Exploring Reflectacles As Anti-Surveillance Glasses and for Adversarial Machine Learning in Computer Vision

Abstract

While technological advances in computer vision have helped in law enforcement, smart video surveillance technologies have led to privacy invasion of law-abiding citizens [8]. Sophisticated visual recognition techniques are being used worldwide in video surveillance in order to monitor public places and analyze data within captured camera footage for intelligence. Current state of the art visual recognition algorithms help boost the performance of the surveillance, and are extensively used in mobile devices and most modern consumer electronic products for user-authentication purposes. In order to counter this critical issue of privacy invasion, several privacy-enhancing research solutions have been proposed by different computer vision researchers for handling the problem at the surveillance system level by altering or enhancing the camera footage capture technique [8]. However, very few of these prior works have attempted to address this issue at the subject or public user level by providing surveilled individuals with the “anti-surveillance” technology to protect themselves from the privacy-invading surveillance cameras. [1, 3, 4, 5, 8]. In this unique research project, we firstly explore the capabilities of the new “Reflectacles” glasses [2] as a potential “anti-surveillance” wearable device for individuals to defend themselves from the privacy-invading surveillance cameras. As part of our experimentation, we exhibit the potential “anti-surveillance” effect of Reflectacles by putting it against current state of the art visual recognition tools, like IBM Watson Visual Analytics and AWS Amazon Rekognition, and showing that Reflectacles successfully reduces the visual recognition capabilities of the latter to some extent. In the process, we also demonstrate how an anti-surveillance wearable glass, like Reflectacles, can be prospectively utilized for adversarial testing and training with visual recognition algorithms, in an effort to evaluate the performance of these techniques, and contribute to their improvement. As part of this innovative research project, our proposed adversarial machine learning approach for testing and training of visual recognition tools is the first of its kind to make use of the Reflectacles in this context.

Research Methodology & Experiment Description

We conducted several tests using the Reflectacles against both IBM Watson Facial Recognition and Amazon Rekognition. The images shown here are selected sample test images used for conducting our experiments. IBM Watson Visual Analytics tool requires a visual recognition model with at least two classes. Our two classes consist of 39 images of an individual in public situations and 39 images in measured distances, different lighting, and body orientations. Both classes are trained together to make up the training class. The test class contains the images of an individual with no wearables, like hats, sunglasses, and Reflectacles. Amazon Rekognition requires an Amazon S3 storage using buckets. All test images containing pictures of an individual with Reflectacles are added to a bucket for quick access while using the command line interface to execute an image recognition scan.

Summary

The provided images and data are taken from our adversarial testing and learning experiment. Training consisted of 39 pictures in training set 1. Images 1 & 2 are without Reflectacles, while images 3 through 6 use infrared to capture the Reflectacles’ capabilities. Reflectacles is the opponent here and the performance scores from both IBM Watson Visual Analytics and Amazon Rekognition are shown underneath each image. The IBM Watson tool ends up generating an average visual recognition confidence percentage of 0.78 corresponding to the Reflectacles based test images in training set 1. The Amazon Rekognition tool ends up being rendered mostly ineffective by the Reflectacles, as indicated in the results. This overall illustrates how Reflectacles can assist in evaluating, analyzing and comparing the performances of these tools.

Results

The Anti-Surveillance Wearable Glasses (Reflectacles has been used as an example Anti-Surveillance glasses in this project for experimental purposes)

Adversarial Training + Testing Data & Outcomes

Conclusion

To our knowledge, this is the first time a research experiment has been conducted using Reflectacles against IBM Watson and Amazon Rekognition. There is novelty in our proposed approach of utilizing Reflectacles as a potential adversary for testing and training with state of art computer vision algorithms and machine learning techniques. The obtained qualitative results indicate that Reflectacles can successfully act as aworthy opponent, and inhibit the performances of visual recognition tools that apply facial detection and recognition. The given block diagram represents our proposed model of adversarial testing and training based learning with anti-surveillance wearable devices and visual recognition based machine learning techniques. Future work will focus on training with Reflectacles.

References