International Journal of Engineering and Techniques - Volume 6 Issue2 March- April 2020

RECOGNIZING USER PORTRAIT FOR FRAUDULENT IDENTIFICATION ON SOCIAL NETWORKS USING BLOCKCHAIN AND WATERMARKING ALGORITHM

Kailash Nath Mandal, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
Kailash.nm05@gmail.com

Ramesh Reddy, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
rameshreddy2511@yahoo.com

Changal Rayudu, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
pasupuletichangalrayudu_srmuniv.edu.in

Deepa R, Assistant Professor, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
r.deepame@gmail.com

ABSTRACT:

On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Well known sites such as Facebook, LinkedIn, Twitter, and Google+ have millions of users across the globe. With the wide popularity there are lot of security and privacy threats to the users of Online Social Networks (OSN) such as breach of privacy, viral marketing, structural attacks, malware attacks and Profile Cloning. Social Networks have permitted people have their own virtual identities which they use to interact with other online users. It is also completely possible and not uncommon for a user to have more than one online profile or even a completely different anonymous online identity. Sometimes it is needed to unmask the anonymity of certain profiles, or to identify two difference profiles as belonging to the same user. Entity Resolution (ER) is the task of matching two different online profiles potentially from social networks. Solving ER has an identification of fake profiles. Our solution compares profiles based similar attributes and user uploaded image streak using block chain and watermarking technology. The system was tasked with matching two profiles that were in a pool of extremely similar profiles.

A. OBJECTIVE:

Our method was designed with two primary modules that work together to solve fake profiles. Dataset acquisition of profiles from social networks, the profile attributes are compared and similarities between them are discovered using a "data hiding" module through "Comparison distributor" component. The "Profile Matching" module is performed through the "Match Selector" component. This second module's purpose is to identify potential matches between the set of profiles by analyzing the previously yielded similarities between profiles.

B. LITERATURE SURVEY:

Title: DETECTING SOCIAL NETWORK PROFILE CLONING [2011].

Description: Social networking is one of the most popular Internet activities, with millions of users from around the world. The time spent on sites like Facebook or LinkedIn is constantly increasing at an impressive rate. At the same time, users populate their online profile with a plethora of information that aims at providing a complete and accurate representation of themselves. Attackers may duplicate a user's online presence in the same or across different social networks and, therefore, fool other users into forming trusting social relations with the fake profile. By abusing that implicit trust transferred from the concept of relations in the physical world, they can launch phishing attacks, harvest sensitive user information, or cause unfavorable repercussions to the legitimate profile's owner. In this paper we propose a methodology for detecting social network profile cloning. We present the architectural design and implementation details of a prototype system that can be employed by users to investigate whether they have fallen victims to such an attack. Our experimental results from the use of this prototype system prove its efficiency and also demonstrate its simplicity in terms of deployment by everyday users. Finally, we present

the findings from a short study in terms of profile information exposed by social network users.

Title: DEEP VISUAL SEMANTIC ALIGNMENTS FOR GENERATING IMAGE DESCRIPTIONS [2015].

Description: We present a model that generates natural language descriptions of images and their regions. Our approach leverages datasets of images and their sentence descriptions to learn about the inter-modal correspondences between language and visual data. Our alignment model is based on a novel combination of Convolutional Neural Networks over image regions, bidirectional Recurrent Neural Networks (RNN) over sentences, and a structured objective that aligns the two modalities through a multimodal embedding. We then describe a Multimodal Recurrent Neural Network architecture that uses the inferred alignments to learn to generate novel descriptions of image regions. We demonstrate that our alignment model produces state of the art results in retrieval experiments on Flickr8K, Flickr30K and MSCOCO datasets. We then show that the generated descriptions outperform retrieval baselines on both full images and on a new dataset of region-level annotations. Finally, we conduct large-scale analysis of our RNN language model on the Visual Genome dataset of 4.1 million captions and highlight the differences between image and region-level caption statistics.

Title: AUTOMATICALLY DISMANTALING ONLINE DATING FRAUD [2012].

Description: Online romance scams are a prevalent form of mass-marketing fraud in the West, and yet few studies have addressed the technical or data-driven responses to this problem. In this type of scam, fraudsters craft fake profiles and manually interact with their victims. Because of the characteristics of this type of fraud and of how dating sites operate, traditional detection methods (e.g., those used in spam filtering) are ineffective. In this paper, we present the results of a multi-pronged investigation into the archetype of online dating profiles used in this form of fraud, including their use of demographics, profile descriptions, and images, shedding light on both the strategies deployed by scammers to appeal to victims and the traits of victims themselves. Further, in response to the severe financial and psychological harm caused by dating fraud, we develop a system to detect romance scammers on online dating platforms. Our work presents the first system for automatically detecting this fraud. Our aim isto provide an early detection system to stop romance scammers as they create fraudulent profiles or before they engage with potential victims. Previous research has indicated that the victims of romance scams score highly on scales for idealized romantic beliefs. We combine a range of structured, unstructured, and deep-learned features that capture these beliefs. No prior work has fully analyzed whether these notions of romance introduce traits that could be leveraged to build a detection system. Our ensemble machine-learning approach is robust to the omission of profile details and performs at high accuracy (97%). The system enables development of automated tools for dating site providers and individual users.

C. EXSITING SYSTEM:

As a user of an Online Social Network one should always see to it that his/her profile is safe and has not been cloned by anyone. For detecting cloned profiles, we have designed a mechanism using which we can find whether the profile of a user is cloned as well as is their presence of fake profile of the user. This strategy succeeds most of the time and sometimes may not as there are many users having similar credentials. The User's profile is analyzed to search for rare pieces of information. This information may be specific to a particular user. The user credentials like name of the user, profile photo, Education details, workplace etc. are used to identify the particular user. Each social network will give various user profiles which have similarity to the legitimate profile. A comparison is made between the original profile and the searched record and after the comparison a similarity Index is calculated. Profile photo is having very important role in the process to verify the cloned profile.

D. PROPOSED SYSTEM:

We designed mechanisms to detect the same site profile cloning profile cloning. This mechanism also detects the Fake profile if it is present in the site. We propose a technique using steganography in which we add an ID to the profile and posted pictures which the id will be an email id of the user which is added to the

image while uploading. The images downloaded from fake profile users and uploaded it when the notification alert sends to the original users. If the original profile user gives the permission when the picture was uploaded otherwise it was blocked.

E. SYSTEM ARCHITECTURE:

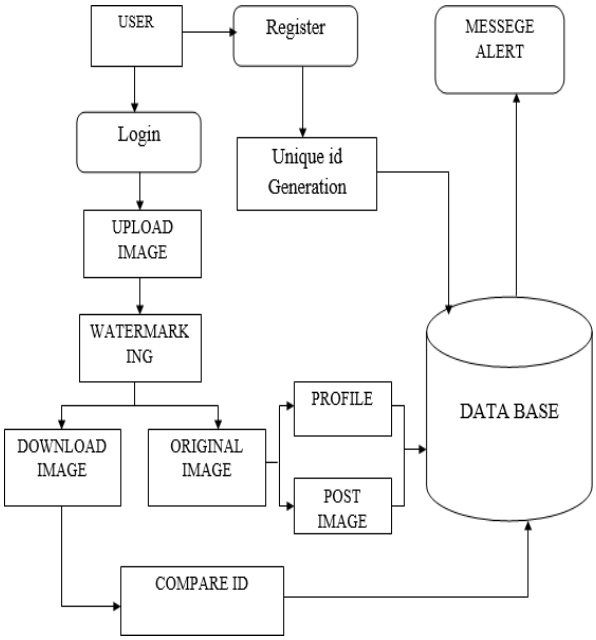

Fig 1: Architecture Diagram

1. BLOCK CHAIN WORKING:

Here we have been using Block chain technology to link all the images that has been uploaded by the user to find the fake identification. Say e.g. user-1 is uploading an image means it will be watermarked and linked in the chain streak as a block with an id. Like this whenever the user uploads an image it will be watermarked and linked an s a block of with a unique id the link. Likewise for all the users this image link streak will be created separately and whenever they are uploading it will be matched with it. If any signature is not matched the image cannot be linked in the streak and it will be detected as fake.

2. WATER MARKING WORK:

Here we will be making the secret key generated as digital signature with the images that the user is being uploading. All those images will be watermarked as digital signature and will be uploaded. For doing this steganography algorithm has been used here. This algorithm makes the secret generated to be merged with the image that has been uploaded by each user.

F. ALGORITHMS:

1. Watermarking Algorithm

Watermarking has been proposed as a method to enhance data security, confidentiality and integrity. Text watermarking requires extreme care when embedding additional data within the images because the additional information must not affect the image quality. Steganography and watermarking are main parts of the fast developing area of information hiding. The watermarking is a method to achieve the copyright protection of multimedia contents. Because the multimedia represents several different media such as text, image, video, audio, and graphic objects, and they reveal very different characteristics in hiding information inside them, different watermarking algorithms appropriate to each of them should be developed.

Step 1- Open Image.

This step will open the file and save header in a file and save the palette value of body in another file.

Step 2- Split the body of the image file.

This step will split the body image in equal blocks to use these blocks in hide text.

Step 3- Convert text watermarking to ASCII code and then convert to Binary code.

Step 4- Divided the stream binary code to parts every part 24 bit represent three character of text watermarking, and compare with pixels in palette of image.

2. Block Chain Algorithm

A Block chain is a method of storing a list of entries, which cannot be changed easily after they are created. This also applies to the list. This is done by using several concepts from cryptography, including digital signatures and hash functions. In most cases, a block chain is managed by a peer-to-peer network. All peers use a common protocol that specifies how they should communicate with each other, how a new block is created and validated. Once recorded, the data in any given block cannot be changed easily any more.

Changing the block means all the blocks after it need to be changed as well. Depending on the protocol, this will require a majority of the peers, or even all the peers, to agree.

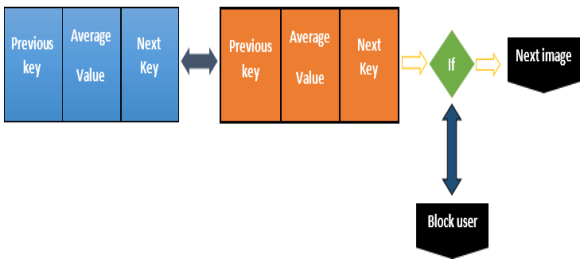

Fig 2: Data Blocks Network (Local Blockchain)

G. MODULES:

1. LOGIN:

The Login Form module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on your website. Which additional resources they will have access to can be configured separately. Once logged in, the Login Form module presents the user with a Logout button. Logged in users who are inactive for a predetermined period of time will be automatically logged out. The Login Form module will appear in whatever module position it is assigned to in the current template. It is also possible to have a Login Form that will appear in place of regular content when a Menu Item is clicked.

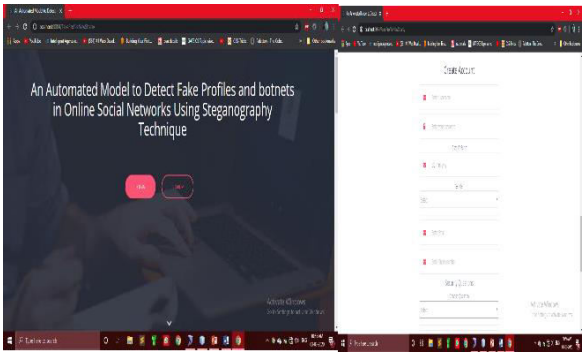

Fig 3(a): User Login

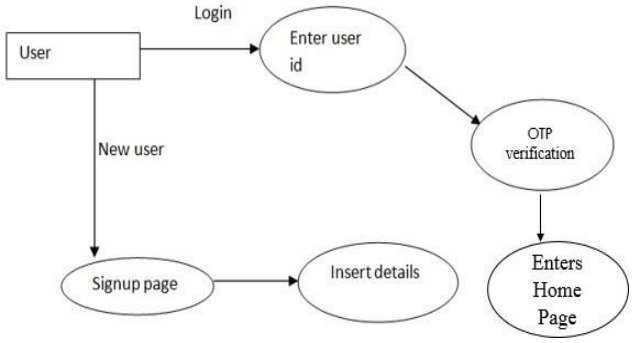

Fig 3(b): Login Data Flow

2. HIDE DATA:

In this module, it consists of a new stenographic algorithm for hiding data in images. Here we have also used a Steganography algorithm. Steganography is the practice of hiding secret message within any media. Most data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. Here 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. In this module, the concern user who uploads the image will have an id that will be hidden within the image. Once another user who downloads the image cannot see the image as it is hidden. We have also used water mark techniques that will not be visible even for the users. Steganography technique finds its main application in the field of secret communication. The main advantage of this algorithm is to keep the size of the cover image constant while the secret message increased in size. It can be used by intelligence agencies across the world .Hence this new stenographic approach is robust and very efficient for hiding data in images.

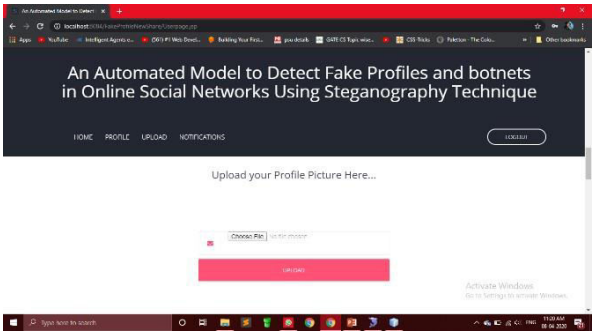

Fig 4(a): Upload Image

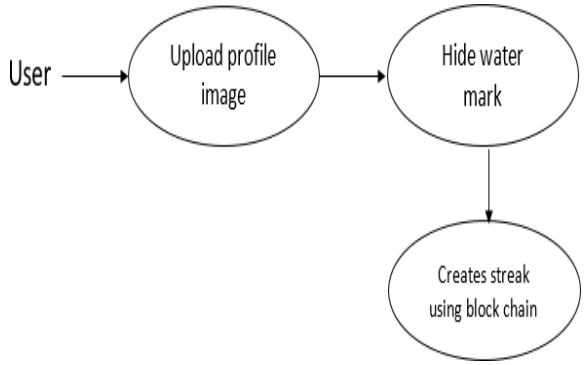

Fig 4(b): Watermarking on data streak

3. PROFILE MATCHING:

In this module, if the user who uploads the entire image can be viewed by the user. The user can downloaded the image but they cannot upload the same image this can be checked by the hidden id. The profile will be checked if the third party who upload the same image, this will be checked by the hidden id and break in image streak created for that user. If the profile matches with the profile, the user cannot upload the same it consists of a new stenographic algorithm for hiding data in images. Another user can, Use the Image or else can upload the Image internal entry criteria matching system that checks for a primary match based on hard-coded, Already some data inside is there are not check. This profile matching module will check if another user who uploads the image which is in exists with the user. There by this can avoids the fake user.

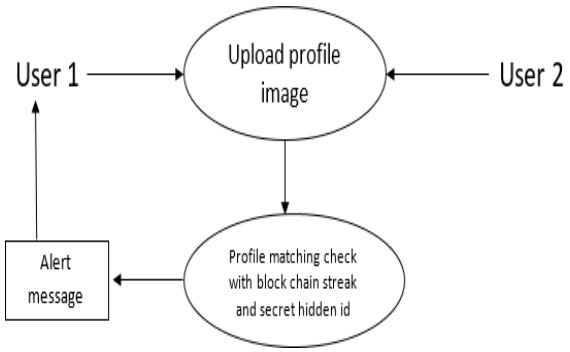

Fig 5: Key Matching & Authentication

4. ALERTED PROFILES:

If the profiles match, then the concern user will be alerted by the alert message. The user will be notified as their profile image has be tried to upload by the user and the user can block the person or else allow its user wish. User will also be notified with the fake users name, mail id, uploaded image, uploading time and system MAC Address. Criteria match fails, no further weighing point match is attempted and the profile is either created newly or rejected based on parameter settings for this interface ID in fake profile. So finally give some Alert Message to the original User.

Fig 6: Alert Notification

H. CONCLUSION:

We solved Entity Resolution with our system and used it to compare online user profiles from social networks in order to identify matches. Our systems are comparing the two images and identify that fake or not. We are using Steganography Algorithm and that algorithm hides the information inside the image. In this way new images upload in our profile and that image compare to existing user profile. If the image is fake when send notification to original user. The

original user allows the uploading notification that images was uploaded otherwise blocked.

I. REFERENCES

[1] J. T. Hancock, L. Curry, S. Goorha, and M. Woodworth Automated linguistic analysis of deceptive and truthful synchronous computer-mediated communication-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. 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.