Asian Journal of Information Technology 15 (11): 1856-1864, 2016
ISSN: 1682-3915

Optimization of Fuzzy Rules for Online Fraud Detection with the Use of Developed Genetic Algorithm and Fuzzy Operators

Mohammad Reza Parsaei, Reza Javidan and Mohammad Javad Sobouti
Department of Computer Engineering and IT, Shiraz University of Technology, Shiraz, Iran

Abstract: The huge numbers of users participating in online auctions and the low cost of creating accounts for such activities have increased the danger of fraud and other criminal endeavors in these environments and have pushed the monetary and financial institutions to seek efficient and quick solutions to detect such offenses. This issue has necessitated the use of fraud detection techniques to prevent fraudulent endeavors in banking and especially electronic banking systems. The objective of the present study was to propose a hybrid approach to detect the fraudulent accounts. This objective was pursued by analyzing the social networks to produce behavioral characteristics and then turning these characteristics into fuzzy rules. The fuzzy rules proposed by the genetic algorithm were then optimized for auction fraud detection model. The introduction of fuzzy crossover and mutation operators specifically modified for this objective was the other contribution of this research to the literature. The results obtained by the implementation of the proposed system showed that using these fuzzy crossover and mutation operators improved the algorithm performance and the speed by which algorithm obtained the optimal solution.

Key words: Online auction, fraud detection, fuzzy rule, social network analysis, genetic algorithm

INTRODUCTION

Fraud is a global multi-million dollar criminal business whose methods and procedures have always kept pace with modern technology.

These new technologies have enabled criminals to commit a new type of scam called online fraud which can inflict significant direct and indirect financial damages on individuals and institutions. Hence, the aim of this paper is to provide a method for online fraud detection. This objective is pursued by providing a new heuristic approach that uses the developed genetic algorithm along with fuzzy operators. The proposed approach uses a proper combination of fuzzy crossover and mutation operators to reduce the time required for reaching the optimal result.

Detecting fraud in financial statements is a complicated and difficult task (Yue *et al*., 2007) and there is no universally accepted definition for financial fraud (Ngai *et al*., 2011). Wang *et al*. (2006) have defined fraud as "any endeavor to gain illegal financial profit by violating the laws, rules or policies". The concept of fraud is as old as human history and is considered a global and lucrative business. The volume of illicit financial profits and transactions made by this business is growing by the day. In recent years, the development of new technologies has opened many new avenues for fraudsters and criminals to be able to commit their business. The creation of new information systems in addition to all their benefits has provided more opportunities for criminals to commit frauds. Such frauds may inflict irreparable losses on investors and eliminate their competition power (Albrecht *et al*., 2008).

The results of a study conducted by KPMG in 2003 indicate the increasing rate of fraud. This study has found that 75% of studied organizations have experienced some instances of fraud. These statistics shows a 13% growth as compared to 1998.

Intelligent fraud detection techniques can identify and analyze any frauds and scams in an organization by also can identify the behavior of users or customers and try to predict their future behavior and reduce the risk of fraud.

Research background: The researchers' findings show that data mining methods have also been successfully employed to detect fraud in the insurance industry and recent years have seen an increasing growth in the use of such algorithms to detect financial and credit abuse.

In 1994, Gosh and Rally proposed a method based on artificial neural networks to detect fraud on credit cards (Phua *et al*., 2004). Game theory has also been employed

Corresponding Author: Mohammad Reza Parsaei, Department of Computer Engineering and IT, Shiraz University of Technology, Shiraz, Iran

for the process of fraud detection. This method models the interaction between the attacker and the fraud detection system as a multi-stage game between two players who each try to maximize the profit from the game. Data mining methods provide another approach to fraud detection. A full review of the research conducted between 1997 and 2008 on using data mining methods to detect financial frauds is provided by Yeh and Lien (2009).

In Aziz *et al*. (2012), a genetic algorithm has been used for intrusion detection. In this study, genetic algorithm has been used to create several detectors and Minkowski distance function has been used instead of Euclidean function. The results of this study indicate that using the Minkowski standard improves the performance of genetic algorithm.

Recently, different techniques have been combined to achieve better results including research done by Anil and Remya (2013) where authors have provided a hybrid method using genetic algorithm and Support Vector Machine (SVM) to detect anomalies in datasets. This method uses genetic algorithm to select the best subset of features that are indicative of anomalies. This optimized data set has been used to train support vector machine. The final results of this study have shown that combination of these techniques has improved the results.

In Duman and Ozcelik (2011), a combination of genetic algorithm and scatter search algorithm has been used to overcome the problem of fraud in financial institutions.

Integration of fuzzy inference system with artificial intelligence methods is a new approach that has been used to solve some problems. Research carried out by Nagi *et al*. (2011) has proposed a method to detect fraud in power network. In this study, authors have used fuzzy inference system and SVM to present a new method for dealing with fraud.

Test data collection: Data collected from a real auction website is used to test the system. This website which has no branch is one of the most popular online auction website in Taiwan. Auction websites in Taiwan provide a black list of accounts to help users identify fraudsters. This black list which includes account ID, type of offense, date of related bids and date of the offense are regularly announced by the auction websites. Unfortunately, most auction websites reports do not provide any detail about the behavior of the offender. This research aims to use the specifications provided in the black list of accounts to propose a fuzzy inference system that would be able to detect fraudulent accounts based on recorded data.

Detection features: According to the studies on social networks and observations on actual bidding information, k-core feature can be considered as one of the best features to match the behavior of the fraudulent group. The density of any transaction network can be realized through k-core. High k-core can show high density of the transaction network. This feature can show collusive behaviors (e.g., two bidders giving false scores or bids to each other) and be used to detect this type of fraud. Wang *et al*. (2006) have used k-core feature to detect abnormally high density in transaction networks (Wang *et al*., 2006; Wang and Chiu, 2008). Results of their research indicate that using k-core feature alone will lead to a high number of false-positives. So, it must be combined with other effective features to gain more accurate results.

A feature called the seller density is another approach to fraud detection which extracts the fame of participants in online auctions. Seller density is explained below.

In this method, two sellers, S_i and S_j are called linked, if there exist a specified number of buyers (min_buyers) who have finalized an auction with both sellers and the final price of each auction have been at least MIN_VALUE.

The number N_{ij} of such buyers is called the link strength and is shown with link (s_i, s_j). Neighborhood of seller S_i is shown with N (S_i) and is introduced as a set of sellers {S_j} that are associated with S_i with respect to the user-defined thresholds of min_buyers and MIN_VALUE. Min_buyers threshold is used to detect sellers with significant sales volume. MIN_VALUE threshold is used for protection against the fraudsters trying to impersonate reputable sellers by the use of "accumulation" fraud. Another measure, called score (indicating the density of sellers) is also defined as follows (Morzy, 2008):

$$score(s_i) = \sum_{s_j \in N(s_i)} density(s_i).\log_{min\_buyers} \left| link(s_i, s)j) \right| \quad (1)$$

Popular analytical perspective of "crime economics" is appropriate to be applied to this detection system. This perspective believed that the primary motives for the crime include three factors of costs, benefits and risks (Yeh and Lien, 2009). Criminal tends to achieve the biggest gains under the lowest cost and lowest risk. According to this view, the auction fraudsters tend to take the approach with the lowest cost, i.e., creating a number of accounts and using them to give false scores and bids to their own accounts. They also tend to fulfill the fraud in a short period of time to reduce the risks of getting caught. So, this type of accounts will have a low positive rating score (the lowest cost to build some fake

accounts), short bidding period (the lowest risk) and a rapid increase in negative rating score (the larger gains leads to larger number of complaints and negative ratings). According to the discussion, a feature called Negative-Positive Ratio (N/P Ratio) is introduced to detect these types of features:

$$\text{NP Ratio} = \frac{\text{Negative\_Rating\_Score}}{\text{Positive\_Rating\_Score}} \quad (2)$$

The observation of actual auction data shows that the positive rating scores of fraudulent accounts are often around 10 and their negative rating scores are often >3. The N/P Ratio is <0.3 for a normal auction seller. The results show that the N/P Ratio can help detect fraudulent accounts.

In addition to the above three features in this study, the main reputation scores of the auction website are used to help detect fraudulent accounts. In summary this study uses a combination of social network analysis, crime economics perspective and the reputation system of the auction website to detect the characteristics of fraud. Detection feature of this study includes four factors of k-core, score (density of sellers), N/P Ratio and reputation score (total minus rating score).

MATERIALS AND METHODS

Figure 1 shows the flowchart of the proposed detection system. The proposed detection system is a fuzzy inference system whose rules have been optimized by using a genetic algorithm. The proposed genetic algorithm is implemented to solve the problem of optimizing the fuzzy system detection rules. The flowchart presented in Fig. 2 shows how the proposed genetic algorithm works. Each part of the presented flowchart will be explained in the following.

The proposed fuzzy inference system: Figure 2 shows an overview of Fuzzy Inference System. Input and output variables are described in Table 1.

Membership functions selected for all variables are triangular and trapezoidal. The reason for this choice is the simplicity and ease of processing this type of membership functions. Inputs include density (k-core and score), N/P Ratio and negative rating score. Density is divided into two levels and negative/positive ratio and negative rating score are divided into five levels. Figure 3-6 represent the membership functions of inputs and outputs of the proposed fuzzy control system. Shows a number of rules devised for the rule base. To get the correct results from the proposed control mechanism, the scheme has been simulated and tested with the existing data to calculate each rule's level of significance.

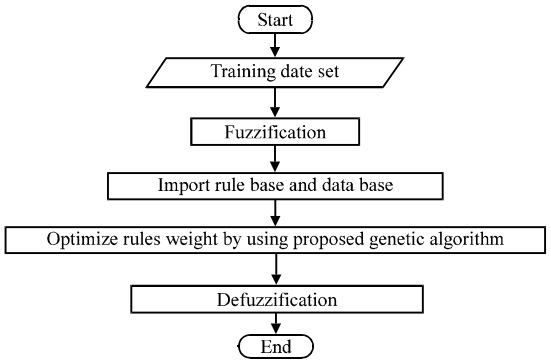

Fig. 1: Flowchart of the proposed detection system

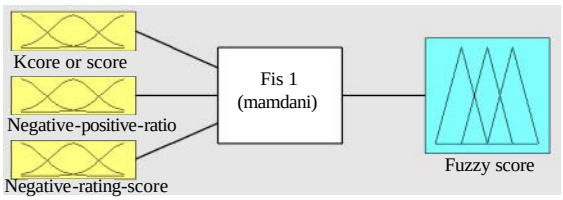

Fig. 2: The general model of the proposed fuzzy inference system

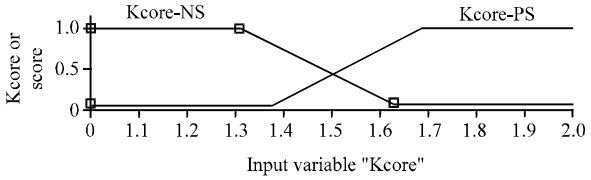

Fig. 3: Fuzzy input variable: Kcore or score

Table 1: Input and output variables

Variable type	Variable name	No. of membership functions	Fuzzy values of membership functions
Input	Kcore	2	NS, PS
Input	Score	2	NS, PS
Input	Negative-positive-ratio	5	NB, NS, ZO, PS, PB
Input	Negative-rating-score	5	NB, NS, ZO, PS, PB
Output	Fuzzyoutput	9	N3, N2, N1, N, O, P, P1, P2, P3

Fuzzy rules:

- If (Kcore is NS) and (Negative-Positive-Ratio is NS) and (negative-rating-score is NB) then (Fuzzy_Score is N2)
- If (Kcore is NS) and (Negative-Positive-Ratio is ZO) and (negative-rating-score is NB) then (Fuzzy_Score is N1)
- If (Kcore is NS) and (Negative-Positive-Ratio is PS) and (negative-rating-score is NB) then (Fuzzy_Score is N)
- If (Kcore is NS) and (Negative-Positive-Ratio is PB) and (negative-rating-score is NB) then (Fuzzy_Score is O)

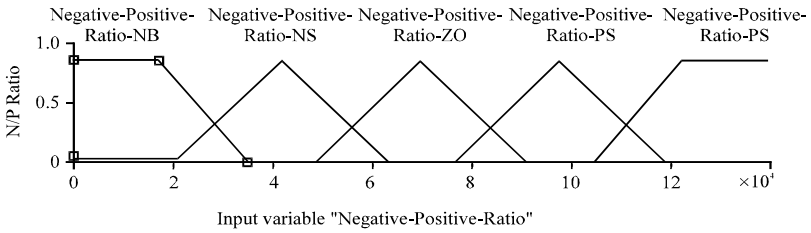

Fig. 4: Fuzzy input variable: N/P Ratio

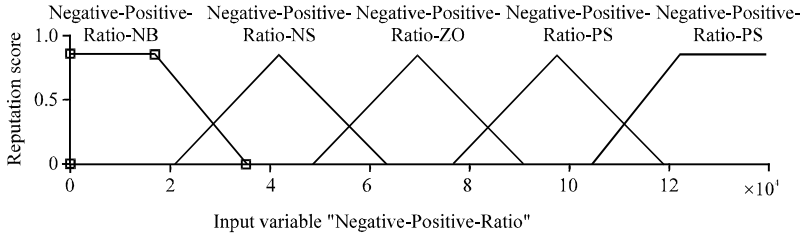

Fig. 5: Fuzzy input variables: reputation score (total negative rating score)

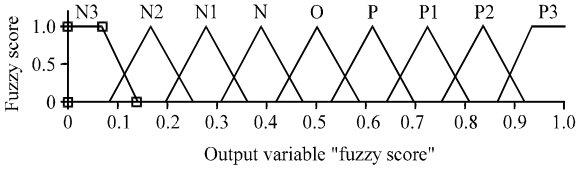

Fig. 6: Fuzzy output variable

- If (Kcore is NS) and (Negative-Positive-Ratio is NB) and (negative-rating-score is NS) then (Fuzzy_Score is N2)
- If (Kcore is NS) and (Negative-Positive-Ratio is NS) and (negative-rating-score is NS) then (Fuzzy_Score is N2)
- If (Kcore is NS) and (Negative-Positive-Ratio is ZO) and (negative-rating-score is NS) then (Fuzzy_Score is N1)
- If (Kcore is NS) and (Negative-Positive-Ratio is PS) and (negative-rating-score is NS) then (Fuzzy_Score is N)
- If (Kcore is NS) and (Negative-Positive-Ratio is PB) and (negative-rating-score is NS) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is NB) and (negative-rating-score is ZO) then (Fuzzy_Score is N1)
- If (Kcore is NS) and (Negative-Positive-Ratio is NS) and (negative-rating-score is ZO) then (Fuzzy_Score is N1)
- If (Kcore is NS) and (Negative-Positive-Ratio is ZO) and (negative-rating-score is ZO) then (Fuzzy_Score is N)
- If (Kcore is NS) and (Negative-Positive-Ratio is PS) and (negative-rating-score is ZO) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is PB) and (negative-rating-score is ZO) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is NB) and (negative-rating-score is PS) then (Fuzzy_Score is N)
- If (Kcore is NS) and (Negative-Positive-Ratio is NS) and (negative-rating-score is PS) then (Fuzzy_Score is N)
- If (Kcore is NS) and (Negative-Positive-Ratio is ZO) and (negative-rating-score is PS) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is PS) and (negative-rating-score is PS) then (Fuzzy_Score is P)
- If (Kcore is NS) and (Negative-Positive-Ratio is PB) and (negative-rating-score is PS) then (Fuzzy_Score is P)
- If (Kcore is NS) and (Negative-Positive-Ratio is NB) and (negative-rating-score is PS) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is NS) and (negative-rating-score is PS) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is ZO) and (negative-rating-score is PS) then (Fuzzy_Score is O)
- If (Kcore is NS) and (Negative-Positive-Ratio is PS) and (negative-rating-score is PS) then (Fuzzy_Score is P)

- If (Kcore is NS) and (Negative-Positive-Ratio is PB) and (negative-rating-score is PS) then (Fuzzy_Score is P1)

The proposed genetic algorithm: The flowchart presented in Fig. 7 shows the genetic algorithm proposed to optimize the weights of fuzzy inference system. Different steps of the algorithm are presented in the following.

Gene encoding: Genes of each chromosome are encoded as a table of fuzzy control rules (G0-G49). Each cell represents the weight of a fuzzy rule. In Table 2, G0 represents the output, when the negative rating score is NB, N/P Ratio is NB and density (Kcore or Score) is NS.

Fitness function evaluation: Objective function is designed to determine the genes that can effectively detect fraudulent accounts. The desired gene can also be used to compare detection features. More important feature receives a higher threshold and the lower threshold indicates lower significance. Fitness function equation is as follows:

$$E_i = Fuzzy\_Score \tag{3}$$

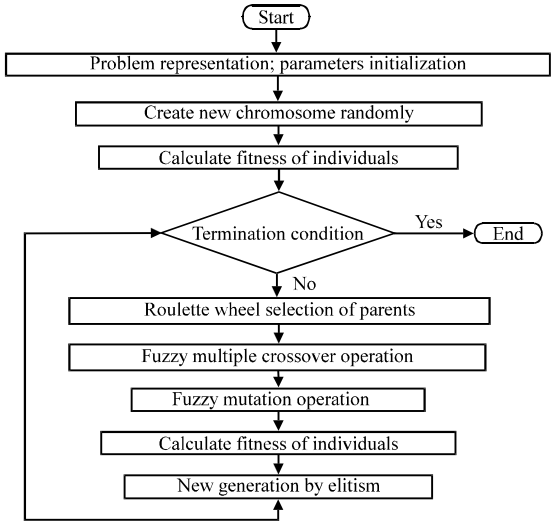

Fig. 7: The proposed genetic algorithm

$$Threshold = \frac{Normal\_Max\_Fuzzy\_Score + Fraud\_Min\_Fuzzy\_Score}{2} \tag{4}$$

$$Recall = \frac{Count(Fraud\_E_i > hreshold)}{Count(Fraud\_Account)} \tag{5}$$

$$Precision = \frac{Count(Fraud\_E_i > Threshold)}{Count(Fraud\_E_i > Threshold) + Count(Normal\_E_i > Threshold)} \tag{6}$$

$$Goal = Max(F\text{-}measure) \tag{7}$$

$$F\text{-}measure = \frac{2.precision.recall}{precision + recall} \tag{8}$$

In Eq. 3 E_i is the fuzzy output value of a chromosome instance in the population. In Eq. 5, recall means the recall rate of the detection rule. Count (Fraud_E_i>Threshold) means the number of account in the fraud list when the threshold>E_i.

The threshold is designed as Eq. 4 and is shown in Fig. 8. The threshold is set as the average of minimum fuzzy score of fraud accounts list and maximum fuzzy score of normal accounts list. The Count (Fraud_Account) means the total number of accounts in the fraud accounts list.

In Eq. 6, precision means the accuracy of the detection rule. The value of Count (Fraud_E_i>Threshold) is defined above and Count (Normal_E_i>Threshold) means the number of accounts in normal accounts list when the threshold>E_i.

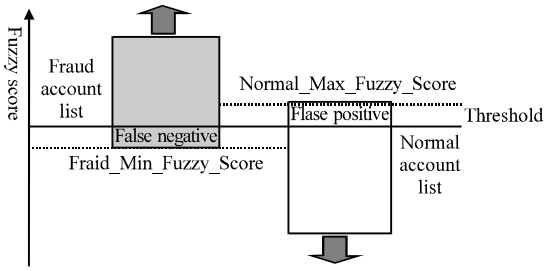

Fig. 8: Threshold design (Yu and Lin, 2013)

Table 2: Genes enconding

	Density (K-core or score) = NS (netative rating score)					Density (K-core or score) = PS (netative rating score)				
N/P ration	NB	NS	ZO	PS	PB	NB	NS	NO	PS	PB
NB	G_0	G_1	G_2	G_3	G_4	G_{25}	G_{26}	G_{27}	G_{28}	G_{29}
NS	G_5	G_6	G_7	G_8	G_9	G_{30}	G_{31}	G_{32}	G_{33}	G_{34}
ZO	G_{10}	G_{11}	G_{12}	G_{13}	G_{14}	G_{35}	G_{36}	G_{37}	G_{38}	G_{39}
PS	G_{15}	G_{16}	G_{17}	G_{18}	G_{19}	G_{40}	G_{41}	G_{42}	G_{43}	G_{44}
PB	G_{20}	G_{21}	G_{22}	G_{23}	G_{24}	G_{45}	G_{46}	G_{47}	G_{48}	G_{49}

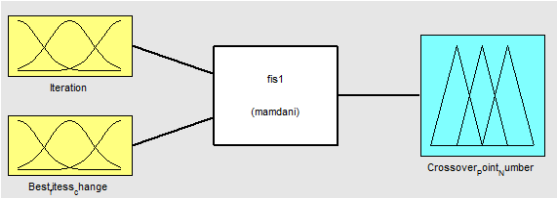

Fig. 9: The general model of the proposed fuzzy inference system for crossover

In Eq. 7, Goal means the goal of genetic algorithms and its maximum value points to the most desirable solution. The F-measure value is defined as an overall approach and provides a balance between the recall rate and precision rate. the assessment of this fitness function enables the optimal detection rules to detect all fraudulent accounts and obtain the maximum value of Count (Fraud_E_i>Threshold). This optimal value will be equal to Count (Fraud_Account). Thus, the best value of Recall will be close to 1.

In addition, the optimal detection rules will prevent a normal account to be detected as a fraud account, thus the minimum value of Count (Normal_E_i>Threshold) and the optimal value will be zero. The best value of Precision and F-measure will be close to 1.

Selection: This study uses the roulette wheel method for the selection operation. This method is a popular technique to perform random sampling with replacement. This chance-based method is carried out by mapping all individuals on adjacent areas of a line, based on their competence. The size of the area of each individual will be determined with accordance to his/her competence. Then, a random number will be generated which will point to the individual who will be selected.

Crossover: This research uses a multiple crossover method for crossover operation. The reason to use multiple crossover method is the fact that as more chromosomes become involved in the generation of children, the search space will be explored better and search will be more efficient. In this study, the proposed fuzzy inference system is used to determine the number of hybrid points. This fuzzy inference system has two input variables: iteration number of the current generation and the changes in the fitness of best solution in previous iterations. The output of this system is a fuzzy number that determines the number of hybrid points from a predetermined range. Figure 9 shows the general model of the proposed fuzzy inference system for crossover. Membership functions of input and output variables of the system are shown in Fig. 10. In this study, the Max point number is assumed to be 5.

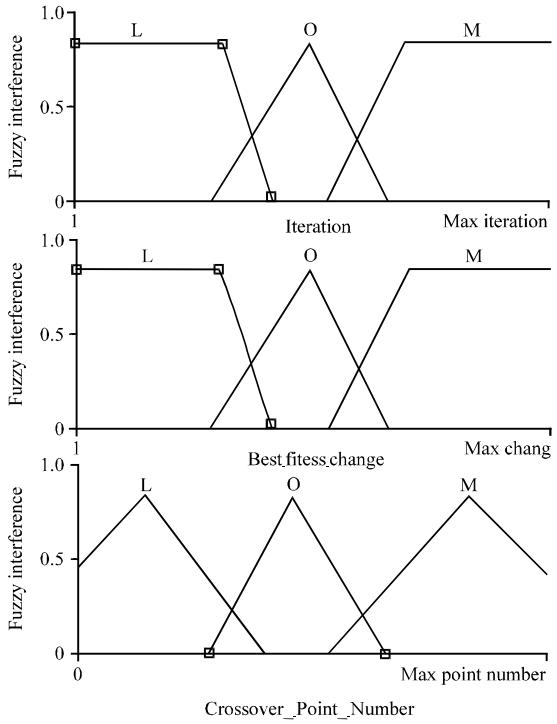

Fig. 10: Membership functions of the proposed Fuzzy Inference System for crossover

Mutation: Genetic algorithms sometimes converge to locally optimal solutions. Mutations can alter some of the genes randomly and guide the evolution towards other solutions by searching other spaces containing possibly desirable solutions. In this study, mutation step is directly related to the change in the fitness of best solution in previous iterations and the current iteration number and is determined in a user-specified range. Mutation speed or number of mutation operations has an inverse relationship with variables above (the change in the fitness of best solution in previous iterations and the current iteration number) and is calculated by the use of fuzzy inference systems designed for this purpose. The input of the fuzzy inference system includes the change in the fitness of best solution in previous iterations and the current iteration number while the output of the system is a fuzzy number that determines the number of mutation operations. Membership functions of input and output variables of the system are shown in Fig. 11. In this research, the Mutation number is considered to be 4.

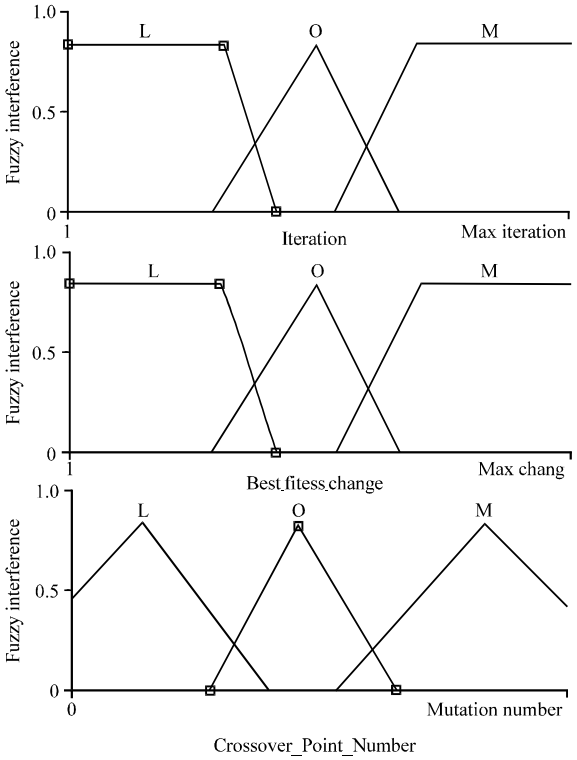

Fig. 11: Membership functions of the proposed Fuzzy Inference System for mutation

RESULTS AND DISCUSSION

In this study, we present and examine the results of the proposed approach and compare them with those of previous work in the literature. These results are obtained by simulating the proposed algorithm in MATLAB environment.

First experiment evaluates the K-core and score features. In this experiment, the initial population is 200, the number of generations is 50 and the genetic algorithm is run 10 times for each feature. As can be seen in Fig. 12, the score feature has achieved the desired result in <50 generations and has outperformed the K-core feature.

Experiment designed in this section is carried out with a population of 100 and maximum iteration of 100 generations.

Figure 13 shows a comparison between the performance of the proposed algorithm and the algorithm proposed by Cheng (Yu and Lin, 2013). The curves presented in this Fig. 12 are the average results obtained from 20 runs of these two algorithms. According to this Fig. 12, the proposed system substantially increases the speed of reaching the optimal result. As can be seen in this Fig. 13, using the same number of fitness function

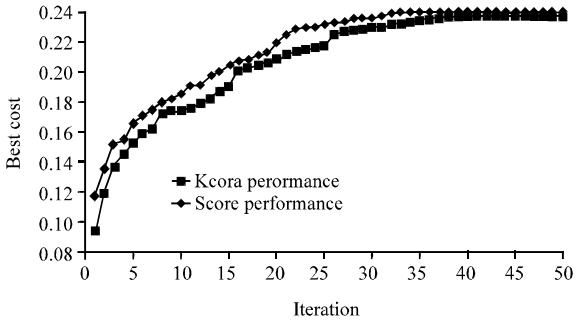

Fig. 12: The performance of K-core feature and score feature

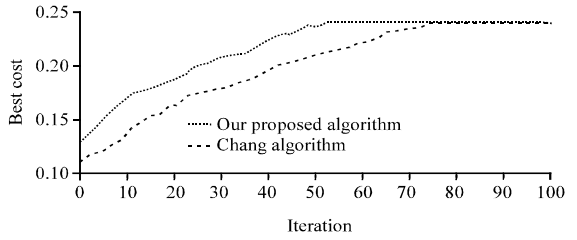

Fig. 13: The performance of the proposed algorithm and the Cheng algorithm

Table 3: Optimized weights of fuzzy rules

Weights of fuzzy rules	Values	Weights of fuzzy rules	Values
G0	0.3573	G25	0.6728
G1	0.4682	G26	0.3226
G2	0.7584	G27	0.2903
G3	0.7596	G28	0.1795
G4	0.2986	G29	0.3940
G5	0.1767	G30	0.1195
G6	0.9450	G31	0.4118
G7	0.8790	G32	0.7629
G8	0.8453	G33	0.6817
G9	0.2625	G34	0.7822
G10	0.0002	G35	0.6969
G11	0.9214	G36	0.2347
G12	0.8120	G37	0.6356
G13	0.3387	G38	0.3856
G14	0.7945	G39	0.2167
G15	0.3437	G40	0.8061
G16	0.3866	G41	0.2999
G17	0.7932	G42	0.7784
G18	0.3106	G43	0.0891
G19	0.7295	G44	0.5339
G20	0.1525	G45	0.6801
G21	0.8199	G46	0.5231
G22	0.2901	G47	0.0869
G23	0.5818	G48	0.2467
G24	0.4520	G49	0.7516

recalls, the proposed system can improve the algorithm performance and the speed by which algorithm reaches the optimal result. The weights optimized for each fuzzy rule which are displayed in the form of superior chromosome genes (G0-G49) are provided in Table 3.

CONCLUSION

In today's world, the development of banks and financial institutions and the increasing number of customers and volume of transactions have generated new types of problems and challenges that require careful data examination. But careful examination of high volumes of data with conventional methods is an impossible task. On the other hand, financial and credit institutions are seeking solutions that can quickly detect criminal acts and intentions. Therefore, the hardware and software capacities made available by modern technology must be combined with available data mining techniques to examine high volume of data used for such applications.

Data mining is "to extract information and knowledge and to discover hidden patterns from very large databases". Data mining techniques are performed on data sets and higher quantity and quality of data stored in any dataset leads to better performance of data mining techniques in assessing that dataset. The data mining methods analyze the data to discover unclear relations and hidden patterns that must be extracted to complete our knowledge base. So, the main goal of data mining is to find models that help us make better decisions.

The main objective of this researh was to provide a new method based on data mining to study the problem of fraud detection. This research also sought to combine the genetic algorithm with other artificial intelligence techniques such as fuzzy systems to provide novel and quick solutions for the problem of identification and differentiation of valid and fraudulent individuals in banking systems.

In this study, a hybrid approach composed of fuzzy inference system and developed genetic algorithm was proposed to detect the fraudulent accounts. The proposed system used the behavioral characteristics derived from auction websites to initialize the fuzzy inference system. Fuzzy rules of the proposed system were optimized for auction fraud detection model by the use of genetic algorithm.

Solution presented in this paper was evaluated by the use of valid data sets. The results of the implementation of the proposed system show that the algorithm performance and the speed by which it reaches the optimal result are significantly improved. One of the factors that increase this speed is the introduction of fuzzy operators of crossover and mutation.

In this research, multi-crossover method was used to ensure greater participation of chromosomes in each generation. This caused the search space to be explored better and led to a more efficient searching process. In addition, the proposed fuzzy inference system was used to determine the number of hybrid points based on iteration number of the current generation and the change in the fitness of best solution in previous iterations.

Another factor increasing the efficiency and speed of the proposed algorithm was the fuzzy mutation operator. The mutation step of the presented fuzzy mutation operator was directly related to the change in the fitness of best solution in previous iterations and the current iteration number and was determined in a predetermined range. Mutation speed or the number of mutation operations had an inverse relationship with the above variables (the change in the fitness of best solution in previous iterations and the current iteration number) and was calculated using the fuzzy inference systems designed for this purpose. The output of the system was a fuzzy number that determined the number of mutation operations.

Finally, the proposed algorithm was compared with a method previously presented in this field. This comparison showed that the use of fuzzy operators presented for the proposed system significantly increases the speed of reaching the optimal result in a way that the implementation of the proposed system by using the same number of fitness function recalls will further improve performance and speed by which algorithm reaches the optimal solution. In the end, the weights optimized for each fuzzy rule which were in the form of superior chromosome genes were obtained with an acceptable speed.

REFERENCES

Albrecht, W.S., C. Albrecht and C.C. Albrecht, 2008. Current trends in fraud and its detection. Inf. Secur. J. Global Perspec., 17: 2-12.

Anil, S. and R. Remya, 2013. A hybrid method based on genetic algorithm, self-organised feature map and support vector machine for better network anomaly detection. Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies, July 4-6, 2013, IEEE, Tiruchengode, India, ISBN: 978-1-4799-3925-1, pp: 1-5.

Aziz, A.S.A., M.A. Salama, A.E. Hassanien and S.E.O. Hanafi, 2012. Artificial immune system inspired intrusion detection system using genetic algorithm. Inf., 36: 347-357.

Duman, E. and M.H. Ozcelik, 2011. Detecting credit card fraud by genetic algorithm and scatter search. Expert Syst. Appl., 38: 13057-13063.

Morzy, M., 2008. New algorithms for mining the reputation of participants of online auctions. Algorithmica, 52: 95-112.

Nagi, J., K.S. Yap, S.K. Tiong, S.K. Ahmed and F. Nagi, 2011. Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system. IEEE. Transac. Power Delivery, 26: 1284-1285.

Ngai, E.W.T., Y. Hu, Y.H. Wong, Y. Chen and X. Sun, 2011. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decis. Support Syst., 50: 559-569.

Phua, C., D. Alahakoon and V. Lee, 2004. Minority report in fraud detection: Classification of skewed data. ACM. SIGKDD. Explorations Newsl., 6: 50-59.

Wang, J.C. and C.C. Chiu, 2008. Recommending trusted online auction sellers using social network analysis. Expert Syst. Appl., 34: 1666-1679.

Wang, J.H., Y.L. Liao, T.M. Tsai and G. Hung, 2006. Technology-based financial frauds in Taiwan: Issues and approaches. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 8-11, 2006, IEEE, Taipei, Taiwan, ISBN: 1-4244-0100-3, pp: 1120-1124.

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.

Yu, C.H. and S.J. Lin, 2013. Fuzzy rule optimization for online auction frauds detection based on genetic algorithm. Electron. Commerce Res., 13: 169-182.

Yue, D., X. Wu, Y. Wang, Y. Li and C.H. Chu, 2007. A review of data mining-based financial fraud detection research. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, September 21-25, 2007, IEEE, Shanghai, China, ISBN: 978-1-4244-1311-9, pp: 5519-5522.