International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

RECOGNIZING USER PORTRAIT FOR FRAUDULENT IDENTIFICATION ON ONLINE APPLICATIONS

Antony Sophia[1], Mukilan[2], Guru Prasath[3]

[1]*Antony Sophia, Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering college, Chennai, India*

[2]*Mukilan, Student, Department of Computer Science and engineering, Jeppiaar SRR Engineering College, Chennai, India*

[3]*Guru Prasath, Student, Department of Computer Science and engineering, Jeppiaar SRR Engineering College, Chennai, India*

Abstract - *On-line Social Applications (OSAs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Notable locales, for example, Facebook, LinkedIn, Twitter, and Google+ have a great many clients over the globe. With the wide ubiquity there are part of security and protection dangers to the users of On-line Social Applications (OSAs) such as breach of privacy, viral marketing, structural attacks, malware attacks and Profile Cloning. Informal communities 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 mysterious online personality. Now and again it is expected to expose the namelessness of specific profiles, or to distinguish two contrast profiles as having a place with a similar client. Entity Resolution (ER) is the errand of coordinating two distinctive online profiles conceivably from interpersonal organizations. Solving ER has a identification of fake profiles. Our solution compares profiles based similar attributes. The system was tasked with matching two profiles that were in a pool of extremely similar profiles.*

Key Word: Online Social Application(OSA), Entity Resolution(ER), Fake Profile, Profile Cloning, Privacy.

1. INTRODUCTION

Social Applications have permitted people have their own virtual identities which they use to interact with other online users. Social Applications such as Facebook, Twitter and Google+ have attracted millions of users. One of the most widely used Social Applications, Facebook, recently had an initial public offering, which was among the biggest in Internet technology. These Social Applications allow real world people to create online profiles based on the information they give. The profiles are online identities that are capable of being totally independent of their real life identity. The interaction between these profiles happens through direct communication with other users, publishing posts and pictures, expressing opinions on other people's content, etc. Each profile can be seen as a node on a graph and the friendship relations between profiles are the vertices, hence the term social network. Such profiles are created during the registration process. Since the registration process for the average social network requires the user to manually enter their information it is very easy and not an uncommon occurrence to create a profile with fake or erroneous information. It could be to the interest of multiple parties to acquire the public information of these profiles from different Social Applications to correlate and match data in order to identify a single entity with different profiles. This process of matching profiles into a single entity representing one real world entity is known as Entity Resolution. ER also has real world uses such as the construction of a more detailed source of information on people, searching for people across different Social Applications, employers being able to realize their worker up-and-comers more before contracting them, improving advertising methodologies, recognizing counterfeit profiles, and so on. we present an alternative form of comparing profiles that takes advantage of other information that is available, without using training phase. To solve ER, we went farther than just comparing image based features between profiles; we also compared other types of information if it was publically available. Image based features such as the profile's images and posted images were compared with string comparison methods that obtain best results.

2. RELATED WORK

In this segment we present the literature survey of detecting fake profile in online social applications. Table 1 represent the survey overview.

AUTHOR	TITLE	DISADVANTAGES
Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis, Evangelos P. Markatos(2011)	DETECTING SOCIAL NETWORK PROFILE CLONING	It doesn't extend its functionality to utilize other popular social networks and create a profile parser for each network
Stephen Gould; Richard Fulton; Daphne Koller(2009)	DECOMPOSING A SCENE INTO GEOMETRIC AND SEMANTICALLY CONSISTENT REGIONS	It doesn't integrate the method with state-of-the-art approaches that reason more explicitly about depth or occlusion.
Olivier Duchenne ; Ivan Laptev ; Josef Sivic ; Francis Bach ; Jean Ponce(2009)	AUTOMATIC ANNOTATION OF HUMAN ACTIONS IN VIDEO	The discriminative model will need the combination of multiple subtasks for a solving complex real-world problem.

2.1. CHALLENGES IN EXISTING WORK

No prior work has fully analyzed whether these notions of romance introduce traits that could be leveraged to build a detection system. Simple categorical information relating to the user, such as age, gender, ethnicity only has been used but it wasn't provided an effective result.

The short textual self-description from the user, in which they advertise their key traits and interests are also results in failure. There is possibility of misuse of account and photos by another user. Once the account has been mistaken it is considered as cybercrime.

3. IMPLEMENTATION

The proposed system detects profile cloning in the same site. The technique uses Steganography in which an id is added to the profile pictures and posted pictures. The id will be an email id of the user which is added to the image while uploading. If another user tries to create a profile using the images from another user profile, notification will be sent to that user. No other account can't be able to create on the same user name. If the user tries to create fake account, notification will be send to respective user.

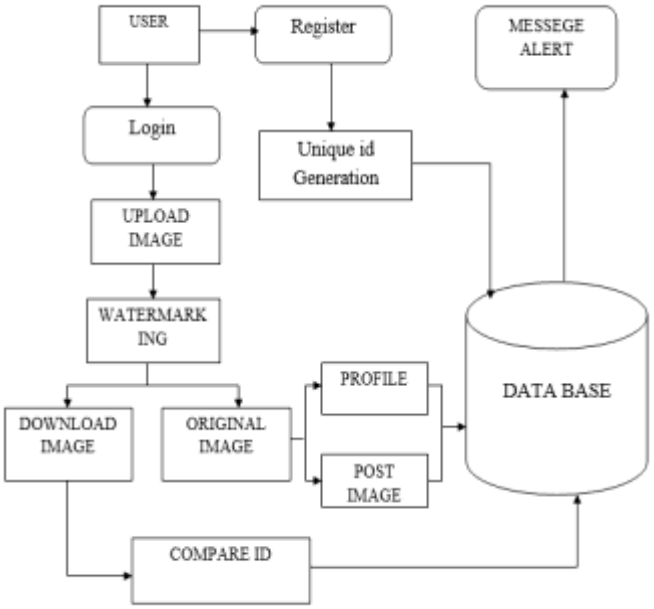

Fig -1: Architecture Diagram

The modules used in application is described as follows

3.1. CREATION AND VERIFICATION OF USER DETAILS

This module presents site visitors with a form with username and password fields. In the event that the client enters a substantial username and secret word they will be allowed access to extra assets on your site.

Fig -2: Creation Page

3.2. USING STEGANOGRAPHY TO HIDE AN ID IN THE USER'S PHOTOS

This module consists of a new stenographic algorithm for hiding data in images. Steganography is the act of concealing secret message inside any media.

Most data hiding systems take advantage of human perceptual weaknesses we have tested few images with different sizes of data to be hidden and concluded that the resulting steno images do not have any noticeable changes.

Once another user who downloads the image cannot see the image as it is hidden. We have likewise utilized water mark strategies that won't be noticeable in any event, for the clients.

Fig -3: Uploading Page

3.3 MATCHING OF UPLOADED PICTURE WITH THE DATABASE

This module checks the picture uploaded during profile creation. The user can download an image but they cannot upload the same image due to the hidden data inside each photo. When another user creates an account using the pictures from another user, it will be immediately flagged as an existing profile picture and therefore preventing the user from creating a fake profile.

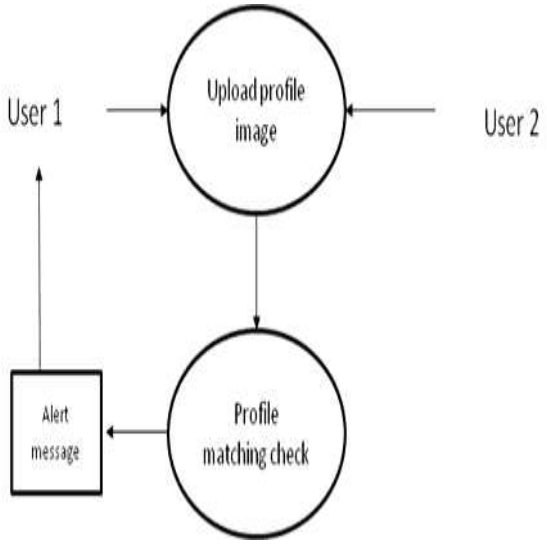

Fig -4: Data flow diagram for matching process

3.4. NOTIFYING THE ORIGINAL USER

This module informs the original user a fake profile implicating him is being created. The user can then verify whether it is him creating a duplicate profile or someone else creating fake profile of him. The original user can then prevent or allow the profile creation. A notification via a text message or mail is sent.

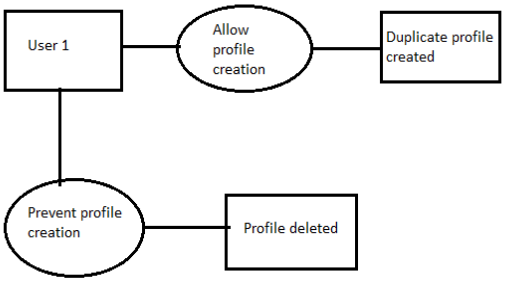

Fig -5: Notification Process

4. CONCLUSION

We solved Entity Resolution with our system and used it to compare online user profiles from social applications in order to identify cloned profiles. Our systems compare two images and identify them as fake or not. We are using Steganography Algorithm that

hides the information inside the image. In this way new images that are uploaded in our site are compare to the existing user profiles. If the image is identified as an existing image then a notification is sent to original user. The original user allows the uploading, then images was uploaded otherwise blocked.

REFERENCES

[1] J. T. Hancock, L. Curry, S. Goorha, and M. Woodworth Automated linguistic analysis of deceptive and truthful synchronous computer-mediated communication. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, page 22c. IEEE, 2005.

[2] A. Karpathy and L. Fei-Fei. Deep visual-semantic alignments for generating image descriptions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 3128–3137, 2015.

[3] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos. Detecting social network profile cloning. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*, pages 295–300. IEEE, 2011.

[4] J. Donahue, L. Anne Hendricks, S. Guadarrama, M. Rohrbach, S. Venugopalan, K. Saenko, and T. Darrell. Long-term recurrent convolutional networks for visual recognition and description. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 2625–2634, 2015

[5] R. Girshick, J. Donahue, T. Darrell, and J. Malik. Rich feature hierarchies for accurate object detection and semantic segmentation. In Proceedings of the IEEE conference on Computer Vision and Pattern Recognition, 2014.

[6] S. Gould, R. Fulton, and D. Koller. Decomposing a scene into geometric and semantically consistent regions. In Computer Vision, 2009 IEEE 12th International Conference on, pages 1–8. IEEE, 2009.

[7] S. Ji, W. Xu, M. Yang, and K. Yu, "3D convolutional neural networks for human action recognition," in IEEE Trans. Pattern Anal. Mach. Intell., 2013.

[8] Y. Wang and G. Mori, "Max-Margin Hidden Conditional Random Fields for Human Action Recognition," Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 872-879, 2009.

[9] O. Duchenne, I. Laptev, J. Sivic, F. Bach, and J. Ponce, "Automatic Annotation of Human Actions in Video," Proc. 12th IEEE Int'l Conf. Computer Vision, pp. 1491-1498, 2009.

[10] M. Ranzato, F. Huang, Y. Boureau, and Y. LeCun, "Unsupervised Learning of Invariant Feature Hierarchies with Applications to Object Recognition," Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2007.