International Journal of Advanced Science and Research
ISSN: 2455-4227; Impact Factor: RJIF 5.12
Received: 29-03-2020; Accepted: 16-04-2020; Published: 23-04-2020
www.allsciencejournal.com
Volume 5; Issue 2; 2020; Page No. 21-25

Feature extraction techniques for SMS spam detection: A review

Fatimoh Abidemi Taofeek-Ibrahim[1*], Taye Oladele Aro[2], Hakeem Babalola Akande[3], Besiru Muhammed Jibrin[4], Nike Toyin Toye[5]

[1, 5] Department of Computer Science, Federal Polytechnic Offa, Kwara State, Nigeria
[2] Department of Mathematical and Computing Sciences, KolaDaisi University, Ibadan, Oyo State, Nigeria
[3] Department of Telecommunication Science, University of Ilorin Ilorin, Ilorin, Nigeria
[4] Department of Computer Science Federal University Kashere, Gombe State, Nigeria

Abstract
The general acceptance of using mobile phones has resulted in a noticeable increase in sending of Short Message Service (SMS) messages. Messages through SMS have been considered as a rapid method of communication due to its stress-free usage and low cost, as a result, SMS has been targeted for several forms of threats, one of these is spamming. The spam SMS is unwanted or undesirable messages received by many mobile phone users, and cause many problems such as anger, displeasure, consumption of network bandwidth, scam and theft of personal information and malware installation. Feature extraction is a significant phase of SMS Spam detection, the extraction of features in SMS involves a procedure of reducing initial original features into to more manageable forms for the classification process. This paper conducted a literature review on some of the commonly used feature extraction techniques for SMS Spam detection system. A contribution was made on how these techniques can be further improved to develop robust systems of SMS Spam detection.

Keywords: feature extraction, network bandwidth, short message service, spam SMS

1. Introduction
SMS remains one of the popular means of communication for people through mobile devices or internet-connected computers [1]. SMS technology was developed out of the GSM, the communications standard, a globally accepted cell phone network specification [2]. SMS is extensively used worldwide, this is due to the high response rate, secure nature, personal service and lowest price cost [3]. SMS is the most powerful tool in terms of communication especially for huge numbers of individuals using mobile phones [4], where sending of messages must take place based on the communication standard protocols. SMS is beyond the conventional texting and is presently used in diverse domains such as online transactions, retrieval systems for information, one-time password delivery, a configuration of smartphone Over-The-Air (OTA) configuration and alerts of social web site [5].
The increase in SMS messages has unnecessarily fascinated spammers to send spam SMS referred to as a junk SMS which also result into a problem of spam SMS message just as in the instance of spam emails [6]. Some challenges have been traceable to SMS in the mobile communication world despite the different benefits associated with SMS [7]. SMS Spam commonly refers to the unsolicited and unwanted SMS usually conveyed to a large number of recipients [8]. The junk mail (bulk) is usually sent in large volume for profitmaking or other reasons [9]. In society today, the bulk of information received by mobile phone users are the annoying spam messages like the credit opportunities, stores' promotion, notices of discount and service providers new tariffs awareness [10]. SMS spamming has attracted much attention over other spamming techniques such as email because SMS has been considered is the present increasing communication channel [11]. It has constituted a great problem to the mobile phone subscribers given its ubiquitous nature. It suffers an extensive cost as a result of large network bandwidth usage, loss of output and break-in of personal privacy. Mobile spam frustrates the mobile phone users just like email spam, it causes societal frictions to mobile phones.
The feature extraction phase has been identified by researchers as s significant phase in detecting spam in SMS [12]. The extraction of features involves a reduction process in which original raw data is decreased to more manageable forms [13]. Dimensionality reduction produces an approximation to original feature in fewer dimensions, while still maintaining the same structure of original features [14]. Several feature extraction algorithms like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Discrete Cosine Transform (DCT), Local Binary Patterns (LBP), Local Ternary Pattern (LTP), Non-negative Matrix Factorization (NMF) Discrete Wavelet Transform (DWT) and Independent Component Analysis (ICA) have been encountered in SMS spam filtering with different approaches, thus resulted in different level of accuracies.
This paper performed a general review on some commonly feature extraction techniques used for the SMS Spam detection system. The study concluded by suggesting how these techniques can be further enhanced to develop effective SMS Spam detection system.

2. Feature Extraction
This is a dimensionality reducing technique that mostly employed for obtaining the significant features from an existing dataset to produce a comparable smaller dataset

which contains all the significant features of an existing dataset [15]. After performing feature extraction on the dataset, the result itself turns to important features of the dataset [16]. By performing feature extraction, it principally forbade the redundancy of raw data forms of the existing dataset. In SMS spam detection, the feature extraction mainly performs the task of choosing the word that which word is spam and which word is not spam [17]. The technique of feature extraction must not be complex to escape the major interruption in messaging services but the feature should possess high correlation with message type to improve the accuracy of spam detection [18]. There are several techniques of feature extraction, this includes PCA, LDA, NMF and ICA [19]. The extraction of features remains the utmost essential part in SMS spam classification or detection techniques.

2.1 Principal Component Analysis (PCA)

It is an approach of analysis for the structure of variance-covariance variables achieved by linear combinations [20]. The PCA represents a dimensionality reduction approach that transforms raw data into a relatively smaller space [21]. For instance, if the data to be decreased contains m features or dimensions. PCA finds m dimensional orthogonal vectors (principal components), where several orthogonal vectors are less than m (features in original data) [22]. The produced principal components are kept in organized order of importance. Components with low variance can be removed to obtain the reduced data size. Researchers have applied PCA to reduce the set of features in SMS spam to produce an enhanced SMS spam detection system [23].

2.2 Linear Discriminant Analysis (LDA)

LDA is generally applied in learning algorithm, statistics, recognition of pattern to find a linear combination of features that characterizes or separates two or more features [24]. The LDA as a discriminant method tries to model changes among samples assigned to certain categories [25]. The purpose of this technique is to maximize the between-class variance and minimize the within-class variance using a function of linear discriminant with the theory that data in each class is termed by a function of Gaussian probability density of the same covariance. The detection of SMS Spam is a categorization problem where the classes to be predicted are spam and legitimate [21]

2.3 Independent Component Analysis (ICA)

It is a technique for splitting a multivariate signal into additive subcomponent [26]. It is achieved by the assumption that non-Gaussian signals are not smaller components and also statistically not depending on each other. ICA is applied to find hidden factors that are under random variables, measurements, or signals [27]. The variables in data are considered to be linear mixtures of specific unidentified latent variables and the mixing system is also unidentified [28]. The general framework of ICA is that the sources are produced through a linear transformation, where additive noise is available.

2.4 Non-negative Matrix Factorization (NMF)

This is a factorization of a matrix approach that is frequently used in an information processing task. The NMF is a technique of multivariate analysis and linear algebra where a matrix V is factorized into two matrices W and H, with the property that all three matrices have no negative elements [29]. NMF transforms a non-negative matrix nearly into the product of two lower-ranked non-negative matrices. One of the major advantages of NMF is that it allows representation of parts-based by additive only combination s[30]. NMF has become an extensively employed technique for the analysis of high data dimensionality as it automatically obtains sparse and significant features from a set of nonnegative data vectors [31]. In the SMS spam detection model, the clusters of SMS can be produced for non-SMS spam messages using NMF [32]

3. Related Work

Sheikhi, Kheirabadi and Bazzazi (2020) [33] developed a new learning algorithm approach for SMS spam detection. The study involved two key phases: decision making and feature extraction. The first stage involved the extraction of those features that were important features from the dataset in terms of the spam and legitimate messages to reduce the problem of computation and increase model effectiveness. Averaged neural network approach was used to classify features extracted into either legitimate or spam. Evaluation of the model was done with SMS dataset of over 5000 messages. Experimental results gave an accuracy of 98.80%, recall of 0. 9967, the precision of 0. 9892 and F1 measure of 0. 9929.

Subba Reddy and Srinivasa Reddy (2020) [23] enhanced the detection accuracy of spam in social media networks by reduction of irrelevant features in large dimension social media dataset. PCA was introduced to decrease the dimensionality of SMS features. The reduced features were passed to two different classifiers: K-Nearest Neighbour and Decision Tree Induction. The algorithms were used to classify samples of data to spam or ham. The developed model was evaluated using Twitter dataset. Results showed that KNN performed better than a Decision tree.

Rajput, Sohal and Athavale (2019) [15] improved the accuracy of the classification by extracting more number of header features. The implementation of an adaptive and collaborative technique was achieved by employing machine learning and cluster computing for fast detection of emails as spam or ham. The adaptive approach was applied to produce new rules for classification and cluster approach for parallel computing power to increase computational speed. Spam Assassin is the main dataset used for testing. The collaborative approach created a parallel environment where multiple anti-spam methods and divided test corpora were used as input. The false-positive and false-negative percentage were recorded and accuracy was calculated.

Annadatha and Stamp (2018) [21] performed analysis and comparison on two techniques for spam images detection. PCA was applied to find eigenvectors corresponding to spam images and also calculate the scores by projecting images to eigenspace output. The next phase considered the image features extraction and an optimal subset obtained using Support Vector Machines (SVM). The two strategies for detection gave the best accuracy with reduced complexity in computation.

Mallikka and Balamurugan (2018) [34] used a shape-based feature in recognition of characters in images and identified whether an image is Ham or Spam. The study elaborated on the techniques for extraction of visual feature (Text layout analysis) and the information of the algorithms were used for image spam detection. The score and performance

metrics of the identified images were produced as the output of the experimental analysis. The effectiveness of the developed model gave a detection accuracy above 90%.

Imani and Montazer (2017) [35] proposed a supervised feature extraction approach referred to as cluster space linear discriminant analysis (CSLDA) to deal with the difficulties in separating spam emails from normal emails. The CSLDA employed the ability of unlabeled testing samples in addition to labelled training ones for estimation of the within-class and between-class scatter matrices. Based on the multimodal distribution of email spam databases, CSLDA clusters the unlabeled testing data for using them in the learning phase of feature extraction. CSLDA used the testing samples without determination of their labels, and just with obtaining a relationship between training and testing samples through clustering. The introduction of the Fisher criterion increased class discrimination. The use of clustered unlabeled samples created a solution to the small sample size problem and gave a better performance for multimodal data. The experimental results using spam-base dataset showed the effectiveness of CSLDA compared to some common feature extraction for spam detection techniques.

Kaya and Ertugrul (2016) [36] developed a new approach to feature extraction approach for SMS spam detection. Ternary Pattern with one dimension (1D-TP) was employed to obtain SMS features in SMS messages. Conversion of text message to UTF- values were achieved. Comparison of individual character (its UTF-8 value) in the message with its neighbours was applied too. Five learning algorithms: Bayesian Network (BN), Naïve Bayes (NB), Radial Basis Feed-Forward Neural Network (RBFF), k-nearest neighbours (KNN), and Random Forest (RF) were used to classify these features. The developed detection model used three different SMS corpora datasets for evaluation. Determining the optimal parameters of 1D-TP was a challenge in the study.

Dagher and Antoun (2015) [37] improved email filtering approach to make the accuracy of filtering robust and to reduce the time of processing. Several scenarios for Principal Component Analysis-Document Reconstruction (PCADR) classifier were developed for the filtering of the email process. The study mentioned the PCADR accuracy variant due to the change in preprocessing of a feature. Consideration of four scenarios was made: scenario 1: classes of Ham and Spam were denoted with different features. Scenario 2: classes of Ham and Spam were denoted with same features, scenario 3: classes of Ham and Spam classes were denoted with common terms, scenario 4: classes of Ham and Spam were denoted with general features and characteristic terms. Diverse experiments were performed using a public corpus obtained from the University of California-Irvine Machine Learning Repository with several training and testing sections. PCADR was compared with SVM and Bayes to show its effectiveness.

Anchal and Sharma (2014) [38] focused on the classification of text like tree architecture. ICA and Neural Network approach was used for the classification of text to stop the user from undesirable spam messages. The study presented an alternative solution using a neural network on a corpus of SMS received by the researchers who conducted the analysis. The dataset for the model employed descriptive attributes of words, symbols and SMS that are usually used by users to appropriately recognize spam received in inboxes.

Uysal *et al*. (2014) [10] analysed the influence caused by different techniques of feature extraction and selection on the filtering of short message service (SMS) spam into Turkish and English language. The framework of feature set for filtering model was made up of the features created from the bag-of-words (BoW) model along with the ensemble of structural features (SF) that are particular to the spam task. The distinct features of BoW were recognized using information-theoretic feature selection techniques. The BoW and SF combinations were used for SMS messages classification. The filtering model was evaluated on datasets of Turkish and English SMS message. The experimental result showed that the BoW and SF combinations recorded a better classification performance rather than individual BoW features.

4. Summary and Discussion

The feature extraction is a predominant phase in SMS spam detection which also similar to filtering of e-mail spam. Feature extraction is a dimensionality reduction process in which original data is decreased to more measurable forms before processing [13]. Dimensionality reduction produces an approximation to original feature in fewer dimensions, while still maintaining the same structure of original features [34]. Also, unlike emails, it is a difficult task to obtain features that are significant in SMS messages, because they are usually short and may contain many abbreviations.

The extraction of feature only takes into consideration the linear reduction of the original features from SMS. It is necessary to look into the relevancy of features to be used for classification. Hence, there is a need to introduce robust feature selection algorithms together with feature extraction to produce effective SMS Spam detection algorithms. The selection of feature involves the procedure of obtaining relevant feature subsets for the classification process and model construction [39]. Feature selection reduces the number of features, eliminate inappropriate and noisy features that show no contribution to the accuracy of the classification model [40]

Obtaining optimal features in feature selection turns out to be usually intractable [41], and many other problems related to feature selection shown to be a non-deterministic polynomial hard problem (NP)[42]. Among the numerous techniques of feature selection techniques, metaheuristic optimization algorithms which mostly are nature-inspired such as firefly, Ant Colony Optimization, Artificial Bee Optimization, Cuckoo, Particle Swarm Optimization, Lion Optimization, Genetic Algorithm and Gravitational Search Algorithm have been proved to be an effective technique for obtaining the most discriminant and relevant features. In future work, the development of SMS Spam detection should introduce the aforementioned metaheuristic techniques for improvement purpose.

5. Conclusion

The upturn in the technology of mobile communication has produced numerous contributions to society. One of the effects is SMS communication, which is one of the most prevalent communication channels nowadays. Similar to other general communication techniques, spam messages are considered as a major in SMS. The total ratio of SMS

spam to overall SMS traffic is increasing daily. Spams SMS do not only consume the users' time but also takes a significant mobile traffic portion. Several SMS Spam detection techniques have been proposed by researchers using types of feature extraction techniques. In SMS Spam detection, feature extraction is a core step which precedes the classification stage. This paper performed a general literature review on some existing feature extraction methods used in SMS spam filtering system. An enhancement approach of SMS Spam detection was suggested for further work.

6. References

1. Jameel NG. "SMS SPAM Detection Using Association Rule," J Theor. Appl. Inf. Technol. 2018; 96(12):3962-3972.
2. Katankar VK. "Short Message Service using SMS Gateway," Int. J Comput. Sci. Eng. 2010; 2(5):1487-1491.
3. Choudhary N, Jain AK. "Towards filtering of SMS Spam Messages using Machine Learning-Based Technique," in Communications in Computer and Information Science, 2017; 712:18-30.
4. Nivaashini P, Soundariya M, Kodiieswari RS, Thangaraj A. "SMS Spam Detection Using Neural Network Classifier," Int. J Pure Appl. Math. 2018; 119(18):2425-2436.
5. Mizuki A, Matsumoto T, Uemura T, Kichimi S. "Improving SMS Processing Power for the Increasing Smartphone Demand," NTT DOCOMO Tech. J. 2013; 14(4):60-62.
6. Gansterer WN, Janecek AGK, Neumayer R. "Spam filtering based on latent semantic indexing," in Survey of Text Mining II: Clustering, Classification, and Retrieval, 2008, 165-183.
7. Abdulhamid M, Shafie M, Latiff A, Chiroma H, Osho O. "A Review on Mobile SMS Spam Filtering Techniques A Review on Mobile SMS Spam Filtering Techniques," no. February, 2017.
8. Mahmoud TM, Mahfouz AM. "SMS Spam Filtering Technique Based on Artificial Immune System," Int. J. Comput. Sci. Issues. 2012; 9(2):589-597.
9. Chaudhari N, Jayvala P, Vinitashah P. "Survey on Spam SMS filtering using Data mining Techniques," Ijarcce. 2016; 5(11):193-195.
10. Uysal AK, Gunal S, Ergin S, Gunal ES. "The Impact of Feature Extraction and Selection on SMS Spam Filtering," Elektron. IR Elektrotechnika. 2014; 19(5):67-72.
11. Subramaniam T, Jalab HA, Taqa AY. "Overview of textual anti-spam filtering techniques," Int. J Phys. Sci. 2010; 5(12):1869-1882.
12. Uysal AK, Gunal S, Ergin S, Gunal ES. "The impact of feature extraction and selection on SMS spam filtering," Elektron. ir Elektrotechnika. 2013; 19(5):67-72.
13. Kaur R, Rajput R. "Face recognition and its various techniques: a review," Int. J Sci. Eng. Technol. Res. 2013; 2(3):670-675.
14. Telgaonkar S, Deshmukh AH. "Dimensionality Reduction and Classification through PCA and LDA," Int. J Comput. Appl. 2015; 122(17):4-8.
15. Rajput AS, Sohal JS, Athavale V. "Email Header Feature Extraction using Adaptive and Collaborative approach for Email Classification," Int. J. Innov. Technol. Explor. Eng. 2019; 8(7):158-164.
16. Apvrille L, Apvrille A. "Identifying unknown android malware with feature extractions and classification techniques," Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust, 2015; 1:182-189.
17. Annadatha A, Stamp M. "Image spam analysis and detection," J Comput. Virol. Hacking Tech. 2018; 14(1):39-52.
18. Hedieh S, Parast GZ, Akbari F. "SMS Spam Filtering Using Machine Learning Techniques: A Survey," Mach. Learn. Res. 2016; 1(1):1-14.
19. Gomez JC, Moens MF. "PCA document reconstruction for email classification," Comput. Stat. Data Anal. 2012; 56(3):741-751.
20. Karamizadeh S, Abdullah SM, Manaf AA, Zamani M, Hooman A. "An Overview of Principal Component Analysis," J Signal Inf. Process, 2013; 4:173-175.
21. Imani M, Montazer GA. "Email Spam Detection Using Linear Discriminant Analysis Based on Clustering," CSI J. Comput. Sci. Eng. 2017; 15(1):22-30.
22. Jollife IT, Cadima J. "Principal component analysis: A review and recent developments," Philos. Trans. R. Soc. A Math. Phys. Eng. Sci, 2016, 374(2065).
23. Subba Reddy K, Srinivasa Reddy E. "Using reduced set of features to detect spam in twitter data with decision tree and KNN classifier algorithms," Int. J. Innov. Technol. Explor. Eng. 2019; 8(9):6-12.
24. Tharwat A, Gaber T, Ibrahim A, Hassanien AE. "Linear discriminant analysis: A detailed tutorial," AI Commun. 2017; 30(2):169-190.
25. Devi MS, Rahul K, Satheesh M, Rajasekhar K. "Count Vectorized Spam and Ham Discernment of Short Message Service using Machine Learning Classification," Int. J Recent Technol. Eng. 2019; 8(4):557-561.
26. Benlin X, Fangfang L, Xigliang M, Huazhong J. "Study on independent component analysis' application in classification and change detection of multispectral images," in The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 2008; 37:871-876.
27. Naik DK, Kumar GR. "An Overview of Independent Component Analysis and its Applications," Inform. 2011; 35(1):63-81.
28. Sompairac N, *et al*., "Independent component analysis for unraveling the complexity of cancer omics datasets," Int. J Mol. Sci, 2019, 20(18).
29. Takeuchi K, Ishiguro K, Kimura A, Sawada H. "Non-negative Multiple Matrix Factorization," in IJCAI International Joint Conference on Artificial Intelligence, 2013, 1713-1720.
30. Wang J, Tian F, Liu W, Wang X, Zhang W, Yamanishi K, *et al*. "Ranking preserving nonnegative matrix factorization," in IJCAI International Joint Conference on Artificial Intelligence, 2018, 2776-2782.
31. Zhang L, Chen Z, Zheng M, He X. "Robust non-negative matrix factorization," Front. Electr. Electron. Eng. China. 2011; 6(2):192-200.
32. Nagwani NK, Sharaff A. "SMS spam filtering and thread identification using bi-level text classification and clustering techniques," J Inf. Sci. 2015; 43(1):1-13.
33. Sheikhi S, Kheirabadi MT, Bazzazi A. "An Effective Model for SMS Spam Detection Using Content-based

Features and Averaged Neural Network," Int. J Eng. 2020; 33(2):221-228.
34. Mallikka M, Balamurugan R. "Shape-Based Feature Extraction in Detection of Image Email," J Phys. Conf. Ser, 2018, 1-10.
35. Imani M, Montazer GA. "Email Spam Detection Using Linear Discriminant Analysis Based on Clustering," CSI J Comput. Sci. Eng. 2017; 15(1):22-30.
36. Kaya OF, Ertugrul Y. "A Novel Feature Extraction Approach in SMS Spam Filtering for Mobile Communication: One-Dimensional Ternary Patterns," Secur. Commun. Networks, 2016; 9:4680-4690.
37. Dagher I, Antoun R. "Different PCA scenarios for email filtering," Int. J Comput. Appl. 2016; 38(1):41-54.
38. Anchal A, Sharma. "SMS Spam Detection Using Neural Network Classifier," Int. J Adv. Res. Comput. Sci. Softw. Eng. 2014; 4(6):240-244.
39. Derakhshii M, Ghaemi MR. "Classifying Different Feature Selection Algorithms Based on the Search Strategies," Int. Conf. Mach. Learn. Electr. Mech. Eng, 2014, 17-21.
40. Raymer ML, Punch WF, Goodman ED, Kuhn LA, Jain AK. "Dimensionality reduction using genetic algorithms," IEEE Trans. Evol. Comput. 2000; 4(2):164-171.
41. Yu L, Liu H. "Efficient Feature Selection via Analysis of Relevance and Redundancy," J. Mach. Learn. Res. 2004; 5(1):1205-1224.
42. Imani MB, Pourhabibi T, Keyvanpour MR, Azmi R. "A New Feature Selection Method Based on Ant Colony and Genetic Algorithm on Persian Font Recognition," Int. J Mach. Learn. Comput. 2012; 2(3):278-282.