

Week 5&6: Summer Internship

23 June 2021- 6 July 2021

Tasks

The main tasks in week 5 were as follows:

- Integrating all the methods in same code for automating and hence better testing (code oriented).
- Compile whole tool and to get detailed data.
- Test the code against various inputs.
- Adding code for other cases also like age, beard/no-beard etc.

Integrating the methods

Taking the directory names and method number as input from command line and calling corresponding functions.

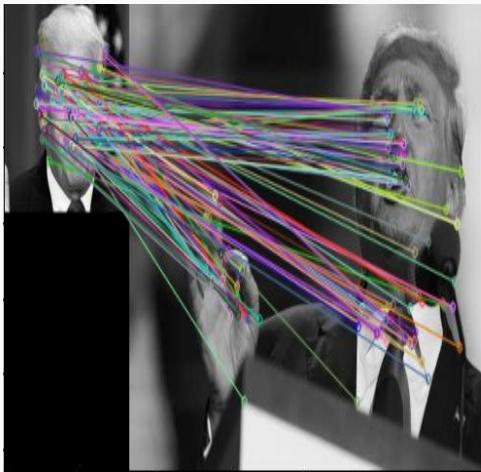
Also ensuring all the exception cases and adding comments for the user.

Also did some optimisations that were possible as we were calling the method multiple times in a loop.

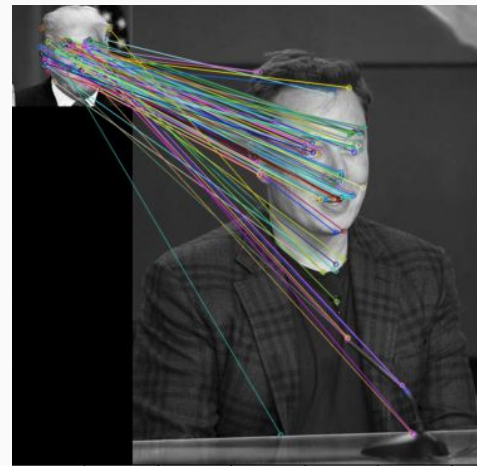
Test-1 (Method1)



Test image



Original-1 (wrong)
Similarity score: 116/260
Score of correct image: 95/260

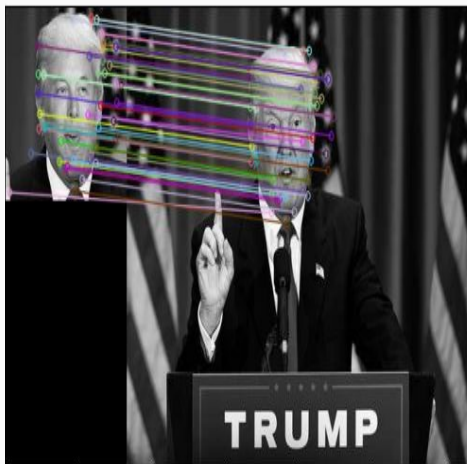


Original-2 (wrong)
Similarity score: 116/260
Score of correct image: 105/260

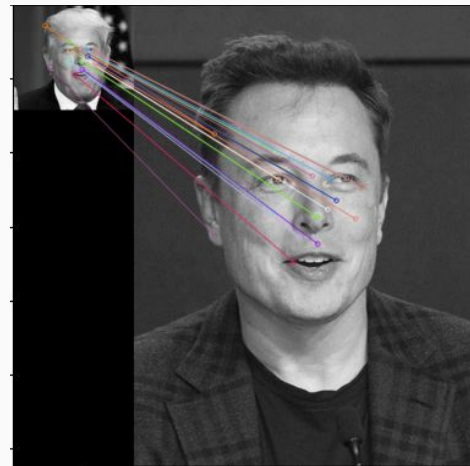
Test-1 (Method2)



Test image



Original-1 (correct)
Similarity score: 49/99

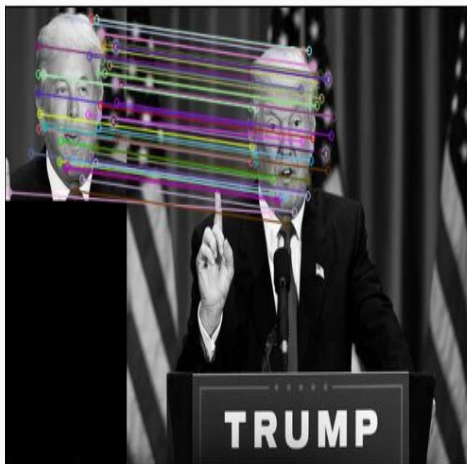


Original-2 (correct)
Similarity score: 18/99

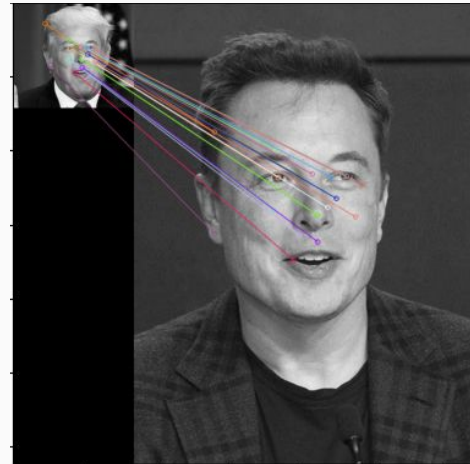
Test-1 (Method3)



Test image



Original-1 (correct)
Similarity score: 149/198

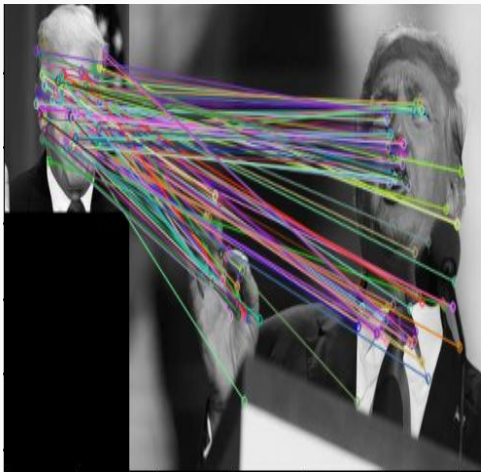


Original-2 (correct)
Similarity score: 116/198

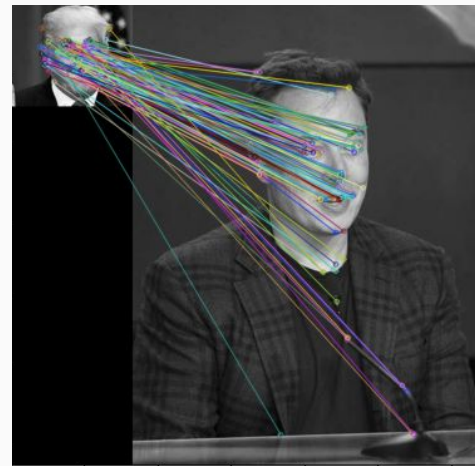
Test-2 (Method1)



Test image



Original-1 (wrong)
Similarity score: 147/500
Score of correct image: 118/500

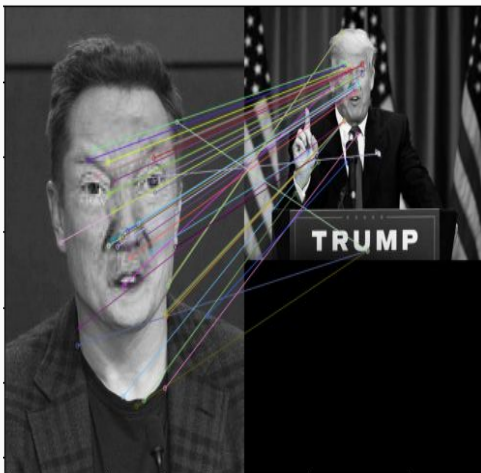


Original-2 (correct)
Similarity score: 155/500

Test-2 (Method2)



Test image



Original-1 (correct)
Similarity score: 42/443



Original-2 (correct)
Similarity score: 184/443

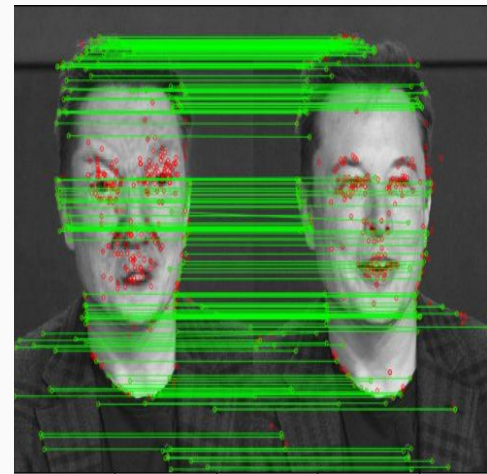
Test-2 (Method3)



Test image



Original-1 (correct)
Similarity score: 479/886



Original-2 (correct)
Similarity score: 622/886

Note

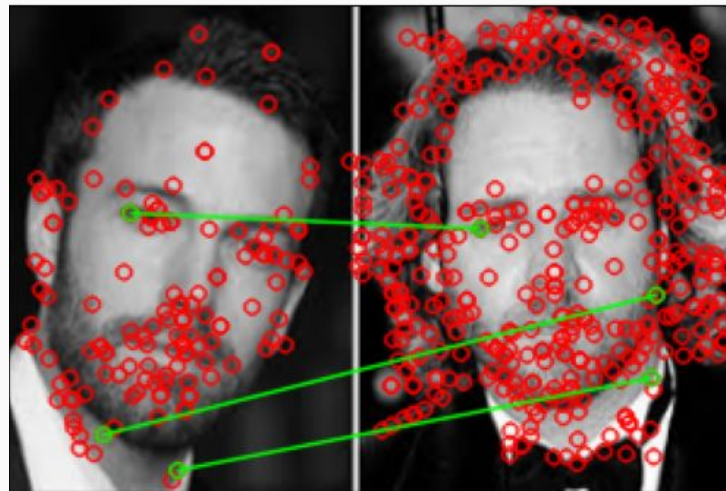
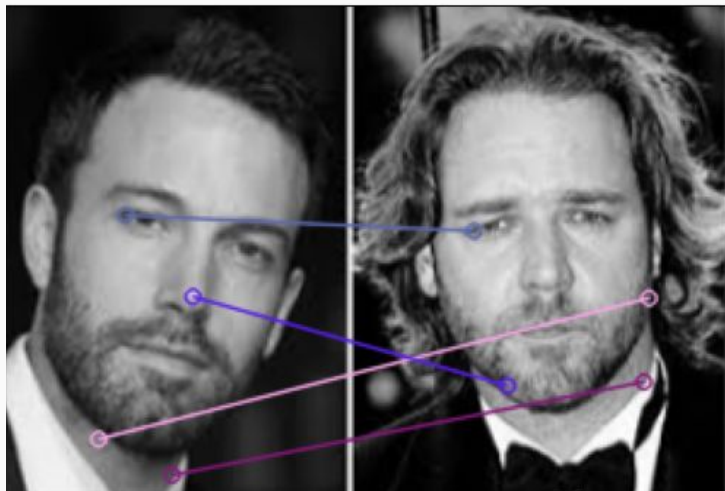
When face of person B is put over image of person A, then major features are corresponding to image of person hence the similarity score corresponding to image of person A is higher (refer to slide 5 and 8 where person A refers to Donald Trump and Elon Musk respectively).

When features other than face (stage, dress and miscellaneous objects) are significant in the image, method 2 and method 3 gives greater similarity corresponding to those features and hence correct output.

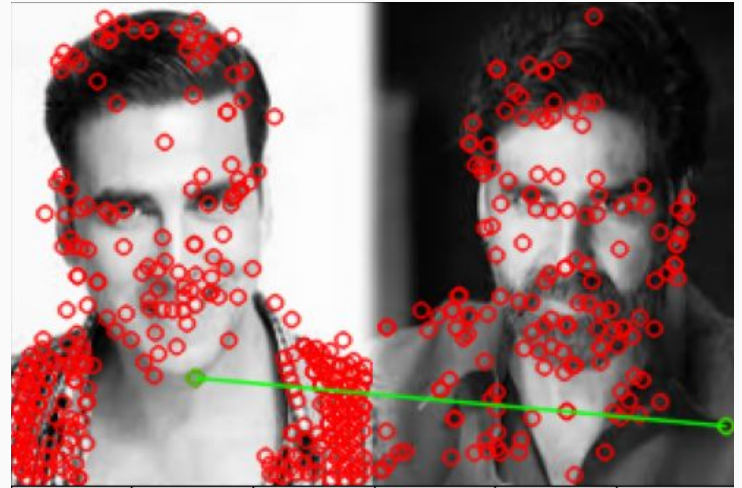
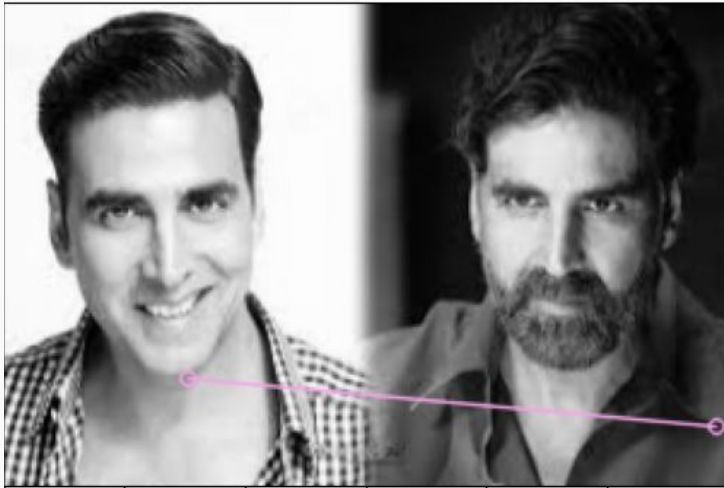
Beard output-1



Beard output-2



Beard output-3



Note -2

Between method 2 and method 3, method 2 focuses more on explicit and distinct features in the image like facial features.

Method 3 on the other hand focuses more on the comparison of outlining structure and skeleton of the features (outlined shape and size).

Summary

- Method 2 and method 3 takes around 16-18 seconds on average to process the dataset of size 300 while method 1 takes nearly 3 seconds.
- Method 1 has lower accuracy than method 2 and method 3.
- Images that compare beard and no beard showed mixed output. In some cases, other features like eyes and nose came out properly while in some cases the features are incorrectly marked.

Tasks

The main tasks in week 6 are as follows:

- Generating deep fakes that are not detectable with naked eye (kaggle like examples).
- Testing the algorithm against the generated deep fakes.
- Look for deep learning algorithms to generate deep fakes by giving custom input images.

Generating deep fakes

1. Used pre-trained model by stylegan for faces and provided seed images to get the corresponding output images.
2. Created a google colab notebook for the same.

Link: https://colab.research.google.com/drive/1z8Q7qWbcWA-SvtfzX_sEqq7agyXpNDPE?usp=sharing

Seed images



Output images



Testing the algorithm

The seed and output were not matching since one output took features (learning by the model) from all the seed images.

Some features match out but overall the image does not seem to be related at all.

Images with people of different age and gender are paired with maximum similarity score.

Algorithm output - 1



Algorithm output -2



Deep learning models for custom deep fake

The model is hungry for images and needs to take a lot of images as input. We could include out 2-3 images in the image dataset but the output would not resemble very much with the original image (as seen earlier).

Google colab notebook link for one such

training:https://colab.research.google.com/drive/1sAg9vBwYbgtxJltg_XHScSSjFD_P6UG2O?usp=sharing

Source:https://github.com/jeffheaton/present/blob/master/youtube/gan/colab_gan_train.ipynb

Minutes of the meeting - 1

1. Deep fakes are not mainly used in profile cloning. Hence, our code should be targeting morphed/photoshopped images.
2. We thus need to explore some morphing techniques for generating images for profile cloning.
3. We also have to establish that morphing and photoshopping are relevant methods and widely used in profile cloning techniques.
4. We will keep deep fakes into consideration as additional method of generating fake images.

Minutes of the meeting - 2

Our algorithm averages out the similarity score over whole image. If 2-3 features are taken from the same image then the similarity score should be higher than the averaged out score (which is given right now).

The weights are currently uniformly distributed. We could use methods like power law to normalise the score.

We would have to look for similarity score corresponding to each feature and return a list of score to then apply techniques for deciding the weights.

Minutes of the meeting - 3

Overall, the main upcoming tasks are as follows:

1. Modify the code to incorporate the feature level similarity scoring.
2. We have to establish relevance of morphing/photoshopping.
3. Test our algorithm on the outputs of those images.