Por la cara

Retos y oportunidades del reconocimiento facial

MARTA BELTRÁN PARDO | @MBeltranPardo

JEFA DEL ÁREA CIENTÍFICA EN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Contenidos

1. Contexto

BIOMETRIC UPDATE.COM

About Us | Subscribe

BIOMETRICS NEWS | DIGITAL ID FOR ALL | FEATURES & INTERVIEWS | INDUSTRY INSIGHTS | BRAND FOCUS

facetec Free NFC Chip Scanning

Share
X/Tweet
Link
Comment

Many airports adopt face biometrics for easier travel, but some see a blunt security tool

Jan 15, 2024, 1:08 pm EST | Joel R. McConvey

CATEGORIES Biometrics News | Border and Port Security | Facial Recognition

Face biometrics are showing steady growth and adoption in the air travel industry, as airports around the world upgrade check-in, pre-check-in and boarding procedures with facial recognition systems, to increase efficiency and improve passenger experience. However, news out of Sri Lanka suggests other, potentially worrying uses for FRT.

IAAA

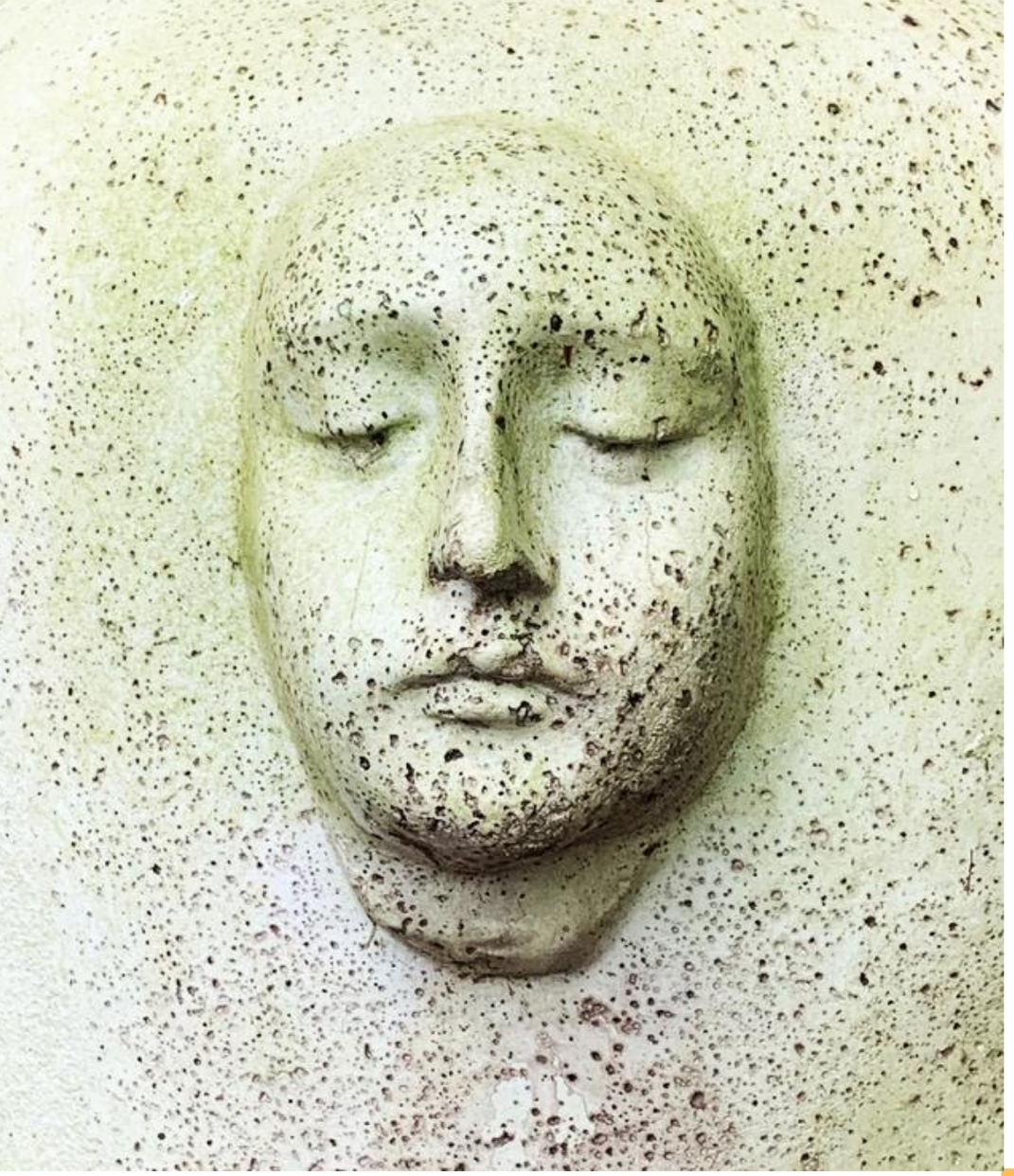
1. Contexto

La identificación es el proceso de reconocer a un individuo particular entre un grupo.

Este proceso compara los datos del individuo con los datos de cada individuo en el grupo.

La autenticación es el proceso de probar que es cierta la identidad reclamada por un individuo.

Este proceso compara los datos del individuo únicamente con los datos asociados a la identidad reclamada.



2. Malentendidos

“No es un método más intrusivo que otros”

Sí que lo es cuando se compara con otros disponibles, revela muchos más datos personales.

“Y sin embargo es un método más preciso”

En la mayor parte de casos no, hay un número de falsos positivos y de falsos negativos diferente de cero. ¿Qué implica equivocarse con un 5% de los usuarios cuando estos son miles o millones?

Li, S., & Deng, W. (2020). Deep facial expression recognition: A survey. *IEEE transactions on affective computing*, *13*(3), 1195-1215.

https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate

2. Malentendidos

“Es mucho más cómodo para los usuarios”

Depende, preguntemos al que sufre los falsos negativos. O pensemos en la situación en la que nos hemos visto hace poco, con mascarillas.

“De los hashes o patrones que usamos no se puede recuperar la cara original”

En muchos casos si es posible cierto grado de reversibilidad, suficiente para implicar riesgos.

http://gendershades.org/

https://pimeyes.com/en

14 equívocos con relación a la identificación y autenticación biométrica

Junio 2020

www.aepd.es/es
www.edps.europa.eu

https://www.aepd.es/documento/nota-equivocos-biometria.pdf

2. Malentendidos

“Es el método más seguro”

- **Ataques de presentación**: En este tipo de ataques el sujeto se presenta ante el sensor que recoge su imagen para realizar la verificación de identidad, empleando algún tipo de artefacto (fotografía o vídeo real, máscara 3D, maquillaje) que le permita hacerse pasar por otro sujeto.

- **Ataques de *morphing***: Este tipo de ataques se basan en conseguir que el sistema utilice como huella o firma facial para un sujeto concreto una imagen generada fusionando (mediante técnicas de *morphing*) las caras de dos sujetos, de manera que el sistema de reconocimiento facial identifique positivamente, en relación con esa huella o firma facial, a los dos sujetos cuya imagen se ha combinado.

Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2021). Face morphing attack generation and detection: A comprehensive survey. *IEEE transactions on technology and society*, *2*(3), 128-145.

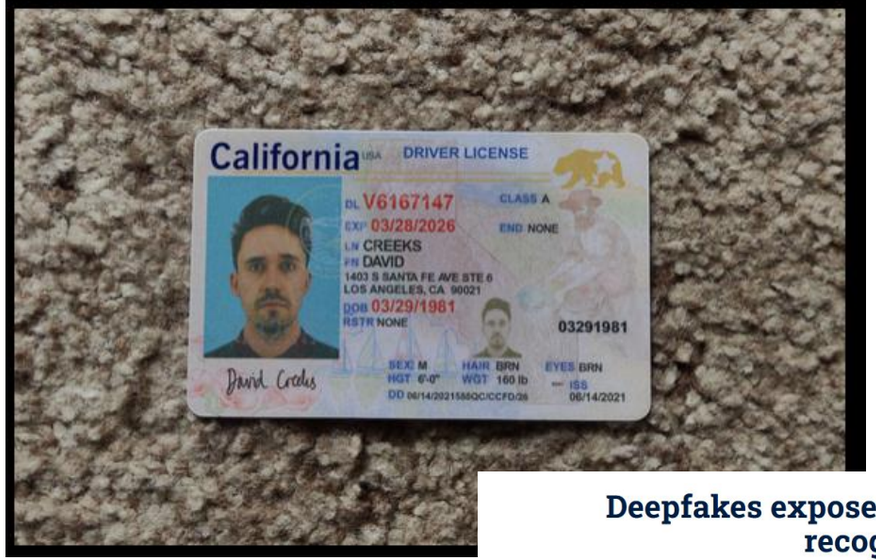
¿Y qué ocurre ahora con los Deep Fakes?

FEATURES

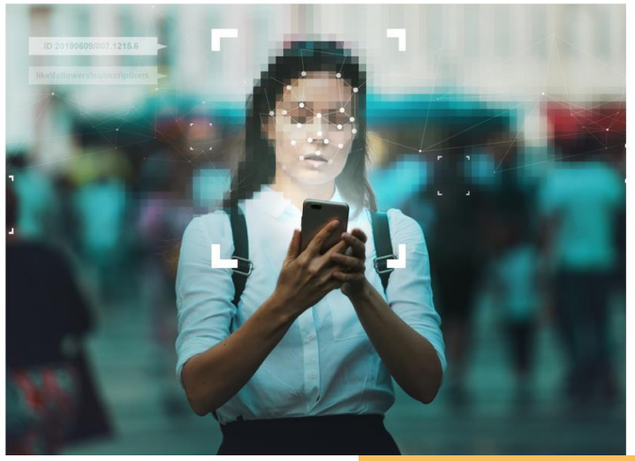
Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs

The site, called OnlyFake, threatens to streamline everything from bank fraud to money laundering, and has implications for cybersecurity writ large.

JOSEPH COX · FEB 8, 2024 AT 9:32 AM



Deepfakes expose vulnerabilities in certain facial recognition technology



Identity, AI/ML, Generative AI, Threat Intelligence

Deepfake face swap attacks on ID verification systems up 704% in 2023

Laura French February 7, 2024

3. Cumplimiento del GDPR

Los datos biométricos dirigidos a identificar/autenticar son categorías especiales de datos

Artículo 9

Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Levantamiento de la prohibición: consentimiento explícito (libre, informado, etc.), el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, para proteger intereses vitales del interesado o de otra persona física, etc.

agencia española protección datos

GUÍA SOBRE TRATAMIENTOS DE CONTROL DE PRESENCIA MEDIANTE SISTEMAS BIOMÉTRICOS

v. noviembre de 2023

https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

4. Amenazas y riesgos

Tengo los malentendidos superados, sé lo que me hago.

Además, tengo claro que para el tratamiento que estoy poniendo en marcha se puede levantar la prohibición de tratar categorías especiales de datos porque concurre una de las circunstancias recogidas en el artículo 9.2 del RGPD.

¡Manos a la obra!: Evaluación de impacto para la protección de datos

¿Qué podría salir mal?

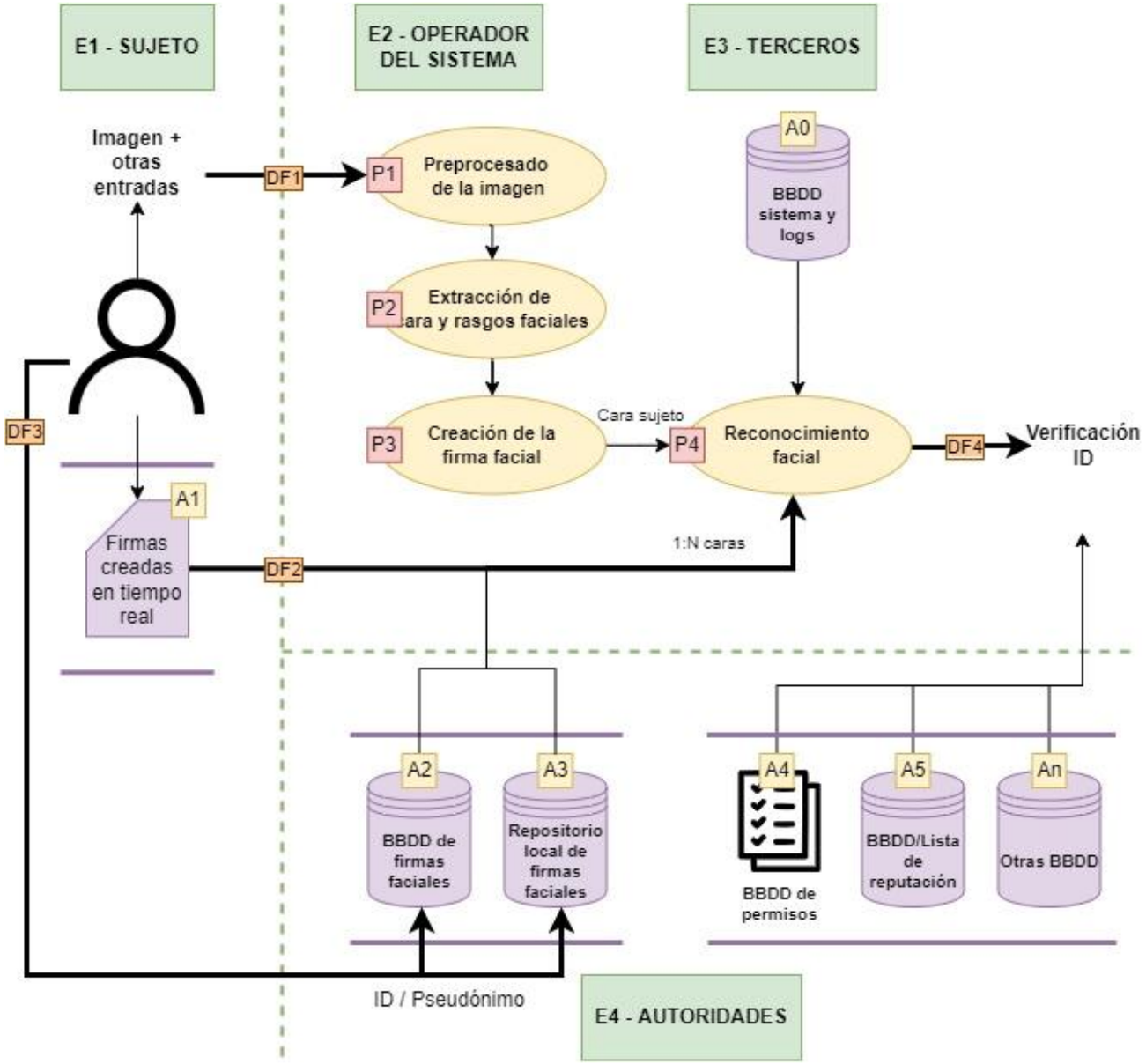
Desde el punto de vista del tratamiento completo

Cuidado, en ciber tendemos a pensar en activos o en sistemas aislados, pero esto es protección de datos y privacidad.

Con impactos en los derechos y libertades

De acuerdo, puede haber brechas de datos, pero no es lo único que puede salir mal, hay que pensar en todas las posibilidades.

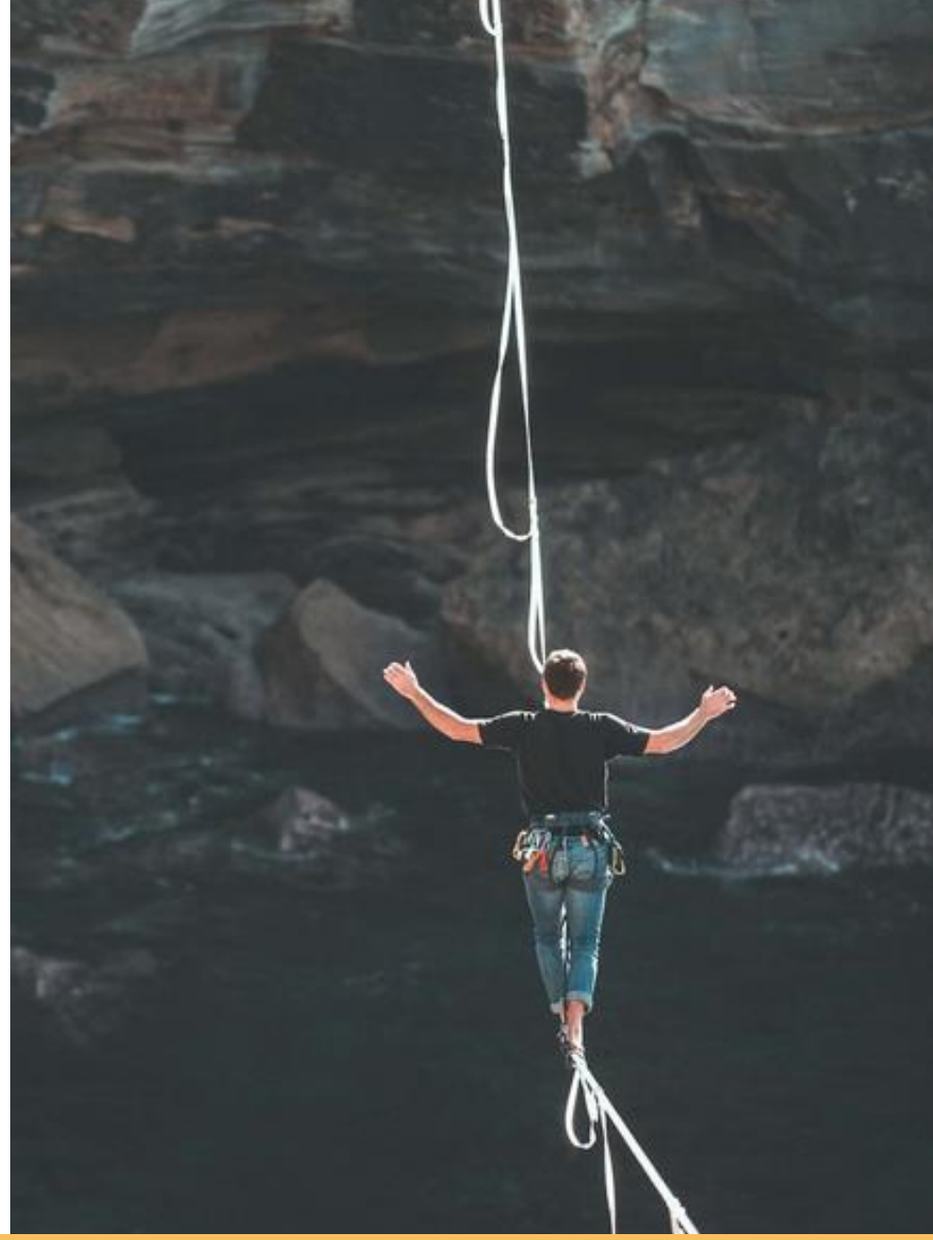
Ejemplo de diagrama de flujo de datos en un caso de uso de identificación



Beltrán, M., & Calvo, M. (2023). A privacy threat model for identity verification based on facial recognition. *Computers & Security*, 103324. https://doi.org/10.1016/j.cose.2023.103324

Algunos factores de riesgo

- Tipos de datos tratados
- Extensión o alcance del tratamiento
- Categorías de interesados
- Efectos colaterales o inesperados
- Fiabilidad y adecuación



¡Gracias! ¿Alguna pregunta?

Por la cara: Retos y oportunidades del reconocimiento facial

Marta Beltrán | mbeltran@aepd.es | @MBeltranPardo

Presentación creada con Visme (https://www.visme.co/es/)
Fotografías: https://unsplash.com
Iconos: https://www.flaticon.es/