Preventing Unauthorized Photo to be Published by Erasing Unapproved User Picture – Proposed Solution

Mansour A. Abu Sameeha
Al-Balqa’ Applied University

Namer Ali Al Etawi
Al-Balqa’ Applied University

ABSTRACT

The main aim of this project is to conceal and hide any photo for any user who does not give the permission for showing his picture, in this case need to have data base set for each user and the permission table for him /her to show his photos on OSN, and a FR system is to be established with a solid dataset for users and also to recognize the faces within photos, after finding a match for user’s face in a the picture a process is triggered to know the type of permission for showing or not this face, if yes the photo will be shown and on the contrary if no the user’s picture within the photo will be selected and the whole users picture will hollowed or emptied, in this case the use of edge detecting technique in image processing will take over the user’s pictureand the selected picture will totally be moved (hollowed).

General Terms

Privacy, security

Keywords

Online social network, edge detection, shared photo.

1. INTRODUCTION

In the last few years, hundreds of OSNs have been launched, allowing the users to associate with others [1].it needs a few steps to becomea member in OSN. It only requires a registration, representing name and electronic mail, address, mostly for free.

After completing the specific details of his own page that can include various (personal) details as well as picture user’s and videos, the user can start connecting with the other members and start uploading videos and photos [2].

While starting building friend list of his own the user unknowingly expands the space of threat over his page, the more his friends list expand the more of hidden friends of friends are watching.

Now a day, there are billions of users of various forms of social media,according to TechCrunch, in 2017, Facebook at the top with about 2 billion users, YouTube with 1.5 billion, and WhatsApp with approximately 1.2 billion; and other platforms support millions of users, including million), Instagram (700 million), Twitter about (300 million), and Snapchat (255 million) [3].

The importance of OSN is progressively increased every day, the way of communication over the internet is mostly passing through social media, the way people posting information and photos on OSN mostly without caring about the privacy of other persons who are involved in the photo. Once a user posts a video and photo on OSN it will be permanent and he/ she is no longer can control who can see or not see this photo.

That means (OSNs) make personal information accessible forlong periods of time, Information that is uploaded to OSNs is not deleted by default [4].

In a simple scenario for what exactly happens, assume user A post a photo for him and some of other persons, then automatically all users in user A friends list will be able to see this photo and they can tag it which leads to expand the range of users who can see this photo witch are friends of friends of User A.

However, not only the increase of participation rates throughout the last years has been stunning, but also the quality and quantity of information they display.

Though the benefits of sharing photographs on Facebook are in large quantities (e.g., self-presentation, communication and entertainment,). The jeopardies associated with their disclosure also abound.

In book “I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy”, Andrews (2012) Reported actual life cases of people who expert the negative consequences of their decision to post photos on Facebook—such as legal battles over child custody to employees losing their jobs[5].

in this paper a new proposed scenario in which easily can upsurge the privacy of individuals in OSN, as long a new user register himself in an OSN a few information is needed, his/her email and soon start to build his/her own profile, whilst a new friend is added to the list, they automatically can see what is published.

Currently, many OSN users do not have controller over the data which is appearing outside of their profile page over OSN [10]

2. LITRETURE VIEW

A paper on "Face/Off: Preventing Privacy Leakage from Photos in Social Networks"[6]. In this paper, an access control applied to the photo is done in addition to new mechanism were adapted to prevent unwanted users to recognize the inadvisable in the photo by blurring the user’s face r who does not giving permissions over his photo to be published.

A paper on "The Image Protector, a Flexible Security Rule Specification Toolkit" [7].in this paper there is a set of rules were applied to enhance privacy for multimedia over OSN, they divide the permission over an object to positive rule or negative rule, also an annotation model was used to enrich any slice of the photo, an image protector was applied and was composed of two main modules: a back office module and a front office module. the back office module is used to manage multimedia objects and specify security rules and alsothe front office module supports queryingmultimedia objects and displaying their filteredcontent.

A paper on "MyPrivacy My Decision: Control of Photo Sharing on OSN Using Cloud "[8]**.**
In this paper an attempt to discourse this concern and when a user shares a photo containing persons other than himself/herself (labeled co-photo for short).

To avoid probable privacy leakage of a photo, a design of new approach to enable each person in a photo to take care of the posting activity and participation in the decision making on the photo he/she posts. This need an efficient facial recognition (FR)system that can identify everyone in the photo

3. PROPOSED WORK

it was noticed that many photos were published without the acceptance of the individuals who were in that photo, therefore some steps are needed to establish a solid privacy system that will not allow for any part in the photo to be published until it goes through a sequence of privacy steps, and those steps without declining any of them are all together build the system in a novel way to prevent the privacy of the photos over OSN.

3.1 Methodology

The first key element in the proposed system is the access control list witch will be defined quicklywhen user A receives a friend request from User B on his wall, in order of the acceptances for the new requesting friendship a new field will be filled by User A that indicates if he gives User B the permission for his own photos either to be published or not on User B wall, that leads to build a new data base for each user and to specify the rule of each new user added to his list with one of two rules(allowed to publish or not allowed), this action will take over all users in our database. This implies that the new access list should be dynamic which means if user B asks user A to accept his friendship, then user A should have a new restriction over user B including his own photo sharing, or publishing any photo that contains pictures of user A.

The second key element is that the system should have an up-to-date face recognition API, a proposed one is the FR that was done using Microsoft cognitive service face API which is a cloud service that has almost advanced face algorithms [9].

In this API has two primary functions: face detection with attributes and FR, Face rectangle with four sides (left, top, width and height) indicating the face location in the image is returned along with each detected face [9]. Optionally, face detection triggers a series of face related attributes such as age, gender (M/F), head pose, facial hair and if his eyes are covered with glasses.

Face recognition is extensively used in many situations including security, natural user interface, image content analysis and management, mobile apps, and robotics [9].

Four face recognition functions are provided: face verification, finding comparable faces, face assemblage, and person identification. This API can also be used for face confirmation, finding similar faces, face grouping[9].

The other key element is Edge detection needed here, according to the outputs coming from a study done by the researchers in Al-Balqa’ Applied University for 135 student, the study aimed to see if the users can identify some persons and recognize any of these individuals by eliminating a part of the photo, a set of photo containing pictures for popular students and some employees and faculty members, these photos were chosen from the sample case Facebook pages randomly, and the faces of persons in that photos were blurred, every person in study sample was shown a set of pictures in his/her college, and the question was if he/she could recognize any of the persons in these photos? The answers were amazing, 38% of the sample can recognize one person at least, 17% of the sample could recognize two persons and 9% of the sample could recognize more than two of persons in the photo.

Most of the sample who could identify persons about 61% said that the body shape was a main factor for them to guess the person, 21% said the special marks led them to identify the persons in the photo (marks as: outfits, accessories (badges, name tag…etc.).

For all the above a mechanism needed to keep the privacy for persons over OSN, the edge detection will take over as the key element for the proposed system, if any person in the photo didn’t give permission to the publishing user then his/her picture will be emptied (hollowed) not only hiding the face but all his/her body.

4. FUTURE WORK

The photo with an emptied space is not suitable for publishing, so a new mechanism is needed to rejoin the photo together by cancelling all the empty spaces and the challenge to maintain a suitable shape of the background and keep it as appropriate as possible.

Keeping the background seen suitable for publishing needs a smooth rejoining for all the parts of the photo and to keep the proper lines within the photo as if there aren’t any part was taken, here an AI techniques could take place by manipulating the both sides of the emptied picture and to see the difference or the resemblance of the shape in horizontal lines and a new background could be generated and looks as much as appropriate.

5. REFERENCES

[1] Journal of Computer-Mediated Communication 12 (2007) 1143–1168 International Communication Association,https://www.lifewire.com/upload-saved-photos-or-videos-to-snapchat-4103878

[2] Ardion D. Beldad & Sabrina M. Hegner (2017) More Photos From Me to Thee: Factors Influencing the Intention to Continue Sharing Personal Photos on an Online Social Networking (OSN) Site among Young Adults in the Netherlands, International Journal of Human–Computer Interaction

[3] Constine, Josh. 2017. “Facebook Now Has 2 Billion Monthly Users…and Responsibility.” TechCrunch. http://social.techcrunch.com/2017/06/27/facebook-2-billion-users/; https://techcrunch.com/2017/06/27/facebook-2-billionusers/

[4] Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. Proceedings of the WPES 2005 Workshop on Privacy in the Electronic Society. New York, NY:ACM.

[5] http://www.ijetcse.com/wp-content/plugins/ijetcse/file/upload/docx/462A-NOVEL-APPROACH-FOR-PRIVACY-PRESERVING-PHOTO-SHARING-ON-SNSS-pdf.pdfSecurity and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on18-21 July 2011

[6] Panagiotis Ilia, Elias Athanasopoulos & Iasonas Polakis (2015). Face/Off: Preventing Privacy Leakage From Photos in Social Networks ,CCS '15 Proceeding of the 22nd ACM SIGSAC conference on computer and communications security paged 781-792

[7] Bechara Al Bouna , Richard Chbeir , Alban Gabillon ,the image protector a flexible security rule specification toolkit, conference: secrypt 2011 - proceedings of the international conference on security and cryptography, seville, spain, 18 - 21 july, (2011)

[8] V.Abinaya, R.Jancy, C.Pavithra, D.Nandhini, K.Saranya (2017), My Privacy My Decision: Control of Photo Sharing on OSN Using Cloud, South Asian Journal of Engineering and Technology Vol.3, No.5 (2017) 130–133

[9] https://docs.microsoft.com/en-us/azure/cognitive-services/face/

[10] Andrews,lori B. I Know Who You Are and I Saw What You Did: Social Networks and the Death of privacy. free press, NY 2011.