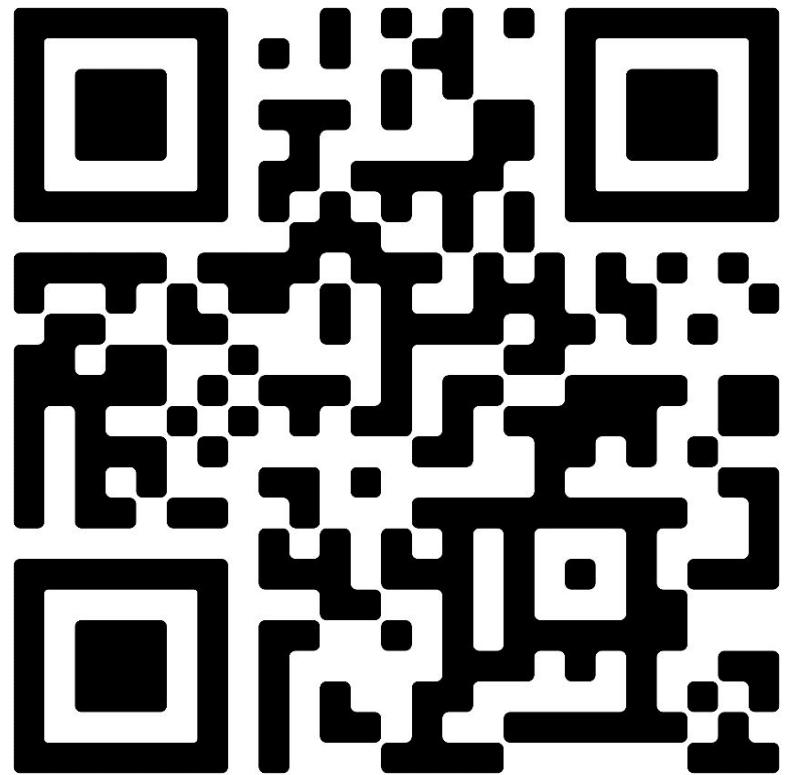


ATACANDO SISTEMAS BIOMÉTRICOS CON IMPRESIÓN 3D





qrco.de/preguntar

SI TIENES PREGUNTAS
DURANTE LA CHARLA
ENTRA AL ENLACE DEL
CÓDIGO QR E INGRESA
ESTE NÚMERO

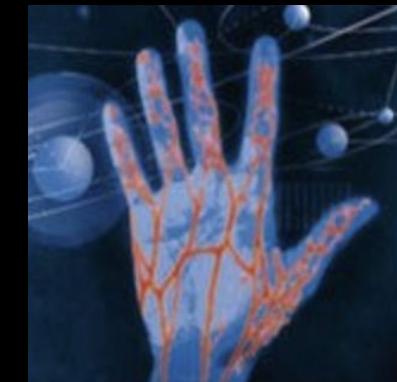
#22617



¿QUE ES UN SISTEMA BIOMÉTRICO?

Rasgos de Comportamiento:

- Forma de caminar
- Firma
- Voz



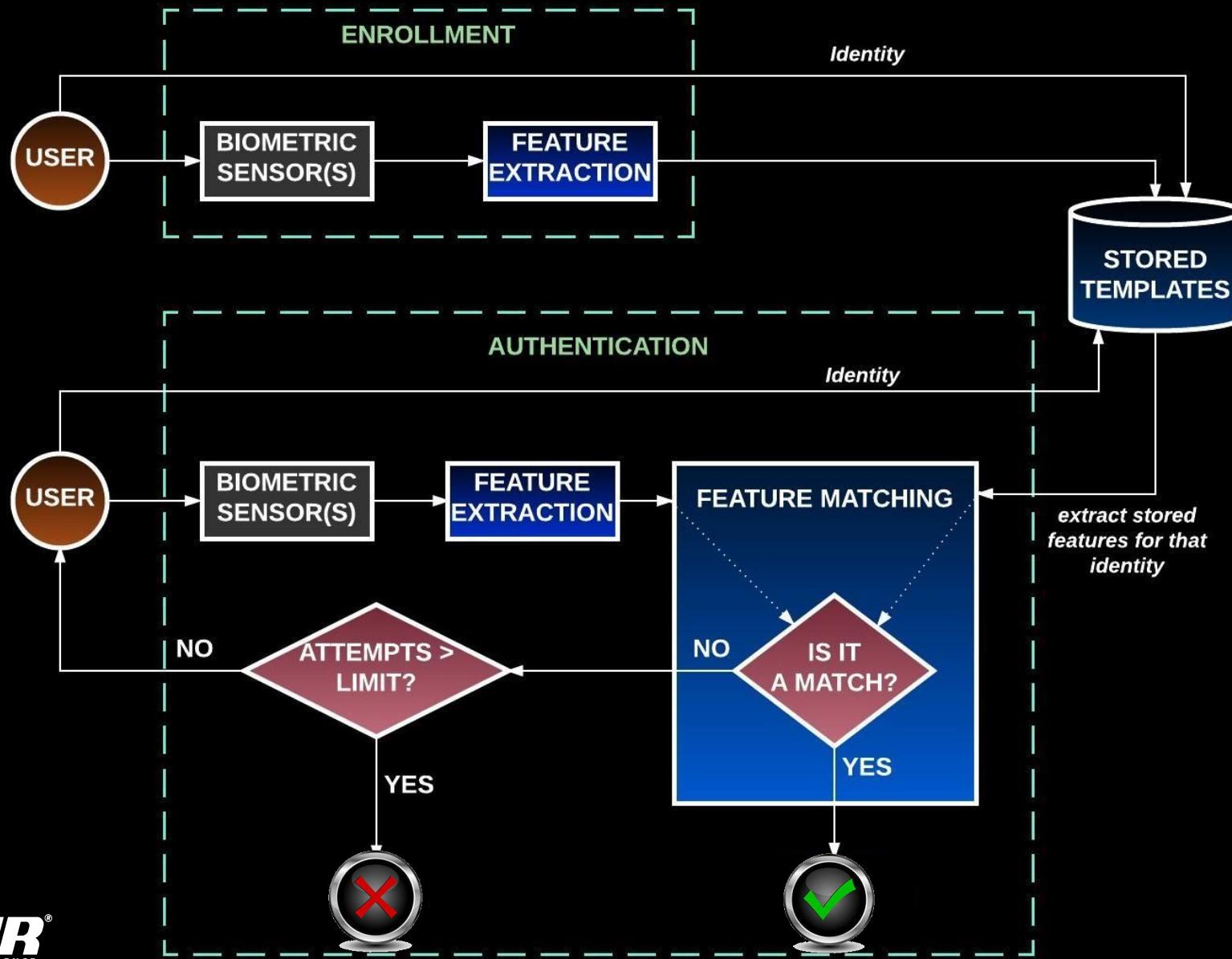
Rasgos Físicos:

- Iris
- Huella Dactilar
- Forma de la Oreja
- ADN
- Rostro
- Patrón de Venas



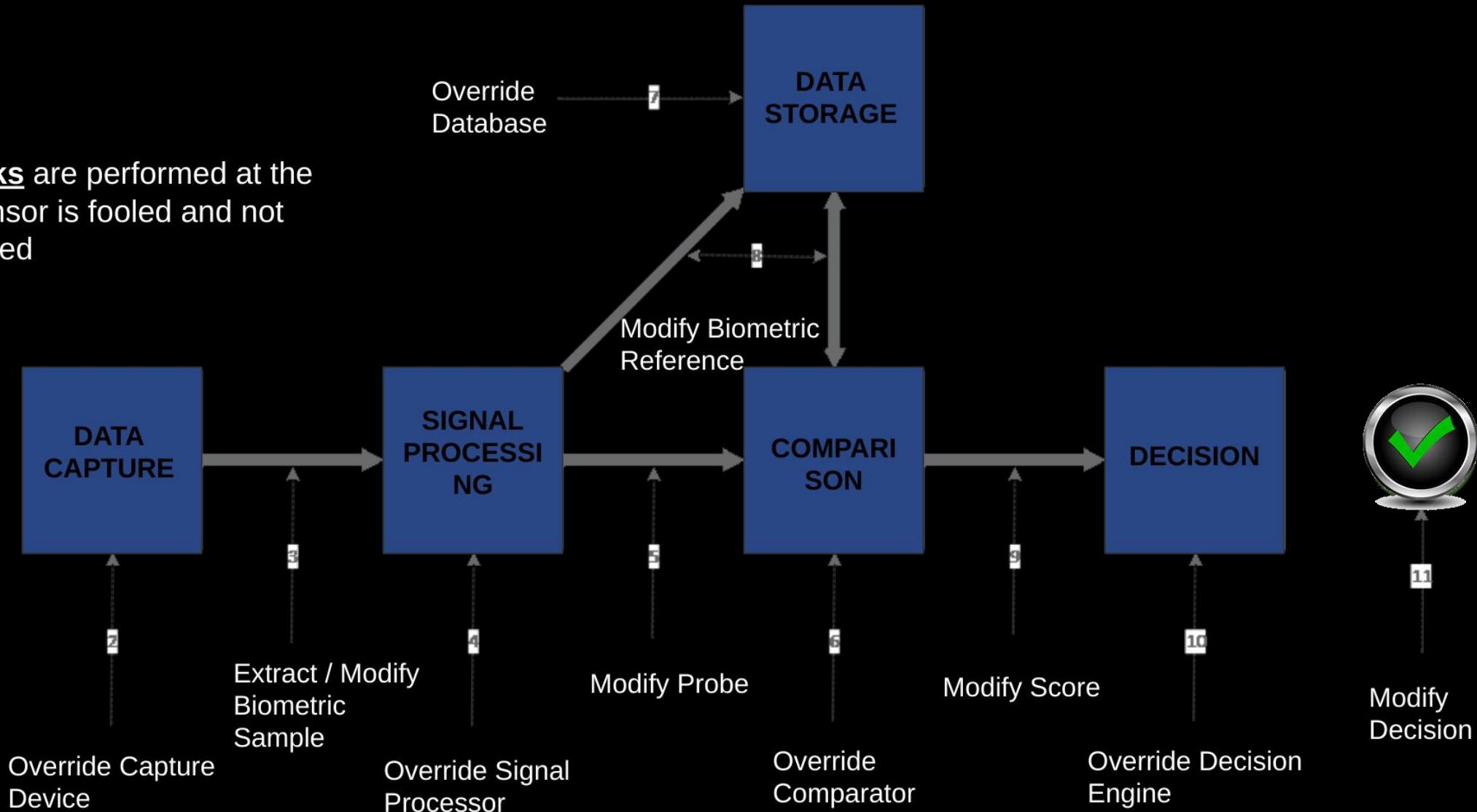
DREAMLAB
TECHNOLOGIES

¿CÓMO FUNCIONAN LOS SISTEMAS BIOMÉTRICOS?



ATAQUES A SISTEMAS BIOMÉTRICOS

Presentation attacks are performed at the sensor level: the sensor is fooled and not replaced nor tampered



ATAQUES DE PRESENTACIÓN EN LA VIDA REAL ROBOS DE BANCO Y PASAJEROS DE AVIÓN



UNITED STATES 2015



UNITED STATES 2010

Sospechosos a la izquierda y sospechosos usando máscaras a la derecha



CANADA 2014



CHINA 2011

ATAQUES DE PRESENTACIÓN EN LA VIDA REAL HUELLAS Y DEDOS FALSOS



ATAQUES DE PRESENTACIÓN EN LA VIDA REAL VOCES FALSAS

Fake voices 'help cyber-crooks steal cash'

© 8 July 2019

f Share



Cvincing fakes of audio are easier to generate than video spoofs

A security firm says deepfaked audio is being used to steal millions of pounds.

Symantec said it had seen three cases of seemingly deepfaked audio of different chief executives used to trick senior financial controllers into transferring cash.

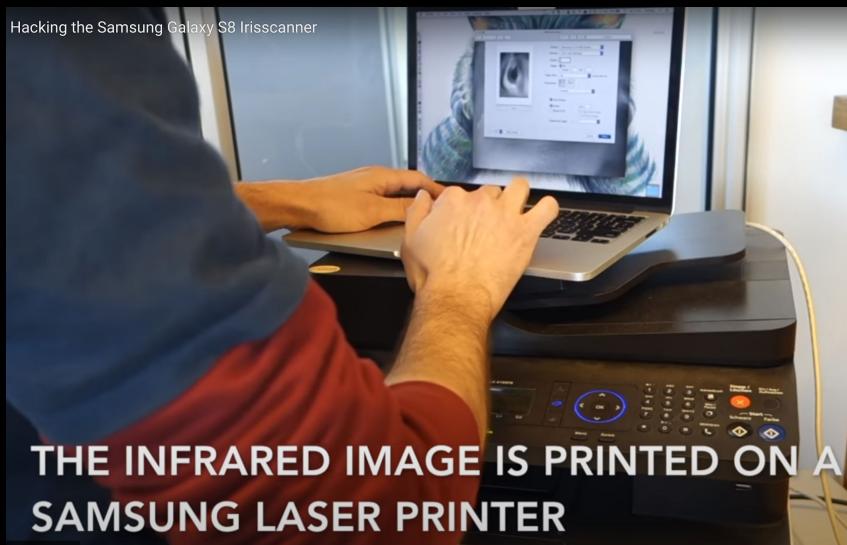
INDUSTRY NEWS

CEO voice deepfake blamed for scam that stole \$243,000

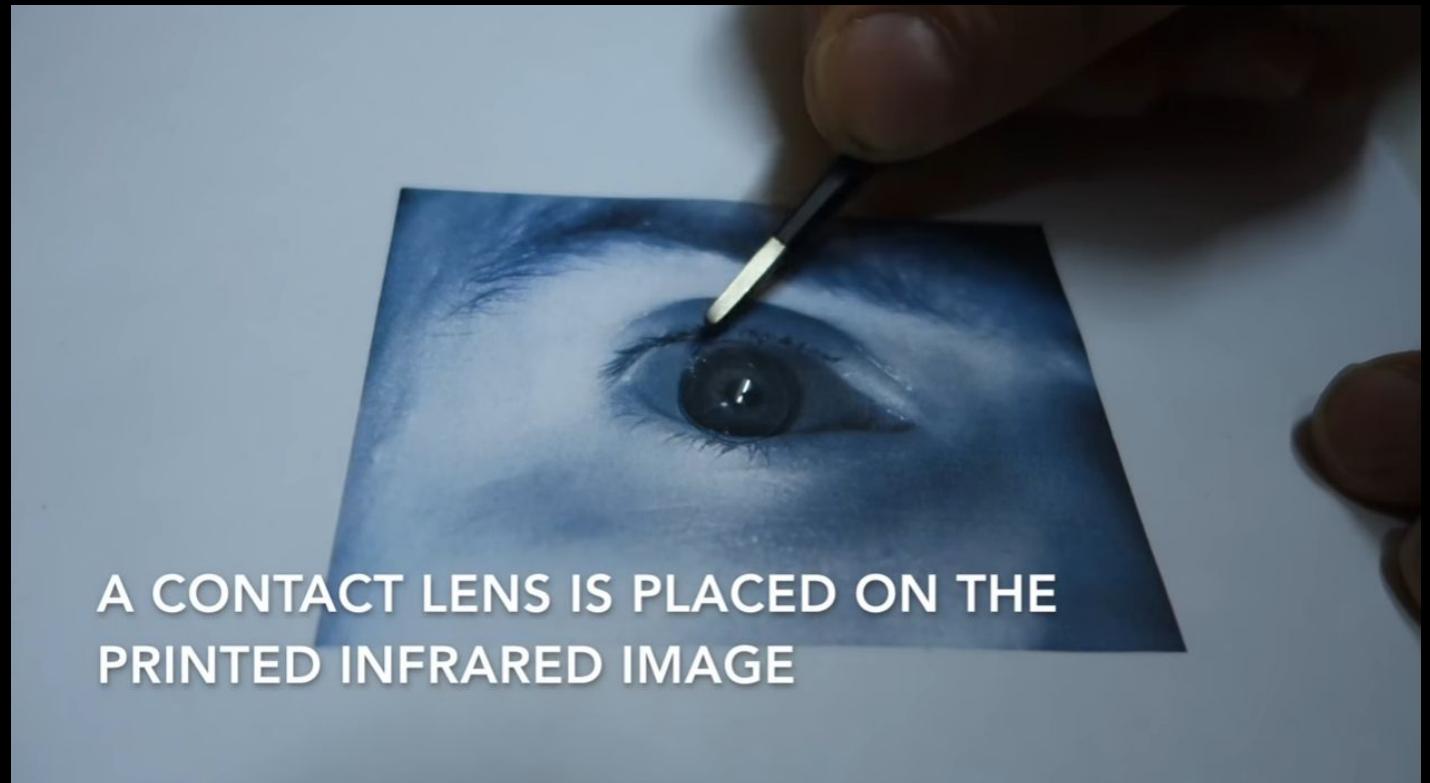
© 5 months ago 3 Min Read



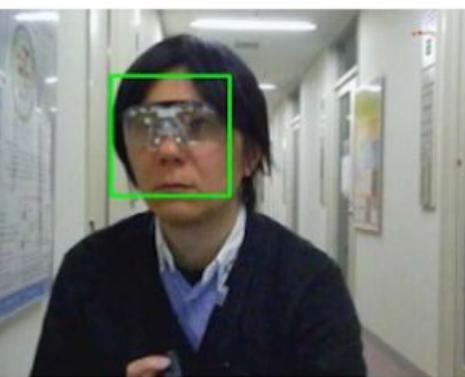
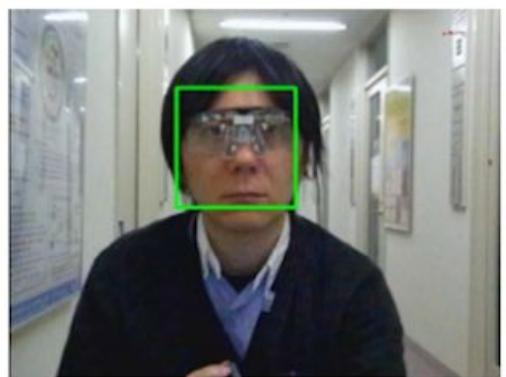
ATAQUES DE PRESENTACIÓN EN LA VIDA REAL ATAQUES A SISTEMAS DE RECONOCIMIENTO DE IRIS



Chaos Computer Club burla el sistema de reconocimiento de iris del smartphone Samsung Galaxy S8 utilizando la impresión de una foto del ojo tomada con cámara infrarroja y lentes de contacto (2017)



ATAQUES DE PRESENTACIÓN EN LA VIDA REAL EVITANDO EL RECONOCIMIENTO FACIAL

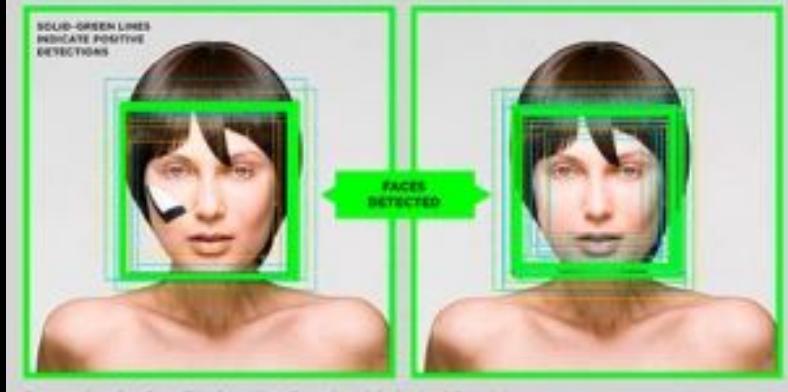


(a) Near infrared LED not lit (detection successful)



(b) Near infrared LED lit (detection failed)

Fig.4 Execution of Facial Detection (Examples) (Area in Green Frame Indicates Successful Detection)



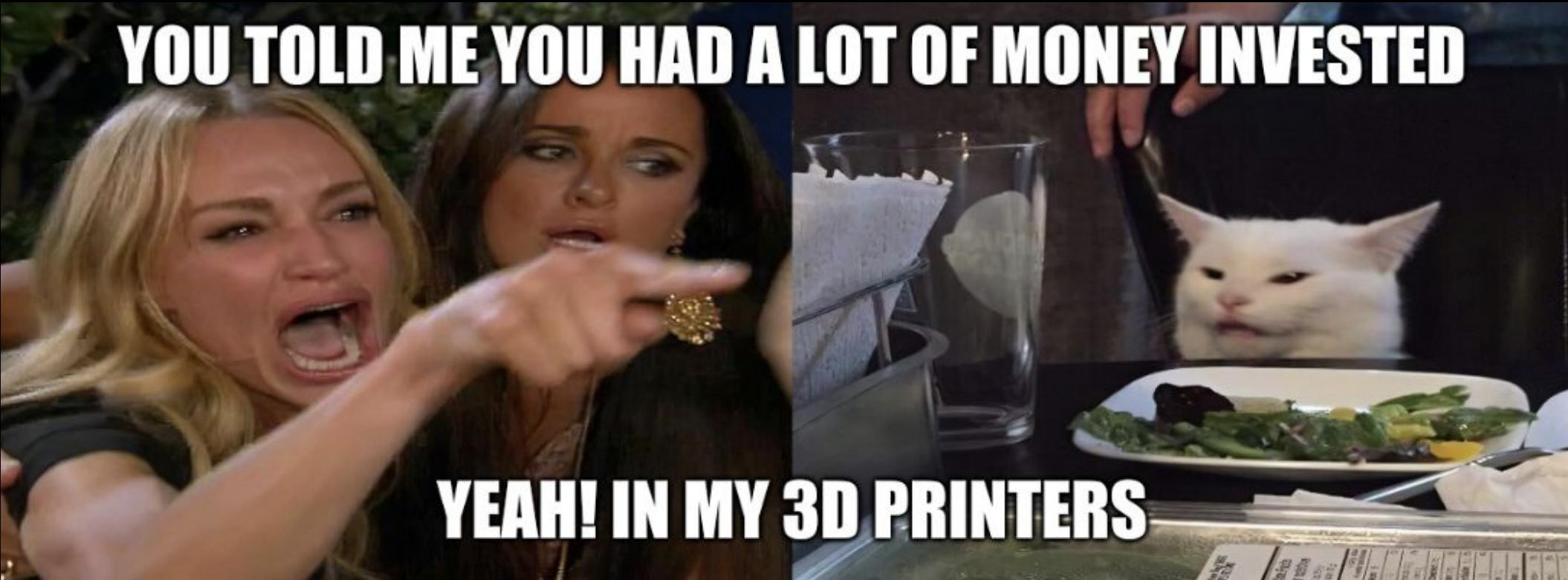
La tasa de error de los sistemas de reconocimiento facial aumenta entre un 5% y un 50% usando barbijos, los barbijos negros que cubran más la nariz presentan las mayores tasas de error.

Los anteojos de colores con patrones también pueden confundir a los sistemas de reconocimiento facial.

¿CÓMO PUEDE AYUDAR LA IMPRESIÓN 3D A ENGAÑAR A LOS SISTEMAS BIOMÉTRICOS?



HACIENDO MIS PROPIOS EXPERIMENTOS PARA BURLAR SISTEMAS BIOMÉTRICOS

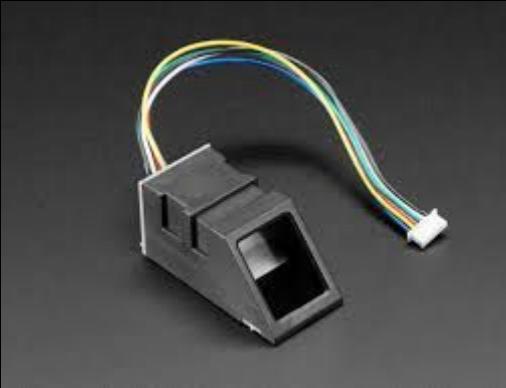


RECONOCIMIENTO DE HUELLAS DACTILARES

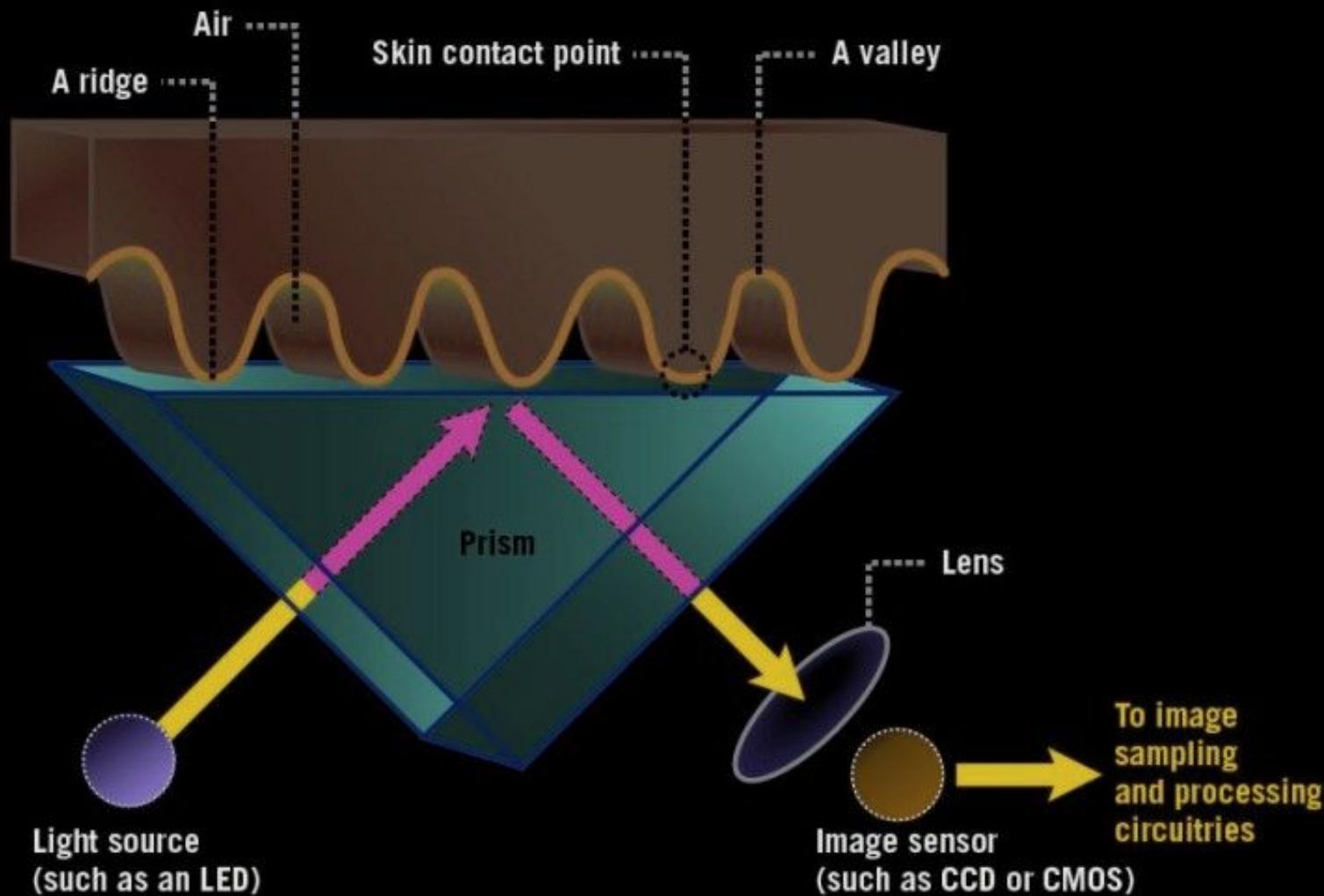


Minucia y Tipica

SENsoRES DE HUELLAS DACTILARES



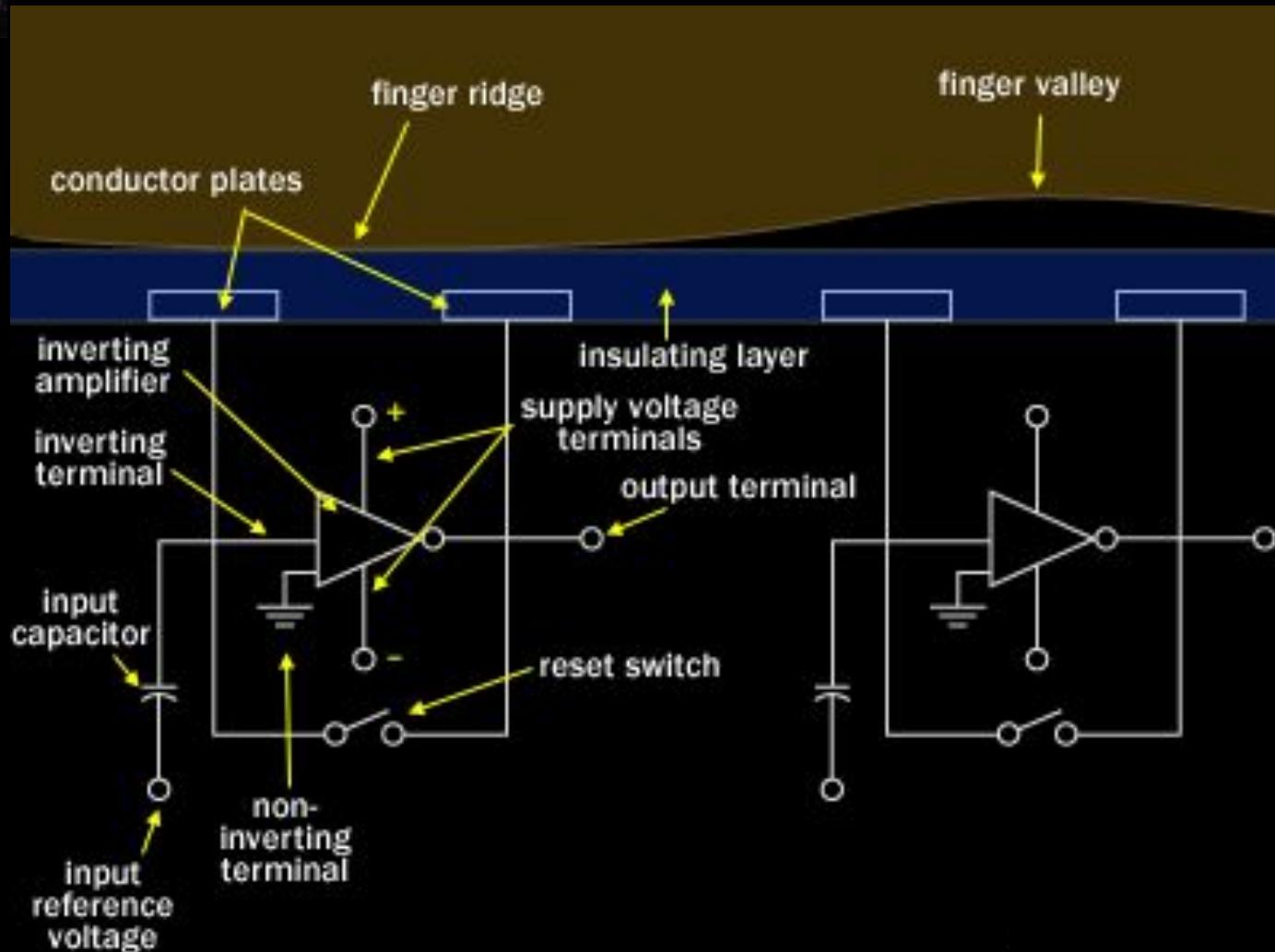
SENSORES DE HUELLAS DACTILARES ÓPTICOS



Los sensores ópticos de huellas digitales son el método más antiguo para capturar y comparar huellas digitales. Esta técnica se basa en capturar una imagen y usar algoritmos para detectar patrones únicos en la superficie, analizando las áreas más claras y oscuras de la imagen.



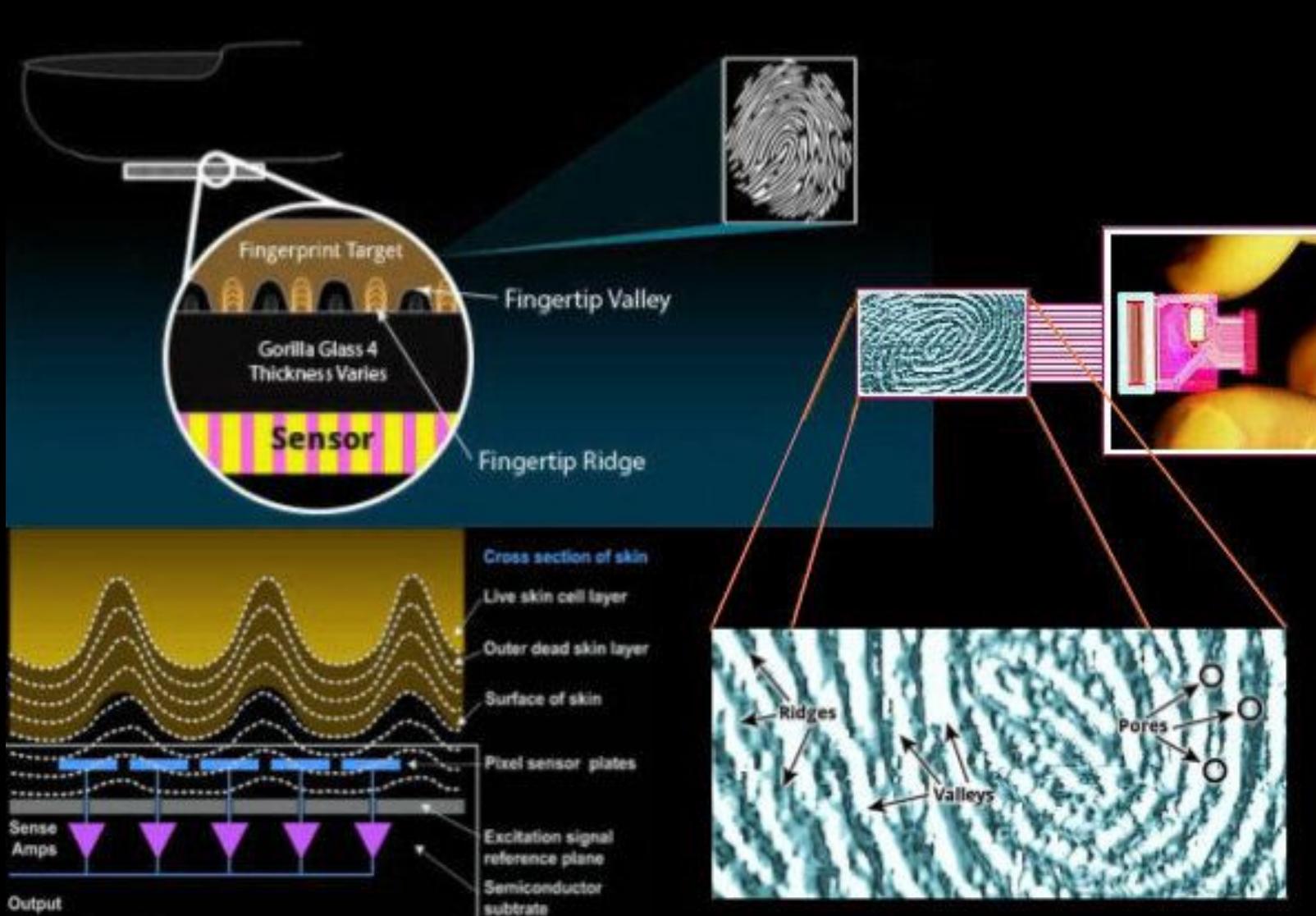
SENsoRES DE HUELLAS DACTILARES CAPACITIVos



Los sensores capacitivos utilizan pequeños circuitos de condensadores para recopilar datos sobre una huella dactilar. Como los condensadores pueden almacenar carga eléctrica, conectarlos a placas conductoras en la superficie del escáner permite que se utilicen para rastrear los detalles de una huella digital.

La carga almacenada en el condensador cambiará ligeramente cuando se coloque el ridge de un dedo sobre las placas conductoras, mientras que un espacio de aire dejará la carga en el condensador relativamente sin cambios.

SENsoRES DE HUELLAS DACTILARES ULTRASÓNICOS



El hardware consiste de un transmisor y un receptor ultrasónicos.

Se transmite un pulso ultrasónico contra el dedo que se coloca sobre el escáner. Parte de este pulso se absorbe y parte se devuelve al sensor, dependiendo de los ridges, los poros y otros detalles que son únicos de cada huella digital.

DISPOSITIVOS A TESTEAR

CELULARES Y SISTEMAS DE CONTROL DE ASISTENCIA

Samsung Galaxy S10
Ultrasonic Fingerprint
Scanner
Face Recognition



SAMSUNG
GALAXY S10



Hysoon FF395
Optical Fingerprint
Scanner
Face Recognition

TA040
Optical Fingerprint
Scanner



Samsung Galaxy A30
Capacitive Fingerprint
Scanner
Face Recognition

MATERIALES NECESARIOS PARA LOS TESTS (ESTOS Y UN MONTÓN MÁS)



ATAQUES DE "GREASE"

Condiciones previas para el ataque

Para utilizar este tipo de ataque, es necesario que haya una mancha o "grease" correspondiente al último usuario del sensor en la superficie del escáner. Debe ser clara y tener la mayoría de las características importantes de la huella dactilar para que el escáner pueda leer de manera confiable los mismos extremos de línea y curvas detectados anteriormente.

Requisitos:

- Sensor de huellas dactilares
- Huella digital registrada de usuario legítimo
- Mancha o "Grease" aplicable en la almohadilla del sensor dejada por el usuario anterior
- Temperatura entre 0-50° C (temperatura de funcionamiento del sensor)
- Ositos de goma, fingertips de silicona, playdoh, guantes de látex

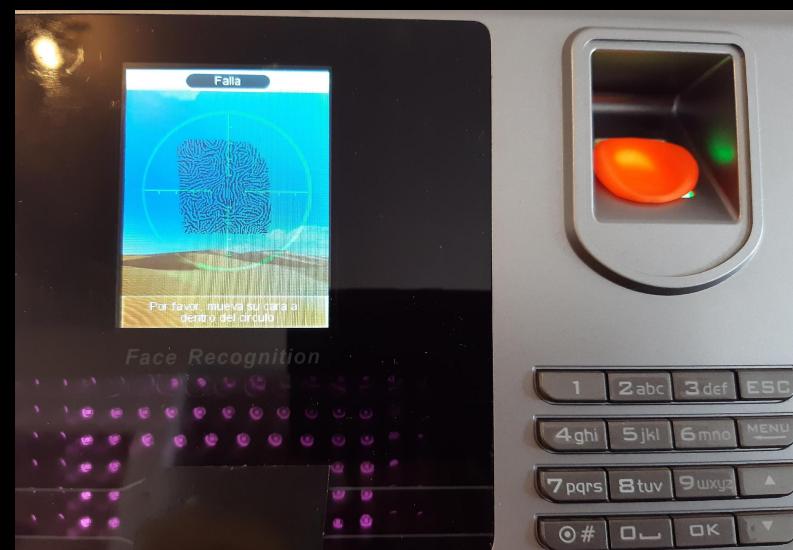


RESULTADOS DE ATAQUES DE "GREASE"

Materiales probados y resultados:

- Ositos de Goma: dedo reconocido
- Playdoh: dedo reconocido
- Guante de Látex: dedo reconocido
- Moist Breathe: no se reconoce el dedo
- Fingertips de Silicona: dedo reconocido

Materials	Sensor Fooled			
	Optical1	Capacitive	Ultrasonic	Optical2
Materiales used				
Gummy Bears	NO	NO	NO	NO
Tinfoil	NO	NO	NO	NO
Playdoh	NO	NO	NO	NO
Latex Glove	NO	NO	NO	NO
Breathe	NO	NO	NO	NO
Silicon Fingertip	NO	NO	NO	NO



ATAQUES DE GREASE "MEJORADOS" Y RESULTADOS

El problema con los ataques de "grease" es que, en la mayoría de los casos, una mancha regular en la superficie del escáner no es suficiente para engañar al sensor. Necesitamos potenciarla con otras sustancias para obtener mejores resultados impersonando usuarios legítimos, estas sustancias deben ser transparentes para que el usuario no las note y con consistencia de pomada para mejorar la mancha de huellas dactilares. Esta sustancia puede esparcirse en la huella digital del usuario legítimo o en el sensor de huellas digitales.



Materials	Sensor Fooled			
Materiales used	Optical1	Capacitive	Ultrasonic	Optical2
Glicerin + Latex Glove	NO	NO	NO	NO
Hand Moisturizer + Latex Glove	NO	NO	NO	NO
Petrolatum Ointment + Latex Glove	YES	YES	NO	YES
Petrolatum + Paraffin + Latex Glove	YES	YES	NO	YES
Cocoa Butter Lip Balm + Latex Glove	YES	YES	NO	YES



ATAQUES CON COOPERACIÓN DEL USUARIO

Condiciones previas para el ataque

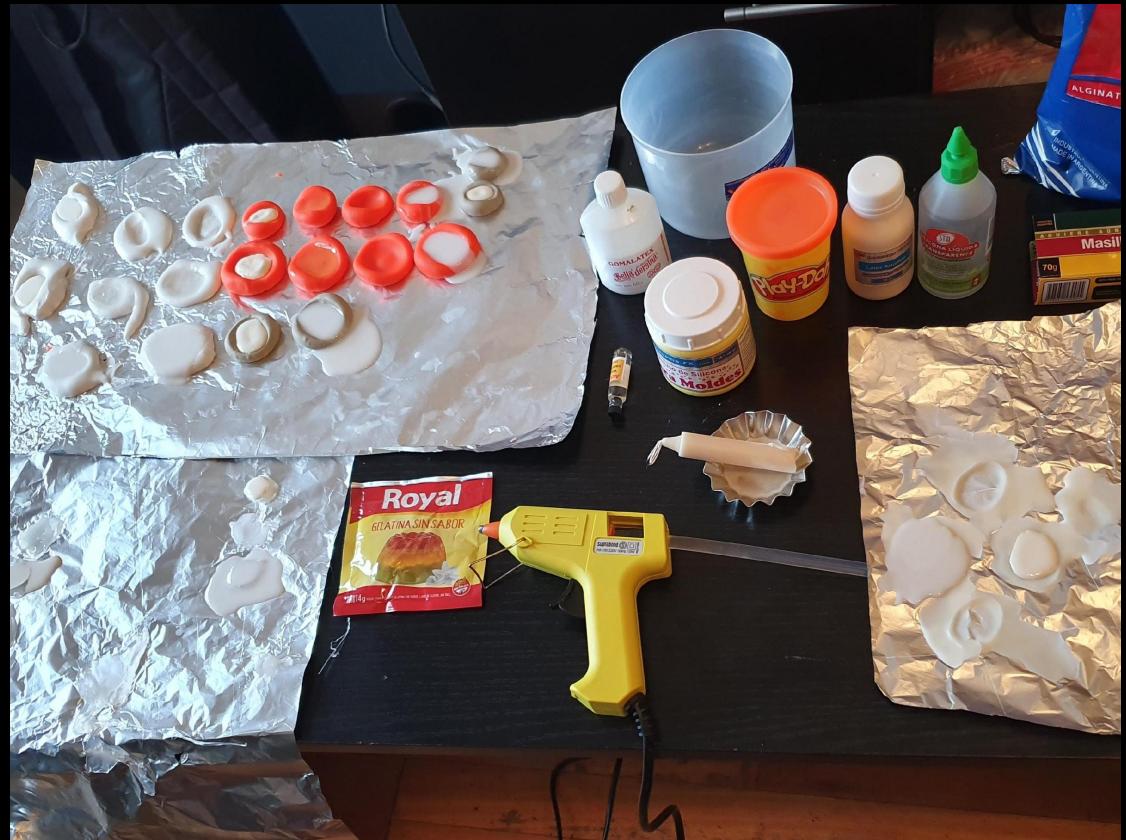
El término cooperativo sugiere que el usuario del que estamos tomando la huella dactilar es consciente del proceso y participa activamente presionando su dedo en una especie de molde. Aunque hemos clasificado este enfoque como "cooperativo", existen formas no consensuadas de lograrlo.

Materiales para el Relleno:

- Silicona
- Gelatina Balística
- Latex Líquido
- Resina Sintética
- Wood Glue

Materiales para Moldes:

- Alginato
- Masilla Epoxy
- Playdoh
- Hot Glue
- Cera de Vela



RESULTADOS DE ATAQUES COOPERATIVOS



Materials		Sensor Fooled			
		Optical	Capacitive	Ultrasonic	Optical2
Mould	Casting				
Alginate	Silicone	YES	NO	NO	YES
Epoxy putty	Silicone	NO	NO	NO	NO
Playdoh	Silicone	YES	NO	NO	YES
Hot Glue	Silicone	YES	NO	NO	YES
Candle Wax	Silicone	YES	NO	YES	YES
Alginate	Ballistic gelatin	NO	NO	NO	NO
Epoxy putty	Ballistic gelatin	NO	NO	NO	NO
Playdoh	Ballistic gelatin	NO	NO	NO	NO
Hot Glue	Ballistic gelatin	NO	NO	NO	NO
Candle Wax	Ballistic gelatin	NO	NO	NO	NO
Alginate	Liquid latex	YES	YES	YES	YES
Epoxy putty	Liquid latex	NO	NO	NO	NO
Playdoh	Liquid latex	YES	YES	NO	YES
Hot Glue	Liquid latex	YES	YES	YES	YES
Candle Wax	Liquid latex	YES	NO	YES	YES
Alginate	Sintetic Resin	NO	NO	NO	NO
Epoxy putty	Sintetic Resin	NO	NO	NO	NO
Hot Glue	Wood glue	YES	YES	YES	YES



ATAQUES SIN COOPERACIÓN DEL USUARIO

Condiciones Previas para el Ataque

En estos ataques el usuario no participa activamente y las huellas dactilares latentes se obtienen de forma no cooperativa.

Suponiendo que se haya identificado la huella digital latente correcta, los siguientes son los pasos a seguir:

Procedimiento

1. Mejorar la huella latente con vapores de pegamento o polvo para huellas
2. Levantar la huella latente con cámara digital con macro o cinta transparente
3. Mejorar digitalmente la huella digital con software
4. Crear un molde
5. Crear huellas artificiales rellenando el molde con silicona, látex líquido o wood glue.

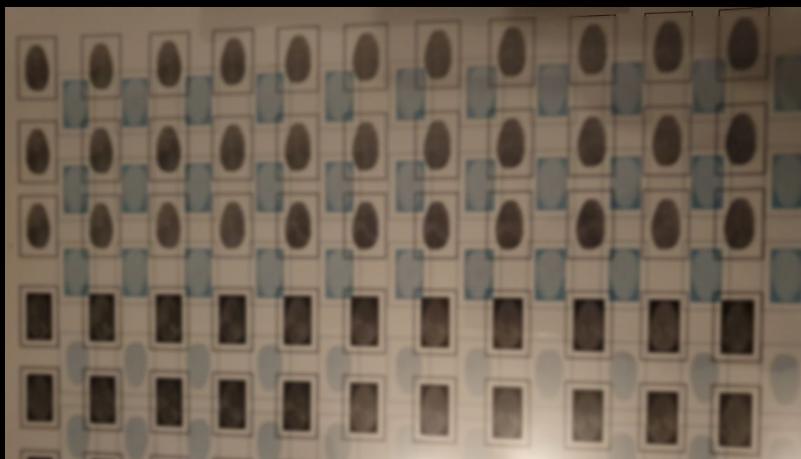
Materiales

- Pegamento con Etil Cianoacrilato
- Pincel y Polvo para Huellas Dactilares
- Camara Digital
- Cinta Adhesiva
- Almohadilla de Tinta
- Transparencia
- Papel Film
- Guantes de Latex
- Silicona
- Látex Liquido
- Wood glue
- Papel



RESULTADOS DE ATAQUES NO COOPERATIVOS

Materials		Results			
Material1	Material2	Optical	Capacitive	Ultrasonic	Optical2
Fingerprint Ink	Paper	NO	NO	NO	NO
Fingerprint Ink	Plastic wrap	NO	NO	NO	NO
Fingerprint Ink	Latex glove	NO	YES	YES	NO
Transparent Tape	Fingerprint enhanced with fingerprint powder	NO	NO	NO	NO
Transparent Tape	Fingerprint enhanced with cyanoacrylate	NO	NO	NO	NO
Offset Plate	Silicone	NO	NO	NO	NO
Offset Plate	Liquid Latex	NO	NO	NO	NO
Offset Plate	Wood glue	NO	NO	NO	NO
Transparency	Silicone	NO	NO	NO	NO
Transparency	Liquid Latex	YES	NO	NO	YES
Transparency	Wood glue	NO	NO	NO	NO

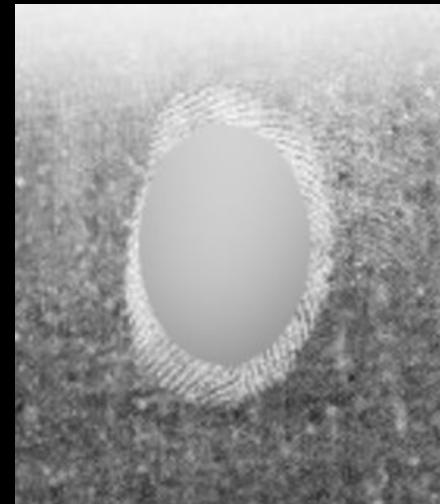


ATAQUES NO COOPERATIVOS CON IMPRESIÓN 3D MATERIALES Y SOFTWARE NECESARIO



```
yl@ws17:~/tools/Fingerprint-Enhancement-Python/src$ ls
enhanced2bw.jpg  image_enhance.py    ridge_freq_2.py  ridge_segment.py
enhanced2.jpg    image_enhance.pyc   ridge_freq.py    ridge_segment.pyc
enhanced.jpg     main_enhancement.py ridge_freq.pyc
frequest.py      ridge_filter.py   ridge_orient.py
frequest.pyc     ridge_filter.pyc  ridge_orient.pyc
yl@ws17:~/tools/Fingerprint-Enhancement-Python/src$ █
```

La precisión de una impresora de resina UV doméstica es de 25 micrones. Los ridges de las huellas humanas en general tienen una profundidad entre 20 y 60 micrones.



ATAQUES NO COOPERATIVOS CON IMPRESIÓN 3D

Procedimiento

1. Levante la huella digital latente con una cámara digital con funcionalidad macro
2. Utilice una herramienta para mejorar digitalmente las huellas digitales, por ejemplo, esta herramienta python basada en la tool `fingerprint-enhancement` de Utkarsh-Deshmukh: <https://github.com/ylevalle/Fingerprint-Enhancement-Python>
3. Convierta el archivo JPG mejorado en un archivo SVG, importe el archivo SVG en Tinkercad para crear un modelo 3D de la huella digital
4. Configure la longitud y el ancho de la huella dactilar de acuerdo con las medidas de la huella latente original, coloque un bloque delgado detrás de la huella dactilar, configure la profundidad del ridge y cree dos modelos 3D diferentes: uno negativo o hueco para usar de molde y otro positivo para pruebas directas.
5. Exporte el archivo con los modelos 3D en un formato de archivo imprimible en 3D (STL) y cárguelo en la impresora 3D Anycubic Photon.
6. Una vez completada la impresión, los moldes impresos en 3D requieren ser enjuagados con alcohol isopropílico y un curado posterior con una lámpara UV o luz solar directa.
7. Llene los moldes huecos o negativos impresos en 3D con látex líquido o wood glue.



Huella digital de prueba mejorada con software



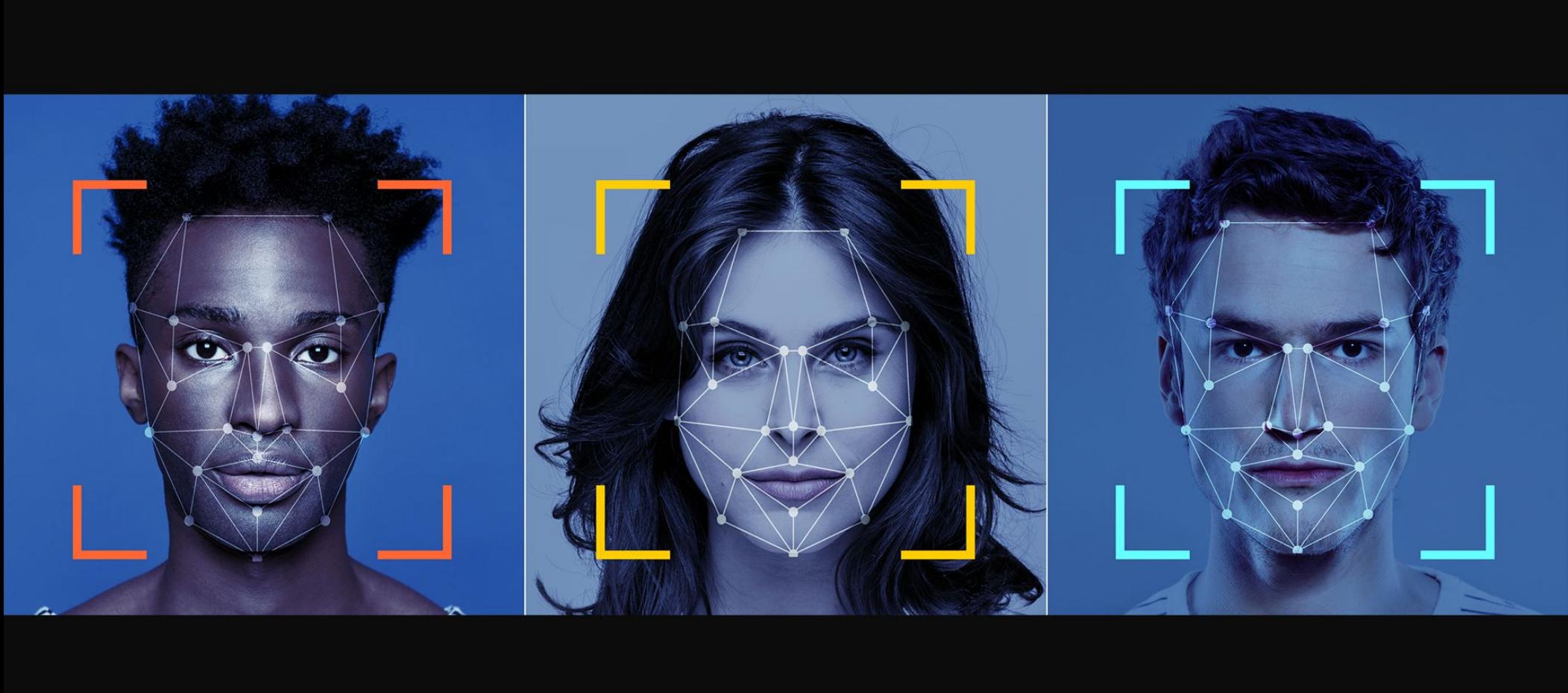
ATAQUES NO COOPERATIVOS CON IMPRESIÓN 3D RESULTADOS



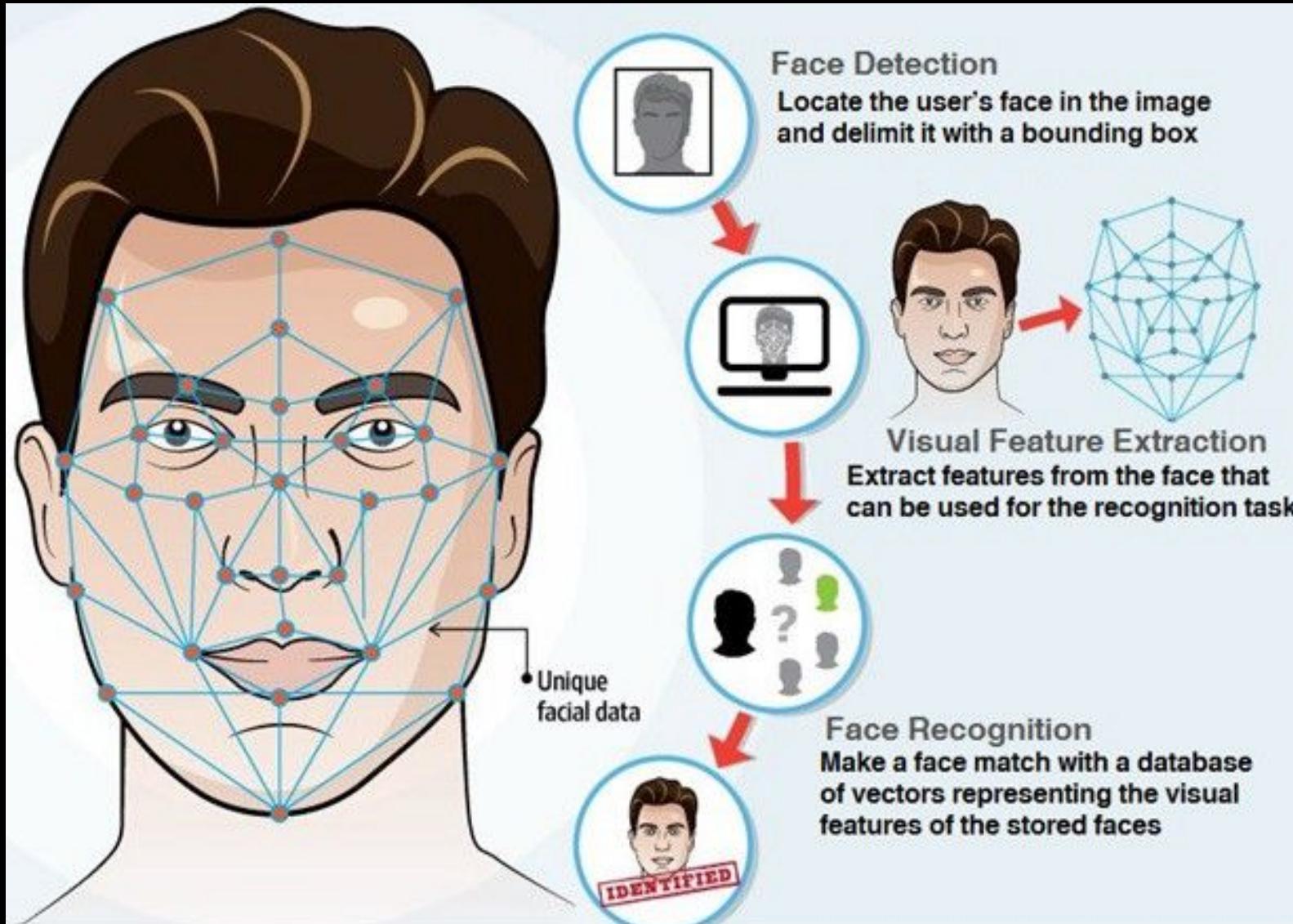
Materials		Results			
Material1	Material2	Optical	Capacitive	Ultrasonic	Optical2
Fingerprint on glass	UV DLP Resin positive from photo	YES	NO	YES	NO
Inked fingerprint	UV DLP Resin positive from photo	YES	NO	YES	NO
Fingerprint on glass	3D mould from photo	YES	YES	YES	YES
Inked fingerprint	3D mould from photo	YES	YES	YES	YES



PRÓXIMO PASO DEL RESEARCH SISTEMAS DE RECONOCIMIENTO FACIAL



SISTEMAS DE RECONOCIMIENTO FACIAL



SISTEMAS DE RECONOCIMIENTO FACIAL ATAQUES USANDO FOTOS Y VIDEOS



SISTEMAS DE RECONOCIMIENTO FACIAL ATAQUES USANDO MÁSCARAS



Máscaras rígidas a pedido con agujeros para los ojos (IDIAP)



Máscaras rígidas a pedido sin agujeros para los ojos (IDIAP)



Máscaras de silicona a pedido (IDIAP)



Arnold Silicone Mask
Silicone Mask
From: \$575.00
Multiple Styles Available

Clarence the Old Man Silicone Mask
\$575.00
Multiple Styles Available

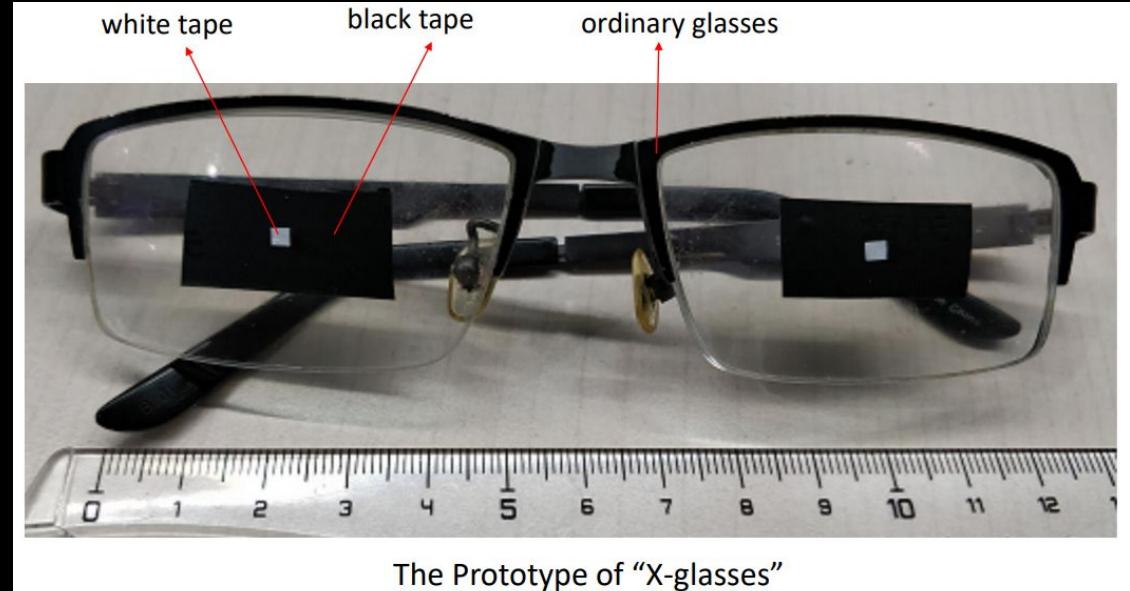
Codger the Old Man Silicone Mask
From: \$575.00
Multiple Styles Available

Máscaras de silicona genéricas

SISTEMAS DE RECONOCIMIENTO FACIAL OTROS ATAQUES



Maquillaje



The Prototype of "X-glasses"

X-glasses para engañar al Face ID en personas dormidas



Morphed Face

(a) Subject 1

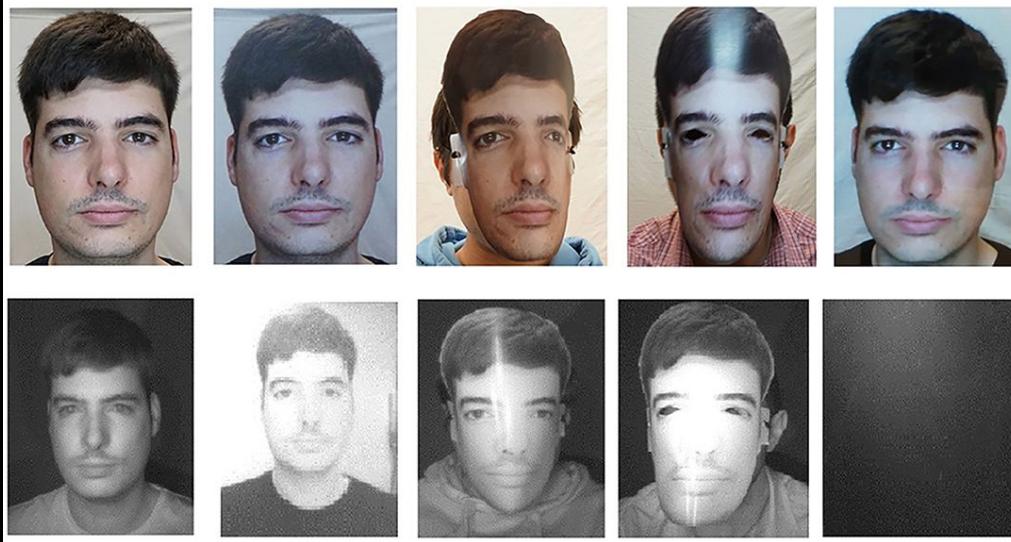
(b) Morph

(c) Subject 2

DETECCIÓN DE ATAQUES DE PRESENTACIÓN EN SISTEMAS DE RECONOCIMIENTO FACIAL Y HUELLAS DACTILARES

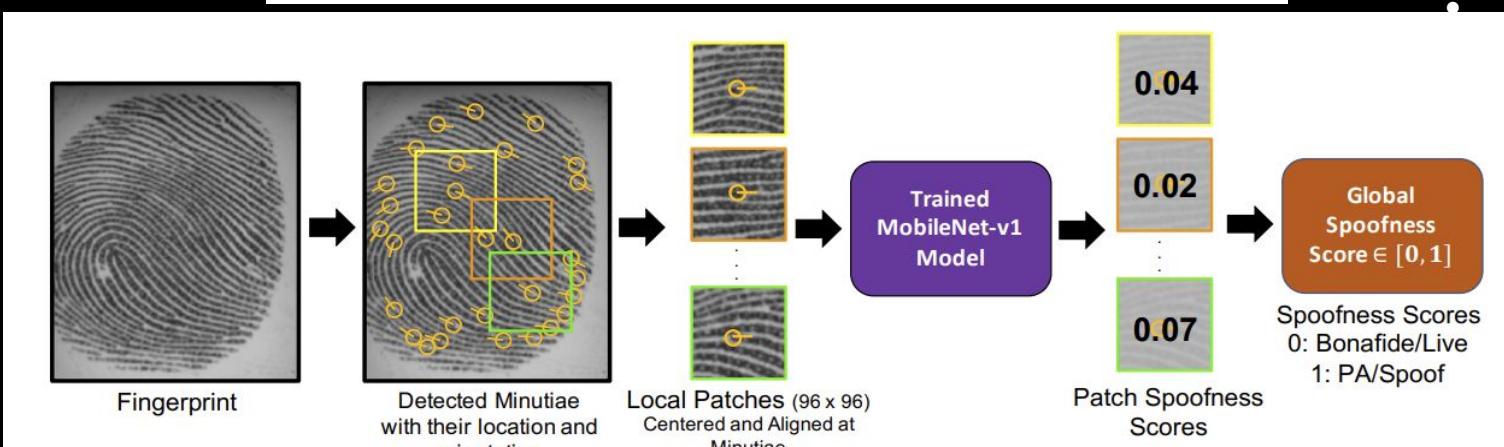
RECONOCIMIENTO FACIAL:

- Parpadeo de ojos
- Desafíos de movimiento
- Análisis de textura
- Análisis de frecuencia
- Análisis de calidad de imagen
- Análisis térmico
- Flash activo



HUELLAS DACTILARES:

- Grado de nitidez
- Niveles de color y luminancia
- Entropía
- Distorsiones estructurales
- Artefactos locales
- Grado de absorción de luz
- Elasticidad del material
- Contenido de humedad

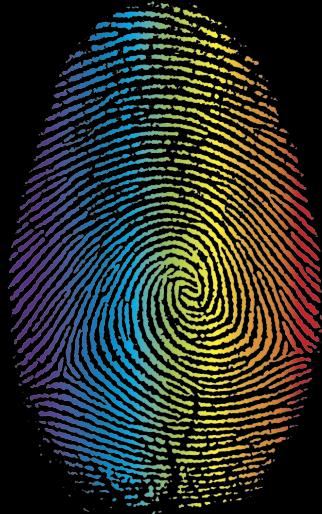


MATERIALES DE REFERENCIA Y LECTURAS RECOMENDADAS SOBRE ATAQUES A SISTEMAS BIOMÉTRICOS

- <https://blog.talosintelligence.com/2020/04/fingerprint-research.html>
- <https://msutoday.msu.edu/news/2017/real-or-fake-creating-fingers-to-protect-identities/>
- http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerpri nt_MSU-CSE-16-2.pdf
- Chugh, Tarang & Jain, Anil. (2018). Fingerprint Presentation Attack Detection: Generalization and Efficiency.
- Pakutharivu, P. & Srinath, M.V.. (2017). Analysis of Fingerprint Image Enhancement Using Gabor Filtering With Different Orientation Field Values. Indonesian Journal of Electrical Engineering and Computer Science. 5. 427-432. 10.11591/ijeeecs.v5.i2.pp427-432.
- Galbally, Javier & Marcel, Sébastien & Fierrez, Julian. (2014). Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition. IEEE Trans. on Image Processing. 23. 710-724. 10.1109/TIP.2013.2292332.
- Wiehe, Anders & Org, Anders@wiehe & Søndrol, Torkjel. (2005). Attacking Fingerprint Sensors.
- Costa-Pazo, Artur & Bhattacharjee, Sushil & Vazquez-Fernandez, Esteban & Marcel, Sébastien. (2016). The Replay-Mobile Face Presentation-Attack Database. 10.1109/BIOSIG.2016.7736936.
- Erdoganmus, Nesli & Marcel, Sébastien. (2014). Spoofing Face Recognition With 3D Masks. Information Forensics and Security, IEEE Transactions on. 9. 1084-1097. 10.1109/TIFS.2014.2322255.
- Bhattacharjee, Sushil & Marcel, Sébastien. (2017). What You Can't See Can Help You - Extended-Range Imaging for 3D-Mask Presentation Attack Detection. 1-7. 10.23919/BIOSIG.2017.8053524.

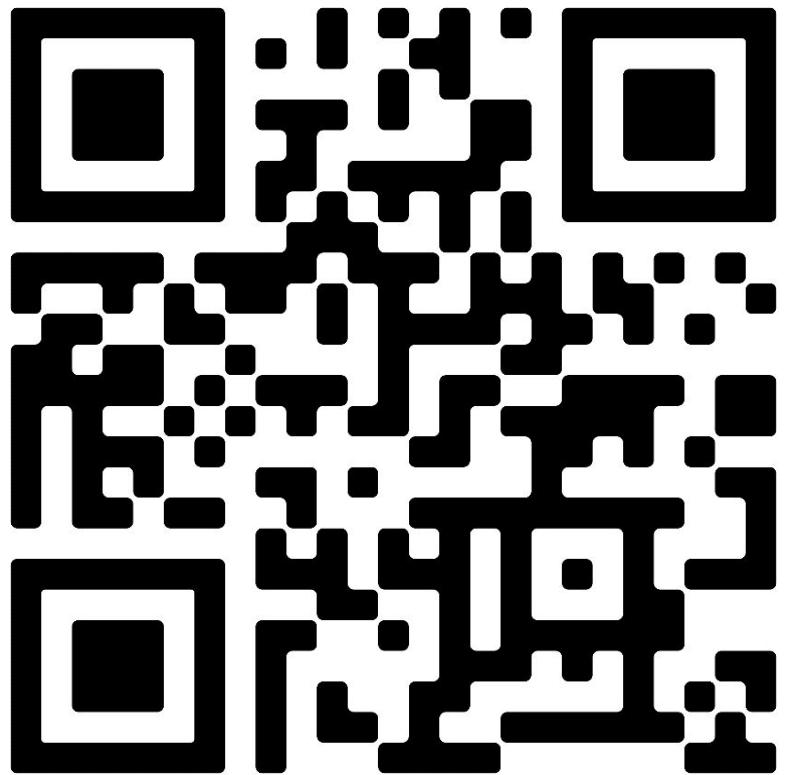
GRACIAS DRAGONJAR!

**Y A TODAS MIS COMPAÑERAS DE TRABAJO Y AMIGAS QUE ME
AYUDARON CON ESTE RESEARCH Y ME PRESTARON SUS DISPOSITIVOS
PARA PROBAR XD @laspibasdeinfosec**



Yamila Levalle @ylevalle





qrco.de/preguntar

SI TIENES PREGUNTAS
DURANTE LA CHARLA
ENTRA AL ENLACE DEL
CÓDIGO QR E INGRESA
ESTE NÚMERO

#22617

