Antonio Coín Castro

BIOMÉTRICO

TEMA 1: Introducción

Def (Rec. biométrico). – Establecer la identidad de una persona basado en atributos físicos o conductuales.

Rasgos

- ↳ Fisiológicos/morfológicos (no se pueden modificar fácilmente; visibles o visualizables): huella, cara, iris, orejas, retina, ...
- ↳ Fisiológicos/biológicos: ADN, EKG, olor
- ↳ Conductuales: voz, firma, forma de andar, ...

Historia

- Huellas de manos → 31.000 años atrás
- Huellas dactilares → transacciones, marcas personales
- 1870: Bertillon sistema antropométrico: medidas estandarizadas cuerpo.
- 1988: Semi-automatic facial recognition.

Autenticación usuarios

- Tradicional: algo que se sabe o se posee (contraseñas, token, ...) ↳ FRAUDE
- Biométrico: algo que es o produce (requiere registro)

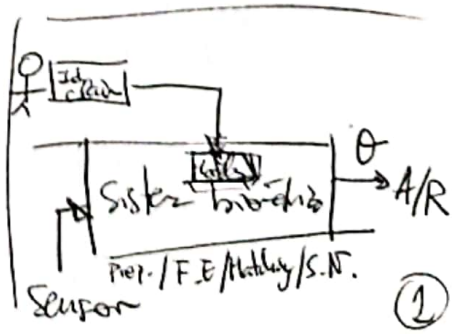
Características ideales

- Universalidad, unicidad, permanencia, facilidad de recolección
- Para un sistema: rendimiento, aceptabilidad, facilidad de elusión

Identificación vs verificación

- Identificación: determinar identidad de una persona (no identity claim). Es one-to-many, coste lineal
- Verificación: comprobar si alguien es quien dice ser. Es one-to-one, coste indep. del nº de usuarios en la BBDD.

↳ Aplicaciones: passport, logins, vigilancia, bancos, medicina, comercio, carné conducir, ...



Privacidad: datos personales, acceso por terceros, seguridad.

TEMA 2: Métricas

Matriz confusión: visualizar rendimiento de sist. verificación

		genuine	impostor
Valor real	genuine	TP	FN
	impostor	FP	TN

Resultado

- **FP**: Ocurre cuando la varianza inter-clase es baja (diferentes sujetos obtienen scores parecidos).
  - ↳ Intencional: ataque
  - ↳ No intencional: gemelos, padre e hijo, ...
- **FN**: Ocurre cuando hay variabilidad intra-clase: la edad, la falta de interoperabilidad del sistema, ...

Métricas

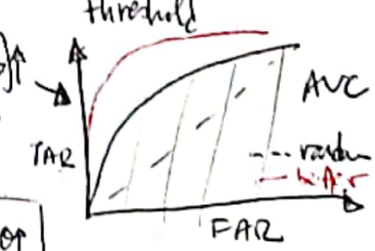
- Accuracy: rendimiento conjunto: $\frac{TP+TN}{TP+TN+FP+FN}$ (tb: 1-acc = error)
- FAR: #FP / all impostor = $\frac{FP}{FP+TN}$ (FAR = 1 − FRR)
- FRR: #FN / all genuine: $\frac{FN}{TP+FN}$

Threshold

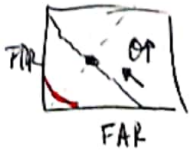
Umbral a partir del cual aceptamos un identity claim (civil = low FN, militar = low FP)

ROC and AVC

Curva que ilustra el rendimiento conforme varía el threshold (comparable): TAR vs FAR



DET: FRR vs FAR (EER = equal)



(logarithmic scale)

CMC (Identificación): % recognized vs Rank

(Rank-n: identificación entre los n primeros)

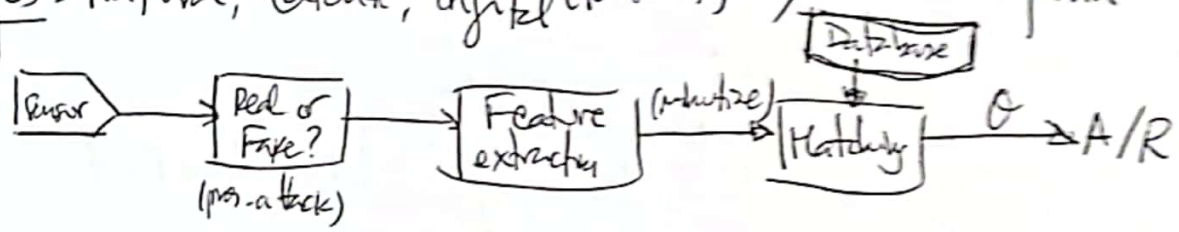
TEMA 3: Fingerprint

Def. – Mosaico de patrones de crestas y valles papilares del dedo humano
↳ Tiene mucha información discriminante (unívoca?)
↳ No cambia apenas con el tiempo; gemelos tienen huellas distintas (rasgo epigenético)

Historia

1888: Galton publica evidencia científica
1902: Bertillon
1924: FBI

Tipos: natural, latente, digital (sensores) ✓; rolled vs plain



Sensores: capacitivos (placa conductora, epidermis), ópticos (luz, 2D), ultrasónicos (ondas de sonido que penetran la epidermis, 3D), térmicos (diferencia temperatura ridges y valleys; problema: disipación).

Calidad de imagen (wet, dry, ...) NFIQ (Nist Fingerprint Image Quality)

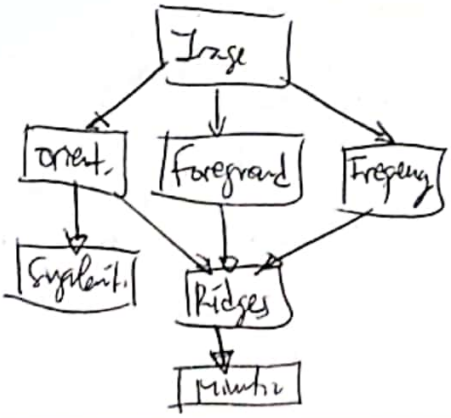
Detección de ataques: spoof vs non-spoof (handcrafted + DL features)

Macro-singularities: whorl (O), loop (U), delta (Δ).

Minutiae / Galton's characteristics: terminación o bifurcación de crestas.

Very local: poros, crestas incipientes, ...

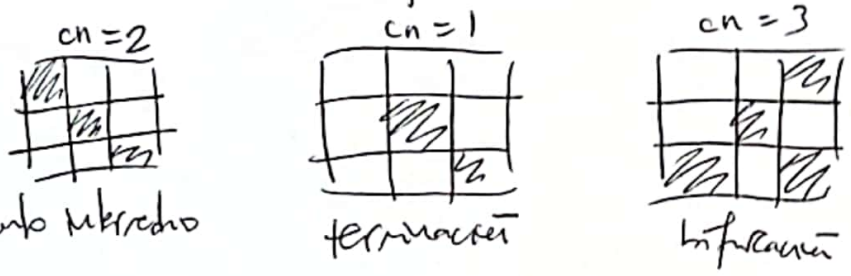
Extracción de características



- **Segmentación**: background (uniform) vs foreground (striped)
- **Orientación**: ángulo de crestas con el eje horizontal en un vecindario
- **Frecuencia**: número de crestas por unidad de longitud en un segmento ⊥ orientación.

- Singularidades (core) → Índice de Poincaré (dividir mapa de orientación en subregiones, y mirar).
- Ridge pattern: enhancement + binarización, thinning (1 px)
  (orientación + frecuencia + filtro Gabor)
- Minutiae: se eligen puntos de partida, se buscan las crestas más cercanas, y se sigue hasta una bifurcación o terminación.
  → (máximos locales con respecto a la dirección ortogonal a ellos).

crossing number



Todo este proceso se puede hacer con DNN (MinutiaeNet), residual CNN. CoarseNet + FineNet.

Matching:
↳ retos: distorsiones no lineales por proyección, posicionamiento, interoperabilidad, calidad

- Minutiae-based: alineamiento que produce más parejas de minucias.
  ↳ Global: transformaciones globales (Hough, RANSAC)
  ↳ Local: local features pairing + consolidation step. (ej: k-closest, k-radius).
- Ridge feature-based: usar patrón de crestas (orientación, frecuencia, singularidades, ...). Gabor filter + euclidean distance.
- Correlation-based: se superponen dos huellas y se calcula la correlación entre píxeles para distintos alineamientos.

Fingerprint Verification Competition (2000+)

Research Lines:
- Fake / altered fingerprint
- Double-Identity
- Latent

TEMA 4: IRIS

Iris: textura única y estable (a través de iris code)

J. Daugman → National Geographic: iris code

Daugman blogs: igual que fingerprint pero con iris code ↔ minutiae.

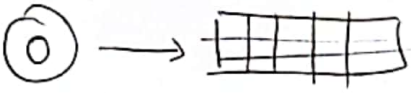
Sensores: Near-InfraRed, short distance

IRIS CODE

(i) Segmentación: encontrar las fronteras limbica (iris) y pupilar.

↳ Operador integro-diferencial de Daugman

↳ BBox de la región ocular más grande

(ii) Unwrapping:  fixed grid

↳ Filtros Gabor 2D (código mismo tamaño) → 2 bits / complex number

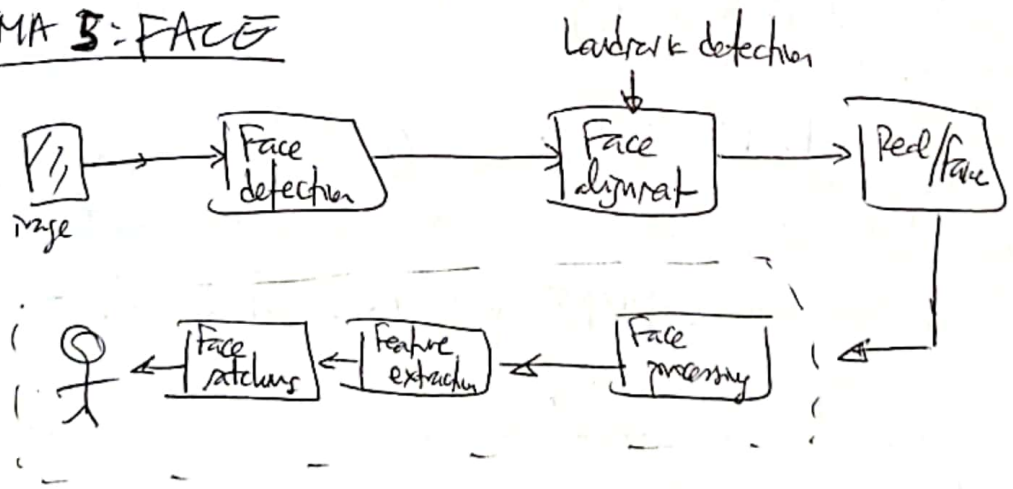
↳ Máscara de oclusión

(iii) Code: 2048 bits: 8×128 rectangle (=1024 patches w/ 2 bits)

Matching: fractional Hamming distance: fraction of XORs that are 1 (fraction of bits that differ).

CNN: feature extraction: Iris ParseNet (autoencoder)

TEMA 5: FACE



Face detection (CNN)

- Region-based: proposals + classify whether they have a face (Faster R-CNN)
- Sliding-window: boundary box + score at every location. Different scales (pyramid)

Alineamiento

- Alinear mediante puntos de referencia (ojos, punta nariz, comisuras, ...)
- Detección de landmarks: deep learning (OpenFace2, Hyperface)

Presentation attack detection

↳ Texture-Based; depth-based (special sensors); physiological-based (video: heart-rate, eye blink, ...)

Face processing (learn invariant features)

Aventar robustez vs pose, oclusión, iluminación, expresión, ...

- One-to-many augmentation: generar varios parches en distintas poses a partir de una sola imagen.
- Many-to-one normalization: recuperar vista canónica (frontal) de una o más imágenes no frontales.

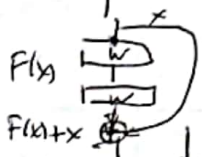
Feature extraction: tres generaciones principales

- Métodos básicos: PCA (eigenfaces) for reconstruction, and LDA (Fisherfaces) for discrimination: ↑ inter-class correlation and ↓ intra-class correlation. Insensitive to light or expression variation.
- Métodos lineales: (i) Sparse matrix minimizing L1 norm (test image = sparse linear comb. of train images). Robust

  (ii) Metric learning
  - ↳ Aprender M mahalanobis que minimize la distancia entre inputs con labels similares, y maximize la de los disimilares.
  - ↳ Learn matrix to improve KNN: penalize large intra-class and small inter-class.
  - ↳ Information-theoretic: Kullback Leibler divergence.
- Métodos no lineales

Deep learning: acceso a grandes BBDD. Usar CNNs ↳ + ejemplos, estructura, loss function

- DeepFace, DeepId (smaller CNNs ensembled, with face patches), DeepId 2 (improve training process) → outperform human recognition (97.5% human), FaceNet (train using triplets of matching/non-matching face patches; using Inception modules), VGGNet (trained on smaller DDBB, competitive performance), ArcFace (improve loss function to maximize class separability) using ResNet) → best result, 99.83



ResNet: shortcut connections (skip layers) to avoid degradation.

Fairness

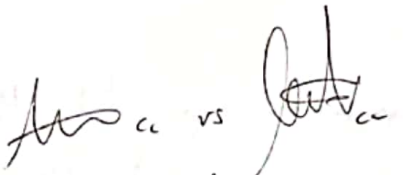
FaceGenderId (reduce gender biases), SensitiveNet (remove sensitive info)

GAN → generate representation of aged person?

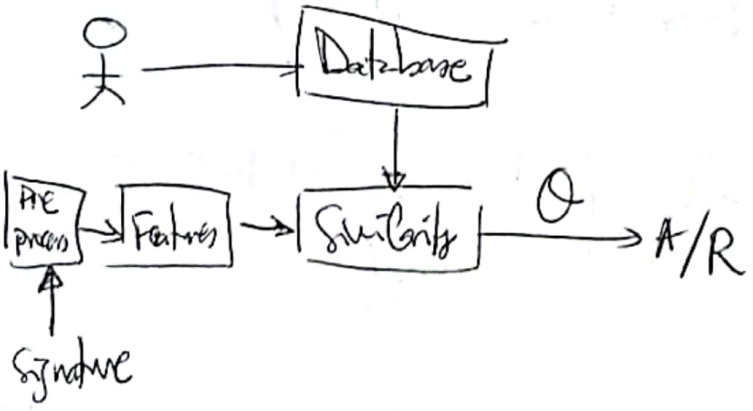
DeepFakes: imágenes y vídeos falsos pero muy realistas.

TEMA 6: ESCRITURA

Retos:

- Gran variabilidad intra-usuario: 
- Pequeña variabilidad inter-usuario: falsificaciones

Enfoques: offline (solo imagen), on-line (señales temporales)
↳ device to capture



Points equally distant in time.

Devices:

- 100/200 samples/s (Nyquist)
- +1000 pixels/inch (ppp)

Signals

- $\bar{X}, Y, P$
- Altitude (?)

Challenges: interoperability

- Different spatial position and/or time res.
- Lack of pressure (finger?)

Pre-processing

- Spatial normalization: size, position, rotation
- Time normalization: same sampling freq. (interpolate)

Feature Extraction

- Global features: multi-dimensional holistic vectors (duration, avg velocity, ...)
- Local features: set of time series (x-coord, pressure, speed, ...)

Similarity computation

(i) Global features: same length

- Distance-based classifiers: Euclidean (scale-dependent, curse of dim), Mahalanobis (problem: difficult to estimate Σ).
- Statistical/other classifiers: SVM, NN, ~~[illegible]~~, ...

(ii) Local features

- Regional (segment-to-segment): Hidden Markov Models
- Local (point-to-point): Dynamic Time Warping
- New approach: deep-learning
  - ↳ Siamese Arch. → learn dissimilarity metric.
  - ↳ Recurrent NNs → LSTM (memory, learn parameters) } improve perf.
  - ↳ DeepSign database
  - ↳ DTW + Deep learning: align time functions and feed to RNN (align test sample and enrolled signature **BEST** ~~[illegible]~~ enroll test

Other research lines

- Generate signatures (decompose into strokes with lognormal velocity and sum) **DNN**
- Use signature complexity to train models (+ robust)
- Structure curve