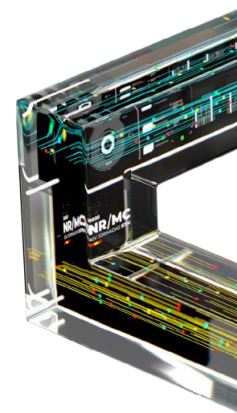


#XIVJORNADASCCNCERT

El Reconocimiento Biométrico: fortalezas y debilidades





Raúl Sánchez Reillo

***Grupo Universitario de Tecnologías
de Identificación (GUTI)***

Universidad Carlos III de Madrid

rsreillo@ing.uc3m.es

Índice de la Presentación

1. ¿Qué es el Reconocimiento Biométrico? ¿Para qué sirve?
2. Estado del Arte Actual
3. Fortalezas y Debilidades
4. Su Uso en Smartphones
 1. Huella Dactilar
 2. Firma Manuscrita
 3. Reconocimiento Facial
5. Conclusiones

¿Qué es el Reconocimiento Biométrico?

- Biometría: Medida de parámetros biológicos
 - Estudios estadísticos de comportamiento de la población
 - Influencias de enfermedades por sectores de población
 - Propagación de insectos en campos de cultivo
 - Etc.
- Reconocimiento Biométrico: Métodos de reconocimiento de sujetos, midiendo parámetros biológicos
 - ¿Qué sujeto?
 - Personas, animales, cosas, etc.
 - ¿Cómo se mide?
 - Por métodos Manuales, por métodos Automáticos
 - ¿Qué parámetros?
 - Físicos, De Comportamiento o Ambos

¿Qué es el Reconocimiento Biométrico?

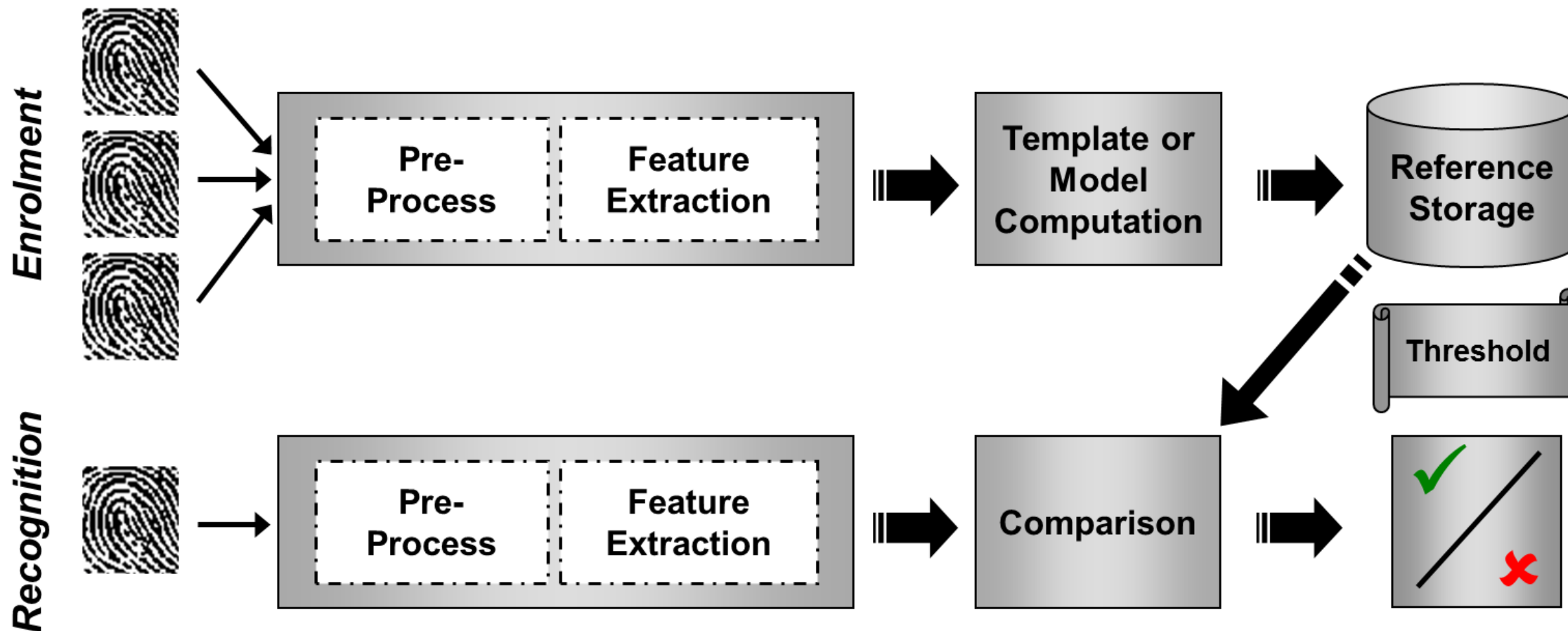
- Múltiples modalidades:
 - Fisiológicas:
 - ADN
 - Facial
 - Huella
 - Iris
 - Vascular
 - ...
 - De Comportamiento:
 - Firma
 - Gait
 - ...
 - Mixtas:
 - Voz



¿Para qué sirve?

- La Biometría intenta automatizar la manera de reconocer el ser humano:
 - En lugares donde no haya posibilidad de tener un agente identificando
 - Para evitar cansancio humano
 - Reduciendo coste en sistemas de identificación
 - No hay que distribuir objetos, documentos, ni claves
- Tarea no trivial:
 - ¿Reconocemos por una sola característica, o por un conjunto de varias?
- Objetivos:
 - ¿Securizar?
 - ¿Ayudar a un operador?
 - ¿Facilitar el proceso de identificación/autenticación?
 - ¿Acercar la tecnología al ser humano?

¿Cómo Funciona el Reconocimiento Biométrico?



Estado del Arte: Huella – Captura



Contactless Fingerprinting Solutions



Mitsubishi



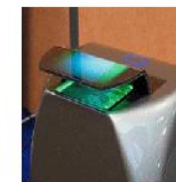
TST



TBS
Single-
Finger



TBS
Ten-
Finger



Sagem
Sécurité



FlashScan3D/
U of Kentucky



UMass
Lowell



GE Global
Research



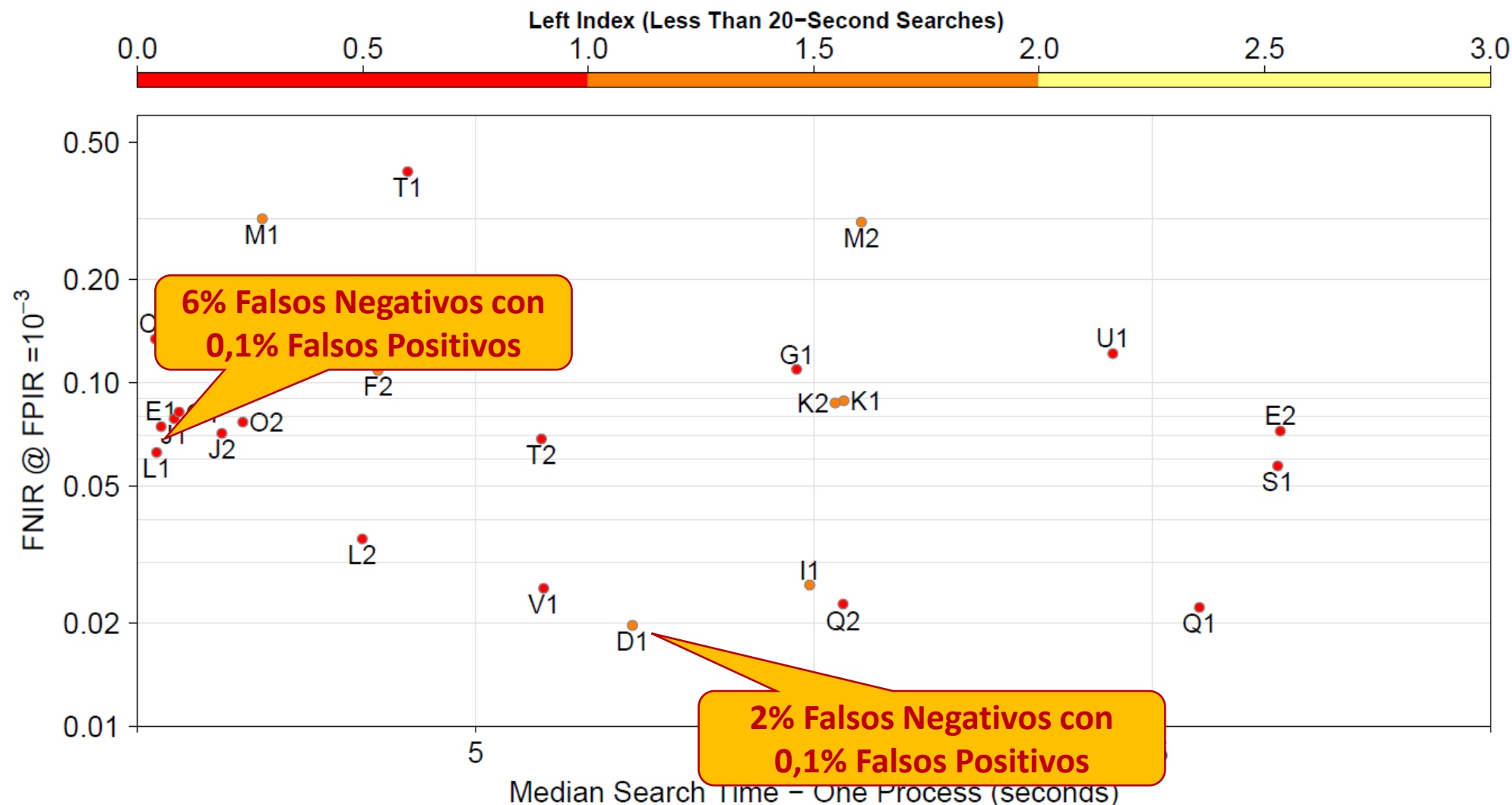
Authenti-Corp/
U of Arizona



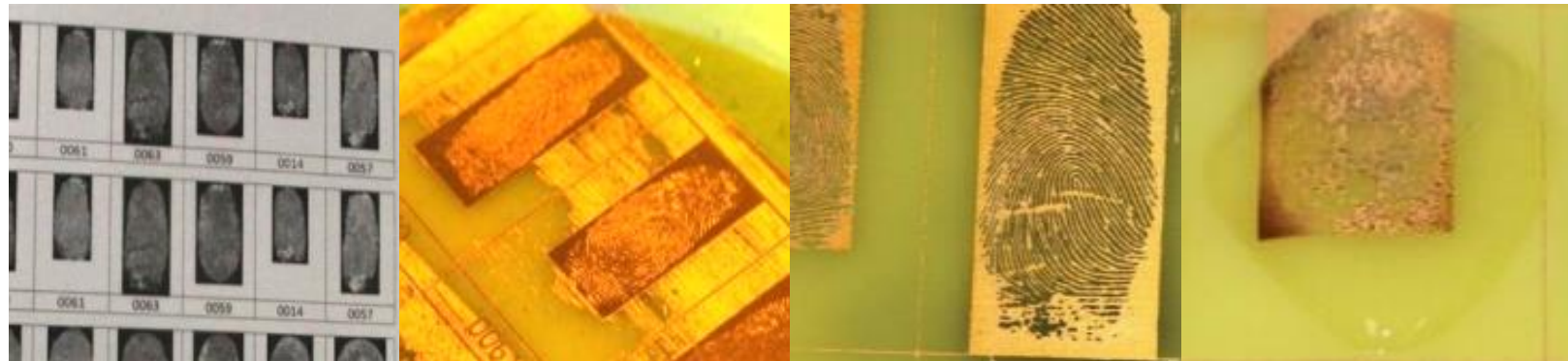
Estado del Arte: Huella – Rendimiento

FpVTE 2012: Identification of a user within a database of 100K users:

<https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf>



Estado del Arte: Huella – Ataques



Estado del Arte: Huella – Ataques



Before

After



Bad quality
mold



Good quality
mold

Each evaluator/attacker gets
different results



Examples



Latex with
graphite

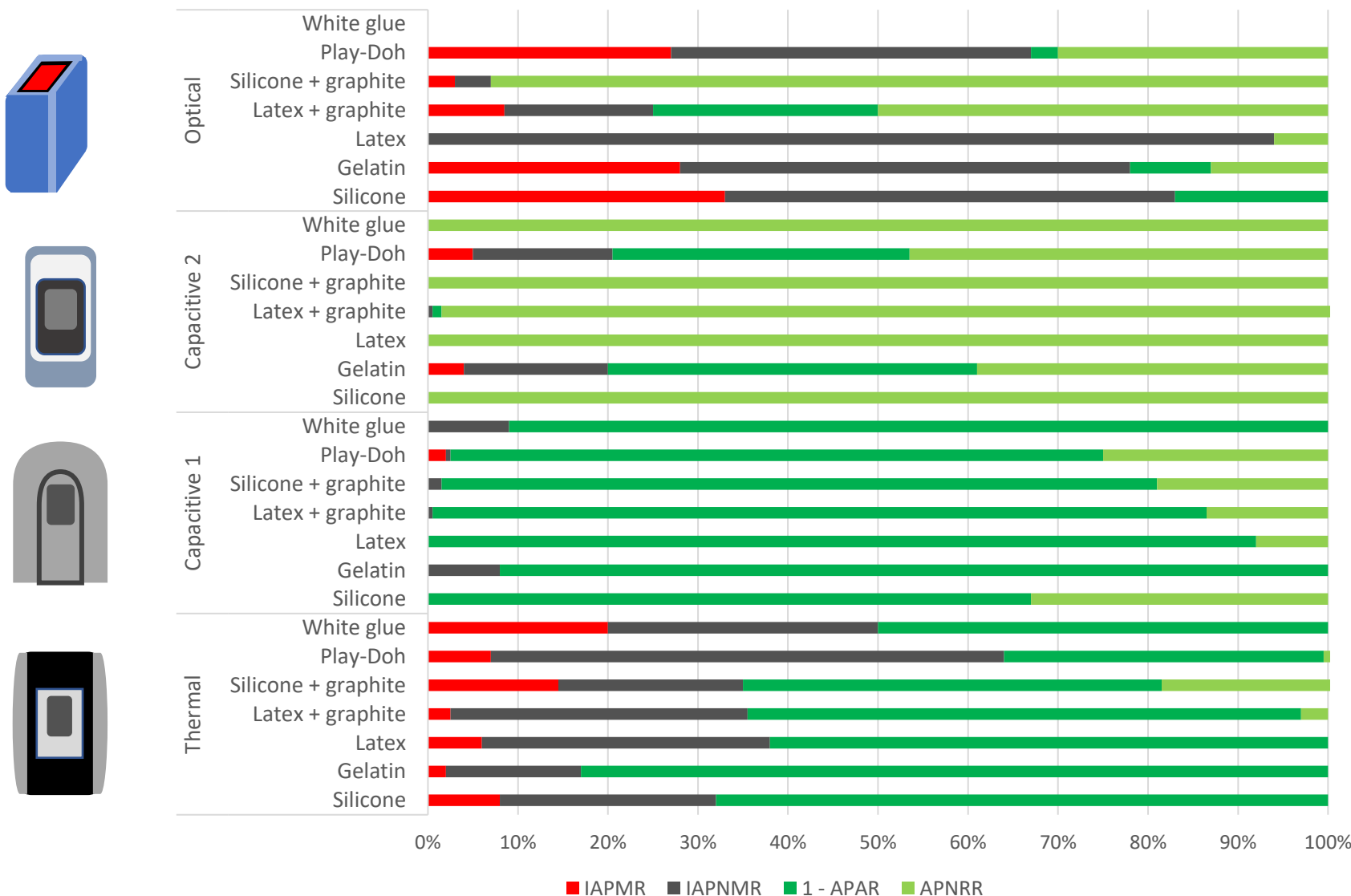


Gelatine



Play-Doh

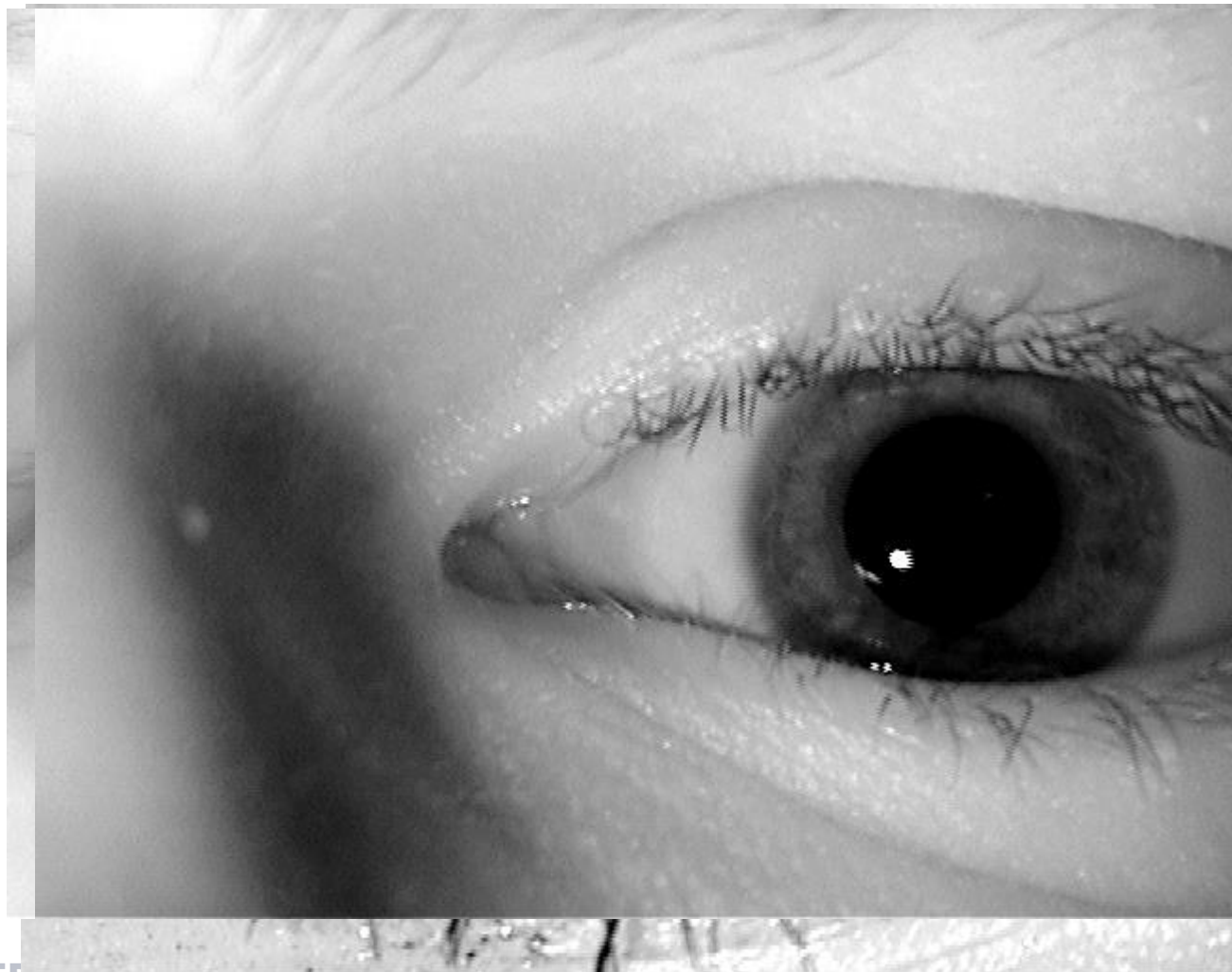
Estado del Arte: Huella – Ataques



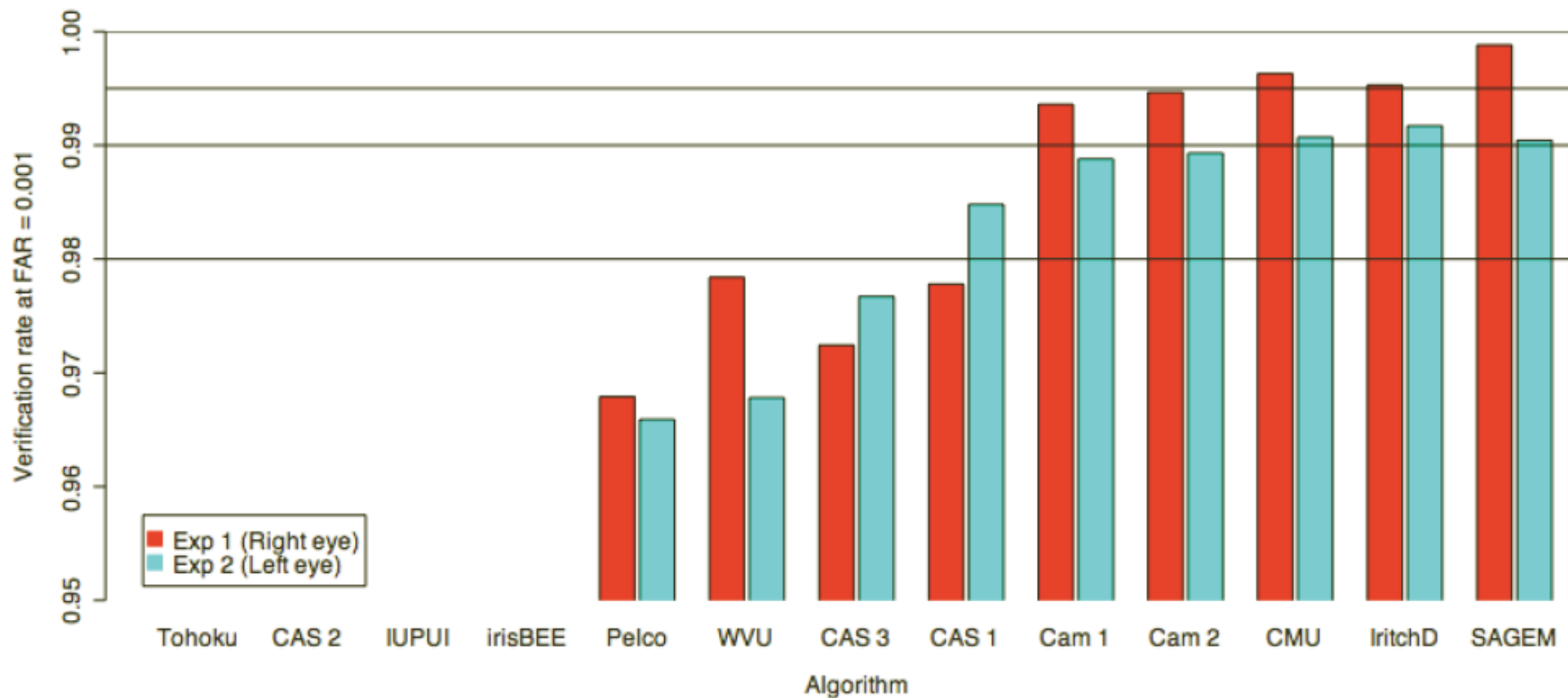
Estado del Arte: Iris – Captura



Estado del Arte: Iris – Rendimiento (ICE 2005)



Estado del Arte: Iris – Rendimiento (ICE 2005)



Estado del Arte: Facial – Captura

- Casi cualquier cámara digital, webcam, cámara de seguridad, móvil, etc.
- La captura se hace típicamente en el rango visible
- Pero si capturaran en NIR podríamos obtener una utilidad adicional:

Standard PiCamera (sensitive to IR and visible spectrum)

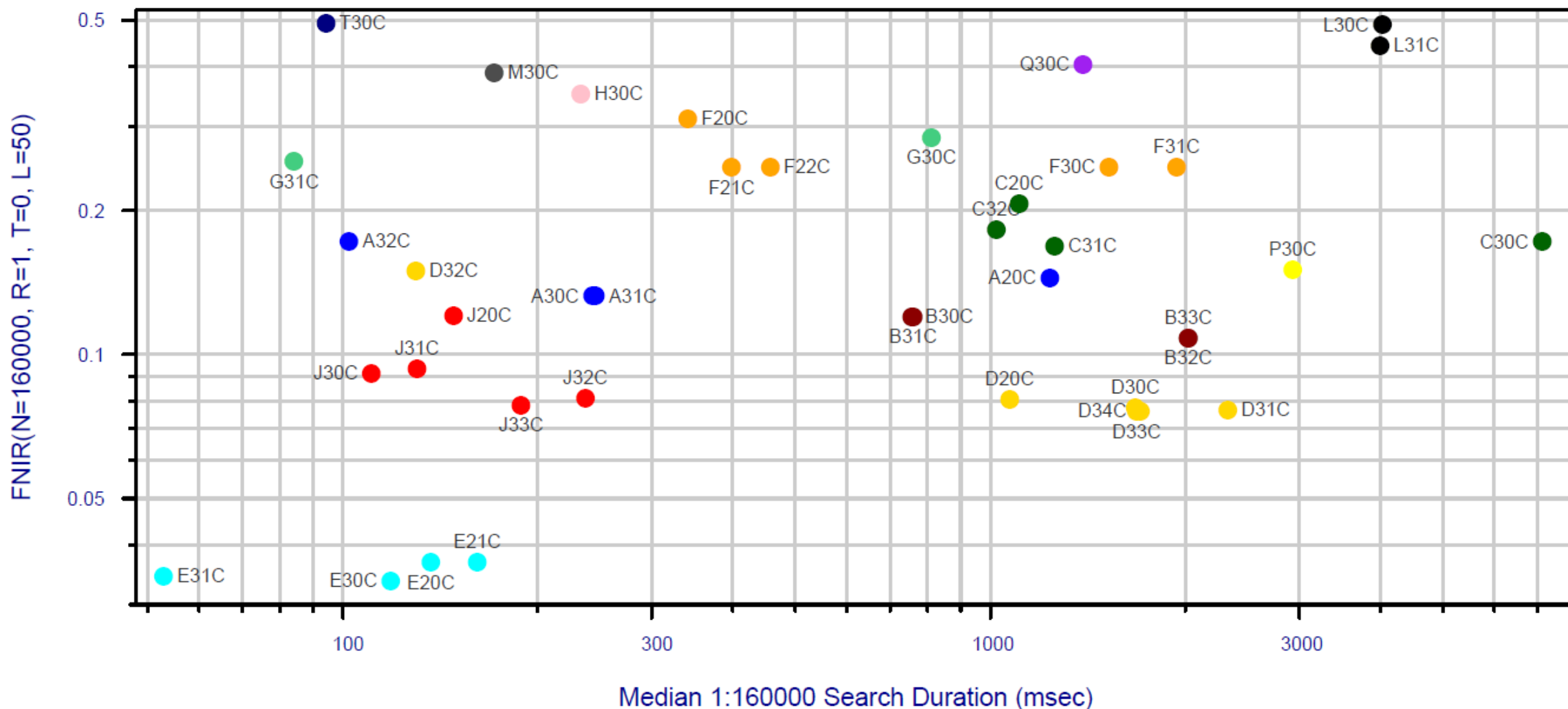


Standard PiCamera with IR-pass filter, and 2x IR LED shining at subject



Estado del Arte: Facial – Rendimiento (FRVT 1:N)

(<https://pages.nist.gov/frvt/html/frvt1N.html>)



Estado del Arte: Facial – Rendimiento: On-Going FRVT 1:1 (<https://pages.nist.gov/frvt/html/frvt11.html>)

Developer	VISA Photos FNMR @ FMR ≤ 0.000001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001 DT ≥ 12 YRS	VISABORDER Photos FNMR @ FMR ≤ 0.000001	BORDER Photos FNMR @ FMR = 0.000001	WILD Photos FNMR @ FMR ≤ 0.00001
visionlabs-009	0.0025 ⁽¹⁾	0.0026 ⁽¹⁾	0.0029 ⁽³⁾	0.0035 ⁽¹⁾	0.0064 ⁽¹⁾	0.0306 ⁽¹³⁾
ntechlab-008	0.0061 ⁽¹⁹⁾	0.0056 ⁽³¹⁾	0.0108 ⁽⁴⁴⁾	0.0042 ⁽²⁾	0.0080 ⁽³⁾	0.0312 ⁽³⁰⁾
deepglint-002	0.0027 ⁽³⁾	0.0032 ⁽⁸⁾	0.0033 ⁽⁴⁾	0.0043 ⁽³⁾	0.0084 ⁽⁴⁾	0.0301 ⁽⁴⁾
vocord-008	0.0038 ⁽⁶⁾	0.0042 ⁽¹⁸⁾	0.0055 ⁽¹⁵⁾	0.0045 ⁽⁴⁾	0.0086 ⁽⁵⁾	0.0310 ⁽²⁴⁾
dahua-005	0.0046 ⁽¹³⁾	0.0035 ⁽¹²⁾	0.0049 ⁽¹³⁾	0.0046 ⁽⁵⁾	0.0076 ⁽²⁾	0.0300 ⁽³⁾
xforwardai-001	0.0034 ⁽⁵⁾	0.0027 ⁽³⁾	0.0028 ⁽²⁾	0.0046 ⁽⁶⁾	0.0088 ⁽⁶⁾	0.0303 ⁽¹⁰⁾
tevian-006	0.0061 ⁽¹⁸⁾	0.0045 ⁽²⁰⁾	0.0066 ⁽²⁰⁾	0.0046 ⁽⁷⁾	0.0091 ⁽⁷⁾	0.0330 ⁽⁴³⁾
cib-001	0.0061 ⁽²⁰⁾	0.0030 ⁽⁶⁾	0.0041 ⁽⁷⁾	0.0048 ⁽⁸⁾	0.0578 ⁽⁷⁶⁾	0.0302 ⁽⁵⁾
cubkee-001	0.0045 ⁽¹¹⁾	0.0031 ⁽⁷⁾	0.0046 ⁽⁹⁾	0.0051 ⁽¹⁰⁾	0.0095 ⁽¹⁰⁾	0.1524 ⁽¹²⁴⁾

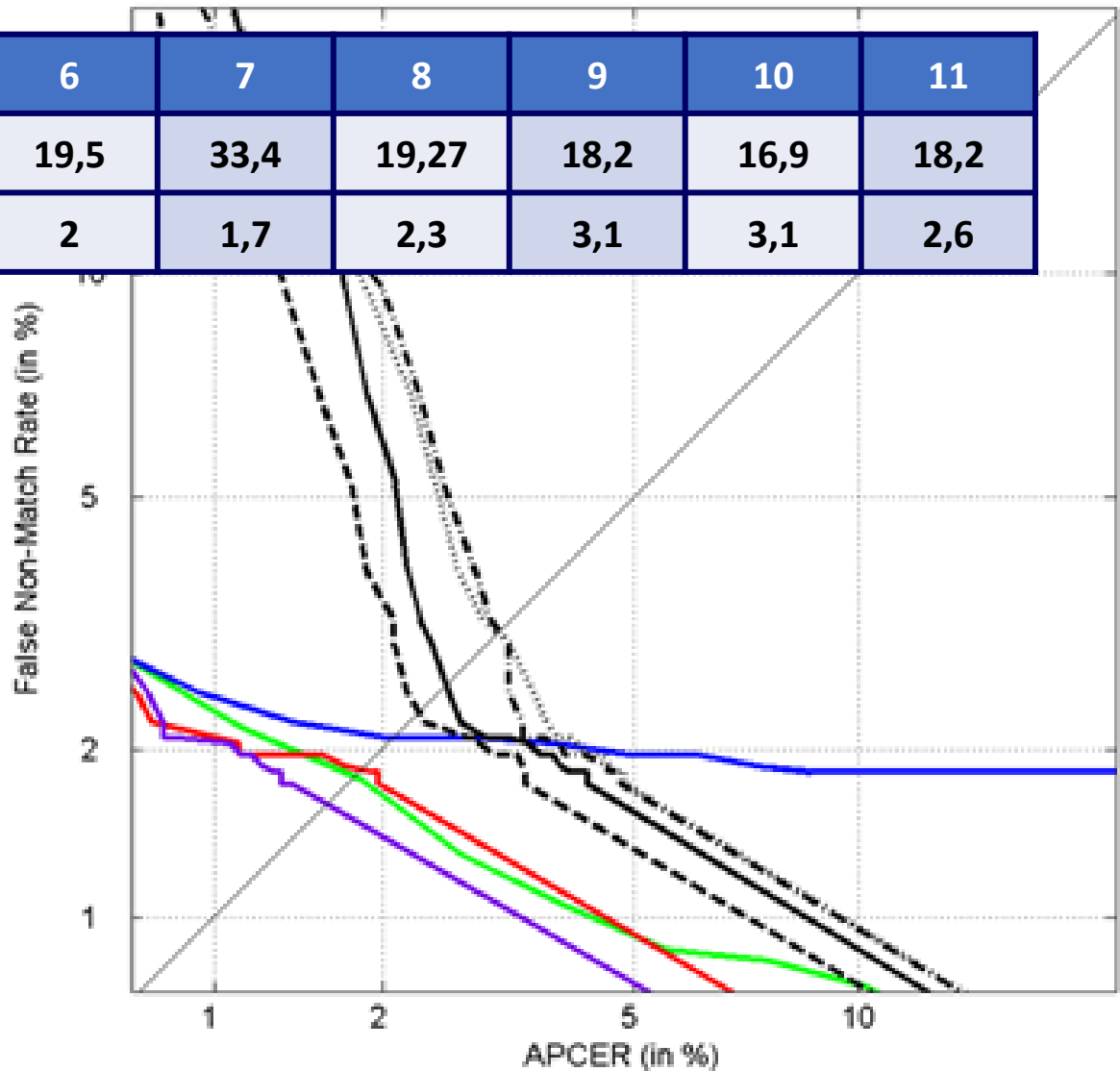
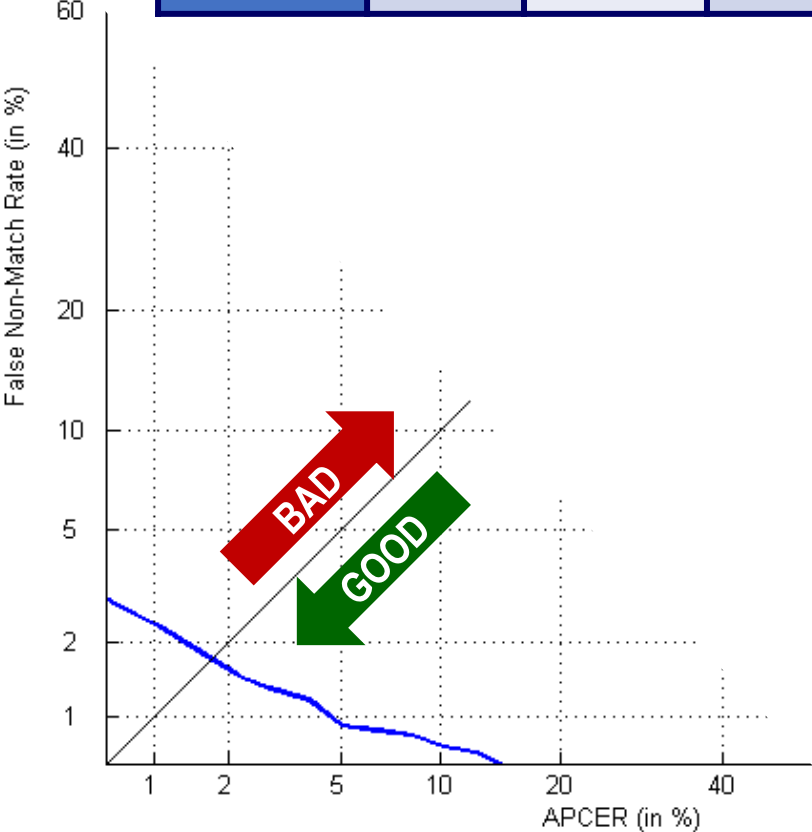
Estado del Arte: Firma – Captura



Estado del Arte: Firma – Rendimiento

DET Experiment "B" (Hysteresis 40%)

EER\Level	1	2	3	4	5	6	7	8	9	10	11
Sin PAD	1,6	6,8	12,9	23,4	17,7	19,5	33,4	19,27	18,2	16,9	18,2
Con PAD	2,1	3,2	1,8	1,8	2,1	2	1,7	2,3	3,1	3,1	2,6



Fortalezas y Debilidades de la Biometría

- Naturalidad del **usuario**
- Velocidad
- Comodidad
- Adaptable
 - Si se considera una solución multimodal
- **¿Barato?**
- No tiene por qué ser una solución única para cada aplicación

- Falsos Positivos y Falsos Negativos
- Rendimiento depende del:
 - **Sensor**
 - **Usuario**
 - Condiciones atmosféricas
- **¿Caro?**
- No es una solución única para cada aplicación

¡Todo es muy relativo!
Depende de la aplicación y el contexto

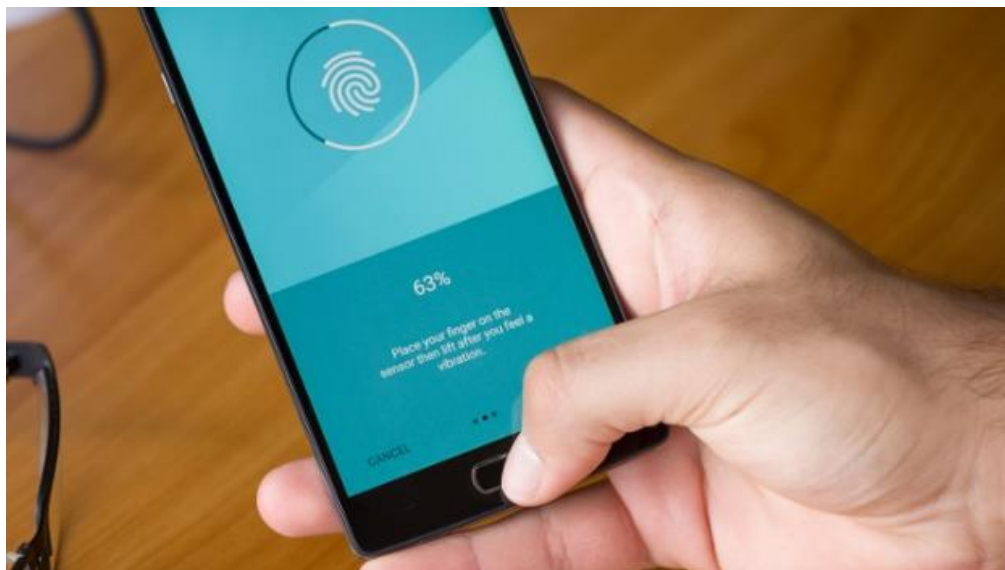
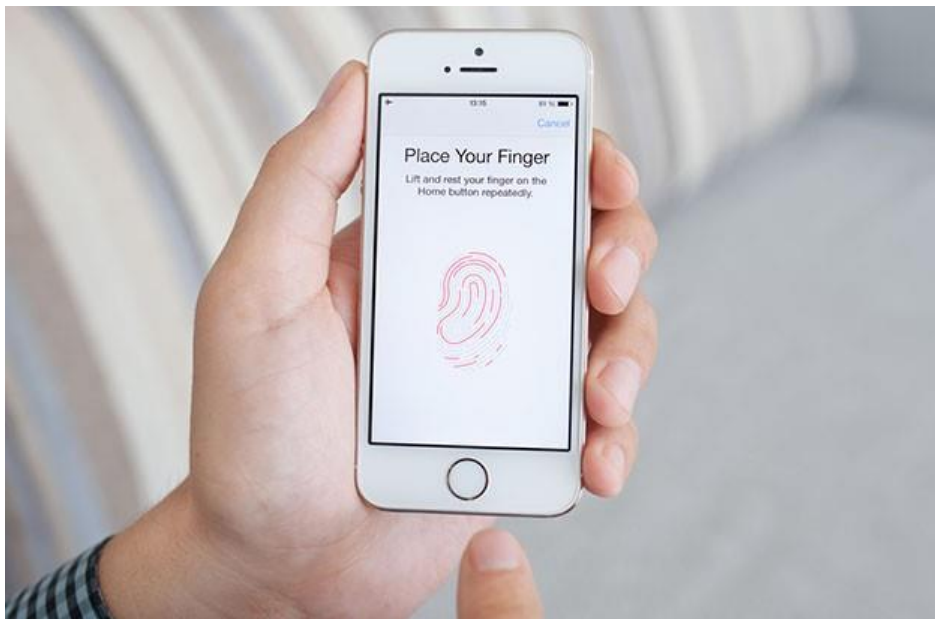
Smartphones

- Un Smartphone **NO** es un producto biométrico, ni de seguridad
 - Es un producto de consumo fabricado y con un nicho de negocio MUY ALEJADO a NUESTRAS necesidades
- Factores de importancia:
 - Bajo consumo
 - Tamaño limitado (especialmente en espesor)
 - Coste
 - Variabilidad de modelos/fabricantes/gamas/etc.
 - Elementos añadidos por el usuario: carcasas, paneles protectores, adornos colgantes, etc.
 - Uso en cualquier situación: sentado, de pie, andando, etc.

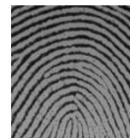
Smartphone – Huella

- Ventajas:
 - Muy extendido
 - Sensor ya disponible (coste nulo)
 - Posibilidad de usar múltiples dedos
 - De forma alternativa
- Inconvenientes:
 - El proveedor de servicio no recibe información biométrica
 - El móvil solo avisa si la verificación ha sido correcta
 - El móvil no identifica qué huella ha sido la reconocida
 - El fabricante no publica sus tasas de error
 - El sensor es muy barato y muy pequeño
 - Bajada enorme en el rendimiento
 - El umbral de decisión puede estar sesgado hacia la comodidad
 - Muy susceptible al fraude, tanto cooperativo, como no-cooperativo

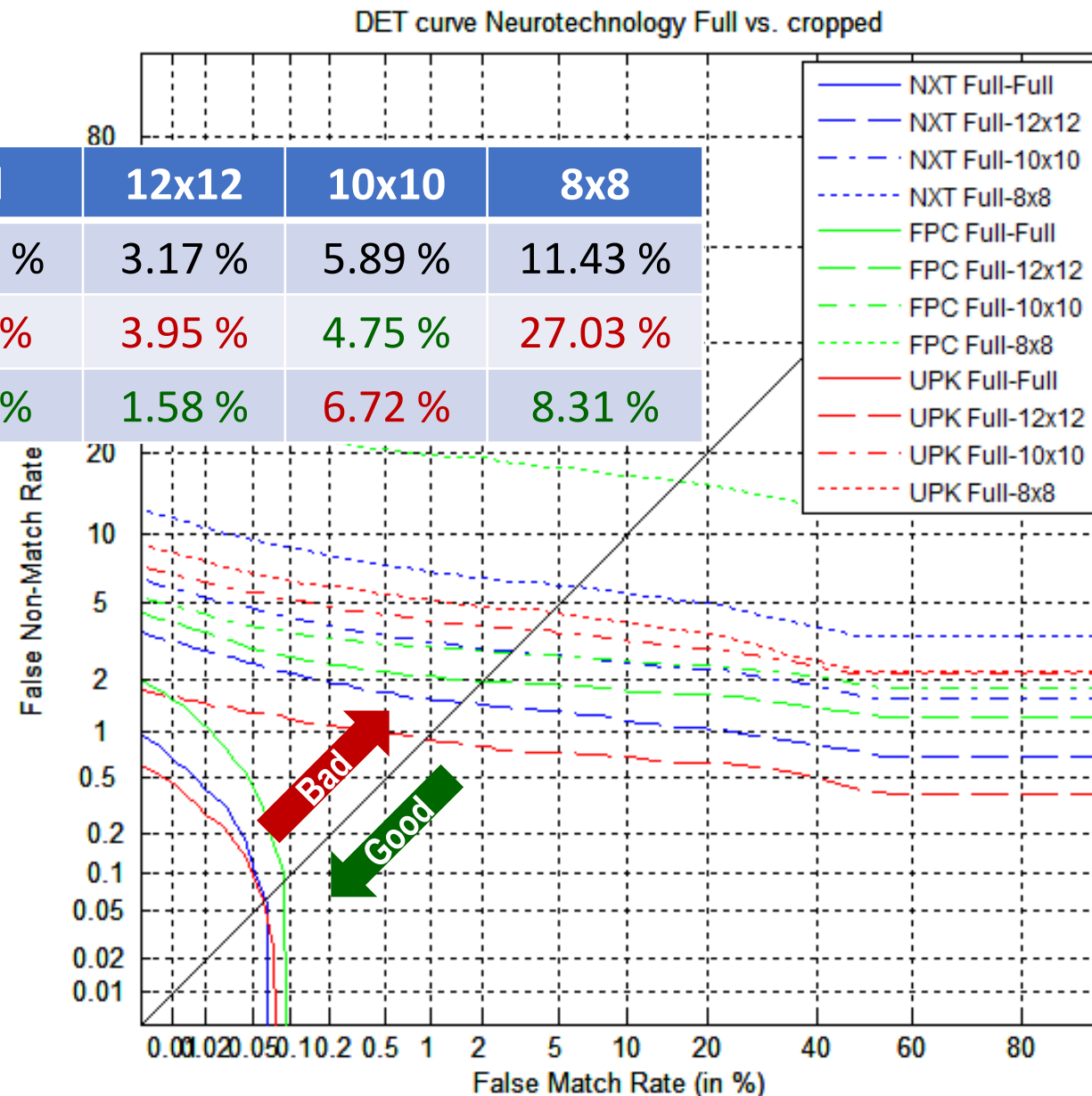
Smartphone – Captura



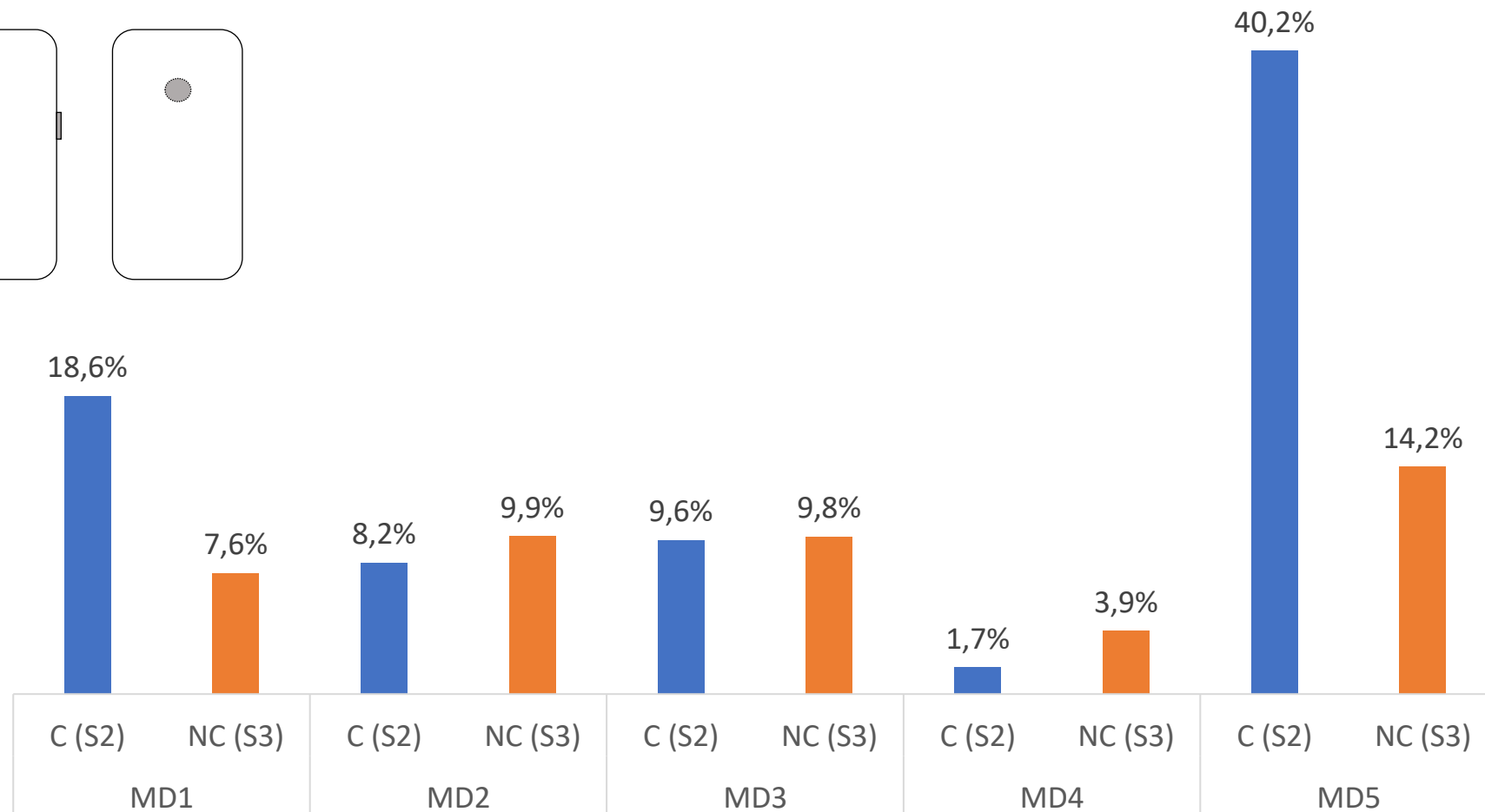
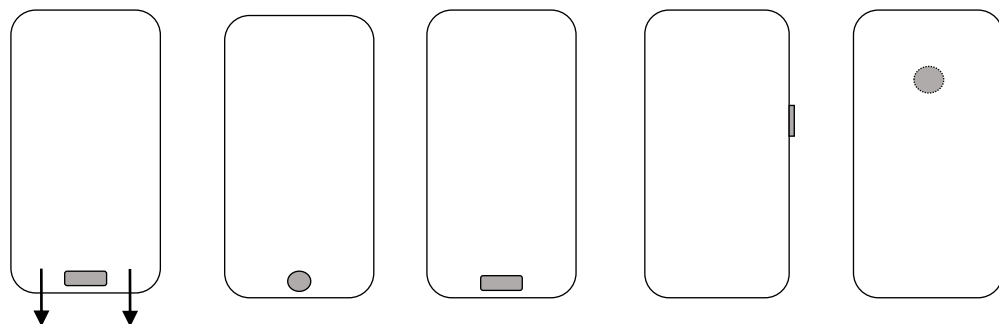
Smartphone – Huella: Tamaño Sensor

NXT 12x17 mm ²	NXT 12x12 mm ²	NXT 10x10 mm ²	NXT 8x8 mm ²
			
FPC 10.6x14 mm ²	FPC 12x12 mm ²		
			
UPK 12.8x18 mm ²	UPK 12x12 mm ²	UPK 10x10 mm ²	UPK 8x8 mm ²
			
192x270 pixels	180x180 pixels	150x150 pixels	120x120 pixels

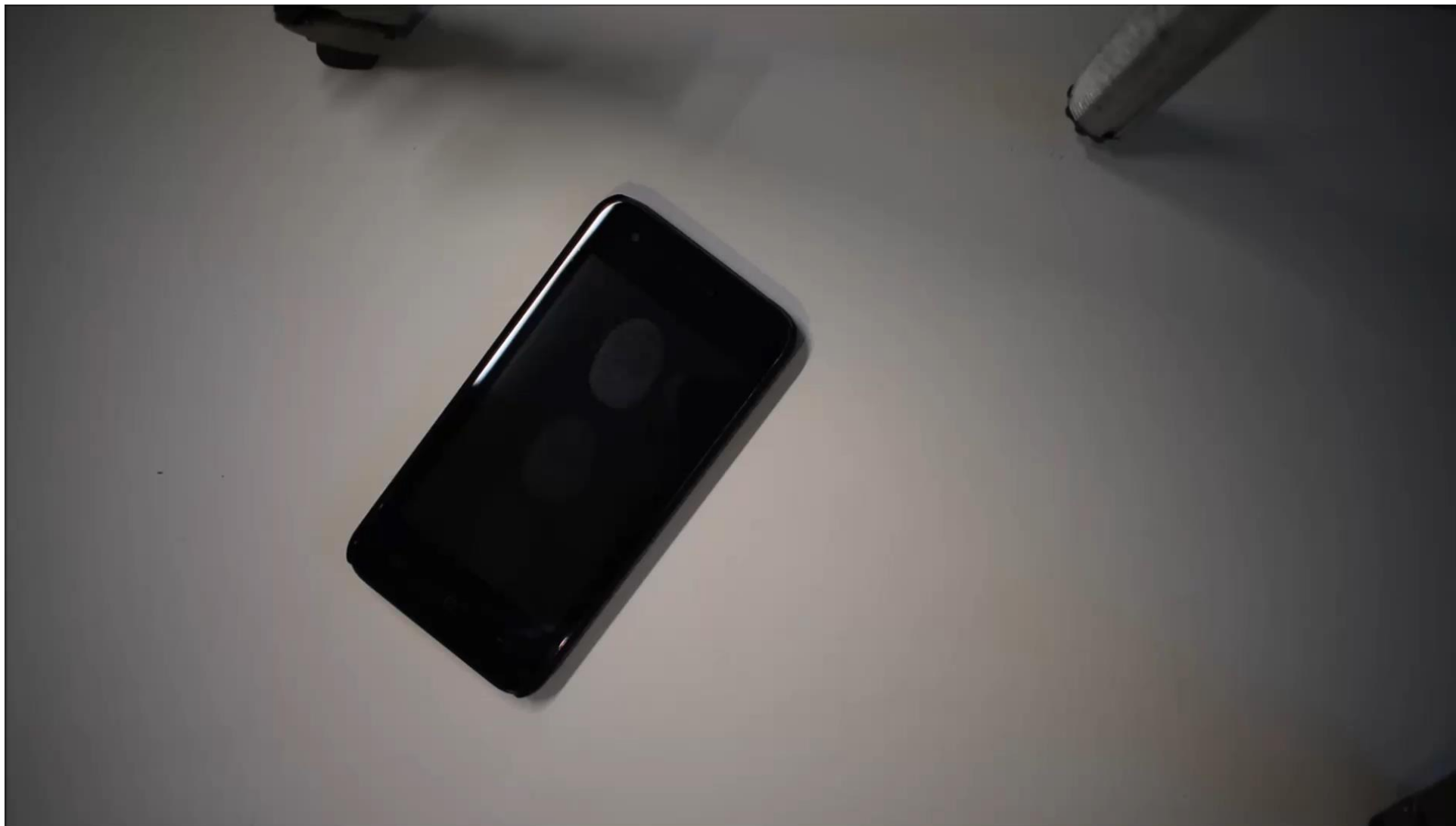
	Full	12x12	10x10	8x8
FRR@FAR=10 ⁻⁴ (NXT)	0.628 %	3.17 %	5.89 %	11.43 %
FRR@FAR=10 ⁻⁴ (FPC)	1.54 %	3.95 %	4.75 %	27.03 %
FRR@FAR=10 ⁻⁴ (UPK)	0.42 %	1.58 %	6.72 %	8.31 %



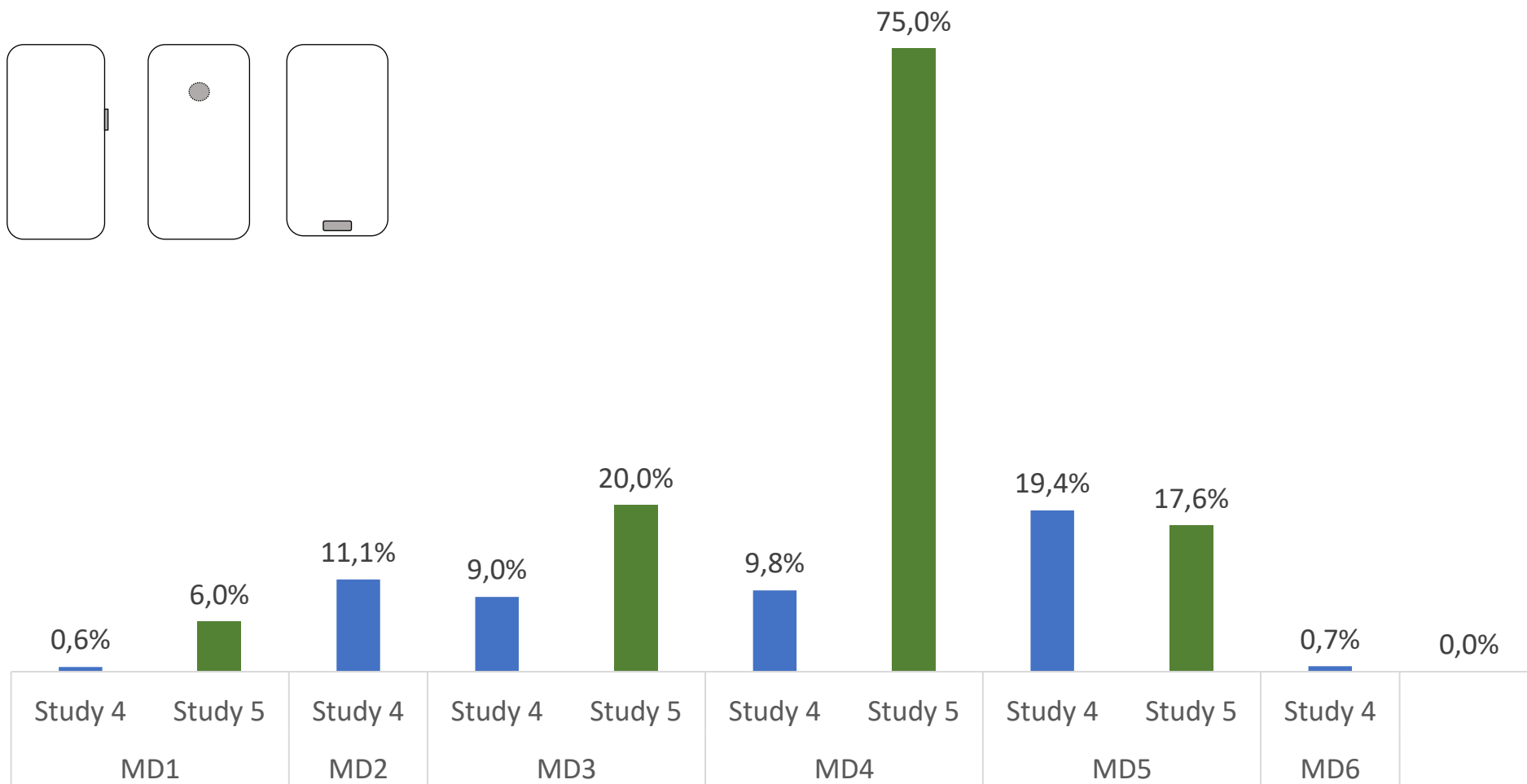
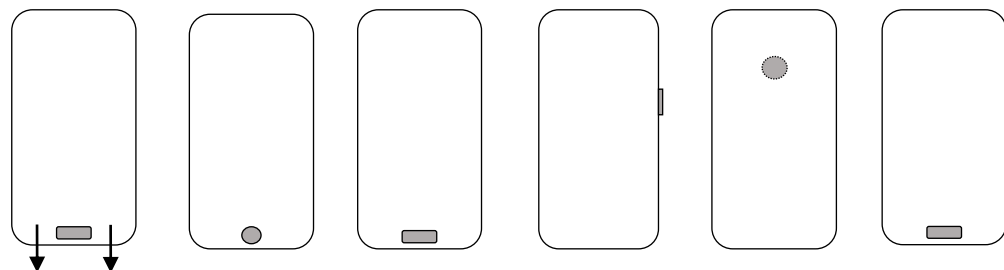
Smartphone – Huella: Ataques por un Experto



Smartphone – Huella



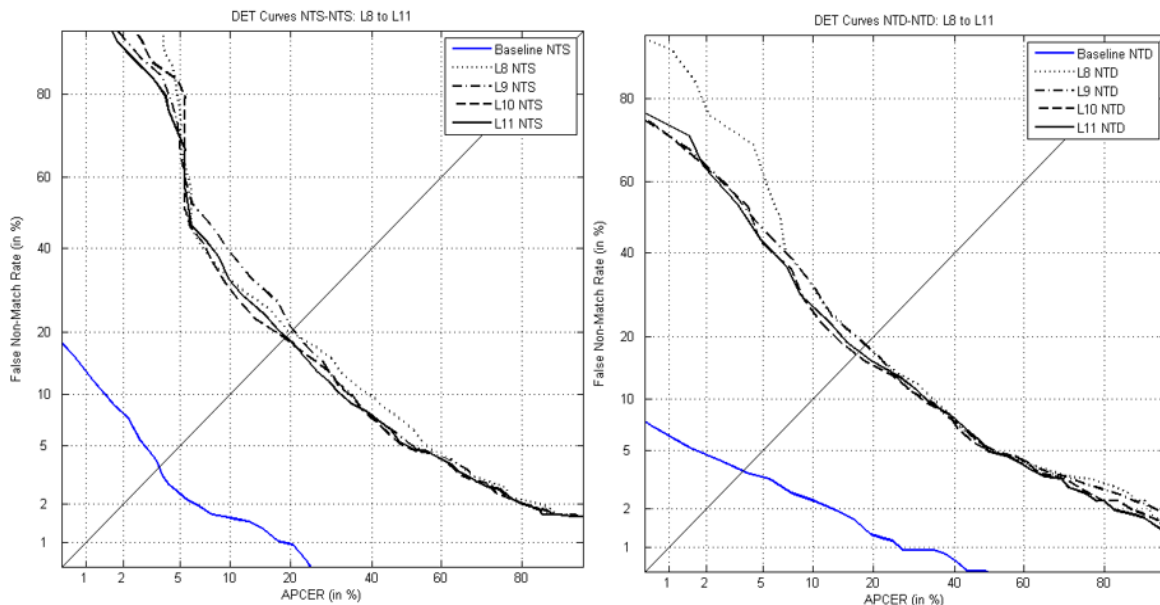
Smartphone – Huella: Ataques Cooperativos por No-Expertos



Smartphone – Firma Manuscrita

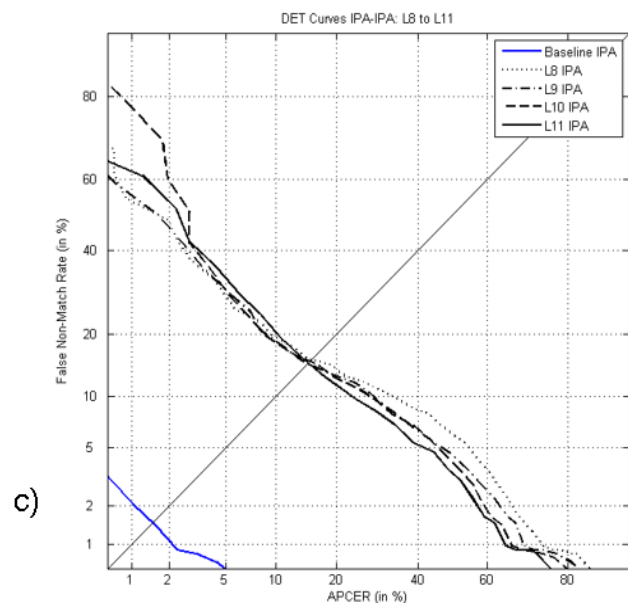
- Ventajas:
 - Sensor ya disponible (coste nulo)
 - Posibilidad de utilizar diferentes firmas
 - De forma alternativa
 - Pero hay que asegurarse que cualquiera de ellas es una “firma habitual”
 - Entendible por el usuario para determinados casos
 - La información biométrica puede ser recibida por el proveedor de servicio
 - Intrínsecamente es una “captura en vivo”: incluso se puede usar un time-stamping
- Inconvenientes:
 - Proceso de captura muy lento (lo que tarda el usuario en firmar)
 - No entendible / No práctico en muchos casos (por ejemplo, desbloquear el móvil)
 - En muchos móviles hay que firmar con el dedo: ¿Inconveniente real?
 - ¿Susceptible al fraude?

Smartphone – Firma Manuscrita



a)

b)



c)

Sin PAD

EER\Level	BL	8	9	10	11
STU	1,7	19,3	18,3	16,9	18,2
Note-Stylus	3,6	20,0	20,4	18,7	19,0
Note-Finger	3,7	18,4	18,5	16,7	17,3
iPad	1,5	15,3	14,7	15,1	14,7

Con PAD la evolución es equivalente:

$EER < 3\%$

Smartphone – Facial

- Ventajas:

- Sensor ya disponible (coste nulo)
- Posibilidad de utilizar diferentes poses
 - Puede servir para evitar ataques de suplantación
 - Complica el reconocimiento y/o el reclutamiento
- Forma natural del ser humano para ser reconocido
- La información biométrica puede ser recibida por el proveedor de servicio

- Inconvenientes:

- Proceso de captura dependiente del “enfoco” del usuario y de la cámara a usar
- Sólo captura en el visible
- En muchos casos sólo se captura información estática
- ¿Susceptible al fraude?
- ¿Flash en cámara frontal?

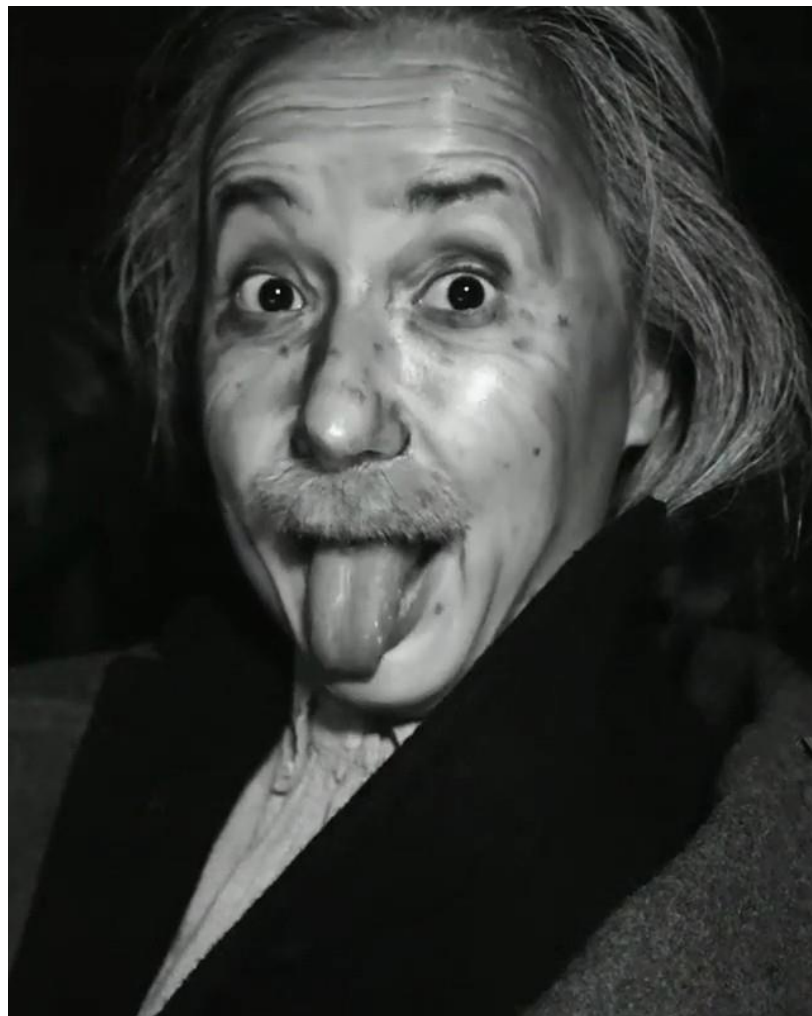
Smartphone – Facial

Developer	VISA Photos FNMR @ FMR ≤ 0.000001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001 DT ≥ 12 YRS	VISABORDER Photos FNMR @ FMR ≤ 0.000001	BORDER Photos FNMR @ FMR = 0.000001	WILD Photos FNMR @ FMR ≤ 0.00001
visionlabs-009	0.0025 ⁽¹⁾	0.0026 ⁽¹⁾	0.0029 ⁽³⁾	0.0035 ⁽¹⁾	0.0064 ⁽¹⁾	0.0306 ⁽¹³⁾
dahua-005	0.0046 ⁽¹³⁾	0.0035 ⁽¹²⁾	0.0049 ⁽¹³⁾	0.0046 ⁽⁵⁾	0.0076 ⁽²⁾	0.0300 ⁽³⁾
ntechlab-008	0.0061 ⁽¹⁹⁾	0.0056 ⁽³¹⁾	0.0108 ⁽⁴⁴⁾	0.0042 ⁽²⁾	0.0080 ⁽³⁾	0.0312 ⁽³⁰⁾
deepglint-002	0.0027 ⁽³⁾	0.0032 ⁽⁸⁾	0.0033 ⁽⁴⁾	0.0043 ⁽³⁾	0.0084 ⁽⁴⁾	0.0301 ⁽⁴⁾
vocord-008	0.0038 ⁽⁶⁾	0.0042 ⁽¹⁸⁾	0.0055 ⁽¹⁵⁾	0.0045 ⁽⁴⁾	0.0086 ⁽⁵⁾	0.0310 ⁽²⁴⁾
xforwardai-001	0.0034 ⁽⁵⁾	0.0027 ⁽³⁾	0.0028 ⁽²⁾	0.0046 ⁽⁶⁾	0.0088 ⁽⁶⁾	0.0303 ⁽¹⁰⁾
teviaan-006	0.0061 ⁽¹⁸⁾	0.0045 ⁽²⁰⁾	0.0066 ⁽²⁰⁾	0.0046 ⁽⁷⁾	0.0091 ⁽⁷⁾	0.0330 ⁽⁴³⁾
bioidtechswiss-001	0.0072 ⁽²²⁾	0.0069 ⁽⁴³⁾	0.0124 ⁽⁵⁴⁾	0.0060 ⁽¹³⁾	0.0094 ⁽⁸⁾	0.0345 ⁽⁵³⁾
tech5-005	0.0072 ⁽²³⁾	0.0069 ⁽⁴²⁾	0.0122 ⁽⁵²⁾	0.0060 ⁽¹⁴⁾	0.0094 ⁽⁹⁾	0.0381 ⁽⁶⁸⁾

Smartphone – Facial

Developer	VISA Photos FNMR @ FMR ≤ 0.000001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001	MUGSHOT Photos FNMR @ FMR ≤ 0.00001 DT ≥ 12 YRS	VISABORDER Photos FNMR @ FMR ≤ 0.000001	BORDER Photos FNMR @ FMR = 0.000001	WILD Photos FNMR @ FMR ≤ 0.00001
ercacat-001	0.0044 ⁽¹⁰⁾	0.0033 ⁽⁹⁾	0.0047 ⁽¹⁰⁾	0.0106 ⁽⁴³⁾	0.0202 ⁽³⁶⁾	0.0293 ⁽¹⁾
nazhiai-000	0.0059 ⁽¹⁶⁾	0.0036 ⁽¹³⁾	0.0048 ⁽¹²⁾	0.0057 ⁽¹²⁾	0.0125 ⁽¹⁹⁾	0.0300 ⁽²⁾
dahua-005	0.0046 ⁽¹³⁾	0.0035 ⁽¹²⁾	0.0049 ⁽¹³⁾	0.0046 ⁽⁵⁾	0.0076 ⁽²⁾	0.0300 ⁽³⁾
deepglint-002	0.0027 ⁽³⁾	0.0032 ⁽⁸⁾	0.0033 ⁽⁴⁾	0.0043 ⁽³⁾	0.0084 ⁽⁴⁾	0.0301 ⁽⁴⁾
cib-001	0.0061 ⁽²⁰⁾	0.0030 ⁽⁶⁾	0.0041 ⁽⁷⁾	0.0048 ⁽⁸⁾	0.0578 ⁽⁷⁶⁾	0.0302 ⁽⁵⁾
fujitsulab-001	0.0082 ⁽³⁰⁾	0.0132 ⁽⁹¹⁾	0.0258 ⁽⁹⁶⁾	0.0140 ⁽⁵⁵⁾	0.0246 ⁽⁴⁶⁾	0.0302 ⁽⁶⁾
everai- paravision-003	0.0050 ⁽¹⁴⁾	0.0036 ⁽¹⁴⁾	0.0052 ⁽¹⁴⁾	0.0092 ⁽³⁵⁾	0.0193 ⁽³⁵⁾	0.0302 ⁽⁷⁾
vinai-000	0.0124 ⁽⁵¹⁾	0.0045 ⁽¹⁹⁾	0.0072 ⁽²³⁾	0.0089 ⁽³¹⁾	0.1814 ⁽⁹⁹⁾	0.0302 ⁽⁸⁾
xforwardai-001	0.0034 ⁽⁵⁾	0.0027 ⁽³⁾	0.0028 ⁽²⁾	0.0046 ⁽⁶⁾	0.0088 ⁽⁶⁾	0.0202 ⁽¹⁰⁾

Smartphone – Facial



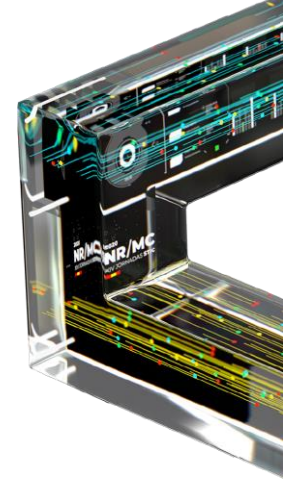
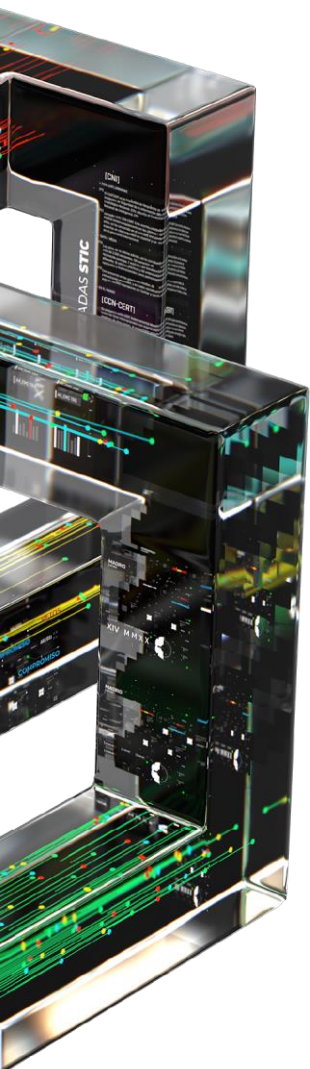
Conclusiones

- Hay que tener muy en cuenta el contexto, el entorno y la aplicación para realizar una correcta selección de:
 - Modalidad
 - Dispositivo de captura
 - Procedimiento de uso
- Las tasas que ofrecen los fabricantes son, siempre, en el mejor de los casos
 - Nunca en entornos reales
 - Y en algunos casos muy discutibles
- Es imprescindible un proceso de certificación del producto ofertado:
 - Tanto en rendimiento, como en robustez frente a ataques
 - Realizado por entidades independientes
- **¡El usuario y su comportamiento es todo un reto!**

Conclusiones

'Mommy, I was shopping': Six-year-old Arkansas girl uses her sleeping mom's fingerprints to unlock iPhone and buy 13 Pokemon gifts on Amazon for a total of \$250

- Bethany Howell of Maumelle, Arkansas, was lying on her couch with her daughter, Ashlynd, one evening earlier this month
- The two were watching a movie shortly before Bethany put her daughter to bed
- After Bethany dozed off, Ashlynd took her mother's thumb and used it to unlock her iPhone
- Ashlynd then bought \$250 worth of Pokemon gifts on Amazon
- The next day, Bethany saw the amount of money that was spent and initially thought she had been hacked



MUCHAS GRACIAS

#XIVJORNADASCCNCERT