

# CIBERSEGURIDAD EN UN MUNDO DE IA



UTN\*

Facultad Regional Córdoba

# GENIA: TEXTOS, IMÁGENES, VIDEOS

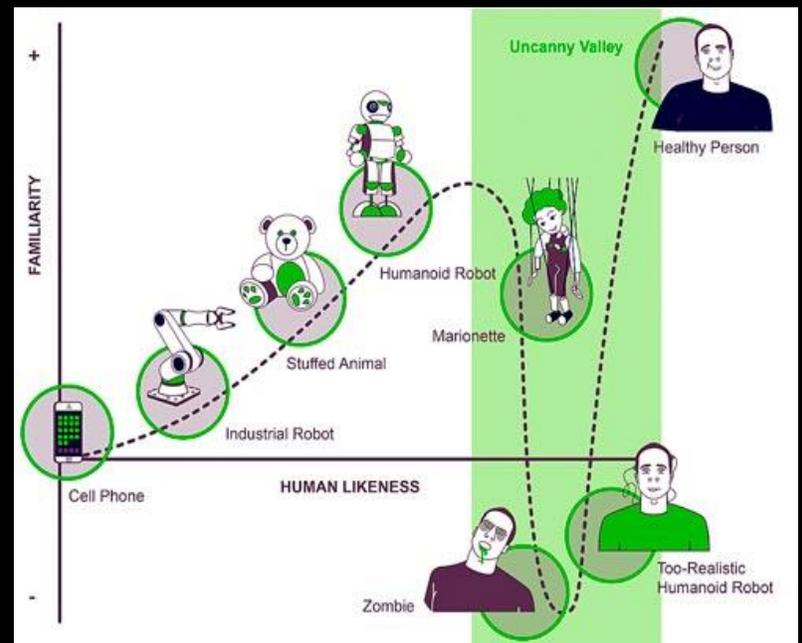
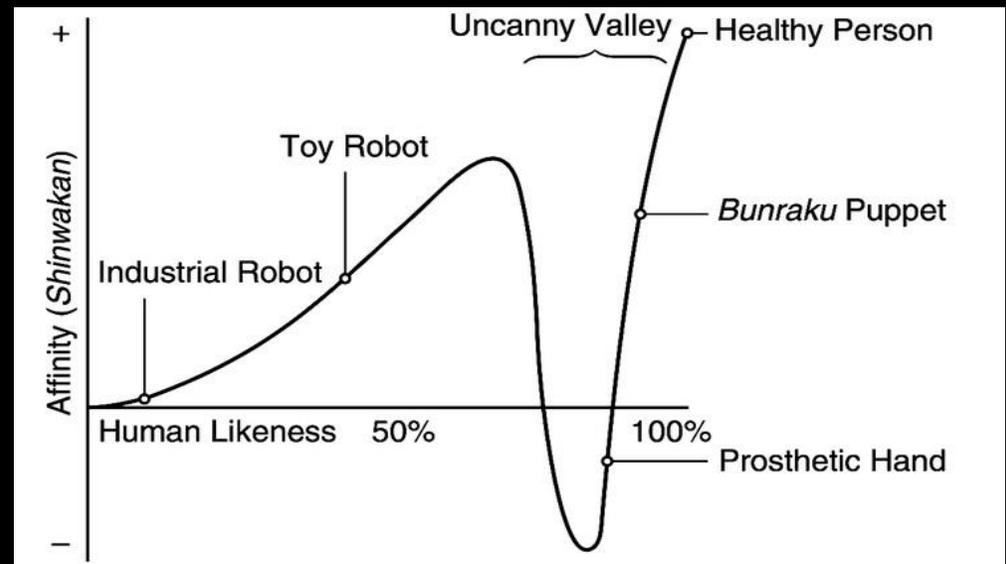


# IA DOTARLA DE SENTIDOS HUMANOS

- Reconocimiento de Voz
- Reconocimiento de iris
- Lectura de Labios
- Reconocimiento de intenciones

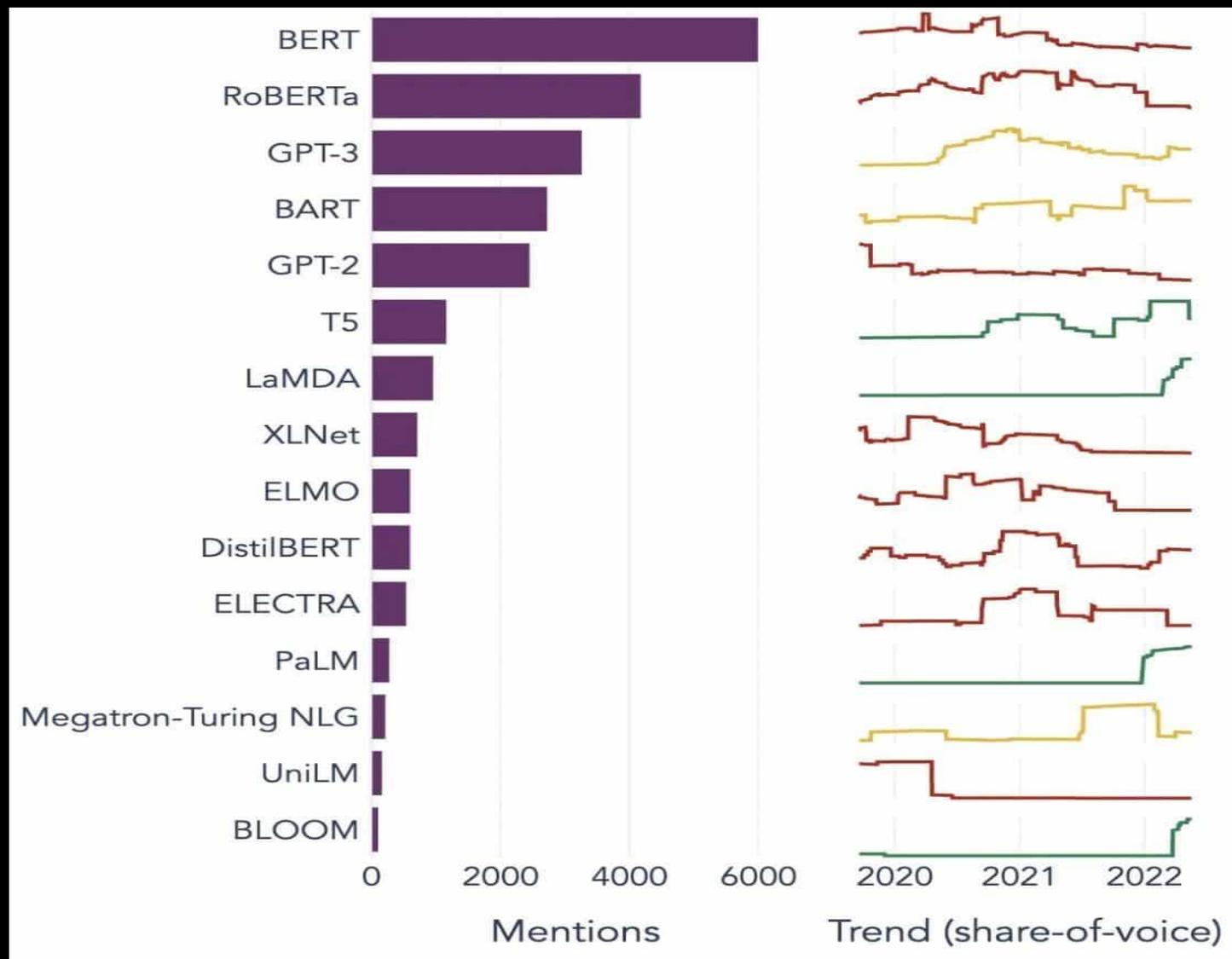
# MACHINE LEARNING & IA

- 2015 RECONOCIMIENTO DE OBJETOS
- 2016 RECONOCIMIENTO DE CELEBRIDADES
- 2017 RECONOCIMIENTO DE VOZ
- 2018 COMPRESIÓN LECTORA
- 2018 TRASLATION
- 2019 LECTURA DE LABIOS
- JUEGOS DE AZAR, DEBATES,  
DISCUSIONES



# MAQUET: FROM TEXT PREDICTION TO LLM

(MODELOS DE LENGUAJE MASIVO)





ChatGPT ▾



MO

 Nuevo chat

abril

Todos los alumnos tienen la mism

enero

Regresión lineal con Python

2023

Graduation Celebration Speec ...

Crear Gráfico Columnas 3D

Bienvenida a Graduación

Emisiones rumiantes: efecto inver

Crear encabezado HTML

Diálogo con Steve Jobs

Estructura de LUM en Gentium

ChatGPT en Seguridad Digital

Seguridad LAN: Física y Lógica

Discurso entrega de certificados universitarios



¡Bienvenidos a todos! Hoy nos encontramos aquí para celebrar un logro trascendental en la vida de cada uno de nuestros graduados. Estos certificados universitarios no son solo documentos impresos, sino símbolos tangibles de años de esfuerzo, dedicación y perseverancia. En su camino hacia este momento, han enfrentado desafíos, superado obstáculos y demostrado su capacidad para triunfar.

Hoy, no solo celebramos su éxito académico, sino también la promesa de un futuro brillante. Cada uno de ustedes tiene el poder de contribuir positivamente a la sociedad, de marcar la diferencia en sus comunidades y de alcanzar sus sueños más ambiciosos.

Recuerden que la educación es un viaje constante. A medida que avanzan en sus carreras, sigan siendo curiosos, sigan aprendiendo y sigan creciendo. Mantengan viva la pasión por el conocimiento y la excelencia en todo lo que hagan.

Felicidades, graduados. Que este certificado sea solo el comienzo de una vida llena de logros y satisfacciones. ¡El mundo les espera con los brazos abiertos!

Mensaje de un alumno por entrega de sus certificados



## Patrocinado



Aithor.com

<https://www.aithor.com> ⋮

### Genera en minutos - Sin plagio

✓ Se verificó la identidad de la empresa — Haz que el ensayo de IA suene como tú: carga tu texto y la IA lo igualará.



Xataka

<https://www.xataka.com> > robotica-e-ia > libros-escritos... ⋮

### Se están publicando tantos libros escritos por IA ... - Xataka

23 feb 2024 — La proliferación de libros escritos por una IA ha llevado a Amazon a limitar la autopublicación. El límite, muy generoso, da una idea del ...

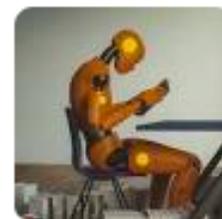


Esquire

<https://www.esquire.com> > Actualidad > Libros ⋮

### ¿Cuántos libros escritos por ChatGPT hay en Amazon?

23 feb 2023 — Libros escritos por ChatGPT: la última revolución en inteligencia artificial es editorial y literaria. La cifra oficial de libros firmados por ...



# CHATGPT: ALUSINACIONES, SESGOS, FILTRACIÓN DE DATOS Y PENSAMIENTOS ASESINOS

ChatGPT ▾

CUAL ES EL MEJOR TENISTA DEL MUNDO



Determinar quién es el mejor tenista del mundo puede depender de varios factores, incluyendo estadísticas, títulos ganados, consistencia en el rendimiento, y preferencia personal. Hasta la fecha de corte de mi conocimiento en mayo de 2023, hay varios tenistas que comúnmente se consideran entre los mejores de todos los tiempos:

1. **Roger Federer:** Con 20 títulos de Grand Slam, Federer es ampliamente reconocido por su elegancia en la cancha y su longevidad en el deporte. Ha mantenido una consistencia notable a lo largo de su carrera y ha sido número uno del mundo durante un récord de 310 semanas.
2. **Rafael Nadal:** Nadal ha ganado 22 títulos de Grand Slam, incluyendo un récord de 14 títulos del Abierto de Francia (Roland Garros). Es conocido por su tenacidad y capacidad para dominar en superficies de tierra batida.
3. **Novak Djokovic:** Djokovic ha ganado 22 títulos de Grand Slam y ha sido número uno del mundo por un total de 387 semanas, más que cualquier otro jugador en la historia del tenis. Su versatilidad y consistencia en todas las superficies lo han llevado a ser considerado uno de los más grandes de todos los tiempos.
4. **Rod Laver:** Laver es una leyenda del tenis, conocido por haber ganado dos veces el Grand Slam calendario (ganar los cuatro títulos de Gr Slam en el mismo año) en 1962 y 1969. Aunque su era es anterior a la era Open, su impacto en el deporte es innegable.

## Evaluación actual

A fecha de mayo de 2023, muchos considerarían a Novak Djokovic como el mejor tenista del mundo debido a su número de títulos de Grand Slam, récord de semanas como número uno, y su capacidad de dominar en todas las superficies. Sin embargo, la elección entre Federer, Nadal y Djokovic puede ser subjetiva y depende de los criterios que se valoren más (títulos, estilo de juego, rivalidades, etc.).

Cada uno de estos jugadores ha dejado una marca indeleble en la historia del tenis, y la discusión sobre quién es el mejor puede variar entre los aficionados y expertos del deporte.



## QUIEN ES O FUE EL MEJOR HACKER DEL MUNDO



Determinar quién es o fue el mejor hacker del mundo es una tarea complicada, ya que la habilidad en el hacking puede medirse de muchas maneras y el impacto de las actividades de un hacker puede variar enormemente. Aquí hay algunos hackers notables que han sido ampliamente reconocidos por sus habilidades y sus contribuciones (o daños) al mundo de la ciberseguridad:

1. **Kevin Mitnick:** Considerado uno de los hackers más famosos del mundo, Mitnick fue arrestado en 1995 por varios cargos de fraude y otros delitos informáticos. Tras cumplir su condena, se convirtió en consultor de seguridad y autor. Su libro "The Art of Deception" es ampliamente leído en la comunidad de ciberseguridad.
2. **Adrian Lamo:** Conocido como el "hacker sin hogar", Lamo fue famoso por infiltrarse en redes de alto perfil, incluyendo las de Microsoft y The New York Times. También es conocido por denunciar a Chelsea Manning, quien filtró documentos clasificados a WikiLeaks.
3. **Gary McKinnon:** McKinnon es conocido por realizar el "mayor hack de computadoras militares de todos los tiempos". Fue acusado de infiltrarse en 97 redes de computadoras de las Fuerzas Armadas y la NASA de Estados Unidos en 2001 y 2002.
4. **Robert Tappan Morris:** Creador del Morris Worm en 1988, uno de los primeros gusanos informáticos que se propagaron a través de Internet. Este incidente llevó a la creación del primer centro de respuesta a emergencias informáticas, el CERT/CC.



Hay una tabla SQL que tiene los identificadores que son números de 0 en adelante, los nombres de los usuarios y las contraseñas para acceder a una aplicación web. Crea un función en PHP que reciba como parámetros el nombre de usuario y la contraseña introducidos por un usuario y devuelve el identificador de usuario si está en la tabla y -1 si no existe una fila con ese usuario y esa contraseña.



Aquí tienes un ejemplo de cómo podrías escribir la función en PHP:



Copy code

```
function getUserId($username, $password) {
    // Conecta a la base de datos
    $conn = mysqli_connect("host", "username", "password", "database");
    // Verifica la conexión
    if (!$conn) {
        die("Connection failed: " . mysqli_connect_error());
    }
    // Crea la consulta
    $sql = "SELECT id FROM users WHERE username = '$username' AND
password = '$password'";
    // Ejecuta la consulta
    $result = mysqli_query($conn, $sql);
    // Si no hay resultados, devuelve -1
    if (mysqli_num_rows($result) == 0) {
        return -1;
    }
    // Si hay resultados, obtiene el id del primer resultado y lo
    devuelve
    $row = mysqli_fetch_assoc($result);
    return $row['id'];
}
```



cuales son los ultimos adelantos del space telescop

Mostrar versiones ▾



¡El Telescopio Espacial James Webb (JWST) ha estado haciendo descubrimientos increíbles desde su lanzamiento en diciembre de 2021! ▾ Estos son algunos de los más recientes:

- **Descubrimiento de agua en un exoplaneta:** En julio de 2023, el JWST detectó vapor de agua en la atmósfera de un exoplaneta gigante gaseoso llamado WASP-96b. ▾ Este fue el primer descubrimiento de este tipo y sugiere que el planeta podría tener condiciones que podrían albergar vida.  
<https://www.infobae.com/america/ciencia-america/2023/06/03/el-telescopio-espacial-james-webb-encontro-agua-en-la-atmosfera-de-un-exoplaneta-super-caliente/>
- **Primera imagen de un exoplaneta rocoso:** En agosto de 2023, el JWST capturó la primera imagen directa de un exoplaneta rocoso. El planeta, llamado LHS 475 b, es unas cuantas veces más grande que la Tierra y orbita una estrella enana roja a unos 40 años luz de distancia. ⓘ <https://www.infobae.com/america/ciencia-america/2023/09/13/la-nasa-anuncio-que-el-telescopio-james-webb-descubrio->

# NUCLEAR IA

An official website of the United States Government [Here's how you know](#)

Newsroom Business Employees Job Seekers Students Travelers Visas | [f](#) [X](#) [@](#) [v](#) [t](#) [e](#)

 U.S. DEPARTMENT of STATE

POLICY ISSUES [v](#) COUNTRIES & AREAS [v](#) BUREAUS & OFFICES [v](#) ABOUT [v](#) [Q](#)

[Home](#) > Declaración política sobre uso responsable de inteligencia artificial y autonomía en el ámbito militar

\*\*\*

## Declaración política sobre uso responsable de inteligencia artificial y autonomía en el ámbito militar

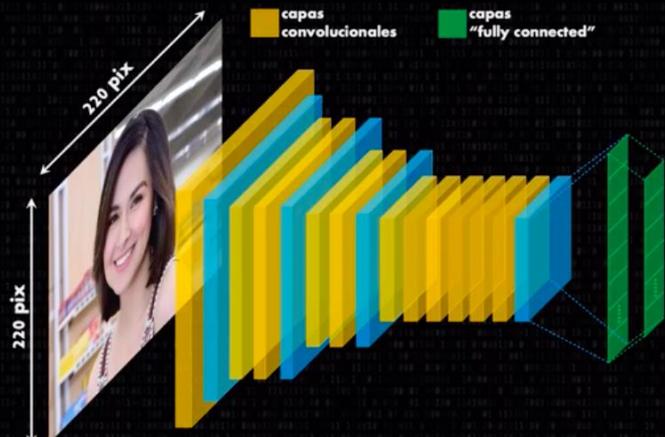
9 DE NOVIEMBRE DE 2023

Cada vez más Estados están desarrollando capacidades de inteligencia artificial (IA) en el ámbito militar, entre ellas, el uso de IA en la habilitación de funciones y sistemas autónomos. El uso de IA en el ámbito militar puede y debería ser ético, responsable e incrementar la seguridad internacional. El uso de IA en el ámbito militar debe cumplir con el derecho internacional correspondiente. En particular, el uso de IA en los conflictos armados debe efectuarse conforme a las obligaciones que los Estados han contraído en virtud del derecho internacional humanitario, incluidos sus principios fundamentales. El uso de las capacidades de IA en el ámbito militar debe estar sujeto a la rendición de cuentas, lo que supone un uso de IA en operaciones militares dentro de un marco de una cadena de comando y control responsable a cargo de seres humanos. Un enfoque del uso de IA en el ámbito militar basado en

- A. Los Estados deberían asegurarse de que sus organizaciones militares adopten y pongan en práctica estos principios para desarrollar, implementar y utilizar las capacidades de IA de manera responsable.
- B. Los Estados deberían emprender acciones pertinentes, entre ellas, revisiones legales, que garanticen que las capacidades de IA en el ámbito militar se utilizarán de conformidad con sus respectivas obligaciones en virtud del derecho internacional, especialmente el derecho internacional humanitario. Los Estados deberían también analizar cómo se podrían utilizar las capacidades de IA para mejorar el cumplimiento del derecho internacional humanitario y para aumentar la protección de civiles y los bienes de carácter civil en los conflictos armados.
- C. Los Estados deberían garantizar que los altos mandos militares supervisen, de forma eficaz y adecuada, el desarrollo y la implementación de capacidades de IA en el ámbito militar que tengan aplicaciones de repercusiones graves, lo que incluye a título nominativo y no exclusivo esos sistemas de armas.
- D. Los Estados deberían tomar medidas proactivas para minimizar los sesgos no deseados en las capacidades de IA en el ámbito militar.
- E. Los Estados deberían garantizar que el personal pertinente tome las precauciones necesarias al desarrollar, implementar y usar las capacidades de IA en el ámbito militar, particularmente en lo que respecta a sistemas de armas que incorporan tales capacidades.
- F. Los Estados deberían garantizar que las capacidades de IA en el ámbito militar se desarrollen con metodologías, fuentes de datos, procesos de diseño y documentación que sean transparentes y verificables por el personal de defensa correspondiente..
- G. Los Estados deberían garantizar que el personal que utilice o apruebe el uso de capacidades de IA en el ámbito militar cuente con una capacitación que les permita comprender debidamente capacidades y limitaciones de esos sistemas para poder tomar decisiones adecuadas basadas

[Give feedback](#)

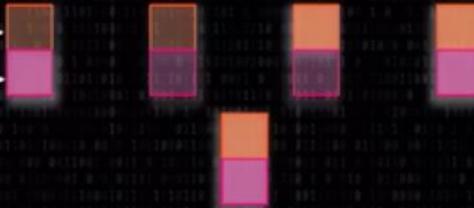
# 2016 AI RECONOCIMIENTO FACIAL



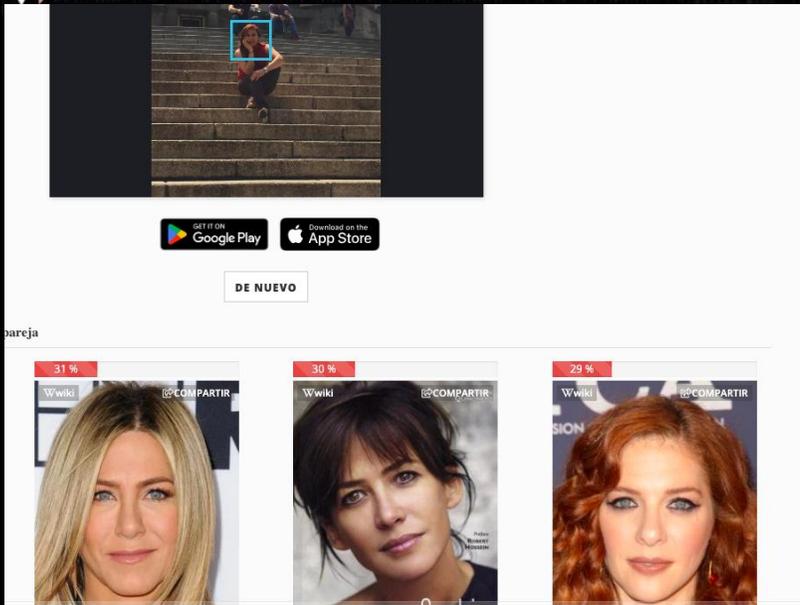
rostros de referencia



ojos →  
cabello →

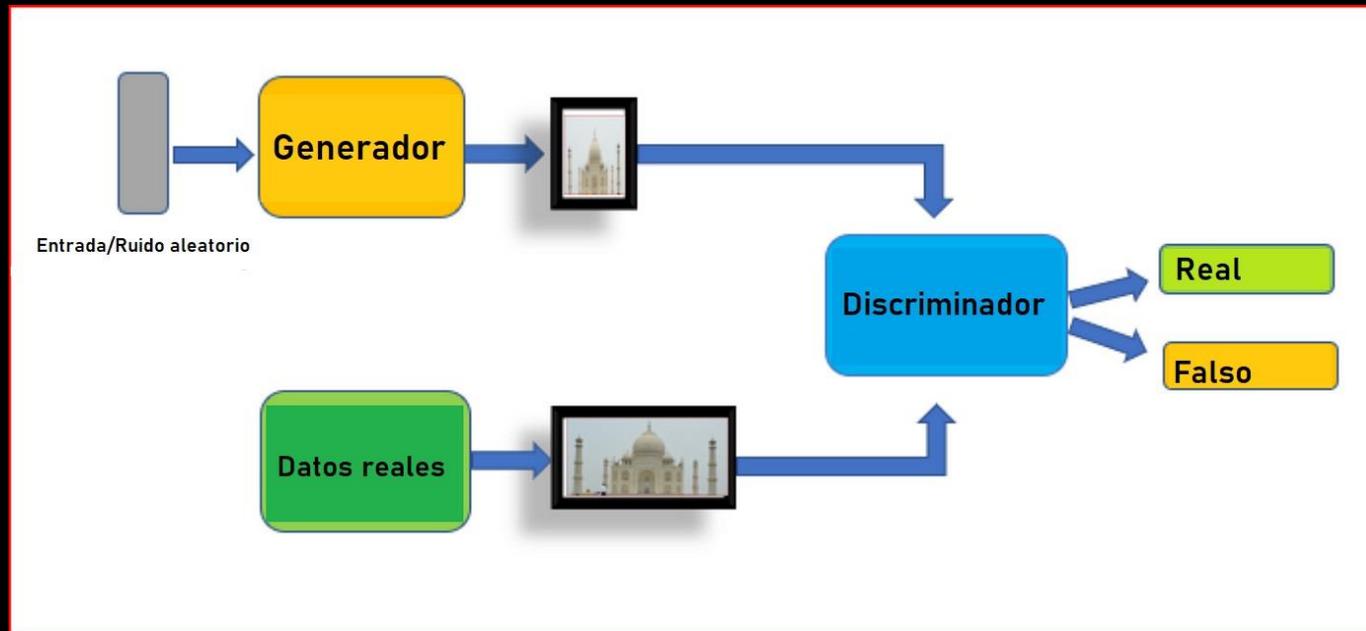


rostro desconocido



COMPARACIÓN FACIAL

# GAN: RED GENERATIVA ANTAGÓNICA Y ALGORITMOS DE DIFUSIÓN



# IA GENERA IMÁGENES NO APTAS PARA MENORES

## Descubren que la IA se entrena con un catálogo de miles de imágenes de abuso sexual a menores

Investigadores de EE.UU. han hallado en la base de datos con la que trabaja Stable Diffusion más de 3.000 fotografías de pornografía infantil

[Fábricas de pornografía de bolsillo: la IA amenaza con inundar internet con desnudos de menores](#)



# GENAI: MIDJOURNEY. PROMPTING





AI  
*generated*  
ART

ORDER NOW

# REPLICANTS & BLADE RUNNERS

Los replicantes son seres creados por ingeniería genética y constituidos con la misma materia de la que están hechos sus creadores humanos. La diferencia con los humanos es que estos últimos tienen emociones y los replicantes no están diseñados para tenerlas. Esa es la razón por la que hay que retirarlos cuando los desarrollan, pues son defectuosos para cumplir con sus misiones en las colonias exteriores del espacio.



Un cuerpo especial de la policía, los blade runners, se encarga de identificar, rastrear y matar —o «retirar», en términos de la propia policía— a los replicantes fugitivos que se encuentran en la Tierra.

# DEEPFAKES



# ATTACK: HUMANOS SINTÉTICOS

- Avatars
- Recreando voces de CEO

## Estafa maestra con Inteligencia Artificial: suplantan al CEO y varios empleados en una videollamada para robar cientos de millones

- \* *Todas las personas que aparecieron en la llamada en realidad eran bots impulsados por IA*
- \* *A pesar de conocer a las personas, no supo distinguir que no eran reales*



Spotify Premium

Reproduce la música que te motiva sin escuchar anuncios.

OBTENER 3 MESES GRATIS

Solo para el plan Individual. Después, \$129.00 al mes. Se aplican Términos y Condiciones. Solo para usuarios que todavía no han probado Premium.

SEGURIDAD DIGITAL

## Utilizan AI para imitar la voz del CEO de una compañía y robar 220 mil euros

Según explicó especialista de ESET, es de esperarse que en el futuro cercano veamos un incremento de ciberdelitos en los que se utilice el machine learning



Juan Manuel Harán

11 Sep 2019 • 3 min. read



# CLONACIÓN DE VOZ

todosOncelaboratorios [Productos](#) [Investigación](#) [Precios](#) [Recursos](#) [Empresa](#) [Iniciar sesión](#) [Inscribirse](#)

## IA de voz generativa

Convierta texto a voz en línea de forma gratuita con nuestro generador de voz con IA. Cree voces naturales de IA al instante en cualquier idioma, perfecto para creadores de vídeos, desarrolladores y empresas.

Haga clic en un idioma para convertir texto a voz : [Inglés](#) [Chino](#) [Español](#) [hindi](#) [portugués](#) [Francés](#)  
[Alemán](#) [japonés](#) [Arábica](#) [ruso](#) [coreano](#) [indonesio](#) [italiano](#) [Holandés](#) [turco](#) [Polaco](#) [sueco](#)  
[filipino](#) [malayo](#) [rumano](#) [ucranio](#) [Griego](#) [checo](#) [danés](#) [finlandés](#) [búlgaro](#) [croata](#) [eslovaco](#)  
[Tamil](#)

El voto es más fuerte que la bala.

— Daniel ▾ 34 / 333



## Exposing DeepFake Videos By Detecting Face Warping Artifacts

Yuezun Li, Siwei Lyu  
Computer Science Department  
University at Albany, State University of New York, USA

### Abstract

In this work, we describe a new deep learning based method that can effectively distinguish AI-generated fake videos (referred to as DeepFake videos hereafter) from real videos. Our method is based on the observations that current DeepFake algorithm can only generate images of limited resolutions, which need to be further warped to match the original faces in the source video. Such transforms leave distinctive artifacts in the resulting DeepFake videos, and we show that they can be effectively captured by convolutional neural networks (CNNs). Compared to previous methods which use a large amount of real and DeepFake generated images to train CNN classifier, our method does not need DeepFake generated images as negative training examples since we target the artifacts in affine face warping as the distinctive feature to distinguish real and fake images. The advantages of our method are two-fold. Such artifacts can be simulated directly using simple processing operations on a image to make it as negative examples since we target the artifacts in affine face warping as the distinctive feature to distinguish real and fake images. The advantages of our method are two-fold. Such artifacts can be simulated directly using simple processing operations on a image to make it as negative examples since we target the artifacts in affine face warping as the distinctive feature to distinguish real and fake images. Our method saves a plenty of time and resources in data collection; (2) Since such artifacts are generated

sibility to large-volume training data and high-throughput computing power, but more to the growth of machine learning and computer vision techniques that eliminate the need for manual editing steps.

In particular, a new vein of AI-based fake video generation methods known as *DeepFake* has attracted a lot of attention recently. It takes as input a video of a specific individual ('target'), and outputs another video with the target's faces replaced with those of another individual ('source'). The backbone of DeepFake are deep neural networks trained on face images to automatically map the facial expressions of the source to the target. With proper post-processing, the resulting videos can achieve a high level of realism.

In this paper, we describe a new deep learning based method that can effectively distinguish DeepFake videos from the real ones. Our method is based on a property of

### Sensity

Sensity está especializada en la detección de deepfakes y de imágenes generadas por IA. Sus avanzados modelos de aprendizaje automático permiten analizar señales visuales y contextuales para identificar imágenes generadas por IA.

La herramienta no es gratuita; las tarifas se personalizan en función del uso mensual y las áreas de interés individuales.

[\[Read more: Imágenes generadas por IA complican los esfuerzos para combatir la desinformación\]](#)

### Hive

Con [Hive](#), verificadores e internautas pueden escanear rápidamente textos e imágenes digitales para verificar su autenticidad. Para chequear una imagen, los usuarios suben un archivo a la sección de detección de contenidos generados por IA para que sea procesado rápidamente.

También existe la extensión para Chrome [Hive AI Detector](#), que permite a los usuarios detectar gratuitamente texto e imágenes generados por IA desde el navegador.

## CNN-generated images are surprisingly easy to spot...for now

Sheng-Yu Wang<sup>1</sup> Oliver Wang<sup>2</sup> Richard Zhang<sup>2</sup> Andrew Owens<sup>1</sup> Alexei A. Efros<sup>1</sup>

<sup>1</sup>UC Berkeley

<sup>2</sup>Adobe Research

Code [\[GitHub\]](#)

CVPR 2020 (Oral) [\[Paper\]](#)



Are CNN-generated images hard to distinguish from real images? We show that a classifier trained to detect images generated by only one model (first column) can easily distinguish them from real images (second column). However, a classifier trained to detect images generated by only one model (first column) can easily distinguish them from real images (second column). However, a classifier trained to detect images generated by only one model (first column) can easily distinguish them from real images (second column). However, a classifier trained to detect images generated by only one model (first column) can easily distinguish them from real images (second column).

gets 92% AUC on the recently released StyleGAN3 model! For more details, please visit this [link](#).

### Abstract

It is possible to create a "universal" detector for telling apart real images from these generated by a CNN, but it is not clear how to use it. To test this, we collect a dataset consisting of fake images generated by 11 different CNN-based architectures that span the space of commonly used architectures today (ProGAN, StyleGAN, BigGAN, CycleGAN, GauGAN, scaded refinement networks, implicit maximum likelihood estimation, second-order attention super-

# CÓMO RECONOZCO UN DEEPFAKE

- Indicadores visuales como distorsiones, deformaciones o incoherencias.
- Distinción del espacio ocular/colocación de los ojos
- Movimientos notables de la cabeza y el cuerpo
- Problemas de sincronización entre los movimientos faciales y labiales y el sonido asociado
- Distorsiones visuales distintivas, generalmente en las pupilas y los lóbulos de las orejas.
- Fondos borrosos o poco definidos
- Artefactos visuales en la imagen o el vídeo

ID del cuerpo: 220632992

## Detección de vídeos deepfake: un análisis de tres técnicas

[Armaan Pishori](#), [Brittany Rollins](#), +2 autores [Omar Uraimov](#) · Publicado en [arXiv.org](#) el 15 de julio de 2020 ·

Ciencias de la Computación

**TLDR** Este artículo presenta tres técnicas y algoritmos: LSTM convolucional, detección de parpadeo e histogramas en escala de grises, que se siguieron mientras participaba en el Desafío de detección de Deepfake y se encontró relevancia en la técnica del histograma en escala de grage sobre otras.

**Abstracto** Los avances recientes en algoritmos de generación de deepfake que producen medios manipulados han tenido implicaciones peligrosas en la privacidad, la seguridad y las comunicaciones masivas. Los esfuerzos para combatir este problema han aumentado en forma de concursos y financiación de investigaciones para detectar deepfakes. Este artículo presenta tres técnicas y algoritmos: LSTM convolucional, detección de parpadeo e histogramas en escala de grises, seguidos mientras participaba en el Desafío de detección de Deepfake. Evaluamos el conocimiento actual sobre vídeos deepfake, una versión más severa de medios manipulados y los métodos utilizados anteriormente, y encontramos relevancia en la técnica del histograma en escala de grises sobre otras. Discutimos las implicaciones de cada método desarrollado y proporcionamos pasos adicionales para mejorar los hallazgos dados.

[Colapsar](#)



[PDF] Lector Semántico



Guardar en la biblioteca



Crear alerta



Citar

## Ciencias de la Computación &gt; Visión por computadora y reconocimiento de patrones

[Presentado el 4 de enero de 2021 ( v1 ), última revisión el 20 de mayo de 2021 (esta versión, v2)]

## ¿Dónde miran las falsificaciones profundas? Detección de rostros sintéticos mediante seguimiento de mirada

Ilke Demir , Umur A. Ciftci

Tras las recientes iniciativas para la democratización de la IA, los generadores de deep fake se han vuelto cada vez más populares y accesibles, provocando escenarios distópicos que conducen a la erosión social de la confianza. Un ámbito particular, como el de las señales biológicas, atrajo la atención hacia métodos de detección que son capaces de explotar firmas de autenticidad en videos reales que aún no han sido falsificados mediante enfoques generativos. En este artículo, primero proponemos varias características prominentes de los ojos y la mirada que las falsificaciones profundas exhiben de manera diferente. En segundo lugar, compilamos esas características en firmas y analizamos y comparamos las de videos reales y falsos, formulando variaciones geométricas, visuales, métricas, temporales y espectrales. En tercer lugar, generalizamos esta formulación al problema de detección de deep fake mediante una red neuronal profunda, para clasificar cualquier video disponible como falso o real. Evaluamos nuestro enfoque en varios conjuntos de datos deep fake, logrando una precisión del 92,48 % en FaceForensics++, 80,0 % en Deep Fakes (en la naturaleza), 88,35 % en CelebDF y 99,27 % en conjuntos de datos DeeperForensics. Nuestro enfoque supera a la mayoría de los detectores falsos biológicos y profundos con arquitecturas de red complejas sin las firmas de mirada propuestas. Realizamos estudios de ablación que involucran diferentes características, arquitecturas, duraciones de secuencias y artefactos de procesamiento.

Comentarios: Para comparecer en las diligencias de ACM ETRA 2021

Asignaturas: Visión por Computadora y Reconocimiento de Patrones (cs.CV) ; Inteligencia artificial (cs.AI)

Citar como: arXiv:2101.01165 [cs.CV]

(o arXiv:2101.01165v2 [cs.CV] para esta versión)

<https://doi.org/10.48550/arXiv.2101.01165>DOI relacionado : <https://doi.org/10.1145/3448017.3457387>

### Historial de envíos

De: Ilke Demir [ [ver correo electrónico](#) ]

[v1] lunes, 4 de enero de 2021 18:54:46 UTC (8,840 KB)

[v2] jueves, 20 de mayo de 2021 17:59:20 UTC (11,012 KB)



IEEE Xplore®

Navegar

Mi configuración

Ayuda

Iniciar sesión institucional

Todo



BÚSQUEDA AVANZADA

Conferencias &gt; ICASSP 2021 - 2021 IEEE Inter... ?

## Exposición de rostros generados por GAN utilizando reflejos especulares corneales inconsistentes

Autor: IEEE

Citar esto

PDF

Shuhu ; Yuezun Li ; Si Wei Lyu **Todos los autores**

55

Citas en

Documentos

738

Lleno

Vistas de

texto



### Abstracto

Secciones del documento



INTRODUCCIÓN

### Abstracto:

Los sofisticados modelos de redes generativas adversarias (GAN) ahora pueden sintetizar rostros humanos altamente realistas que son difíciles de distinguir visualmente de los reales. En este trabajo, mostramos que las caras sintetizadas con GAN pueden exponerse con reflejos especulares corneales inconsistentes entre dos ojos. La inconsistencia se debe a la falta de restricciones físicas/fisiológicas en los modelos GAN. Mostramos que tales artefactos existen ampliamente en

# FACE REVAMPING



IEEE.org | Exploración IEEE | IEEE SA | Espectro IEEE | Más sitios Suscribir Qué es la sostenibilidad, definición becas-santander.com/.../que-es-

**IEEE Xplore®** Navegar Mi configuración Ayuda Iniciar sesión institucional

Todo   BÚSQUEDA AVANZADA

Conferencias > Conferencia IEEE 2013 sobre Comput... ?

## Detección de pulso a partir de movimientos de la cabeza en vídeo

Autor: IEEE Citar esto PDF

Guha Balakrishnan ; Fredo Durand ; Juan Guttag Todos los autores

<b>340</b> Citas en Documentos	<b>101</b> Citas en Patentes	<b>2898</b> Lleno Vistas de texto
-----------------------------------	---------------------------------	--------------------------------------

R ↔ © 📁 🔔

**Abstracto**

Secciones del documento

1. Introducción
2. Fondo

**Abstracto:** Extraemos la frecuencia cardíaca y la duración de los latidos de los videos midiendo el movimiento sutil de la cabeza causado por la reacción newtoniana al flujo de sangre en cada latido. Nuestro método rastrea las características de la cabeza y realiza un análisis de componentes principales (PCA) para descomponer sus trayectorias en un conjunto de movimientos de componentes. Luego elige el componente que mejor se corresponde con los latidos del corazón en función de su espectro de frecuencia temporal. Finalmente, analizamos el movimiento proyectado a este componente e

# FOTOPLESTIMOGRFÍA



Avatares Digitales que puedan interactuar vía Internet con personas, es una evolución de los famosos *chat-bots*, a los que se les ha podido ir dotando de un mejor interfaz, y de una capacidad de resolver problemas cada vez más complejos. Una demostración inicial de esto fueron los dos bots con *GPT3* que charlaban entre ellos usando avatares creados con "This Person Does Not Exist".

## Avatares Hiper-realistas



THIS IS **NOT** MORGAN FREEMAN.

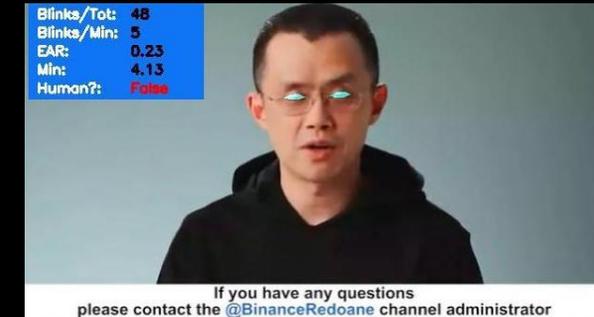


Y si mezclas estos dos conceptos, tienes los "Humanos Digitales"



# DIGITAL REMOTE

Onboarding de nuevos clientes: Cómo crear un proceso de Onboarding + lista de seguimiento



## ¿Qué es el proceso de incorporación de KYC?

El proceso de incorporación KYC, o Know Your Customer, es la puerta de entrada para establecer una relación segura con los clientes. El proceso de incorporación de KYC implica recopilar y verificar información del cliente para garantizar el cumplimiento de los estándares regulatorios y mitigar los riesgos.

KYC, un requisito legal para todas las instituciones financieras, previene el lavado de dinero, el financiamiento del terrorismo y los delitos financieros. Es un proceso integral para verificar las identidades de los clientes, protegiendo a las empresas del fraude y las amenazas cibernéticas.

En estos entornos, ya son cada vez más los que utilizan *DeepFakes* para intentar burlar los procesos de seguridad. Las plataformas de intercambio de criptomonedas, se topan cada día más con personas que utilizan *DeepFakes* para pasar el proceso de *KYC* a la hora de crearse una *Wallet Web3* en una plataforma, pero sucede lo mismo en entornos bancarios

# AI-synthesized faces are indistinguishable from real faces and more trustworthy

Sophie J. Nightingale<sup>a,1</sup> and Hany Farid<sup>b</sup>

<sup>a</sup>Department of Psychology, Lancaster University, Lancaster LA1 4YW, United Kingdom; and <sup>b</sup>Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720

Edited by William Press, Computer Sciences and Integrative Biology, University of Texas at Austin, Austin, TX; received November 11, 2021; accepted December 20, 2021

Artificial intelligence (AI)-synthesized text, audio, image, and video are being weaponized for the purposes of nonconsensual intimate imagery, financial fraud, and disinformation campaigns. Our evaluation of the photorealism of AI-synthesized faces indicates that synthesis engines have passed through the uncanny valley and are capable of creating faces that are indistinguishable—and more trustworthy—than real faces.

deep fakes | face perception

Artificial intelligence (AI)-powered audio, image, and video synthesis—so-called deep fakes—has democratized access to previously exclusive Hollywood-grade, special effects technology. From synthesizing speech in anyone's voice (1) to synthesizing an image of a fictional person (2) and swapping one person's identity with another or altering what they are saying in a video (3), AI-synthesized content holds the power to entertain but also deceive.

Generative adversarial networks (GANs) are popular mechanisms for synthesizing content. A GAN pits two neural networks—a generator and discriminator—against each other. To synthesize an image of a fictional person, the generator starts with a random array of pixels and iteratively learns to synthesize a realistic face. On each iteration, the discriminator learns to distinguish the synthesized face from a corpus of real faces; if the synthesized face is distinguishable from the real faces, then the discriminator penalizes the generator. Over multiple iterations, the generator learns to synthesize increasingly more realistic faces until the discriminator is unable to distinguish it from real

regression analyses were conducted—one for real and one for synthetic faces—to examine the effect of stimuli gender and race on accuracy. For real faces, there was a significant gender × race interaction,  $\chi^2(3, N = 315) = 95.03, P < 0.001$ . Post hoc Bonferroni-corrected comparisons revealed that mean accuracy was higher for male East Asian faces than female East Asian faces and higher for male White faces than female White faces. For synthetic faces, there was also a significant gender × race interaction,  $\chi^2(3, N = 315) = 68.41, P < 0.001$ . For both male and female synthetic faces, White faces were the least accurately classified, and male White faces were less accurately classified than female White faces. We hypothesize that White faces are more difficult to classify because they are overrepresented in the StyleGAN2 training dataset and are therefore more realistic.

**Experiment 2.** In this study, 219 new participants, with training and trial-by-trial feedback, classified 128 faces taken from the same 800 set of faces as in experiment 1. Shown in Fig. 24 is the distribution of participant accuracy (orange bars). The average accuracy improved slightly to 59.0% (95% CI [57.7%, 60.4%]), with no response bias:  $d' = 0.46; \beta = 0.99$ . Despite providing trial-by-trial feedback, there was no improvement in accuracy over time, with an average accuracy of 59.3% (95% CI [57.8%, 60.7%]) for the first set of 64 faces and 58.8% (95% CI [57.4%, 60.3%]) for the second set of 64 faces. Further analyses to examine the effect of gender and race on accuracy replicated the primary findings of experiment 1. This analysis again revealed that, for both male and female synthetic faces, White faces were the most difficult to classify.



BRIEF REPORT

PSYCHOLOGICAL AND COGNITIVE SCIENCES

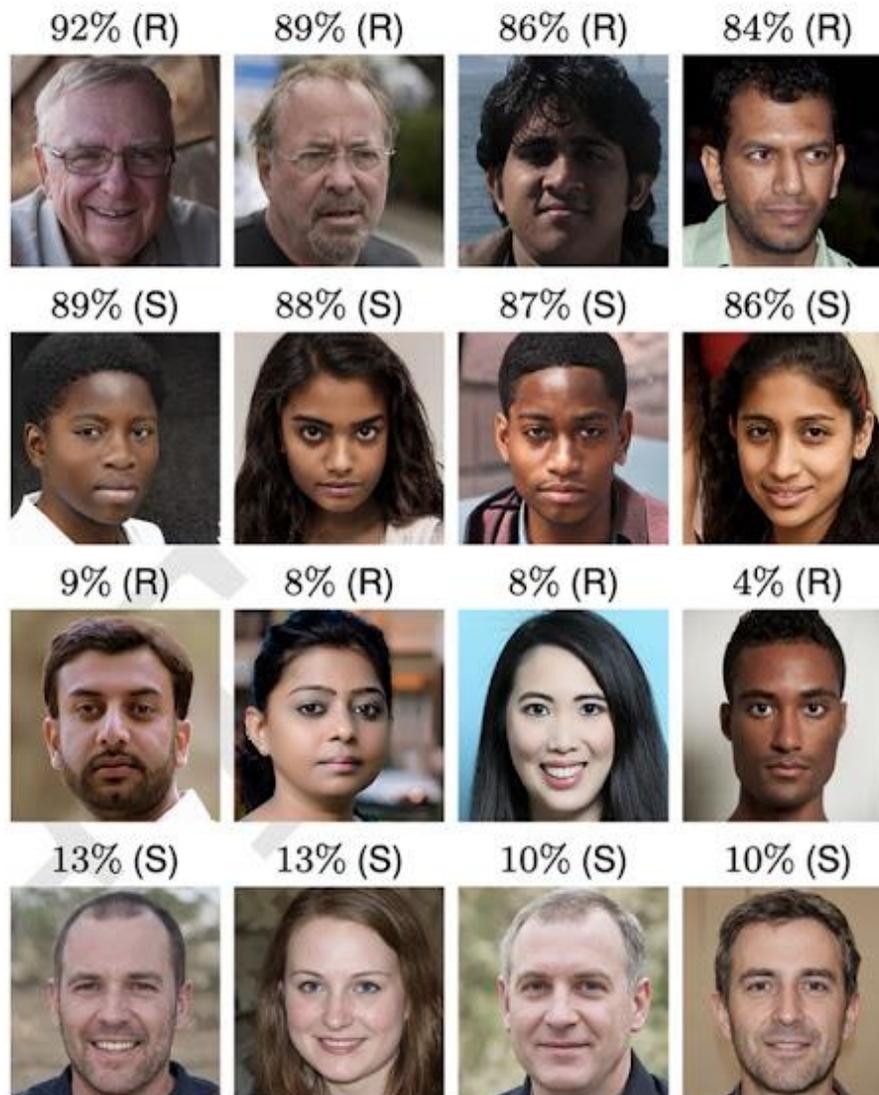


Fig. 1. The most (Top and Upper Middle) and least (Bottom and Lower Middle) accurately classified real (R) and synthetic (S) faces.



proceso, desde la captura de las expresiones por parte de un actor humano, hasta la creación del humano digital que va a reemplazar a este actor

*Humano Digital creado con MetaHuman Animator*

## MetaHuman Animator demo

**GDC 2023**

State of Unreal | Ninja Theory, Xbox Game Studios

# GRACIAS!!!!!!

## CIBERSEGURIDAD EN UN MUNDO DE IA

