Proceedings of 2017 Tenth International Conference on Contemporary Computing (IC3), 10-12 August 2017, Noida, India

Resolving Identities on FaceBook and Twitter

Suyash Somani
Jaypee Institute of Information Technology
Noida, India
suyash.somani@gmail.com

Somya Jain
Jaypee Institute of Information Technology
Noida, India
somya.jain@jiit.ac.in

***Abstract*— In the current time zone, the utilization of online web-based social networking systems has developed exponentially with clients investing the vast majority of the energy of their life associating with the world by means of web-based social networking. Systems like Twitter, Facebook, Instagram, LinkedIn and so forth are the most acclaimed ones with greatest number of clients over the world.**

The un-linking of the systems enables clients to contaminate the web-based social networking by undesirable materials and still stay mysterious. With the utilization of a worldwide identifier, it will be anything but difficult to inquiry them. In the writing proposed, personality determination has been broken into 2 sections i.e. Identity Search and identity matching with various traits mulled over. Properties like Username, Profile picture, Content of the posts and specified URLs are contemplated and a group of these gave enhanced outcomes.

Keywords— Identity Resolution, Profile Matching, Content Matching, Edit Distance, Cosine Similarity, SSIM Model, Fake Users, Spammer.

I. INTRODUCTION

On every interpersonal organization, client makes its own particular one of a kind personality that separate it from others which incorporates username, picture, likes despises and so forth. In all such cases false hood is the issue. By characterizing another personality on various online networking systems, its numerous characteristics remain unlinked with each other [2]. Answers for the issue have various application spaces. In security space, our answer can help scanning for pernicious client's numerous online personalities. Malevolent clients abuse online web-based social networking for exercises, for example, Phishing, Spam, Identity robbery, and so forth. Such malignant clients make various records on various systems administration destinations to upgrade reachability to targets (casualties). To recognize vindictive clients, security specialists have formulated elements on Twitter, YouTube, MySpace and other informal organizations. Arrangements proposed to distinguish pernicious client records are organize subordinate, subsequently security experts need to recognize malignant records on each systems administration site. Connecting noxious client personality displayed on various online interpersonal organizations is proposed. However in true, vindictive clients exhibit dynamic confusion of their scribes to maintain a strategic distance from identification and linkage of their various personalities. To address this test, conduct based personality determination can help in authoritative and connecting malignant client's personalities crosswise over informal communities. In the protection space, issues and its application in understanding the amount and nature of the client's data spillages is difficult. Here and there, in light of a portion of the diverse qualities, it is hard to discover them and match them together. In this venture, focus is on this issue by utilizing diverse calculations. An attempt is made to distinguish a solitary client over different web-based social networking stage with the dataset of Facebook and Twitter.

II. DEFINITIONS

A. Identity

A character of a client on an online social network (OSN) is made out of three measurements of properties namely profile, content and network. Profile is made out of set of traits which portrays her persona, for example, username, name, age and area. Substance is what he/she makes or is imparted to her for example content and time of post. Network is made out of association qualities which depict the system; she creates to associate with different clients, for example, number of companions [3,4]. A certifiable client is meant by I and her personality on a social network arrange (SNA) is meant by IA.

B. Identity Resolution

For non-exclusive methodology given a character IA of client I on informal community SNA and her right personality IB on different social arrange SNB [4]. The procedure of personality resolution in online informal communities takes after two sub processes such as character pursuit and personality coordinating. Character process records an arrangement of hopeful characters on SNB, which are like given character IA and conceivably have a place with client IB. Personality coordinating procedure then ascertains the comparability score amongst IA and each applicant character returned by personality look handle on specific measurements. Applicant identities are then positioned on the premise of likeness score, and the hopeful character with most astounding match-score is returned as IBs.

III. METHODOLOGY

The identity search methods which were used to search for a user’s candidate identities on Facebook are profile search, and content search.

978-1-5386-3077-8/17/$31.00 ©2017 IEEE

C. Profile Search

For profile matching, edit distance is calculated between two strings. Now, if the edit distance is coming to be less than or equal to 0.3, then assign the Score as 1 which means that there are high chances that they are of same profile and if the edit distance is coming out as greater than 0.3 then assign the Score as 0.5 which further means that there are still chances that it will match with someone's profile. Score is represented as S1.

D. Content Search

To connect with various systems together, a client is encouraged with a decision to push a similar substance on numerous systems all the while. Content search strategy utilizes content as a parameter for clients. For instance, Twitter gives a usefulness to interface Twitter and Facebook character to post client's tweets on her Facebook course of events. Twitter feed enables a client to associate Twitter, Facebook, and LinkedIn to push bolsters in three informal organizations all the while. In view of such administrations, it is likely that a client creates same substance on different interpersonal organizations. Such a client conduct can be uncovered by Twitter API which gives the "source" of a tweet i.e. from where the tweet is posted e.g. Facebook, Twitter channel, and so on. This conduct of specifying one's Facebook organize personality on Twitter expressly is termed as "Self-Identification". Two assortments of self-ID conduct are seen to be here, one in which a client straightforwardly gives her Facebook character on her URL quality and other in which a client in a round way gives her Facebook personality by means of alluding to a page on her URL property.

IV. EXPERIMENTS AND ANALYSIS

This section illustrates the control flow diagram and model used for the analysis. Figure 1 demonstrates all the steps involved in identity resolution algorithm.

E. Edit Distance

It is characterized to be the most modest number of alter operations (inclusions, erasure and substitutions) required to change one string into another. In its essential frame, each alter has taken a toll 1. Utilizing dynamic programming, separation between two strings ST1 and ST2 can be figured in time O(|ST1|x|ST2|) and O(min(|S1T|,|ST2|)) space. Distance between ST1 and ST2 is given as dist(ST1,ST2) = 1.0 - (dist(ST1,ST2)/max(|S1|,|S2|)). The Edit separation is symmetric and it generally holds that 0 <= dist (ST1, ST2) <= max(|ST1|, |ST2|) and abs(|ST1|-|ST2|) <= dist(ST1,ST2).

After all calculations, we have assigned S1 score mentioned above for this matching. Each acceptable record has been taken into account for further calculations i.e. the corresponding matches have been recorded.

F. SSIM (Structural Similarity)Model

There are numerous models available to match the images. Some are Peak Signal-to-noise ratio, mean squared error (MSE) and SSIM model. We used SSIM model for measuring the image similarity and then assign them appropriate scores. Score S2 is assigned for each matching. Here, Score means that by how much similarity the two images got matched. If nothing is matched, S2=0.5.

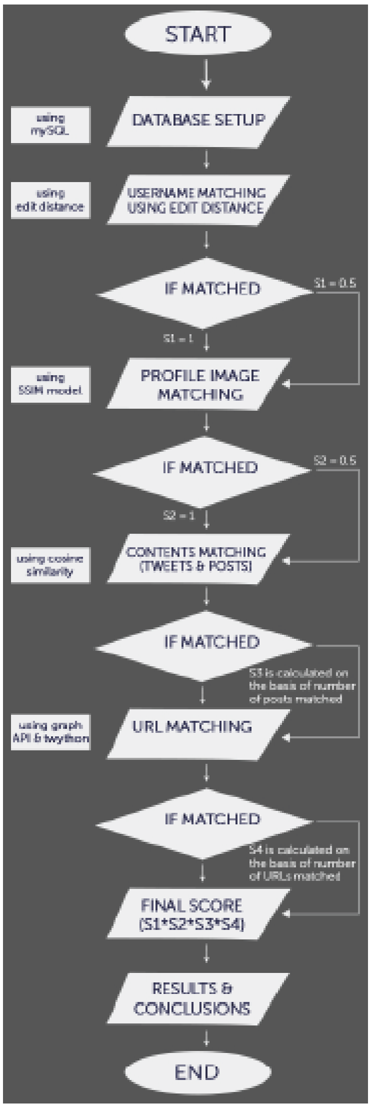
START
using mySQL
DATABASE SETUP
using edit distance
USERNAME MATCHING USING EDIT DISTANCE
IF MATCHED
S1 = 0.5
S1 = 1
using SSIM model
PROFILE IMAGE MATCHING
IF MATCHED
S2 = 0.5
S2 = 1
using cosine similarity
CONTENTS MATCHING (TWEETS & POSTS)
IF MATCHED
S3 is calculated on the basis of number of posts matched
using graph API & twython
URL MATCHING
IF MATCHED
S4 is calculated on the basis of number of URLs matched
FINAL SCORE (S1*S2*S3*S4)
RESULTS & CONCLUSIONS
END

Fig.1. Algorithm for resolving identities

G. Cosine Similarity

Previously, we were using Knuth-Morris-Pratt (KMP) algorithm for the matching of content but now Cosine Similarity method was adopted due to fact of different users writing skills and its time complexity. First of all, database with tweets and posts from different users is created. The tweets have been collected using Twitter API which extracts username and tweets (approx. 20 per user) from Twitter ID and similarly posts from a particular Facebook ID which were stored in MySql database. After the data connection has been established, input data is stemmed using Porter Stemmer. Stemmer reduces the inflectional forms of the related words to common forms. Then, the tokenization of the tweets was done. The list of tokens is then passed as input for further text mining. For this, first of all, all the words have been converted into ASCII form and the words which are not convertible are replaced by "?". After that, we vectorize all the tweets by multiplying the tokens of that tweet by their corresponding tf-idf weights. Then we use, Gensim's Word2Vec model for calculating the vector values of the tweets and then train our model for final calculations of Cosine similarity.

Now, if the value of cosine similarity comes out to be > 0.5 then we have taken this post as a matched post. We have kept the record of cumulative cosine score for any particular user. Ratio of number of post matched to the number of total posts of that user is found out. Score for matched identity assigned as S3 which is cumulative value of Cosine Similarity. If nothing is matched, S3=0.5

H. URL Matching

URL matching is to look for the users who have mentioned the links of cross platforms posts/tweets and tried to find out if there is any user who has mentioned his/her posts/link into another social media platform. This matching is given a Score S4. If nothing is matched, S4=0.8.

Assign each one of the matching a score and if a user's name match with another user's name and none of the other attributes matches use other scores as 1. After all the results, product of all the scores are taken i.e. Final Score (F) = (S1*S2*S3*S4). Specific values chosen for these scores were random as they cannot be zero. Table 1 shows all the test cases labeled i.e. rejected/accepted/ cannot be determined (CBD) with respect to final score. Manual check has been done for each test case.

TABLE I. TEST CASES

Final Score (F)	< 0.9	1 < F < 1.5	> 1.5
Labeled Class	Rejected	CBD	Accepted

V. FINDINGS

By implementing the algorithm discussed in the previous section successfully, we matched the profiles of some users on the social media networks. Table II shows the result of some matched profiles. Table III shows the results of number of test cases passed/failed/accepted/rejected/CBD. Accuracy comes out to be 0.7. Apart from these, we are also able to identify those accounts which could be or could not be fake. Table IV shows some of the fake accounts found against twitter handler which represents impersonation.

TABLE II. USER NAME ALIAS

Twitter Id	@Shashitharoor	@iamsrk	@AnupamPkher	@Billgates
Twitter Username	Shashi Tharoor	Shah Rukh Khan	Anupam Kher	Bill Gates
Facebook Username	Shashi Tharoor	Shah Rukh Khan	Anupam Kher	Bill Gates

TABLE III. RESULTS OF TEST CASES

No. of Test Cases	4	11	5	14	6
Labeled Class	Accepted	Rejected	CBD	Passed	Failed

TABLE IV. FAKE ACCOUNT

Twitter Handle	@narendramcdi	@UrvashiRutela
Fake Accounts Found	Narendra Modi	Urvashi Rautela

VI. CONCLUSION

This work enables to identify users across online social networks but not with 100% accuracy for some reasons. First and foremost reason is the less availability of the content and number of matched post. Although the user is same on both the accounts but because of less matched content, the program could not identify if it's the same person. Secondly, some accounts were there which could be termed as fake accounts of the real users but we cannot be 100% sure because they show different results in both the matching. Thirdly, in some cases only names were matched or nothing matched with any of the users of the other platform. Those kinds of cases have to be labeled as CBD because it is the main limitation of the work which has been mentioned earlier. Lastly, the 4 accounts which have been successfully identified are those which have username and a considerable amount of same posts across both of the social networks.

REFERENCES

[1] E. Raad, R. Chbeir and A. Dipanda, "User Profile Matching in Social Networks", 10 Proceedings of the 13th International Conference on Network-Based Information Systems (NBIS), 2010.

[2] S. Bartunov, A. Korshunov, S.T. Park, W. Ryu and H. Lee, "Joint Link-Attribute User Identity Resolution in Online Social Networks", 6th SNA-KDD Workshop '12 (SNA-KDD'12) Beijing, China.

[3] T. Iofciu, P. Fankhauser, F. Abel and K. Bischoff, "Identifying Users Across Social Tagging Systems", proceedings of the Fifth International Conference on Weblogs and Social Media, Barcelona, Catalonia, Spain.

[4] P. Jain ,"Automated Methods for Identity Resolution across Online Social Networks" HT 15 Proceedings of the 26th ACM Conference on Hypertext & Social Media.

[5] A. Malhotra, L. Totti, W. Meira, P. Kumaraguru, and V. Almeida, "Studying User Footprints in Different Online Social Networks", International workshop on cybersecurity of online social network(CSOSN).

[6] M. Ozuysal, M. Calonder, V. Lepetit, "Fast Keypoint Recognition Using Random Ferns", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 32, Issue 3, March 2010.

[7] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, and M. Goncalves, "Detecting spammers and content promoters in online video social networks", proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval, ser. SIGIR, 2009.

[8] I. Sutskever, K. Chen, G. Corrado, J. Dean," Distributed Representations of Words and Phrases and their Compositionality", Proceedings of the 26th International Conference on Neural Information Processing Systems, December 2013.

[9] Q. Luo, W. Xu, J. Guo, "A Study on the CBOW Model's Over fitting and Stability Web-Kr'14", Proceedings of the 5th International Workshop on Wescle Knowledge Representation Retrieva:l & Reasoning, Shanghai, China, pp.9-12.

[10] Tomas Mikolov, Anoop Deoras, Daniel Povey, Lukas Burget and Jan Cernocky., "Strategies for Training Large Scale Neural Network Language Models", In Proc. *Automatic Speech Recognition and Understanding*, 2011.