Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
ISSN: 2412-7485
Available online at www.sciarena.com
2018, Vol, 4 (1): 9-19

Detection of the Suspicious Transactions by Integrating the Neural Network and Bat Algorithm

Nikfar Safari[1]*, Touraj Banirostam[2]

[1]Department of computer Engineering, E-Campus, Islamic Azad University, Tehran, Iran,
[2]Department of computer Engineering, Islamic Azad University, Central Tehran Branch, Tehran, Iran.

***Corresponding Author**

Abstract: *Banking system fraud is one of the challenges of banking and e-commerce development. One of the main challenges of machine learning and data mining techniques in bank fraud detection is their low accuracy in identifying these transactions. This research presented a hybrid method based on a multi-layer artificial neural network and bat algorithm to reduce the fraud detection fault. In the proposed method, the parameters of the neural network such as weights and bias are selected optimally by the bat algorithm to reduce the fault rate in the fraud detection. The proposed method is a type of learning intensification in which the bat algorithm improves the learning of the neural network. In the proposed method, the Kmeans clustering is used to remove data from the dataset to increase the accuracy of the proposed method. MATLAB software was used to run the data. The data related to bank fraud indicate that the accuracy, sensitivity, and specificity of the proposed method for detecting bank fraud were as much as 91.46%, 88.97%, and 90.32%, respectively. The comparison of our proposed method with other methods shows that the proposed method is more accurate than methods such as regression and backup machine.*

Keywords: *Artificial Neural Network, Bank Fraud, Bat Algorithm, Clustering, Data Mining.*

INTRODUCTION

New technologies have affected many areas, including financial and banking systems. Today, the new technologies provided in the context of Internet services have flourished banking and increased the banking transactions. The provision of financial and banking services in the context of the Internet and the use of related technologies has transformed the traditional banking system, and many banks and financial and credit institutions use their services and technologies on the Internet for their services (Van Vlasselaer et al., 2015). The use of new technologies in the banking system and the expansion of e-banking provide many benefits to bank customers, simplify the turnaround of capital in the labor market, and promote financial markets. Electronic banking has made the bank using banking services in a very short time without being in urban traffic customers and saving them time and money. Like any other emerging technology, e-banking faces challenges, the most important of which is fraud (Barraclough et al., 2013) and money laundering (Choo, 2015), which is considered as a threat to expand online banking activities. Fraud in the banking system has reduced the credibility of e-banking and provided a platform for illegal practices such as tax evasion. Fraud in a banking system has a devastating effect on the economy and its economic development. Hence, many efforts have been made to deal with this harmful economic, social, and political phenomenon. There is no specified definition for fraud and money laundering, but most authors believe that fraud is actually an attempt to obtain funds from illegal means and attempt to legitimize them. There is no exact boundary between the two concepts of fraud

and money laundering, and there is no precise boundary between the two concepts of fraud and money laundering, and in most cases, these two concepts are applied together (Omar et al., 2014). Methods and techniques of fraud are wide and extensive, and they can also be tracked based on financial transactions of individuals or corporations. Fraud in the banking system is usually done with successive transactions to eliminate the nature of money and its origin, or unrealistic accounts are created and transactions are done with these accounts. The analysis of financial transactions in the banking system can reveal a lot of fraud, but the challenge and difficulty is that the pattern of fraud in bank transactions is hidden and is not easily discoverable. Knowledge discovery method such as machine learning and data mining can be used to detect fraud in the banking system based on the analysis of transactions (Moro et al., 2015). Different techniques are presented or machine learning and data mining that detect fraud from the normal transaction based on the set of features in the transactions. In other words, machine learning techniques and data mining can classify transactions into two types of bank fraud and normal. Pattern recognition and classification by machine learning and data mining methods will increase our knowledge of bank transactions and detect fraud. This paper tries to identify and detect patterns of fraud in order to increase the credibility of the banking system with the help of data mining techniques. The proposed method has initially identified the type of transactions that are outliers with the help of the Kmeans clustering algorithm and removed them or examined separately. Then, the pre-processed dataset is normalized and a suitable classification algorithm such as artificial neural network is used to detect bank fraud. Here, minimizing the classification fault of banking transactions from normal transactions is considered as the objective function of the problem. Given that the nature of the problem is optimization, it is possible to use metaheuristic algorithms to minimize the fault rate in the objective function. So far, many algorithms have been developed to solve the complex problem solving problems. The bat algorithm is one of the most successful algorithms in this field because it has a high accuracy and convergence than other algorithms such as genetic algorithm and particle optimization algorithm (Yang, 2010).

Fraud and money laundering are considered an important challenge in the banking system and have devastating effects on economic activity. Fraud and money laundering can harm a country's economy, with some examples listed below (Gjoni et al., 2015):

- It causes turbulence in financial markets, such as the currency market, because the money from fraud and money laundering will be used to clear the source of capital into these markets. Then, it enters the banking system to be considered as a legal currency.
- It harms the economy of the country and the private sector and thus increases unemployment and inflation.
- Fraud and money laundering can be derived from criminal activities such as trafficking in human beings, drug trafficking, etc., and for the purpose of terrorism support.

Bank Fraud

Fraud and money laundering are a threat to economic activists, shareholders, suppliers, investors and business partners, and the role of fraud in financial losses is significant. According to the report of the US Banking Fraud Protection Organization presented in 2014, there are about 36.6% of banking activities, public utilities, government systems, etc., of which about 17.8% of organized fraud is committed in banks and the financial system, which is estimated at around $ 200 million per year due to the large financial turnover of banks (Sanusi et al., 2015). Figure 1 shows the fraud share in various sectors, including the banking system, is shown as a circular graph. According to the chart below, the fraud share in each banking, insurance, telecommunications and e-commerce sectors is about 53%, 31%, 6%, and 10% respectively, which indicates the importance of identifying fraud in the banking and financial sector:

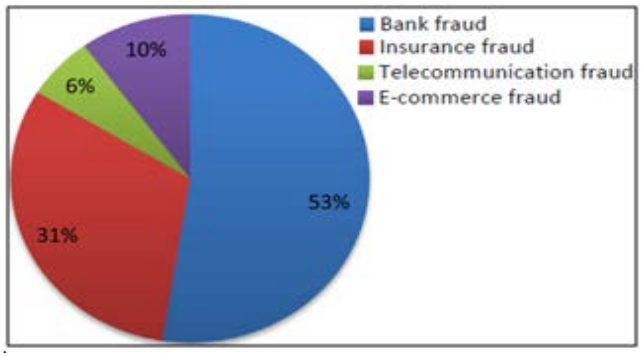

Figure 1: The rate of different types of cyberspace fraud (Abdallah et al., 2016)

According to the above, it can be observed that fraud in the banking system entails a lot of damage to the economy and the banking system. On the other hand, fraud reduces confidence in e-banking. In some ways, recognizing fraud based on its complex and cyclic approach requires the use of knowledge discovery techniques such as data mining and machine learning. Therefore, the current paper is an attempt to apply knowledge discovery systems to deal with banking frauds. Different definitions of fraud in the banking system have been proposed and a single definition for this phenomenon cannot be considered. However, the following definitions of fraud are presented below, which seems to be useful (Abdallah et al., 2016):

- The Association of Certified Fraud Examiners (ACFE) (2007) has considered fraud as a person's intentional misuse of the use and utilization of a government's resources and assets.
- Phua et al. (2005) stated that fraud has different types of internal and external divisions. In the internal type, an employee exploited the internal rules of the company to provide his own interests, and in the external type, which involves a broader range of abusive practices can include individuals, such as customers, vendors, and investors.
- China et al. (2013) divided the bank fraud into three categories of soft fraud, fraudulent fraud, and organized fraud.

West and Bhattacharya divided financial fraud into three categories: bank fraud, corporate fraud, and insurance fraud (West & Bhattacharya, 2016).

Nghi et al. divided various kinds of fraud in the financial area into four categories: banking, insurance, securities and commodities fraud, and fraud in other areas such as mass marketing fraud (Ngai et al., 2011).

There are two general techniques for fraud detection and fraud prevention in the face of fraud in the banking system as shown in figure (2):

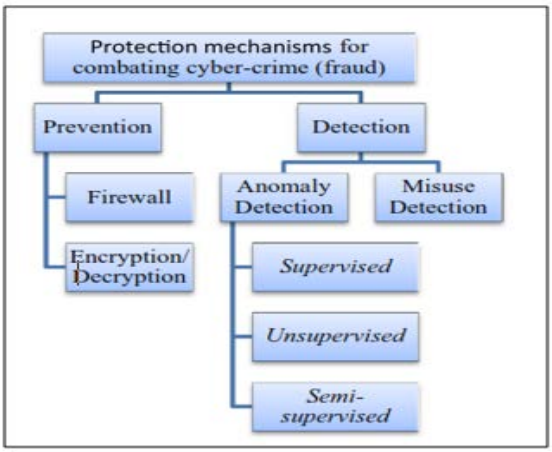

Figure 2: Classification of fraud detection methods (Ngai et al., 2011)

At the stage of fraud detection and prevention, it is tried to delete the transaction or not execute it. In general, there are two methods based on the firewall and encryption and decryption techniques for fraud prevention that can be effective in doing or not doing transactions. In the domain of fraud detection, there are two general techniques (Ngai et al., 2011):

- Anomaly detection technique: In this method, it is tried to detect fraud patterns in the banking system using knowledge discovery techniques. Anomaly detection techniques attempt to extract the fraud pattern using the learning mechanism and use these patterns to identify fraud.
- Misuse detection techniques: In these methods, the bank attempts to deal with fraud using bank records and information. Misuse detection techniques are also sometimes referred to as pattern and signature behaviors.

Anomaly detection behaviors are categorized in a variety of ways, including supervised learning, unsupervised learning, and semi-supervised learning. In supervised learning methods, banking-related datasets are divided into two categories of data with fraud tags and without fraud tags and certainly learning is deeper. In supervised learning methods, classification is practiced by techniques such as the artificial neural network (ANN), logistic regression (LR), support vector machine (SVM), and Naïve–Bayes (NB). In unsupervised learning method, each data have no tag and thus, fraud detection is more difficult in this case. Clustering technique can be mentioned in this regard. In semi-supervised learning methods, a small percentage of the data is tagged, but more data is missing (Ngai et al., 2011).

Materials and Methods

Knowledge discovery techniques are generally divided into two categories of data mining and machine learning, each of which has various techniques can detect knowledge based on the characteristics of banking transactions. One of the most important challenges in fraud transitions based on the money laundering is the existence of noise or outlier data in the dataset related to fraud. In other words, the data collected from the banking system can have faults and some transactions have a significant difference over other transactions, and therefore, they are considered as outlier data and their separation from the banking dataset for learning can increase the precision and performance of the algorithms. By eliminating data from bank transactions, the precision of data mining techniques will also be enhanced to detect useful patterns as disturbing data interferes with learning algorithms. There are several ways to remove noise and data from transactions. One of which is the clustering methods that are considered as a data mining technique. Clustering techniques can separate transactions, identify data that is far from cluster centers, and consider it as noise data. This paper uses a new technique to detect fraud and money laundering, which has two basic steps involved in the first step in the removal of overlap data using the clustering algorithm. In the second phase, classification technique based on the bank transaction data is evaluated and fraud-based transactions are identified. In the proposed method, an artificial neural network is used as a classification technique. Given that the multi-layer artificial neural network has a simple and efficient structure for classification and pattern recognition, this article uses this artificial neural network as a classification technique. An artificial multi-layer artificial neural network is suitable for detecting fraud and money laundering. However, the classification fault can be compensated for money laundering and fraud. Hence, the present paper innovatively applied the concepts of metaheuristic algorithms to reduce the fault of artificial neural network classification in detecting bank fraud as a NP-hard optimization problem.

In fact, a metaheuristic algorithm conducts a learning algorithm to increase the accuracy of the artificial neural network in identifying bank fraud along with a multi-layered artificial neural network. The role of the metaheuristic algorithm in the proposed method is considered as an artificial neural network classification fault reducer. For this purpose, the metaheuristic algorithm attempts to select the artificial neural network parameters during the training so that the fault rate of its classification is reduced in the identification of fraud.

- **Removing Noise or Outlier Data**

The existence of outlier data transactions has a negative effect on the efficiency of data mining and classification algorithms and increases the fault rate. Thus, in the proposed method, these data are eliminated and adjusted. In this paper, the Kmeans clustering algorithm is used to remove noise data, which has a simple structure suitable for detecting outlier data types. By deleting the data by the clustering mechanism, the data is pre-processed, and each attribute is normalized to limit the scope of each attribute. Normalization increases the quality of learning in the artificial neural network as a classification tool and it is therefore used in the proposed method.

- **Learning improvement with bat algorithm**

In the second step, the proposed method requires the use of an artificial neural network as a classification technique for detecting bank fraud, and the bat algorithm is used to reduce the classification error. In the proposed method, any neural network, which is a set of weights and thresholds, is considered as a member of the population of the bat algorithm to reduce the fault of classification and identify bank fraud. These weights and thresholds are chosen optimally to reduce the classification error and to identify bank fraud more accurately by the global and local search mechanism of the bat algorithm. A conceptual framework of this step in Figure 3 is presented to improve the accuracy of the artificial neural network with bat algorithm:

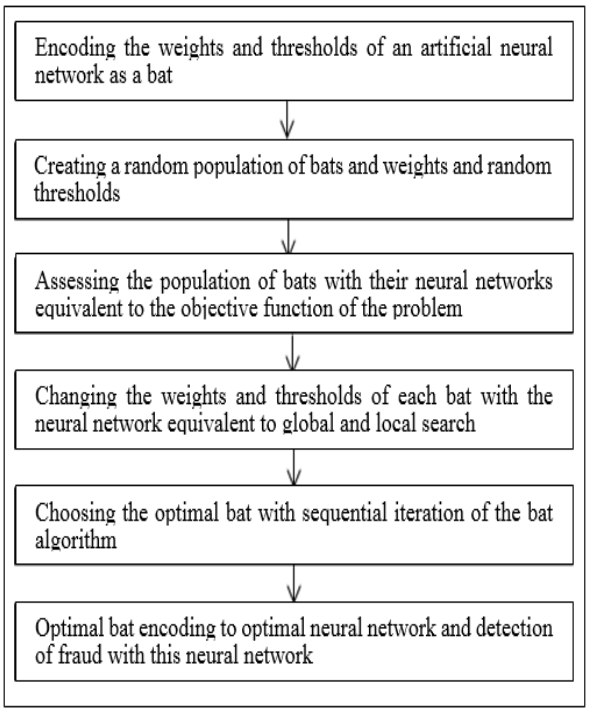

Figure 3: The mechanism for improving the accuracy of the artificial neural network with bat algorithm in detecting bank fraud.

According to the proposed framework, an artificial multi-layer artificial neural network is selected for the classification of banking transactions, and then this artificial neural network consisting of weight and threshold is eventually considered as an array or a bat.

In fact, the multi-layer artificial neural network uses a set of weights and thresholds to classify information that affects inputs and determines the proper output, which is often the class number of a given data. Optimal selection of these weights and thresholds can increase the accuracy of multilayer artificial neural network in classification and reduce the fault rate. The selection of weights and thresholds is normally done by the training process through training data, but these values are not necessarily optimal, and thus the fault rate can be

significant in classification. Each multi-layer artificial neural network has two important indicators and a weight and threshold parameter, which determines the fault rate for artificial neural network classification. In the proposed method, it is necessary that these parameters be selected optimally by the bat algorithm. Therefore, a neural network must be encoded in a suitable format and considered as a bat to apply the bat algorithm on these weights and thresholds and calculate its optimal values. Therefore, in the proposed method, each bat or artificial neural network is assumed to be in the form of Equation 1:

$$\text{Bat(i)} = \{w_1, w_2, \dots, w_m, b_1, b_2, \dots, b_k\} \quad (1)$$

In which, $\{w_1, w_2, \dots, w_m\}$ and $\{b_1, b_2, \dots, b_k\}$ sub-array represent the weights and thresholds of an artificial neural network, respectively. Their outcome is a bat. In the proposed method, a population of bats, such as Equation (2), is considered as artificial neural networks, which attempts to select the best artificial neural network for detection of fraud:

$$\text{Bat} = \{\text{Bat}(1), \text{Bat}(2), \dots, \text{Bat}(n)\} \quad (2)$$

In which, Here, Bat is the population of bats or equivalent artificial neural networks, Bat (i) is the artificial neural network or ith bat and n is the number of bats or primary population.

- **Target function**

In the proposed method, it is necessary to determine the quality of a multi-layer artificial neural network in detecting bank fraud. For this purpose, the average fault of classification according to Equation 3 can be considered as a criterion for the suitability of a neural network or an equivalent bat:

$$e = \frac{1}{n}\left(\sum_{i=1}^{n}(\tilde{o}_i - o_i)^2\right) \quad (3)$$

In the objective function, o_i and $\tilde{o}_i$ are respectively the principal and estimated number of a banking transaction such as the ith transaction. Here, n and e, respectively, are the number of samples used to assess bat suitability and the average error of a bat or artificial neural network equivalent to detecting bank fraud.

- **Optimal Neural Network Selection**

In the proposed method, each of the weights and thresholds used in the bat population in the first step selects a random number in the range [L, U] according to Equation 4 to create a random number of bats:

$$\text{Bat(i)} = L + (U - L).\,\text{rand}(0,1) \quad (4)$$

To create a primary population of bats, each one has a set of weights and random thresholds that can be performed in the global and local search problem. In the proposed method, it is assumed that if the position vector of the bats or $\{w_1, w_2, \dots, w_m, b_1, b_2, \dots, b_k\}$ has m + k member, these bats also have a vector for velocity m + k whose initial value is considered to be zero. To change the weights and thresholds of bats, a general search of the bat algorithm is initially performed, and according to Equation 5, its frequency is determined randomly between two f_{min} and f_{max} ranges. In the following, based on the best optimum multi-layered artificial neural network, the population with the minimum error in the objective function or the function $\frac{1}{n}\left(\sum_{i=1}^{n}(\tilde{o}_i - o_i)^2\right)$ and the current position of the bat as well as the frequency of the bat can be updated by the speed of a bat in accordance with Equation 6. Finally, the bat position can be updated based on the global search through the current position of the bat, or the weights and thresholds used in it, and the new velocity vector, according to Equation 7. In other words, in this case, the weight and threshold of the bat are updated by global search:

$$f_i = f_{min} + (f_{max} - f_{min}).\,\text{rand}(0,1) \quad (5)$$
$$v_i^t = v_i^{t-1} + (\text{Bat(i)} - \text{Bat}^*)f_i \quad (6)$$

$$\text{Bat}(i) = Bat(i) + v_i^t \quad (7)$$

In the bat algorithm, local search can also change these weights and thresholds in addition to a global search that can modify and update the weight and threshold used in a bat. Each bat or multi-layer artificial neural network can use global search to change its weights and thresholds, but local searches are done with a random probability for each bat. In other words, a bat with random probability can perform around the best bat population that is here the optimal multi-layered artificial neural network according to Equation 8:

$$Bat(i) = Bat^* + \varepsilon.rand(0,1) \quad (8)$$

In which, $Bat(i)$ tries to put its weights and thresholds closer to the optimal bat orBat^*. In the above equation, ε is considered a small numerical constant, which acts as a search radius to select the weight and threshold. The population members in the proposed algorithm are constantly updated locally and probably locally to update the weights and thresholds of multi-layer artificial neural networks and to minimize the target function or $\frac{1}{n}(\sum_{i=1}^{n}(\tilde{o}_i - o_i)^2)$. By choosing the optimum bat in the last iteration of the proposed method, it can be seen that the weights and thresholds of this multi-layer artificial neural network are optimal and can be used to detect bank fraud. In the following, the flowchart of the proposed method is presented for detecting bank fraud, which consists of two main stages of clustering and proposed classification, as shown in Figure 4. According to the proposed flowchart, the noise data are initially deleted. Then, learning on a set of neural networks that are optimized by the bat algorithm for their weights and thresholds, so that ultimately the most optimal artificial neural network is used to detect fraud:

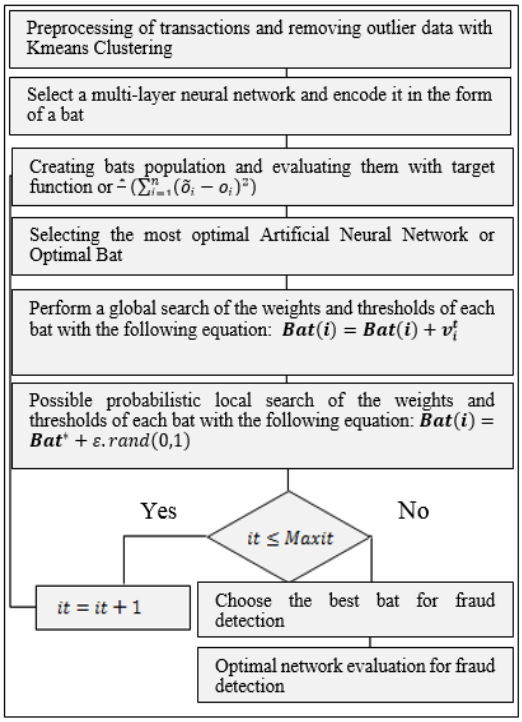

Figure 4: Flowchart of the proposed method

Findings

In this section, we implement the proposed method on a dataset related to bank fraud using the MATLAB software and compare its results with other methods of data mining in a software such as WEKA. In this section, we evaluated the proposed method based on various tests and various indicators such as accuracy, sensitivity,

and precision to analyze its effectiveness in detecting fraud. The bank fraud dataset used in this paper is compiled from the UCI[1] Online Database and has 24 different attributes, 23 of which are inputs, and the last feature shows the type of output that number 1 shows fraud and zero indicates the normalization of the output. This dataset has features such as the amount of individual bank credit in dollars, gender, type of educational degree, marital status, age, payments for the past six months, and the number of statements in the last few months.

To improve the quality of the proposed classification technique, the applied data are required to be pre-processed in normalization type after removing the outlier data. The normalization process here is to determine the maximum and minimum range for each attribute, which is typically selected from zero to one. In other words, the maximum value of an attribute is considered equal to one, and the least value of the attribute is assumed to be zero, and the remainder is normalized as a linear equation in accordance with equation 9:

$$\text{data}' = \frac{\text{data}-\text{min}}{\text{max}-\text{min}}(\text{b}-\text{a})+\text{a} \quad (9)$$

In which, data′, data, min, max, a, and b are the normal values of a given data, the abnormal amount of a data, minimum and maximum of the abnormalized interval of a feature, normalized minimum and maximum of a feature, respectively. The proposed method in this paper is a data mining and classification method to identify bank fraud. Therefore, it is necessary to be evaluated with indicators related to classification such as accuracy, specificity, sensitivity, and precision, each of which are demonstrated in Equation 10, 11, 12, and 13:

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (10)$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN}+\text{FP}} \quad (11)$$

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (12)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (13)$$

To calculate the indicators of classification i.e. accuracy, specificity, sensitivity, and precision the primary indicators such as true positive (TP), false positive (FP), true negative (TN), and false negative (FN) samples must be calculated.

In implementations, the population size of bats or artificial neural networks is variable, the maximum number of bat algorithms is 100, the minimum and maximum frequencies used by a bat are zero and 2 and the sound amplitude generated by a bat is about 0.5. The bounce rate of each bat is about 0.5, the local search coefficient in the bat algorithm is about 0.002, the number of hidden layers of the artificial neural network is equal to 2, the number of neurons of each hidden artificial neural network layer is 4, and the number of experiments is assumed an average of 25. In the implementations performed in this chapter, the data are initially preprocessed and normalized. Then they are classified by improved the artificial neural network through the bat algorithm to identify bank fraud. In order to detect bank fraud, it is necessary to consider a number of training data in which 500 random records as training data and 500 records are considered as test data. In a test, we determine the initial population size of the bat and the number of iterations. Then, we calculate the fault rate through $\frac{1}{\text{n}}(\sum_{\text{i}=1}^{\text{n}}(\tilde{\text{y}}_{\text{i}}-\text{y}_{\text{i}})^2)$ which is the problem function objective. We show the fault rate of bank fraud detection in terms of iteration in MATLAB environment. In Figure 7, an example of the output of the proposed algorithm is shown for population 5 and the number of iterations 20:

[1] https://archive.ics.uci.edu/ml/datasets/default+of+credit+card+clients#

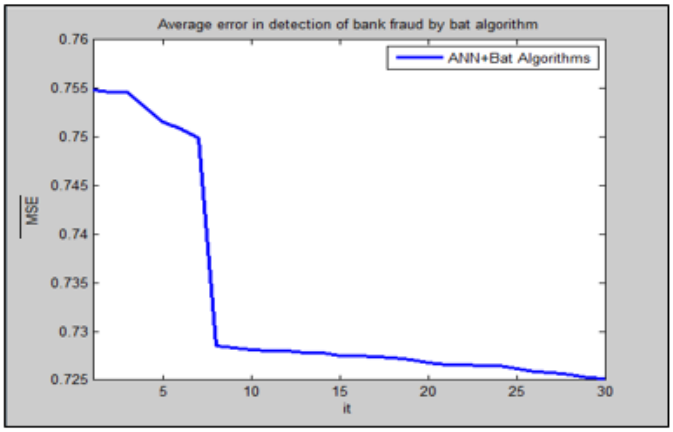

Figure 5: Reducing detection fault through iteration in the proposed method

According to the above diagram, it can be concluded that the fault rate of bank fraud detection in the best artificial neural network in each repetition shows a decreasing trend. The fault reduction in terms of iteration shows that the bat algorithm has successfully managed the weights and thresholds of the artificial neural network so that the classification fault in the detection of bank fraud is reduced. The fault in this test sample is as much as 0.755, but with a continuation of the iteration it eventually reached 0.625. In order to evaluate the proposed method, the average population fault is considered as much as 5, 10, 20, 30, and 40, and the repeat size is assumed as much as 30. Each test has also been run 25 times to determine the average error rate per population, and the error test diagram is based on the population of the proposed method in Figure 6:

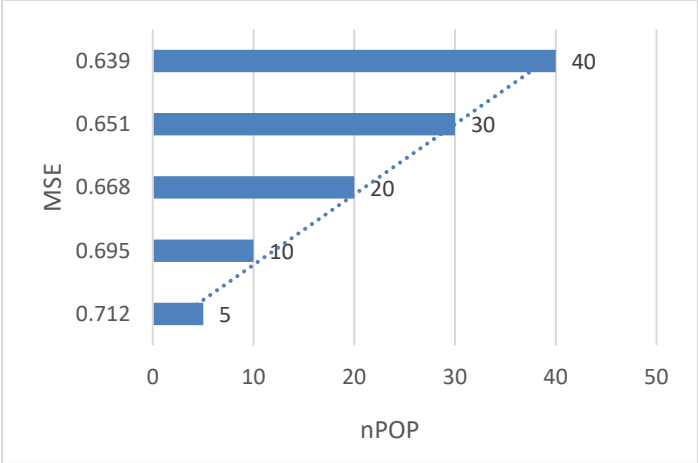

Figure 6: Average reduction of bank fraud detection fault in terms of population size

According to the above figure, it can be concluded that the population increase from 5 to 40 changes the average fault of bank fraud detection from 0.712 to 0.639, which is almost a decrease as much as 10.25%. In order to evaluate the efficiency of the proposed method, the correct positive, false positive, correct negative, and false negative samples are calculated and their mean values are used to measure indicators such as accuracy, specificity, and sensitivity. For this purpose, the population size and the number of iteration are considered as much as 30 and 50, respectively. The test is repeated 30 times, and the average indicators of accuracy, specificity, and sensitivity were calculated and the results of the test indicate that the indicators are as much as 91.46%, 88.97%, and 90.32%, respectively. In table (1), the proposed method has been compared with several machine learning techniques in detecting bank fraud (Gandomi & Yang, 2014):

Table 1: Comparison with other learning methods

Method	detection	Sensitivity	Accuracy
MLFF	82.79	62.24	75.32
SVM	69.68	73.60	72.36
GP	93.16	85.64	89.27
LR	76.46	65.23	70.86
PNN	94.07	87.53	90.77
Proposed	90.32	88.97	91.46

According to Table 1, the average of accuracy, sensitivity, and specificity are as much as 91.46%, 88.97% and 90.32%, respectively. The indicators of accuracy and sensitivity are more accurate than methods such as MLFF, SVM, GP, LR, and PNN. The specificity index is better than MLFF, SVM, and LR methods, and weaker than other methods, such as GP and PNN.

Conclusion

In this paper, a new method was introduced based on clustering and artificial neural network to detect bank fraud along with the technique of metaheuristic algorithms. In the proposed method, the outlier and noise data were removed using clustering from the banking transaction dataset. Then, the classified bank transactions to abnormal transactions were identified with the help of multi-layer artificial neural network techniques. In the proposed classification method, the bat metaheuristic algorithm was used to improve the classification of the artificial neural network to identify bank frauds more accurate. The results of the research and test in this paper illustrate that increasing the population size and the iteration number of bat algorithms can reduce the fault rate of fraud detection, and increasing the population size proportional to increasing the number of iteration has a greater impact on reducing the bank fraud detection fault. Increasing the size of the initial population makes the problem space better searchable, and weights and thresholds have a greater chance of converging to optimal values. On the other hand, increasing the number of iteration can give enough opportunity to weights and thresholds to optimize the selection. The results of the research show that the accuracy, sensitivity, and specificity indicators in the proposed method are as much as 91.46%, 88.97% and 90.32%, respectively and they are more accurate and more sensitive than data mining and learning methods such as MLFF, SVM, GP, LR, and PNN. Only, their specificity was less than GP and PNN.

References

1. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113.
2. Barraclough, P. A., Hossain, M. A., Tahir, M. A., Sexton, G., & Aslam, N. (2013). Intelligent phishing detection and protection scheme for online transactions. Expert Systems with Applications, 40(11), 4697-4706.
3. Choo, K. K. R. (2015). Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks. In Handbook of Digital Currency (pp. 283-307).
4. Gandomi, A. H., & Yang, X. S. (2014). Chaotic bat algorithm. Journal of Computational Science, 5(2), 224-232.
5. Gjoni, M., Gjoni, A., & Kora, H. (2015, November). Money Laundering Effects. In Proceedings of 4th UBT Annual International Conference on Business, Technology and Innovation (p. 13).
6. Moro, S., Cortez, P., & Rita, P. (2015). Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation. Expert Systems with Applications, 42(3), 1314-1324.

7. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.
8. Omar, N., Johari, Z. A., & Arshad, R. (2014). Money laundering–FATF special recommendation VIII: a review of evaluation reports. Procedia-Social and Behavioral Sciences, 145, 211-225.
9. Sanusi, Z. M., Rameli, M. N. F., & Isa, Y. M. (2015). Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss. Procedia Economics and Finance, 28, 107-113.
10. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. Decision Support Systems, 75, 38-48.
11. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & Security, 57, 47-66.
12. Yang, X. S. (2010). A new metaheuristic bat-inspired algorithm. In Nature inspired cooperative strategies for optimization (NICSO 2010) (pp. 65-74). Springer, Berlin, Heidelberg.