International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 5 | ISSN : 2456-3307
DOI : 10.32628/CSEIT19556

A Review on Various Credit Card Transaction Based on Face Recognition

[1]Payal Sahare, [2]Rohini Khobragade, [3]Sachi Ambade, [4]Samiksha Deshmukh, [5]Prof. S. M. Malode

[1234]BE Student, Computer Technology, K. D. K. College of Engineering, Nagpur, Maharashtra, India
[5]Assistant Professor, Computer Technology, K. D. K. College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

Money is an important thing in this world. The payment modes at Point of Sales (PoS) have different modes such as cash on delivery, online transaction, credit card transaction and monthly instalments etc. Whenever online transactions take place, the customer involves opting for credit/debit cards or internet banking. The credit card provides prominent use of payment method, so it is followed in many scenarios. As we know, during online transactions there are many chances to steal the confidential information by the attackers or hackers. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great efforts to rescue the unsafe situation at the Credit Card Transactions. In this paper, we looked into the various system that integrates facial recognition technology for identity verification process for Credit Card Transactions.

Keywords : Credit Card Fraud, Transaction, Verification, Face Recognize, Image Processing

I. INTRODUCTION

The people having the right to purchase anything with a price tag for the required items. Multiple and multilevel people have involved for the production of commodities and these are used by the people at different parts of the world. People purchase what they require and the important parameter that allows a person to allow buying a thing or reject them from buying power is only the money. There are different methods of payment of money and the merchant who sells the product always expects the payment method to be cash. This is because when the buyer gives cash and then purchases the product the transactions gets over immediately and the merchant can earn the value of the original profit whether with actual price or profit. The problem with having cash by the user is the chance of being lost or stolen. Carrying huge amount of cash makes it difficult to take everywhere with high intense of care to safe guard the money. To avoid these tedious steps, the new technique implied was payment through the credit cards or debit cards. The credit/debit card usage has grown in the recent years. This practice indicates the development of technology in every place. Evenly, the risks also increase in this mode of payment [1].

In internet, there are many chances of intruders' gaining illegal access. The intension is to steal to private data or take compensation by an attack to systems that are vulnerable to extortion. When the money involves, surely there are huge number of possibilities liable to such attacks. Hence, the merchants use various encryption algorithms to provide security against these intruders. In addition, the cardholder uses secure programs like anti-viruses, virtual keyboards etc. But, some attacks which take against human interest which are likely shoulder surfing, monitoring through eagle eyes or recording in a camera while data in entered are against the odds.

Credit card processing companies make sure credit card transactions are processed accurately and on time, for a fee. As more and more customers get comfortable with cashless transactions, businesses are pulling all the stops to make credit card transactions secure and painless. Cashless transactions benefit your business. Funds are transferred into your merchant account on time with hardly any effort from your side. The fundamental problem faced by the credit card users is to have a secure online transaction using credit cards. Credit card fraud is the biggest risk in credit card transactions. Credit cards are stolen and used to make large purchases, often leading to heavy losses for the credit card processing service and the business.

One of the solution is verification of the biometric linkage between the signed facial image of the credit card holder embedded in credit card and the user's facial image captured by a webcam during usage of the card.

A face recognition technology identify a person information through a digital image. It is automatically identify. It is mainly used in security systems. The face recognition will directly capture information about the human faces. It match the face identity in different angles. It is mostly used in airports. It will recognize the face identity and we can avoid some unwanted fraud using face recognition system .The main advantage of face recognition is used for fraud restriction and crime controlling purpose because face images that have been archived and recorded, so that it will help us to identify a person later. Face recognition is it identifies each skin tone, which is individual of a human face's surface, like the cheek, curves of the eye hole and nose etc. this technology may also be used in very dark condition and preventing identity theft.

II. REVIEW OF LITERATURE

Nowadays the frauds are increased in various fields such as online transactions, ATM's. Fraud detection involves identifying fraud quickly as possible once it has been committed. Generally, frauds are detected by using outlier analysis. This has made it easier for fraudsters to indulge in a new and abstruse ways of committing credit card fraud over online transaction. Face recognition technique are used for recognizing a special face from set of different faces. Face has a significant role in human beings communications where, each person along with his/her feelings mainly is distinguished by user face image [1]. One can easily find out that one of the main problems in machine-human being interactions is the face recognition problem. A human face is a complex object with features varying over time. So a robust face recognition system must operate under a variety of conditions. Rapid progression through customs by using face as a live passport in immigration, comparison of surveillance images against an image database of known terrorists and other unwanted people in security/counterterrorism, and verifying identity of people found unconscious, dead or individuals refusing to identify themselves in hospital are examples of governmental uses. Withdrawing cash from an automated teller machine (ATM) without cards or pin numbers in banking and access control of home and office in premises access control are some examples of commercial uses of face recognition systems which demonstrate the importance of these systems [4]. There have been a several faces recognition methods, common face recognition methods are Geometrical Feature Matching, Eigen faces method, Bunch Graph Matching, Neural

Networks, Support Vector Machines, Elastic Matching and Hidden Markov Models (HMM). Instead of outlier, Face image is taken as an input. A wide variety of techniques have been proposed for feature extraction by using HMM and SVD coefficient.

The popularity of online shopping is growing day by day. During the last few years there has been an increase in online fraud of global scope and geometrically increasing proportions. There are now actual companies that specialize in spam and other illegal marketing techniques, like Phishing and Hacking. Credit-card-based purchases can be categorized into two types: Physical card & Virtual card In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company [3]. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the “usual” spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds.

Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection [4]. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. This article defines common terms in credit card fraud and highlights key statistics and figures in this field. Depending on the type of fraud faced by banks or credit card companies, various measures can be adopted and implemented. The proposals made in this paper are likely to have beneficial attributes in terms of cost savings and time efficiency. The significance of the application of the techniques reviewed here is in the minimization of credit card fraud. Yet there are still ethical issues when genuine credit card customers are misclassified as fraudulent. Some time, there has been a strong interest in the ethics of banking as well as the moral complexity of fraudulent behaviour. A critical task to help businesses and financial institutions including banks is to take steps to prevent fraud and to deal with it efficiently and effectively [15].

Bankruptcy fraud is one of the most difficult types of fraud to predict [16]. Purchasers use credit cards knowing that they are not able to pay for their purchases. The bank will send them an order to pay. However, the customers will be recognized as being in a state of personal bankruptcy and not able to recover their debts. Usually, this type of fraud loss is not included in the calculation of the fraud loss provision as it is considered a charge-off loss. The only way to prevent this bankruptcy fraud is by doing a pre-check with credit bureaux in order to be informed about the banking history of the customers.

Theft fraud means using a card that is not yours. The perpetrator will steal the card of someone else and use it as many times as possible before the card is blocked. The sooner the owner will react and contact the bank, the faster the bank will take measures to stop the thief [9]. Similarly, counterfeit fraud occurs when the credit card is used remotely; only the credit card details are needed. At one point, one will copy your card number and codes and use it via certain web-sites, where no signature or physical cards are required. Recently, Pago, one of the leading international acquiring &

payment service providers, reveals in its Pago Report that credit card fraud is a growing threat to businesses selling goods or services through the internet. On-line merchants are at risk because they have to offer their clients payment by credit card. In cases where fraudsters use stolen or manipulated credit card data the merchant loses money because of so-called "charge-backs" that charge-backs are generated if credit card holders object to items on their monthly credit card statements because they were not responsible for the purchase transactions.

III.FACE RECOGNITION TECHNIQUES

Different Algorithms and techniques have been designed to implement the facial recognition as a key element for authentication of cardholder. These cards were not normal office cards or any other card than the credit card. Many institutions use e-ID cards as access control authorization, it means that one just needs to possess card in order to get access to resources e.g. room or elevator. In such a scenario, it is sufficient to steal or duplicate a card of legitimate user in order to get all its credentials. It is also possible to borrow such an e-ID card from third parties in an unlimited way. Based on these arguments we propose a new solution preventing from using electronic cards by unauthorized persons as well as limiting the usage of stolen cards.

Simultaneously the whole system should be as transparent as possible for users and not force them to change their habits in major way. We aim to provide such a solution that fulfils the following criteria: it is based on electronic card technology (e- ID/RFID cards), almost transparent for users, does not require any special additional actions, increases system security, and eliminates undesired behaviors e.g. borrowing cards. In face recognition, there are also various techniques. Some of them are:

-Linear Binary Pattern

-Eigen faces

-Fisher faces

A. Linear Binary Pattern:

The LBP is one of the best performing texture descriptors and it has been widely used in various applications. It has proven to be highly discriminative and its key advantages, namely, its invariance to monotonic gray-level changes and computational efficiency, make it suitable for demanding image analysis tasks.

B. Eigen Faces:

Much of the previous work on automated face recognition has ignored the issue of just what aspects of the face stimulus are important for identification, assuming that predefined measurements were relevant and sufficient. This suggested to us that an information theory approach of coding and decoding face images may give insight into the information content of face images, emphasizing the significant local and global “features”. Such features may or may not be directly related to our intuitive notion of face features such as the eyes, nose, lips, and hair. In the language of information theory, we want to extract the relevant N information in a face image, encode it as efficiently as possible, and compare one face encoding with a database of models encoded similarly. A simple approach to extracting the information contained in an image of a face is to somehow capture the variation in a collection of face images, independent of any judgment of features, and use this information to encode and compare individual face images.

C. Fisher Faces:

This paper introduces a new face coding and recognition method that employs the enhanced Fisher classifier (EFC) operating on integrated shape and texture features, and assesses comparatively the types of input for face representation against some popular face recognition methods. The dimensionalities of the shape and the texture spaces are first reduced using principal component analysis (PCA). The corresponding but reduced shape and texture features are then combined through a normalization procedure to form the integrated shape and texture features. The other two types of input assessed in this paper are the shape images and the masked images. Shape images undergo the same alignment procedure as the shapes do, but preserve the intensity information within the contours of the faces.

IV. CONCLUSION

As the technology grows day to day, there are lots of changes happening throughout entire system and importantly security for each component is necessary. In this paper, the review of different facial recognition techniques is presented. The different techniques such as Linear Binary Pattern, Eigenfaces, Fisherfaces is explained. We also presented the study of various work conducted by diffrent researchers.

V. REFERENCES

[1] Anshul Singh, Devesh Narayan. (2012), 'A Survey on Hidden Markov Model for Credit Card Fraud Detection', (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-Ant´onio Miguel Louren¸co. (2009), "Techniques for keypoint detection and matching between endoscopic images".

[2] Avinash Ingole, Dr. R. C. Thool. (2013), "Credit Card Fraud Detection Using Hidden Markov Model and Its Performance", ijarcsse, Volume 3, Issue 6, pp. 626-632

[3] Clifton phua, Vincent Lee, Kate Smith & Ross Gayler. (2010), "A Comprehensive Survey of Data Mining-based Fraud Detection Research"

[4] D. Madhu Babu, M. Bhagyasri, K. Lahari, CH. Madhuri, G. Pushpa Kumari. (2014), "Image Based Fraud Prevention", (IJCSIT), Vol. 5 (1), pp.728-731

[5] Dipti Deodhare, NNR Ranga Suri R. Amit. (2005), "Preprocessing and Image Enhancement Algorithms for a Form-based Intelligent Character Recognition System", IJCSA, Vol. II, No. II, pp.131 - 144

[6] Dong ping, Tian. (2013), "A Review on Image Feature Extraction and Representation Techniques", IJMUE, Vol. 8, No. 4, pp.385-395

[7] https://www.jumio.com/2011/07/jumio-turns-webcam-into-credit-card-reader/

[8] http://www.marketcalls.in/credit-cards/the-history-of-credit-cards.html

[9] http://wwwen.uni.lu/snt/research/research_projects2/prevention_of_fraud_by_pattern_detection_in_credit_card_transaction

[10] Khyati Chaudhary, Jyoti Yadav Bhawna Mallick. (2012), "A review of Fraud Detection Techniques: Credit Card", IJCA, Vol. 45, No. 1, pp.39-44

[11] Kumar.G. (2014), "A Detailed Review of Feature Extraction in Image Processing Systems", ACCT, pp.5 - 12

[12] Mark S. Nixon, Alberto S. Aguado. (2008), "Feature Extraction and Image Processing", ISBN 0 7506 5078 8

[13] Rashmi G.Dukhi. (2011), "Soft Computing Tools in Credit card fraud & Detection", ijetae.com, ISSN 2250-2459, Volume 1, Issue 2, pp. 60-64

[14] Vinay Hiremath, Ashwini Mayakar. (2012), "FACE RECOGNITION USING EIGENFACE APPROACH"

Cite this article as : Sh