FIND TRANSACTION FRAUD USING FACE DETECTION AND HIDDEN KEYBOARD

Chaitanya Sumant[1] ,Irshad Shaikh[2],Abhishek Jadhav [3],Prof. Poorva Agrawal[4]
G H Raisoni College of Engineering And Technology Wagholi Pune

Abstract: The financial services sector has undergone a transformation in the last ten years. Customers no longer need to visit their bank – Internet, mobile, and self-service kiosks including ATMs now provide access to services at all times. Whilst cash and cheque still have their place, credit and debit cards are universally accepted, and the mobile phone is moving to take its place as a popular way to pay. A significant manner of police investigation fraud is to extract the behavior profiles (BPs) of users supported their historical dealings records, thus to verify if associate degree incoming dealings is also a fraud or not ocular of their bits per second. Markov process models unit widespread to represent bits per second of users, that's effective for those users whose dealings behaviors unit stable relatively. However, with the event and popularization of on-line trying, it is a heap of convenient for users to consume via Infobahn that diversifies the dealings knowledge entropy-based on To cipher a path-based transition likelihood from associate degree attribute to a distinct one. Here we tend to area unit able to realize Face by pattern viola jones and LBP acknowledge formula for face detection as we tend to use invisible keyword sequence for authentication of the relation of attributes of dealings records. Supported LGBP and users dealings records, we tend to area unit able OTP. The keyword sequence modification once. At constant time, we've an this paper, we've an inclination to propose logical graph of BP (LGBP) that will be a complete order-based model to represent inclination to stipulate associate degree diversity constant thus characterizes the behaviors of users. Therefore, Markov process models unit unsuitable for the illustration of these behaviors. Throughout variability of dealings behaviors of a user. We've an inclination to in addition track fraud user with location by mackintosh address of the user laptop computer transportable or computer that have last dealings successfully. In addition, we've an inclination to stipulate a state transition likelihood matrix to capture temporal choices of transactions of a user. Consequently, we tend to area unit able to construct a BP for each user thus use it to verify if associate degree incoming dealings is also a fraud or not. Our experiments over a real data set illustrate that our methodology is healthier than three progressive ones

Keywords: Behavior profile & e-commerce security, Face Detection, Invisible Keyboard Sequence, fraud detection, on-line dealings.

1. Introduction

According to a report by Hindustan Times, India has lost of rs615.39 crores in more than 1.17 lakh cases of online banking frauds from April 2009 to September 2019. Credit cards area unit wide used in on- line looking, and card-not-present transactions in master card operations becomes a great deal of and a great deal of modish since web payment gateways (e.g., Pay- Pal and AliPay) become modish. However, there has been a coincident growth of dealing fraud that finishes up in associate degree extremely dramatic impact on users. A survey of over 100 and sixty companies reveals that the number of on-line frauds is twelve times over that of net frauds, and thus the losses can increase yearly at double-digit rates by 2020. A physical card is not required at intervals true of on-line looking and entirely the info of the cardboard is enough for a trans- action. Therefore, it is a ton of easier for a fraudster to make a fraud. There area unit some ways that by that fraudsters can illicitly acquire the cardboard data of a user: phishing (cloned websites), pseudo base station, Trojan virus, collision attack, malicious executive director, and so on. Therefore, it's really attention-grabbing and vital to review the ways of fraud detection. Currently, there are a unit two forms of ways of fraud detection: misuse detection and anomaly detection. The previous is to assemble associate degree outsize info of fallacious signatures associated uses it as a connection notice associate degree incoming dealing. This kind of approach typically has to apprehend the previous

cases of fraud so on get the varied fraud patterns. Varied supervised learning ways like neural networks, call trees, offer regression, and support vector machine area unit generally accustomed acquire the fraud patterns. They are economical for police work those fraud cases that belong to the prevailing patterns. However, they are unsuitable for the fraud transactions that weren't recognized earlier. In addition, the individual behavior characteristics of each user area unit unobserved in these ways.

2. Motivation

- Day by day the transaction fraud is increasing exponentially.
- It is an issue for the most of the users, so we decided to stop this type of fraud in the online transaction domain.
- It is very complicated to detect the fraud availability of the messaging services.
- The solution for the issue is the system will send transaction fail message after 24 hr**.**

3. Problem Statement

In existing system many banking sectors victimization the Signature based transactions there is likelihood of duplicate signature by someone. entirely OTP verification is accessible on mobile, but someone's making an attempt to induce your phone and sees OTP and transfer money from one account to the another account. Even by the upper than two mentioned methodologies the fraud dealings is up to the mark.

3.1 Goals and Objectives

- To protect the bank details from the unwanted person.
- To reduce loss due to payment fraud on customer's part.
- Adding more security layers to the buying process.

3.2 Project Scope

It may help collecting perfect management in details. In a very short time, the collection will be obvious, simple and sensible. It will help a person to know the management of past years perfectly vividly

3.3 Application

To be used for making online transaction securely with face recognition

4. System Architecture

We propose logical graph of BP (LGBP) that would be a complete order-based model to represent the relation of attributes of dealings records. Supported LGBP and users' dealings records, we are going to reckon a path-based transition likelihood from associate attribute to a unique one. Here we are going to notice Face by exploitation viola jones and LBP acknowledge rule for face detection we have a tendency to tend use invisible keyword sequence for authentication of OTP. The keyword sequence modification whenever. At an identical time, we have a tendency to tend to stipulate associate information entropy-based diversity constant therefore on characterize the vary of dealings behaviors of a user. To boot, we have a tendency to tend to stipulate a state transition likelihood matrix to capture temporal choices of transactions of a user.

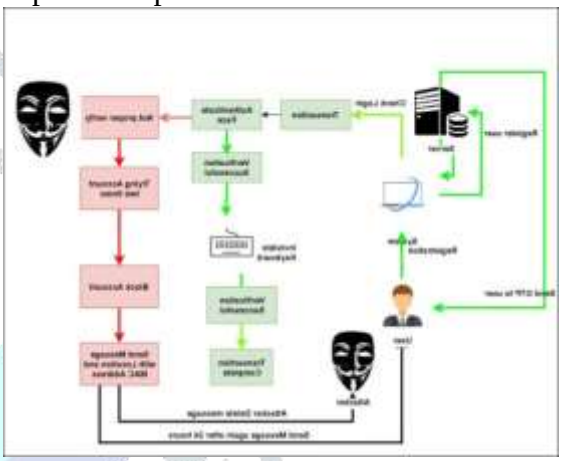

Fig1. System Architecture

5. Mathematical Model

- Let S be the system
- P={I,P,O}
- Where,
- I= Input(Users, Attacker)
- P={Setup, Trans, OTP, Detect Fraud, send MSG}
- Setup={U}
- U={u1, u2, …., un}
- U: No of Users
- KeyGen(OKpri; TKpri)
- OKpri=User Private Key
- TKpri=User Transaction Iden
- TKpri=User Transaction Identity
- Trans= {t1, t2, …., tn}

- Trans: No of transaction done by users
- User can do transaction by using OTP or secret Key, Here user can add new user account to transfer money otherwise select any existing user details to transfer amount.
- Output={O1,O2}
- Output : Either transaction success of fail

6. Algorithm Details

6.1 Viola-Jones Algorithm

Set the minimum window size, and sliding step corresponding to that size.For the chosen window size, slide the window vertically and horizontally with the same step. At each step, a set of *N* face recognition filters is applied. If one filter gives a positive answer, the face is detected in the current widow.If the size of the window is the maximum size stop the procedure. Otherwise increase the size of the window and corresponding sliding step to the next chosen size and go to the step2.

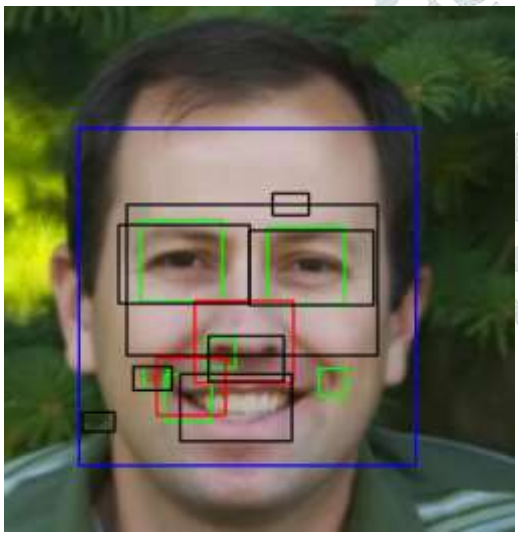

Fig 6.1: Viola Jones Face Recognition

6.2 LBP Algorithm

Divide the examined window into cells.For each pixel in a cell, compare the pixel to each of its 8 neighbors where the center pixel's value is greater than the neighbor's value, write "0". Otherwise, write "1". Compute the histogram, over the cell, of the frequency of each "number" occurring Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window

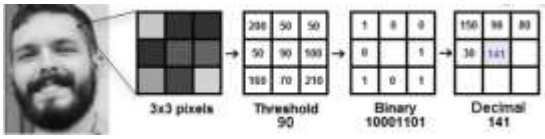

Fig 6.2: LBP Algorithm

7. Result

Fig. 7.3: admin View accounts

Fig.7.4: admin view block accounts

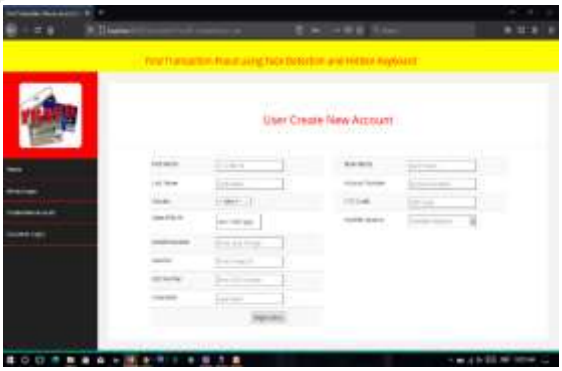

Fig.7.5 User Registration

Fig.7.7: User View Profile

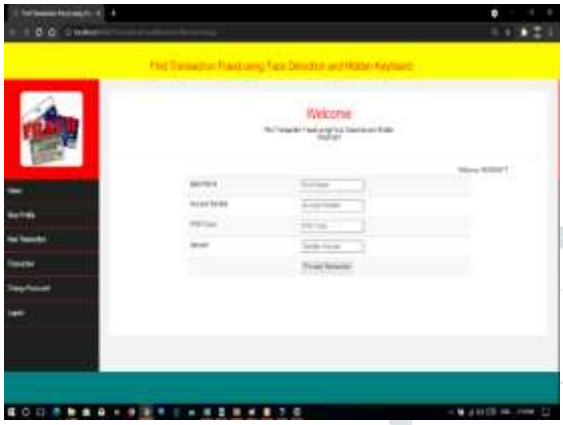

fig.7.8: New transaction

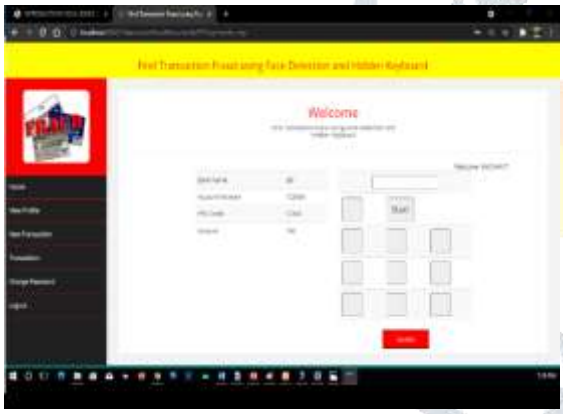

Fig.7.10Invisible keyboard

Fig 7.11: Invisible Keyboard Sequence

Fig.7.12: Mobile OTP

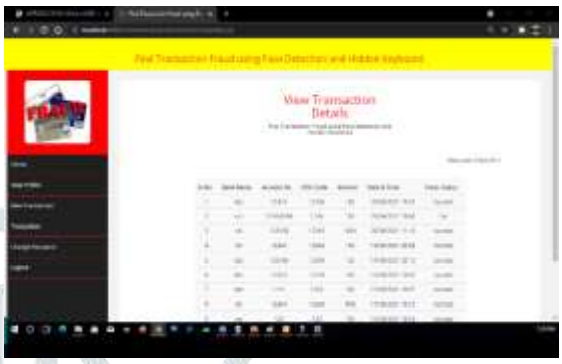

Fig.7.13: Transactions

Fig.7.14: Change Password

Fig.7.15: Login fail/Transaction Fail SMS

8. Conclusion

In this project, we've got a bent to propose the simplest way to extract users bits per second supported their dealing records, that's utilized to seek out dealing fraud at intervals the on-line looking out scenario by using the face detection. Overcomes the defect of Mark off process models since it
Characterizes the vary of user behaviors. Experiments together illustrate the advantage of OM. the long haul work focuses on some machine-learning ways that to automatically classify the values of trans- action attributes so as that our model can characterize the users bespoke behavior loads of specifically. in addition, we've got a bent to plan to extend BP by considering totally different data like users comments

9. References

[1] Ranjeet Singh, Mandeep Kaur, Face Recognition and Detection using Viola-Jones and Cross Correlation Method
, International Journal of Science and Research (IJSR)., Volume 4 Issue 1, January 2015
[2] Kirti Dang, Shanu Sharma, Review and Comparison of Face Detection Algorithms: IEEE 2017
[3] YudongGuo, JuyongZhangy, JianfeiCai, Boyi Jiang and Jianmin Zheng, CNN-based Real-time Dense Face Reconstruction
with Inverse-rendered Photo-realistic Face Images. IEEE. 2018
[4] Shweta Jamkavale, Ashwini Kute, RupaliPawar, Komal Jamkavale4, PrashantJawalkar, Secure Transaction by Using Wireless Password
with Shuffling Keypad, IJRASETVolume 4 Issue X, October 2016
[5] Zigong Zhang, Xu Chen, Beizhan Wang, Guosheng Hu, WangmengZuo, Senior Member, IEEE,
and Edwin R. Hancock, Face Frontalization Using an Appearance-Flow-
Based Convolutional Neural Network, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 28, NO. 5, MAY 2019
[6] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, Behavioralanalysis of insider threat: A survey and bootstrapped prediction in imbalanceddata, IEEE Trans. Compute. Social Syst., vol. 1, no. 2, pp. 135155, Jun. 2014.
[7] V. Bhusari and S. Patil, Application of hidden Markov model in credit cardfraud detection, Int. J. Distrib. Parallel Syst., vol. 2, no. 6, pp. 203210, 2011.
[8] R. Brause, T. Langsdorf, and M. Hepp, Neural data mining for credit card frauddetection, in Proc. IEEE Int. Conf. Tools Artif. Intell., 1999, pp. 103106.
[9] T. Carter, An Introduction to Information Theory and Entropy, S. Fe, Eds.CiteSeer, 2007.
[10] R. C. Chen, S. T. Luo, X. Liang, and V. C. S. Lee, Personalized ap- proachbased on SVM and ANN for detecting credit card fraud, in Proc. Int. Conf.NeuralNetw. Brain, Oct. 2005, pp. 810815.
[11] C. Cortes and D. Pregibon, Signature-based methods for data streams, DataMiningKnowl. Discovery, vol. 5, no. 3, pp. 167182, 2001.
[12] V. Dheepa and R. Dhanapal, "Behavior based credit card fraud detectionusing support vector machines," *ICTACT J. Soft Comput.*, vol. 4, no. 4, pp. 391–397, 2012.
[13] S. G. Fashoto, O. Owolabi, O. Adeleye, and J. Wandera, "Hybridmethods for credit card fraud detection using K-means clustering withhidden Markov model and multilayer perceptron algorithm," *Brit. J.Appl. Sci. Technol.*, vol. 13, no. 5, pp. 1–11, 2016.
[14] Global Online Payment Methods: Full Year 2016, GmbH & Co. KG, Berlin, Germany, Mar. 2016.
[15] S. Gordon and R. Ford, "On the definition and classification of cybercrime," J. Comput. Virol., vol. 2, no. 1, pp. 13–20, 2006.