Sustainable Cities and Society xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Obfuscated image classification for secure image-centric friend recommendation

Kazi Wasif Ahmed*, Omit Chanda, Noman Mohammed, Yang Wang

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada

ARTICLE INFO

Keywords:
Friend recommendation
Online smart community
Deep neural network
Image obfuscation
Image classification

ABSTRACT

Image sharing is one of the most popular activities of smart citizens in recent time. People tend to frequently upload images through smart devices to express different aspects of their life with connected peers using the image sharing feature facilitated by different social media services such as Facebook, Flickr, Pinterest, and Instagram, etc. The service providers of such web services are utilizing the image features and high availability of cloud storage at low cost for providing friend recommendation service to build online smart community. However, after reports of citizens surveillance by government agencies and the celebrity photo leakage incident in iCloud, users have become concerned about their photo privacy. In addition to that, the cloud services are vulnerable to security threats and an adversary capable of breaching the security would be able to access the images residing in the cloud storage. Obfuscating images before sharing can be considered as a potential solution; however, de-obfuscating and then classifying millions of images at the service provider's end does not provide privacy guarantee and it is computationally expensive. Motivated by this scenario, we propose a practical privacy-preserving image-centric friend recommendation framework compatible with smart devices which protects the privacy of images through obfuscation and classifies obfuscated images using the deep neural network to build user profiles for friend recommendation.

1. Introduction

Social networking expands the network of a person by grouping individuals and organisations based on one's likes and dislikes and common interests. Facebook, Twitter, LinkedIn, and Google+ are examples of such social networks which have gained much popularity during the past few years. As of April 2016, Facebook has 1.59 billion active users whereas the Facebook-owned WhatsApp has 1 billion (Chaffey, 2016). The recent analysis identifies the social network as a key component of social capital, important in its own right and worthy to be analyzed for building online smart communities (Alvarez, Borsi, & Rodrigues, 2017). In addition to that, the introduction of smart personal devices has facilitated the users to interact with their peers via the social networking sites virtually anywhere and everywhere. Analyzing the available data of social networks can help to provide a better understanding of users behaviour as well as an insight regarding how people communicate and operate in virtual communities or neighbourhoods.

1.1. Motivation

An online community is a group of people having common interests who use the online services to interact, work, and pursue together their interests over time. Understanding the link between people is a primary requirement to build online smart communities (Tella, 2014). The social network is one of the tools people are adopting to create virtual neighbourhoods and bonding (Alvarez et al., 2017). Recently, the recommendation has emerged as a vital service provided by almost all social networking sites (e.g., Facebook, Google+, and LinkedIn, etc.) in the road towards forming the online smart community among the citizens of the smart city. The recommendation can come in various forms such as joining online blogs or communities, friend recommendation and product recommendation, etc.

Social network analysis might reveal some new insights regarding the preferences of an individual and it is essential for supporting the smart recommendation services. For example, today one of the most common behaviours of a smart citizen is to share pictures of their travels or a decent meal on the social networks even before enjoying it; this results in a massive amount of photos and videos to be hosted online. According to a report in 2014 (Souza Araujo et al., 2014),

* Corresponding author.
E-mail addresses: wasif@cs.umanitoba.ca (K.W. Ahmed), omitum@cs.umanitoba.ca (O. Chanda), noman@cs.umanitoba.ca (N. Mohammed), ywang@cs.umanitoba.ca (Y. Wang).

http://dx.doi.org/10.1016/j.scs.2017.10.001
Received 15 August 2017; Received in revised form 2 October 2017; Accepted 2 October 2017

around 60 million images are shared every day on Instagram to that date. The availability of this large quantity of images enables the social networking service providers to provide smart recommendations of similar users using the visual features of the user's uploaded images.

The correct reasoning of users mentality and behaviour can be very useful for generating the relevant smart personalized recommendations (Cheng, Liu, & Yu, 2016). In particular, similar people are more likely to interact with each other and have a connection among them. Therefore, if the contents of the uploaded images of a user in social networking sites are similar to another user, they might have a common interest and therefore, they might want to expand their circle by connecting with each other. However, image-centric recommendation service requires building user profiles extracting visual features from the images. As a result, the quality of recommendation services depends on the accuracy of feature extraction.

The recent advancement in machine learning based on artificial neural networks has led to seminal improvements for extracting visual information from images. The deep convolutional neural (DCNN) network and autoencoder are two promising techniques in this field. Because of the resemblance with the human brain, these techniques can classify objects more accurately than the existing models (e.g., the bag of words and feature based methods) and helps service providers to build relevant user profiles. It is no surprise that many social networking applications are now considering the image features as one of the major factors to provide better recommendation service (Yuan, Wang, Wang, Squicciarini, & Ren, 2014). Unfortunately, there are some privacy concerns which may demotivate the users sharing image contents in order to get recommendation services. Overcoming these challenges to provide image-centric friend recommendation is the focus of this paper.

1.2. Privacy implications

The image-centric friend recommendation service has some privacy implications as these user's images contain many sensitive attributes which can be used by the malicious adversaries to re-identify a user. For example, one can upload images in a social network containing his preferred objects (e.g., dog, sky, flower, etc.) that can reveal his personal preferences to the adversaries. In addition to that, the metadata associated with images such as geolocation and time when the photo is taken is sensitive as it can reveal personal information and used for executing re-identification attack. Moreover, different techniques have been developed that can identify objects in images. For example, the face recognition technology developed by Facebook is one of its most appealing features which has become a matter of privacy concerns (Ra, Govindan, & Ortega, 2013). Due to this controversy, Facebook turned off the service of face recognition in 2012 but bought it back again due to the popularity of image search. Furthermore, Google has decided to disable face recognition in Google Glasses (Zhang et al., 2015).

To some extent, the above privacy concerns come from the fear that images may be illegally accessed by some malicious adversaries as most of the service providers are using the cloud as a solution to storage constraint problem. Simply disabling the feature of automatic face recognition does not solve the problem as it also eliminates the data utility for image search functionality.

Apart from the concerns stated above the cloud services are also prone to privacy attacks. Some recently published news clearly demonstrates that privacy should not be expected to be preserved by cloud service providers (Chen, Geyer, Dugan, Muller, & Guy, 2009). One prime example which underlines this scenario is the recent incident regarding the hacking of the iCloud image storage service and celebrity photo leakage (Lewis, 2014). Similarly, there exist some other glaring examples which demonstrate the risk of the privacy breach in cloud-based visual data storage. These are the primary reasons that made the users concerned about protecting the privacy of their images.

1.3. Privacy protection

Various tools to ensure image privacy exist, including image blurring, mosaic, scrambling and encryption. In 2012, YouTube introduced a technique to automatically blur all faces in a video (Youtube Official Blog, 2012). This automatic facial blurring is presented as an effective solution to improve video privacy of Youtube users. For example, this technology motivates someone to share sensitive protest footage without exposing the faces of the activists involved. Similar technologies can be adopted to protect the privacy of images.

There are some other privacy preserving techniques which perform face detection and divides the images into private and public parts. However, this approach does not address our privacy goals completely and makes the system more complex in architecture. For example, if an image is leaked from the cloud; the attackers can obtain significant information from the non-obfuscated parts (e.g., objects in the background) (Ra et al., 2013).

Some recent attack models in the literature concentrate on partially obfuscated parts of the images to re-identify obfuscated parts also demonstrate the risk (McPherson et al., 2016). Therefore, obfuscating the full image using the lightweight image obfuscation techniques such as symmetric encryption or photo blurring is a more practical solution for protecting the sensitive information of images while enabling classification task to provide different utility services.

1.4. Contributions

- The main contribution of this paper is designing a practical framework for privacy-preserving image-centric friend recommendation which protects the privacy of user's shared images and at the same time allows user profile generation classifying the obfuscated images.
- We have used two popular image obfuscation techniques blurring and encryption in our proposed model. To the best-of our knowledge, our work is the first to deal with obfuscated image classification for providing image-centric friend recommendation service.
- Our work demonstrates that deep neural networks can be used as a tool for obfuscated image classification. The proposed model utilizes the efficiency of DCNN for classifying blurred images and deep autoencoder for classifying encrypted images.
- We compare the accuracy of our proposed image obfuscation techniques encryption and photo blurring. The experimental results signify the utility of the proposed model. Our proposed model achieves 83.94% accuracy while the existing model (Wang, Vong, Yang, & Wong, 2016) achieves 79.83% for encrypted image classification over MNIST dataset.

The rest of the paper is organized as follows: Section 2 gives an overview of our proposed model. Section 3 formally presents the methodology used in this paper. Section 4 describes the steps of our proposed method. Our performance evaluation is done in Section 5. Section 6 discusses the related works. Finally, we summarize our work and conclude the paper in Section 7.

2. System overview

Generally, in recommendation systems, a user profile is built for every user capturing the user's preferences. When a user requests for recommendation to the service providers, a similarity comparison is performed with other users based on his/her user profile, and the computed results are returned back by the service providers. To get a recommendation or to be recommended, users need to reveal some information to the service providers which is utilized by the service providers to build user profiles. The matter of concern is how to hide information in such a way that it reduces the risk of privacy breach as well as preserves the utility of friend recommendation service.