Back Propagation Networks for Credit Card Fraud Prediction Using Stratified Personalized Data

Rong-Chang Chen, Chih-Yi Lai
Department of Logistics Engineering and Management
National Taichung Institute of Technology
No. 129, Sec. 3, Sanmin Rd., Taichung, Taiwan 404, ROC

Abstract: - A personalized approach (PA) has been presented recently to prevent fraud in using credit cards. This new approach proposes to predict a user's new transactions by his/her personalized model instead of using multiple-user approaches (MUA) which are based on transaction data of many other users. This approach has shown its potential to deal with the credit card fraud problem. The purpose of this paper is to investigate the performance of back propagation networks (BPN) on predicting credit card fraud using PA. The trained and tested data are stratified, i.e., each class has representative data. To facilitate the decision of the network architecture, Bubble charts are employed. Results from this study show that with stratified data, BPN can obtain good prediction performance. In addition, Bubble chart is a convenient tool to help decide the architecture of the network.

Key-Words: credit card fraud, back propagation networks, personalized approach

1 Introduction

Credit cards have become a popular tool for transactions in many countries lately. As the income rises and rises, consumption style changes diversely. There are lots of ways to pay for consumers. Among them, credit card is the most convenience tool. This is partly because consumers can get products or service before pay. Given such convenience, the quantity of circulation of credit cards increases year by year. Figure 1 shows this trend [1].

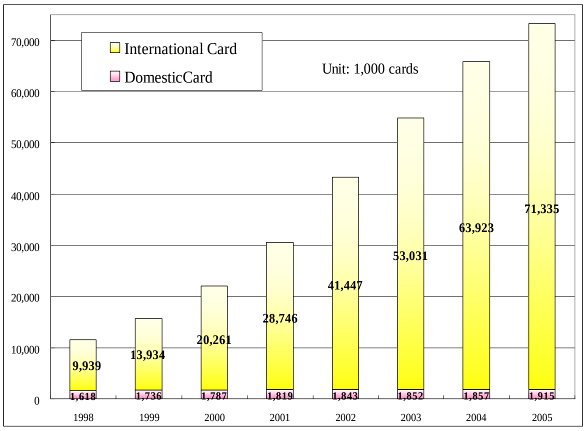

Fig. 1. Statistic of cards in circulation via the national credit card center (NCCC) of ROC [1]

Though credit cards bring much convenience, some problems are accompanied with them. The more people use credit cards, the more credit card fraud problems may happen. When coping with credit card fraud problems, traditionally, real transaction data are used to create models for predicting a new case. This approach provides a good solution in some conditions. However, the most conventional fraud for credit cards happens when a pilferer uses personal information to open a credit card account in one's name or a new card is stolen before the use of an applicant. Notwithstanding, there are no or few transaction data for new users. Rather than detecting credit card fraud by past transaction data, Chen et al. [2-5] proposed a novel approach to solve credit card fraud problems. They suggested building up a personalized model based on personal data collected by an online questionnaire system. Since the illegal user's and the cardholder's transaction behaviors are different, the fraud can be avoided from the initial use of a credit card.

The personalized approach (PA) is promising. Therefore, we will employ PA in this study. The analytical tool we use in this study is Back Propagation Networks (BPN), which can have a high tolerance to noisy data and have the ability to classify patterns which they have not been trained [6-7]. We first collect the transaction data of users by using an online questionnaire system, and then class them into different kinds of consumer styles mainly according to their consumption amounts, transaction time, and transaction items. PBN is then used to train, test, and predict new transactions. When a new transaction is going, the model can predict whether the transaction is abnormal or not. If the prediction result is to be abnormal, the transaction is considered as a fraudulent behavior.

The rest of this paper is organized as follows. Section 2 gives a brief overview of literature review. The subsection 2.1 reviews on credit card fraud detection and the subsection 2.2 introduces BPN. In Section 3, the approach to predict new transactions is introduced. The results are illustrated and discussed in Section 4. Finally, conclusions are presented in Section 5.

2 Literature Review

2.1 Credit Card Fraud Detection

Preventing credit card fraud has become a top priority in many countries. Present approaches to identifying credit card frauds can be generally classified into two types [5]. One is the multiple-user approach (MUA), which is based on data of multiple credit card users [8-12]. The other is PA, which is based on personal data [2-5]. In the MUA, investigations for credit card fraud include taking many users' transaction data to generate models for predicting new cases. This type of approach has some good results. Nevertheless, there are still some problems for using this kind of approach [5].

1) Consumer behavior varies significantly from one individual to another. When predicting consumer behavior of a certain user by using a model based on many credit card users' transaction data, the prediction accuracy could be very low in many situations. Above all, for new users, there are no or few transaction data. MUA cannot address an instance problem where fraud involves illegally using a cardholder's personal information to open a credit card account or a newly-issued card is stolen. Under this situation, fraud occur became the transaction are prosecuted before the legal cardholder has had access to it.

2) There are many overlapping data where legitimate transactions are similar to fraudulent transactions. The opposite also happens. When handling a particular transaction item in a similar situation, like a coin having two sides, one will do it, the other not. For this reason, overlapping or contradictory data are unavoidable when using MUA.

3) Consumer behavior converts over time. Hence, it is normally very difficult to deal with time-varying behavior by using MUA.

To improve the problems mentioned above, Chen et al. [2-5] proposed and employed a novel type of approach, i.e., PA, to prevent fraud. They first collect user's personal transaction data by a self-completion online questionnaire system. The collected *questionnaire-responded transaction* (QRT) data, including both the normal and abnormal parts, are regarded as the transaction records and are used to build up a personalized model, which is in turn used to predict and decide whether a new user's consumer behavior is genuine or not. Since PA is promising in dealing with credit card fraud problem, we will employ it to be the analytical tool in this study.

2.2 Back Propagation Networks

Artificial Neural Network (ANN) has become a powerful tool for decision-making [13-16]. It is an information-processing pattern that is stimulated by biological nervous systems like the brain. The primary element of this pattern is the architecture of the information-processing system. It comprises a large number of highly interconnected processing elements (neurons) to solve particular problems. ANN like people can gain knowledge by learning of examples. It has been applied to a wide variety of fields, such as fraud detection, classification of micro-arrays, and pattern recognition, through a learning process. Learning in biological systems implicates adjustment to the synaptic connections that exist between the neurons. This is also true for ANN.

There are many forms of ANN models. Amongst them, BPN is one of the most powerful models since it is easy to understand, and can be easily implemented as a software simulation. The back propagation networks were probably the main reason behind the re-popularisation of neural networks. BPN also has other advantages. It can allow a high tolerance to noisy data and can classify patterns which they have not been trained [6-7]. It is an incremental mining technique that allows new data be submitted to a trained neural network to substitute the previous training result. Consequently, it is adequate to use BPN to cope with the detection of credit card fraud. In this research, we will utilize BPN to detect fraud.

3 Approach

The personalized approach for predicting credit card fraud is depicted in Fig. 2 [2]. To begin with, we collect the transaction data of new users by using an online, self-completion collecting system. This method is very appropriate for new users who only have few transactions or haven't any transactions. After that, the data are trained by BPN and hence personalized classifiers are created. Finally, these personalized classifiers are used to predict new transactions as fraudulent or genuine ones.

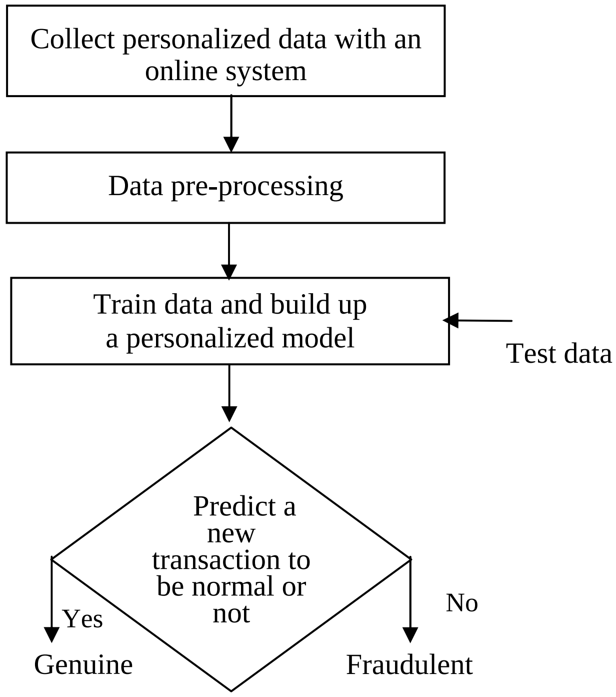
Collect personalized data with an online system
Data pre-processing
Train data and build up a personalized model
Test data
Predict a new transaction to be normal or not
Yes
No
Genuine
Fraudulent

Fig. 2. The procedure for predicting credit card fraud

A. Data Collection

To examine the effectiveness of the proposed approach, data are collected and then personalized models are built up for users. To get representative data for a better modeling of the reality, we let users select the priority of six main classes, which can be further divided into 16 subclasses, of transaction items, and collect different amount of data according to pre-specified ratios. The design platform of the online questionnaire system was Windows. The program we used was ASP. The database was MySQL 2000.

The questions on the questionnaires are generated in keeping with the individual's consuming preference from surveys [17-20]. Consumer behavior changes considerably with each individual. It is accordingly practical to classify their behavior in relation to several main attributes. The collected personal data consist mainly of several parts: age, gender, transaction intervals, transaction amount, and transaction items. The details are described as follows.

1) Transaction Intervals. Each day can be divided into some intervals. In this study, 8 intervals are selected. 8 intervals are enough to characterize the consumer behavior. The transaction time can be merged into 4 intervals if the consumer behavior does not depend considerably on the transaction time.

2) Transaction Item. Each individual has its preferred consuming tendency, according to the survey of consumer behavior. Therefore, in this paper, we divide transaction items into six major classes: eating, wearing, housing, transporting, educating, and recreating. Each main class can be further divided into more detailed subclasses. In total, 16 subclasses are categorized.

The data can be collected anytime. To investigate if the present classifier is able to predict future data, the data were collected monthly. The influence of the time-varying effect on the prediction performance is investigated.

B. Data Training

In this study, we employed BPN to train all personalized data. The BPN tool we used is the **SmartNeuron 0.42,** which was developed by Professor C.C. Chang with Department of Logistics Engineering and Management, National Taichung Institute of Technology (NTIT), Taichung, Taiwan. **SmartNeuron** was built up by Visual C++.

Some parameters are needed to train data using BPN. Among the most important parameters are the numbers of hidden layer, hidden nodes, learning rate, training epochs, and momentum rate. The setting of the parameter values remains as an art rather than a science. Complicated problems can be increasingly better modeled by adding hidden layers, but the improvement generally goes together with a related cost in terms of training time and data overfitting. To improve the above problems, we evaluated some parameter values in preliminary training, which decided the number of hidden layer, the number of nodes, and the number of epochs, based on recommendations from previous literature and our past experience. Besides, the effect of the ratio of the number of training to total data is studied since the collected data of personalized approach are finite.

C. Data Overlapping

Consumer behavior usually changes over time, and thus may cause data overlapping, i.e., many genuine transactions may be similar to fraudulent transactions. The opposite also occurs, as a fraudulent transaction appears to be normal. Figure 3 displays an overview of the data distribution of collected personal data by self-organizing maps (SOM) [5]. The data in white regions are normal, while in black regions are fraudulent. A darker color indicates a stronger tendency to the fraudulent behavior. As illustrated in this figure, there are some overlapping data; i.e., some genuine data are similar to fraudulent data. Consequently, to get higher detection rates, it is very important to choose an appropriate classifier to classify the genuine and fraudulent behaviors.

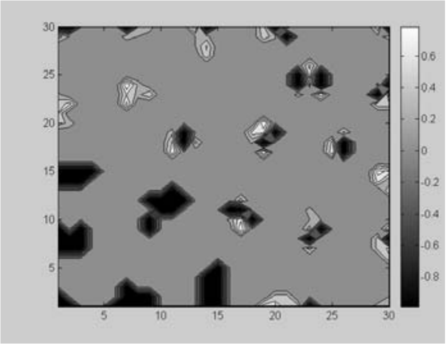

Fig. 3. A typical overview of collected credit card data [5]

In order to effectively analyze the dataset of contradictory data among the transaction data, we use a simple method to do the calculation. Let 1 be the normal condition and 0 the abnormal condition, as shown in Fig. 4. Consider 2 adjacent samples from a specified person. When the transaction items, the transaction amounts, and the transaction intervals are the same and both of them have different signs, or when the transaction items and the transaction intervals are the same, the transaction amounts are different but the sequential information alters from positive to negative or the opposite (low transaction amount is abnormal, higher transaction amount is normal), under such conditions, we know that the data collected are contradictory.

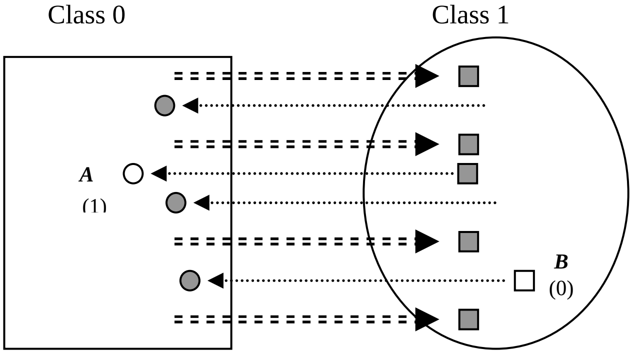

Fig. 4. A schematic diagram of contradictory points

4 Results and Discussion

In this study, we employed BPN to train all personalized data. The BPN tool we used is the **SmartNeuron 0.42,** which can be executed online. All the experiments were performed with desktop PC.

The data are divided into three parts: training, testing, and validation. There are 28 data in the validation subset, 16 data in testing subset, and 64 data in the training subset. Totally, there are 108 data selected for each experiment. As mentioned in [1], users are generally not willing to answer too many questions and they averagely answer about 100-120 data. Therefore, 108 data are appropriate for the following experiments. In addition, another 100 data were randomly selected from *future dataset*, which was collected after one month.

For the convenience of discussion, let us denote the number of nodes in layer 1 and layer 2 as $N_{L1} \times N_{L2}$, where N_{L1} is the number of nodes in hidden layer 1 and N_{L2} is the number of nodes in hidden layer 2, respectively.

A. Effect of Network Architecture on Prediction Performance

To train data with BPN, some parameters must be set. According to the results from the preliminary training, we decided to use the following settings: the learning rate is 1, the momentum rate is 0.5, and the learning cycle is 10000.

The influence of the network architecture on the prediction accuracy is illustrated by a Bubble chart, which is a variation of a Scatter chart in which the data points are replaced with bubbles. The chart contains values for three types of data: number of hidden nodes, average accuracy, and standard deviation. The size of the bubbles is determined by the values of standard deviation. The value of the bubble center indicates the average accuracy. In our experiments, each structure was run 10 times to get average and standard deviation. Notice that the data in this Bubble chart is plotted as follows: Number of nodes is displayed along the horizontal (x) axis. Accuracy is displayed along the vertical (y) axis. Standard deviation is represented by the size of the bubbles.

Figure 5 depicts the results of testing. The ratio of the number of training data to testing data is 20:80. The position of the center of the Bubble stands for average accuracy and the radius of the Bubble represents the standard deviation. The higher the position of the center, the better the prediction is. On the other hand, the smaller the Bubble, the better the prediction is. As we can easily see from Fig. 5, 5×13 has a higher center position and a smaller Bubble, indicating that it is a good architecture.

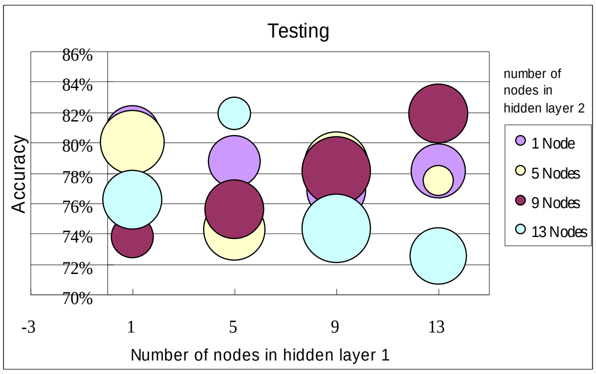

Fig. 5. The influence of the network architecture on the testing accuracy

A good classifier should not only be able to predict accurately the present data but also future data. If the overfitting occurs, the classifier will fail to predict future data correctly. The Bubble chart can provide visualized convenience to check if overfitting occurs. Figure 6 shows the validation result of overfitting. Form Fig. 6, we can see that all the architectures have about the same accuracy, including 5×13. Thus, 5×13 is a good classifier since it has higher and more stable testing and validation results.

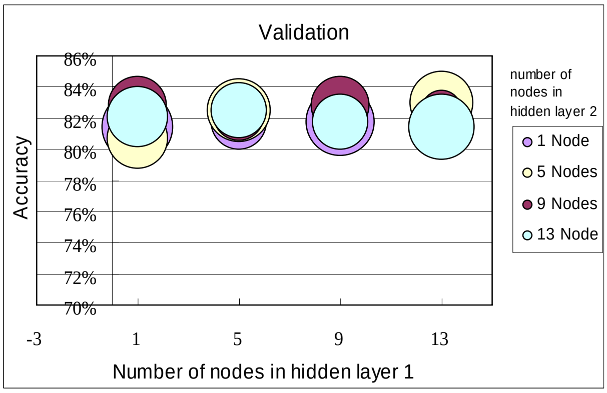

Fig. 6. The influence of the network architecture on the validation accuracy

B. The Influence of the Number of Contradictory Data

The number of the contradictory data plays an important role in prediction. To investigate the influence of the number of contradictory data on the prediction accuracy, we let the number of contradictory data vary from 1 to 4. As the number of contradictory data increases, the prediction accuracy decreases. Figure 7 shows this trend. Therefore, to ensure good performance, contradictory data should be reduced.

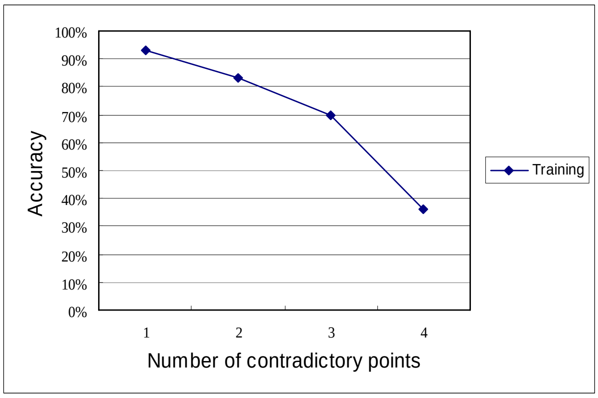

Fig. 7. The influence of the number of contradictory data on the prediction accuracy

C. Time-varying Effect

A good classifier should be able to classify the future data. Table 1 shows the result of predicting future data, which were collected one month later than the former dataset. Again, the architecture of 5×13 was used. In addition, 13×5 architecture was also selected since it has smaller Bubble and higher validation accuracy. From Table 1 we can observe that both architectures have good prediction performance, i.e., high prediction accuracy and small standard deviation, which indicates the results are stable.

Table 1. The performance of predicting future data with 5×13 and 13×5 architectures

Accuracy	Architecture	
	5×13	13×5
Average	81%	82%
Standard deviation	0.02646	0.02854

5 Conclusions

We have employed a personalized approach to detect credit card fraud and designed a series of experiments to test the prediction performance of neural networks on credit card fraud. The approach is to prevent fraud from users' initial use of their cards. Unlike the traditional way, we come up with a model before use of new cards. First, we collect the personalized data of new users by using an online questionnaire system. After that, the collected data are trained by using back propagation networks (BPN) and personalized classifiers are generated.

The bubble chart was employed to visualize the architecture of the neural network. Results from this study show that BPN can have good tested accuracy. However, higher tested accuracy may have a higher degree of tendency to overfitting, which in turn causes worse prediction on the future behavior. In addition, the prediction accuracy depends strongly on the number of the contradictory data. Further studies are encouraged to reduce the influence of the contradictory data on prediction accuracy and to find an optimal solution with both good tested accuracy and validation accuracy.

Acknowledgments

The authors wish to express their sincere appreciation to Professor Cheng-Chih Chang with Department of Logistics Engineering and Management, National Taichung Institute of Technology (NTIT) for his **SmartNeuron** software. Thanks are also given to the Institute of Computer Science and Information Technology, NTIT, which developed the online data-collecting system. Our thanks also go to Lin-Ti Chen with Tamkang University for her help on the review of this paper. This work was supported by the National Science Council under grant no. NSC 94-2213-E-025-010.

References:

[1] National Credit Card Center (NCCC) of R.O.C., Annual Report, http://www.nccc.com.tw/year-book/94yearbook/94Chinese.pdf,

[2] R.C. Chen, M.L, Chiu, Y.L. Huang, and L.T. Chen, "Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines," *Lecture Notes in Computer Science (LNCS)*, Vol. 3177, pp. 800-806, 2004.

[3] R.C. Chen, T.S. Chen, Y.E. Chien, and Y.R. Yang, "Novel Questionnaire-Responded Transaction Approach with SVM for Credit Card Fraud Detection," *Lecture Notes in Computer Science (LNCS)*, Vol. 3497, pp. 916-921, 2005.

[4] R.C. Chen, S.T. Luo, X. Liang, and V.C.S. Lee, "Personalized Approach Based on SVM and ANN for Detecting Credit Card Fraud," Proceedings of the *IEEE International Conference on Neural Networks and Brain (ICNN&B 2005)***,** Beijing, China, Vol. 2, pp. 810-815, 2005.

[5] R.C. Chen, T.S. Chen, and C.C. Lin, "A New Binary Support Vector System for Increasing Detection Rate of Credit Card Fraud," accepted by *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 20, No. 2, pp. 227-239, 2006.

[6] J. Han and M. Kamber, *Data Mining: Concepts and Techniques*, Morgan Kaufmann Publishers, San Francisco, USA, 2001.

[7] C. Phua, D. Alahakoon, and V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data," *ACM SIGKDD Explorations: Special Issue on Imbalanced Data Sets*, Vol. 6, No. 1, pp. 50-59, 2004.

[8] P. Chan and S. Stolfo, "Toward Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection," *Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining*, pp. 164-168, AAAI Press, Menlo Park, California, 1997.

[9] P.K. Chan, W. Fan, A. L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," *IEEE Intelligence Systems*, pp. 67-74, Nov.-Dec., 1999.

[10] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," *Proceeding of IEEE International Conference on Tools with Artificial Intelligence*, 1999.

[11] F.S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit Card Fraud Detection Using Bayesian and Neural Networks," *Proceedings of Neuro Fuzzy*, Havana, Cuba, 2002.

[12] S. J. Hong and S. M. Weiss, "Advances in Predictive Models for Data Mining" *Pattern Recognition Letters*, pp. 55-61, 2001.

[13] M. Lam, "Neural Network Techniques for Financial Performance Prediction Integrating Fundamental and Technical Analysis," *Decision Support Systems*, Vol. 37, pp. 567-581, 2004.

[14] W. Cheng, B.W. McClain, and C. Kelly, "Artificial Neural Networks Make their Mark as a Powerful Tool for Investors," *Review of Business*, pp. 4-9, summer, 1997.

[15] X. Liang, "Impacts of Internet Stock News on Stock Markets Based on Neural Networks," *Lecture Notes in Computer Science (LNCS)*, Vol. 3497, pp. 897-903, 2005.

[16] D.S. Huang, *Systematic Theory of Neural Networks for Pattern Recognition*, Publishing House of Electronic Industry of China, Beijing, 1996.
[17] http://www.104pool.com/
[18] http://www.sino21.com/
[19] http://isurvey.com.tw/
[20] http://b-times.com.tw/