Authorship Acknowledgement For Social Media Forensics

P. Saranya.[1], B. Shanthi[2], Mr.S.Praveen kumar M.E., (Ph.D)[3], Mr.G.Arulselvan M.E[4]
[1, 2]Dept of CSE
[3, 4]Assistant Professor, Dept of CSE
[1, 2, 3, 4] E.G.S. Pillay Engineering College, Nagapattinam,Tamil Nadu,India

Abstract- *The veil of anonymity provided by smartphones with pre-paid SIM cards, public Wi-Fi hotspots, and distributed networks like Tor has drastically complicated the task of identifying users of social media during forensic investigations. In some cases, the text of a single posted message will be the only clue to an author's identity. How can we accurately predict who that author might be when the message may never exceed 140 characters on a service like Twitter? For the past 50 years linguists, computer scientists and scholars of the humanities have been jointly developing automated methods to identify authors based on the style of their writing. All authors possess peculiarities of habit that influence the form and content of their written works. These characteristics can often be quantified and measured using machine learning algorithms. In this article, we provide a comprehensive review of the methods of authorship attribution that can be applied to the problem of social media forensics. Further, we examine emerging supervised learningbased methods that are effective for small sample sizes, and provide step-by-step explanations for several scalable approaches as instructional case studies for newcomers to the field. We argue that there is a significant need in forensics for new authorship attribution algorithms that can exploit context, can process multimodal data, and are tolerant to incomplete knowledge of the space of all possible authors at training time.*

Keywords- Authorship attribution, computational linguistics, forensics, machine learning, Social media

I. INTRODUCTION

It is wellknown that the real lives of internet users sometimes turn out to be entirely different from who they appear to be online, but the nature and consequence of this phenomenon are changing.A recent expos´e in the New York Times Magazine documented the case of a Russian media agency that allegedly executed organized disinformation campaigns on social media using pseudonyms and virtual identities. It is assumed that some of these campaigns were state sponsored. With an office full of media professionals, the agency achieved success in promoting false news events and influencing public opinion on politics, and was even able to deceive the journalist covering the story for the Times.NLP (Neuro-linguistic Programming) is the most powerful approach I've found for communications, change, and excellent performance.

Authorship attribution has been crucial in identifying authors of texts and has been very successful for literary and conventional writings. Specially, stylometric features have been extensively used for long time. This line of research is called stylometry and it consists of the analysis of linguistic styles and writing characteristics of the authors for identification, characterization, or verification purposes. It is based on the fact that the writing style is an unconscious habit and furthermore it varies from one author to another in the way he/she uses words and grammar to express an idea. Stylometry is therefore the study of the unique linguistic styles and writing behaviors of individuals in order to determine authorship. A person's writing pattern contains many features that reveal an individual uniqueness and identity.

Social networking sites are an important communication medium. Just like emails and instant messaging, social networking sites are excellent place for companies, businesses and governments to interact with the public and their customers. These social networking sites become an important communication medium for many organisations and people. Currently there are many criminal cases that are related to social networking sites or the use of social networking sites in order to commit crime. Chua (2009) stated that "The distribution of malware on social networking sites first occurred in small amounts towards the end of 2007, but that trend appears to be on the rise". Further to this, he predicted that this trend is expected to increase every month and is only going to continue. For example, Facebook is only going to be used more and Web 2.0 based websites, such as blogs and wikis, will only become more important in any cases in the digital forensics area With the popularity of social media, many people are willingly publicising where they live, their religion, their medical status, their friends, personal email addresses, phone numbers, photos of themselves and status updates, which informs people where they are and what they doing. Criminals can use these social networking sites to commit crimes. For example, a terrorist group may use a social networking site such as Google Plus (location-based social networking website) to identify popular locations for bombing, while drug dealers can use social networking sites in order to communicate with other dealers or their customers. Digital Forensics has been developed in recent years and it has been widely used for computer crime investigation and tested in a court of law. Social network forensics can learn much from this process, as social network forensics is part of digital forensics, which deals with digital evidence gathered from social networking sites. In any digital forensic cases, investigators must follow the process that ensure the evidence is legally acceptable, and present all digital evidence in a forensically sound manner.

II. LITERATURE SURVEY

This paper [15] tells majorly figures out the security issues that happens in the social media. The main aim of the paper is to track the pattern of the author ,how the author used to post the messages when he enters the websites. On tracking the pattern of the user we will be able to identify the rumour messages that are posted by unknown authors. We can track this by first preprocessing the messages that are posted by the various users in the social media. We can do this by sentiment analysis of tweets. Based on this analysis we have to classify the messages as good and bad. By this classification process we can easilly detect the bad messages that are posted in the social media. By identifying this we can find the wrong messages that are posted by unknown authors. The verification process is carried out ,in this we have to compare the messages with the author pattern. Finally if we found any rumour messages we have to identify the author of the message and therby we have to block the particular author and stop him by further sending messages.

III. ARCHITECTURE DIAGRAM

The architecture diagram concept based on Internet query top news and topics of the database of news articles and twitter of preprocessing interaction and team terms extraction used by preprocessing .The user use news topics of ranked news topics of content selection and ranking used by social graph construction .The node weighting used by (UA) User Attention estimation (UI) User Interaction estimation are used media focus estimation used by content selection and ranking. The key term graph clustering term frequency relevant term Identification of term similarity used . The graph clustering Between ness transitivity used.

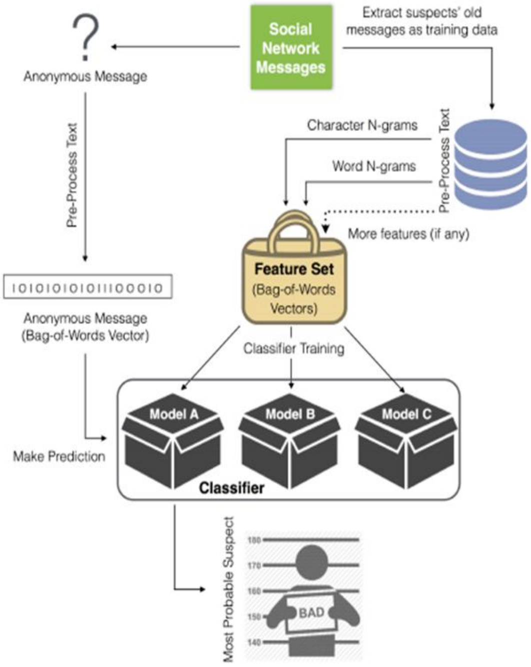

Figure 3.1 Architecture diagram

IV. MODULES

4.1.Author User Registration :

In every social media for the purpose of identification there is always an option for the user to register themselves in the application. The authors register as users in the system before posting messages .

4.2.. Post The Tweet:

In this project we are focusing on the twitter media. Hence every user in the media who has registered is eligible to tweet messages in the application.

4.3. Sentiment Analysis Of Tweets.:

The tweets that are posted by various users are fetched. The messages preprocessed inorder to is a good message or bad message or whether it is a rumour

4.4. Verification:

The test data message is input ,this input is preprocessed and then sent and then the message is identified whether it is good or bad. Then the messages are classified as good or bad.

4.5. Result-Block Rumor

Based on the classification of messages into good or bad the user who has sent the message is also identified he is classified as good/bad.If the user is found to be bad a warning message is sent to the particular user and that user is blocked and stopped and he cannot transfer messages anymore.

V. CONCLUSION

The project thus makes the user to be registered before ploading or posting any message. The pattern of the author is watched accordingly whenever he enters into the website and attempts for a search or post any messages. The words or messages that are posted by the user is extracted by using lexical anaysis and the exact meaning of the word is found and fetched. If that word is found to be the bag of words then that particular user is warned and he cannot post further messages in the website. This kind of processing the messages will be helpful in finding the bad users or the users spreading the messages unwantedly. Since the particular user is been blocked and stopped from being sending the messages the rumours can be easily stopped

REFERENCES

[1] A. Abbasi and H. Chen. Writeprints: A stylometric approach to identity-level identification and similarity detection in cyberspace. ACM Transactions on Information Systems, 26(2):7, 2008.

[2] H. Baayen, H. van Halteren, A. Neijt, and F. Tweedie. An experiment in authorship attribution. In Journal of Textual Data Statistical Analysis, pages 29–37. Citeseer, 2002.

[3] H. Baayen, H. Van Halteren, and F. Tweedie. Outside the cave of shadows: Using syntactic annotation to enhance authorship attribution. Literary and Linguistic Computing, 11(3):121–132, 1996.

[4] J. N. G. Binongo. Who wrote the 15th book of Oz? an application of multivariate analysis to authorship attribution. Chance, 16(2):9–17, 2003

[5] M. L. Brocardo, I. Traore, S. Saad, and I. Woungang. Authorship verification for short messages using stylometry. In Intl. Conference on Computer, Information and Telecommunication Systems, pages 1–6, 2013.

[6] M. Koppel, J. Schler, and S. Argamon. Authorship attribution in the wild. Language Resources and Evaluation, 45(1):83–94, 2011.

[7] M. Koppel and Y. Winter. Determining if two documents are written by the same author. Journal of the Association for Information Science and Technology , 65(1):178–187, 2014.

[8] R. Layton, P. Watters, and R. Dazeley. Authorship attribution for Twitter in 140 characters or less. In Cybercrime and Trustworthy Computing Workshop, pages 1–8, 2010.

[9] T. Qian, B. Liu, L. Chen, and Z. Peng. Tri-training for authorship attribution with limited training data. In Annual Meeting of the Association for Computational Linguistics, pages 345–351, 2014.

[10] R. Schwartz, O. Tsur, A. Rappoport, and M. Koppel. Authorship attribution of micro-messages. In Conference on Empirical Methods on Natural Language Processing, pages 1880–1891. ACL, 2013..

[11] Spirit. Guess Language: Guess the natural language of a text 2014. Accessed on July 1, 2015 via https://bitbucket.org/spirit/guess_language.