ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

Article Title: An Enhanced Credit Card Fraud Detection Using Modified Convolutional Neural Network

An Enhanced Credit Card Fraud Detection Using Modified Convolutional Neural Network

R. Sahila Devi
Assistant Professor, Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Palkulam, India. r.sahiladevi@gmail.com

ABSTRACT

Credit card fraud has played a major issue for both cardholders and the issuing authorities as a notable financial challenge. To address this issue here involves modified Convolutional Neural Network (CNN) to identify fraudulent activities. The proposed methodology involves data pre-processing, data visualization, validation and evaluation. Here the data is preprocessed by normalization to improve the quality of data performance and training stability of deep neural network. One hot encoding is used to convert categorical variables into binary format and is highly essential for data processing which in turn improve the prediction and classification accuracy of the method. Furthermore by using CNN with a modified Quantum Vortex Search Algorithm (MQVSA) is developed to increase the accuracy and effectiveness of the credit card fraud detection. The MQVSA improves CNN capacity of classification and to identify complex pattern indicative of fraud and model parameters. Thus the proposed method used in this work is performed in the python software and thus the classifier achieve the remarkable precision of 98% and the sensitivity value of 97% and effectively predicting the credit card fraud by evaluation and validation.

Keywords: Data preprocessing, Data visualization, Modified Convolutional Neural Network (CNN), Deep learning, Credit card, MQVSA.

1 Introduction

Credit card fraud has increased in frequency, complexity and presenting serious difficulties for individuals in businesses and in financial institutions [1]. The digital era have made financial transactions more convenient than ever before but it made it easier for increasing complex fraudulent schemes. Deep learning is used in the detection process and the approach is dependable to implement, and thus the detection procedure becomes more efficient [2].The transaction history of a customer's benign transactions is normally used to infer customer related features. The data is preprocessing to build the data model that is used for classification based on this technique the data is normalized. Here the dataset is normalized to ensure all the variables in the dataset is on the same scale [3].

Here the datasets are normally transformed into equivalent numerical features .One-Hot encoding, transforms categorical variables into numerical form during the first stage of data preparation and a column containing categorical data is used to generate new columns with an equal number of distinct categorical values as the original column. Therefore data

preprocessing [4] is an essential step in the deep learning process to increase the accuracy of the detection and the system needs preprocessing time for further preprocessing the data. Thus without reducing the important features the size is optimized by preprocessing execution.

After the preprocessing the data transaction undergoes data visualization that makes the data to be reliable for handling and understanding. The data visualization [5] tools promise for improving the efficiency and effectiveness of fraudulent transaction identification that convert data representation from text to graphics and filter out subsets of transactions for additional analysis. The deep learning method uses the minority class data from the original training set and use it as a training set [6] and then creates false minority class data. The created false data is then mixed with the initial training set to create an improved training set .Thus the classification model trained on the training set achieve better results than the model trained only on original training set. Hence dealing with fraud transaction [7] datasets, all of the data that has gathered and processed is also updated during the data visualization process improving detection accuracy and processing efficiency.

When the features of data is reliable and easy to handle it undergoes classification process. SVMs is only good for binary classification in hyper plane based situations. It is advisable to locate a hyper plane and yields the highest margin while requiring the fewest number of points possible. However it does not handle multi-class classification. A ML method called Random Forest is used to resolve problems of regression and classification. During the training process it constructs multiple decision trees and determines the outcome through a majority vote in order to enhance accuracy. The ML technique improve detection accuracy of credit card fraud detection by comparing with unrecognized fraudulent patterns [8] however it require a large amount of high quality data and also it is expensive to implement and maintain. To overcome this issue, modified CNN is used to detect the fraud behaviours and to identify a set of latent patterns for data sets. The main intention of modified CNN is to make fast and reliable model formation for real time and feasible detection [9]. Because of the performance and resilience, deep learning techniques have been used extensively in many domains. Deep learning has recently demonstrated remarkable results in the identification [10] of credit card fraud. To overcome the difficulties in detecting credit card fraud, a combination of CNN and a MQVSA is used. Thus it make to improve the accuracy, speed and flexibility of fraud detection systems and aims to advance reliable and effective methods for spotting credit card fraud transactions in real world environment.

This paper propose the CNN with MQVSA for the identification of fraud activities during the transaction. The data is pre-processed by two technique one is normalization and other is one hot encoding. Here the normalization technique improves the quality of the dataset and also uses one hot encoding to improve prediction of data. Under the data visualization the patterns in the dataset is known clearly and also to improve the effective and efficiency of fraudulent transaction. CNN with MQVSA in credit card fraud detection guide to develop more robust

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

and efficient fraud detection and also secure financial transactions and reducing the economic impact of fraud.

2 Related Work

Emmanuel Illeberi et al (2024), have developed Adaptive Synthetic Minority Oversampling Technique (ADASYN) to balance an imbalanced dataset so that it improve the models ability to detect fraudulent transactions. By using Recursive Feature Elimination with Cross Validation technique (RFECV) it enhances model robustness and generalizability and effectively preventing overfitting. The combination of ADASYN and RFECV improve the performance of the model in detecting fraudulent transactions. However working with large datasets it is computationally expensive.

Fawaz Khaled Alarfaj et al (2022), have analyzed machine learning and deep learning algorithms to perform efficient outcomes. Here the machine learning technique is used to improve the accuracy of detection of the fraud and the Convolutional Neural Network (CNN) is applied to improve fraud detection performance. However, machine learning is too expensive to implement and maintain and also it requires diverse datasets for training. Similarly, deep learning is expensive and also it is difficult to understand.

Emmanuel lleberi et al (2021), have analyzed machine learning based framework for credit card fraud detection using SMOTE and adaptive boosting (AdaBoost) technique. By using this techniques, enhances issue of class imbalance and to increase the quality of classification. SMOTE helps in building models that generalize better to unseen data. Nevertheless, it requires diverse datasets for training and also it is expensive to implement and maintain and also struggles in complex pattern recognition in high dimensional data.

Ibomoiye Domor Mienye et al (2023), have developed deep learning approach with SMOTE-ENN to detect credit card fraud effectively. By using this technique it is employed to balance the class distribution in the dataset and also the data resampling is achieved using hybrid SMOTE-ENN method. However it has the risk of work well with high dimensional data that lead to overfitting and poor performance.

Jabber Jemai *et al* (2024), have introduced ensemble learning on real and simulated CCF datasets. By using this methodology, identify credit card fraud and the performance is discussed in classifying credit card transactions as authentic or malicious. Thus it provide more reliable predictions by capturing different aspects of the data. However, it is expensive and time-consuming and it is more difficult to interpret.

3 Proposed work explanation

In this paper, examined the execution process of an enhanced credit card fraud detection using modified CNN and figure 1 in this paper provide a visual overview of the proposed model to increase the model performance.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

Article Title: An Enhanced Credit Card Fraud Detection Using Modified Convolutional Neural Network

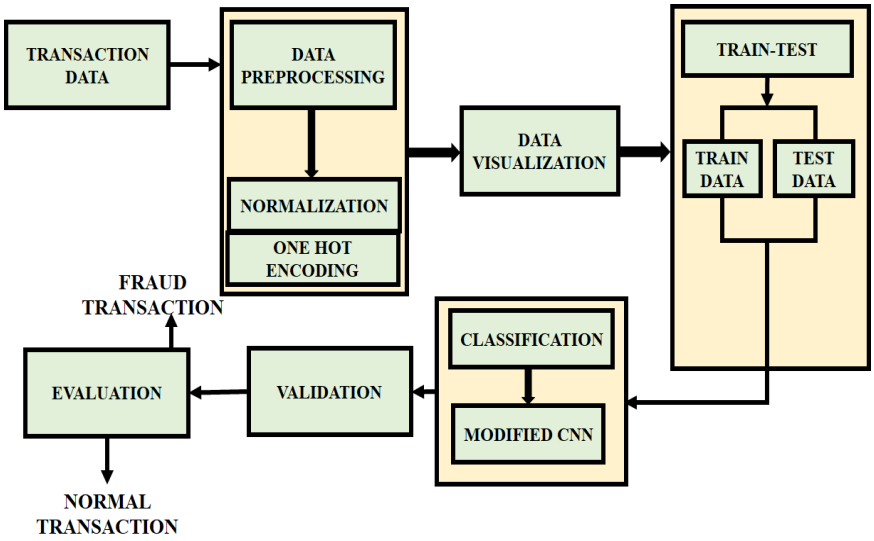

Figure 1: *Block Diagram for Proposed Methodology*

Pre-processing is the technique used here to describe the changes in the data before input it in the process. Data pre-processing is used to transform raw data into a clean data set. Here the data is preprocessed by normalization to improve the quality of data performance and training stability of deep neural network to speed up computation and stabilizes training. Thus one hot encoding in the data pre-processing is the essential process of converting the categorical variables to binary format which in turn improves the prediction as well as classification. In data visualization, the key information in the big dataset is highlighted using any type of display to improve comprehension of the input data. CNN uses a series of layers which detects different features of an input image. Depending on the complexity of its intended purpose a CNN contain dozens, hundreds or even thousands of layers each building on the outputs of previous layers to recognize detailed patterns. The modified CNN utilizes the deep learning approach. Then the classification method offers outstanding sensitivity and specificity. To increase integrity data validation is then used. The evaluation block finally identifies the anticipated fraudulent transaction.

4 Transaction Data

In the proposed methodology, Processing is done after the machine has read the transaction data. After that the pre-processed image is displayed using data visualization, which presents the information in a way that makes it simple to understand and available for additional classification. Then during the data classification, deep learning method is used with modified CNN which efficiently finds important data as part of its search process. Following with validation and model evaluation, it is possible to determine whether the data is fake or not. The procedures of data processing, data visualization, and deep learning classification using

modified CNN, validation, and model evaluation are included in the modelling of this proposed system.

4.1 Data Preprocessing

The process of converting raw data into a clean dataset in order to prepare it for analysis is known as data preprocessing. Preprocessing is a first step in preparing datasets for financial fraud analysis and modelling. In these processes duplicate records are eliminated, missing data is handled, and data scaling is standardized. The aim of these steps is to organize and clean the dataset in order to provide a solid foundation for accurate analysis and effective modelling and to find potential instances of financial fraud. Managing missing values means addressing the gaps in our dataset that result from incomplete or missing data. By minimizing noise distortions, this procedure is typically utilized to carry out data extraction. This will make the primary characteristics of the data more apparent, which makes easier and efficient the visualization process.

4.1.1 Normalization

A data preprocessing technique called normalization enhances the efficiency and precision of deep learning technique by converting a dataset features to a common scale. By increasing convergence, decreasing the influence of outliers and accelerating training the normalization enhances model performance. Normalization speeds up convergence during gradient-based training by fostering stability in the optimization process. It helps the model to arrive the optimal solutions more quickly by mitigating problems with vanishing or ballooning gradients. The normalized data is easier to grasp and evaluate. Finding and visualizing the links between various features and performing insightful comparisons are also made simpler when all of a dataset features are on the same scale.

4.1.2 One Hot Encoding

One-hot encoding is a data preparation technique it converts categorical data into a binary format that is comprehensible and useful in deep learning technique. Because of this change every category is handled separately without suggesting any inaccurate connections between them. Here each distinct category in a feature requires the creation of a new binary column. Every column denotes a distinct category and the existence or absence of that category is indicated by a value of 1 or 0.

4.2 Data Visualization

Data visualization is important in the early stage of a fraud investigation, when the investigator try to conduct an effective and efficient data analysis and gain a better understanding of the links that exist in a complicated data collection. Data visualization is used by the fraud investigator as a proactive detection method to look for trends in the data that point to fraudulent activity. Data visualization technique enable investigators to convert textual data

representation to visual representations and filter out subsets of transactions for additional analysis. Thus it promise to improve the effectiveness and efficiency of fraudulent transaction identification. Data Visualization improve the speed of important structures and relationships to be found by the discovery of questionable patterns that is hidden by the amount of data. Visual representation makes it easy to understand and learn from even big collections. These modules are used for detailed data observation, exploration, and comprehension.

4.3 Deep Learning Classification

Deep learning is a branch of machine learning that learns representations of the input data by using modified (CNN). Here the variety of tasks including classification of deep learning models is to attain state-of-the-art performance by automatically extracting pertinent features and patterns from the data. When the dataset is large neural networks prove themselves to be efficient and robust. Even though a multilayer is challenging it helps as an application for fraud detection. For this purpose deep learning classifiers like modified (CNN) are preferable because hundreds of thousands of credit card transactions are made daily. It require more time to train but this trade off provide the classification is accurate. Thus deep learning neural network is used in the proposed methodology. Deep learning model is trained iteratively to imply that the model is updated with fresh data on a regular basis until it finds a solution. The model receives a data point and its label at each iteration. The model then predicts the data point label using its neural network. After comparing the prediction and the actual label, the model is modified to reduce the discrepancy between the two.

4.3.1 Modified Quantum Vortex Search Algorithm

CNN reduces the interaction of human experience with the derivative feature that are advantage to the classification results. CNN is used to extract local information from the transactions that point to the fraudulent activity. CNN is computationally effective and capable of handling large scale credit card datasets by sharing parameters that are trained. CNN enhances the models capacity to distinguish between fraudulent and legitimate.

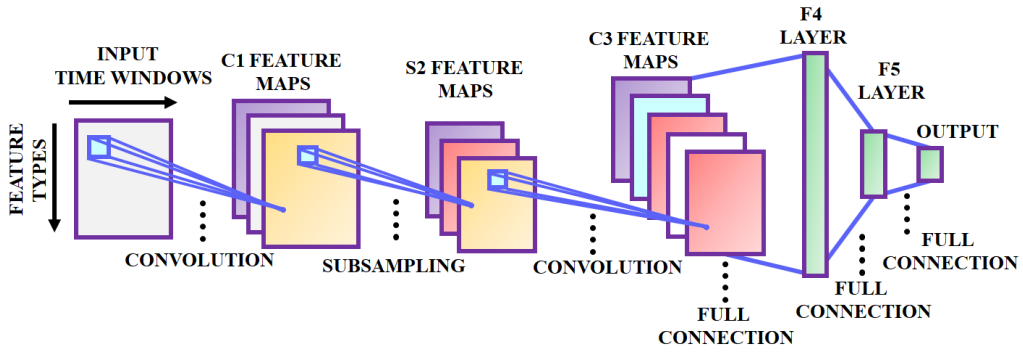

Figure 2: *CNN with MQVSA*

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

An iterative optimization approach is required for the integration of MQVSA with CNN. MQVSA is first used to generate a set of candidate features and hyper parameters, which are subsequently assessed using CNN model training and validation. In order to direct the search towards more promising areas of the solution space, the performance metrics such as precision, recall, and F1score are input back into the MQVSA. This feedback loop keeps going until the algorithm finds an ideal combination of feature subsets and hyper parameters. The robustness and generalizability of the finished model in identifying financial fraud are next assessed using a test dataset. This iterative optimization makes use of the quantum-inspired improvements offered by MQVSA to guarantee the CNN is precisely adjusted for optimal performance.

4.4 Data Validation

Data validation is the process of ensuring the source data is accurate with high quality before it is imported or processed. Different types of validation can be performed depending on destination constraints or objectives. Data validation is a form of data cleansing. To provide an error-free dataset for additional analysis is the main goal of data validation. Cleaning up data or eliminating inputs that are not standardized, incomplete, or fall outside the range is another aspect of data validation. This procedure reveal the data and offer more information about the results.

4.5 Data Evaluation

Data evaluation.is the process of determining that the data support an organizations objectives by evaluating its completeness, accuracy and relevance. Even for bigger datasets of transactions the operational evaluation provides a more realistic representation of the system. The evaluation approach focuses on the model to predict the final results. The most important step in evaluating a deep learning model is determining its prediction accuracy, even though there are other steps involved. Real-time datasets are used for additional processing and process enhancement.

5 Result and Discussion

In the proposed methodology the deep learning technique is used for the credit card fraud detection to make the work more efficient and with high accuracy. Here the data is distributed to analyse the fraudulent activities and prevent it from further occurrence. Initially the transaction data are collected for preprocessing, classification, validation and finally evaluation.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

Article Title: An Enhanced Credit Card Fraud Detection Using Modified Convolutional Neural Network

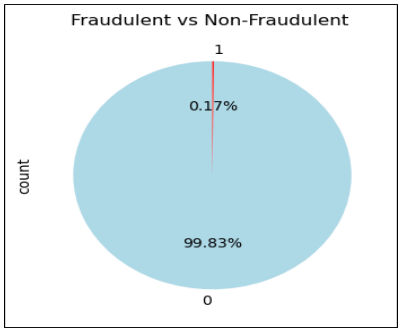

Figure 3: *Distribution of Data*

Here the pie chart for the distribution of data representing in figure 3 shows whether the credit card detection is fraudulent or not. Here the count of the prediction accuracy is mentioned to show the accurate level of the fraudulent activities and shown that the indication is 99.83%.

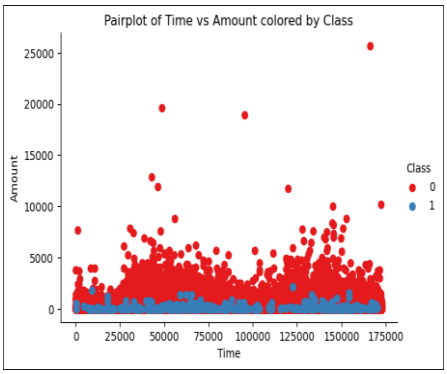

Figure 4: *Distribution of Class*

The class already classified is compared with the distribution of class based on the number of transaction are shown in the figure 4. Here the pair plot of time Vs amount by coloured class is discussed to shown how the prediction time is lowered even if large class of amount of transaction set data is collected.

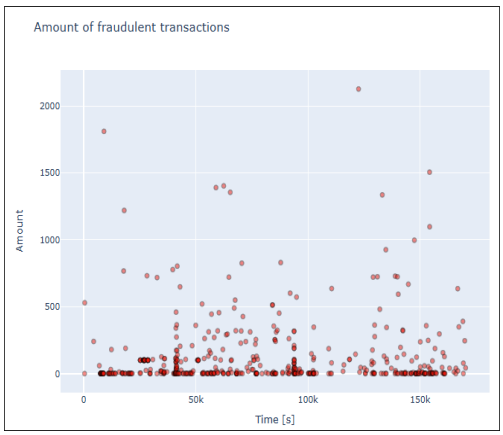

Figure 5: *Fraudulent Transaction*

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

Figure 5 indicates the transaction process during the credit card fraud detection which are shown in fraudulent transaction. The transaction of collected data model is even large the prediction is more accurate as shown by time and amount of data collection.

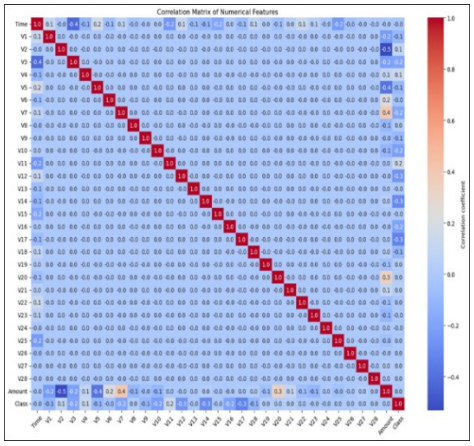

Figure 6: *Confusion matrix of MQVSA*

Figure 6 shows the result of MQVSA algorithm represented with confusion matrix. The estimation of the matrix in this figure shown is modelled to prove that the MQVSA is efficient and robust than other algorithms.

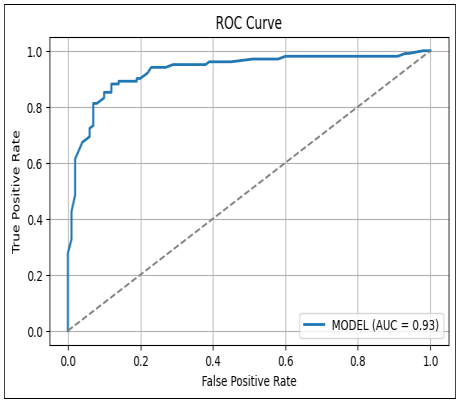

Figure 7: *ROC curve of MQVSA*

Figure 7 shows the outcome of the MQVSA algorithm with the representation of the ROC curve. Here the ROC curve indicates that the true positive rate of the prediction and shown that the prediction level is 93%. When compare with other previous works this is more efficient and valuable approach.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03 (09), September 2024, pp. 12-23

Article Title: An Enhanced Credit Card Fraud Detection Using Modified Convolutional Neural Network

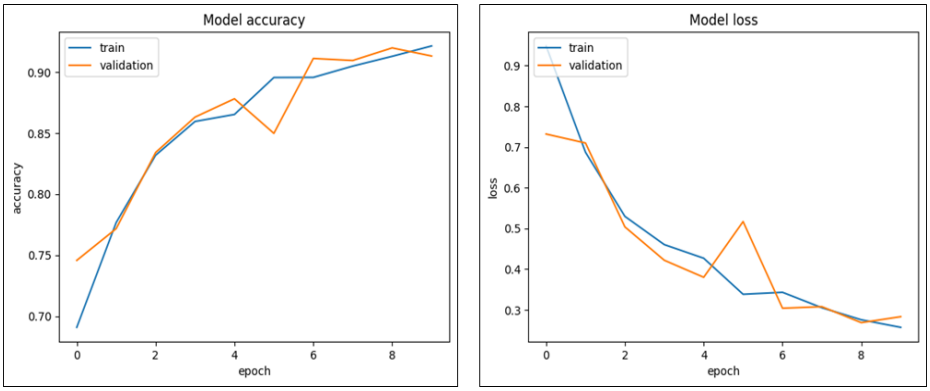

Figure 8: *Accuracy and Loss of the model*

Figure 8 indicates the accuracy and loss obtained as a result of the CNN with MQVSA for the credit card fraud detection shows that the prediction is high with accuracy and efficient in the detection analysis. After comparing the prediction and the actual label, the model is modified to reduce the discrepancy between the two.

Table 1: *Comparison in classification of accuracy in credit card fraud detection*

Method	Accuracy
Modified CNN	98%
GANs[7]	96%
SMOTE[15]	86%

Table 1 represents a comparison of various classification methods for the detection of credit card fraud prevention highlight that the modified CNN achieves the highest accuracy at 98% and then GANs model at 96% and smote at 86%.

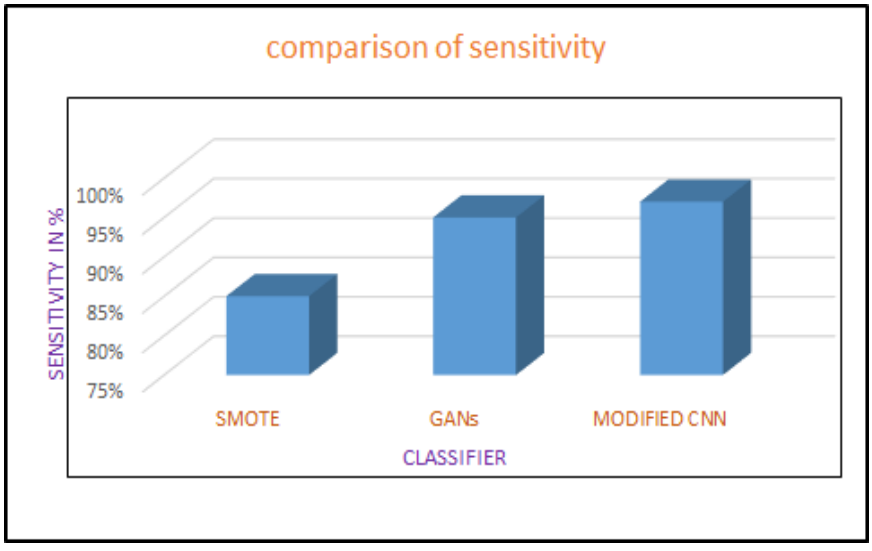

Figure 9: *Sensitivity Graph for Credit Card Fraud Detection*

Figure 9 represents the analysis of sensitivity in credit card fraud detection by collecting a detailed transaction performance across different classification techniques. The result of the graph indicates that the modified CNN classifier demonstrates a superior sensitivity at 97%, with outperforming both the classifiers GANs [7] at 95% and SMOTE [15] at 85%.

6 Conclusion

In the proposed methodology, introduced a deep learning method for detecting and preventing fraudulent transactions. By integrating convolutional neural network with a Modified Quantum Vortex Search Algorithm (MQVSA), demonstrating significant improvement in the fraud detection method. The proposed CNN-MQVSA model efficiently makes use of CNN with deep learning capabilities to identify complex patterns in transactional data and choose the most relevant features. This integrated approach performance highlights its potential for use in credit card where the accurate fraud detection is essential. Finally the method is evaluated with high accuracy in the classifier and the classifier produces the best result in the CNN-MQVSA modifier. The modified CNN with MQVSA has high sensitivity with 97% and classification accuracy with 98% that is dependable method for detecting credit card fraud. By using this technique the detection of credit card fraudulent is more effective compare to other better modifiers.

References

1. T. T. H. Le; Y. Hwang; H. Kang; H. Kim, Year: 2024, "Robust Credit Card Fraud Detection Based On Efficient Kolmogorov-Arnold Network Models," In IEEE Access, Vol: 12, pp. 157006-157020.

2. F. A. Ghaleb; F. Saeed; M. Al-Sarem; S. N. Qasem; T. Al-Hadhrami, Year: 2023, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," In IEEE Access, Vol: 11, pp. 89694-89710, 2023.

3. A. M. Babu; A. Pratap, Year: 2020, "Credit Card Fraud Detection Using Deep Learning," 2020 Ieee Recent Advances In Intelligent Computational Systems (Raics), Thiruvananthapuram, India, pp. 32-36.

4. F. Ogme; A. G. Yavuz; M. A. Guvensan; M. E. Karsligil, Year: 2021, "Temporal Transaction Scraping Assisted Point Of Compromise Detection With Autoencoder Based Feature Engineering," In IEEE Access, Vol: 9, pp. 109536-109547.

5. H. M. Shakeel; S. Iram; H. Al-Aqrabi; T. Alsboui; R. Hill, Year: 2022, "A Comprehensive State-Of-The-Art Survey on Data Visualization Tools: Research Developments, Challenges and Future Domain Specific Visualization Framework," In IEEE Access, Vol: 10, pp. 96581-96601.

6. Y. Ding; W. Kang; J. Feng; B. Peng; A. Yang, Year: 2023, "Credit Card Fraud Detection Based On Improved Variational Autoencoder Generative Adversarial Network," In IEEE Access, Vol: 11, pp. 83680-83691.

7. F. A. Almarshad; G. A. Gashgari; A. I. A. Alzahrani, Year: 2023, "Generative Adversarial Networks-Based Novel Approach for Fraud Detection for the European Cardholders 2013 Dataset," In IEEE Access, Vol: 11, pp. 107348-107368.

8. A. A. Almazroi; N. Ayub, Year: 2023, "Online Payment Fraud Detection Model Using Machine Learning Techniques," In IEEE Access, Vol: 11, pp. 137188-137203.

9. H. Palivela et al, Year: 2024, "Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds," In IEEE Access, Vol: 12, pp. 125629-125642.

10. I. D. Mienye; N. Jere, Year: 2024, "Deep Learning For Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," In IEEE Access, Vol: 12, pp. 96893-96910.

11. E. Ileberi; Y. Sun, Year: 2024, "Advancing Model Performance with Adasyn and Recurrent Feature Elimination and Cross-Validation in Machine Learning-Assisted Credit Card Fraud Detection: A Comparative Analysis," In IEEE Access, Vol: 12, pp. 133315-133327.

12. F. K. Alarfaj; I. Malik; H. U. Khan; N. Almusallam; M. Ramzan; M. Ahmed, Year: 2022, "Credit Card Fraud Detection Using State-Of-The-Art Machine Learning And Deep Learning Algorithms," In Ieee Access, Vol: 10, pp. 39700-39715.

13. E. Ileberi; Y. Sun; Z. Wang, Year: 2021, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using Smote and Adaboost," In IEEE Access, Vol: 9, pp. 165286-165294.

14. I. D. Mienye; Y. Sun, Year: 2023, "A Deep Learning Ensemble With Data Resampling For Credit Card Fraud Detection," In IEEE Access, Vol: 11, pp. 30628-30638.

15. J. Jemai; A. Zarrad; A. Daud, Year: 204, "Identifying Fraudulent Credit Card Transactions Using Ensemble Learning," In IEEE Access, Vol: 12, pp. 54893-54900.