Secure Mechanism for Credit/Debit Card Transaction Fraud Detection by using Fingerprint Authentication System

Priyanka A. Jamdar, Supriya K. Bendale, Deepali A. Durgawale

Computer Department Siddhant College Of Engg Maval, Pune-409

Summary
As credit card is becoming more efficient for online financial transaction, at the same time fraud associated with it is also increasing. This method is to increase the security level of the society against the fraudsters. This paper is totally concerned with the feature of fingerprint authentication which makes the transaction more secure as compared to the traditional Credit/Debit card payment. Here we are going to implement fingerprint biometric authentication for identifying and verifying person. The fingerprint biometric authentication is used to authenticate the original user so that the unauthorized person should not be able to perform the transaction. If any suspicious transaction will occurred then proposed system blocked the current transaction and will notify the valid user on respective available information.

Key words:
Credit/Debit card fraud detection and Security, Threshold transaction, fingerprint biometric authentication.

1. Introduction

With article guides a stepwise walkthrough by Experts for the great increase in credit and debit cards, ATM CARDS & E- transactions, frauds are also increasing excessively in recent years. The credit and debit cards are the most popular mode for online payment. Increase in the use of the internet for online shopping has result a considerable proliferation of credit/debit card transactions throughout the world. Credit/Debit card frauds employ large number of techniques to commit fraud. As per as the literature survey & study of paper in the field of Artificial Intelligence, Genetic algorithm, Neural network they have been analyzed & observed that the technologies are meant for fraud detection. But the use of online shopping has increased rapidly in last few years with some limitations. There are many ways for authentication such as-Multi level password authentications, hard codes, Session Passwords, and encrypted One Time Password. Every method has some advantages and disadvantages. Our main approach is to increase the security in the field of E-commerce, E-banking & ATM. The main intention of frauds is to damage another individual or for personal Gain. Here we will discuss about overcome the security level. Credit/Debit Card Fraud is defined as, when an individual uses another individuals‘ credit card for personal use while the owner of the card as well as the card issuer are unaware about the activity performed by the fraud with the help of card. In this study we are more concern to increase the security level and will particularly focus on detecting fraudulent credit card transactions.

2. Overview of Fraud Detection System

The 2-factor authentication (Password, OTP) for Credit card transaction gives high level security but there are some limitations involved. To overcome these limitations our system is introduced. This paper introduces a novel technique to secure our credit/debit card towards fraudsters with the help of biometric authentication. As fingerprint authentication is the strongest amongst all other Tradition authentication system, we are going to introduced same for authentication in our proposed system. In biometrics, Tradition authentication will provide some level of security to each transaction but in this paper we have added one more addition factor to provide the better security to Credit/Debit card transaction by adding fingerprint authentication. The sample fingerprint templates will store in banking database for each card holder customer at the time of registration of Credit/Debit card and this phase is known as training phase for fingerprint authentication. The additional information for notification of fraud is also stored in the database of respective bank such email address or contact number (Mobile etc).
When user perform any transaction by using Credit/Debit card then after performing all the traditional steps fingerprint authentication phase will introduced in which user must enroll their fingerprint with particular fingerprint scanner device which known as Authentication Phase of user fingerprints. In authentication phase user has consecutive three chances to enroll their fingerprints, if any one sample is get matched with the fingerprints which is taken at training phase then transactions is completed without any disturbance else no any matched found with previously stored fingerprints then our system will stored the suspicious fingerprint as proof of fraud with the other information such as IP address of fraud detected machine and immediately notify the valid user and bank for the same. In this way we are able to detect

Manuscript received March 5, 2016
Manuscript revised March 20, 2016

the fraud in our proposed system with the help of fingerprint recognition system.

The Minutiae-Based Matching Algorithms in Fingerprint Recognition system is used for fingerprint authentication. Minutiae matching algorithm is the most popular approach to fingerprint identification and fingerprint verification. Minutiae based fingerprint recognition consists of Thinning, Minutiae extraction, Minutiae matching and Computing matching score. Fingerprints are mostly used in biometrics technique for personal identification. They are widely used due to their feasibility, distinctiveness, accuracy, reliability and acceptability. When a card is copied or stolen or lost and captured by fraudsters it is usually used until its available limit is depleted.
In the figure1, it shows how fingerprint authentication is accomplished in Credit/Debit card transaction system. We are going to implement this concept with the help of dummy merchant website which stores the some dummy products. The process of making transactions will going to keep as same as present in existing real time system. First the user has to provide the necessary information which is used to make transaction with Credit/Debit card in banking database. Addition to that he/she also need to store the 3 valid fingerprint sample for further authentication. When user going to perform any transaction on merchant website then he/she fulfil all the respective steps to complete their transaction in traditional way like by using OTP password or PIN number will be verified for first level of authentication and then the second level of authentication will be occur as fingerprint authentication. Once the user gets authenticated he/she will be able to complete their transaction otherwise notification will send to respective user via email or SMS with the help of respective contact information stored at banking database.

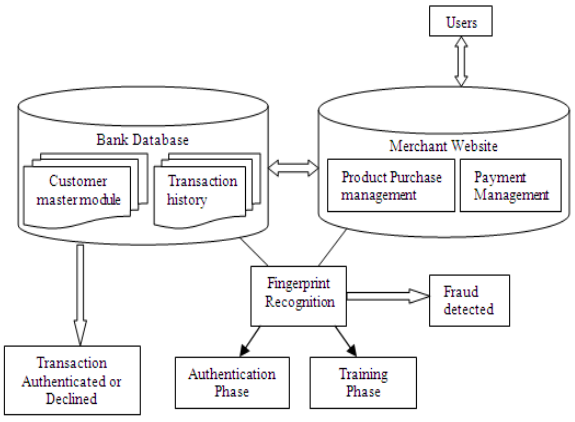

Figure 1: System Architecture

3. Minutiae Matching Algorithm

Based on an information theory approach, The popular Biometric used to authenticate a person is Fingerprint which is unique and permanent throughout a person's life. Biometric systems operate on behavioral and physiological biometric data to identify a person. The behavioral biometric parameters are signature, gait, speech and keystroke, these parameters change with age and environment. However physiological characteristics such as face, fingerprint, palm print and iris remains unchanged throughout the life time of a person. The biometric system operates as verification mode or identification mode depending on the requirement of an application. The verification mode validates a person's identity by comparing captured biometric data with readymade template. The identification mode recognizes a person's identity by performing matches against multiple fingerprint biometric templates. Fingerprints are widely used in daily life for more than 100 years due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. Fingerprint is a pattern of ridges, furrows and minutiae, which are extracted using inked impression on a paper or sensors.
The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae. A minutia matching is widely used for fingerprint recognition and can be classified as ridge ending and ridge bifurcation. More complex fingerprint features can be expressed as a combination of these two basic features. So for Fingerprint Recognition we are using Minutia Score Matching method (FRMSM). For Fingerprint thinning, the Block Filter is used, which scans the image at the boundary to preserves the quality of the image and extract the minutiae from the thinned image. The false matching ratio is better compared to the existing algorithm. Minutiae matching essentially consist of finding the best alignment between the template (set of minutiae in the database) and a subset of minutiae in the input fingerprint, through a geometric transformation. Minutia based fingerprint recognition consists of Thinning, Minutiae extraction, Minutiae matching and Computing matching score.

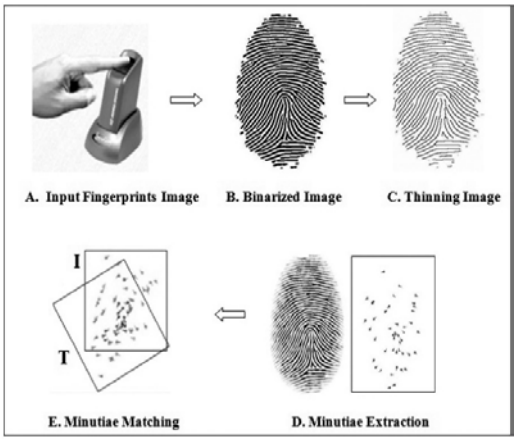

Figure 2: Block Diagram Of Fingerprint Recognition using Minutiae Score Matching method

3.1 Fingerprint Image

The input image taken for authentication is converted into a gray scale image of a person. The intensity values of input fingerprint ranging from 0 to 255. In a fingerprint image, the dark lines are ridges and valleys are the light area between the ridges. A ridge can either come to an end, which is called as termination or it can divided into two ridges, which is called as bifurcation. The terminations and bifurcations is a two type of minutiae which is more suitable for further processing compared to other features of a fingerprint image.

3.2 Binarization

The pre-processing of FRMSM uses Binarization by fixing the threshold value to convert gray scale image that is input fingerprint image into binary image. The original fingerprint image and the output image after Binarization are shown in the Figure 3.

Figure 3: Original image and binarized image

3.3 Block Filter

In Block Filtering process convert the binarization image into the thinning image as a output to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. As compare to the original fingerprint thinning does not change the location and orientation of minutiae points. This two processes which are used for thinning the ridges that is dilation and erosion. A binarized Fingerprint and the image after thinning are shown in Figure 4.

Figure 4: Binarized image and thinning image

3.4 Minutiae Extraction

After completing the block filtering process, We have to extract the minutiae points that are bifurcation or ridge ending by using the minutiae extraction. The terminations position lie at the outer boundaries which are not considered as minutiae points. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels. If crossing Number is 1, 2 and 3 or greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively, is shown in figure 5. It shows the original image and the extracted minutiae points image. which is shows the position of termination and position of bifurcation.

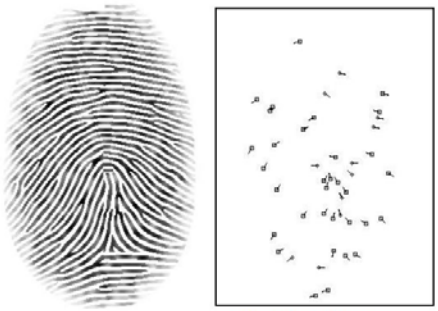

Figure 5: Grey scale fingerprint and extracted minutiae points

3.5 Minutiae Matching

In Minutiae matching we compare the input fingerprint with the template fingerprint which is store in database. The extracted data is stored in the matrix format for the efficient processing. 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.

The process of matching fingerprint each input minutiae point is compared with template minutiae point and then finds the matching score. The matching score of two images is computed, if matching score is 1 image is matched otherwise it is mismatched.

Figure 6: Cancellable Fingerprint

If input fingerprint is mismatched with template fingerprint then the fraud is occur then detect it using IP address of that device and it will be stored in database with the invalid fingerprint which may be used as evidence of fraud. With the help of this evidence we can detect the fraud person.
The motivation behind the work is growing need to identify a original person for security. The fingerprint is one of the popular biometric methods used to authenticate human being. The proposed fingerprint verification FRMSM provides reliable and better performance than the existing technique.

4. Conclusions

The main focus of this paper is the detection of fraudsters in Credit/Debit card applications and by implementing a novel mechanism which helps in performing a secure transaction. It has documented the development and evaluation in Credit/Debit card application fraud detection system. In our system the implemented feature extraction algorithm is accurate and fast in minutiae extraction. Experimental results show that our proposed system performs very well in a real operational environment.
We are going to provide a high level security for online transactions using authentication system. The proposed system will secure our society from frauds.

Acknowledgement

We take this humble opportunity to express my deep sense of gratitude to my project guide Prof. Shyam Gupta, who in all respect helped us tangibly from the beginning till the fulfilment of this paper. His expert guidance and inspiration brought completion of the paper.
We would like to thank Prof. Kumbharkar P.B, Head of Computer Engineering Department, who gives me this opportunity. I would also like to thank to all my teachers and those who directly or indirectly supports time to time.
Last but not least I would like to express a deep sense of gratitude from the bottom of heart to my parents, without whom it was impossible for me to reach at this stage.

References

[1] ALKA HERENJ, SUSHMITA MISHRA, "Secure Mechanism for credit card transaction fraud detection system" issue 2, February 2013.
[2] KOICHI ITO, AYOMI MORITA, TAKAFUMI AOKI, HIROSHI NAKAJIMA, "A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching-2012".
[3] RAVI. J, K. B. RAJA, VENUGOPAL. K. R., "Fingerprint Recognition Using Minutia Score Matching", International Journal of Engineering Science and Technology Vol.1(2), 2009, 35-42
[4] CLIFTON PHUA, KATE SMITH-MILES, VINCENT CHENG-SIONG LEE AND ROSS GAYLER, "Resilient Identity Crime Detection", IEEE Transactions on Knowledge and Data Engineering, vol.2, no. 3,pp.533-546, 2012.
[5] 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).
[6] PRATEEK VERMA ,YOGESH BAHENDWAR, AMRITA SAHU, MAHEEDHAR DUBEY "Feature Extraction Algorithm of Fingerprint Recognition "Volume 2, Issue 10, October 2012
[7] CLIFTON PHUA, KATE SMITH-MILES, VINCENT CHENG-SIONG LEE AND ROSS GAYLER, "Resilient Identity Crime Detection", IEEE Transactions on Knowledge and Data Engineering, vol.2, no. 3,pp.533-546, 2012.
[8] 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).