IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 33, No. 2, April, 2019, pp. 81-87
Journal homepage: http://iieta.org/journals/ria

Terrorism Prediction Using Artificial Neural Network

Ghada M.A. Soliman*, Tarek H.M. Abou-El-Enien

Faculty of Computers & Artificial Intelligence, Cairo University, Giza, Egypt

Corresponding Author Email: gh.tolan@fci-cu.edu.eg

https://doi.org/10.18280/ria.330201

Received: 7 January 2019
Accepted: 22 March 2019

Keywords:
feedforward neural networks, hybrid algorithm, wrapper approach, metaheuristics algorithms, fitness function, supervised machine learning

ABSTRACT

The main purpose of this research is to develop a hybrid computational intelligent algorithm (framework) as a decision support (DS) tool for terrorism phenomenon that has been defeated for years by governments, countries, and different multiple institutions and hence it needs multiple and integrated research from different science disciplines with a hope of being eliminated in the future. The proposed hybrid prediction algorithm based on integrated different Operations Research (OR) and Decision support tools with Data Mining (DM) techniques especially prediction and classification algorithms as well as different directions of modification and improvements in a number of recent and popular metaheuristics inspired algorithms. The proposed system has been developed, implemented, and evaluated according to different set of assessment measures. Through this study, it was found that, the proposed system is capable of predicting the terrorist group (s) responsible of terror attacks on different regions (countries). The findings of this research may serve as an alarm tool to determine the terrorist groups' networks and so minimize the terrorist attacks.

1. INTRODUCTION

Terrorism is a complex adaptive system, evolving phenomenon [1] and it is a type of collective violence which has direct negative impact on peace, normal routine of countries and societies security and also a way to generate fear in civilians using violence. [2].

Many researchers and various institutions based on analyzing terrorism incident data around the world which could help in retrieving some patterns or an important information that can contributes in choosing an appropriate action to prevent similar types of attacks. Some of them are:

(1) Hawkes Process, a process that is applied to predict terrorist attacks in Northern Ireland which considered 5000 explosions ranging between year 1970-1998. The process was used to analyze when and where the Irish Republicans Army (IRA) launched the attack, how British security forces responded [3].

(2) Social Network Analysis (SNA) whose goal was to degrade the lethality of terror network i.e. what happens when terrorist is removed from network. (i) Quantifying terror network lethality (ii) Predicting successor of removed terrorist (iii) Identifying whom to remove. And some of the activities carried out are fake account, social media fraud [4].

(3) Terrorist Group Prediction Model (TGPM) aims to predict the group involved in a specific attack or the group that is responsible for that attack which uses crime prediction model and group detection model concepts. It uses clustering and association technique which showed some fair degree of accuracy [5].

(4) Dynamic Bayesian Network used to predict the likelihood of future attacks, which acts an initial step in predicting the terrorist behavior at critical transport infrastructure facility [6].

(5) Feed forward back propagation neural network, which is used for counter terrorism to predict whether a person is terrorist or not. Data set is collected from a game called cutting corners and result showed success rate between 60 %-68 % for correctly identifying terrorist behaviour [7].

(6) Characterizing a terrorist using pattern classification and SNA which predicts whether a person is terrorist or not and resulted in 86 % accuracy [8].

(7) Both random forest classification and random forest regression are used in a prediction model for future attacks where the model achieved the accuracy of 76 %-79 % for attack type, 84 %-86 % for weapon type and 33 %-36 % for target type [9].

Artificial Neural Networks (ANNs) known as one of the popular and important efficient machine learning paradigms for classification as well as for prediction. ANNs relatively new computational tools that have found extensive utilization in solving and supporting many complex real-world applications across a diversity of business and scientific disciplines (financial, manufacturing, marketing, telecommunications, and biomedical).

The attractiveness of ANNs comes from their remarkable information processing characteristics pertinent mainly to nonlinearity, high parallelism, fault and noise tolerance, and learning and generalization capabilities [10]. ANN is more like a black box that is able to learn something and predicts various kinds of data. Various applications of ANNs can be summarized into classification or pattern recognition, prediction and optimization, modeling, associative memory, and control [11].

There have been many attempts to formally define neural networks. “A neural network is a system composed of many simple processing elements operating in parallel whose function is determined by network structure, connection strengths, and the processing performed at computing elements or nodes” –DARPA Neural Network Study [12].

The most commonly used family of neural networks for pattern classification tasks [13] is the feed-forward network, which includes multilayer perceptron and Radial-Basis Function (RBF) networks. Another popular network is the Self-Organizing Map (SOM), or Kohonen-Network [14], which is mainly used for data clustering and feature mapping.

The remainder of this research is organized as follows: Section 2 shows the details of the proposed system framework its tools, techniques as well as the used and modified metaheuristics, while section 3 explains the prediction of the terrorist groups based on using artificial neural networks as well as the data pre-processing , the classification process, the used fitness functions. In Section 4 the prediction results provided by ANN is explained in details, and finally the conclusions and future research directions are discussed in Section 5.

2. METHODOLOGY

The details of the used methodology and the main phases of the proposed system are explained in details in Figure 1.

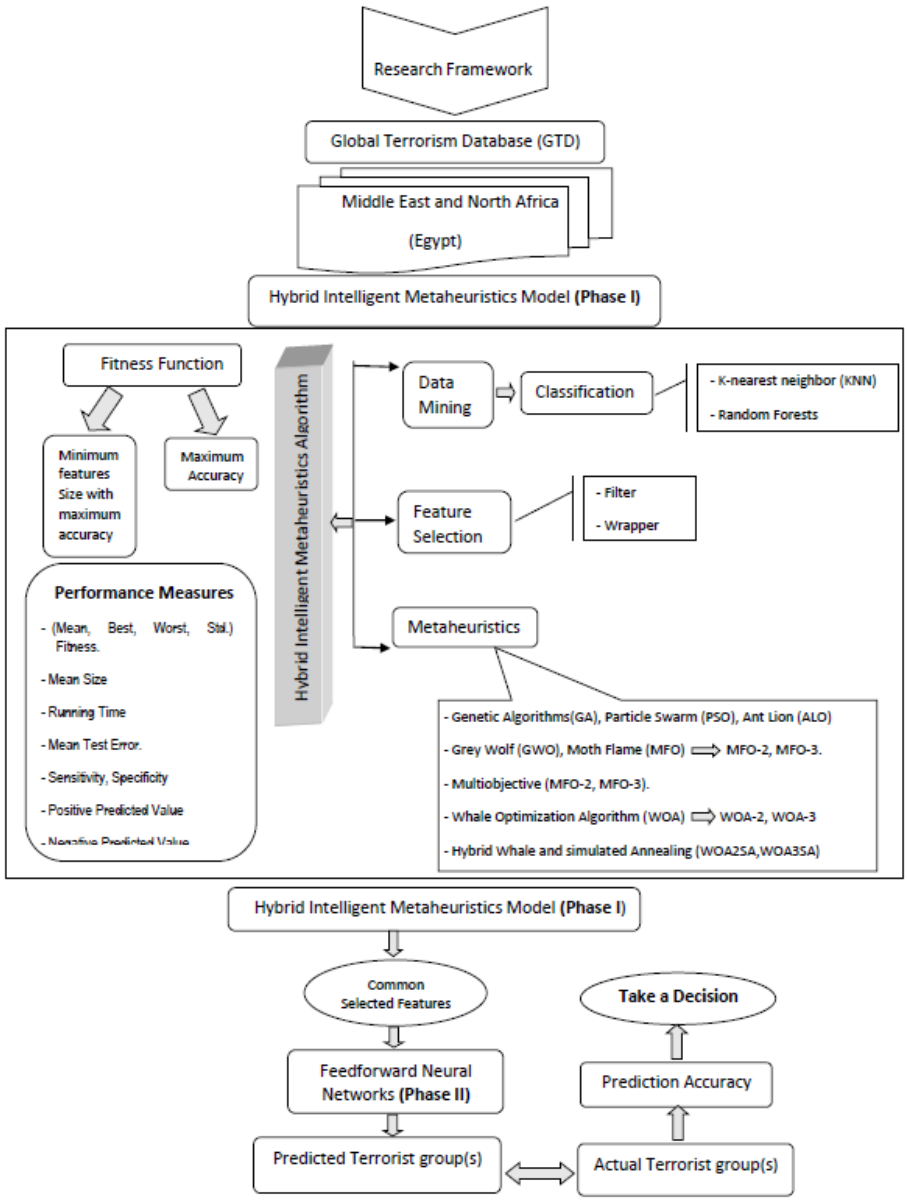

Figure 1. The framework of the prediction model

3. TERRORIST GROUP(S) PREDICTION USING ANNs

In this research we proposed a hybrid prediction algorithms based on using different metaheuristic algorithms such as (GWO, MFO [16], WOA [17], ALO, GA, PSO), modified metaheuristics such as (MFO2, MFO-3 proposed by Soliman, et al. [18], and (WOA-2, WOA-3) proposed by Soliman, et al. [19], developed (hybrid) algorithms such as (Multi-objective MFO2, Multi-objective MFO3) proposed by Gh. et al, [20], and memetic (hybrid) WOA2SA, WOA3SA recently proposed by Soliman, et al.

Phase I

In each one of the implemented algorithms we integrate a feature selection approach (either wrapper approach or integrate both filter with wrapper approaches into a hybrid system) with a machine learning classification algorithm

(KNN, RFs) controlled by the optimimization process that is guided by the metahuristics optimization algorithm in order to determine the minimum number of selected features that achieve highest classification accuracy (minimum classification error).

To achieve the main objective of the proposed research which is the prediction of the terrorist group (s) responsible for the terrorist attacks on Egypt during the time period (from year 1996 till year 2017), we determined the common number of features among the obtained selected features from the multiple implementations of the proposed hybrid systems.

3.1 The proposed hybrid prediction (classification) algorithm

Algorithm 1: The Proposed Hybrid Classification Algorithm

Step1: Data Pre-Processing,
Step2: Data partitioning into training and testing sets,
Step3: Then using the wrapper approach as a feature selection method guided by the classifiers (RFs, KNN) in the classification process to select the feature subset and with the help of the optimization algorithm to evaluate the selected feature subset by using the fitness function in multiple runs via different number of iterations.
Step4: Stopping Criterion (If Maximum No. of iterations > *NIter*, then go to Step 6; otherwise go to step3).
Step5: Results & performance analysis.
Step6: Stop.

3.1.1 Data pre-processing phase

This section explains how the terrorism data has been pre-processed to be used in the prediction. The data used is real terrorism data and describes the terrorist attacks in Middle East & North Africa especially the attacks that happened in Egypt (from year 1996 till year 2017). The data set derived from the Global Terrorism Database (GTD) [15] which is taken from an open source of the National Consortium for the Study of Terrorism and Responses to Terrorism (START):

- Initiative at University of Maryland USA.
- Broadcasts the terrorism incidents reports about the globe from 1970 to 2018.
- Since 1970 it contains the information over than 13,000 eliminations, 38,000 bombings and 4,000 kidnappings.
- GTD includes systematic data on domestic as well as international terrorist incidents that have occurred during this time period and now includes more than 170,000 cases.
- This dataset is under the supervision of counseling board of 12 terrorism research experts.

The data are required to be prepared for using in the classification process and it passed on multiple steps as explained below:

- Data Cleaning: Preprocess data in order to reduce noise and handle missing values by applying (Litwise-Deletion, Mode-Imputation) approaches.
- Data transformation (from Categorical into Numeric based on GTD coding system)

(1) The features in our data are classified as (Date, Incident location, Location Details, Attack information, Weapon Information, Target/Victim information, Casualties & Consequences) features

(2) For the time domain features; we applied a feature reduction where we transformed the "day, month, and year" features into an equivalent "day per year, Hijiri day per year, and an equivalent day per week ".

(3) For the position or location feature we transformed it into city-latitude, and city-longitude.

(4) Due to the huge number of classes in some features in our data; we had to combine the classes in some features into groups.

After the preprocessing step, the dimension of Terrorism data on the time period from year 1996 till year 2017 became 45 (predictors/attributes or features) besides "Terrorist group name" that is considered as (response class), and the total number of attacks (records) became 813, the total set of features are described as below in Table 1.

3.1.2 Feature selection & extraction phase

A wrapper approach for feature selection and attribute reduction is used in our research study; where the attribute space consists from 46 attributes in the used time domain is explored to find an attribute (feature) subset guided by classification performance of individual attribute subsets. Hence intelligent exploration of search space is always a challenge as the single evaluation of fitness function is always time consuming. This approach may be slow since the optimization algorithm must be retrained on all candidate subsets of the attribute set and its performance must be also measured to find the attribute combination that balance between the minimum numbers of features which achieve the maximum classification accuracy (minimize the classification error) as in the used fitness function in Eqn.(1).

3.1.3 Classification process phase

The data used about terrorism is divided into three equal parts; one for training the classifier, the second for validation and the third for testing the model. GWO proposed by [21], WOA, the modified versions WOA2, WOA3, MFO, the modified MFO2, and MFO3 algorithms results' are compared to some of well-known and highly efficient metaheuristics algorithms such as particle swarm optimization (PSO) and Genetic Algorithm (GA), Ant lion algorithm (ALO) as they are known with their popularity in space searching. The classification process of the terrorist groups of attacks is performed based on KNN classifier which is one of the top ten classifiers used for the classification process and is simple and commonly utilized learning algorithm, KNN is utilized in the experiments based on trial and error basis where the best choice of (K=5) is selected.

Through the training process, every (wolf, moth, whale) position represents one attribute subset. Training set is used to evaluate the RF ensemble classifier which is compared with KNN classifier; on the validation set throughout the optimization process to guide the feature selection process. The test data are kept hidden from the optimization and is left for final evaluation.

Table 1. Terrorism dataset features of time period (1996 till 2017) for Egypt

Feature	Type	Feature	Type
Month	Numeric Variable	Vicinity	Categorical Variable
Day	Numeric Variable	Crit1 (Inclusion Criteria1)	Categorical Variable
Year	Numeric Variable	Crit 2(Inclusion Criteria2)	Categorical Variable
Equivelant-Day Per Year	Numeric Variable	Crit 3(Inclusion Criteria3)	Categorical Variable
Equivalent Hijiri day/year	Numeric Variable	Doubtterr (Doubt Terrorism Proper?)	Categorical Variable
Equivalent week per year	Numeric Variable	Alternative (Alternative Designation)	Categorical Variable
Equivalent day per week	Numeric Variable	Multiple (Part of Multiple Incident)	Categorical Variable
Extended Incident	Categorical Variable	Success(Successful Attack)	Categorical Variable
Provstate	Text Variable	Suicide(Suicide Attack)	Categorical Variable
City	Text Variable	Attack-Type	Categorical Variable
City-Latitude	Numeric Variable	TargetType	Categorical Variable
City-Longitude	Numeric Variable	Target-subtype	Categorical Variable
Specific	Categorical Variable	Weapon-Type	Categorical Variable
Weapon-Subtype	Categorical Variable	Compclaim (Competing Claims of Responsibility?)	Categorical Variable
Nkill (Number of fatalities)	Numeric Variable	Property(Property damage)	Categorical Variable
Nkilter(Prepetrator Fatilities)	Numeric Variable	Propextent (Extent of Property Damage)	Categorical Variable
Nwound (total Number of Injured)	Numeric Variable	Ishostkid (hostage/kidnapping vicitms)	Categorical Variable
Nwoundte (Number of Perpetrators Injured)	Numeric Variable	Nhostkid (Total num. of Hostage/Kidnapped)	Numeric Variable
Guncertain (Perpetrator Group Suspected /Unconfirmed?)	Categorical Variable	Nhours(Kidnapping hours)	Numeric Variable
Individual (Unaffiliated Individual(s)	Categorical Variable	Ndays(Kidnapping days)	Numeric Variable
Nperps (Total perps. In the incident)	Numeric Variable	Rnsome (Ransom Demanded)	Categorical Variable
nperpcap (Number of Perpetrators captured)	Numeric Variable	Ransomamt (Total Ransom Amount Demanded)	Numeric Variable
Claimed (Claim of Responsibility?)	Categorical Variable	Ransompaid (Total Ransom Amount Paid)	Numeric Variable
Claimmode (Mode for Claim of Responsibility)	Categorical Variable	Hostkidoutcome (Kidnapping/Hostage Outcome)	Categorical Variable
Victim-Nationality	Categorical Variable	Predetator, (Terrorist) Group-Name	Text Variable

3.1.4 Fitness function

Fitness function is important for metaheuristic algorithms, it is used evaluate the quality of each selected subset. fitness evaluation is designed to combine the accuracy of classifier with the length of feature subset. A fitness function combines both the classification error (classification accuracy) and the number of selected features and hence achieve that balance between the classification performance and the reduction size.

There are two fitness functions used in our research study to evaluate the individual search agents ACC fitness which evaluate the accuracy of the model, and ACCSZ which evaluate the selected feature size that achieve the minimum classification error. The fitness function that is used in our optimization algorithms to evaluate individual search agents is shown as follows:

$$\text{Minimize} \quad \text{ACCSZ} \quad \text{Fitness} = \propto \boldsymbol{\gamma_T(C)} + \boldsymbol{\beta}\frac{|\boldsymbol{T}|}{|\boldsymbol{D}|} \qquad (1)$$

where, $\boldsymbol{\gamma_T(C)}$: is the error rate for the classifier used in which $\boldsymbol{\gamma_T(C)}$=1- CCR(C), **T**: is the size (length) of selected feature subset, **D**: Total number of features in the data set.

α, β: Parameters or (constants) corresponding to the importance of classification performance and subset length and so can control the quality of the classification.

α ∈ [0, 1] and β = 1 – α.

$$\text{Maximize} \quad \text{ACC} \quad \text{Fitness} = \text{CCR(C)}$$
$$\text{CCR(C)} = \text{N\_C/N} \qquad (2)$$

where, CCR(C): is the classification performance measure that

represents the correct classification ratio. N_C is the number of correctly classified data instances and N is the total number of instances in the data set.

The random weights which represented by the terms α and β are used to balance the trade-off between exploration and exploitation. Through the training process, every agent position that represented research by the (Grey-wolf, moth, whale, antlion) position represents one feature subset. The training set is used to train the prediction model through optimization and hence evaluate the used classification algorithm (RFs, KNN) on the validation set during the optimization to guide the feature selection process, while in the validation set the performance of the predicted model is assessed during the optimization process. The final evaluation of the selected features is performed in the testing set. The proposed optimization algorithms are used to find the minimum number of features that maximize the prediction performance (minimizes classification error). Each feature in the search space is represented as an individual dimension, each dimension ranges from 0 to 1 and hence requires an intelligent searching method to find the optimal feature set in the huge search space that optimizes a given fitness function.

The global and optimizer-specific parameters setting is showed in Table 2. the values of the parameters are set either according to domains specific-knowledge as the α; β parameters of the fitness function in Eq. (1), or based on the trial and error on small simulations which is common in the literature as the rest of the parameters.

Table 2. Parameter setting for experiments

Parameters	Value
No. of search agents	5
No. of iterations	50, 70, 100, 150
Problem Dimension	46
Search Domain	Data sets of terrorism
No. of Repetition of Runs	15, 30
Inertia Factor of PSO	0.1
Individual Best Acceleration of PS	0.1
Crossover Fraction in GA	0.8
α Parameter in the fitness Function	0.99
β Parameter in the fitness Function	0.01

3.1.5 Performance measures

In order to compare between the optimization algorithms that used separately in the proposed hybrid prediction model, we used a set of statistical measures that evaluate the performance of the model by calculating the mean, best, worst fitness, as well as the measures of error such as the mean test error, also there are the measures of the speed of the model as the execution time, and other important measures as the specificity, sensitivity, Fisher average, Wilixicon and T-Test for the different optimizers.

Phase II

We used the common selected features from Phase I as an input into a Two Layer Feedforward Neural Network, then the predicted terrorist group will be compared with the actual terrorist group to determine the prediction accuracy.

(1) Different Activation functions used in the Neural Network for the Hidden Layer such as "Tansig"," radbas", "logsig", "purelin" " Sigmoid".

(2) We Implemented the NN prediction model using different numbers of neurons in the hidden layer such as 15, 20, 25, 30 neurons.

(3) The performance measure that used for evaluation is the Mean Square Error (MSE).

(4) The Input data matrix dimension are 15 common selected features, and 818 records (terrorist attack).

(5) The target matrix dimension are 24 terrorist groups set as the matrix rows, and 818 as the matrix columns.

3.2 Common selected features

By the end of Phase I; the set of common selected features among the implemented proposed algorithms are determined from the different experimentations and used for the input in the neural network training as explained in Figure 2.

3.3 Network training

The input data are divided into training, validation, testing. The input terrorism data matrix is a numeric matrix where; the number of records represented by the common selected features (obtained from Phase I of the proposed prediction system) and the number of columns represent the total number of instances or the terrorist attacks. The network trained on the first two third of the input data, and the testing will be performed on the last third of the data.

4. NEURAL NETWORK PREDICTION

The target matrix constructs from the number of terrorist groups as the matrix rows, and the total number of terrorist attacks or instances as matrix columns. The target matrix has been constructed as matrix of (+1, -1) following the "Tansig" activation or transfer function (where +1 given for the terrorist group that performed the terrorist attack, -1 otherwise). According to the output matrix from the network, a terrorist group is selected for each terrorist attack that has the highest value near to (+1) that will be considered the predicted terrorist group. And hence the prediction accuracy of the network can be easily calculated as follows in Eq. (3):

$$\text{Prediction Accuracy} = \frac{\text{Total number of True (correct) predicted terrorist group}}{\text{sample Size}} \quad (3)$$

In the following subsection we present a sample of the output obtained from the network via changing in the activation functions and the used number of neurons as given bellow:

Based on the obtained accuracy of the neural network; the decision maker can decide either to accept the neural model or repeat the runs till reaching to the required accuracy.

When the network is trained based on using "Tansig" is used for the hidden and for the output layers, and the number of used neurons in the hidden layer are 20, the obtained performance (MSE)=0.0181 and Validation performance at iteration 10=0.086003 from 16 iterations, and hence the neural network produce the Prediction Accuracy of the model=74.77 % as shown in Figure 3.

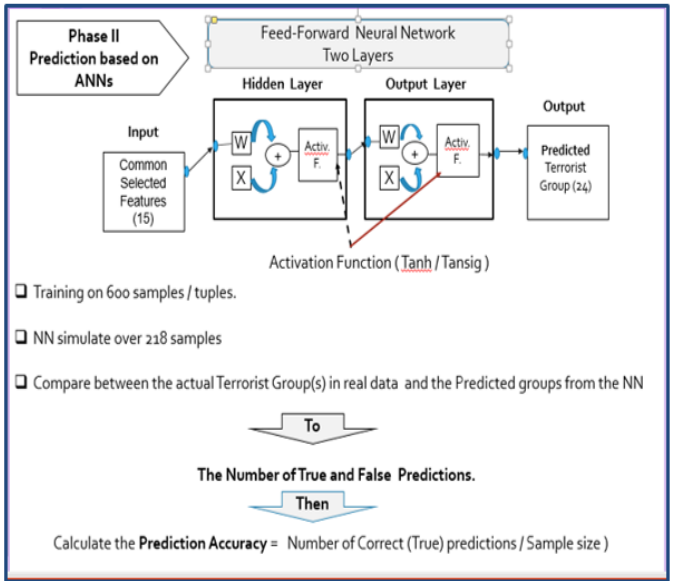

Figure 2. Feed-forward neural network of the hybrid prediction model

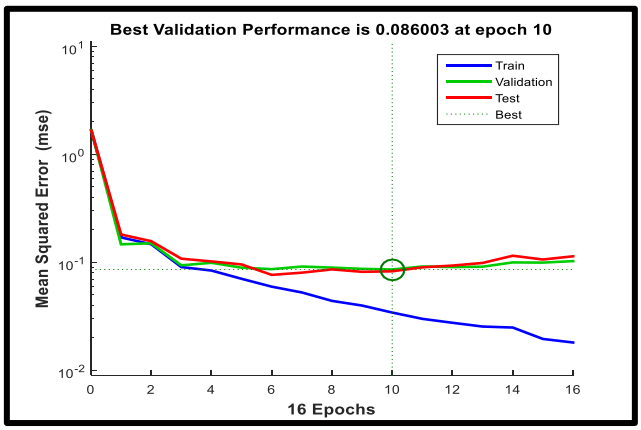

Figure 3. The best validation performance for run 1

For another run with the same number of neurons and "Tansig" activation functions, the network produced Prediction Accuracy = (151 / 218)*100 = 69.0266 %, and Best validation performance = 0.073728 at iteration 8 out of 16 iterations as explained in Figure 4.

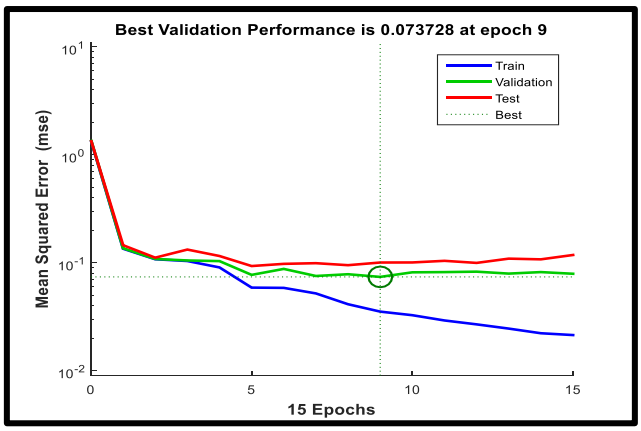

Figure 4. The best validation performance for run 2

When the number of neurons is 40 for the same activation functions "Tansig", the network produced the output as follows in Figure 5 where the Prediction Accuracy of the model=73.39 %, and Best Validation Performance=0.074298 at iteration 12 out of 18 iterations.

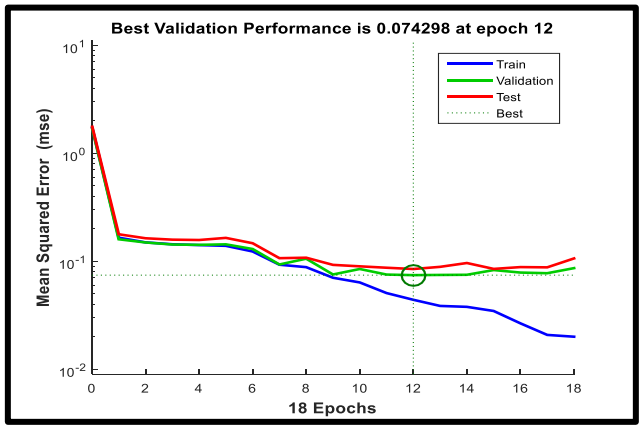

Figure 5. The best validation performance for run 3

When the Activation functions are "Radbas' for the hidden layer, 'tansig' for the output layer as well as the number of Neurons=25, the network produced the following output: Prediction Accuracy: 75 % as explained by Figure 6.

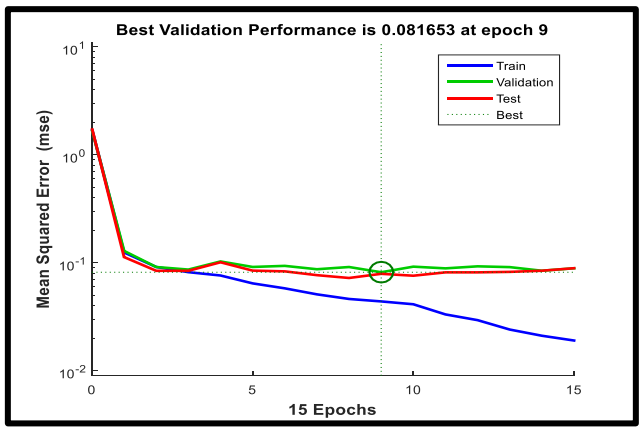

Figure 6. The best validation performance for run 4

5. CONCLUSIONS

In this research we proposed a hybrid computational intelligent algorithm (framework) as a decision support (DS) tool for terrorism phenomenon. The proposed hybrid prediction algorithm based on integrated different Operations Research, and Decision support tools as well as Data Mining (DM) techniques especially prediction and classification algorithms and different directions of modification and improvements in a number of recent and popular metaheuristics inspired algorithms. The proposed system has been developed, implemented, and evaluated according to different set of assessment measures. Through our research; the proposed research proved its ability of predicting the terrorist group (s) responsible of terrorist attacks on different regions on Egypt during specified time periods (from year 1996 to 2017) via determine the optimum feature subset that provide the highest classification accuracy.

The implementation results of the proposed computational approach gives promising prediction accuracy based on using the Artificial Neural Networks as a final phase of the

prediction system that allows the prediction system to be used as an alarm in the future as an investigated tool for the existence of the terrorists groups networks and hence minimizes and eliminates the terrorist attacks .

For future research study, our proposed prediction system can be used to predict the terrorist groups in different countries. There are different directions where a researcher can enhance and modify in the proposed algorithm as using a hybrid embedded feature selection approach instead of the wrapper approach and using various metaheuristics optimization algorithms.

REFERENCES

[1] Ibrahim, T., Aryya, G. (2015). Analyzing real time terrorism data. IEEE International Symposium on Technologies for Homeland Security, Waltham, MA, USA. https://doi.org/10.1109/THS.2015.7225299

[2] https://www.slideshare.net/shaanyadav3/terrorismcauses-and-types (2015).

[3] Ana, S. (2016). The eerie math that could predict terrorist attacks. International Journal of the Care of the Injured, 47(3): 646-652. https://doi.org/10.1016/j.injury.2015.12.021

[4] Subrahmanian, V.S. (2016). Terrorist social network analysis: Past, present, and future. UMIACS University of Maryland.

[5] Abhishek, S., Devshri, R. (2012). TGPM: Terrorist group prediction model for counter terrorism. International Journal of Computer Applications, 44(10): 49-52. https://doi.org/10.5120/6303-8516

[6] Dixon, S.J., Dixon, M.B., Elliott, J., Guest, E., Mullier, D.J. (2011). A neural network for counter-terrorism. SGAI 2011: Research and Development in Intelligent Systems XXVIII, pp 229-234. https://doi.org/10.1007/978-1-4471-2318-7_18

[7] Coffman, T.R., Marcus, S.E. (2004). Pattern classification in social network analysis: A case study. Published in IEEE Aerospace Conference Proceedings, Big Sky, MT, USA. https://doi.org/10.1109/aero.2004.1368121

[8] Erik, M. (2014). Terrorism: Its past, present and future prospects. Journal Studies in Conflict & Terrorism, 38(1): 62-74. https://doi.org/10.1080/1057610X.2014.976011

[9] Snehanshu, S., Abu, S. (2017). Future terrorist attack prediction using machine learning techniques. National Institute of Science Technology and Development Studies. https://doi.org/10.13140/RG.2.2.17157.96488

[10] Basheer, A.I., Hajmeer, M. (2000). Artificial neural networks: Fundamentals, computing, design, and application. Journal of Microbiological Methods, 43(1): 3-31. https://doi.org/10.1016/S0167-7012(00)00201-3

[11] Walczak, S., Cerpa, N. (2019). Advanced methodologies and technologies in artificial intelligence, computer simulation and human-computer interaction. A Volume in Advances in Computer and Electrical Engineering Information Resource Management Association, USA.

[12] Mizuno, H., Kosaka, M., Yajima, H., Komoda, N. (1988). Application of neural network to technical analysis of stock market prediction. Studies in Informatic and Control, 7(3): 111-120. https://doi.org/10.5815/ijisa.2012.11.08

[13] Jain, A.K., Mao, J., Mohiuddin, K.M. (1996). Artificial neural networks: A tutorial. Computer, 31-44.

[14] Kohonen, T. (1995). Self-organizing Maps. Springer Series in Information Sciences, Berlin, 30. https://doi.org/10.1007/978-3-642-56927-2

[15] Global Terrorism Database (GTD), https://www.start.umd.edu/gtd. (2009). University of Maryland. National Consortium for the Study of Terrorism and Responses to Terrorism. A Center of Excellence of the U.S. Department of Homeland Security. University of Maryland, USA.

[16] Soliman, G.M.A., Khorshid, M.M.H., Abou-El-Enien, T.H.M. (2016). Modified moth-flame optimization algorithms for terrorism prediction. International Journal of Application or Innovation in Engineering & Management, 5(7): 47-58.

[17] Mirjalili, S. (2015). Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. Elsevier, Knowledge-Based Systems, 89: 228-249. https://doi.org/10.1016/j.knosys.2015.07.006

[18] Mirjalili, S., Lewis, A. (2016). The whale optimization algorithm. Advances in Engineering Software, 95: 51-67. https://doi.org/10.1016/j.advengsoft.2016.01.008

[19] Soliman, G.M.A., Abou-El-Enien, T.H.M., Emary, E., Khorshid, M.M.H. (2018). A hybrid whale optimization algorithm with adaptive spiral for terrorism prediction (the case of Egypt). European Journal of Scientific Research, 149(2): 165-184.

[20] Soliman, G.M.A., Abou-El-Enien, T.H.M., Emary, E., Khorshid, M.M.H. (2018). A novel multi-objective moth-flame optimization algorithm for feature selection. Indian Journal of Science and Technology, 11(38): 1-13. https://doi.org/10.17485/ijst/2018/v11i38/128008

[21] Mirjalili, S., Andrew, L. (2014). Grey wolf-optimizer. Advances in Engineer Software, 69: 46-61. http://dx.doi.org/10.1016/j.advengsoft.2013.12.007