

Fighting DeepFakes with Technologies

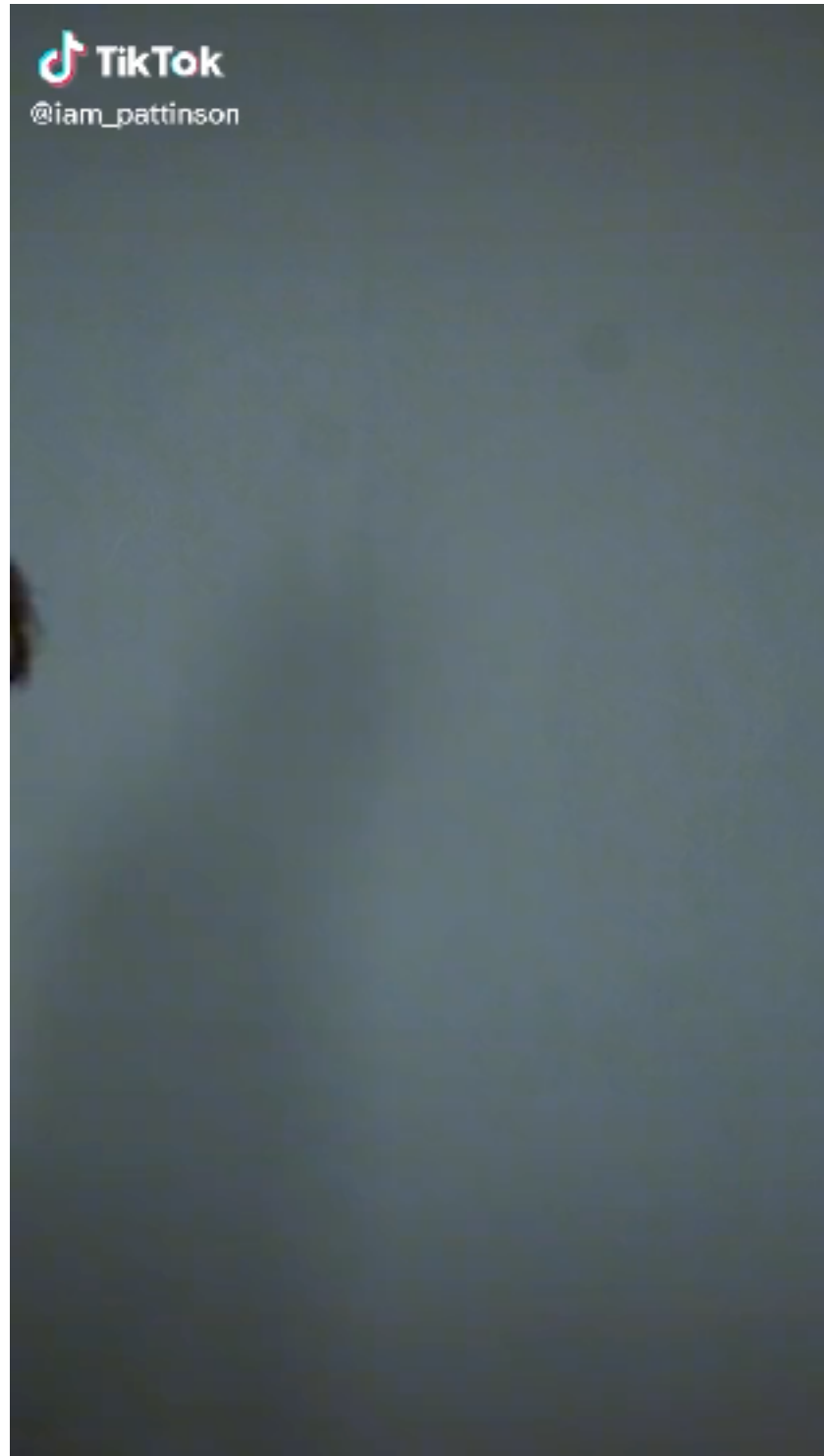
Siwei Lyu

Department of Computer Science
and Engineering

University at Buffalo,
State University of New York

Email: siweilyu@buffalo.edu

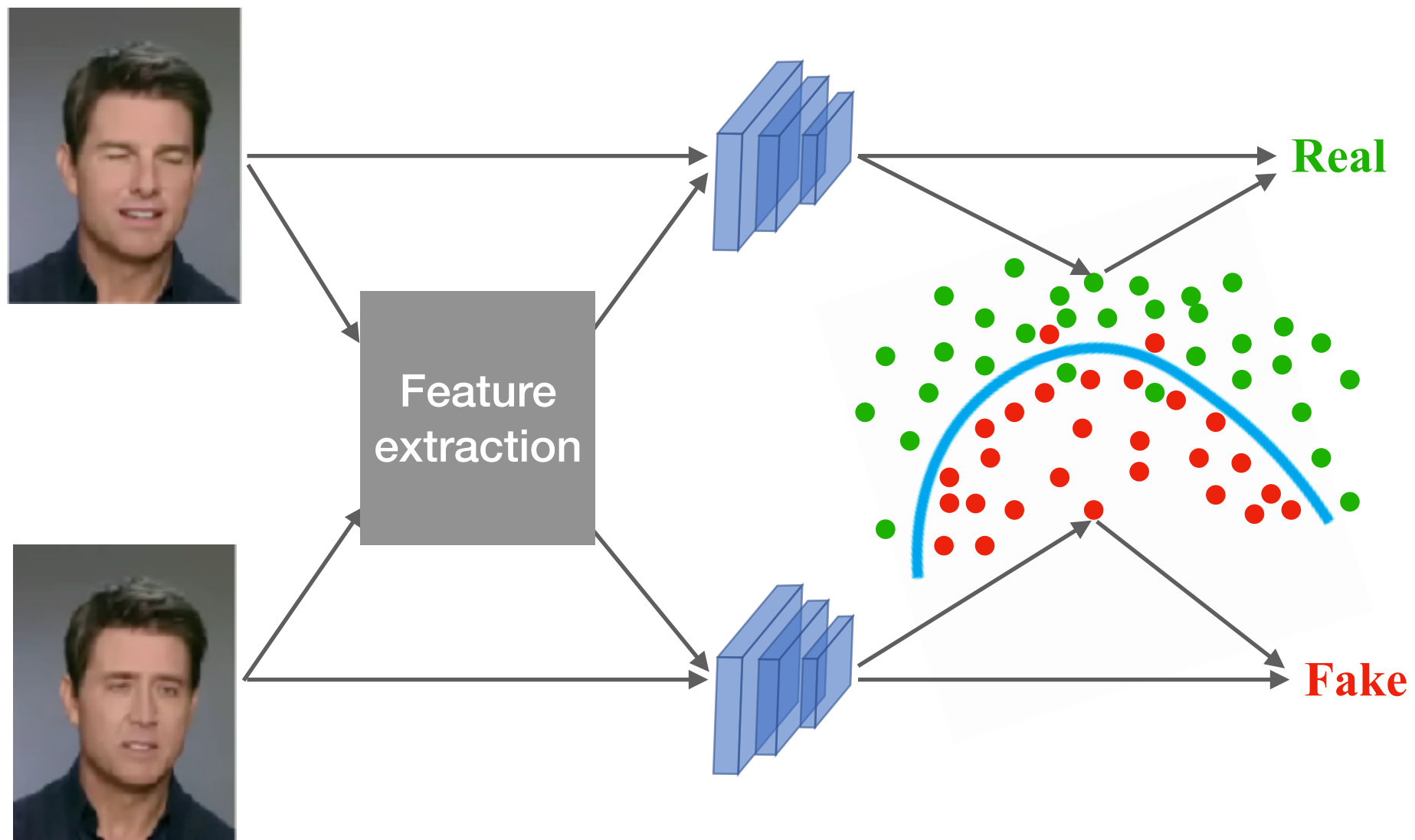
Is this Robert Pattinson?



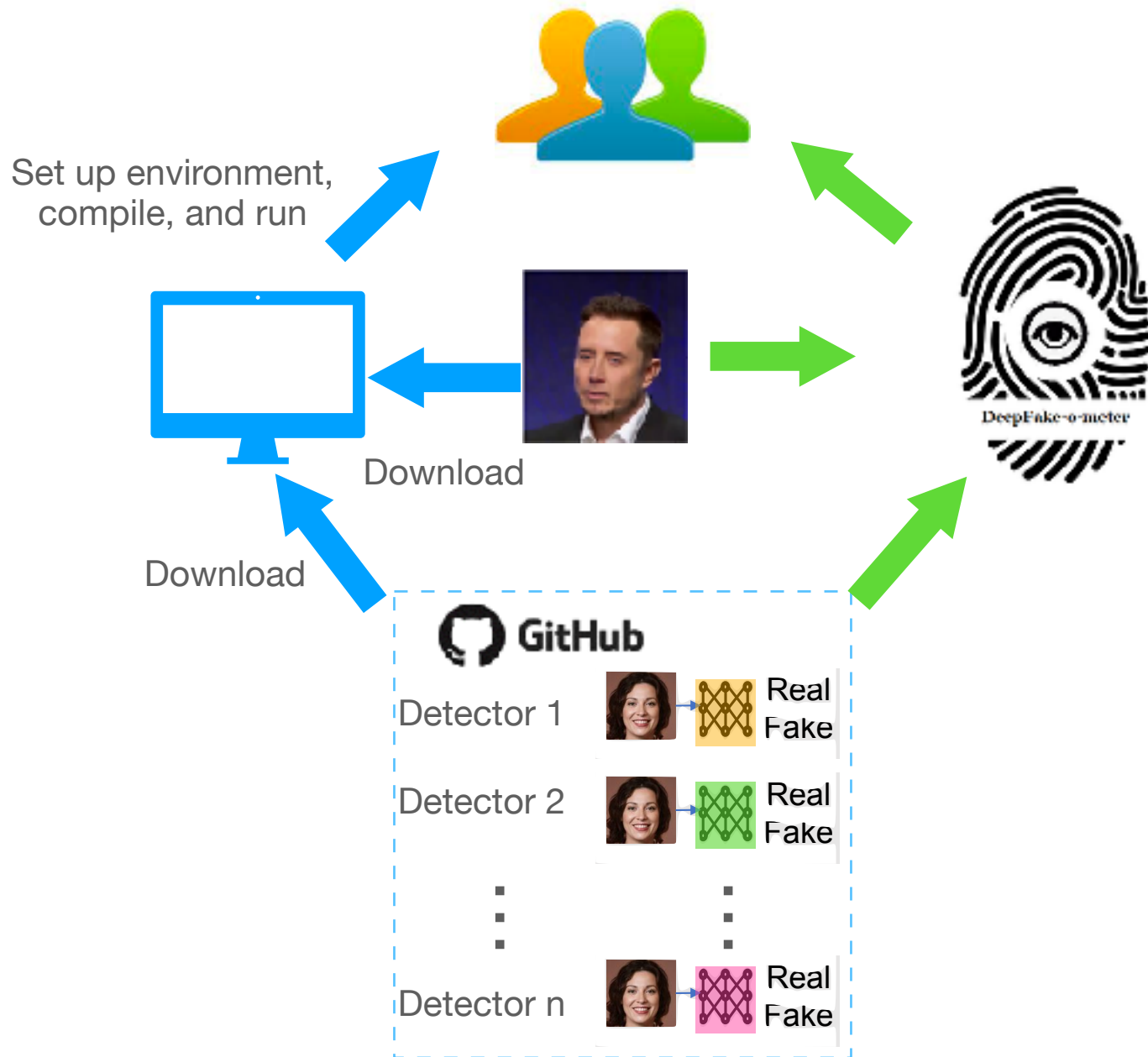
Source: https://www.tiktok.com/@iam_pattinson

Source: IMDB

DeepFake detection methods



DeepFake-o-meter



DeepFake-o-meter

An open platform integrating state-of-the-art DeepFake detection methods

If you are a developer and want your DeepFake detection method to be included in DeepFake-o-meter, please follow [these steps](#).

Please find instructions of using DeepFake-o-meter in this [video tutorial](#).

Upload Video

you can enter a YouTube video URL or upload video from your computer. Note the video should contain only one subject and upload one video each time.

• Upload an url.

Video Url:

• Or upload the video (maximum size is 50MB).

no file selected

Select DeepFake Detection Methods

Select the deepfake Methods. [Instruction Reference](#)

Input your e-mail and PIN code

The submission notification and download link of your results will be sent to your email. Only one email is required.

• E-mail address:



Is this Robert Pattinson?



```
-----Step2: PDI faces matching (5 faces for detection)-----  
PDI 5 faces detection and matching time: 6.05 seconds  
  
-----Step3: Deepfakes detection-----  
I am loading a detection model pre-trained/detection_model.pth  
ProbManipulation: 0.9857, LLR: 0.9823  
PDI video detection time: 3.53 seconds
```

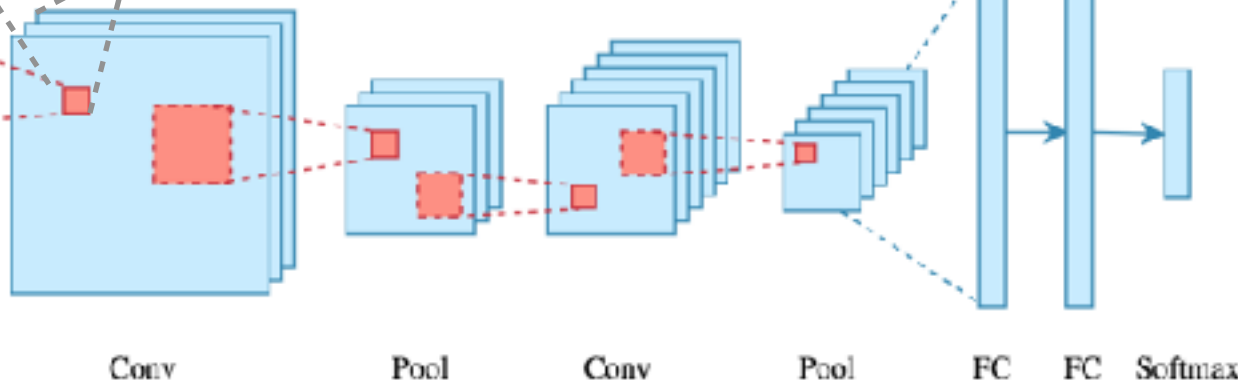
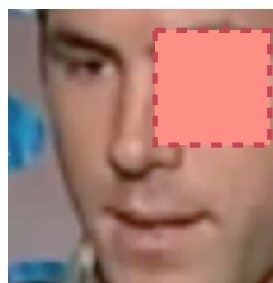
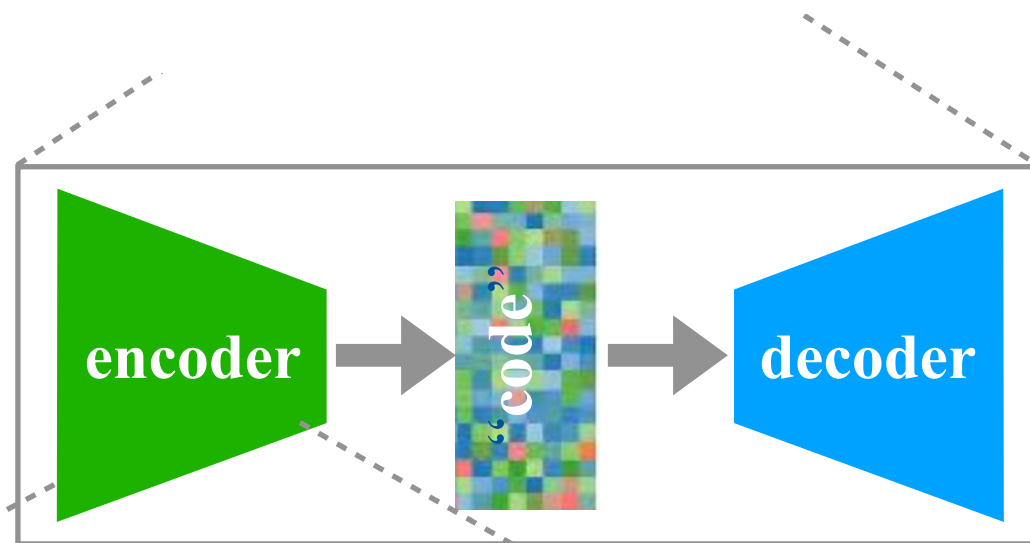
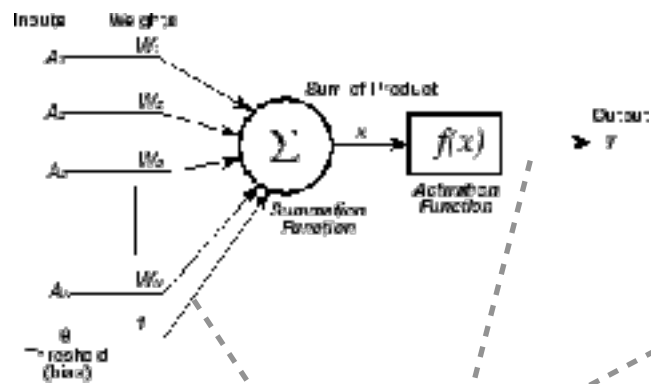
Fake



Source: https://www.tiktok.com/@iam_pattinson

Source: IMDB

How to make DeepFake videos



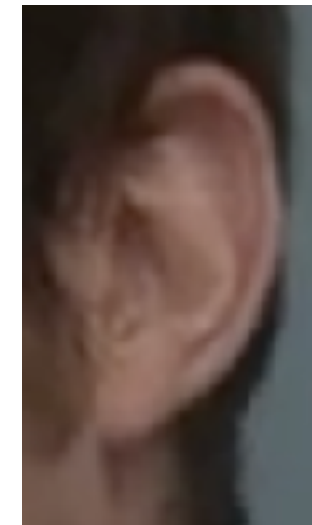
Is this Robert Pattinson?



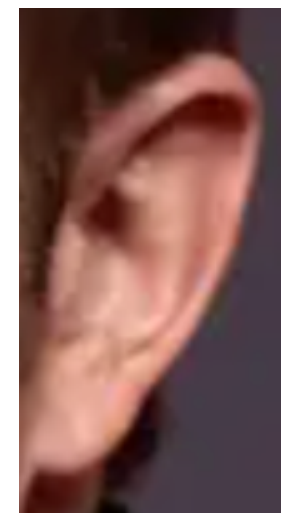
```
-----Step2: PMI faces matching (5 faces for detection)-----  
PMI 5 faces detection and matching time: 6.05 seconds  
  
-----Step3: Deepfakes detection-----  
I am loading a detection model pre-trained/detection_model.pth  
ProbManipulation: 0.9857, LLR: 0.9823  
PMI video detection time: 3.53 seconds
```

Fake

Tiktok



IMDB

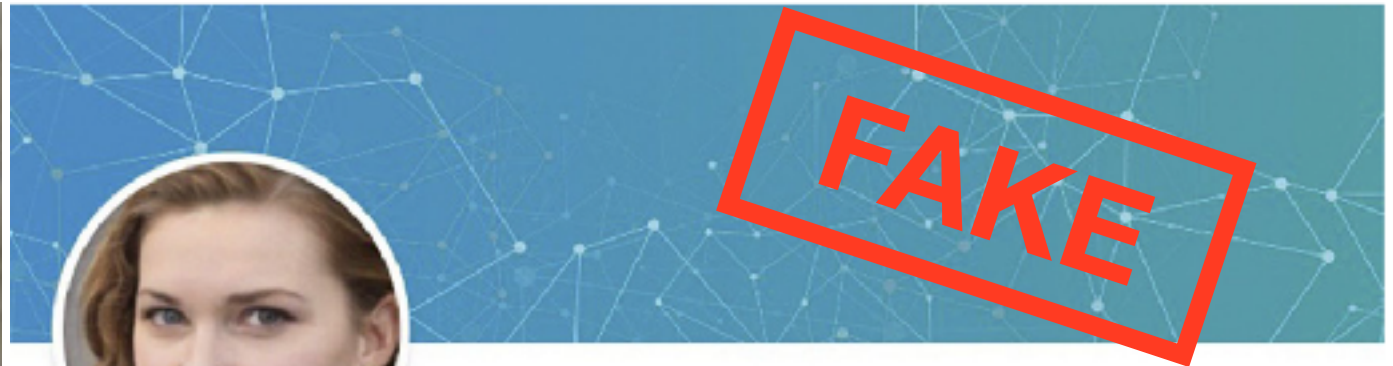


Source: https://www.tiktok.com/@iam_pattinson

Source: IMDB

Reference: A. Shruti and H. Farid, Detecting Deep-Fake Videos from Aural and Oral Dynamics, CVPR Workshop on Multimedia Forensics, 2021

GAN synthesized faces



Connect



Katie Jones

Russia and Eurasia Fellow

Center for Strategic and International Studies (CSIS) ·
University of Michigan College of Literature, Science...
Washington · 49 connections

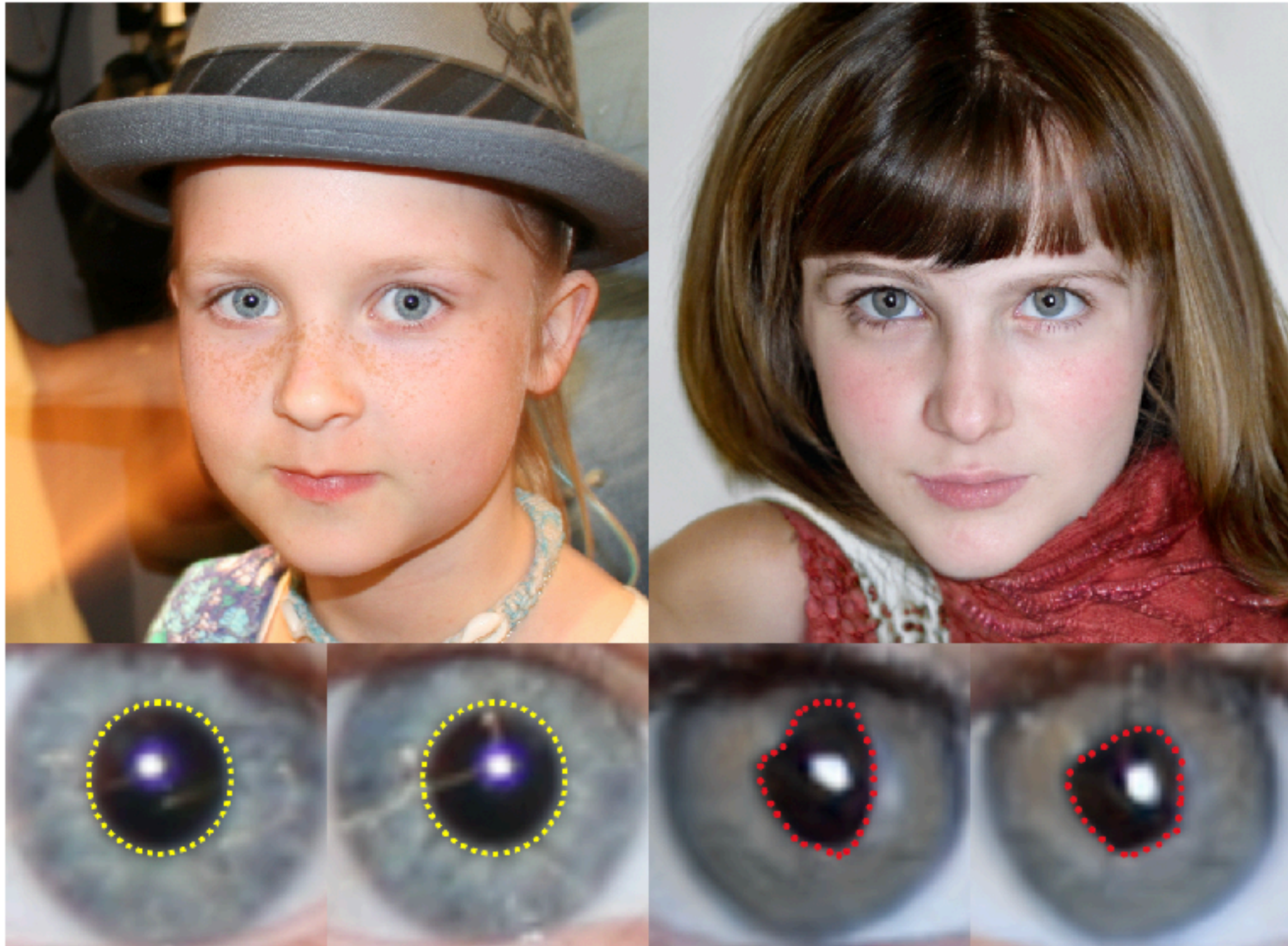


Source: www.thispersondoesnotexist.com

Expose GAN synthesized faces



Expose GAN synthesized faces



Summary

- Detection algorithms are useful, but most of them are *unexplainable* black boxes
- Looking for semantic cues that are rooted in physiological and physical constraints of the real world may provide more explainable and effective approaches for detection
- The competition between DeepFake making and forensics is a perpetual cat-and-mouse game, and will continue for the foreseeable future
- All DeepFake detection methods are post mortem analysis, and we need more preemptive approaches to protect the users from becoming victims of DeepFakes



Thank You!