Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

DeepFake

Edição nº20
Fevereiro/2022

Deepfake é uma tecnologia que usa inteligência artificial (IA) para criar imagens e vídeos falsos, mas realistas, de pessoas fazendo coisas que elas nunca fizeram na vida real. A técnica que permite fazer montagens de vídeo já gerou desde conteúdos pornográficos com celebridades até discursos fictícios de políticos influentes.
O termo Deepfake é uma mistura das expressões deep learning("Aprendizagem Profunda", em português) e fake("Falsidade", em português). Deepfake é baseada em deep learning, uma subclassificação de inteligência artificial para definir algoritmos que podem reconhecer padrões com base em um banco de dados. Isso significa que, para criar um vídeo de deepfake, o sistema precisa ser alimentado com fotos e vídeos em que ela aparece. Quanto mais material houver, maiores serão as chances de se obter um bom resultado. Treinada com base no conteúdo fornecido, a IA aprende como a pessoa se comporta, passando a reconhecer padrões de movimento, trações do rosto, da voz e de outras características.
Depois de treinado, o sistema usa uma técnica chamada redes adversárias generativas (GAN, na sigla em inglês) para reproduzir os movimentos e a fala como se estivessem sendo realizados pela pessoa que será o alvo do vídeo.

Seguem alguns apps que é possível baixar e instalar em seu dispositivo Android ou iOS para realizar Deepfake de um jeito criativo e divertido (e sem prejudicar ninguém):

- **DeepFaceLab**
- **FakeApp**
- **Toongineer Cartoonizer**
- **ZAO Deepfake**
- **Reface**
- **Deepfakes web Beta**
- **Wombo**
- **Instagram DeepFake Bot**
- **Vocodes**

Normalmente, vídeos desse tipo não são perfeitos, mas são realistas o suficiente para enganar muita gente. Má intenção não faz parte do conceito de deepfake, mas está na equação. Com ferramentas tão acessíveis, fica mais fácil espalhar informações falsas de acordo com interesses próprios, fundamentadas por supostas provas em vídeo. Isso pode representar um perigo para a democracia e para sociedade, inclusive ameaçando a credibilidade de tudo o que é publicado.

Seguem algumas dicas de como distinguir o que é real do que é falso:

- **Vá devagar: pergunte-se se isso pode mesmo ser verdade;**
- **Observe se os lábios estão mal sincronizados com a fala;**
- **Veja se há mudanças no tom da pele;**
- **Verifique os olhos para notar se eles estão piscando: na maioria das vezes, os algoritmos não reproduzem bem esse aspecto nem a respiração da pessoa;**
- **Assista ao vídeo quadro a quadro para detectar inconsistências: geralmente aparece iluminação instável, mudando de um quadro para o outro.**

Um dos grandes casos de uso ilegal da tecnologia de deepfake é para a produção de conteúdos que prejudiquem a imagem de políticos, sobretudo em contexto eleitoral. Muitos especialistas já colocam a tecnologia no patamar mais elevado da lista de desafios para as próximas eleições, tendo um combate ainda mais difícil que o feito sobre as fake news.

A maior parte da desinformação é publicada para semear dúvidas, reforçar crendices ou para se opor ruidosamente a outras ideias.
É muito desafiador verificar imagens e sons que foram retirados de contexto, editados ou encenados. Ainda assim, por enquanto, você pode treinar para identificar melhor uma deepfake.
E lembre-se: se você não tiver certeza, não compartilhe!

Fique ligado! No próximo mês falaremos sobre Defacement

Tribunal Regional Eleitoral - RN