

SCC0530 - Inteligência Artificial

DEEP FAKE





Membros do grupo

- **Leonardo Gonçalves Chahud**
- **Lucas Bichara**
- **Lucas Veiga Betoni**
- **Rafael Jun Teramae Dantas**



DEEP FAKE

SEEMS LEGIT - And Very, Very Scary



O QUE É ?

Um vídeo manipulado digitalmente, altamente realista e difícil de detectar, de alguém dizendo ou fazendo algo que nunca fez



“DEEP”

Vem do fato de usar algoritmos de “deep learning”, que aprendem a resolver problemas dado um conjunto enorme de dados.



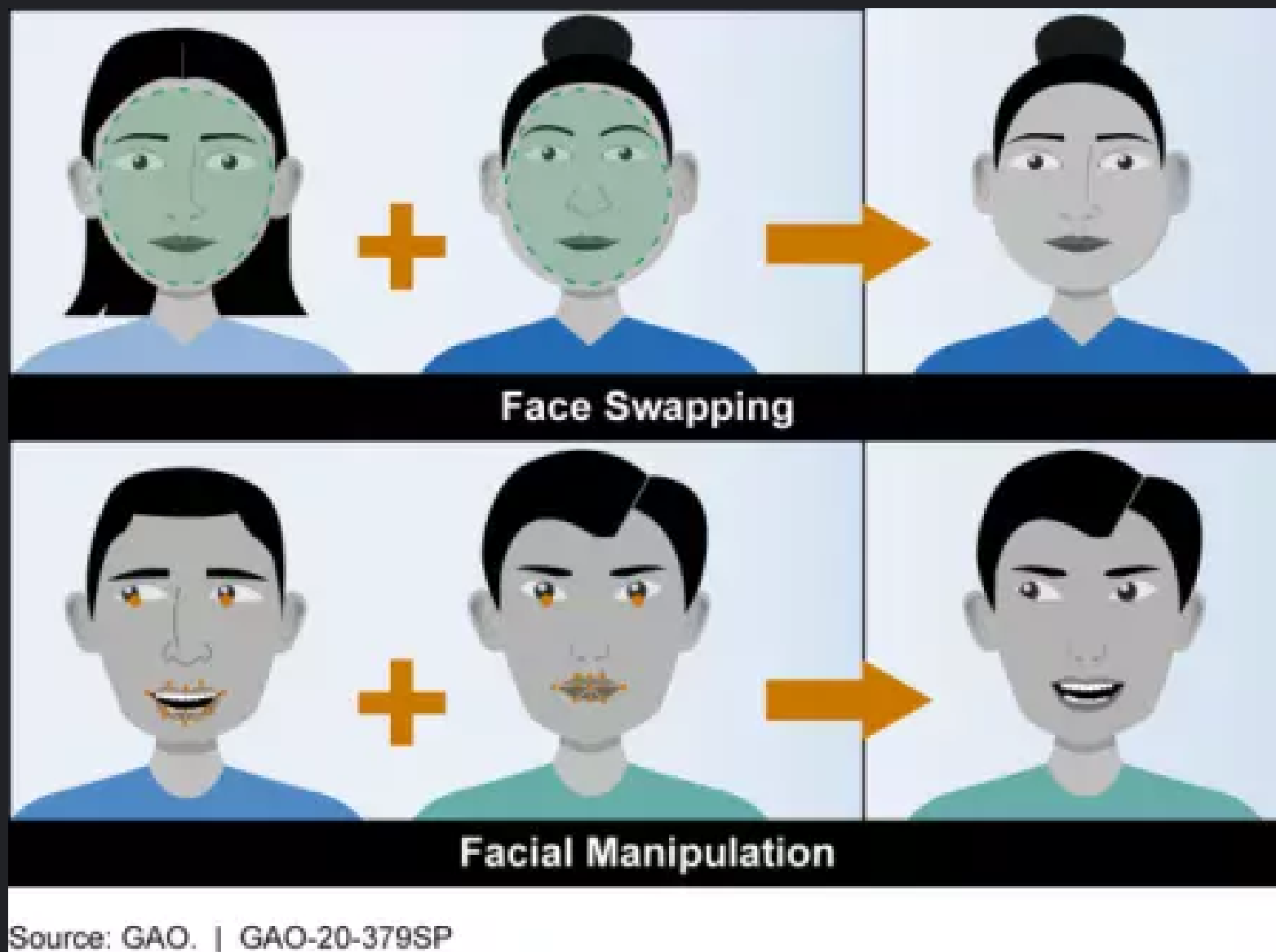
TÉCNICA

Utiliza ferramentas de inteligência artificial para alterar ou criar vídeos, imagens e áudios, gerando mídias falsas e realistas.

O QUE É DEEP FAKE?



COMO O DEEP FAKE FUNCIONA?



Redes Adversárias Generativas (GANs): técnica que utiliza duas redes neurais competindo entre si, uma rede cria exemplos de dados e a outra tenta distinguir esses dados gerados de exemplos reais;

Processamento de
imagem e vídeo

Clonagem de voz





Efeitos positivos na sociedade




Facilidade de produção de vídeos: Atores podem apenas assinar um documento em que concordam participar com uma propaganda ou vídeo sem a necessidade de estarem presentes.

Tradução de vídeos: Vídeos podem ser traduzidos para outras línguas facilmente utilizando a tecnologia


Entretenimento: Deep fakes podem ser usados para criar conteúdo de entretenimento, como filmes, programas de TV e vídeos engraçados.

Educação: Deep fakes podem ser usados para criar simulações educacionais, como recriar eventos históricos para fins de aprendizado ou treinamento em habilidades práticas, como aprimorar a habilidade de falar em público.

Saúde: Com deep fakes, um modelo de rede neural pode ser treinado para criar uma prótese personalizada que corresponda aos traços faciais e musculares de um paciente.



Efeitos negativos na sociedade



Desinformação: podem ser usados para criar "fake-news" (que são danosas mesmo após descobertas) , propagar informações enganosas e ideologias.

Danos a Imagem pessoal: podem ser usados para comprometer a imagem de pessoas, com imagens e vídeos falsos que podem ser usados para fins maliciosos (ex: política, difamação, pornografia).

Crime virtual: podem ser usados para cometer fraudes, extorsões, chantagens.

Falta de confiança: Podem minar a confiança nas informações e na mídia, levando as pessoas a desconfiar de tudo o que veem e ouvem.

ALGUMAS PREVISÕES

Certificates, certificates everywhere!

Olhando para a W3 e Windows
Media Digital Rights Management

Dificuldades com implantação de
certificação em hardware de
câmeras

Importância de documentos
oficiais e mídias com certificados

Certificação de Autoridades para
streaming

BIBLIOGRAFIA

- <https://tecnoblog.net/responde/como-identificar-deepfake-para-fugir-de-informacoes-falsas/>
- <https://proximonivel.embratel.com.br/dia-da-mentira-os-exemplos-do-bem-do-deepfake/>
- https://en.wikipedia.org/wiki/Generative_adversarial_network
- <https://pt.wikipedia.org/wiki/Deepfake>
- https://www.youtube.com/watch?v=cQ54GDm1eL0&ab_channel=BuzzFeedVideo
- <https://tecnoblog.net/noticias/2022/02/03/personagem-classico-de-star-wars-retorna-em-boba-fett-e-pode-ser-um-deepfake/>
- <https://www.gao.gov/blog/deconstructing-deepfakes-how-do-they-work-and-what-are-risks>
- <https://www.debatingeurope.eu/2019/03/27/can-we-still-trust-what-we-see-and-hear-online/#.ZDWj6nbMKUk>