Machine Learning II Project Proposal

FACE GENERATOR USING GENERATIVE ADVERSARIAL NETWORKS

GROUP 5 MEMBERS

Renzo Castagnino

Aira Domingo

PROBLEM

The ability to manipulate and recreate realistic images at scale has had a big impact on how modern societies perceive the truth about certain facts. Fake visuals is a trending topic in AI and has allowed the creation of fake news, propaganda, and other persuasive information .

We've selected this topic because most people still don't understand how modern machine-learning techniques can be used to synthetize realistic images; and thus we would like to create awareness in this area. Our main goal is to create fake faces that are unrecognizable as fake to the human eye.

In order to do this, the network must be able to distinguish between a real human face versus a fake generated face. This will allow the generator to create realistic faces as defects are caught by a discriminator.

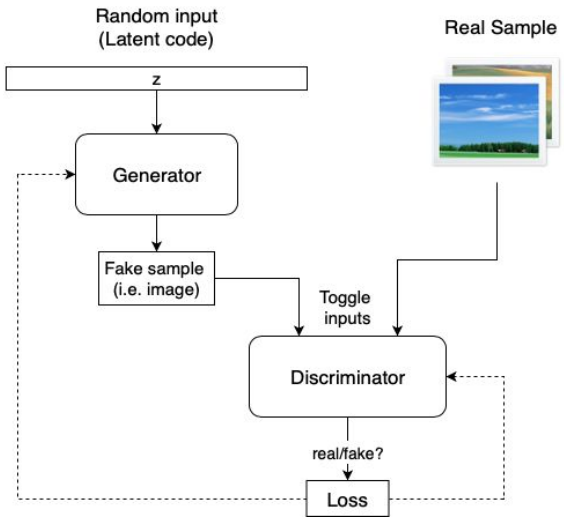
DATASET

The dataset selected from VGGFace2, a large-scale collection of pictures with more than 3.3 million faces. The characteristic of the dataset are as follows:

The dataset can be used to train and test our model. Furthermore, we're also considering a possible merge with another dataset that contains more images with similar characteristics; but this point is still under review.

DEEP NETWORK

For this project we will use Deep Generative Adversarial Networks (DGANs), together with CNN and VGG-Face net. We expect to use these networks as a base, but to increase the capacity of our model we will have to customize it.



FRAMEWORK

For this project, we will implement the network by using Tensorflow and Keras since the Keras API is integrated into Tensorflow. This will allow us to use the Keras API to build the network. Keras is a high-level framework that is modular and easy to customize. Working with Keras in the Tensorflow integration gives us the flexibility to use Tensorflow when needed.

REFERENCE MATERIALS

http://cs231n.stanford.edu/reports/2016/pdfs/006_Report.pdf

http://www.robots.ox.ac.uk/~vgg/data/vgg_face2/

https://www.lyrn.ai/2018/12/26/a-style-based-generator-architecture-for-generative-adversarial-networks/?fbclid=IwAR0bngOpEfmesyWSOC4Y83ctJVwrdltZxCFN2Km0YJiAOL5qXFNGazLZnsE

http://vis-www.cs.umass.edu/lfw/

https://www.robots.ox.ac.uk/~vgg/publications/2015/Parkhi15/parkhi15.pdf

https://arxiv.org/pdf/1511.06434.pdf

https://www.kdnuggets.com/2020/03/generate-realistic-human-face-using-gan.html

https://arxiv.org/pdf/1901.08971.pdf

https://arxiv.org/pdf/1909.12962.pdf

PERFORMANCE METRIC

We will use accuracy to measure the performance of the network to see if the discriminator model can accurately identify which faces are real and which faces were created by the generator. To optimize the model, we will use binary cross entropy as the loss function.

SCHEDULE

April 6 (Monday): Finalize dataset selection.

April 7 (Tuesday): Submit project proposal.

April 12 (Sunday): Set up Github, cloud, folder structure, collaborative environment.

April 17 (Friday): Complete data cleaning, understanding & preprocessing.

April 19 (Sunday): Model identification and network architecture.

April 25 (Saturday): Finalize model. Write the report.

April 27 (Tuesday): Presentation and Submission.