Fraud detection in E-banking by using the hybrid feature selection and evolutionary algorithms

Alireza Pouramirarsalani1, Majid Khalilian2, Alireza Nikravanshalmani3

[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, discovering knowledge from the mass set of data is considered by researchers. In this regard, data mining as one of the most efficient tools of data analysis has attracted the attention of many people. The use of different techniques and algorithms of this tool in various fields like customer relationship management, fraud management and detection, medical sciences, sport and etc. proves this claim. It is one of the areas that can be considered as one of the fields of data mining. In today's world, financial and banking systems and services have been developed with the advancement of information technology and communication infrastructure. Banks and financial institutions have invested the field of modern technologies to provide more updated and efficient products and services. Thus, the variety of relevant products and services and also the number and value of transactions have increased. In addition to this development, securing transactions, detection of new ways of fraud and abuse in financial documents, discovery of finished and unfinished frauds, detection and discovery of processes and operations of money laundering and etc. are among the most challenging issues inj this area. The present study provides a new method for fraud detection in e-banking that is based on a hybrid feature selection and genetic algorithm.

Keywords:
fraud detection, e-banking, hybrid feature selection, genetic algorithm

1. Introduction

With the increasing development of people's access to the internet, the use of e-commerce in daily trades has also increased. One of the most important pillars of e-commerce is e-payment systems and fraud in e-payments is one of the big problems. Financial fraud does not only can cause financial damages to the relevant organization, but also causes the loss of credit and damage to customer confidence to the system. Thus, in case of not using the fraud detection mechanisms, we should expect the increase of fraud statistics in e-banking system.

Today, a large volume of financial and monetary transactions are performed on the internet and on the one hand the increasing development of these services and transactions makes the criminals remain unknown on the internet and on the other hand encourages and stimulates the swindlers and fraudsters.

Due to the lack of physical presence of customers in the context of electronic services (e-services), the need to recognize the identity in providing these services is very important and critical from the perspective of financial and monetary institutions. Perhaps it can be claimed that the main limitation in providing more extensive banking services is the need to recognize the identity of individuals. This issue is the most important factor of fraud attractiveness in the context of e-services that is increasing due to the development of e-banking services.

Fraud detection refers to the set of operations or measures based on some methods to discover and detect the frauds that have been performed or are being performed. Financial and monetary institutions are severely looking for the required speed to detect the activities of fraudsters. This issue is of great importance due to its indirect effect on customer service in these institutions, decreased operational costs as a provider of valid and reliable financial services.

The algorithms which are used for fraud detection in banking are mainly performed through the study of customer information like the account number of individuals and finished transactions. In the present study, the abuses conducted by e-banking are studied specifically. In general, the fraud detection methods are divided into the two following main groups:

- Anomaly detection: min this method, the history of customer behavior is considered as a normal behavior and any deviation from this behavior can be recovered as an anomaly or fraud.

- Misuse detection: this method focuses on specific behaviors of customer and assumes some known behaviors as fraud.

Two common techniques of data mining in fraud detection are regression and neural networks. Neural networks method is based on learning. In most cases, the words are

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

done better by neural networks in comparison to traditional statistical methods. Especially when we are dealing with a massive volume of statistical data, the use of neural networks is a technique that has a highly function in fraud detection systems. The idea of this technique is that a neural network , unlike the computers that need specific and explicit commands, does not need pure mathematical models, but like human it has the ability of learning by a number of certain examples.

In the present study, we intend to provide a new approach based on neural network and reinforcement learning method with the aim of fraud detection in e-banking.

This study was developed in 5 chapters. The second chapter reviews the literature in the field of fraud detection. The third chapter introduces the genetic algorithm in general and in the fourth chapter the proposed method is introduced. The fifth and sixth chapters are respectively related to the introduction of research results and conclusion.

2. Review of literature

Reilly and Ghosh in 1994 [3] presented a three layer, feed-forward, radius-limited perception network. This mode was used to detect the algorithm. In this method, the experimental data are read only twice. In the external layer, a numerical value is created as transaction rank. It is lower than the threshold, that transaction will be detected as a fraudulent transaction.

Falcon fraud management system that is a very powerful tool to prevent the activity of fraudsters in the misuse of credit cards uses the algorithms of neural networks. This system predicts the probability of fraud on an account by comparing the current transactions and the previous activities of each holder (Hassibi 2000). [4]

In 2004 [5], a framework was presented on the base of security systems [6] and Case based reasoning [7] for fraud detection. First, a set of normal and fraud cases are made from labeled data. Then, the primary detectors are made with random or genetic algorithms. Then, negative selection and clonal selection operations are applied on primary detectors in order to obtain a set of detectors with different algorithms that can detect a variety of frauds.

The article presented by Bhattacharyya in 2010 is about fraud detection in credit cards of financial institutions and in this article 50 million transactions related to one million credit cards were used. Since the ratio of appropriate transactions to transactions with fraud in this study have been equal to 0/05%, the authors used the following sampling method in order to create a set of data with different ratios from fraudulent records in the dataset (2%, 5%, 10% and 15%). [8]

One of the newest published articles in the field of fraud detection in credit cards is the study of Dal Pozzdo et al [9]. In this study, the authors focused on 3 important issues of data imbalance, inconsistency, and assessment of methods. They considered the transactions of credit cards as data flow, that the fraud detection system must be able to detect the fraudulent transactions immediately.

Sasirekha in his study in 2012 [10] stated that many fraud detection systems that have been presented so far, have used data mining and neural network approaches. While no fraud detection system with the combination of anomaly detection, misuse detection and decision making system have been used so far for fraud detection in credit cards. Then, a system was proposed that used Hidden Markov Model to detect the fraudulent transactions.

Lago in 2008 [17] used 5 methods of classification for fraud detection: ‹Naive Bayes ‹Bayesian Network ‹ Artificial Immune System and Decision Tree. To implement these methods, Weka tool was used except Artificial Immune System method that has a separate program. Each of these methods was evaluated in two modes of sensitive to cost and simple. It means that in the first mode, the cost related to normal cases that are detected as fraudulent by mistake differ from the costs related to fraudulent cases that are detected as normal by mistake. Also, the parametric methods were evaluated once by Weka parameters and another time by optimized parameters. The results of comparing these two modes show that in any of these methods, Weka parameters were not optimum. To optimize the parameters, hybrid feature selection and genetic algorithm were used.

Akhilomen in 2013 [18] presented a mode by using hybrid feature selection and anomaly detection algorithm in order to detect fraud in credit cards. In this study, the people who perform fraudulent activities in the field of credit cards were classified in 3 groups of 1. The buyers of credit cards information. 2. Black hat hackers. And 3. The Thieve of credit cards. The authors have noted that fraud detection on the internet must be done online and immediately. Since the use of credit card by card holders follows a fixed pattern, this fixed pattern can be extracted from a usual legal activity of card holders in 1 or 2 years .thus, this pattern is compared to the use of process of card holder and in case of non-similarity in the pattern, the activity is considered illegal. It should be noted that the neural networks were used to teach the patterns detection in the model in this study.

3. Genetic algorithm

Since 1960, the imitation of living creatures to use in powerful algorithms was considered for optimization problems and was called evolutionary computation techniques. In fact, the genetic algorithm [11] is a programming technique that uses the genetic evolution as a problem solving algorithm. Figure 1 shows a processing flowchart for the genetic algorithm.

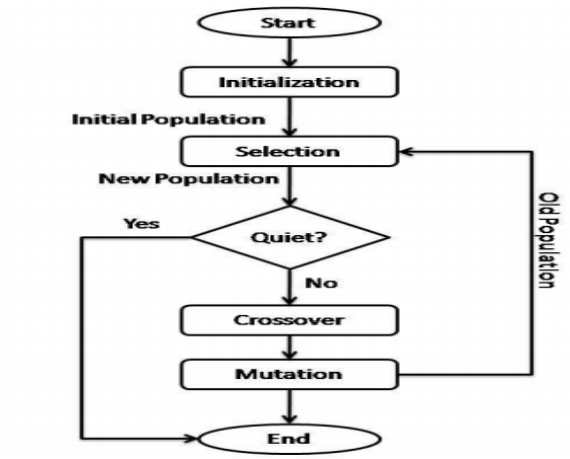


Figure 1

The processing steps in this method are as follows:

1. First, a primary random population is generated. Each of the members of this population is generated. Each of the members of this population contains a solution for problem solving.
2. At this step, the solutions are evaluated. the evaluation of solutions are performed by the target function. The target function allocates some values to solutions according to the study challenges that can be efficiency, security, and other factors in the system. These values show the extent the solutions are close to the intended target.
3. Crossover operation
4. Mutation operation

Crossover and mutation operations are performed to prevent the premature convergence and creation of divergence in solutions. The appropriate selection of the number of times that these two operations are performed in the set of elements evaluation cycles is one of the effective factors in the efficiency of algorithm.

Different implementations of genetic algorithm have been proposed to solve this problem. Genetic processing and making it multi –purpose are among these implementations.

4. whale algorithm

One of the largest whales is Megaptera novaeangliae. It is an adult humpback whale that is as big as a school bus. Its favorite baits are the shoal of small fish. The most interesting thing about the humpback whale is the way it hunts. This process of finding food is called bubble network nutrition. In fact, the whale prefers to hunt the shoal of small fish that are closer to the water surface. It was observed that this nutrition method is done by creating circle bubbles. The whale dives down about 12 meters and swims to the surface by creating spiral bubbles around the bait. The scientists have specified two maneuvers related to bubbled network and called them upward spiral and double loops. This nutrition method is a specific method that was only seen in whales. In the whale algorithm, the spiral maneuver of bubble network was modeled mathematically to perform the model optimization.

This algorithm includes two main parts that was modeled mathematically.

- Spiral bubble network
- Search for the bait

The whale can detect the place of fish and its circle of life since the best place of the bait is not certain from the beginning, the algorithm assumes that the best solution of the current candid is the target bait or close to optimum. When the best search factor was defined, the other search factor attempted to update its situation according to the best search factor. This behavior was shown by the following equations:

$$\vec{D} = \left|\vec{C}.\vec{X}^{*}(t) - \vec{X}(t)\right|$$

$$\vec{X}(t+1) = \vec{X}^{*}(t) - \vec{A}.\vec{D}$$

In the above formula, t is the current iteration, $\vec{A}$ and $\vec{C}$ are coefficients vector, $\vec{X}^{*}$ is the place vector of the best solution, $\vec{X}$ is the vector of place (location), $|\ |$ is absolute value and .is dot product of element in element.

If there was a better solution at each iteration, X* would be updated.

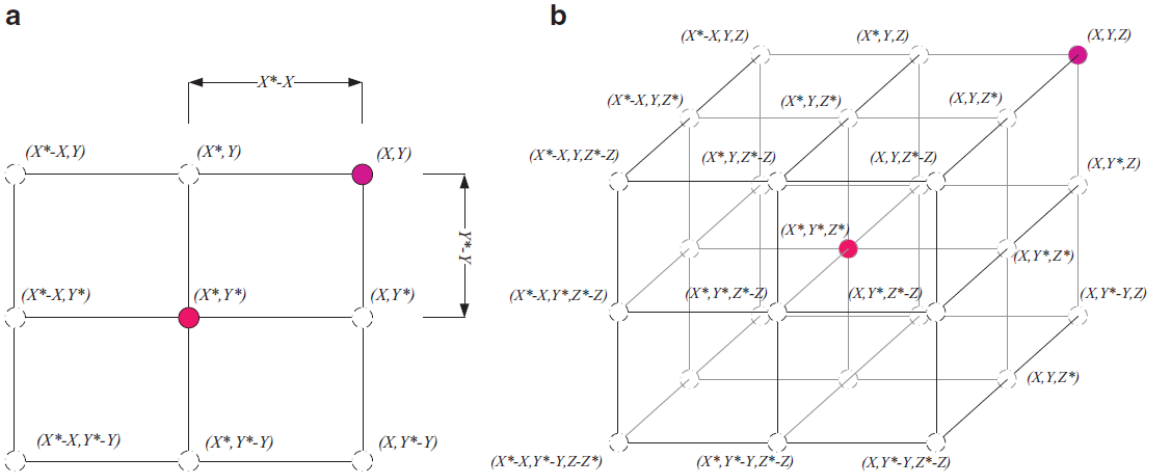
$\vec{A}$ and $\vec{C}$ vectors are calculated as follows:

$$\vec{A} = 2\vec{a}.\vec{r} - \vec{a}$$

$$\vec{C} = 2.\vec{r}$$

Where $\vec{a}$ in each iteration reduces linearly from 2 to 0 (both in search phase and extraction phase) and $\vec{r}$ is a random vector between [0 and 1].

The following figure shows the logic in the formula.



The situation (X,Y) obtained from the search factor can be updated according to the best situation (X*,Y*). The different places of the best factor are obtained according to the current situation by adjusting the values of $\vec{A}$ and $\vec{C}$ vectors.

To formulize the behavior of bubble network, two approaches were designed as follows:

- The mechanism of minimizing the blockade: the behavior is obtained by reducing the value of $\vec{a}$ in the following formula:

  $$\vec{A} = 2\vec{a}.\vec{r} - \vec{a}$$

  $$\vec{C} = 2.\vec{r}$$

- The spiral update of the situation: the spiral situation between the situation of whale and bait to imitate the spiral movement of the whale is as follows:

  $$\vec{X}(t+1) = \vec{D}'.e^{bl}.\cos(2\pi l) + \vec{X}^*(t)$$

The following figure states the pseudo code of whale algorithm.

```
Initialize the whales population Xi (i = 1, 2, ..., n)
Calculate the fitness of each search agent
X*=the best search agent
while (t < maximum number of iterations)
    for each search agent
    Update a, A, C, l, and p
        if1 (p<0.5)
            if2 (|A| < 1)
                Update the position of the current search agent
            else if2 (|A| ≥ 1)
                Select a random search agent (Xrand)
                Update the position of the current search agent
            end if2
        else if1 (p≥0.5)
                Update the position of the current search
        end if1
    end for
    Check if any search agent goes beyond the search space and amend it
    Calculate the fitness of each search agent
    Update X* if there is a better solution
    t=t+1
end while
return X*
```

5. The proposed method

In this section of the study, the new solution is introduced. The proposed solution was developed by using the reinforcement learning in the neural network. Artificial neural network is a practical method for learning different functions like functions with real values, functions with discrete values and functions with vector values. A neuron alone can be used only for the detection of functions that are linearly separated. Since the functions are not linearly separable in real problems, a network of neurons is needed. A variety of neural networks is used for solving different learning problems with monitoring, learning without monitoring and reinforcement learning. Neural networks are divided into two groups of FNN (feed-forward neural networks) [12] and RNN (recurrent networks) [13] based

on a variety of connections. FNN(s) are the most regular types of neural networks that are used in different functions. The first layer is called the input layer and the last layer is called the output layer and each number of layer among these two layers is called middle or hidden layer, because we are only involved with the inputs and outputs of the neural network. Neural network works as a black box and direct access to middle layers is not possible. Recurrent neural networks have oriented cycles in their graphs structure. in other words, we can return to previous and early nodes by tracking the connections between nodes. RNN(s) have a complex dynamic according to their structure and makes it difficult to teach these networks. Also, FNN networks are biologically closer to reality.

FNN networks with more than one hidden layer are called MLP (multi layer perception) and FNN network with one hidden layer are called SLP in which the output of neurons in each layer is a nonlinear function of outputs in previous layer. The number of neurons in the input and output layer is constant and the number of neurons in the input layer is equal to the space of features and the number of neurons in the output layer is specified according to the number of classes. In MLP, the nodes (neurons) are usually ordered in some layers of neural network. Each node only receives the inputs from the previous layer and provides a function of inputs.

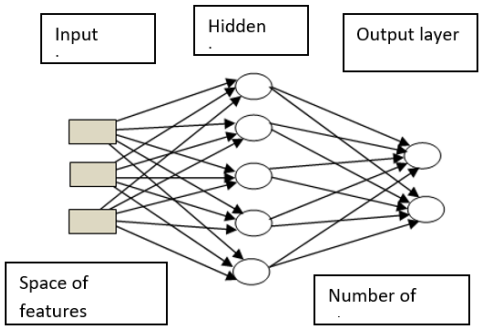


Figure 2

There are two methods to teach (determination of weights and biases) the FNN neural network: classical methods like hybrid feature selection and back propagation algorithm (BP) and intelligent optimization methods like hybrid feature selection and genetic algorithm and hybrid feature selection and PSO (particle swarm intelligence). [14]

BP method is based on descending gradient in the error space that has local search ability. The correction of neural network weights occurs in such a way that the optimums output and neural network output reduces at every round of error. This error is defined as follows:

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

So that the error is calculated for n training samples, t is the optimum output and y is the output of neural network. The power of feature selection and BP algorithm in the ability of calculating the effective error for each unit is hidden. Finally, each weight in m+1 round changes as follows:

$$w(m+1) = w(m) + \Delta w$$

$$\Delta w = \eta \delta x$$

In the above equation, η is learning rate and δ is the difference between the optimum output and neural network output. The general structure of feature selection algorithms was stated 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 algorithm output of data samples has X features. The number of these features is equal to n and J that is the evaluation criterion of the algorithm and the objective of the algorithm is the maximization of this criterion and GS

is the operator of selecting the next feature at each stage of the algorithm. [15]

Genetic algorithm is used in search problems and optimization. First, a primary generation is created (randomly) that is in fact primary chromosomes. Each of these chromosomes is a solution to the problem but is not the main solution we are looking for. Then, the mutation phenomenon may occur with a very low probability. Finally, the chromosomes are ranked in terms of score. This scoring is usually based on the value of objective function. Some chromosomes are combined together and create the next generation. The probability of selecting chromosomes with higher score is higher, but there is the probability of being selected for all chromosomes even the chromosomes with the lowest score. We repeat these stages with the new generation in order to achieve the absolute solution.

Single point crossover operator is applied on two chromosomes and creates two infants by combining two chromosomes structure. The important concept that is raised in relation to this operator is crossover rate (p_c). If the number of created chromosome is shown with x and the number of primary population with $\mathrm{pop}-\mathrm{size}$, we will have:

$$p_c = \frac{x}{\mathrm{pop}-\mathrm{size}}$$

The bigger crossover rate allows the more extensive part of solution to be searched.

Among the variety of crossover operators, we only study the single point crossover. In single point crossover, a point was considered randomly as cutting point along the chromosome that was selected as parents, and chromosomes were divided into two parts and then the place of two parts of them are changed. Consider the two following parent chromosomes, these two chromosomes had a crossover at the fifth situation and the results of this crossover are two new chromosomes called infant.

parents	infants
01100110	10110110
10110010	01100010

Mutation operator has created unplanned random changes in different chromosomes and inserts the genes that were absent in the primary population in o the population. An important concept has been raised about this operator that is called mutation rank pm.

Mutation rate refers to the percent of the total genes that are changed. If the mutation rate is too small, a large number of the genes that could be useful will not be tested, but if the mutation rate is too big, the infants will lose their similarities with the parents. It leads to the devastation of the historical memory of the algorithm. There are different mutation operators and we only study its uniform type. In this operator, a gene related to the chromosome was selected randomly and its value is converted into another random value. First a random number in the range [1L] that is the length of the intended chromosome and the current gene in that place of chromosome changes. Assume that the parent chromosome is as follows:

parents	010010110

As can be seen, the length of chromosome is 10. Assume that the generated random is equal to 5 in the range [1.10], thus the current gene is changed in place 5, namely 1 is converted to 0.

infant	010000110

To select the best solution to regenerate the generation (generation of new population), a method must be used that can select the best solutions. Among the different methods, we study Roulette wheel that was proposed by Holland.

Random selection by Roulette wheel: the main idea of this method is to determine the probability of survival for each chromosome according to its fitness value. Roulette wheel is used to show these probabilities and process of selection is based on simultaneous rotation of wheel numbers as much as the size of population.

Calculate the competence values or V_k related to each chromosome. If f is the objective function:

$$\mathrm{eval}(V_k) = f(m), k = 1,2,\dots,\mathrm{pop}-\mathrm{size}$$

Calculate the total values of competence for all available chromosomes:

$$F = \sum_{K=1}^{POP-SIZE} \mathrm{eval}(V_k)$$

Calculate the relative probability P_k related to each chromosome:

$$P_k = \frac{eval(V_k)}{F} \quad k = 1,2,\dots,pop - size$$

Calculate the cumulative probability q_k related to each chromosome:

$$q_k = \sum_{j=1}^{k} P_j$$

The procedure of selecting the rotation of Roulette wheel has began for pop-size times and each time one chromosome is selected as follows to attend the new generation:

Step 1: generate a random number like r in the range [0,1]

Step 2: if $r < q_1$, then chromosome V_1 , that is the first chromosome will be selected, other wise the k-th chromosome in which $2 \le k \le pop - size$ and $q_{k-1} \le r \le q_k$ will be selected. [16]

The general structure of the genetic algorithm was shown in figure 3.

```
Procedure: Genetic Algorithm
initializing population(Composition Services)
While (not termination cordination) do:
    Computing fitness values of all Composition Services
    Using crossover operation to build a new composition service
    Mutation operation
    Selecting Composition Services based on fitness values
    Building new population
End.
```

Figure 3

6. Simulation results

In this study, 80 % data were selected as training data and the rest were selected as test data. Data were selected randomly.

The software used in this study is MATLAB version 2015.

In the performed studies in the field of error prediction in software, the classification models based on software matrices predict a software module as error-prone or not error-prone.

Double classification methods are used to predict the classes that have probable an error. In fact, this mode can be used on time to guide the effort for the improvement of the quality of modules that are likely detected as error prone during the operation. Thus, the quality can be tested in a cost effective way and the resources can be improved. One of the things that can be done to study the accuracy of hybrid selection feature and information classification algorithms is the use of confusion matrix:

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

In which TP is the number of modules with error that were appropriately predicted as error prone, FP is the number of modules without error that were predicted as error prone by mistake, TN is the number of modules without error that were appropriately predicted as not error prone and finally Fn is the number of modules with error that were predicted as not error prone by mistake.

The quality assessment criteria of error prediction models in the software include the following items:

Misclassification rate

Except cost of Misclassification

Normalized Except cost of Misclassification

sensivity

specificity

Accuracy

Precision

Recall

F-measure

Consistency

Receiver oprating charecteristic

Balance measure

To implement the research proposed solution, the readymade function of MATLAB were used that work on the basis of fcm clustering. The obtained results are as follows: the following figure shows the confusion for the proposed system.

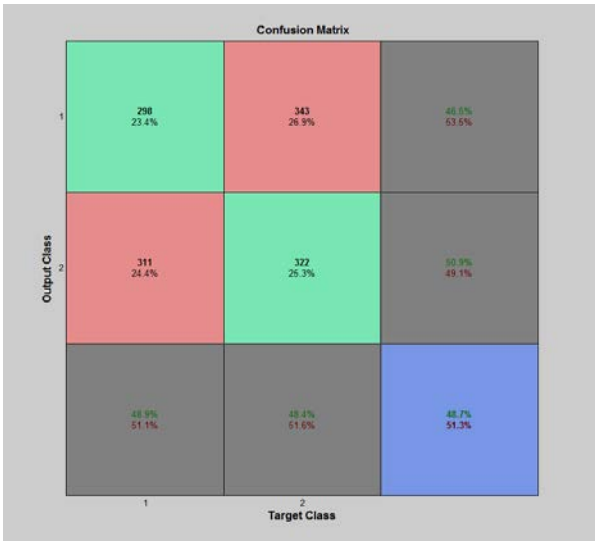


Figure 4

For hybrid feature selection and genetic algorithm, the number of chromosomes was considered as 10, the number of iteration as 100 and crossover and mutation rate were considered as 0/9 and 0/1. The results of this hybrid feature selection and algorithm are as follows. Figure 5 shows convergence to the intended solution in different generations in hybrid feature selection and genetic algorithm.

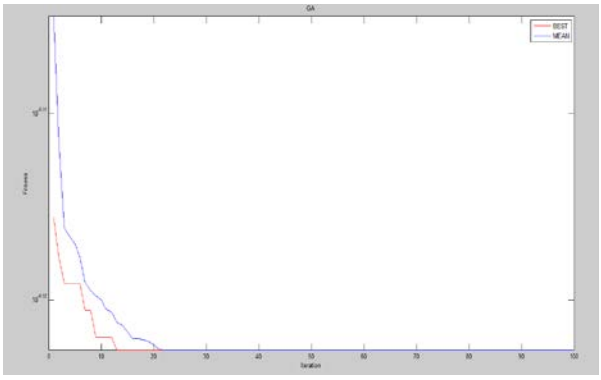
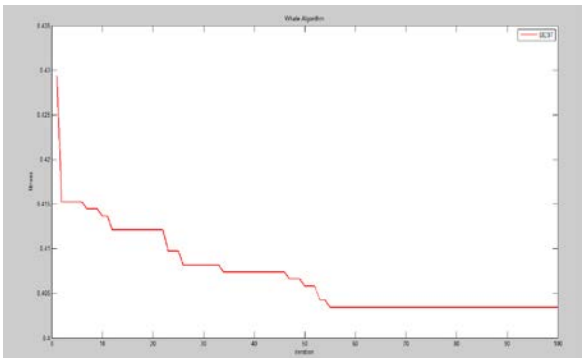


Figure 5

The proposed solution was compared to whale algorithm [19]. In this algorithm, the process of finding bait with the help of bubbles by whales was used. In the whale algorithm, the spiral maneuver of bubble network was modeled mathematically to perform the model optimization. The output of hybrid feature selection and whale algorithm was shown in the following figure.



7. Conclusion

one of the methods that has been considered by many researchers to detect fraud in banks and financial institutions is data mining. Data mining that is an intergroup process can detect the hidden knowledge and information in a mass volume of data and use them to solve different problems. Some technologies like statistics, artificial intelligence, database and etc. form the theoretical foundations of data mining. Due to the large number of data in banks, data mining has had lots of functions in financial and monetary affairs so far. Credit risk management, fraud detection, money laundering , customer relationship management and banking services quality management are some examples of data mining function in banks. In this study, a new method was proposed for fraud detection in e-banking by using the hybrid feature selection and genetic algorithm.

According to the obtained results, it can be said that the proposed system is very efficient for fraud detection in e-banking.

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] Vose, M. D. (1999). The simple genetic algorithm: foundations and theory(Vol. 12). MIT press.
[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
[16] Holland, J. H. (1992). Adaptation In Natural And Artificial Systems: An Introductory Analysis With Applications To Biology, Control, And Artific
[17] Gadi, Wang, Lago; Comparison with Parametric Optimization in Credit Card Fraud Detection; IEEE; 2008
[18] Akhilomen. John, 2013, "Data Mining Application for Cyber Credit-Card Fraud Detection System", Springer-Verlag Berlin Heidelberg, pp. 218–228
[19] Mirjalili, S., & Lewis, A. (2016). The Whale Optimization Algorithm.Advances in Engineering Software, 95, 51-67.