Credit Card Fraud Detection Using Boundary Reconstruction and Integrated Classification

Wei Zhou
School of Finance, Yunnan University of Finance and Economics, Kunming, 650221, P.R. China
zw453@163.com

Xiaorui Xue
School of Finance, Yunnan University of Finance and Economics, Kunming, 650221, P.R. China
87208608@qq.com

Danxue Luo*
School of Finance, Yunnan University of Finance and Economics, Kunming, 650221, P.R. China
1034159312@qq.com

ABSTRACT

With the popularity of electronic payment, it not only brings great convenience, but also increases the risk of fraudulent transactions. At present, there are two problems in the identification of credit card fraud. The number of fraud and normal transactions is extremely unbalanced and the classification boundary is fuzzy. In order to solve these problems, this paper proposes an integrated classification framework for boundary reconstruction, which uses different machine learning algorithms as base learners to compare the original data with the data modeling after boundary reconstruction. The research shows that data boundary reconstruction can not only effectively alleviate the deviation caused by data imbalance to machine learning. It can also improve the data quality, so as to improve the accuracy of model classification; The integrated classification method can accurately identify credit card transactions, and the prediction effect of decision tree is the best. The proposed model is also applicable in other abnormal situations.

CCS CONCEPTS

• **Information systems**; • **Information systems applications**; • **Data mining**;

KEYWORDS

Boundary reconstruction, Machine learning, Credit card fraud detection, Integrated learning

ACM Reference Format:
Wei Zhou, Xiaorui Xue, and Danxue Luo. 2022. Credit Card Fraud Detection Using Boundary Reconstruction and Integrated Classification. In *2022 4th International Conference on Big Data Engineering (BDE 2022), May 26–28, 2022, Beijing, China.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3538950.3538962

1 INTRODUCTION

With the rapid development of the Internet, electronic payment has gradually replaced cash payment and become the main tool of payment in people's daily life. While the electronic payment platform brings great convenience to people, it also increases the risk of fraudulent transactions. Although credit card fraud accounts for less than 1% of credit card transactions, it may still cause huge losses. Data show that on May 15, 2016, a premeditated gang of 100 people stole $12.7 million from 1400 convenience stores in Tokyo with more than 1600 South African credit cards in just three hours. By the end of 2020, China had 778 million cards in use, 0.56 cards per capita, and the credit card fraud rate was 1.91%. If not controlled, credit card fraud will even impact the financial system and increase financial risks.

In order to prevent huge losses caused by credit card fraud, many banks detect and identify their credit card transaction data. Credit card transaction data is usually composed of text information such as data of both parties, transaction amount and relevant background information of both parties. For example, private information such as credit card number of both parties and family conditions of the lender are encrypted and desensitized by the bank and converted into digital data that can be used by machine learning algorithm. At present, the mainstream model of credit card fraud detection is data-driven machine learning deep learning model. Although many models have modeled credit card data and produced good detection results, the identification of credit card fraud still has the following two challenges:

Firstly, how to find the classification boundary between normal transactions and fraudulent transactions in credit card transactions. The quantitative data of normal transactions and fraudulent transactions are usually highly coincident, and the boundary between them is difficult to define. Because there are some abnormal transactions in the normal behavior of the legal person; to cover up their behavior, fraudsters will hide the fraud under "normal" behavior as much as possible. Therefore, how to distinguish the highly overlapping two types of credit card transaction data is a major challenge in modeling. Secondly, how to solve the problem of low amount of fraudulent transaction data in the training model. In the face of unbalanced data, data-driven models or algorithms prefer to predict most samples in the optimization process of minimizing error and regard a few fraudulent transactions as noise factors in the data, to obtain false good model performance indicators. But in practice, the model cannot identify fraudulent transactions, causing huge losses to banks. Therefore, the imbalance of data sets also increases the difficulty of detection.

Based on the above challenges, this paper proposes a boundary reconstruction integrated classification framework to detect fraud. Specifically, boundary reconstruction is used to improve the imbalance and quality of data sets, and integration classes are used to

*Corresponding Author

BDE 2022, May 26–28, 2022, Beijing, China

ACM ISBN 978-1-4503-9563-2/22/05…$15.00
https://doi.org/10.1145/3538950.3538962

learn various potential characteristics of fraudulent transactions. The rest of the paper is structured as follows: the second section introduces the research on dealing with specific problems, the third section introduces the overall framework of the model, and the fourth section introduces the data set, the parameter setting of the model and the empirical results. Finally, concluding remarks are discussed in Section V, followed by a list of literature.

2 RELATED WORK

Credit card fraud causes huge losses every year. Researchers aim to find a solution to detect fraudulent transactions. At present, several methods have been proposed and tested. These related studies are briefly described below.

Firstly, since the number of fraudulent transactions in credit card transactions is far less than the number of normal transactions, this imbalance will make the machine learning algorithm treat the fraudulent transactions as noise and ignore them [2]. Literature [18] and [24] studied the identification of credit fraud from the perspective of uneven data distribution. Literature [31] proposed a transaction aggregation framework for the heterogeneity of credit card transaction data and studied it with two real data. It was found that transaction aggregation can improve the performance of the model in many cases; In addition to using transaction aggregation to learn a variety of transaction behaviors, literature [19] adds a behavior feedback mechanism to the framework, so that the model can dynamically capture the changes of transaction behavior. On the other hand, literatures [27] and [32] solve the problem caused by the uneven distribution of credit card data by data remodeling. General data reconstruction methods include over-sampling [6, 11, 15] and under-sampling [16, 28, 29]. In addition, literature [1] focuses on the losses caused by credit card fraud to banks and modifies the loss function to make the model sensitive to the possible high losses; Other scholars also consider cost sensitive factors in the loss functions of different models [11, 26, 26], which improves the accuracy of prediction. Literature [7] makes an additional difference adjustment questionnaire for cardholders. The results show that the questionnaire can also make the model further capture the characteristics of cardholders' transaction behavior. Literatures [20] and [30] preprocess the data by clustering and find that the correct clustering can significantly improve the performance of the model, but the inappropriate clustering will make the model easier to ignore the rare fraud.

Ensemble learning is also used in credit card fraud detection scenarios. Literature [23] used random forest to model and predict credit card data, verified that it is suitable for high-dimensional credit card data, and has a certain processing ability for missing value data. Aiming at the conceptual drift of credit card user behavior change, literature [27] proposed ITrAdaboost model, which updates (i.e. increases or decreases) the weight of misclassified instances in the source domain according to the distribution distance from the instance to the target domain, and verified the accuracy of its prediction on five credit card data sets. Deep learning also performs well in the field of credit card fraud detection. Both references [13] and [14] apply convolutional neural network to credit card fraud identification and detection. The empirical results show that CNN has better prediction effect. Literature [22] proposed a new loss function - total center loss function (FCL), which considers the distance and angle deviation between features, and empirical analysis shows that this loss function is better than other methods. In addition, Literature [25] introduced the encoder decoder architecture into the field of credit card fraud identification to solve the extremely unbalanced distribution of credit card transaction data. Literature [12] uses the example of generating a small number of classes using the generative countermeasure network Gan into an enhanced training set, and the empirical results show that the accuracy of the classifier trained with the enhanced data set is significantly higher than that trained with the original training set.

The above models or methods provide valuable experience for fraud detection. However, most of them innovate in the model, and there is little research on improving data quality. This paper proposes an integrated classification framework of boundary reconstruction, which can improve the separability of data while manually generating a few class samples. Then use the integrated classification model to detect the credit card transaction data.

3 PROPOSED MODEL

This section will introduce the overall architecture of the credit card fraud detection model. The model is mainly composed of three parts: data boundary reconstruction module, integrated classification module and model evaluation module. The boundary reconstruction of credit card data uses the borderline smote method to improve the quality of the data set and reduce the impact of imbalance on the algorithm; AdaBoost model is used to learn the characteristics of credit card fraud transactions and classify the transaction data; Finally, select the appropriate indicators to evaluate the model.

3.1 Data Boundary Reconstruction

Data driven machine learning models often perform poorly in the face of data with extremely unbalanced distribution, and the model is more inclined to predict most classes. In this paper, the borderline smote resampling method is used to expand the data, which effectively alleviates the problem of unbalanced data distribution, and improves the accuracy of machine learning algorithm. The most common resampling method is random over sampling. Although this method improves the imbalance of data distribution, it will make the model over fit a very small number of fraud samples and have poor recognition ability for unlicensed fraud transactions. Chawla et al. proposed an improved scheme based on random oversampling method - synthetic minority over sampling technology [3]. Smote algorithm analyzes a small number of fraud samples and manually generates new samples to be added to the data set. This oversampling method alleviates the problem of model over fitting caused by ROS to a certain extent. However, for the credit card fraud data set, in order to avoid detection, the transaction data often highly coincides with the normal transaction behavior, which makes a small number of samples synthesized by smote algorithm partially coincide with the normal transaction data, resulting in the model easy to misjudge some normal transactions. In order to avoid this situation, Han et al proposed an improved smote method - synthetic minority over-sampling technique [8]. Based on the smote method, this method divides a few samples into three categories:

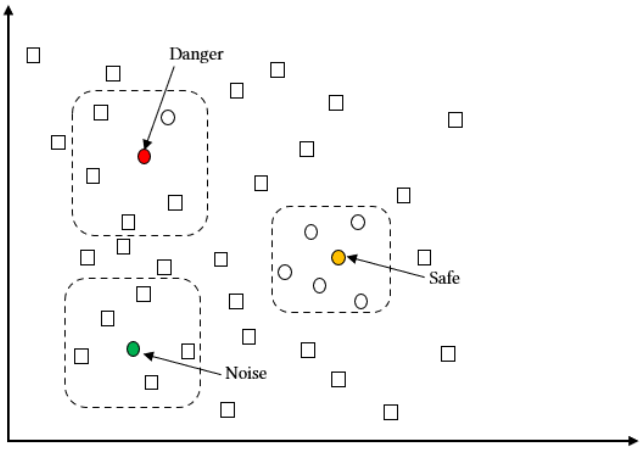

Figure 1: Schematic diagram of SMOTE point classification

safe, danger and noise. Only the danger samples are sampled to make the generated samples. The data boundary reconstruction method is as follows:

Suppose that the data set is composed of majority class sample set $P = \{p_1, p_2, \ldots\}$ and minority class sample set $N = \{n_1, n_2, \ldots\}(|P| \gg |N|)$. $P_{i,J}$ is the subset of majority class sample obtained by minority class sample points n_i using K nearest neighbor algorithm, and $N_{i,L}$ is the subset of minority class sample obtained by minority class sample points n_i using K nearest neighbor algorithm, where J and L respectively represent the number of subset of majority class and minority class sample.

Firstly, for any minority sample $n_i \in N$, calculate and confirm the sum of its nearest neighbor's sample set $P_{i,J}$ and $N_{i,L}$, where $P_{i,J} \in P$, $N_{i,L} \in N$, and $J + K = L$. Then judge the category of a few samples n_i. If more than half of the nearest neighbor points of the sample points n_i belong to the subset of majority classes $P_{i,J}$, that is $\frac{K}{2} \leq J < K$, they belong to Danger class; If more than half of the nearest neighbor points of the sample points n_i belong to a minority subset $N_{i,L}$, that is $L > \frac{K}{2}$, they belong to Safe class; If all the nearest neighbor points of the sample points n_i are samples of majority classes, that is $J = K$, they belong to Noise class, as Figure 1

After classifying the sample points, a few sample points based on the Danger class manually generate new samples. For any sample point n_i of Danger class, randomly select the sample points $n_{i,l}$ $(0 < l \leq L)$ in its nearest neighbor set (1) and synthesize new samples through linear interpolation.

$$n_i^* = n_i + rand\,(0,\ 1) \times n_i - n_{i,l_2} \tag{1}$$

Finally, repeat the above operations to generate samples until the number of samples of a few types meets the conditions.

After the boundary reconstruction module, the fraudulent transaction of the credit card data set is expanded to the same amount of data as the normal transaction, which greatly alleviates the model error caused by the extreme imbalance of categories in the machine learning algorithm. At the same time, compared with other data enhancement methods, the quality of fraud transaction samples manually generated by borderline smote method is significantly improved, and the classification boundary formed by data is more obvious, so as to further improve the recognition performance of the model.

3.2 Integrated Classification

AdaBoost is a very popular integration algorithm in the field of machine learning. The main idea of the integration algorithm is to train multiple weak learners and form a strong learner through certain methods (such as bagging and boosting), so that the strong learner has a better prediction accuracy. AdaBoost algorithm continuously increases the weight of misclassified instances in the iterative process, and finally weights the results of all weak classifiers as the prediction results. Suppose the dataset is $D = \{(x_1, y_1),\ (x_2, y_2), \ldots\}$, $|D| = m$, which represents the number of instances in the dataset. The training process of AdaBoost algorithm is as follows:

Initialize the weight of each sample in the dataset. Each sample is given equal weight at the beginning of training. The sample weight vector of the data set is expressed as $W_1(X) = (w_1(x_1), w_1(x_2), \ldots, w_1(x_m)) = (\frac{1}{m}, \frac{1}{m}, \ldots, \frac{1}{m})$, where the lower corner of the weight vector represents the iteration round. Perform iterative training $t = 1, 2, \ldots, T$. In iteration t :

1. Select the weak classifier α with the worst prediction effect as the t-th base classifier A_t.

2. Calculate the training error e_t of the classifier $A_t : X \rightarrow \{-1,\ 1\}$. The training error of the t-th iteration is (2):

$$e_t = P\left(\sum_{i=1}^{m} A_t\,(x_i) \neq y_i\right) = \sum_{i=1}^{m} w_i I\,(A_t\,(x_i) \neq y_i)\,, \tag{2}$$

where $I(\cdot)$ indicates the indicator function.

3. Calculate the weight of the classifier in the last strong classifier A_t (not normalized) (3):

$$a_t = \frac{1}{2}\ln\left(\frac{1 - e_t}{e_t}\right) \tag{3}$$

4. Update the weight distribution $W_{t+1}(X) = (w_{t+1}(x_1), w_{t+1}(x_2), \ldots, w_{t+1}(x_m))$ of the data set D in the next iterative training (4):

$$w_{t+1} = \frac{w_t\,(x_i) \exp\,(-a_t y_i A_t\,(x_i))}{Z_t},\ i = 1, 2, \ldots, m \tag{4}$$

where Z_t is the normalization constant, $Z_t = \sum_{i=1}^{m} w_t(x_i)\exp(-a_t y_i A_t(x_i)) = 2\sqrt{e_t(1 - e_t)}$.

After the iteration is completed, the weighted average is carried out according to the weight of each weak classifier, and then the final output result $\hat{y}$ is obtained through the sign function (5):

$$\hat{y} = sign\,(f\,(x)) = sign\left(\sum_{i=1}^{T} a_t A_t\,(x)\right) \tag{5}$$

3.3 Model Evaluation

The last module is to test and evaluate the model. Model evaluation is the most important link in any modeling task. In this module, the test set is used to test each generated base classifier, and then the results of the test set are determined by aggregating the results of all base classifiers. Finally, the prediction results are used to calculate

Table 1: Basic form of confusion matrix

		True	
		Legality 0	Fraud 1
Prediction	Legality 0	TN	FN
	Fraud 1	FP	TP

the indicators to evaluate the fraud recognition performance of the model. Evaluating the performance of the model mainly involves three aspects. The first is the selection of indicators to evaluate the performance of different fraud identification models. The second is whether the model recognition is effective, that is, to compare the difference between the trained model and the random prediction model. Finally, whether the credit card fraud identification model based on machine learning is better than other machine learning models. In order to measure the representation of credit card fraud identification model, this paper intends to use accuracy, recall, specificity and f indicators. In this paper, all evaluation indexes are composed of four classification types in the confusion matrix: true positive (TP), true negative (TN), false positive (FP) and false negative (FN). The confusion matrix is the most basic situation analysis form based on real value and predicted value in the classification algorithm. For a binary classification problem, the basic forms of confusion matrix and various indexes are:

Precision refers to the proportion of real fraudulent transactions in the data predicted as fraudulent transactions, which reflects the discrimination and classification ability of the model for normal transactions and fraudulent transactions. For different model algorithms, the higher the accuracy rate, the lower the cost for the issuer to misjudge the normal transaction as a fraudulent transaction.

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

Recall refers to the proportion of correctly classified samples in the total sample of fraudulent transactions. This indicator focuses more on reflecting the learning ability of the model to the characteristics of fraudulent transactions. The higher the recall rate, the better the effect of the model in learning fraudulent transactions.

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

Specificity refers to the proportion of correctly classified samples in the total sample of normal transactions. The special gradient is opposite to the recall rate, and focuses on the learning ability of the model to the characteristics of normal transactions. The higher the specificity, the better the effect of the model to learn normal trading behavior.

$$Specificity = \frac{TN}{TN + FP} \tag{8}$$

Accuracy is usually an indicator that reflects the overall prediction accuracy of the model. However, in this paper, due to the large gap between the data volume of ordinary transactions and fraudulent transactions, the model will get a very excellent accuracy indicator, but the model does not have the ability to identify fraudulent transactions. This paper will use this index to show the deceptiveness of the model in the face of unbalanced data.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

F1-score is an index composed of accuracy and recall rate. It no longer focuses on the performance of one aspect of the model, but gives a comprehensive index according to the overall performance of the model. Similarly, the higher the F1-score, the better the overall performance of the model.

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{10}$$

4 RESULTS AND DISCUSSION

4.1 Dataset

The credit card fraud data set used in this paper is the public data set of credit card transactions from Kaggle platform. This dataset contains all credit card transactions recorded by European cardholders on a certain two days in September 2013[3-5, 8-10, 21]. Due to the confidentiality agreement of credit card user information, the data provider cannot provide the original data and relevant background information of credit card transactions. In addition to leaving the "time" and "amount" features in the original transaction data, the principal component analysis (PCA) is used to convert the personal transaction data into features v1-v28, the "time" feature shows the time between the first transaction and all other transactions in the data set, and the "amount" feature represents the transaction amount of each transaction. For the data label, the data identified as fraudulent transactions in the "class" feature is marked as 1 and the normal transaction is marked as 0. Finally, the data set includes 284807 transaction records, of which 492 transactions are fraudulent transactions, and all transactions are true. Considering these figures, we can see that this data set is highly unbalanced, and only 0.173% of transactions are marked as fraud. Because the distribution proportion of classes plays an important role in the accuracy and accuracy of the model, data preprocessing is very important. This paper adopts the following processing methods for the data:

The credit card data set is collected and marked by ULB's machine learning team. There are no missing values in the data, so there is no need to fill in the data. Due to the differences in the maximum and minimum values of different features of credit card data, in order to avoid the impact of different feature dimensions on model training, we need to normalize the features of credit card transaction data. The most common normalization is the minimum and maximum normalization. In this paper, the features in the credit card data set are normalized, and the normalization formula is as follows:

$$x_{i,0-1} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \tag{11}$$

4.2 Model Selection and Parameter Setting

In order to better measure the performance of the fraud identification model, this paper uses different machine learning algorithms as the base learner algorithm of the model framework, and compares the fraud identification model trained by the original credit card data with the model trained by the boundary reconstruction credit card data. We use Python 3 9 model with the third-party library scikit learn 0.24.2. The following are the parameter settings of different base learners:

Decision tree (DT) is a tree structure machine learning algorithm. It generates the internal nodes of the tree based on some index of different characteristics, so as to realize the modeling of data. The parameter settings are as follows: set the classification standard to "Gini"; Feature selection is set to "best"; The classification algorithm is set to "CART".

Logistic regression (LR) is a logarithmic linear model. It linearly models the data characteristics in the form of logarithmic probability. The parameters of logistic regression classifier are set as follows: the penalty item is set as l_2 penalty, and the penalty parameter $\lambda = 1$; The optimization algorithm uses "lbfgs".

$$l_2 = \lambda \sum_{w} w_2^2 \tag{12}$$

where w is the model parameter.

Perceptron is a machine learning algorithm for binary classification. It divides the data set by minimizing the loss function training hyperplane. It is the prototype of neural network. The parameters of perceptron classifier are set as follows: the penalty item is set as l_2 penalty, the optimization algorithm uses random average gradient descent method, and the learning rate $\eta = 1$.

Support vector machines (SVM), similar to perceptron algorithm, aims to find a hyperplane to divide the data set, but the difference is that support vector machines use interval maximization to determine the optimal hyperplane. In this paper, linear support vector machine is used as the base learner, and its parameters are set as follows: the penalty term is set as l_2 penalty, and the penalty parameter $\lambda = 1$; The loss function uses the squared hinge function. The hinge loss function is:

$$hinge\ loss = \max(0,\ 1 - \hat{y}y) \tag{13}$$

where $\hat{y}$ is the predicted value and y is the real value.

Naïve Bayes (NB) is a machine learning classification algorithm based on Bayesian theorem. Under the assumption of independent feature conditions, the maximum a posteriori probability of samples is obtained. In this paper, Bernoulli naive Bayes is used as the base classifier of fraud recognition model, and its parameters are set as follows: the smoothing factor α is 1; The prior probability of the sample is not given in advance.

Finally, about the parameter setting of AdaBoost ensemble classifier, setting the number of base learners to 50; The learning rate is set to 1; For the base classifier that can predict the probability, the faster convergence optimization algorithm “SAMME.R” is used, and the other base classifiers use the optimization algorithm “SAMME”.

4.3 Results

Firstly, reconstruct the boundary of the normalized original data set, and retain the original data set as the comparison data set, as shown in the Table 2 there are 284315 normal transactions in the original data set, while there are only 492 fraudulent transactions, and the distribution of the data is extremely unbalanced; However, after data boundary reconstruction, the number of fraudulent transactions also reached 283415. To some extent, it alleviates the problem of category imbalance in the data set.

Then, the original data set and the reconstructed data set are divided into the training set and the test set in a ratio of 4:1. Based on the training set of credit card transaction data, the machine learning algorithm described in the previous section is used as the integrated algorithm AdaBoost base learner to train the credit card fraud identification models of multiple different base learners respectively to verify the ability of boundary reconstruction to improve the data quality. Figure 2 shows the confusion matrix of the prediction results of the test set of the original data by the model under different base learners, and Figure 3 shows the confusion matrix of the prediction results of the test set of the reconstructed data (the four values from left to right are TN, FP, FN and TP respectively).

It can be seen from the Figure 2 and Figure 3 that the models under different data have good learning effects on the characteristics of normal transactions. However, the number of FN in the prediction results of the model trained with the original data set is slightly higher than FP, indicating that the model is more inclined to predict the credit card transaction as a normal transaction. The model trained with reconstructed data set has little difference between FP and FN in the test process, which shows that the model has no obvious preference behavior for normal transactions and fraudulent transactions, that is, boundary reconstruction alleviates the model deviation caused by sample imbalance to a certain extent.

Finally, to better present the effect of reconstructing the integrated classification model, Table 3 shows the performance indicators of the model test results under the two data sets. It can be seen that under the original data set, the specificity index of the model is close to 1, which shows that no matter what kind of machine learning algorithm, the integrated classification module of the model can capture and learn the characteristics of normal transactions; In addition to the accuracy of the learning tree model, which is not conducive to the recognition of fraud, the recall rate of the model is not higher than that of other transaction machines. The accuracy index performs well and is generally better than the accuracy of reconstructed data sets. If you only pay attention to the accuracy index, you will be deceived by the model and miss the fraudulent transaction. Under the reconstructed data set, the specificity of the model decreases slightly, but the accuracy and recall rate are more than 95%, which shows that boundary reconstruction can not only alleviate the imbalance of data categories, but also improve the quality of data, to improve the classification effect of the model. Overall, the effect of reconstructing the integrated classification model based on decision tree is the best.

5 CONCLUSION

With the data-driven technology gradually replacing the traditional model and becoming the mainstream identification mode of credit card transaction, various fraud identification models emerge in

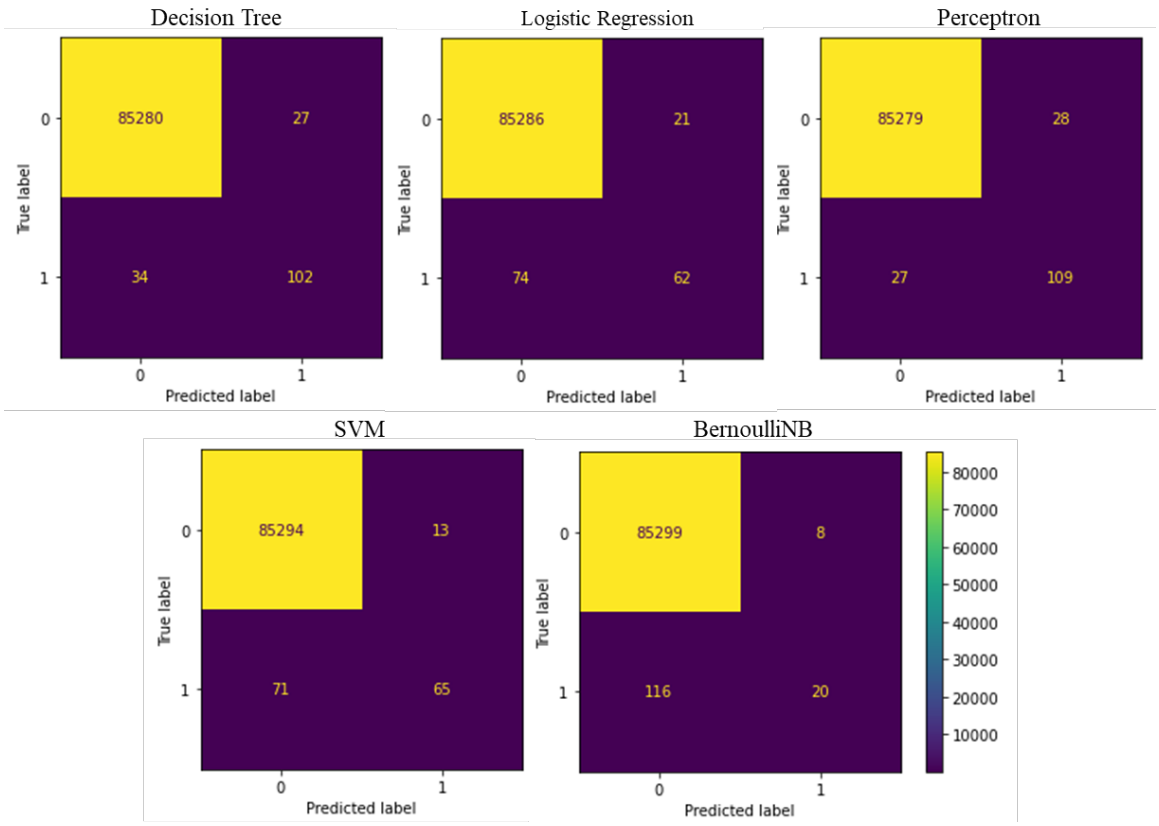

Figure 2: Confusion matrix of prediction results of original data test set

Table 2: Comparison between original data set and reconstructed data set

	Legal transactions	Fraud transactions	Fraud / Legal	Normalized or not
Original dataset	284315	492	0.1730%	Yes
Reconstruction dataset	284315	284315	100%	Yes

Table 3: Indicators of integrated classification model under different data sets

	Base estimator	Precision	Recall	Accuracy	Specificity	F1-Score
Original dataset	DT	0.7907	0.7500	0.9993	0.9997	0.7698
	LR	0.7470	0.4559	0.9989	0.9998	0.5662
	Perceptron	0.7956	0.8015	0.9994	0.9997	0.7985
	SVM	0.8333	0.4779	0.9990	0.9998	0.6075
	NB	0.7143	0.1471	0.9985	0.9999	0.2439
Reconstruction dataset	DT	0.9932	0.9953	0.9943	0.9932	0.9943
	LR	0.9845	0.9558	0.9703	0.9849	0.9699
	Perceptron	0.9835	0.9796	0.9816	0.9835	0.9815
	SVM	0.9779	0.9932	0.9854	0.9775	0.9855
	NB	0.9651	0.9618	0.9634	0.9651	0.9634

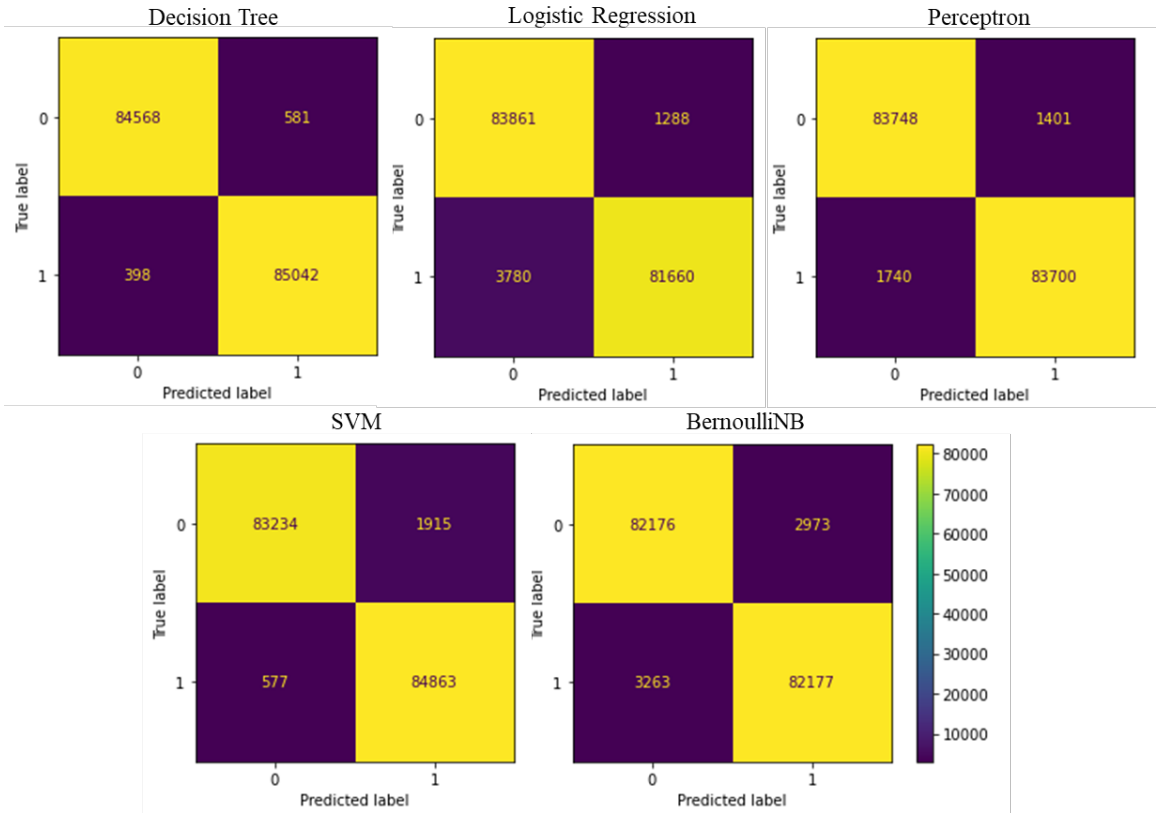

Figure 3: Confusion matrix of prediction results of reconstruction data test set

endlessly. However, due to the particularity of credit card transaction data, how to design a scientific and reasonable data expansion method and effectively improve the data quality has become a key problem in the field of fraud identification. At present, machine learning method has become an important tool in the field of fraud identification and plays an important role in judging fraud. Ensemble learning is a kind of machine learning method that combines multiple weak learners into strong learners, which can learn and be compatible with different transaction behavior characteristics. Aiming at the existing credit card fraud detection model, there are two problems: the extreme imbalance of credit card transaction data category and the fuzzy classification boundary. This paper proposes an integrated classification model based on data boundary reconstruction.

Firstly, a few fraudulent transactions in the data are classified based on the instance point category of k-nearest neighbor. Secondly, the noise and interference points are removed, and only the useful fraud transaction data are expanded, which makes the data form a better data boundary and effectively improves the quality of the data. Finally, the integrated classification model is trained to identify fraudulent transactions. It is found that the reconstructed integrated classification model proposed in this paper is significantly better than the recognition effect of using only the integrated classification model in identifying credit card data. The research of this paper enriches the new direction of credit card fraud identification, that is, from model improvement to the improvement of the quality of credit card data itself, which has important application value.

ACKNOWLEDGMENTS

This work was supported by the Natural Science Foundation of China (No. 72071176).

REFERENCES

[1] Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013, December). Cost sensitive credit card fraud detection using Bayes minimum risk. In 2013 12th international conference on machine learning and applications (Vol. 1, pp. 333-338). IEEE.
[2] Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical science, 17(3), 235-255.
[3] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). Scarff: a scalable framework for streaming credit card fraud detection with spark. Information fusion, 41, 182-194.
[4] Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2018). Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization. International Journal of Data Science and Analytics, 5(4), 285-300.
[5] Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. Information sciences, 557, 317-331.
[6] 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.
[7] Chen, R. C., Chiu, M. L., Huang, Y. L., & Chen, L. T. (2004, August). Detecting credit card fraud by using questionnaire-responded transaction model based

on support vector machines. In International Conference on Intelligent Data Engineering and Automated Learning (pp. 800-806). Springer, Berlin, Heidelberg.
[8] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), 3784-3797.
[9] Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015, December). Calibrating probability with undersampling for unbalanced classification. In 2015 IEEE Symposium Series on Computational Intelligence (pp. 159-166). IEEE.
[10] Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. Expert systems with applications, 41(10), 4915-4928.
[11] Devi, D., Biswas, S. K., & Purkayastha, B. (2019, July). A cost-sensitive weighted random forest technique for credit card fraud detection. In 2019 10th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-6). IEEE.
[12] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448-455.
[13] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016, October). Credit card fraud detection using convolutional neural networks. In International conference on neural information processing (pp. 483-490). Springer, Cham.
[14] Ghosh Dastidar, K., Jurgovsky, J., Siblini, W., & Granitzer, M. (2022). NAG: neural feature aggregation framework for credit card fraud detection. Knowledge and Information Systems, 1-28.
[15] Han, H., Wang, W. Y., & Mao, B. H. (2005, August). Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning. In International conference on intelligent computing (pp. 878-887). Springer, Berlin, Heidelberg.
[16] Hart, P. (1968). The condensed nearest neighbor rule (corresp.). IEEE transactions on information theory, 14(3), 515-516.
[17] He, H., Bai, Y., Garcia, E. A., & Li, S. (2008, June). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In 2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence) (pp. 1322-1328). IEEE.
[18] Hordri, N. F., Yuhaniz, S. S., Azmi, N. F. M., & Shamsuddin, S. M. (2018). Handling class imbalance in credit card fraud using resampling methods. Int. J. Adv. Comput. Sci. Appl, 9(11), 390-396.
[19] Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), 3637-3647.
[20] Kasa, N., Dahbura, A., Ravoori, C., & Adams, S. (2019, April). Improving credit card fraud detection by profiling and clustering accounts. In 2019 Systems and Information Engineering Design Symposium (SIEDS) (pp. 1-6). IEEE.
[21] Lebichot, B., Borgne, Y. A. L., He-Guelton, L., Oblé, F., & Bontempi, G. (2019, April). Deep-learning domain adaptation techniques for credit cards fraud detection. In INNS Big Data and Deep Learning conference (pp. 78-88). Springer, Cham.
[22] Li, Z., Liu, G., & Jiang, C. (2020). Deep representation learning with full center loss for credit card fraud detection. IEEE Transactions on Computational Social Systems, 7(2), 569-579. López, V., Fernández, A., García, S., Palade, V., & Herrera, F. (2013). An insight into classification with imbalanced data: Empirical results and current trends on using data intrinsic characteristics. Information sciences, 250, 113-141.
[23] Prasetiyo, B., Muslim, M. A., & Baroroh, N. (2021, June). Evaluation performance recall and F2 score of credit card fraud detection unbalanced dataset using SMOTE oversampling technique. In Journal of Physics: Conference Series (Vol. 1918, No. 4, p. 042002). IOP Publishing.
[24] Puh, M., & Brkić, L. (2019, May). Detecting credit card fraud using selected machine learning algorithms. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1250-1255). IEEE.
[25] Pumsirirat, A., & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. International Journal of advanced computer science and applications, 9(1), 18-25.
[26] Singh, A., & Jain, A. (2020). Cost-sensitive metaheuristic technique for credit card fraud detection. Journal of Information and Optimization Sciences, 41(6), 1319-1331.
[27] Somasundaram, A., & Reddy, S. (2019). Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance. Neural Computing and Applications, 31(1), 3-14.
[28] Tomek, I. (1976). An experiment with the edited nearest-neighbor rule. IEEE Transactions on Systems Man & Cybernetics, SMC-6(6), 448-452.
[29] Tomek, I. (1976). Two modifications of CNN. IEEE Trans. Systems, Man and Cybernetics, 6, 769-772.
[30] Wang, C., & Han, D. (2019). Credit card fraud forecasting model based on clustering analysis and integrated support vector machine. Cluster Computing, 22(6), 13861-13866.
[31] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data mining and knowledge discovery, 18(1), 30-55.
[32] Wu, J., Xiong, H., & Chen, J. (2010). COG: local decomposition for rare class analysis. *Data Mining and Knowledge Discovery, 20* (2), 191-220.
[33] Yu, S., Li, X., Zhang, X., & Wang, H. (2019). The OCS-SVM: An objective-cost-sensitive SVM with sample-based misclassification cost invariance. *IEEE Access*, *7*, 118931-118942.
[34] Zheng, L., Liu, G., Yan, C., Jiang, C., Zhou, M., & Li, M. (2020). Improved TrAdaBoost and its application to transaction fraud detection. *IEEE Transactions on Computational Social Systems*, *7* (5), 1304-1316.