Communication in Physical Sciences, 2020, 7(2):82-86

Evaluation of Time Complexities of Bayesian Vs Hybridized Word Stemming Techniques for Advanced Fee Fraud Emails Filtering

Okunade Oluwasogo, Adekunle, Afolorunso Adenrele and Adebayo Adegboyega

Received 18 December 2020/Accepted 20 April 2021/Published Online 12 May 2021

Abstract: *Time execution of content-based spam filter was investigated using the Bayesian statistical algorithm against Bayesian statistical algorithm incorporated with a word stemming. The execution time intervals for the algorithms implementation of the two techniques were evaluated by subjecting the filters to manipulated and non-manipulate spam mails. The experiment shown that both single technique (Bayesian) and combined techniques (Bayesian incorporated with word stemming) executed suspicious terms manipulated mails faster (within a short time) compared to non-manipulate suspicious terms mails. Combined algorithms performed better and faster in a sophisticated and manipulated environment. The algorithm is more rugged and performed better when suspicious term/tokens were manipulated to deceit the filter.*

Key Words: *Time execution, Classification, Spam, Mail, Word stemming.*

Okunade Oluwasogo Adekunle*
Department of Computer Science, Faculty of Sciences, National Open University of Nigeria, Cadastral Zone, Nnamdi Azikiwe Expressway, Jabi, Abuja, Nigeria
Email: aokunade@noun.edu.ng
Orcid id: 0000-0002-1625-8749

Afolorunso Adenrele
Department of Computer Science, Faculty of Sciences, National Open University of Nigeria, Cadastral Zone, Nnamdi Azikiwe Expressway, Jabi, Abuja, Nigeria
Email:

Adebayo Adegboyega
Department of Computer Science, Faculty of Sciences, National Open University of Nigeria, Cadastral Zone, Nnamdi Azikiwe Expressway, Jabi, Abuja, Nigeria
Email:

1.0 Introduction

Internet has become an important and fastest means of communication. It makes use of electronic mail (eMail) for communication, which is one of the most personal and professional ubiquitous communication method. Consequently, spam mail tends to dominate and compete with the real mail in a manner that seems to be explosive (Sanjay, 2015). In spite of expanding roles and relevance of internet and communication via email, reported challenges associated with email have been confirmed to be significant (Ali and Tunga, 2007). More is known of the assurance of the mail one sends than the safety of unsolicited mails that have been received. Spam or junk mails are unsolicited email messages sent in bulk (multiple recipient) by spamming and may have some fraudulent benefit to the sender of their mission is not detected by the (Tian, 2020). It is currently regarded as one of the major problems in the internet that is yet to be completely neutralised (Garacia *et al*., 2004). Spam message volumes have doubled over the past years and now account for about 80% of the total messages on the Internet (Zhe, *et al., 2007*). Spam is waste of time, storage space and communication bandwidth and can be a source of virus attack on the internet, which may be potent in destroying user's information or reveal identity or data. Emails are used by number of user to communicate around the world. Along with growth of internet and email, there has been dramatic growth in spam in recent year. Spam can originate from any location across globe, where internet access is available (Savita and Santoshkumar, 2014).

Most emails circulating on the Internet are unsolicited bulk emails called Spam (Albercht, 2006). According to The United States Federal Trade Commission in Alireza, Raheleh and Soheil (2012) 66% of spams have false information somewhere in the message and 18% of spams advertise "Adult" material. Several years ago most of the spam could be reliably dealt with by blocking the address of such e-mails or filtering out messages with certain subject lines (Fight Cybercrime, 2008; Hall, 1996; Monthy, 1989). However, in recent times, spammers have step beyond to the extent of escaping mechanism that could trap their messages through filtering-(Awad and. ELseuofi, 2011). Consequently, global research efforts are concentrated on the development of varied spam filtering techniques because current spam filters is prone to collapse if the spam keywords are manipulated or avoided in the email system (Almomani *et al.*, 2015). Like other types of filtering programs, a spam filter looks for certain criteria on which it bases its' judgments (Hall, 1996; Rekha and Sandeep, 2014).

2.0 Bayesian Spam Filtering Method

This is a content based spam filtering method that contains the word probability database that check for the matches of any of the contents of the mail against the suspicious terms in the database table named (Offensive). Content based spam filtering is a promising filtering approach capable of executing automatic identification of spam and legitimate email messages (Andrej, *et al*., 2006). It employs the laws of mathematical probability to determine which messages are legitimate (ham) and those that are spam. The word probabilities (also known as likelihood functions) are used to compute the probability that an email with a particular set of words in it belongs to either of the categories. This contribution is called the posterior probability and is computed using Bayes' theorem (Christina *et al*., 2010). It searches for the keywords in the mail, that is it scans through the mail content for suspicious related terms. This is a simple language analysis, which operates by matching match specific terms or phrases. This method makes use of Bayesian Statistical Probability formula (Process, 2010). The probability formula enhances each term be checked, compare and contrast for the similarity/equality with the terms enlisted in the content of the Offensive table in the database where the entire mail can then be classified to be Mail/Spam, depending on the result values of the calculation of the suspicious terms. If the result value calculated (that is the Spamicity value) or Probability value calculated is less than or equal to (<=) 0.5 (set threshold), the entire mail will be classified as Ham and will be send to the Ham folder of the recipient inbox but if otherwise (that is the Spamicity value) greater than (>) 0.5 (set threshold), then the entire mail can be classified as Spam. The Spamicity value of 0.5 is neutral, meaning that it has no effect on the decision as to whether a message is Spam or not. See Fig. 1.

2.1 Bayesian Spam Filtering Method Incorporated with Word Stemming Technique

Stemming is the removal of all unwanted prefixes, affixes and suffixes from a term in order to generate its actual value/root. When an incoming mail is received through the Mail Transfer Agent (MTA), it will pass through the word Stemming where the term stemming processing activities will be implemented through checking and extraction, when it comes across any of unwanted special characters used to modified the suspicious terms in order to deceit the Bayesian filters. Also the word stemming will equivalent any identified modified terms to its original value if any of the characters of the suspicious terms is been rearranged/modified to foil the Bayesian filter. Having done the above Word Stemming process activities on the mail content, mail can then be transfer to the Spam filter using next the Bayesian Statistical Probability formula as used above in the Bayesian Spam filtering process. See figure 2.

3.0 Materials and Methods

The experimental setup shown in Fig. 1 is the executing process of pure Bayesian Statistical filtering process while Fig. 2 is the executing process of the Bayesian Statistical filter incorporated with the Word Stemming (Word Stemming process), and the experimental result is shown in Fig. 1.

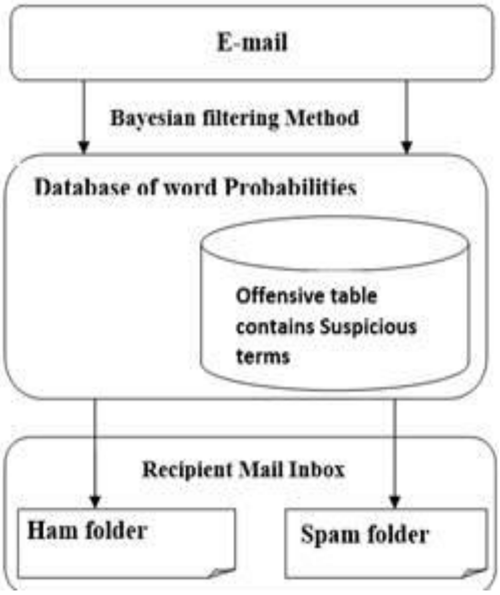

E-mail
Bayesian filtering Method
Database of word Probabilities
Offensive table contains Suspicious terms
Recipient Mail Inbox
Ham folder
Spam folder

Fig. 1: Bayesian Spam filtering Method Experimental setup

Bayesian filtering Method Experimental Algorithm

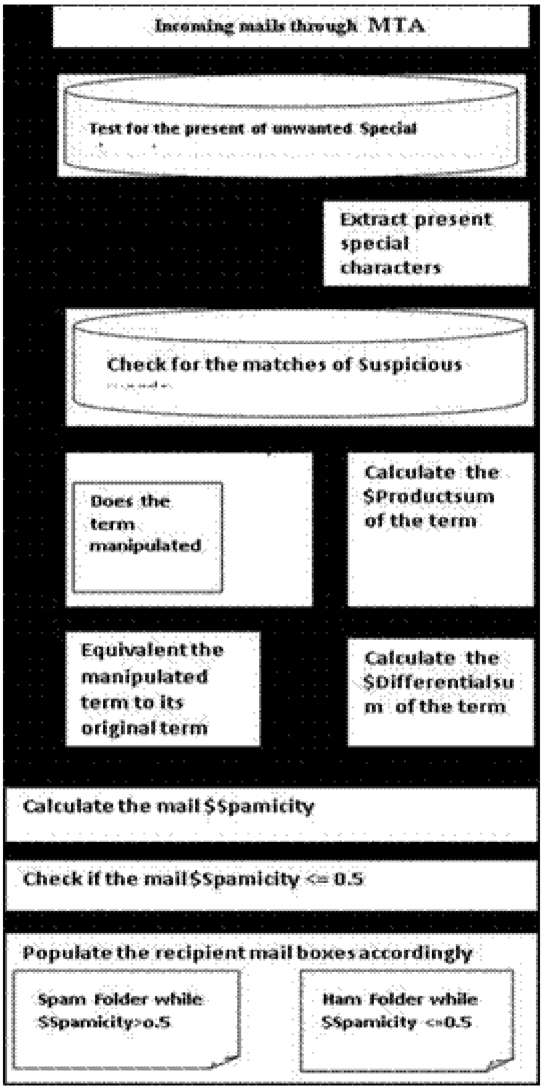
Step 1

Let \$Productsum = 1, \$Differentialsum=1

Step 2

If Term > Total Mail terms

```
        End
Step 3
Check the input terms against the Suspicious terms database
        If fund/matches?, then
                Calculate values
        End
Step 4
Calculate Values:
$Productsum *= $Spamicitydb
$Differentsum *= (1 - $Spamicitydb)
Step 5
$Spamicity = $Productsum / ($Productsum + $Differentialsum)
If $Spamicity <=0.5 Then
      Populate the recipient mail box Ham folder
Else, Populate the recipient mail box Spam/Junk folder
End
```



Incoming mails through MTA
Test for the present of unwanted Special
Extract present special characters
Check for the matches of Suspicious
Does the term manipulated
Calculate the $Productsum of the term
Equivalent the manipulated term to its original term
Calculate the $Differentialsum of the term
Calculate the mail $Spamicity
Check if the mail $Spamicity <= 0.5
Populate the recipient mail boxes accordingly
Spam Folder while $Spamicity>0.5
Ham Folder while $Spamicity <=0.5

Fig. 2: Bayesian Spam filter Incorporated with Word Stemming Experimental flow process

Bayesian Spam filter Incorporated with Word Stemming Experimental Algorithm

```
Step 1
Let $Productsum = 1, $Differentialsum=1
Step 2
If Term > Total Mail terms
        End
Step 3
Check input term against unwanted Special characters used as prefix, infix and suffix
        If any fund?, then
                Extract them all
        End
Step 4
Check the input terms against the Suspicious terms database
        If fund/matches?, then
                Calculate values
        End
Step 5
Check input term for any modified/manipulated suspicious terms If fund, then Equivalent it to the actual suspicious term
        End
Step 6
Calculate Values:
$Productsum *= $Spamicitydb
$Differentsum *= (1 - $Spamicitydb)
Step 7
$Spamicity = $Productsum / ($Productsum + $Differentialsum)
If $Spamicity <=0.5 Then
      Populate the recipient mail box Ham folder
Else, Populate the recipient mail box Spam/Junk folder
End
```

3.0 Results and Discussion

Fig. 3 shown result of the Experiment of execution time interval (shown in Figs. 1 and 2) conducted in previous section. X-axis signify spam mail content measured per numbers of words make up the spam mail content (such as 173,199,..,…, and 448) and y-axis signify the time it takes an Algorithm to complete each/its execution per seconds. From Fig. 3 appeared in twos the number values per mail meaning that, from the given values: 173, 173, 199,199, …, 448, 448, the first mail value (1st "173") is the spam mail executed without manipulating the Suspicious terms while the 2nd mail with "173" numbers of words/terms is the spam mail with manipulated Suspicious terms, the third spam mail (1st "199") is the spam mail without manipulated Suspicious terms while the forth mail (2nd "199")is the spam mail with manipulated Suspicious terms and so on up to the second to the last mail (1st "448") is spam mail without manipulate Suspicious terms and the last mail (2nd "448") is spam mail with manipulated Suspicious terms. They appeared to be longer execution time per second for each mail. The y-axis represent the execution time interval of the algorithm with word stemming (which appeared in blue) while the shorter execution value per seconds on y-axis is the execution time of Algorithm without the word Stemming (which is indicated with brown colour).

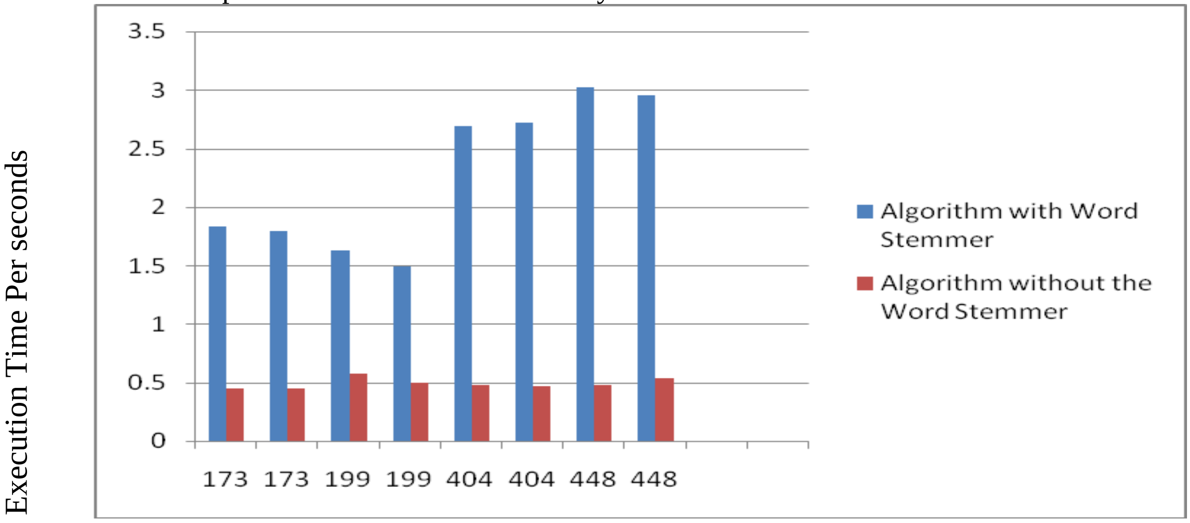


Fig. 3: Mail per Words or Tokens

Fig. 3: Result of Execution Time Comparison of Bayesian Algorithm against Bayesian Incorporated with Word Stemming Algorithm.

The result of execution time comparison of the two Algorithm experiment indicated that the execution time of Bayesian incorporated with the Word Stemming is significantly longer compared to that of ordinary Bayesian mail classification. Also, that suspicious terms manipulation has no or less effect on execution time of both algorithms.

4.0 Conclusion

The experiment shown that both single technique (Bayesian) and combined techniques (Bayesian incorporated with word stemming) executed suspicious terms manipulated mails faster (within a short time) compared to non-manipulate suspicious terms mails. Combined algorithms performed better and faster in a sophisticated and manipulated environment. The algorithm is more rugged and performed better when suspicious term/tokens were manipulated to deceit the filter.

5.0 References

Albercht. K, (2006). Mastering Spam: A Multifaceted Approach with the Spamato Spam Filter System *DSS. ETH NO. 16839*

Ali, C. & Tunga, G. (2007). Time-efficient spam e-mail filtering using n-gram models. *Department of Computer Engineering, Bogazic University, Istanbul 34342, Turkey*

Alireza, N. P., Raheleh, K. & Soheil, B. R. (2012). Minimizing the time of spam mail detection by relocating filtering system to the sender mail server. *International Journal of Network Security & Its Applications (IJNSA)*, 4, 2, pp. 53-62. doi: 10.5121/ijnsa.

Almomani, A., Obeidat1, A., Alsaedi, A., Obaida, M. A. & Al-Betar, M. (2015). Spam e-mail filtering using ecos algorithms. *Indian Journal of Science and Technology*, 8, S9, pp. 260-272

Andrej, B., Gordon, V. C., Bogdan, F. C., Thomas, R. L. & Blaz, Z. (2006). Spam filtering using statistical data compression models. *Journal of Machine Learning Research*, 7, pp. 2673-2698.

Awad, W..A. &. ELseuofi, S.M. (2011). Machine learning methods for spam e-mail classification. *International Journal of Computer Science & Information Technology (IJCSIT)*, 3, 1, doi: 10.5121/ijcsit. 3112 173.

Christina, V., Karpagavalli, S. & Suganya, G. (2010). A study on email spam filtering techniques. *International Journal of Computer Applications*, *Applications (0975 – 8887), 12, 1, pp. 7-9*

Fight Cybercrime (November, 2008) *Anti-phishing Techniques* SpamAlert.org

Garacia, F. D, Hoepman, J & Nieuwenhuizen, J. V. (2004). Spam filter analysis. *IFIP International Information Security Conference*, 74, pp. 395-410

Hall, R. J, (1996). Channels: Avoiding unwanted electronic mail. *In Proceeding Symposium on Network Threats. DIMACS.*

Monthy, P. (1989). Flying Circus. *Just the word*. *Menthuem Publishing Ltd.* 2, 25, pp. 27-28.

Process (2010). Bayesian filtering example using bays' formula to keep spam out of Your Inbox. *http://www.process.com/*

Rekha & Sandeep, N. (2014). A Review on different spam detection approaches. *International Journal of Engineering Trends and Technology (IJETT)*, 11, pp. 315-319.

Sanjay, K. N. (2015). Spam filtering using the social anthropology and data mining technique. *International Journal of Computer Science and Mobile Computing. IJCSMC, 4, 4, pp. 234-237*.

Savita, T. & Santoshkumar, B. (2014). Effective Spam Detection Method for Email. *IOSR Journal of omputer Science (IOSR-JCE). e-ISSN: 2278-061, p-ISSN: 2278-8727, pp. 68-72 www.iosrjurnals.org*

Tian, X. (2020). Constant time complexity spam detection algorithm for boosting throughput on rule-based filtering systems. *IEEE Access.*

Zhe, W., William, J., Qin, L., Moses, C. and Kai, L. (2007). Filtering image spam with near-duplicate detection. *Computer Science Department, Princeton University, USA*

Conflict of Interest

The authors declared no conflict of interest