A NEW BUSINESS MODEL FOR ATM TRANSACTION SECURITY USING FINGERPRINT RECOGNITION

[1]SOWMYA RAVIKUMAR, [1]SANDHYA VAIDYANATHAN, [2]B.THAMOTHARAN, [2]S.RAMAKRISHNAN

[1] Student, School of Computing, SASTRA University, India,
[2] Asst. Prof., School of Computing, SASTRA University, India,
E-mail: sowmya6691@gmail.com, sandhyavaithy@gmail.com, balakrishthamo@gmail.com, srk@ict.sastra.edu,

ABSTRACT

Money transactions play a vital role in the nature of trade. Today, ATMs and Credit cards are used for this purpose, the authentication of these transactions are unsecure. To overcome this shortcoming of piracy in money transactions, the author proposes the idea of using fingerprints of customers as password in place of traditional pin number. Here, if the fingerprint is recognized, then it allows transaction. This model has an additional feature i.e., a reference fingerprint of the nominee or a close family member of the customer can be used if the customer is not available in case of emergencies. This proposed business model helps the society, mainly the rural people, by enhancing the security using Fingerprint recognition in Digital image processing. As the fingerprint of every person is unique and unchangeable, this biometric feature is used over the others.

Keywords: *ATM, Fingerprint, PIN, Fingerprint Recognition, Reference Fingerprint*

1. INTRODUCTION

An Automated Teller Machine (ATM) is a computerized telecommunications device that enables the clients of any financial institution to perform financial transactions like deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash etc. without the need for a cashier, human clerk or bank teller. There are two types of ATMs: first, it is a simple ATM used only for cash withdrawal and to receive a report on account's balance and second one is a complex unit, which is used for deposits and money transfer. Frequently and popularly, people use the first type of ATM.

ATMs are located not only in banks' premises but also in other places where people need cash frequently like shopping malls, airports & railway stations, hotels and restaurants. They are scattered throughout the cities, allowing the clients to access their accounts easily. Usually to perform a transaction a customer has to use an ATM card which is issued by the respective financial institution and a personal identification number (PIN) is given along with each card for authorization of the customer's account.

Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Many people, who aren't familiar with the concept of PIN are unlikely to memorize and recognize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel unsafe that their account could be accessed by others and they would lose all their money.

To enhance security and authentication of the customer's account, the concept of using the fingerprint of the customer as password instead of PIN is proposed, since biometric fingerprint is unique for each and every human being and it has more authentication than the PIN.

In this paper, the author discusses the existing ATM system; the proposed system; resource requirements; fingerprint recognition; the advantages of the proposed system and few insights on future work.

2. EXISTING ATM SYSTEM

People use the ATM for transactions such as cash withdrawal, money transfer and payment of electricity and telephone bills. ATM is the most convenient to access the accounts and funding transactions. Personal Identification Number (PIN) is an important aspect of the current ATM system in providing security and it is a commonly used method in protecting the transaction of one's account. PIN is a four digit number which is generated by the respective financial institution. PIN is very easily remembered and is also changeable according to the user. But, sometimes PIN's strength is decreased as the tracking of the code is increased. "Most commonly PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN." In the existing system, the user has to insert the card and the PIN number. If PIN is correct, the system allows for transaction. Else, the system asks for PIN again and it allows maximum of three times to enter it.

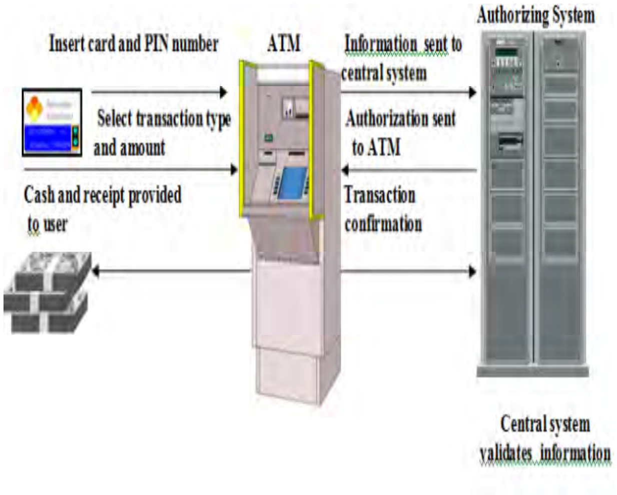

Authorizing System
Insert card and PIN number
ATM
Information sent to central system
Select transaction type and amount
Authorization sent to ATM
Cash and receipt provided to user
Transaction confirmation
Central system validates information

Figure 1- Existing ATM system

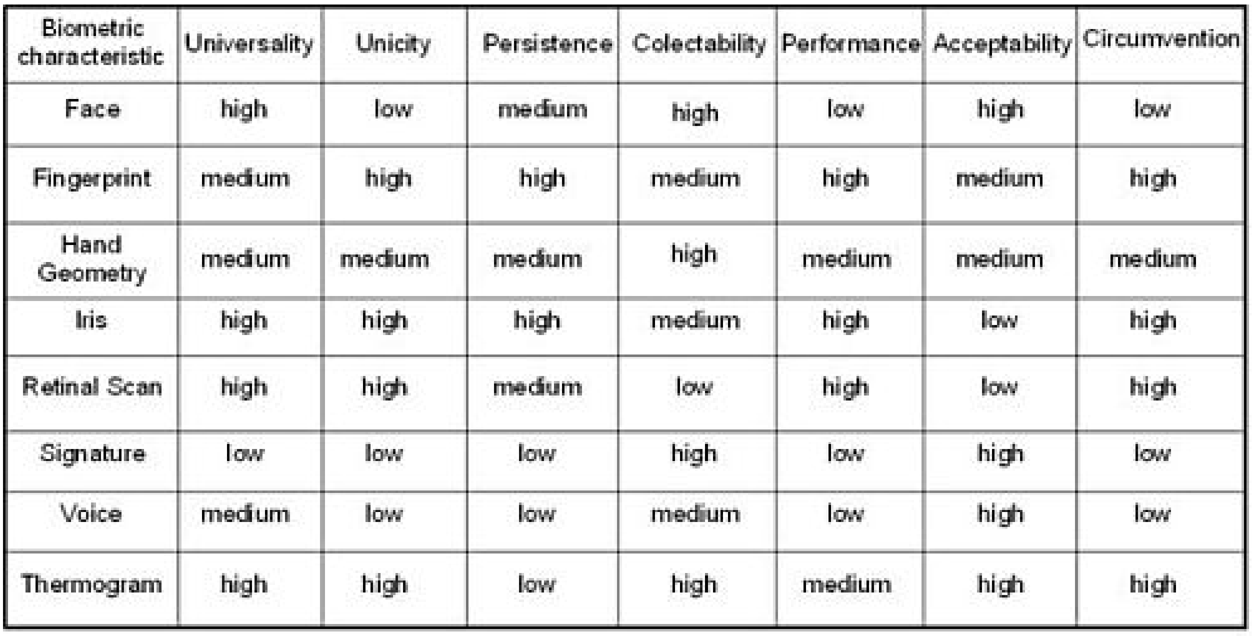
3. PROPOSED SYSTEM

The basic reasons of the proposed system along with its design are mentioned as follows.

3.1. Why Fingerprint. There are many biometric characteristics like fingerprint, hand geometry, iris, retina, ear, voice and face. Each of these characteristics has its own advantages and disadvantages, and hence the selection among the biometrics depends on the requirements and authentication of the application. Among these, fingerprints are chosen. Fingerprints are patterns formed on the epidermis of the finger, composed of ridges and valleys. This interleaved pattern of ridges and valleys make an important and evident characteristic of the fingerprint. Following are some reasons for the selection:

- Reliable: The findings of (Jain et al, 1999) showed that every human being has unique fingerprint. Not even twins have the same.
- Universality: The findings of (Jain et al, 1999) showed that majority of the population in the world have fingerprints.
- Permanent: The findings of (Jain et al, 1999) showed that fingerprints are permanent in nature; their characteristics don’t change over the course of time. They are formed in the fetal stage and it remains structurally unchanged.
- Storage: Fingerprint requires only small amount of storage.
- Accuracy: The findings of (Jain et al, 1999) showed that fingerprints offer the more accuracy when compared to other biometrics.
- Inexpensive: Fingerprint acquisition, operations and maintenance are relatively inexpensive in nature.

The following table gives the comparison of characteristics of different biometrics based on the findings of (Delac et al, 2004):



Biometric characteristic	Universality	Unicity	Persistence	Colectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice	medium	low	low	medium	low	high	low
Thermogram	high	high	low	high	medium	high	high

Table 1-Comparison of biometrics' characteristics

3.2. Proposed system's strategy. The author proposes the idea of using fingerprints (primary and reference) in ATMs as passwords instead of the traditional pin number. By using fingerprint recognition, the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. Here every account has two passwords, i.e., two fingerprints. The primary fingerprint is that of the account holder's and the reference fingerprint could be of the nominee's or a close family member. The reason behind the introduction of two passwords is to provide access to the account even if he/she is in an emergency situation and is in need of money, or when he/she has met with an accident, or has injuries on finger tips the nominee can access the account. The nominee will be given a controlled or minimum access, i.e., he/she will not be able to withdraw more than a certain amount on the same day. This proposed system is a benefit for both banks and customers in terms of security. And hence is a good business model.

3.3. Procedure. The proposed system's steps are as follows.

STEP 1: Insertion of ATM Card by the user.

STEP 2: Input fingerprint on the scan pad (Primary or Reference print)

STEP 3: Fingerprint verification

STEP 4: If Valid

STEP 5: Execute Transaction

ELSE RETRY (GOTO STEP 2 Max.3 times)

STEP 6: Terminate

3.4. Design. The design is supported with the help of UML tools to represent how the user interacts with the proposed system. To keep it simple, ATM system which is used only for cash withdrawals and report inquiries is considered.

3.4.1. Use case diagram. Use case diagram represents the interaction between the customer and the system. In this diagram, Admin controls the proper functioning of ATM machine; User performs the transaction process (Withdrawal, Inquiry) and the Database requests and permits valid transactions.

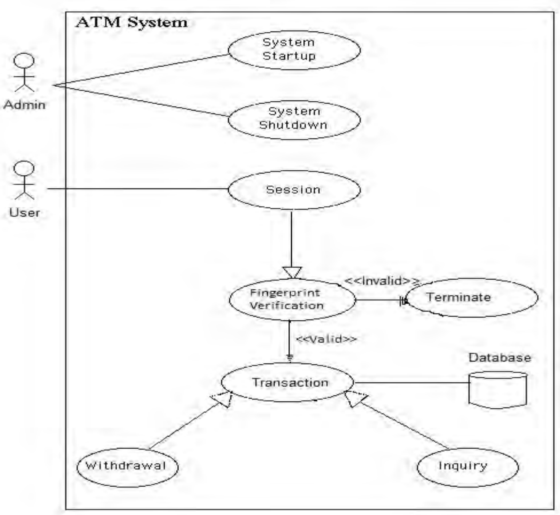


Figure 2- Use Case Diagram

4. RESOURCE REQUIREMENTS

For the proposed system, a fingerprint reader and embedded software which performs fingerprint verification process along with the ATM machine is required. The fingerprint reader is nothing but a sensor. It is used to capture the digital image of the customer fingerprint. The captured image is a live scan, which is used for the verification with templates stored in the database server. Here, an optical multispectral sensor is used for scanning because it provides a clean and clear image even in the presence of dirt, pressure changes, temperature changes and humidity changes. The source code which performs the fingerprint recognition is done using MATLAB.

5. FINGERPRINT RECOGNITION

Fingerprint recognition is a process which is used to compare the given input image with the template fingerprint image that is stored in the database. Fingerprint Recognition comprises of four steps. They are:

1. Image acquisition-which is done by the optical multispectral sensor.
2. Image enhancement-used to adjust the contrast of the image and also to remove noise.
3. Fingerprint image segmentation- this is used to extract the region of interest, which is further used for feature extraction such as minutiae.
4. Matching-based on the extracted features, the verification of the given image is done with the image in the database and returns the result either as true or false.

The matching result determines whether the customer can access the account or not. Its design is represented in the following diagram:

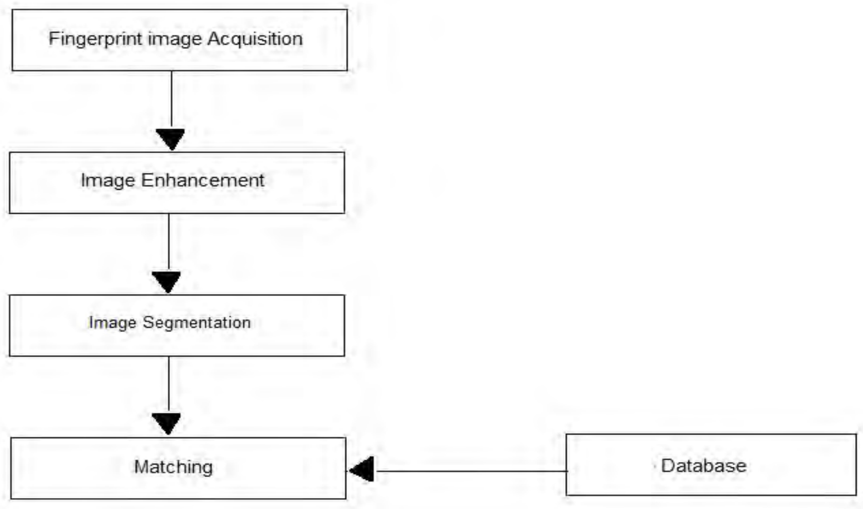


Figure 3- Fingerprint recognition system’s design

5.1. Image enhancement. This process comprises of two steps, they are:

1. Histogram equalization: it is a normalization method to adjust the image's intensity values, such that the contrast of the image is enhanced.
2. Gabor filters: these are used to further enhance the clarity of the image by detecting the edges, i.e., the ridges of the fingerprint. The Gabor filter capture the periodic nature of the fingerprint and its mathematical form is given:

$$G(x, y, f) = \exp \{-0.5* [x^2/ \ {}^2{}_x + y^2/ \ {}^2{}_y]\} \cos (2\pi fx)$$

$$x= x \cos \theta+ y \sin \theta$$

$$y= -x \sin \theta+ y \cos \theta$$

where f represents the ridge frequency.

5.2. Image segmentation. Segmentation of the image is done to retrieve the region of interest from the image, which alone can be used further in the processing. This process is of three steps they are:

1. Binarization: The gray level enhanced image is converted to a binarized image with 0 as ridges and 1 as valleys.
2. Orientation field estimation: in this, the angle of orientation at each and every pixel is calculated using the x and y gradients of Sobel operator and the orientation field is calculated using the least mean square method implemented by Hong et al.
3. ROI extraction: the region of interest is extracted from the image using the morphological operators 'open' and 'close'.

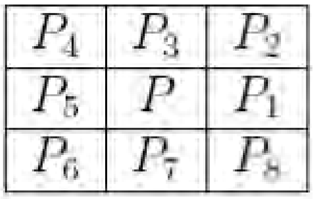
The further processing of fingerprint recognition is done only on this ROI.

5.3. Matching. Matching of two fingerprints is done based on the features extracted from the fingerprint. In this proposed business model, we use minutiae based matching technique.

Minutiae are the most important features of fingerprint; these include ridge bifurcations- ridge dividing into two and ridge terminations- abrupt end of a ridge.

Before the process of minutiae extraction, thinning of the segmented image is performed. Thinning is done, so that the ridges are only one pixel wide. After thinning, many spurious pixels may be formed, such as H-breaks and spikes. These spurs are removed using morphological operators.

5.3.1 Minutiae extraction. Crossing number method is used to extract minutiae from the fingerprint image. The findings of (Bansal et al, 2007) showed that the minutiae are extracted by using a 3X3 window, which scans the local neighbourhood of every pixel.



P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 4-Neighbourhood of pixel P

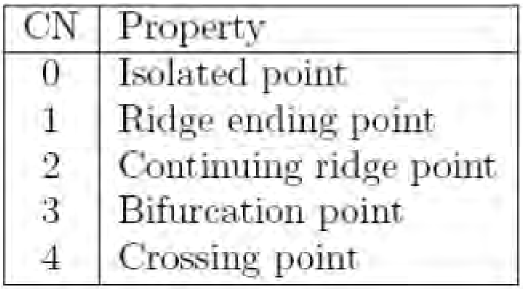
The findings of (Bansal et al, 2007) showed that the CN value is computed as:

$$CN=0.5\sum(P(i)-P(i+1)); \qquad i=1 \text{ to } 8$$

Where P(i) : pixel value in the neighbourhood of P.

After the CN value is computed, based on its properties, we find the nature of the pixel.

The findings of (Bansal et al, 2007) showed that CN's properties are as follows:



CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Table 2- CN's properties.

For each extracted minutiae; its x & y co-ordinates, the orientation angle of the associated ridge and its type are recorded.

5.3.2. Minutiae based matching. Each and every minutiae of the input image is compared to every minutia in the template image. In each case of input and template, reference points are selected. These reference points are used to convert the remaining minutiae set into polar co-ordinates. For both the input and template, the radial distance, the radial angle and the orientation angle of each minutia is found out. These formulae are given below as per the findings of (Feng, 2008):

Radial distance:

$$r_k = \sqrt{\left\{\left(x_k - x_{ref}\right)^2 + \left(y_k - y_{ref}\right)^2\right\}}$$

Radial angle:

$$\varphi_k = \tan^{-1}\frac{\left(x_k - x_{ref}\right)}{\left(y_k - y_{ref}\right)}$$

Orientation angle:

$$\theta_k = \theta_k - \theta_{ref}$$

Here,x_k,y_k,θ_k are the x, y co-ordinates and the orientation angle of the respective minutia. And $x_{ref}, y_{ref}, \theta_{ref}$ are those of the reference point selected.

Once calculated for both input and template, these are compared and the matching score is found out. The matching score is given as per the findings of (Feng, 2008):

$$Matching\ Score = \frac{MatchingMinutiae}{\max\left(NI, NT\right)}$$

Where NI=number of minutiae in input image and NT= number of minutiae in template image.

If the matching score is 1, then the fingerprint is matched exactly and 0 if they are mismatched. Thus the fingerprint recognition is done in this system.

6. ADVANTAGES OF THE PROPOSED SYSTEM

These are the advantages of the proposed system when compared to existing system:

1. Provides increased security.
2. Helps the less educated people in rural India, as it alleviates the burden of remembering the pin number.
3. In the case of pin number as password all those who are aware of the pin can access the account whereas, the facility of the reference fingerprint allows only one other person to use the account which is a win-win situation for both customers and bank.
4. Compared to all other biometric systems this is cost effective.

7. FUTURE WORK

To enhance authentication, multi modal biometric security systems, such as Iris or Face recognition along with fingerprint recognition can be used. This will increase security and also clients are given more secrecy and privacy. And also this application of using fingerprint as password can be extended to e-polling through ATM.

8. CONCLUSION

ATMs have become more important to the society. There are millions of money transactions that happen in a single day through ATM. There are many frauds that occur in ATM, mainly due to PIN. So, this proposed system enhances security on money transactions and has also made ATMs an easier access for the less educated. This method when fully deployed will not only increase the authentication, but will also help in the implementation of complex ATMs (performs deposits and money transfer), as this system provides increased security.

REFERENCES

[1] Misra, D. K., Dr. Tripathi, S. P., Singh, A., (2012),*Fingerprint Image Enhancement, Thinning and Matching,* International Journal of Emerging Trends & Technology in Computer Science (ISSN 2278-6856), Volume 1, Issue 2.

[2] Selvaraju, N. and Sekar, G., (2010), *A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm,* International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6.

[3] Feng, J.,(2008),*Combining minutiae descriptors for fingerprint matching,* Pattern Recognition 41, 342 – 352.

[4] Jain, A.K., Prabhakar, S., Hong, L., (1999), *A multichannel approach to fingerprint classification*, IEEE Trans. Pattern Anal. Mach. Intell. 21 (4),348–359.

[5] FVC2002, Second international fingerprint verification competition, _http://bias.csr.unibo.it/fvc2002/_.

[6] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S.,(2009), *Handbook of Fingerprint Recognition (2nd Edition)*. Springer.

[7] Jiang, X. and Yau, W. Y.,(2000), *Fingerprint Minutiae Matching Based on the Local and Global Structures*, In Proc. of ICPR, volume 2, pages 6038–6041, Barcelona, Spain.

[8] Mathlab Works ,Inc.

[9] Delac, K. and Grgic, M.,(2004), *A Survey of Biometric Recognition Methods*, 46th International Symposium Electronics in Marine, ELMAR.

[10] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). *Biometrics: Personal Identification in Networked Society*', Kluwer Academic Publications, ISBN 978-0-7923-8345-1.

[11] Bansal, R., Sehgal, P. and Bedi, P.,(2011), *Minutiae extraction from fingerprint images- a review*, IJCSI, Vol. 8, Issue 5.