Facial Recognition for Deepfake Detection

Firaol Desta and Emily J Brown
Johns Hopkins University, Applied Physics Lab, USA
Email: firaold24@gmail.com and emily.brown@jhuapl.edu

2022 IEEE Integrated STEM Education Conference (ISEC) | 978-1-6654-8429-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISEC54952.2022.10025295

Abstract

Facial recognition is a tool utilized by social media companies to assist in tagging people in photos. Facial recognition's ability to detect modified images is useful for these companies to prevent privacy violations, or even online impersonation. For example, deepfakes are very realistic pictures and/or videos that are created by pasting a face onto someone else's body, which are of concern to social media companies. Deepfakes are very dangerous media that could be used to hijack someone else's identity for malicious purposes. In order to prevent this, facial recognition must be accurate in recognizing modified faces. By using the Python facial recognition library, we researched if facial recognition can be used to recognize when an image has been modified. To start off, we first checked if facial recognition can identify an alternate photo of someone, like if they are in a different position, wearing sunglasses, or of a different age. We did this by creating a folder of known celebrity faces, and an unknown folder with the alternate photos. Once we could do it manually, we automated the code to cycle through a folder of unknown images and compare each of them to a known target image, and count how many times a match was found in the folder. We are ultimately trying to use this library to check the accuracy of facial recognition in recognizing original and modified faces. Understanding the current effectiveness of facial recognition technologies against modified faces will enable us to improve these technologies, and in turn allow us to defend better against deepfakes, and even greater threats against privacy and security.

978-1-6654-8429-9/22/$31.00 ©2022 IEEE