A Constraint-based Biometric Scheme on ATM and Swiping Machine

Sweta Singh
Department of Computer Science and Engineering
Madan Mohan Malaviya University of Technology, Gorakhpur, India
swetasss22691@gmail.com

Akhilesh Singh
Department of Computer Science and Engineering
Madan Mohan Malaviya University of Technology, Gorakhpur, India
akhilesh840@gmail.com

Rakesh Kumar
Department of Computer Science and Engineering
Madan Mohan Malaviya University of Technology, Gorakhpur, India
rkiitr@gmail.com

***Abstract*—In this modern scientific world, technologies are transforming rapidly but along with the ease and comfort they also bring in a big concern for security. Taking into account the physical security of the system to ensure access control and authentication of users, made us to switch to a new system of Biometric combined with ATM PIN as PIN can easily be guessed, stolen or misused. Biometric is added with the existing technology to double the security in order to reduce ATM frauds but it has also put forward several issues which include sensor durability and time consumption. This paper envelops two questions "Is it really worthy to go through the entire biometric process to just debit a low amount?" and "What could be the maximum amount one can lose if one's card is misused?" As an answer we propose a constraint on transactions by ATM involving biometric to improve the system performance and to solve the defined issues. The proposal is divided in two parts. The first part solves sensor performance issue by adding a limit on amount of cash and number of transactions is defined in such a way that if one need to withdraw a big amount OR attempts for multiple transactions by withdrawing small amount again and again, it shall be necessary to present biometric. On the other hand if one need to make only balance enquiry or the cash is low and the number of transactions in a day is less than defined attempts, biometric presentation is not mandatory. It may help users to save time and maintain sensor performance by not furnishing their biometric for few hundred apart from maintaining security. In the second part this paper explains how fingerprint verification is conducted if the claimant is allowed to access the system and what could be the measures to increase performance of fingerprint biometric system which could be added to our proposed system to enhance the overall system performance.**

Keywords—Access Control; Biometric; Electronic Data Capture (EDC; Fingerprint Verification; Constraint based Biometric

I. INTRODUCTION

Security has always been a major concern and goal of all organization. There is no such object which can be considered as completely secure especially if it is about money. Security is not only confined to network but also includes Physical security. When talking about ATM machines or EDC we are mainly concerned with Physical security which aims at ensuring Access control, Identification and Authentication. Access control is another consideration of Information System security to confirm the identity of individual so that only authorized entity is accessible to the system. With the development of banking technology the way of banking has changed. On one hand where it has freed us from standing in long queues to carry out cash withdrawal, depositing money, transferring money and many more on the other it has also increased the risks of theft [1]. ATM (Automatic Teller Machine) has proved to be an easy and convenient way to carry out all our banking tasks in just few minutes [2]. An ATM card or debit card authenticates person after verification of card number, Expiry date, card holders name and the PIN. But what in case your card is stolen, or PIN is known to an unknown entity. For this we require a higher level of security which coined up an idea of adding Biometric to the current technology. Biometric has emerged as a measure for highly secure identification and personal verification [3]. Biometric system, to conduct the verification requires a sensor every time to collect the biometric sample. This sensor is exposed to dusty, sweaty and oily hands depending on person to person thus effects the sensitivity of sensor to gather the accurate sample for verification. There can be a chance when a person needs to withdraw only a low amount or want the mini-statement and behind him is a long queue. So, just to debit a little cash, being the first transaction, waiting for biometric identification is simply time-consuming. To skip this problem we propose a concept of introducing a cash and day-transaction limit with the biometric, where one has to present one's biometric only if one wants to withdraw above the defined cash limit OR if the number of transactions are more than specified "k" times (let k=3) or both condition is found to be true else cash withdrawal without biometric is permitted. It also guarantees security as each ATM has its cash limit and bank has its transaction limit. So, in case of card misuse, will prevent withdrawal of large cash in one transaction or even restrict to debit low cash multiple times by making multiple transactions. It will also limit the maximum amount that can be withdrawn by unauthorized person in case of card misuse.

The rest part of the paper envelops: Section II discusses the background of Biometric. Section III, discusses the papers been studied to define the problem and solution approach. Working of biometric is discussed in Section IV. Section V defines the problem statement and the proposed system in brief with the problems it solves and advantages and finally,

978-1-5090-0082-1/16/$31.00 ©2016 IEEE

Section VI concludes the paper with the future scope to further enhance the system.

II. RESEARCH BACKGROUND

This section throws a light upon the concept of biometrics, its working to ensure physical security. It also envelops the concept of Constraint-Based Biometric; the proposed system to improve the efficiency of Biometric system. Some papers [11] [12] [13] have been proposed the approach to lower the time and space complexity of fingerprint matching. By adding their concept to our proposed system, can improve overall performance of Biometric system. The constraint will reduce some time of verification and few seconds will also be reduced by implementing the already defined schemes in verification phase.

*Bi*ometrics: The rise in level of security breaches and transactional frauds has made us to bring in the concept of combining Biometrics with the current banking technology to provide a confidential and authorized financial transaction. Biometrics (Bio + Metrics) is an automated system which defines a security measure related to human behavioural and physiological characteristics [1][3] to accomplish the Identification goal of the personnel. For convenience, Bank institutions have provided us ATM or debit cards to conduct all our transactions or enquiries without visiting bank and waiting in long queues. For security a PIN (Personal Identification Number) is provided by bank which is a secret 4-digit code which authenticates the genuinity of card holder. But still there are chances of misuse and security risks as anyone who knows the PIN is authorized personnel and is allowed to make transactions. There is also a chance of forgetting the PIN or theft using ATM card. Biometrics in such cases provides a full-proof security by recognizing the individual based on the behavioural and physiological characteristics [3]. Physiological characteristics comprises the parts of the body such as fingerprint, face, palm, hand geometry, iris, retina etc whereas Behavioural characteristics (sometimes referred as behaviometrics [6]) covers the pattern of person's behaviour, including flow of typing, gait, and voice. It is added with the ATM to identify the genuine card owner and only granting access to particular individual [1]. It is capable of both verification (one-to-one process to verify if the individual is one who he claims to be) and Identification (one-to-many attempt to identify an unknown entity) [3]. Biometrics involves several mechanisms for data capturing which includes- face recognition, fingerprint identification, voice-based biometric, iris scans, retina scan, and signature.

Fingerprints are unique characteristics of individual which remains same throughout life and are not even same of the identical twins. For identification the person has to submit his fingerprint to the sensor condition that the hands should be clean else could affect the efficiency and accuracy of the system. It is the most widely used scheme for banking system [4]. Later in our paper, we aim to eliminate this particular issue of the biometrics system.

III. LITERATURE REVIEW

As a result of rapid enhancement in Information and Communication Technology security challenges have popped up as the security breachers always aims at finding a loophole in the system. In ATM Security Using Fingerprint Biometric Identifer: An Investigative Study by M.O. Onyesolu has described how biometric procedure has enhanced security to ATM machines by solving the drawback of additional system. A.T. Siddiqui [4] has explained how biometric has emerged to control ATM spam as it only allows genuine entry to the system. A.K. Jain et al. [9] have explained the complete procedure of conduction biometric verification in ATM devices. K. Archana and A. Gowardhan [3] has explained how biometric performance and security can be increased by adding concept of Multimodal Biometrics in place of Unimode Biometric scheme. In a guide [7] describes in detail the collection and matching procedure of biometric sample. Jain et al. [9] describes the detailed concept of miniature extraction in fingerprint verification scheme. Authors of [16][18] has explained and defines a complete analysis of performance by making comparison with various schemes. R.S Germain [14] et al. has defined parameter clustering mechanism to speed up matching technique of biometric procedure. U. Jayaraman et al. [12] has defined how fingerprint verification scheme could be improved reducing time of verification.

IV. WORKING OF BIOMETRIC SYSTEM

Biometric data and Biometric Identification combine to form Biometric System. It involves two phase. First is the Enrollment Phase which is defined as the interval when the individual encounters the biometric system initially, here the subject gets their biometric information stored in the database. Since it is a single-time work it is conducted slowly and multiple times to make an accurate entry in the system. Second is the Verification Phase which involves several steps [4]:

a) *Data Collection:* The very first, time consuming step where the user presents its characteristics to sensing device. In case of fingerprint or palm geometry scan requires a physical contact each time with the sensor. In schemes such as retina scan requires no physical contact.

b) *Transmission*: It is only carried out in open system where the sensor is located at one location and processor at the other. It involves compression of data.

c) *Signal Processing or Pre-Processing*: Having acquired the biometric characteristics need to prepare it for matching. It involves removal of noise and distortion.

d) *Feature Extraction*: The pre-processed data is re-processed to obtain more précised feature with reduced size.

e) *Template Creation*: Template defines a model or standard for making comparison. Thus, a template is created and relayed to comparison algorithm.

f) *Matching*: The last step involves implementation of comparison algorithms to compare the stored template of the individual with the collected sample. On the basis of

978-1-5090-0082-1/16/$31.00 ©2016 IEEE

this comparison the decision to grant or deny access is made.

V. PROPOSED SYSTEM

A. Issue related to Biometric System

Having undergone the concept and working of Biometric, we came across its limitations with respect to input of the system i.e. the sensor .While providing the biometric sample the subject has to physically contact with the sensor of the Biometric system. This touching of sensor each time could degrade the working capability and accuracy of the system. As each time a new individual have to enter and provide his biometrics irrespective of the cleanliness of their hands. It affects the sensitivity of input device being used again and again even in case of small amount. In other schemes too, comes an issue of time consumption as for data capturing the system requires the subject to continuously look at the sensor for a fixed duration. Any movement could blur the image e.g. Retina scans or Face recognition.

Here we apply our concept on ATM and EDC (Electronic Data Capture) machines which is also called swipe card machine which facilitates payment through debit cards.

B. The Proposal to solve Sensor-Issue

The continuous tangible contact with the sensor could degrade the sensitivity of the sensor and can increase the false-positive rate of the system. A number of customers enter the ATM to withdraw money who can present their biometric with wet, dusty, unclean or sweaty hands without any concern that it could affect the sensing plate. As a result the durability of the sensor decreases. Thus to solve this issue we define "Constraint-based Biometric scheme" in which we apply a cash-limit and a transaction limit on the ATM so that if a person willing to withdraw cash, shall only have to present his biometric If the amount entered is greater than the defined cash limit OR minimum transaction done by one on a particular day is greater than the defined limit (say 3), or both conditions is found true else can only work with their PIN. The minimum transaction (min_trans) is updated every 24 hr by banks. For balance enquiry, mini statements biometric application is not essential. If a customer enters the ATM to just withdraw a small amount like Rs.500 and the card is being used for first time (less than the defined limit), need not to wait for a long for giving biometric, a cash limit check on the machine will allow one to debit money by simple entry of PIN. Thus, saving both his and other users time. Even balance enquiry will not require biometric. So, if the fraudster enters the ATM with an intension of multiple transactions to sum it up to a large amount, it will be denied by the bank authority itself thus ensuring the security of the system.

If (amount<cash_limit) AND (min_trans< 3) biometric skipped
Else
If (amount>cash_limit) OR (min_trans> 3) biometric essential

It is also applicable to swiping machines which are now-a-days available in almost all the shopping centers. Swiping card has made customers to walk cash-free and not carry large cash in their wallet. On swiping debit card on EDC machines which reads the magnetic tape of the card and records information of the card holder and the shop including the time of transaction. This information together with the PIN is carried over a network channel and the entered cash amount is deducted from the customer's account and credited to the merchants account. Here too we can apply concept of biometrics so that no purchase can be made by fraudsters in case the card is stolen or misused, as mostly the stolen card is used for shopping as it is untraceable and no additional security feature is added on swipe machines. The customer simply enters their PIN and put their signature on the bill, which is kept for record by the merchant irrespective of whether the customer is the genuine card holder or not. By applying constraint on these devices too will be fruitful as for a purchase of few hundred biometric verification will not be required and the customers will be asked for the biometric only in case they make a purchase of huge amount i.e. greater than the defined cash-limit. Thus we can define our system as Cash-Bound biometric System. For every huge amount purchase will ask for biometric and even if one attempts to make multiple purchases of low amount will be restricted by the bank authority.

Thus, this concept of adding a cash limit to the ATM or EDC will preserve the durability and working of the sensor. The sensor will not be affected as a withdrawer will not have to present biometric for few bucks and thus saving time. It will reduce the chance of false detection or inaccuracy of system.

C. Working of the system

In our proposed system, Fingerprint verification scheme is used in the machine (ATM or EDC) preserving the advantages of existing technology added with the proposed concept solving the sensor efficiency issues.

While using the ATM equipped with biometric system, the person first enters the PIN, which is first verified and if matched is asked for option of cash withdrawal or balance statement. If balance enquiry is opted the request is fulfilled without the need of biometric. Once cash withdrawal is selected min_trans is incremented to 1(min_trans=0 initially updated at very 00:00 hour). According to the selected option the system responds i.e. if only enquiry is to be done, system does not require any biometric verification but for withdrawal, amount is to be entered. After the amount is entered, a check is conducted to determine if the amount exceeds the defined cash-limit OR min_trans> 3. If satisfied then the individual has to undergo biometric verification else if amount is below the cash-limit withdrawal AND the min_trans< 3 is allowed without undergoing biometric procedure. In case of biometric verification the individual has to present the fingerprint to the sensor. This collected characteristics sample is sent to the server to match with the stored template. If matched then the individual is authorized personnel and is permitted to dispense cash from ATM else access is denied. The min_trans counter is set to 0 at every 24 hrs to record the number of transactions made per day. The procedure is represented as under:

978-1-5090-0082-1/16/$31.00 ©2016 IEEE

Procedure:
Initial Conditions: min_trans=0 (updated at each 00:00 hr)
Cash_limit=defined

1) Read card info and PIN
2) Verify card detail and PIN
3) IF PIN not matched GOTO (10)
   Else
   Enquire for Balance Enquiry or Cash Withdrawal
   a) IF cash withdrawal proceed to (4)
   b) In case of balance enquiry GOTO (9)
4) min_trans++ //(min_trans will be updated and will be set to 0 at every 24 hr)
5) Enter amount
6) IF (amount< cash_limit) AND (min_trans< 3)
   a) GOTO (9)
   b) Else GOTO (7)
7) Enter biometric and go through biometric procedure
8) IF biometric matched
   a) GOTO (9)
   b) Else ACCESS DENIED
9) ACCESS GRANTED
10) End Transaction

D. Implementation of the Concept

Here we have implemented the concept using C code where a system time is extracted and the algorithm is being implemented. The constraint is checked after cash entry is made. Accordingly the min_trans record will be extracted from database and according to system time (i.e. 24 hour is over) will set the min_trans to 0 again. Once both conditions are found true biometric procedure will be skipped. For database related implementation the code will be included in scripting language. Fig. 1, 2, 3 represent certain cases when the cash limit is defined or balance enquiry is opted. This code will run on the system to permit or allow the skipping of biometric procedure.

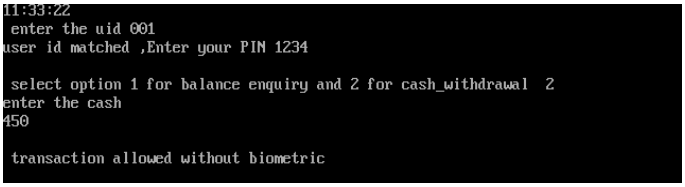

Fig.1. Case: When cash amount is less than 500

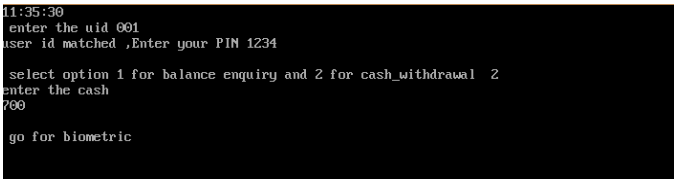

Fig.2. Case: When cash amount is greater than 500

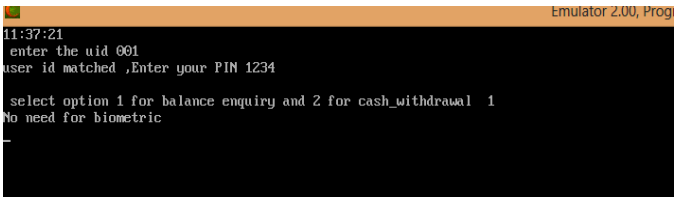

Fig.3. Case: When only balance enquiry is to be made

E. Fingerprint Verification Scheme

Once the system asks to undergo biometric procedure, the claimant need to present its fingerprint on the sensor and further verification phase starts. Fingerprint is considered to be a non-repudiated identification scheme which could not be forged [7].

a) An overview to Fingerprint Biometric Process:

Beginning with the Enrolment phase where a sample is picked up by the system. Once an enrolment is complete a template is generated. Depending upon the usage of fingerprint biometric it could be classified to Single-factor and 2-factor authentication scheme [7]. In a single factor scheme only biometric is accomplished for access permission and no PIN or password i.e. in simple words, Fingerprint serves as both Id and Password. For verification the entire database is scanned to search the matching fingerprint which is too time-consuming job. The 2-factor authentication scheme on the other hand calls for both id and Biometric. The fingerprint template is either stored in the card or token, or is attached with the user Id. During the verification once the id is entered the live fingerprint template is matched to the enrolled template attached with the entered Id.

b) Need for Accuracy:

The concept of introducing biometric is to ensure the authenticated entry to the system. It depends on factors:

1. The sample collected
2. Reliability of data collection at each scan.
3. Speed and time of collection and Verification

The performance of Fingerprint depends upon False Identification Rate (FIR) where a non-genuine entry is permitted and False Rejection Rate (FRR) where a genuine entry to system is restricted [16].While considering the speed, and while improving the time and speed factor to reduce time FRR or FIR should not increase. A little more time consumption is better than a non-authenticated entry.

c) Process: Identification and Verification

Fingerprint matching encompasses Identification and verification such that the claimant template matches the live or sample template collected by the sensor. It requires pattern matching where the features or pattern on finger is being matched [8] represented in Fig. 4.

- Ridges and Valley: The lines flowing in different patterns across the fingerprints are *ridges* and the gap between them is *valley*. Some matching scheme for identification considers these patterns size or distance between ridges.
- Minutiae Matching: Minutiae feature includes finding of the *endings* and *bifurcations*. Ending defines the terminating point of ridges and bifurcation is point where three ridges meet i.e. a Y-junction.
- Core and Delta: Core is the centre or circular pattern of the fingerprint whereas delta is the point where three patterns deviate. Sometimes these features are picked up for matching the fingerprint.

978-1-5090-0082-1/16/$31.00 ©2016 IEEE

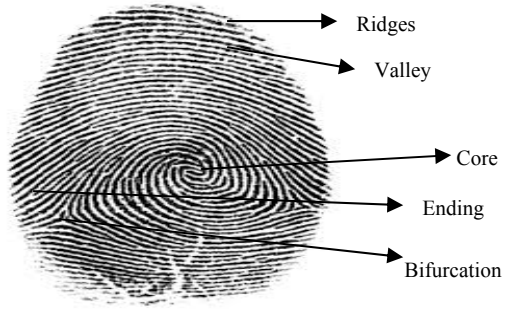

Fig.4. Features representing core, delta, ridges, valley, endings and bifurcation

d) Fingerprint processing steps:

Due to noise and sensor issues some extra minutia might be found in the image captured. This could be a spur and not necessarily a pattern. To remove this, a threshold is set such that any variation or any measurement lying below it is removed. E.g. a pattern with a small ending is skipped considering it to be scar or noise, ending found at the ending-pattern of the fingerprint is not considered, as there exists no endings at the ending ridges. The (x,y) coordinates for core, delta is marked down in template and is located. If the location is matched along with direction and pattern, the biometric is verified.

e) Factors to improve Fingerprint Biometric System accuracy to improve overall system performance:

By enhancing the accuracy of the system can also result in increasing the system performance. By bringing some modification in certain areas we can improve image processing and verification phase of biometric with increases accuracy and reduction in duration of Biometric procedure. To improve the accuracy should aim to improve Live Scan Quality and Enrolment Scan Quality [7]

1. *Increasing resolution of the scanner:* By increasing resolution of the scanner (~1000dpi) a more refined and clear quality of image can be captured. This image would be clearer with little blur or scar reducing the processing time and cleaning task making edges and boundaries more clear, highlighted and differentiable. Thus overall accuracy of biometric will increase.

2. *New Sensor technology:* Touch based sensors depends upon the measurement of figure surface. But collecting of samples of old-age people is difficult as their fingerprints are flattened with number of broken lines as well a number of physical contact could affect the sensor durability. Improper pressure while giving the fingerprint could also degrade the quality. To eliminate this issue new sensor technology is being researched based on *touch less 2-D and 3-D imaging spectral* technology [9] which scans the fingerprint pattern from below the surface of skin.

3. *Scanner placement area, measurement area and Technology:* A scanning device need to be placed such that user could correctly place it for correct image capturing. Wrong placement can give inappropriate result. Even the scanner measurement area should be enough to capture the entire fingerprint region. Smaller area cause incomplete image-capturing. Direct imaging technology must be promoted than touch-based system.

4. *Multimodal Biometric scheme by not restricting to contact-based measurement scheme:* Sometimes due to skin problems, cuts or some skin conditions fingerprint scan becomes unreliable. Hence a multimodal biometric scheme (i.e. a fusion of several biometric traits such as iris, fingerprint, etc.) can be used [10].

5. *Monitoring and Security of template:* Introducing cryptography based system will add security to the template stored as well the live template so that no future mischief could be thought of. Continuous monitoring can check sensing and capturing performance.

6. 3-D image capturing: If the sensory takes a 3-D image of the trait or feature the image would be clearer with every fine pattern capturing. Improved image quality will require less processing, reducing verification time.

f) Various schemes to reduce the matching time of fingerprint verification:

Various algorithms have been defined to reduce the matching time of fingerprint biometric. In paper [12] distance and relationship between minutia's have been taken, and stored in hash table to reduce the computation cost. The entry is made in hash table exactly once [12]. Concepts has been proposed by German et al [14] who has made use of fingerprint indexing scheme [14] in his paper with an aim to reduce the time complexity of the system by using minutiae triplet {distance between ridges, ridge count, angle between the x-axis and the ridges between two points}. But this encountered a problem where image quality affected the ridges. A modification is made by authors of [15] where the triplets are added with certain additional considerations. In [13] homographic relationship between fingerprints is considered. Barman [11] has coined the concept on Euclidean distance between minutiae points which are sorted and then stored in distance-vector. Here [11] for speeding up computation hashing and indexing of distance is used for faster matching.

Thus any of the proposed concept if, can be added with our proposed concept will improve biometric system of ATM's such that on one hand it will cut short users coming for balance enquiry and for low-cash withdrawal, whereas on other if the biometric is necessary to be furnished by using any above defined mechanism will increase computation speed reducing few more seconds.

F. Advantage of Proposed Scheme

A new concept is coined considering both the issues of existing system and benefits of the new proposed model.

a) Solving sensor issue with accuracy: The defined cash constraint will prevent all the users using ATM or EDC machines to give their biometric every time for a low cash debiting or purchase. This scheme will also prune customers who come to use ATM only for balance enquiry. The system will be less exposed to dirty hands of innumerable customers

978-1-5090-0082-1/16/$31.00 ©2016 IEEE

and sensor sensitivity will not be harmed. Hence, reducing the false positive rate and maintaining accuracy of system.

b) Durability of Sensor: This scheme will increase the durability of sensing plate as every customer need not to place their hands or palm on the sensor. The sensor will be able to collect the accurate sample for longer time.

c) Reduced time consumption and congestions outside ATM: This scheme will cut short biometric collection time of person who aim at enquiring about the balance or need only few hundred rupees. In simple words, for just debiting a small amount in the very first time or getting the mini statement one does not need to make the crowd waiting for minutes.

d) Security and Reliability: A system is preferred only if it is secure. Here security is not compromised as this constraint will maintain security and not even allow the fraudsters to make multiple small amount transactions. And in case of swiping machine (highly unsecure and untraceable), it will restrict unauthorized individual trying to use stolen ATM for purchases as cash limit will bound them to give their biometric for large amount purchase. Even a person won't lose large amount in case the ATM card is lost.

e) Easily merged with the existing system: This scheme does not require a large manipulation in the existing system. What is required is to implant a condition in the ATM or EDC to check this cash limit. A single condition checking and a more efficient biometric system obtained with no compromise in security.

VI. Conclusion and Future Scope

The sudden growth in electronic transaction and banking technology has demanded for higher level of security. Traditional methods of PIN or I-Cards can be forged or stolen and many times are too easy to be cracked as mostly these PIN are birth dates, security number, contact number or as such which can be easily guessed, but Biometric measures provide a hard-core security which neither can be stolen or forged. It provides a high level security by authentication and access permission to only genuine card holder. The proposed scheme aims at solving the sensor performance issues by limiting the users going through biometric verification and screening the customers who just want to know their balance. If the card user needs to withdraw an (amount>cash_limit) but the (min_trans< 3) or (amount<cash_limit) but (min_trans>3) need to present biometric else if (amount<cash_limit AND min_trans< 3) biometric procedure can be compromised. It also saves time together with solving sensitivity issue of input system. This model does not compromise with the security when added with ATM or EDC, preventing fraudsters to gain invalid advantages. Along with the constraint in fingerprint biometric system if we involve any of the concept [11] [12] [13] [14] will enhance performance and speed up matching result, saving time of customers and reducing biometric verification process time of the system. Many banks have already implemented concept of Biometric in their ATMs [4] now they only need to add a condition to adopt this constraint-based scheme to their system with solving issues related to fingerprint biometric system to improve the overall system performance.

This system could be more secure by adding concept of soft biometric for low cash, making biometric essential for both cases of low and high cash withdrawal. Multimode biometric [3] scheme can also be implemented to raise the security level of organization. In addition fingerprint biometric system performance can also be increased by reducing FIR and FRR. A new sensor must be designed to remove touch-based concept to solve sensor issue by capturing image from a distance.

References

[1] M. O. Onyesolu and I. M. Ezeani, "ATM security using fingerprint biometric identifer : An investigative study," International Journal of Advanced Compuer Science and Applications, vol. 3, no. 4, pp. 68–72, 2012.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, vol. 14, no. 1, pp. 4–20, January 2004.

[3] K. Archana and A.Govardhan, "Enhance the security in the ATM system with multimodal biometrics and two-tier security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 261–266, October 2013.

[4] A. T. Siddiqui, "Biometrics to control ATM scams : A study," International Conference on Circuit Power and Computing Technology ICCECT, pp. 1598–1602, 2014.

[5] F. S. Hossian, A. Nawaz, and K. Grihan, "Biometric authentication scheme for ATM banking system using energy efficient AES processor," International Journal of Information and Computer Science, vol. 2, pp. 57–63, 2013.

[6] A. Singh, S. Singh, and R. Kumar, "Secure swipe machice with help of biometric security," unpublished.

[7] Frost & Sullivan "a-best-practices-guide-to-fingerprint-biometrics.pdf." (White Paper)

[8] L. O. Gorman, "Fingerprint verification," springer, vol. 3, no. 1, pp. 43-64, 1998.

[9] A. K. Jain, H. Faulds, F. Galton, and E. Henry, "Fingerprint matching," IEEE Computer Society, pp. 36-44, 2010.

[10] A. A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multibiometrics," Springer, 2006.

[11] S. Barman, S. Chattopadhyay, D. Samanta, S. Bag, and G. Show, "An efficient fingerprint matching approach based on minutiae to minutiae distance using indexing with effectively lower time complexity," International Conference of Information Technology IEEE, pp. 179–183, 2014.

[12] U. Jayaraman, J. Viswanthan, A. K. Gupta, and P. Gupta, "Minutiae based geometric hashing for Fingerprint database," International Conference on IntelligentComputing, (ICIC -12), July 2012.

[13] R. Boro and S. D. Roy, "Fast and robust projective matching for fingerprints using geometric hashing" In Proceedings of the 4th Indian Conference on Computer Vision, Graphics and Image Processing, pp. 681-686, 2004.

[14] R. S. Germain, A. Califano, and S. Colville, "Fingerprint matching using transformation parameter clustering," IEEE Computational Science and Eng., vol. 4, no. 4, pp. 42-49, 1997.

[15] B. Bhanu and X. Tan, " Fingerprint indexing based on novel features of minutiae triplets" IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 616-622, 2003.

[16] P. Grother and E. Tabassi. "Performance of biometric quality measures." IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 531-543, 2007.

[17] P. Gnanasivam and S. Muttan, "An efficient algorithm for fingerprint preprocessing and feature extraction," Procedia Computer Science, vol. 2, no. 2009, pp. 133–142, 2010.

[18] D. A. Kumar and T. U. S. Begum, "A comparative study on fingerprint matching algorithms for EVM," vol. 1, no. 4, pp. 55–60, 2013.

978-1-5090-0082-1/16/$31.00 ©2016 IEEE