International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0047
ISSN (Online): 2279-0055

International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

Uncovering of Fake Users in Twitter Using Classifiers

[1] Sanjeev Dhawan, [2] Kulvinder Singh, [3]Satinder
[1,2]Faculty of Computer Science & Engineering, [3]Student of M.Tech.(Computer Engineering),
[1,2,3]Department of Computer Science & Engineering,
University Institute of Engineering and Technology (U.I.E.T),
Kurukshetra University, Kurukshetra (K.U.K)-136119, Haryana, INDIA

Abstract*: In the modern era, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way people pursue their social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake identity, fake profiles, and online impersonation have also grown. To overcome this problem, writeprint technique is used. This technique is proposed for the user identification by using the different classifiers. Comparison between various classification techniques will be done to find out which one is best in case of detection of user identification whether it is fake or genuine. The data which has been provided for the entire process to be performed is extracted from the Twitter with the help of R package as it provides interface with the Twitter web API (Application Programmable Interface). Various calculations are performed to calculate the accuracy, precision, recall, fmeasure, gmean, and time complexity.*

Keywords*: Identity recognition, R package, social networks, text mining, writeprint.*

I. Introduction

A social networking site is a website where each user has a profile and can keep in contact with family, friends, share their updates, and meet new people who have the same interests. These Online Social Networks (OSN) uses web2.0 technology, which allows users to interact with each other. These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends. Popular method now combine many of these, with American-based services such as FACEBOOK, GOOGLE +, and twitter widely used worldwide. From the last few years social networking sites for example Facebook , Twitter etc. have gained so much popularity it becomes the daily routine of almost every person to check their profile at least once in a day. Social networks are also called as the web networks which helps its users to create the semi public profiles which means this site allows one to share their information whether it is personal or professional depending on their wish. These online social networks are growing rapidly and there are more than 160 major social network websites exist in the world. 300 million active accounts in Facebook, Twitter has more than 500 million users, out of which more than 332 million are active. Apparently, of some 500 million users, a lot are fake profiles created to spread spam and viruses. There are often categorized as spammers or attackers. Some 60 percent of fake accounts purport to be bisexuals, about 10 times more than real users. Fake Twitter accounts tend to have lots of friends, about six times more than real users. On average this is about 726 friends versus 130. The rise of the fake accounts is a growing issue on Twitter. It is difficult to verifying the owners of the real social accounts in order to eliminate the effect of any fake account on mass people. Recognize the fake accounts are very big problem in front of researchers. These problems can be found out by recognize the user identity using writeprint. This paper targets to detect the fake identity of the social network user by comparing a claimed text against the original text of the user. The rest of this paper is structured as follow: section 2 discusses the related work, section 3 describes the experimental design and the expected results and section 4 closes with conclusion.

II. Related Work

The social networks became very effective in the recent time. Many people use it to communicate, lead and manage people activity either to support or oppose different causes. This raised the issue of verifying the owners of social accounts in order to eliminate the effect of any fake account on mass people. The aim of this paper is to detect the fake identity of the social network user by comparing a claimed text against the original text of the user. The researchers used a technique that analyses short message from the social network of twitter and extract linguistic features that can distinguish between the writing styles of different users. The present literature survey concentrates on the work done by a number of researchers worldwide in the field of recognize user identity in social networking websites. Fingerprint based identification has been the oldest biometric technique successfully used in conventional crime investigation. The unique, immutable patterns of a fingerprint- the pattern of ridges

and furrows as well as the minutiae points-can help a crime investigator infer the identities of suspects. The absence of fingerprints in cyberspace leads law enforcement and intelligence community to seek new approaches to trace criminal identity in cyber-crime investigation. To overcome this problem they proposed new approach called 'writeprint' hidden in people's writings. Similar to a fingerprint, a writeprint was composed of multiple features, such as vocabulary richness, length of sentence, use of function words, layout of paragraphs, and keywords [1]. The writeprint of an individual is the combinations of features that occur frequently in his/her written texts. The most commonly used features are lexical, syntactical, and structural and content-specific attributes. By matching the writeprint with the written texts, the true author can be identified. Most importantly, the matched writeprint should provide credible evidence for supporting the conclusion. The research community (De Vel, 2000; Zheng *et al.*, 2006; Teng *et al*., 2004[2]) has devoted a lot of efforts in studying stylistic and structural features individually, but very few of them has studied the combination of features that form a writeprint. This approach was developed by R.Zheng *et al*. (2006) [3] to help identify an author in cyberspace. They also developed a GA-based feature selection model to identify the key features of writeprint for online messages and the identified key features achieve more comparable, higher accuracy and effective differentiate the writeprint of different online authors. Furthermore, they also applied the writeprint identification approach to other problems like intellectual property checking and plagiarism detection. Writeprint is the technique of predicting the most likely authorship of anonymous text by using stylistic information hidden in texts. A. Abbasi and H. Chen (2008) [4] introduced the use of stylometric analysis techniques to help identify individuals based on writing style. Stylometric analysis techniques have been used for analyzing and attributing authorship of literary texts for numerous years. Three important characteristics of stylometry are the analysis tasks, writing-style features used, and the techniques incorporated to analyze these features. In similar way A. Narayanan *et al*. 2012 [5] also studied the investigation into the possibility that stylometry techniques might pose a wide-spread privacy risk by identifying authors of anonymously published content based on nothing but their style of expression. Previous work has applied similar techniques to distinguish among up to 300 authors. The linguistic stylometry was used for identified an anonymous author i.e., compared the writing style against the corpus of texts of known authorship. They experimentally demonstrate the effectiveness of the techniques with as many as 100,000 candidate authors. An e-mail analysis framework to extract different writing styles from a collection of anonymous e-mails was introduced by the H. Binsalleeh *et al.* (2010) [6]. This proposed method first clusters the given anonymous e-mail based on the stylometric features and then extract unique writing styles from each cluster. The writing styles in term of feature patterns provide more concrete evidence than producing some statistical numbers. This proposed method was useful in the initial stage of investigation, in which the investigator usually have very little information of the case and the true authors of suspicious e-mail collection. Then onwards in 2000, O. De Vel [7] introduced an investigation into e-mail content mining for author identification, or authorship attribution, for the purpose of forensic investigation. Significant work has been done in 2000, O. De Vel *et al*. [8] [9] investigated the learning of authorship categories for the case of both aggregated and multi-topic e-mail documents. They used an extended set of predominantly content free e-mail document features like linguistic pattern and structural characteristics. The classification models employed in previous contributions on authorship attribution have two broad categories: Decision tree and Support Vector Machine (SVM) (Cristianini and Shawe-Taylor 2000) [10]. While building a decision tree, a decision node was constructed by simply considering the local information of one attribute. Therefore, it fails to capture the combine effect of several features. In contrast, SVM avoids such problem by considering all features when a hyper plane is created. However, SVM is like a black-box function which takes some input and provides an output. Consequently, from this background analysis, it can be inferred that different researchers have introduced different classification techniques to detect the writeprint or authorship attribution.

III. Implementation

The work is performed in five steps namely; extracting the data, Pre-processing, Feature Extraction, Classifier and Evaluation. Extraction involves the use of R package named tool which helps to get the data from the Social Networking Website Twitter, Pre-processing is the method which is to be performed on the data provided so that the complexity can be reduced. After this Feature Extraction is performed and for this certain parameters has been set and according to those parameters whole data gets checked. Later, classifiers are applied and then evaluation is performed.

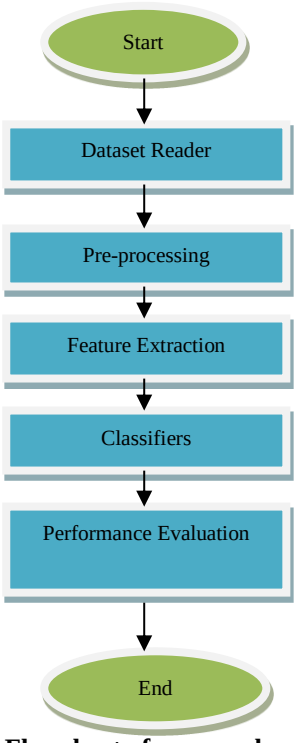
A) Extracting the data

This is the very first step of performing the detection of user identity. As, it has already been said that for identity detection there is a requirement of some input data. The data from the Twitter can be downloaded with the help of a tool which is called as R package tool. R based Twitter client provides an interface to the Twitter web API. R is a free software environment for statistical computing and graphics. It runs on windows, Linux and Mac OS.

B) Pre-processing

The pre-processing of the data is performed and this is done with the help of the Stop Word Removal Technique. Stop word is referred to as the removal of the common and unnecessary words before or after processing of the

natural language data (text). Most commonly used stop words are *the*, *is*, *at*, *which* and *on*. The stop word removal process is followed by Steaming. These both processes are included in the pre-processing section.



Flowchart of proposed work

C) Feature Extraction

This is referred to as the process of extracting out the features which are redundant in the provided input to the algorithm. When the input given to the algorithm is too large for the processing then some of the features get reduced. This process is called Feature Extraction. In this work , the set maintained is combination of four features and that is, total number of words in a line (word count), no. of URL (url) , no. of URL present per word count (URL/word count), Retweets (rt).

For example: Input: *RT @BBCJamesCook: Rangers investigate Mohammed tweet: http://t.co/hLyC1BGeli #Rangers*

D) Classifiers

KNN classification is used which is basically a non-parametric method and used for classification and regression. It depends on the output of the system whether KNN is used for the classification or for regression.

The K-Nearest Neighbor algorithm is amongst the simplest of all machine learning algorithms: an object is classified by a majority vote of its neighbors, with the object being assigned to the class most common amongst its *k* nearest neighbors (*k* is a positive integer, typically small).

Support Vector Machines (SVM) is supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis.

The process of constructing lexical ontology by analyzing unstructured text is termed as ontology refinement by decision tree. Different algorithms of decision tree are used for classification in many application areas, like financial analysis, astronomy, molecular biology, and text mining.

E) Evaluation

On the basis of the process performed above, Accuracy, Time Complexity, F-measure, Recall, G-mean, Precision are evaluated and then the corresponding graphs get generated.

Classifiers	Accuracy	Recall	Precision	Fmeasure	Time Complexity
SVM	0.64	0.7469	0.7262	0.7302	0.0231
Decision Tree	0.648	0.785	0.7034	0.7394	0.005
KNN	0.808	0.8472	0.8588	0.8512	0.005

Table 1: Results on the basis of Trained Data

Entire work is performed in MATLAB which is abbreviated as Matrix Laboratory, it is used to perform the data visualization, data analysis and it is a very high-level interactive programming language. Different classifiers are implemented in MATLAB for analyze the Accuracy, Precision, Recall, and Time Complexity. For performing this work, a dataset of 150 records has been maintained and those records are basically the tweets, which are downloaded from Twitter using the R package tool [11].

a) Accuracy:

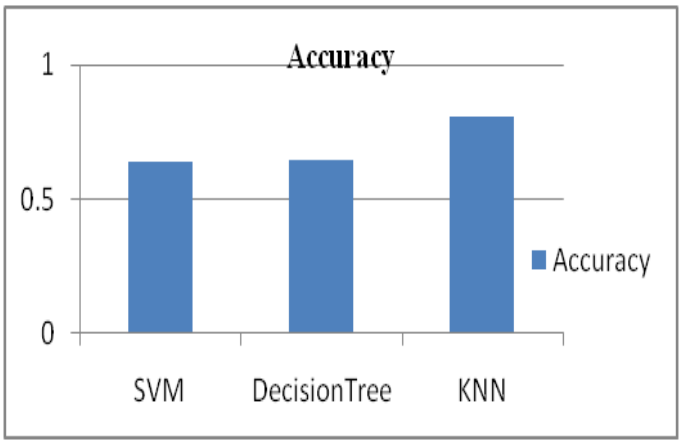


Figure 1 Accuracy of Different Classifiers

b) Recall:

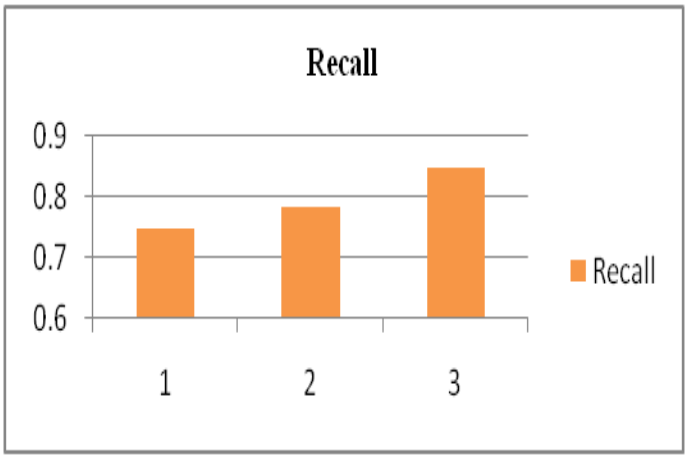


Figure 2 Recall of Different Classifiers

c) Precision:

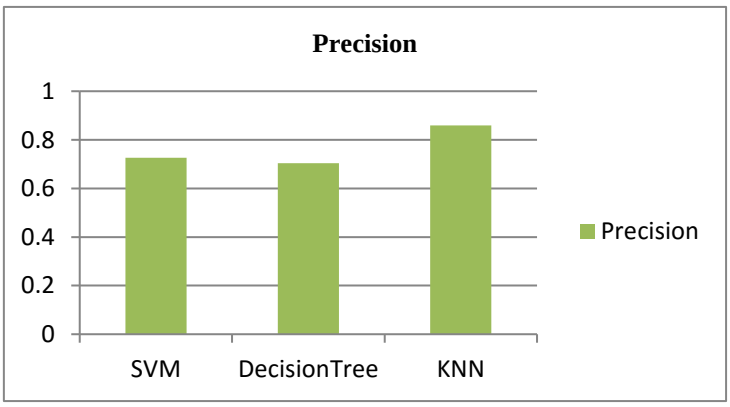


Figure 3 Precision

d) Time Complexity:

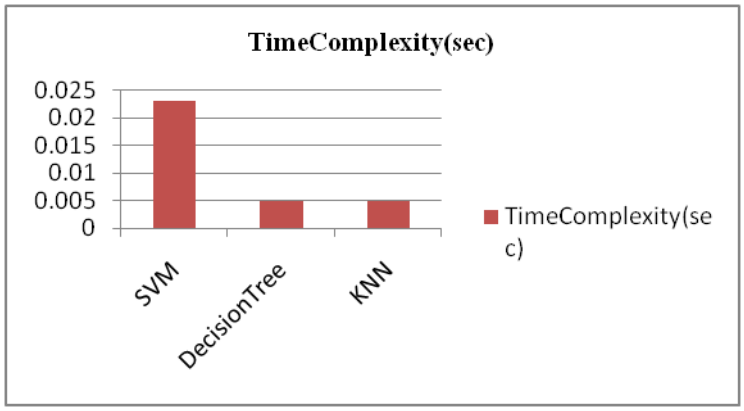


Figure 4 Time Complexity of Different Classifiers

IV. Conclusion

This research presented different classifiers techniques that are used to identify the user identity whether it is fake or genuine. Different classification techniques are used to optimize the accuracy, precision, time complexity, and recall for a given input. On the basis of graphs obtained, it can be concluded that the KNN classifier is giving best results as compared to other two classifiers.

References

[1] J. Li, R. Zheng, and H. Chen, "From fingerprint to writeprint", Communications of the ACM (2006); 49(4): pp.76-82.

[2] Teng G-F, Lai M-S, Ma J-B, Li Y, "E-mail authorship mining based on SVM for computer forensic", In: Proceedings of the third international conference on machine learning and cyhemetics, Shanghai, China; August 2004.

[3] Zheng. R, Li. J, Chen H, Huang Z, "A framework for authorship identification of online messages: writing-style features and classification techniques", Journal of the American Society for Information Science and Technology, February 2006; 57(3): pp.378-393.

[4] Abbasi A, Chen H, "Writeprints: a stylometric approach to identify level identification and similarity detection in cyberspace", ACM Transactions on Information Systems, March 2008; 26(2): pp.1-29.

[5] A. Narayanan, H.S. Paskov, N.Z. Gong, J. Bethencourt, E.C.R. Shine, E. Stefanov, D. Song, "On the feasibility of internet-scale author identification", In: Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P), California, USA, 2012.

[6] F. Iqbal, H. Binsalleeh, B.C.M. Fung, and M. Debbabi, "Mining writeprint from anonymous e-mails for forensic investigation", Digital Investigation, October 2010; 7: pp.56-64.

[7] De Vel O, Mining e-mail authorship", Workshop on text mining, ACM international conference on knowledge discovery and data mining (KDD), 2000

[8] De Vel O, Anderson A, Mohey G, Corney M, " Mining e-mail content for author identification forensics", SIGMOD, 2001a; 30(4): pp.55-64.

[9] De Vel O, Anderson A, Mohey G, Corney M, "Multi-topic e-mail authorship attribution forensic", ACM conference on computer security- Workshop on data mining for security applications, November 2001b.

[10] Cristianini N, Shawe-Taylor J, "An introduction to support Vector Machine", UK Cambridge University Press; 2000

[11] Satinder, Sanjeev Dhawan, Kulvinder Singh, "Detection of User Identity in Social Networks", Advances in Computer Science and Information Technology (ACSIT), 2016, pp. 319-321.