DOCENT | studios

CornCon 11

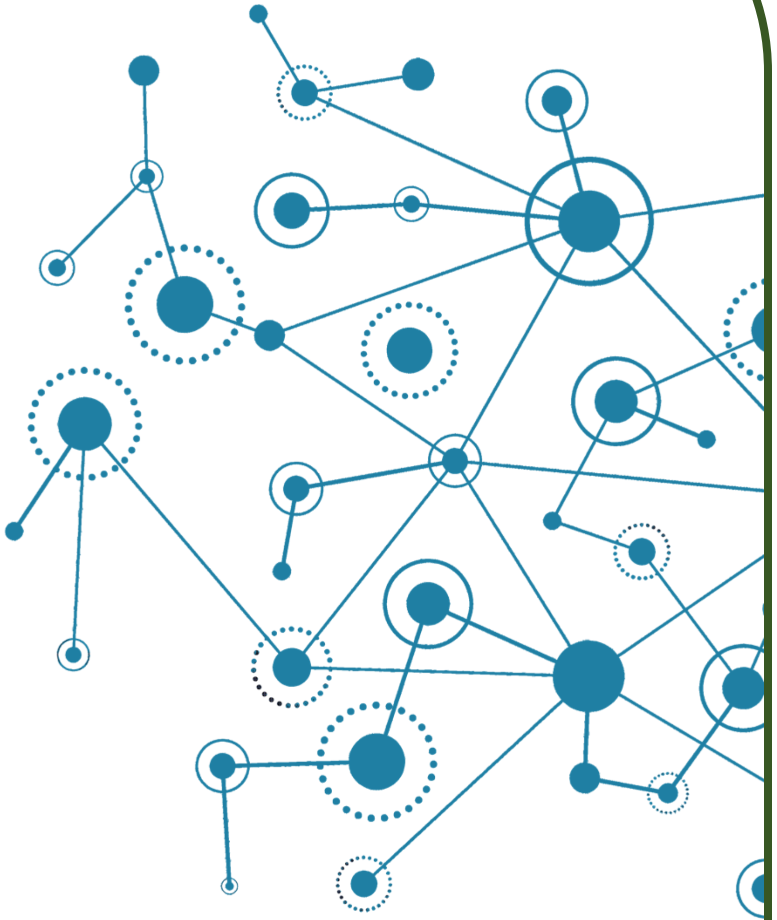
Manifest your inner Cyber Superhero

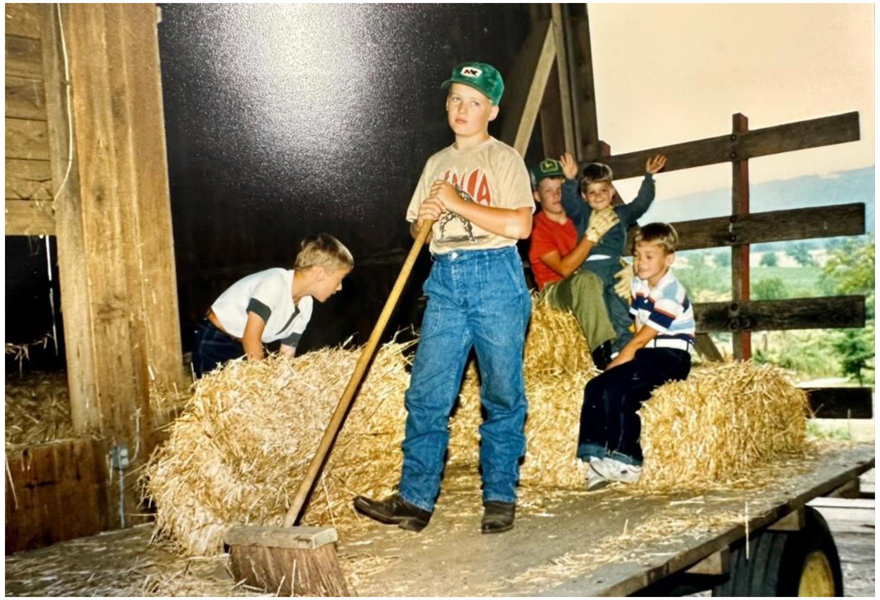
AI Deepfake Detection: The Process and Security Considerations

October 11, 2025

Joshua Miller

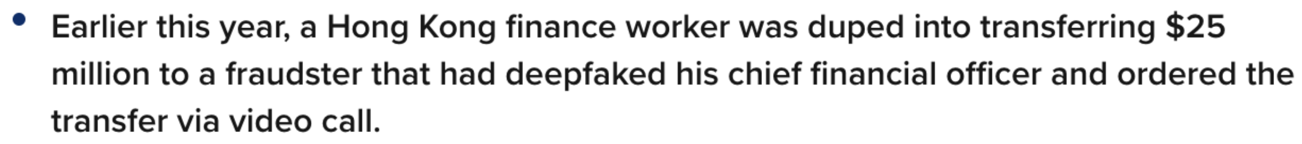
Chief of Staff to CISO
John Deere





Joshua Miller

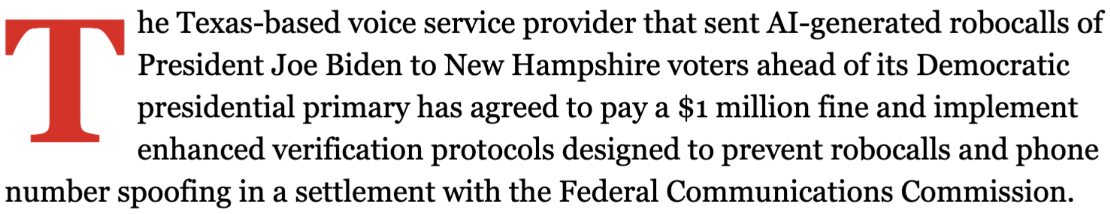
- **Current role:** Sr. Cybersecurity Engineer
- Global IT Security
- **Career path:**
  - Years with John Deere: 20 years
    - Chief of Staff to CISO
    - Enterprise Risk Manager and 3rd Party Risk
    - Chief Security Architect, Global IT Security
    - Technology Architect, Enterprise Architecture
    - Team Lead, HPC and Windchill Central Services
    - Technology Architect, High Performance Computing
    - Project Manager, High Performance Computing
    - SME - Technical lead - Enterprise Email and Fax
  - Previous employer/s:
    - US Navy, Yeoman
- **Education:**
  - MIS (Master of Information Systems) – 2009
  - BA, Computer Science - 2002
- **Family profile:**
- Married with 3 children
- Lives in Bettendorf, Iowa
- **Hobbies & personal interests:**
- Luthier, CrossFit, Runner, Hawkeye football, activities with family, motorcycles
- Linkedin
- Guitar Page Instagram



- Earlier this year, a Hong Kong finance worker was duped into transferring $25 million to a fraudster that had deepfaked his chief financial officer and ordered the transfer via video call.

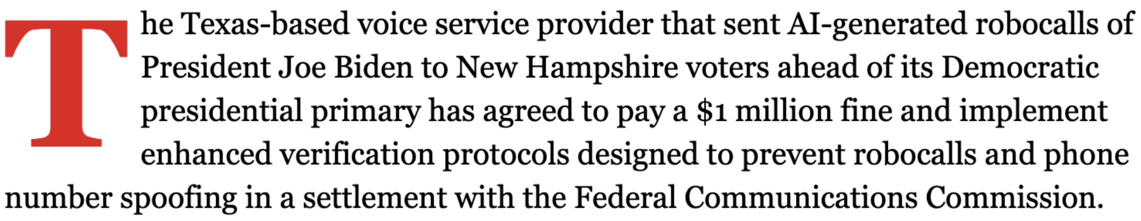
What are Deepfakes?

- Deepfakes are audio/videos/images created using artificial intelligence
- They are manipulated to depict events/messages that never actually happened
- This media can be harmful and cause serious consequences
  - Identity Fraud
  - Financial
  - Reputational damage
  - Manipulation of public opinion
  - ________________________________
- Stats
- 1 in 4 leaders unfamiliar with deepfakes
- 31% underestimate deepfake fraud risk
- 32% doubt employee ability to detect deepfakes
- 1 in 10 executives have already faced deepfake threats
- 10x increase in deepfakes detected globally across all industries in 2023.



The Texas-based voice service provider that sent AI-generated robocalls of President Joe Biden to New Hampshire voters ahead of its Democratic presidential primary has agreed to pay a $1 million fine and implement enhanced verification protocols designed to prevent robocalls and phone number spoofing in a settlement with the Federal Communications Commission.

AI Deepfake Statistics


The Texas-based voice service provider that sent AI-generated robocalls of President Joe Biden to New Hampshire voters ahead of its Democratic presidential primary has agreed to pay a $1 million fine and implement enhanced verification protocols designed to prevent robocalls and phone number spoofing in a settlement with the Federal Communications Commission.

25 US States have AI Deepfake regulations in elections

Market projection: The deepfake market is projected to reach $1.9 billion by 2030.

Detection accuracy: Texas State University researchers developed a deepfake detection method with 96.4% accuracy in 2023. Chinese researchers have developed AI models capable of detecting deepfakes with 90% accuracy.

Social media platforms: Major social media platforms like Facebook and Twitter have removed thousands of deepfake videos since 2018, with counts rising each year.

Detection challenges: Deepfake detection algorithms have improved their accuracy from 70% in 2019 to over 95% in 2023. However, the number of false positive alerts from deepfake detection systems has decreased by 35% between 2021 and 2023.

Legal actions: The number of legal actions related to deepfakes increased by 150% between 2020 and 2023.

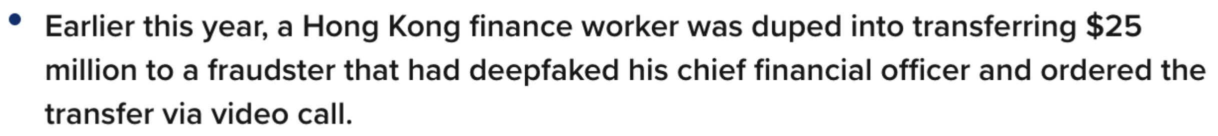
Gartner®

According to Gartner By 2027, 50% of enterprises will be investing in disinformation security products or services and by 2028 25% of all job applicants will be fake to conduct fraud or corporate harm by nation states.

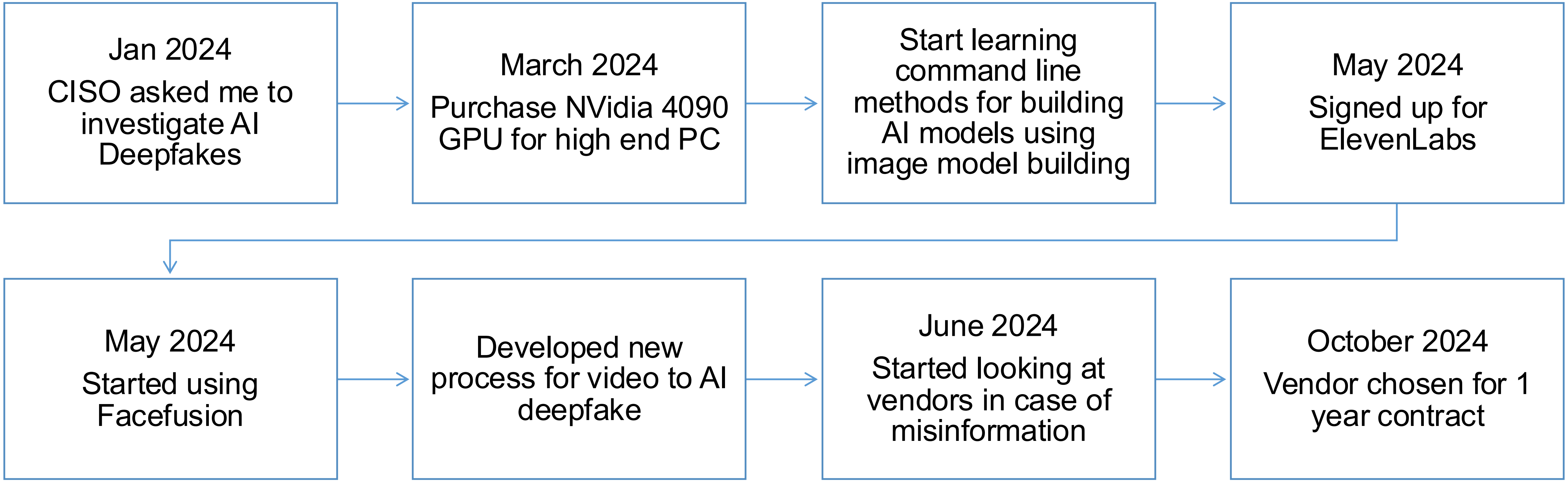
DIVE BRIEF

A job applicant can be deepfaked into existence in 70 minutes, cybersecurity firm finds

https://www.hrdive.com/news/fake-job-applicant-deepfake-70-minutes/745924/


- Earlier this year, a Hong Kong finance worker was duped into transferring $25 million to a fraudster that had deepfaked his chief financial officer and ordered the transfer via video call.

My Journey: High Level Deepfake Learning Timeline



Jan 2024
CISO asked me to investigate AI Deepfakes

March 2024
Purchase NVidia 4090 GPU for high end PC

Start learning command line methods for building AI models using image model building

May 2024
Signed up for ElevenLabs

May 2024
Started using Facefusion

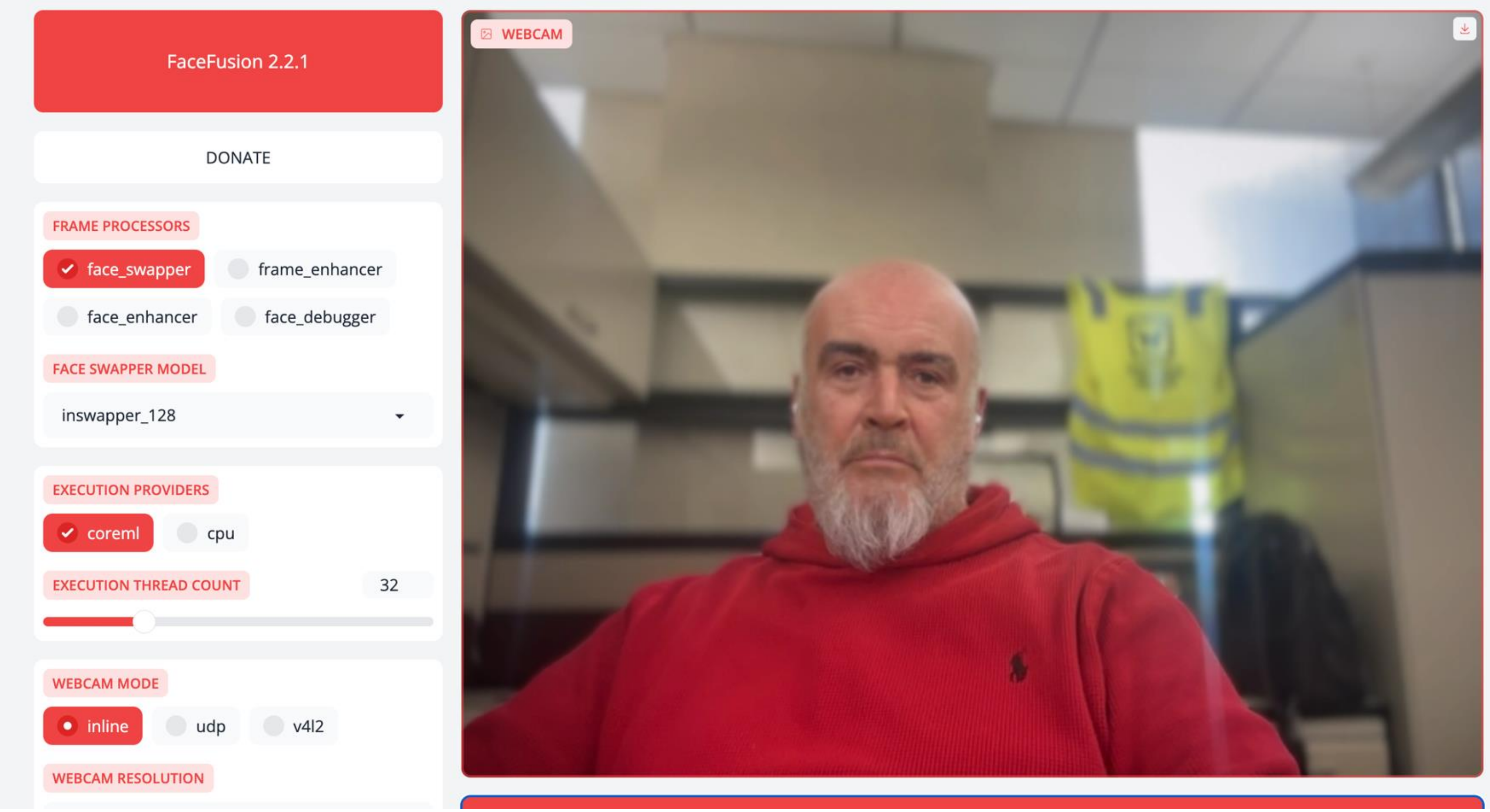
Developed new process for video to AI deepfake

June 2024
Started looking at vendors in case of misinformation

October 2024
Vendor chosen for 1 year contract

Live Meeting Deepfakes

- Facefusion gives the ability to go live as someone else with 1 single image of a person



FaceFusion 2.2.1

DONATE

FRAME PROCESSORS

☑ face_swapper ○ frame_enhancer

○ face_enhancer ○ face_debugger

FACE SWAPPER MODEL

inswapper_128

EXECUTION PROVIDERS

☑ coreml ○ cpu

EXECUTION THREAD COUNT 32

WEBCAM MODE

● inline ○ udp ○ v4l2

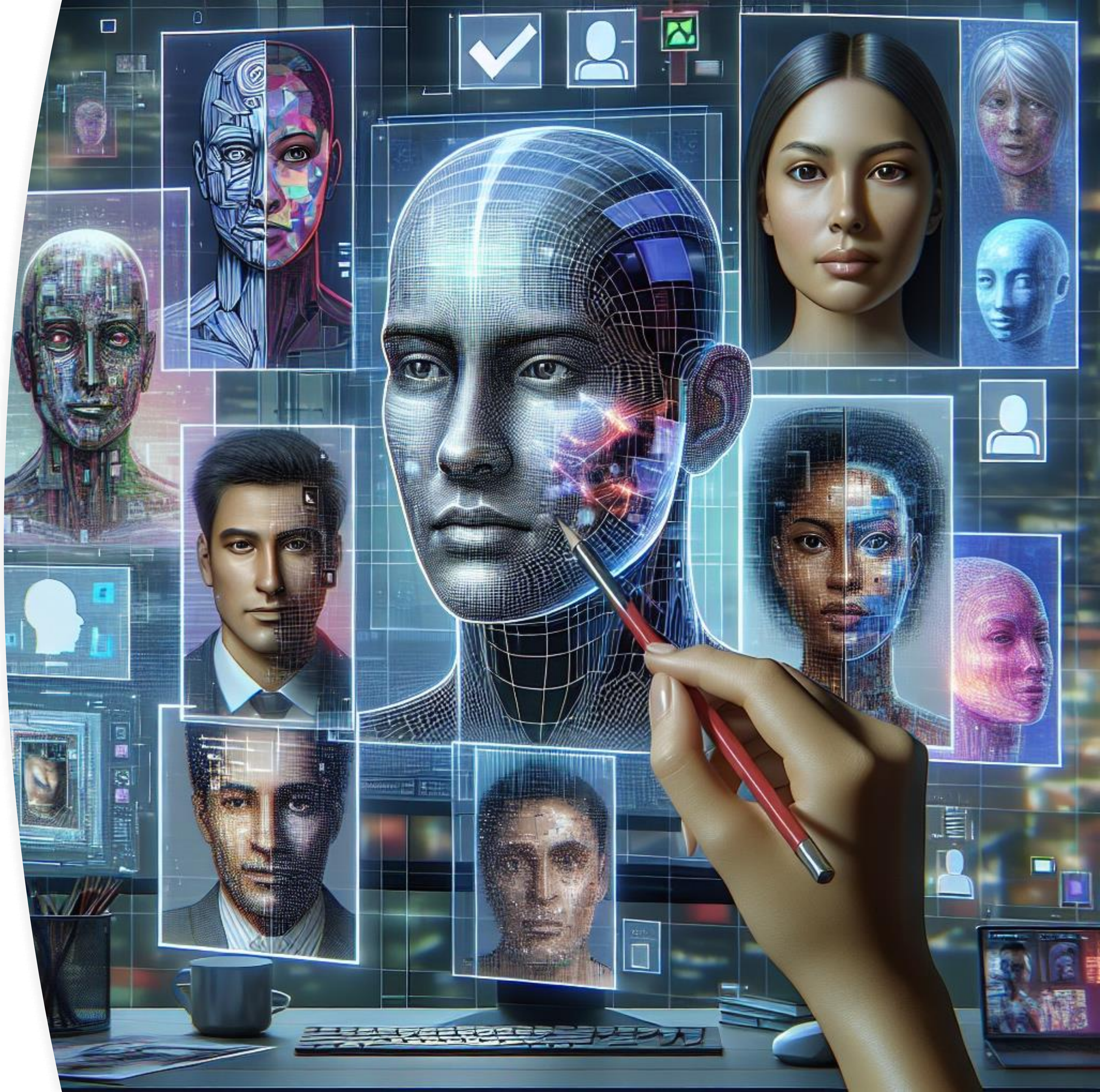
WEBCAM RESOLUTION

How Deepfake Detection Works

- Machine Learning Algorithms
  - AI algorithms are trained to detect inconsistencies in videos/images/audio
  - This is done by analyzing facial movements, voice, and Open-source models
- Signal context
  - Time of day
  - Weather anomalies
  - Seasonal
  - Background noises
- The system looks for signs of tampering in the file
- Benchmark Datasets:
  - Training models on known deepfakes increases accuracy.

Advantages of Detecting Deepfakes

- Enhances trust in digital media by identifying fake content.
- Protects individuals and organizations from misinformation.
- Reduces potential financial losses due to fraudulent activities.
- Supports law enforcement in combating identity theft and fraud.
- Promotes responsible use of AI technology in media.



The Future of Truth: Challenges and Limitations

- Deepfakes are getting better and harder to detect
- Computational Resources
- Barrier to entry is becoming easier
- The detection techniques are not 100% accurate
- More research is needed in this field

Proactive Measures Against Deepfakes

Proactive controls enhance the detection of deepfake content.

Preventative measures build trust in digital communications.

Educating users is essential for recognizing deepfake threats.

Establishing policies minimizes the impact of misinformation.

Regularly updating detection systems keeps pace with evolving technology.