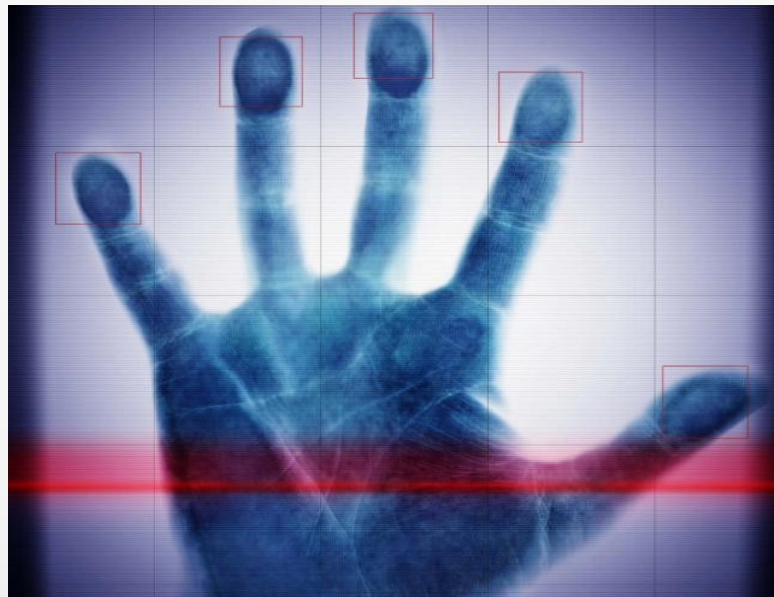


Jugando con sistemas biométricos



¿Quién soy?

ReD

Especialista en seguridad
Cofundador de M4H
Cofundador de Hacklabs
Defensor de la privacidad



Sistemas Biométricos

- Bio (vida) métrico (medida)
- Características morfológicas únicas y medición..

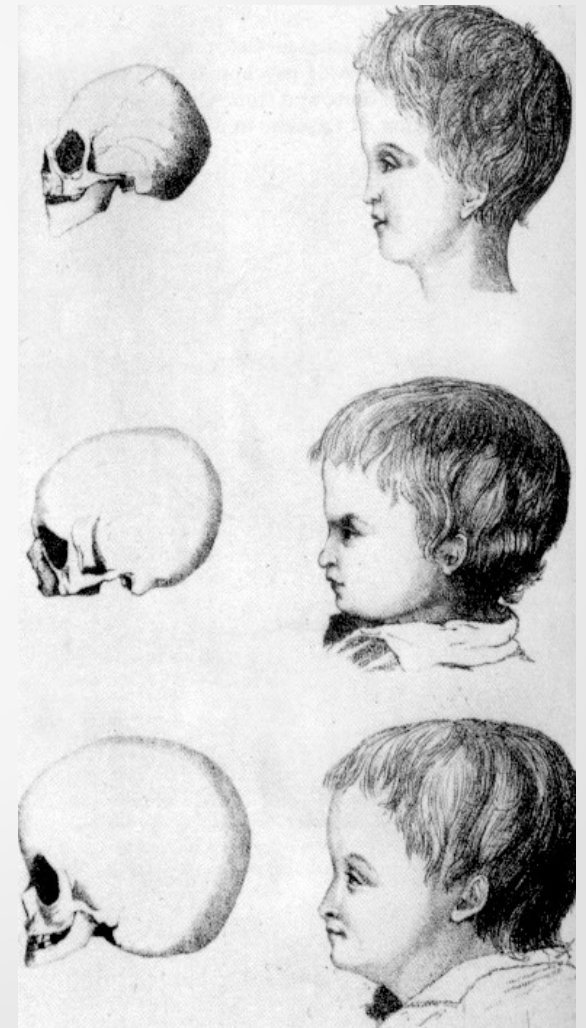


Como el ser

ales

Sistemas Biométricos

- XIX se uso para intentar distinguir a criminales.
- Tamaño de cabeza inteligencia
- Espinas dendríticas



Estándares sistemas biométricos

- **ANSI X.9.84** sistemas financieros
- **PIV-071006** sobretodo huellas dactilares
- **ANSI/INCITS 358** interoperabilidad de sistemas biométricos
- **NISTIR 6529** formato de los datos en las interfaces de salida de sistemas biométricos
- **ISO/IEC 19794-2:2005**; formato de los datos en los sistemas basados en huella dactilar
- **INCITS 378-2009**; intercambio de datos basado en la huella dactilar

Estándares sistemas biométricos

- **Pro**

- Se puede mejorar la implementación.

- **Contra**

- El atacante conoce el funcionamiento.

Conceptos básicos

- **FAR** (False Acceptance Rate)
- FMR (tasa de coincidencia falsa)
- **FRR** (False Rejection Rate)

Vectores de ataque

- Sistema de registro.
- Lectura de parámetros.

Sistema de registro

- Pueden tener:
 - Elementos agrupados.
 - Elementos replicados.



Dispositivo lector

- Reconocer a un individuo y diferenciarlo de los demás



Extractor de características

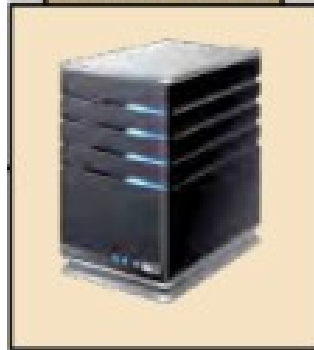
- Extraer la característica en que se basa el sistema bio.
- Detectar ruido en la muestra desecharla si es preciso
- Se lleva a un modelo que buscará la característica y si está ok.



Proceso de **comparación**

- Busca en BD una concordancia con la menos desviación. Se implementa el número de en acceso o no y el numero de reintentos dependiendo de la desviación.

Punto 5



Proceso de
comparación

Base de datos

- Almacenamiento.
- Centralizado, tarjetas de acceso.
- Bases de datos replicadas por velocidad de acceso.



Dispositivo final

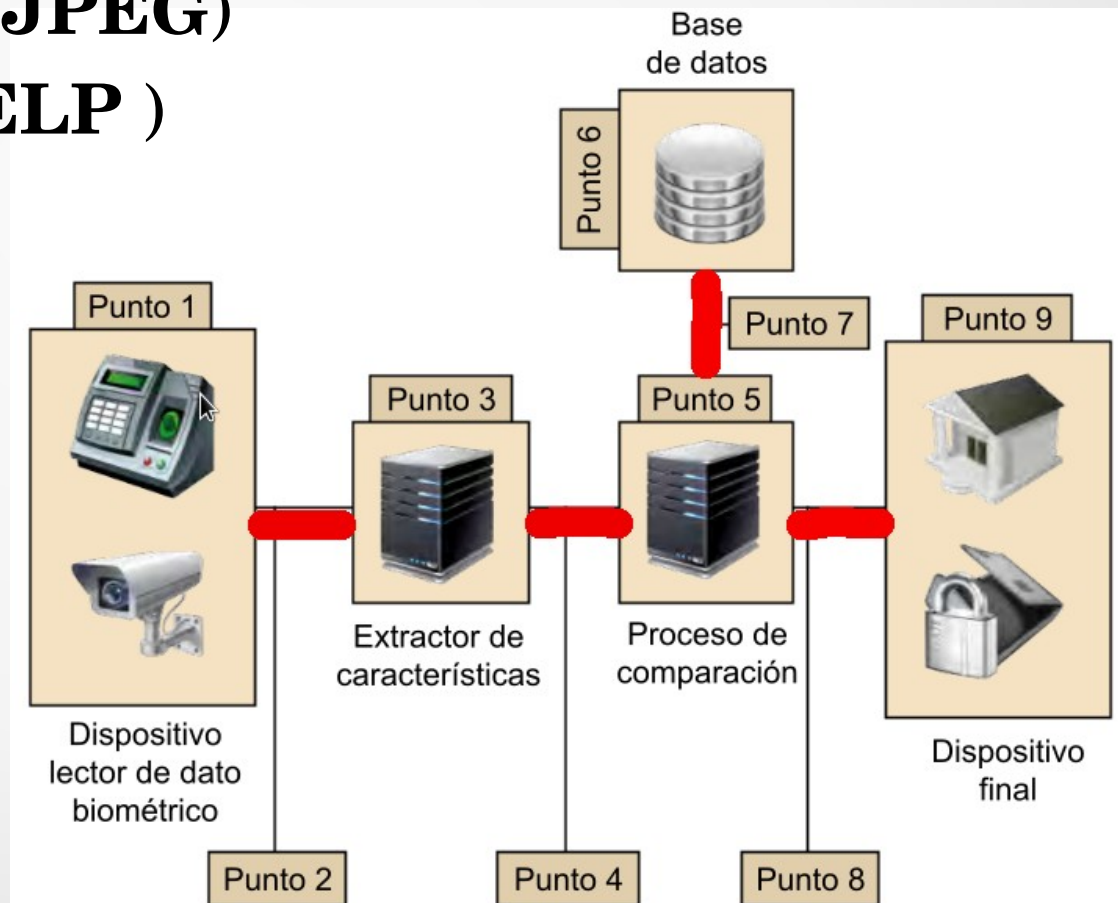
Punto 9



Dispositivo
final

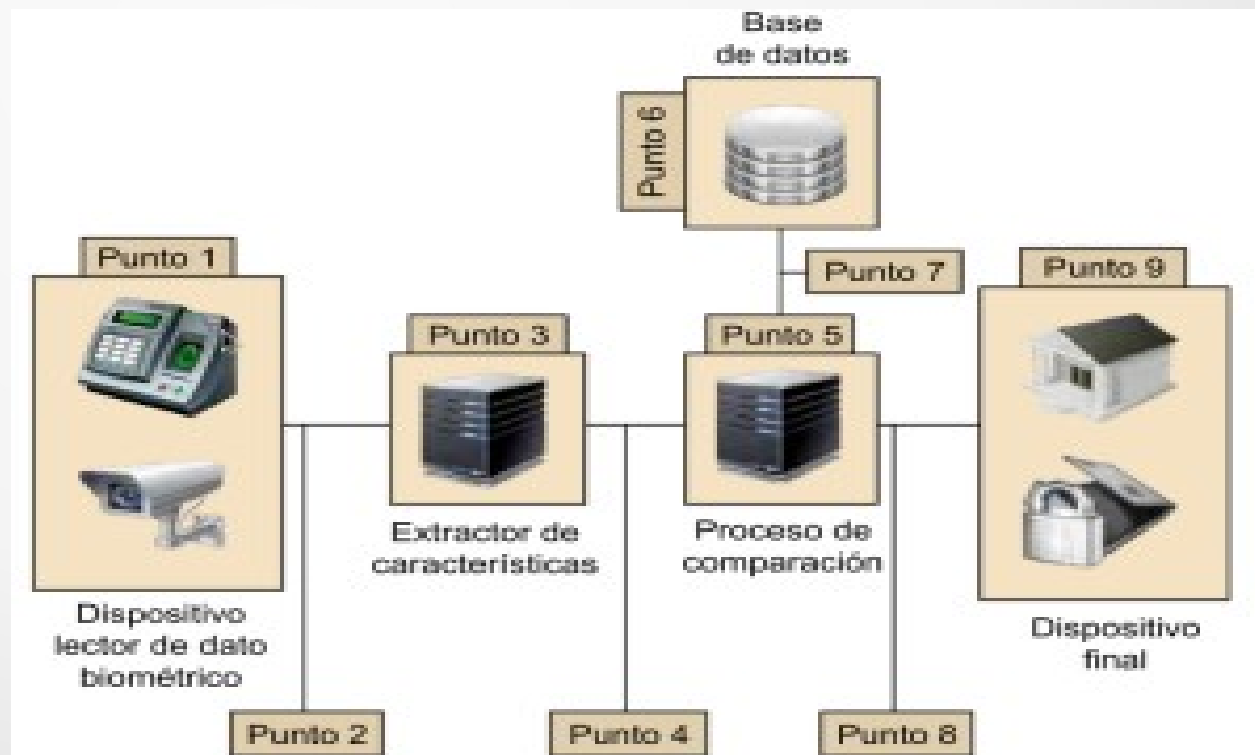
Transmisión

- Se comprime según estándares:
 - Huella digital (**WS1Q**)
 - Imágenes faciales (**JPEG**)
 - Datos de la voz (**CELP**)



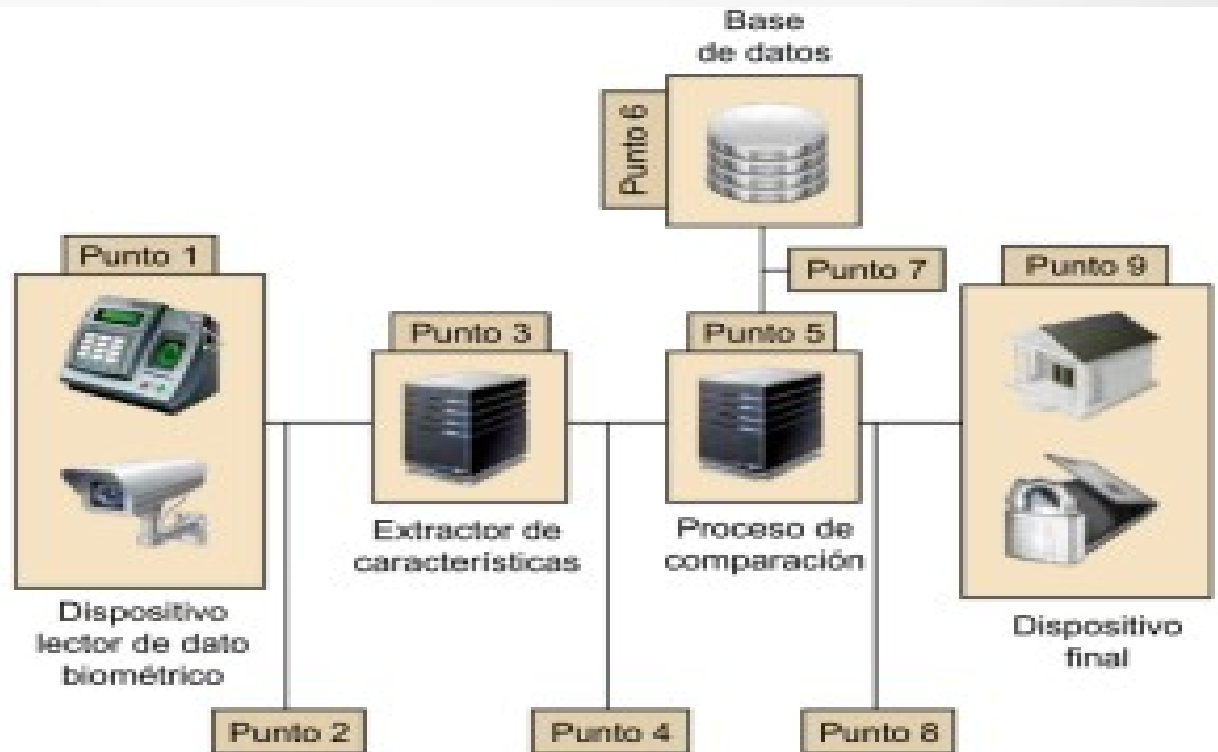
Sistema de registro - ataques

- Acceso a datos temporales del hardware.
- Inyección de paquetes en los puntos 2, 4, 7 y 8
- Generando biomaterial falsa sobre los puntos 1, 3, 5 o 6.



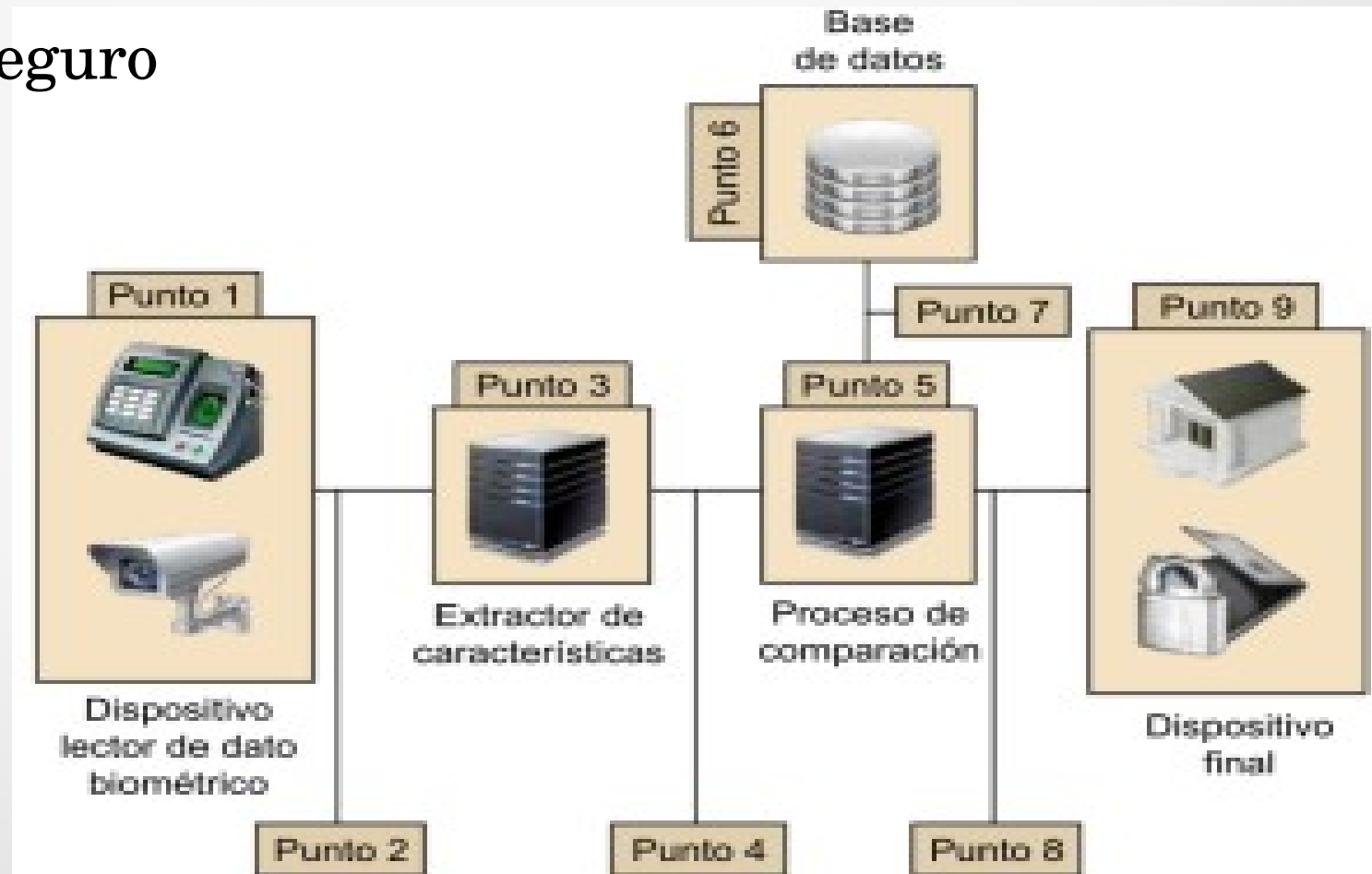
Sistema de registro - ataques

- 2 por repetición
- 4 por modificación
- 7 modificación de permisos usuario.
- 8 falsa respuesta

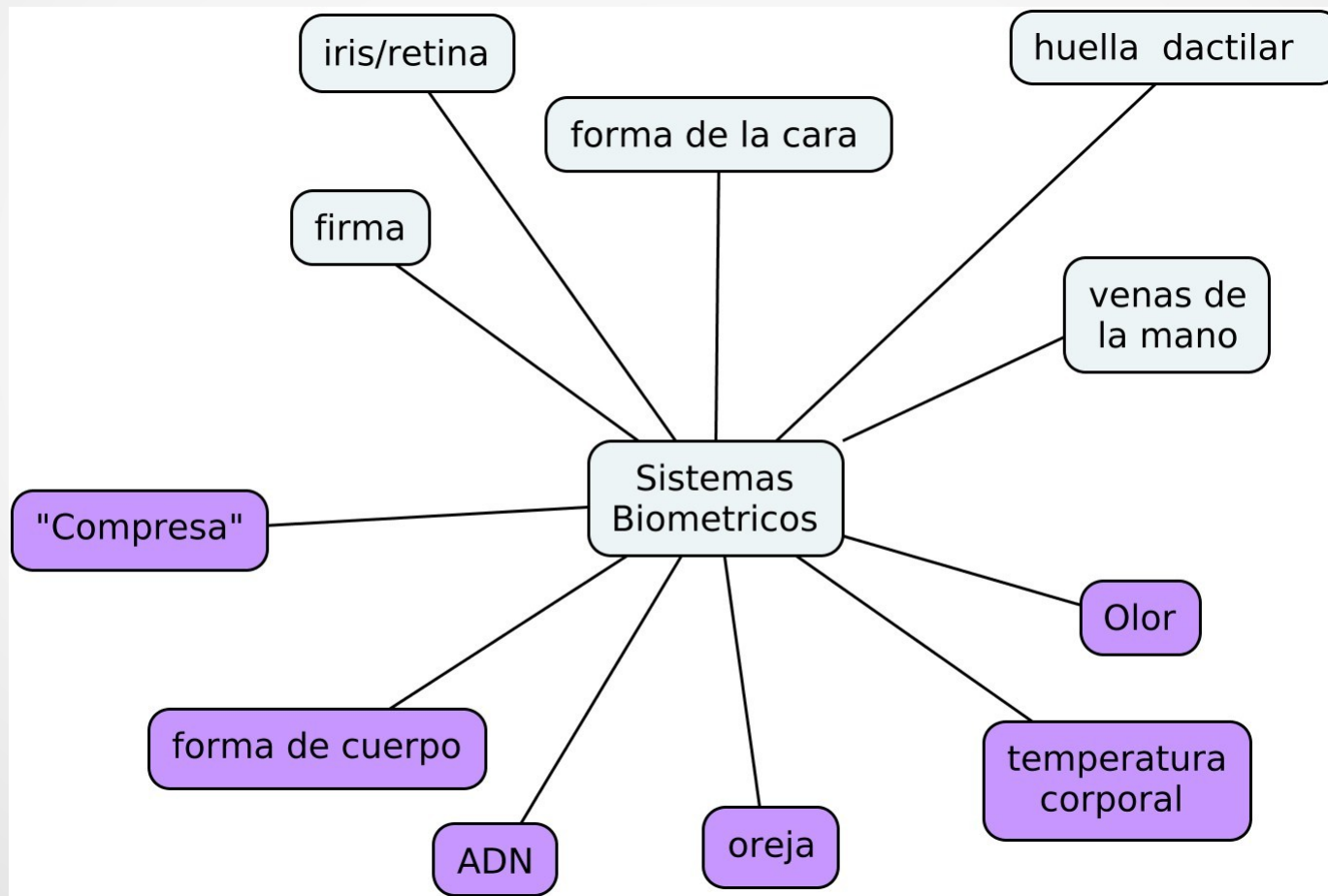


Sistema de registro - Contramedidas

- Detección sniffers
- Encriptación
- Borrado seguro
- IDS
- DMZ

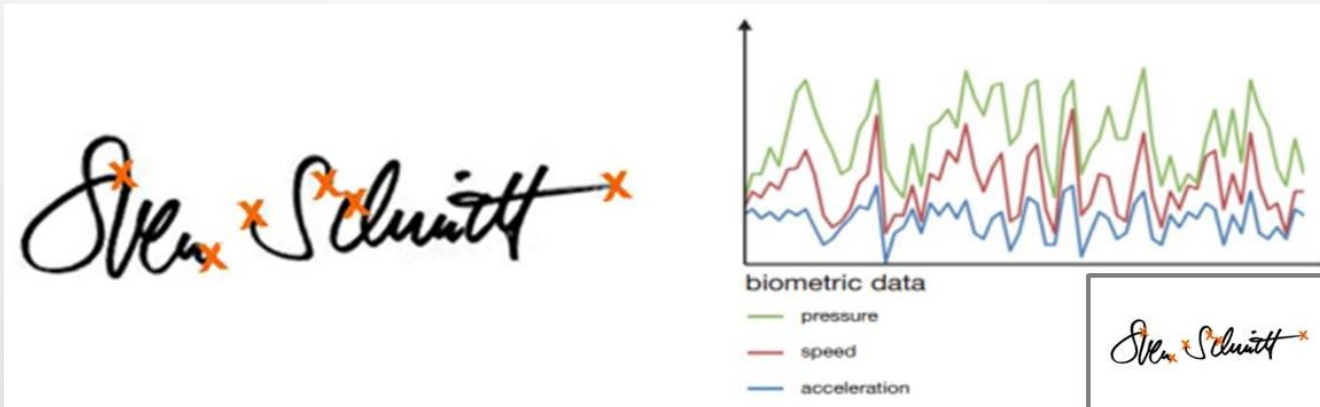


Sistemas Biométricos



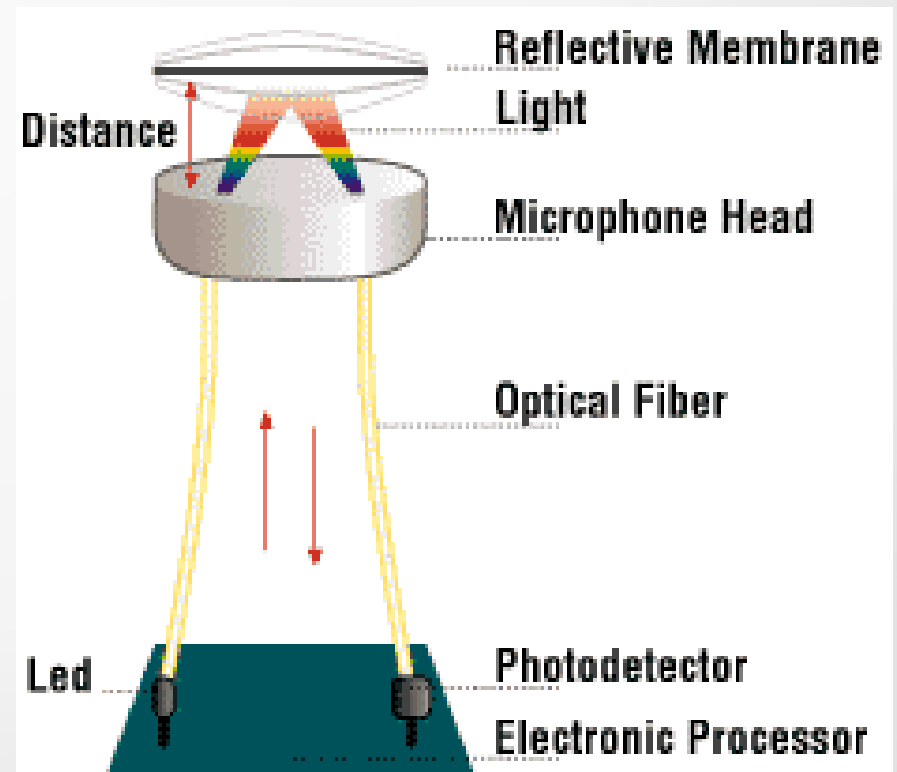
Reconocimiento de la firma

- Usa el patrón caligráfico de firma
 - Presión
 - Velocidad
 - Inclinação
- Barato



Autenticación de la voz

- Requiere micrófono
- Se basa en los lazos armónicos en las vocales
- Micrófonos ópticos unidireccionales



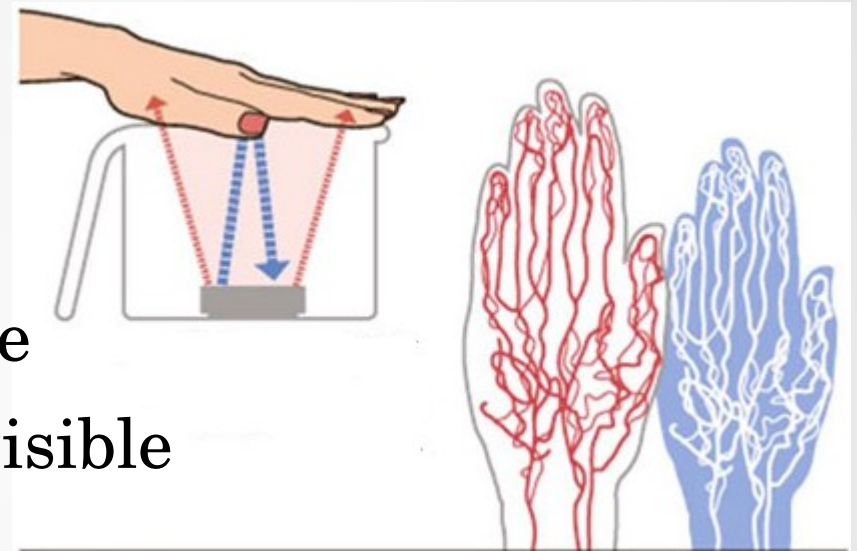
Autenticación de la voz - Ataques

- Grabaciones HD en sistemas de detección de voz



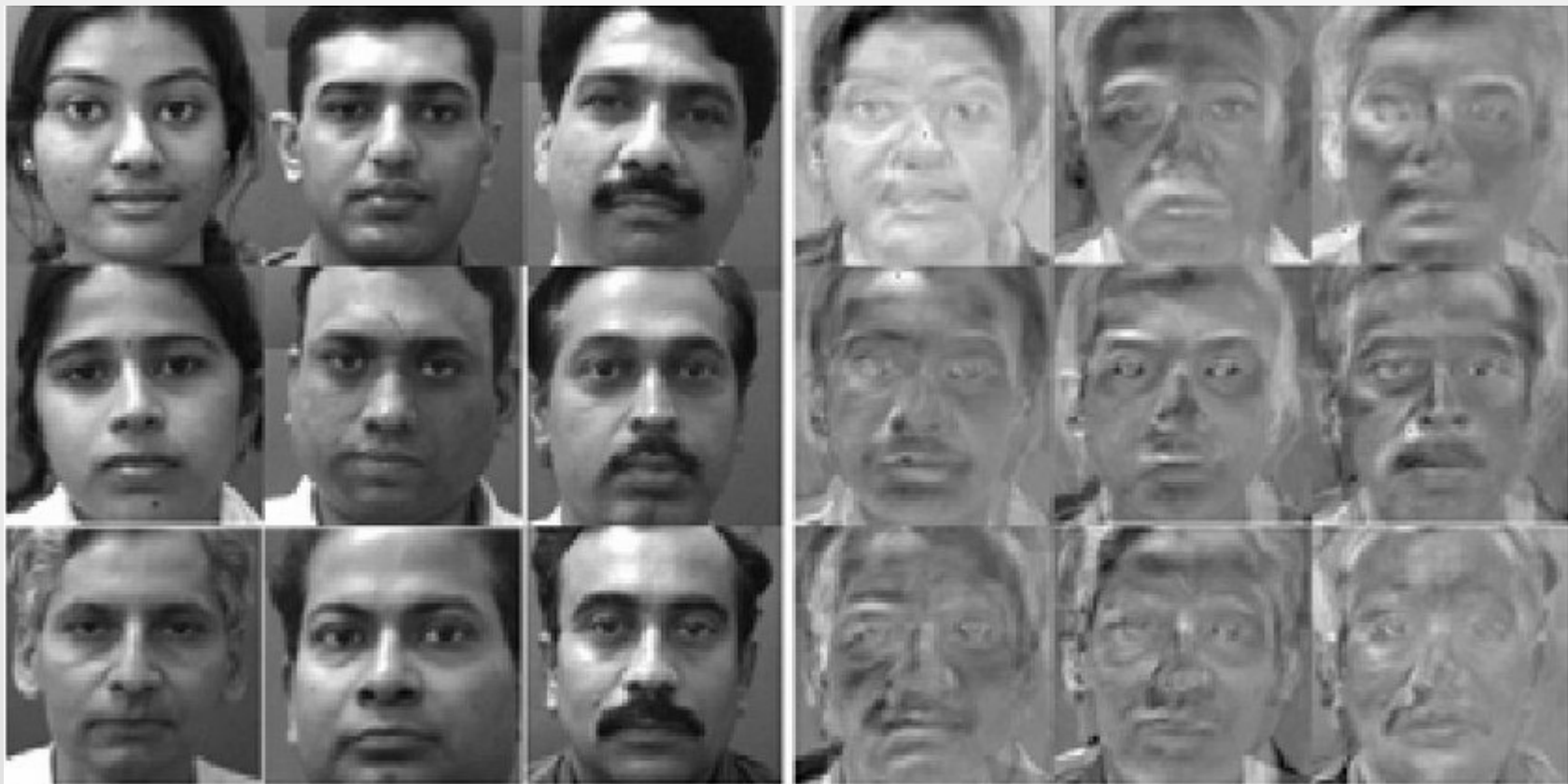
Biometría Vascular

- Usa haces infrarrojos:
 - NIR - Near Infrared
 - FIR – FarInfrared
- Cualidades férricas de la sangre
- Cámara CCD con filtro de luz visible



Reconocimiento facial

- Requiere cámara
- Se basa en **Eigenface (eigenvectors)** y **Fisherfaces**



Reconocimiento facial - **contras**

- Usar sudaderas con capucha
- Uso de maquillaje
- Fotografías originales
- Fotografías con pequeñas modificaciones

Reconocimiento facial - Contra medidas

- Reflejos de las pupilas (relieve)
- Variando plano de enfoque en lente de la cámara



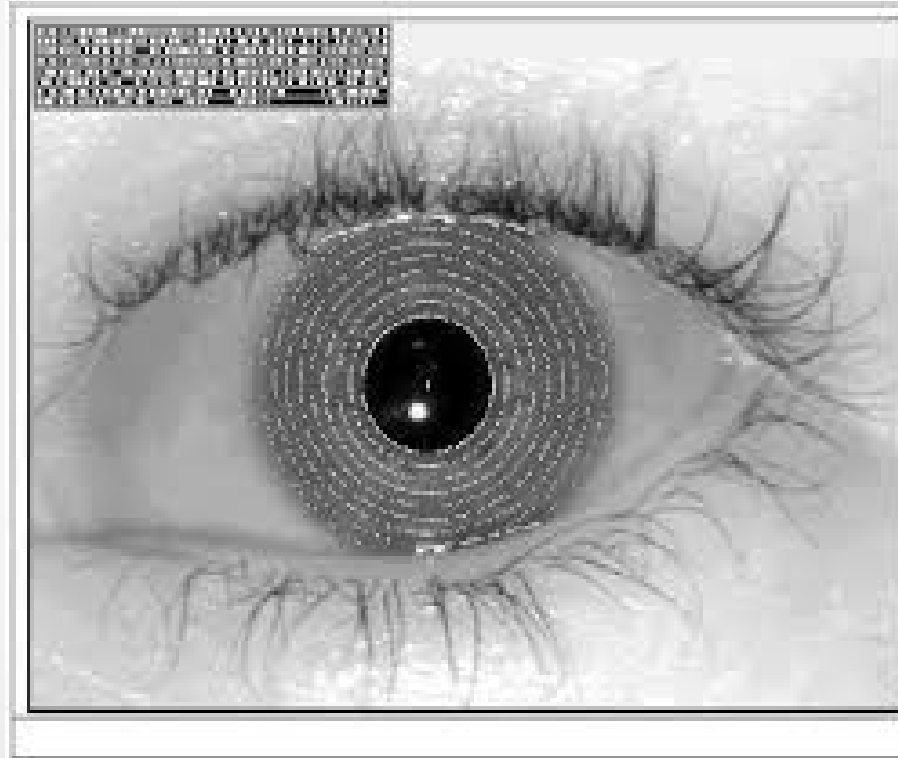
Reconocimiento facial - ataques

- Fotos con agujeros para los ojos.
- Vídeo HD resaltando los factores de detección
- Contra, acercar y alejar la imagen
- Simular de movimiento de pestañas, boca



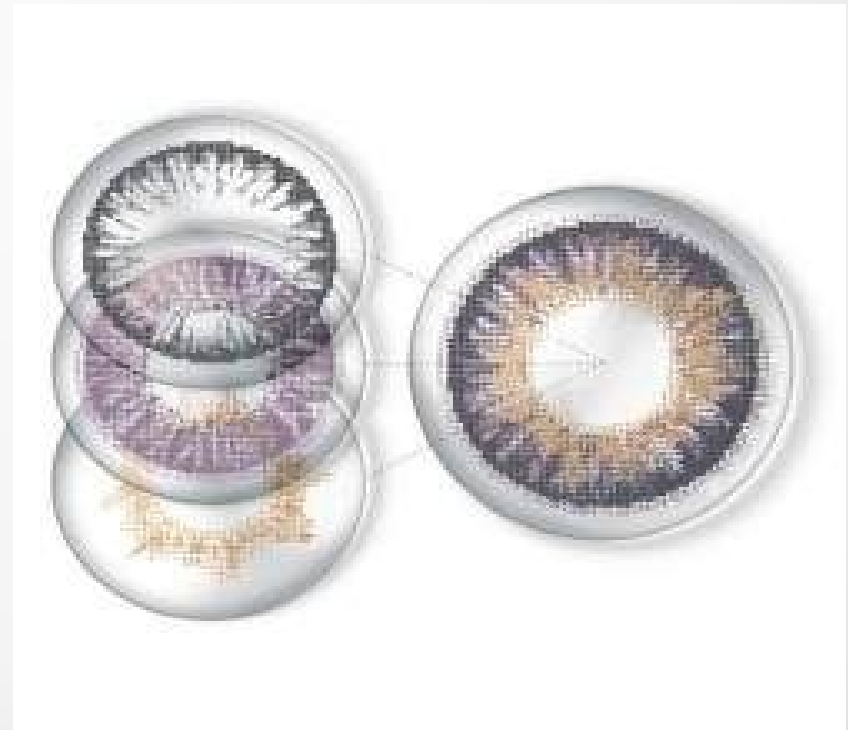
Reconocimiento de iris/retina

- Requiere cámara CCD



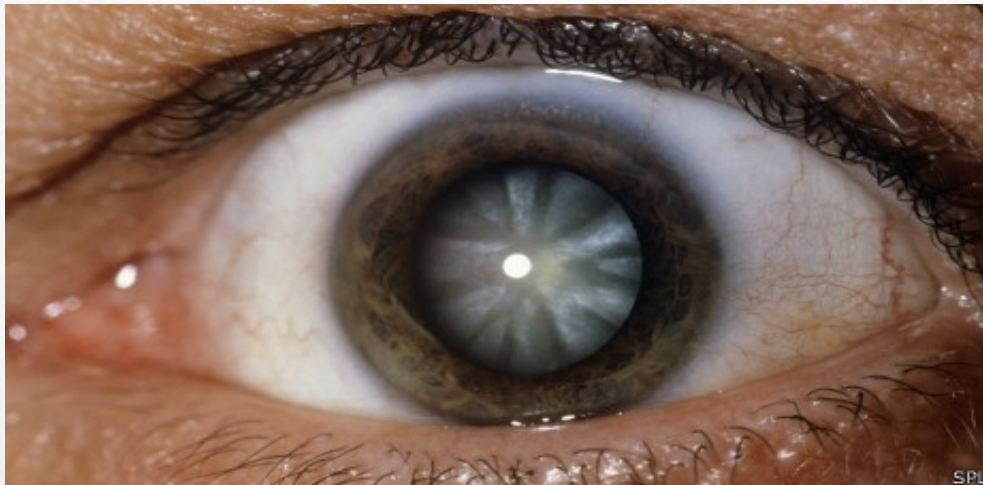
Reconocimiento iris/retina - ataque

- Lentes de contacto impresas.
- Impreso en papel mate.



Reconocimiento iris/retina - Contra medidas

- BD patrones lentillas (espectros luminosos)
- Reflexión de la luz.



Huella dactilar

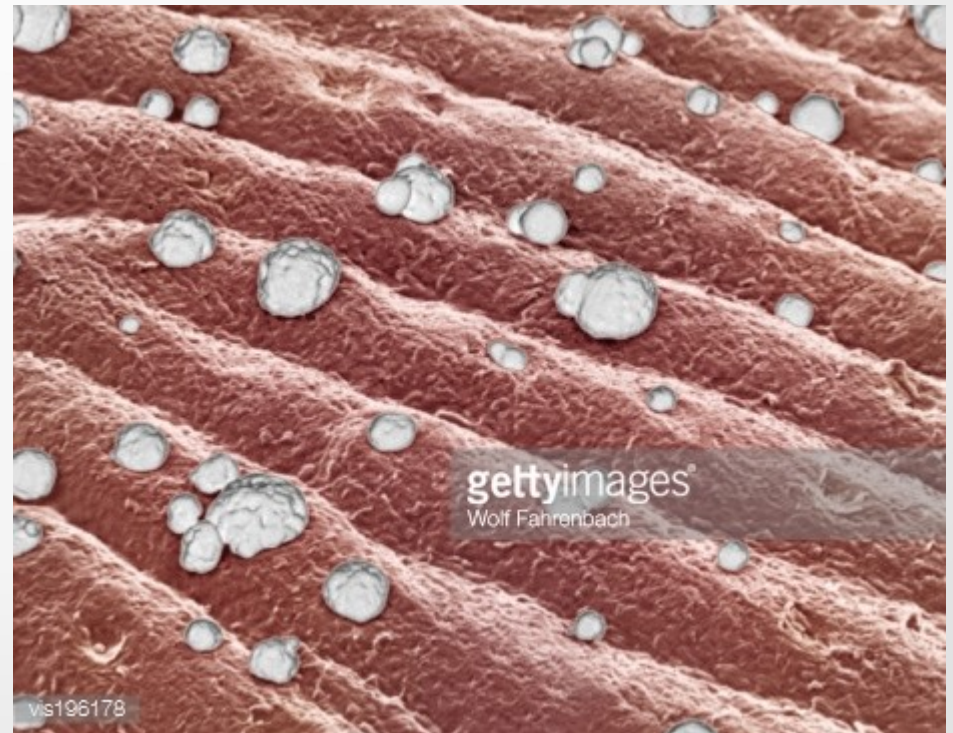
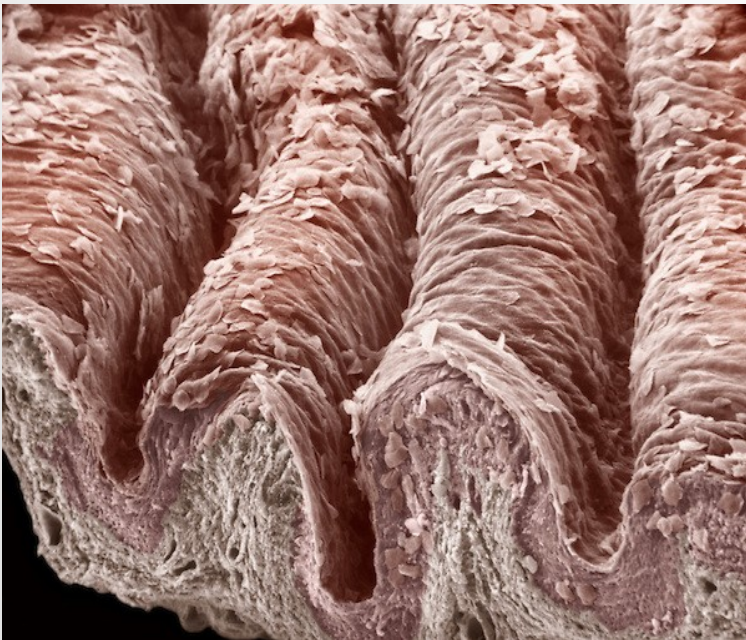


Huella dactilar

- El mas corriente
- Sigue estándares ANSI/NIST, FBI
- Colisiones de 1 cada 64.000 millones
- Usa **Minutiae** para identificar

Huella dactilar

- crestas papilares (salientes)
- Valles (surcos interpapilares)
- La grasa **produce facsímil** o negativo de la huella



Huella dactilar - Clasificación

- Según el patrón de las líneas:
 - Arco
 - Lazo
 - Espiral
- Cada dedo presenta al menos una de estas características.



ARCO



LAZO

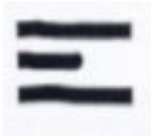


ESPIRAL
o
CIRCULAR



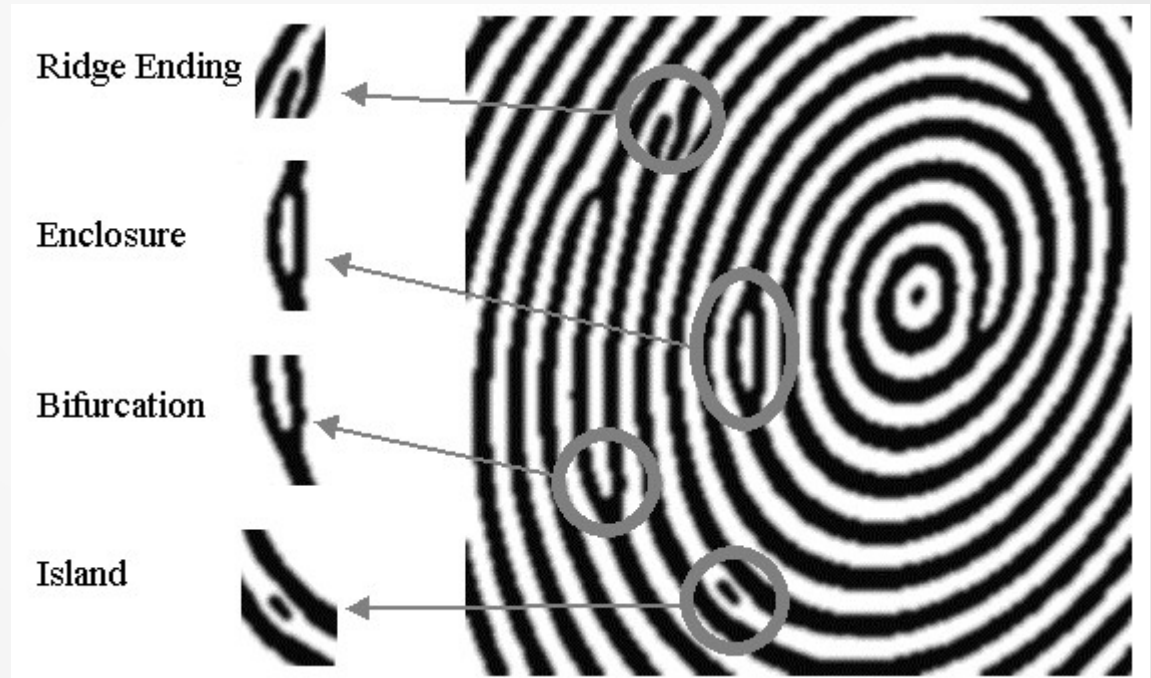
Puntos de Minutiae

- Puntos de corte de las líneas
- Más de **100** por huella
- Los mas usados *

Minutiae	Example	Minutiae	Example
<u>ridge ending</u>		<u>bridge</u>	
<u>bifurcation</u>		double bifurcation	
<u>dot</u>		trifurcation	
island (short ridge)			
<u>lake (enclosure)</u>		ridge crossing	
<u>hook (spur)</u>			

Puntos de Minutiae - Ejemplo

- Se guarda:
 - Punto
 - Dirección
 - Coordenada x
 - Coordenada y
 - Tipo



Procesado de puntos Minutiae



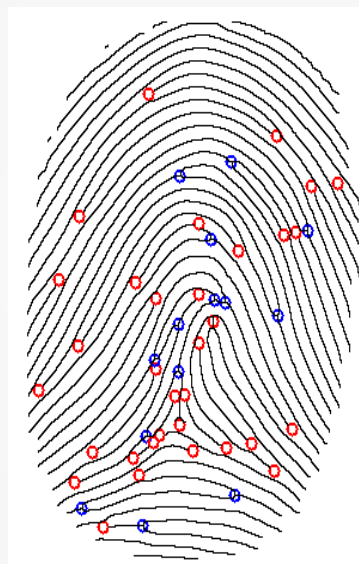
binarization of minutiae extraction

Procesado de puntos Minutiae



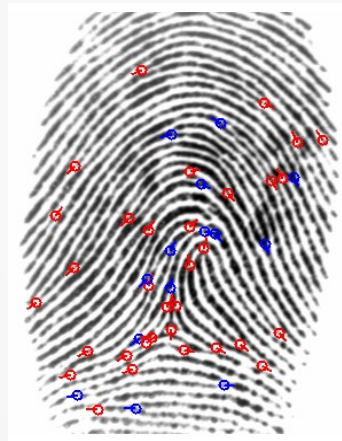
thinning

Procesado de puntos Minutiae



minutiae detection

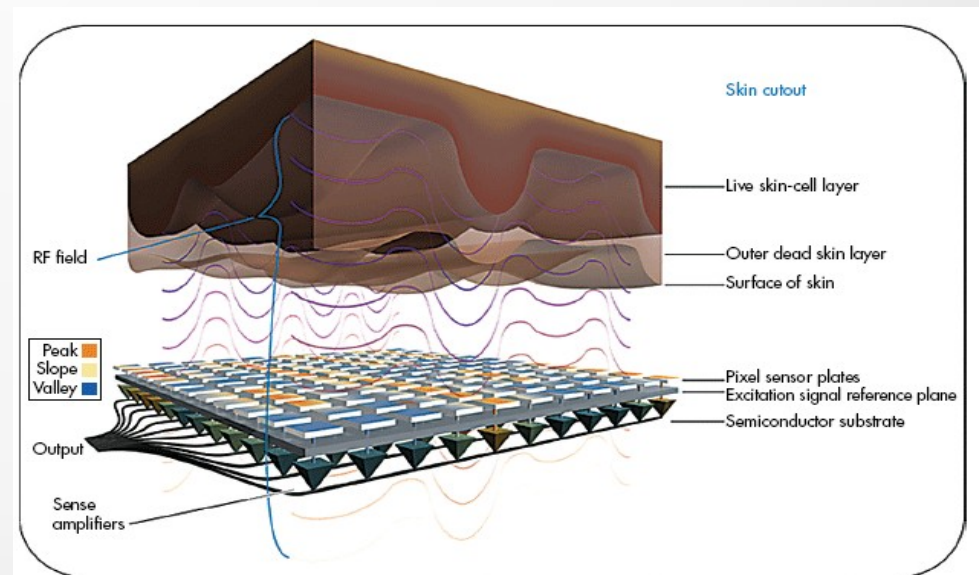
Procesado de puntos Minutiae



Result

Sensores **E-Field** - De Campo Eléctrico

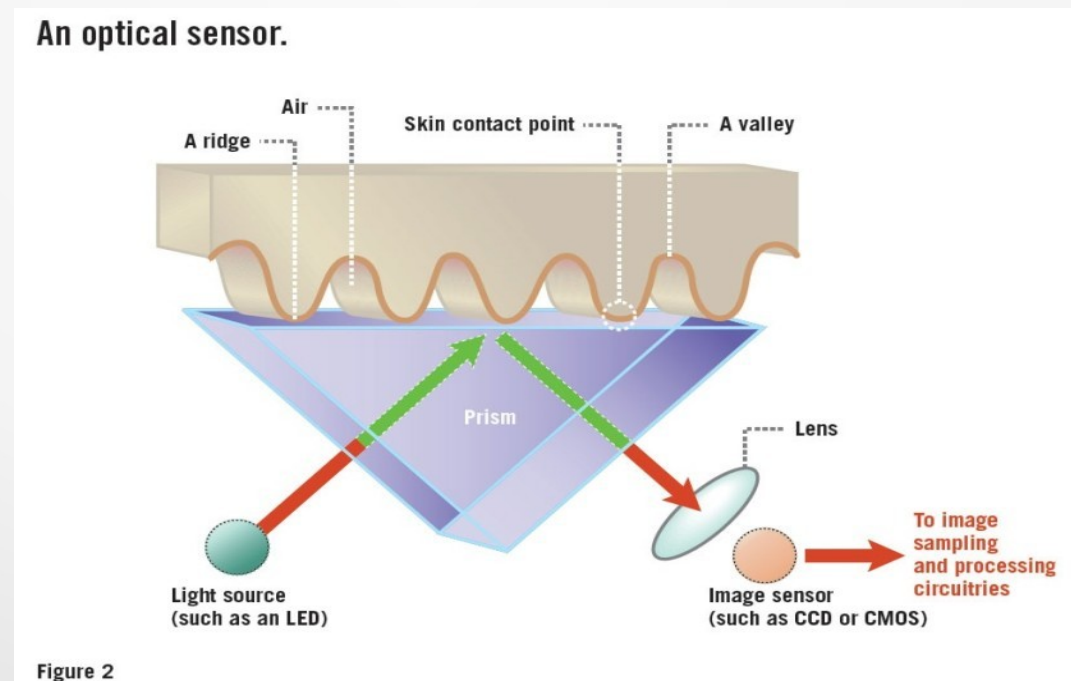
- Integrado de silicio
- Resolución típica de 500 dpi (transductores)
- Se reduce con crestas
- Se reduce menos con valles
- Huella en perfecto estado



2. AuthenTec's TruePrint technology reads beyond the surface layer of the skin to the live layer where the true fingerprint resides. Unlike surface-based optical, thermal, and dc capacitive technologies, this sensor can produce accurate images without being affected by dry, worn, callused, oily, or dirty skin.

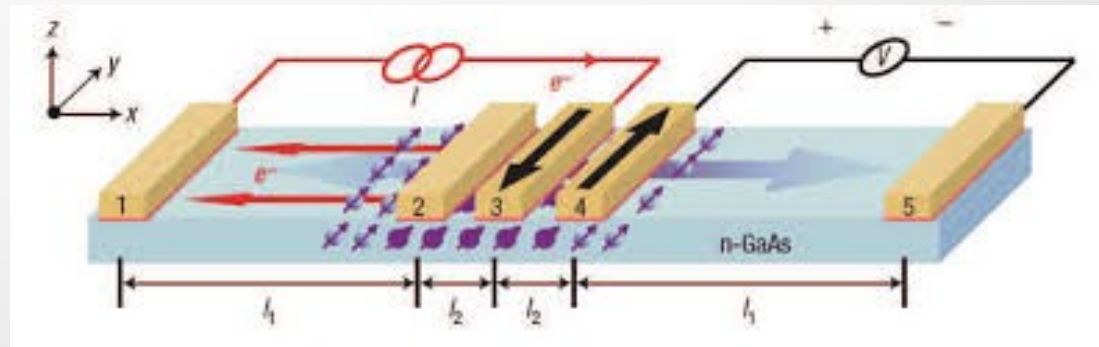
CCD (Dispositivo de Carga Acoplada)

- Cientos de miles de elementos (píxeles)
- Cada píxel se ve estimulado con la luz
- Los píxeles se encuentran dispuestos en forma de malla
- Esta transferencia de señales ocurre 6 por segundo.



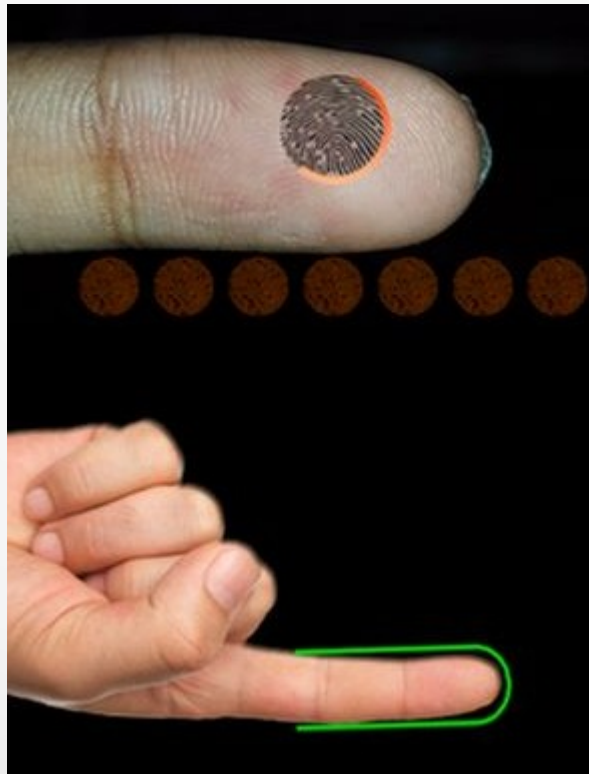
Sensores Termoeléctricos

- Seebeck, Tomas sucesivas (slices)
- 500 puntos por imagen
- 256 escalas de gris
- Limpiado de huellas (arrastras a través del sensor)
- Efecto Peltier y Efecto Thomson
- Contras: Calor ambiente, usuarios con entrenamiento.



Sensores sin contacto

- Como foto
- Algoritmos nuevos para huellas esféricas



Reconocimiento dactilar - ataque

- Huellas de cadáveres
- Huellas de silicona, gelatina, plástico
- Fotocopias de huellas dactilares
- Residuos acumulados

Reconocimiento dactilar - ataque

- Algoritmo hill climbing. contra punto 5.
- No se conoce ninguna información del usuario.
- Generar minutiae suficientes para positivo.
- Atacante conoce el algoritmo de comparación.
- Con minutiae 12 o 15 OK.

Reconocimiento dactilar - ataque

- Pasos:
 1. Se genera minutiae aleatoriamente. posición en la imagen y orientación
 2. Se compara con los del usuario a suplantar
 3. Se calcula positivos
 4. Se generan nuevos minutiae hasta Ok.
- Contra muchos reduce el tiempo.

Reconocimiento dactilar - Contra medidas

- Ocultar la tasa de aceptación.
- Limitar las autenticaciones/día



Reconocimiento dactilar - Contra medidas

- **8-10 grados** por encima del exterior.



Reconocimiento dactilar - Ataque

- **Aliento**



Reconocimiento dactilar - Contra medidas

- **Presión sanguínea**



Reconocimiento dactilar - Ataque

- Materiales **mas finos**



Reconocimiento dactilar - Contra medidas

- **Conductividad** (aprox 200 ohmios mas menos)



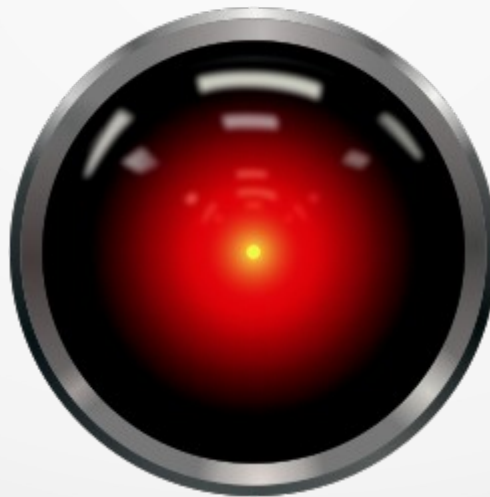
Reconocimiento dactilar - Ataque

- Constante dieléctrica **piel** $\leftrightarrow$ **silicona**



Resumen

Son sistemas montados por humanos



GRACIAS

¿Preguntas?

red@nosoloaulas.com