# SPAM DETECTION SYSTEM USING MACHINE LEARNING TECHNIQUE

Atul Khosla*, Priyanka Dayal

Division of research and development, Lovely Professional University, Phagwara, Punjab 144411, India.

**Abstract**

It is a normal practice for e-commerce Web sites to authorize their customers to write good reviews that they have get. Such comments present significant information source on these goods. They are utilizing by an intrinsic user to decide opinions of presented users before selecting to pay money for a product. They are also employed by manufactured goods producers to identify problems of their goods and to find out competitive intellect data about their opponent. In this research work, we develop a Spam detection system for different communities such as social, recommendation, Movies, and religious information. The weighted values are generated for all the mentioned categories. ANN (Artificial Neural Network) is used to classify the spammer present in the communities. The performance of the system has been evaluated by considering different parameters such as true positives, true negatives, precision, and recall.

**Keywords:** Spam, artificial neural network, MATLAB.

## I. Introduction

For the last couple of years, mobile spam messages have been a constant problem in remote East countries. Also, it has been observed that the increasing number of spam messages increases the spam emails. In few countries, legal action is taken for overcoming this spam problem. Email is one of the fastest, simplest and most traditional medians of communication. Millions of peoples use email every day and become the cause of changing the working style and life of users. The purity of email performs it vulnerable to various threats [1]. The most common threats that are found to email is spam (any undesirable marketing communication). The extension of spam transfer is becoming a disturbing problem since it utilizes the bandwidth (B.W) of the system, consumes memory and time of users and creates the financial loss to the users as well as the organizations. The spammers use a number of methods for gathering e-mail address records [2]. For example, marketers collect e-mail addresses from postings on several Internet Sites like newsgroup sites, chat room Sites, catalogue Services sites, and by recognizing “mail to' address link displayed on web pages [3]. Using these methods and other similar techniques, electronic mass marketers might be efficiently obtained large amounts of mailing addresses that become victims for their advertisements and other undesired information. The main aim of this research work is to design an algorithm that can effectively distinguish between spam and non spam [4]. The features of e-mail are extracted and stored in the database. For identifying spam email, we have to train our system in such a way so that the system can differentiate between the spam and non spam emails [5]. In the proposed research work, artificial neural network (ANN) algorithm is used for classification purpose [6]. For detecting spam the steps used to identify the spam are discussed below.

### 1.1 Spam detection system

In the proposed research work, we are designing a spam detection system for four numbers of communities named as Community 1, community 2, community 3 and community 4. These four communities include data related to movies, recommendation, religious and social respectively [7].

The figure 1 represents the work layout of the proposed work. There are two sections in the work layout namely training and classification. The training part contains Feed Forward Back propagation neural network, 4 community values, the generator function which generates the numeral values of the words passed to each community.


**Fig. 1 GUI of proposed work**

In the recommendation system [8], the data is collected from various online shopping sites. Before purchasing any product, the user always checks the reviews about the related product. Thus by comparing the quality of the product based on the reviews and cost the user purchase the product [9]. The system is developed in such a manner that it can distinguished between fake reviews. The community that is used in the proposed work is social network. The 'Social Network" helps user to remain connected with friends. The most commonly used social sites are Face book and Twitter that are visited by most of the users through Smartphone at any place[6]. The spam has been detected in social network by extracting the features and then generating the token values [10].

## II. Research Methodology

The research focuses on identifying the spam classification technique using Artificial Neural Network (ANN) [11]. The algorithm of ANN is shown below.

**Algorithm: ANN Algorithm**

**Input:** Training_data, Group and Neurons

**Output:** Trained ANN Structure

Training_data = Feature of spam data

Generate group of data = Group (G) according to spam type

Initialize ANN = newff (Training_data, G, N)

Set iteration = 50

**For I = 1 to iteration**

Weight = Training_data (i)

Hidden_Neurons = [N] (tansig)

Net_algo = trainlm

Generat Net structure of ANN (net)

Net = train (net, Training_data, G)

**End**

**Return**; Trained ANN Structure

**End** Function

### 2.1 Flowchart

The steps undertaken to execute the simulation work are defined below:

Step 1: Load dataset for training and testing.

Step 2: Calculate feature as a weighted value for both training

Step 3: Trained data using Artificial Neural Network (ANN) and save in database.

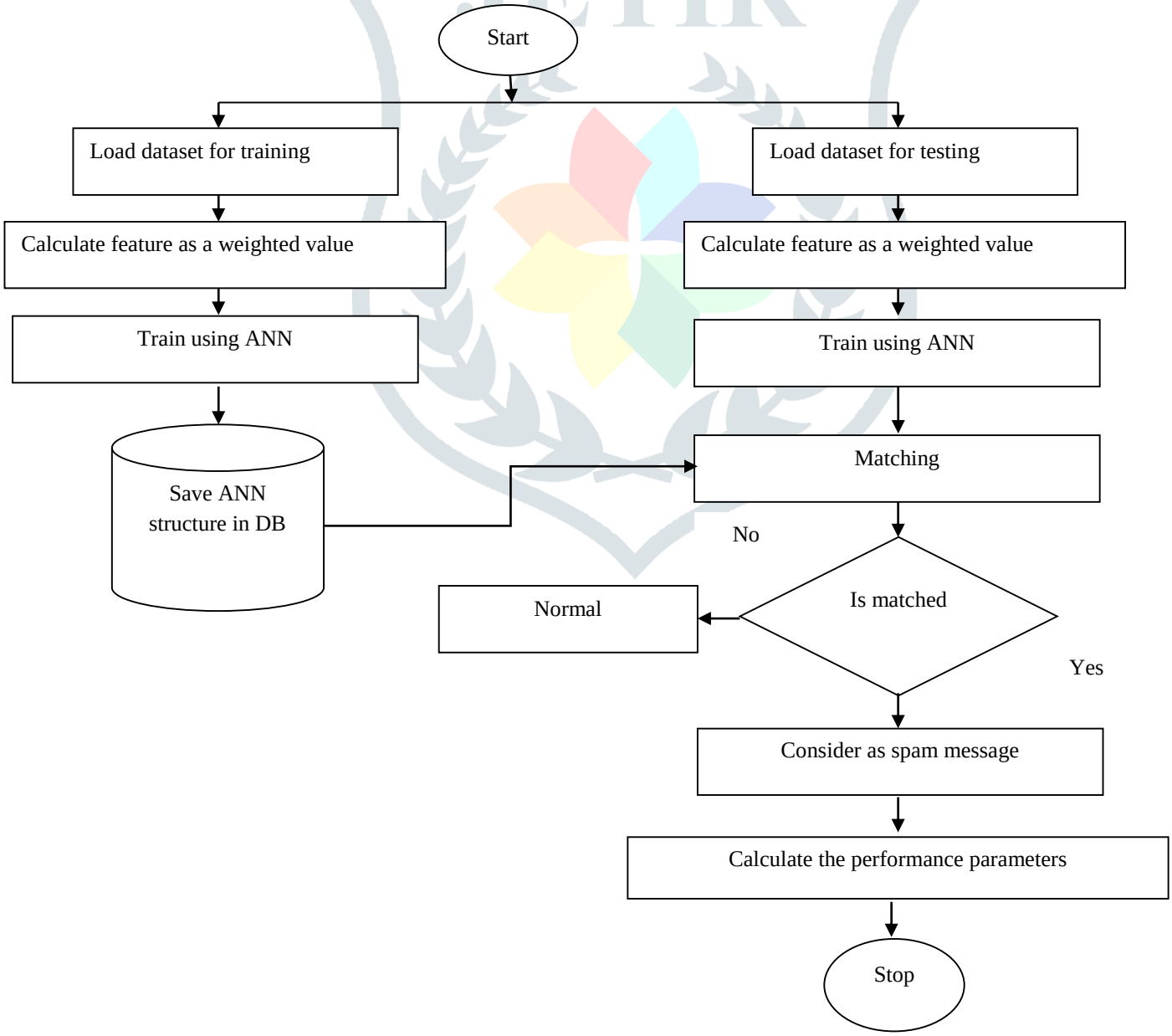


**Fig.1: Methodology of the proposed work**

As depicted, the training phase requires each incoming message to be treated as a text file, thereafter the message is passed for identification of header information (namely; From, Received, Subject, or to) and for differentiating it from the main message to be conveyed. Here, simulation is done by implementing Artificial Neural Network.

## III. Simulation results

The results obtained for the designed spam detection are discussed in detail. In order to calculate the efficiency of the proposed design, the performance parameters mainly precision, recall, true positive and true negative are measured.

**Table 2: Simulation results using Artificial Neural Network (ANN)**

| No. of iterations | Precision values | Recall values | True positive values | True negative values |
|---|---|---|---|---|
| 1 | 1.421 | 1.32 | 0.0007975 | 0.00058389 |
| 2 | 1.323 | 1.28 | 0.0007768 | 0.00057975 |
| 3 | 1.31 | 1.34 | 0.0007689 | 0.00058375 |
| 4 | 1.20 | 1.25 | 0.0007975 | 0.00058396 |
| 5 | 1.47 | 1.30 | 0.0008096 | 0.00056874 |
| 6 | 1.33 | 1.36 | 0.0007832 | 0.00054568 |
| 7 | 1.47 | 1.40 | 0.0007875 | 0.00059679 |
| 8 | 1.40 | 1.47 | 0.0007965 | 0.00059242 |

## IV. Conclusion

In the proposed work, four different categories for spam detection named as Social, Film industry, Religious and recommendation are created. Then, their stop words are generated for different categories and Token values are created. The neural network has been used as a classifier to detect the spam in four different categories. The parameters named as percentage error has been measured. The computed value of % error obtained is 3.8392%. From the above discussion, it is concluded that the ANN classification technique provides better results when compared with existing techniques.

In future, we can combine ANN classification technique with optimization algorithm so that the QoS performance of the proposed work can be improved. Even other spam filtering techniques can be used along with machine learning algorithm so that the identification of spam can be enhanced.

## References

[1]. H. Faris, A. Z. Ala'M, & I. Aljarah, “Improving email spam detection using content based feature engineering approach”, *IEEE Jordan Conference on* pp. 1-6, October ,2017.

[2]. S. H Seyyedi, & B. Minaei-Bidgoli, “Estimator learning automata for feature subset selection in high-dimensional spaces”, case study: Email spam detection. *International Journal of Communication Systems*, 2018.

[3]. M. ZhiWei, M. M Singh, & Z. F Zaaba, “Email Spam Detection: A Method Of Metaclassifiers Stacking”, In The 6th International Conference on Computing and Informatics pp. 750-757, 2017.

[4]. U.K Sah, & N. Parmar, “An approach for Malicious Spam Detection”, In Email with comparison of different classifiers, 2017.

[5]. A. E. Skudlark, J. Erman, Y. Jin, A. Srivastava, & L.K Tran, U.S. Patent No. 9,584,989. Washington, DC: U.S. Patent and Trademark Office, 2017.

[6]. G. Jain, M. Sharma, & B. Agarwal, "Spam detection on social media using semantic convolutional neural network", International Journal of Knowledge Discovery in Bioinformatics (IJKDB), 8(1), 12-26, 2018.

[7]. Y. Ren, & D. Ji, "Neural networks for deceptive opinion spam detection: An empirical study", Information Sciences, 385, 213-224, 2017.

[8]. P. Sethi, V. Bhandari, & B. Kohli, "SMS spam detection and comparison of various machine learning algorithms", In Computing and Communication Technologies for Smart Nation (IC3TSN), 2017 International Conference on pp. 28-31, IEEE, October, 2017.

[9]. D. Basaran, E. Ntoutsi, & A. Zimek, "Redundancies in Data and their Effect on the Evaluation of Recommendation Systems", A Case Study on the Amazon Reviews Datasets. In Proceedings of the 2017 SIAM International Conference on Data Mining, pp. 390-398, Society for Industrial and Applied Mathematics, June, 2017.

[10]. S. Mahajan, & V. Rana, "Spam Detection on Social Network through Sentiment Analysis", Advances in Computational Sciences and Technology, 10(8), 2225-2231, 2017.

[11]. A. J. Choobbasti, F. Farrokhzad, & A. Barari, "Prediction of slope stability using artificial neural network", case study: Noabad, Mazandaran, Iran, Arabian journal of geosciences, 2(4), 311-319, 2009.