

---

---

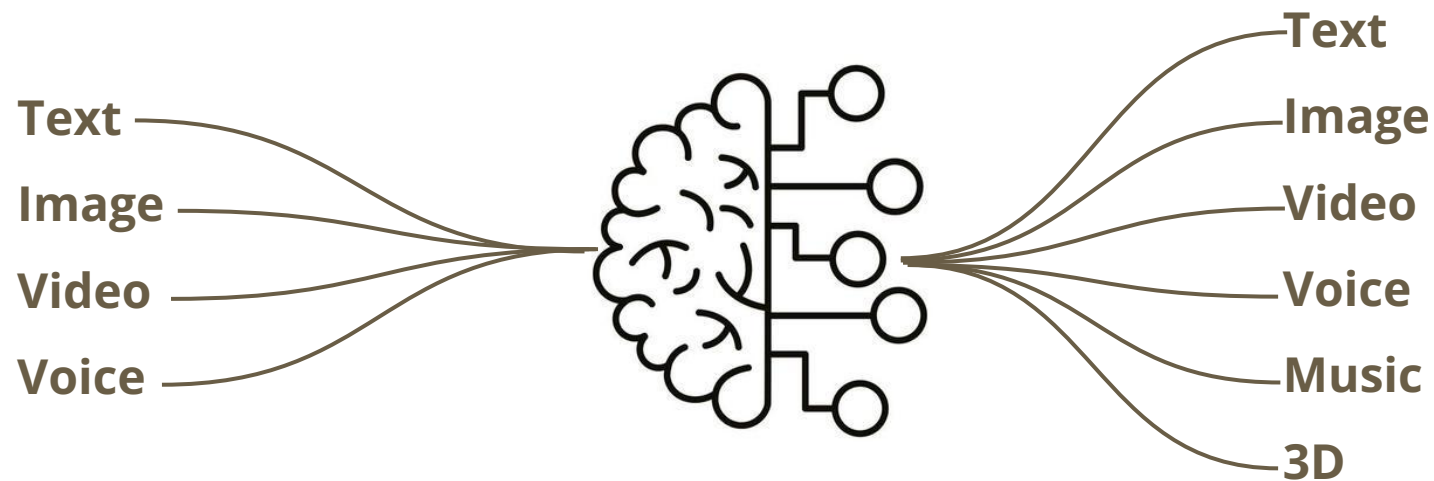
# Multi-Modal AI

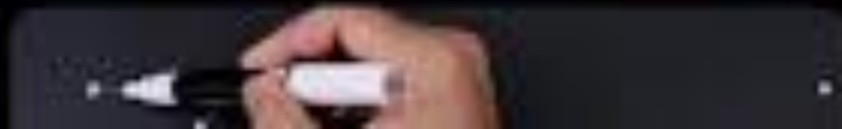
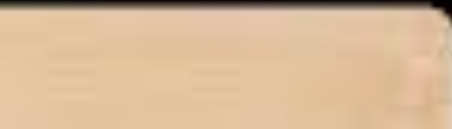
— And their use by threat actors —

---

---

# Multi-Modality





# Text-to-Text

## Chatbot

- OpenAI - ChatGPT
- Anthropic - Claude
- Google - Gemini
- Microsoft - Copilot



# Image

## Text-to-Image

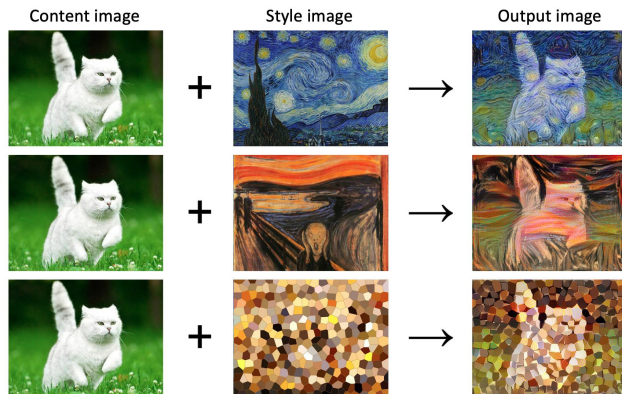
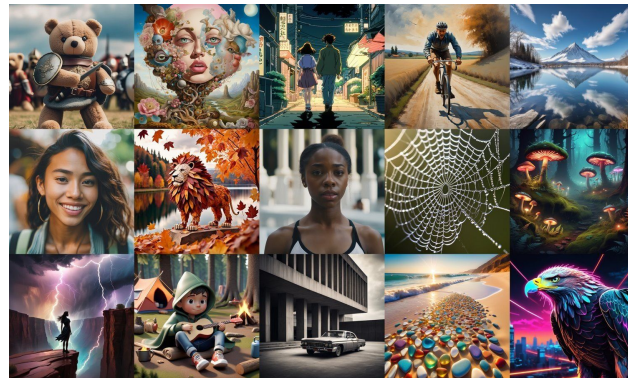
- Dall-E
- StableDiffusion

## Image-to-Text

- GPT-4
- Claude 3

## Image-to-Image

- Super-resolution
- Style-transfer



# Video

## Text-to-Video

- OpenAI Sora

## Image-to-Video

- [VideoPoet](#)

## Image-to-Face

- [VASA-1](#)



# Audio

## Speech-to-Text

- Siri, ChatGPT

## Text-to-Speech

- Voice cloning

## Text-to-Music

- Sona
- AI Drake/Ghostwriter



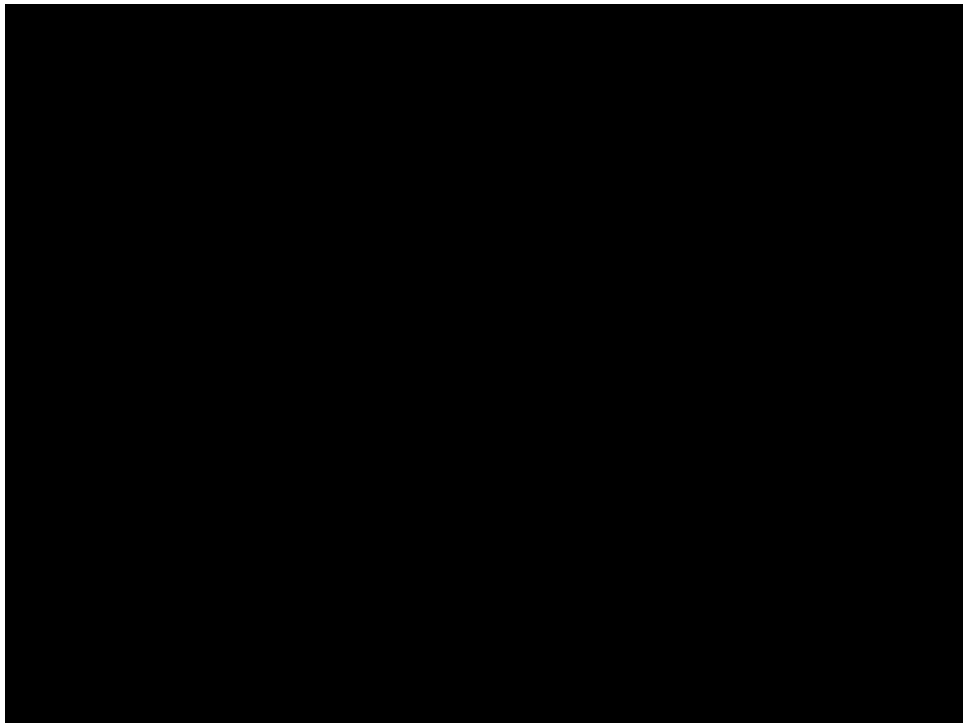
# 3D model

Text-to-3D

- NVidia - Magic3D

Image-to-3D

- [HuggingFace](#)





# Use by threat actors

## The AI-Enabled IO Toolkit



### IMAGES

---

GAN-Generated Images  
Text-to-Image Models  
AI-Manipulated Images



### VIDEO

---

AI-Generated Avatars  
AI-Manipulated Video



### TEXT

---

LLMs



### AUDIO

---

Text-to-Voice Models  
Voice Cloning

# Disinformation

- Venezuelan State Media<sup>1</sup>
- Hindu nationalist party corruption denial<sup>2</sup>



**An Indian politician says scandalous audio clips are AI deepfakes. We had them tested**

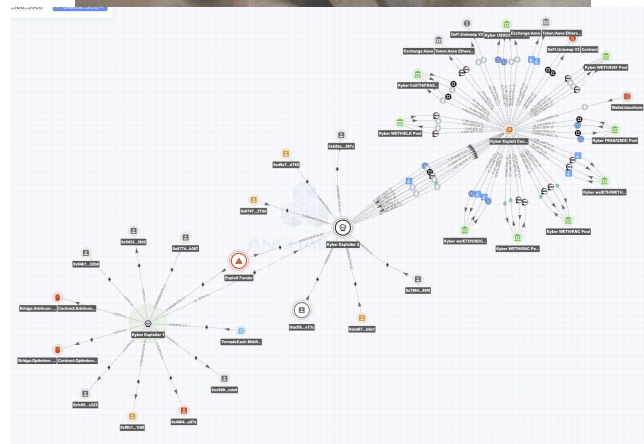
Deepfake experts noted that AI can be used as a cover by politicians when embarrassing audio and video clips of them emerge.



# Bypassing KYC

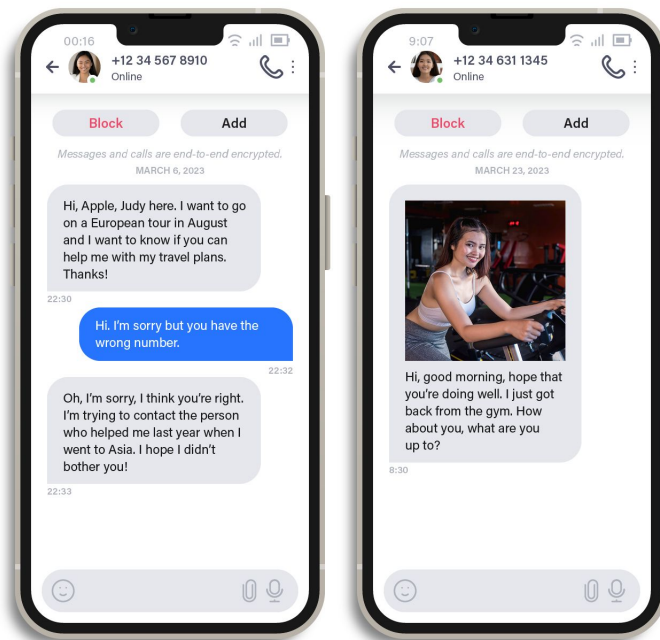
OnlyFake - \$15 fake IDs [123](#)

Used to bypass KYC on crypto exchange and enable money laundering



# Pig Butchering

- Chatbots being used to make initial contact
- Image generators used to make fake Instagram profiles
- Voice generator used to further scam
- Generated fake IDs used to launder money



# Virtual Kidnapping

- Voice cloners used to impersonate supposed victim
- Rise of image, video, and face generators increase risks

## Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

