Pushing Deepfakes to the Limit

Fake Video Calls with AI

TNG TECHNOLOGY CONSULTING

AS SEEN ON TV

> When a new technology like this comes along, the most dangerous period is when the technology is out there but the public isn't aware of it. That's when it can be used most effectively.

Carl Bergstrom
University of Washington

Speakers

Thomas Endres

Partner

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2019

Martin Förtsch

Principal Consultant

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2019

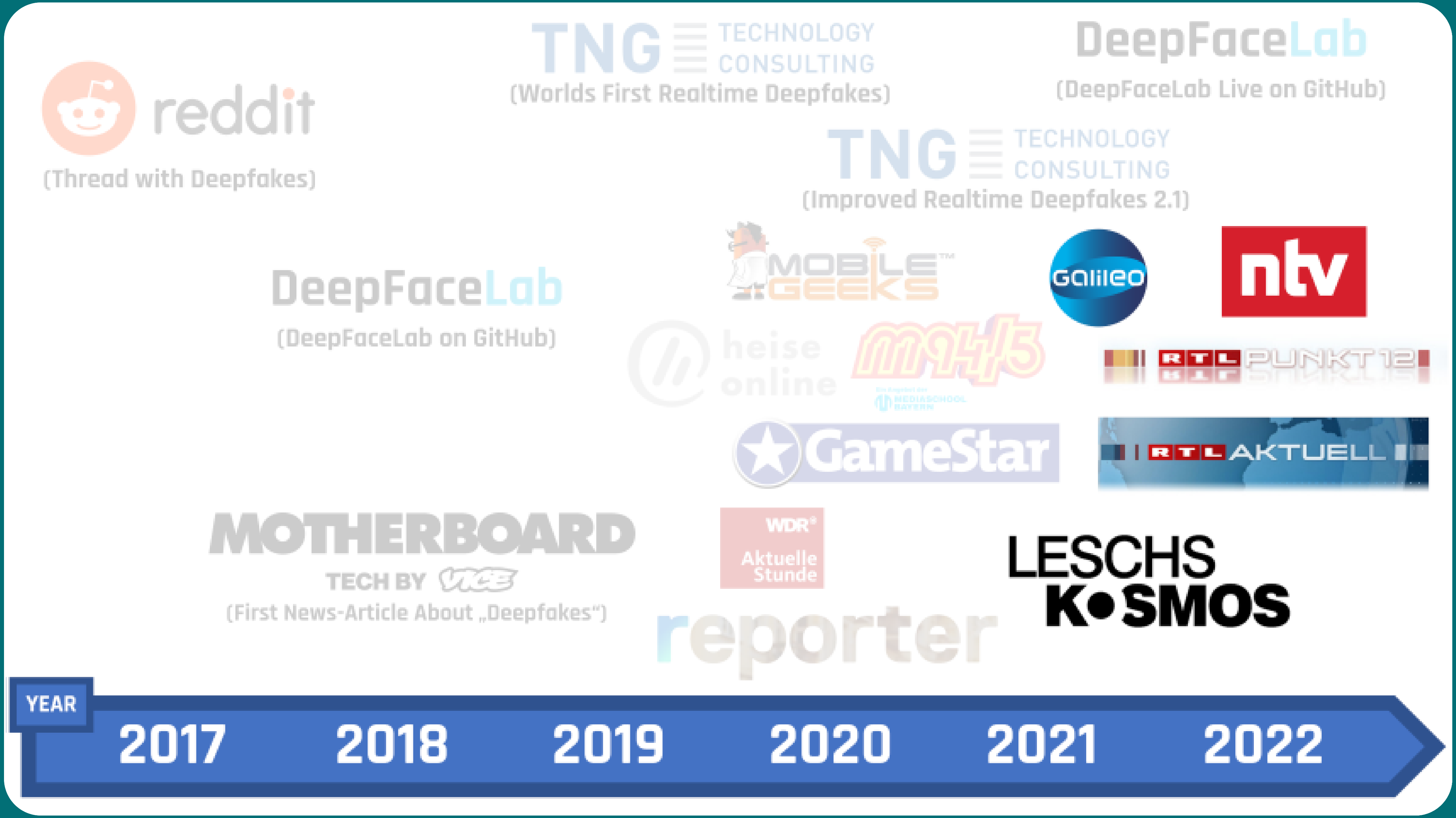
Jonas Mayer

Senior Consultant

Bedroom DJ
Teakwondo Black Belt
GameStar Certified Hacker
Intel® Software Innovator

Our Story

The Evolution of Deepfakes



(Thread with Deepfakes)

(Worlds First Realtime Deepfakes)

(DeepFaceLab Live on GitHub)

(Improved Realtime Deepfakes 2.1)

(DeepFaceLab on GitHub)

(First News-Article About „Deepfakes“)

Evolution of Deepfakes

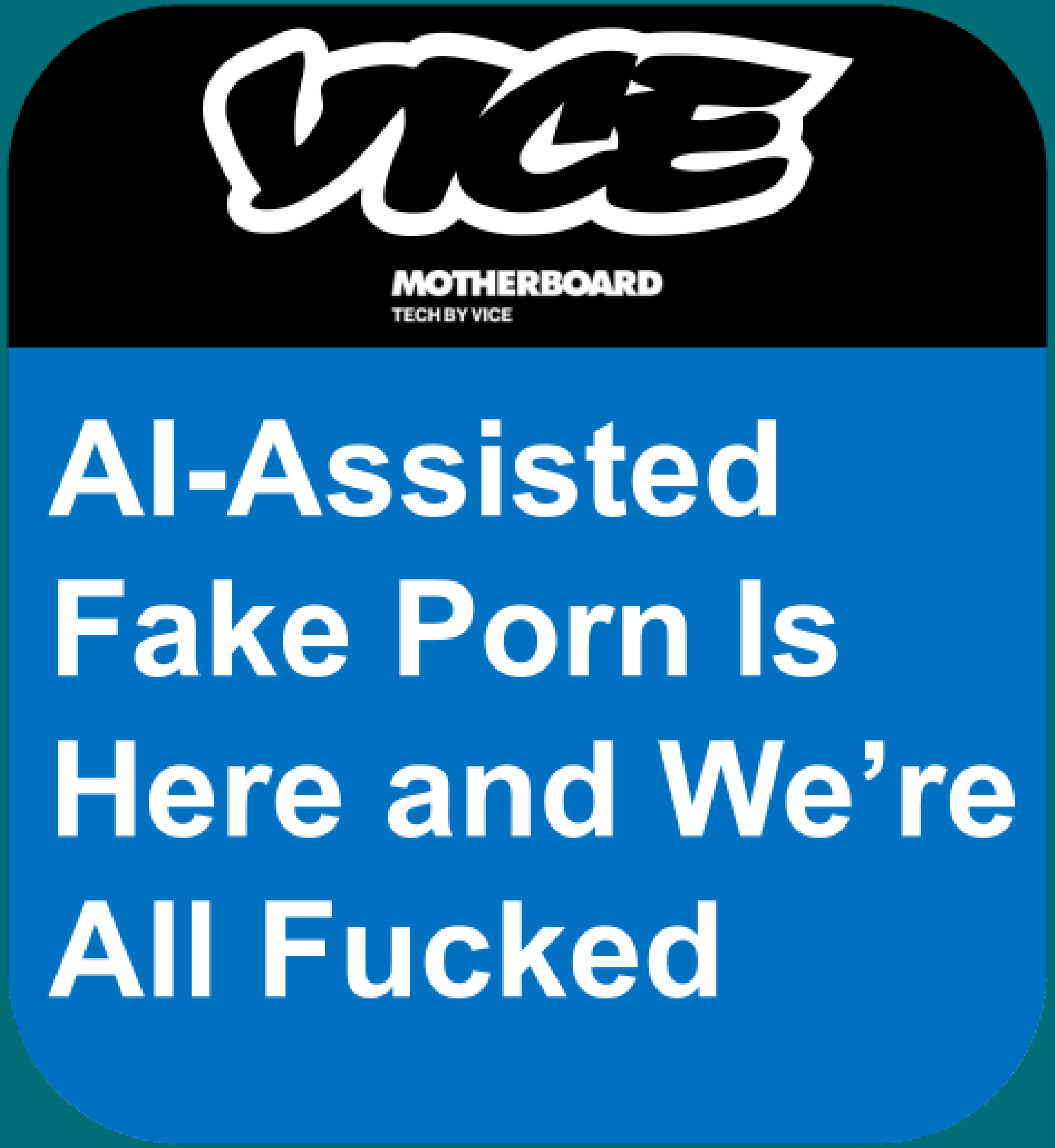
First Deepfake Videos Were Published on Reddit in Autumn 2017

Evolution of Deepfakes

First Deepfake Videos Were Used for NSFW-Videos

Evolution of Deepfakes

First News Article on Deepfakes at VICE Motherboard in Spring 2018



VICE

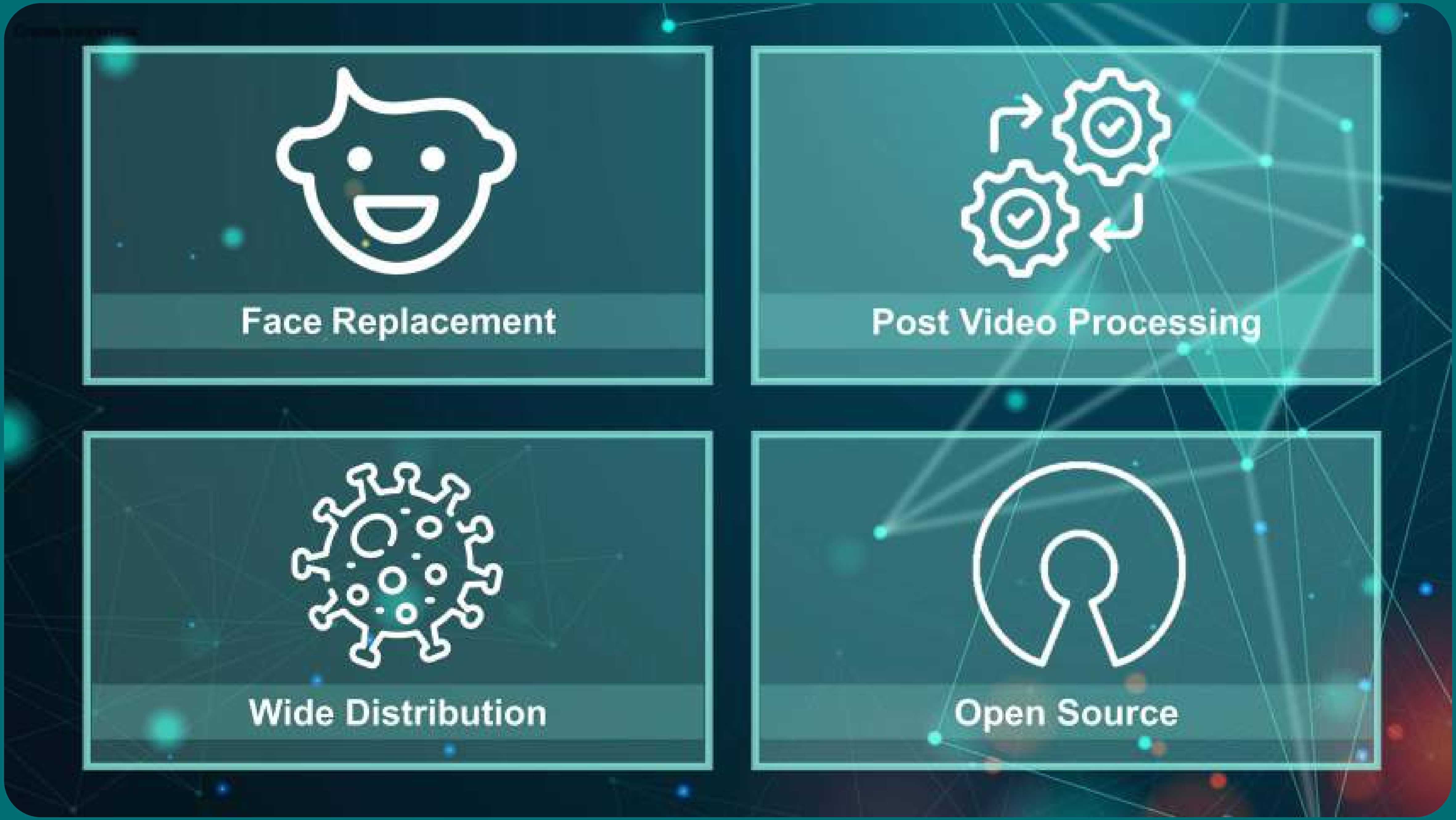
MOTHERBOARD

TECH BY VICE

AI-Assisted Fake Porn Is Here and We're All Fucked

Evolution of Deepfakes

DeepFaceLab Published on GitHub (2018)



Face Replacement

Post Video Processing

Wide Distribution

Open Source

Evolution of Deepfakes

"Perfectly Real" Deepfakes Will Arrive in 6 Months to a Year (2019)

Realtime Deepfakes

The Motivation behind Deepfakes 2.0 (2019)

Realtime Deepfakes

Whole Head Replacement

Work with any Source Actor

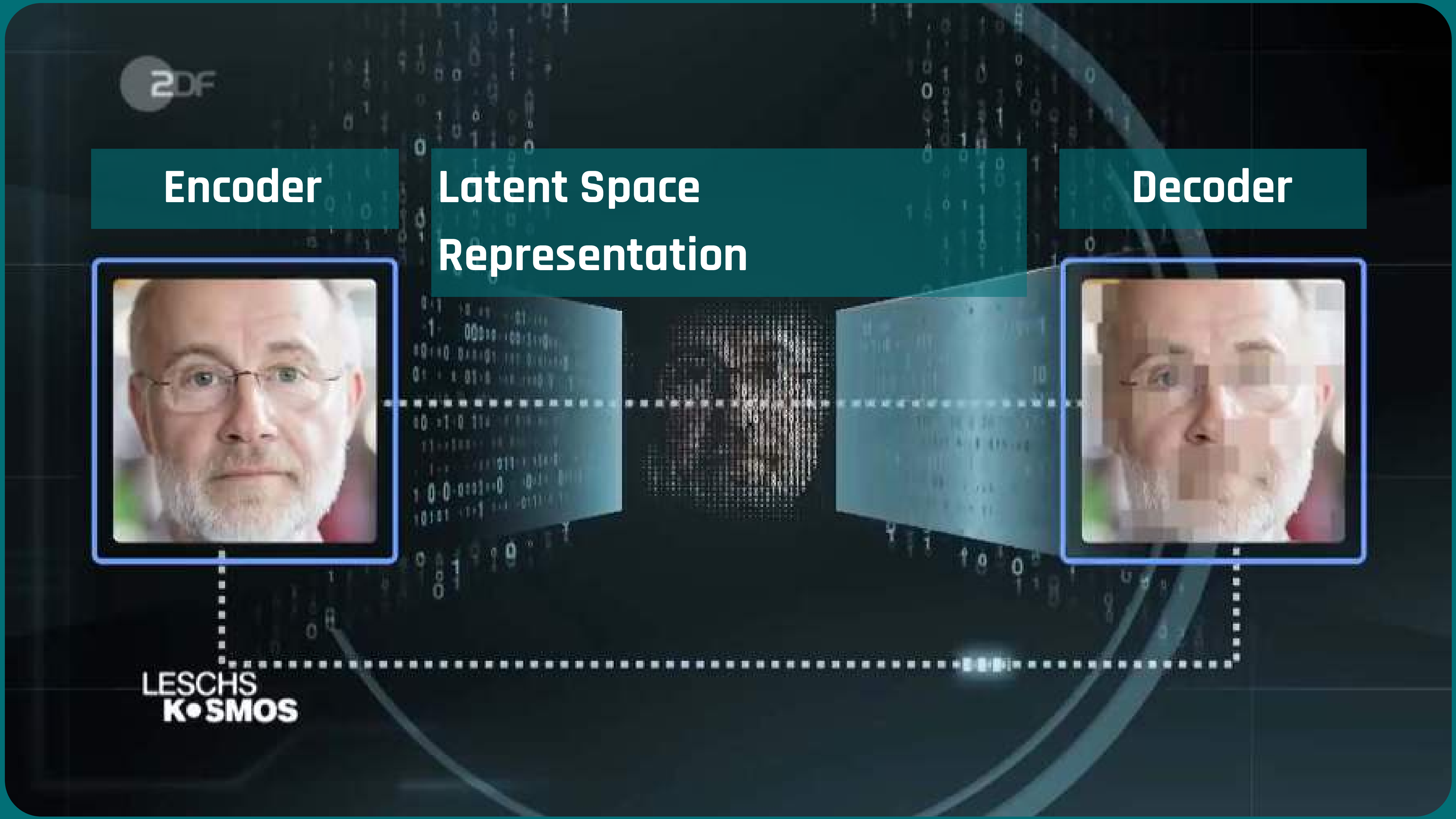
Create Awareness

Agenda

- ► Deepfakes in a Nutshell
- ► Realtime Deepfakes
- ► Pushing Deepfakes to the Limit
- ► Videocalls with Deepfakes
- ► Conclusion

Deepfakes in a Nutshell

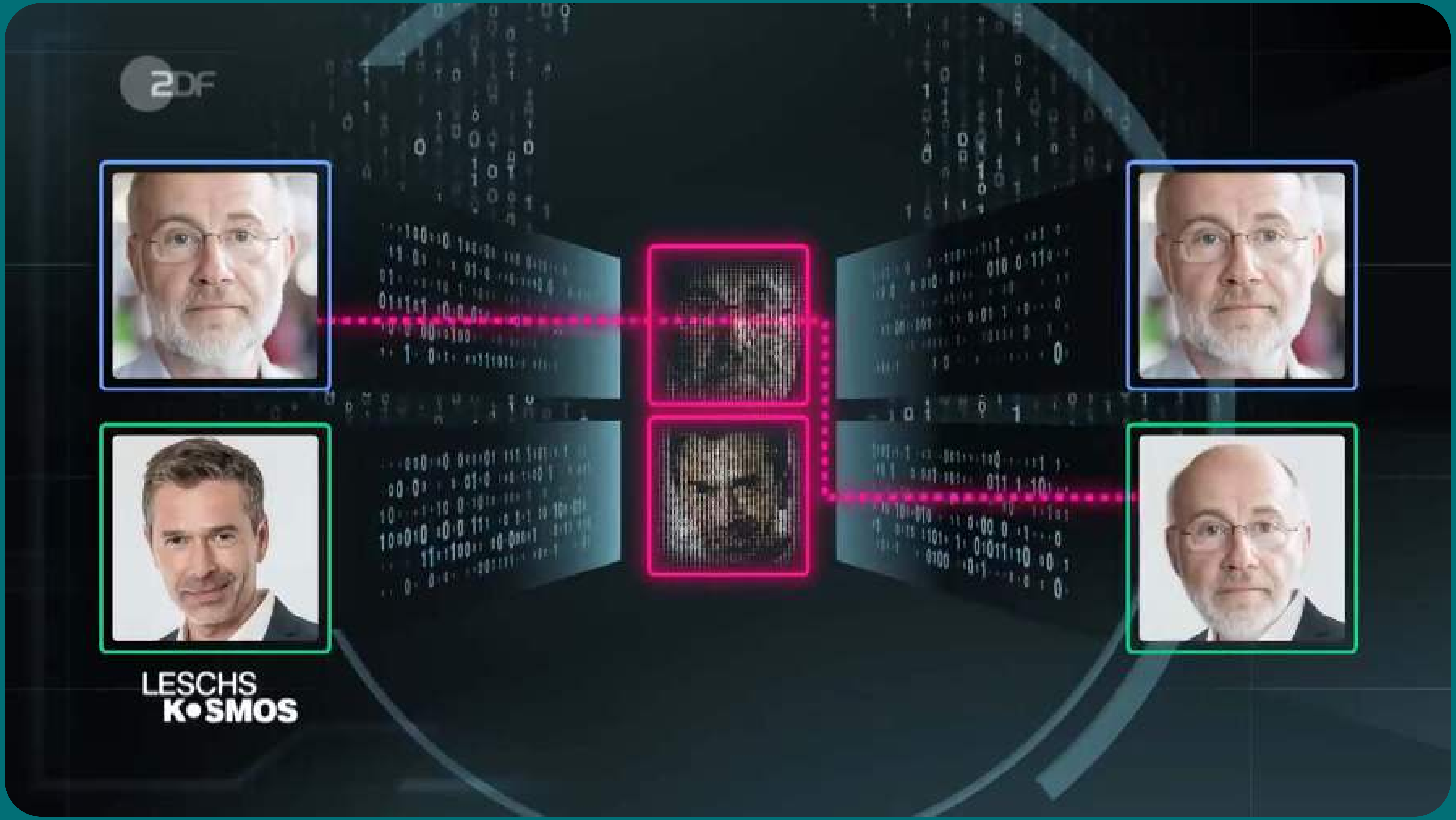
Training Encoder and Decoder on Harald Lesch



https://www.youtube.com/watch?v=ItTvXIM4cjE

Deepfakes in a Nutshell

Use Face Encoder but Different Face Decoder



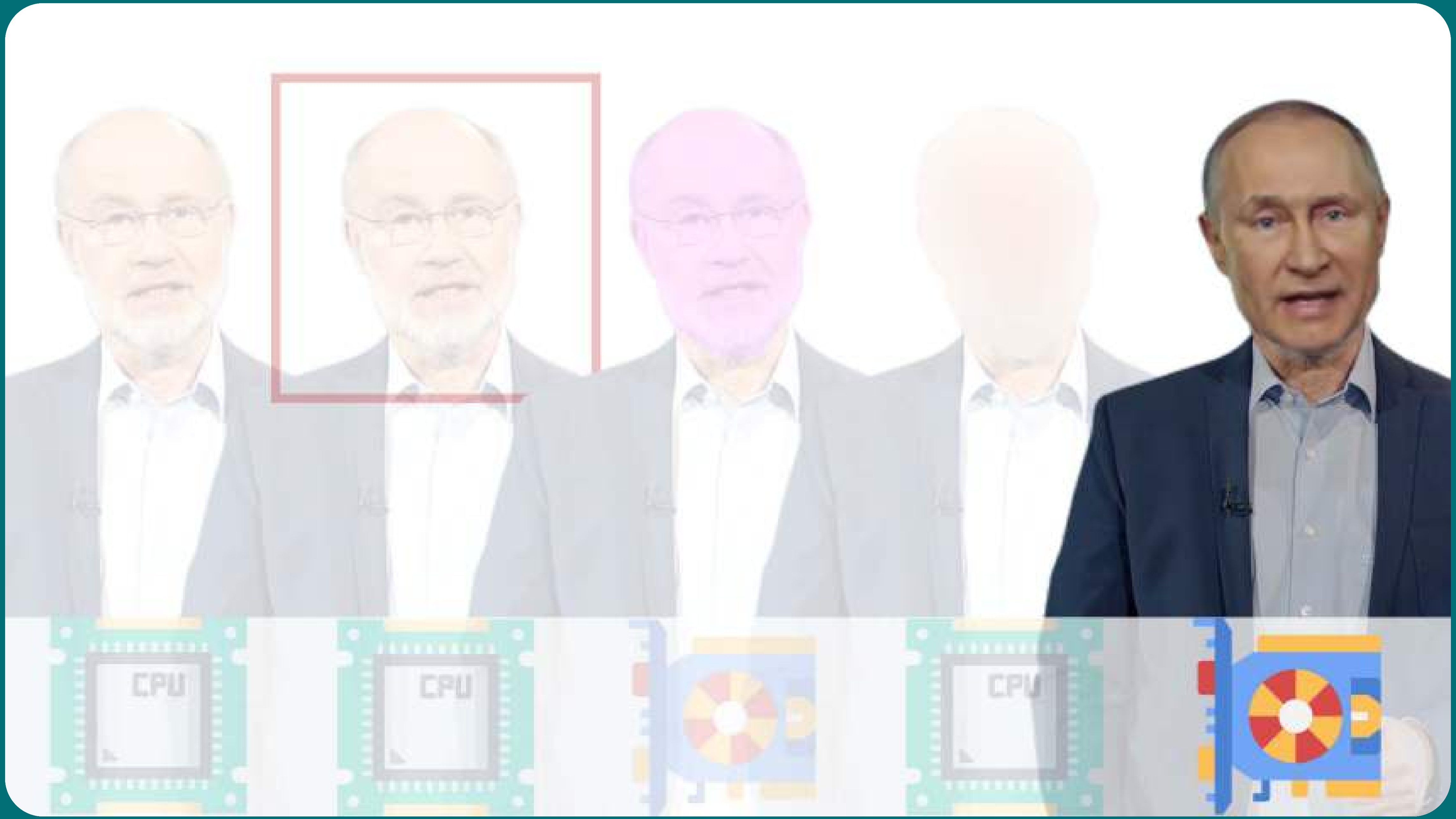
https://www.youtube.com/watch?v=ItTvXIM4cjE

Agenda

- ► Deepfakes in a Nutshell
- ► Realtime Deepfakes
- ► Pushing Deepfakes to the Limit
- ► Videocalls with Deepfakes
- ► Conclusion

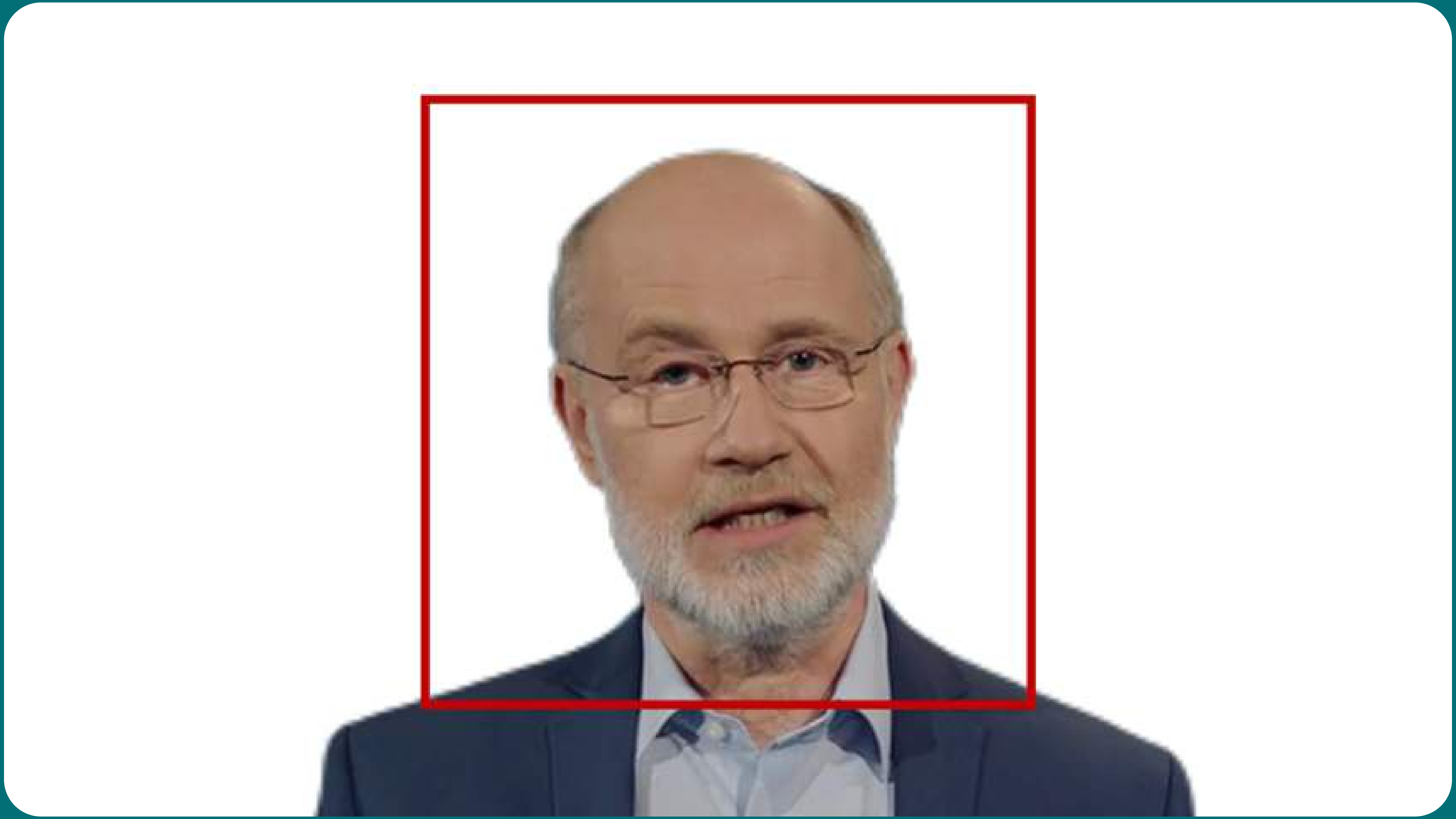
Realtime Deepfakes

Inference Workflow with TNG Realtime Deepfakes 2.0



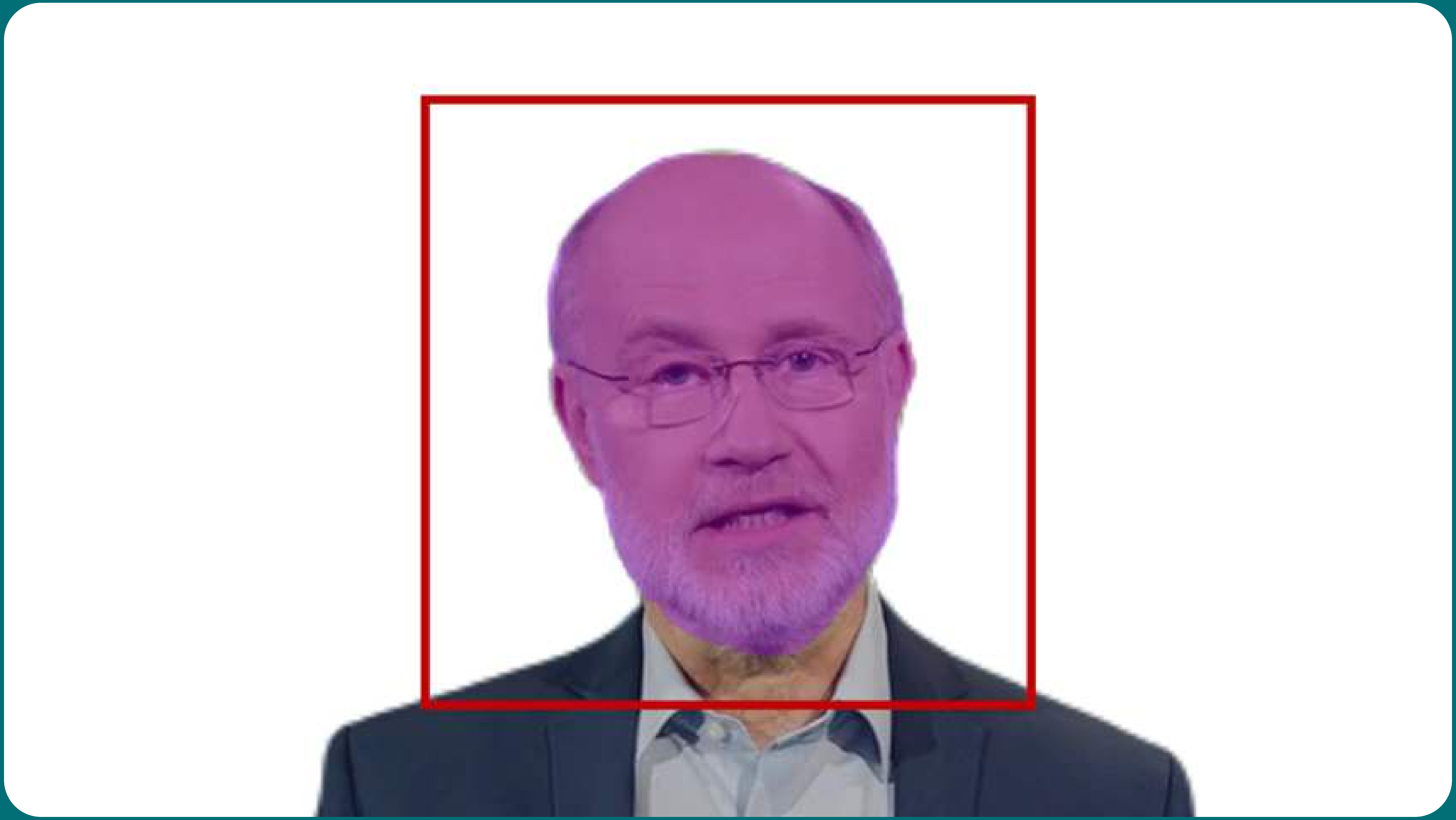
Realtime Deepfakes

Fast Face Detection Demo



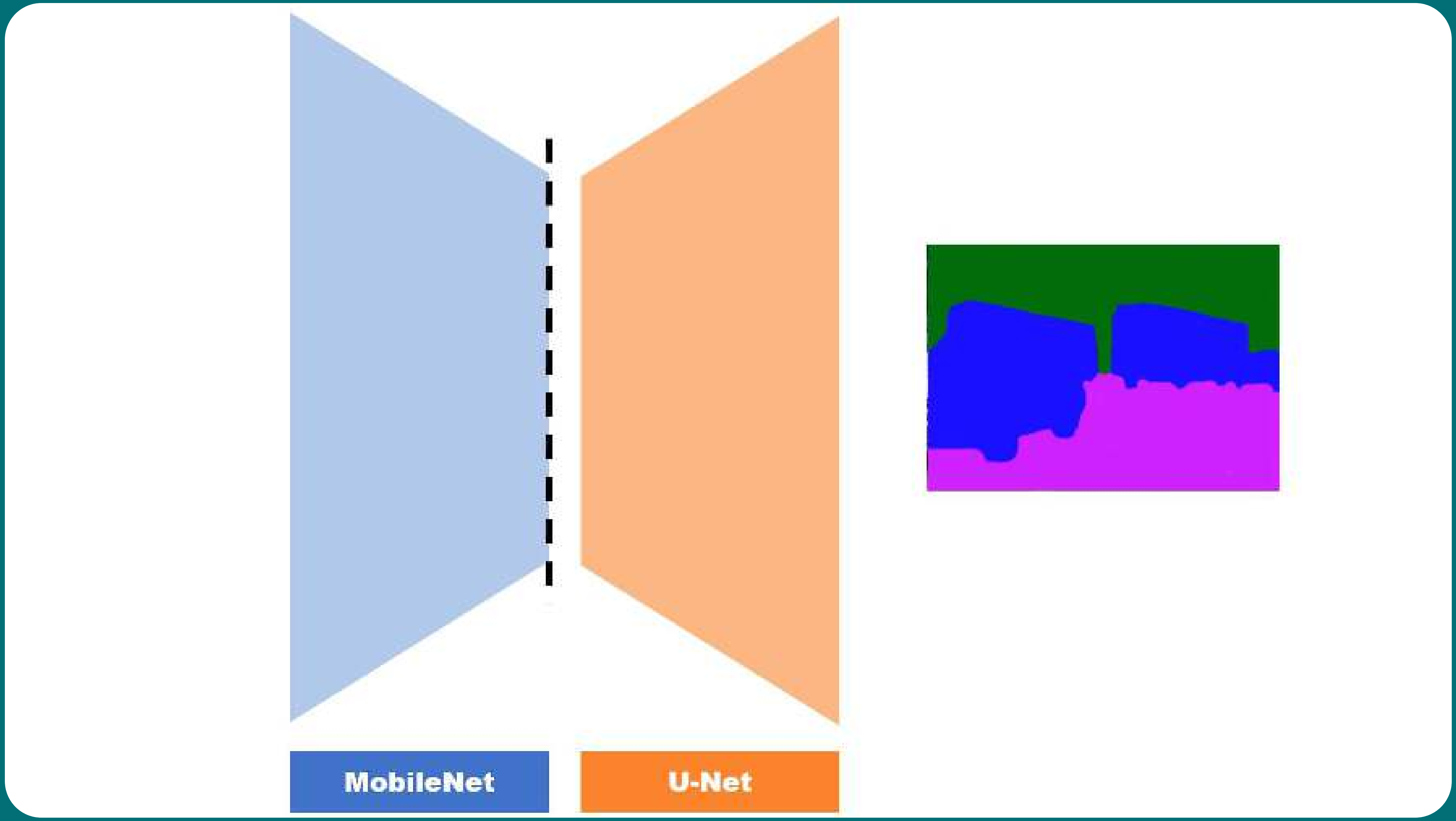
Realtime Deepfakes

Face Segmentation Demo



Realtime Deepfakes

Transfer Learning for Face Segmentation



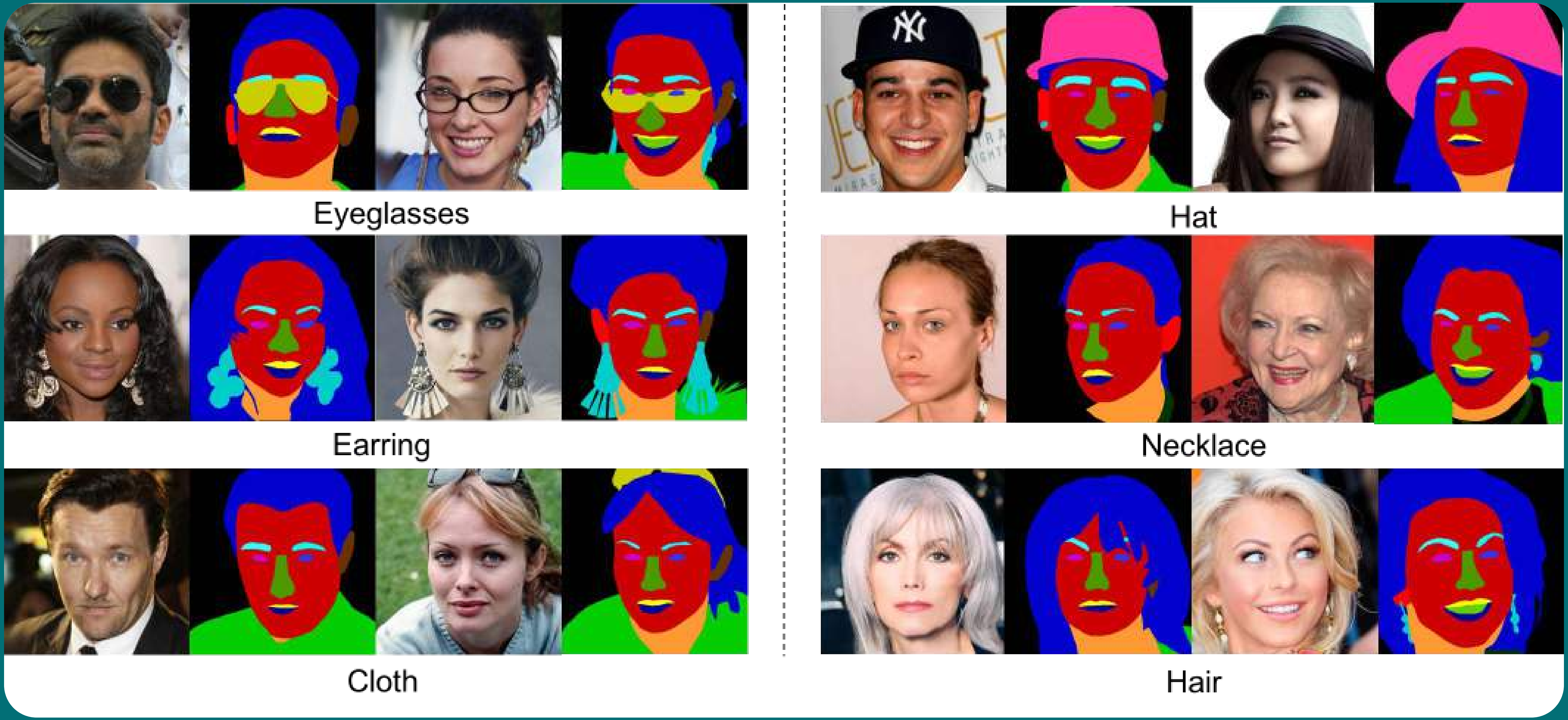
Realtime Deepfakes

Segmentation Dataset: CelebAMaskHQ

https://github.com/switchablenorms/CelebAMask-HQ

Realtime Deepfakes

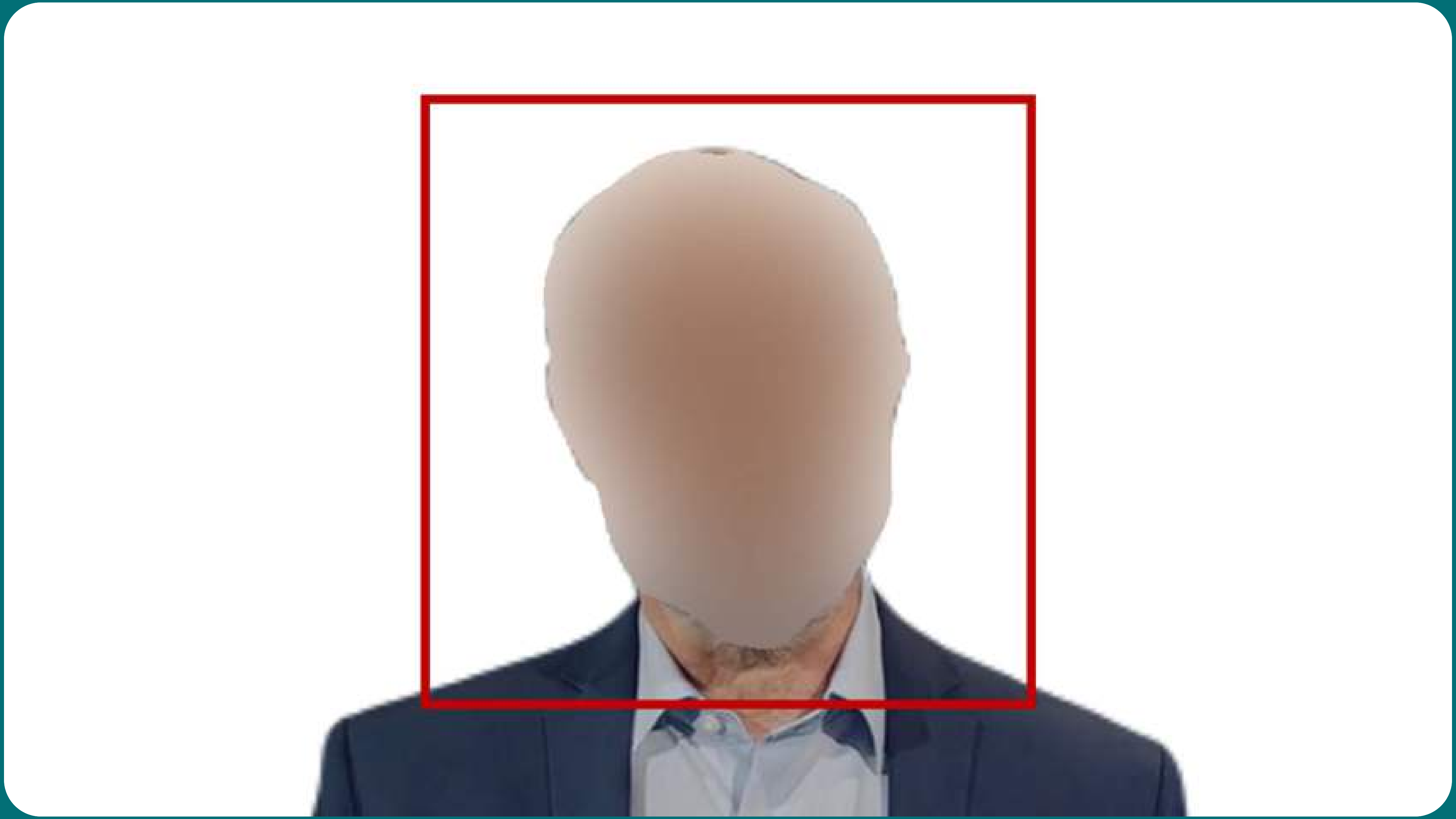
Segmentation Dataset: CelebAMaskHQ



https://github.com/switchablenorms/CelebAMask-HQ

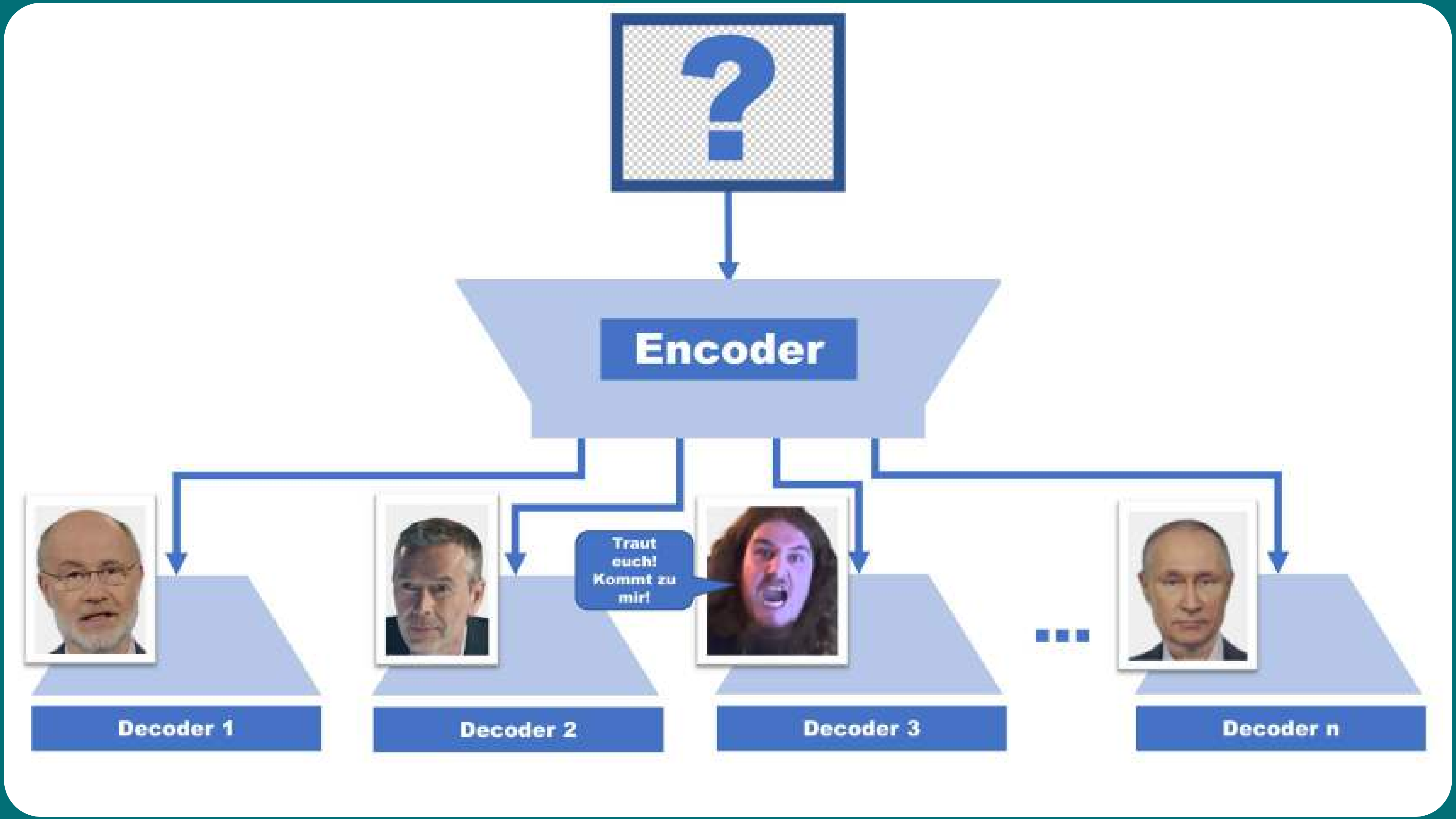
Realtime Deepfakes

OpenCV Inpainting Demo



Realtime Deepfakes

Multi-Decoder

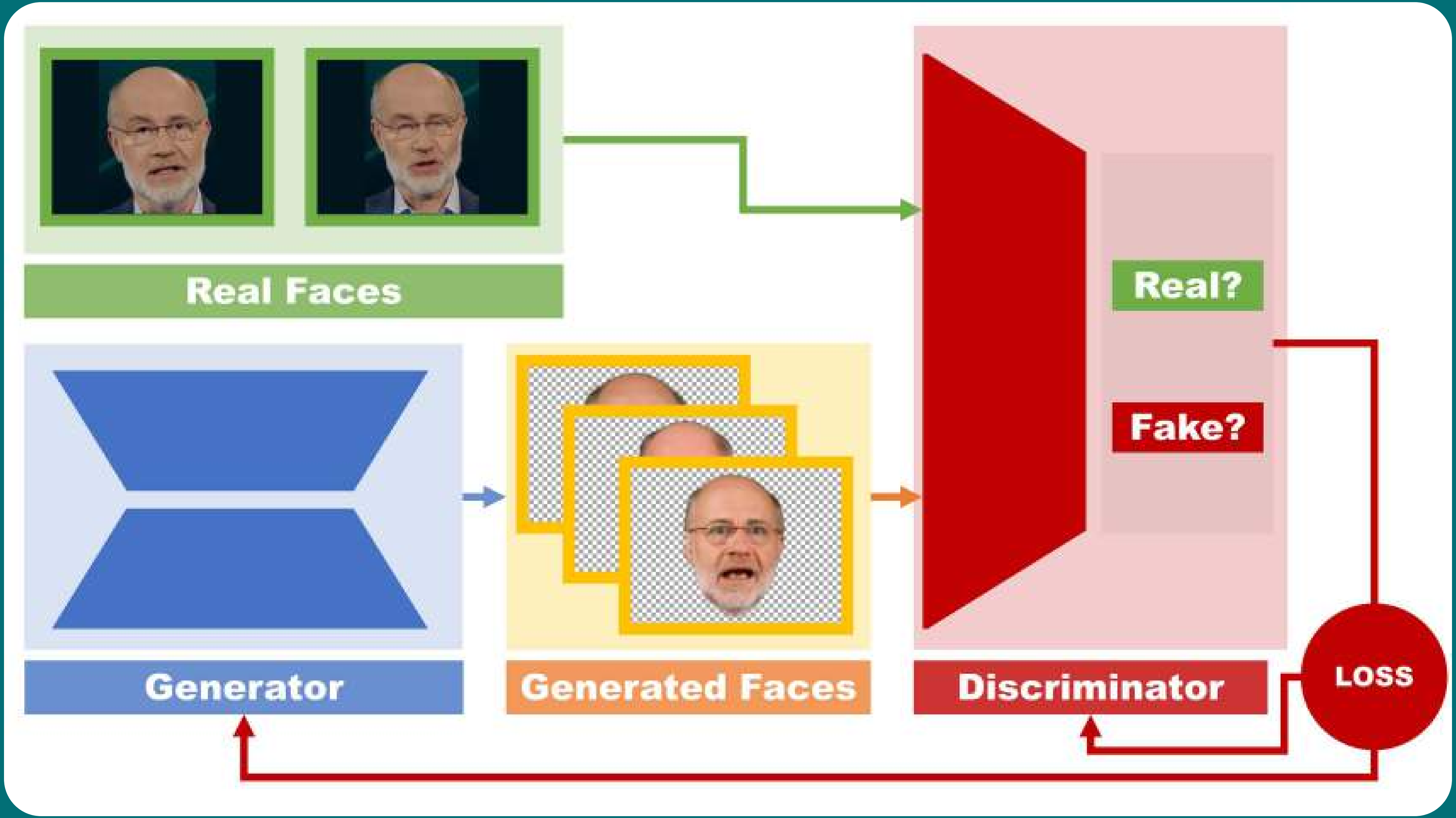


Realtime Deepfakes

First Results

Realtime Deepfakes

GAN (Generative Adversarial Networks) Training



Realtime Deepfakes

Breaking News

BREAKING
NEWS
r
ANGST VOR
FAKE-VIDEOS
A
Thomas Endres
Informatiker TNG Technology Consulting GmbH

Software ermöglicht Deep Fakes in Echtzeit
(heise.de)

Deutsche Software schafft Deepfakes in Echtzeit
(mobilegeeks.de)

Deep-Fake-KI: Forscher tauschen Gesichter in Webcam-Aufnahmen in Echtzeit
(GameStar)

Realtime Deepfakes

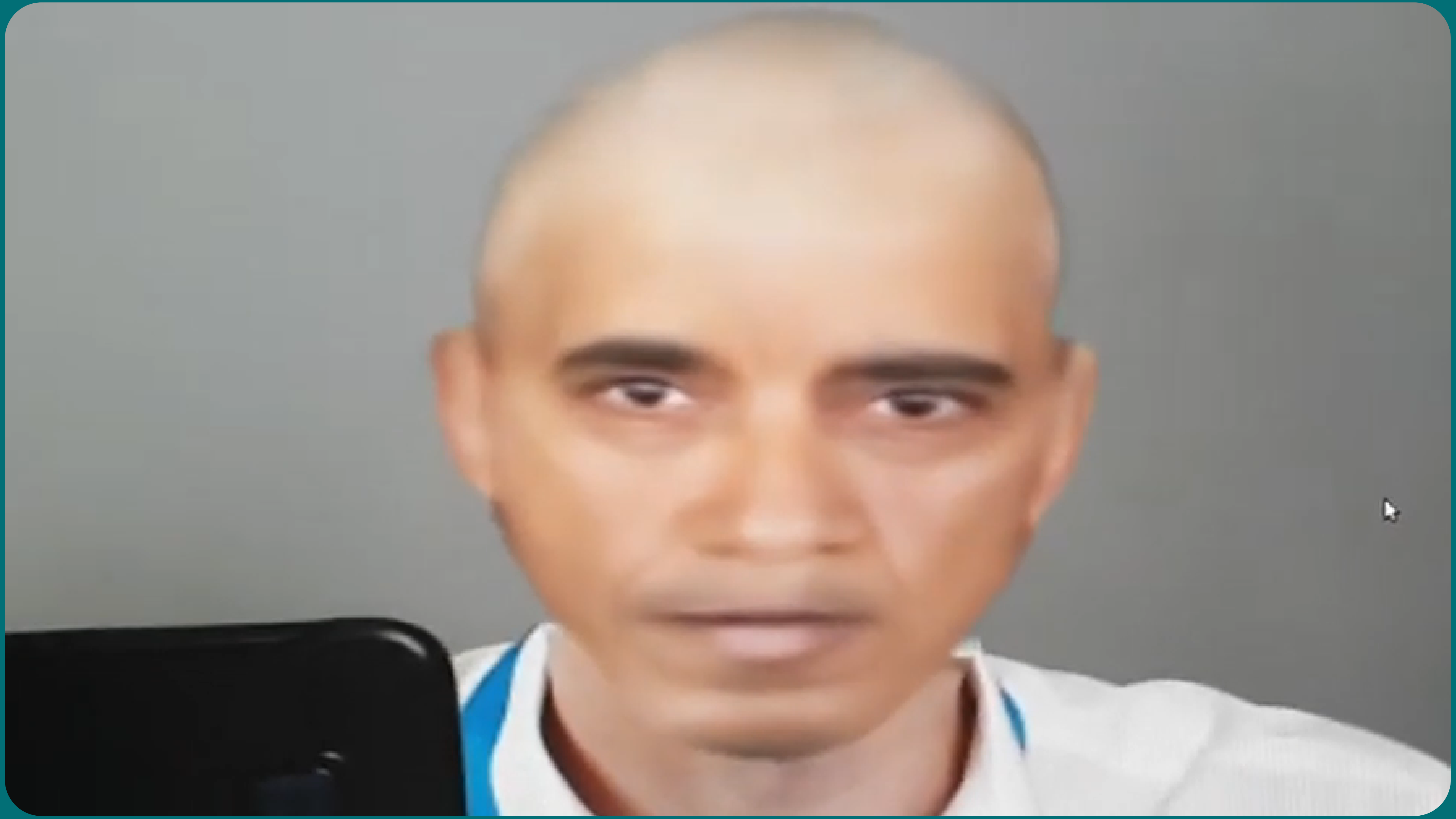
Talks! Talks! Talks!

Realtime Deepfakes

Leschs Kosmos (ZDF) Wants to Report on Realtime Deepfakes

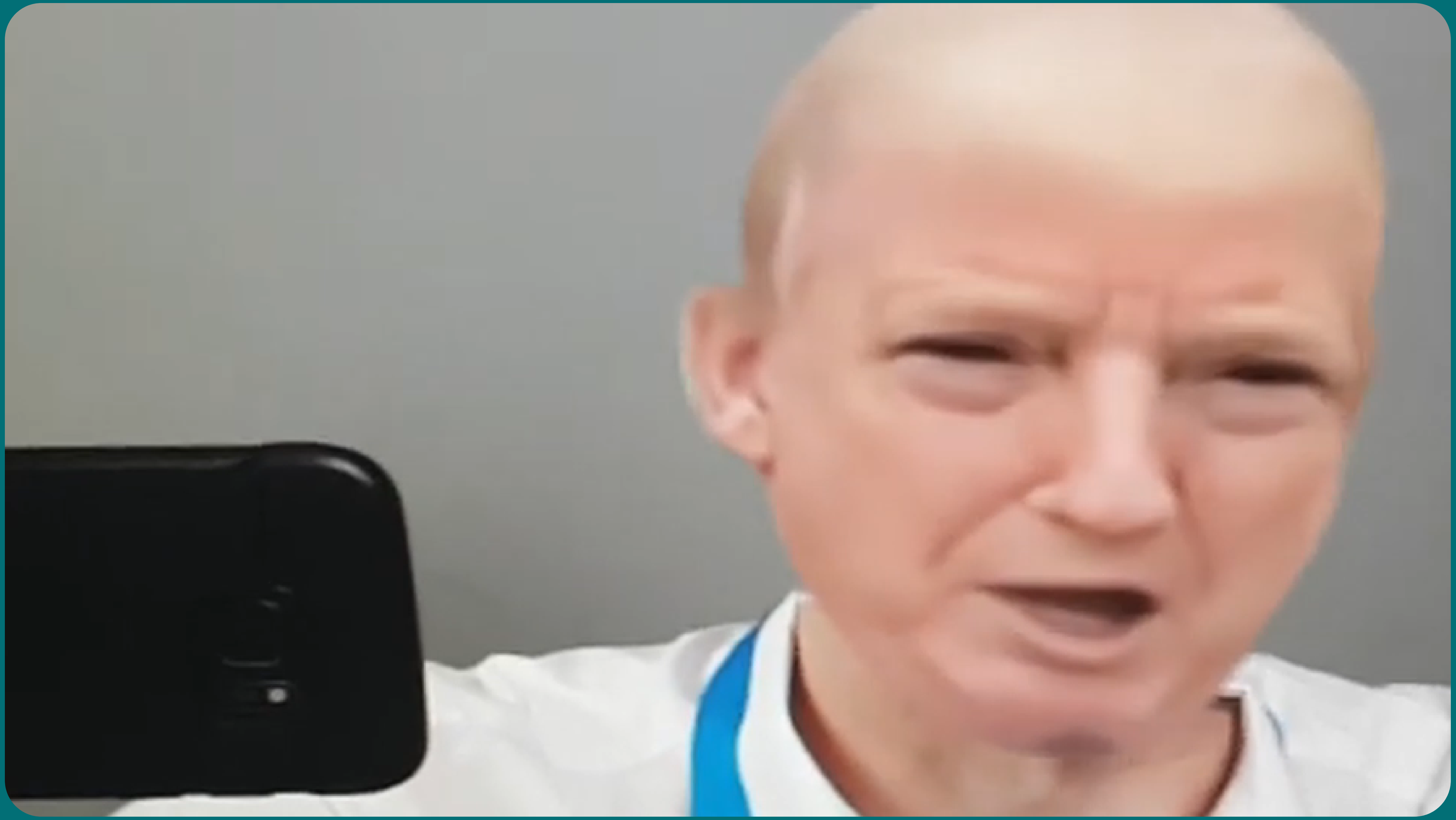
Realtime Deepfakes

Challenges: Blurry Details



Realtime Deepfakes

Challenges: Disappearing Hair



Agenda

- Deepfakes in a Nutshell
- Realtime Deepfakes
- Pushing Deepfakes to the Limit
- Videocalls with Deepfakes
- Conclusion

Deepfakes 2.1

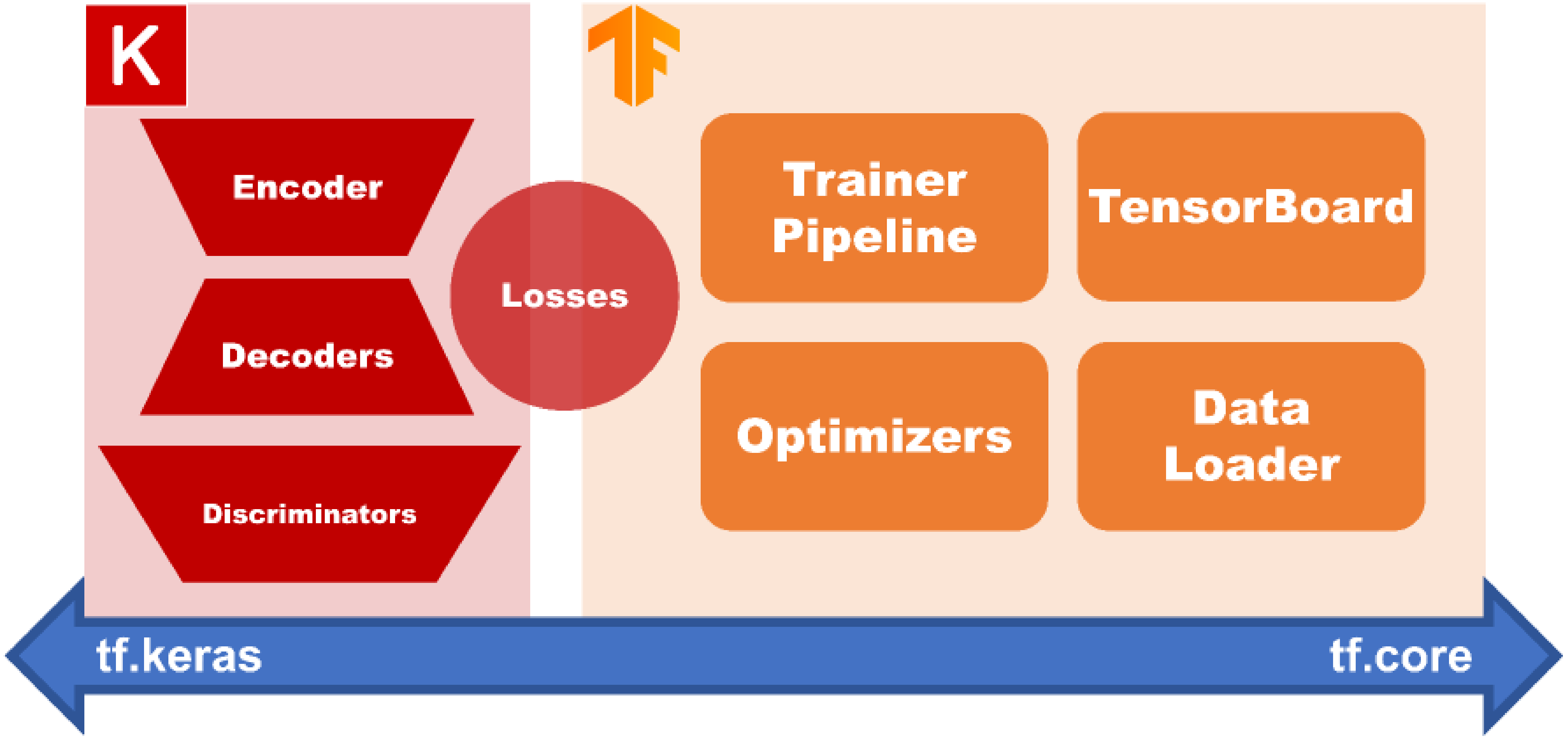
Introducing Tensorflow 2

Deepfakes 2.1

Tensorflow 💕 Keras

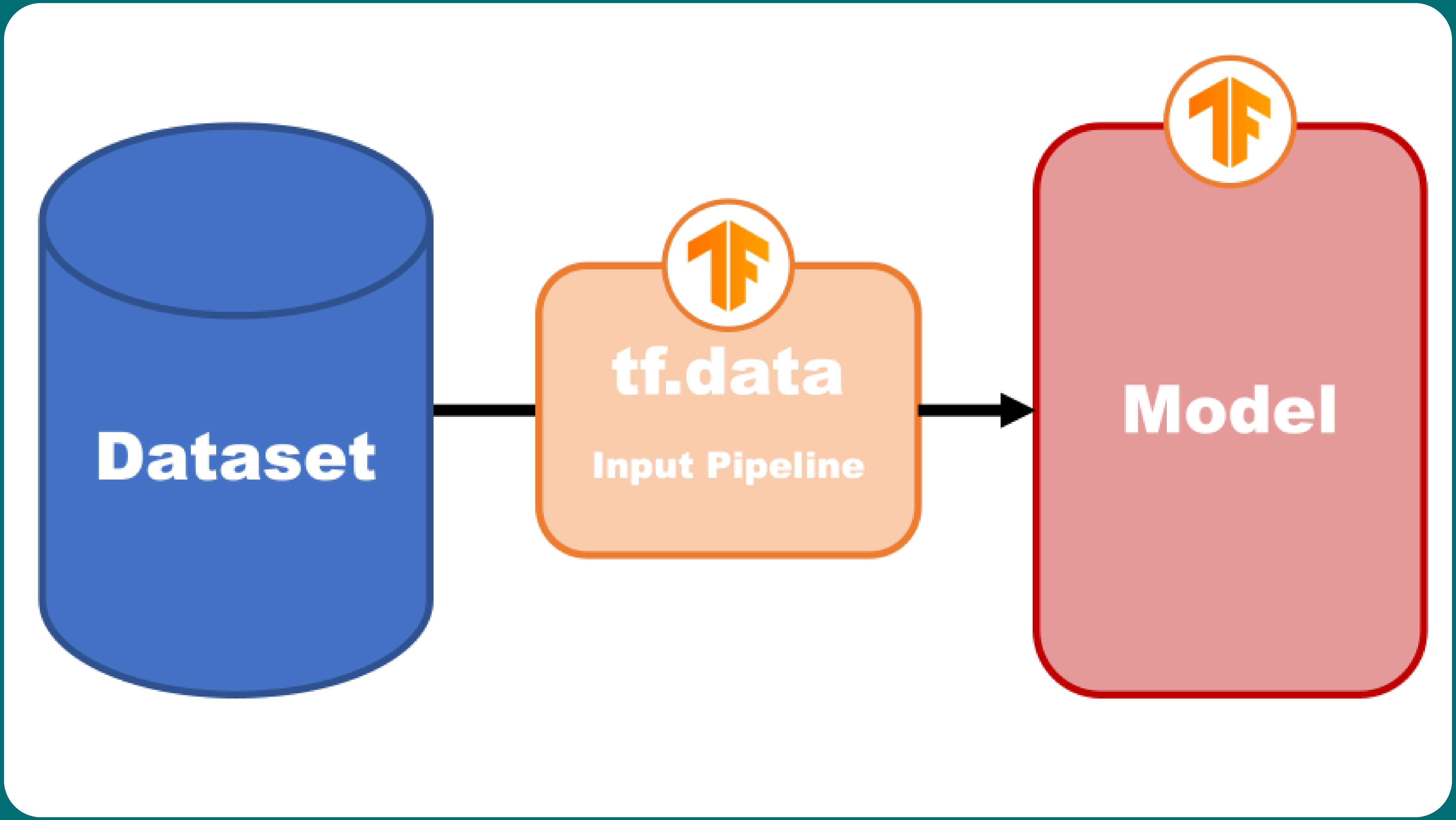
Deepfakes 2.1

Rewrite Trainer in Tensorflow 2



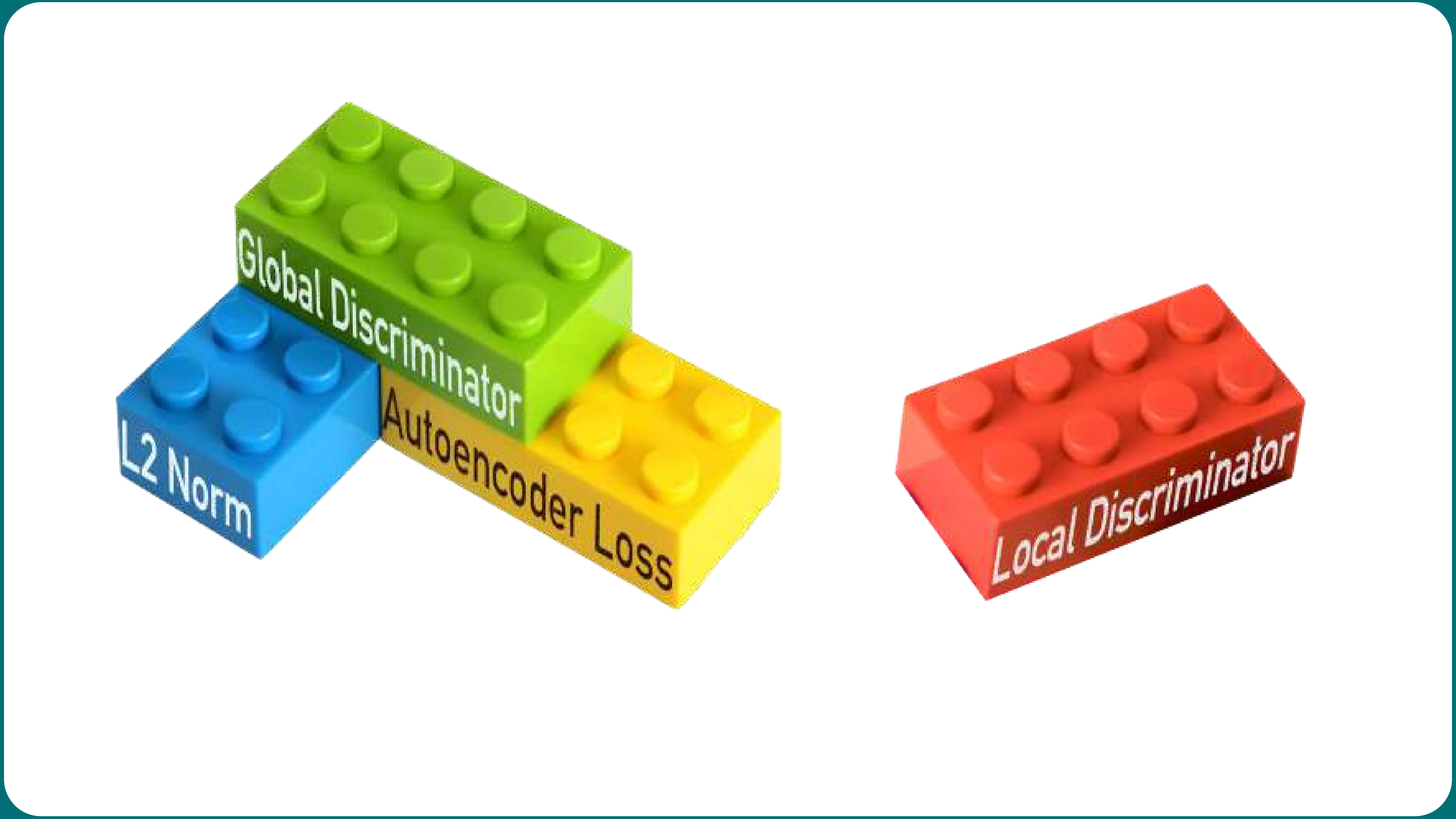
Deepfakes 2.1

tf.data: Faster loading of larger Datasets



Deepfakes 2.1

Modular Training Pipeline



Deepfakes 2.1

Remaining Issues

Realtime Deepfakes 2.0 - Challenges

1. Distortions
2. Alignment Problems
3. Centering Issues
4. Improvable Performance

Deepfakes 2.1

Introducing MediaPipe (2021)

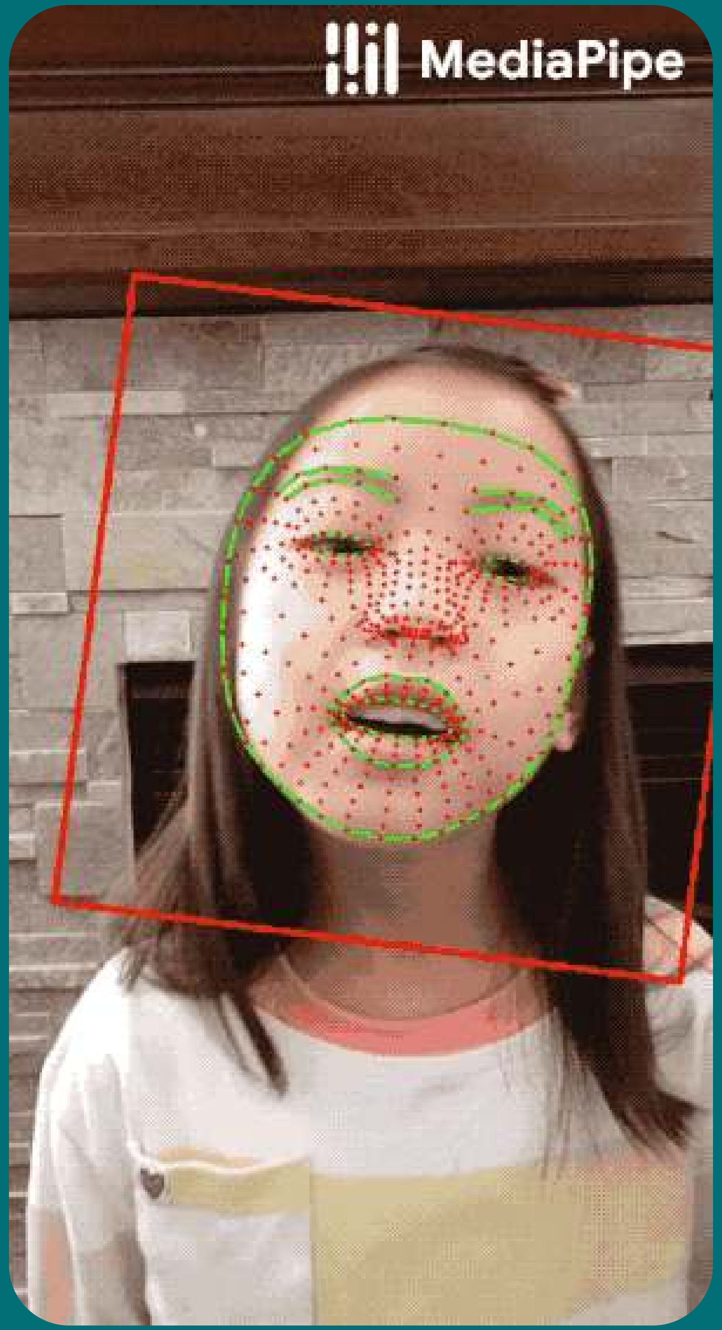
Deepfakes 2.1

Introducing MediaPipe (2021)

Ready-to-use solutions
Build once, deploy anywhere
End-to-End acceleration
Free and open source

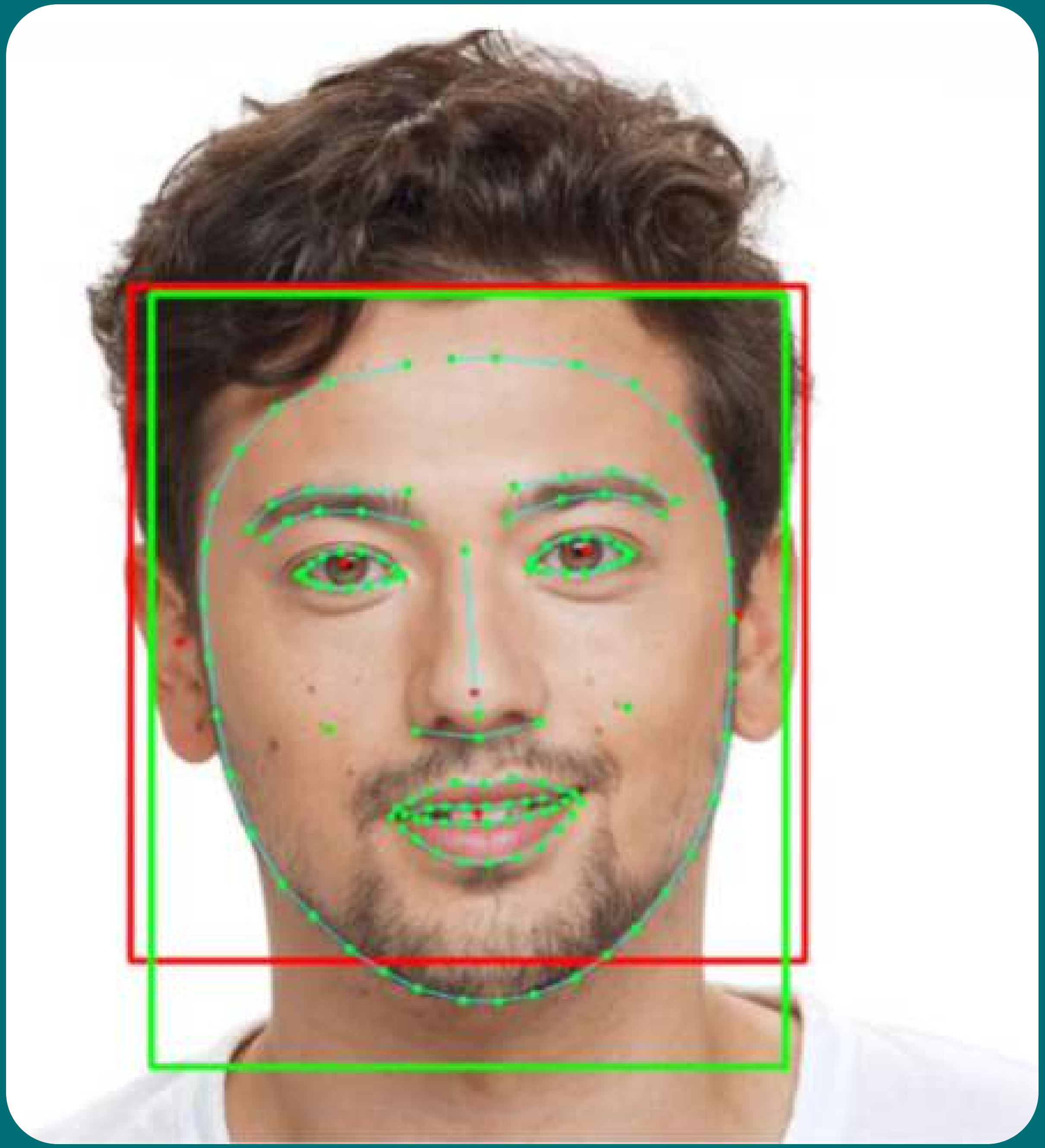
Deepfakes 2.1

Face Mesh for Fast Face Landmark Detection



Deepfakes 2.1

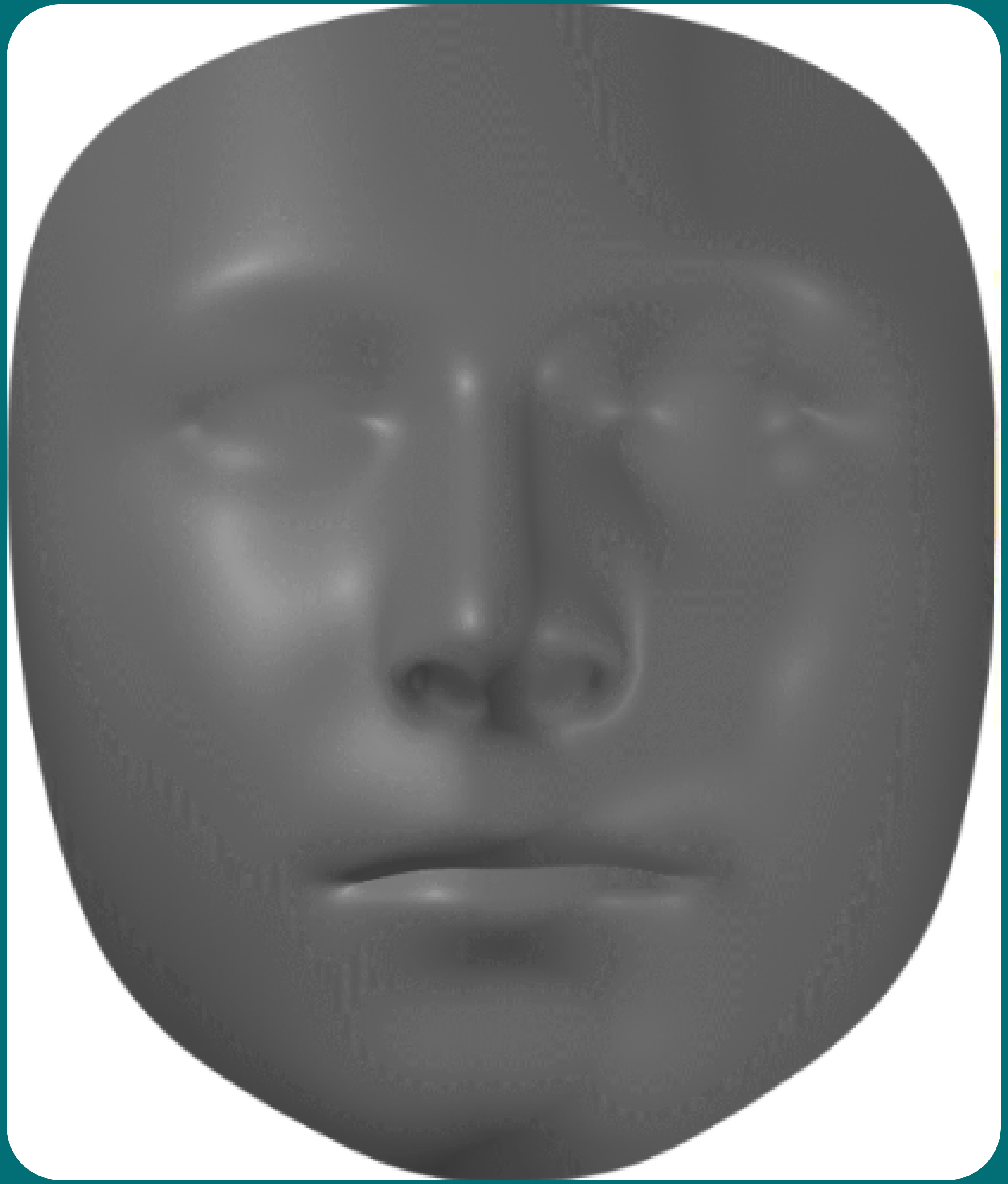
FaceMesh Is Based on BlazeFace Face Detection



SCAN ME

Deepfakes 2.1

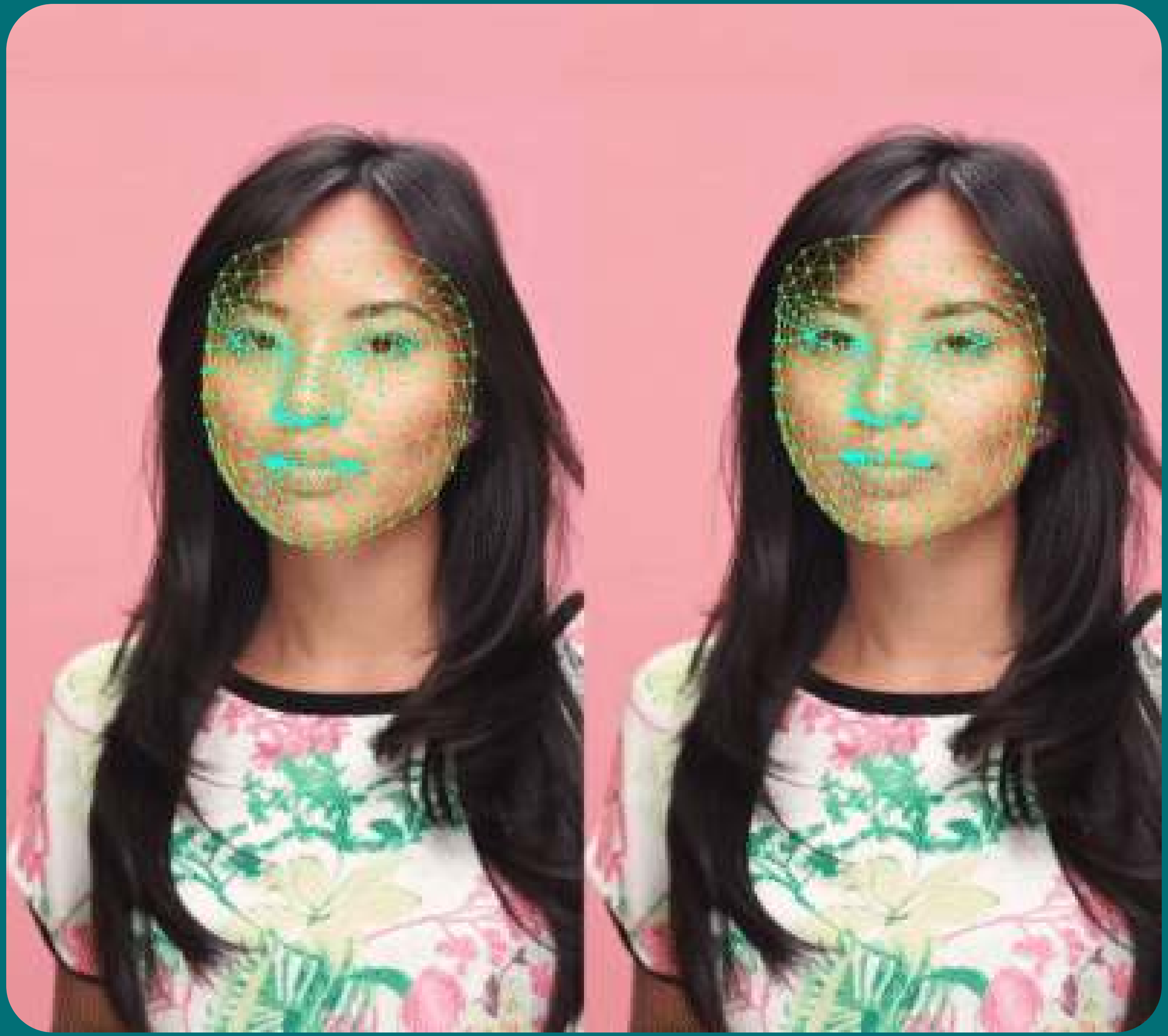
From Face Mesh with 468 Landmark Points to Facial Surface



SCAN ME

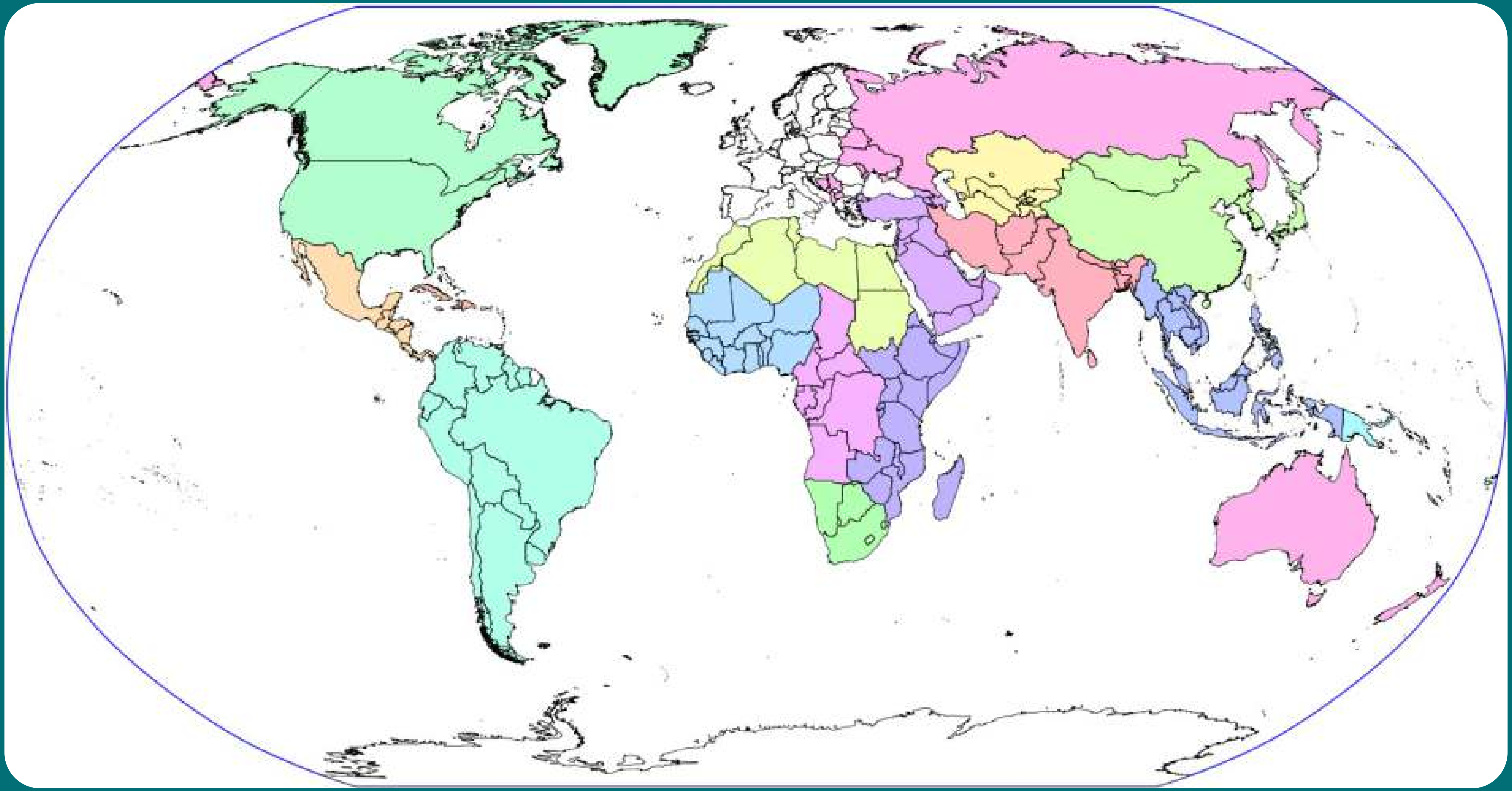
Deepfakes 2.1

Temporal Consistency



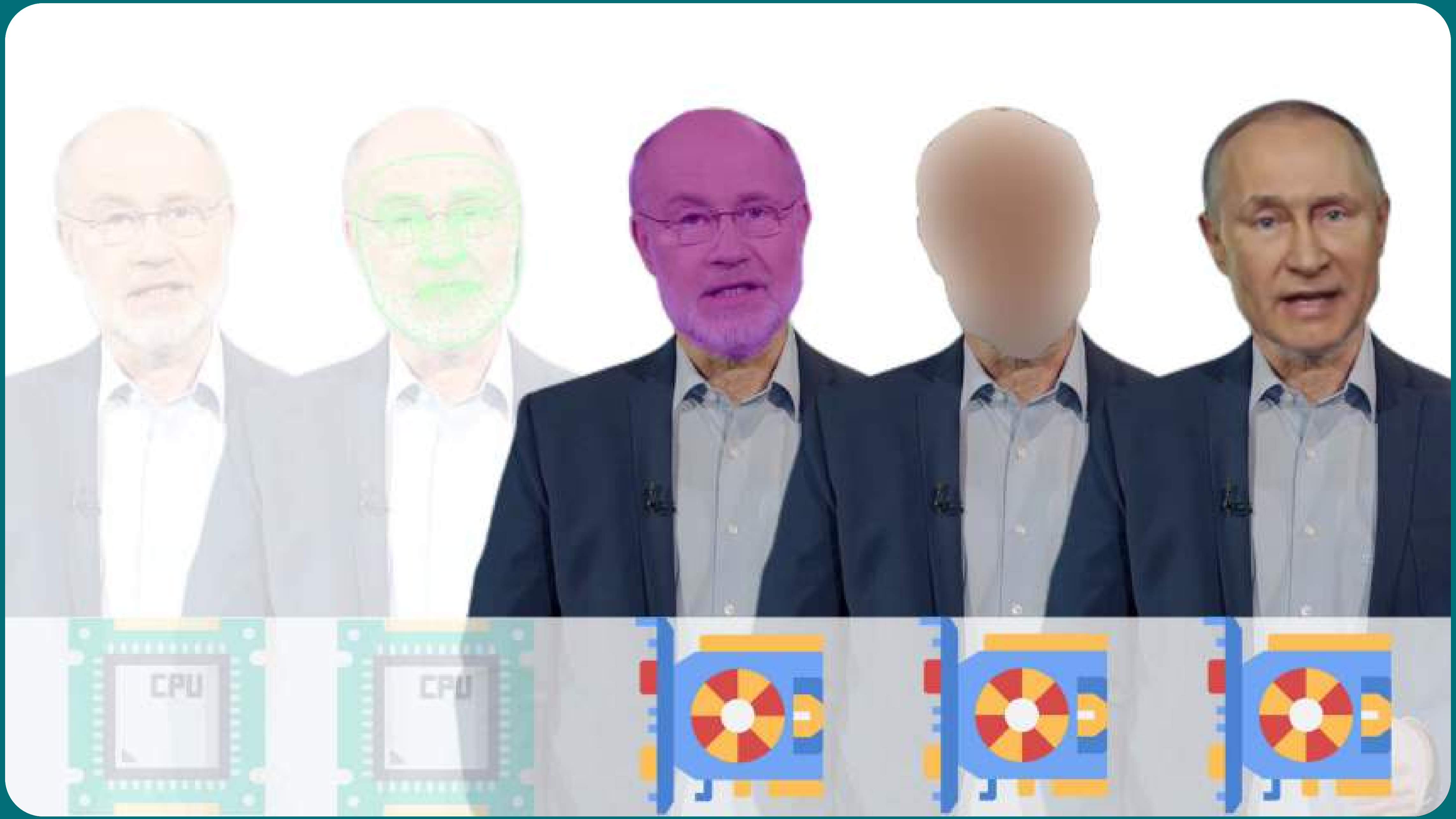
Deepfakes 2.1

FaceMesh Fairness Evaluation



Realtime Deepfakes 2.1

Inference Workflow



Agenda

- Deepfakes in a Nutshell
- Realtime Deepfakes
- Pushing Deepfakes to the Limit
- Videocalls with Deepfakes
- Conclusion

Pro7 Galileo

Can You Cheat People on Video Calls?

Pro7 Galileo

Can You Cheat People on Video Calls?

Harro Füllgrabe

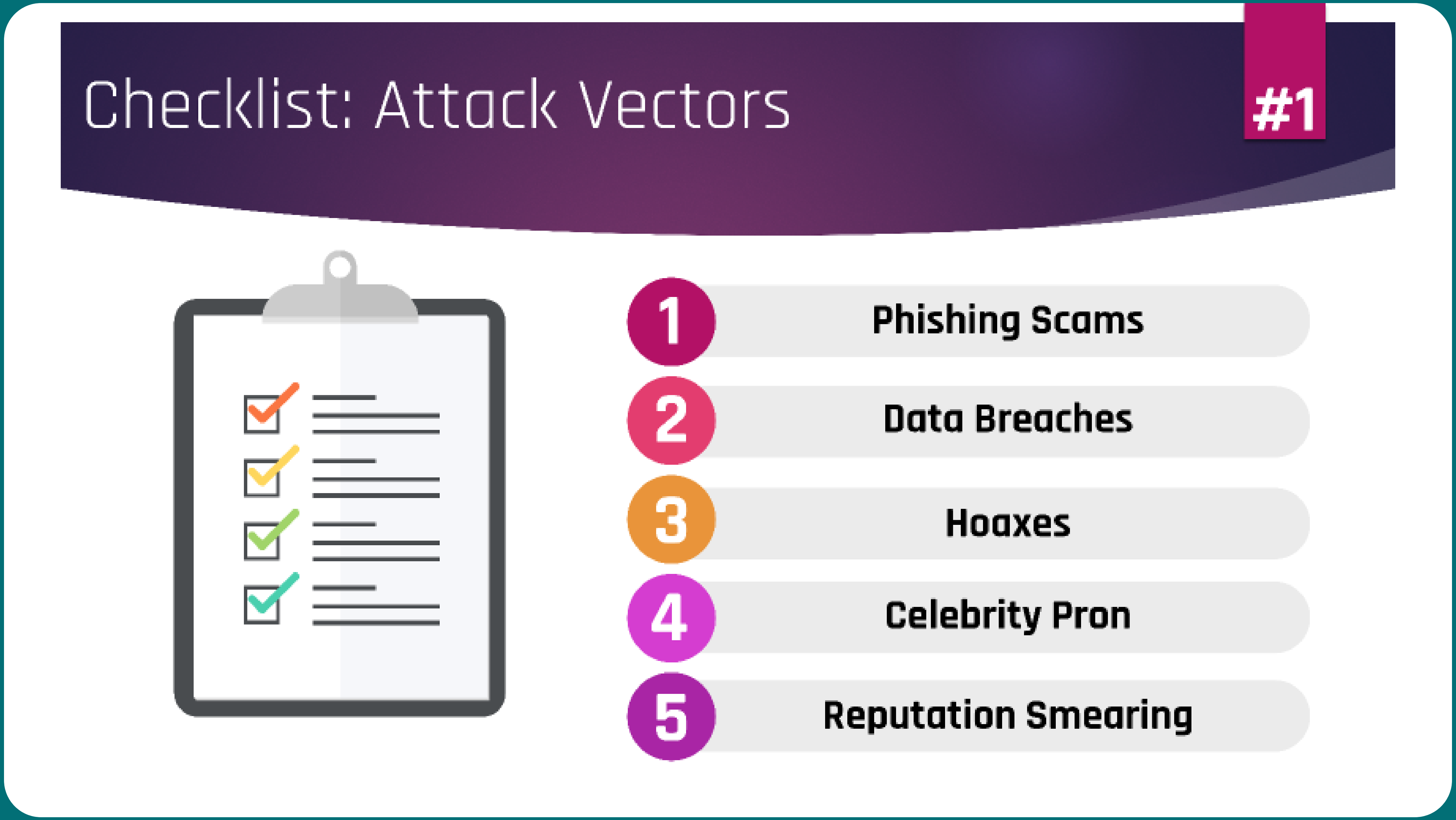
Matthias Fiedler

Pro7 Galileo

Can You Cheat People on Video Calls?

Realtime Deepfakes as Attack Vector

They Are Real and You Should Know about That!



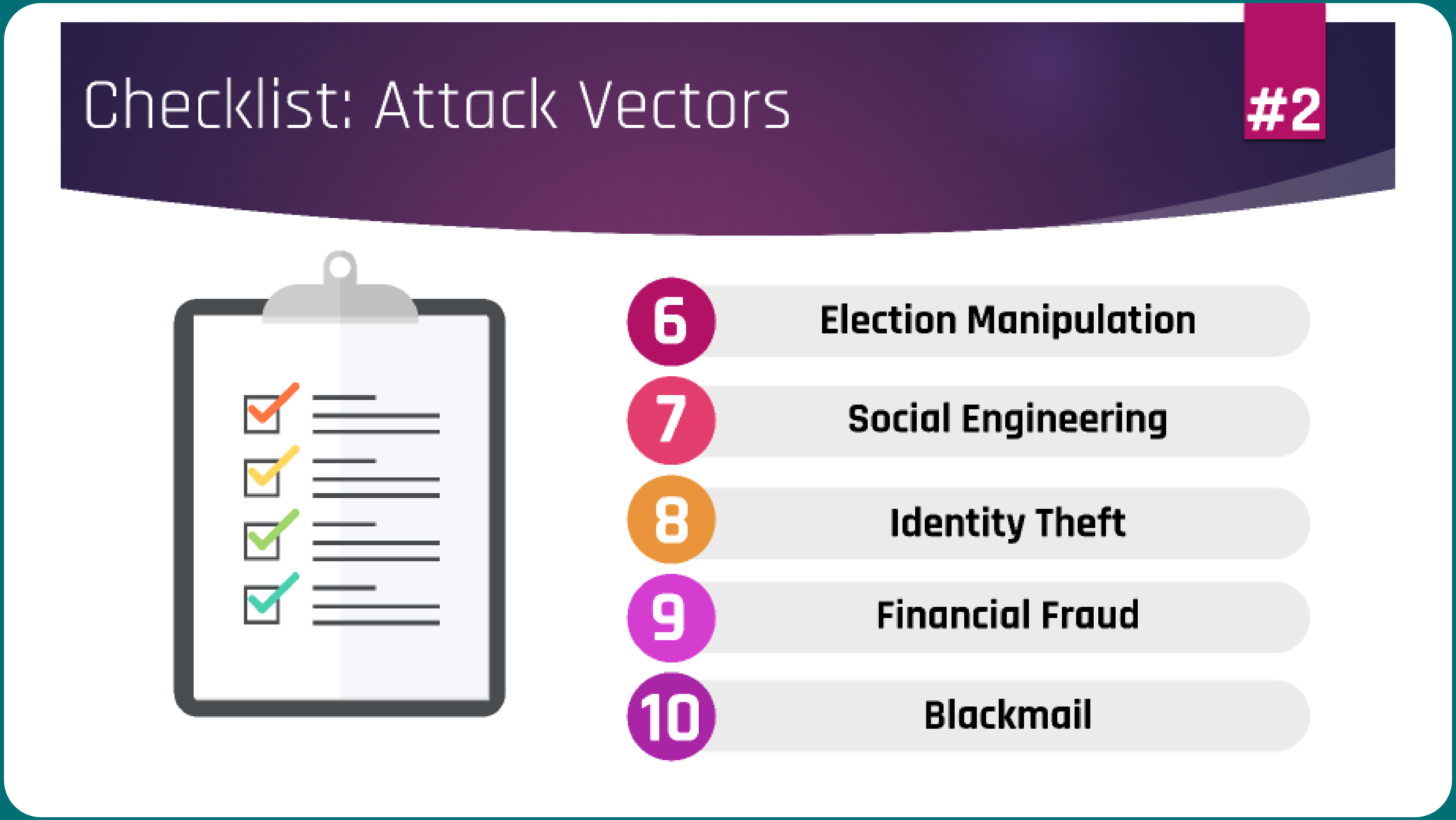
Checklist: Attack Vectors

#1

1. Phishing Scams
2. Data Breaches
3. Hoaxes
4. Celebrity Pron
5. Reputation Smearing

Realtime Deepfakes as Attack Vector

They Are Real and You Should Know about That!



Checklist: Attack Vectors

#2

6. Election Manipulation
7. Social Engineering
8. Identity Theft
9. Financial Fraud
10. Blackmail

Scam Alert!⚠

Woman Thought Vin Diesel Loved Her - Sent £5,000 in Online Scam

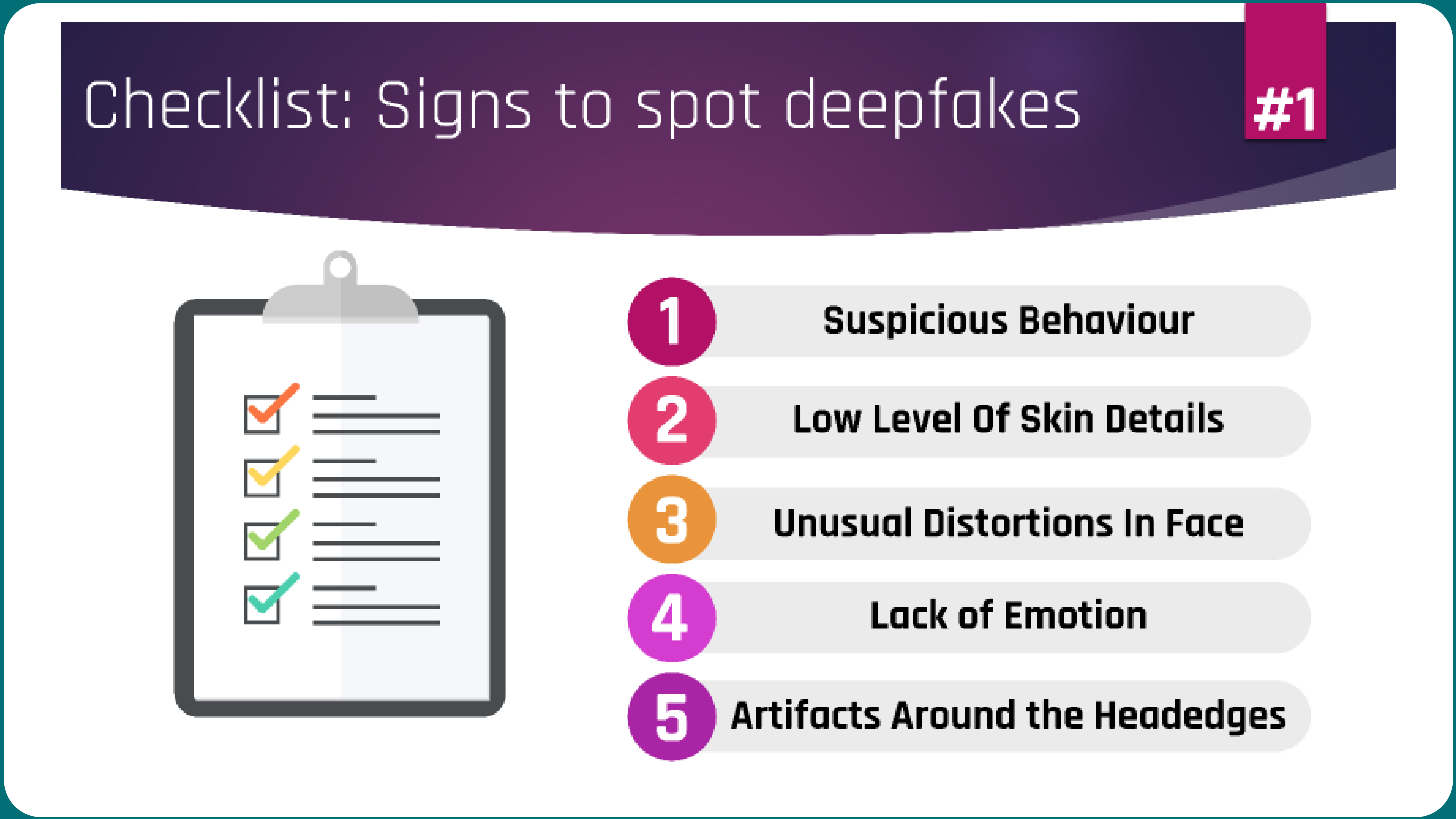
https://www.ladbible.com/news/news-woman-thought-vin-diesel-loved-her-sends-him-5000-20200819

Pro7 Galileo

Part 2 - Fooling Parents

Realtime Deepfakes As Attack Vector

They Are Real and You Should Know about That!



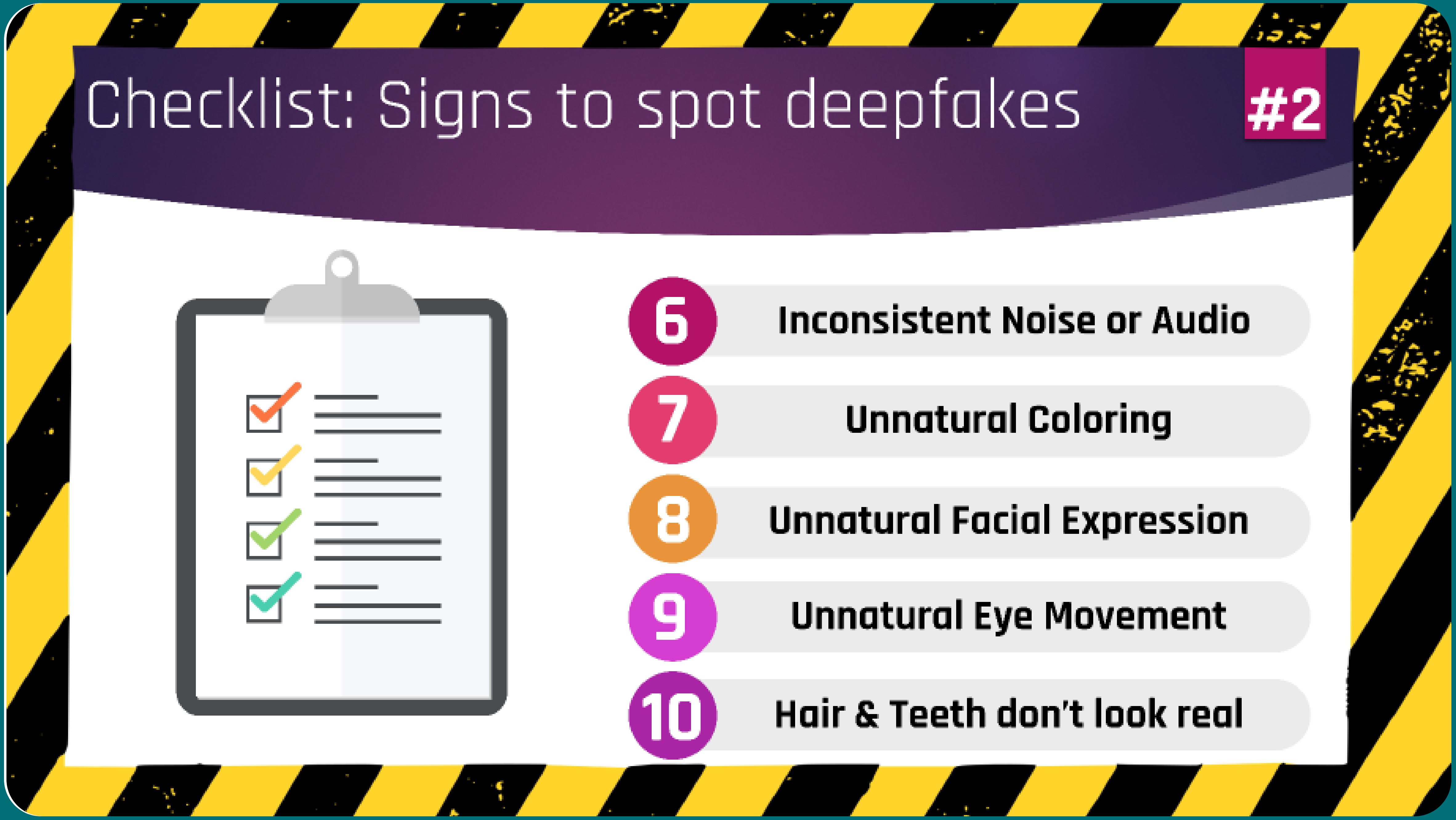
Checklist: Signs to spot deepfakes

#1

1. Suspicious Behaviour
2. Low Level Of Skin Details
3. Unusual Distortions In Face
4. Lack of Emotion
5. Artifacts Around the Headedges

Realtime Deepfakes As Attack Vector

They Are Real and You Should Know about That!



Checklist: Signs to spot deepfakes #2

6 Inconsistent Noise or Audio

7 Unnatural Coloring

8 Unnatural Facial Expression

9 Unnatural Eye Movement

10 Hair & Teeth don't look real

Agenda

- Deepfakes in a Nutshell
- Realtime Deepfakes
- Pushing Deepfakes to the Limit
- Videocalls with Deepfakes
- <u>Conclusion</u>

Movie Industry

Our Predictions came true!

Lucasfilm hires the YouTube deepfaker who put its Luke, Leia and Tarkin cameos to shame

(theverge.com)

Lucasfilm Hires YouTuber After His Deepfake of Luke Skywalker in *The Mandalorian* Goes Viral

(gizmodo.com)

Other AI related talks

SCAN ME

Style Transfer AI

This talk introduces you
into deep neural networks,
how they work internally and
how they process images.

Artificial Neurons, Gradient Descent,
Deep Neural Networks, Cost Function

SCAN ME

Realtime Deepfakes

This talk introduces you
into how deep fakes can be created
and what it took to realize deep fakes
in realtime.

Deep Neural Networks, Autoencoder,
Transfer Learning,
Generative Adversarial Networks

Speakers

Thomas Endres

Partner

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2018

Martin Förtsch

Principal Consultant

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2018

Jonas Mayer

Senior Consultant

Bedroom DJ
Teakwondo Black Belt
GameStar Certified Hacker
Intel® Software Innovator