JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

A HYBRID ANN-PSO APPROACH FOR EMAIL SPAM DETECTION

Salahahaldeen Duraibi[1] and Nawaf A Almolhis[2]

[1]Department of Computer and Network Engineering, Jazan University, Jazan 82822-6649, Saudi Arabia

[2]Department of Computer science, Jazan University, Jazan 82822-6649, Saudi Arabia

Sduraibi@jazanu.edu.sa[1] and naalmolhis@jazanu.edu.sa[2]

Abstract

In today's world, technology extends into all areas of human life and emails is one of these technologies that expand communication platforms with suitable and inexpensive manner. Market organizations and advertising use these low-cost platforms to spread their desired information in the form of spam. To protect Internet users from spam danger, various strategies, tools, and techniques are presented. Therefore, this paper introduces a hybrid model, namely ANN-PSO which combines Artificial Neural Network (ANN) and Particle Swarm Optimization (PSO) for spam detection. The PSO is employed to pick most important features to be then used as inputs to the ANN model. The developed ANN-PSO model is assessed using several evaluation measurements and compared to ANN, k-Nearest Neighbor (KNN), Logistic Regression (LR) and Support Vector Machine (SVM) models. The results show that proposed ANN-PSO approach got a promising outcomes and achieved better performance than the other comparative models.

1. Introduction

E-mail messaging is one of the most widely used, most economical, and most effective methods of exchanging files and digital messages over the Internet. E-mail also has a significant role in many aspects of individuals' lives, as a form of both personal and public communication. Growth in e-mail use has changed the way people work and collaborate and has had a direct impact on business operations as well [1]. Spam refers to unwanted direct or indirect e-mails that could contain malicious messages or unsolicited commercial-related messages sent to a recipient having no relationship with the sender [2]. With one click and essentially no expense, it is feasible to send unsolicited messages to thousands of consumers worldwide. As a result, e-mail users around the world receive hundreds of spam messages daily through e-mail, Short Message Service (SMS), and mobile phones.

In an effort to either eliminate spam danger or lessen the enormous volume of spam that is delivered to individuals, a number of solutions have been devised. These strategies include using legislative measurements like anti-spam systems and filter [3]. Filtering approaches are the most widely used and common methods: Based on the presence of words associated with junk mail, the system examines the message's content and other aspects. [4] Other simplistic approach includes black-listing: rejection of messages from the addresses of known un-trusted

Submitted: 24/11/2022 **Accepted**: 14/12/2022

senders automatically and white-listing: automatic acceptance of messages arrived form trusted correspondents [5].

There is still an enormous amount of spam online nowadays despite the different tactics tried to counter the menace of email spam. In this context, spam emails can be considered as a serious threat to emails, and therefore, greater attention is required to eliminate the danger of spam. Due to this, there is an urgent need to develop smart techniques that have the ability to provide the essential facilities that make individuals, companies and organizations safe from spam and their negative consequences.

A wide range of studies from around the world have used machine learning (ML) and data mining approaches to create precise spam detection and filtering systems. These approaches aim to find optimum solutions for spam classification in an intelligent manner, Artificial Neural Network (ANN) was applied for email spam detection [6, 7, 8, 9]. The ANN was used with negative selection algorithm for email spam classification and it was confirmed to be effective and efficient compared to other techniques such as Support Vector Machine (SVM) [10]. The authors in [11], employed neural network for spam categorization. The authors used evasive patterns that spammers can employ to achieve their desired goals rather than the frequency of keywords or content in the message. In their experiment, 2788 legitimate and 1812 spam e-mails were used. Their findings showed that while ANN is effective, it should not be used by itself as a spam filtering method. In another study [12], the authors combined rectified linear units and neural network to differentiate between legitimate and spam classes. The achieved results were compared to other Machine Learning (ML) models. The ultimate results indicated good classification accuracy by the ANN was attained compared to other empirical ML models. In [13], Artificial Bee Colony (ABC) is used to choose the optimized subset from extracted set of features and then the selected ones are used as inputs to the ANN model. The results showed that ABC with ANN achieved biter results than SVM and Naïve bayes models for spam detection.

Several works have carried out using PSO method to extract and select the most important features to avoid processing overhead [14, 15, 16, 17]. In [18], the authors used the PSO to select the best features and eliminate irrelevant features for email categorization; the selected features are then used as inputs to Random Forest (RF) algorithm. The developed hybrid approach PSO-RF showed better performance compared to SVM, Naïve Bayes (NB) and k-NN. In another study [19], the authors presented Swarm Negative Selection Algorithm (SNSA) model. The PSO was applied to enhance defector generation in NSA and to gain better accuracy than using NSA alone. The experimental findings supported the higher performance of the improved approach.

In this paper, a hybrid approach by integrating ANN and PSO is developed to increase the accuracy of email spam detection. The PSO is used to find optimal feature subset and then the selected features are used as inputs to ANN model. The contribution of this work is to use the PSO algorithm to find the optimal features for ANN and to investigate the suitability of the combined PSO-SVM method for email spam classification. This paper consists of five sections.

Section 1 provides an introduction to email spam. Section 2 presents an overview of ANN, PSO and the dataset used in this work. Section 4 discusses the experimental results of this work. Finally, Section 5 presents the conclusion of this paper

.

2. Methods and Material

2.1.Artificial Neural Network (ANN)

ANN is employed in a variety of fields, including medicine, business, finance, electrical transformers, and energy [20, 21]. The most often used neural network structure is feed-forward multilayer perceptron.

As depicted in Figure 1, the network topology typically consists of three primary levels: input, output, and hidden layers. The input and output dataset serves as the basis for defining the input and output layers. The quantity of inputs reflects the quantity of input nodes, whereas the quantity of outputs denotes the quantity of output nodes. The major purpose of the hidden layers, which act as intermediary layers between the input and output layers, is to multiply each value entered by weights, which stand for predetermined numbers. The lines connecting the nodes show the direction of information flow from one node to the next.

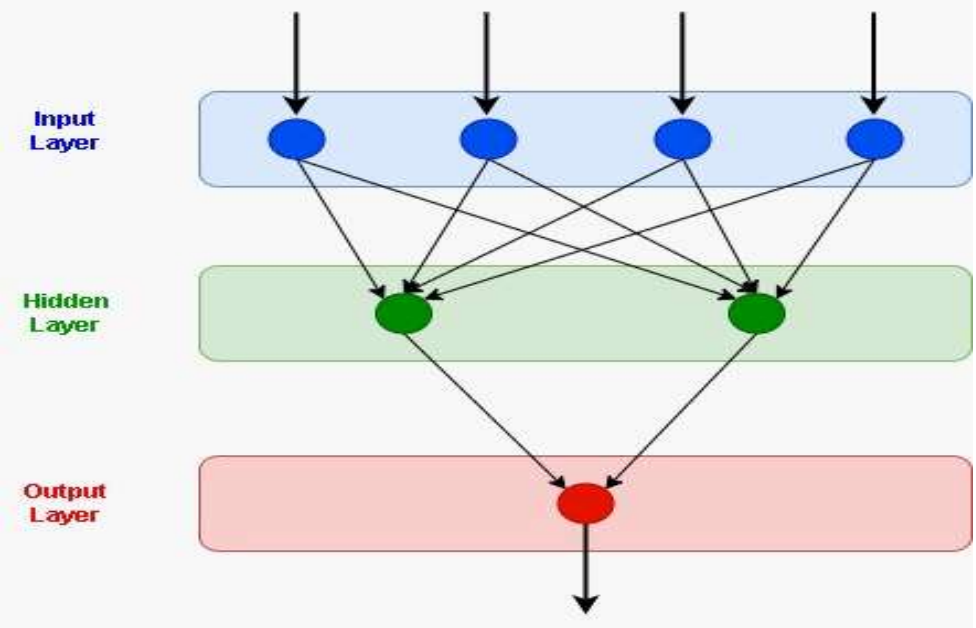


Figure **1** Multilayer neural network Architecture

It is possible to determine the outputs of each neuron activity in the hidden and the output layers can be computed as:

$$h_j = f(\sum_{i=1}^{n} w_{ij} x_i) \tag{1}$$

$$y_k = f(\sum_{j=1}^{i} w_{jk} h_j) \tag{2}$$

where h_j represents number of hidden node outputs, y_k is the output of output node, the function f is also known as the activation function, defines the rule for mapping a neuron's total input to its output.

2.2.Particle Swarm Optimization (PSO)

In an effort to comprehend and characterize how social animals adhere to global goals while performing individually, Kennedy & Eberhart [22], researched the behavior of social animals. The amount of particles needed for PSO must be determined in order to solve an issue. Each particle's optimal solution, position, and velocity are unique. The PSO method's core concept can be summed up as follows:

The i^{th} particle swarm position in a D space can be represented as follows:

$$X_I = \{X_{i1}, X_{i2}, \cdots X_{id}\} \tag{3}$$

Every particle keeps a record of its most recent ideal position. The following provides the ideal swarm position:

$$P_{gbest} = \{P_{g1}, P_{g2}, \cdots P_{gd}\} \tag{4}$$

The velocity can be represented as:

$$V_i = \{V_{i1}, V_{i2}, \cdots V_{id}\} \tag{5}$$

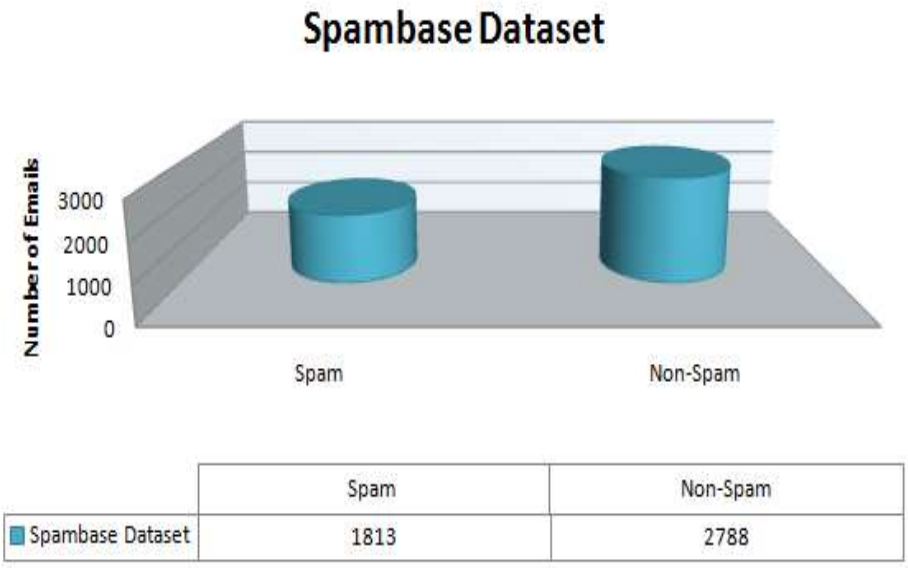
A particle velocity should be updated using:

$$V_{id} = w v_{id} + c_1 r_1 (p_{id} - x_{id}) + c_2 r_2 (p_{gd} - x_{id}) \tag{6}$$

where, r_1 and r_2 are random values between 0 and 1, and the parameters c_1 and c_2 are constants. The best local solution for the ith particle up to the ith iteration is called p-id, while the best overall solution for all particles is called p-gd. The impact of the particle's former velocity on its current one is controlled by the "inertia weight," orw. The particle gives more weight to the current best places if w value was less than 1, and it preferred searching over exploitation if w value was more than 1.

2.3. Used dataset

Several benchmark datasets available and can be used by researchers to develop and test spam classification. Spambase dataset was used and taken from UCI machine leaning repository[23] The dataset consists of 4601 emails; it contains (1813) messages marked as spam while the remaining (2788) belong to non-spam emails. The analysis of spambase dataset is presented in Figure 2.



	Spam	Non-Spam
Spambase Dataset	1813	2788

Figure 2. Spambase Dataset Analysis

3. Performance evaluation measurements

A classifier's performance and accuracy can be evaluated using a variety of metrics. The following statistical methods are used to assess the efficacy of the suggested method and alternative methods.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FN + FP} \tag{7}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{8}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{9}$$

$$\text{F1-score} = \frac{2\,P\,R}{P + R} \tag{10}$$

4. Experimental results and discussion

All the models are implemented using Python and are executed using 12GB NVIDIA Tesla P100 GPU and Intel Xenon CPU @ 2.00GHz with 13-GB RAM. The hyper-parameters settings of the ANN-PSO, ANN, KNN, LR and SVM models are provided in Table 1. These settings are assigned after we experimentally find that these are the best settings of parameters for training the models.

Table 1. Parameter settings

Model	Parameters
SVM	Regression cost = *1*, complexity bound = *0.5*, kernel= *Linear*
LR	Regression type = *Lasso (L1)*, Regression coefficient = *1*
kNN	k=*8*, Metric = *Euclidean*, Weight= *Distance*
ANN	Hidden layers = [*30, 4*], Activation= *ReLu*, Optimizer= *Adam*, Regularization= *0.0001*, Epochs=*200*
PSO-ANN	Population=*30*, Max. iteration=*100*, Hidden layers= [*25, 4*], Activation= *ReLu*, Optimizer= *Adam*, Regularization= *0.0001*, Epochs=*200*

The Spambase dataset was split into two portions, because of the large number of samples connected to the datasets: 70% were used for training, and the remaining 30% for testing and validating. The performance and accuracy evaluation measures in equations (7)–(10) were applied to the PSO-ANN. The convergence behavior of PSO is depicted in Figure 3. This figure demonstrates that the PSO is suitable for usage as a feature selection approach and has a good

convergence speed over 100 iterations.

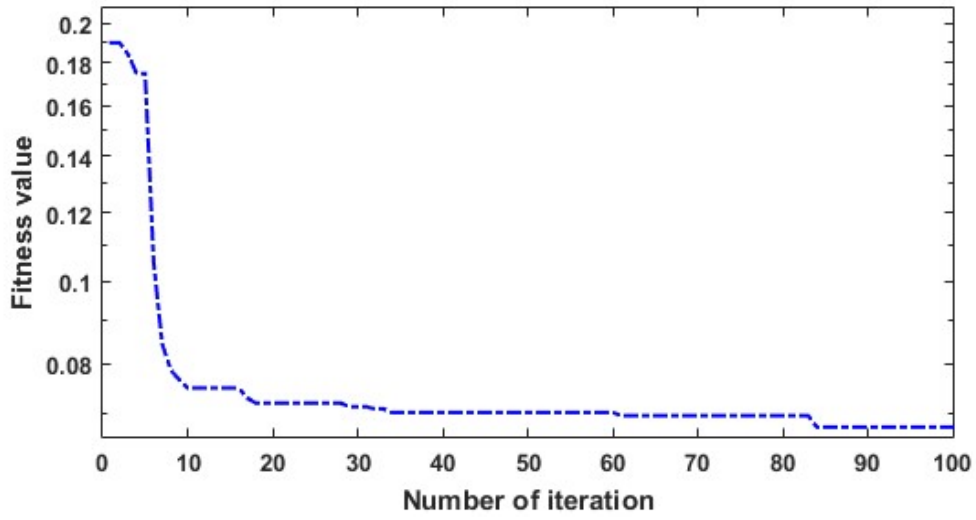
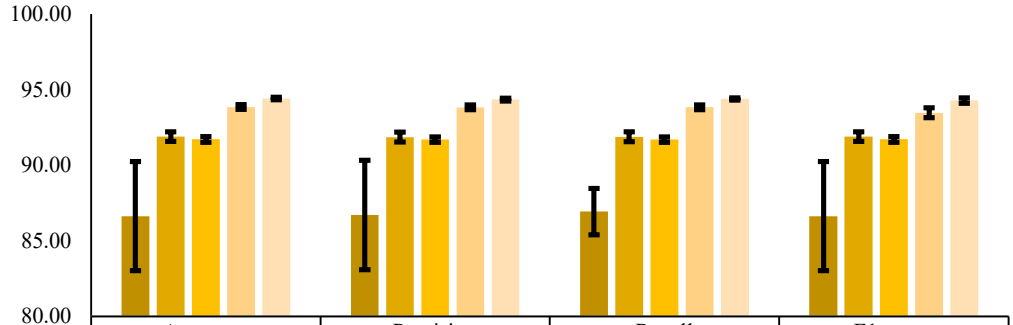


Figure. 3. Convergence behavior of PSO using Spambase dataset for spam detection.

Figure 4 displays the outcomes in terms of the employed evaluation measurements. As can be observed in this chart, the suggested ANN-PSO outperforms all other measures. This demonstrates that it is suitable as a model for spam detection



	Accuracy	Precision	Recall	F1-score
SVM	86.63	86.71	86.94	86.63
LR	91.89	91.86	91.88	91.89
kNN	91.71	91.69	91.69	91.71
ANN	93.85	93.83	93.84	93.47
PSO-ANN	94.41	94.34	94.38	94.28

Figure 4. Quantitative comparison of proposed ANN-POS and other models using Spambase dataset.

5. Conclusion and future works

Spam messages, particularly spam emails, are a constant threat to internet users and for this, researchers conducted a number of studies to identify and defense against spam danger. The

protection of Internet users from spam has addressed using a variety of strategies, tools, and techniques. The purpose of this work is to present ANN-PSO, a hybrid technique that combines ANN and PSO to enhance the effectiveness of email spam classification. The PSO method is used to choose main features in Spambase dataset and then use selected features as inputs to the ANN model. The suitability level of the ANN-PSO is evaluated using several evaluation measures and its effectiveness is compared to other models including ANN, KNN, LR and SVM. The outcomes showed that the suggested ANN-PSO produced good results and outperformed the other models for spam identification. In future, will plan to use ANN-PSO in different applications such as intrusion detection, signal processing and big data. Another possible avenue is to work on metaheuristic methods to be applied as a FS in the application of spam detection, because these optimization algorithms have shown great potential in other domains

References

[1] Kumar, N., & Sonowal, S. (2020, July). Email spam detection using machine learning algorithms. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 108-113). IEEE.

[2] Kumar, N., & Sonowal, S. (2020, July). Email spam detection using machine learning algorithms. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 108-113). IEEE.

[3] Bhuiyan, H., Ashiquzzaman, A., Juthi, T. I., Biswas, S., & Ara, J. (2018). A survey of existing e-mail spam filtering methods considering machine learning techniques. Global Journal of Computer Science and Technology.

[4] Wiehes A, Master Thesis, “Comparing anti-spam methods”, Master of Science in Information Security, Department of Computer Science and Media Technology, Gjovik University College, 2005.

[5] Qi, M., & Mousoli, R. (2010, August). Semantic analysis for spam filtering. In 2010 Seventh International Conference on Fuzzy Systems and Knowledge Discovery.

[6] Özgür, L., Güngör, T., & Gürgen, F. (2004). Adaptive anti-spam filtering for agglutinative languages: a special case for Turkish. Pattern Recognition Letters, 25(16), 1819-1831.

[7] Behjat, A. R., Mustapha, A., Nezamabadi-pour, H., Sulaiman, M. N., & Mustapha, N. (2013). A PSO-Based Feature Subset Selection for Application of Spam/Non-spam Detection. In Soft Computing Applications and Intelligent Systems (pp. 183-193). Springer Berlin Heidelberg.

[8] Ghaleb, S. A., Mohamad, M., Abdullah, E. F. H. S., & Ghanem, W. A. (2021). Spam classification based on supervised learning using grasshopper optimization algorithm and artificial neural network. In International Conference on Advances in Cyber Security (pp. 420-434). Springer, Singapore.

[9] Bansal, C., & Sidhu, B. (2021, September). Machine Learning based Hybrid Approach for Email Spam Detection. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-4). IEEE.

[10] Idris, I. (2011). E-mail spam classification with artificial neural network and negative selection algorithm. Int J Comput Sci, 1(3), 227-231.

[11] Puniškis, D., Laurutis, R., & Dirmeikis, R. (2015). An artificial neural nets for spam e-mail recognition. Elektronika ir Elektrotechnika, 69(5), 73-76.

[12] Barushka, A., & Hájek, P. (2016). Spam Filtering Using Regularized Neural Networks with Rectified Linear Units. In AI* IA 2016 Advances in Artificial Intelligence (pp. 65-75). Springer International Publishing.

[13] Singh, A., Chahal, N., Singh, S., & Gupta, S. K. (2021, January). Spam detection using ANN and ABC Algorithm. In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 164-168). IEEE.

[14] Zhang, Y., Wang, S., Phillips, P., & Ji, G. (2014). Binary PSO with mutation operator for feature selection using decision tree applied to spam detection. Knowledge-Based Systems, 64, 22-31.

[15] Bahgat, E. M., Rady, S., & Gad, W. (2016). An e-mail filtering approach using classification techniques. In The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), November 28-30, 2015, Beni Suef, Egypt (pp. 321-331). Springer International Publishing.

[16] Idris, I., Selamat, A., Nguyen, N. T., Omatu, S., Krejcar, O., Kuca, K., & Penhaker, M. (2015). A combined negative selection algorithm–particle swarm optimization for an email spam detection system. Engineering Applications of Artificial Intelligence, 39, 33-44.

[17] Idris, I., & Selamat, A. (2014). Improved email spam detection model with negative selection algorithm and particle swarm optimization. Applied Soft Computing, 22, 11-27

[18] Faris, H., Aljarah, I., & Al-Shboul, B. (2016, September). A Hybrid Approach Based on Particle Swarm Optimization and Random Forests for E-Mail Spam Filtering. In International Conference on Computational Collective Intelligence (pp. 498-508). Springer International Publishing.

[19] Idris, I., & Selamat, A. (2015). A Swarm Negative Selection Algorithm for Email Spam Detection. J Comput Eng Inf Technol 4, 1, 2.

[20] Al-Janabi S,Rawat S, Patel A, Al-ShourbajiI (2015) Design and evaluation of a hybrid system for detection and prediction of faults in electrical transformers. International Journal of Electrical Power & Energy Systems 67: 324-335

[21] Damour, C., Benne, M., Grondin-Perez, B., & Chabriat, J. P. (2010). Nonlinear predictive control based on artificial neural network model for industrial crystallization. Journal of Food Engineering, 99(2), 225-231.

[22] Kennedy, J.; Eberhart, R. (1995). "Particle Swarm Optimization". Proceedings of IEEE International Conference on Neural Networks. pp. 1942–1948.

[23] Hopkins, M., et al., 1999. Spam Base Dataset. Hewlett-Packard Labs

.