Face Detection Countermeasures

eSoc 495: Information Privacy with Applications

Due: 19 October 2021

Total Homework/Assignment Points: 100

Face detection and recognition from video surveillance is a distinctive source privacy problems. Face detection algorithms can be fooled, however—sometimes in unintuitive ways. Here 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, 'Detecting and Recognizing Faces,' of *Learning OpenCV 4 Computer Vision with Python* 3, available at `https://arizona-primo.hosted.exlibrisgroup.com/permalink/f/6ljalh/01UA_ALMA51766166570003843` .

1. If you are not using the VM, install opencv. Otherwise, you may skip this step.
2. (20) Write a script called 'face_detect.py' to perform simple face detection in video. Use 'haarcascade_frontalface_default.xml' as your classifier cascade file. Be sure to include copious, useful comments, and to write clear code.
3. (40) 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. (40) Now suppose you can intercept the video stream. Implement a DARKLY-style 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. (10) 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 classifer to recognize your own face, and print your name above the box.