International Business Management 10 (16): 3514-3517, 2016
ISSN: 1993-5250

Combining Neural Network and Genetic Algorithm to Detect Fraud in Credit Cards

Morteza Talebi
Department of Information Technology, Faculty of Management,
Islamic Azad University, South Tehran Branch, Tehran, Iran

Abstract: In recent years, we can see a significant increase in electronic transactions because of the popularity of the world wide web. Beside transaction increasing, we can see fraud increasing by abnormal users which leads to billions of dollars in financial losses in world. The goal of this research is studying the proposed methods in field of data mining to detect fraud in credit cards and proposing a solution base on neural networks techniques and genetic algorithm for this situation.

Key words: Network, genetic algorithm, credit cards, solution, Iran

INTRODUCTION

Now a days, banks and financial institutions are faced with many customers and transaction volumes everyday because of expand financial services that exact study of them is impossible by normal methods; on the other hand financial and credit institutions try to find a solution to have the ability of knowing criminal acts quickly. To study the high amount of such information data mining techniques are useful.

In this study, we try to give a solution to recover the existing algorithms and testing these solutions on the whole data of financial institutions by studying different methods that are proposed in data mining field with help of neural networks and Genetic algorithms to prevent fraud and criminal acts in financial institutions.

Literature work Fraud in electronic banking system is an increasing world wide problem. Therefore, financial institution, need fraud detecting systems based on artificial intelligence for establishment and continuation of the activity (Alford and Mike, 2013). In research area, different techniques of fraud detecting has evaluated by different research groups that are studied by many research completely (Phua *et al*., 2010). It has been used different techniques to solve this problem that we introduce some of them in this study.

Neural networks are a method to study statistical data modeling that is designed based on human brain performance (Yeh and Lien, 2008). Neural networks have been used widely in clustering and classifying. It has been proposed a clustering model to detect fraud by using neural networks (Green and Choi, 1997). By using fraud detecting the ability of fraud prediction in companies managing level will be possible (Cerullo and Cerullo, 1999). In researchers study the effect of neural networks, decision tree and Bayesian method to detect fraud in financial information (Kirkos, 2007). We can see that when financial ratio is using as data sets, using neural networks gives better results than other methods (Fanning and Cogger, 1998).

Consolidated use of artificial intelligence different methods in data mining process has been considered by researchers recently. Using multi methods with each others can consolidate the advantages of these methods and make a better result. In a method has been proposed to detect telecommunication fraud (Olszewski and Dominik, 2012). This method has been done based on users profiling by using Latent Dirichlet Allocation (LDA), a production model in statistics. In a fraud detecting method has been proposed based on users account illustration and threshold type identification. Illustration method that is used in this approach is self-organizing mapping SOM (Olszewski and Dominik, 2014). In transaction integration strategy has been used to detect fraud in credit cards. In this method, transaction characteristic has been collected before transaction to understand users buying behavior to identify fraudulent transactions before happening (Jha *et al*., 2012). In a new approach of cost-sensitive decision tree has been proposed to decrease classified expenses which solve the problem of fraud identification (Sahin *et al*., 2013).

In the problem of credit cards fraud detecting has been solved by using artificial safety system (Halvaiee *et al*., 2014). In this study, it has been proposed a new model which is named artificial safety system fraud detecting model or AFDM. This model has been used by using artificial safety system and its recovery to detect fraud. Random forest RF is one of the most popular methods for classification, prediction, determining variable importance, variable selection and outland point detection (Verikas *et al*., 2011). Different usages of RF has

been proposed in different areas that can name and in pattern and fraud detecting in credit cards (Bhattacharyya *et al*., 2011; Zhou *et al*., 2015).

MATERIALS AND METHODS

Effective properties in fraud detecting: There are not stable and specific properties to detect fraud among financial transactions based on paper studies and research. Properties that are studying in banks and financial institutions to detect fraud are not declared because of high sensitivity and safety of this institution. Therefore, there is not a source dataset to study and compare the works that are done before in this area and research works that is done does not publish its studied dataset and does not declare informational properties which exist in it. In this study, it has been used collected data of one of the real discount sites for studying and testing system. The mentioned site in one of the limbless and popular online discount sites in Taiwan. Discount sites in Taiwan have proposed black and white accounts list to help users and identify frauds. Black and white accounts list, account ID, crime type, related tender date and history of crime is reported by these sites. Unfortunately, the properties of criminal behavior are not proposed in most of discount sites. This study tries to suggest a combined system of neural system and genetic algorithm which identifies fraud accounts based on registered data.

Suggested approach: In suggested fraud detected system, it has been used neural network techniques and Genetic algorithm combination for attention and identification system usage rather than existing systems. In this fraud detecting system, the proposed neural network tries to find the relation between properties and fraud detecting by studying effective properties in identifying fraud in credit cards. On the other hand, Genetic algorithm tries to recover the results by suggesting different configurations for neural network. Therefore, suggested genetic algorithm leads to better usage of proposed neural network in detecting fraud. The suggested artificial neural network flow chart is available in Fig. 1. The usage of suggested genetic algorithm will describe in continue to optimize neural network fraud detection.

Chromosome show: In this study, chromosome is used to determining hidden layers number and existing neurons number in every layer. Chromosome genes are shown as binary numbers. Based on applied restrictions, every 4 genes show a layer of neural network. Binary numbers that are shown by 4 genes indicate existing neuron

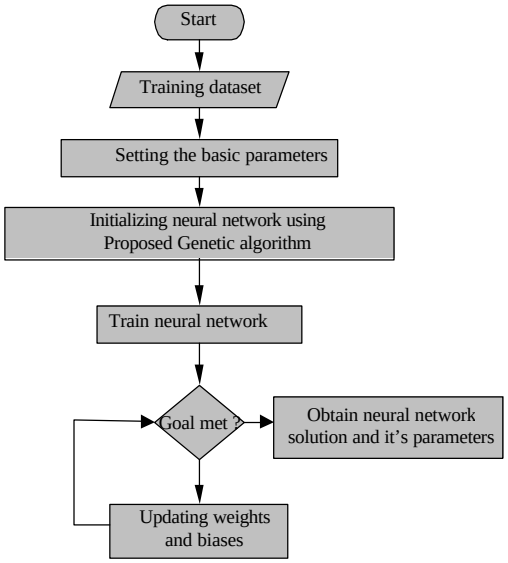

Fig. 1: The suggested neural genetic system flowchart for detecting fraud

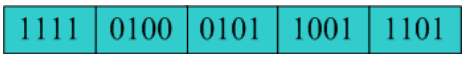

Fig. 2: Chromosome show

numbers in every layer. Figure 2 has been shown as a sample of these chromosomes. This chromosome shows that neural network has 5 hidden layers. Other information which is understandable from this chromosome is the number of existing neurons in every system. As an example in first layer there are 11 neurons and in second one there are 7 neurons.

Fitness function: In defined goal function in this study, it is determined that for configuration of network by current chromosome, how correct the duty of fraud detecting is done. In this relation, the number of transactions that is studied correctly by neural network black transactions as fraud transactions and white ones as no fraud are considered as fitness of every solution based on the whole studied transactions.

Selection: In this study, it has been used roulette whiled method for doing selection performance. This method is a random or alternative sampling. This method that is based on chance is done in a way that all people are mapped base on their own competency on neighboring areas of a line. The size of related area to everyone will define based on his own competency. Then, a random number is produced and man is selected based on the size of this number.

Recombination: In this study, we choose a random combination point as a multiple of 4 for doing recombination performance to make the selected solutions combination from genes that define layers. A sample of recombination performance doing has been shown in Fig. 3.

Mutation: It is possible for Genetic algorithms to have problem with optimized areal solutions. Mutation can change a part of gene randomly and guide evolution to other solutions in order to search possible spaces to find desirable solutions.

To do the mutation, related genes to a layer will be selected randomly and the related neurons number will change. You can see a sample of mutation performances sample in Fig. 4 as an example. In this example, second layer has been selected for mutation. As you see in Fig. 4, the selected number for this layer is 4. In this performance,

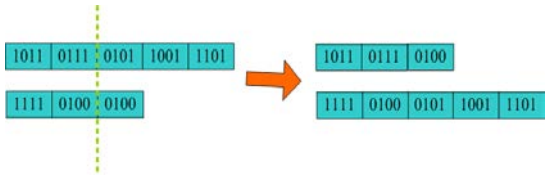

Fig. 3: A sample of recombination performance doing

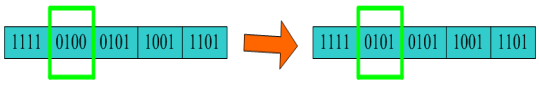

Fig. 4: A sample of mutation performance

a random step mutation will add or minus to this number step mutation has been considered 1. In this Fig. 4, a unit has been added to related number and neurons number of second layer has been increased to 5.

RESULTS AND DISCUSSION

In this part, we try to study the proposed neural genetic system's performing way. To do this work, at first we study the performing way of proposed neural network without using the studied Genetic algorithm. In this case, all of the neural network's parameters will be amounted manually. The obtained result for this system will be specified by performing neural network and accuracy of fraud detecting in this system is 0.512.

In second case, the offered neural network optimizes its structure by using proposed Genetic algorithm and tries to test the system by using different input parameters, therefore, it will have positive situation during neural network learning algorithm performance. In Table 1, it has been proposed the considered amounts for suggested algorithms variables.

For doing this experiment, the offered algorithm in both cases that defined above, have been performed 10 times. Primary population in this experiment is 100 and generation number is considered 100. The previewed chart in Fig. 5 shows the system's performing way in second

Table 1: The amounts of suggested algorithm variables

Variables	Amount
No. of primary population	100.0
No. of generation repetition	100.0
Recombination rate	0.8
Mutation rate	0.4

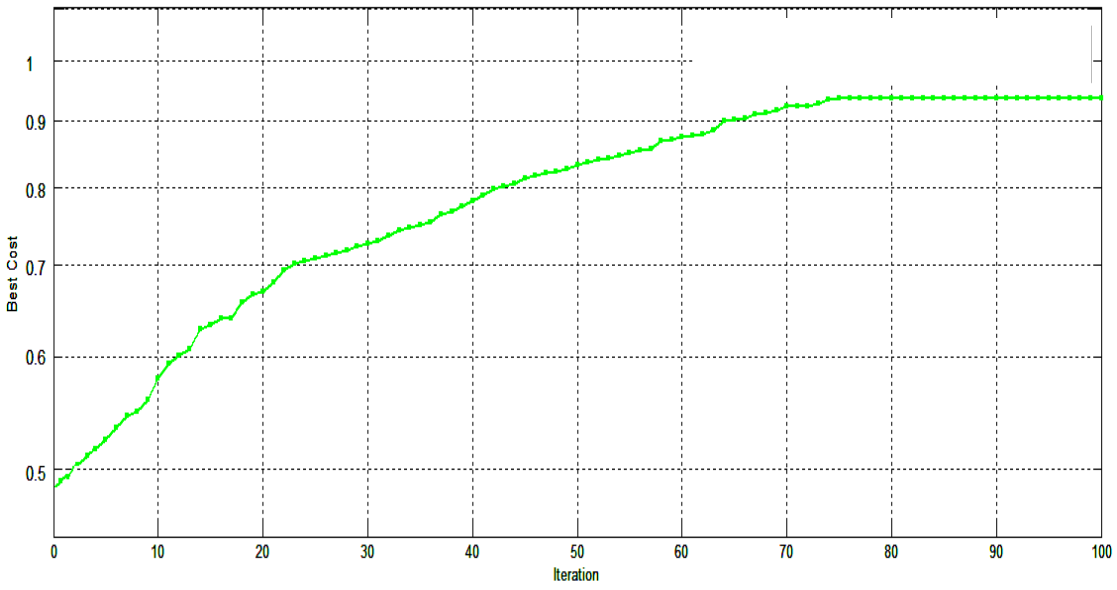

Fig. 5: Performance of suggested genetic system during 100 repetitions

mentioned case. As you see in this Fig. 5, the accuracy of fraud in offered neural network will be able to recover the performance by using suggested Genetic algorithm and its accuracy is 0.941.

CONCLUSION

One of the important obstacles for using and promoting electronic banking is insecurity of transactions and fraud detection in financial exchanges. Therefore, electronic fraud detection is one of the important problems in financial institutions and banks. The goal of this paper is offering a solution based on artificial neural network and Genetic algorithm for detecting fraud of credit cards. The offered Genetic algorithm in this study, tries to give the most suitable configuration for neural network by suggesting different input parameters for neural network and fraud detecting accuracy. Simulation results show that the offered Genetic algorithm has significant effect in performance increasing and neural network accuracy to detect fraud in credit cards.

REFERENCES

Alford, M., 2013. Intelligent fraud detection: A comparison of neural and Bayesian methods. Comput. Fraud Secur., 2013: 14-16.

Bhattacharyya, S., S. Jha, K. Tharakunnel and J.C. Westland, 2011. Data mining for credit card fraud: A comparative study. Decision Support Syst., 50: 602-613.

Cerullo, M.J. and V. Cerullo, 1999. Using neural networks to predict financial reporting fraud: Part 2. Comput. Fraud Secur., 1999: 14-17.

Fanning, K.M. and K. Cogger, 1998. Neural network detection of management fraud using published financial data. Int. J. Intellig. Sys. Account. Finance Manag., 7: 21-24.

Green, B.P. and J.H. Choi, 1997. Assessing the risk of management fraud through neural network technology. Auditing, 16: 14-28.

Halvaiee, N.S. and M.K. Akbari, 2014. A novel model for credit card fraud detection using Artificial Immune Systems. Appl. Soft Comput., 24: 40-49.

Jha, S., M. Guillen and J.C. Westland, 2012. Employing transaction aggregation strategy to detect credit card fraud. Expert Syst. Appli., 39: 12650-12657.

Kirkos, E., C. Spathis and Y. Manolopoulos, 2007. Data mining techniques for the detection of fraudulent financial statements. Expert Syst. Appl., 32: 995-1003.

Olszewski, D., 2012. A probabilistic approach to fraud detection in telecommunications. Knowl. Based Syst., 26: 246-258.

Olszewski, D., 2014. Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Syst., 70: 324-334.

Sahin, Y., S. Bulkan and E. Duman, 2013. A cost-sensitive decision tree approach for fraud detection. Expert Syst. Appli., 40: 5916-5923.

Verikas, A., A. Gelzinis and M. Bacauskiene, 2011. Mining data with random forests: A survey and results of new tests. Pattern Recognit., 44: 330-349.

Yeh, I.C. and C.H. Lien, 2009. The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients. Exp. Syst. Appli., 36: 2473-2480.

Zhou, Q.F., H. Zhou, Y.P. Ning, F. Yang and T. Li, 2015. Two approaches for novelty detection using random forest. Expert Syst. Appl., 42: 4840-4850.