CREDIT CARD READER WITH FACE RECOGNITION ON WEBCAM

Pooja More, Vishakha Thorat, Radhika Khandagle, Rutuja Sankpal

SKNSITS, Lonavala, India

ABSTRACT

In today's world the credit card fraud is the biggest issue and now there is need to combat against the credit card fraud. "Credit card fraud is the process of cleaning dirty money, thereby making the source of funds no longer identifiable." On daily basis, the financial transactions are made on huge amount in global market and hence detecting credit card fraud activity is challenging task. As earlier (Anti- credit card fraud Suite) is introduced to detect the suspicious activities but it is applicable only on individual transaction not for other bank account transaction. To Overcomes issues of we propose Machine learning method using 'Structural Similarity', to identify common attributes and behaviour with other bank account transaction. Detection of credit card fraud transaction from large volume dataset is difficult, so we propose case reduction methods to reduces the input dataset and then find pair of transaction with other bank account with common attributes and behaviour.

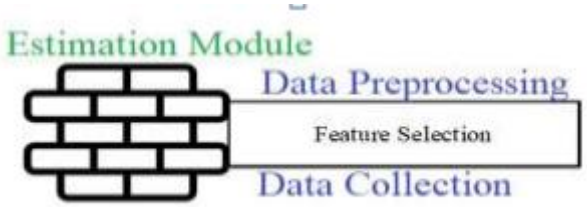
Keywords— Machine Learning, Raspberry Pi

INTRODUCTION

Credit card fraud scrub as much as 5 of the world's GDP (Gross Domestic Product.) every year. Combating credit card fraud using AI is to detect the suspicious activities. Combating credit card fraud typically requires most entities that complete financial transactions to keep thorough records of their clients' accounts and activities. If they come across any information that appears to be suspicious, they are required to report it to the government for further investigation. In this Transaction records is check to detect credit card fraud activity if the suspicious data is detected. Here we use Artificial Intelligence and Machine Learning Algorithm to detect the suspicious activities and solve it by training the data of that activity. We are going to use supervised and unsupervised algorithm techniques. Credit card Reader has been around for years now and with time, the model has grown stronger and better with each passing day.built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

DATASET AND METHODOLOGY

In this section, we introduce the Capture Image dataset that we have used in our machine learning experiments. The pre-processing procedures that we have made to the data before doing the machine learning tasks will be discussed. As shown in figure below:



METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY ISSUES AND OUTCOME

In this project we are using Haar cascade algorithm. And using Raspberry pie .then also used Figure print and RFID. RFID is used for After the Figure print Authenticate. The system can use the HTTP protocol for communication over the Internet and for the intranet communication will be through TCP/IP protocol suite. proceedings, and not as an independent document. Please do not revise any of the current designations.

OBJECTIVES

1. Opportunity to build credit. 2. Earn rewards such as cash back or miles points. 3. Protection against credit card fraud. 4. Free credit score information. No foreign transaction fees. 5. Increased purchasing power. Not linked to checking or savings account. 6. Putting a hold on a rental car or hotel room.

Motivation

We can identify and group potential credit card fraud accounts. The goal is to develop a Desktop application which can detect classify the tweets on the basis of text as well as images it contains during disastrous situations into informative and non-informative categories using Haar Cascade Algorithm. User friendly system. We can identify and group potential credit card fraud accounts.

Math Model

S=I, P, O.
Where,
S=System
I=Input
P=Procedure
O=Output.
I= {CD, F, PI} Where,

CD=Card Details,
F=Face capture,
PI=Personal Information.

Procedures:-

Step1:-User The user will do the registration, enter the required card details, Personal Information and the images of face registration will be successful.

User= {CD, F, PI}.
CD=Card Details,
PI=Personal Information,
F=Face.

Step2:-Admin The admin will add the account, view the account, and View the blocked account.

Admin= {AA, VA, VBA}
Where,
AA=Add account,
VA=View account,
VBA=View blocked account.

Output:- Verification of face the time payment, if the face matches then the payment successful and if the face doesn't matches then the payment is not successful.

Authors and Affiliations

1. **Paper Name:** - A Survey on Hidden Markov Model for Credit Card Fraud Detection**.**

   Author Name: - Anshul Singh, Devesh Narayan.

   Affiliations - Credit card frauds are increasing day by day regardless of the various techniques developed for its detection. Fraudsters are so expert that they engender new ways for committing fraudulent transactions each day which demands constant innovation for its detection techniques as well. Many techniques based on Artificial Intelligence, Data mining, Fuzzy logic, Machine learning, Sequence Alignment, decision tree, neural network, logistic regression, nave Bayesian, Bayesian network, metal earning, Genetic Programming etc., has evolved in detecting various credit card fraudulent transactions. A steady indulgent on all these approaches will positively lead to an efficient credit card fraud detection system. This paper presents a survey of various techniques used in credit card fraud detection mechanisms and Hidden Markov Model (HMM) in detail. HMM categorizes card holder's pole as low, medium and high spending based on their spending behavior in terms of amount. A set of probabilities for amount of transaction is being assigned to each cardholder. Amount of each incoming transaction is then matched with card owners category, if it justifies a predefined threshold value then the transaction is decided to be legitimate else declared as fraudulent.

2. **Paper Name:** Techniques for key point detection and matching between endoscopic images.

   Author Name: Loureno, Antnio Migue. Description: - The detection and description of local image features is fundamental for different computer vision applications, such as object recognition, image content retrieval, and structure from motion. In the last few years the topic deserved the attention of different authors, with several methods and techniques being currently available in the literature. The SIFT algorithm, proposed in, gained particular prominence because of its simplicity and invariance to common image transformations like scaling and rotation. Unfortunately the approach is not able to cope with non-linear image deformations caused by radial lens distortion. The invariance to radial distortion is highly relevant for applications that either require a wide field of view (e.g. panoramic vision), or employ cameras with specific optical arrangements enabling the visualization of small spaces and cavities (e.g. medical endoscopy). One of the objectives of this thesis is to understand how radial distortion impacts the detection and description of key points using the SIFT algorithm. We perform a set of experiments that clearly show that distortion affects both the repeatability of detection and the invariance of the SIFT description. These results are analyzed in detail and explained from a theoretical viewpoint. In addition, we propose a novel approach for detection and description of stable local features in images with radial distortion. The detection is carried in a scale-space image representation built using an adaptive Gaussian that takes into account distortion, and the feature description is performed after implicit gradient correction using the derivative chain rule. Our approach only requires a rough modeling of the radial distortion function and, for moderate levels of distortion, it outperforms the application of the SIFT algorithm after explicit image correction.

3. **Paper Name:** - Credit Card Fraud Detection Using Hidden Markov Model and Its Performance.

   Author Name: - Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun Majumdar.

   Affiliations:-Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In this paper, we model the sequence of operations in credit card transaction processing using a hidden Markov model (HMM) and show how it can be used for the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature.

   4. Paper Name: - A Comprehensive Survey of Data Mining-based Fraud Detection Research.
   Author Name: - CLIFTON PHUA1, VINCENT LEE1 , KATE SMITH1 ROSS GAYLER2.

   Affiliations :- This survey paper categorizes, compares, and summarizes from almost all published technical and review articles in automated fraud detection within the last 10 years. It defines the professional fraudster, formalizes the main types and subtypes of known fraud, and

presents the nature of data evidence collected within affected industries. Within the business context of mining the data to achieve higher cost savings, this research presents methods and techniques together with their problems. Compared to all related reviews on fraud detection, this survey covers much more technical articles and is the only one, to the best of our knowledge, which proposes alternative data and solutions from related domains. **5. Paper Name:** - Image Based Fraud Prevention.

Author Name: - D. Madhu Babu, M. Bhagyasri, K. Lahari, CH. Madhuri, G. Pushpa Kumari.

Affiliations: - Multiple validations of printed documents incorporating image information and authorizing data on a printed document assist in the printed document validation process. This technique requires the authorized document holder to have an image identification accompany the application or production of the document. Image information is converted to a storable image that is used in one of a plurality of validating schemes that assures that the presenter of the printed document is not a substitute. Such schemes included visual comparison of the printed document presenter and extracted image in- formation and validation that the data has not been altered. Non-reversible encryption of the data, as it is read from the document at the document presentation site is used to formulate encoded authorization data that is then compared against like encoded authorized document holder data stored at a centrally located data base.

ACKNOWLEDGMENT

Finally, it is concluded that The Credit card is an intrinsically secure device. Credit cards have proven to be useful for media. Eventually replacing all of the things we carry around in our wallets, including credit cards. The credit card can be an element of solution to a security problem in the modern world.

REFERENCES

[1] R. Dhanpal and P. Gayathiri, Credit card fraud detection using decision tree for tracing email and ip", International Journal of Computer Science Issues, Vol. 9, no. 2, 2012.

[2] R. Patidar and L. Sharma, Credit Card Fraud Detetion Using Neural Network, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-1, Issue-NCAI2011, June 2011.

[3] A. Srivastava and A. Kundu, Credit card fraud detection using hidden markov model", IEEE Transactions on Dependable and Secure Computing, Vol. 5, no. 1, 2008.

[4] K. P. Adhiya and Dinesh L. Talekar, Credit card fraud detection, International Journal of advanced studies in Computer Science, Issue 3, 2015.

[5] V. Bhusari and S. Patil, Study of hidden markov model in credit card fraudulent detection", International Journal of Computer Applications, vol. 2, no. 5, 2011.

[6] R. D. Patel and D. K. Singh, Credit card fraud detection prevention of fraud using genetic algorithm", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 6, 2013.

[7] K.RamaKalyani and D.UmaDevi, Fraud detection of credit card payment system by genetic algorithm", International Journal of Scientific Engineering Research, vol. 3, no. 7, 2012.