Research Inventy: International Journal Of Engineering And Science
Vol.2, Issue 9(April 2013), Pp 44-50
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Credit Card Duplication and Crime Prevention Using Biometrics

[1,]Prithika.M , [2,]P.Rajalakshmi
[1,2,]*Computer Science and Engineering, R.M.K. Engineering College,*
Chennai, Tamil Nadu, India.

Abstract *– A phenomenal growth in the number of credit card transactions, especially for on-line purchases, has also led to a substantial rise in fraudulent activities. Credit card fraudulent transactions are very easy to conduct, while very difficult to recover, compared to the fraud cases in hard-products transactions. In real life, fraudulent transactions could be interspersed with genuine transactions and simple pattern matching techniques are not often sufficient to detect the fraudulent transactions efficiently. Moreover, surrogate representations of identity can be easily forgotten, lost, guessed, stolen, or shared. Further it can be hacked through malicious websites or prone to security breaches. Implementation of efficient fraud detection systems has thus become imperative for all credit card companies in order to minimize their losses.In this paper, we propose a IRPV (Iris Recognition and Palm Vein) recognition technology which will help add even more security to existing biometric devices that may be susceptible to fraud. The techniques used are Palm vein technology, along with iris recognition. It is difficult to crack, because each person's vein pattern is unique. Thus, biometric systems impart higher levels of security when appropriately integrated into applications requiring user authentication. The experimental results show that the detection rate would prove 99.995% compared to traditional methods.*

Keywords *- Biometrics, Credit Card Fraud, ICP Algorithm, Iris Recognition, Palm Vein technology.*

I. INTRODUCTION

Plastic money is the technology that enables customers to access banking and financial services through the use of their credit/debit. Since the need for banking has greatly increased over the past few years, banks and financial institutions allow customers to withdraw, transfer and deposit money using cards. Although plastic money may offer benefits, there are risks involved. Card transaction like other types of traditional and online banking systems, is susceptible to security breaches. Accessing financial services through credit/debit cards may result in sensitive financial data falling into wrong hands. Also other risks include loss of a customer's cards or theft of valuable PIN information. Credit card fraud detection [1] has drawn a lot of research interest and a number of techniques, with special emphasis on data mining. Credit card fraud can be defined as "Unauthorized access of credit card by a person for his own use. The person using the card does not have any connection with the cardholder or issuer. Credit card fraud can happen in a variety of ways, from low tech diving to high tech hacking. To overcome the limitations mentioned above, in this paper we have proposed an idea of using two techniques of biometric authentication. In Iris recognition phase the iris information is encrypted and sent to the bank server along with the customer's account number. The bank server also has an encryption algorithm which is identical to encrypt iris to make a match. This would make the mobile banking process well secured. The palm vein technology is an authentication scheme that scans a person's palm and authorizes him based on his vein pattern. The device sends out infrared radiations that pass deep into the person's palm and scans his vein pattern. Also the already discussed risk of possibility of others accessing one's bank account when his credit card is stolen is eliminated since palm vein technology is used for authentication of the user who login.

II. EXISTING SYSTEM

A. Personal Identification Number

A personal identification number (PIN, pronounced "pin") is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. The user is granted access only when the number entered matches with the number stored in the system. Hence, despite the name, a PIN does not *personally* identify the user. Financial PINs are often four-digit numbers in the range 0000-9999, resulting in 10,000 possible numbers[2]. Many PIN verification systems allow three attempts, thereby giving a card thief a 0.06% probability of guessing the correct PIN before the card is blocked.The significant disadvantage of using a PIN is that the number can be stolen using skimmers. Using pre-fabricated geared device perfectly matched to the hardware of Bank ATMs, they will be able to read the magnetic stripe off of victims' cards and even record victims punching in their PINs as shown in figure 1. After this clones are made from their victims' cards, and are used with the recorded PIN.

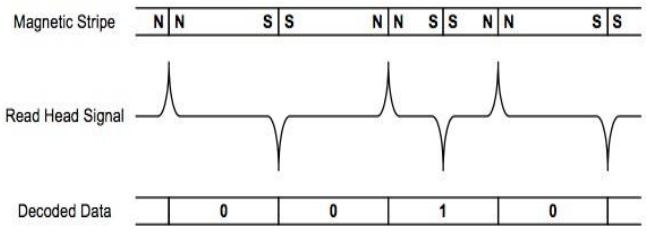

Fig 1: Recording the PIN using skimmers

B. Mechanical Imprint

Until the introduction of Chip and PIN, all face-to-face credit or debit card transactions used a magnetic stripe or mechanical imprint to read and record account data, and a signature for verification. Under this system, the customer hands their card to the clerk at the point of sale, who either "swipes" the card through a magnetic reader or makes an imprint from the raised text of the card. In the former case, the account details are verified and a slip for the customer to sign is printed[3]. In the case of a mechanical imprint, the transaction details are filled in and the customer signs the imprinted slip. In either case, the clerk verifies that the signature matches that on the back of the card to authenticate the transaction. This system has proved to be ineffective, because it has a number of security flaws, including the ability to steal a card in the post, or to learn to forge the signature on the card. More recently, technology has become available on the black market for both reading and writing the magnetic stripes, allowing cards to be easily cloned and used without the owner's knowledge.

C. Finger Print Authentication

Fingerprints are one of many techniques used to identify individuals and verify their identify. Matching algorithms used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. Pattern based algorithms compare the basic fingerprint patterns (arch, whole, and loop) between a previously stored template and a candidate fingerprint. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. The major disadvantage here is that Finger print authentication cannot be successful if the user has a band aid on his finger. Another disadvantage is fingerprint remains the same even if the person is unconscious or dead. This leads to unauthorized use of a person's fingerprint without his consent.

III. PROPOSED SYSTEM

To overcome the limitations of the existing authentication systems of the usage of credit cards, we have proposed a new system of authentication in which authentication is done through two phases. The first phase is verifying the identity of the user using iris recognition and the second phase is the authentication using palm vein technology.

The entire process of our proposed IRPV recognition technology is shown in Fig 2.

Fig. 2: Block Diagram IRPV recognition technology

Initially the user will be asked to insert his card. The database is checked to verify if such an account exists. If exists, the user will be authenticated using iris recognition. If the user is authenticated in this phase, he will then be asked to stretch out his palm for the vein pattern authentication. This is compared with the stored pattern and if it matches the user is, authenticated. A simple flowchart for the proposed system is shown in Fig 3.

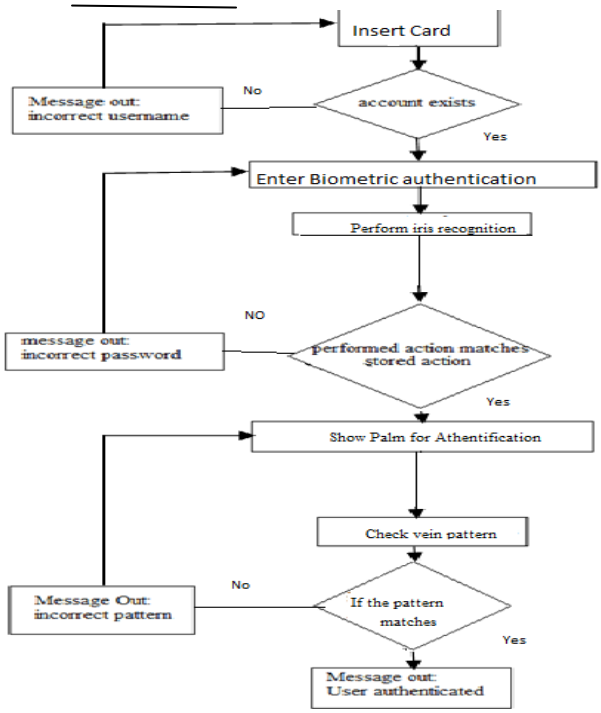

Fig 3: Flowchart for IRPV recognition technology

A. Algorithm for IRPV technique:

Insert card
Checks if it is a valid account
If account exists
Enters iris recognition phase
Converts to data pattern
Compares scanned iris pattern with stored pattern
If patterns match
Show palm for authentication
Converts to data pattern using ICP algorithm
Compares scanned pattern with stored pattern
If patterns match
Transaction Occurs successfully
Else
Mismatch in palm pattern
Transaction failed
Else
Mismatch in iris pattern
Transaction failed
Else
Account does not exist

B. Iris Recognition :

Users today mostly use textual passwords that follow an encryption algorithm. Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play. Therefore we use Biometrics in our authentication which is more customizable and very interesting way of authentication.

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the iris of an individual's eyes. Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits; the False Reject Rate (FRR) of these systems can be rather high .Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates.

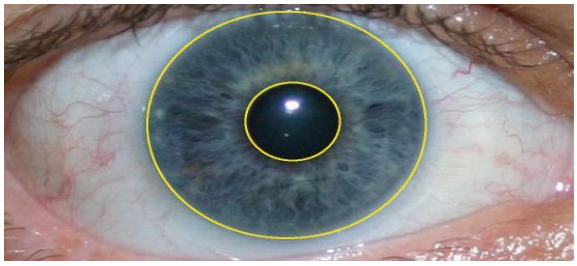

Fig 4: Iris recognition

A typical iris recognition system in involves three main modules:
Image acquisition: It is to capture a sequence of iris images from the subject using a specifically designed sensor.
Preprocessing Stage: It includes determining the boundary of the iris within the eye image, and extracts the iris portion from the image to facilitate its processing. It includes various stages such as:
a. Iris Segmentation
d. Iris Normalization
e. Image Enhancement
Feature extraction and Encoding : This is the most key component of an iris rrecognition system and determines the system's performance to a large extent. Iris recognition produces the correct result by extracting features of the input images and matching these features with known patterns in the feature database.

IV. IMAGE ACQUISITION

Image acquisition is considered the most critical step since all subsequent stages depend highly on the image quality. In order to accomplish this, the resolution is set to 640x480, the type of the image to jpeg, and the mode to white and black for greater details. Furthermore, we took the eye pictures while trying to maintain appropriate settings such as lighting and distance to camera.

V. SEGMENTATION

The main purpose of this process is to locate the iris on the image and isolate it from the rest of the eye image for further processing. Some other important tasks that are also performed in this iris segmentation block include image quality enhancement, noise reduction, and emphasis of the ridges of the iris. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector, then using the Hough transform to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radius are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array. Thus, after all radiuses and edge pixels have been searched, the maximum from the accumulator array is used to find the center of the circle and its radius according to the equation. Where X, Y are the center of the circle and r is the radius of the circle. The highest two points in the Hough space correspond to the radius and center coordinates of the circle best defined by the edge points.

VI. NORMALIZATION

Once the iris region is segmented, the next stage is to normalize this part, to enable generation of the "iris code" and their comparisons. Since variations in the eye, like optical size of the iris, position of pupil in the iris, and the iris orientation change person to person, it is required to normalize the iris image so that the representation is common to all with similar dimensions. Normalization process involves unwrapping the iris and converting it into its polar equivalent. Since in most cases the upper and lower parts of the iris area are occluded by eyelid, it was decided to use only the left and right parts of the iris area for iris recognition. Therefore, the whole iris is not transformed in the proposed system. Experiments were conducted by

normalizing the iris ignoring both upper and lower eyelid areas. The size of the rectangular block is reduced accordingly. Left and right images each one of size 112×60 are obtained. By applying this approach, detection time of upper and lower eyelids and 64.4% cost of the polar transformation are saved. Results have shown that information in these portions of iris is subjective for iris recognition.

VII. FEATURE EXTRACTION

The wavelets to signal and image processing have provided a very flexible tool for engineers to apply in various fields such as speech and image processing. In an iris recognition system, the 2-D wavelet transform is only used for preprocessing. The preprocessing helps to reduce the dimensionality of feature vector and to remove noise. Nevertheless, the computational complexity is comparatively high. The wavelet filters are used to decompose signals into high and low frequency by convolution. The wavelet filters are used to decompose signals into high and low frequency by convolution.registered one or to the bank of stored files for verification, all in a period of seconds. Numbers and positions of veins and their crossing points are all compared and, depending on verification, the person is either granted or denied access.

C. Palm Vein Technology:

Users today mostly use textual passwords that follow an encryption algorithm. Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play. Therefore we use Biometrics in our authentication which is more customizable and very interesting way of authentication.The vein matching, [4] also called vascular technology is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin. An individual first rests his wrist, on some devices, such that the palm is held centimeters above the device's scanner, which flashes a near-infrared ray on the palm. Unlike the skin, through which near-infrared light passes, deoxygenated hemoglobin in the blood flowing through the veins absorbs near-infrared rays, illuminating the hemoglobin, causing it to be visible to the scanner. Arteries and capillaries, whose blood contains oxygenated hemoglobin, which does not absorb near-infrared light, are invisible to the sensor. The still image captured by the camera, which photographs in the near-infrared range, appears as a black network, reflecting the palm's vein pattern against the lighter background of the palm

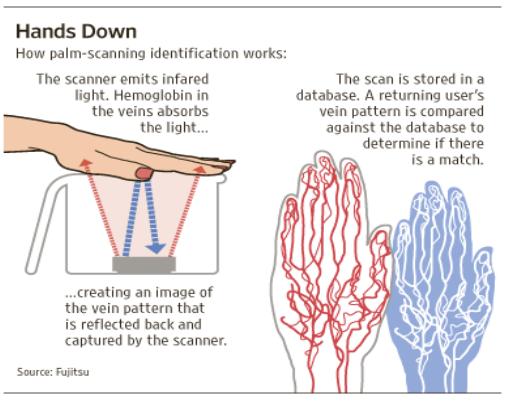

Fig 5: Scanned vein pattern

An individual's palm vein image is converted by Iterative Closest Point algorithms into data points, which is then compressed, encrypted, and stored by the software and registered along with the other details in his profile as a reference for future comparison. Iterative Closest Point is an algorithm employed to minimize the difference between two clouds of points. ICP is often used to reconstruct 2D or 3D surfaces from different scans, to localize robots and achieve optimal path planning (especially when wheel odometry is unreliable due to slippery terrain), to co-register bone models, etc. The algorithm as depicted in Fig 4 is conceptually simple and is commonly used in real-time[5]. It iteratively revises the transformation (translation, rotation) needed to minimize the distance between the points of two raw scans as in Fig 5.

Thus, each time a person logs in attempting to gain access by a palm scan to a particular bank account or secured entryway, etc., the newly captured image is likewise processed and compared to the registered one or to the bank of stored files for verification, all in a period of seconds. Numbers and positions of veins and their

crossing points are all compared and, depending on verification, the person is either granted or denied access.Compared with a finger or the back of a hand, a palm has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification. The palm is an ideal part of the body for this technology; it normally does not have hair which can be an obstacle for photographing the blood vessel pattern, and it is less susceptible to a change in skin colour, unlike a finger or the back of a hand. Even if one has registered as a child, and uses it after a very long period, it still remains the same because the vein pattern is established in the uterus even before birth.Palm vein authentication has a high level of authentication due to the uniqueness and the complexity of the vein pattern. It is better than finger print scanning because a fingerprint remains the same even if the person is dead. Thus there are a lot of chances for the unauthorized user to hurt or kill the card holder for the finger print.

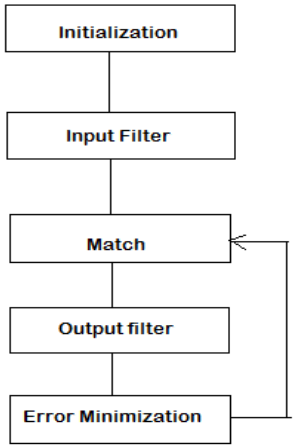

Fig 6: General procedure of the ICP algorithm.

Whereas in the case of palm vein technology, killing a person for the authentication is of no use because the vein pattern changes due to the stop of the flow of oxygenated and deoxygenated blood.Using the data of 140,000 palms from 70,000 individuals, Fujitsu has confirmed that the system has a false acceptance rate of less than 0.00008% and a false rejection rate of 0.01%, provided the hand is held over the device three times during registration, with one retry for comparison during authentication. This data does not vary even in various situations, including after drinking alcohol, taking a bath, going outside, and waking up etc.

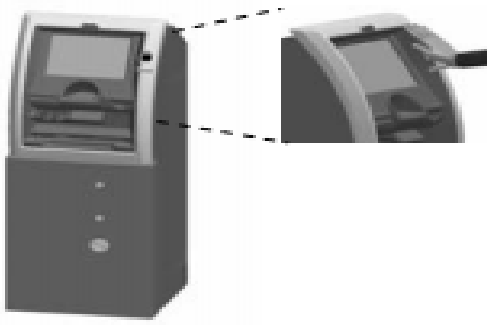

Fig 7: ATM for convenience stores with downsized palm vein pattern sensor unit

In ATM or credit card transaction, instead of entering the PIN number, we use palm vein technology for a secure transaction.

VIII. CONCLUSION

Traditional banking can be quite tedious. Hence the uses of credit, debit and ATM cards have been introduced. In this paper, the various techniques of credit card fraud and the traditional method to overcome it have been discussed. A IRPV recognition technology is being proposed which uses biometrics to completely eradicate credit card fraud. Two different techniques are discussed which can be used separately or together in order to completely reduce credit card fraud thus making the system more secure and robust.

IX. FUTURE WORK

To enhance the security of the transaction and to reduce the percentage of credit card crime we propose a future project where a person's iris is scanned for authentication even for mobile and online banking. Also it must be made platform independent and hence it can be run on various types of mobile equipment embedded with basic ccd camera. By doing this it will eliminate the effort of everyone trying to get specific mobile equipment that may be too expensive for them to afford.In total, by using this method, the transaction can in no way be carried without the consent of the card holder. Thus it becomes 100% secure and credit card fraud and related crimes can be minimized greatly.

REFERENCES

[1] Benson Edwin Raj, S.; Portia, A.A.; , "Analysis on credit card fraud detection methods,"Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on , vol., no., pp.152-156, 18-19 March 2011

[2] Murdoch, Steven J.; Drimer, Saar; Anderson, Ross; Bond, Mike; , "Chip and PIN is Broken," Security and Privacy (SP), 2010 IEEE Symposium on , vol., no., pp.433-446, 16-19 May 2010

[3] Nasir, M.H.N.; Hamid, S.; Hassan, H.; , "Thread-Level Parallelism & Shared-Memory Pool Techniques for Authorization of Credit Card System," Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on , vol., no., pp.447-452, 21-23 Oct. 2008

[4] Xiangqian Wu; Enying Gao; Youbao Tang; Kuanquan Wang; , "A Novel Biometric System Based on Hand Vein," Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on , vol., no., pp.522-526, 18-22 Aug. 2010

[5] Shitu Luo; Yanling Wang; Yin Liu; Xiaopin Hu; , "Research on geomagnetic-matching technology based on improved ICP algorithm," Information and Automation, 2008. ICIA 2008. International Conference on , vol., no., pp.815-819, 20-23 June 2008

[6] Nguyen, M.H.; Ho, D.N.; Luu, D.H.; Moldovyan, A.A.; Moldovyan, N.A.; , "On functionality extension of the digital signature standards," Advanced Technologies for Communications (ATC), 2011 International Conference on , vol., no., pp.6-9, 2-4 Aug. 2011

[7] Zuguang Xuan; Zhenjun Du; Rong Chen; , "Comparison Research on Digital Signature Algorithms in Mobile Web Services," Management and Service Science, 2009. MASS '09. International Conference on , vol., no., pp.1-4, 20-22 Sept. 2009 doi: 10.1109/ICMSS.2009.

[8] "Statistics for General and On-Line Card Fraud," http://www.epaynews.com/statistics/fraud.html , Mar. 2007.

[9] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems,vol. 3, pp. 621-630, 1994.

[10] M. Syeda, Y.Q. Zhang, and Y. Pan, "Parallel Granular Networks for Fast Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Fuzzy Systems, pp. 572-577, 2002.

[11] Organism Information Visualization Technology Editing Committee Edition: Organism Information Visualization Technology. (in Japanese), Corona Publication Co., Ltd., p.235 (1997).

[12] The Federation of Bankers Associations of Japan: Statistics from the Questionnaire on the Number of Withdrawals and the Amount of Money Withdrawn Using Stolen Passbooks. http://www.zenginkyo.or.jp/en/news/index.html

[13] "Palm Vein Authentication Technology" white paper, Bioguard, Innovative Biometric Solutions, March, 2007.

[14] Yuhang Ding, Dayan Zhuang and Kejun Wang, "A Study of Hand Vein Recognition Method", The IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada, July 2005.

[15] [10] Shi Zhao, Yiding Wang and Yunhong Wang, "Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices", Fourth International Conference on Image and Graphics, 2007.