

Assignment 1

eSoc 488: Information Privacy with Applications

Due: 24 October 2017

Total Homework/Assignment Points: 333

omissions List omissions here.
substitutions List substitutions here.
additions List additions here

Short Essay

Strive to answer these clearly and completely; incomplete or confusing answers will not get full points. Place all answers to these questions in a file called 'SHORT_ESSAY'.

1. (50) In what ways is privacy a social good? How might it be harmful to society? Choose several examples from the history we have discussed to illustrate your points.
2. (50) Should Congress pass a law requiring commercially-available products and services to be designed with backdoors allowing for compliance with search warrants? Are products and services without backdoors like locks in a home, or is an apartment a better analogy? Is a company that designs such a product or service failing to fulfill its civic obligations to the country it operates from?
3. (50) Explain Gen. Hayden's remark about 'translucence' as preferable to 'transparency.' Give several scenarios in which different parties should decide what is in the public interest to know about intelligence agencies' activities. Possible parties to consider include: intelligence agencies themselves, secret/nonsecret courts, special intelligence committees in Congress, journalists, others.
4. (50) Choose two named NSA programs from the Snowden revelations and describe who is affected (intentionally and 'incidentally'), and how they worked.

Face Detection

Face detection algorithms can be fooled, sometimes in unintuitive ways. We will set up facial recognition in python, and then experiment with fooling it. For this portion of the assignment you will find useful chapter five of *Learning OpenCV 3 Computer Vision with Python*, available at http://proquestcombo.safaribooksonline.com.ezproxy4.library.arizona.edu/9781785283840/ch05_html.

1. If you are not using the VM, install opencv. Otherwise, you may skip this step.
2. (44) Write a script called 'face_detect.py' to perform simple face detection in video. Use 'haarcascade_frontal_face_default.xml' as your classifier cascade file. Be sure to comment, and to write clear code.
3. (44) Read a little about how face detection using Haar Cascades works, and apply your understanding to try different things to reduce the confidence scores for the classification. Answer, in a file called 'anti-face-detection': Suppose this face detector were running on a surveillance camera that is out of your control. What actions could you take in the video to decrease the confidence of the classifier?

What did you try? Can you find a method that would be workable for an everyday person walking in the street? *Hint: You will need to figure out how to get the confidence score from the detectMultiScale method.*

4. (45) Now suppose you can intercept the video stream. Implement a method to add noise to the video stream until your face is no longer detected. Try by experiment to find the minimum amount of noise to prevent detection, then save two images `minimum_noise_detect.png` and `minimum_noise_nodetect.png` showing images with noise that is close to this boundary on either side (i.e., one detecting a face, one not).
5. (20) Extra credit: Improve somehow the script given in the book to train a classifier to recognize a face in a video stream (not just detect a face), then use it to train a classifier to recognize your own face, and print your name above the box.