Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.9854897

RESEARCH ON SUSPICIOUS TRANSACTION IDENTIFICATION BASED ON ALEXNET DEEP CONVOLUTIONAL NETWORK

Huixin Luo
South China Normal University, school of Economics & Management
Guangzhou, China, 19120653508@163.com

Abstract: Suspicious transaction identification is an important element of anti-money laundering work, and it has become a new trend to use algorithmic models as tools to analyze and identify suspicious transactions. Deep convolutional neural networks can effectively and automatically extract classification features from data, and have been widely used in various fields of research as they have shown good recognition results in many classification tasks. In this paper, we firstly design an 8-layer model framework based on Alexnet network theory for suspicious transaction identification analysis. Secondly, the Elliptic data set is divided into training and testing sets in the ratio of 7:3, and the divided data are used to train and test the model. Finally, the robustness of the model to data input is explored by randomly disrupting the ordering of the elements in the input data. The results show that the Alexnet convolutional neural network has good applicability for suspicious transaction recognition, and the overall classification accuracy of the Elliptic dataset can reach 94%, and the proposed model in this paper has good recognition accuracy in general.
Keywords: Alexnet, part defects, deep learning, board parts

THEORY IDENTIFICATION

Money laundering is the act of converting illegal proceeds into legal assets. Such behavior poses a major threat to social stability and the order of the financial market, and provides a source of funds for various criminal acts, so all countries have adopted anti-money laundering measures to varying degrees. Although China has achieved phased results, there is still a big gap compared with developed countries and international standards. As a transit point for the flow of funds, financial institutions have an important position in the anti-money laundering system. Although FATF and regulatory authorities have been working to assess the effectiveness of AML in financial institutions, there is a big gap between regulatory requirements and the practices of financial institutions, which hinders AML efforts. Suspicious transaction identification is an important measure to prevent money laundering. China's AML laws and regulations only provide for the design principles of suspicious transaction monitoring, and financial institutions have greater autonomy. This situation has led to a lack of effective monitoring by financial institutions, a high rate of misjudgment of early warning, and a waste of AML resources or even a decrease in effectiveness. Therefore, it is important to improve the effectiveness of suspicious transaction identification for AML work. There are two modes of suspicious transaction identification at the present stage. One is based on the supervisory department or the institution's own risk alert itself, combining customer identity information, transaction frequency and associated customer transaction behavior to design monitoring and early warning indicators, and setting different thresholds to achieve early

warning of suspicious transactions, which has the characteristics of simple and convenient operation. The form of money laundering is complex, and it is impossible to identify suspicious transactions by a single indicator or multiple indicators. Machine learning algorithms applied to suspicious transaction identification can be divided into unsupervised learning algorithms and supervised learning algorithms. Unsupervised learning algorithms use a clustering algorithm model to cluster and sub-cluster samples of unknown categories, and thus identify customers with suspicious transactions. Supervised learning algorithms must carry classification labels in order to guide the model for updating iterations to achieve an acceptable classification accuracy. The identification of suspicious transactions by machine learning algorithms can continuously update and iterate to optimize the model and improve the effectiveness of suspicious transaction warning. Lu Rui et al. used random forest algorithm for feature selection, designed a suspicious transaction monitoring model, and applied it to credit card transaction data suspicious transaction identification; Hassan applied various classification models, including multilayer perceptron, support vector machine, and decision tree, in credit card unusual transaction monitoring and verified its effectiveness in European credit card fraud dataset. Although traditional classification algorithms have good classification recognition, they suffer from high feature design cost because of the large labor cost required to achieve the selection of model features. As a result, deep neural networks have emerged. Deep neural network models are able to extract robust feature sets from samples by constructing multilayer networks and exhibit excellent classification results. In this study, based on Alexnet deep neural network theory, a one-dimensional convolutional neural network is selected as a model and a model framework containing eight layers is designed to be applied to suspicious transaction identification analysis in order to provide a new way for suspicious transaction identification..

Related technology and method

AlexNet is a deep convolutional neural network model proposed by Alex Krizhevsky, Ilya Sutskever and Geoffrey Hinton in 2012. It uses eight convolutional layers and three fully connected layers with over 60 million parameters, making it one of the largest deep neural networks at the time. alexNet achieved a significant advantage in the ImageNet image recognition challenge, marking the dawn of the deep learning era. The activation function used in the AlexNet model in this design is the ReLU (Rectified Linear Unit) function. The function is defined as: $f(x) = \max(0, x)$, which means the output is x when the input x is greater than or equal to 0, and the output is 0 when the input x is less than 0. The ReLU function is designed to have the following advantages: Nonlinear: The ReLU function is a nonlinear function, which can better fit nonlinear data and thus improve the expressiveness of the model. Computational simplicity: The ReLU function is very simple to compute, only needing to determine whether the input is greater than 0. It is less computational than other activation functions, thus speeding up the training and inference process of the model. Mitigating the gradient disappearance problem: Gradient disappearance is a common problem in deep neural networks, which can cause the model to fail to converge. the ReLU function can mitigate the gradient disappearance problem, because when the input is positive, the gradient is 1, and there is no gradient disappearance. Sparsity: When the input is negative, the output of the ReLU function is 0. Therefore, it can make the output of neurons sparse, i.e., only some neurons will be activated,

thus reducing the complexity of the model and improving the generalization ability. The loss function in this experiment in the AlexNet model is the cross-entropy loss function. The cross-entropy loss function can be used to measure the difference between the model output and the true label, which is defined as Equation 1:

$$L\big(y, f(x)\big) = -\sum y^i * log\ (f(x_i)) \qquad (1)$$

where y is the true label vector, f(x) is the model output vector, and i denotes the i-th element of the vector. The AlexNet model loss function we set as the cross-entropy loss function. The cross-entropy loss function is designed to be meaningful in that it can be used to measure the performance of a classification model: The cross-entropy loss function can measure the difference between the predicted probability of the model for each category and the true label, and therefore can be used to evaluate the classification performance of the model. It can promote the model to learn better feature representation: The optimization process of the cross-entropy loss function can promote the model to learn better feature representation and thus improve the generalization ability of the model. It can avoid the gradient vanishing problem: The derivatives of the cross-entropy loss function do not suffer from the gradient vanishing problem when the gradient is back-propagated, and thus can accelerate the training of the model. the network structure of AlexNet is shown in Figure 1.

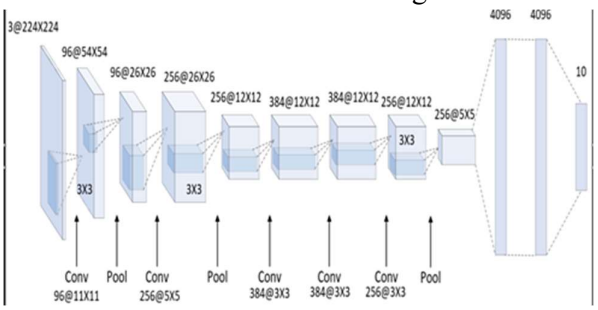

Figure 1 Alexnet network structure diagram

As can be seen from the figure, AlexNet consists of five convolutional layers and three fully-connected layers. The first two layers are the data layers, the third layer is the first convolutional layer, the fourth layer is the second convolutional layer, the fifth layer is the third convolutional layer, the sixth layer is the first fully connected layer, the seventh layer is the second fully connected layer, and the eighth layer is the output layer. In addition, AlexNet uses dropout technique to avoid overfitting. alexNet also uses local response normalization technique to improve the generalization performance of the model. alexnet convolutional neural network in financial field suspicious transaction identification application aspect of AlexNet in financial field suspicious transaction identification The application can be divided into the following steps:

1. Data pre-processing

In the financial field, data pre-processing is very important. Generally, the data format of suspicious transactions is time series data. Therefore, we need to convert these time series data into picture data (i.e., two-dimensional data) and normalize them. The purpose of this step is to convert the time series data from different sources into a matrix with similar structure, so that it can be easily processed by the deep learning model.

2. Training the model

Before training the model, it is necessary to divide the training set and the test set. In the training set, transaction data is used, including normal transaction data and known suspicious transaction data. In the test set, we use unknown transaction data. Next, we need to use a large amount of normal transaction data and known suspicious transaction data to train the AlexNet convolutional neural network model. In the process of training the model, super parameter adjustment is required to find the optimal model configuration parameters.

3. Suspicious transaction identification

After completing the model training, we can use the trained AlexNet model to identify new transaction data. Specifically, for new transaction data, we need to use the trained AlexNet model to classify them, and if they are classified as suspicious transactions, further manual review is required. In the application of AlexNet convolutional neural network for suspicious transaction identification, the powerful features of AlexNet convolutional neural network are utilized to identify and learn complex patterns hidden in the data, identify abnormal images in the suspicious transaction data, and perform further manual review. This approach can capture complex patterns in fraudulent behavior, such as multiple attempts to access the same account, abnormal transaction totals, etc., thus effectively reducing losses from financial fraud.

In conclusion, the application of AlexNet convolutional neural network for suspicious transaction identification in finance is very promising. By providing effective automatic bias and data correction capabilities, it can provide financial institutions with better fraud detection means to manage larger datasets and more dimensions of data.

Dataset Description and Analysis

In order to verify the effectiveness of the proposed classification model, the bitcoin transaction dataset released by Elliptic, a cryptocurrency compliance company, is selected as the experimental data for training the 1D convolutional neural network model with a total of 27,938 transaction records. the Elliptic dataset is a bitcoin transaction information dataset, and its purpose is to provide real virtual currency data to facilitate researchers to test and verify the effectiveness of the suspicious transaction model. The purpose of the Elliptic dataset is to provide real virtual currency data for researchers to test and validate the classification effect of suspicious transaction models, and to advance the development of suspicious transaction identification models. The dataset includes 200,000 transaction records, 203,769 nodes and 234,355 edges, with a total value of $6 billion. The transaction data is labeled into three categories, namely legal categories, illegal transactions, and unknown data. And for each transaction record data, Elliptic dataset provides 166 transaction features, among which the first 94 features mainly describe the basic situation of the data, and the last 72 features mainly describe the transaction characteristics among the associated subjects. Due to the sensitivity of transaction data of financial institutions and the confidentiality requirements of customer data, there is no official dataset related to suspicious transactions of financial institutions. Therefore, in this paper, we only use the transaction data with labels existing in the Elliptic dataset to train and test the model, i.e., 4545 transaction records for legal categories and 42019 transaction records for illegal transactions, with a total of 46,564 transaction records. The data used in total accounts for about 23.3% of the Elliptic dataset.3.2 Experimental hardware and effect analysis, combined with Alexnet neural network theory, and designed a model framework containing 8 layers applied to suspicious transaction identification analysis. The experimental environment

and parameters are set as follows: (1) Experimental environment. The hardware specifications are: CPU: i7-10700/GPU: GTX3080/graphic memory: 10G/operating system: Windows10/development language: Python 3.8/deep learning framework: PyTorch. and training. (2) Elliptic data training and test set partitioning. In order to ensure the comparability of the experimental results, we divide the training data and test data into 7:3 according to the time step of transactions, with the first 40 time steps containing transaction data as training data and the last 15 time steps containing transaction data as test data. (3) The parameters of the model training phase are set. In order to ensure that there are positive and negative samples in each iteration, the Mini-batch is set to 2048 samples; Epoch is set to 500; LR is set to 0.01; the loss function is set to cross-entropy loss function, and the model weights are regularized by L2 parametrization. （The Elliptic dataset contains 166 features per record, but since the time step is only used as a marker to classify different time steps, this feature is excluded and only the remaining 165 features are used as the input of the model. In this study, the tableau model and the training results are compared with the EvolveGCN model, Label-GCN model and GCN-based model as the comparison models.

From the above figure, it can be seen that the neural network model designed for detection has some improvement over the EvolveGCN, Label-GCN and GCN-based models, and the mAP value has increased by about 5.3%.

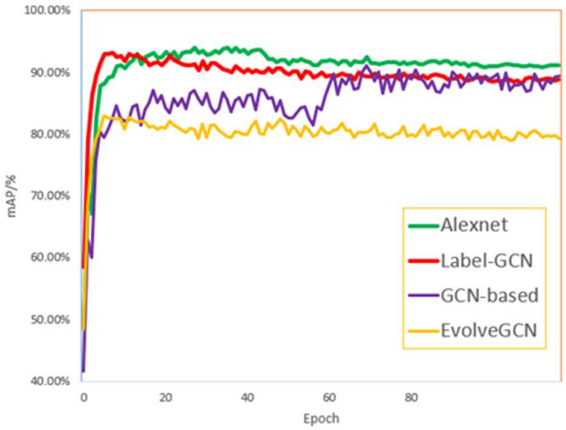

Fig. 2 Network model index mAP comparison

From the above figure, it can be seen that the neural network model designed for detection has some improvement over the EvolveGCN, Label-GCN and GCN-based models, and the mAP value has increased by about4.3%

CONCLUSION

Accurate and effective identification of suspicious transactions in customer transaction records is important to prevent money laundering risks and improve the performance of anti-money laundering. Traditional machine learning algorithms for suspicious transaction identification require a large amount of manual cost to select features for the model in order to determine the best set of features, but they still cannot guarantee the effective classification features. Therefore, this paper exploits the advantages of deep neural networks in automatic feature extraction, and based on the theoretical foundation of deep convolutional neural networks, a one-dimensional convolutional neural network is selected and a model framework with seven

layers is designed to investigate the applicability and effectiveness of the model by applying it to the Elliptic bitcoin transaction dataset and comparing different classification models. The findings are as follows: (1) The deep neural network models such as EvolveGCN model, Label-GCN model and GCN-based model, and the proposed convolutional neural network model for suspicious transactions have higher recognition effect than the above-mentioned comparison models, which verifies the model has better effectiveness. (2) The model is robust and tolerant to the arrangement distribution of the model input data elements, i.e., the model input data is randomly disrupted, which has little impact on the classification effect of the model and does not produce significant fluctuations in classification accuracy. The model can promote financial institutions to make full use of mechanisms such as money laundering risk self-assessment and suspicious transaction monitoring index assessment. In-depth analysis of suspicious transaction reports (STRs) can be used to identify the types of money laundering and risk prevention and control measures applicable to the institution.

Acknowledgment

The project S202210623085 is supported by Sichuan Undergraduate Training Program for Innovation and Entrepreneurship & Provincial and ministerial level discipline platform open topic jkgl2018-042.

References

[1] Chen, Hao-Meng. Research on monitoring and analysis of underground money laundering based on clustering algorithm[J]. Financial Development Research, 2020(06):9-16.

[2] Small sample object image recognition based on convolutional network feature migration[J]. Bai Jie; Zhang Jinsong; Liu Qianyu. Computer Simulation,2020(05)

[3] Abstract image emotion recognition based on two-layer migrating convolutional neural networks[J]. Yang ZW;Chen L;Pu JY. Journal of the University of Science and Technology of China,2019(01)

[4] A combined SARIMA and LSTM based prediction model [J]. Ding, R.; Li, W.; Wang, Ruozhou. Computer and Digital Engineering,2020(02)

[5] Research on stock influencing factors based on linear regression model[J]. Liu Siqi. National circulation economy,2020(05)

[6] Research on credit risk control of banks in the era of big data[J]. Zhang Hongyang. Value Engineering,2020(04).

[7] Alarab I,Prakoonwit S,Nacer M I.Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain[C].Proceedings of the 2020 5th International Conference on Machine Learning Technologies.2020: 23-27.

[8] Bellei C,Alattas H,Kaaniche N.Label-GCN: An Effective Method for Adding Label Propagation to Graph Convolutional Networks[J].arXiv preprint arXiv:2104.02153, 2021.

[9] Hassan H M,Ahmed A H A.The effectiveness of the Random Forest algorithm in monitoring abnormal withdrawals to detect credit cards frauds[J]. AL-BUTANA JOURNAL Of APPLIED SCIENCE,2022, 44- 64.

[11] Weber M,Domeniconi G,Chen J,et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics[J]. arXiv preprint arXiv:1908.02591, 2019.