ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.8, 5713–5730
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.8.40

APPLICATION OF AN EFFECTIVE WRAPPER FEATURE SELECTION TECHNIQUE TO CLASSIFY SOCIAL SPAMMERS

R. KRITHIGA[1] AND E. ILAVARASAN

ABSTRACT. Spamming has become pervasive. With the advent of several online social networks, the population of spammers to disturb and disrupt the network is increasing. Hence, there is a crucial need to devise methods to effectively detect spammers in these platforms. As spammers spread malicious activities, the detection process is to be quick and robust to prevent the system at an early stage. In this paper, we apply the Whale Optimization Algorithm (WOA), a population-based heuristic technique, to classify spammers. Further, IP-address based features are proposed apart from utilizing user, content-related features. To accomplish this, a Twitter data was constructed with 9688 instances, balancing the classes equally. To evaluate the performance of WOA, several baseline classifiers were compared based on the metrics Accuracy, Precision, Recall, and F-Measure. The research outcomes suggest that the WOA + Decision Tree approach yields an accuracy of 95.34% and is effective in selecting an optimal subset of features.

1. INTRODUCTION

Spamming has become pervasive. With the advent of online internet communication, businesses have started adopting various online platforms as a tool for branding, promotions, and sales. Heterogeneous fields such as movies, hotels, televisions, photography, arts, and job portals make use of these online media

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 91D30.

Key words and phrases. WOA, Spam Profile Detection, Classification of spammers, Twitter Data, Online Social Networks, IP-address based features.

to satisfy its needs to showcase products or services. Spamming is widespread in the form of opinion spam, product review spam, movie review spam, hotel review spam, web spam, and social media spam, etc., [20]. In this work, we address the social media spamming and attempt to identify the hidden spammers based on several characteristics.

Most of the Online Social Networks (OSN) suffer from spammers who execute spamming or malicious activities that would disturb the user experience [19].

Several techniques have been proposed in the past to fight against these spammers. However, the spammers smartly find alternative ways to escape from the trap and continue delivering spamming actions [1]. A more generic way that had widely been adopted to address this problem is by employing a classifier which in turn categorizes the profiles as spam or genuine [21]. The machine learning algorithms are utilized as classifiers in the process. The classification process involves the collection of relevant attributes that would contribute to the process of categorization. However, practically not all the attributes would be essential for category prediction. In this phase, the attribute selection process plays a vital role to reduce the number of attributes input to the machine learning algorithms thereby reducing the prediction time or speeding up the labeling process without affecting the prediction accuracy. And, in this work, we apply one of the efficient population-based algorithms, the Whale Optimization Algorithm (WOA), a swarm intelligence technique to effectively classify the spammers among a pool of online social networkers.

To tackle the evolving spammers [18], IP-Address based features are also recommended in this study.The remainder of the paper is organized as follows: Section II briefs the literature survey with the state of art techniques that had been applied earlier. The proposed technique of WOA based feature selection process and spam classification is detailed in Section III. The newly designed features to overcome the evading spammers are listed and explained in Section IV along with a brief description of the dataset constructed and compared with that of several base classifiers based on predefined metrics and Section V concludes the work.

2. Literature Survey

Social Media houses wealth of data, which upon mining uncovers valuable information. Several mining approaches have been performed on social networks

as in [2]. In this work, the author gathered Twitter data that are publicly available from five fitness mobile apps. They concluded that a wealth of information source is available from the Twitter data that is shared by the fitness mobile app users. A spam detection framework was proposed in [3] to detect spammers across social networks based on user-profile, message, and web pages. However, the behavior of spammers was not considered in the model.

The author provided a detailed study of the behavior of suspended users in [4]. The study concluded that apart from bots that are noisy to the social networks, the noisy users are also present, who would influence the platform. Spamming is also prevalent in web medium and hence in [5], a study was conducted to classify spam web pages based on the content and link oriented approaches. It further experimented on the WEBSPAM-UK200K dataset that consisted of 11,402 web pages.

As spammers are existent in all forms of social media networks, besides continuing researches in popular Facebook and Twitter medium, a spam detection work was carried out in [6] on Sina Weibo, a popular Chinese social networking platform. The message content and user-related features were extracted from profiles using APIs and fed to the Extreme Machine Learning (ELM), an ML classifier, which inturn labels the profiles as spam and non-spam. The results of ELM were compared to that of SVM, Naïve Bayes, Decision Tree, and Bayes Network. Though ELM and SVM were competitive in results, ELM outperformed in terms of training and testing time. In [7], Twitter spam detection was conducted and yielded an interesting pattern about spammers. The author demonstrated the existence of two different classes of spammers, viz., the one whose account is compromised and the other one, a fraudulent entity.

In [8], the author performed yet another twitter spam detection task using PCA and K-means clustering. Besides retaining the conventional features, a new set of features in the tweet based category was proposed. MLP, SVM, and Random Forest were used to test the effectiveness of the proposed features. Random Forest achieved a True Positive Rate of 96.20% with reduced error rates. The twitter data extracted consisted of 15,000 non-spam & 10,280 spam accounts. The algorithms were implemented using Weka. In contrast to all the earlier works, spam detection in mobile social networks was performed in [9]. By utilizing fog computing, a methodology called COLOR+ was proposed that considers only the interaction between the account and its neighbors. The method

reached an accuracy of 85.95% with an effective detecting time of 0.01 seconds. Not only the individual spam accounts initiate malicious activities, but they also formulate a spamming community and use the medium for spamming purposes. In [10], SpamCom, an unsupervised approach to detect spam communities was proposed by utilizing URL-based, community-related, and graph-based features of individual accounts.

Social graphing and accounting features are computationally expensive methods. Hence, employing only user and tweet based features and Random Forest as an ML algorithm, a spam labeling was done in [11] and resulted in an accuracy of 90%. The tweet based features included emoji, words, and numbers present in the tweet content.

The social network comprises a huge set of attributes and not all of them significantly aid in the process of spam categorization. Hence, reducing the feature set size before initiating the classification process would increase the prediction time. This time reduction is very crucial as the spammers are to be spotted before they could harm the network. The author in [12] proposed a rough set theory-based approach to select the features and obtained promising performance with these minimal set of features.

3. Whale optimization Algorithm for Spam Detection

The Whale optimization algorithm (WOA) was primarily developed based on the hunting behaviour of humpback whales [13]. The humpback whales display a movement called "Bubble net feeding" to gulp the prey by establishing a structure with a circle of bubbles. The algorithm consists of two phases. (a) Exploration (randomly searching for the prey), and (b) Exploitation (encircling prey and spiral bubble net attacking method). The encircling pattern is mathematically demonstrated using the equation (3.2) to update the position of the whales:

$$\vec{E} = \vec{C_2}.\vec{X^*}(t) - \vec{X}(t), \tag{3.1}$$

$$\vec{X}(t+1) = \vec{X^*}(t) - \vec{C_1}.\vec{E}, \tag{3.2}$$

where 't' denotes the present iteration, X^* represents the best solution obtained till present iteration, X is the current solution, C1 & C2 are co-efficient vectors

and are calculated using the equations (3.3) and (3.4),

$$\vec{C_1} = 2\vec{s}.\vec{r} - \vec{s}, \tag{3.3}$$

$$\vec{C_2} = 2.\vec{r}, \tag{3.4}$$

$$s = 2 - t\frac{2}{t_{Max}}, \tag{3.5}$$

where 's' decreases from 2 to 0 as in Eq. (3.5) and r is a random vector in the range [0,1], t_{Max} is the maximum iteration defined in the algorithm. As can be seen in the process of encircling prey, the positions are updated based on the best solution. The humpback whales traverse towards the prey in a shrinking encircling pattern as well as a spiral-shaped path. The movement of a spiral-shaped path is formulated as follows,

$$\vec{X}(t+1) = \vec{D'}.e^{vu}.cos(2\pi u) + \vec{X^*}(t), \tag{3.6}$$

$$\vec{D'} = |\vec{X^*}(t) - \vec{X}(t)|, \tag{3.7}$$

where $\vec{D'}$ is the distance from the i^{th} solution to the best source, v is a constant that defines the shape of the spiral & u is a random number in the range [-1, 1]. The humpback whales move around the target as well as wander along a spiral path simultaneously. This synchronized behavior is simulated as in Eq. (3.8) by invoking a likelihood that assumes 50% to select between the encircling mechanism and a spiral path updating procedure to transform the locations,

$$\vec{X}(t+1) = \begin{cases} \vec{X^*}(t).\vec{C_1}.\vec{E} & p < 0.5 \\ \vec{D'}.e^{vu}.cos(2\pi u) + \vec{X^*}(t) & p \geq 0.5 \end{cases}, \tag{3.8}$$

where p is a random number in [0, 1].

Besides displaying the aforementioned mechanisms for updating the locations, the whales also execute a random search to discover the target that constitutes the exploration phase or global search of this algorithm.

A whale is randomly chosen and the positions of the rest of the whales are accordingly updated. The condition $|\vec{C_1}| > 1$ greatly facilitates the global search process and is executed using the equation (3.10),

$$\vec{E} = |\vec{C_2}.\vec{X_{rand}} - \vec{X}| \tag{3.9}$$

$$\vec{X}(t+1) = \vec{X_{rand}} - \vec{C_1}.\vec{E}, \tag{3.10}$$

where $X_r\vec{a}nd$ is a whale randomly chosen from the population. WOA is a global optimizer that facilitates both diversification and intensification.

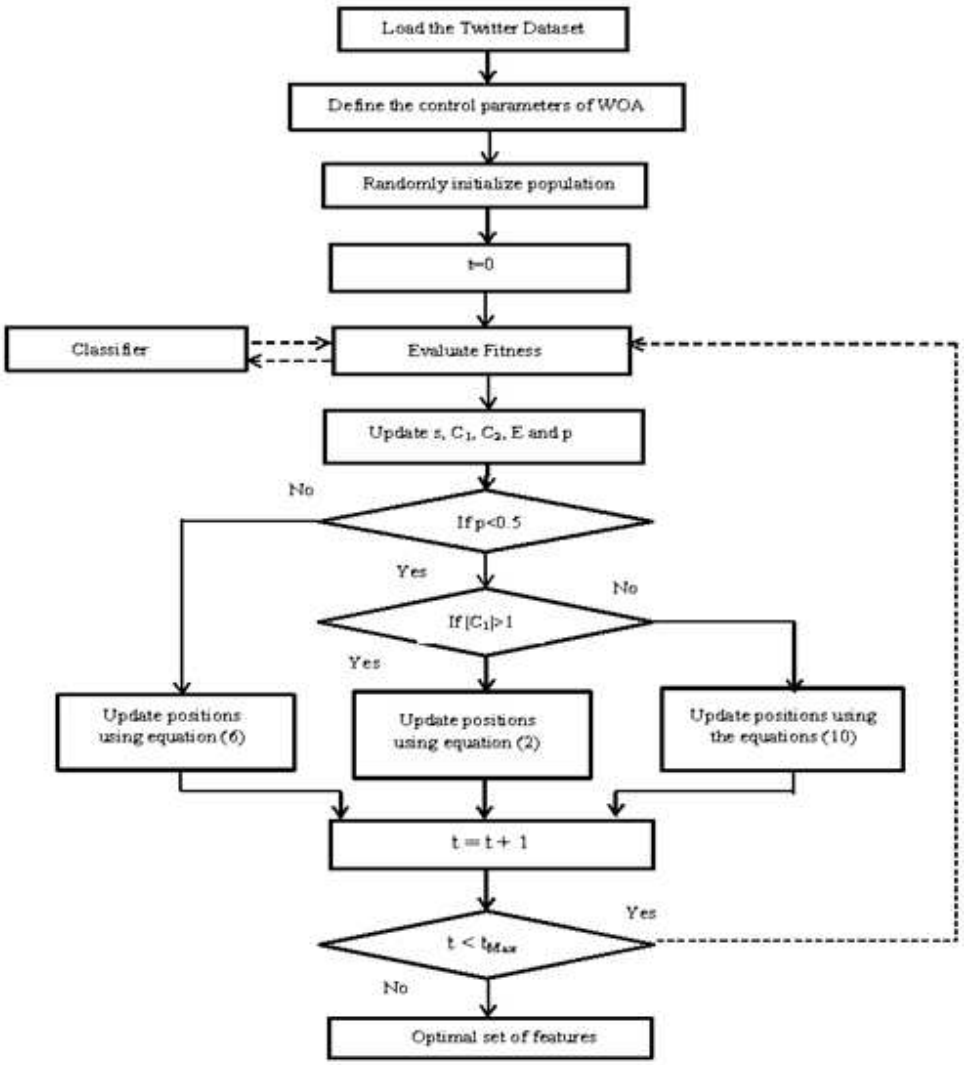

Fig. 1 WOA for Spam Detection

The solution is represented in a binary encoding format, where each dimension of a solution vector holds a value of '1' or '0'. The presence of a 1 indicates that the feature is included in the solution and a 0 indicates the exclusion of feature from the solution vector. The accuracy of the classifier serves as the fitness value for evaluation. All the feature dimensions, for which a '1' has been marked, are extracted from the original dataset. Only those attributes are served

to the classifier for training and testing purposes. Thus, for all the combinations of binary vector displayed by the initial population, fitness scores are calculated and the algorithm enters the phases of WOA for further refinement of feature subset selection.

$$Accuracy = \frac{A}{B}, \tag{3.11}$$

where, A = TP + TN and B = TP + TN + FP + FN.

The values to calculate accuracy are derived from the metrics defined in Table 1. Apart from accuracy, the other measured adopted for the study is described in section IV and these are also constructed based on Table 1.

TABLE I. METRICS FOR CLASSIFICATION OF TWITTER PROFILES

Metric	Description
True Positive (*TP*)	The ratio of Twitter profiles that have correctly been classified as spam
False Positive (*FP*)	The ratio of Twitter profiles that have incorrectly been classified as spam
True Negative (*TN*)	The ratio of Twitter profiles that have correctly been classified as non-spam
False Negative (*FN*)	The ratio of Twitter profiles that have incorrectly been classified as non-spam

4. EXPERIMENT AND RESULT ANALYSIS

The feature subset selection using WOA is then followed by subset evaluation. Each subset is evaluated using a classifier. In this work, machine learning algorithms such as Naïve Bayes classifier, Support Vector Machines, K-Nearest Neighbours, Random Forest, and Decision Trees are used for evaluation. These ML Algorithms have widely been used for the spam identification problem [14,15].

A. Dataset preparation

To perform the spam profile classification problem, a twitter dataset was manually constructed, and using the oversampling techniques, a balanced dataset

was created with 9,688 instances. The details of the dataset are provided in Table II.

TABLE II. TWITTER DATA SET DESCRIPTION

Dataset Description	
No. of Instances	9688
No. of Attributes	26
No. of Classes	2

B. Feature framework

Attributes related to user, profile, activity, and account are employed for the classification procedure. Furthermore, we propose a novel set of features to enhance spam detection. A method devised during a particular period may not be effective during another course of time as the spammers keep evolving and altering the strategies to evade the network of trust. Hence, there is a pressing need to have detector systems that would be robust with time and locates the spammers in the heavily populated social network. The IP addresses are numerical labels that are assigned to devices connected to the network. The values of IP addresses cannot be modified, manipulated, or camouflaged unlike features such as no. of followers, tweets, URLs, etc., Thus, analyzing the IP address based activities would simplify the task of uncovering the adversaries hidden in the network. The spammers exhibit a unique pattern that could visibly be traced using the IP address based features. Table IV shows the proposed feature set $F_{22}, F_{23}, F_{24}, F_{25}$ and F_{26}. Based on an extensive study and analysis from the literature, a complete feature set considered for the problem is listed in Table III [16] & [17].

C. Evaluation Metrics

The Precision, Recall, and F-Measure are used as evaluation metrics and is calculated as:

$$Precision = \frac{TP}{TP + FP)}, \tag{4.1}$$

$$Recall = \frac{TP}{TP + FN}, \tag{4.2}$$

$$F - Measure = \frac{2 \times Precision \times Recall}{Precision + Recall}. \tag{4.3}$$

D. Experimental Setting

The algorithms devised and used in this work are all manually coded in Python language using Spyder, a free integrated development environment included with Anaconda. The Scikit package was imported to evaluate the subset using ML algorithms. The experiments were performed on a Windows 10 machine with Intel Core i7-3630, 2.40 GHz processor and 8 GB RAM.

The default setting of the Scikit package was used for all the classifiers. The training and test data were split based on 70% and 30% ratio respectively. In the first phase of the experiment, all the features are considered for classification. This phase did not involve any feature selection algorithm. The results are presented in Table IV.

As can be seen in Table IV, the best accuracy was obtained by the Decision tree with an accuracy of 94.94%. The subsequent best values have been obtained by Random Forest, K-NN, Naïve Bayes, and SVM with accuracy measures 88.06%, 74.2%, 58.64%, and 49.94% respectively. The decision tree output a fair value for all metrics. However, Naïve Bayes outperformed the other classifiers for Recall with a measure of 99.67% and SVM with 98.41%. The Random Forest yielded an outstanding Precision measure of 97.67%.

The WOA was then applied for feature selection and the performance was evaluated using the baseline classifiers. The initial population was set to 7 with the boundary vector [0, 1]. The values are averaged over 5 runs. The values for various metrics for WOA with 10 iterations are provided in Table V. WOA + Decision Tree achieves an accuracy of 95.34% which is higher than the classification result performed without feature selection. The Random Forest yields the second-best accuracy with 88.15%. It is to be noted that all the classifiers produced a similar or better output concerning the entire metrics when classification is performed comprising the feature selection process. The WOA, when employed along with Decision Tree, gives better values in terms of Accuracy, Precision, Recall, and F-Measure. For Random Forest, the performance is maintained in union with WOA.

TABLE III. LIST OF FEATURES USED

List of Features	
F_1	Twitter Account No.
F_2	Account age
F_3	No. of followers
F_4	No. of followings
F_5	No. of user favorites
F_6	No. of lists
F_7	No. of tweets
F_8	No. of re-tweets
F_9	No. of hashtags
F_{10}	No of user mentions
F_{11}	No of URLs
F_{12}	Repeated Words
F_{13}	Words in capital
F_{14}	The frequency of function words
F_{15}	Special character
F_{16}	Emoticons
F_{17}	Digits
F_{18}	Minimum time between Tweet postings
F_{19}	Maximum time between Tweet postings
F_{20}	Tweets Posted Per Day
F_{21}	Tweets Posted Per Week
F_{22}	IP address changed last 1 week
F_{23}	IP address changed 24 hours
F_{24}	No. of IP address for posts
F_{25}	No. of IP address for comments
F_{26}	No of Tweets deleted

TABLE IV. PERFORMANCE OF CLASSIFICATION ON BASELINE CLASSIFIERS

	Accuracy	*Precision*	*Recall*	*F-Measure*
Naïve Bayes	0.5864	0.5468	**0.9967**	0.7062
KNN	0.7420	0.7321	0.7623	0.7469
SVM	0.4994	0.4982	0.9841	0.6615
Decision Tree	**0.9494**	0.9393	0.9607	**0.9499**
Random Forest	0.8806	**0.9767**	0.7761	0.8649

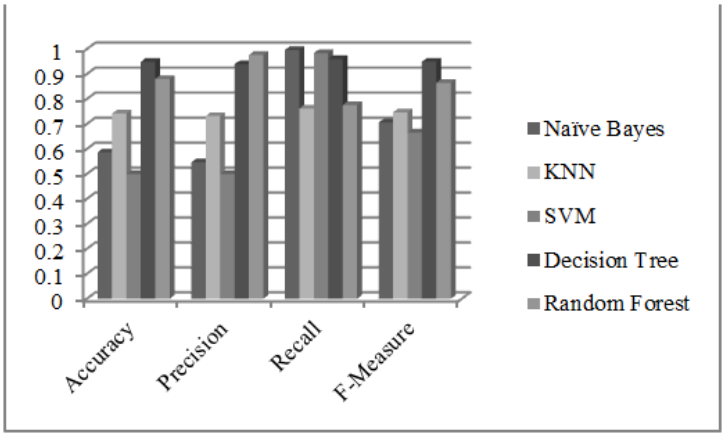

TABLE V. PERFORMANCE OF CLASSIFICATION ON BASELINE CLASSIFIERS WITH WOA FOR ITERATION = 10

	Accuracy	*Precision*	*Recall*	*F-Measure*
WOA+Naïve Bayes	0.6955	0.6556	0.8223	0.7295
WOA+KNN	0.7358	0.7394	0.7272	0.7332
WOA+SVM	0.4946	0.4946	**0.9988**	0.6616
WOA+Decision Tree	0.9534	0.9451	0.9624	0.9537
WOA+Random Forest	0.8815	0.9773	0.7774	0.8660

The algorithm was analyzed for results when iteration was increased to 15 and is displayed in Table VI. With an increase in iteration, the Recall measure of Naïve Bayes was increased to 98.55% from 82.23%. However, Accuracy and Precision were degraded. Except for a slight increase in Recall measure for K-NN, the other values obtained were more similar to that of for 10 iterations. The SVM displayed a degraded performance for Recall and F-Measure while maintaining the performance of Accuracy and Precision. The Decision Tree retains similar results except for a slight decrease for Recall with 95.59%. As in the other cases, Random Forest also didn't showcase an enhanced performance with an increase in iterations.

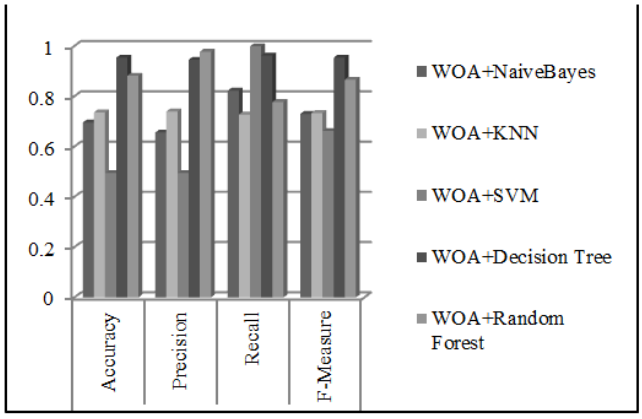

TABLE VI. PERFORMANCE OF CLASSIFICATION ON BASELINE CLASSIFIERS WITH WOA FOR ITERATION = 15

	Accuracy	*Precision*	*Recall*	*F-Measure*
WOA+Naïve Bayes	0.6191	0.5685	**0.9855**	0.7211
WOA+KNN	0.7316	0.7267	0.7417	0.7341
WOA+SVM	0.4941	0.4957	0.9696	0.6560
WOA+Decision Tree	0.9525	0.9480	0.9559	0.9519
WOA+Random Forest	0.8815	0.9557	0.7963	0.8687

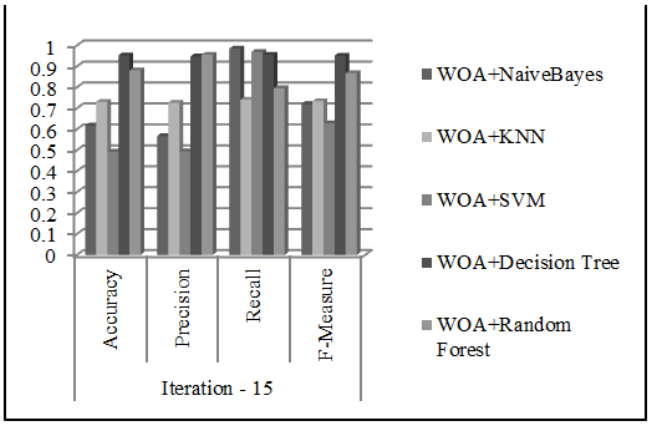

TABLE VII. PERFORMANCE OF CLASSIFICATION ON BASELINE CLASSIFIERS WITH WOA FOR ITERATION = 20

	Accuracy	*Precision*	*Recall*	*F-Measure*
WOA+Naïve Bayes	0.6728	0.6229	0.8739	0.7274
WOA+KNN	0.7533	0.7351	0.7913	0.7621
WOA+SVM	0.4876	0.4812	**0.9832**	0.6123
WOA+Decision Tree	0.9531	0.9514	0.9534	0.9524
WOA+Random Forest	0.8837	0.9479	0.8084	0.8726

The iteration count was further increased to 20 to investigate the effects on the results produced by WOA and presented in Table VII. The WOA + Naïve Bayes showed improved performance on increasing the iteration count to 20. However, the results produced for 10 iterations stand best. The KNN showed considerably improved performance when iteration is set to 20. Similarly, though SVM showed improved results, the better values were obtained for 10 iterations. As in for other iteration counts, the WOA + Decision Tree and WOA + Random Forest preserved the quality of all the metrics. Hence, it is concluded that WOA + Decision Tree yields the best accuracy of 95.34% for the Twitter spam detection problem. An increase in iteration does not result in improved performance.

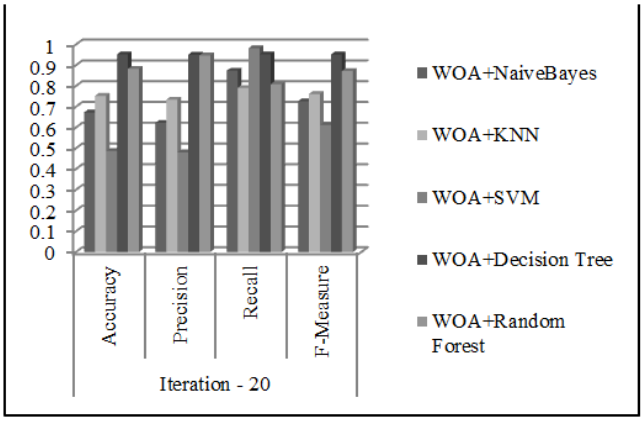

Fig. 5 Performance Comparison of Baseline classifiers + WOA for Iterations = 15

TABLE VIII. FEATURES SELECTED OVER ITERATIONS 10, 15, AND 20

	I=10	I=15	I=20
WOA+Decision Tree	19	19	19
WOA+Random Forest	22	22	24

To further evaluate the number of features selected, the two best performing classifier combinations WOA + Decision Tree and WOA + Random Forest are presented in Table VIII.

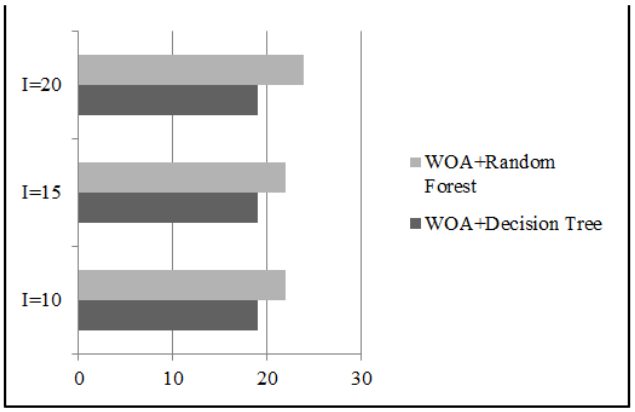

Fig. 6 Comparison of Features selected over iterations 10, 15 and 20

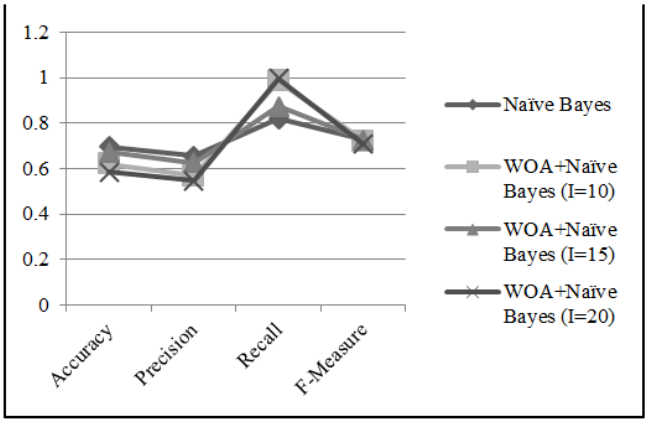

Fig. 7 Comparison of Metrics obtained by Naïve Bayes and in combination with WOA

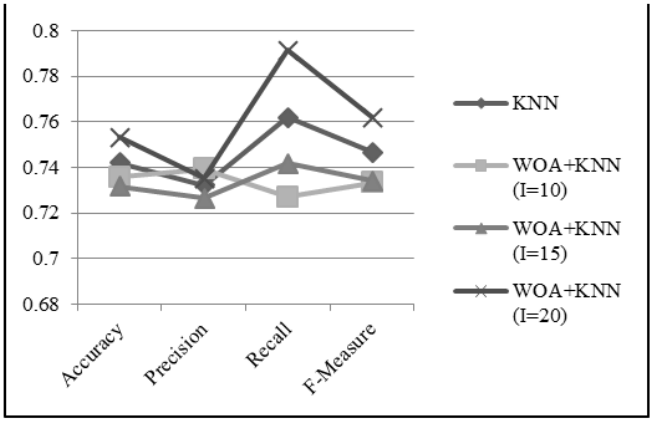

Fig. 8 Comparison of Metrics obtained by KNN and in combination with WOA

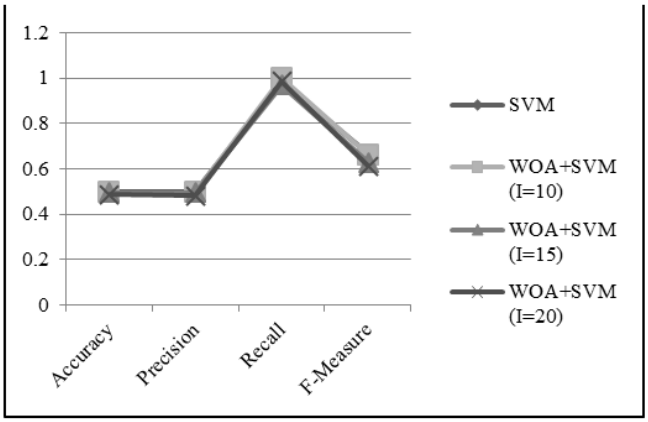

Fig. 9 Comparison of Metrics obtained by SVM and in combination with WOA

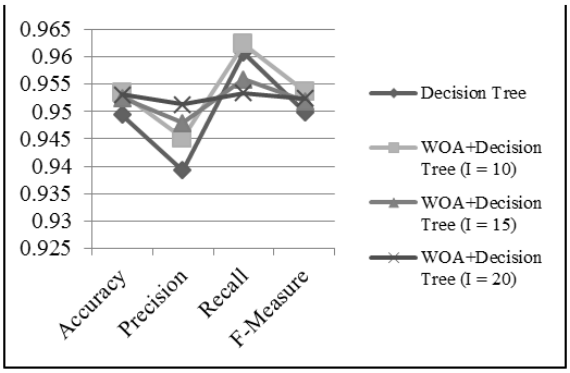

Fig. 10 Comparison of Metrics obtained by Decision Tree and in combination with WOA

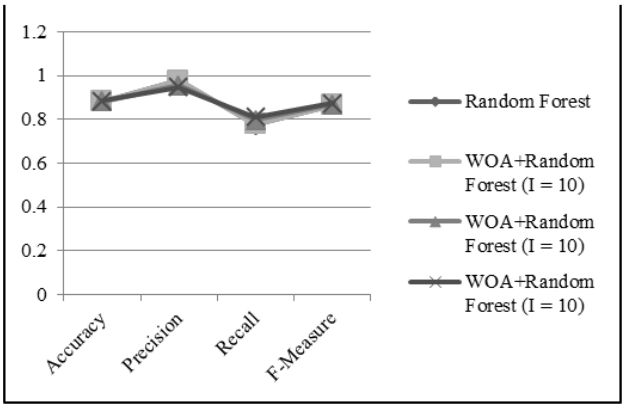

Fig. 11 Comparison of Metrics obtained by Random Forest and in combination with WOA

5. CONCLUSION

This paper addressed the spam detection problem in online social networks. To accomplish this, a twitter dataset was manually constructed. Feature categories such as user, content-related attributes were used. Additionally, to cope up with the evading spammers, a new set of IP-address based features were proposed. These features are strong, powerful, and difficult to manipulate by spammers. To reduce the feature set size and select only the most contributing subset, Whale Optimization Algorithm, a population-based heuristic technique was applied to effectively choose the feature subsets. The performance was evaluated on several baseline classifiers. The overall performance suggests that the

performance of the classification was either improved or retained on the account of employing WOA for pre-processing. And, the best accuracy was obtained by WOA + Decision Tree.

REFERENCES

[1] G. MUHAMMAD AJMAL AZAD, R. MORLA: *Early Identification of Spammers Through Identity Linking, Social Network and Call Features*, Journal of Computational Science, **23** (2017), 157-172. http://dx.doi.org/10.1016/j.jocs.2016.10.019

[2] T. A. VICKEY, K.M. GINIS, M. DABROWSKI: *Twitter classification model: the ABC of two million fitness tweets*, Translational Behavioral Medicine, **3** (2013), 304–311. doi: 10.1007/s13142-013-0209-0

[3] D. WANG, D. IRANI, C. PU: *SPADE: a social-spam analytics and detection framework*, Social Network Analysis and Mining, **4**, Article number: 189, (2014). doi: 10.1007/s13278-014-0189-1

[4] W. WEI, K. JOSEPH, H. LIU, K. M. CARLEY: *Exploring characteristics of suspended users and network stability on Twitter*, Social Network Analysis and Mining, **6**, Article number: 51, (2016). doi 10.1007/s13278-016-0358-5

[5] R. KUMAR ROUL, S. ROHAN ASTHANA, M. SHAH, D. PARIKH: *Detection of spam web page using content and link-based techniques: A combined approach*, Sadhana, **41**(2) (2016), 193-202.

[6] X. ZHENG, X. ZHANG, Y. YU, T. KECHADI, C. RONG: *ELM-based spammer detection in social networks*, The Journal of Supercomputing, **72** (2016), 2991–3005. doi 10.1007/s11227-015-1437-5

[7] A. ALMAATOUQ ET AL: *If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts*, International Journal of Information Security, **15** (2016), 475–491. doi 10.1007/s10207-016-0321-5

[8] K. SAKARIYAH ADEWOLE, T. HAN, W. WU, H. SONG, A. KUMAR SANGAIAH: *Twitter spam account detection based on clustering and classificationmethods*, The Journal of Supercomputing, **76** (2018), 4802–4837. https://doi.org/10.1007/s11227-018-2641-x

[9] J. ZHANG, Q. LI, X. WANG, B. FENG, D. GUO: *Towards fast and lightweight spam account detection in mobile social networks through fog computing*, Peer-to-peer Networking and Applications, **11** (2017), 778–792. doi 10.1007/s12083-017-0559-3

[10] P.V. BINDU, RAHUL MISHRA, P. SANTHI THILAGAM: *Discovering spammer communities in twitter*, Journal of Intelligent Information System, **51** (2018), 503–527. https://doi.org/10.1007/s10844-017-0494-z

[11] K. ROBINSON, V. MAGO: *Birds of prey: identifying lexical irregularities in spam on Twitter*, Wireless Networks, 2018. https://doi.org/10.1007/s11276-018-01900-9

[12] S. DUTTA, S. GHATAK, R. DEY, A. KUMAR DAS, S. GHOSH: *Attribute selection for improving spam classification in online social networks: a rough set theory-based approach*, Social Networking and Mining, **8**, Article number: 7 (2018), https://doi.org/10.1007/s13278-017-0484-8

[13] S. MIRJALILI, A. LEWIS: *The Whale Optimization Algorithm*, Advances in Engineering Software, 2016, 51-67.

[14] M. KARIM SOHRABI, F. KARIMI: *A Feature Selection Approach to Detect Spam in the Facebook Social Network*, Arabian Journal for Science and Engineering, **43** (2017), 949–958. doi 10.1007/s13369-017-2855-x

[15] A. BARUSHKA, P. HAJEK: *Spam detection on social networks using cost-sensitive feature selection and ensemble-based regularized deep neural networks*, Neural Computing and Applications, **32** (2019), 32, 4239–4257. https://doi.org/10.1007/s00521-019-04331-5

[16] I. INUWA-DUTSE, M. LIPTROTT, IOANNIS KORKONTZELOS: *Detection of spam-posting accounts on Twitter*, Neurocomputing, (2018), 496-511.

[17] A. M. AL-ZOUBI ET AL: *Spam Profile Detection in Social Networks Based on Public Features*, 8th International Conference on Information and Communication Systems (ICICS), (2017), 130-135.

[18] C. YANG, R. HARKREADER, G. GU: *Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers*, IEEE Transactions On Information Forensics And Security, **8**(8) (2013), 1280-1293.

[19] W. ZHANG H.-M. SUN: *Instagram Spam Detection*, IEEE 22nd Pacific Rim International Symposium on Dependable Computing, 2017, 227-228, doi 10.1109/PRDC.2017.43

[20] C. VISANI ET AL: *A Study on Different Machine Learning Techniques for Spam Review Detection*, International Conference on Energy, Communication, Data Analytics and Soft Computing, (ICECDS), Chennai, 2017, 676-679.

[21] S. GHEEWALA, R. PATEL: *Machine Learning Based Twitter Spamaccount Detection: A Review*, Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC), 2018, 79-84.

PUDUCHERRY, INDIA
Email address: kriithiga@gmail.com

PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE& ENGG., PONDICHERRY ENGINEERING COLLEGE, PUDUCHERRY, INDIA.
Email address: eilavarasan@pec.edu