International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

# RECOGNIZING USER PORTRAIT FOR FRAUDULENT IDENTIFICATION ON ONLINE SOCIAL NETWORKS

**T.KALAICHELVI[1], S BASKARAN[2], P KRISHNAMOORTHY[3], A MOHAMMED ANSARI[4]**

*[1-4]Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai.*

---

***Abstract-*** *Conceptual On-line Social Networks (OSNs) are progressively affecting the manner in which individuals speak with one another and share individual, proficient and political data. Notable locales, for example, Facebook, LinkedIn, Twitter, and Google+ have a huge number of clients over the globe. With the wide prevalence there are part of security and protection dangers to the clients of Online Social Networks (OSN, for example, break of security, viral advertising, auxiliary assaults, malware assaults and Profile Cloning. Informal organizations have allowed individuals have their own virtual characters which they use to communicate with other online clients. It is likewise totally conceivable and normal for a client to have more than one online profile or even a totally unique unknown online personality. Some of the time it is expected to expose the secrecy of specific profiles, or to distinguish two distinction profiles as having a place with a similar client. Element Resolution (ER) is the assignment of coordinating two diverse online profiles conceivably from interpersonal organizations. Comprehending ER has a recognizable proof of phony profiles. Our answer looks at profiles based comparative credits. The framework was entrusted with coordinating two profiles that were in a pool of incredibly comparable profiles*

## I. INTRODUCTION

The Web Application centers around to give a Graphical User Interface that takes after the Social Media Prototype for the User and enter the OSN website where they can get to their profiles and perform Social Surfing. The User can get to their profiles once they are associated with a steady web association. The client should be Authenticate themselves by giving their User Id and Password alongside the OTP send to their Mail. A substantial Mail Id must be given to verification during Registration, and a Stable Network association must be set up for appropriate Functioning. The client can transfer their profile qualifications and Profile photograph simply after Successful Login into the Account. The Images which are transferred by the User are implanted with client Id by steganography and are get put away in the Database. At the Server side, the Database Interaction is important to give the viable handling by putting away and getting to the information by the Admin, so as to store the client qualifications and furthermore their Activity logs which can be gotten to by Admin at whenever. In this way if the current media is utilized by another record, the installed information can be coordinated appropriately. Profile Cloning is an endeavor to Create or utilize a Profile with existing media Files. Such Activities might be endeavored by the Fake clients. Through Image Processing, such exercises can be recognized quickly and the Existing client can be found by Profile Matching. With the assistance of information Embedded in the media, an admonition message is sent to the current client, until it confines the Activities of the new client.. Impeding Fake Profiles If the User Unauthorized the Activity, Immediately the New Account will be Blocked and Terminated. Or disaster will be imminent on the off chance that it is Authorized, at that point the new User can Upload the picture with another Entry in Database. Steganography is the act of hiding a document, message, picture, or video inside another record, message, picture, or video. The main recorded utilization of the term was in 1499 by Johannes Trithemius in his Steganographia, a composition on cryptography and steganography, camouflaged as a book on enchantment. By and large, the concealed messages seem, by all accounts, to be (or to be important for) something different: pictures, articles, shopping records, or some other spread content. For instance, the concealed message might be in imperceptible ink between the noticeable lines of a private letter.

## II. RELATED WORK

The User interacts with the Web Application Module for Online Social Media Surfing. At First the user need to register their account by providing necessary Credentials. Once after the successful registration the user can login and view their profile. The user can upload the profile picture and other images which are thereby embedded with user data and such that the media files can be secured. On the other hand the fake user try to clone existing profile by replicating the user credentials and try to upload the existing profile picture. On this situation the Profile Matching operation is performed by which the existing id can be found. A Warning Message is thereby send to the existing id in which the user can allow or block the cloned profile. Based on the user response the server can perform accordingly. The Web Application focuses on to provide a Graphical User Interface that resembles the Social Media Prototype for the User and enter the OSN site where they can access their profiles and perform Social

Surfing. The User can access their profiles once they are connected to a stable internet connection. The user need to be Authenticate themselves by providing their User Id and Password along with the OTP send to their Mail. A valid Mail Id must be provided for authentication during Registration, and a Stable Network connection must be established for proper Functioning. The user can upload their profile credentials and Profile photo only after Successful Login into the Account. The Images which are uploaded by the User are embedded with user Id by steganography and are get stored in the Database. At the Server side, the Database Interaction is necessary to provide the effective processing , by storing and accessing the data by the Admin, in order to store the user credentials and also their Activity logs which can be accessed by Admin at anytime. Thereby if the existing media is used by another account, the embedded data can be matched accordingly. Profile Cloning is an attempt to Create or use a Profile with existing media Files. Such Activities may be attempted by the Fake users. Through Image Processing, such activities can be identified immediately and the Existing user can be found by Profile Matching. With the help of data Embedded in the media, a warning message is sent to the existing user, until it restricts the Activities of the new user.. Blocking Fake Profiles If the User **U**nauthori**z**ed the Activity, Immediately the New Account will be Blocked and Terminated. Or else if it is Authori**z**ed, then the new User can Upload the image with a new Entry in Database. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

## III. EXISTING SYSTEM

As a client of an Online Social Network one ought to consistently make sure that his/her profile is protected and has not been cloned by anybody. For recognizing cloned profiles, we have planned an instrument utilizing which we can discover whether the profile of a client is cloned just as is their quality of phony profile of the client. This procedure succeeds more often than not and in some cases may not as there are numerous clients having comparative accreditations. The User's profile is investigated to look for uncommon snippets of data. This data might be explicit to a specific client. The client accreditations like name of the client, profile photograph, Education subtleties, working environment and so forth are utilized to recognize the specific client. Every informal community will give different client profiles which have comparability to the genuine profile. A correlation is made between the first profile and the looked through record and after the examination a likeness Index is determined. Profile photograph is having significant function in the process to check the cloned profile.

## IV. PROPOSED SYSTEM

The Proposed System has a planned instrument which identify a similar site profile cloning. This system likewise identifies the Fake profile in the event that it is available in the site. We propose a procedure utilizing Steganography in which we add an Id to the profile and posted pictures. The Id will be email id of the client which is added to the picture while transferring. The transferred pictures might be downloaded by counterfeit profile clients and transferred it as their own Credentials. As of now a warning alarm sends to the first clients. In the event that the first profile client gives the consent, at that point the id which transferred the image will be Authorized, else it is considered as a Fake Profile and promptly the Id will be hindered.

## V. METHODOLOGY

**User Interfaces**:

The Web Application focuses on to provide a Graphical User Interface that resembles the Social Media Prototype for the User and enter the OSN site where they can access their profiles and perform Social Surfing. The User can access their profiles once they are connected to a stable internet connection.

The user need to be Authenticate themselves by providing their User Id and Password along with the OTP send to their Mail. A valid Mail Id must be provided for authentication during Registration, and a Stable Network connection must be established for proper Functioning.

**Data Embedding:**

The user can upload their profile credentials and Profile photo only after Successful Login into the Account. The Images which are uploaded by the User are embed with user Id by steganography and are get stored in the Database.

At the Server side, the Database Interaction is necessary to provide the effective process in, by storing and accessing the data by the Admin, in order to store the user credentials and also their Activity logs which can be accessed by Admin at anytime. Thereby if the existing media is used by another account, the embedded data can be matched accordingly.

**Profile Cloning**

Profile Cloning is an attempt to Create or use a Profile with existing media Files. Such Activities may be attempted by the Fake users .Through Image Processing, such activities can be identified immediately and the Existing user can be found by Profile Matching.

With the help of data Embedded in the media, a warning message is sent to the existing user, until it restricts the Activities of the new user.. Blocking Fake Profiles If the User **U**nauthori**z**ed the Activity,

Immediately The New Account will be Blocked and Terminated .Or else if it is Authorized, then the new User can Upload the image with a new Entry in Database

**Overview of User Interface:**

The User interacts with the Web Application Module for Online Social Media Surfing. At First the user need to register their account by providing necessary Credentials. Once after the successful registration the user can login and view their profile. The user can upload the profile picture and other images which are thereby embedded with user data and such that the media files can be secured

On the other hand the fake user try to clone existing profile by replicating the user credentials and try to upload the existing profile picture. On this situation the Profile Matching operation is performed by which the existing id can be found. A Warning Message is thereby send to the existing id in which the user can allow or block the cloned profile. Based on the user response the server can perform accordingly.

## VI.CONCLUSION

This application is to provide Online Social Network Platform which accounts for various functionalities such as to reduce the profile Cloning, Fake Profile, Misuse of User's credentials in Social Media and thereby to increase the safe Social Network Surfing. Identify the cyber crime before it is implemented. No other account can't be able to create on the same user name and can't use the images which had been previously uploaded by another account. If the user tries to create fake account, notification will be send to respective user. Moreover, this prototype Secures the user and their credentials.

## VII. FUTURE ENHANCEMENT

Our Proposed System can precisely recognize counterfeit or cloned Social Media profiles, with high accuracy. As future Directions, we plan to all the more comprehensively analyze the accessible information on online Fake Id misrepresentation, looking for data noteworthy for authorization and different Countermeasures. We likewise would like to investigate the topic of how, at a nearby level, intercessions intended to caution and shield clients from con artists can abstain from framing conditions that diminish mindfulness.

## VIII.REFERENCES

1. K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and Evaluation of a Real-Time URL Spam Filtering Service," in IEEE Symposium on Security and Privacy,2015.
2. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in ACM Conference on Computer and Communications Security (CCS), 2017.
3. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting Spammers on Twitter," in Conference on Email and Anti-Spam (CEAS), 2010 Computer and Communications Security (CCS), 2016.
4. M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Detecting compromised accounts on social networks," in Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, February 2015
5. W. Magdy, Y. Elkhatib, G. Tyson, S. Joglekar, and N. Sastry. Fake it till you make it: Fishing for catfishes. arXiv preprint arXiv:1705.06530, 2017.
6. K. Morley. One million pensioners will be on 'suckers lists' by2019, 2017 Obada-Obieh, S. Chiasson, and A. Somayaji : 'Don't break my heart!': user security strategies for online dating. In Proceedings of the Usable Security Mini Conference (USEC). Internet Society, 2017.
7. J. W. Pennebaker, R. L. Boyd, K. Jordan, and K. Black-burn. The development and psychometric properties of LIWC2015. Technical report, 2015.
8. D. Ramalingam and V. Chinnaiah. Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 2017.
9. K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and Evaluation of a Real-Time URL Spam Filtering Service," in IEEE Symposium on Security and Privacy, 2015.
10. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in ACM Conference on Computer and Communications Security (CCS), 2017.
11. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting Spammers on Twitter," in Conference on Email and Anti-Spam (CEAS), 2010 Computer and Communications Security (CCS), 2016.
12. M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Detecting compromised accounts on social networks," in Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, February 2015
13. W. Magdy, Y. Elkhatib, G. Tyson, S. Joglekar, and N. Sastry. Fake it till you make it: Fishing for catfishes. arXiv preprint arXiv:1705.06530, 2017.

14. K. Morley. One million pensioners will be on 'suckers lists' by2019, 2017 Obada-Obieh, S. Chiasson, and A. Somayaji: 'Don't break my heart!': user security strategies for online dating. In Proceedings of the Usable Security Mini Conference (USEC). Internet Society, 2017.

15. J. W. Pennebaker, R. L. Boyd, K. Jordan, and K. Black-burn. The developmentand psychometric properties of LIWC2015. Technical report, 2015.

16. D. Ramalingam and V. Chinnaiah. Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 2017.