International Journal of Information Technology and Knowledge Management
January June 2009, Volume 2, No. 1, pp. 173-175

A NOVEL METHOD TO PROVIDE THREE LEVELS SECURITY FOR THE CREDIT CARD SYSTEM

Pavani. T.[*], O. Rama Devi[*] & C. Naga Raju[*]

In this paper a novel method is proposed to provide three levels Security for Credit Card System. At the first level it verifies magnetic stripe reader which is provided for Credit Card, at second level it verifies PIN and at third level it verifies biometrics. In the current Credit Card system a fundamental weakness is that banks use to keep Credit Card PIN codes secret while they are transported across bank networks causes that could undermine the entire credit card system. In the current system a two level security is provided. At the first level it verifies magnetic stripe reader which is provided for Credit Card, at second level it verifies PIN. A hacker could siphon off thousands of PIN codes and compromise hundreds of banks, could then print phony debit cards and simultaneously withdraw vast amounts of cash using ATMs around the world. To overcome this drawback here I am proposing a novel method to provide more security for Credit Card system by combining the present system with biometric system. This novel method has been tested on several samples and results have been placed in the form of table. This method provides better security over the traditional systems.

Keywords: ATM, Biometrics, PIN, Edge-flow, Mode and Correlation

1. Introduction

The software designed will control a simulated automated teller machine (ATM) having a magnetic stripe reader for reading an credit card, a keyboard and display for interaction with the customer, a slot for depositing envelopes, a dispenser for cash, printer for printing customer receipts, and a key-operated switch to allow an operator to start or stop the machine[1]. The ATM will communicate with the bank's computer over an appropriate communication link ATM will service one customer at a time. A customer will be required to insert a credit card and enter a personal identification number (PIN) both of which will be sent to the bank for validation as part of each transaction, will display an explanation of the problem, and will then ask the customer whether he/she wants to do another transaction. The main problem with ATM system is if the credit card is hacked by some one then Hackers may broke into the ATM network through a server at a third-party processor, which means they probably didn't have to touch the ATMs at all to pull off the heist[3]. They could have gained administrative access to the machines which means they had carte blanche to grab information through a flaw in the network or by figuring out those computers' passwords [3]. Or it's possible they installed a piece of malicious software on a banking server to capture unencrypted PINs as they passed through. Consumers should watch their accounts for any signs of suspicious activity, but other than that there isn't much they can do in response to this research.

[*] Department of C. S. E., K L College of Engineering, Andhra Pradesh, INDIA, *E-mail: pavani_cse@klce.ac.in, odugu_rama@yahoo.co.in, Cnrcse@yahoo.com*

In this paper a novel method is proposed to provide more security by applying biometrics. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern [4,5]. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns [6]. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

2. Proposed Method

The Proposed method contain the following steps

Step 1: verify the magnetic stripe reader

Step 2: Enter PIN code for the verification

Step 3: Acquire finger prints during touch screen process. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template which is stored and used for matching.

Step 4: The image acquired from the fingerprint sensor often results in poor quality. To overcome these problems image enhancement process is necessary for accurate of the parameters. The goal of the image enhancement process is to make the non-continuous ridges and valleys of the fingerprint continuous, highly interesting foreground

extraction from the noisy and irrelevant background. Mode filter has been used for noise elimination.

Step 5: In the feature extraction the major features of fingerprint are Minutia points, ridges, ridge endings, bifurcations, and short ridges are extracted. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. To extract these features a novel edge flow technique is used.

Step 6: Pattern based algorithms compare the basic fingerprint patterns like arch, whorl, and loop between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. Correlation matching algorithm is used to compare previously stored templates of fingerprints against candidate fingerprints for authentication. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared. In this paper features like ridge ending, bifurcation, and short ridge are compared.

3. EXPERIMENTAL RESULTS

Figure 1: Original Finger Print

Figure 2: Canny Edge Detection

Figure 3: Type 1

Figure 4: Canny Edge Detection

Figure 5: Correlation Matching

Figure 6: Type 2

Figure 7: Canny Edge Detection

Figure 8: Correlation Matching

Figure 9: Type 3

Figure 10: Canny Edge Detection

Figure 11 Correlation Matching

Table 1

Image 1	*Image2*	*Correlation matching*	*Matching Percent*
Original Finger Print	Type 1	1	100%
Original Finger Print	Type 2	0.0468073	10%
Original Finger Print	Type 3	0.092539	19%

4. CONCLUSIONS

As in the credit card system security is rapidly deployed, the security in the present environment will be mandatory. There exist various levels and various types of security. Here, we deal with the type of the Security called biometrics, which is the rising threat of attacks to the credit card system services. One of the biggest difficulties in defending against this type of attack is that attackers always use spoofed to disguise their true origin. Here a novel method is proposed to provide three levels Security for Credit Card system. At the first level it verifies magnetic stripe reader which is provided for Credit Card, at second level it verifies PIN and at third level it verifies biometrics. This helps in providing more security to the credit card system by using biometrics. This novel method has been tested on several samples and results have been placed in the form of table. This method provides better security over the traditional systems. How ever this method may not provide 100% of security because of finger prints acquisition difficulties. The future extends to this paper are digital water marking methods which will provide robust security to the credit card system.

References

[1] Jain, L. C. *et al.* (Eds.). 1999. "Intelligent Biometric Techniques in Fingerprint and Face Recognition.'' Boca Raton, FL: CRC Press.

[2] Johnson, B. (2005, August 29), Lecture Presented in Electrical and Computer Engineering 586, University of Virginia, Charlottesville, VA. Retrieved December 13, 2005 from *https://toolkit.itc.virginia.edu/cgi-local/tk/UVa_SEAS_2005_Fall_ECE586-1/displaymaterials:LectureSlides+Lecture-2.ppt/SESSION:113453174811608:44402702625757/Lecture-2.ppt*

[3] Johnson, B. (2005, August 31), Lecture Presented in Electrical and Computer Engineering 586, University of Virginia, Charlottesville, VA. Retrieved December 13, 2005 from *https://toolkit.itc.virginia.edu/cgi-local/tk/UVa_SEAS_2005_Fall_ECE586-1/displaymaterials:LectureSlides+Lecture-4.ppt/SESSION:113453174811608:44402702625757/Lecture-4.ppt*

[4] Johnson, B. (2005, September 12), Lecture Presented in Electrical and Computer Engineering 586, University of Virginia, Charlottesville, VA. Retrieved December 13, 2005 from *https://toolkit.itc.virginia.edu/cgi-local/tk/UVa_SEAS_2005_Fall_ECE586-1/displaymaterials:LectureSlides+Lecture-5.ppt/SESSION:113453174811608:44402702625757/Lecture-5.ppt*

[5] Minutia vs. Pattern Based Fingerprint Templates. (2003). Retrieved December 13, 2005, from *http://www.ibia.org/membersadmin/whitepapers/pdf/9/M_vs_P_White%20Paper_v2.pdf*

[6] Setlak, D.R. "Advances in Biometric Fingerprint Technology are Driving Rapid Adoption in Consumer Marketplace." Retrieved December 13, 2005 from *http://www.authentec.com/getpage.cfm?sectionID=43*

http://www.authentec.com/getpage.cfm?sectionID=43

http://redtape.msnbc.com/2006/11/researchers_who.html