A Fraud Detection Method for Online Payment Transactions Based on Deep Learning

Caixia Cui[a], Zhenyao Li[b], Yuanyuan Song[c]

[a]manta_dyl@163.com,[b]499847249@qq.com,[c]2858276455@qq.com

Taiyuan Normal University, Jinzhong 030619, Shanxi,China

Abstract. With the rapid development of the Internet, e-commerce and internet finance have achieved rapid development, but it has also brought serious problems of online payment risk fraud. Among them, the imbalance of financial data and the accuracy of online fraud detection are the main problems. Processing the original data and optimizing the algorithm model are important means to improve the accuracy of online fraud detection of unbalanced financial data. Among them, SMOTE algorithm, deep learning model, and mixed sampling algorithm are widely used. The deep learning model improves the accuracy of online fraud detection by improving the network structure. This article proposes an online transaction fraud detection method based on deep learning and SMOTE algorithm, which synthesizes minority class samples using the SMOTE algorithm and extracts data features using deep learning models to solve the problems of data imbalance and low fraud detection accuracy. This method is expected to provide more reliable guarantees for relevant industries, assist financial institutions and online payment platforms in timely and effective fraud detection and prevention, and provide guidance and suggestions for industry behavior.

Keywords: SMOTE algorithm; Deep learning; Data imbalance; Online fraud detection; Hybrid sampling algorithm

1 Introduction

To solve the classification problem of imbalanced data, scholars have proposed many methods, which are mainly divided into the processing of raw data and the optimization of algorithmic models[1]. The data processing methods are mainly based on statistical theory and other methods [2], which make the sample set change from category imbalanced distribution to balanced distribution by expanding or eliminating the sample set operation. For example, Wu, Haiyan et al [3] used the idea of SVM algorithm to improve the robustness of SMOTE model and used to deal with the classification of balanced data. Zhong-Yu Chen [4] used a logistic regression model to classify imbalanced data. Feng-Dong Han et al [5] improved the SMOTE algorithm and used it to deal with complex feature relationships.

Among them, the classical methods include SMOTE algorithm, improved SMOTE algorithm and hybrid sampling algorithm combining upsampling and downsampling.Haibo He et al [6] designed the refined Borderline-SMOTE method to solve the data imbalance problem, which improves the class distribution of the sample set by repeatedly sampling the boundary samples of small class samples. Jingxue Xuan et al. proposed an imbalanced data expansion sampling

ICEMBDA 2023, October 27-29, Tianjin, People's Republic of China

DOI 10.4108/eai.27-10-2023.2341915

algorithm by random linear interpolation between the center of a small class sample and its nearest neighbors through distance metric [7].

Deep learning is also used as an important tool to deal with imbalanced data. Based on the characteristics of traditional machine learning classification algorithms and the characteristics of imbalanced data sets, targeted improvements and optimizations are made to deep learning models and their fully connected neural network structures. Common ways include introducing penalty factors, using different activation functions, increasing the number of layers and nodes, and employing regularization techniques. Research on improving deep learning algorithms includes improvements to integrated learning algorithms, improvements to traditional binary classification algorithms and log-probability regression algorithms, and improvements to cost-sensitive algorithms based on In dealing with imbalanced data, Wang Zhongzhen et al. proposed to rank the large class data weights before the Adaboost iteration and select the large class data to be combined with the small class data to train the classification model based on the ranking result [8]. With these improvements, the performance of deep learning models and fully connected neural networks can be improved when dealing with imbalanced data. In conclusion, the processing of data imbalance problem is mainly to make the class distribution of the sample set more balanced, so as to improve the accuracy of fraud detection.

In order to solve the above problems, this paper proposes an improved classification method by combining deep learning and SMOTE algorithm. The main idea of the improved algorithm is to improve the class balance of the dataset using the SMOTE technique, i.e., the SMOTE technique increases the number of samples of fraudulent transactions by synthesizing a few classes of samples, thus balancing the dataset and enabling the classifier to better learn the features of fraudulent transactions. Then, the complex fraud patterns are captured using the powerful feature extraction and representation capabilities of the deep learning model. The improved algorithm is effective in improving the accuracy of fraud detection. The improved algorithm is expected to play an important role in online payment risk fraud detection and provide more reliable assurance and advice to guide the transaction behavior of related industries.

2 Related Technologies

2.1 SMOTE algorithm

SMOTE algorithm is an oversampling method for synthesizing minority class samples, the basic idea of which is to analyze the minority class samples and synthesize new samples based on the minority class samples and add them to the dataset, thus alleviating the problems caused by unbalanced data [9]. Steps for synthesizing new samples:

1) for each sample x_i in the minority class sample, calculate the Euclidean distance from that point to the other sample points to obtain k nearest neighbor samples;

2) Determine the sampling multiplicity N according to the imbalance ratio, and randomly select N samples among the k nearest neighbor samples for each minority class sample x_i, assuming that each selected nearest neighbor sample is x_{old};

3) Random current interpolation is performed between the original sample x_i and the randomly selected sample x_{old} to synthesize the new sample, and the interpolation is shown in table 1:

$$x_{new} = x_i + y(x_i - x_{old}) \tag{1}$$

where y denotes a random number between the interval (0,1).

Table 1. Algorithm specific flow

Input: minority class sample set T, sample x, number of sample nearest neighbors k, sampling multiplicity N; Output: synthetic minority class sample set S.
1 for i=1 to T do; 2 compute k nearest-neighbor samples of xi; 3 for n=1 to N do 4 randomly select samples x_{old} among the k nearest neighbor samples; 5 Generate a random number g between 0 and 1. 6 synthesize a new sample x_{new} according to the interpolation formula (1); 7 end for 8 add the new sample x_{new} to the set S 9 end for

2.2 Deep neural network

A deep neural network consists of an input layer, a hidden layer and an output layer. Neurons in each layer are connected to each other by full connectivity, and neurons in the same layer are not connected. The process of neuron transfer is as follows: the output value d^{l-1} of each neuron is multiplied with the corresponding weight W^l and summed cumulatively, and bias b^l is added to pass to the neuron connected with the value in the next layer, and then mapped by the activation function as the input value of the neuron in the next layer, as shown in Eq. 2:

$$a_i^{\zeta} = \sigma(Z_i^{\zeta}) \tag{2}$$

where Z_i^{ζ} is shown in equation 3:

$$z_i^{\zeta} = \sum_{k=1}^{m} w_{ik}^{\zeta} a_k^{\zeta-1} + b_i^{\zeta} \tag{3}$$

where Z_i^{ζ} is the input value of the ith neuron in layer L, $a_k^{\zeta-1}$ is the output value of the kth neuron in layer L-1, w_{ik}^{ζ} is the weight corresponding to the kth neuron in layer L-1 connected to the ith neuron in layer L, b_i^{ζ} is an offset, and $\sigma(Z_i^{\zeta})$ is an activation function.

2.3 Model analysis

1.Evaluation indicators

The confusion matrix is shown in Table 2:

Table 2. Confusion matrix of classification results

The real situation	Predicted Situation	
	Positive category	Reverse class
Positive category	TP	FN
Reverse class	FP	TN

Table 1 Confusion matrix of classification results

In Table 2, Ture Positive (TP) represents the number of positive classes predicted as positive classes. True Negative (TN) represents the number of negative classes predicted as negative classes. False Positive (FP) represents the number of negative classes predicted to be positive. False Negative (FN) represents the number of positive classes predicted as negative classes. tP and TN represent the cases of correct predictions, and FN and FP represent the cases of incorrect predictions.

Based on the confusion matrix, common evaluation metrics include Accuracy, Loss, Precision, Recall, G-mean, F1 value, and AUC (Area Under ROC Curve).

Accuracy represents the proportion of TP and TN to the number of all samples, as shown in equation 4:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

Generally speaking, the higher the ACC, the better the classifier.

Precision represents the ratio of TP to the total number of TPs and FPs, as shown in Equation 5:

$$\Pr ecision = \frac{TP}{TP + FP} \tag{5}$$

Recall represents the proportion of TP to the total number of TP and FN, as shown in equation 6:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{6}$$

The F1 value is shown in equation 7:

$$F1 = \frac{2 \cdot TP}{2 \cdot TP + FP + FN} \tag{7}$$

The AUC represents the area under the ROC curve, which is between 0.5 and 1. The ROC curve is an important tool for studying the generalization performance of a learner, and the vertical coordinate of the ROC is the True Positive Rate (TPR) and the horizontal axis is the False Positive Rate (FPR) as shown in Eqs. 8 and 9:

$$TPR = \frac{TP}{TP + FN} \tag{8}$$

$$FPR = \frac{FP}{TN + FP} \tag{9}$$

G-mean is shown in equation 10:

$$G - mean = \sqrt{TPR \cdot TNR} \tag{10}$$

These evaluation metrics can help us assess the performance of the model in classification and regression tasks.

2. online transaction fraud detection model based on deep learning

In this paper, we propose a fully connected neural network based online transaction fraud detection method and combine the hybrid sampling technique using SMOTEENN model to construct a SMOTEENN-FCNN model (SFC) for solving the transaction fraud detection data imbalance problem.The steps of SMOTEENN are as follows:

1) Construct the SMOTEENN model by combining SMOTE and ENN;

2) generate synthetic minority class samples using the SMOTE algorithm, thus increasing the number of minority class samples;

3) Use the ENN algorithm to remove the noise and overlapping samples from the majority class samples, thus reducing the number of majority class samples.

SMOTEENN can better balance the data set and improve the generalization ability and robustness of the model.

The core idea of SFC is to extract key features from complex transaction data and achieve accurate fraud detection by building a fully connected neural network model and using its powerful learning capability.

The algorithmic steps of SFC are as follows:

1) Data collection and pre-processing: Collect online transaction datasets, including information on normal and fraudulent transactions. Pre-processing operations such as cleaning, de-duplication and handling missing values are performed on the data. Data set partitioning and label processing: The data set is partitioned into a training set and a test set. The labels are set to 1 and 0 for dichotomous classification according to fraudulent transactions and normal transactions. For data columns containing string features, they are processed using One-Hot encoding to convert them into numerical features. This preserves the classification information and makes it suitable for deep learning algorithms. After processing, the feature data of both the training and validation sets are One-Hot encoded. Feature scaling is performed on the feature data of both training and validation sets, and RobustScaler is used for the scaling operation. The feature scaling can unify the feature values of different scales into one range, which is beneficial to the training and convergence of the model.

2) Data balancing processing: A hybrid sampling technique is used, combining oversampling and undersampling methods, to achieve the effect of data set balancing by synthesizing a few class samples and randomly reducing the majority class samples. Construction of SMOTEENN model: The SMOTE algorithm is used to generate synthetic minority class samples and increase the number of minority class samples. The noise and overlapping samples in the majority class samples are removed using the ENN algorithm to reduce the number of majority class samples. Fully-connected neural network model construction and training:

3) Design a fully connected neural network model including multiple fully connected layers for feature extraction and learning. Training and parameter tuning of the model using appropriate activation functions, loss functions, and optimization algorithms.

4) Model testing and prediction: Use the trained model to predict the new transaction data and get the prediction results. Fraud classification judgment is performed according to the prediction results and the set threshold.

5) Result evaluation and analysis: Evaluate the prediction results of the model, including accuracy, recall, precision and other indicators. The performance of the model is analyzed, and improvement strategies and adjustment parameters are proposed.

By using the SFC model, the method in this paper can effectively cope with the data imbalance problem in transaction fraud detection and improve the accuracy and reliability of fraud detection. The method is of great significance in practical applications and can help financial institutions and online payment platforms, etc. to conduct timely and effective fraud detection and prevention.

3 Experimental results and analysis

3.1 Experimental design

The experimental environment of this paper: the CUP is Intel core i5, RAM is 32GB, and the programming language is Python.

3.2 Experimental Data

The experimental data used in this paper comes from the transaction records of online payment fraud detection publicly available on kaggle (https://www.kaggle.com/datasets/rupakroy/online-payments-fraud-detection-dataset). The dataset is provided by Rupak Roy and contains 6,362,620 transaction records. The characteristics of the dataset are shown in Table 3:

Table 3. Feature table of the data set

Features	Meaning
step	Time steps in seconds from the start of data collection
type	Types of transactions, including payments, refunds, withdrawals, etc.
amount	Transaction amount
nameOrig	Indicates the name of the original account

	that initiated the transaction
oldbalanceOrg	Indicates the name of the target account receiving the transaction
newbalanceOrig	Indicates the balance of the original account before the transaction
nameDest	Indicates the name of the target account receiving the transaction
oldbalanceDest	Indicates the balance of the target account before the transaction
newbalanceDest	Indicates the balance of the target account after the transaction
isFraud	Indicates whether the transaction is fraudulent (1 is fraudulent, 0 is normal)
isFlaggedFraud	Indicates whether a transaction is flagged as fraudulent

3.3 Comparison of experimental models

To demonstrate the prediction effectiveness of SFC, this paper compares the performance of SFC with S-XGB-SMOTE [10], XGBOOST [11], SVM, AdaBoost [12], and GBDT [13]. Among them, the datasets used for S-XGB-SMOTE, XGBOOST, SVM, AdaBoost and GBDT are the ATEC competition (http://www.atecup.com/home) held by Anthem in 2018, where the risky payment identification event publicly provides desensitized online transaction payment data.

3.4 Experimental results

In terms of evaluation metrics, this paper will mainly use AUC, G-mean, F1, Recall, and Precision, which are most commonly used in imbalanced data classification studies, to make performance judgments, with data including 4 decimal places, as shown in Table 4:

Table 4. Performance comparison effect of 6 models

	AUC	G-mean	F1	Recall	Precision
SFC	0.9958	0.9970	0.9856	0.9941	0.9772
S-XGB-SMOTE	0.8963	0.5784	0.7128	0.6703	0.5121
XGBOOST	0.9402	0.6942	0.6476	0.4820	0.9866
SVM	0.8654	0.6895	0.6444	0.4754	1.0000
AdaBoost	0.9341	0.6964	0.6366	0.4852	0.9250
GBDT	0.9333	0.6987	0.6354	0.4885	0.9085

From Table 4, it can be seen that based on the five evaluation metrics, the prediction performance of SFC is optimal compared with the other five classification models, which illustrates the prediction effectiveness and processing capability of SFC for imbalanced data such as online payment transaction fraud data.

Setting EPOCH as 10, SFC is trained and tested, and the Accuracy of the training and testing process of SFC is recorded as shown in Figure 1:

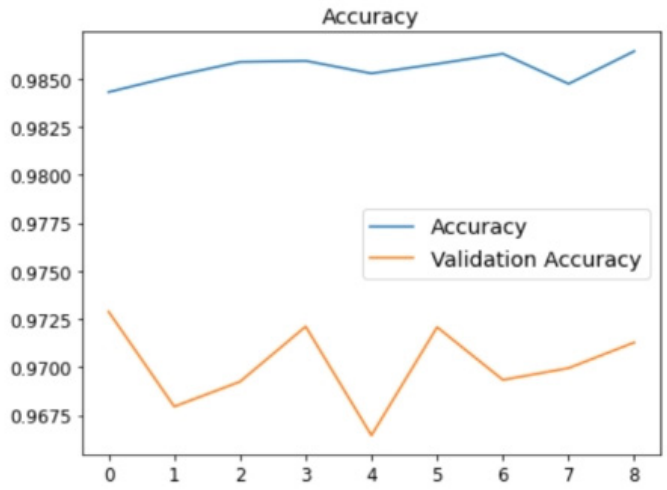

Fig. 1. Accuracy curve of SFC

From Fig. 1, it can be seen that SFC can obtain high accuracy in a very short EPOCH, no matter under the training set or under the test set, although the accuracy of SFC under the test set is lower than that under the training set, but the accuracy of SFC under the test set is still very high, higher than 0.95. This indicates that the prediction of SFC for unbalanced data The accuracy of SFC is very high.

The Losses recording the training and testing process of SFC are shown in Figure 2:

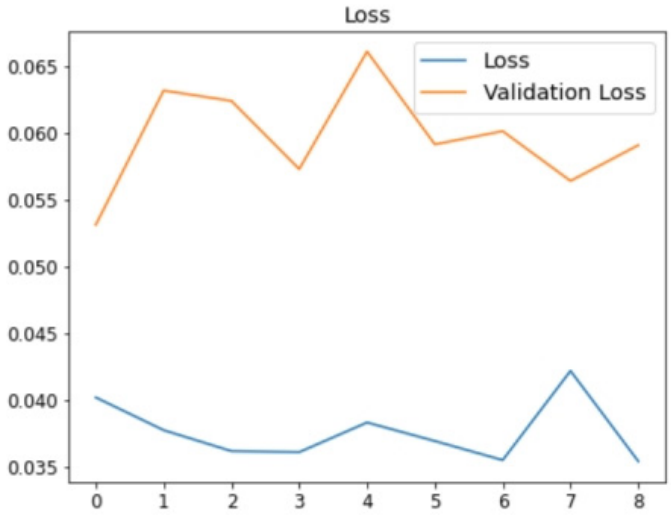

Fig. 2. Loss curve of SFC

From Fig. 2, it can be seen that the loss of SFC in the training set is very small, although there is a peak at EPOCH 7, the loss value is still only 0.043, which indicates that the prediction accuracy of SFC in the training set is very high. At the same time, the arc of change of the Loss

curve in the test set is relatively small, which indicates that the prediction performance of SFC is relatively stable under the test set. In summary, the performance of SFC is very accurate in the prediction of unbalanced data.

4 Conclusion and Prospect

In this paper, SFC is proposed for detecting fraud based on imbalanced transaction data.SFC uses a layer-by-layer increase in the number of neurons to construct a neural network model to extract feature information at different levels.SFC introduces an activation function for nonlinear features to better output binary classification results. Comparative experiments are designed using five classical classification algorithms to verify the prediction performance of SFC for fraud on unbalanced data. The experimental results show that SFC has higher prediction performance compared with other 5 classification algorithms, which indicates that SFC effectively improves the imbalance problem of unbalanced data and reduces the impact of data imbalance on the prediction ability of the classifier, which provides guidance suggestions for the decision-making behavior of related industries.

SFC solves the imbalance problem of imbalanced data to a certain extent and is also able to predict fraudulent behavior in the context of imbalanced data efficiently. However, there are still some aspects of SFC that can be improved, such as SFC only considers the imbalance of data but not the time-series of data, and the data set used in this paper is relatively homogeneous. Based on the above problems, future work will focus on the following two points: (1) To propose a time-series based SFC, so that the time-series of the data can also be fully considered. (2) Exploring the prediction performance of SFC on more classical datasets and the ability to deal with imbalance of unbalanced data.

References

[1] Xiu Hua. Research on the current situation and countermeasures of e-commerce fraud governance in China [D]. Qingdao University, 2020.

[2] Mike Josn. A review of research on classification methods for unbalanced datasets[J]. Computer Application Research,2022,39(06):1615-1621.

[3] Wu H Y,Chen X L,Fan G X. An adaptive kernel SMOTE- SVM algorithm for imbalanced data classification[J]. Journal of Beijing University of Chemical Technology (Natural Science Edition),2023,50(02):97-104.DOI:10.13543/j.bhxbzr.2023.02.012.

[4] Chen, J. Y., Yin, J. L.. FL logistic regression algorithm for imbalanced data classification problem[J]. Statistics and Decision Making,2023,39(05):33-37.

[5] Mary Yone. Research application of feature learning and classification for network security imbalance data[J]. Science, Technology and Engineering,2023,23(03):1130-1137.

[6] He, H., Bai, Y., Garcia, E. A., & Li, S. (2009). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. in IEEE International Joint Conference on Neural Networks (IJCNN) (pp. 1322- 1328). IEEE.

[7] Peter Pmer Improvement of SMOTE-based unbalanced expansion sampling algorithm[J]. Science and Technology Wind,2023,No.524(12):1-3.

[8] Wang ZZ, Huang B, Fang ZJ, et al. Improved SMOTE for imbalanced data integration classification algorithm[J]. Computer Applications,2019,39(9):2591-2596.
[9] Li Y, Liu ZD, Zhang N. A review of integrated classification algorithms for imbalanced data[J]. Computer Application Research,2014,31(05):1287-1291.
[10] Xu M. Research on online transaction fraud detection based on time-series unbalanced data[D]. University of Electronic Science and Technology,2019.
[11] Yang, L.K., He, P.Y., Pan, Fan, Fang, A.C.. Research on emotional recognition of ECG signals based on XGBoost-RFE-CBR[J]. Journal of Chengdu University of Information Engineering,2023,38(03):258-263.DOI:10.16836/j.cnki.jcuit.2023.03.002.
[12] Xu W. Qian. Credit risk assessment model based on ADASYN-AdaBoost-CNN [J]. Modern Computer,2021,27(28):39-44.
[13] Wang Shiyang. Research on sales volume prediction based on a new data imbalance processing method[D]. Nanchang University, 2022. DOI:10.27232/d.cnki.gnchu.2022.004446.