Undergraduate Thesis Prospectus

Access security using facial recognition AI

(technical research project in Computer Science)

Face recognition: a compromise between security and convenience

(sociotechnical research project)

by Nikita Semichev

May 14, 2021

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.
Nikita Semichev

Technical advisor: Hongning Wang

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can building access control reliably but unintrusively (respecting privacy) limit access to authorized persons?

Building owners and tenants need secure buildings. The terrorist attacks in the U.S. of September 11, 2001, led many owners and tenants to tighten access control. Since then, more buildings have had access control 24 hours a day, seven days a week (Craighead, 2011). Automated access control systems can be much less expensive than human guards (Hager, 1996). Access control systems can improve security and reduce costs. However, such systems are subject to discriminatory biases. Face recognition algorithms use training data that mostly consists of images with white faces, so the results are not accurate for all skin colors (Silva & Kenney, 2018). The identification accuracy of faces with dark skin is very low compared to faces with lighter skin. Facial data can also be collected and used for racial or religious discrimination (Cataleta, 2020). Malicious actors can use exploit AI algorithms' vulnerabilities to cause biases (Scharre et al., 2018). In a badly designed AI access control system, a person can show a picture of a building employee and gain access. Effective access control systems optimally balance security and privacy.

Access security using facial recognition AI

How can cameras with face recognition technology be used for managing entrances in public and private buildings?

The goal of the project is to use a collection of facial images to properly match a person's face to the image in the collection with facial recognition and image similarity algorithms. I am in the CS department and will work on an independent project, with Aaron Bloomfield as my advisor.

This project will be useful for monitoring anyone entering a building using face recognition to decide whether access is allowed. The main goal of the project is to deliver a system that uses facial recognition technology to find similarity between faces in the context of access control. There are several companies such as Microsoft that use a similar approach for monitoring employees entering the work buildings. Recently, many AI focused companies have developed facial recognition technology that can be used for access control systems. AI developers significantly improved the performance of image similarity algorithms, reducing the search time for a matching image in a database (Feldstein, 2019). Current facial recognition access control systems can be improved and applied to other domains. The domain of the system will determine the tradeoff between accuracy and speed.

Open source facial recognition AI libraries will be used to analyze facial data, and determine image similarity. To test the system, volunteers will be asked to provide a photo that could be saved in a database, and then to provide another photo to be tested for similarity within the first set of images in the database. The project will use manually taken images. If the project is completed before the deadline, several improvements could be made to the system. A live camera functionality could be added to make the system more automated. The system could also be applied to areas other than access control, such as a public database for finding lost pets.

Face recognition: a compromise between security and convenience

In the U.S. since 2010, how have social groups competed to draw the line between necessary building security and invasive building security?

Facial recognition surveillance is proliferating worldwide (Feldstein, 2019). As components of access control, facial recognition systems can improve security. Such systems, however, can be subject to discriminatory biases and can compromise privacy. Because AI systems are subject to bias, they cannot be trusted unconditionally (Scharre et al., 2018). AI systems incorrectly match employees with darker skin more often than other groups (Cataleta, 2020). Social groups compete to draw the line between necessary security and invasions of privacy.

Companies and countries started to use facial recognition for surveillance and security (Ünver, 2018). As facial recognition capacities develop, authoritarian governments may abuse them at the expense of civil liberties (Sherman, 2019). Companies could be selling facial data of employees to the government. This could lead to increased surveillance and compromise the privacy of regular citizens. AI facial recognition technologies have become very accurate for specific datasets (Feldstein, 2019). Diverse datasets should be used to reduce racial bias in facial recognition algorithms (Cataleta, 2020). In a similar problem, parents monitoring online activity of teens, increased surveillance resulted in a change in behaviour and world perception (Youn, 2008). Privacy concerns can influence the behavior of employees and other participant groups.

Participants include security companies that serve building owners and tenants. Some sell facial recognition and fingerprint systems. FaceKey serves clients who want to "control access, shelter assets, prevent labor fraud and provide a safe workplace" (FaceKey, 2020).

But many privacy advocates oppose facial recognition, contending it is subject to discriminatory bias and invades privacy. They claim that facial recognition AI “misidentifies people of color, women, and children” and puts “vulnerable people at greater risk of systemic abuse” (Fight for the Future, 2020). They are also concerned that collected information is “an easy target for identity thieves.”

Some large tech vendors, including Microsoft, position themselves as responsible companies that take privacy seriously (Smith, 2018). Microsoft contends that governments and the tech sector “play a vital role” to ensure that facial recognition technology “creates societal benefits while curbing the risk of abuse.” Some cities regulate surveillance systems. A New York City Council member stated that building owners’ use of facial recognition technology “poses a serious threat to the rights of tenants,” specifically, to “lower-income communities of color” (Lander, 2019).

References

Cataleta, M. (2020). Humane Artificial Intelligence: The Fragility of Human Rights Facing AI. *East-West Center*. JSTOR.

Craighead, G. (2011). Impacts on Building Security Measures. *CTBUH Journal*, (3), 42-43. JSTOR.

FaceKey (2020). Facial Recognition Access Control for biometric access control solutions. https://www.facekey.com/solutions/face-or-fingerprint-recognition-systems/

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment for International Peace* (pp. 16-21, Rep.). JSTOR.

Fight for the Future (n. d.). Ban Facial Recognition. https://www.banfacialrecognition.com/

Hager, R. (1996). Building Security: Are You Overlooking Something? *The Military Engineer, 88*(581), 25-27. JSTOR.

Lander, B. (2019). New City Council legislation would protect tenants from facial recognition & “smart” key surveillance. https://council.nyc.gov/brad-lander/2019/10/07/new-city-council-legislation-would-protect-tenants-from-facial-recognition-smart-key-surveillance/

Scharre et al. (2018). Artificial Intelligence: What Every Policymaker Needs to Know. *Center for a New American Security* (pp. 11-16, Rep.). JSTOR.

Sherman, J. (2019). Essay: Reframing the U.S.-China AI “Arms Race”: Why This Framing is Not Only Wrong, But Dangerous for American Policymaking. *New America* (pp. 12-17, Rep.). JSTOR.

Silva, S., & Kenney, M. (2018). Algorithms, Platforms, and Ethnic Bias: An Integrative Essay. *Phylon* (1960-), 55(1 & 2), 9-37. JSTOR.

Smith, B. (2018). Facial recognition: It's time for action. https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

Ünver, H. Akın. (2018). Politics of Digital Surveillance, National Security and Privacy. *Centre for Economics and Foreign Policy Studies*. JSTOR.

Youn, S. (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. *The Journal of Consumer Affairs*, 42(3), 362-388. JSTOR.