IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 34, No. 4, August, 2020, pp. 429-436
Journal homepage: http://iieta.org/journals/ria

An Efficient Method for Detection of Fake Accounts on the Instagram Platform

Saeid Sheikhi

Department of Computer, Gorgan Branch, Islamic Azad University, Gorgan 39975, Iran

Corresponding Author Email: S.Sheikhi@outlook.com

https://doi.org/10.18280/ria.340407

Received: 8 June 2020
Accepted: 6 August 2020

Keywords:
Instagram, fake account detection, social media, fake followers, machine learning

ABSTRACT

In recent years, social media platforms such as Instagram, Twitter, and Facebook have gradually become important ways to disseminate information. One of these social platforms that have attracted more attention in past years is Instagram. Instagram has widely used for sharing photos and videos and is profitable for celebrities, businesses, and people with a considerable number of followers. In the meantime, this high profit made this platform prone to be the potential place to be used for malicious activities. One of the essential malicious activities in the Instagram platform is fake accounts. However, in this paper, an efficient method for identifying Instagram fake accounts is proposed. In the presented model. First, a dataset of legitimate and fake accounts is created. Then, the collected dataset has been used as input of the bagging classifier to classify fake users on the dataset. Furthermore, the proposed method compared to the five well-known machine-learning classifiers in terms of classification accuracy to better evaluate effectiveness of the method. The experimental results show that the proposed method performs better than other considered algorithms and correctly classified over 98% of the accounts with a low error rate.

1. INTRODUCTION

In recent years, online social networks (OSNs), such as Instagram, Twitter, and Facebook, have become popular platforms to disseminate and share information [1]. These services provide fast and suitable communication and other types of tools that make their users be able to directly share and publish their multimedia contents such as pictures, videos, and audios over the internet [2]. Hence, besides the significant number of users on social platforms, these features and tools have interested many cyber criminals in using them to perform their malicious activities on social media platforms effectively. Unlike in the past, many attacks with a limited or small effect can now have a considerable impact by using online social platforms [3].

However, social media's effect is significant in people's lives, and many people use them to build more extensive connections [4]. One of the most popular social media is Instagram [5]. Instagram is a free social networking app built for sharing photos and videos over the internet. It is similar to most other social media, where those who create an account have a profile and news feed and can share photos and videos through that.

In recent years, many celebrities and businesses have created their accounts on Instagram; they use Instagram to grow their business and fans [6]. Furthermore, many of them and other famous users use it as a platform for advertising. When someone is boosting the number of followers over a hundred thousand or millions, it is no surprise to use that person's account as a lucrative earner. In the last years, many celebrities and ordinary people who reached a considerable number of followers on Instagram have used their accounts as a place for advertising. People also try to increase the number of their followers for other reasons, such as achieving more fame, being trustworthy, and being influential.

Such versatility and spread of use have made Instagram the perfect platform for the proliferation of abnormal accounts, which behave in unusual ways. Most academic researchers have mostly focused on spammers and accounts, which put their efforts into spreading advertising, spam, malware, and other suspicious activities [7]. These malicious accounts are usually using automatic programs to improve their performance, hide their real identity, and look like real users. In past years, media have reported that account of celebrities, politicians, and some popular business has indicated suspicious inflation of followers. Fake Instagram accounts specifically used to increase the number of followers of a target account.

Therefore, artificially inflating the number of followers can also be concluded to obtain an account more influential and trustworthy in order to stand from the crowd to attain and attract more legitimate followers to their account [8]. In past years, some of the banks and financial institutions in the U.S. decided to analyze social media accounts of the loan applicants, before genuinely giving the loan. Hence, having a popular account can help effectively to increase the creditworthiness and reliability of the applicant. Furthermore, if a spammer adopted fake followers, it can effectively act as a legitimate user and post more authoritative messages and launch various efficient advertising campaigns [9].

Some professional users think fake account detection is an easy task with their rules based on anomaly account behavior. Though, such rules are usually matched neither with analytic algorithms to aggregate them nor with validation mechanisms. Most academic researchers have focused mainly on spam and bot detection in various social media like Facebook and

Twitter, with brilliant results in classifying fake accounts based on their legitimate and fraudulent features, mainly utilizing machine-learning methods. However, the paper's remaining part proceeds as follows: the second section will give a brief overview of the previous research in fake and spam accounts detection in different environments and highlights their shortcomings and achievements. The third section describes the methodology used for this study, including the feature extraction, and dataset. The fourth section presents information about the proposed detection model, such as the used methods and detection process. The fifth section presents experiments such as a description of the experiment setup, conditions, and evaluation metrics used in the experiment. It also discusses the results and the research findings, besides comparing the results with other techniques. Finally, the sixth section sums up the paper with concluding remarks.

2. RELATED WORKS

Today, social media is developing amazingly fast; these services are critical for many people in society, especially for marketing campaigns and celebrities and politicians who attempt to promote themselves using followers and fans on social media [10]. Hence, fake accounts created on behalf of people and organizations can be harmful and damage to these people and businesses' reputations and finally led to the decreasing number of their real likes and followers. Moreover, all types of fake profiles have an adverse effect on the advantages of social media for marketing and businesses in advertising [11]. These fake profiles can be a way for the cyberbullying; real users also have different anxieties about their privacy in the online environment with these fake profiles [12].

Therefore, over the past years, many researchers have investigated the problem of detecting malicious activities and spammers in social media using machine learning techniques. However, there are a limited number of research articles relating to detecting fake accounts or fake followers. In this section, we shed light on both spammers and fake accounts solutions that recently were introduced.

Ferrara et al. [13] introduced a method to detect bot users on Twitter based on the highly shared features that distinguish them from legitimate users. In their proposed method, they have used a machine learning technique and behavioral patterns between legitimate and bot accounts in order to classify accounts into the bot or legitimate class. Cresci et al. [14] have created and used a baseline dataset of verified human and fake followers on Twitter. In their work, they exploited the baseline dataset to train a set of machine learning classifiers built based on reviewed rules and features set using the media. Their proposed method is efficient in detecting fake accounts; the results achieved by their method show it can classify more than 95% of the accounts correctly from the original training set.

In a slightly different method, Zhang and Lu. [15] Introduced a novel method for the detection of fake accounts in Weibo. Their proposed solution has different aspects. At first, they had this premise why such accounts exist in the first place. In the second, they investigated the overlap between followers list of the customers of fake followers, and they found a high overlap between their follower lists. Their investigation found 395 near-duplicates, which led to 11.90 million fake accounts that sent a million links in the network. Thomas et al. [16] made a collection of 1.8 million tweets sent by 32.9 Twitter accounts. In their investigation, they found Twitter suspended about 1.1 million of those accounts. They have selected randomly 100 of those accounts to analyze their tweets and verify they were spamming accounts. They made a further analysis on that 100 selected accounts, and they find 93 of the selected accounts were suspended for posting spam and the unsolicited advertisement of various products. Three other accounts were suspended for retweeting content of different news accounts, and the other 4 remained accounts were suspended for duplicate and aggressive marketing posts.

Gao et al. [17] have used a set of features for efficiently reconstructing spam tweets into campaigns instead of studying them separately. The result shows their proposed solution obtained over 80% detection rate. However, the disadvantage of their method is its low detection accuracy. Benevenuto et al. [18] proposed a solution to detect spammers from non-spammers. In their method, they used an SVM classifier, which is a supervised machine learning algorithm. They have used 23 behavior and 39 content features to distinguish spammers from non-spammers, and they performed experiments by 5-fold cross-validations. The experiments show they were almost successful in identifying spammers from non-spammers. BalaAnand et al. [19] developed a new system to detect fake users on the Twitter platform using a graph-based semi-supervised learning algorithm (EGSLA) and analyze and gathering behavioral and user-generated content (UGC) information. The model first collected users' information, analyzed them to extract useful features, and then performed classification on these features and made decisions. The experimental results show that the EGSLA algorithm achieved high performance and was more beneficial than other algorithms such as decision tree, KNN, SVM, and game theory-based methods in terms of classification accuracy. Sahoo et al. [20] presented a hybrid model to detect malicious profiles on social media focusing on Twitter. The proposed hybrid model includes two modules; first, they analyzed and extracted features using Petri net structure, then they used these features as the classifier's input to classify profiles as malicious and legitimates classes. The experimental outcomes show that the proposed approach successfully distinguished different twitter accounts and obtained a high detection rate in terms of classification accuracy.

Therefore, according to literature, many researchers have been using machine learning techniques to overcome security problems in social networks. Surveyed studies mostly focused on spam detection on microblogging social media. They have investigated many solutions to solve the problem of spam and fake accounts on Twitter and other microblogging social media. However, to date, there is no comprehensive solution to fake accounts on the Instagram platform, which is one of the motivations behind this study. Hence, in this paper, we have proposed an efficient method for detecting fake accounts on the Instagram platform, which can effectively classify different Instagram user accounts.

3. METHODOLOGY

This section presented the collected Instagram accounts dataset, which was used to conduct our experiments in this research. Moreover, we have described how each of them was collected and how these accounts were verified and classified into fake and legitimate classes.

3.1 Data collection

Like most social media platforms, the public Instagram developer API only provides the public information of users. It is not possible to access some users' activities and login information, mostly when a user already has set that account to private mode. This problem is considered as an obstacle to the process of data collection. To solve the issues and crawl users' information, we have developed a specific data crawler and feature collection tool described in the following steps (see Figure 1).

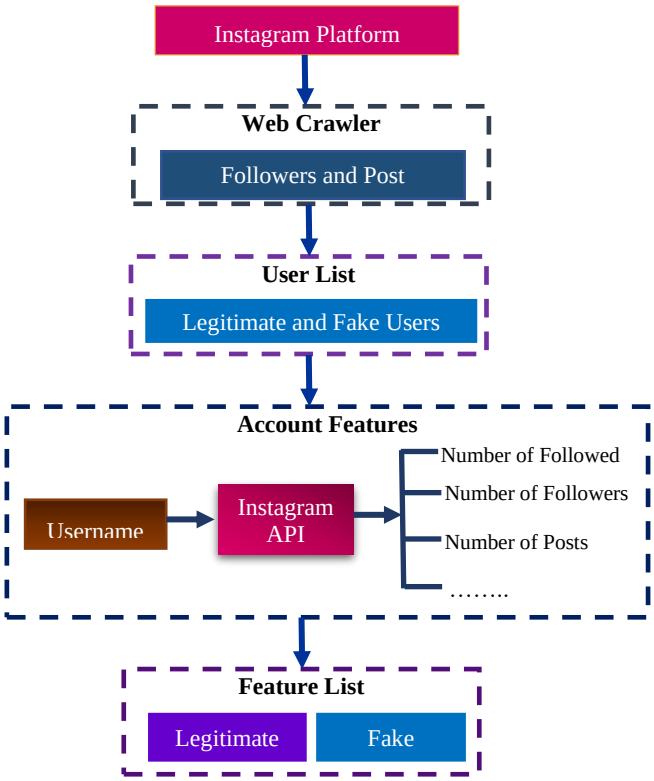

Figure 1. Dataset and feature collection procedure

The 6868 regular users, such as celebrities, companies, and ordinary legitimate users, plus 3132 anomaly users who manually checked and selected, have collected in the dataset. We have developed two types of data crawlers for achieving regular and anomaly users, respectively. The ordinary user crawler has used Instagram's explore feature to identify regular users and add them to the list of ordinary users in the dataset. Instagram's Explore feature displays recent posted pictures and videos that reached other users' attention, which show accounts posted are mostly real and legitimate.

Furthermore, to discover and achieve fake users on Instagram, first, the developed crawler used to obtain fake users ID through the follower list of users who considered a considerable number of fake users in their follower list. In second, we have developed another tool to manually check all of the fake archived users in the dataset, be assured about their identity, and improve the dataset's quality.

Table 1. Description of the dataset

	Legitimate	Fake	Total
Records	6868	3231	10000
Percentage	68.68	32.31	100

For each user, some public information crawled using Instagram API; the description of the dataset and list of the crawled features are listed in Tables 1 and 2, respectively.

The collected features are listed in the following Table 2.

Table 2. The list of collected features

Index	Feature	Description
1	UName	Username Length
2	Uid	Real ID of user on Instagram
3	Fullname	Full name Length
4	has_pic	Does account set a profile picture
5	biography	Biography Length
6	Followedby	The number of users Followed the account
7	Followed	The number of users the account Followed them
8	Is_Followed_More	Is number of Followed are more than Followed by
9	Postcount	The number of shared posts by the account
10	is_business	Is it a business account
11	is_private	Is the user set profile as private
12	is_verified	Is the account verified by Instagram
13	has_channel	Does the account have a channel
14	external_url	Is the account linked to an external URL
15	highlight_reel_count	The number of highlights is pinned to the account
16	connected_fb_page	Is the account linked to a Facebook profile

Figure 2 illustrated four of the essential features in our dataset. Figure 2 (a) shows the distribution of accounts with a profile picture in the dataset, and it indicates most accounts that have not set profile pictures to their accounts belong to the fake category. Similarly, the number of followed by fake accounts are quite large, and most fake accounts followed more people than their followers, as shown in Figure 2 (b) and (c). It may be explained that most fake users created only to increase the number of followers of regular users and that is because many Instagram regular users try to buy fame using increase the number of their accounts followers.

Figure 2 (d) indicates the number of posts in each account. As expected, most fake accounts do not contain many posts or mostly have zero or one post because many of these accounts only aim at following other users or advertising, so their creator consumes a short time on the increasing number of their post or design appearance of them. However, the recent creator of these fake accounts tries to design their appearance and increase the number of their posts, so their accounts look more normal and satisfy their customers.

Furthermore, by this trick, they can sometimes bypass Instagram's limitations. Though, their account still has a small number of followers and a large number of following. Some of these fake account producers tried to decrease these vast differences between the numbers of their accounts followers and followed by using the other fake accounts they own. Accordingly, they make fake activities between their fake accounts and make their fake accounts which are mostly bots following each other to their number of followers look like regular users. Finally, all of their fake accounts will have some followers, and it helps them look more like regular users.

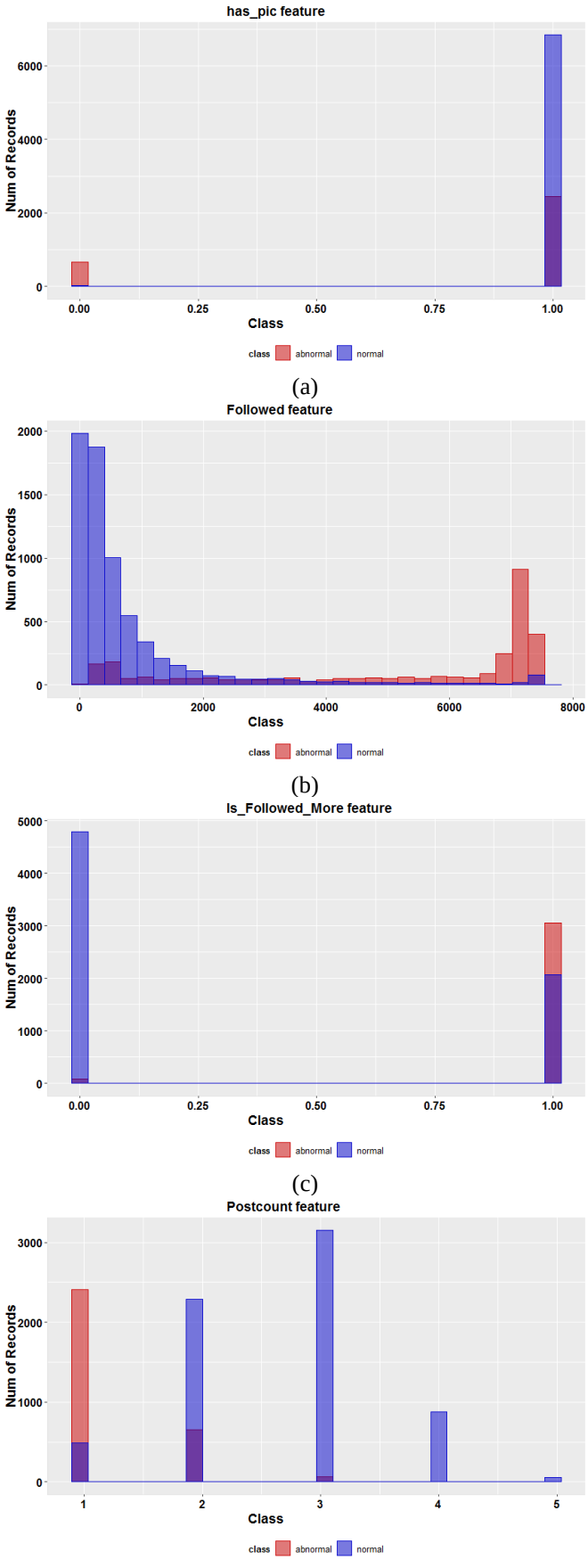

Figure 2. The distribution of four important features on the dataset

Feature analysis

Unlike normal Instagram users, fake users are usually aimed at commercial intent, such as advertisements spreading and following more users. This section randomly selected some of the fake users from the dataset and manually studied them. Therefore, an analysis of the differences between fake and legitimate users from both content and behavior points of view is discussed as follows:

(1): Most fake accounts do not contain a significant number of posts; many of them have zero or only a small number of posted pictures and videos.

(2): Almost all fake users follow a multitude of legitimate users. The main aim of fake accounts is to increase the number of followers of the other authorized users. Thus, most fake accounts followed a considerable amount of people, so they followed more people than they followed by. That makes the fraction of followed per followers huge in comparison with legitimate users.

(3): After analyzing some of the fake accounts, as expected, it indicates the considerable fraction of fake users did not set a picture to their profile, and also their profile does not contain a biography description more than the name they entered in the process of creating the account. The reason behind that is, most of the fake accounts only created for increasing the number of other users' followers, and they use a limited time on the design of the account appearance. Though this is just for a fraction of fake accounts, and many of them seem legitimate users.

4. PROPOSED MODEL

In this section, we introduced a machine learning model based on the features set and dataset presented in the previous section to identify fake accounts.

4.1 Bagging (bootstrap aggregating)

The bagging technique has various applications and can use for both the regression and classification solutions. It improves the prediction process by reducing the variance associated with the prediction. Breiman has introduced this technique in 1996 [21]. The bagging algorithm's purpose is to estimate a list of various classifiers on collected datasets using disturbing the training set with bootstrap resampling, and then it combines these estimated classifies with some aggregation methods.

In general, when individual classifiers are not too correlated to each other, this algorithm improves individual classifiers' efficiency that happens when the classifier is so sensitive to the small perturbations of the training set [22]. The bagging technique has conceptually simple implantation; it can be used in many different settings and works so well in practice [21].

In the original bagging technique, the various trees trained on bootstrap samples are aggregated using class majority voting. i.e., voting of class forecasts for a new observation. Furthermore, according to Breiman [21], it gets the average of the conditional class probability estimators. It selects the class with the highest average conditional class probability, which leads approximately to the same results. Therefore, in this study, to better perform fake users' classification, the bagging algorithm was used as the base of the proposed method, and its parameters tuned using the grid search method.

4.2 Bagging based detection model

Figure 3 represents the structure of our proposed fake accounts detection model. In the method, the crawling tool is used to achieve information about the users and convert this information to a series of features. These collected features were utilized as input for the decision-tree based bagging algorithm. After building the dataset, we implemented a classification model using a bagging algorithm to identify whether the particular user belongs to the legitimate or fake classes. Since fake and regular users have different social behavior, it can distinguish abnormal behavior from legitimate ones by analyzing user behavior and content features.

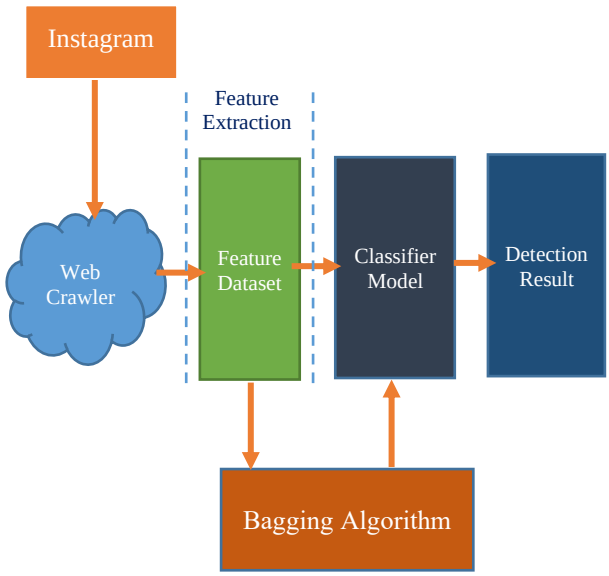

Figure 3. Overview of fake accounts detection model

5. EXPERIMENTS AND RESULT ANALYSIS

This section presents our conducted experiments that illustrate the effectiveness of the proposed solution for detecting fake accounts. In this section, first, we have introduced baselines and the experimental setup. Next, we have described the evaluation metrics used to measure the efficiency of the proposed solution. Finally, we have analyzed the experimental results achieved by the proposed method. These results indicated that the introduced method has an excellent performance in terms of accuracy, and it can effectively recognize fakes accounts.

5.1 Experiment setup

All of our experiments were conducted on a device with 16 GB RAM, and all classification algorithms were implemented using Weka software. Additionally, we have applied the collected dataset, which has information on 10000 Instagram users in all experiments, and these Instagram users samples belong to two main classes of normal and anomaly.

In all the experiments, to reduce overfitting and have a rational evaluation of the models obtained by the algorithms, we have used a well-known 10-fold cross-validation measuring method. Besides, five well-known classification algorithms were evaluated with the proposed model; these algorithms are Random tree, J48, SVM, RBF, MLP, Hoeffding tree, and Naïve Bayes.

The fake account detection method is based on the bagging algorithm used to the bagged decision tree. In general, parameters influence every classifier performance [23]. The Bagging method has two training parameters: BagSizePercent manages the bag size, as a percentage; and NumIterations controls the number of iterations. Hence, we applied a useful tool for parameter selection based on grid search with a 10-fold-cross-validation to automatically find the best parameter values to reach the highest classification accuracy. Finally, most optimal parameters that BagSizePercent and NumIterations equal with 55 and 1500 respectively are produced to train the model to achieved high performance in distinguishing different Instagram accounts.

5.2 Evaluation metrics

We have applied a confusion matrix to calculate evaluation measurements to evaluate the performance of the model; the description of the confusion matrix is illustrated in Table 3.

Table 3. The description confusion matrix

Actual	**Predicted**	
	Fake	Legitimate
Fake	TP	FP
Legitimate	FN	TN

where,

TP: the number of fake accounts correctly classified as fake.

FP: refers to the number of fake accounts incorrectly classified as legitimate.

FN: expresses the number of legitimate accounts incorrectly classified as the fake ones.

TN: represents the number of legitimate accounts that correctly classified.

The accuracy (ACC) = total of records has been classified correctly.

$$ACC = \frac{(TP + TN)}{(TP + FP + TN + FN)} \quad (1)$$

The true-positive rate (TPR): It shows records that have been classified as legitimate correctly.

$$TPR = \frac{TP}{TP + FN} \quad (2)$$

The false-positive rate (FPR): It presents records that have been classified incorrectly as legitimate instead of fake.

$$FPR = \frac{FP}{FP + TN} \quad (3)$$

According to the confusion matrix, some of the metrics are usually evaluated in the machine learning field researches, namely: precision, recall, and F-measure.

Precision (P): represents the ratio of the number of the samples correctly identified to the total number of samples and the value of that measured using the formula expressed in Eq. (4).

$$Precision = \frac{TP}{TP + FP} \quad (4)$$

Recall (R): represents the ratio of the number of the samples which correctly identified to the total number of classified samples. The value of that measured using the formula in Eq. (5).

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

F-measure: have the harmonic mean within recall and precision, it is expressed in Eq. (6).

$$F - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (6)$$

5.3 Result analysis

Tables 4 and 5 show a comparison between the proposed model and five other classifiers. We also compared the results with RBF and MLP algorithms. These algorithms are among suitable methods for solving classification ad regression problems [24]. The results demonstrate that our proposed method is very efficient, with the detection of 98.45% of accounts correctly, and leaving only a low number of fake and legitimate accounts misclassified.

Table 4. Comparison the model and other classifiers

Algorithm	TPR	FPR	Classified	Misclassified
Hoeffding Tree	0.964	0.042	96.38	3.62
Random Tree	0.972	0.036	97.2	2.8
RBF	0.949	0.052	94.92	5.08
MLP	0.979	0.035	97.90	2.10
SVM	0.687	0.687	68.68	31.32
Naïve Bayes	0.946	0.042	94.58	5.42
Bagged Decision Tree	0.985	0.025	98.45	1.55

Table 5. Comparison of evaluation metrics between classifiers

Classifier	Precision		Recall		F-measure	
	Fake	Normal	Fake	Normal	Fake	Normal
Hoeffding Tree	0.932	0.979	0.954	0.968	0.943	0.974
Random Tree	0.954	0.980	0.957	0.979	0.955	0.980
RBF	0.897	0.975	0.947	0.950	0.921	0.963
MLP	0.983	0.977	0.952	0.992	0.967	0.985
SVM	-	0.687	0.0	1.0	-	0.814
Naïve Bayes	0.873	0.985	0.968	0.935	0.918	0.960
Bagged Decision Tree	0.982	0.985	0.968	0.992	0.975	0.989

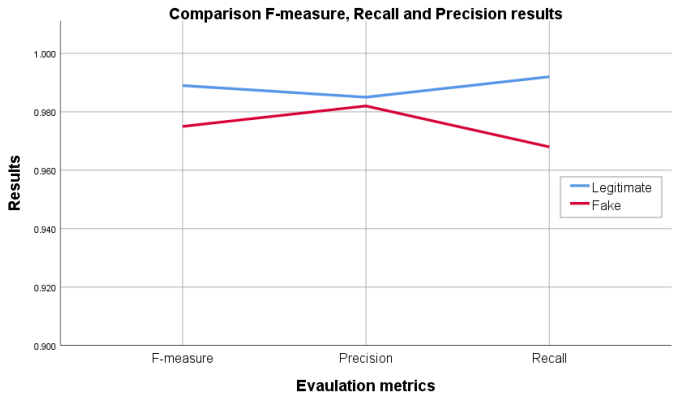

Figure 4. Comparison between F-measure, Recall and Precision results

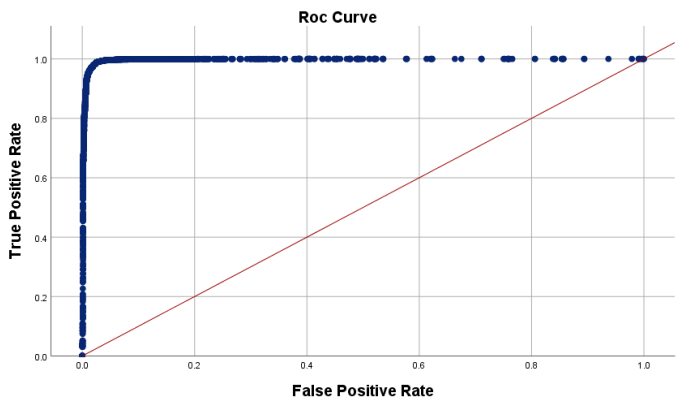

Figure 5. Receiver operating characteristic curve for the legitimate class

Table 5 illustrates the value of evaluation metrics in which precision, recall, and F-measure are measured for fake and legitimate accounts. Moreover, we have compared the proposed approach to other well-known classifiers: Random tree, J48, SVM, Naïve Bayes, and Hoeffding tree. The comparison between the proposed method and the mentioned algorithms is presented in Table 5.

As shown in Tables 4 and 5, we see that the bagging decision tree-based algorithm produced better performance than the other five classification algorithms. It successfully classified 98.45 of accounts with 1.55% misclassified, respectively. After the bagging algorithm, the MLP, Random Tree, and Hoeffding Tree algorithms obtained the highest performance on the dataset with a 97.9, 97.2%, and 96.38% classification accuracy. The RBF and Naive Bayes produced almost the same results, with an accuracy of 94.92% and 94.58%. The SVM algorithm obtained the lowest accuracy of 0.613, respectively. As presented in Table 4, the other four considered algorithms also achieved good detection accuracy. This is because of distinctive useful features (including content and user behavior) helps classification algorithms effectively distinguish fake users from legitimate ones. However, Figure 4 describes precision, recall, and F-measure ratios obtained by the model to illustrate the difference between each of the criteria better.

Figure 5 represents the result of the receiver operating characteristic (ROC) curve. ROC curve is a useful tool for visualization that can decide whether a model is suitable regarding cost sensitivity. In the represented (ROC) curve, the curve's x-axis denotes the false positive rate while the y-axis describes the false negative. The area found under the curve with the value of (0.989) shows that it is a suitable model.

In the next test, we classified accounts using each feature independently; this method is not very common but lets us find the influence of each feature's impact on detecting fake

accounts independently. The following two tables provide the information about the F-measure, accuracy, best feature type, and full feature set results on the datasets with different user accounts.

Table 6. Best feature types across different size of datasets

No. of Items	Best Feature	Accuracy	F-Measure
800	Followed	92.75	0.896
2000	has_pic	92.7	0.912
5000	Postcount	90.78	0.913
8000	Postcount	88.93	0.889
10000	Postcount	87.85	0.877

The results obtained in Table 6 demonstrate the feature type "Postcount" performed better than other features, which shows the number of account posts has a significant role in identifying the legitimacy of the Instagram accounts since many spammers who create fake accounts spend less time designing account appearances. Moreover, as shown in Table 7, there is a progressive increase in accuracy and F-measure ratios as the dataset size increases.

Table 7. The Full set of features results across different size of datasets

No. of Items	Accuracy	F-Measure
800	99.00	0.990
2000	98.1	0.981
5000	98.26	0.982
8000	98.31	0.983
10000	98.45	0.984

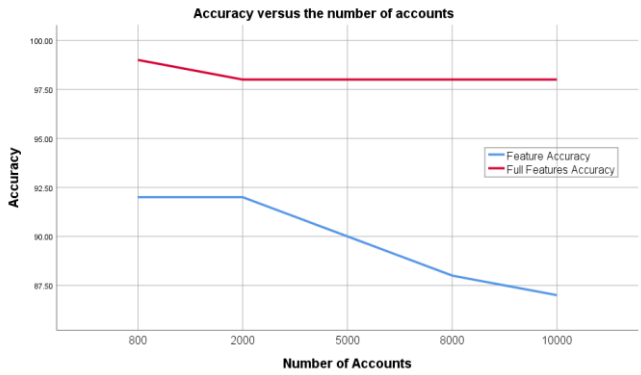

Figure 6. Accuracy versus the number of accounts across datasets

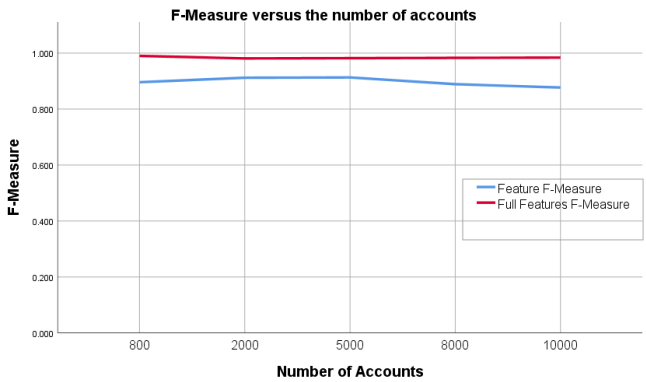

Figure 7. F-measure versus the number of accounts across datasets

Figures 6 and 7 show the changes in F-measure and accuracy as the number of accounts have increased over the datasets.

As shown in Figure 6, there is a progressively decrease in best feature accuracy results as the dataset size increases. This shows the role of the best feature in the final result gets lower when dataset size increases. Moreover, a gradual increase in accuracy levels of full features set results as the number of accounts is increased across the datasets. This increase is a sign that the features used perform satisfactorily across the data sets. We have only worked with a dataset of 10000 Instagram accounts, and the exhibited trends show that if the dataset size has increased, the accuracy could improve further. We present the F-measure trends over the dataset in Figure 7.

We can observe in Figure 7 that there has been a decrease in best feature F-measure results while there is progressively increasing in full features set results as the dataset size increases. This is similar to the accuracy trends obtained earlier in Figure 6.

6. CONCLUSIONS

Fake accounts are dangerous for social platforms since they may alter concepts like popularity and influence on Instagram and impact the economy, politics, and society. This paper has introduced a fake account detection method based on machine learning for the Instagram platform. To reach the proposed method's goal, we have created a dataset of legitimate and fake accounts for the Instagram platform. Then, various proposals for detecting fake accounts have been surveyed based on classification algorithms and feature sets. The introduced approach considered the user's content and behavior features and applied them to the bagging classifier algorithm for fake and legitimate accounts classification. Therefore, through a multitude of analysis, experiment, evaluation, and implementation work, the experiments' results have shown that the proposed method is feasible and capable of classifying over 98% of users accurately.

REFERENCES

[1] Guo, G., Zhu, Y., Yu, R., Chu, W.C.C., Ma, D. (2020). A privacy-preserving framework with self-governance and permission delegation in online social networks. IEEE Access, 8: 157116-157129. https://doi.org/10.1109/ACCESS.2020.3016041

[2] Boididou, C., Middleton, S.E., Jin, Z., Papadopoulos, S., Dang-Nguyen, D.T., Boato, G., Kompatsiaris, Y. (2018). Verifying information with multimedia content on twitter. Multimedia Tools and Applications, 77(12): 15545-15571. https://doi.org/10.1007/s11042-017-5132-9

[3] Alqatawna, J., Madain, A., Al-Zoubi, A., Al-Sayyed, R. (2017). Online social networks security: Threats, attacks, and future directions. In Social Media Shaping e-Publishing and Academia, pp. 121-132. https://doi.org/10.1007/978-3-319-55354-210

[4] Lőrincz, L., Koltai, J., Győr, A.F., Takács, K. (2019). Collapse of an online social network: Burning social capital to create it? Social Networks, 57: 43-53. https://doi.org/10.1016/j.socnet.2018.11.004

[5] Arora, A., Bansal, S., Kandpal, C., Aswani, R., Dwivedi, Y. (2019). Measuring social media influencer index-

insights from Facebook, Twitter and Instagram. Journal of Retailing and Consumer Services, 49: 86-101. https://doi.org/10.1016/j.jretconser.2019.03.012

[6] Boerman, S.C. (2020). The effects of the standardized Instagram disclosure for micro-and meso-influencers. Computers in Human Behavior, 103: 199-207. https://doi.org/10.1016/j.chb.2019.09.015

[7] Yang, C., Harkreader, R., Gu, G. (2013). Empirical evaluation and new design for fighting evolving twitter spammers. IEEE Transactions on Information Forensics and Security, 8(8): 1280-1293. https://doi.org/10.1109/TIFS.2013.2267732

[8] Han, Y., Fang, B., Jia, Y. (2014). Predicting the topic influence trends in social media with multiple models. Neurocomputing, 144: 463-470. https://doi.org/10.1016/j.neucom.2014.03.054

[9] Jr Barbon, S., Igawa, R.A., Zarpelão, B.B. (2017). Authorship verification applied to detection of compromised accounts on online social networks. Multimedia Tools and Applications, 76(3): 3213-3233. https://doi.org/10.1007/s11042-016-3899-8

[10] Blair, S.J., Bi, Y., Mulvenna, M.D. (2020). Aggregated topic models for increasing social media topic coherence. Applied Intelligence, 50(1): 138-156. https://doi.org/10.1007/s10489-019-01438-z

[11] Jiang, X., Li, Q., Ma, Z., Dong, M., Wu, J., Guo, D. (2019). QuickSquad: A new single-machine graph computing framework for detecting fake accounts in large-scale social networks. Peer-to-Peer Networking and Applications, 12(5): 1385-1402. https://doi.org/10.1007/s12083-018-0697-2

[12] Ramalingam, D., Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 65: 165-177. https://doi.org/10.1016/j.compeleceng.2017.05.020

[13] Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7): 96-104. https://doi.org/10.1145/2818717

[14] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., Tesconi, M. (2015). Fame for sale: Efficient detection of fake Twitter followers. Decision Support Systems, 80: 56-71. https://doi.org/10.1016/j.dss.2015.09.003

[15] Zhang, Y., Lu, J. (2016). Discover millions of fake followers in Weibo. Social Network Analysis and Mining, 6(1): 16. https://doi.org/10.1007/s13278-016-0324-2

[16] Thomas, K., Grier, C., Song, D., Paxson, V. (2011). Suspended accounts in retrospect: An analysis of twitter spam. In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, pp. 243-258. https://doi.org/10.1145/2068816.2068840

[17] Gao, H., Chen, Y., Lee, K., Palsetia, D., Choudhary, A. N. (2012). Towards online spam filtering in social networks. In NDSS, 12(2012): 1-16.

[18] Benevenuto, F., Magno, G., Rodrigues, T., Almeida, V. (2010). Detecting spammers on twitter. In Collaboration, Electronic Messaging, Anti-abuse and Spam Conference (CEAS), p. 12.

[19] BalaAnand, M., Karthikeyan, N., Karthik, S., Varatharajan, R., Manogaran, G., Sivaparthipan, C.B. (2019). An enhanced graph-based semi-supervised learning algorithm to detect fake users on Twitter. The Journal of Supercomputing, 75(9): 6085-6105. https://doi.org/10.1007/s11227-019-02948-w

[20] Sahoo, S.R., Gupta, B.B. (2019). Hybrid approach for detection of malicious profiles in twitter. Computers & Electrical Engineering, 76: 65-81. https://doi.org/10.1016/j.compeleceng.2019.03.003

[21] Breiman, L. (1996). Bagging predictors. Machine Learning, 24(2): 123-140. https://doi.org/10.1023/A:1018054314350

[22] Mordelet, F., Vert, J.P. (2014). A bagging SVM to learn from positive and unlabeled examples. Pattern Recognition Letters, 37: 201-209. https://doi.org/10.1016/j.patrec.2013.06.010

[23] Sheikhi, S., Kheirabadi, M.T., Bazzazi, A. (2020). An effective model for SMS spam detection using content-based features and averaged neural network. International Journal of Engineering, 33(2): 221-228. https://doi.org/10.5829/ije.2020.33.02b.06

[24] Sheikh Khozani, Z., Sheikhi, S., Mohtar, W.H.M.W., Mosavi, A. (2020). Forecasting shear stress parameters in rectangular channels using new soft computing methods. Plos One, 15(4): e0229731. https://doi.org/10.1371/journal.pone.0229731