How did you hear about the program?

Referral

Project name

Improving the accuracy of deepfake detection using convolutional neural networks

Project start date

20/01/2020

Proposal

Progress in synthetic image generation and manipulation has come to a point that its societal impact is undeniable. The most realistic techniques involve videos and images of which it is nearly impossible for humans to distinguish real from fake. Such techniques generally involve Generate Adversarial Nets and are included in the umbrella-term “Deepfakes”. Deepfakes will not disappear any time soon, and their impact is already being felt on a global scale. It is essential to develop countermeasures to protect individuals and organisations from the harmful applications of deepfakes. Similar to the Deepfake Detection Challenge, we intend to create a convolutional neural network that outperforms other networks in determining image authenticity. Training well-performing neural networks for this task is computationally extremely intensive, and thus we require access to multiple GPUs in order to train accurate neural networks. We aim to use AI Platform, and more specifically Deep Learning VM Image, AI Platform Training, and AI Platform Prediction to aid our analysis.

At this point we have extracted all data from the FaceForensics++ GitHub repository, and preprocessed them. We are currently using Keras, with auxiliary functions that are already in place in Google Colab. The Tesla K80 GPUs in Google Colab, however, do not offer us adequate computational power. To improve upon current architectures, instead of looking at frames, we intend to look at videos in their entirety, and for this we will look into multi instance learning which utilises set functions. We plan to train our network using 4 Tesla P100 GPUs in parallel, which should be sufficient to complete our research within the required timeframe (by August 2020).

Ideally, we would create a network that would work well with deepfakes but generalises well to other GANs. We intend to dive deep into potential architectures from the start of June onwards. By August we intend to have created networks that achieve a better accuracy than the state-of-the-art technologies.

How GCP can support your research in the future:

(?)

Field of research

Computer and information sciences

How do you intend to apply awarded cloud credits?

Evaluation/Comparison?

Does your research project have an external funding source?

No

Have you used cloud infrastructure for you research before?

Yes

Have you used GCP before?

Yes

Please provide information on how you intend to fund your project after your credit expires in 1 year.

Our project finishes in August 2020.