Detect Credit Card Fraud Using Machine Learning Model

Prof. Dr.Mahesh Navale[1] , Mrudula Prasad Dawalbhakta[2],

Pallavi Sakharam Chavhan[3]

1,2,3,Department of Computer Engineering, Zeal College of Engineering and Research,Pune, India

---***---

Abstract -With the surge in online transactions, credit card fraud has become a significant issue, demanding efficient solutions for early detection and prevention. The rise in digital transactions has increased the demand for robust fraud detection systems. This project aims to develop a hybrid fraud detection system that integrates facial recognition technology with behavioral analysis to enhance security in credit card transactions.

The system employs facial recognition algorithms, including Haar Cascades, Local Binary Patterns (LBP) to verify user identity. When a user initiates a transaction or logs in, their facial image is captured and compared to previously stored data using feature extraction techniques. Additionally, the system analyzes behavioral data, such as login times, transaction locations, and spending habits, to identify anomalies indicative of fraud. By leveraging machine learning algorithms such as Support Vector Machines (SVM), CNNs the system learns from historical data and adapts to emerging patterns. This two-step verification process requires both a valid facial match and consistent user behavior, significantly reducing false positives and negatives.

Key Words: Face Recognation Technology, Credit Card Fraud Detection, Haar Cascades, Support Vector Machine (SVM), CNNs, Two-Step Verification, Real-Time Authentication, Data Security.
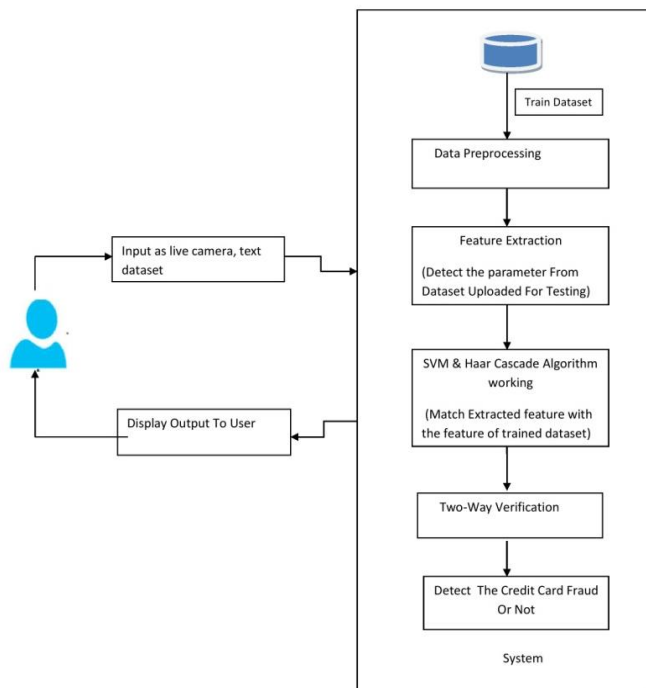
1. INTRODUCTION

Credit card fraud is a pervasive and evolving challenge in the modern financial landscape. As electronic transactions become increasingly prevalent, the need for robust fraud detection mechanisms becomes paramount. Traditionally, credit card fraud detection has relied on transaction data analytics, machine learning algorithms, and anomaly detection techniques. Credit card fraud, in particular, has emerged as a significant threat to both consumers and financial institutions. Traditional fraud detection systems primarily rely on analyzing transactional data, identifying irregular patterns to flag potentially fraudulent activities. However, these methods often fall short when it comes to detecting unauthorized access by fraudulent users, leading to financial losses and compromised user trust.

To address these challenges, this project proposes a hybrid fraud detection system that integrates facial recognition technology with behavioral analysis. By combining these two approaches, the system enhances security in credit card transactions, providing a robust defense against fraudulent activities. Facial recognition serves as a vital layer of user authentication, ensuring that the person attempting to access the account is indeed the legitimate cardholder. Meanwhile, behavioral analysis assesses user behavior patterns—such as login times, transaction locations, and spending habits—allowing the system to detect anomalies indicative of potential fraud.

Utilizing advanced machine learning algorithms, including Support Vector Machines (SVM), Convolutional Neural Networks (CNNs), the proposed system learns from historical data and adapts to emerging fraud patterns. This two-step verification mechanism not only improves the accuracy of fraud detection but also fosters user trust by ensuring secure transactions.

2. SYSTEM DESIGN

Haar Cascade is a Machine Learning algorithm mainly used for detection of objects. But in our project we are going to implement face recognition technology using haar cascade. Haar cascade will help us in hypothetical analysis . Haar cascade will be used in image processing for using our credit card fraud detection system. Haar cascade algorithm will mainly capture the facial parameters of the user using the system. This will help in data authenticity and security.

1.Preprocessing the data: Pre- processing the data collected from users that can be in the form of their transaction details and credit card information.

2.Feature Extraction: Feature Extraction transforms an arbitrary data, such as text or images, into numerical features that is understood by machine learning algorithms.

3.Haar Cascade & SVM Algorithm: This algorithm is used to identify the images and the facial parameters. The distinct facial features are extracted which can be used for the further analysis.

4.Two-Way Verification: Approve or deny transactions based on both facial verification and SVM classification.

5.Detect the fraud or not: Based on the transactions of the user ,if a transaction exceeds a certain limit or a high value transaction occurs then the system will detect it as a fraud.

3. TECHNIQUES FOR CREDIT CARD FRAUD

we propose a two-way verification system for credit card fraud detection by integrating Support Vector Machine (SVM) for transactional analysis with facial recognition technology.

SVM algorithm analyzes transaction data based on historical patterns, distinguishing legitimate transactions from potentially fraudulent ones.

facial recognition uses Haar Cascade Classifiers to verify the user's identity, comparing real-time facial features with stored images. This dual-layered approach improves accuracy and minimizes false positives and negatives.

This system is designed for real-time applications in online banking and e-commerce, fostering customer trust by ensuring only authorized users can conduct transactions.

4. FUTURE SCOPE

The System enhances the use of facial recognition technology and two step verification process in detecting fraud.

1.Advanced Algorithms for Facial Recognition: Machine learning and deep learning algorithms for high-level recognition.

2.Awareness regarding use of two-step verification: The importance of two-step verification process for the accuracy and efficient working of system.

3.User friendly system: Allowing users to ask queries or questions related to Generation of OTP, other verification process.

4.Behavourial analysis: Tracking users way of interacting with their devices which will additional security to system's data.

5. CONCLUSION

We have implemented the credit card fraud detection system using face recognition technology and two step verification. Our system offers complete security to data as the verified users can access the system only. After verification of the user's identity and tracking their transaction details, analysis regarding the frauds committed are made. The additional way of including two-step verification process in fraud detection systems is successfully implemented. Next by taking advantage of

structural similarity, we can identify and group potential Credit card accounts. Our model is based on machine learning algorithm's efficient used and results are predicted based on the accuracy.

6. ACKNOWLEDGEMENT

REFERENCES

[1] Nasir Ayub (2023) "Online Payment fraud detection using machine learning techniques, IEEE."

[2] Amit Kumar Sah (2022)"Authentication of credit card using facial recognition"

[3] Dhanmiga S (2022) "Credit Card Fraud Detection and Prevention using Face Authentication",IJRPR.

[4] Nobert Jere(2024) "Deep learning for credit card fraud detection, IEEE."

[5] Fawaz Khaled Alarfaj,Iqra Malik(2022) "Credit Card Fraud Detection using State of Art Machine Learning and Deep learning Algorithms, IEEE."

[6] Ashwini.M.Zinjurde, Vilas.B.Kamble(2021) "Credit card Fraud Prevention by facial recognition,IEEE."

[7] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten(2014) "Improving credit card fraud detection with calibrated probabilities,SDM"