International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Email Spam Detection using Recurrent Neural Network

T. Veda Reddy,
Department of Computer Science and Engineering, Anurag Group of Institutions, India
vedareddy@cvsr.ac.in

Mr. T. Vinay Kumar,
Department of Computer Science and Engineering, Anurag Group of Institutions, India
Tedlavinay4@gmail.com

Ms. T. Laxmi Keerthi,
Department of Computer Science and Engineering, Anurag Group of Institutions, India
Thumburukeerthireddy0240@gmail.com

Mr. Calvin Johnson Joseph.
Department of Computer Science and Engineering, Anurag Group of Institutions, India
calvinjohnson747@gmail.com

ABSTRACT

Email is one of the mobile communication services that allows easy and inexpensive communication. Producing unwanted messages with the aim of advertising or harassment and sending these messages on Email have become the biggest challenge in this service. Various methods have been presented to detect unsolicited short messages; many of which are based on machine learning. Neural Networks have been applied to separate the unwanted text messages known as spam from normal short messages known as ham in Email. To the best of our knowledge, Recurrent Neural Network (RNN) has not been used in this issue yet. In this paper, we proposed a new method which utilizes RNN to separate the ham and spam with variable length sequences, even though we used a fixed sequence length. The proposed method, indicates a considerable improvement compared to Support Vector Machine SVM, token-based SVM and Bayesian algorithms. There are two main types of methods to detect unwanted EMAIL: techniques along with user participation and content-based methods. Methods based on user participation are based on feedback from users and sharing their experiences. Because of the problems associated with data access and user experience, these methods are rarely used, but content-based methods act based on content analysis of text messages and are more common.

Keywords—Email, RNN, Machine Learning, spam detection, Neural Networks.

1. INTRODUCTION

This project aims to provide users with accurate predictions of spam and ham mails based on parameters obtained by spam.csv. The project aspires to reach three key milestones. The first milestone being, outperforming message prediction score or come close to it. The second milestone is to get rid of an overestimation problem. The final milestone is to narrow down the most influencing factors affecting the mails. To reach these milestones

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

the project proposes to use both recurrent neural network and various machine learning algorithm. One particular reason is that there many factors that influence the potential of a mail, making it more complicated for an individual to decide how to find a spam mail on their own without external help. This can lead to people making poorly informed decisions about whether the mail received by them is a ham or spam. Because mails cannot be predicted, it is imperative that people make their decisions with the most accurate information possible. Objective of this system is to predicted unwanted messages accurately using Recurrent Neural Network (RNN). Innovations in this project are the Use of methods that apply pre-processing actions as a part of algorithm. Show higher accuracy with the increase in the number of layers of neural networks used. Moreover, the recursive nature of this algorithm has made it suitable for sequential data and effective in achieving high accuracy of the algorithm. This system has uses RNNs to predict whether messages are unwanted or normal. The architecture used in this project is RNN. It consists of a sequence of inputs from a marked text to RNN, and classifies the last output of RNN according to its zero or one value as an unwanted or normal text message. After entering the tokens to the initial state, they are applied to central functions of hidden layer, and determined in the last layer of the intended output, which is in fact the class related to entering data. Based on RNN, the proposed method in this system achieved an good accuracy, which suggests a considerable improvement compared to the SVM, token-based SVM, and Bayesian algorithms, which were used in the most recent studies.

2. EXPERIMENTAL

There are many architectures based on machine learning require a sufficient amount of training data used for categorizing labelled models. Ahmed et al. have offered a monitoring strategy that has used Bayes algorithms with Appriori for classification of short messages. Nejadet et al. have offered a new classification algorithm that uses the combination of classification algorithms without change in the original algorithm to obtain better performance. A variety of clustering techniques are used for the detection of unwanted short message in email. One of the first studies in this regard concerns using SVM. Gomez et al. used a similar classification method that uses Information Gain (IG) to choose the marks. Logzhen et al used a k-nearest neighbour algorithm along with other methods of detection of unwanted message on a data set containing 750 cases of unwanted and normal short messages. Liu and Wang used the recurrence of some text units as input parameters to Bayesian classification algorithms, k-nearest neighbours, SVM and so on. Almeida et al. tested 13 classification algorithms on a data set of more than 5500 mail messages 4827 normal mails. Their results show that SVM with alphabetic marking has the best performance. Alphabetic marking includes separating alphabetic and non- alphabetic characters. Finally, they extracted 8100 marks from SMSs. Delaney et al changed the methods and data sets used in the study by Almeida et al. This study focused on factors of assessment of categories of unwanted EMAIL messages.
This is where machine learning comes into play. The prediction system can learn from the dataset to teach itself to refine its parameters and make data driven predictions. The ability of the brain to process huge volumes of information in a short time, the use of parallel structure in data analysis, and the remarkable ability of the human brain in

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

learning various issues are special features. Therefore, simulation has always been tempting, and deep neural networks have been created for this purpose. Among all machine learning algorithms, Deep Recurrent Neural Networks work on data sequence. Sequential data are data whose current values depend on previous values. Among such data, the following can be noted. Frames of speech signal Continuous Frames of Video Climatic condition. The stock price of a company. The sequences generated by the grammar Words within a text RNNs are very powerful because of combining the following features. Distributed hidden layers, which allow them to save a lot of information about previous layers. Non-linear dynamics, which allows such networks to update hidden layers in a complex way. RNNs have the potential to provide implementation and enforcement for small and parallel programs, and thus have a great interaction for producing more complicated results. With the number of neurons at hand and enough time, RNNs have the ability to do any calculations performed by a computer.

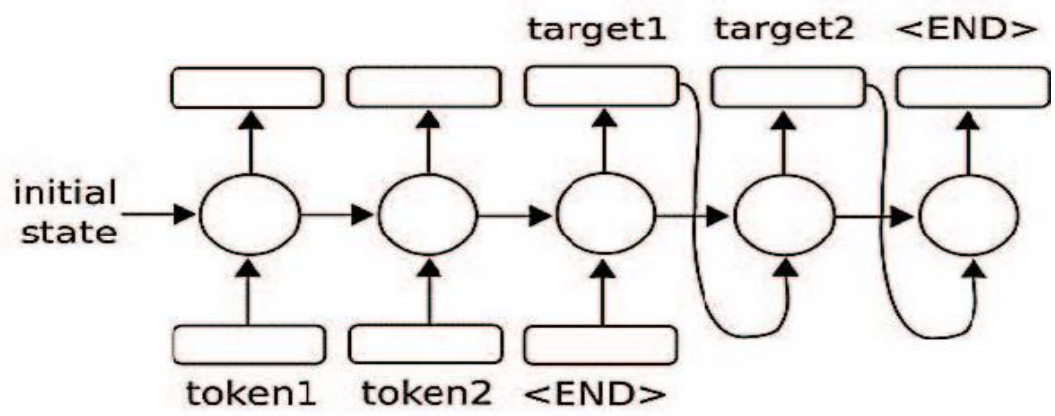

Fig 1.1

3. RESULTS AND DISCUSSION

To prepare the dataset for the prediction system, some changes were made: There are few data sets to predict spam in short message service systems, among which UCI datasets are used in most studies. In this study, we have used RNNs as an appropriate classifier algorithm on this dataset. Thus, in this section of the paper, we first introduce this data set briefly. Then we explain the quality of performing the experiments, where the results on this data set in classification show satisfactory improvement. A. Data set used The dataset used in this study are of dataset prepared in UCI known as UCI SMS Spam , and the dataset includes 5574 SMS labeled classified into two groups: 747 SMS messages are unwanted and 4827 SMS messages are normal SMS messages or an SMS message with the user's consent. As it can be seen in system. some of the statistical characteristics of the messages in the dataset employed in this paper.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

For the implementation of the proposed method, similar to many machine learning algorithms, we have considered a training algorithm, a cycle or a period of applying algorithm on all training vectors which called epoch. The proposed method has been implemented for a number of different epochs listed in the results. The parameters considered in this study are shown. One method which is used to increase the accuracy is batching data. In this paper, it was chosen as 25. This means that in each entry in a batch with 25 sequences of words, and the maximum size of each word sequences, we have adopted to be 25. In this system we have considered 100 for rnn_size, and each word in a training vector got a size of 50. Learning rate considered in this article is 0.0005. In the simulations carried out in this paper, 70% of the data, i.e. 3901 records as training and 30% of data, equivalent to 1673, as the test are used in the system.

Software Requirements:

- OS : Windows
- Python IDE : Python 2.7.x and above
- IDE : Pycharm

Library Requirements:

- NUMPY: A fundamental package for scientific computing in python
- PANDAS: A data structure and data analysis tool.
- MATPLOTLIB: A 2D plotting library.
- SCIKIT-LEARN: A machine learning package for python.

Hardware Requirements:

- RAM : 4GB and Higher
- Processor : Intel i3 and above
- Hard Disk : 500GB

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

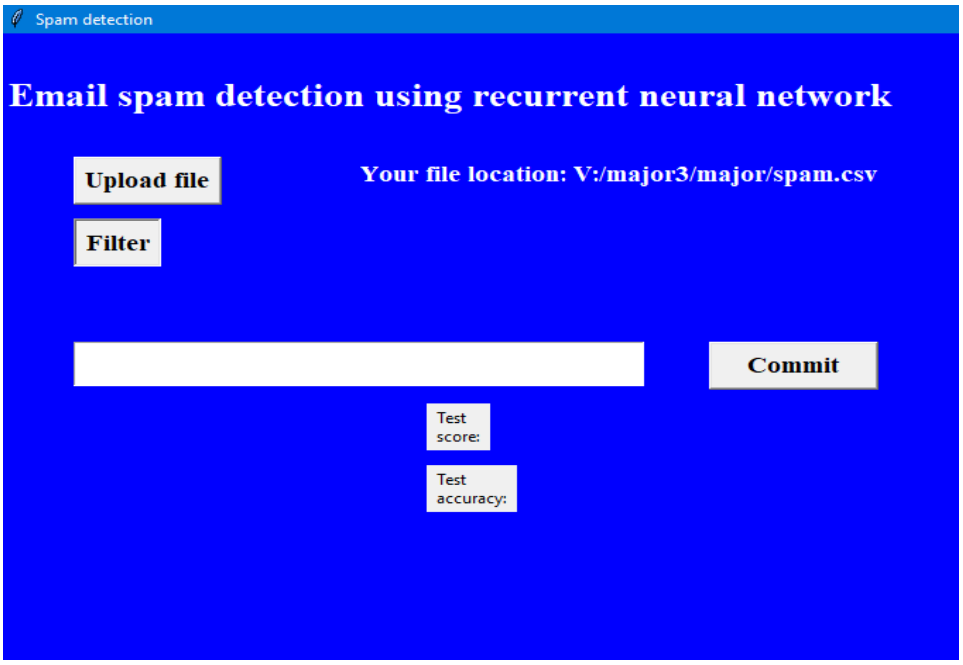

Fig 2.1

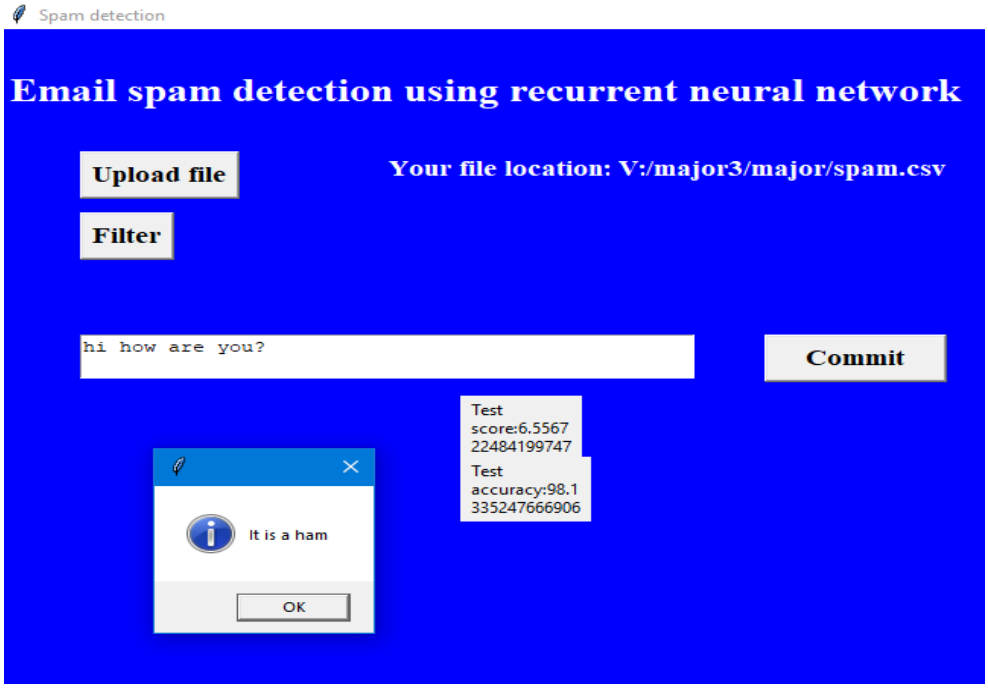

Fig 2.2

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

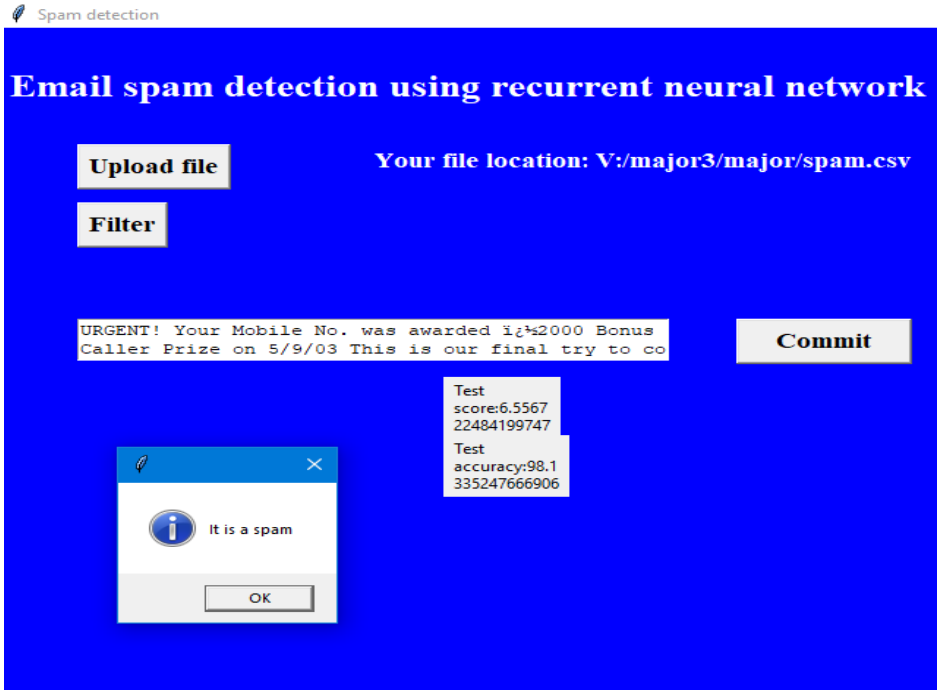

Fig 2.3

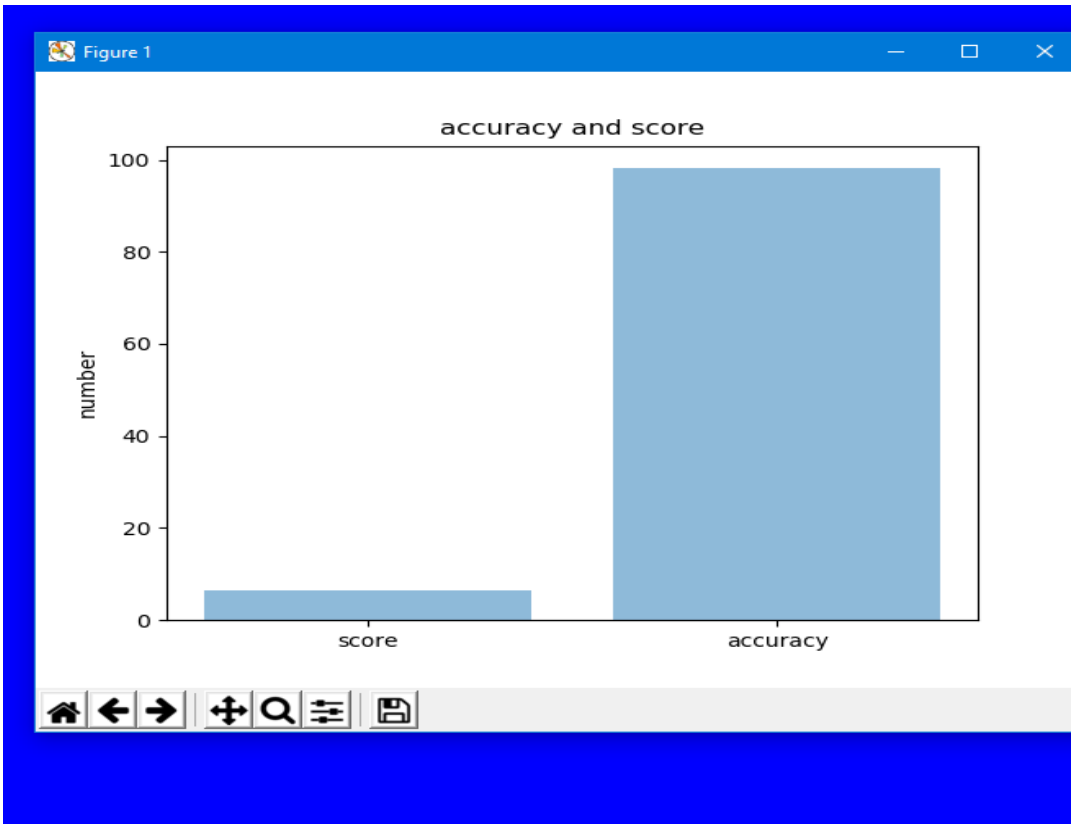

Fig 2.4

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

4. CONCLUSION

In previous systems, a classification method is provided for detecting unwanted and normal messages. So far, in the previous studies, SVM or Bayesian methods is used. The proposed method RNNs is used. Test results on standard datasets UCI SMS spam showed the efficiency of the proposed method. In the proposed method, after 100 initial epochs, when a steady state is observed, a high accuracy of 98% is obtained has not achieved so far in any other researches, and increase the number of epochs of the algorithm implementation will not impact of the result. The proposed method in this paper considers the pre-processing stage part of the classification algorithm and offers a higher accuracy compared to the most recent studies. Moreover, the proposed method can be used an appropriate alternative to the previous methods considering its acceptable runtime The success of our approach to creating a web application for generating predictions can be applied to other problem sets concerned with geographical variations in the prediction model. Despite having produced a working application that met our initial require-ments, there are various improvements that can be made in the future. These include improvements we did not make due to limited time on the project, and suggestions provided by users after using our web application. We still aim to apply a GUI which allows the user to input their values.

5. REFERENCES

1. P. Sethi, V. Bhandari and B. Kohli, "SMS spam detection and comparison of various machine learning algorithms," in International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, 2017
2. Karami and L. Zhou, "Improving Static SMS Spam Detection by Using New Content-based Features," in Twentieth Americas Conference on Information Systems, Savannah, 2014
3. F. Akbari and H. Sajedi, "SMS spam detection using selected text features and Boosting Classifiers," in 2015 7th Conference on Information and Knowledge Technology (IKT), Umia, 2015
4. H. Shirani-Mehr, "SMS Spam Detection using Machine Learning Approach," [Online]. Available: http://cs229.stanford.edu/proj2013/ShiraniMehr-SMSSpamDetectionUsingMachineLearningApproach.pdf. [Accessed 27 August 2018].
5. N. K. Nagwani and A. Sharaff, "SMS spam filtering and thread identification using bi-level text classification and clustering techniques," Journal of Information Science, vol. 43, no. 1, pp. 75-87, 2017.
6. Barushka and P. Hajek, "Spam filtering using integrated distribution-based balancing approach and regularized deep neural networks," Applied Intelligence, vol. 48, no. 10, pp. 3538-3556, 2018.