Spam Detection Using Dense-Layers Deep Learning Model and Latent Semantic Indexing

Yasser D. Al-Otaibi¹, Shakeel Ahmad², Sheikh Muhammad Saqib³

Department of Information Systems-Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia¹

Department of Computer Science-Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University,

Jeddah 21589, Saudi Arabia²

Department of Computing and Information Technology, Gomal University, D.I.KHAN, Pakistan³

Abstract— In the digital age, online shoppers heavily depend on product feedback and reviews available on the corresponding product pages to guide their purchasing decisions. Feedback is used in sentiment analysis, which is helpful for both customers and company management. Spam feedback can have a negative impact on high-quality products or a positive impact on lowquality products. In both cases, the matter is bothersome. Spam detection can be done with supervised or unsupervised learning methods. We suggested two direct methods to detect feedback orientation as 'spam' or "not spam", also called "ham," using the deep learning model and the LSI (Latent Semantic Indexing) technique. The first proposed model uses only dense layers to detect the orientation of the text. The second proposed model uses the concept of LSI, an effective information retrieval algorithm that finds the closest text to a provided query, i.e., a list containing spam words. Experimental results of both models using publicly available datasets show the best results (89% accuracy and 89% precision) when compared to their corresponding benchmarks.

Keywords—Spam; supervised learning methods; unsupervised learning methods; LSI; dense; deep learning

I. INTRODUCTION

The company is shocked when there is a complaint about their high-quality product. How did they find the complaint? Obviously, from the webpage concerned with the feedback of the customer, if a complaint is factual, it can be found in a product; if not, these types of comments degrade the product's star rating or sentiment score. Before sentiment analysis, these comments or reviews should be filtered. These reviews can be considered spam. Researchers have done much work to separate spam from the given reviews [1]. Most spam is delivered as emails, so there should be a strong filter to detect the spam.

Classifiers trained using a combination of features are more effective than those learned using only one type of feature [2]. A machine learning algorithm has also been investigated for filtering spam emails [3]. Most supervised machine learning algorithms are not suitable for spam detection due to the lack of features or words that indicate the hint that the review is actual or not [4]. Although Support Vector Machines (SVM) is an important and powerful technique for detecting reviews as spam. However, for big data, the efficiency of SVM is reduced because of the many data processing complexities [5]. Unsupervised learning algorithms has also been investigated for spam detection such as clustering algorithm [6] has proved that these algorithms are well suited for spam clustering. A novel unsupervised text mining model was developed and integrated into a semantic language model for detecting untruthful reviews [7]. Unsupervised methods are currently unable to match the performance of supervised learning methods, research is limited, and results are inconclusive, warranting further investigation [8].

Deep learning is a new trend, through which classification can be done in a very descent way. This learning can be learned automatically, without predefined knowledge explicitly coded by the programmers. Although previous work which has been done on spam detection is based on bidirectional LSTM (Long Short Term Memory) [9] a resource hunger technique. The proposed work develops a simple sequential dense layer's model using scaling of data to detect spam text and found best performance, which require less computational processing.

The supervised learning approach employs training data based on labels ("ham" and "spam") sent to a classifier, which detects "spam" using this learned corpus. Unsupervised learning, on the other hand, necessitates the discovery of rules and patterns from supplied data. Both techniques need a significant amount of work, but, in this case, the suggested methodology does not necessitate the use of training data or rules. Latent Semantic Indexing was used to filter the "spam" and "ham" (not-spam), reviews. LSI is simple to comprehend, execute, and employ. When compared to other approaches, the results of LSI are far more precise and speedier. It seeks the most representational, rather than the most discriminative, qualities for document representation [10] The manually compiled Spam Words (SW) list includes 956 entries, which might be used in spam reviews [11]. This study makes the following key contributions:

- A method has been suggested to make a sequential deep learning model with scaling that can tell when text is spam.
- A method is proposed to detect reviews as either "spam" or "ham" using Latent Semantic Indexing (LSI) with an Automatic Generated Query (AGQ) that serves as a major input to LSI. Hence, there is no need to provide a separate query.

A. Significance of the Study

This study emphasizes the critical importance of maintaining the integrity of customer feedback systems by filtering spam reviews. Genuine feedback is essential for ensuring accurate product sentiment scores and star ratings. By addressing the issue of spam detection, the research highlights how filtering out non-factual reviews can prevent negative impacts on product perception. Additionally, the study advances the field by exploring modern machine learning and deep learning techniques, demonstrating their potential to improve spam detection accuracy while overcoming computational challenges in handling large datasets. These innovations contribute to more reliable systems for analyzing customer reviews.

B. Key Contributions

The study makes several notable contributions to the field of spam detection. First, it proposes a sequential deep learning model with data scaling, which not only achieves high performance but also requires significantly lower computational resources compared to traditional methods. Second, it introduces the integration of Latent Semantic Indexing (LSI) with an Automatic Generated Query (AGQ), enabling the filtering of "spam" and "ham" reviews without the need for a predefined query. This innovation simplifies the detection process and improves efficiency. Lastly, the research demonstrates that LSI outperforms existing approaches by providing more precise and faster results, focusing on representational features for document representation rather than solely discriminative ones.

C. Research Gap

Despite substantial progress in spam detection, significant gaps remain in existing methodologies. Supervised machine learning methods often fail to achieve optimal results due to insufficient features or words that indicate the authenticity of reviews. Additionally, Support Vector Machines (SVM), though recognized as a powerful technique, face reduced efficiency when dealing with large datasets because of data processing complexities. While unsupervised learning methods, such as clustering algorithms, have shown potential, their performance is still inferior to supervised techniques, and research in this area is limited and inconclusive. Furthermore, current deep learning approaches, such as bidirectional LSTMs, are resource-intensive, highlighting the need for simpler yet effective models that can be practically implemented for large-scale spam detection tasks.

II. RELATED STUDY

Deep learning has gained significant prominence across various research domains, including applications in natural image processing [12], electricity theft detection [13], diagnosis of human and animal diseases [14][15], and sentiment analysis [16].

For Sentiment analysis, filtration of objective reviews not necessary but also filtration of spam reviews will also increase the accuracy of sentiment analysis. With respect to sentence polarity, there is lot of studies which is about determining the sentiment orientation of a review or comment [17]. Sentiment orientation means that a positive opinion will be an exact

positive, and a negative opinion will be an exact negative [18]. The view, assessment or feeling of a person towards a product, aspect [19], or service is known as a sentiment. Most of the work on reviews or blogs is based on sentiment analysis based on binary classification i.e. positive or negative classes [20]. As text classification is done using machine learning based [21], deep learning based [22] and score based approaches [23]. Training data is used in machine learning and deep learning approaches while different rules based on attributes and entities are used in other methods. To find polarity of opinion based on aspects, lot of researches has been done to extract aspect and aspect based sentiment analysis [24]. Besides machine learning, lot of sentiment analysis work has also been done by deep learning from different dimensions [25]. Work of [26] used word2vec to reduce number of parameters by considering of bag of words in deep learning. Authors [27] investigated the impact on performance over multiple runs by changing hyper parameters for convolutional neural network. OpCNN model based on k-max pooling was presented in [28] by considering word order problem of Chinese. Sentiment classification on tweets to detect tweet as either positive or negative was implemented by LSTM neural network [29].

Different research techniques are available for spam filtration such as filtering Technique based on content [30], spam filtering technique based on heuristic rules [31], spam filtering technique based on previous likeness [32], adaptive spam detection [33] etc. There are many proposed email classification techniques, which detect the spam emails such as case-based technique [9], ANN (Artificial Neural Networks) [34] and SVM (Support-Vector-Machine) [35]. For this purpose LSI (Latent Semantic Indexing) is better [36]. For clustering purpose LSI has also been considered to filter unwanted emails in Chinese and English [37][38].

III. PROPOSED METHODOLOGY

Generally, tasks of proposed work consist of different steps shown in Fig. 1. Manual Feature extraction work excluded in deep learning because it is responsibility of deep learning model-training to handle it automatically.

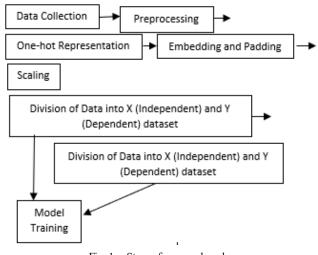


Fig. 1. Steps of proposed work.

The used dataset consists of two columns; one contains text, and the other has a decision as spam or ham [2]. The data set contains 20718 texts, of which 10369 are spam and 10349 are ham. The preprocessing process removes irrelevant opinions, duplicate words, extra spaces, and stop words. It also involves tokenization, converting all words into lower cases, contractions, stemming, and lemmatization. The onehot encoding process is used to convert categorical variables into a form that the machine can easily read. The one-hot encoding performs better in prediction. The proposed work package from TensorFlow. The next step is embedding and padding, where a large sparse vector represents each word with a score (representing an entire vocabulary), and padding adds zeros at the end or start of the sequence to make the sample the same size as the sequence. The proposed work uses embedding and pad sequences packages from TensorFlow.

To train proposed model, we require training data which is a complete set of dependent (Y) and independent (X) variables, across a model can learn. Proposed model has used train_test_split package for this purpose.

A. Model Training on Dataset

This model consists of only dense layers. The name indicates that layers are fully connected through the neurons in a network layer. Each neuron in a layer collects input from all the neurons that appeared in the previous layer, thus, they are densely attached. Fitting of model is shown in Fig. 2.

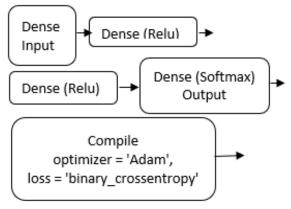


Fig. 2. Model structure of dense layers.

B. Training of Model without Scaling

A simple sequential model has been created with four dense layers. First and last layers are input and output layers and remaining two are hidden layers. Description of model is given below in Table I.

Layer (type)	Output Shape	Param #					
dense (Dense)	(None, 400)	160400					
dense_1 (Dense)	(None, 20)	8020					
dense_2 (Dense)	(None, 15)	315					
dense_3 (Dense)	(None, 1)	16					
Total params: 168751							
Trainable params: 168751							
Non-trainable params: 0							

First three layers are using activation function 'relu' and output layer is using activation function 'softmax'. A 'binary_crossentropy' loss function is used, because 'spam' or 'ham' is a binary problem. Proposed model has been compiled using 'adam' optimizer, because we are using batch option and there also there is neither 'vanishing gradient problem' will occur nor 'dead neurons' will occur. Different attempts have been made to achieve high accuracy based on epoch and batch size. But achieved 69% at 100 epochs with 40 batch-size shown in Table II.

 TABLE II.
 Accuracies of Model (without scaling) with Different Attempts

Epochs	Batch Size	Accuracy
10	40	0.63
50	40	0.68
100	40	0.87
100	100	0.86

C. Training of Model with Scaling

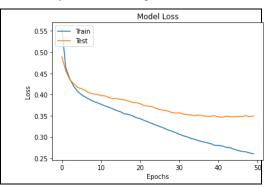
Here scaling concept is used to enhance the accuracy.

To normalize the range of independent variables, scaling feature is used. Its basic purpose is to convert the whole independent variables into range 0 to 1, because this range is very suitable for deep learning models [39].

 TABLE III.
 ACCURACIES OF MODEL (WITH SCALING) WITH DIFFERENT ATTEMPTS

Epochs	Batch Size	Accuracy
10	40	0.80
50	40	0.88
50	100	0.84
Previous Work[28] 0.82	0.82

Different attempts have been made to achieve high accuracy based on epoch and batch size, shown in Table III. And achieved 88% at 100 epochs with 40 batch-size. Remaining measures of confusion matrix are given below in Table IV. Performance of model with respect to loss and with respect to accuracy is shown in Fig. 3.



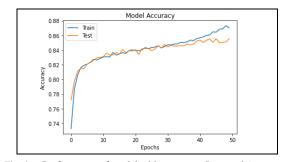


Fig. 3. Performance of model with respect to Loss and Accuracy.

TABLE IV. DIFFERENT MEASURES OF CONFUSION MATRIX

'ork	Precision	Recall	F1-score	
	0.93	0.83	0.87	
	0.80	0.92	0.86	
ted avg	0.87	0.88	0.87	
0.82	0.78	0.80		
	ted avg	0.93 0.80 ted avg 0.87	0.93 0.83 0.80 0.92 ted avg 0.87 0.88	0.93 0.83 0.87 0.80 0.92 0.86 ted avg 0.87 0.88 0.87

opCNN [28] achieved 84% accuracy while proposed deep learning model achieved 88% accuracy. Furthermore, since deep learning models require a lot of resources such as Keras, TensorFlow, Activation Functions, etc., further supervised and unsupervised machine learning models also earn unsatisfactory accuracy for spam detection. In contrast, the proposed LSI technique is comparatively effective.

IV. SPAM DETECTION USING LSI

Major inputs to the proposed model are "reviews" and "automatically generated queries" (AGQ). After processing through LSI, the output is measured in terms of scores. A decision based on these scores will be made, i.e., whether the review is spam or not. Here, the classification category is "spam" and "ham" (not spam). The decision depends upon the pivot value; in the result section, we made different attempts to find the pivot value. If the score of each review is greater than the pivot value, it will be considered "spam," otherwise "ham." The whole process is depicted in Fig. 4.

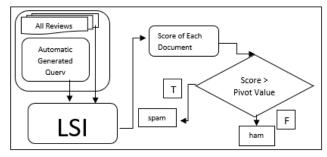


Fig. 4. Proposed framework.

A. Latent Semantic Indexing

The LSI proposed by [40] is an efficient information retrieval algorithm. In LSI, there is a cosine similarity measurement between the coordinates of a document vector and the coordinates of a query vector. The result of cosine similarity measurement "1" means the document is 100% and the result of cosine similarity measurement "0" means the document is very far from a query. A feature matrix from the frequencies of all words in the documents and query will be formed, and singular value decomposition (SVD) will be calculated from this matrix. Singular value decomposition (SVD) can be used to determine the coordinates of the documents and the query. Three matrices, S, V, and U can be easily extracted from SVD. The document coordinates will be determined from S and V as depicted in the algorithm shown in Fig. 5. Finally, a cosine similarity function is applied to these coordinates to find the texts that best match the spam query [41]. Based on LSI techniques algorithm for proposed work is shown in Table V.

TABLE V.	ALGORITHM FOR SPAM DETECTION USING LSI
----------	--

Function 1	LSI (AllReviews, AGQ)
1.	Matrixf: Frequency Matrix from AllReviews
2.	Matrixq: Query Matrix from AGQ from List of
	Spam words and Reviews
3.	V, S, U = numpy.linalg.svd(Matrixf)
4.	UK = Rank 2 Approximation of U
5.	VK = Rank 2 Approximation of V
6.	SK = Rank 2 Approximation by taking two columns
	and two rows of S
7.	CoorR: Each row of V relates to Coordinates of a
	Review
8.	Query Coordinates: Coorq = (Matrixq)TUkSk-1
9.	Find dot product of Coorq with each document
	coordinates CoorR
10	$\sum_{i=1}^{m} (Coor, Coor) = \sum_{i=1}^{n} Coor_R(i) * Coor_q(i)$
10.	$\bigcup_{x=1}^{m} (Coor_{R}, Coor_{q}) = \frac{\sum_{l=1}^{n} Coor_{R}(l) * Coor_{q}(l)}{\sqrt{\sum_{i=1}^{n} (Coor_{R}(l)^{2} \sqrt{\sum_{i=1}^{n} (Coor_{q}(l)^{2}})}}$
	Return (Score of all Documents)
End Func	tion

B. Preprocessing

First of all, it is very necessary to remove noise from the reviews, Eq. (1), Eq. (2), Eq. (3) and Eq. (4) are used to filter the reviews based on stop words and negations.

$$R = \bigcup_{x=1}^{n} R_x \tag{1}$$

$$C(x) = \bigcup_{i=1}^{n} R_i \tag{2}$$

$$FC(x) = \bigcup_{i=1}^{n} \{Antonyme(C_i), if C_{i-1} \notin Negations(3)\}$$

$$FC(x) = \bigcup_{i=1}^{n} \{T_i, if \ T_i \notin StopW$$
(4)

where x = 1, 2, 3...n, StopW means stop words, R represents the total number of reviews, C(x) represents the chunks of the xth reviews, and FC(x) represents the filtered chunks of the xth reviews.

C. AGQ (Automatic Generated Query)

All reviews I and a list of spam words (SW already identified in the introduction) are major inputs for AGQ. The intersection of chunks of each review and spam words (SW) will be determined. Then this list will be updated with AGQ as a union. If a chunk does not belong to SW, then it will be checked in the dictionary (WordNet). If this chunk is not present in the dictionary, then it will also be added in AGQ as a union. Because sometimes spam reviews also contain meaningless words. Since the motive of the proposed model is to find those reviews close to spam words, i.e., AGQ, the whole process is shown in Fig. 6, and the creation of AGQ has been portrayed in Eq. (5) and Eq. (6).

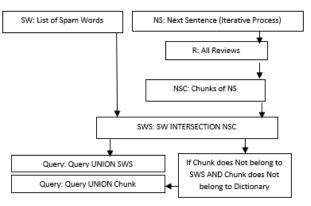


Fig. 5. Process for generating automatic query.

$$AGQ = \bigcup_{x=1}^{n} \{FC(x)_i, \bigcup_{i=1}^{n} \text{ if } FC(x)_i \in SW$$
 (5)

$$AGQ = AGQ \text{ UNION } \bigcup_{x=1}^{n} \{FC(x)_i, \bigcup_{i=1}^{n} \text{ if } FC(x)_i \neq SW \text{ AND } FC(x)_i \neq WordNet$$
(6)

where x = 1, 2, 3...n and $FC(x)_i$ means ith words of xth review. AGQ contains those words from all reviews which belongs to SW (spam words) and those which does not belong to wordnet dictionary.

D. Scoring

Already we have determined FC(x) and AGQ. Now Eq. (7) will find the score of each review FC(x) with spam-query AGQ.

$$LSI(Score)_{x} = \bigcup_{x=1}^{n} (LSI_{x} (FC(x), AGQ))$$
(7)

Decision

If LSI score is greater than pivot value, it means review is 'spam' because it is closest with spam query otherwise considered as 'ham'. Following equation Eq. (8) is used for filtering purpose.

$$R_{decision}(x) = \\ \bigcup_{x=1}^{n} \{ spam_{x} , if \ (LSI(Score)_{x}) > Pivot Value) \\ ham_{x} , else \qquad (8)$$

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

The SMS Spam Collection is a set of SMSs tagged messages that have been collected for SMS Spam research [42]. It consists of column v1 and v2. Column v1 contains 5,574 English messages with label 'ham' and 'spam' and column v2 contains the text of message. The sample listing of the said datasets is presented in Table VI.

IADLE VI. SAMPLE SIMS FROM DATASET	TABLE VI.	SAMPLE SMS FROM DATASET
------------------------------------	-----------	-------------------------

v1	v2
ham	Absolutely wonderful – silky and sexy and comfortable
ham	This dress is perfection! So pretty and flattering.
Ham	Super cute and comfy pull over. Sizing is accurate. Material has a little bit of stretch.
Ham	Loved this top and was really happy to find it on sale!
Spam	100 dating service call 09064012103 box334sk38ch
spam	FREE entry into our 250 weekly competition just text the word WIN to 80086 NOW 18 T&C www.txttowincouk
spam	XXXMobileMovieClub To use your credit click the WAP link in the next txt message or click here httpwap xxxmobilemovieclubcom?n=QJKGIGHJJGCBL
spam	500 New Mobiles from 2004 MUST GO Txt NOKIA to No 89545 & collect yours today From ONLY 1 www4tcbiz 20ptout 08718726270150gbpmtmsg18

A confusion matrix [43] is formed from the four outcomes produced as a result of binary classification. A binary classifier predicts all data instances of a test dataset as either 'spam' or 'ham'. This classification (or prediction) produces four outcomes -true spam (TS), -false spam (FS), -true ham (TH) and -false ham (FH).

Here, in start 0.7 was considered as pivot value, then achieved accuracy was 84%, at pivot values 0.8 & 0.9 accuracy was 88% while at 0.99 accuracy was 54%. So, 0.8 or 0.9 can be considered as pivot value as shown in Fig. 7. Graphs of Confusion matrices at different scores in Fig. 6, also predict that values greater or equal to 0.8 and less or equal to 0.9 can be considered as pivot value.

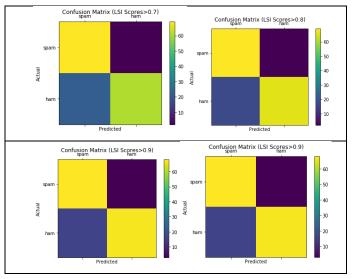


Fig. 6. Confusion matrices at all selected scores.

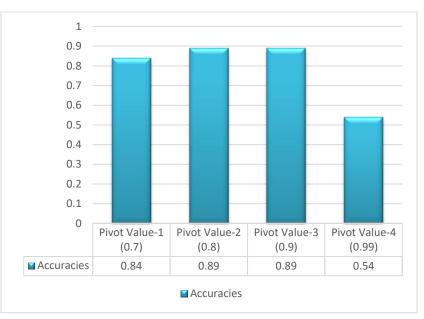


Fig. 7. Accuracies at different scores.

Table VII shows some of sampled documents based on proposed method to detect text as 'ham' or 'spam' using LSI-score greater than pivot values 0.8 and 0.9.

Now at detected pivot values, proposed model achieved 0.89 precision and 0.88 recall as shown in Table VIII.

TABLE VII. SAMPLE OF DOCUMENTS WITH LSI SCORES GREATER THAN 0.8 AND 0.9

S.	Revi	LSI	Act	Detected Based on	Detec
No	ews	Score	ual	Score > 0.8	ted
					Base
					d on
					Score
					> 0.9
1	d[0]	0.999	На	Spam	
		82	m	-	spam
2	d[1]	0.337	На	Ham	ham
		082	m		nam
3	d[2]	0.492	На	Ham	ham
		025	m		nam
4	d[3]	0.491	На	Ham	ham
		148	m		nam
5	d[4]	0.989	На	Spam	spam
		738	m		span
6	d[5]	0.551	На	Ham	ham
		706	m		nam
7	d[6]	-	На	Ham	
		0.181	m		ham
		23			
8	d[7]	-	На	Ham	
		0.215	m		ham
		59			
9	d[8]	0.271	Ha	Ham	ham
		523	m		nam
10	d[9]	0.431	На	Ham	ham
		423	m		nam
20	d[82]	0.975	Spa	Spam	spam
		451	m		span
21	d[83]	0.976	Spa	Spam	snam
		627	m		spam
22	d[84]	0.976	Spa	Spam	spam
		538	m		spam

TABLE VIII. STATISTICAL RESULTS AT DIFFERENT PIVOT VALUES

Pivot Values	Class	Precision	Recall	F1- Score
	Ham	0.97 0.80 0.87	0.80 0.80 0.87	0.87 0.80 0.87
0.8	Spam	0.80 0.80 0.87	0.97 0.80 0.87	0.88 0.80 0.87
	Avg	0.89 0.80 0.87	0.88	0.88
0.9	Ham	0.96	0.81	0.88
0.9	spam	0.81	0.96	0.88
	avg	0.89	0.88	0.88

Recently accuracies of supervised learning approaches have been increased, while unsupervised approaches are still working on increasing the efficiency. Because major used source are spam words, which are not only present in spamtext while also in ham-text. Table IX is showing that proposed model gained high performance with respect Supervised, Unsupervised, Combined and Active Learning.

TABLE IX. COMPARISON WITH DIFFERENT APPROACHES

Methods	Precision	Accuracy
Supervised Learning Methods	49%	78%
Unsupervised Learning Methods	42%	80%
Combined Approach	64%	83%
Adaptive Resonance Theory (ART)	75%	89%
Active Learning	87%	88%
Proposed Work	89%	89%

VI. CONCLUSION

Spam is a serious issue that is not just annoying to the enduser but also financially damaging and security risks. In this paper, state-of-the-art models and LSI model were experimented against the task of detecting spam emails. To validate the generalization capabilities of the proposed method, its experimental results have been compared with CNN and OPCNN models. CNN achieved 82% and opCNN achieved 84% accuracy while proposed deep learning model achieved 88% accuracy. Although accuracy of proposed model is less than the accuracy of another base line whose accuracy is 96% (Spam with Deep Model). But this work uses bidirectional LSTM, which is computationally expensive and also uses reviews with sequence length less than 300 with dataset length 5000. Proposed work has been implemented on 20718 lengths of dataset also containing reviews with length more than 300.

Another less computationally expensive proposed model has been implemented using LSI concept to detect 'spams' from given data. The major theme of this work is to avoid laborious work for detecting patterns and making rules and implementation from machine learning methods. Based on the experimental results through confusion matrix, it found that results generated from the proposed method show a significant improvement from existing techniques related not only to precision and accuracy, but also to recall and f1-score which are 88% shown in Table IX. Fig. 8 shows that the proposed work provides better results than previous approaches.

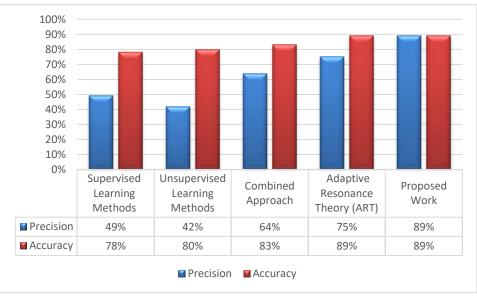


Fig. 8. Comparison of proposed LSI work with alternative approaches.

VII. LIMITATIONS AND FUTURE WORK

This study demonstrates significant progress in spam detection; however, certain limitations remain that open avenues for future research. The dataset used in this study comprises 5,574 English-language messages, which, while effective for the current analysis, limits the generalizability of the findings. Future work could focus on increasing the dataset size and incorporating data from other languages to improve model robustness and applicability across diverse linguistic contexts. Additionally, the automatic query process in this work relies on the WordNet dictionary. While effective, the exploration of other dictionaries or lexical resources could enhance the flexibility and accuracy of the query generation process. The pivot value of 0.7, achieved with the current dataset size, may vary with larger or smaller datasets, suggesting the need for further investigation into optimal pivot values for datasets of different sizes.

ACKNOWLEDGMENT

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under

Grant No. 94-830-1442. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

References

- A. Qazi, N. Hasan, R. Mao, M. E. M. Abo, S. K. Dey, and G. Hardaker, "Machine Learning-Based Opinion Spam Detection: A Systematic Literature Review," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3399264.
- [2] H. Khan, M. U. Asghar, M. Z. Asghar, G. Srivastava, P. K. R. Maddikunta, and T. R. Gadekallu, "Fake Review Classification Using Supervised Machine Learning," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12664 LNCS, pp. 269–288, 2021, doi: 10.1007/978-3-030-68799-1_19.
- [3] S. Si, Y. Wu, L. Tang, Y. Zhang, and J. Wosik, "Evaluating the Performance of ChatGPT for Spam Email Detection," Comput. Lang., 2024, [Online]. Available: http://arxiv.org/abs/2402.15537.
- [4] M. Gaur, R. Aggrawal, A. Garg, and A. Singh, "Fake Profile Detection on Social sites," Proc. - 2024 6th Int. Conf. Comput. Intell. Commun. Technol. CCICT 2024, pp. 530–537, 2024, doi: 10.1109/CCICT62777.2024.00089.
- [5] Z. S. Torabi, M. H. Nadimi-Shahraki, and A. Nabiollahi, "Efficient Support Vector Machines for Spam Detection: A Survey," IJCSIS) Int. J. Comput. Sci. Inf. Secur., vol. 13, no. January, pp. 10–28, 2015, [Online]. Available: http://sites.google.com/site/ijcsis/.
- [6] J. S. Whissell and C. L. A. Clarke, "Clustering for semi-supervised spam

filtering," ACM Int. Conf. Proceeding Ser., pp. 125-134, 2011, doi: 10.1145/2030376.2030391.

- [7] R. Y. K. Lau, S. Y. Liao, R. Chi-Wai Kwok, K. Xu, Y. Xia, and Y. Li, "Text mining and probabilistic language modeling for online review spam detection," ACM Trans. Manag. Inf. Syst., vol. 2, no. 4, 2011, doi: 10.1145/2070710.2070716.
- [8] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. Al Najada, "Survey of review spam detection using machine learning techniques," J. Big Data, vol. 2, no. 1, 2015, doi: 10.1186/s40537-015-0029-9.
- [9] I. AbdulNabi and Q. Yaseen, "Spam email detection using deep learning techniques," Procedia Comput. Sci., vol. 184, no. 2019, pp. 853–858, 2021, doi: 10.1016/j.procs.2021.03.107.
- [10] A. Sharma and S. Kumar, "Machine learning and ontology-based novel semantic document indexing for information retrieval," Comput. Ind. Eng., vol. 176, 2023, doi: 10.1016/j.cie.2022.108940.
- [11] "https://blog.prospect.io/455-email-spam-trigger-words-avoid-2018.".
- [12] S. M. Saqib, M. Z. Asghar, A. Al-rasheed, M. A. Khan, and Y. Ghadi, "DenseHillNet: a lightweight CNN for accurate classification of natural images," PeerJ Comput. Sci., pp. 1–21, 2024, doi: 10.7717/peerjcs.1995.
- [13] S. M. Saqib et al., "Deep learning-based electricity theft prediction in non-smart grid environments," Heliyon, vol. 10, no. 15, 2024, doi: 10.1016/j.heliyon.2024.e35167.
- [14] S. M. Saqib et al., "Cataract and glaucoma detection based on Transfer Learning using MobileNet," Heliyon, vol. 10, no. 17, 2024, doi: 10.1016/j.heliyon.2024.e36759.
- [15] S. M. Saqib et al., "Lumpy skin disease diagnosis in cattle: A deep learning approach optimized with RMSProp and MobileNetV2," PLoS One, vol. 19, no. 8 August, 2024, doi: 10.1371/journal.pone.0302862.
- [16] S. Ahmad, S. Muhammad, and A. Hassan, "CNN and LSTM based hybrid deep learning model for sentiment analysis on Arabic text reviews," Mehran Univ. Res. J. Eng. Technol., vol. 43, no. 2, pp. 183– 194, 2024, doi: https://doi.org/10.22581/muet1982.3130.
- [17] F. Wu, Y. Huang, and Z. Yuan, "Domain-specific sentiment classification via fusing sentiment knowledge from multiple sources," Inf. Fusion, vol. 35, pp. 26–37, 2017, doi: 10.1016/j.inffus.2016.09.001.
- [18] B. Liu, Sentiment Analysis and Opinion Mining, vol. 5, no. 1. 2012.
- [19] L. Shu, H. Xu, and B. Liu, "Lifelong Learning CRF for Supervised Aspect Extraction," in Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, 2017, pp. 148–154, doi: 10.18653/v1/P17-2023.
- [20] A. A. A. Esmin, R. L. De Oliveira, and S. Matwin, "Hierarchical classification approach to emotion recognition in twitter," in Proceedings - 2012 11th International Conference on Machine Learning and Applications, ICMLA 2012, 2012, vol. 2, no. March, pp. 381–385, doi: 10.1109/ICMLA.2012.195.
- [21] N. Sureja, N. Chaudhari, P. Patel, J. Bhatt, T. Desai, and V. Parikh, "Hyper-tuned Swarm Intelligence Machine Learning-based Sentiment Analysis of Social Media," Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15415–15421, 2024, doi: 10.48084/etasr.7818.
- [22] D. Elangovan and V. Subedha, "Adaptive Particle Grey Wolf Optimizer with Deep Learning-based Sentiment Analysis on Online Product Reviews," Eng. Technol. Appl. Sci. Res., vol. 13, no. 3, pp. 10989– 10993, 2023, doi: 10.48084/etasr.5787.
- [23] E. Aljohani, "Enhancing Arabic Fake News Detection: Evaluating Data Balancing Techniques Across Multiple Machine Learning Models," Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15947–15956, 2024, doi: 10.48084/etasr.8019.
- [24] S. Gojali and M. L. Khodra, "Aspect based sentiment analysis for review rating prediction," 2016, doi: 10.1109/ICAICTA.2016.7803110.
- [25] K. Dashtipour, M. Gogate, A. Adeel, H. Larijani, and A. Hussain, "Sentiment analysis of persian movie reviews using deep learning," Entropy, vol. 23, no. 5, pp. 1–16, 2021, doi: 10.3390/e23050596.
- [26] R. Johnson and T. Zhang, "Effective use of word order for text categorization with convolutional neural networks," in NAACL HLT

2015 - 2015 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Proceedings of the Conference, 2015, no. 2011, pp. 103–112, doi: 10.3115/v1/n15-1011.

- [27] Y. Zhang and B. Wallace, "A Sensitivity Analysis of (and Practitioners' Guide to) Convolutional Neural Networks for Sentence Classification," in Pro_ceedings of the 8th International Joint Conference on Natural Language Processing, 2015, pp. 253–263, [Online]. Available: http://arxiv.org/abs/1510.03820.
- [28] S. Zhao, Z. Xu, L. Liu, M. Guo, and J. Yun, "Towards Accurate Deceptive Opinions Detection Based on Word Order-Preserving CNN," Math. Probl. Eng., vol. 2018, pp. 1–8, 2018, doi: 10.1155/2018/2410206.
- [29] D. Tang, B. Qin, and T. Liu, "Document modeling with gated recurrent neural network for sentiment classification," in Conference Proceedings - EMNLP 2015: Conference on Empirical Methods in Natural Language Processing, 2015, no. September, pp. 1422–1432, doi: 10.18653/v1/d15-1167.
- [30] V. Christina, "Email Spam Filtering using Supervised Machine Learning Techniques.," Int. J. ..., vol. 02, no. 09, pp. 3126–3129, 2010, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scop e=site&authtype=crawler&jrnl=09753397&AN=58495579&h=iA3%2F X2tuV1JYXccJpWbuYj6fk0pDvAcACLAAXisHLHSX%2FLt4Hz9xiQ MueUTWkrzsKKireW27Sl2NterjVC9NCQ%3D%3D&crl=c.
- [31] J. R. Méndez, F. Fdez-Riverola, F. Díaz, E. L. Iglesias, and J. M. Corchado, "A comparative performance study of feature selection methods for the anti-spam filtering domain," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 4065 LNAI, pp. 106–120, 2006, doi: 10.1007/11790853_9.
- [32] G. Sakkis, I. Androutsopoulos, G. Paliouras, V. Karkaletsis, C. D. Spyropoulos, and P. Stamatopoulos, "Stacking classifiers for anti-spam filtering of e-mail," 2001, [Online]. Available: http://arxiv.org/abs/cs/0106040.
- [33] L. Pelletier, J. Almhana, and V. Choulakian, "Adaptive filtering of SPAM," Proc. - Second Annu. Conf. Commun. Networks Serv. Res., pp. 218–224, 2004, doi: 10.1109/DNSR.2004.1344731.
- [34] G. M. Shahariar, S. Biswas, F. Omar, F. M. Shah, and S. Binte Hassan, "Spam Review Detection Using Deep Learning," 2019 IEEE 10th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2019, no. October, pp. 27–33, 2019, doi: 10.1109/IEMCON.2019.8936148.
- [35] N. Bouguila and O. Amayri, "A discrete mixture-based kernel for SVMs: Application to spam and image categorization," Inf. Process. Manag., vol. 45, no. 6, pp. 631–642, 2009, doi: 10.1016/j.ipm.2009.05.005.
- [36] S. M. Saqib, K. Mahmood, and T. Naeem, "Comparison of LSI algorithms without and with pre-processing: using text document based search," Accent. Trans. Inf. Secur., vol. 1, no. 4, pp. 44–51, 2016.
- [37] A. Huang, D. Milne, E. Frank, and I. H. Witten, "Clustering Documents using a Wikipedia-based Concept Representation," in PAKDD 2009: Advances in Knowledge Discovery and Data Mining, 2009, pp. 628– 636.
- [38] Q. YANG, "SUPPORT VECTOR MACHINE FOR CUSTOMIZED EMAIL FILTERING BASED ON IMPROVING LATENT SEMANTIC INDEXING," in , Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 2005, pp. 18–21.
- [39] "https://www.atoti.io/when-to-perform-a-feature-scaling/ (Visited On 3 July, 2021).".
- [40] F. Horasan, "Latent Semantic Indexing-Based Hybrid Collaborative Filtering for Recommender Systems," Arab. J. Sci. Eng., vol. 47, no. 8, pp. 10639–10653, 2022, doi: 10.1007/s13369-022-06704-w.
- [41] G. J. Phadnis N, "Framework for document retrieval using latent semantic indexing," Int. J. Comput. Appl., vol. 94, no. 14, 2014.
- [42] "https://www.kaggle.com/ishansoni/sms-spam-collection-dataset ." .
- [43] S. Muthulakshmi, "Comparative Study on Classification Meta Algorithms," Ijircce.Com, 2013. https://www.rroij.com/openaccess/comparative-study-on-classificationmetaalgorithms.php?aid=43760.