Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/2023333

Impact of different transaction features on credit card fraud detection by neural networks

Ertong Wei

University of Toronto, Toronto, Ontario, Canada, M5S 1A4

ertong.wei@mail.utoronto.ca

Abstract. A perfect credit card fraud detection model is necessary because of the economic loss caused by credit card fraud. Since many models have already gained great performance, this research focuses on the influences of different credit card transaction features on the accuracy of the fraud detection model constructed by a neural network, which is favorable for economists to study credit card fraud better. The data used in this research from Kaggle contains a million credit card transaction records with seven features for each. To analyze the importance of different details, different parameters are used in the input layer of the neural network model to compare the performance. Furthermore, the result is that the feature *ratio to the median purchase price* is the most significant one. The second important feature is the *distance from home*, and then *online order* is followed. Compared with the accuracy when inputting all the seven features(99.81%), the model performs well with only the above three features in the input layer(95.43%).

Keywords: Neural network, Credit card fraud, Transaction feature, SMOTE.

1. Introduction

With the development of technology and society, credit cards have gradually become the mainstream consumption method. While credit cards make transactions faster and easier, crises ensue, especially credit card fraud. Credit card fraud is when people unauthorized use others' credit cards by getting others' credit cards, card information, or personal identification number(PIN) inappropriately [1]. In general, the amount of credit card fraud has shown an upward trend in the recent five years [2]. Especially from 2019 to 2020, the number of credit card frauds increased by around 45% [3]. If the trend continues, this problem will gradually become serious. In 2020, there was nearly a $140 million loss due to credit card fraud in the U.S. [3]. These losses could have been significantly reduced with a perfect credit card fraud detection model. The parameters of each credit card transaction are the primary information used to detect whether it is fraudulent, and each transaction contains several features, such as the amount of money, whether the transaction happened from the same retailer as the previous transaction, and whether it used the PIN. Different parameters may affect the accuracy of credit card fraud detection, and researching the importance of different features can make the expert pay more attention to that information to build the detection model and better detect credit card fraud. Although most current detection models gain great performance, the influence of transaction features is also important to prevent credit card fraud. Hunter points out that chip and PIN are nearly useless in

DOI: 10.54254/2755-2721/4/2023333

preventing credit card fraud when the cardholder does not present [4]. This provides ideas not only for bank staff but also for modeling fraud identification. Moreover, once the less influenced feature is known, researchers in related fields can strengthen the identification of information related to this feature and fundamentally eliminate credit card fraud, which can reduce the losses caused by credit card fraud more than improve the accuracy of the credit card detection model. In addition, there will always be outliers that cannot be accurately detected, so it makes more sense to protect information that has less impact. This research constructs a neural network with four dense layers, records the detection accuracy when using all seven selected features, and then compares the new accuracy after removing some transaction features to analyze the significance of these features to the whole credit card detection model.

2. Literature review

Most detection models are built by different machine learning methods, and many current models have substantial detection accuracy. This research will first review the current models. The accuracy of the models constructed by K-nearest neighbors(KNN) and Naive Bayes is 97.69% and 97.92%, separately, and the KNN classifier using Euclidean distance and the model performs well when K=3 [5]. Compared with the KNN and support-vector machine, the artificial neural network(ANN) is much more suitable for detecting credit card fraud, and it shows a better accuracy of approximately 100%[6]. The ANN is constructed by 15 hidden layers, and the active function of this model is ReLU, and the researchers use normalization and under-sampling to process the imbalanced data [6]. Other neural network models also have high performance. Chen & Lai constructed a deep convolution neural network (DCNN), which combined memory-based Deep Learning Neural Network(DLNN) and Convolution Neural Network(CNN) and has 99% accuracy in 45 seconds when facing a large amount of data [7]. Chen & Lai process 30 input features in the preapplication stage by normalization and validation. Then, they apply the DCNN model to predict the status of the credit card transaction. The specificity is that this model can store memory data for an extended period by the long memories [7]. Furthermore, Linear Regression(LR) model, Multilayer Perceptron(MLP) model, and Random Forest(RF) model also perform well. LR model obtains 94.46% accuracy. MLP model has 99.93% accuracy. Contrasting to the previous two models, RF model has the highest accuracy — 99.96% [8]. The RF algorithm is based on the decision tree, and each decision tree gives a result. It performs well when there are more decision trees. Besides, the MLP is a feedforward artificial neural network, and it contains four hidden layers with 50, 30, 30, and 50 neurons in each layer, and the researchers find that this model performs better with more layers. Then, they build the model with increasing layers until the performance reaches an appropriate level, choosing ReLU as the active function and Adam as the optimizer [8].

3. Methodology

3.1. Data

3.1.1. Data analysis. The credit card fraudster data used in this research comes from Kaggle [9]. In this dataset, each credit card transaction contains eight features: distance from home; distance from the last transaction; ratio to the median purchase price; repeat retailer(whether the transaction happened from the same retailer as the previous transaction); used chip(whether the transaction occurred through a chip); used PIN(whether the transaction occurred by using the PIN); online order(whether the transaction is an online order); fraud(whether the transaction is fraudulent). Only the first three features are digital parameters, and the rest are boolean features(0 for false, 1 for true). Additionally, there are one million credit card transaction records total, where 912,597 transactions are normal, and 87,403 transactions are fraudulent, which is highly imbalanced. Therefore, data processing is necessary to avoid the effect of unbalanced data. Besides, there is no data cleaning step since no missing data exists in this dataset.

DOI: 10.54254/2755-2721/4/2023333

3.1.2. Data processing. A synthetic minority oversampling technique(SMOTE) is then applied to this dataset to reduce the effect of unbalanced data on the neural network model. There are five main steps in SMOTE [10]:

Step 1: Pick a data point x from the minority class;

Step 2: Find the k nearest neighbors of x;

Step 3: Randomly select a neighbor z from the k neighbors;

Step 4: Construct the new data point y based on the following formula;

$$y = x + random(0, 1) * (x - z)$$

Step 5: Repeat the previous steps.

After applying SMOTE, there is the same amount of fraudulent and normal transaction data [10]. Then, split the data into 70% training and 30% testing data.

3.2. Model architecture

The credit card fraud detection model in this research is constructed by the neural network, consisting of the input layer, two hidden layers, and the output layer. Figure 1 shows the details of this model [11]. The inputs of this model are different features of each transaction, with up to seven input features. Moreover, the input layer fully connects with a hidden layer containing 64 neurons, and the activation function is ReLU, which performs better than other activation functions. Then, another 32 neurons hidden layer connected with the previous layer, which has the same activation function. The last layer is the output layer which has 2 neurons since there are two classes in this classification problem — normal transaction or fraudulent transaction. The activation function used in the output layer is Softmax which makes the two output values between 0 and 1 and sum to 1. Additionally, a dropout is added between the two hidden layers to avoid overfitting and set the dropout rate=0.3. According to Table 1, adding dropout enhances the model's performance. Because the accuracy experiences a growth of around 0.2%, the loss decreases from 0.01289 to 0.00755.

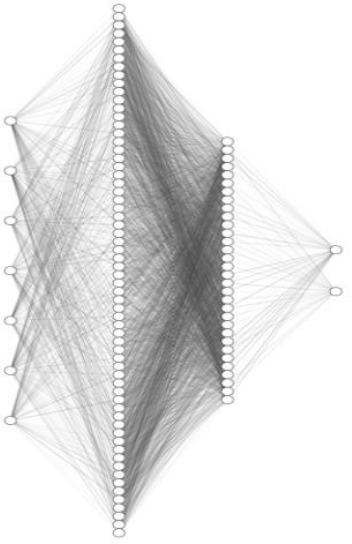

Figure 1. Neural Network Model.

DOI: 10.54254/2755-2721/4/2023333

Table 1. Influence of dropout on model performance.

	Before Adding Dropout	After Adding Dropout
Testing Accuracy	99.62%	99.81%
Testing Loss	0.01289	0.00755

3.3. Training

The optimizer of this neural network model is Root Mean Squared Propagation (RMSProp), and the loss function is categorical cross-entropy. Before fitting the model, categorical the labels first. Then, using the training data to train the detection model with batch size=1024. According to Figure 4, which represents the testing accuracy when setting all seven features as input, there is nearly no massive improvement in the model after the 20th iteration. Thus, setting epochs=20 is enough for the later analysis.

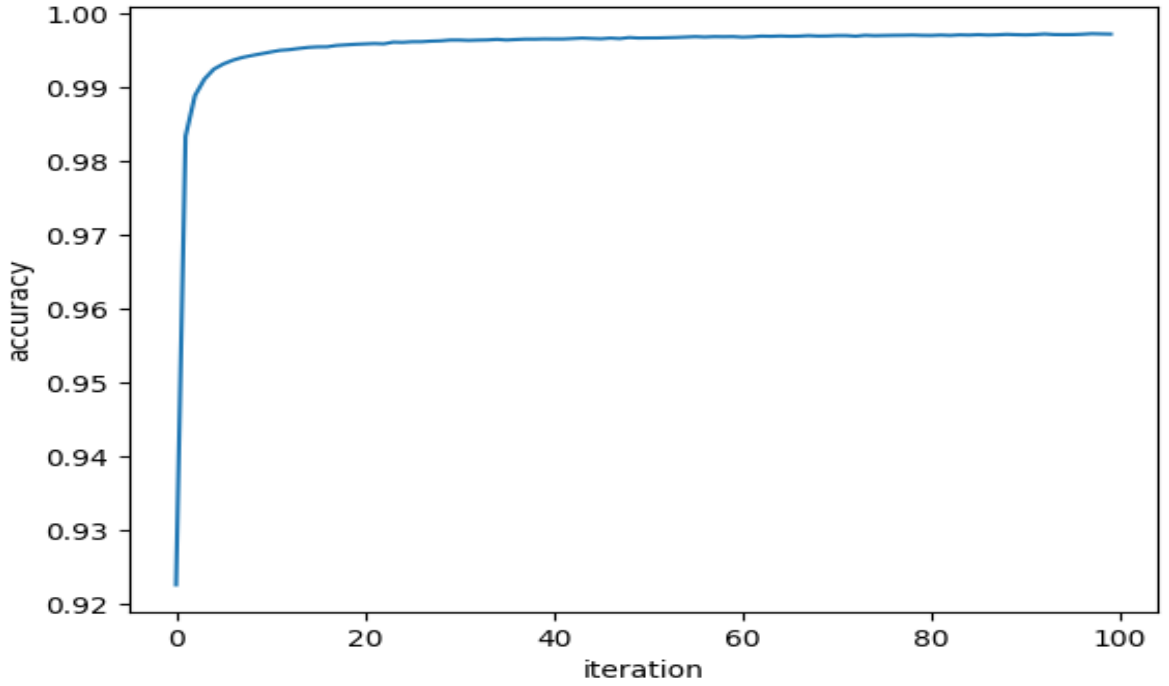

Figure 2. Testing accuracy.

3.4. Results and discussion

Applying the credit card fraud detection model based on the neural network declared above, the accuracy is 99.81% when inputting all the seven transaction features. To figure out the influence of different features on the detection accuracy, the author records the results after removing different parameters and the results are as Table 2 displays.

DOI: 10.54254/2755-2721/4/2023333

Table 2. Model accuracy after removing a feature.

Feature be Removed	Accuracy
distance from home	89.52%
distance from the last transaction	96.72%
ratio to the median purchase price	70.96%
repeat retailer	99.53%
used chip	98.67%
used PIN	99.17%
online order	97.44%

Although the detection accuracy has decreased after removing any of the seven transaction features, there is only a slight decrease in the accuracy without some parameters, such as *repeat retailer* (0.28%), *used PIN*(0.64%), and *used chip*(1.14%). Moreover, without *online order* or *distance from the last transaction* lowering the accuracy around 2.5%. Based on the results in Table 2, *ratio to the median purchase price* and *distance from home* are the two most significant features in this neural network model since the accuracy falls to 70.96% and 89.52%, respectively. Then, this paper analyzes whether there is a noticeable fall in accuracy after deleting two of the top five unimportant features. The results are as shown below.

Table 3. Model accuracy after removing top five unimportant features.

Features be Removed	Accuracy
distance from the last transaction & repeat retailer	96.60%
distance from the last transaction & used chip	96.17%
distance from the last transaction & used PIN	96.20%
distance from the last transaction & online order	94.65%
repeat retailer & used chip	99.00%
repeat retailer & used PIN	98.30%
repeat retailer & online order	97.39%
used chip & used PIN	98.50%
used chip & online order	96.55%
used PIN & online order	96.72%

Removing *repeat retailer* and *used chip* has an almost negligible effect on the model's accuracy, and removing *distance from the last transaction* and *online order* influences the performance most. In addition, it can be found from Table 3 that *repeat retailer* and *used chip* are the two features with the least significant among the five features, and *distance from the last transaction* and *online order* are the two features that have the most influence. Thus, the model is affected least without the most unimportant two features and influenced most by removing the most significant two input parameters. Furthermore, the performance of the model after removing two features is related to the accuracy after deleting each one of them, and there is no combination of two features that causes a surprise fall in the accuracy of the model after deleting them in the input layer.

To analyze more the impacts of features on transaction status detection, this research sets each feature as input separately to compare the accuracy of the neural network model. Under the case that there is only one feature in the input layer, *the ratio to the median purchase price* helps the neural

DOI: 10.54254/2755-2721/4/2023333

network model detect the highest accuracy(84.65%). The second best feature is *online order*, and the accuracy is 66.97%, which is unexpected since the model's accuracy is decreasing by around 3% after deleting this feature in the input layer when using all features. Therefore, *online order* might also play a significant role in detecting credit card fraud. Besides, *distance from home* also performs well, getting 61.31% accuracy. Then, under the situation that there is only one credit card transaction feature in the input layer, the accuracy getting by the rest features is around 50%, which means all the four features that *distance from the last transaction*, *repeat retailer*, *used chip*, and *used PIN* are nearly useless when any of them is in the input layer alone.

Table 4. Model Accuracy with top three important features.

Features	Accuracy
distance from home & ratio to the median purchase price	92.77%
distance from home & online order	66.78%
ratio to the median purchase price & online order	84.91%
distance from home & ratio to the median purchase price & online order	95.43%

After comparing the accuracy of the model with a single feature as input, the performance of different feature combinations is compared. The results of different combinations of *distance from home*, *ratio to the median purchase price*, and *online order* are presented in Table 4. Since the accuracy of the model with *distance from home* and *ratio to the median purchase price* as input is 66.97% and 84.65%, respectively, there is nearly no difference after adding *online order* to the input layer.

Moreover, when only inputting *distance from the last transaction*, *repeat retailer*, *used chip*, and *used PIN* in the neural network, the accuracy obtained by this model is 58.67%, which seems to indicate these four features do not play important roles. Then, adding *online order* to the input layer, the new accuracy is 71.06%. According to the data in Table 5, after adding *online order* to the input layer, the model is highly advanced when the only one feature is *distance from the last transaction* or *repeat retailer* or *used chip* or *used PIN*. Furthermore, the accuracy of any combination of two features among the above four features is lower than 57%. Then it can be concluded that the transaction feature *online order* can improve the model's performance with specific features.

Table 5. Model accuracy with one feature before and after adding online order.

Feature	Accuracy	New Accuracy After Adding online order
distance from the last transaction	53.62%	67.22%
repeat retailer	50.05%	66.97%
used chip	49.97%	67.11%
used PIN	55.43%	70.48%

Then, combine *distance from the last transaction*, *repeat retailer*, *used chip*, and *used PIN* with the top two essential features(*ratio to the median purchase price & distance from home*) to investigate the potential effects of these four features. Recall from the previous that the accuracy of *ratio to the median purchase price* is 84.65%, and the accuracy of *the distance from home* is 61.31%. After adding one of the above features, the accuracy shows no significant growth. Moreover, adding all four features is around a 5% increase in accuracy. Thus, *repeat retailer*, *used chip*, and *used PIN* have imperceptible influence on the neural network model.

After that, this paper will analyze the potential reasons for the fewer impacts on the detection model of the previous three features(*repeat retailer*, *used chip*, *used PIN*). Based on Figure 3, most

DOI: 10.54254/2755-2721/4/2023333

transactions happened from the same retailer, i.e., the value of *repeat retailer* is 1. In the dataset after applying SMOTE, around 49.958% of transactions from the same retailer are normal, and 50.042% are fraudulent. This makes the model can hardly detect fraud by *repeat retailer*. Similarly, about 47.206% of transactions without PINs are normal, and 52.794% are fraudulent. Moreover, nearly 47.054% of transactions without using chips are normal, 52.946% are fraudulent, 56.211% of transactions using chips are normal, and 43.789% are fraudulent. Therefore, the neural network detection model is less influenced by the three features since all the distributions of the three features are half on normal and half on fraudulent transactions.

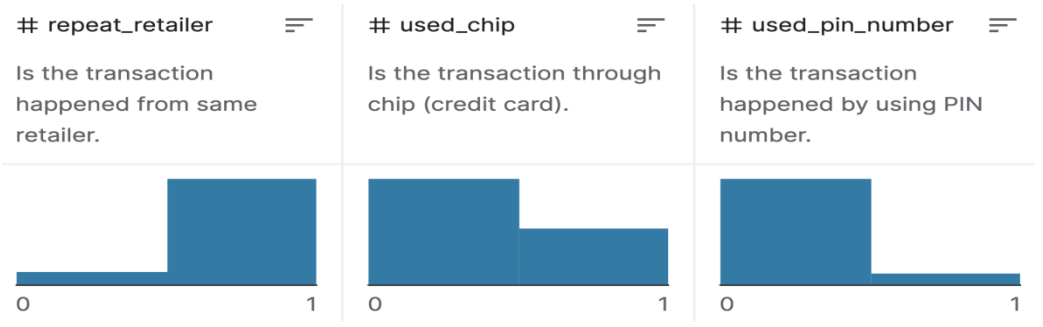

Figure 3. Data distribution.

According to the above analysis, *distance from home* and *ratio to median purchase price* have relatively significant influences on model performance, while *repeat retailer*, *used chip*, and *used PIN* have less influence. A potential reason for this result might be that the amount of information sent by features differs. Because *repeat retailer*, *used chip*, and *used PIN* are boolean features, they only send 0 (false) or 1(true) to the neural network model. However, the values of *distance from home* and *ratio to the median purchase price* are digits, which makes them able to send more hidden messages to the neural network. Therefore, the influence of the feature might depend on whether its value is boolean or digital type.

4. Conclusion

This research uses SMOTE to process imbalanced data and then constructs a credit card fraud detection model using the neural network containing four layers. There are seven features in total. After inputting different combinations of credit card transaction features, the finding is that although all details play different roles in the detection, their significance are different. The most influential feature is *ratio to the median purchase price*, and the second important parameter is *distance from home*. The accuracy of the detection model is 92.77% if there are only these two features in the neural network input layer. Additionally, the third meaningful parameter is *online order*. However, it cannot improve the model's performance when *the ratio to the median purchase price* or *distance from home* is already in the input layer, and the previous accuracy increases to 95.43% after adding *online order* as the input. Furthermore, the rest features(*distance from the last transaction, repeat retailer, used chip, and used PIN*) only have a little impact on this neural network model since the accuracy is 58.67% when only these four parameters are in the input layer. However, there are still some defects in this research. Since only seven features in the dataset are used for analysis in the research, there might be more details than this in the real world. The influence of the feature might be slightly different if more parameters were provided for each credit card transaction. In future, the author will find a balanced datastet with more credit card transaction features, and use model build by other type of neural networks to more accurately analyze the influences of different credit card transaction features.

DOI: 10.54254/2755-2721/4/2023333

Acknowledgment

First of all, I would like to thank professors in the university who taught me useful knowledge which laid a good foundation for me to complete this paper. Then, I am grateful to my parents and friends for their supports. Also, the data provided by Kaggle is important to this research.

References

[1] Financial Consumer Agency of Canada 2022, Credit card fraud, Retrieved March 22nd, https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html

[2] Federal Trade Commission 2022, Identify Theft Reports, Retrieved May 5th, https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime

[3] Federal Trade Commission. (2021) Consumer sentinel network data book 2020. https://www.ftc.gov/

[4] Hunter, P. (2004) Chip and PIN–biggest UK retail project since desalinization, but not enough on its own to defeat card fraud. Computer Fraud & Security, (5), 4-5.

[5] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017, October) Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 international conference on computing networking and informatics (ICCNI) (pp. 1-9). IEEE.

[6] Asha, R. B., & KR, S. K. (2021) Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), 35-41.

[7] Chen, J. I. Z., & Lai, K. L. (2021). Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence, 3(02), 101-112.

[8] Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019, March) Credit card fraud detection-machine learning methods. In 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-5). IEEE.

[9] Credit card fraud, Kaggle, https://www.kaggle.com/datasets/dhanushnarayananr/credit-card-fraud.

[10] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002) SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, 321-357.

[11] NN-SVG: Publication-Ready Neural Network Architecture Schematics, https://alexlenail.me/NN-SVG/.