Introduction to Deep Fake Media

Abstract:

Deep fake media is a growing concern due to the potential abuse directed towards individual, organizations, and governments. Attackers typically craft deep fake media by altering existing content to give the appearance that someone is saying or doing something which they did not actually do. For example, a video of a politician can be modified so that their lips and face are changed to match speech that was generated by techniques such as speech editing or neural text-to-speech. The recent introduction of generative adversarial networks (GANs) has the potential to significantly simplify the production of deep fake videos. In this talk, we provide a background of deep fakes and an overview of some of the generation techniques and proposed detection methods.