Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008

NEURAL DATA MINING FOR CREDIT CARD FRAUD DETECTION

TAO GUO, GUI-YANG LI

College of Computer Science and Technology in Sichuan Normal University, Chengdu, 610068, China
E-MAIL: tguo35@163.com, gyl@sicnu.edu.cn

Abstract:

Due to a rapid advancement in the electronic commerce technology, use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment, credit card frauds are becoming increasingly rampant in recent years. In this paper, we model the sequence of operations in credit card transaction processing using a confidence-based neural network. Receiver operating characteristic (ROC) analysis technology is also introduced to ensure the accuracy and effectiveness of fraud detection. A neural network is initially trained with synthetic data. If an incoming credit card transaction is not accepted by the trained neural network model (NNM) with sufficiently low confidence, it is considered to be fraudulent. This paper shows how confidence value, neural network algorithm and ROC can be combined successfully to perform credit card fraud detection.

Keywords:

Fraud detection; Neural network model; Spending pattern; Confidence; ROC

1. Introduction

Along with the development of e-commerce, credit card becomes the most popular mode of payment for both online as well as regular purchase and credit card fraud has also become increasingly rampant in recent years. Banks and credit card companies have accumulated large amounts of credit card account transactions. How to make use of the transaction data to better understand the spending pattern of customer and to detect credit card fraud is a requirement for providing good service. In China, credit card users are growing greatly, but only a few credit card holders use credit cards to pay for day-to-day purchase with great confidence and a sense of security. The reason is that credit card holder has no enough confidence to trust the payment system. For example, in China, it is the cardholder's own responsibility if the credit card was overdraft by unauthorized user before the loss report was made. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company or cardholder [1]. The only way to detect this kind of fraud is to decipher the spending pattern on every card and to figure out any inconsistency with respect to the "usual" spending pattern. Fraud detection based on analyzing existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behavioristic profiles, such as typical purchase category, shopping time, and transaction amount, deviation from such patterns is a potential threat to the model.

The remainder of this paper is organized as follows. Section 2 reviews relevant studies. Section 3 provides a brief description of the research methods used. Section 4 describes the experiment results and analysis. Section 5 makes the conclusions.

2. Related work on credit card fraud detection

From the work of view for preventing credit card fraud, more research works were carried out with special emphasis on data mining and neural networks. Ghosh and Reilly（1994）[2] have proposed credit card fraud detection with a neural network. They have built a detection system which is trained on a large sample of labeled credit card account transactions. The feasibility study demonstrated that due to its ability to detect fraudulent patterns on credit card accounts, it is possible to achieve a reduction of from 20% to 40% in total fraud losses, at significantly reduced caseload for human review. Aleskerov and Freisleben （1997）[3] present CARDWATCH, a database mining system used for credit card fraud detection. The system uses neural network to train specific historical consumption data and generate neural network model. The model was adopted to detect fraudulence. Sam and Karl (2002) [4] suggest a credit card fraud detection system using Bayesian and neural network techniques to learn models of fraudulent credit card transactions. Kim and Kim have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of credit card fraud detection

978-1-4244-2096-4/08/$25.00 ©2008 IEEE

[5]. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections.

All above-mentioned approaches do not concern to convert the training data into confidence value before putting into neural network. Furthermore, a fixed threshold is set to detect abnormal and normal spending pattern in the above-mentioned approaches without concerning the cost problem derived from false positive and false negative. The Threshold can not be adjusted dynamically based on frequency of fraudulent either. In this paper, NNM combining with confidence and ROC analysis technology for fraud detection is introduced in detail. In this study, confidence-based neural network is tested for its applicability in fraud detection.

3. Research methodology

3.1. Data set

It is difficult to obtain available credit card data sets since the security, privacy and cost issues. Currently, most of the researchers generate realistic synthetic data using data generator to facilitate the development and testing of data mining tools [6]. The original applications for this experiment are credit card transaction data sets generated by data generator developed by ourselves. The model of the data generator is based on reference [7]. All data sets are saved in database for future preprocessing. This part of function is dependent to NNM.

It is necessary for neural network to provide genuine as well as fraudulent transactions to train the classifiers. The original set of portfolio transactions was sampled in such a way that all fraud transactions were included, while a sample of the good transactions was chosen so as to have a ratio of roughly 100 good transactions for each fraudulent transaction in the training data set [2]. The data set for experiment contains 5000 synthetic transaction data. In NNM, credit card payment-related training data attributes include: time (Time), location (Cy_pq), type of merchandise (Mer_type), business code for merchandise (Bu_code), business type for merchandise (Bu_type), and transaction amount for consumption (P_m). Actual target values (for classification) are used to guide for neural network learning. Actual target value 1 represents abnormal, and 0 represents normal.

3.2. Calculation of confidence value

In this system, both training and testing data are required to convert to confidence value before putting into NNM. Through the confidence calculation, neural network input is formatted to the range [0.0, 1.0] and each input contains historical information at this time. Besides, the differences among different customers are shielded and it is useful for us to use lesser model to detect all consumptions. In the input attributes: time, location, type of merchandise, business code for merchandise, business type for merchandise belong to discrete value, and transaction amount for consumption belong to continuous value. Therefore, NNM adopts two methods to perform the calculation of confidence value:

Take the location as an example to demonstrate the first calculation method for discrete attributes. Our transaction can be seen as a data tuple X, $X=\{x_1,x_2\ldots\ldots, x_n\}$, where n is the number of using credit card. Suppose xi, for $i=1,2,\ldots,n$, is the location of use credit card in consumption i. Let m_{xi} denote the number of using credit card in the location xi. For xi, the confidence $C(x_i)$ is

$$C(x_i)=\frac{m_{xi}}{n} \tag{1}$$

Other discrete attributes are calculated to confidence value with same method.

The second calculation method for continuous value is performed as following.

Since the spending pattern for common consumers are normal [2,8,9,10,11], we suppose $X=\{x_1,x_2\ldots\ldots, x_n\}$, where n is the number of using credit card, x_i, for $i=1,2,\ldots,n$, is transaction amount in consumption i by use credit card, σ is standard deviation for the transaction amount in consumption of using credit card, μ is the average of transaction amount. The confidence $C(x_i)$ for the transaction amount in consumption i is

$$C(x_i)=e^{-\frac{1}{2}(\frac{x_i-\mu}{\sigma})^2} \tag{2}$$

After performing confidence calculation, all input values achieve the purpose of format and the confidences contain statistical meaning for specific customers. In the mean time, the high confidence value means high happiness possibility of transaction. The formatted data will help to speed up the neural network learning process [12].

3.3. Methods

3.3.1. Neural networks

Neural networks topologies, or architectures, formed by organizing nodes into layers and linking these layers of neurons with modifiable weighted interconnections. Being

a nonlinear mapping relation from the input space to output space, neural networks can learn from the given cases and summarize the internal principles of data even without knowing the potential data principles ahead. And it can adapt its own behavior to the new environment with the results of formation of general capability of evolution from present situation to the new environment. In this system, we use multi-layer neural network model and backpropagation (BP)algorithm[12] runs on the network. Backpropagation learns by iteratively processing a data set of training tuples X, $X=\{x_1, x_2\ldots\ldots,x_n\}$, comparing the network's prediction for each tuple with the actual known target value. For each training tuple, the weights are modified so as to minimize the mean squared error between the network's prediction and the actual target value. The modifications are made in the backwards direction, that is, from the output layer Y, $Y=\{y_1, \ldots\ldots y_n\}$, through each hidden layer down to the first hidden layer.

In this study, a sigmoid function is used for the nodes in the hidden layers and the output layer. The learning rate *l* involved in the change of weight is set to countdown of the number of entries in training data [10].

3.3.2. Neural network topology

There is no good way to determine the number of hidden layers of neural network and the number of hidden nodes in each layer currently [13]. In order to overcome the problem, we determine the hidden layers and nodes in each hidden layer dynamically by means of GUI provided by the system. Through the operation of neural network, we select a neural network model with smaller average error.

The system provides two methods to determine the weight and bias: 1) generated random number of weight and bias to the range [-1.0, +1.0] by system; 2) set through GUI provided by system. System also provides two options to terminate the training model: 1) when the change of weight is less than a specified threshold, the training model is terminated. 2) when the iteration cycle excesses the pre-defined iteration cycle, the training model is terminated.

3.4. ROC

After establishing the NNM, new transaction record is tested through it and the output of NNM will be the confidence value $Y=\{y_1, \ldots\ldots y_n\}$. We determine whether the consumption is normal or abnormal by judging whether the y_n is higher or lower than threshold. For normal confidence value, the banks will authorize to use the credit card directly and for abnormal confidence value, it is required to call for further confirmation according to the degree of abnormality before authorize to use of credit card. Therefore, setting of threshold has a great influence to the detection performance. To ensure that the threshold is set reasonable, and guarantee the accuracy of the detection, we use ROC analysis technique to determine the threshold. The testing result present by using 2 × 2 confusion matrix is constructed by using the most popular two-types of ROC analysis [14] in ROC analysis algorithm. Table 1 is a confusion matrix under the normal and abnormal spending pattern using credit card.

Table1 Confusion matrix for two-types of problems

		Prediction classification	
		Y	N
Actual classification	P	True Positive (TP)	False Negative (FN)
	N	False Positive(FP)	True Negative (TN)

Confusion matrix is the base of ROC analysis. FPR (False Positive rate) is the ratio of the number which abnormal spending pattern is detected as normal (FP) by NNM with the number of all abnormal spending pattern (N).

$$FPR = \frac{FP}{FP + TN} \quad (3)$$

TPR (True Positive rate) is the ratio of number which normal spending pattern is detected as normal (TP) by NNM with the number of all normal spending pattern (P).

$$TPR = \frac{TP}{TP + FN} \quad (4)$$

According to the requirement of credit card detection, some thresholds are chosen in this experiment. The ROC curve is a two-dimensional axis of points representing the relationships between FRP and TPR value. Each point on ROC curve denotes the change's relationship between FPR and TPR. For the optimal point on ROC, the maximal number of Youden exponent E [15] will be adopted without considering cost. The exponent E is defined as following:

$$E = TPR - FPR \quad (5)$$

If we consider the cost of false negative and false positive, the cost weighted exponent (CE) is proposed and defined as following:

$$CE = \frac{FNC}{FPC + FNC} \times TPR - \frac{FPC}{FPC + FNC} \times FPR \quad (6)$$

FNC is the cost of false negative, FPC is the cost of false positive. FNC and FPC satisfy the following three rules:

（1）$0 \le FPC \le 1$

（2）0≤FNC≤1

（3）FPC+ FNC≠0

When FPC=FNC≠0，the value of CE in formula (6) is:

$$CE = \frac{1}{2} \times (TPR - FPR) = \frac{1}{2} E$$

Here, the optimal value of CE is same as the optimal effect of E. Therefore, formula (6) is the general format of formula (5). Using cost of weighted exponent overcomes the unreasonable shortcomings for setting threshold without considering error cost.

4. Experiment results and analysis

When running the fraud detection system, each incoming transaction is submitted to the system for verification. We determine whether the spending pattern is fraudulent or not by judging whether each output yi, for i=1, 2…n, is higher or lower than a threshold. For normal value, the banks will authorize to use the credit card directly and for abnormal value, it is required to call for further confirmation according to the degree of abnormality before authorize to use of credit card.

In this study, 7000 synthetic data is used for training, and 3000 is used for testing. Table 2 shows 10 records of consumer behavior attributes after performing calculation of confidence.

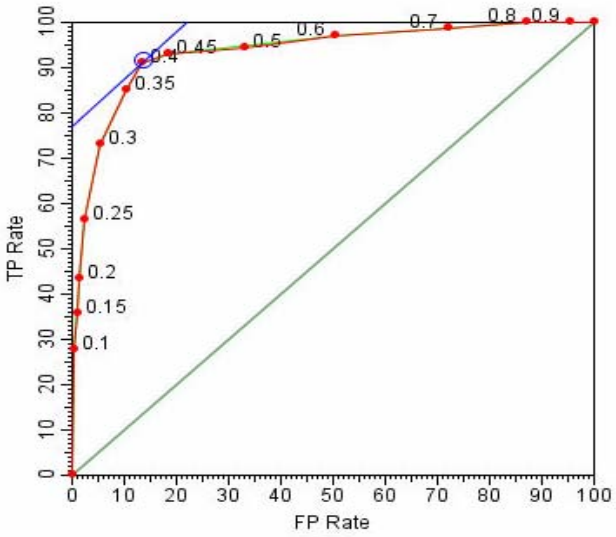
After performing the training, we got a NNM model with smaller average error. Then we got ROC curve shown in Figure 1. Figure 1 illustrates that when the threshold is set to 0.4, the model has better recognition. As the improvement of true positive, the false positive is also increased. If we don't consider the cost factor, the system obtains the optimal value which the rate of true positive (TP) reaches 91.2% and the rate of false positive (FP) reaches 13.35% according to formula (5). If the cost factor is considered, the threshold can be determined according to formula (6). When the relative cost changes, the optimal threshold will be adjusted.

5. Conclusions

Credit card fraud has become more and more rampant in recent years. To improve merchants' risk management level in an automatic, scientific and effective way, building an accurate, available and easy-
handling credit card risk monitoring system is one of the key tasks for the merchant banks. In this paper, we present our work and demonstrate the advantages of the data mining techniques including neural networks, and calculation of confidence. The results show that the proposed classifier of neural networks based on confidence approach performs preferable practicability and successful detection rate in credit card fraud detection. Further studies are encouraged to improve the fraud detection criteria, to set more suitable weight and cost factor with both good tested accuracy and detection accuracy.

Table2：Spending pattern records after calculation of confidence and classification

Record_ No.	*Time*	*Cy_pq*	*Mer_type*	*Bu_code*	*Bu_type*	*P_m*	*Class*
1	0.56	0.83	0.55	0.72	0.65	0.74	1
2	0.41	0.49	0.12	0.32	0.73	0.89	1
3	0.73	0.57	0.09	1.00	0.55	0.45	1
4	0.72	0.06	0.78	0.15	0.40	0.78	1
5	0.50	0.63	0.56	0.33	0.80	0.63	1
6	0.41	0.00	0.67	0.60	0.51	0.12	0
7	0.23	0.67	0.45	0.67	0.54	0.91	1
8	0.76	0.01	0.15	0.09	0.12	0.75	0
9	0.89	0.67	0.34	0. 49	0.78	0.34	0
10	0.25	0.71	0.56	0.76	0.81	0.90	1



Acknowledgments

The author gratefully acknowledges the support of Sichuan Provincial Education Department. (Granted No.: 2005A095).

References

[1] http://www.pay4.cn/?viewnews-565.html

[2] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii

International Conference on System Sciences: Information Systems: Decision Support and Knowledge-Based Systems, vol. 3, pp. 621-630, 1994.

[3] E. Aleskerov, B. Freisleben, and B. Rao, CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, Proc. IEEE/IAFE: Computational Intelligence for Financial Engineering, pp. 220-226, 1997.

[4] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick. Credit Card Fraud Detection Using Bayesian and Neural Networks First International NAISO Congress on Neuro Fuzzy Technologies, Havana, Cuba. 2002.

[5] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. International Conference on Intelligent Data Engineering and Automated Learning, Lecture Notes in Computer Science, Springer Verlag, no. 2412, pp. 378-383, 2002.

[6] Yufeng Kou, Chang-Tien Lu, Sirirat Sirwongwattana, Survey of Fraud Detection Techniques, Proc. IEEE : International Conference on Networking , Sensing & Control, pp. 749-754, 2004.

[7] [Jeske, D.R. Lin, P.J. Rendon, C. Rui Xiao Samadi, B., Synthetic Data Generation Capabilties for Testing Data Mining Tools. IEEE : Military Communications Conference, pp.1-6, 2006.

[8] S. Hawkins, H. X. He, G. J. Williams, and R. A. Baxter. Outlier detection using replicator neural networks. In Proc. of the Fifth Int. Conf. and Data Warehousing and Knowledge Discovery (DaWaK02), 2002.

[9] Fawcett and F. Provost. Adaptive fraud detection. Data Mining and Knowledge Discovery Journal, 1(3):291-316, 1997.

[10] [W. DuMouchel and M. Schonlau. A fast computer intrusion detection algorithm based on hypothesis testing of command transition probabilities. In Proc. 4th Int. conf. on Knowledge Discovery and Data Mining, Pages 189-193, 1998.

[11] R.Brause, T.Langsdorf, M.Hepp, Credit Card Fraud Detection by Adaptive Neural Data Mining, J.W. Gorthe-University, Comp. Sc. Dep., Report 7/99, Frankfrut, Germany, 1999.

[12] Margare H.Dunham，Data Mining Introductory and Advanced Topics，Prentice Hall，2003。

[13] Jiaowei Han, Micheline Kamber， Data Mining Concepts and Technology, Mechanic Industry Publish House, 2006.

[14] Xiaolong Zhang, Chuan Jiang, Mingjian Luo, Application of ROC analysis in machine learning. Computer Engineering and Applications, 2007, 43 (4) : 243- 248.

[15] http://www.unu.edu/Unupress/foods/UIDOE/uid10elk.htm，Use of statistics for predictive purpos