Using Face Detection and Virtual Keyboard Find Transaction Fraud

Namrata Salve[1], Abhilash Paunikar[2] , Vaibhav Kamble[3], Lakhan More[4], Prof. Deepali Patil [2]

[1-4]NUTAN MAHARASHTRA INSTITUTE OF ENGINEERING AND TECHNOLOGY

Abstract: The rate of online trying, dealings fraud is increasing seriously. Therefore, the study on fraud detection is attention-grabbing and vital. 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 behaviors of users. Therefore, Markov process models unit unsuitable for the illustration of these behaviors. Throughout this paper, we've an inclination to propose logical graph of BP (LGBP) that will be a complete order-based model to represent the relation of attributes of dealings records. Supported LGBP and users dealings records, we tend to area unit able 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 OTP. The keyword sequence modification once. At constant time, we've an inclination to stipulate associate degree knowledge entropy-based diversity constant thus on characterizes the 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.

Index Terms—Behavior profile & e-commerce security, Face Detection, Invisible Keyboard Sequence, fraud detection, on-line dealings.

I. INTRODUCTION:

The volume of the electronic dealing has rise significantly in recent years due to the popularization of on-line looking (e.g., Amazon, eBay, and Alibaba). the worldwide e-commerce market is anticipated that it will be worth a staggering u. s. twenty four trillion by 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 transaction. 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.

II. Objective

To evaluate as well as compare the merits of existing and future Transaction of accounts. To support multi-user environment and fully automated. To track fraud is using Face detection and virtual keyboard. This project is to detect ,analyze the transaction fraud and provide multiple solution like invisible keyboard to avoid fraud transaction.

III. Problem Statement

In the recent days the bank fraud is most headache problems faced by many person. Many people store their password and personal information very confidential but sometimes is may be stolen by someone unexpectedly and then we faced the many problem by that time and get a loss by financial. To face this problem we introduced the Transaction Fraud Detection Using Face Authentication And Invisible VirtualKeyboard in ML . By using the face recognition we optimize the fraud detection from the unwanted person. It will help us to protect our information very confidential and manage all the account details with our virtual keyboard and Face detection

IV. LITERATURE SURVEY:

1. Paper Name: Face Recognition and Detection using Viola-Jones and Cross Correlation Method
Author Name: Ranjeet Singh, Mandeep Kaur
Description: The face detection is method of detection region of face from an image of 1 or multiple persons along. The detected face is extracted within the planned victimisation the viola-Jones algorithmic rule. The viola-Jones algorithmic rule is taken into account effective so as to mark and extract the face options. The planned model is victimisation the correlation model for the aim of the face recognition. The face recognition method will sight the person among the information of faces while not knowing the other details concerning the person specific. The planned face detection and recognition model will be deployed anyplace it's needed. The results have shown the effectiveness of the proposed model.

2. Paper Name:Review and Comparison of Face Detection Algorithms
Author Name: Kirti Dang, Shanu Sharma
Description: With the tremendous increase in video and image info there's a good would like of automatic understanding and examination of information by the intelligent systems as manually it's changing into out of reach. Narrowing it all the way down to one specific domain, one among the foremost specific objects that may be copied within the pictures area unit individuals i.e. faces. Face detection is changing into a challenge by its increasing use in range of applications. it's the primary step for face recognition, face analysis and detection of alternative options of face. during this paper, varied face detection algorithms area unit mentioned and analyzed like Viola-Jones, SMQT options & SNOW Classifier, Neural Network-Based Face Detection and Support Vector Machine-Based face detection. of these face detection ways area unit compared supported the preciseness and recall worth calculated employing a DetEval package that deals with précised values of the bounding boxes round the faces to administer correct results.

3. Paper Name: CNN-based Real-time Dense Face Reconstruction with Inverse-rendered Photo-realistic Face Images
Author Name:YudongGuo, JuyongZhangy, JianfeiCai, Boyi Jiang and Jianmin Zheng.
Description: This paper presents a unique face knowledge generation method. Specifically, we

have a tendency to render an outsized range of photo-realistic face pictures with completely different attributes supported inverse rendering. what is more, we have a tendency to construct a fine-detailed face image dataset by transferring completely different scales of details from one image to another. we have a tendency to additionally construct an outsized range of video-type adjacent frame pairs by simulating the distribution of real video knowledge With these nicely created datasets, we have a tendency to propose a coarse to-fine learning framework consisting of 3 convolutional networks. The networks are trained for period of time elaborated 3D face reconstruction from monocular video furthermore as from one image. in depth experimental results demonstrate that our framework will turn out high-quality reconstruction however with a lot of less computation time compared to the progressive. Moreover, our methodology is powerful to cause, expression and lighting because of the range of knowledge.

4. Paper Name:Secure Transaction By Using Wireless Password with Shuffling Keypad
Author Name:Shweta Jamkavale, Ashwini Kute, Rupali Pawar, Komal Jamkavale, Prashant Jawalkar.
Description: In general, all swiping card authentication system having completely different potentialities of secret dead reckoning by mean of shoulder surf riding is AN attack and commanding attack. This downside are often overcome with new advance resolution by coming up with shuffled input device that displays the shuffled variety on user's screen, that is difficult to acknowledge for the one who stand close to you to guess the secret. the most purpose of this technique is to develop a secure ATM PIN in future for group action purpose and the group action notification directly goes to the user's application and request PIN to user rather than merchant's hardware machine.

5. Paper Name: Face Frontalization Using an Appearance-Flow-Based Convolutional Neural Network
Author Name: Zhihong Zhang , Xu Chen, Beizhan Wang, Guosheng Hu , WangmengZuo , Senior Member, IEEE,and Edwin R. Hancock.
Description: Facial create variation is one among the main factors making face recognition (FR) a difficult task. One standard solution is to convert non-frontal faces to frontal ones on that FR is performed. Rotating faces causes facial picture element price changes. Therefore, existing CNN-based ways learn to synthesize frontal faces in color house. However, this learning drawback in an exceedingly color house is very non-linear, inflicting the artificial frontal faces to lose fine facial textures. during this paper, we tend to take the view that the non frontal-frontal picture element changes area unit basically caused by geometric transformations (rotation, translation, and so on) in house. Therefore, we tend to aim to find out the non frontal-frontal facial conversion within the spatial domain instead of the color domain to ease the training task. to the current finish, we tend to propose associate degree appearance-flow-based face formalization convolutional neural network(A3F-CNN). Specifically, A3F-CNN learns to determine the dense correspondence between the non-frontal and frontal faces. Once the correspondence is constructed, frontal faces area unit synthesized by expressly "moving" pixels from the non-frontal one. In this way, the artificial frontal faces will preserve fine facial textures. To improve the convergence of coaching, associate degree appearance-flow guided learning strategy is planned. additionally, generative adversarial network loss is applied to attain a lot of photo realistic face, and a face mirroring technique is introduced to handle the self-occlusion drawback. in depth experiments area unit conducted on face synthesis and create invariant atomic number 87. Results show that our technique will synthesize a lot of photorealistic faces than the existing ways in each the

controlled and un controlled lighting environments. Moreover, we tend to reach a awfully competitive FR performance on the Multi-PIE, LFW and IJB-A databases.

V. EXISTING SYSTEM:

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 methodology the fraud dealings is up to the mark.

Disadvantages**:**

- Multiple times generate duplicate signature by someone.
- Only OTP verification is available on mobile

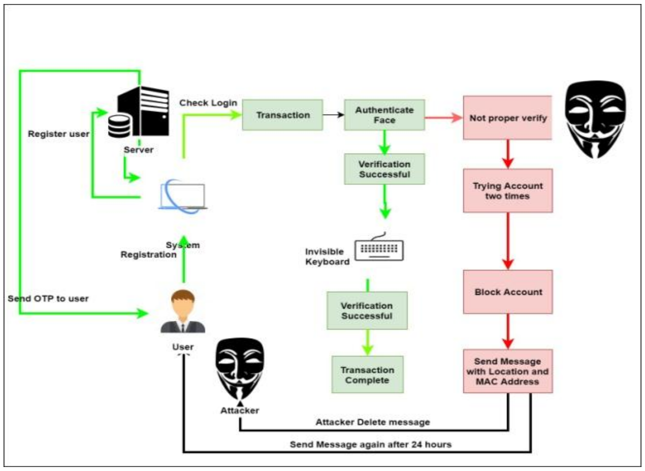
VI. PROPOSED SYSTEM:

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 voialo 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.

Advantages:

- Reduction among the range of fraud detection.
- Added layer of security.
- The detection of the fraud use of the cardboard is found plethoric faster that the prevailing system.

VII. SYSTEM ARCHITECTURE:



VIII. 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 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.

IX. ALGORITHM DETAILS:

- **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 step 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.

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 Markov 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.

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]Kirtissssss 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]Zhihong 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, Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data, IEEE Trans. Comput. Social Syst., vol. 1, no. 2, pp. 135155, Jun. 2014.

[7] V. Bhusari and S. Patil, Application of hidden Markov model in credit card fraud 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 fraud detection, 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. ss13–20, 2006.