TRANSFORMATION TOLERANCE OF MACHINE-BASED FACE RECOGNITION SYSTEMS

Kyle Keane, Ashika Verma, Alyssa Unell, Anna Musser & Pawan Sinha
The MIT Quest for Intelligence Massachusetts Institute of Technology Cambridge, MA 02139, USA
{kkeane,ashikav,aunell}@mit.edu

ABSTRACT

Face recognition is widely acknowledged to be a very complex vision task for both humans and computers. Remarkably, humans excel at this task, robustly recognizing individual faces in highly dynamic environments with few examples of faces. Research has shown this robustness quantitatively by testing people's ability to recognize celebrity faces under dramatic degradations of images such as blur, grayscale, and pseudocolor as a result of shifting an image's hue. We evaluate the performance and robustness of a current state-of-the-art facial recognition architecture as it "recognizes" faces in a dataset which have undergone naturalistic image degradations. We qualitatively compare our results to studies that measured the human ability to retain accuracy in facial recognition under these same conditions. We use a CNN trained on Augmented CASIA-WebFace Data and test the quality of the "identity" clustering of the net-encoded faces in the resulting encoded vector-space. To create our undegraded dataset, we took the CelebAMask-HQ dataset and downselected the identities with 19 to 25 front facing images. We then degrade our base dataset by applying filters (grayscale, pseudocolor, and full color). For each filter, we apply a Gaussian blur to establish how the network performs at different blur levels for each of the filters. In the study, we found a statistically significant trend downwards showing that as blur increases, the performance of the network declines under all the filters, with color outperforming hue shift which in turn outperformed grayscale. These results are different from human data which suggests that humans perform optimally with data that has undergone a hueshift, and then original color and grayscale, respectively. In the future we want to explore various network architectures' robustness in response to additional filters and augmentations. Facial recognition is depended upon in numerous industries, from criminal justice to security, and as such it is imperative that work is done to identify the limitations of robustness of commonly used networks.