Face Forgery Detection

Problem:

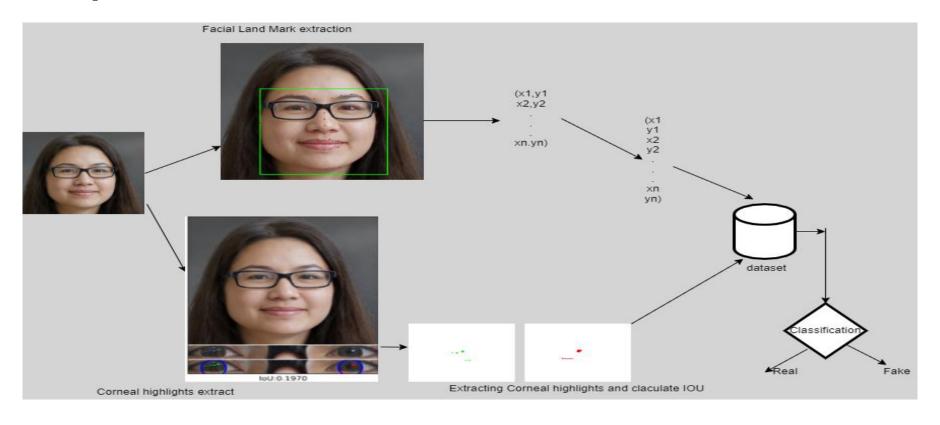
 Face forgery detection becomes a difficult task to find the authenticity of an image with the naked eye. Images synthesized by powerful generative adversarial network (GAN) based methods have drawn moral and privacy concerns.

Differentiating GAN generated realistic Human Faces from Real Human Faces
Based on physical and physiological inconsistencies.

Proposed method:

GAN-synthesized images can be exposed using the locations of the facial landmark points and with the inconsistent corneal specular highlights between two eyes. The inconsistency is caused by the lack of physical/physiological constraints in the GAN models. Such artifacts exist widely in high-quality GAN synthesized faces which is a vulnerability of GAN images that we can use to differentiate a real image from GAN synthesized one.

Proposed Method:



Conclusion:

Deep Learning-based methods achieved impressive performance on GAN-face detection. However, it is difficult to explain or interpret the decision process of the learned model as a black box. Nonetheless, fake face detection in the real-world favors explainability, alongside from the overall accuracy. Particularly, people do care more for use cases such as "This picture looks like someone I know, and if the AI algorithm tells it is fake or real, then what is the reasoning and should I trust?"