SECURED CREDIT CARD TRANSACTIONS USING WEBCAM

Janani.S.R[1], Sivaparthiban.C.B[2] , Lekha T. R[3]

[1,2] Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India.
[3] Department of Inforamation Technology, SNS College of Engineering, Coimbatore,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. So, we suggest a new method to avoid fraudulent during online transactions and to secure the information by a two step verification process. The information is processed and the acknowledgement is sent to the bank for both the valid and invalid transactions. A new method of credit card scanning has beneficial attributes in terms of cost savings and time efficiency. The significance of the application techniques reviewed here is in the minimization of credit card fraud by sending the photo of the unauthorized user to the bank.

Key Words: Credit card scanning, face recognize, webcam, transaction, verification

1.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. Also, 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.

To avoid the above discussed problems, this paper suggests a new mechanism to avoid the defects in a credit card payment system. We use the webcam to read the data from the credit card. This avoids the time in which the data is being entered since a scan can capture data fast than the manually entering process. A second step of verification is done where the face of the person who is handling the payment is scanned using the webcam. After scanning, credit card data and person face was compared with the database and when both the results are positive, the transaction is completed successfully.

The remainder of the paper is organized as follows. The relevant works on credit card fraudulent detection mechanism and face recognizing algorithms are surveyed in Section II. Section III details our envisioned concepts about the new technology. The implementation of the proposed system and its results are discussed in Section IV. Finally, concluding remarks are provided in Section V.

2. RELATED WORKS

IMAGE BASED FRAUD PREVENTION

Now a day's 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.

CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL

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.

CREDIT CARD FRAUD AND DETECTION TECHNIQUES

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

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/COUNTERFEIT FRAUD

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.

3. SYSTEM ARCHITECTURE

A.Training

The proposed mechanism can be used for payment only by the cardholder. The credit card will be scanned through a webcam and Scanning is done effectively with high quality webcam. While user get credit card from the Bank, name of the cardholder, bank account details, credit card information such as unique credit card number, the Card Verification Value (CVV) number, expiry date, are maintained in the database along with photo of the user.

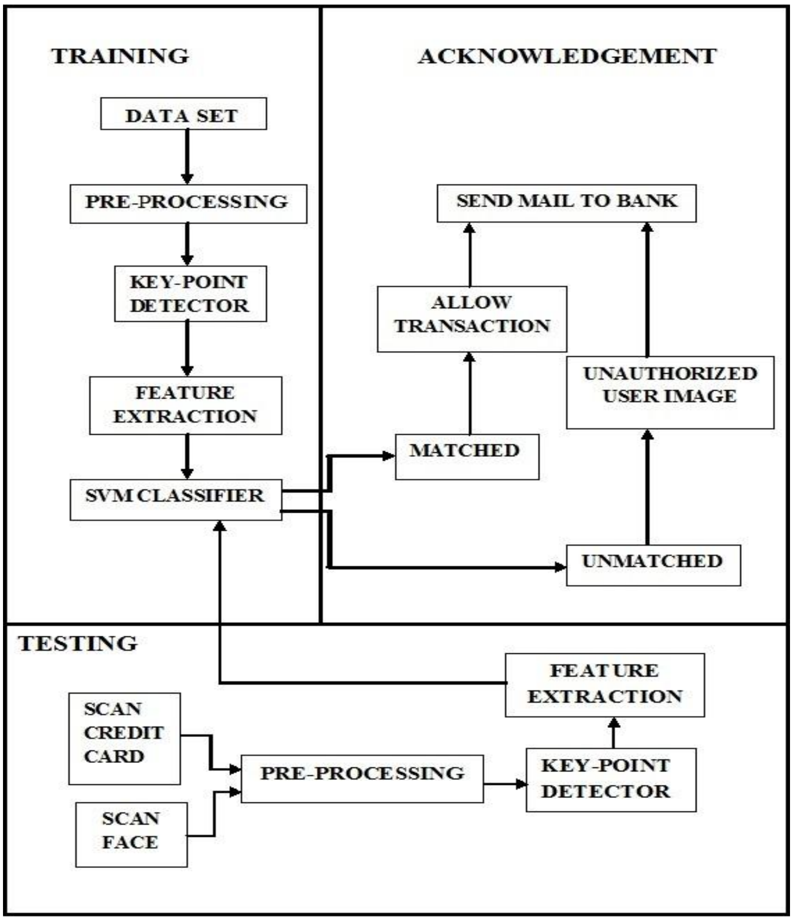


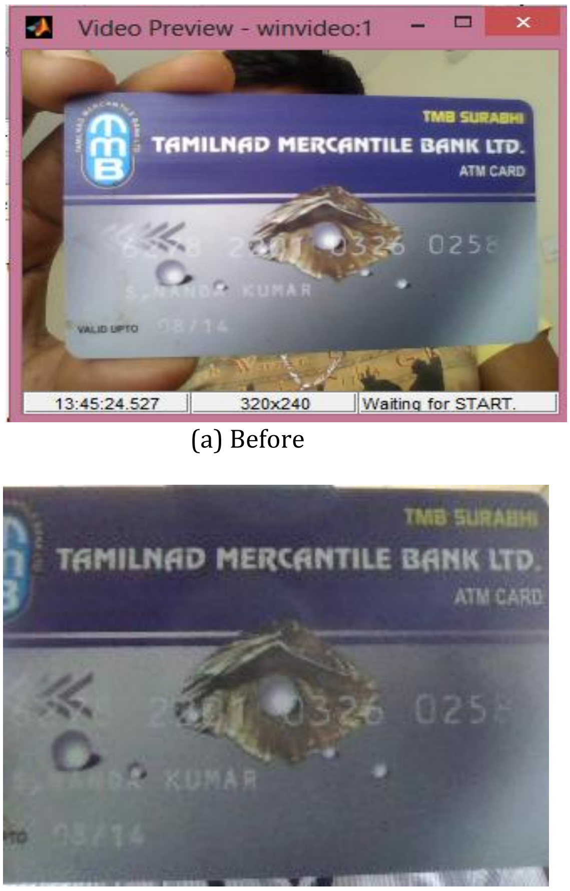
Fig. 1

4.1 Data Sets

Using the matlab software, the preview of the credit card is obtained. The credit card consists of different sections like unique credit card number, the name of the cardholder and the expiry date till which the credit card can be utilized at different PoS and finally there is a unique number present on the back side of every credit card which is known as the Card Verification Value (CVV) number. This CVV number is a three digit representation of any combination and it is requested each and every process of the credit card usage during the online transaction. User face will be scanned and features are extracted by using key point detector. Credit card and User face will be taken as a Data set.

4.2 Pre-processing

If the card or card holder's details are mistyped then this will be recognized in this phase and it will be processed and checks whether the given information is right or wrong [6]. During scanning, if there is any direction or shake in card or credit card scanning it would not affect the result.



(a) Before

(b) After

Fig. 2 Pre-processing

As shown in the Fig. 2(a) the credit card will be scanned as normal and the whole image is displayed. The pre-processing involves the recognizing the integral part as shown in the Fig.2(b) of the image and process only this for future puposes.

The pre-processing technique recognizes only the specific location in an image. This enhances the ability to perform the processing of data efficiently during the transactions. Even if the quality of the image is low during the scanning process, the acquired positions help to identify the image accurately.

4.3 Key Point Detector

The current directory contains functions allowing extracting key points also called "feature points", "corners", "interest points". The input image must be a gray level image. The output is a matrix of dimension Nx2 or Nx3 with N the number of keypoints extracted. The first column gives the row position of the keypoints and the second column gives the column position of the keypoints [2]. The third column gives the feature scale of the keypoints as shown in Fig. 3. This scale corresponds to the radius of the local neighborhood to consider.

Key point detector will detect the key points in scanning and checks whether the scanned key will matches with the key already entered. The different kinds of key will be entered for both credit card and card holders. If both match, then the transaction will be performed.

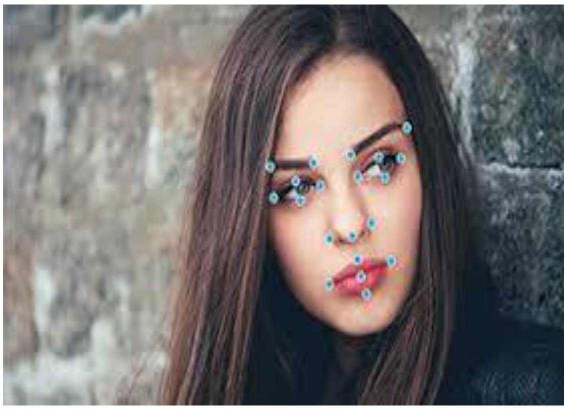


Fig. 3 Key point detector

4.4 Feature Extraction

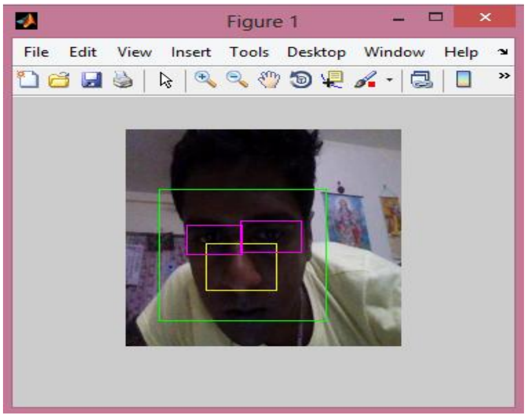


Fig. 4 Feature extraction

Feature extraction is an attribute reduction process. Unlike feature selection, which ranks the existing attributes according to their predictive significance, feature extraction actually transforms the attributes [7]. The transformed attributes, or features, are linear combinations of the original attributes.

Feature extraction a type of dimensionality reduction that efficiently represents interesting parts of an image as a compact feature vector. This approach is useful when image sizes are large and a reduced feature representation is required to quickly complete tasks such as image matching and retrieval.

Feature detection, feature extraction, and matching are often combined to solve common computer vision problems such as object detection and recognition, content-based image retrieval, face detection and recognition, and texture classification.

The feature extraction process results in a much smaller and richer set of attributes shown in Fig. 4. The maximum number of features is controlled by the FEAT_NUM_FEATURES build setting for feature extraction models [12], [13]. Some applications of feature extraction are latent semantic analysis, data compression, data decomposition and projection, and pattern recognition. Feature extraction can also be used to enhance the speed and effectiveness of supervised learning.

All the features of the card and the card holder are to be defined clearly then it the system will enters the key points to differentiate from others. Then, the key features that are to be identified are to be extracted.

4.5 SVM Classifier

For classification of activities from the data, the SVM classifier needs to be trained with training data set. On training SVM, the classifier extracts data (like bias value, support vectors) required for classification. For further classification of data, this data will be used by the SVM.

Steps involved in Classification are given below:

Step 1: Prepare the feature data matrix

Step 2: Choose an optimal Kernel Function

Step 3: Execute the training algorithm and obtain alpha value

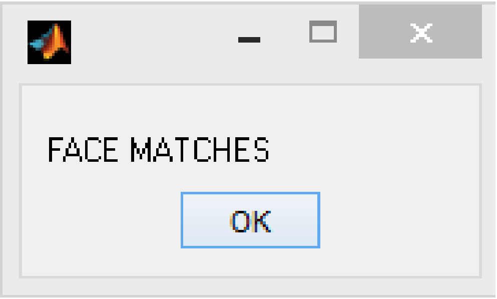
Step 4: The test data can be classified using the alpha value and support Vector

B. Testing

Only, the cardholder who has created an account with the bank is given rights to make the purchase using the credit card. To do secure transaction, cardholders have to show the credit card to webcam and it will be scanned. Next process is to detect the face from webcam. For that the user or card holder shows their face in front of the camera, the system will automatically take the face image. As like in training process, Pre-Processing, Key Point Detection are done and extracted features are passed to SVM Classifier.

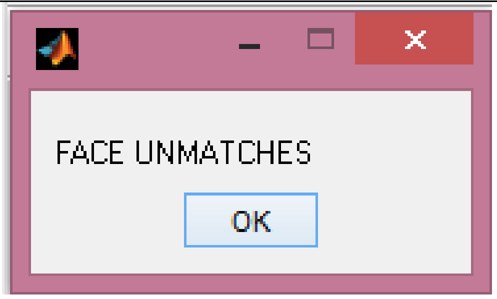
3.3 Acknowledgement

SVM Classifier results are shown in the Fig. 6. The Fig. 6(a) denotes the positive label and the negative label is shown in the Fig. 6(b). If SVM Classifier result is positive, the transaction is allowed and if the result is negative, transaction is not allowed. For both the cases acknowledgement mail will be send to the bank along with photo of the accessing person. This Photo will be helpful to find the unauthorized person easily.



FACE MATCHES

(a) Positive Result



FACE UNMATCHES

(b) Negative Result

Fig. 6 SVM Classifier

4. CONCLUSIONS

As the technology grows day to day, there are lots of changes happening throughout entire system and importantly security for each component is necessary. By using an automated reading of credit card details through a webcam and the face recognising technique, the credit card system for online transactions is secured. The chances to steal credit card information or unauthorized users are avoided. So, the transactions are secured and the credit card users are more reliable with the merchants.

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-3, pp. 49-52

[2] Ant´onio Miguel Louren¸co. (2009), "Techniques for keypoint detection and matching between endoscopic images"

[3] 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

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

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

[6] 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

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

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

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

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

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

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

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

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

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

[16] www.experian.com/credit-advice/topic-bankruptcy.html

[17] www.mathworks.com/matlabcentral/.../48632-multiclass-svm-classifier