# A PERCEPTIVE FAKE USER AND FAKE REVIEW DETECTION AND VISUALIZATION ON SOCIAL NETWORK AND E-COMMERCE

**G.KEERTHANA[1], K.PUSHPAVALLI[2]**

Department of Information Technology, Agni College Of Technology, Chennai.

**Abstract-** In social media, users are allowed to express their opinions by commenting on an item or rating an item with scores. The collection of user reviews would generate a positive or negative influence to the media audience. Some malicious users may create multiple variant accounts on the same social media so as to influence or manipulate public opinions for business or criminal purposes. To maintain good social environment, it is necessary to find those fake users. The proposed system we investigate the user variants identification problem using both user behaviour and item related information. It scans the characteristics of user behaviours on social media and introduces two concepts visibility and distinguishability to preliminarily quantify whether a fake user can be identified. To better understand user intention and characteristics, we profile a user with apparent and implicit features, which are extracted from three aspects: User Generated Contents (UGC), user behaviour context and item information. Based on these features, we propose the user Variants Identification Problem (VIP) and an Identification algorithm, which finds the top-k similar variants in a social media.

## 1.INTRODUCTION

Fake user identification is very related to the user mapping problem between two different social networks, which has been well investigated. They model a user based on user relationship, user attributes and user generated contents (UGCs) in social media.

Then they compute the distance between users and find the most similar users to a target user. However, in many social network platform, user profile, attributes and user relationships are not available under privacy settings. Some users may leave attributes empty or fill in with misinformation. These methods can not be applied to such social media.

The variant identification problem (VIP), which finds the variants for an appointed user on the same social media website. We need not have any background knowledge about the target user in advance. The basic philosophy behind such identification is that user behaviours on items are intentional interaction and there must exist many hints of the similarity between two variants, such as the frequently used words, the time stamps of rating, the sort of reviewed items etc.

To achieve their business or criminal purposes, the variants of the same user should have the same or similar attitude on the same item. In case a user intentionally performs differently using variants, this user could not generate large collective influence on the same item to the audience and it is not necessary to recognize him/her.

## 2.EXISTING SYSTEM

The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption.

Moreover, the possibility of expanding invalid information to users through fake identities has increased those results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs).

In the existing system, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. User-based features are established because of relationship and properties of user accounts. It is essential to append user-based features for the spam detection model. As these features are related to user accounts, all attributes, which were linked to user accounts, were identified.

### 2.1 DRAWBACKS OF EXISTING SYSTEM

- Users can’t always validate the trustworthiness of everyone providing recommendations.
- High sampling rates are required for transient feature extraction.
- Harm the interests of users on website.
- High complexity with the size of network such that they are not suitable for largescaled networks
- Highly competitive compared with other techniques

## 3. PROPOSED SYSTEM

Fake user identification is very related to the user mapping problem between two different social networks, which has been well investigated. They model a user based on user relationship, user attributes and user generated contents (UGCs) in social media.

Then they compute the distance between users and find the most similar users to a target user. However, in many social network platform, user profile, attributes and user relationships are not available under privacy settings. Some users may leave attributes empty or fill in with misinformation. These methods cannot be applied to such social media.

The variant identification problem (VIP), which finds the variants for an appointed user on the same social media website. We need not have any background knowledge about the target user in advance. The basic philosophy behind such identification is that user behaviours on items are intentional interaction and there must exist many hints of the similarity between two variants, such as the frequently used words, the time stamps of rating, the sort of reviewed items etc.

To achieve their business or criminal purposes, the variants of the same user should have the same or similar attitude on the same item. In case a user intentionally performs differently using variants, this user could not generate large collective influence on the same item to the audience and it is not necessary to recognize him/her.

### 3.1 ADVANTAGES OF PROPOSED SYSTEM

- Fake reviews are recognized with high accuracy and precision.
- Higher efficiency and preciseness.
- Much accurate and higher than any of the existing system.

## 4. ARCHITECTURE

We have provided a clear architecture (Fig.No1) for our proposed system. Here the system works by giving the input data set into the algorithm for user mapping and De-anonymization. This datasets are classified into three models of training data where the user behavior is analyzed along with the item feature and Corpus for training the system to detect fake users and fake news. This data sets are then fed into a user variants identification algorithm and the contents of the user generated content modelling, behaviour content modelling and item-based user content modelling are formed and the fake users are predicted.

Input

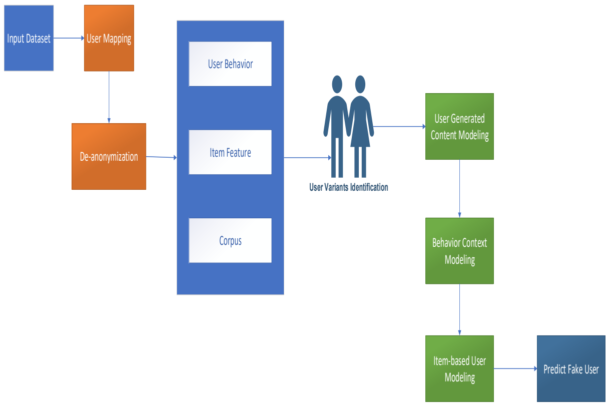


Fig.1 Architecture Diagram

### 4.1Data Cleaning and Preprocessing

Before working on data, data needs to be refined so that it is easier to work upon it. Datasets were refined by stop word removal, conversion to lower case, punctuation removal, tokenization, and sentence segmentation.

### 4.2 Removal of stop words

Stop words are such words that are not significant and can add error when used as a feature in classification. They are mainly articles, prepositions, conjunctions and pronouns such as a, an, that, what and so on. These words were omitted from the documents and documents are then passed to the next step.

### 4.3 Tokenize

Tokens are usually individual words and tokenization is a task in NLP in which a set or set of text is taken and broken into individual words. These tokens are then used as input for lemmatization.

### 4.4 Lemmatize

Lemmatization involves reducing a word to its base form by usually chopping the ends of the words. In lemmatization, this is done by morphological analysis of words and use of a vocabulary. For example, the word ‘saw’ is reduced to either ‘see’ or ‘saw’ depending on the usage of word. After lemmatization, all the letters of words are converted to lower form.

### 4.5 Advantages of Proposed Algorithm:

- It produces a highly accurate classifier.
- It runs efficiently on large datasets.
- It can handle thousands of input variables without variable deletion.
- It gives estimation of what variables are important in the classification.
- It generates an internal unbiased estimate of the generalization error as the forest building progresses.

## 5.MODULE DESCRIPTION

### 5.1 Gathering Input datasets

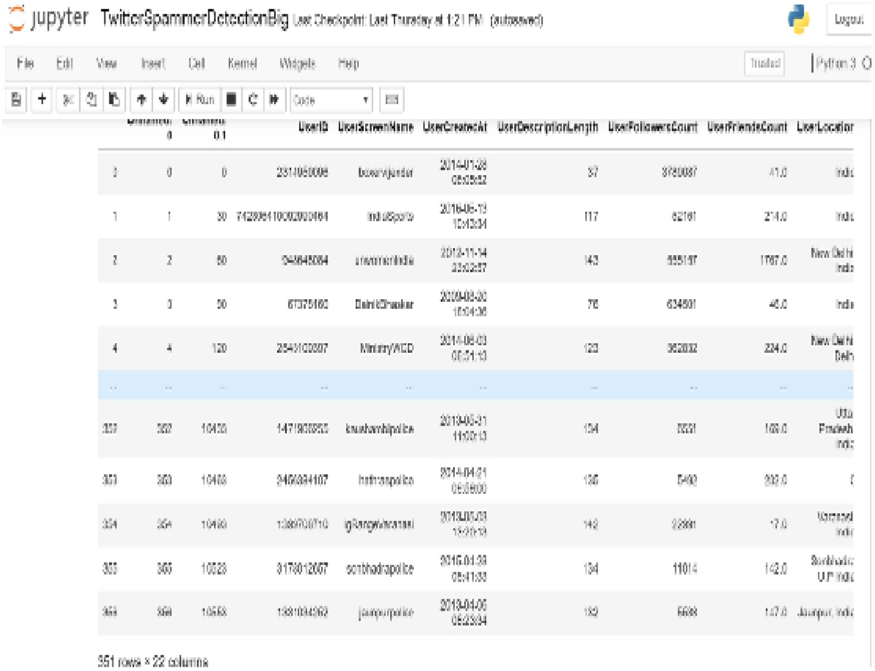
In social media, users are allowed to express their opinions by commenting on an item or rating an item with scores. The collection of user reviews would generate a positive or negative influence to the media audience. Some malicious users may create multiple variant accounts on the same social media so as to influence or manipulate public opinions for business or criminal purposes.

To maintain good social environment, it is necessary to find those fake users. In this paper, we investigate the user variants identification problem using both user behaviour and item related information. The proposed system scans the characteristics of user behaviours on social media and introduces two concepts visibility and distinguishes ability to preliminarily quantify whether a fake user can be identified.

To better understand user intention and characteristics, we profile a user with apparent and implicit features, which are extracted from three aspects: User Generated Contents (UGC), user behaviour context and item information. Based on these features, we propose the user Variants Identification Problem (VIP) and an identification algorithm, which finds the top-k similar variants in a social media.

### 5.2 Classifying The Datasets

To better understand user intention and characteristics, we profile a user with apparent and implicit features, which are extracted from three aspects: User Generated Contents (UGC), user behaviour context and item information. Based on these features, we propose the user Variants Identification Problem (VIP) and an identification algorithm, which finds the top-k similar variants in a social media.


jupyter TwitterSpammerDetectionBig Last Checkpoint: Last Thursday at 1:21 PM (autosaved)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Trusted
Python 3
Run
Code

| | Unnamed: 0 | Unnamed: 0.1 | UserID | UserScreenName | UserCreatedAt | UserDescriptionLength | UserFollowersCount | UserFriendsCount | UserLocation |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 2314050096 | bcsarvjander | 2014-01-28<br>05:05:52 | 37 | 3780087 | 41.0 | Indi |
| 1 | 1 | 30 | 742806410092880464 | IndiaSports | 2016-06-13<br>10:13:34 | 117 | 62161 | 214.0 | Indi |
| 2 | 2 | 50 | 948845084 | unwomenIndia | 2012-11-14<br>23:02:57 | 143 | 555197 | 1767.0 | New Delhi<br>Indi |
| 3 | 3 | 50 | 67375160 | DainikBhaskar | 2009-08-20<br>16:04:36 | 76 | 634501 | 46.0 | Indi |
| 4 | 4 | 120 | 2541100007 | MinistryWCD | 2014-05-03<br>05:51:13 | 123 | 352032 | 224.0 | New Delhi<br>Delh |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 350 | 352 | 10420 | 1471900950 | kaushambipolice | 2013-05-31<br>11:00:13 | 134 | 8551 | 169.0 | Utta<br>Pradesh<br>Indi |
| 351 | 353 | 10468 | 2469394107 | hathraspolice | 2014-04-21<br>05:59:00 | 136 | 5402 | 302.0 | I |
| 354 | 354 | 10480 | 1389700710 | igRangeVaranasi | 2013-05-03<br>13:20:13 | 142 | 22881 | 17.0 | Varnasi<br>Indi |
| 355 | 356 | 10523 | 3178012067 | sonbhadrapolice | 2015-04-28<br>05:41:33 | 134 | 11014 | 142.0 | Sonbhadra<br>UP Indi |
| 358 | 358 | 10558 | 1381094262 | jaunpurpolice | 2013-04-05<br>05:23:34 | 132 | 5688 | 147.0 | Jaunpur, Indi |

351 rows × 22 columns

Fig 2. random forest algorithm output

### 5.3 Training the Algorithm

Training data is given to the algorithm and the algorithm is trained on how to analyse and detect the fake data's. To maintain good social environment, it is necessary to find those fake users. In this paper, we investigate the user variants identification problem using both user behaviour and item related information. The proposed system scans the  characteristics of user behaviours on social media and introduce two concepts visibility and distinguish ability to preliminarily quantify whether a fake user can be identified.

### 5.4 Getting the Inputs

In the existing system, we perform a review of techniques used for detecting spammers on Twitter. Moreover, taxonomy of the Twitter spam detection approaches
is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. User-based features are established because of relationship and properties of user accounts. It is essential to append user-based features for the spam detection model. As these features are related to user accounts, all attributes, which were linked to user accounts, were identified.

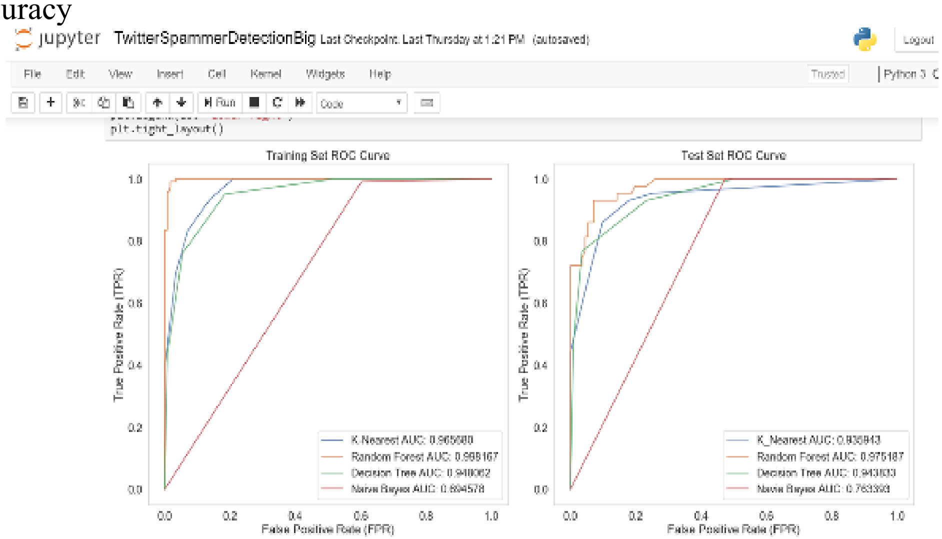
### 5.5 Data Pre-processing

The distance between users and find the most similar users to a target user. However, in many social network platforms, user profile attributes and user relationships are not available under privacy settings. Some users may leave attributes empty or fill in with misinformation. These methods cannot be applied to such social media.

(Fig 2)Variant identification problem (VIP), which finds the variants for an appointed user on the same social media website. We need not have any background knowledge about the target user in advance. The basic philosophy behind such identification is that user behaviours on items are intentional interaction and there must exist many hints of the similarity between two variants, such as the frequently used words, the time stamps of rating, the sort of reviewed items etc.

### 5.6 Detecting Fake Users and Fake News

(Fig 3) This system helps to maintain a good social media environment without any misinformation spreading through fake user accounts and also identifies fake users in social media sites and applications. The Existing system uses Naïve Bayes Algorithm which produces only 76% (0.763393) accurate results. This accuracy is not enough to find fake users and their contents immediately within a short duration. The proposed algorithm, Random Forest Algorithm Produces 97% (0.975187) accurate results in finding the fake users. The Random Forest Algorithm, Unlike any other Algorithm can be trained with multiple random datasets and it creates various random root nodes and feature nodes according to the datasets given. Since Twitter is an open source API, we can access user accounts directly from twitter using the tweedy class in python language, we use twitter as our test application. A total of 1000 random accounts are gathered, analyzed and classified for training and testing. After training the Algorithm the trained datasets is analyzed with the testing datasets. When compared out of the four algorithms used Random Forest Algorithm was able to find the fake users and contents with 96% accuracy



```
plt.tight_layout()
```

jupyter
TwitterSpammerDetectionBig Last Checkpoint: Last Thursday at 1:21 PM (autosaved)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Trusted
Python 3
Run
Code
Training Set ROC Curve
Test Set ROC Curve
True Positive Rate (TPR)
False Positive Rate (FPR)
0.0
0.2
0.4
0.6
0.8
1.0
K Nearest AUC: 0.965680
Random Forest AUC: 0.998167
Decision Tree AUC: 0.940062
Naive Bayes AUC: 0.694578
K_Nearest AUC: 0.936943
Random Forest AUC: 0.975187
Decision Tree AUC: 0.943833
Naive Bayes AUC: 0.763393

Fig 3. False Positive Rate

## 6.CONCLUSION

This system investigates the user variants identification problem using both user behaviour and item related information. We study the characteristics of user behaviours on social media and introduce two concepts visibility and distinguish ability to preliminarily quantify whether a fake user can be identified. To better understand user intention and characteristics, we profile a user with apparent and implicit features. Based on these features, we propose the user Variants Identification Problem (VIP) and an identification algorithm, which finds the top-k similar variants in a social media.

## REFERENCES:

*a) N. Jindal and B. Liu, "Opinion Spam and Analysis," in Proceedings of the 2008 international conference on web search and data mining, New York, NY: ACM, 2008.*
*b) H. Ahmed, I. Traore and S. Saad, "Detecting opinion spams and fake news using text classification," Security and Privacy, vol. 1, no. 1, 2018.*
*c) V. P´erez-Rosas, B. Kleinberg, A. Lefevre and R. Mihalcea, "Automatic Detection of Fake News," 2017.*
*d) Z. Jin, J. Cao, Y. Zhang, J. Zhou and Q. Tian, "Novel visual and statistical image features for microblogs news verification," IEEE Transactions on Multimedia, vol. 19, no. 3, pp. 598-608, 2017.*
*e) Z. Zhao, J. Zhao, Y. Sano, O. levy, H. Takayasu, M. Takayasu, D. Li, J. Wu and S. Havlin, "Fake news propagate differently from real news even at early stages of spreading.," 2018.*
*f) M. Egele, G. Stringhini, C. Kruegel and G. Vigna, "Towards detecting compromised accounts on social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 447-460, 2017.*
*g) A. Campan, A. Cuzzocrea and T. M. Truta, "Fighting fake news spread in online social networks: Actual trends and future research directions," in IEEE International Conference on Big Data (Big Data), Boston, MA, 2017.*
*h) E. Okoro, B. Abara, U. Alex and Z. Isa, "A hybrid approach to fake news detection on social media," in Nigerian Journal of Technology (NIJOTECH, Nsukka, 2018.*
*i) M. Alrubaian, M. Al-Qurishi, M. M. Hassan and A. Alamri, "A Credibility Analysis System for Assessing Information on Twitter," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 661-674, 2018.*
*j) A. Figueira and L. Oliveira, "The current state of fake news: challenges and opportunities," Procedia Computer Science, vol. 121, pp. 817-825, 2017.*
*k) E. Tacchini, G. Ballarin, M. L. D. Vedova, S. Moret and L. d. Alfaro, "Some Like it Hoax: Automated Fake News Detection in Social Networks," School of Engineering, University of California, Santa Cruz, California, 2017.*