ANALYZING REAL AND FAKE USERS IN INSTAGRAM NETWORK

ANUSRI P[1], JANAPRIYA P[2], KAVIPRIYA[2], LOKESWARI SS[2], ANITHA M[3]

1UG Scholar, Department of CSE, Kingston Engineering College, Vellore-59
2UG Scholar, Department of CSE, Kingston Engineering College, Vellore-59
3Asst.Professor, Department of CSE, Kingston Engineering College, Vellore-59

Abstract - People are highly dependent on online social networks (OSNs) which have attracted the interest of cyber criminals for carrying out a number of malicious activities. A whole industry of bootleg market administrations has developed which offers counterfeit records based administrations available to be purchased. We, in this way, in our work, center around recognizing counterfeit records on an exceptionally famous (and hard for information assortment) online interpersonal organization, Instagram. Key commitments of our work are as per the following.

The primary commitment has been assortment of information identified with genuine and counterfeit records on Instagram. Because of exacting security settings and consistently advancing API of Instagram with every rendition including more limitations, gathering client accounts information turned into a significant test. Our second commitment is the utilization of client channel data on Instagram to comprehend client profile movement and distinguishing a broad set of 17 highlights which assume a key job in segregating counterfeit clients on Instagram with genuine clients. Third commitment is the utilization these highlights and recognizing the key AI based classifiers who perform well in identification task out of a sum of 12 classifiers utilized. Fourth commitment is the distinguishing which kind of exercises (like, remark, labeling, sharing, and so forth) contribute the most in counterfeit client location. Results show arrangement exactness of 79% among the best performing classifiers. In wording of exercises, likes and remarks contribute well towards location task. In spite of the fact that the precision isn't exceptionally high, be that as it may, our work structures a standard for additional improvement. Our outcomes demonstrate that many phony clients are delegated genuine proposing plainly that counterfeit records are imitating genuine client conduct to sidestep recognition instruments. Our work finishes up by enrolling various future course of activities that can be embraced.

***Key Words*:** Machine Learning, Naive Bayes, Random Forest, Decision Tree, Detection ,Fake Account

1.INTRODUCTION

Social networking sites have commonly used the channel of communication between people. Users of social networking sites can share their information and daily activities, which attract a number of people towards these sites. One of the most widely used social networking sites is 'Instagram'. The Figure shows the increasing popularity of Instagram from the year 2004 to 2016. Instagram allow the users to add friends and share various kind of information such as personal, social, political, business etc. Moreover, they can also share photos, videos, travels and other day-to-day affairs. However, some people do not use these sites with good intent. Therefore, they create fake accounts on social networking sites. Fake accounts do not have any real identity. The person who creates fake accounts is known as Attacker. The attacker uses incorrect information or statistics about some real world person to create a fake account. Using theses fake accounts, attacker spread false information, which affects other users. To protect such sensitive data of users is one of the major challenges of social networking sites. There is a range of machine learning techniques that have been developed to detect fake accounts in social networking sites. Some of these techniques are Neural Network, Naive Bayes, Markov Model and Bayesian Network. In recent researches, it has been found that these techniques make available enhanced results to detect fake accounts. Neural Network consists of many interconnected processing elements. It takes decisions just like a human brain. SVM is supervised machine learning techniques used for classification. It finds the hyper plane to classify the data. Neural network and SVM are able to accept a large amount of random data and suitable to detect the fake accounts.

Online Social Networks (OSNs), such as Instagram, Twitter and LinkedIn, have become increasingly popular over the last few years. People use OSNs to keep in touch with each other's, share news, organize events, and even run their own e-business. Instagram community continues to grow with more than 2.2 billion monthly active users and 1.4 billion daily active users, with an increase of 11% on a year-over-year

basis. For the purpose to detect fake accounts on the social media platforms the dataset generated was pre-processed and fake accounts were determined by machine learning algorithms.[3] The classification performances of the algorithms Random Forest, Neural Network and Support Vector Machines are used for the detection of fake accounts. The accuracy rates of detecting fake accounts using the mentioned algorithms are compared and the algorithm with the best accuracy rate is noted.

2. LITERATURE SURVEY

2.1 CLASSIFICATION OF SENTIMENT REVIEWS USING N-GRAM MACHINE LEARNING APPROACH

AUTHOR: Tripathy, A., Agrawal, A., &Rath, S. K.

DESCRIPTION:

With the ever increasing social networking and online marketing sites, the reviews and blogs obtained from those, act as an important source for further analysis and improved decision making. These reviews are mostly unstructured by nature and thus, need processing like classification or clustering to provide a meaningful information for future uses. These reviews and blogs may be classified into different polarity groups such as positive, negative, and neutral in order to extract information from the input dataset. Supervised machine learning methods help to classify these reviews. In this paper, four different machine learning algorithms such as Naive Bayes (NB), Maximum Entropy (ME), Stochastic Gradient Descent (SGD), and Support Vector Machine (SVM) have been considered for classification of human sentiments. The accuracy of different methods are critically examined in order to access their performance on the basis of parameters such as precision, recall, f-measure, and accuracy.

2.2 COMMUNITY-BASED WEIGHTED GRAPH MODEL FOR VALENCE-AROUSAL PREDICTION OF AFFECTIVE WORDS

AUTHOR: JinWang ; Liang-Chih Yu ; K. Robert Lai ; Xuejie Zhang

DESCRIPTION:

Compared to the categorical approach that represents affective states as several discrete classes (e.g., positive and negative), the dimensional approach represents affective states as continuous numerical values in multiple dimensions, such as the valence-arousal (VA) space, thus allowing for more fine-grained sentiment analysis. In building dimensional sentiment applications, affective lexicons with VA ratings are useful resources but are still very rare. Several semi-supervised methods such as the kernel method, linear regression, and the pagerank algorithm have been investigated to automatically determine the VA ratings of affective words from a set of semantically similar seed words. These methods suffer from two major limitations. First, they apply an equal weight to all seeds similar to an unseen word in predicting its VA ratings. Second, even similar seeds may have quite different ratings (or an inverse polarity) of valence/arousal to the unseen word, thus reducing prediction performance. To overcome these limitations, this study proposes a community-based weighted graph model that can select seeds which are both similar to and have similar ratings (or the same polarity) with each unseen word to form a community (subgraph) so that its VA ratings can be estimated from such high-quality seeds using a weighted propagation scheme. That is, seeds more similar to unseen words contribute more to the estimation process. Experimental results show that the proposed method yields better prediction performance for both English and Chinese datasets.

2.3 AUDIT AND ANALYSIS OF IMPOSTORS: AN EXPERIMENTAL APPROACH TO DETECT FAKE PROFILE IN ONLINE SOCIAL NETWORK

AUTHOR: Sarode, A. J., & Mishra, A

DESCRIPTION:

In the present generation, the social life of every person has become associated with online social networks (OSN). These sites have made drastic changes in the way we socialize. Making friends and keeping in contact with them as well as being updated of their activities, has become easier. But with their rapid growth, problems like fake profiles, online impersonation have also increased. The risk lies in the fact that anybody can create a profile to impersonate a real person on the OSN. The fake profile could be exploited to build online relationship with a targeted person purely through online interactions with the friends of victim.

In present work, we have proposed experimental framework with which detection of fake profile is feasible within the friend list, however this framework is restricted to a specific online social networking site namely Instagram. This framework extracts data from the friend list and uses it to classify them as real or fake by using unsupervised and supervised machine learning.

2.4 DATA MINING EMOTION IN SOCIAL NETWORK COMMUNICATION: GENDER DIFFERENCES IN MYSPACE

AUTHOR: Thelwall, M., Wilkinson, D., &Uppal, S.

DESCRIPTION:

Despite the rapid growth in social network sites and in data mining for emotion (sentiment analysis), little research has tied the two together, and none has had social science goals. This article examines the extent to which emotion is present in MySpace comments, using a combination of data mining and content analysis, and exploring age and gender. A random sample of 819

public comments to or from U.S. users was manually classified for strength of positive and negative emotion. Two thirds of the comments expressed positive emotion, but a minority (20%) contained negative emotion, confirming that MySpace is an extraordinarily emotion-rich environment. Females are likely to give and receive more positive comments than are males, but there is no difference for negative comments. It is thus possible that females are more successful social network site users partly because of their greater ability to textually harness positive affect.

2.5MUTUAL CLUSTERING COEFFICIENT-BASED SUSPICIOUS-LINK DETECTION APPROACH FOR ONLINE SOCIAL NETWORKS

AUTHOR: Wani, M.A., Jabin, S.

DESCRIPTION:

Online social networks (OSNs) are trendy and rapid information propagation medium on the web where millions of new connections either positive such as acquaintance, or negative such as animosity, are being established every day around the world. The negative links (or sometimes referred to as harmful connections) are mostly established by fake profiles as they are being created by minds with ill aims. Detecting negative (or suspicious) links within online users can better aid in the mitigation of fake profiles from OSNs.

A modified clustering coefficient formula, named as Mutual Clustering Coefficient represented by MCC, is introduced to quantitatively measure the connectivity between the mutual friends of two connected users in a group. In this paper, a classification system based on mutual clustering coefficient and profile information of users has been presented to detect the suspicious links within the user communities. Profile information helps us to find the similarity between users. Different similarity measures have been employed to calculate the profile similarity between a connected user pair. Experimental results demonstrate that four basic and easily available features such as work w ,education e , home_town ht and current_city (cc) along with MCC play a vital role in designing a successful classification system for the detection of suspicious links.

2.6 THE ENSEMBLE METHOD TO DETECT THE PHISHING SCAMS IN SOCIAL NETWORKS

AUTHOR: A. Saberi et al. (2007)

DESCRIPTION:

This paper present ensemble method to detect the phishing scams. Data mining classification algorithms such Naive Bayes, K-nearest neighbor and Poisson probabilistic theory and Naive Bayes are used to classifying spam and non-spam. The result of these classifiers is combined to get higher accuracy. Naive Bayes, k-nearest neighbor and Poisson algorithm separately provide accuracy of 88%, 87.5%, and 90.6% respectively. After combining these three techniques, it provides increased accuracy with 94.4%. The accuracy to detect the scams can be improved by using other techniques such as Neural Networks and SVM .

2.7SUPERVISED MACHINE LEARNING TECHNIQUES TO DETECT THE SPAMMERS ON SOCIAL NETWORKS

AUTHOR: Durgesh k. Srivastav et al. (2009)

DESCRIPTION:

This paper presents the overview of SVM and the selection of a kernel function among the functions. SVM is a supervised machine learning techniques which can be applied to various kinds of data sets. Dimensions of data and Limited samples do not create any limitation in an SVM. There are two types of SVM, linear SVM, and nonlinear SVM. For nonlinear data set, we can use nonlinear SVM with its kernel functions. The commonly used kernels are the linear kernel, polynomial kernel, RBF kernel and sigmoid kernel. In RBF kernel there are less numerical difficulties. It nonlinearly maps data sample into higher dimensional space and it also has fewer hyperplanes than the polynomial kernel. SVM always gives better accuracy than other algorithms .

2.8THE DETECTION SPAMMERS ON TWITTER SOCIAL NETWORK

AUTHOR: G.MAGNO ET AL. (2010)

DESCRIPTION:

This paper presents the problem to detecting spammers on twitter. In this dataset of twitter is collected and labeled the pre-classified spammer and non-spammer users. Then attributes are identified based on the social behavior of the user. In this paper supervised machine learning technique SVM is used to discover the spammers. Radial Basis Function (RBF) kernel of Nonlinear SVM is used classifies very complex data. Based on the ten attributes this technique differentiates the spammer and non-spammers. In this 70% of spammers and 96% of non-spammers are rightly recognized. The approach of this paper is also able to detect spam as an alternative of spammers. The accuracy of detecting spam is 87.2% .

2.9 THE CLASSIFICATION TECHNIQUES TO DETECT THE FAKE ACCOUNTS ON TWITTER

AUTHOR: A. AZAB ET AL. (2016)

DESCRIPTION:

This paper presents the classification techniques to detect the fake accounts on twitter. To detect the fake accounts this paper used feature based approach. The minimum weighted feature set is used. In this approach, the behavior of the user is identified. The real user behaves differently than fake users. This

behavior is used to identify the fake accounts. Different classification techniques such as random forest, decision tree, naive Bayes, neural network, and SVM are used. The accuracy of all techniques is provided. The gain measure is used to assign the weights to the feature set. To train and test the algorithms five-fold cross-validations are applied SVM gives best accuracy results to detect the fake accounts .

2.10 TECHNIQUE TO DETECT FAKE ACCOUNTS ON SOCIAL NETWORKING SITE CALLED FAKE PROFILE RECOGNIZER

AUTHOR: ALI M. MELIGY (2017)

DESCRIPTION

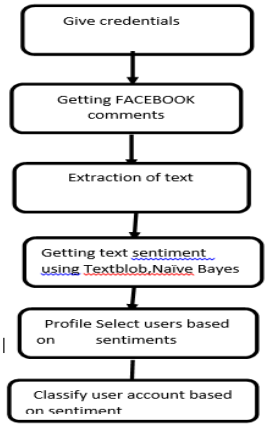
This paper presents a technique to detect fake accounts on social networking site called fake profile recognizer. This technique is based on two methods i.e regular expression and deterministic finite automata. A regular expression is used to authenticate the profiles and deterministic automata recognize the identities in trusted manner. This technique is applied on Instagram Google Plus and Twitter data set. The accuracy of Instagram, Twitter and Google + data set is 89.73%, 76.94%, 81.9% respectively. The Precision for Instagram is 88.9% for Google+ is 77.41 Percent and for twitter is 81.81%. The false positive rate for Instagram is 11.66, for Google+ is 26.10% and for Twitter is 20.86%. The false negative rate for Instagram is 11.04%, Google + 22.60% and for Twitter 18.20% .

3.PROPOSED SYSTEM

In proposed work, In on-line social networks to detect the fake accounts is a major challenge. The people using on-line social networks suffer from the various problems, which affects their personal as well as business life. The number of fake accounts on a social network is increased. Online social network suffers from fake accounts which are created. Fake accounts present fake news, web rating, and spam. Our proposed plan detects the fake accounts in the Instagram. There are various techniques are available to detect the fake accounts on the on-line social networks. Each has their own advantages and purposes. But still, existing methods do not have a very high value of f-measure and recall value. This proposed work combines the weighted feature set with machine learning techniques to obtain the best results Using the proposed technique for detecting the fake accounts on Instagram will improve the accuracy and exactness.

This proposed work uses the techniques like neural networks and support vector machine for classification of real and fake accounts. The feature set that influences the detection of fake accounts detection of the fake on Instagram will be used. This proposed work is expected to generate the higher value of f-measure and recall required for detection of fake account in Instagram. The machine learning techniques are neural network and Support vector machine provides the accurate results. Neural network and Support vector machine gives the better results in data classification. Machine learning techniques have been widely used in promoter prediction techniques because of its capability to be taught and resolve many real time problems. They can adjust their inner configuration without human intervention to produce estimated outcome for the specified problem and to find a connection between input and output. Therefore neural network and support vector machine results in higher accuracy for detecting the fake accounts on Instagram.

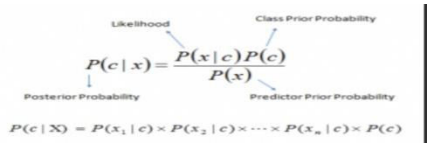
FLOW CHART



3.1 ALGORITHMS USED

NAIVE BAYES ALGORITHM :

- It is a classification technique based on bayes' theorem with an assumption of independence among predictors. In simple terms, a naive bayes classifier assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature.
- Naive bayes model is easy to build and particularly useful for very large data sets. Along with simplicity, naive bayes is known to outperform even highly sophisticated classification methods.
- **Naive bayes** can be extremely fast relative to other classification algorithms. It works on bayes theorem of probability to predict the class of unknown data sets.



RANDOM FOREST ALGORITHM:

- Random forests is a supervised learning algorithm. It can be used both for classification and regression. It is also the most flexible and

easy to use algorithm. A forest is comprised of trees. It is said that the more trees it has, the more robust a forest is. Random forests creates decision trees on randomly selected data samples, gets prediction from each tree and selects the best solution by means of voting. It also provides a pretty good indicator of the feature importance.

- Random forests has a variety of applications, such as recommendation engines, image classification and feature selection. It can be used to classify loyal loan applicants, identify fraudulent activity and predict diseases. It lies at the base of the boruta algorithm, which selects important features in a dataset.

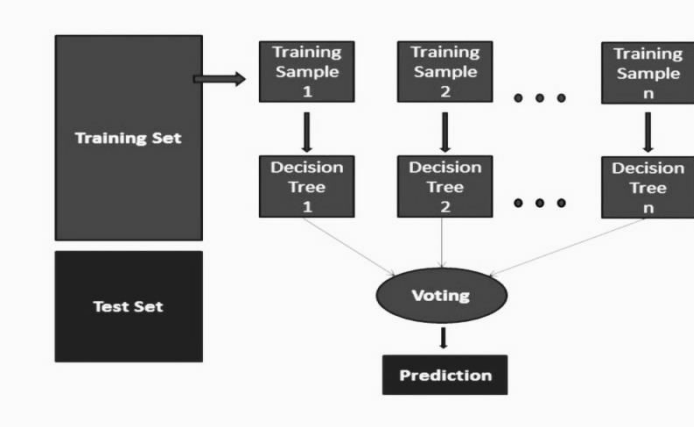
It works in four steps:

STEP-1 Select random samples from a given dataset.

STEP-2 Construct a decision tree for each sample and get a prediction result from each decision tree.

STEP-3 Perform a vote for each predicted result.

STEP-4 Select the prediction result with the most votes as the final prediction.



3.2 CONCLUSION

- In this research, We have come up with an ingenious way to detect fake accounts on OSNs By using machine learning algorithms to its full extent, we have eliminated the need for manual prediction of a fake account, which needs a lot of human resources and is also a time-consuming process. Existing systems have become obsolete due to the advancement in the creation of fake accounts. The factors that the existing system relayed upon is unstable. In this research, we used stable factors such as engagement rate, artificial activity to increase the accuracy of the prediction.

- This proposed work presents a hybrid approach to detects the fake accounts on Instagram. In this proposed technique clustering, classification and feature selection algorithms are applied to get better results. The following points mention some idea that can be further implemented.

- This technique can also be used for other social networking sites such as Twitter and LinkedIn with the minor changes.

- The accuracy of proposed technique can also be improved using different feature selection techniques.

REFERENCES

1.Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. (2010, November).

2. Tran, D. N., Min, B., Li, J., & Subramanian, L. (2009, April).

3. Galán-García, P., Puerta, J. G. D. L., Gómez, C. L., Santos,I., &Bringas, P. G. (2016).

4. Doerr, B., Fouz, M., & Friedrich, T. (2012).

5. Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., &Razak, S. A. (2017).