Enhanced Fingerprint Recognition with OTP using Delaunay Triangulation to Improve ATM Security

S. Vijaya Ranjini* and S. Rajarajan

School of Computing, SASTRA University, Thanjavur – 613401, Tamilnadu, India; vijayanjini113@gmail.com, srajarajan@cse.sastra.edu

Abstract

Objectives: The main objective of this paper is to develop an alternative fingerprint verification system to overcome the false rejections that occur due to the external changes on fingers such as scratches by blade or knife. Those minute deformities on the finger might deny access to the authorized users. Methods: “Delaunay triangulation-based matching” method is proposed in this work in order to avoid the authentication error caused by inaccurate enrollments and sending OTP to ensure maximum security in authentication. This triangulation method provides seamless access for the authorized users at ATMs even with altered fingerprints and also it improves the security. Findings: This technique is implemented by forming the triangle, make the reference point at the center and then it is used for the matching. If the difference is less than the predetermined threshold value, it approves the authentication. It otherwise rejects user’s authentication. So this proposed method will be useful for authorized users when their fingerprints are wounded or slightly cracked which will be usually rejected in existing methods. Applications/Improvements: Delaunay triangulation-based matching method can be effectively used in applications of banking like ATMs, E-banking, and POS counters etc.

Keywords: ATM, Authentication, Biometric System, Delaunay Triangulation, Dots Minutiae, Extracting and Matching, Fingerprints, Password

1. Introduction

In comparison to the existing knowledge based authentication methods, bio-metric schemes offer better precision, user convenience and cost effectiveness. The knowledge based authentication schemes are attacked quite easily. But the bio-metric schemes are much harder to break and are more reliable to authenticate users are highly sensitive environments. Biometric systems accumulate evidence (e.g., face, fingerprint, and iris) in order to recognize a person. Hence, fingerprint based biometric authentication recognizes users in a guaranteed manner such that it alleviates user inconvenience, reduces cost of managing the security and offers user-specific provisioning. More and more organizations are moving towards biometric authentication for their employees and customers given its advantages over non-biometric schemes. A fingerprint is unique—and copies can be detected and prevented. The fingerprint can be used as both the user ID and the password. So the combination of both passwords with fingerprint bio-metric system will enhance security. The system will provide output as a matching if according to a pre-defined similarity measure; a query is similar to the template means matched or a mismatch if it is not similar. Since biometric templates are stored and retrieved from the organization's databases residing in the servers, it is relatively easier to recover them during the occasions when they are attacked without the loss of time. But when the biometric data is exposed and it's confidentiality is lost then it is very difficult to overcome that loss. Since biometric data are physical they can not be replaced by new data like a password or PIN. The loss is a more permanent loss. Another complication with bio-metric compromise is that since the same information is likely to have been used on different systems for authentication of the same users, the compromise in biometric is likely
to result in more widespread damage. The proposed scheme combines the biometric and password schemes to present a stronger authentication that is relatively stronger against attacks. Experimental results show that both the biometric system and the password scheme proposed in this paper offer superior security compared to their rudimentary biometric based counterparts. These components are synchronized in the Multi biometric concepts altered fingerprint technique. This technique performs the Delaunay Triangulation with dots minutiae. The fingerprint image, the dots are selected from the scanned image. The dots are formed into triangle and process can synchronize from biometric to biometric process. Many methods have been proposed for biometric template protection with some advantages and limitations where the main objective is to keep: 1. Revocability - when two or more templates are extracted from the same source of biometric features it should be computationally harder to establish that they both are hailing to the same biometric seed, and 2. Non-inevitability – given a biometric template, it must be computationally challenging to detect a feature which will match with the given template.

The paper\(^1\) has proposed a scheme that offers the security benefits of Biometric Encryption along with different uses of biometrics. The most purpose is that BE technology can facilitate to beat the prevailing “zero-sum” mentality, namely, that adding privacy to identification and data of systems can essentially weaken security and functionality. In this paper\(^2\), the authors tend to take a “fusion” of a minutiae-based fingerprint authentication theme associated and an SVD-based face authentication theme, and show that by using a recently planned cryptographically primitive known as “secure sketch”, and a notable geometric transformation on trivia, thus it will create it easier to mix completely different modalities at a time associated to create impracticable to forge an “original” combination of fingerprint and face image that passes the authentication. The paper\(^4\) suggests a multimodal biometric scheme that has several advantages over single modal biometric systems. It provides better recognition accuracy. The multimodal biometric system creates two common biometrics statistics, face and fingerprint by employing real multimodal information and two unreal multimodal databases. Through the experimental results it was identified that there is a significant difference between the system performances obtained with the real and unreal multi-modal databases. The Paper\(^4\) shows that three levels of data regarding the knowledge of parent fingerprint are often extracted from the minutiae or trivia template alone. The orientation-estimation algorithm controls the direction of native ridges using the tiny triplets. In paper\(^3\) fingerprint recognition is aided by minutiae matching. The system\(^3\) is made up of fingerprint improvement and quality control. It employs a new matching algorithm for fingerprint feature extraction. Embedded systems comprising of small sensors are used\(^5\). A system\(^6\) was designed with low cost fingerprint recognition that maintains the constant rate of classic solutions for identification along with best response time perceived at user side strictly supported by binary operations. The development of architecture is designed in order to lighten the computational for the expensive data redundancy within the database\(^7\). This new system shows associated 97% greater than user identification rate with improved performance and reduced price because of cheap scalable FPGA device without losing response time. The research of\(^8\) has planned a fingerprint recognition approach by confined strong features extraction and matching ways. First the confined features are extracted using Speeded-Up Robust Feature (SURF) algorithm and then the test fingerprint image are compared against two or more exiting template image features for matching purpose by using a matching threshold value. Two features match when the distance between them is smaller than the matching threshold and also eliminates ambiguous matches when difference is higher than the matching threshold. Finally it calculates the similarity matching score and takes the choice on matching. It is scalable and rotation invariant system shows better recognition accuracy and efficiency in presence of rotation, scaling and partial distortion of the test image\(^9\). There is a new technique\(^{10}\) developed which utilizes finger print recognition along with password entry. As it utilizes two forms of authentication together, it drastically improves the security of authentication. The scheme of\(^{10}\) is aimed at ensuring successful authentication of card holders at ATMs. Typically most ATMs across the world utilize ATM cards with magnetic stripe which is to be inserted at the swiping machine\(^{11}\). Normally the ATM cards contain a chip which is imbibed with the secret information to recognize the actual user. It is usually a four digit number called the PIN\(^{12}\). Loss of cards is another big problem along with the password getting stolen. That will bring enormous financial loss to the customer\(^{13}\). So to rectify these problems, an authentication system and algorithm based on fingerprint image is
proposed in order to improve the authentication of customers using ATM machines.

2. Enhanced Fingerprint Recognition using Delaunay Triangulation for ATM

Fingerprint images that are scanned by the fingerprint scanner which is not a optimum quality. So we remove noises and enhance the quality of images. We extract features like minutiae and Delaunay triangulation method for matching the fingerprint is stored in the database or in the scanner. If the sets of minutiae are matched with those in the database, then the fingerprint of user is identified and verified which allow authentication, if the fingerprint is not matched with database then the unauthorized tried to access the authorized user account so the buzzer/alarm will alert. If the fingerprint is matching, after matching we perform post-matching steps and perform matching fingerprint process. It also provide alternative fingerprint when difference between the matching fingerprint is less than 5% because of external damage then it allow the authorized user to access the authentication. This technique is done by using Delaunay triangulation method which will form the triangle and make the reference point at the center and then it is used for matching if the difference is less then it allow the authentication otherwise it will reject the authentication. So this proposed method will improve the security and also useful for authorized user when the fingerprint is damaged or slightly cracked which will be rejected in previous existing method.

Figure 1 shows Finger print sensor consists of Arm processor circuit, memory and sensor. The fingerprint sensor is interfaced with PC and AT mega 328 microcontroller. The sensor memory consists of cells. The memory cells may have hundred or thousand user entries depends upon the sensor requirement of the applications. Each fingerprint is allocated with ID number which is used to store randomly in the system. While every time user try to access the permission the fingerprint is verified with the stored images and then do the proper operation for authentication.

2.1 Enrolment Mode

In entry mode the sensor is interfaced with PC. In PC we have written software which helps the users entries stored in the sensor memory cells along with respective ID numbers.

2.2 Verification Mode

In the verification mode the sensor is interfaced with microcontroller. In order to verify the finger we have to place the finger on the sensor and press the button. The microcontroller sends the protocol to the Arm processor circuit. Now the sensor is activated and senses the finger print which is compared with stored entries in the memory. If the sensing finger print is matched, the arm processors circuit sends the corresponding person ID number to the microcontroller. The microcontroller displays the received ID number on the LCD display.

2.3 Perform Matching

If comparison operation is not properly done, the microcontroller is displays the “Result is not in Time” on the LCD display. If the sensing finger print is not valid with stored entries then the micro-controller displays the “Authentication Fail” on the LCD display and raise the buzzer. If the sensed fingerprint image is matched with the stored image then it displays the “Authentication is Successful” and then it sends the random OTP number to the valid user mobile number. If the correct OTP password is typed, then it allow the transaction in ATM, otherwise it does not allow the transaction because of the wrong OTP password and also raise alarm.

2.4 Delete Mode

If the user need to delete their account then delete mode is used to delete the current user account by using Delete user Id option. Otherwise if the administrator needs to delete all user account and to create a new account for
all then delete all user mode is used by using Delete all user_Id option. This option is only available for management and security system in order to provide security.

2.5 Delaunay Triangulation

Delaunay triangulations are being employed in computing applications. Though there are several algorithms for constructing triangulations, this method is preferred since it posses geometric properties of the Delaunay triangulation. Delaunay Triangulation is made by appending 0 or more edges to the Delaunay Graph. The Delaunay algorithm has been employed to build a triangulation from a unique set of points. If the points applied to the triangulation then it reveals the duplicate locations and the duplicate point is ignored. It generates a triangulation with reference point in the center of the original input and detects the duplicate. A Delaunay triangulation DT (P) is one that has no point in P is inside the circumference of DT (P). There exists a unique Delaunay triangulation for P if P is a set of points in general position. Once a new triangle is constructed, then the record of base edge in the hull is to be removed as shown in Figure 2. Correspondingly two new edges linking to the current reference point to each vertex of the base edge are created, and then each new edge is to be checked whether its reversed edge already exists in the hull; if true, the reversed edge is removed, otherwise, the new edge is inserted into the hull. As all hull edges are saved in the linked list sequentially and circularly, the above checking of reversing edges can be performed directly; only the precursor or next link of the base edge need be checked. Thus each newly added edges will be checked with the current reference point in the hull or triangle. The main Advantages of Delaunay triangulation is High Resolution and Precise Location.

3. Experimental Results

The proposed method is evaluated by using fingerprints matching using Delaunay triangulation procedure. Minutiae dots are extracted from each image in the databases so that the similarity between those images is determined. The snapshot of similarity matching between original image and stored image in MATLAB with minutiae dots is shown in Figure 3. Figure 4 shows the similarity score between two images in MATLAB. The above Figure 5 shows ROC curve for fingerprint that stored in database. False Acceptance Rate (FAR) and False Rejection Rate (FRR) were used as performance measures in our experiments. In the Experimental results shows, FRR is reduced by using our proposed system and additionally increase the strength to improve FAR.
Figure 5. ROC curves for FVC2002 DB1, DB2 and DB3.

Figure 6 shows the experimental hardware output where Arduino is connected with LCD display, Fingerprint scanner, Buzzer, GSM module and Keypad for controlling the action to be done. The Fingerprint scanner scans the fingerprint and verified with stored images and then the decision is displayed in LCD, if matched then GSM module sends OTP number to user mobile. Then the password is typed using keypad. If password is correct authentication is successful message is displayed in LCD.

4. Conclusion

Biometric security systems play major role in the banking systems. This paper addressed the issue of authentication failures that arise due to minor deviations between stored and received fingerprint value. Thus the proposed work is a method with single biometric based on fingerprint with OTP which improves the security with higher precision for ATM transactions. The altered fingerprint is provided by Delaunay triangulation method such that the users who have cracks can also access their accounts and it also avoids fraudulent users to breach the authentication with the help of OTP. In future this system may also be enhanced by using two or three different fingerprints of the same person that are stored for a single user account so that even if wounds or changes happen in one finger, the user may still be authenticated with the help of other fingers. In future this scheme may be further enhanced by encompassing multiple fingerprint prints of the same person so that more severe damages and changes to the fingers could be handled effectively.

5. Acknowledgement

The authors owe their gratitude to the Department of Science & Technology, New Delhi, India (Project ID: SR/FST/ETI/-371/2014). They are also thankful to the SASTRA University, Thanjavur, India for extending the infrastructural support to carry out the research work.

6. Reference

1. Ann Cavoukian, Alex Stoianov. A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, Information and Privacy Commissioner of Ontario. Toronto, 2007.
2. Yagiz Sutcu, Qiming Li, Nasir Memon. Secure Biometric Templates from Fingerprint-Face Features, Computer Vision and Pattern Recognition. IEEE Conference on Computer Vision and Pattern Recognition; 2007 Jun. p. 1–6.
3. Wencheng Yang, Jiankun Hu, Song Wang, Chi Chen. Mutual Dependency of Features in Multimodal Biometric Systems, Electronics Letters. 2015; 51(3):234–35.
4. Ross A, Shah J, Jain AK. From Template to Image: Reconstructing Fingerprints from Minutiae Points, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007; 29(4):544–60.
5. Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, Parvinder S. Sandhu. Fingerprint Verification System using Minutiae Extraction Technique, International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2008; 2(10):3405–10.
6. Yuan W, Lixiu Y, Fuqiang Z. August. A Real Time Fingerprint Recognition System based on Novel Fingerprint Matching Strategy. Electronic Measurement and Instruments, 2007. ICEMI’07. IEEE 8th International Conference; 2007. 1–81.
7. Fronthaler H, Kollreider K, Bigun J, Fierrez J, Alonso-Fernandez F, Ortega-Garcia J, Gonzalez-Rodriguez J.
Enhanced Fingerprint Recognition with OTP using Delaunay Triangulation to Improve ATM Security

Fingerprint Image-Quality Estimation and its Application to Multi-algorithm Verification, IEEE Transactions on Information Forensics and Security. 2008 Jun; 3(2):331–38.
8. A New Low Cost Fingerprint Recognition System on FPGA. http://iesolution.in/product_extra_files/06505806.pdf.02/2013.
9. Hany U, Akter L. Speeded-Up Robust Feature Extraction and Matching for Fingerprint Recognition. In: Electrical Engineering and Information Communication Technology (ICEEICT), IEEE International Conference; 2015 May 21. p. 1–7.
10. Priya R. Tamilselvi V, Rameshkumar GP. Novel Algorithm for Secure Internet Banking with Finger Print Recognition, International Conference on Embedded Systems - (ICES 2014); 978-1-4799-5026-3/14©2014 IEEE.
11. John Mashurano, Wang Liqiang. ATM Systems Authentication based on Fingerprint using ARM Cortex-M3, International Journal of Engineering Research and Technology (IJERT). 2013 Mar; 1–6.
12. Annu Saini. Image Enhancement Techniques for Fingerprint Images, International Journal of Emerging Trends and Technology in Computer Science. 2012 Sep-Oct; 1(3):215–17.
13. Pennam Krishnamurthy, Maddhusudhan Reddy M. Implementation of ATM Security by Using Fingerprint Recognition and GSM, International Journal of Electronics Communication and Computer Engineering. 2012; 3(1):1–4.
14. Khatmode Ranjit P. Arm7 Based Smart ATM Access and Security System Using Fingerprint Recognition and GSM Technology, International Journal of Emerging Technology and Advance Engineering. 2014 Feb; 4(2):856–60.
15. Lee C, Kim J. Cancelable Fingerprint Templates using Minutiae-based Bit Strings, Journal of Network and Computer Applications. 2010 May; 33(3):236–46.
16. Chaudhari NM, Pawar BV. Experimental Analysis of Fingerprint Techniques: Variance and ROC, Indian Journal of Science and Technology. 2010 May; 3(5):598–601.
17. Khanaa V, Krishna Mohanta. ATM Terminal Design using Biological Technology, Indian Journal of Science and Technology. 2013 Jun; 6(S6):1–4.