Radiance

Security and Privacy Concerns of Facial Recognition Technology

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By
Ethan Cha

October 10, 2023

Technical Team Members:
Kousuke Tapia
Minsol Kim
Joshua Yu
Kiki Wong

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Joshua Earle, Department of Engineering and Society

Adam Barnes, Department of Electrical and Computer Engineering

Introduction

Among the common forms of identification, biometrics is generally accepted as a reliable identification system. Some common forms of biometrics used in criminal identification are fingerprint analysis, retina scans, and facial recognition technology. Facial recognition technology, in particular, has gained popularity beyond just criminal identification. From getting into our phones, bank accounts, to social media, our society has become accustomed to using some sort of facial identification system to authenticate access to our accounts. That being said, this technology is far from perfect. Not only is it one of the most unreliable biometrics, but it also comes with negatives such as privacy concerns and racial bias. How do these negatives affect facial recognition technology in the context of criminal justice, a field in which this technology is prevalent? How do the pros weigh against its cons? Is it too early to fully utilize this technology?

Facial recognition technology represents a more specific application within the broader field of image processing. Our technical project revolves around image processing to identify living objects within a camera feed. Our technical project is a security system that is able to monitor an area by shining a spotlight on any living object. We accomplish this by doing image processing on a thermal camera feed and accordingly turn on the light and point it at the target. This product would be able to notify the homeowner if any unauthorized humans or animals are in the surveillance area and deter them away from the property.

My prospectus will go into more detail of both the technical project and the STS project and at the end will cover methods of research and potential use of articles in the final research paper.

Technical Project

Radiance is a surveillance and intruder detection system that uses thermal imaging to detect any life within a designated perimeter, automatically illuminating the entity and tracking its position as it moves. A Raspberry Pi will analyze images from the thermal camera in real-time, identifying potential intruders using their heat signatures and silhouettes. This software analysis will then serve as input to the microcontroller, which will precisely drive motors to orient the system to point at the identified intruder. The light will receive a signal from the microcontroller as soon as an intruder is within the illumination zone. The system will also include a web server which will allow users to view the thermal feed overlayed with information from the analysis, as well as be able to manually control the system to illuminate any points of interest inside the perimeter. This project is an example of computer vision and autonomous robotics in security, a field that has expanded into the consumer market from military technology.

STS Project

The main technology my STS project revolves around is facial recognition technology which has raised some eyebrows when it comes to privacy. The big privacy questions are: How is facial recognition technology being used in public areas with cameras? Are my personal photos safe and private? Who has access to data involving things such as Apple's FaceID? And many others. It has been reported that Federal agencies use facial recognition technology mostly for criminal investigations but the tracking of this use is not required. This means that government agencies can run facial recognition software on pretty much anyone who is around technology without our consent. "Police use face recognition to compare suspects' photos to mugshots and driver's license images; it is estimated that almost half of American adults – over

117 million people, as of 2016 – have photos within a facial recognition network used by law enforcement. This participation occurs without consent, or even awareness, and is bolstered by a lack of legislative oversight." (Najibi, 2020)

In order to train image processing software, you must feed in large sets of data that inadvertently sets biases. One prominent example of this is the censorship found in AI chat tools in China. The censorship in China reflected in these machine-learning tools, finding words such as "surveillance" and "CCP" as positive words and associated words such as "democracy" with negative words such as "chaos" (Cook, 2023). Similarly, this kind of bias can be seen in facial recognition software as well through the datasets used to train them. In order to train an image processing program to recognize different objects, the developer needs to label the image and in order for the machine to understand what it is. This is where politics and bias comes into play. After training, "a photograph of a woman smiling in a bikini is labeled a 'slattern, slut, slovenly woman, trollop.' A young man drinking beer is categorized as an 'alcoholic, alky, dipsomaniac, boozer, lush, soaker, souse.' A child wearing sunglasses is classified as a 'failure, loser, non-starter, unsuccessful person.'"(Crawford & Paglen, 2021) "Consciously or not, deliberately or inadvertently, societies choose structures for technologies that influence how people are going to work, communicate, travel, consume, and so forth over a very long time." (Winner, 1980, page 127) In some cases biases can be made intentional for example in the criminal investigation sector to be more biased towards black Americans while others can be made unintentionally by simply reflecting the general sentiment of the public that could be inherently racist or sexist unconsciously as well.

With all this in mind some major questions that I will answer in this project are: How do these negatives affect facial recognition technology in the context of criminal justice, a field in

which this technology is prevalent? How do the pros weigh against its cons? Is it too early to fully utilize this technology due to issues of privacy and consent?

The two most obvious social groups involved in this research are the general public and the government. The main questions deal with the privacy of citizens and the role of the government when it comes to the utilization of this technology as well as the regulation of it. A lesser involved social group that might be considered is the developers of this technology. The question of if it's too early to utilize this technology can be classified as an ethical issue that developers should consider as they write and publish this code.

As for the methods and frameworks, I will primarily be finding, reading, and synthesizing previous literature in order to get a better understanding of my topic as well as be able to answer my questions. I will be conducting a race studies analysis because it makes sense in the context of facial recognition technology in criminal justice. There are multiple cases where the use of facial recognition technology as sole evidence in the conviction of a black person has led to wrongful arrests such as the example of Nijeer Parks in 2019 (Sarlin, 2021). This is due to the fact that facial recognition softwares are “more prone to error when trying to match the faces of darker skinned people” (Sarlin, 2021), especially women who had error rates 34% higher than white males (Najibi, 2020). There are more resources regarding racial injustice within this specific field of criminal justice and facial recognition, and I plan on diving deeper into this topic.

Key Texts

The main method in my research involves identifying and examining recent literature that addresses the research questions. The first article I have chosen is titled, “Public Attitudes Towards the Use of Automatic Facial Recognition Technology in Criminal Justice Systems

Around the World" and, like the title suggests, is about how different countries feel about the use of this technology. For example, US citizens were more accepting of the use of automatic facial recognition (AFR) technology in tracking citizens, use by private companies, and less accepting of use by police than UK and Australian citizens. This article also goes into their personal recommendations when it comes to AFR including the practice of being more transparent about the accuracy and data protection as well as setting legal boundaries in the context of criminal justice. This article is related to the STS topic because it touches on the idea of what it would take to use this technology ethically in terms of citizens privacy and will help answer the question of if it is too early to utilize this technology if proper boundaries are not set yet.

The second article I have chosen is titled, "Racial Discrimination in Face Recognition Technology" which is a short article published to Harvard. It points out bias and inaccuracy when it comes to darker skin-toned people and the discrimination that comes when this technology is used by law enforcement. Like the first article, this one also gives suggestions regarding the improvement of facial recognition technology. It talks about the improvement from both the algorithmic as well as the legislative perspective. This article will help answer questions about the STS topic but it also helps raise new questions and avenues of research that will be needed to complete this project.

The third article I have chosen is titled, "The Inconsentability of Facial Surveillance" and builds upon a previous piece of literature by Nancy Kim "Consentability: Consent and Its Limits" and expands upon her argument to conclude that facial recognition technology has a "fatal consent problem". In other words, valid consent cannot be given for this technology. The authors make a strong statement that this technology should be banned until there is proper

regulation for it. The article helps question whether facial recognition technology is ready to be used at all.

The fourth article I have chosen is titled, “Facial Recognition and the Future of Privacy: I always feel like … somebody’s watching me” which expresses concern for the privacy of citizens when it comes to facial recognition and monitorization. Similar to how the industrial revolution required heavy regulation to protect human rights, technology such as this should be regulated to avoid abuse of power. This article as well argues for the need for more boundaries especially as artificial intelligence becomes more powerful.

Works Cited

Brenda Leong (2019), Facial recognition and the future of privacy: I always feel like … somebody's watching me, Bulletin of the Atomic Scientists, 75(3), 109-115. DOI: 10.1080/00963402.2019.1604886

Cook, S. (2023, February 27). China's Censors Could Shape the Future of AI-Generated Content. The Japan Times. https://www.japantimes.co.jp/opinion/2023/02/27/commentary/world-commentary/china-artificial-intelligence/

Crawford, K., & Paglen, T. (2021). Excavating AI: The Politics of Images in Machine Learning Training Sets. Ai & Society. https://link.springer.com/article/10.1007/s00146-021-01162-8

Najibi, A. (2020, October 26). Racial Discrimination in Face Recognition Technology. Science in the News. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Ritchie, K. L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., et al. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. PLoS ONE, 16(10), e0258241. https://doi.org/10.1371/journal.pone.0258241

Sage, K., & Young, S. (1999). Security applications of computer vision. IEEE Aerospace and Electronic Systems Magazine, 14(4), 19–29.

Sarlin, J. (2021, April 29), A false facial recognition match sent this innocent black man to jail | CNN business. CNN. https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html

Selinger, E., & Hartzog, W. (2020). The inconsentability of facial surveillance. Loyola Law Review, 66(1), 33-54.

Winner, L. (1980). Do Artifacts Have Politics? Daedalus, 109(1), 121–136.