Recognition of fraud in online banking by using confirmatory learning in neural network

Alireza Pouramirarsalani[1], Majid Khalilian[2], Alireza Nikravanshalmani[3]

[1]Master of Science, software, Department of Computer, Faculty of Mechatronic, Islamic Azad University, Karaj branch, Iran
[2]PhD, software, Department of Computer, Faculty of Mechatronic, Islamic Azad University, Karaj branch, Iran
[3]PhD, software, Department of Computer , Faculty of Mechatronic, Islamic Azad University, Karaj branch, Iran

Abstract:
Nowadays, exploring knowledge from huge collections of data attracts many experts. Because of this matter, data mining is considered as one of the most efficient tool for analysis of data. Application of different techniques and algorithms of this tool in different areas like management of communication with customer, management and exploration of fraud, medical, sport etc. are evident for this claim and it is one of areas that can be considered as a field of data mining. In modern world, synchronous with advancement of information technology and communication infrastructures, banking systems and financial services also have developed. Banks and financial institutions try to present update and more efficient services and products by investing in modern technologies. Therefore, variety of products and related services and also number and proportional value of transactions are increased. In contrast with this advancement and development, immunization of transactions, identification of new ways of fraud and misuse of financial documents, exploration of performed frauds or in progress, identification and exploration of processes and money laundering operations are always the taut discussions in this field. This research introduces new approach for exploring fraud in online banking that has high speed in recognizing and predicting the fraud and automatically updated and completed.

Keywords:
recognition of fraud, online banking, confirmatory learning, neural network

1. Introduction:

By ever-increasing development of accessibility of society people to internet, the application of E-commerce in daily trades also increases. From most important pillars of E-commerce are electronic payment systems and fraud in electronic payments is one of main problems. Not only financial fraud can inject financial damage to related organization but also causes remove of validity and compromises trust of customers. Then, in the case of lack of employing certain mechanisms and preventing from fraud, we should predict increase of fraud statistics in the space of online banking.

Today high volume of financial and monetary transactions and redeployment perform in Internet and electronic bed. Ever increasing growth of these services and transactions on one side and unknowing of guilty in Internet bed encourage and motivate cheaters and fraudulent to enter this area. Because of lack of physical presence of customers in electronic services, the necessity of identification in presenting these services is very important and beneficial in the view of monetary and financial institutions and maybe we can claim that main limitation in presenting more developed and extensive banking services is the necessity of identification. This problem is the main factor of attraction of fraud in electronic services that increases based on development of online banking services.

Operations and acts that are performed based on approaches and methods to explore and recognize occurred or in progress frauds define as fraud recognition. Monetary and financial institutions want promptitude strongly in recognition of activities of cheaters. This matter is very important because of its direct impact on customer services of these institutions, reduction of operational expenses and remaining as valuable and trustworthy financial institution.

The algorithms that are used for recognition of fraud generally performed by consideration of related information of customer like account number and performed transactions. In this research, we consider specially the misuses that perform through online banking. Generally, the approaches of fraud recognition divide into two main categories:

Anomaly detection: in the approach of anomaly detection, the history of customer behavior considers as normal and usual behavior and any deviation from this behavior can be registered as anomaly.

Manuscript received August 5, 2017
Manuscript revised August 20, 2017

Misuse detection: the recognition approach emphasizes on special behaviors of customer and hypothesizes exactly identified behaviors as fraud.

Two current techniques of data mining for fraud detection are regression neural network. The approach of neural networks is based on learning. In most cases, performance of works by neural networks has better result in comparison with traditional statistical approaches. When we encounter with huge amount of statistical data, use of neural networks is the most optimum technique. The approach of neural networks is a technique that has high application in systems of fraud detection. The idea of this technique is that a neural network doesn`t need pure mathematical models unlike computers that need full clear and definite commands and has the capability of learning like human by some certain examples.

In this research, we want to present new approach based on neural network and approach of confirmatory learning by the purpose of fraud detection in online banking.

This research formulates in five chapters. In second chapter, we review history of research about fraud detection. Third chapter defines generally the confirmatory learning and fourth chapter introduces suggested approach. Fifth and sixth chapters show results and conclusions of research, respectively.

2. The history of research:

Reily and Ghosh (3) presented a Three-layer, feed-forward, radius-limited perceptron network in 1994. This model uses for recognition of pattern. In this model, experimental data read only two times. In output layer, a numerical value creates as rank of transaction that if is lower than a threshold, that transaction will be recognized as fraud.

Falcon Fraud Management System that is very strong tool for preventing from activity of cheaters in misuse of credit and debit cards uses algorithms of neural network. This system predicts the probability of fraud on an account in comparison with current transaction and previous activities of card owner (Hassibi, 200)(4).

In 2004, they presented a framework based on safety systems (6) and case based reasoning for recognition of fraud. At first, a collection of normal and fraud cases are created from labeled data. Then, early recognizers are created with random or genetic algorithms. After that, negative selection and clonal selection operations apply on early recognizers to achieve a collection of recognizers with different patterns that can recognize different frauds.

Presented paper by Bhattacharyya (2010) is about consideration of fraud in credit cards of one financial institution that in this research, 50 million transactions of 1 million credit cards are used. Because the relation of correct transactions than transactions with fraud is 0.05% in this research, writers used sampling approach for creation of datasets with different relations from fraudulent transactions in dataset of (2%, 5%, 10%, and 15%) (8).

From newest published papers about fraud recognition in credit cards is Dal Pozzolo et al. paper. In this paper, writers emphasized on three main problems of imbalance of data, instability and evaluation of approaches and considered transactions of credit cards as data process that system of fraud recognition should have the ability of fraudulent transaction recognition immediately.

Sasirekha(2010) expressed in his research that many of presented fraud detection systems used data mining and approaches of neural networks. While a fraud detection system is not used with combination with anomaly detection, detection of misuse and decision-making system in detection of fraud of credit cards. Then, a system by use of hidden Markov model is suggested for recognizing fraudulent transactions.

3. Confirmatory learning

Confirmatory learning (11) is one of learning aspects of machine learning that develops based on behavior of animals and humans. The purpose of this approach is making decisions in terms of environment to attain most prizes. Confirmatory learning can be defined simply in one sentence: learning by interaction with environment to achieve certain goal. Decider and person that learn called agent. The things that agent interacts with them are environment. This interaction occurs continuously as the agent decides and performs an act based on decision and environment in response to this acct gives a prize to it and moves to new mode.

Rather agent and environment interacts with each other continuously during time steps of t: 0.1.2….. . In each step for example time T, the agent receives new mode from environment.

St that is subgroup of S with general modes indicates mode in time T. based on mode in intended time, related act also performs.

In time of t+1, environment gives numerical prize based on agent action in previous step to it and agent finds itself in new mode of St+1.Below figure shows this interaction.

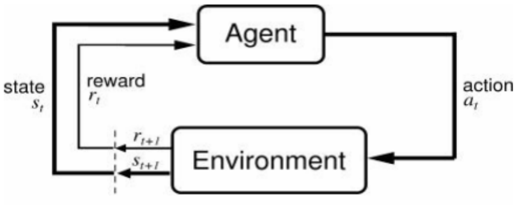


Figure 1

Learning algorithm is:

First level: observation of environment mode in time t that is shown by St.

Second level: control strategy gives as output of At decision making.

Third level: after accomplishment of At action, transfer of environment to St+1 mode is performed and rt confirmatory signal achieved for control system simultaneously.

$$\varepsilon = r_{t+1} + [\gamma V_t(x_{t+1}) - V_t(x_t)]$$

Fourth level: regarding rt and mode transfer, ε calculated.

Fifth level: function of mode evaluation and control strategy updated according to ε.

$$\varepsilon = r_{t+1} + [\gamma V_t(x_{t+1}) - V_t(x_t)]$$

These five levels create learning cycle. Learning levels repeat until optimum strategy is achieved.

4. Suggested approach

In this section of paper, modern approach of paper is introduced. Suggested approach developed by using confirmatory learning in neural network. Artificial neural network is operational approach for learning different functions like functions with real values, functions with discrete values and functions with vector values. A neuron can be used for identifying functions that separated linear. While in real problems, linear functions cannot be separated generally, we need a network of neurons. Different neural networks are used for resolving different problems of learning with supervision, learning without supervision and confirmatory learning. Neural networks divide into two kinds of onward FNN (12), recursive RNN (13). FNNs are the most current kinds of neural networks that used in different applications. The first layer called entrance layer and last layer is output layer and several layers between these two layers called middle or hidden layers because we only work with inputs and outputs of neural networks. Neural network acts as black box and there isn`t direct access to middle layers. Recursive neural networks have oriented cycles in their relation graphs structures. It means that they follow relations among nodes and return to previous and first nodes. RNNs have complicated dynamic based on their structures and this matter difficult training of these networks. Also, from biological point of view, recursive neural networks near to reality further.

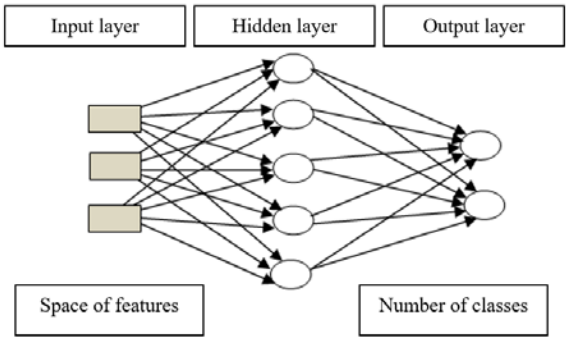


Figure 2

For training (determination of weights and biasing) of FNN neural network, there are two ways: classic approaches like hybrid of feature selection and back propagation algorithm and smart optimization approaches like hybrid of feature selection and genetic algorithm and hybrid of feature selection and optimization algorithm of particles swarm intelligence PSO (14).

BP approach is based on descending gradient in error space and has local search ability. Modification of weights of neural networks performs as in each round, the error between desirable output and output of neural network decreases. This error defines as follows:

$$E = \frac{1}{2} \sum_{n \in \text{training}} (t^n - y^n)^2$$

According to these cases, error is calculated for collection of n numbers of training samples. t is desirable output and y is output of neural network. The power of hybrid selection of feature and BP algorithm is hidden in calculation capability of effective error for each unit. Finally, each weight changes in round of m+1 as follows:

$$w(m+1) = w(m) + \Delta w$$
$$\Delta w = \eta \delta x$$

In the above relation, η is learning rate and δ difference between desirable output and output of neural network.

General structure of algorithms of feature selection expressed below.

Input:

S − data sample with features X, |X| = n

```
J − evaluation measure to be maximized
GS – successor generation operator
Output:
Solution – (weighted)feature subset
L := Start_Point(X);
Solution := { best of L according to J };
repeat
L := Search_Strategy (L, GS(J), X);
X' := {best of L according to J };
if J(X') ≥ J(Solution) or (J(X') = J(Solution) and
|X'| < $|Solution|$) $then\ Solution := X'$;
until Stop(J, L).
```

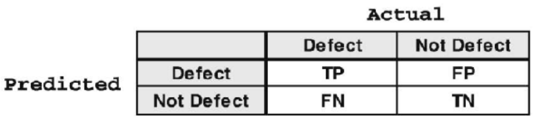
The input of algorithm is given samples with X features. That the number of these features is equal to n and j that is criteria for algorithm evaluation and the purpose of algorithm is maximizing this criterion and GS is operator of next feature selection in each level of algorithm (15).

5. Simulation results:

In this research, 80% of data selected as training data and the rest as test data. The approach of data selection is randomly. Used software in this research is MATLAB version 2015.

In performed researches about error prediction in software, categorization models based on software metrics predict a software modular as error talented or unlike it.

From categorization approaches are binary approaches for prediction of classes that have error with high probability. In fact, we can use this model for directing and trying to improve quality of modular that recognized as error with high probability during operations. As a result, we can test quality and improve resources. From actions for consideration of hybrid accuracy of feature selection and categorization algorithms of information is use of confusion matrix:



		Actual	
		Defect	Not Defect
Predicted	Defect	TP	FP
	Not Defect	FN	TN

Figure 3

In which TP is number of modular with defect that are predicted error talented correctly, FP number of modular without defect that are predicted error talented wrongly, TN number of modular without defect that are predicted non error talented correctly and finally FN number of modular with error that are predicted non error talented wrongly.

Evaluation criteria of quality of error prediction models in software are:

Misclassification rate

Except cost of Misclassification

Normalized Except cost of Misclassification

Sensitivity

Specificity

Accuracy

Recall

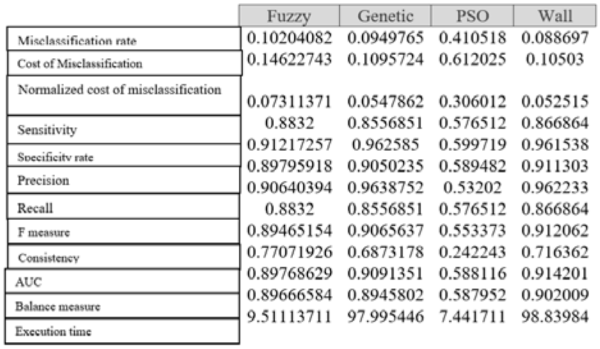
F-measure

Consistency

Receiver operating characteristic

Balance measure

Following table shows the results of its implementation and comparison with other useful approaches.



	Fuzzy	Genetic	PSO	Wall
Misclassification rate	0.10204082	0.0949765	0.410518	0.088697
Cost of Misclassification	0.14622743	0.1095724	0.612025	0.10503
Normalized cost of misclassification	0.07311371	0.0547862	0.306012	0.052515
Sensitivity	0.8832	0.8556851	0.576512	0.866864
Specificity rate	0.91217257	0.962585	0.599719	0.961538
	0.89795918	0.9050235	0.589482	0.911303
Precision	0.90640394	0.9638752	0.53202	0.962233
Recall	0.8832	0.8556851	0.576512	0.866864
F measure	0.89465154	0.9065637	0.553373	0.912062
Consistency	0.77071926	0.6873178	0.242243	0.716362
AUC	0.89768629	0.9091351	0.588116	0.914201
Balance measure	0.89666584	0.8945802	0.587952	0.902009
Execution time	9.51113711	97.995446	7.441711	98.83984

6. Conclusion:

From tools that are considered by many experts for recognition of cheat in banks and financial institutions is data mining. Data mining that is middle group process can identify hidden knowledge and information in huge amount of data and uses them for resolving different problems. The technologies like statistic, artificial intelligence, data set etc. formed theoretical bases of data mining. Because of existence of high data in banks, data mining doesn`t have much efficiency in monetary and financial affairs. Management of credit risk, exploration of fraud and money laundering, management of relationship with customer and management of quality of banking services are the samples of data mining application in banks. In this research ne approach is introduced for recognition of fraud in online banking by use of confirmatory learning in neural network.

Based on achieved results, it can be said that smart artificial intelligence systems are efficient in detection of fraud in online banking. In this research, we use different kinds of confirmatory learning systems and neural network that results show that Percepteron multi layers neural network has the best function among other approaches.

References

[1] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.

[2] Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. In Networking, sensing and control, 2004 IEEE international conference on (Vol. 2, pp. 749-754). IEEE.

[3] Ghosh and D.L. Reilly; "Credit Card Fraud Detection with a Neural-Network"; IEEE, vol. 3, pp. 621-630, 1994.

[4] Hassibi, K. (Ed.).(2000). Detecting Payment Card Fraud With Neural Networks. Singopore: World Scientific

[5] Tue, Ren, Liu; Artificial Immune System for Fraud Detection; IEEE, vol. 2, pp. 1407-1411, 2004.

[6] Dasgupta, D., Ji, Z., & González, F. A. (2003, December). Artificial immune system (AIS) research in the last five years. In IEEE Congress on Evolutionary Computation (1) (pp. 123-130).

[7] Kolodner, J. (2014). Case-based reasoning. Morgan Kaufmann.

[8] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.

[9] Pozzolo. A, Boracchi. G, Caelen. O, Alippi. C, Bontempi. G, “Credit Card Fraud Detection and Concept-Drift Adaptation with Delayed Supervised Information”

[10] M. Sasirekha, Thaseen. Sumaiya, Banu. Saira, 2012, “A DEFENSE MECHANISM FOR CREDIT CARD FRAUD DETECTION”, International Journal on Cryptography and Information Security (IJCIS), pp. 89-100.

[11] Wiering, M., & Van Otterlo, M. (2012). Reinforcement learning. Adaptation, Learning, and Optimization, 12.

[12] Bebis, G., & Georgiopoulos, M. (1994). Feed-forward neural networks. IEEE Potentials, 13(4), 27-31.

[13] Medsker, L. R., & Jain, L. C. (2001). Recurrent neural networks. Design and Applications.

[14] Kennedy, J. (2011). Particle swarm optimization. In Encyclopedia of machine learning (pp. 760-766). Springer US.

[15] S.Vanaja K.Ramesh kumar,” Analysis of Feature Selection Algorithms on Classification: A Survey” International Journal of Computer Applications, 2014, Volume 96