Facelock—A Labware for Teaching Photo Privacy in Online Social Networks through Face Recognition*

Sadia Shormin, Lin Li, Na Li
Department of Computer Science
Prairie View A&M University
Prairie View, Texas 77446
sshormin@student.pvamu.edu, {lilin,nali}@pvamu.edu

Abstract

Online photo sharing has become a popular activity for Internet users. Semantically rich photos often contain not only the information that the uploaders want to share but also the information that is sensitive to others. However, most of the current online social networks do not have well-defined mechanisms for user privacy protection. This paper discusses the design and implementation of a labware—Facelock which was developed for teaching photo privacy. The goal is to increase students' awareness of privacy protection while sharing photos in online social networks. Through the labware, students can gain a thorough understanding of the photo privacy and essential concepts of face recognition. This labware can be used in both cybersecurity and data science courses. It was pilot-tested through a workshop in 2019 among thirteen students majoring in Computer Science. Surveys results showed the effectiveness of the labware and the attainment of the learning objectives

1 Introduction

Today, people frequently interact with their families, friends, and colleagues through online social networks (OSN), especially with the advent of smart

phones with high-quality camera embedded which enables users to record their life anytime and anywhere. People enjoy posting and sharing their photos in online communities, blogs, and content sharing sites. For example, there are over 350 million photos uploaded daily on Facebook [11], and users share over 700 million photos daily on Snapchat [5].

Many times, the semantically rich pictures contain sensitive contents which may disclose users' private information such as location and personal habits. More importantly, sharing such pictures online may unnecessarily expose users' friends and acquaintances involved in the photos, thereby leading to their privacy breach [3]. Most photo sharing websites allow users to configure their privacy preferences to some extent. For example, Facebook allows users to decide whether they want to share a photo with their friend group or family group or the public. Unfortunately, recent studies have shown that users had struggles to set up and maintain such privacy settings [13]. One of the primary reasons addressed is that, given the amount of shared information, such configuration process can be tedious and error-prone as too many factors need to be evaluated before the decision is made. Therefore, many researchers have acknowledged the need of access control and privacy policy recommendation systems which can assist users to properly configure privacy settings.

The education on image privacy, however, has not been well integrated into the undergraduate security classes. The main obstacle is the lack of effective hands-on learning labs related to this topic. To address this problem, the authors were motivated to develop a labware with the following objectives: (1) increase students' awareness of image privacy protection; (2) make students understand different users' privacy preferences; (3) teach students basic protection mechanisms for image privacy; and (4) understand the trade-off between privacy protection and its cost.

The rest of the paper is organized as follows: Section 2 briefly discusses the literature related to image privacy protection and describes the current development of privacy education. Section 3 introduces the design and implementation of the Facelock system. Section 4 presents the evaluation results after surveying thirteen students majoring in Computer Science at Prairie View A&M University through a workshop conducted in 2019. Finally, a conclusion is made in Section 5.

2 Related Work

2.1 Image Privacy Protection

To enhance image privacy protection, some existing work [7, 15] focused on developing access control based approaches. They leverage photo tags which are either labelled by people or generated by the tagging service provided in most

photo sharing sites for purposes including organization, search, communication, and description of photos. The tags can help users intuitively create and maintain fine-grained access-control policies more. Another group of technologies focus on developing privacy policies which help photo uploaders automatically decide whether a photo should be labeled as public or private. Different photo related information, including tags, captions, comments, meta data and image content, is used to classify private and public photos [12, 16, 8]. More recently, big data technologies are also used to extract better features which can be used for the photo classification [17, 14]. In addition, some photo privacy preservation technologies [7, 15] manage privacy protection level to objects involved in photos instead of the entire photo [14]. Then some image operations, such as blurring, local encryption, warping, pixelation, and masking, are applied on the sensitive objects identified from the photos [6, 9].

2.2 Privacy Education

The ACM's Computer Science Curriculum 2013 has acknowledged the importance of privacy education [1]. Currently, the development of curriculum for teaching privacy to younger students is still insufficient. A team of cross-disciplinary members, including computer scientists, educators, and social scientists, from the International Computer Science Institute (ICSI) and the University of California at Berkeley, have developed an online privacy curriculum [2] including ten principles with the purpose of spreading the awareness of protecting online privacy among younger students. However, their curriculum focuses on the general education of online privacy instead of photo privacy in OSN. To the best of the authors' knowledge, the work described in this paper is the first one on a learning labware development particularly for educating younger students to protect privacy while sharing photos in OSN.

3 Design of the Labware

The in-house developed labware—Facelock is a web based system. It consists of three components: (1) a SQLite database, (2) a web server, and (3) a face recognition library. The three components work together with an emphasis on the image privacy protection principles, photo recognition, and the access control procedure. A framework of the labware is illustrated in Figure 1.

3.1 SQLite Database

The Facelock system uses SQLite database to store the information of the registered users, including their post records, profiles, friend lists, etc. For face recognition purpose, each registered user must upload a "standard" picture as

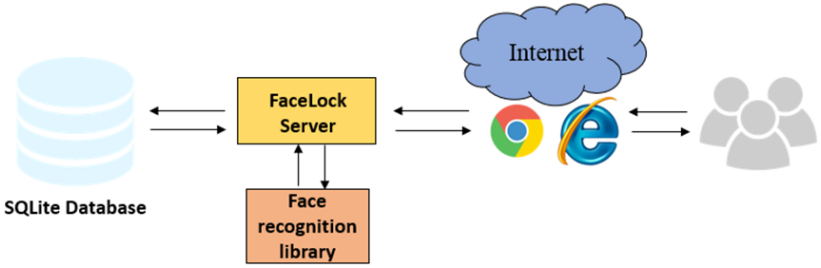


Figure 1: The system architecture of the Facelock labware

part of his/her profile, as shown in Figure 2. The profile pictures of the users will be used for face recognition by the face recognition library. Compared with other relational database management systems, SQLite is a lightweight disk-based database system contained in a C programming library. It does not require a separate server process and allows database access using a nonstandard variant of the SQL query language.

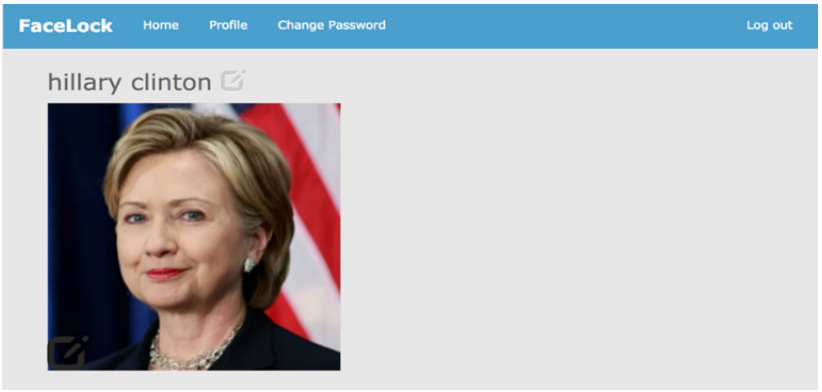
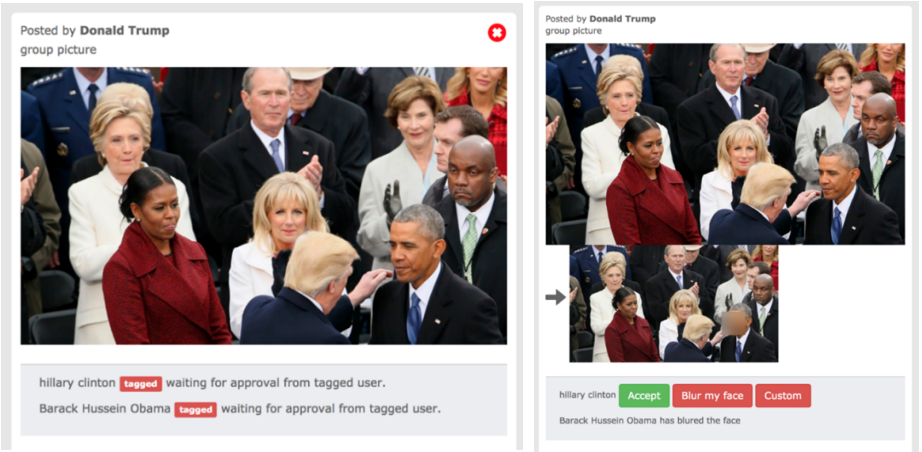


Figure 2: The profile page of a Facelock user

3.2 Facelock Web Server

The Facelock web server hosts a Facebook like social network environment where users can post messages and pictures, search people, and join friend circles, etc. Apart from these basic functions, Facelock reinforces photo privacy protection. Specifically, when a user attempts to post a photo, the web server will utilize the face recognition library to tag users on Facelock who are included



(a) Tagged users through face recognition (b) After clicking "Blur my face"

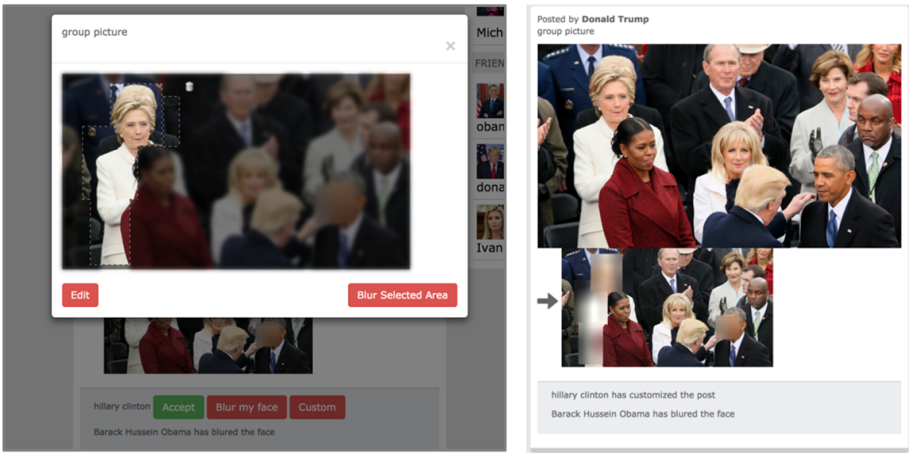
Figure 3: Individually tagged users through face recognition

in the photo. Each tagged user will receive an alert and then take action to edit the photo to meet his privacy preference. The post will not be made publicly available until all tagged users respond with their privacy protection choices. Figure 3a depicts a scenario where the user "Donald Trump" tries to post a picture, in which recognized Facelock users such as "Hillary Clinton" and "Barack Obama" are tagged. Therefore, "Donald Trump" has to wait for them to grant the releasing of the picture before sharing it with the public.

At the current stage, the Facelock system implemented three privacy protection options for tagged users, including *no anonymization*, *face anonymization*, and *selected area anonymization*.

No anonymization does not provide any protection to the user. The tagged user who selects this option (by clicking the "Accept" button shown in Figure 3b) is careless about releasing his picture to public by the uploader. With this option, the tagged user grants the system and the uploader to post the picture.

Face anonymization allows the tagged user to protect his face image. Once the "Blur my face" button is clicked, the tagged person's face will be blurred automatically and the blurred picture will be displayed together with the original picture for preview. After that, the photo uploader and other tagged users will be notified that this tagged person has rejected the post and chosen to hide his identity in the image. Figure 3b shows a scenario that when the tagged user "Hillary Clinton" logged into the system, she noticed that her



(a) Custmize blurring area (b) After area blurring

Figure 4: Photo preview after privacy protection using "Custom" option

face was shown in a new post created by "Donald Trump" and that another tagged user "Barack Obama" already chose to blur his face.

Selected area anonymization enables the tagged user to customize the image anonymization if he is not satisfied with simply blurring his face. In this case, the user can click the "Custom" button, and then he will see a modal window with the "Edit" option. By clicking the "Edit" button, the user can select multiple areas to blur and then confirm it by clicking "Blur Selected Areas". Figure 4 shows a scenario where the tagged user "Hillary Clinton" further customized the picture by blurring her image.

Once all tagged users made their privacy protection choices, the original photo uploader can review the altered photo. The blurred areas will be the "cost" of posting the picture online. This is because a blurred picture may lose its original value for visual aesthetics. Therefore, the uploader can make a decision to post the photo edited by the tagged users or to give up the post. In Facelock, the image manipulation function was implemented using OpenCV which is a library of functions commonly used in the research and applications related to computer vision [10]. The library contains different options for blurring images such as Gaussian Blurring, Median Blurring, and Bilateral Filtering. In Facelock, Gaussian Blurring was used.

3.3 Face Recognition Library

A key component of Facelock is the Face Recognition library which is used to recognize faces in the photos for user tagging. There have been different machine learning models developed for image classification. Considering the model complexity and the speed required for fast web processing, the one adopted by Facelock is a deep leaning based open source application available on GitHub [4]. As the script was written in Python and Facelock was also developed using the same language with the Django framework, this model was seamlessly integrated into Facelock. The advantage of this library is its light weight and high accuracy. Particularly, it only requires the registered user to upload one "standard" profile picture to reach high accuracy and it can achieve the recognition accuracy of 99.38% on the labeled faces in the Wild benchmark (`http://vis-www.cs.umass.edu/lfw/`). All photos posted in Facelock will be examined with the existing profile pictures to recognize users. A code snippet of using the library is as follows:

```
# Import the face recognition library
import face_recognition
# Detecting "Trump" by comparing the profile picture with the unknown picture
known_image = face_recognition.load_image_file("trump.jpg")
unknown_image = face_recognition.load_image_file("unknown.jpg")
trump_encoding = face_recognition.face_encodings(known_image)[0]
unknown_encoding = face_recognition.face_encodings(unknown_image)[0]
results = face_recognition.compare_faces([trump_encoding],
                                         unknown_encoding)
```

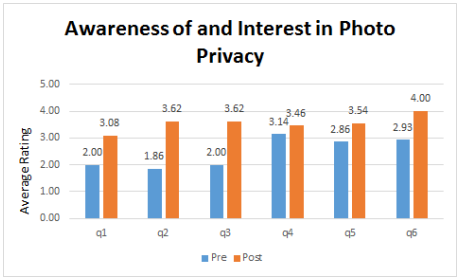
4 Evaluation

In order to expose students to privacy preservation and inspire their learning interests, the authors pilot-tested this educational tool in an educational workshop conducted in fall 2019 for student training. A total of thirteen undergraduate students from Prairie View A&M University majoring in Computer Science participated in the evaluation of the labware. The learning and evaluation activities fell into two categories: (1) classroom presentation to introduce photo privacy in OSN and anonymization basics, and (2) hands-on labs using Facelock to examine the three anonymization options discussed in Section 3 and understand the tradeoff between privacy preservation and its cost. Pre and post surveys were conducted at the beginning and the end of the testing sessions to evaluate and analyze the outcomes. The student survey questions are listed in Table 1. All questions use a rating scale of 1 to 5 with 5 being the greatest deal or the most positive.

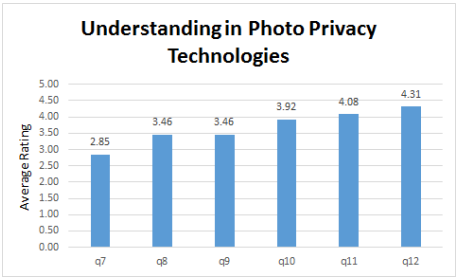
Questions 1 to 6 were surveyed in both pre and post questionnaires. Figure 5a plots the average rating with regard to the discrepancy of pre and post

Table 1: Pre and post survey questions

#	Survey Questions	Type
1	Rate your awareness of access control mechanism in OSN?	Pre & Post
2	Rate your awareness about privacy disclosure from photo sharing?	Pre & Post
3	Rate your awareness about photo anonymization mechanism?	Pre & Post
4	Rate your interest in access control mechanism in OSN?	Pre & Post
5	Rate your interest in privacy disclosure from photo sharing?	Pre & Post
6	Rate your interest in photo anonymization mechanism?	Pre & Post
7	Rate your learning about access control mechanism in OSN?	Post
8	Rate your learning about privacy disclosure from photo sharing?	Post
9	Rate your learning about photo anonymization mechanismlab?	Post
10	This lab helped me understand the access control mechanism in OSN	Post
11	This lab helped me know how a privacy-aware tagging system works	Post
12	This lab and privacy preservation should be taught in security courses	Post



(a) Awareness and interest change



(b) Understanding of photo privacy

Figure 5: Experimental results

survey results. A significant increase is observed on students' awareness of and interest in access control mechanism in OSN, privacy disclosure of photo sharing, photo anonymization after the lab. Questions 7-12 measured how much students gained in understanding the related concepts. The survey results were positive and encouraging with the average rating being greater than 3.4 from five of the questions, as shown in Figure 5b. One lesson the authors learned from the lab is to extend the lecturing time on the access control mechanism which would bring better feedback for questions 4 and 7.

5 Conclusion

This paper presents the design and implementation of a tool intended for teaching photo sharing privacy in online social networks. The goal was to provide

students with a solid understanding of the topic by using an in-house developed labware—Facelock, which not only enables students to be aware of the possible privacy disclosure of photo sharing in online social networks, but also equips them with necessary defense technologies. After pilot-testing the labware among thirteen students in fall of 2019, the authors got very positive feedback. Students confirmed that they thoroughly understood the photo privacy in OSN through the lab activities, and the tool helped them learn the concepts effectively. This shows that the teaching tool can be widely used in classrooms and integrated into security curriculum.

References

[1] Computer science curricula 2013. `https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf`.

[2] Teaching privacy. `http://teachingprivacy.org`.

[3] Andrew Besmer and Heather Richter Lipford. Tagged photos: Concerns, perceptions, and protections. In *Proceedings of the 27th International Conference Extended Abstracts Human Factors Computer System*, pages 4585–4590, 2009.

[4] Adam Geitgey. Face recognition. `https://github.com/ageitgey/face_recognition`.

[5] Ellis Hamburger. Real talk: the new snapchat brilliantly mixes video and texting. `http://www.theverge.com/2014/5/1/5670260/real-talk-the-new-snapchatmakes-texting-fun-again-video-calls`.

[6] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David James Crandall, Roberto Hoyle, and Apu Kapadia. Viewer experience of obscuring scene elements in photos to enhance privacy. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[7] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of 22nd ACM SIGSAC on Computer and Communication Security*, pages 781–792, 2015.

[8] Fenghua Li, Zhe Sun, Ang Li, Ben Niu, Hui Li, and Guohong Cao. Hideme: Privacy-preserving photo sharing on social networks. In *Proceedings of IEEE Conference on Computer Communications*, 2019.

[9] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. In *Proceedings of the ACM: Human Computer Interaction*, 2017.

[10] Kari Pulli, Anatoly Baksheev, Kirill Kornyakov, and Victor Eruhimov. Real-time computer vision with opencv. *Communications of ACM*, 55(6):61–69, June 2012.

[11] Cooper Smith. Facebook users are uploading 350 million new photos each day. `http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9`.

[12] Anna Cinzia Squicciarini, Dan Lin, Smitha Sundareswaran, and Joshua Wede. Privacy policy inference of user-uploaded images on content sharing sites. *IEEE Transaction on Knowledge and Data Engineering*, 27(1):193–206, Jan. 2015.

[13] Katherine Strater and Heather Richter Lipford. Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, pages 111–119, 2008.

[14] Ashwini Tonge and Cornelia Caragea. Image privacy prediction using deep features. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, pages 4266–4267, 2016.

[15] Nishant Vishwamitra, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail joon Ahn. Towards pii-based multiparty access control for photo sharing in online social networks. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, pages 155–166, 2017.

[16] Jun Yu, Zhenzhong Kuang, Baopeng Zhang, Wei Zhang, Dan Lin, and Jianping Fan. Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing. *IEEE Trans. Information Forensics and Security*, 13(5):1317–1332, May 2018.

[17] Jun Yu, Baopeng Zhang, Zhengzhong Kuang, Dan Lin, and Jianping Fan. iprivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning. *IEEE Transaction on Information Forensics and Security*, 12(5):1005–1016, May 2017.