Lab 6 - Computer Vision

ME 451 - Introduction to Instrumentation and Measurement Systems, Spring 2019

### Lab Objectives

* Implement your own basic facial recognition algorithm.
* Implement your own learning-based image detection algorithm.
* Get experience with the quirks of computer vision techniques.

**Sensors for report:** CCD Digital Camera sensors.

*Note:* This lab occurs entirely in MATLAB. We will only give you one lab day for this lab in interest of giving you more time to work on your projects. With that in mind, we have simplified the structure of this lab (there are no signoffs) to enable you to complete the entire lab at home.

# Section 1: Face Recognition

1. Ensure MATLAB is set up properly. You will need the vision toolbox.
   1. Extract the provided image files to your MATLAB directory.
   2. If you experience problems with MATLAB, use [matlab.mathworks.com](http://matlab.mathworks.com)
2. Familiarize yourself with the Viola-Jones algorithm
   1. Some background on the [Viola-Jones algorithm](https://youtu.be/c0twACIJYm8?t=5m54s)
   2. **Discussion Question 1:** Describe in general terms how the Viola-Jones algorithm works.
3. Using the vision.CascadeObjectDetector in MATLAB, implement a script that:
   1. Finds the faces in a picture (use lab image 1).
   2. Draws a colored box around them.
      1. *Hint:* MATLAB has great documentation for doing this exact thing... and often provides well done examples.
   3. The algorithm usually fails to detect several faces in image 1. **Save** this image for DQ 2.
4. Using your implementation, try to find the faces in images 2, and 3.
   1. **Save** the pictures with the faces boxed for DQ 3 a/b.
5. After doing task 3, you should have a decent intuition of how faces are chosen.
   1. Using that understanding, draw a face that’s recognized by the algorithm. Step by step (make sure to document each step!), cut away at features of the face you get to a point where you cannot remove any more of the face without it not being recognized.
      1. **Save** the images you take. See DQ 4 for specific instructions on what you should show us.
   2. In a second picture, draw something (or find an image online) that is not a face but it tricks the system into thinking it’s a face, with the following specifications:
      1. Image cannot be of something living, or a drawing of something living.
      2. Face detection boxes need to have some area to them. Pixel-sized or otherwise miniature faces that are detected in an image will not count.
      3. *Note:* We have observed that an image that fakes out the algorithm on one person’s computer doesn’t work on another’s computer. Keep this in mind when trying images out.

## Section 1 Discussion Questions

**Discussion Question 1:** Describe how the Viola-Jones Algorithm works to detect faces.

**DQ 2:** Show your results for the image 1 face detection. Look at the faces it failed to detect. Is the vision algorithm racist, or is there another reason? Describe why.

S*poiler*: It’s not racist. What is another consistent difference that exists in the people who are excluded?

**DQ 3 (a/b):** The detection algorithm did not find everything in files 2 and 3. Separately for both files 2 (a) and 3 (b), pick a total of three faces that were not recognized and explicitly state a potential reason why each of the three faces wasn’t recognized.

Include the image files with the face detection boxes and also show a cropped image for each face that you chose. Be specific in your answers and reference how the Viola Jones algorithm works (and how it failed in this case) for each answer.

*Note:* The answer is not the same for every face (think about how the algorithm works and choose faces that highlight different failures).

**DQ 4:** Show us the most minimal face you are able to make and describe why you think the program is not able to go any farther. Show at least 4 variations of your faces to prove that it is the most minimal face you are able to make. Based on your findings, what do you think is the most important feature on the face for the detector? Why?

*Note:* Use explicit examples to show us that the algorithm won’t work if you cut away any more of the face.

**DQ 5:** Provide the image that you used to fake the algorithm, with the face-detection box. Why do you think you were able to trick the face detector? What features in the image you used do you think contributed the most?

# Section 2: Training a Stop Sign Detector

1. Now we are going to train the object detector to find a new object: stop signs. We are going to use a built-in MATLAB example found on [this page](https://www.mathworks.com/help/vision/ug/train-a-stop-sign-detector.html).
   1. Implement the training procedure.
      1. Use your trained detector on images stop1, stop2, stop3, stop4, and stop5 from the lab images.
      2. **Save** your results for each image for DQ 7.
   2. Using your intuition gathered from inspecting the results in task 5.a.i., predict whether the algorithm will detect stop signs in lab images 4, 5, 6, and 7. Write down your reasons why before you continue.
   3. Test your hypothesis by running your stop sign detector on each image.
      1. **Save** each image with the stop-sign detection for DQ 8.
   4. Make/find your own image without stop signs in it that will trick your stop-sign detector.
      1. **Save** this image with the stop sign detected for DQ 9.
      2. *Note:* Stop-sign detection boxes need to have some area to them. Pixel-sized or otherwise miniature areas that are detected in an image will not count.
2. *Note:* There are no signoffs report associated with this lab. This lab’s grade will be solely based on the other sections of the report.
   1. Because of this, make sure to answer all your Discussion Questions with enough detail so we know that you know what is going on (normally the signoffs help us with this).

## Section 2 Discussion Questions

**DQ 6:** Describe what happens when you train your stop sign detector. Does the computer actually understand high-level information (like what a stop sign is) or does it only understand low-level information? What does the computer look for when detecting stop signs?

**DQ 7:** Show your stop sign detection results for images stop1, stop2, stop3, stop4, and stop5 and describe how well you think your stop sign detector works. What are the quirks that your system has when detecting stop signs (anything weird going on with stop sign detection)? Does your system detect any false positives (meaning that non-stop signs objects are perceived as stop signs)?

**DQ 8:** What were your hypotheses for images 4, 5, and 6? How did your predictions hold up for each image? Show us your stop sign detection results for each image. Does your system detect any false positives? How could you improve your stop sign detector?

**DQ 9:** Show us your image that fakes out the stop-sign detector. Describe your strategy in picking images to fake out the detector. How well did your strategy work? What features in the image you used do you think contributed the most?

# Post-Lab Questions

**Post-Lab Question 1:** Ever since the usage of facial recognition algorithms in public, like with Facebook’s auto-tagging feature and with police facial surveillance, there have been attempts to fight computer vision algorithms. Some anti-surveillance techniques try to camouflage the face so it won’t be detected (for instance, CV dazzle and hyperface).

Describe how CV Dazzle or another facial camouflage technique interferes with facial recognition. Also, describe the downsides of facial camouflage. Remember to be specific in your answers. Provide your references in links at the end of your answer.

**PLQ 2:** Not only can computers read images, but they can also make images and videos. Look up and describe what deepfakes are. Briefly describe how these images are made. Comment on how deepfakes could affect society and explain how people attempt to detect deepfakes. Provide references in links at the end of your answer.

**PLQ 3:** Check out this research on tricking machine learning algorithms: [video](https://www.youtube.com/watch?v=M2IebCN9Ht4). Describe how they are able to trick machine learning algorithms. What does a machine learning algorithm look for when detecting objects? What are the implications of this work?

# Lab 6 Signoffs

There are none!