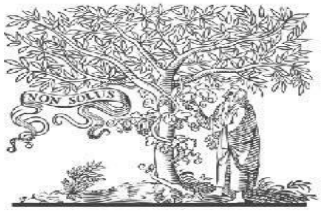
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/110

Title SPAM MESSAGE CLASSIFICATION

Volume 12, ISSUE 04, Pages: 876-883

Paper Authors

Mr.K.Parishuddha Babu, Illuri Sireesha, Hari Rasajna, Gali Annie Preni

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SPAM MESSAGE CLASSIFICATION

Mr.K.Parishuddha Babu[1] ,M.Tech, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Illuri Sireesha[2], **Hari Rasajna[3]**, **Gali Annie Preni[4]**
UG Students, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
kpbabuvvit@gmail.com[1], isireesha17203@gmail.com[2], tararasajna@gmail.com[3],
nirmalaburri19@gmail.com[4]

Abstract

Smart technologies, especially cell phones, are widely utilised for communication in today's society. Unfortunately, the overuse of SMSs has resulted in a rise in spam messages, which are unwelcome and frequently include useless information. Numerous businesses use SMSs to advertise their goods and services, which leads to more spam messages than actual messages. In this study, we suggest filtering and classifying SMSs as either spam or not using text classification approaches, such as machine learning algorithms. By doing this, we hope to give a succinct description of the spam filtering procedure. The report also discusses OCR and the use of several classification techniques to spot spam communications. The images of user-provided messages are also pre-processed using the optical character recognition (OCR) approach.

Keywords: Spam Messages, Classification, Spam Filtering, OCR

Introduction

Data science is an associative discipline that uses experimental methods, algorithms, procedures, and systems to gather crucial information and observations from a variety of structured and disorganised data. It is related to data mining, deep learning, and big data. The purpose of the computer science discipline known as "data mining" is to analyse unusable data and turn it into useful knowledge. Also, the system mostly used data to extract information. There are numerous techniques for such, including classification, clustering, and many others. SMSs are short message services. You can only send 160-character messages by SMS, and you must break up long texts into many smaller messages. Short text messages might be exchanged between cell phones using the established communication protocols. The government wants to keep up with the rapid technological change.. The lowest SMS rates have made it possible for customers and service providers to move away from the issue and limited availability of spam filtering apps for mobile devices. In this paper, we demonstrate a few techniques for classifying things. To determine if text messages are spam or not, we employ

classification algorithms. There must be a training set with the materials at this location. Texts sent by individuals indicate that these messages are coming from human class or mobile phone firms to advertise their products. Due to voice mail messages being regularly utilised, mobile phones or smartphones are generally a communication device and are used by people in a wide range. Due to the fact that SMS spam datasets are typically small in size, email filter spam has a greater number of datasets than SMS spam. Due of the small size of spam SMS, the email spam filtering system's filtering scheme could not be applied to SMS. Email spam is less common than SMS spam in some countries, including Korea. However, in western regions, the opposite strategy was used, with email spam being more prevalent due to its lower cost than SMS spam, which is more expensive and infrequent. On mobile devices, about 50% of SMS messages are received as text messages and are flagged as spam. We used ham and spam as real data in our analysis. We use a number of categorization methods, some of which were used in earlier research and some of which were novel, and spam messages are typically generated by organisations and analysis. The system primarily uses techniques like classification and clustering to extract knowledge from data. Text messages can be exchanged between mobile devices utilising Short Message Services (SMS) and industry-standard protocols. While being an issue, SMS spam is not as common as email spam. To solve this problem, we use classification algorithms to determine whether or not text messages are spam. SMS is the main topic of this study because it includes text messages. Messages are classified as either human or spam using classification algorithms. Applying email filtering techniques to SMS is difficult since SMS spam datasets are smaller than email spam datasets in size. An SMS filtering system should reserve resources using mobile phone hardware to address this problem.

Literature Survey

Many approaches for building the spam filter has been proposed. Each having their own advantages over previous ideas and disadvantages with respect to the current approach.

1.Research on SMS Spam Filtering

The increased usage of mobile devices has led to a sharp rise in the number of SMS spam messages. Yet, there are a number of reasons why countering mobile phone spam is difficult, including the low SMS message rate that has caused many users and service providers to ignore the problem and the scarcity of mobile phone spam-filtering software. The lack of publicly available datasets for SMS spam presents a significant challenge for the evaluation and comparison of various classifiers in academic contexts. Furthermore, since SMS messages are often brief, efficiency of content-based spam filters may be impacted.

2.A Novel Method for Classifying Spam Text Messages

In this work, a dual-filtering strategy for SMS texts is suggested. To separate spam messages from real messages, the KNN classification algorithm and rough set are first combined. Certain messages are re-filtered using the KNN classification algorithm to avoid precision erosion. Based on a basic set of the KNN classification algorithm, this technique not only increases classification speed but also retains excellent accuracy.

3.SMS Spam Filtering System Using Support Vector Machine

This work presents a robust and flexible SMS (Short Messaging Service) spam filtering system that makes use of a thesaurus and SVM (Support Vector Machine). The system uses a pre-processing device to extract words from sample data, integrates these words' meanings using a thesaurus, generates features of the integrated words using chi-square statistics, and then analyses these features.

4.Visualizing Decision Table Classifiers

Decision tables are categorization models, like decision trees and neural nets, that are produced by machine learning algorithms and used for prediction. A decision table is a hierarchical table made up of entries from one table that is divided down into two other tables by the values of two additional characteristics. The study offers a visualisation technique that enables even those with no prior knowledge of machine learning to understand a model based on numerous attributes. This visualization's utility in comparison to other static designs is increased through the inclusion of various forms of interaction.

Problem Statement

Spam texts are unsolicited communications that are sent to mobile devices via SMS or instant messaging apps. Typically, unwanted texts come from unknown numbers or are robotexts that are sent out in bulk by auto-dialers. Like other forms of spam messages, spam texts often promote a product or service. The prevalence of spam SMS messages has increased significantly, and anyone can fall prey to them regardless of their location or phone model. Clicking on a link in an SMS might seem like a minor action, but the link could lead to a convincing yet phony website where you will be prompted to enter your personal information and potentially pay a fee, which could be the start of a theft of your life savings.

Methodology

The focus of our system is to develop a spam classfier which classifies SMS's spam/ham that uses machine learning to increase accuracy compared to existing approaches.

steps involving in spam classifier are as follows:

1. Gathering dataset consisting of spam and ham messages

2. Upload and view the dataset
3. Preprocessing the uploaded data
4. Training the model
5. Prediction of results

1.Gathering dataset consisting of spam and ham messages:

Initially a sample dataset is collected from the web which is having spam and ham messages. The dataset is containing huge amount of records which are unstructured and then need to be structured in furthur steps. Mostly csv format data is gathered.

2.Upload and view the dataset:

Firstly the dataset is selected and uploaded into the system.The data which is loaded into the system can be viewed by the user to know what type of data is available in the dataset. Since the dataset is having thousands of rows only few rows are displayed instead of loading the entire dataset to reduce the time delay.

3.Preprocessing the uploaded data:

In this step resizing and reshaping of the data into appropriate format to train our model. Unstructured data formatted in such a way it can useful for furthur process. The data is resized into a number splits such as x_train,y_train,x_test,y_test for the smooth functioning of data.

4.Training the model:

In this step we firstly fit the data to two algorithms i.e., NB and SVM , then we check the accuracy of prediction of each algorithm. Afterwards , the algorithm with greater accuracy is used for training the model to predict the results, in this system we used naïve bayes for training which majorly depends on conditional probability concept.

5.Prediction of results:

During this phase , we supply an input sms for prediction. Here, both text and image of messages are accepted.This helps the user to make use of this spam message classification system with ease. By just taking a snapshot of the sms the user can know whether it is spam or ham. The algorithm is chosen based on accuracy it provides. OCR (Optical Character Recognition) systems utilize software to convert a digital image of a document containing printed or handwritten text into a machine-readable text format. The tesseract tool is one of the software applications that can be used to implement OCR.

Implementation

Naïve Bayes is most popular algorithm for text classification is a popular technique for solving multi-class problems due to its ability to calculate conditional probabilities easily and accurately. The Naive Bayes (NB) algorithm is often used for this task, as it does not require an iterative process and supports both binary and multinomial classification. While NB assumes feature independence, it still performs well on short texts like tweets and can even outperform other classifiers with feature selection. On the

other hand, the Support Vector Machine (SVM) algorithm is more powerful for non-linear classification tasks and works well in high-dimensional spaces, such as those found in text data. SVM is typically used as a binary model, but it can be adapted for multi-class classification with good results. However, when comparing the accuracy of SVM and NB in spam classification, the basic NB algorithm produced the best prediction results.

Prerequisites

To follow along with this discussion, readers will need certain prerequisites.

1.To participate, you will need to have Python installed on your computer.

2.Pycharm & Mysql work bench are to be installed and configured on your system.

3.A CSV file containing a dataset should be available for use.

Support Vector Machine (SVM) Algorithm :

The support vector machine (SVM) algorithm's goal is to locate a hyperplane in an N-dimensional space—where N is the number of features—that can successfully divide and categorise the data points.

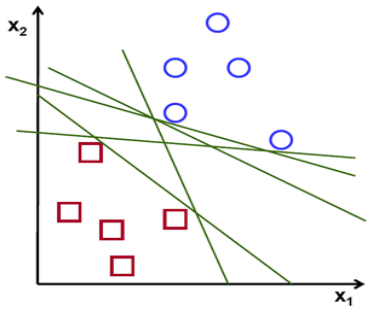


Fig.1.Possible hyperplanes

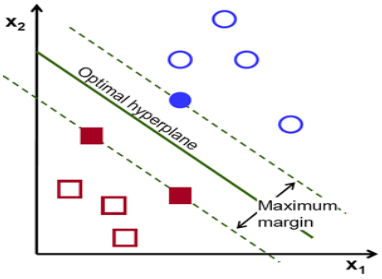


Fig.2.Construction of optimal hyperplane

There are several possible hyperplanes that might be used to categorise the two groups of data points. Finding the hyperplane with the highest margin—i.e., the greatest separation between datapoints in both classes—is the aim of the SVM algorithm. In order for the hyperplane to successfully categorise new data points, this margin distance is maximised to provide some robustness. Data points are classified using hyperplanes as decision boundaries. Depending on how many features are used, the hyperplane's position will change. The hyperplane is a line, for instance, if there are just two features. The hyperplane turns into a two-dimensional plane if there are three features. When there are more than three characteristics, though, it is more difficult to see hyperplanes.

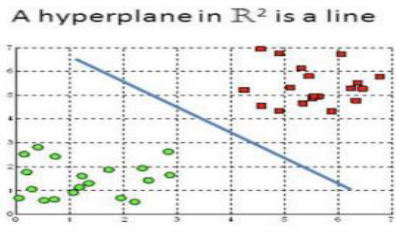


Fig.3. 2D feature space hyperplane

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

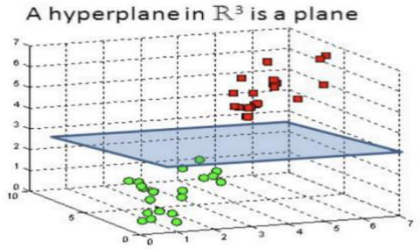


Fig.4.3D feature space hyperplane

Python implementation of support vector algorithm

Similar to the implementation of SVM, the implementation of the Naive Bayes algorithm involves several steps:

Step 1: Add the necessary libraries.

Step 2: Load dataset into memory.

Step 3: The dataset should be divided into features and the desired outcome.

Step 4: Divide the dataset into a training set and a testing set.

Step 5: Include the training set into the Naive Bayes model.

Step 6: Predict the outcomes of the test set.

Step 7: Use the confusion matrix to evaluate the model.

Step 8: Visualize the test set results (if applicable)

Naive Bayes Algorithm :

A probabilistic model, the Naive Bayes technique makes it simple and quick to predict the class of the test dataset. In comparison to other models like logistic regression, it performs well in multi-class prediction and needs less training data. However, it makes the assumption that the predictors or features are independent, which may not always hold true. Additionally, for numerical variables, the algorithm assumes a normal distribution, which can be a strong assumption.

The steps involved in the Naive Bayes algorithm:

1. Making a frequency table out of the dataset.

2. By gathering probabilities, constructing a likelihood table.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

3. In order to determine the posterior probability for each class, use the Naive Bayes equation. The result of the prediction is the class with the highest posterior probability.

Results

Once the user has successfully logged in to the Spam Message Classification website, they will be directed to the homepage where the results are displayed below:

Fig.5 shows the homepage.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

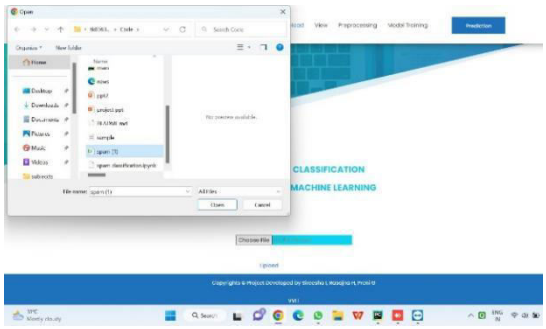


Fig.6 displays the process of uploading the dataset.

Fig.7. Viewing a few records in the dataset.

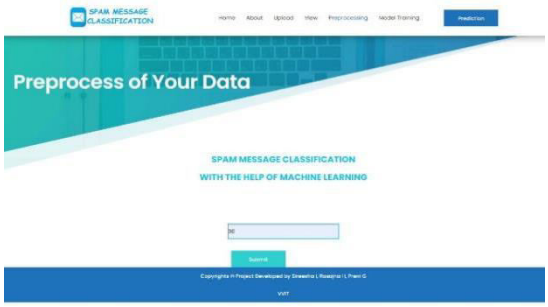


Fig.8 data is preprocessed to make it readily available for model training.

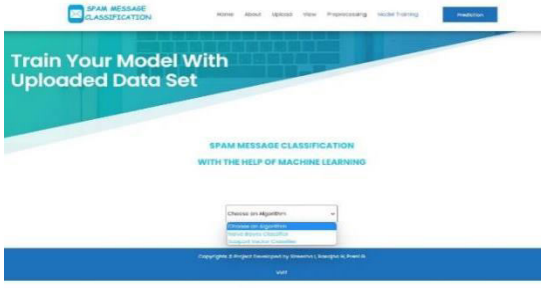


Fig.9. The preprocessed data is used to train the model by selecting the appropriate algorithm

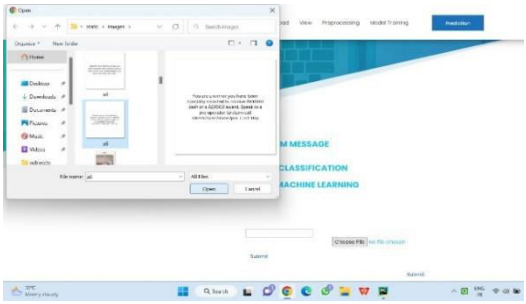


Fig.10. Enter an image of a ham SMS as input.

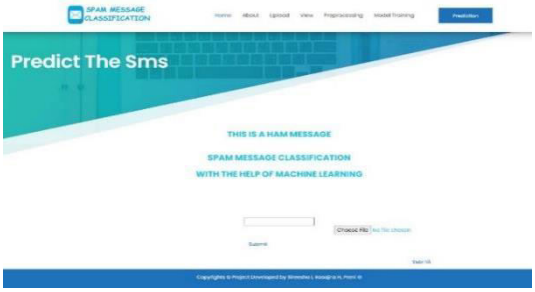


Fig.11.The SMS has been predicted as ham.

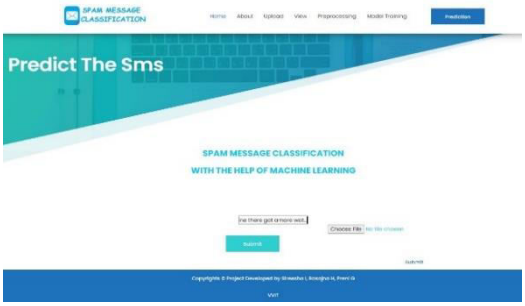


Fig.12. provide a text input of a spam SMS.

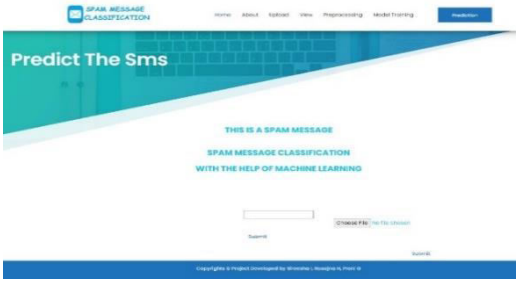


Fig.13.The SMS has been predicted as spam.

Conclusion

In this paper, we present a new technique for determining if a message is spam or not. Using the support vector and naive bayes algorithms, we can determine whether a message is spam or not. Our model utilizes SVM and Naive Bayes techniques to train on a pre-processed dataset, allowing it to determine whether a message is spam or not. The support vector algorithm assigns an index to each word in the dataset, and after training, test case messages are evaluated for accuracy. Our model achieves up to 98% accuracy when classifying text messages. At the end of the process, a sample message is classified as either spam or ham. The Naive Bayes algorithm is particularly useful for text classification and allows for real-time predictions.

Future work

In this article, we presented a web application that can classify spam messages in both image and text formats. However, our future work aims to expand this classification system to include all types of SMS on an Android platform.

References

[1] In 2006, Elsevier Inc. published the second edition of "Data Mining Concepts and Techniques" by J. Han and M. Kamber

[2] "Contributions to the Study of SMS Spam Filtering" was conducted by A. Tiago Almeida, José María Gómez, and Akebo Yamakami at the University of Campinas in Sao Paulo, Brazil.

[3] The Division of Computer Science and Engineering at Hanyang University in Seoul, South Korea, developed "An SMS Spam Filtering System Using Support Vector Machine," authored by Inwhee Joe and Hyetaek Shim.

[4] The paper "A New Spam Short Message Classification" was presented by L. Duan, N. Li, and L. Huang at the First International Workshop on Education Technology and Computer Science in 2009. The paper was published in the conference proceedings and its page numbers are 168-171.

[5] The article "Visualizing Decision Table Classifiers" was written by B. G. Becker and published in IEEE in 1998. The article spans pages 102-105.