriate for 1-to-1 matching, only fingerprint and eye technologies are proven to have acceptable recognition rates to be practical for 1-to-many matching. This is an indication that these two modalities provide the highest recognition rates for verification as well.
- Variation of the salient features used for recognition is very different for different modalities. Fingerprint and eye features remain consistent for a lifetime, whereas the others change with growth. On a day-to-day basis, there is far less variation for all modalities, though voice can change with illness and signature with demeanor.
- As far as sensor cost, eye systems are currently more costly than the others; voice systems can be zero cost to the user if a telephone is used.
- Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest.[1][2][9][11][14]

IV. Introduction of Fingerprint

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example,when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges also assist in gripping rough surfaces, as well as smooth wet surfaces.Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the eccrine glands that are present in friction ridge skin, or they may be made by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.[1][3][7][8][12]

V. Fingerprints For Identification

A.Electronic recording

There has been a newspaper report of a man selling stolen watches sending images of them on a mobile phone, and those images included parts of his hands in enough detail for police to be able to identify fingerprint patterns. Classifying fingerprints Before computerisation replaced manual filing systems in large fingerprint operations, manual fingerprint classification systems were used to categorize fingerprints based on general ridge formations (such as the presence or absence of circular patterns on various fingers), thus permitting filing and retrieval of paper records in large collections based on friction ridge patterns alone. The most popular ten-print classification systems include the Roscher system, the Juan Vucetich system, and the Henry Classification System. Of these systems, the Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries.[9] In the Henry system of classification, there are three basic fingerprint patterns: Loop, Whorl and Arch, which constitute 60–65%, 30–35% and 5% of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches,and into loops that may be radial or ulnar, depending on the side of the hand the tail points towards. Whorls may not have sub-group classifications it including only plain whorls. [21] [23]

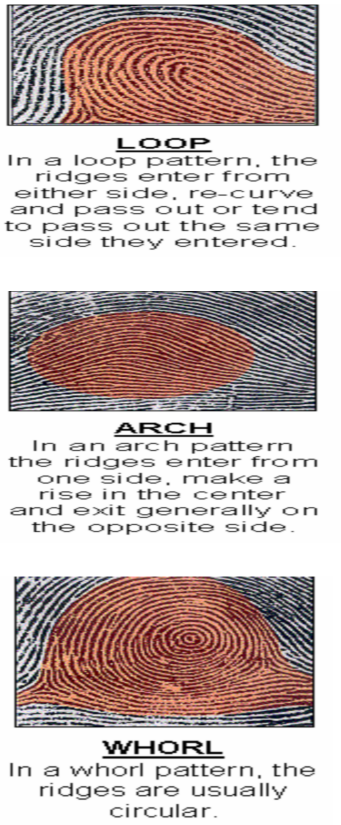


Fig.3 Characterics Of Fingerprint

VI. ALGORITHM

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.

- Ridge Termination/ end **:** The location where a ridge comes to an end.
- Ridge Bifurcation/Branch **:** The location where a ridge divides into two separate ridges

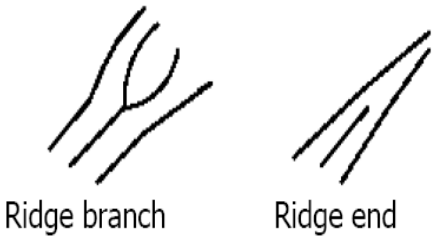


Fig 4.Ridge end and bifurcation of the fingerprint

2.Fingerprint recognition

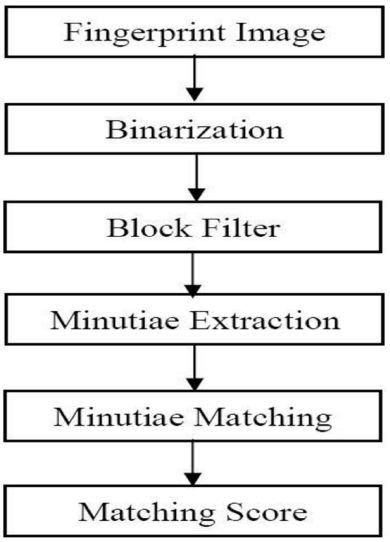


Fig 3: Block Diagram of FRMSM

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. An original image and the i mage after Binarization are shown in the Figure 5.

Fig 5: (a) Original Fingerprint (b) Binarized image.

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. A binarized Fingerprint and the image after thinning are shown in Figure 6.

(a) (b)

Fig6:(a)BinarizedFingerprint (b) Image after thinning

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, is shown in figure7

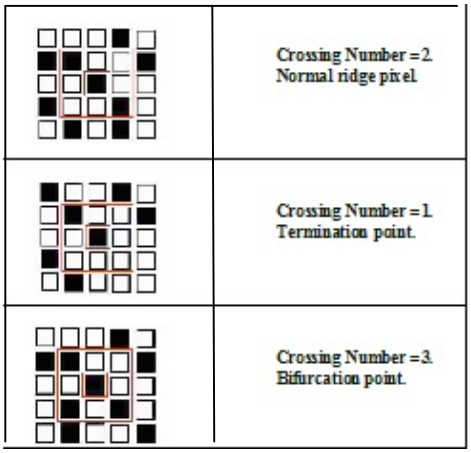
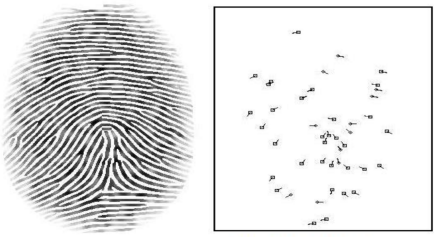


Fig 7: Crossing Number and Type of Minutiae.

Figure.8 shows the original image and the extracted minutiae points. Square shape shows the position of termination and diamond shape shows the position of bifurcation as in figure.8 (b)



(a) (b)

Fig 8: (a) Gray-scale Fingerprint (b) Minutiae points.

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.

Input: Gray-scale Fingerprint image.
Output: Verified fingerprint image with matching score.
1. Fingerprint is binarized
2. Thinning on binarized image
3. Minutiae points are extracted. Data matrix is generated to get the position,
orientation and type of minutiae.
4. Matching of test fingerprint with template
5. Matching score of two images is computed, if matching score is 1 images are
matched and if it is 0 then they are mismatched.

Table 1: Algorithm of FRMSM

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) ------- (3)

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.[12][15][18][21][22][23]

FUTURE SCOPE

A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [5]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations [6]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. 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 since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. This technique is very useful in future for avoiding the fraud in ATM system.

CONCLUSION

In this way, the implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additional, the system also contains the original verifying methods which was inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was build on the fingerprint technology which makes the system more safe, reliable and easy to use.

REFERENCES

1]. G.Sambasiva Rao, C. NagaRaju, L. S. S. Reddy and E. V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", International Journal of Computer Science and Network Security, vol. 8, pp. 394-397, (2008).
2]. Robert Hastings, "Ridge Enhancement in Fingerprint Images Using Oriented Diffusion", IEEE Computer Society on Digital Image Computing Techniques and Applications, pp. 245-252, (2007).
3]. Jinwei Gu, Jie Zhou, and Chunyu Yang, "Fingerprint Recognition by Combining Global Structure and Local Cues", IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 1952 – 1964, (2006).
4]. V. Vijaya Kumari and N. Suriyanarayanan, "Performance Measure of Local Operators in Fingerprint Detection", Academic Open Internet Journal, vol. 23, pp. 1-7, (2008).
5]. Raju Sonavane and B. S. Sawant, "Noisy Fingerprint Image Enhancement Technique for Image Analysis: A Structure Similarity Measure Approach", Journal of Computer Science and Network Security, vol. 7 no. 9, pp. 225-230, (2007).
6]. Eric P. Kukula, Christine R. Blomeke, Shimon K. Modi, and Tephen J. Elliott, "Effect of Human Interaction on Fingerprint Matching Performance, Image Quality, and Minutiae Count", International Conference on Information Technology and Applications, pp. 771-776, (2008).
7]. M. R. Girgisa, A. A. Sewisyb and R. F. Mansourc, "Employing Generic Algorithms for Precise Fingerprint Matching Based on Line Extraction", Graphics, Vision and Image Procession Journal, vol. 7, pp. 51-59, (2007).
8]. Luping Ji, Zhang Yi, "Fingerprint Orientation field Estimation using Ridge Protection", The Journal of the Pattern Recognition, vol. 41, pp. 1491-1503, (2008).
9]. Duresuoquian Miao, Qingshi Tang, and Wenjie Fu, "Fingerprint Minutiae Extraction Based on Principal Cures", the Journal of the Pattern Recognition Letters, vol. 28, pp. 2184-2189, (2007).
10]. Alessandra Lumini, and Loris Nann, "Advanced Methods for Two-Class Pattern Recognition Problem Formulation for Minutiae-Based Fingerprint Verification", the Journal of the Pattern Recognition Letters, vol. 29, pp. 142-148, (2008).
11]. Xifeng Tong, Songbo Liu, Jianhua Huang, and Xianglong Tang, "Local Relative Location Error Descriptior-Based Fingerprint Minutiae Matching", the Journal of the Pattern Recognition Letters, vol. 29, pp. 286-294, (2008).
12]. L. Lam S W Lee, and C Y Suen, "Thinning Methodologies-A Comprehensive Survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, pp. 869-885, (1992).
13]. Mohamed. S. M and Nyongesa.H, "Automatic Fingerprint Classification System using Fuzzy Neural techniques", IEEE International Conference on Artificial Neural Networks, vol. 1, pp. 358-362, (2002).
14]. 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]. Liu Wei, "Fingerprint Classification using Singularities Detection", International Journal of Mathematics and Computers in Simulation, issue 2, vol. 2, pp. 158-162, (2008).
16]. Hartwing Fronthaler, Klaus kollreider, and Josef Bigun, "Local Features for Enhancement and Minutiae Extraction in Fingerprints", IEEE Transactions on Image Processing, vol. 17, no, 3, pp. 354- 363, (2008).
17]. Mana Tarjoman, and Shaghayegh Zarei, "Automatic Fingerprint Classification using Graph Theory",Proceedings of World Academy of Science, Engineering and Technology, vol. 30, pp. 831-835, (2008).
18]. 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).
19]. Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique", Proceedings of World Academy of Science, Engineering and Technology vol. 36, pp. 497-502, (2008).
20]. Haiping Lu, Xudong Jiang and Wei-Yun Yau, "Effective and Efficient Fingerprint Image Post processing", International Conference on Control, Automation, Robotics andVision,vol.2,pp.985-989,(2002)
21]. Bhawna Negi 1 , Varun Sharma"Fingerprint Recognition System", International Journal of Electronics and Computer Science Engineering 872 , www.ijecse.org ISSN- 2277-2011.
22]. 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)
23]. 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)

AUTHOR'S PROFILE

[1]Mr.Mahesh Annasaheb Patil

Anuradha Engineering College,Chikhli
Dist-Buldhana State-Maharashtra
Email-Patilmahesh670@gmail.com

[2]Mr.Sachin Pralhad Wanere

Anuradha Engineering College,Chikhli
Dist-Buldhana State-Maharashtra
Email-swanere692@gmail.com

[3]Mr.Rupesh Pandurang Maighane

Anuradha Engineering College,Chikhli
Dist-Buldhana State-Maharashtra
Email-rups768@gmail.com

[4]Mr.Aashay Ramratan Tiwari

Anuradha Engineering College,Chikhli
Dist-Buldhana State-Maharashtra
Email-tiwari.aashay@gmail.com