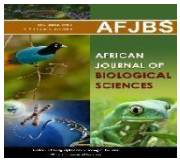
https://doi.org/10.48047/AFJBS.6.15.2024.1148-1154

African Journal of Biological Sciences



Research Paper Open Access

Credit Card fraud detection with optimized flower pollination and temporal CNN

Jayapradha J [1], Palanivel N [2], Nandhini R[3], Swethaa P [4], Haripriya S [4]

[1]Assistant Professor, [2]Professor, Department of Computer Science Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India

[2, 3,4]UG Scholar, Manakula Vinayagar Institute of Technology, Puducherry, India.

Volume 6, Issue 15, Sep 2024

Received: 15 July 2024

Accepted: 25 Aug 2024

Published: 05 Sep 2024

doi: 10.48047/AFJBS.6.15.2024.1148-1154

Abstract-In order In the era of digital finance, credit card fraud detection has become a critical issue for financial institutions and consumers alike. This study proposes a novel approach to credit card fraudulent classification by integrating a Stacked Convolutional Neural Network (CNN) with the Flower Pollination Algorithm (FPA). The Stacked CNN is the deep learning model that leverages multiple layers of CNNs to extract complex patterns from data, making it highly effective for image and pattern recognition tasks.The Flower Pollination Algorithm, inspired by the natural process of pollination, is a Meta heuristic optimization algorithm that has shown promising results in various optimization problems. The proposed methodology combines the strengths of both the Stacked CNN and the FPA to create a robust framework for credit card fraud detection. The Stacked CNN is employed to analyze transaction data, identifying patterns indicative of fraudulent activities. The FPA is then used to optimize the CNN's parameters, ensuring that the model is not only accurate but also efficient in its detection capabilities.Through extensive experiments and comparisons with traditional machine learning models, this study demonstrates that the integration of Stacked CNN with FPA significantly improves the accuracy and efficiency of credit card fraud detection.The proposed methodology not only outperforms existing models in terms of detection accuracy but also reduces the computational complexity, making it a practical solution for real-world applications.This research contributes to the ongoing efforts to enhance security measures in the financial sector and provides a foundation for further research in the application of deep learning and optimization algorithms in fraud detection.

Keywords: Hybrid, credit card, CNN, FPA, Deep learning.

I. Introduction

The primary objective of this research project is to recognizecreditcard transactionsthatarefraudulent. This can only be achieved by categorizing the transactions as fraudulent ornot. Themajoraim is to create a fraud detection algorithm which can quickly and accurately identify fraudulent transactions using machine learning-based classification algorithms. Rapid technological advancements have led to a decrease in cash payments and an increase in online payments, which has allowed fraudsters to conduct anonymous transactions.

Certainonlinepaymentmethodsonlyrequirethecard number, expiration date, and CVV; however, those details may be lost without our knowledge or awareness. In certain situations, we may not even be awarethatourinformationisbeingstolen.Evenafter making purchases online, when scammers utilize phishing tactics to obtain personal information, we have been unaware that our information was compromised.Heonlyrequiresthedetailsofthecard for a few purchases to perform fraud, and the user might not be aware by which their information of credit card was compromised. It is best to keep

The card details confidential.But occasionally, we have no control over it. Phishing websites have the potential to leak information, and occasionally the card itself might get stolen & lost. The most effective technique to establish whether a transaction isFraudulent or not is to utilize machine learning to establish the patterns of customer spending using already-existing data

II. Literature Review

Credit card fraud has significantly increased as a result of the The quick growth of digital financial transactions has made fraud detection a top priority for academics and financial organizations. Conventional approaches to fraud detection, such as statistical models and rule-based systems, are not very effective at spotting intricate and dynamic fraud patterns. This limitation has prompted research into increasingly complex deep learning and machine learning techniques [1][2].

Deep Learning in Fraud Detection

Convolutional Neural Networks (CNNs), a type of deep learning, have become an extremely useful tool for problems involving pattern identification and categorization [3], [16]. Because CNNs can extract complex features from data, they have been adapted for a wide range of applications, including fraud detection [4]. CNNs are typically employed in image processing; however, research has shown that by learning hierarchical representations that disclose underlying fraudulent tendencies, CNNs are effective at identifying anomalies in transaction data [5]. To attain optimal performance, deep learning models—including CNNs—require substantial computational resources and large datasets, which presents a significant challenge [6].

Optimization Algorithms in Deep Learning

Algorithms for optimization have been incorporated into the training process to help deep learning models overcome computational difficulties and become more effective [7]. Among these, metaheuristic algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and, most recently, the Flower Pollination Algorithm (FPA) have drawn considerable interest [8][9]. These algorithms are designed to locate the best solutions in challenging search environments, drawing inspiration from natural processes. In particular, the FPA has demonstrated promise in a variety of optimization issues because of its capacity to strike a balance between exploration and exploitation, resulting in effective convergence [10].

CNNs and Optimization Algorithm Integration

Several studies have investigated the combination of CNNs with optimization methods to enhance the performance of deep learning models [11]. In tasks like image classification and medical diagnosis, for instance, CNNs paired with PSO or GA have shown increased accuracy and efficiency [12][13]. The use of these integrated models for fraud detection is still in its infancy, however. There is a need for more research in this field because there have been limited studies explicitly on the application of FPA for CNN parameter optimization [14]

III. Proposed Methodology

The proposed system for credit card fraud detection using the Flower Pollination Optimization Algorithm (FPOA) with Stacked Temporal Convolutional Networks (STCN) aims to enhance the accuracy and efficiency of financial anomaly fraud detection. This approach combines the strengths of both optimization algorithms and deep learning techniques to create a robust system capable of identifying fraudulent transactions.

The FPOA is a nature-inspired optimization algorithm that mimics the process of pollination in flowers. It is known for its ability to explore the search space efficiently and find optimal solutions [1], [2]. In the context of fraud detection, FPOA can be used to optimize the parameters of the STCN, ensuring that the model is tuned to best detect fraudulent transactions. Stacked Temporal Convolutional Networks (STCN) are a type of deep learning model specifically designed for time-series data. They consist of multiple layers of temporal convolutional networks stacked on top of each other, allowing the model to learn complex patterns and dependencies in the data over time [3], [4]. This makes STCN particularly suitable for financial data, where transactions are often sequential and exhibit temporal dependencies. By combining FPOA with STCN, the proposed system leverages the strengths of both algorithms to achieve high accuracy in fraud detection. The FPOA optimizes the STCN's parameters, ensuring that the model is tuned to best detect fraudulent transactions. This combination allows the system to adapt to the dynamic nature of financial data, making it more effective at identifying fraud [5], [6].

In summary, the proposed system for credit card fraud detection using FPOA with STCN represents a sophisticated approach that combines the efficiency of optimization algorithms with the power of deep learning techniques. This system is designed to provide high accuracy and efficiency in detecting fraudulent transactions, making it a valuable tool for financial institutions and organizations dealing with credit card fraud [7]-[15].

Followingsteps to implement:

Data Preparation: First, gather and preprocess your credit card transaction data. This involves cleaning the data, handling missing values, and normalizing the features. The target variable should be binary, indicating whether a transaction is fraudulent or not.

Feature Extraction: Use a CNN to extract features from the transaction data. CNNs are particularly effective for image and signal processing tasks, but they can also be used for structured data like credit card transactions by treating each transaction as a "signal" or "image" with features such as transaction amount, time of transaction, and location.

Stacked CNN Architecture: Design astacked CNN architecture for feature extraction. This involves multipleconvo

layers to reduce the dimensionality of the data. The outputofthelastpoolinglayercanbefedintoafully connected layer to produce a feature vector for each transaction.

Trainingand Validation: Use the optimized hyper parameters to train the CNN on a portion of your dataset. Validate the model's performance on a separate validation set to ensure it generalizes well to unseen data.

Fraud Detection: Once the CNN is trained and validated, use it to classify new transactions as fraudulent or not. The model should output a probability score for each transaction, which can be thresholdedtomakeabinaryclassificationdecision.

Evaluvating: Evaluate the performance of your model using appropriate metrics such as accuracy, precision,recall,andthe F1score.Adjustthemodel and the FPA parameters as needed based on the evaluation results.

A. FlowerPollinationAlgorithm (FPA):

To implement the Flower Pollination Algorithm (FPA) for optimizing the hyperparameters of a Convolutional Neural Network (CNN) in credit card fraud detection, follow these steps:

Hyperparameter Optimization with FPA: The FPA is a swarm intelligence-based algorithm that simulates the natural pollination process of flowers. In this algorithm, each flower represents a potential solution, which in this context is a set of hyperparameters for the CNN. The pollination process is analogous to the exchange of information between solutions, allowing the algorithm to explore the search space and identify the optimal set of hyperparameters [9], [12].

Representation of Solutions: In the context of credit card fraud detection, each potential fraudulent transaction can be represented as a solution. This involves encoding various features associated with the transaction, such as transaction amount, location, time, and merchant category, into a format suitable for the algorithm [4], [7].

Objective Function for Fraud Detection: Define an objective function that evaluates the likelihood of a transaction being fraudulent based on the features mentioned above. This function could incorporate machine learning models such as logistic

regression, decision trees, or neural networks trained on historical data to classify transactions as either fraudulent or legitimate [10], [13].

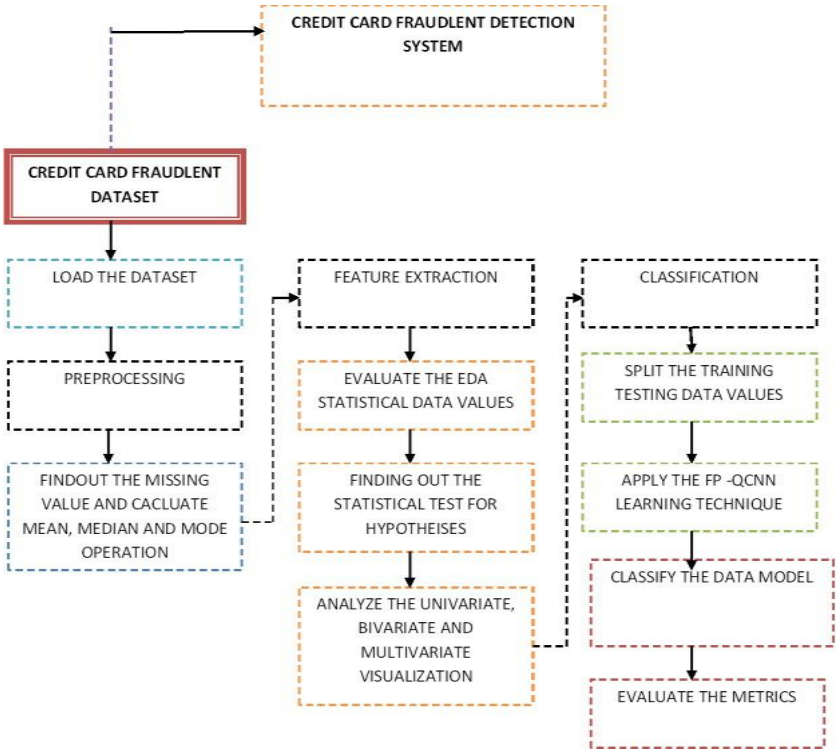


Fig. 1. The figure shows Credit Card Fraud Detection System Workflow from Data Loading to Model Evaluation

Pollination steps : In the FPA, flowers exchange pollen to find better solutions. Similarly, in the context of fraud detection, you could simulate this pollination process by allowing 'flowers' (representingtransactions)toexchangeinformation. This exchange could involve modifying certain features of one transaction based on features of another transaction.

Local and Global Analysis : The FPA balances between exploration and exploitation by performing bothlocalandglobalsearchoperations.Inthecontext of fraud curateandrobustfraud detection systems.

Pattrens and Emerging: Like natural pollination,theFPA allows for adaptation and evolution over time. As new types of fraud emerge or patterns change, the algorithm can adapt by updating its parameters or strategies accordingly.

Evaluation and Validation: As with any machine learning-based approach, it's crucial to evaluate the performance of the FPA-based fraud detection system using appropriate metrics and validate its effectiveness on real-world data.

By implementing the flower pollination algorithm in credit card fraud detection, you can potentially enhance the ability to detect fraudulent transactions by exploring a wider range of patterns and adapting to evolving fraud tactics.

Convolutional Neural Network Algorithm (CNN)

In the credit card fraud detection involves representing transactions as input data andleveraging the CNN architecture to learn featuresand patterns indicative of fraudulent activity. Here'show you could implement this:

Data Representation: Represent each credit card transaction as a data point. Features could includetransaction amount, location, time, merchant category, type of card used, etc. These features would form the input data for the CNN.

Data Preprocessing: Before feeding the data into the CNN, preprocess it to ensure consistency and normalization. This could involve scaling numerical features, encoding categorical variables, handling missing values, and possibly applying techniques like PCA (Principal Component Analysis) fordimensionality reduction.

CNN Architecture: Design a CNN architecture suitable for processing the transaction data. Since credit card fraud detection typically deals withtab ular data rather than images, you might design an1D CNN or a hybrid model combining CNNs with other types of layers like fully connected layers.

Training: Train the CNN on a labeled dataset of credit card transactions, where each transaction is labeled as either fraudulent or legitimate. During training, the CNN learns to extract relevant featuresfrom the transaction data and classify transactions accordingly.

Validation and Testing: Evaluate the performance of the trained CNN on a separate validation dataset and/or testing dataset. Use appropriate metrics such as accuracy, precision, recall, and F1-score to assess the model's effectiveness in detecting fraudulent transactions while minimizing false positives.

Integration into Fraud Detection System: Once you have a trained and validated CNN model, integrate it into your credit card fraud detection system.

By implementing the capabilities of CNNs, you can effectively capture complex patterns and relationships within credit card transaction data, potentially leading to more accurate and robust fraud detection systems.

IV Performance Analysis

1. Accuracy:

Definition: It shows the proportion of correct predictions out of the total predictions.

$$\text{Formula:Accuracy}=\frac{\text{True}_{\text{positive}}+\text{True}_{\text{negative}}}{\text{TotalPrediction}}$$

Interpretation: Accuracy gives an overall measure of howwellthemodelperformsacrossbothpositiveand negative cases.

2. Precision(PositivePredictiveValue):

Definition: It measures the accuracy of positive predictions, indicating the proportion of positive predictions that were correct.

$$\text{Formula:Precision}=\frac{\text{True}_{\text{positive}}}{\text{True}_{\text{positive}+\text{False}_{\text{positive}}}}$$

Interpretation: Precision is crucial when the cost of falsepositivesishigh;itreflectsthemodel'sabilityto avoid false alarms.

3. NegativePredictiveValue:

Definition: It assesses the accuracy of negative predictions, indicating the value ofproportion of negative predictions that were correct.

$$\text{Negativepredictive value} = \frac{\text{True}_{\text{negative}}}{\text{True}_{\text{negative}+\text{False}_{\text{negative}}}}$$

Interpretation: Negative Predictive Value is particularly relevant when correctly identifying non- fraudulent transactions is essential

4. Recall(Sensitivity):

Definition: It gauges the ability of the model to identifyallrelevantcases,capturingtheproportionof actual positive cases correctly identified.

$$\text{Formula:Recall} = \frac{\text{True}_{\text{positive}}}{\text{True}_{\text{positive}+\text{False}_{\text{negative}}}}$$

Interpretation:Recalliscriticalwhenmissingpositive cases (fraudulent transactions) is more costly than false positives

Particularity: the extent of genuine negative cases which are accurately recognized.

These metrics collectively provide a comprehensive evaluation of a classification model's performance. Depending on the specific goals and costs associated with false positives and false negatives in credit card frauddetection,onemightemphasizeprecision,recall, or a balance of both. The confusion matrix, from which these metrics are derived, is a valuable tool for assessing the strengths and weaknesses of a model in a binary classification problem.

V Result and Evaluation

The suggested Flower Pollination optimization algorithm with Queued Convolution Neural Network(FPO_QCNN) is compared with the existing technique QCNN. The Performance of the proposed FPO_QCNN and existing techniques QCNN is given in the following table.

Technique	Accuracy (%)	Precision (%)	Recall (%)
Existing QCNN	**99.80**	**92**	**72**
ProposedFPO_ QCNN	**99.95**	**97**	**77**

VI Conclusion

Theuseofcreditcardpaymenttechnologiesbyscam artists is rising quickly as a result of credit cards becoming the most widely used payment method, especiallyintheonlinemarket.Financialinstitutions need to continuously enhance their system of fraud detection systems to avoid catastrofsphic losses. This research aims to create a new CCFD system by sequentially modeling data and employing LSTM deep recurrent neural networks and attention mechanisms. In contrast to the studies that came beforeit,themodelthathasbeenproposedtakesinto accountthesequentialstructureoftransactionaldata. This enables the classifier to recognize the most significant transactions within the input sequence and to accurately predict fraudulent transaction.

Future Work

Our experiment's next steps will involve expanding the dataset's record count in order to train the data more thoroughly and produce accurate results. A larger dataset will also enable the network to learn more effectively. Our goal is to carry out the same experiment with different programs, like JOONE, Weka, and Rapid Miner. Additionally, we want to compare the outcomes of these programs to discover the much effective program for CCFD by adjusting different parameters like momentum, learning rate, etc., and analyzing the same.

References:

[1] B. A. Garner, Black’s Law Dictionary, 8th ed. Toronto, ON, Canada: Thomson West, 2004, p. 1805.

[2] A. Ethem, *Introduction to Machine Learning*, 2nd ed. Cambridge, MA, USA: The MIT Press, 2014.

[3] Y. Kültür and M. U. Çağlayan, "Hybrid approaches for detecting credit card fraud," *Expert Syst.*, vol. 34, pp. 1–13, 2017.

[4] M. Krivko, "A hybrid model for plastic card fraud detection systems," *Expert Syst. Appl.*, vol. 37, pp. 6070–6076, 2010.

[5] R. Sarno, R. D. Dewandono, T. Ahmad, and M. F. Naufal, "Hybrid Association Rule Learning and Process Mining for Fraud Detection," *IAENG Int. J. Comput. Sci.*, vol. 42, pp. 59–72, 2015.

[6] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: a realistic modeling and a novel learning strategy," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, pp. 3784–3797, 2018.

[7] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," *arXiv preprint arXiv:1009.6119*, 2010.

[8] A. C. Bahnsen, D. Aouada, and B. Ottersten, "Example-dependent cost-sensitive decision trees," *Expert Syst. Appl.*, vol. 42, pp. 6609–6619, 2015.

[9] F. Carcillo, A. Dal Pozzolo, Y. A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with spark," *Information Fusion*, vol. 41, pp. 182–194, 2017.

[10] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. E. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," *Expert Syst. Appl.*, vol. 100, pp. 234–245, 2018.

[11] C. Whitrow, D. Hand, P. Juszczak, D. Weston, and N. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Min. Knowl. Discov.*, vol. 18, pp. 30–55, 2009.

[12] D. Sánchez, M. A. Vila, L. Cerda, and J. M. Serrano, "Association rules applied to credit card fraud detection," *Expert Syst. Appl.*, vol. 36, pp. 3630–3640, 2009

[13] S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit card fraud detection using Bayesian and neural networks," in *Proc. 1st Int. Naiso Congr. Neuro Fuzzy Technol.*, 2002, pp. 261–270.

[14] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, pp. 235–249, 2002.

[15] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, pp. 602–613, 2011.

[16] N. Palanivel, K. Madhan, A. Venkatvamsi, G. Madhavan, S. B and L. Priya G, "Design and Implementation of Real Time Object Detection using CNN," *2023 International Conference on System, Computation, Automation and Networking* (ICSCAN), PUDUCHERRY, India, 2023, pp. 1-5, doi: 10.1109/ICSCAN58655.2023.10394752.