Transaction Fraud Detection using Invisible Keyboard and Face Detection

Abhishek B Jagdale, Ketan J Agawane, Suyog D Malusare, Ravindra C Hase , Prof. Rahul Kadam
Information Technology, D Y Patil College of Engineering, Ambi

Abstract: With the popularization of on-line trying, dealings fraud is growing seriously. Therefore, the study on fraud detection is attention-grabbing and vital. a big manner of police work fraud is to extract the behavior profiles (BPs) of users supported their historical dealings records, thus to verify if associate incoming dealings is additionally 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's 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 those behaviors. Throughout this paper, we've an inclination to propose logical graph of BP (LGBP) which will be an entire order-based model to represent the relation of attributes of dealings records. Supported LGBP and users dealings records, we tend to square measure ready to cipher a path-based transition likelihood from associate attribute to a definite one. Here we tend to square measure ready 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 knowledge entropy-based diversity constant thus on characterizes the variability of dealings behaviors of a user. we've an inclination to additionally track fraud user with location by mackintosh address of the user laptop pc transportable or computer that have last dealings successfully. additionally , we've an inclination to stipulate a state transition likelihood matrix to capture temporal choices of transactions of a user. Consequently, we tend to square measure ready to construct a BP for every user thus use it to verify if associate incoming dealings is additionally a fraud or not. Our experiments over a true 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:

At present, Markov chains and their extensions are often used because the models of personalized transaction BP [1], [2], [3], [4], [5], [6]. the most idea of Markov chain model of fraud detection is that some attribute values of transaction records (e.g., transaction amount and category of goods) are because the nodes of a model and therefore the transition probabilities among those nodes are wont to quantify the transaction behavior features. Markov chain models are good at describing their BPs for those users whose transaction behaviors are stable, and our experiences also prove this. However, with the event and popularization of online shopping, the transaction behaviors of a user vary often then her/his BP should be ready to characterize transaction diversity. Therefore, Markov chain models aren't too suitable for those users. during this paper, we propose a replacement model to represent a user's BP under considering behavior diversity, then present a fraud detection method supported this new model.

Face recognition (FR) may be a highly topical research direction in computer vision. Recently, significant progress has been achieved in face recognition using deep learning methods and enormous database of labeled face images. However, face recognition remains a challenging problem in uncontrolled lighting environments, and especially , within the presence of huge pose variations. Specifically, strong pose variations significantly decrease the accuracy of the evaluated methods. As verified in [7]–[9], pose may be a major factor for reducing the accuracy. As a result, Pose Invariant Face Recognition (PIFR) has attracted great interest. Research into PIFR are often categorized into two areas a) Latent Space Learning (LSL) and b) Analysis-by-

Synthesis (AbS). LSL methods are essentially general metric learning techniques from computer vision. During training, LSL methods project the features extracted from input images under various poses into a standard space [7], [8] where the image features of an equivalent identity are clustered together but otherwise are distant from each other . During testing, the test face features are mapped to an equivalent latent space for recognition. The features are often hand-crafted or learned. Handcrafted features (SIFT [9], HOG [10], Gabor [11], LBP [12], etc.) aim to capture pose-invariant information, but their performance isn't very promising. Learning-based methods, mainly deep learning methods [13]–[17], are able to do more robust PIFR performance across different poses. Hand-crafted features behave just like the features from shallow layers of deep learning, which may achieve a low-level of robustness. Unlike hand-crafted features, the deeper layers can capture more abstract and robust information across different poses. Although LSL methods achieve promising performance, PIFR is conducted during a latent space, which is sort of a recorder and makes the intermediate representation less interpretable. With in the world , the interpretability or visualization of the popularity process is vital in many practical applications, like enforcement and visually identifying suspects.

II. LITERATURE SURVEY:

1. Paper Name: Fraud detection system:
A survey
Author Name: A. Abdallah, M. A. Maarof, and A. Zainal
Description: The increment of technology use and therefore the continued growth of companies have enabled most financial transactions to be performed through the electronic commerce systems, like using the credit card system, telecom system, healthcare insurance system, etc. Unfortunately, these systems are employed by both legitimate users and fraudsters. Additionally, fraudsters utilized different approaches to breach the electronic commerce systems. Fraud prevention systems (FPSs) are insufficient to supply adequate security to the electronic commerce systems. However, the collaboration of FDSs with FPSs might be effective to secure electronic commerce systems. Nevertheless, there are issues and challenges that hinder the performance of FDSs, like concept drift, supports real time detection, skewed distribution, great deal of knowledge etc. This survey paper aims to supply a scientific and comprehensive overview of those issues and challenges that obstruct the performance of FDSs. we've selected five electronic commerce systems; which are master card, telecommunication, healthcare insurance, car insurance and online auction.

2. Paper Name: Frontal to Profile Face Verification in the Wild
Author Name: Soumyadip Sengupta , Jun-Cheng Chen , Carlos Castillo , Vishal M. Patel , Rama Chellappa , and David W. Jacobs
Description: We have collected a replacement face data set which will facilitate research within the problem of frontal to profile face verification ‘in the wild’. The aim of this data set is to isolate the factor of pose variation in terms of utmost poses like profile, where many features are occluded, along side other ‘in the wild’ variations. We call this data set the Celebrities in Frontal-Profile (CFP) data set. we discover that human performance on Frontal-Profile verification during this data set is only slightly worse (94.57% accuracy) than that on Frontal Frontal verification (96.24% accuracy). However we evaluated many state-of-the-art algorithms, including Fisher Vector, Sub-SML and a Deep learning algorithm. We observe that each one of them degrade quite 10% from FrontalFrontal to Frontal-Profile verification. The Deep learning implementation, which performs like humans on Frontal-Frontal, performs significantly worse (84.91% accuracy) on Frontal-Profile. this means that there's a niche between human performance and automatic face recognition methods for giant pose variation in unconstrained images.

3. Paper Name: A comprehensive survey on pose-invariant face recognition,
Author Name: C. Ding and D. Tao,
Description: The capacity to acknowledge faces under varied poses may be a fundamental human ability that presents a singular challenge for computer vision systems. Compared to frontal face recognition, which has been intensively studied and has gradually matured within the past few decades, Pose-Invariant Face Recognition (PIFR) remains a largely unsolved problem. However, PIFR is crucial to realizing the complete potential of face recognition for real-world applications, since face recognition is intrinsically a passive bio-metric technology for recognizing uncooperative subjects. during this article, we discuss the inherent difficulties in PIFR and present a comprehensive review of established techniques. Existing PIFR methods are often grouped into four categories, that is, pose-robust feature extraction approaches, multi view subspace learning approaches, face synthesis approaches, and hybrid approaches. The motivations, strategies, pros/cons, and

performance of representative approaches are described and compared. Moreover, promising directions for future research are discussed

4. Paper Name: Semantic facial expression editing using autoencoded flow
Author Name : R. Yeh, Z. Liu, D. B. Goldman, and A. Agarwala. (2016).
Description: High-level manipulation of facial expressions in images like changing a smile to a neutral expression is challenging because countenance changes are highly non-linear, and vary counting on the looks of the face. We present a totally automatic approach to editing faces that combines the benefits of flow-based face manipulation with the newer generative capabilities of Variational Autoencoders (VAEs). During training, our model learns to encode the be due one expression to a different
over a low-dimensional latent space. At test time, expression editing are often done simply using latent vector arithmetic. We evaluate our methods on two applications: 1) single-image countenance editing, and 2) countenance interpolation between two images. We demonstrate that our method generates images of upper perceptual quality than previous VAE and flow-based methods.

5. Paper Name: Deepwarp: Photorealistic image resynthesis for gaze manipulation
Author Name: Y. Ganin, D. Kononenko, D. Sungatullina, and V. Lempitsky, “
Description: In this work, we consider the task of generating highly realistic images of a given face with a redirected gaze. We treat this problem as a selected instance of conditional image generation and suggest a replacement deep architecture which will handle this task alright as revealed by numerical comparison with prior art and a user study. Our deep architecture performs coarse-to-fine warping with a further intensity correction of individual pixels. of these operations are performed during a feed-forward manner, and therefore the parameters related to different operations are learned jointly within the end-to-end fashion. After learning, the resulting neural network can synthesize images with manipulated gaze, while the redirection angle are often selected arbitrarily from a particular range and provided as an input to the network.

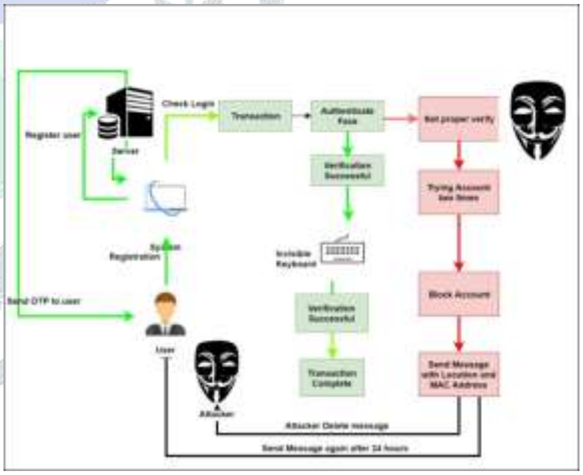
III. PROPOSED SYSTEM:

We propose logical graph of BP (LGBP) that might be an entire order-based model to represent the relation of attributes of dealings records. Supported LGBP and users’ dealings records, we are getting to reckon a path-based transition likelihood from associate attribute to a singular one. Here we are getting to notice Face by exploitation voialo jones and LBP acknowledge rule for face detection we've a bent to tend use invisible keyword sequence for authentication of OTP. The keyword sequence modification whenever. At a uniform time, we've a bent to tend to stipulate associate information entropy-based diversity constant therefore on characterize the vary of dealings behaviors of a user. to boot, we've a bent 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.

IV. SYSTEM ARCHITECTURE:



V. MATHEMATICAL MODEL

- Let S be the system
- P={I,P,O}
- Where,
- I= Input(Users, Attacker)

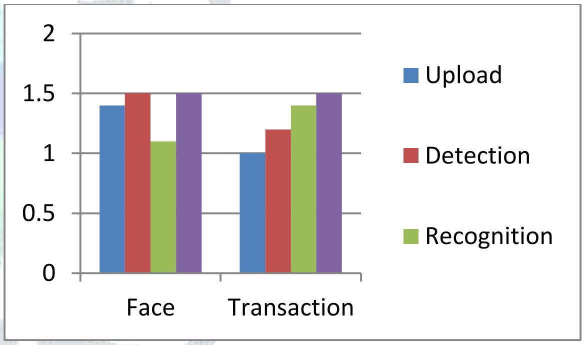
- P={Setup, Trans, OTP, Detect Fraud, send MSG}
- Setup={U}
- U={u1, u2, …., un}
- U: No of Users
- KeyGen(OKpri; TKpri)
- OKpri=User Private Key
- TKpri=User Transaction Identity
- Trans= {t1, t2, …., tn}
- Trans: No of transaction done by users
- User can do transaction by using OTP or secret Key, 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.

VI. 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.

VII. RESULTS AND SCREEN SHOTS:



Type/Time in ms	Upload	Detection	Recognition	Invisible Keyboard
Face	1.4	1.5	1.1	1.5
Transaction	1	1.2	1.4	1.5

Screen Shots

CONCLUSION:

In this project, we have got a bent to propose the only thanks to extract users bits per second supported their dealing records, that's utilized to hunt out dealing fraud at intervals the on-line searching scenario by using the face detection. Overcomes the defect of Markov process models since it characterizes vary of user behaviors. Experiments together illustrate the advantage of OM. the end of the day work focuses on some machine-learning ways in which to automatically classify the values of trans- action attributes so as that our model can characterize the users bespoke behavior a lot of specifically. Additionally, we have got a bent to decide to extend BP by considering totally different data like users comments.

REFERENCES:

[1] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

[2] S. Sengupta, J.-C. Chen, C. Castillo, V. M. Patel, R. Chellappa, and D. W. Jacobs, "Frontal to profile face verification in the wild," in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Mar. 2016, pp. 1–9.

[3] C. Ding and D. Tao, "A comprehensive survey on pose-invariant face recognition," ACM Trans. Intell. Syst. Technol., vol. 7, no. 3, p. 37, 2016.

[4] R. Yeh, Z. Liu, D. B. Goldman, and A. Agarwala. (2016). "Semantic facial expression editing using autoencoded flow." [Online]. Available: https://arxiv.org/abs/1611.09961

[5] Y. Ganin, D. Kononenko, D. Sungatullina, and V. Lempitsky, "Deepwarp: Photorealistic image resynthesis for gaze manipulation," inProc. 14th Eur. Conf. Comput. Vis. Amsterdam, The Netherlands: Springer, 2016, pp. 311–326.

[6] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jun. 2005, pp. 886–893.

[7] J. G. Daugman, "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters," J. Opt. Soc. Amer. A, Opt. Image Sci., vol. 2, no. 7, pp. 1160–1169, 1985.

[8] T. Ahonen, A. Hadid, and M. Pietikäinen, "Face description with local binary patterns: Application to face recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[9] Z. Zhu, P. Luo, X. Wang, and X. Tang, "Multi-view perceptron: A deep model for learning face identity and view representations," in Proc. 27th Int. Conf. Neural Inf. Process. Syst. (NIPS), 2014, pp. 217–225. [10] B. Egger, S. Sch¨onborn, A. Schneider, A. Kortylewski, A. Morel-Forster, C. Blumer, and T. Vetter. Occlusion-aware 3d morphable models and an illumination prior for face image analysis. International Journal of Computer Vision, 2018.

[11] R. Garg, A. Roussos, and L. Agapito. Dense variational reconstruction of non-rigid surfaces from monocular video. In IEEE Conference on Computer Vision and Pattern Recognition, pages 1272–1279, 2013.

[12] C. Ledig et al. (2016). "Photo-realistic single image superresolution using a generative adversarial network." [Online]. Available: https://arxiv.org/abs/1609.04802

[13] C. Li and M. Wand, "Combining Markov random fields and convolutional neural networks for image synthesis," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2016, pp. 2479–2486.

[14] X. Yu and F. Porikli, "Face hallucination with tiny unaligned images by transformative discriminative neural networks," in Proc. 31st AAAI Conf. Artif. Intell., 2017, pp. 4327–4333.

[15] K. He, X. Zhang, S. Ren, and J. Sun, "Identity mappings in deep residual networks," in Proc. 14th Eur. Conf. Comput. Vis. Amsterdam, The Netherlands: Springer, 2016, pp. 630–645.