Indian journal of
Engineering

To Cite:
Aiyeniko O, Aro TO, Olukiran OA, Alfa AA, Umoru LC, Owonipa A. Enhanced accuracy for sms spam detection using One Dimensional Ternary Patterns (1D-TP) and firefly algorithm. *Indian Journal of Engineering*, 2023, 20, e4ije1004
doi: https://doi.org/10.54905/disssi/v20i53/e4ije1004

Author Affiliation:
[1]Department of Computer Sciences, Lagos State University, Lagos State. Nigeria
[2]Department of Computer Science, Confluence University of Science and Technology, Osara, Kogi State, Nigeria
[3]Department of Computer Engineering, Ladoke Akintola University, Ogbomoso, Oyo State, Nigeria
[4]Division of Computer Science and Mathematics University of Stirling, United Kingdom

[*]**Corresponding author**
Department of Computer Science, Confluence University of Science and Technology, Osara, Kogi State
Nigeria
Email: taiwo774@gmail.com

Peer-Review History
Received: 03 February 2023
Reviewed & Revised: 05/February/2023 to 24/February/2023
Accepted: 26 February 2023
Published: 3 March 2023

Peer-Review Model
External peer-review was done through double-blind method.

Indian Journal of Engineering
pISSN 2319–7757; eISSN 2319–7765

DISCOVERY
SCIENTIFIC SOCIETY

Enhanced accuracy for sms spam detection using One Dimensional Ternary Patterns (1D-TP) and firefly algorithm

Aiyeniko O[1], Aro TO[2*], Olukiran OA[3], Alfa AA[2], Umoru LC[2], Owonipa A[4]

ABSTRACT

The Short Message Service (SMS) is a broadly used mobile communication channel; its attractiveness is traceable to many factors such as easy delivery method, cheap approach and expedient usage. However, unwanted messages referred to as SMS Spam has been identified to be one of the major problems for users and mobile service providers. This paper developed an SMS Spam detection model by optimization of One-Dimensional Ternary Pattern (1D-TP) feature extraction algorithm through the application of a robust optimization algorithm known as the firefly algorithm. The implementation of the model was done in a python environment due to its unique features in data/text analysis and classification. Accuracy of the optimised 1D-TP was done using five selected learning algorithms; Artificial Neural Network (ANN), Decision Tree (C4.5), Naïve Bayes (NB), K Nearest Neighbour (KNN) and Support Vector Machne (SVM). The accuracy of SMS Spam detection was evaluated with three datasets: Kaggle SMS Spam, British English SMS Corpora and SMS Spam Corpus v0.1 dataset. Results showed the effectiveness of the firefly algorithm with the best accuracy of 93.94% recorded in the Kaggle SMS Spam dataset using NB classifier when $\beta = 0$ for upper features compared with the other two SMS spam datasets, which the best accuracy obtained is 92.96% in British English SMS Corpora dataset using NB when $\beta = 1$ for lower features and accuracy of 91.97% was recorded in SMS Spam Corpus v0.1 dataset using NB when $\beta = 4$ for upper features. The improvement was shown in the output through a reduction in the level of misclassification.

keywords: Accuracy, Firefly Algorithm, SMS Spam, One Dimensional Ternary Pattern

1. INTRODUCTION

Short Message Service remains the strongest tool for communication that is predominantly used by mobile users (Shah and Farik, 2017; Jameel, 2018). SMS is more than the usual texting, it has been employed in several fields for authentication like retrieval systems for information, one-time password

delivery, configuration of a phone, configuration of Over-The-Air (OTA) and shared website notifications (Mizuki et al., 2013). SMS Spam is a recognised major problem in mobile communication across the globe despite the several advantages connected with SMS (Devi et al., 2019). SMS Spam is usually referred to as unsolicited or undesirable SMS sent to many receivers (Osho et al., 2015). An unsolicited message is generally conveyed in bulk for money-making or other purposes (Chaudhari et al., 2016). Detection of SMS Spam is more perplexing than e-mail spam detection due to the SMS's restricted length, regional content usage, abbreviations and shortcut words and limited information in header format (Rodan et al., 2016).

Researchers have identified the feature extraction phase as one of the most significant procedures in the detection of Spam SMS detection (Uysal et al., 2013). Extraction of features entails the decrease of the original set of data to a more manageable form (Kaur and Rajput, 2013). Feature reduction gives an estimate of original features in reduced proportions; however, a similar structure of initial features is retained (Telgaonkar & Deshmukh, 2015). Feature extraction has been considered a pertinent stage in SMS Spam detection. There are quite a lot of features that will be useful to differentiate spam from ham. The limitation of feature extraction is that no consideration of how relevant features are during the extraction phase, there may exist the inclusion of redundant features (Fasna et al., 2016). It is therefore necessary to apply a feature selection algorithm which considers the subset of the feature. The approach to obtaining a subset of original features for use in classification and model construction is known as feature selection (Derakhshii & Ghaemi, 2014). This reduces the number of features, removes irrelevant and noisy features that show no effect on the accuracy of the classification model (Kumar and Minz, 2014).

This paper introduced one-dimensional ternary patterns (1D-TP) algorithm as a new feature extraction technique to choose features from SMS messages. 1D-TP is a statistical approach built on the order of occurrence of the characters Vikas & Kaur, (2016), the algorithm patterns were developed from the comparison of the Unicode value of the characters in SMS messages with the Unicode values of their neighbours. A firefly algorithm was used to optimise the 1D-TP parameters to obtain significant and discriminant features before classification.

Related work

An optimised SVM was used for the detection of SMS Spam through the application of a meta-heuristic algorithm (Xia and Deng, 2020). The English spam classification and obtained features with unique sensitive word coding were achieved. The model has a particular reference value for spam classification. The convergence speed of the algorithm was increased when Particle Swarm Optimization (PSO) was used. The proposed optimised SVM model was compared with the conventional SVM, the model time taken was decreased nearly to half and the improvement in classification was by 12.841%.

Agarwal and Kumar, (2019) came up with a detection model for email spam using a combined technique. Naïve Bayes (NB) algorithm and PSO were applied in the study. NB was used for learning and classification of email content as either non-spam or spam. The PSO was considered for the global optimization of the parameters of the NB approach. The evaluation of detection model for email spam was done using Ling spam dataset. The metrics for evaluation were achieved using accuracy precision, recall and f-measure. Outputs of PSO performed better the individual NB approach.

Shuaib et al., (2019) presented a detection system by the introduction of a nature-inspired optimization method, the whale optimization algorithm (WOA) was employed for salient features selection in the email corpus dataset. A classification of emails as spam and non-spam using rotation forest. The complete datasets were used and the rotation forest algorithm evaluation was done before and after feature selection with WOA. Results revealed that the rotation forest algorithm after feature selection with WOA recorded an accuracy of 99.9% and a low false-positive rate of 0.0019.

Faris et al., (2018) built an intelligent detection system using a Genetic Algorithm (GA) and Random Weight Network (RWN) to detect email spam. Also, a programmed identification capability was incorporated into the system to identify the most significant features at the detection stage. Naïve Bayes (NB), 1-Neural Network (1-NN), 5- Neural Network (5-NN), Grid Support Vector Machine (G-SVM) and Random Weight Network (RWN) were used to classify SMS spam. The system was evaluated through a series of experiments based on three email corpora: SpamAssassin, Ling Spam and CSDMC2010 Corpus. Results showed that the RWN gave the highest accuracy of 92.20% in SpamAssin, 89.50% in Lungspam and 88.70% in CSDMC2010.

Chaudhari and Shah, (2017) developed a system for SMS filtering using a hybrid method of data mining techniques through a combination of Booyer more and Support Vector Machine (SVM) algorithms. This helps to overcome the problem of some companies' experience with Spammers that use unsolicited services for advertisement or promotion to convey the undesirable Spam message to the mobile phone user. The SMS spam produces disruption in communication and also consume the network bandwidth. The result gave a better accuracy of 89.33% in combined Booyer more and SVM, while 86.64% was recorded in the only SVM.

Kaya and Ertugrul, (2016) introduced a new technique for the extraction of features in the detection of SMS Spam. One-Dimensional Ternary Pattern was applied to obtain features from SMS messages. Five machine learning techniques; Bayesian Network (BN), Naïve Bayes (NB), Radial Basis Feed-forward Neural Network (RBFNN), K-Nearest Neighbours (KNN) and RF were used for classification. The system was evaluated with three different SMS corpora datasets. SMS Spam Corpus v.0.1 (DS1), British English SMS Corpora (DS2) and DS3. Accuracies recorded and other metrics showed that the proposed approach can be successfully employed in SMS spam filtering.

2. MATERIALS AND METHODS

The enhanced accuracy of the SMS Spam detection model follows stepwise processes. Acquisition of datasets was done through three publicly available datasets online: Kaggle SMS Spam, British English SMS Corpora and SMS Spam Corpus v0.1 dataset Kaya and Ertugrul, (2016). The data were preprocessed to eliminate unwanted characters by stemming and converting a message to UTF-8 values of characters in the text using the python function. After the preprocessing phase, the preprocessed data was passed into the 1D-TP feature extraction algorithm. Firefly Optimization algorithm was applied to optimize the 1D-TP extracted features through parameters setting. The optimized features were classified into spam or ham. The framework of the SMS SPAM detection model is shown in Figure 1.

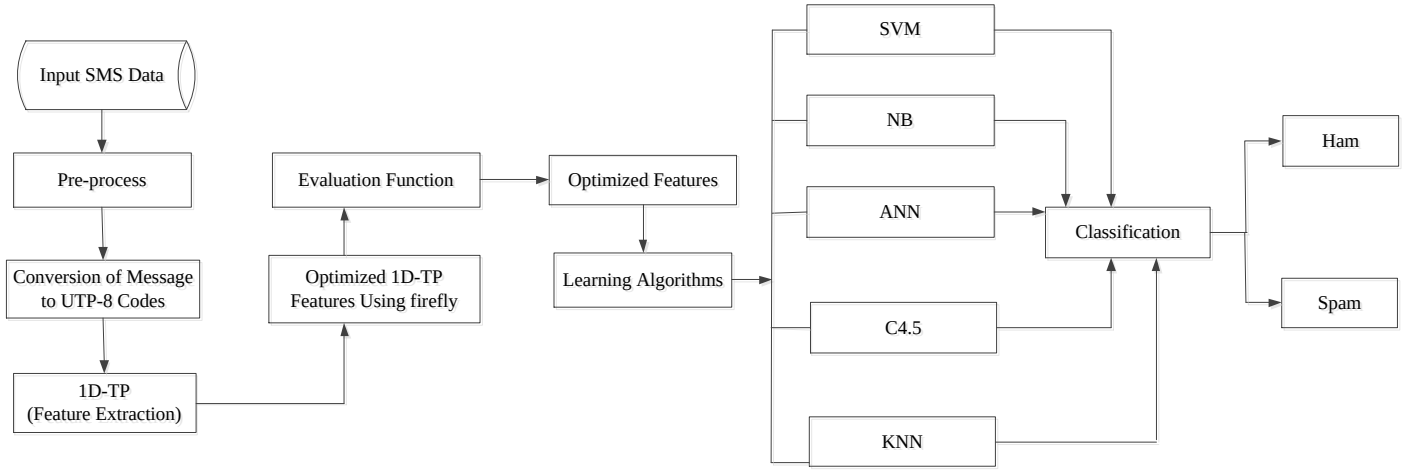

Figure 1 Block Diagram of the developed SMS Spam Detection Model

Method of Dataset Collection

The improved accuracy of the SMS Spam detection model was evaluated using three different SMS datasets: Kaggle SMS Spam dataset, SMS Spam Corpus v.0.1 and British English SMS Corpora Kaya and Ertugrul, (2016).

Kaggle SMS Spam Dataset

The dataset comprises English SMS messages of about 5,574 messages, labelled to be either legitimate (ham) or spam. The files contain one message per line. Each line is composed of two columns: V1 contains the label (ham or spam) and v2 contains the raw text. The messages are classified as Spam or Ham using NLTK and Scikit-learn.

SMS Spam Corpus v.0.1

The SMS Spam Corpus is a set of SMS-tagged messages collected for SMS Spam research. It consists of 1002 legitimate (ham) messages and 322 spam messages.

British English SMS Corpora Dataset

The dataset was acquired from Grumble Text, a website that gathers SMS Spam that was uploaded by people who complain about receiving SMS Spam. This corpus contains a total number of 450 legitimate (ham) and 425 spam.

Data Preprocessing

Preprocessing was achieved by the removal of stop words, words lesser than or equal to two, performing stemming to reduce the vocabulary and converting the remaining part of the message to UTF-8 values of characters in the text. Stemming was done using the Porter Stemming Algorithm. The Pre-process step is shown in Figure 2.

Step 1: Start
Step 2: Perform stemming
/*Porter's algorithm*/
from nltk.stem import PorterStemmer
from nltk.tokenize import sent_tokenize, word_tokenize
ps = PorterStemmer()
Step 3: Convert the message to UTF-8 values of the characters in the text
Step 4: Output the UTF-8 values of the SMS message
Step 5: End

Figure 2 Pre-process phase

One-Dimensional-Ternary Pattern (1D-TP) Algorithm

In 1D-TP, patterns are formed from the comparisons of the Unicode values of the characters in SMS messages with the Unicode values of their neighbours. The value of each member of the 1-D series is compared with its neighbours and the result of these comparisons is expressed as a decimal number. For text messages, the comparisons were carried out after converting the characters to their UTF-8 values.

Firefly Algorithm (FA)

A firefly algorithm is a computationally efficient, nature-inspired metaheuristic population-based optimization algorithm that mimics a firefly's attraction to a flashing light (Ali et al., 2014). The attractiveness is proportional to the brightness and they both decrease as their distance increases. Thus, for any two flashing fireflies, the less bright one will move toward the brighter one. If there is no brighter one than a particular firefly, it will move randomly. The procedures of the algorithm are shown in Figure 3.

Step 1: Start
Step 2: Generate initial population of fireflies
Step 3: Evaluate fitness of all fireflies from the objective function
Step 4: Update the light intensity (fitness value) of fireflies
Step 5: Rank the fireflies and update position
Step 6: If maximum iteration is met Goto Step 7 else Goto Step 3
Step 7: End

Figure 3 Firefly Algorithm

4. RESULTS AND DISCUSSION

The results of the improved accuracy for SMS Spam detection using the optimized 1D-TP technique are discussed in these sections. Different accuracies were obtained for the three datasets used as shown in the following tables.

From Table 1, the highest accuracy of 89.88% was recorded in NB when the β = 2 in upper features, The lowest accuracy of 85.12% was obtained in NB when the β = 1 for lower features.

Table 1 British English SMS Corpora Dataset (Accuracy with no feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Lower Features	NB	88.72	85.12	88.53	87.89	87.39
	C4.5	89.16	85.31	88.32	89.05	87.95
	ANN	87.07	86.34	87.94	86.92	88.70
	KNN	87.32	89.41	87.71	88.08	89.26
	SVM	86.15	85.50	84.35	87.23	88.62
Upper Features	NB	87.59	88.83	89.88	88.77	86.12
	C4.5	88.92	87.57	88.59	87.11	88.49
	ANN	87.61	88.99	87.92	88.79	89.85
	KNN	88.17	87.68	89.79	88.43	87.95
	SVM	87.91	88.87	86.88	88.96	87.30

Table 2 British English SMS Corpora Dataset (Accuracy with feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Low Features	NB	90.23	90.74	91.50	90.58	91.70
	C4.5	90.25	91.46	90.09	91.39	90.69
	ANN	91.16	90.94	90.30	91.33	91.69
	KNN	90.87	90.29	91.85	90.04	91.43
	SVM	90.71	90.97	91.23	90.75	91.76
Upper Features	NB	91.53	92.96	90.95	90.53	91.45
	C4.5	90.53	91.53	90.12	91.92	91.15
	ANN	90.34	90.84	91.19	90.52	91.54
	KNN	91.90	90.57	91.09	90.05	90.56
	SVM	90.97	91.59	90.86	90.89	91.45

From Table 2, the highest accuracy of 92.96% was recorded in NB when $\beta = 1$ for lower features. The lowest accuracy of 90.04% was obtained in KNN when $\beta = 3$ for lower features.

Table 3 Kaggle SMS Spam Dataset (Accuracy with no feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Lower Features	NB	86.97	85.54	85.81	85.32	85.56
	C4.5	86.42	86.45	88.09	88.15	87.98
	ANN	85.56	86.89	85.76	86.89	86.15
	KNN	86.54	86.94	86.97	85.22	86.90
	SVM	86.65	86.23	85.37	86.96	86.38
Upper Features	NB	87.85	86.23	86.30	86.42	86.29
	C4.5	87.36	87.29	86.34	87.51	86.96
	ANN	85.50	86.92	87.70	86.79	85.75
	KNN	85.03	85.31	85.78	85.34	86.40
	SVM	86.85	86.81	86.25	86.91	85.86

From Table 3, the highest accuracy of 88.15% was recorded in NB when $\beta = 3$ for lower features. The lowest accuracy of 85.03% was recorded in KNN when $\beta = 0$ for lower features.

Table 4 Kaggle SMS Spam Dataset (Accuracy with feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Lower Features	NB	91.65	90.46	91.98	91.49	90.52
	C4.5	90.26	91.95	91.10	91.85	91.01
	ANN	91.79	90.82	91.46	92.67	90.65
	KNN	90.59	92.20	81.50	90.30	91.45
	SVM	91.30	91.75	92.56	91.04	91.51
Upper Features	NB	93.94	92.45	93.67	92.40	93.05
	C4.5	91.16	90.95	91.75	90.19	91.91
	ANN	91.45	90.20	90.28	90.81	90.50
	KNN	91.71	91.45	90.01	90.25	90.97
	SVM	92.65	91.90	91.60	92.25	92.09

From Table 4, the highest accuracy of 93.94% was recorded in NB when $\beta = 0$ for upper features. The lowest accuracy of 90.01% was obtained in KNN when $\beta = 2$ for lower features.

Table 5 SMS Spam Corpus V0.1 Dataset (Accuracy with no feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Lower Features	NB	87.97	87.12	88.18	87.27	88.92
	C4.5	86.41	88.14	88.10	85.67	86.87
	ANN	85.98	88.54	87.24	86.20	86.45
	KNN	87.60	87.96	86.50	85.30	87.92
	SVM	86.40	85.82	85.71	86.92	86.45
Upper Features	NB	88.12	89.29	88.09	88.19	89.92
	C4.5	86.18	87.19	87.91	86.90	87.75
	ANN	85.62	86.14	85.91	86.53	86.10
	KNN	85.60	85.01	86.90	86.93	85.95
	SVM	86.85	85.78	86.02	86.84	86.29

From Table 5, the highest accuracy of 89.92% was recorded in NB when $\beta = 4$ for upper features. The lowest accuracy of 85.01% was obtained in KNN when $\beta = 1$ for lower features.

Table 6 SMS Spam Corpus V0.1 Dataset (Accuracy with feature selection %)

Features	Model	$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
Lower Features	NB	90.34	91.40	90.50	90.54	91.30
	C4.5	90.03	90.93	91.60	90.11	90.59
	ANN	90.95	91.01	91.68	90.95	90.98
	KNN	91.16	90.51	91.05	90.89	91.02
	SVM	91.52	91.93	91.92	91.13	91.42
Upper Features	NB	91.34	90.45	91.34	90.67	91.97
	C4.5	91.45	90.75	91.27	90.36	90.65
	ANN	91.04	90.36	91.19	91.09	90.58
	KNN	90.80	91.23	91.03	91.71	91.84
	SVM	90.93	91.78	90.34	91.53	90.80

From Table 6, the highest accuracy of 91.97% was recorded in NB when $\beta = 4$ for lower features. The lowest accuracy of 90.03% was obtained in C4.5 when $\beta = 0$ for lower features.

5. CONCLUSION

This paper developed an enhanced accuracy for SMS SPAM detection using a one-dimensional ternary pattern as a feature extraction approach. A nature-inspired optimization known as firefly Algorithm was introduced to optimize the 1D-TP extracted features through parameters setting. Three publicly available online datasets; British English Corpus, Kaggle SMS Spam and SMS Spam Corpora v0.1 datasets were used employed to evaluate the model. The following enhanced accuracy results were recorded in the three SMS Spam datasets; the British English SMS Corpora dataset gave the highest accuracy of 92.96% in NB when β = 1 for lower features, the Kaggle SMS Spam dataset gave the highest accuracy of 93.94% in NB when β = 0 for upper features and SMS Spam Corpus v0.1 dataset gave the highest accuracy of 91.97% was recorded in NB when β = 4 for lower features. The study concluded that the accuracy of the optimised 1D-TP with firefly using NB for the Kaggle SMS Spam dataset performed better than other datasets, which thus revealed the effectiveness of the introduced nature-inspired optimization algorithm.

Ethical issues

Not applicable.

Informed consent

Not applicable.

Funding

This study has not received any external funding.

Conflict of Interest

The author declares that there are no conflicts of interests.

Data and materials availability

All data associated with this study are present in the paper.

REFERENCES AND NOTES

1. Agarwal K, Kumar T. Approach of Naïve Bayes and Particle Swarm, in 2018 Second International Conference on Intelligent Computing and Control Systems 2019; 685–690.
2. Ali N, Othman MA, Husain MN, Misran MH. A review of firefly algorithm, ARPN. J Eng Appl Sci 2014; 9(10):1732–1736.
3. Chaudhari N, Shah V. SMS filtering in binary classification using Hybrid Approach of Data mining Techniques. Int J Adv Res Comput Commun Eng 2017; 6:184–186.
4. Chaudhari N, Jayvala P, Vinitashah P. Survey on Spam SMS filtering using Data mining Techniques. Int J Adv Res Comput Commun Eng 2016; 5(11):193–195.
5. Derakhshii M, Ghaemi MR. Classifying Different Feature Selection Algorithms Based on the Search Strategies. Int Conf Mach Learn Electr Mech Eng 2014; 17–21.
6. 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.
7. Faris H, Al-zoubi AM, Asghar A, Aljarah I, Mafarja M. An Intelligent System for Spam Detection and Identification of the most Relevant Features based on Evolutionary Random Weight Networks An intelligent system for spam detection and identification of the most relevant features based on evolutionary Random. Inf Fusion 2018; 1–18.
8. Fasna KK, Remya Krishna JS, Athira P. A Review on Iris Feature Extraction Methods. Int J Eng Res Gen Sci 2016; 4(2): 663–667.
9. Jameel NG. SMS SPAM Detection Using Association Rule. J Theor Appl Inf Technol 2018; 96(12):3962–3972.
10. Kaur R, Rajput R. Face recognition and its various techniques: A review. Int J Sci Eng Technol Res 2013; 2(3):670–675.
11. Kaya OF, Ertugrul Y. A novel Feature Extraction Approach in SMS Spam Filtering for Mobile Communication: One-Dimensional Ternary Patterns. Secure Commun Networks 2016; 9:4680–4690.
12. Kumar V, Minz S. Feature Selection: A Literature Review. Smart Comput Rev 2014; 4(3):211-229.
13. 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.
14. Osho O, Ogunleke OY, Falaye AA. Frameworks for mitigating identity theft and spamming through bulk messaging, IEEE. Int Conf Adapt Sci Technol 2015.

15. Rodan A, Faris H, Alqatawna J. Optimizing Feedforward Neural Networks Using Biogeography Based Optimization for E-Mail Spam Identification. Int J Commun Netw Syst Sci 2016; 09(01):19–28.
16. Shah N, Farik M. Ransomware - Threats Vulnerabilities and Recommendations. Int J Sci Technol Res 2017; 6(6):307–309.
17. Shuaib M, Abdulhamid SM, Adebayo OS, Osho O, Idris I, Alhassan JK, Rana N. Whale optimization algorithm-based email spam feature selection method using rotation forest algorithm for classification. SN Appl Sci 2019; 1(5):1–17.
18. Telgaonkar S, Deshmukh AH. Dimensionality Reduction and Classification through PCA and LDA. Int J Comput Appl 2015; 122(17):4–8.
19. 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.
20. Vikas A, Kaur. Face Recognition using Local Ternary Pattern. Int J Sci Res 2016; 04(12):2115–2120.
21. Xia Z, Deng J. Application and Research of Spam Classification Based on Cluster Intelligence Algorithm to Optimize SVM. J Phys Conf Ser 2020; 1617(1):1–9.