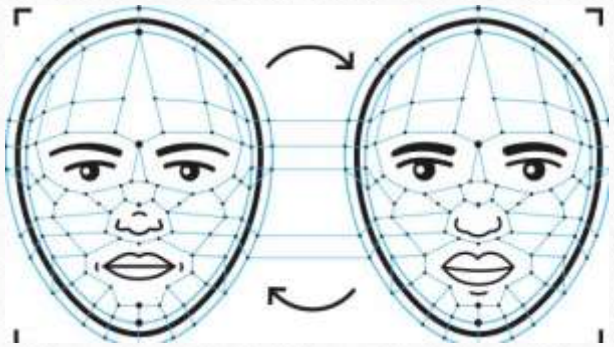
LOS DEEPFAKES

LUIS FERNANDO HERRERA LLOREDA

¿QUÉ SON LOS DEEPFAKES?

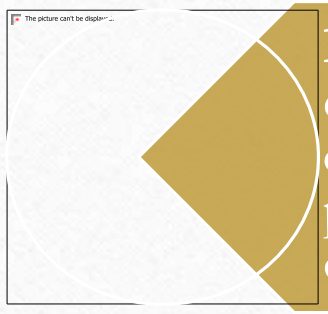
La palabra **Deepfake** es una composición de los términos *Deep learning* y *fake*, es decir: **aprendizaje profundo**, una de las ramas de la inteligencia artificial, y la palabra **falso**. Es una tecnología basada en la Inteligencia Artificial que consigue **superponer el rostro de una persona en el de otra y falsificar sus gestos** para hacernos creer que están haciendo o diciendo algo que no ha pasado en realidad.

Deepfake generalmente se refiere a vídeos en los que la cara y / o la voz de una persona, generalmente una figura pública, ha sido manipulada utilizando software de inteligencia artificial de una manera que hace que el vídeo alterado se vea auténtico.



TIPOS DE DEEPFAKES

Deepfaces: Consiste en crear fotos convincentes pero completamente ficticias desde cero. Aprovecha el aprendizaje automático para manipular y generar imágenes o vídeos que reemplazan a una persona por otra.



Deepvoice: Es la suplantación de la voz de una persona en un audio, haciendo que parezca su voz real. Se trataría de unir frases y palabras sueltas utilizadas por una persona para crear un discurso. Incluso, es capaz de clonar la voz original a partir de estos fragmentos.

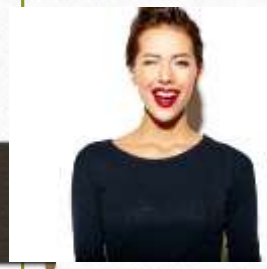
¿CÓMO SE REALIZA UN DEEPFACES?

Es uno de los últimos avances en Inteligencia Artificial y, si bien pueden ser usados para ayudar en la vida diaria de las personas que han perdido el habla y el oído, también hay que ser conscientes del peligro que entrañan en caso que lleguen a hacerse pasar por un vídeo verdadero

Otra forma de hacer deepfakes utiliza lo que se llama una red de confrontación generativa, o Gan. Un Gan enfrenta dos algoritmos de inteligencia artificial uno contra el otro. El primer algoritmo, conocido como generador, recibe ruido aleatorio y lo convierte en una imagen. Esta imagen sintética se agrega a una secuencia de imágenes reales, de, digamos, que se introducen en el segundo algoritmo, conocido como discriminador,

Las 'Deepfakes' son más que GAN, para lograr sus resultados, tan escalofriantemente realistas, usan otras herramientas de inteligencia artificial para acoplar un rostro o una parte del rostro generada artificialmente en un video real.

¿CÓMO DETECTAR UN DEEPFACE?



1.- Parpadeo: Una forma de detectar los deepfakes es fijándonos en las veces que parpadea la persona. Todos parpadeamos una vez cada tres o seis segundos y cada parpadeo dura unas tres décimas de segundo.

Cuando estamos ante un vídeo falso, la persona parpadea menos veces que si fuera real ya que el algoritmo a través del que está realizada esa falsificación no puede parpadear a la misma velocidad que un humano.

2.- Cuello y cara: Los deepfakes son principalmente sustituciones de caras ya que sustituir un cuerpo es mucho más complicado. Por eso, debemos fijarnos en el cuerpo de la persona a la que se le ha sustituido la cara y, si las características de ese cuerpo no coinciden con las del de la persona real, estamos ante una falsificación.

3-. Detalles: También es importante estar al tanto de los detalles de la grabación. Si reproducimos el vídeo a velocidad más reducida, nos daremos cuenta de modificaciones repentinas de la imagen o cambios en el fondo de una persona que demostrarán que se trata de una falsificación.

4.- Origen de la grabación: A la hora de detectar un deepfake, también nos ayuda encontrar al primero que compartió ese vídeo. De esa forma podremos verificar el contexto en el que se produjo esa publicación y si el material de origen tenía más detalles.

5.-Sonido: Muchas veces, el algoritmo que modifica la grabación no ajusta el sonido. Podemos darnos cuenta de que estamos ante una falsificación cuando el sonido no coincide con la imagen porque no exista una correcta sincronización con el movimiento de los labios.

¿ CÓMO PROTEGERSE DE LOS DEEPAKES?

Educación y capacitación

La educación y la capacitación son cruciales para combatir los deepfakes. A pesar de la considerable cobertura de noticias y las inquietudes presentadas por las autoridades, la amenaza de deepfakes aún no ha sido considerada por el público. las formas más eficientes para combatir la propagación de las falsificaciones profundas implican una combinación de avances legales, educativos y sociotécnicos, por lo que lo más recomendable sería no acceder a contenido mal intencionado o que nos resulte sospechoso.


THANK
YOU

REFERENCIA

Yola González (2020) Grupo Atico 34 [Blog]
https://protecciondatos-lopd.com/empresas/deepfakes/

Marta Sanz Romero(2018) ComputerHoy [Blog]
https://computerhoy.com/reportajes/tecnologia/consiste-deepfake-446355