Katherine Stanton

ITAI 1378- Intro to Computer Vision

Professor Patricia McManus

08-25-2024

Lab 01- Exploring Real-World Applications of Computer Vision

Facial recognition is a controversial branch of computer vision technology where, using biometrics and AI, computer software is fed data in the form of images of human faces with the goal of being able to identify an individual based on their face alone. This technology serves many purposes, according to Clare Stouffer for Norton blog, “companies can use it for marketing, sending targeted ads to consumers. Law enforcement agencies use it to identify suspects or track down missing persons. And tech companies use it to allow consumers to unlock their devices easily”. [1]

Stouffer succinctly lays out the process of facial recognition; first, “software analyzes photos or videos of a face.” Second, “software creates a map of a person’s facial features.” Then, “facial recognition systems compare the individual’s facial signature to its database.” Lastly, “the facial recognition system determines whether or not the facial signature is a match to anything in its database.” [1] AWS states that “human face recognition systems use unique mathematical patterns to store biometric data”, then “using complex artificial intelligence (AI) technology, computer vision automates extraction, analysis, classification, and understanding of useful information from image data. The image data takes many forms… single images, video sequences, views from multiple cameras, and three-dimensional data” [2]

The ethical dilemmas of facial recognition are at the forefront of its status today. According to Jay Peters for The Verge, in a letter to Congress in June 2020, IBM publicly stated they would no longer “offer general purpose facial recognition or analysis software” and “will also no longer develop or research the technology.” [3] Privacy is the main concern surrounding this technology, like any other biometric data, it has the potential to be abused by government agencies or private companies. Despite this, AWS lists facial recognition’s benefits being efficient security (in comparison to other biometric authentication methods), improved accuracy in identifying individuals, and easier integration with most security software. [2]

Despite companies like IBM ceasing to work with facial recognition altogether, the technology is still advancing and being applied to new and creative applications the world over. Lystloc names several of these future and on-the-precipice applications including, using facial recognition to verify someone’s age or in lie detection based on facial cues known to be red flags for lying. Using AI technology, facial recognition systems could potentially gain insight and adjust to diverse scenarios, increasing accuracy. It could also help to prevent hacking as more websites and apps are requiring facial recognition as a means of access. [4] The real privacy concerns that could result in unregulated use of this technology in the future could have an negative impact on the individual which far outweigh the convenience or ease of its use.

Sources

1.) https://us.norton.com/blog/iot/how-facial-recognition-software-works

2.) https://aws.amazon.com/what-is/facial-recognition/

3.) https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software

4.) https://www.lystloc.com/blog/7-new-facial-recognition-technology-trends-to-boom-in-the-future/