March 2021

DeepFake Generation & Detection

David Weinflash

Department of Computer Science

UC SANTA BARBARA

Research Papers

DeepFake Generation

- *First Order Motion Model for Image Animation*
  - Siarohin *et al.*
  - Neural Information Processing Systems (NeurIPS) 2019

DeepFake Detection

- *Video Face Manipulation Detection Through Ensemble of CNNs*
  - Bonettini *et al.*
  - International Conference on Pattern Recognition (ICPR) 2020

DeepFake Generation

First Order Motion Model for Image Animation

First Order Motion Model for Image Animation

Problem

- **Image Animation:**
  - Automatically synthesize videos by combining the contents of a source image with the motion patterns derived from a driving video.

First Order Motion Model for Image Animation

Problem

- **Image Animation:**
  - Automatically synthesize videos by combining the contents of a source image with the motion patterns derived from a driving video.

- **Challenge:**
  - Traditional approaches (GANs and VAEs) rely on pre-trained models built upon ground-truth data annotations.

First Order Motion Model for Image Animation

Problem

- **Solution:**
  - Introduce a framework that does not depend on prior information or annotated data sets.

First Order Motion Model for Image Animation

Problem

- **Solution:**
  - Introduce a framework that does not depend on prior information or annotated data sets.

- **Framework:**
  - *Motion Estimation Module*
    - Encoder-decoder network predicts a dense motion field aligning the driving video and the source image.
  - *Image Generation Module*
    - Utilize a CNN and output of *motion estimation module* to generate a moving version of the source image.

First Order Motion Model for Image Animation

Analysis

- **Claim #1:**
  - *Our method significantly outperforms state-of-the-art image animation methods and can handle high-resolution datasets where other approaches generally fail.*

1 Mbps

8 Mbps

First Order Motion Model for Image Animation

Analysis

- **Claim #2:**
  - *We introduce an occlusion-aware generator, which adopts an occlusion mask to inpaint object parts that are not visible in the source image and should be inferred from the context.*

First Order Motion Model for Image Animation

Analysis

- **Claim #3:**
  - *One limitation of transferring relative motion is that we need to assume that the objects in the source image and driving video have similar poses.*

DeepFake Detection

Video Face Manipulation Detection Through Ensemble of CNNs

Video Face Manipulation Detection Through Ensemble of CNNs

Problem

- **DeepFake Detection:**
  - Identifying DeepFake videos in real-world scenarios.

Video Face Manipulation Detection Through Ensemble of CNNs

Problem

- **DeepFake Detection:**
  - Identifying DeepFake videos in real-world scenarios.

- **Challenge:**
  - Detecting the ever-growing production of DeepFakes across the internet requires a solution that is robust, efficient and scalable.

Video Face Manipulation Detection Through Ensemble of CNNs

Problem

- **Solution:**
  - Fuse together state-of-the-art CNNs to accurately detect facial manipulation artifacts in a minimal amount of time.

Video Face Manipulation Detection Through Ensemble of CNNs

Problem

- **Solution:**
  - Fuse together state-of-the-art CNNs to accurately detect facial manipulation artifacts in a minimal amount of time.

- **Framework:**
  - *EfficientNet Models*
    - Use attention layers to teach the network what regions of the input image are most important to analyze during classification.
    - Use siamese training to extrapolate additional information from the data and uncover generalizabilities.

Video Face Manipulation Detection Through Ensemble of CNNs

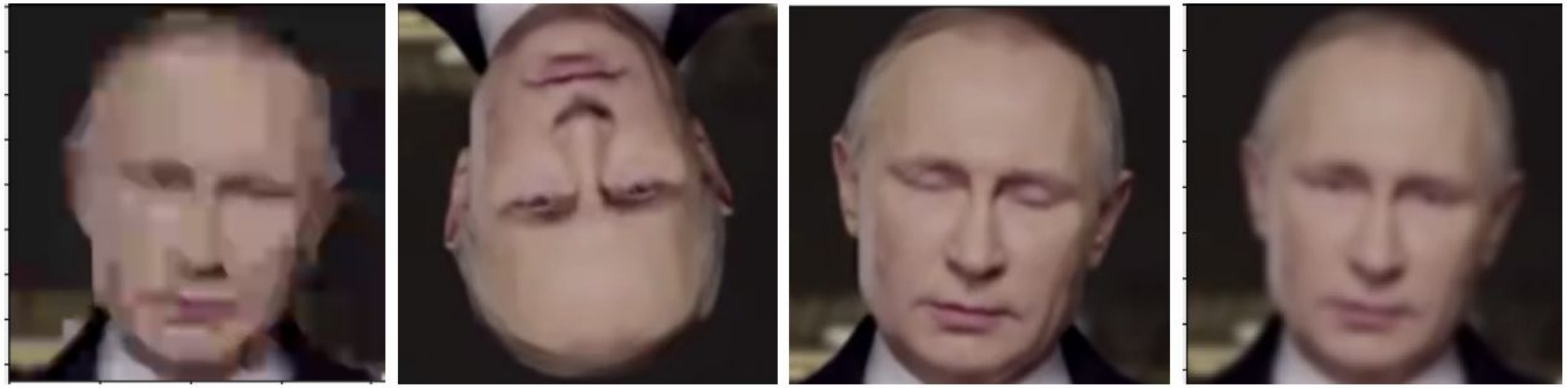
Analysis

- **Claim #1:**
  - *Network fusion helps both the accuracy of the DeepFake detection and the quality of the detection.*

Video Face Manipulation Detection Through Ensemble of CNNs

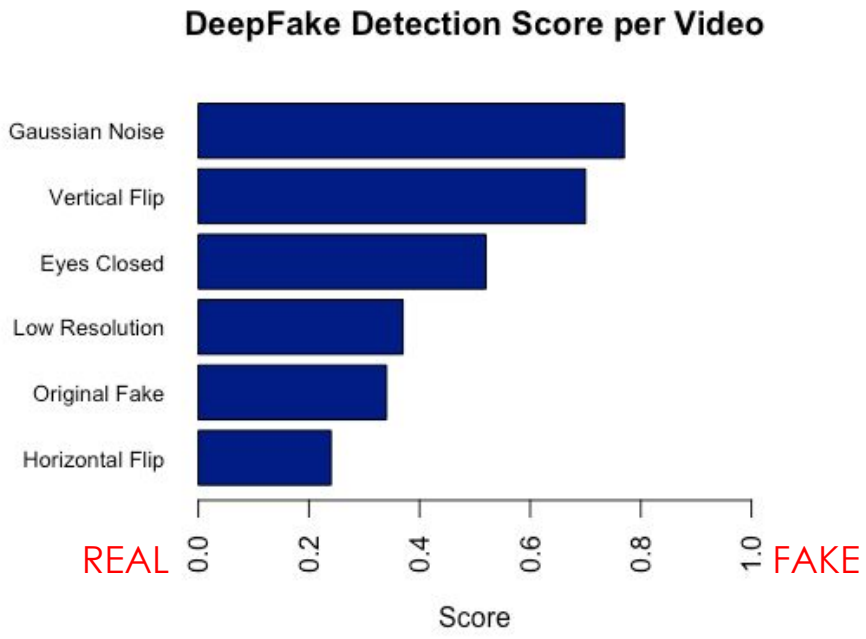
Analysis

- **Claim #2:**
  - *To make our models more robust, we perform data augmentation operations (downscaling, horizontal flipping, noise addition, etc.) on the input faces.*



Analysis

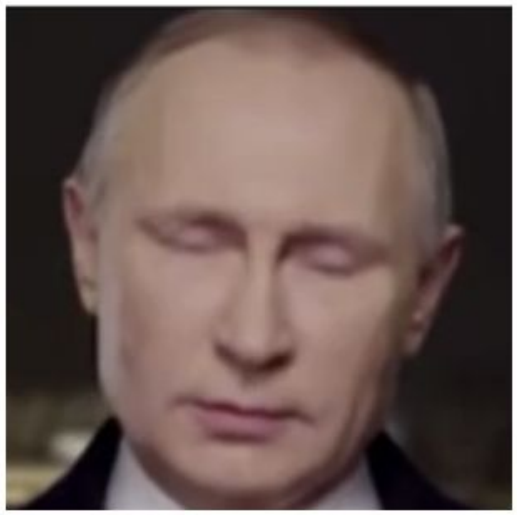
- **Claim #2:**
  - *To make our models more robust, we perform data augmentation operations (downscaling, horizontal flipping, noise addition, etc.) on the input faces.*



Video Face Manipulation Detection Through Ensemble of CNNs

Analysis

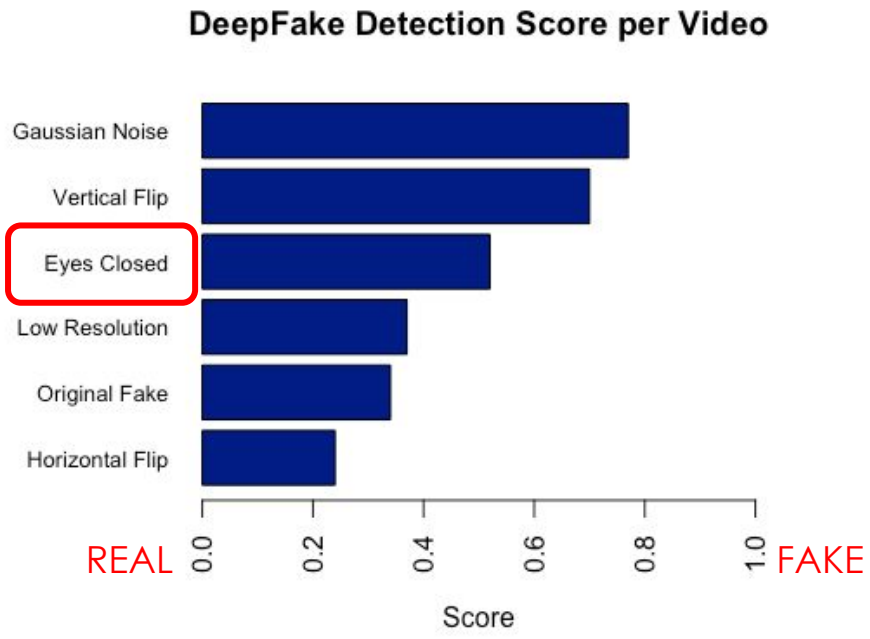
- **Claim #3:**
  - *Roughly modeled eyes and teeth, showing excessively white regions, are the main trademarks of DeepFake generation methods.*



Video Face Manipulation Detection Through Ensemble of CNNs

Analysis

- **Claim #3:**
  - *Roughly modeled eyes and teeth, showing excessively white regions, are the main trademarks of DeepFake generation methods.*



Thank you!