

Week 1&2: Summer Internship

26 May 2021- 8 June 2021

26 May - 27 May

First official meeting after the commencement of internship (26 May).

Discussed major project ideas and overview of the overall workflow.

Picked up the “Deep Fake Analysis and Detection” as the topic of interest (27 May).

Read about the topic and got familiar with the terms and tools.

Also listed down some of the popular image search engines and other deep fake detection tools.

28 May - 30 May

Setting up of the machine for generation of deepfakes along with exploring the tools available (28 May).

Got into learning how deep fakes are made and tried to make some deep fake videos (29 May).

Created some more deep fake images and listed some more advanced level deep fake detection tools and search engines.

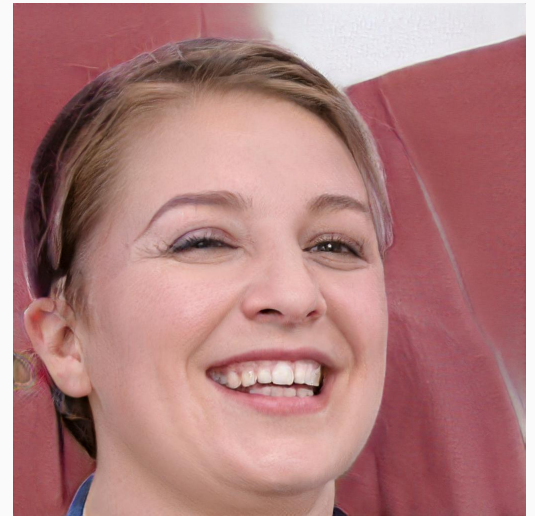
Deep fake images and videos



Deep fake of Elon Musk
singing Memories



Easy to detect deep fake of
Donald Trump and Elon Musk



Advanced deep fake.
Source: kaggle.com

31 May-1 June

Tested the search engines for images and videos.

Tested corresponding to basic and advanced deep fake images.

Got familiar with google collab for training the model as local machine would take a lot more time.

Deep fake images and videos



Tested at: <https://deepware.ai/>

✓

NO DEEPPAKE DETECTED

New Scan

Name: result.mp4

Size: 288.9 KB

User

2021-05-28 17:16:35 UTC

Source

6 seconds ago

DETAILS

Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.

1.00

Model Results

Deepware: NO DEEPPAKE DETECTED(45%)

Seferbekov: NO DEEPPAKE DETECTED(36%)

Ensemble: NO DEEPPAKE DETECTED(38%)

Video

Duration:

11 sec

Resolution:

256 x 256

Frame Rate:

23.98 fps

Codec:

h264

Audio

Duration:

11 sec

Channel:

stereo

Sample Rate:

44 khz

Codec:

aac

Deep fake images -1



Submission date: 2021 May 28

File: 00KPGHV40E.jpeg

image / jpeg

Visual threats:

▲ Detected

Detection of

Result

Confidence ⓘ

Model Generator ⓘ

AI face swap ⓘ

✓ Undetected

-

-

GAN-generated face ⓘ

▲ Detected

99.9%

Stylegan

Tested at: <https://sensity.ai/>

Deep fake images -2



Submission date: 2021 May 28

File: 00H858UYSD.jpeg

image / jpeg

Visual threats:

Detected

Detection of	Result	Confidence ⓘ	Model Generator ⓘ
AI face swap ⓘ	✓ Undetected	-	-
GAN-generated face ⓘ	⚠ Detected	99.9%	Stylegan

Tested at: <https://sensity.ai/>

Deep fake images -3



Submission date: 2021 May 28

File: 0004STET6P.jpeg

image / jpeg

Visual threats:

▲ Detected

Detection of

Result

Confidence ⓘ

Model Generator ⓘ

AI face swap ⓘ

✓ Undetected

-

-

GAN-generated face ⓘ

▲ Detected

99.9%

Stylegan

Tested at: <https://sensity.ai/>

Deep fake images -4



Tested at: <https://sensity.ai/>



Submission date: 2021 May 28

File: 000N7AlAFT.jpeg

image / jpeg

Visual threats:

▲ Detected

Detection of

Result

Confidence ⓘ

Model Generator ⓘ

AI face swap ⓘ

✓ Undetected

-

-

GAN-generated face ⓘ

▲ Detected

99.9%

Stylegan

Deep fake images -5



Tested at:
<https://images.google.com/>



Image size:
167 × 144

No other sizes of this image found.

Possible related search: **suit separate**

<https://www.menswearhouse.com> › Suits › Suit Separates


Suit Separates - Men's Suit Separate Combinations | Men's ...

Shop for men's suit separates including dress slacks, vests & tuxedos. See the latest **suit separate** combinations in the latest styles from Men's Wearhouse.

<https://www.amazon.in> › Dockers-Mens-Suit-Separate-P...

Buy Dockers Men's Suit Separate Pant, Grey Sharkskin, 40x32 ...

Buy Dockers Men's **Suit Separate** Pant, Grey Sharkskin, 40x32 from Casual Trousers at Amazon.in. 30 days free exchange or return.

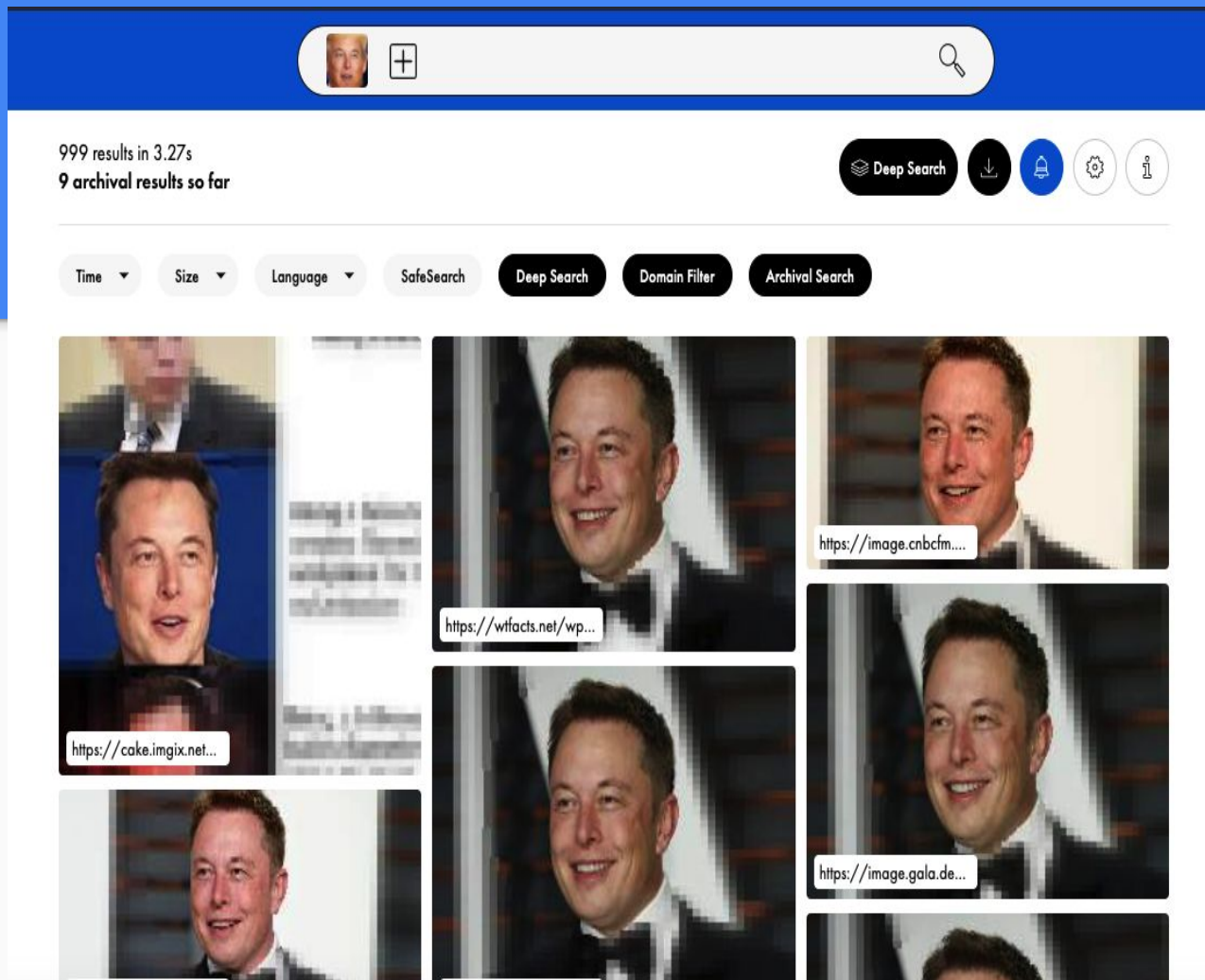
 **Visually similar images**



Deep fake images -5



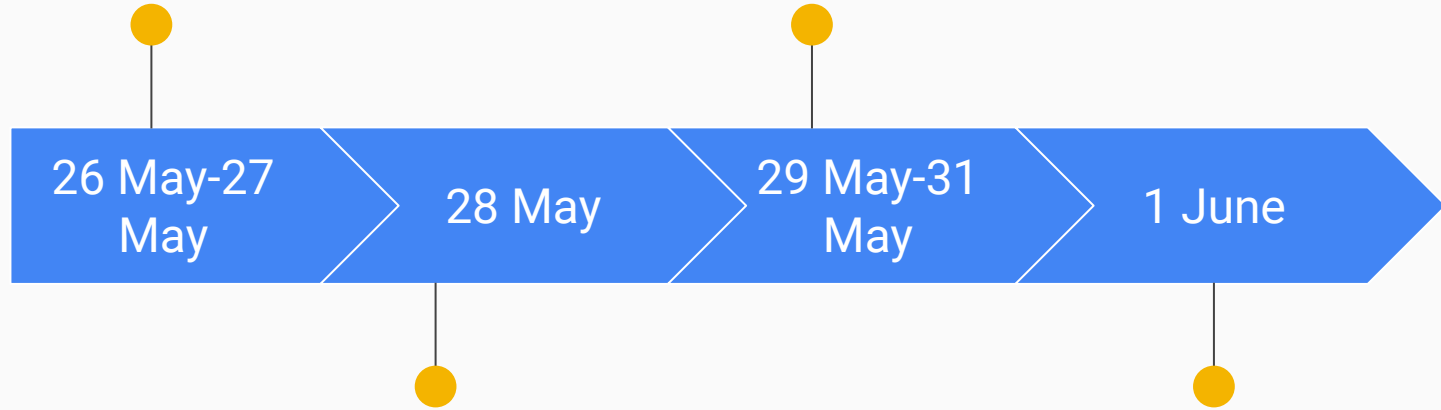
Tested at:
<https://pimeyes.com/en>



The screenshot shows the Pimeyes search results page. At the top, there is a search bar with a small image of the target face and a plus icon. Below the search bar, it displays "999 results in 3.27s" and "9 archival results so far". On the right side, there are several icons: a "Deep Search" button, a download icon, a bell icon, a settings icon, and a user profile icon. Below these, there are filter buttons: "Time", "Size", "Language", "SafeSearch", "Deep Search", "Domain Filter", and "Archival Search". The main area displays a grid of search results, which are images of Elon Musk. Each image has a URL label at the bottom, such as "https://cake.imgix.net...", "https://wtfacts.net/wp...", "https://image.cnbcfm...", "https://image.gala.de...", and "https://image.cnbcfm...".

Commencement of
the internship

Created the first deep
fake video of Elon
Musk singing
Memories



Learning deep fake
generation and using
generation tools.

Testing the search
engine against various
inputs

Tasks

The main task in week-2 for extensive reading of research papers to get insights about the techniques.

Another task was to collect datasets for testing the search engines. The engines are provided with deep fake image and it is evaluated on 2 conditions:

- Detection of deep fakes
- Extraction of original image from the deep fake image.

Paper-1

Link: <http://www.ws.binghamton.edu/fridrich/Research/copymove.pdf>

Using some image processing tools, specific areas are detected and other noise is blacked out. Then comparisons are made to detect the forgery/find the original.

Talks about block matching algorithm that compares images in chunks and not as a whole.

Paper-2

Link:

https://www.researchgate.net/publication/264276516_Detection_of_Clones_in_Digital_Images

This paper discusses detection of cloning. Compare small blocks from the image and then compare those blocks in separate threads to get the output.

There were other methods like DCT and PCA that calculated the gray factor of each block to compare the blocks.

Paper-3

Link: <https://ieeexplore.ieee.org/document/8782292>

This paper discusses the efficient methods to detect cloning of an image. It talked about doing this in 3 ways which are as follows:

- Take the image and convert it to grayscale.
- Divide into disjoint blocks and extract the main features.
- Do the matching process (comparison) and detect the duplicates.

Retrieving original from deep fake-1



Tested at:
<https://images.google.com/>



Image size:
167 × 144

No other sizes of this image found.

Possible related search: **suit separate**

<https://www.menswearhouse.com> › Suits › Suit Separates

Suit Separates - Men's Suit Separate Combinations | Men's ...

Shop for men's suit separates including dress slacks, vests & tuxedos. See the latest **suit separate** combinations in the latest styles from Men's Wearhouse.

<https://www.amazon.in> › Dockers-Mens-Suit-Separate-P...

Buy Dockers Men's Suit Separate Pant, Grey Sharkskin, 40x32 ...

Buy Dockers Men's **Suit Separate** Pant, Grey Sharkskin, 40x32 from Casual Trousers at Amazon.in. 30 days free exchange or return.



Visually similar images



Getting original from deep fake image

In the previous image, the most part of the image was taken by the face only that resulted in different results in different search engines (google and pimeyes).

So, I took an image where the face did not take much area and other features of the image (which are crucial for cloning/deep fake detection) get more area.

The results were much better in that case verifying the algorithm described in the research papers.

Retrieving original from deep fake-2



Tested at:
<https://images.google.com/>

Google

Photo...929087.jpg x virat kohli

Pages that include matching images

<https://twitter.com/imvkohli/status/12009087>

Virat Kohli on Twitter: "Quarantine diaries. Un-ironed T-shirt ...

1200 × 900 · 16-Nov-2020 — Virat Kohli Fans™ @vk_devotee 16 Nov 2020. More. Copy link to Tweet; Embed Tweet. Replying to @imVkohli. ❤️ 2 replies 0 retweets 7 ...

<https://www.indiatvnews.com/Sports/Cricket>

'Quarantine diaries': Virat Kohli shares picture from Australia ...

715 × 402 · 17-Nov-2020 — Virat Kohli took to Twitter to post a picture of him in quarantine as the Indian cricketers prepare for the upcoming series against Australia.

[https://www.filmfare.com/news/bollywood/throwback...](https://www.filmfare.com/news/bollywood/throwback)

Throwback: Virat Kohli is stunned that Katrina Kaif spoke to ...

600 × 450 · 14-Apr-2021 — Indian skipper Virat Kohli and actor and producer Anushka Sharma are one of India's most-loved and followed couples. The celebrity couple ...

<https://www.dnaindia.com/Sports/Cricket>

THIS is how Virat Kohli is spending his quarantine in Australia

640 × 360 · 17-Nov-2020 — The decision of Virat Kohli to leave the Australian series has drawn mixed reactions from Indian and foreign audiences. Virat Kohli's presence for ...

<https://zeenews.india.com/Cricket>

Retrieving original from deep fake-3



Tested at:
<https://images.google.com/>

Google

Photo...929376.jpg X effort to level the playing field barron trump will X

<https://www.ndtv.com> > World

Donald Trump Changes Campaign Logo After Being Mocked ...

360 × 222 · 17-Jul-2016 — The campaign of US Republican Presidential nominee Donald Trump unveiled a new logo on Saturday, a day after an original logo was ...

<https://imgflip.com> > ...

It seems Biden is afraid of a real debate. - Imgflip

500 × 955 — It seems Biden is afraid of a real **debate**. | BIDEN WON'T DEBATE. share. 49,236 views · 42 upvotes · Made by Perspicacity 12 months ago in politics · Joe Biden ...

<https://www.ndtv.com> > World

Saddam Hussein Killed Terrorists 'So Good': Donald Trump ...

360 × 222 · 07-Jul-2016 — Donald Trump, who frequently criticizes US foreign policy under President Barack Obama and former Secretary of State Hillary Clinton, ...

<https://www.ndtv.com> > World

Donald Trump's Plans Could Cripple Economy, Says New ...

360 × 222 · 13-Jul-2016 — An analysis by the New York City Council finds that Donald Trump's lightning-rod proposals to deport illegal immigrants and temporarily ban ...

<https://www.ndtv.com> > World

Donald Trump Promises To Herald US Economic Resurgence

360 × 222 · 29-Jun-2016 — Criticising the current US trade policies that has wiped

Getting original from deep fake image

After output of certain search engines on deep fakes, we could see original images as output.

This becomes another parallel work of analysing original image retrieval from deep fakes.

Features apart from faces play vital role in such cases. This is partly because faces are swapped and thus that region has a lot of “noise”. Apart from it, during comparison of blocks of images other than the face, that would match with the image on the bottom.

Certain search engines that are not meant for detecting deep fakes were able to give output of original image especially if it was from **some famous event**.

Kaggle deep fake result -1



Tested at:
<https://images.google.com/>

A screenshot of a Google Images search for the term "lady". The search bar at the top shows "lady" and a thumbnail of the image being searched. Below the search bar, the results show "About 2 results (2.31 seconds)". The first result is a thumbnail of the same woman, with "Image size: 1024 x 1024" and "No other sizes of this image found." Below this, it says "Possible related search: lady". The main result is a link to "Lady - Kenny Rogers - YouTube" with a description: "11-Jan-2008 — lady kenny rogers If you enjoyed my channel and decide to tip in crypto. I thank you for your support. Bitcoin wallet: ...". Below this is another link to "Lady - Kenny Rogers - YouTube" with a description: "28-May-2018 — Youtube RadioUtopia Video Creations Subscribe https://bit.ly/2Mi6DG7 ...". At the bottom, there is a section for "Visually similar images" showing a grid of 16 small images of the same woman. On the right side of the search results, there is a sidebar with the title "Lady" and a definition: "The word lady is a term of respect for a girl or woman, the equivalent of gentleman. Once used to describe only women of a high social class or status, the female equivalent of lord, now it may refer to any adult woman. Informal use of this word is sometimes euphemistic or, in American slang, condescending. Wikipedia". Below the definition is a section "People also search for" with four icons labeled "Knight", "Gentleman", "Viscount", and "Goddess".

Kaggle deep fake result -2



Tested at:
<https://images.google.com/>

The screenshot shows a Google Images search interface. At the top, the Google logo is on the left, and search filters (All, Images, Maps, Shopping, More) are in the center. The search bar contains 'boy'. Below the search bar, it says 'About 2 results (0.66 seconds)'. The first result is a small thumbnail of a young boy, with 'image size: 1024 x 1024' and 'No other sizes of this image found.' below it. To the right of the main results, there is a 'Boy' knowledge panel with a definition: 'A boy is a young male human. The term is usually used for a child or an adolescent. When a male human reaches adulthood, he is described as a man. Wikipedia'. Below the main results, there are links to YouTube videos: 'Charlie Puth - BOY [Official Audio] - YouTube' and 'TREASURE - 'BOY' MV - YouTube'. At the bottom, there is a 'Visually similar images' section showing a grid of 16 small images of various young boys.

Getting original from kaggle deep fakes

The search results of deep fakes of kaggle were not giving original images as output.

They were giving general output as searches corresponding to “boy”, “lady” etc.

Possible reason could be that the large part of image was taken by faces and no other feature to compare with, unlike the example of Virat Kohli's image.

Facts on profile cloning (non technical)

- Facebook alone removed over **580 million profiles** in the first quarter of 2018 alone while Twitter removed **70 million accounts** from May to June of 2018.
- **Profile photo and location** are the most important information that is checked by any user for checking the originality of any profile.
- The main problem with deep fakes is that it can preserve the pose, facial expressions and lighting of the photographs.
- They also **reduce the quality** a bit to make some of the current deep fake detection algorithms give false negatives.

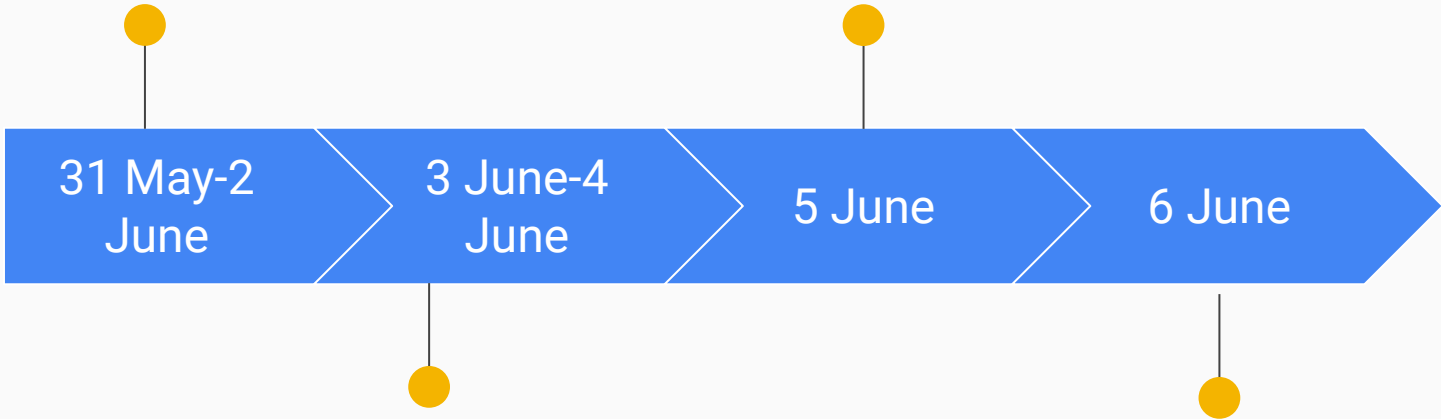
Datasets

Dataset 1: http://www.diid.unipa.it/cvip/?page_id=48

Dataset 2: <https://www.kaggle.com/tunguz/1-million-fake-faces>

Reading research
papers

Testing the search
engine against various
inputs.



Collecting data sets
and more reading
(post meeting)

Report + summarizing