ENJEUX ET SÉCURITÉ DES SYSTÈMES BIOMÉTRIQUES ACTUELS

PAULINE PUTEAUX – LIRMM, UNIV. MONTPELLIER/CNRS

HMIN407 – SÉCURITÉ INFORMATIQUE : ENJEUX ET FACETTES

LE 30/01/19

MOTIVATIONS

- Nous devons pouvoir nous identifier au quotidien
- Impossible de se souvenir de 100 mots de passe différents

- Facile de perdre ou oublier son mot de passe

Pourquoi ne pas utiliser les **caractéristiques physiques/physiologiques** ou **comportementales** ?

QU'EST-CE QUE LA BIOMÉTRIE ?

- Biométrie = mesure + vivant
- « Un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à l'individu » (CLUSIF).
- La reconnaissance **automatique** des individus, basée sur leurs **caractéristiques physiques, physiologiques, comportementales** (ou **psychologiques**)

PROPRIÉTÉS D'UN SYSTÈME BIOMÉTRIQUE

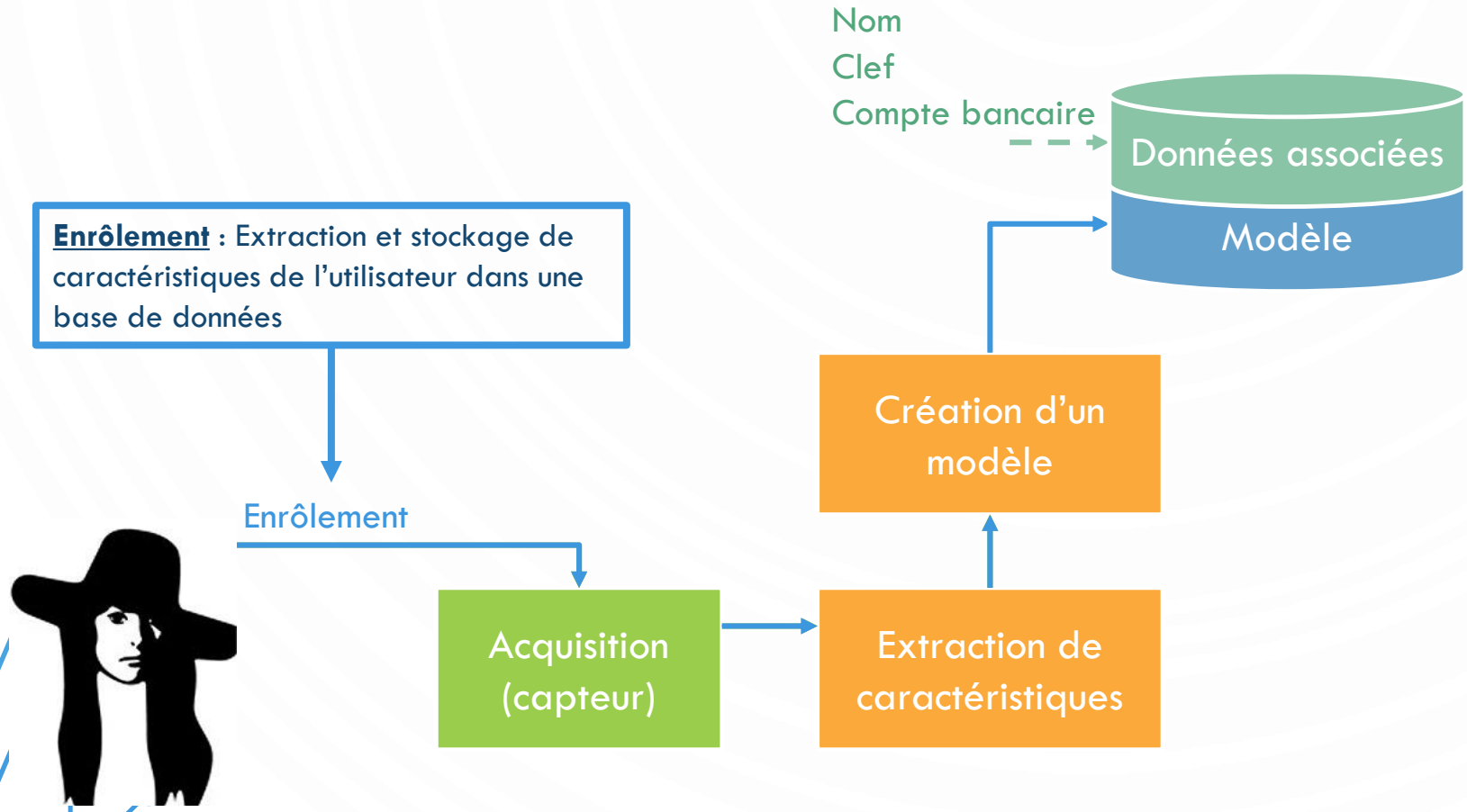
- Données « infalsifiables et uniques »
- Universalité :
  - Caractéristique mesurée au sein de la population
- Distinctivité :
  - Inter-variabilité importante
- Robustesse :
  - Stable et facile à reproduire, invariant dans le temps
  - Difficile à imiter/contourner (impossibilité de duplication d'une caractéristique)
- Accessibilité :
  - Facile à acquérir et performante (bons taux d'erreur)
- Acceptable :
  - Non-intrusif
  - Bonne acceptation par les utilisateurs

AVANTAGES ET INCONVÉNIENTS

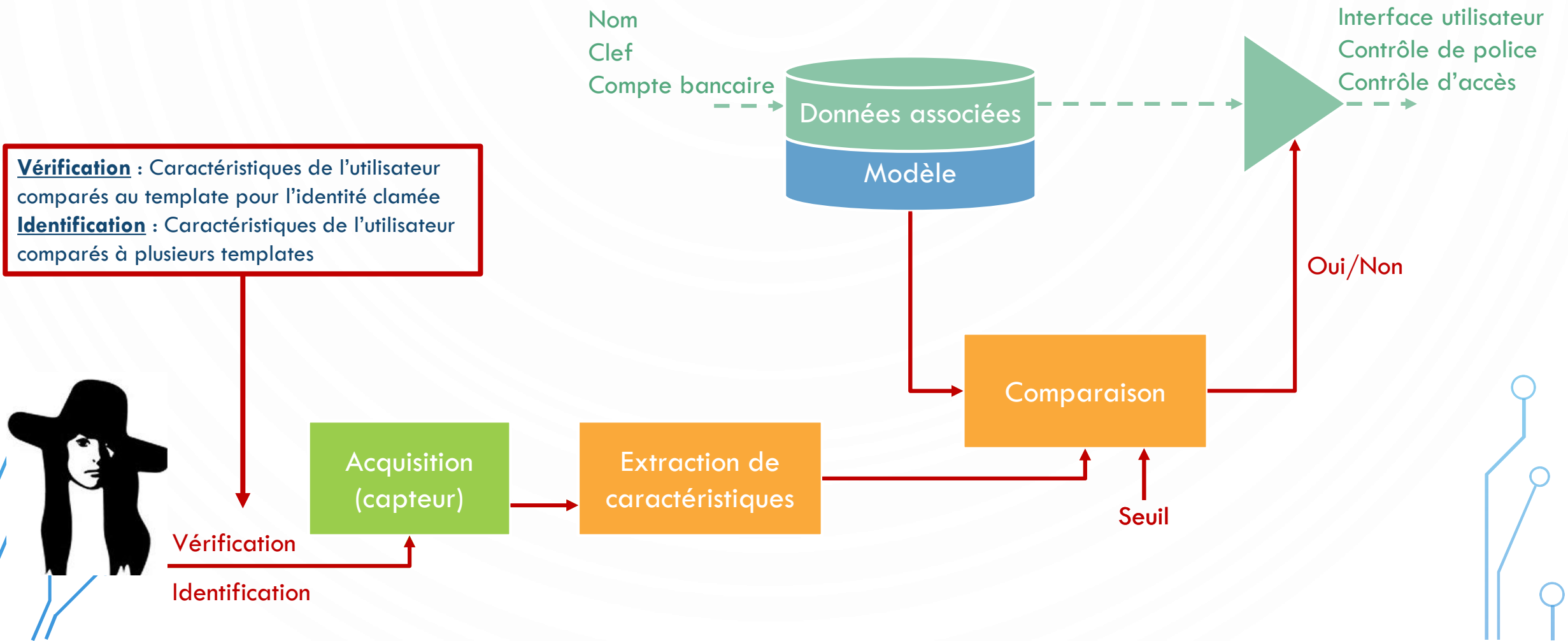
- Pas besoin de retenir des mots de passes
- L'**usurpation d'identité** peut être **détectée**
- **Une seule** caractéristique utilisée dans **plusieurs** applications, **sans diminuer le niveau de sécurité**

- Attaques par **présentation**
- **Renouvellement** impossible
- La biométrie n'est pas un secret
- Informations sensibles

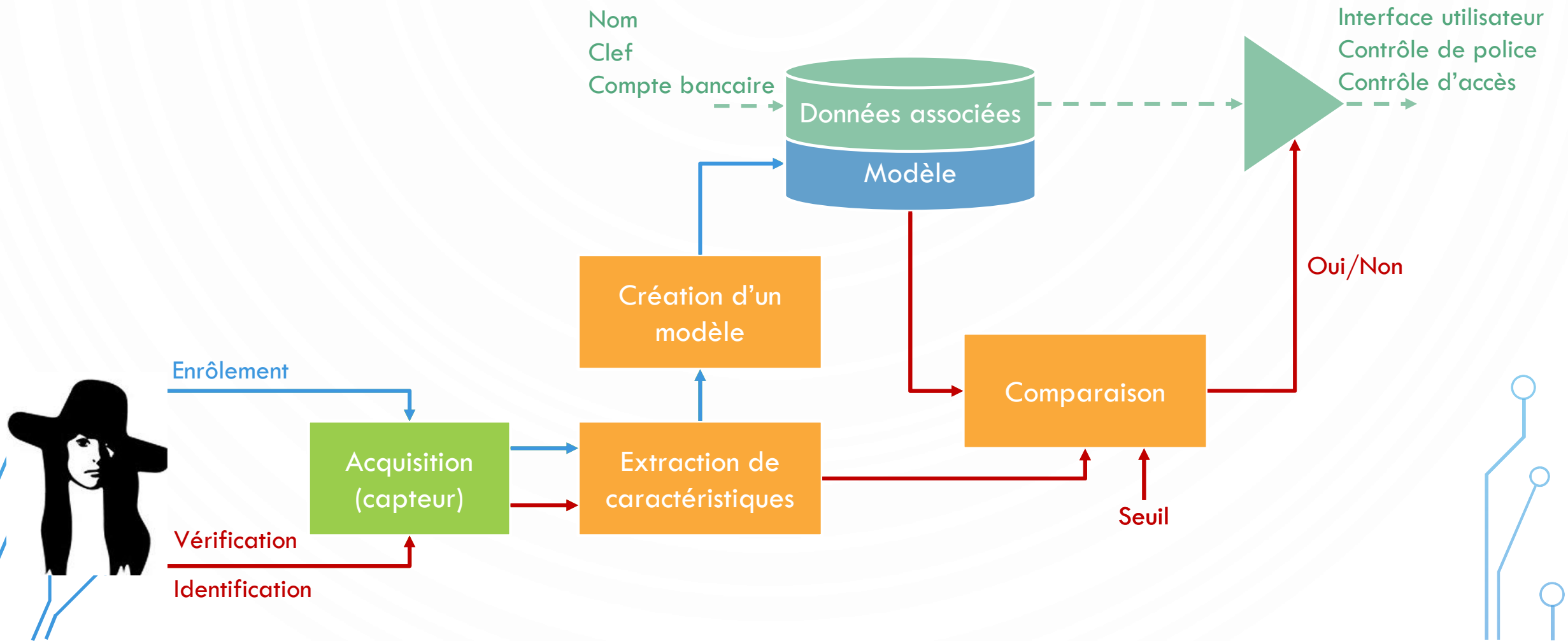
SYSTÈME BIOMÉTRIQUE



SYSTÈME BIOMÉTRIQUE



SYSTÈME BIOMÉTRIQUE



CARACTÉRISTIQUES BIOMÉTRIQUES

PHYSIQUES/PHYSIOLOGIQUES

- Doigt (empreinte, géométrie, ongles)
- Yeux (iris, rétine)
- Main (géométrie, veines, paume, jointure)
- Visage (morphologie, 2D ou 3D)
- Voix
- ADN (sang, salive…)
- Odeur
- Lobe d'oreille
- Lèvres / Langue

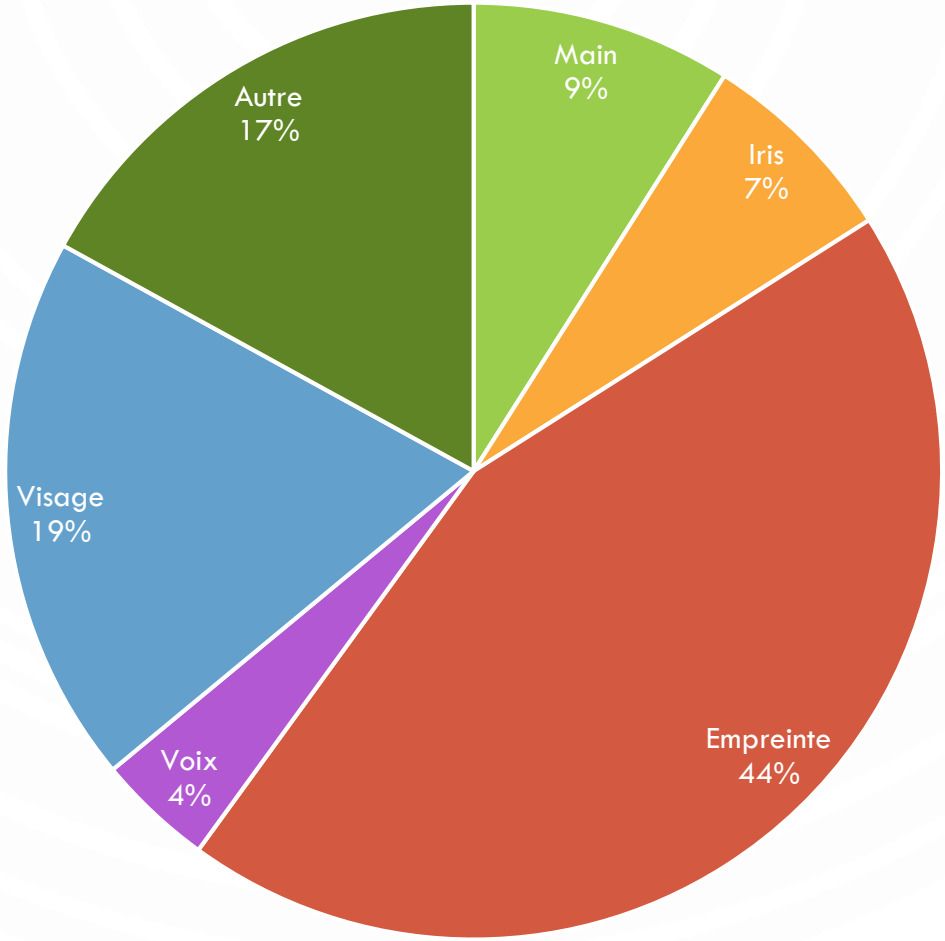
COMPORTEMENTALES

- Signature
- Geste de la main
- Voix
- Dynamique de frappe au clavier
- Démarche/allure

BASÉES SUR LA PSYCHOLOGIE

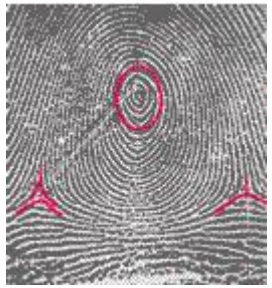
- Réaction à des situations concrètes, à des tests spécifiques, pour correspondre à un profil psychologique

CARACTÉRISTIQUES BIOMÉTRIQUES



QU'EST CE QU'UNE EMPREINTE DIGITALE ?

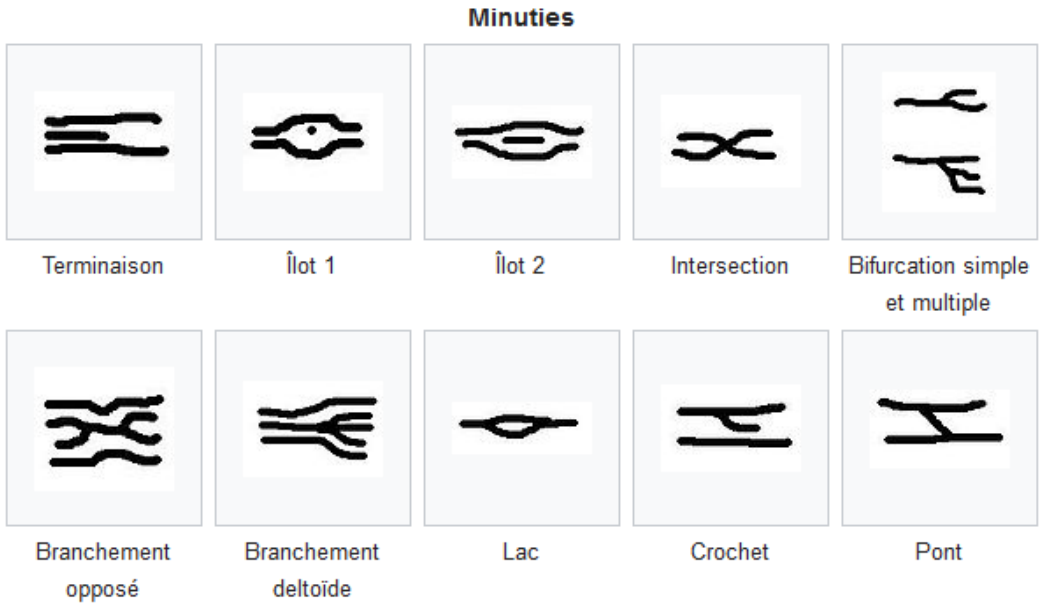
- La peau des doigts est composée de dermatoglyphes
- Figures dessinées par les plis et les crêtes épidermiques
- 3 grands types d'empreintes :
  - Boucles (à droite ou à gauche)
  - Verticilles (appelés spires ou tourbillons)
  - Arcs (appelés arches ou tentes)


- Correspondent à 95 % des doigts humains :
  - Boucles : 60%
  - Verticilles : 30%
  - Arcs : 5%

QU'EST CE QU'UNE EMPREINTE DIGITALE ?

- Motifs différenciés à l'aide de points singuliers :
  - Points singuliers globaux :
    - Noyau (ou centre) : lieu de convergence des stries
    - Delta : lieu de divergence des stries
  - Points singuliers locaux :
    - Irrégularités
    - Appelés « minuties »

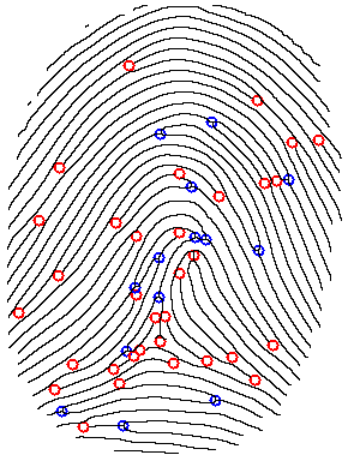


ALGORITHMES DE COMPARAISON D'EMPREINTES

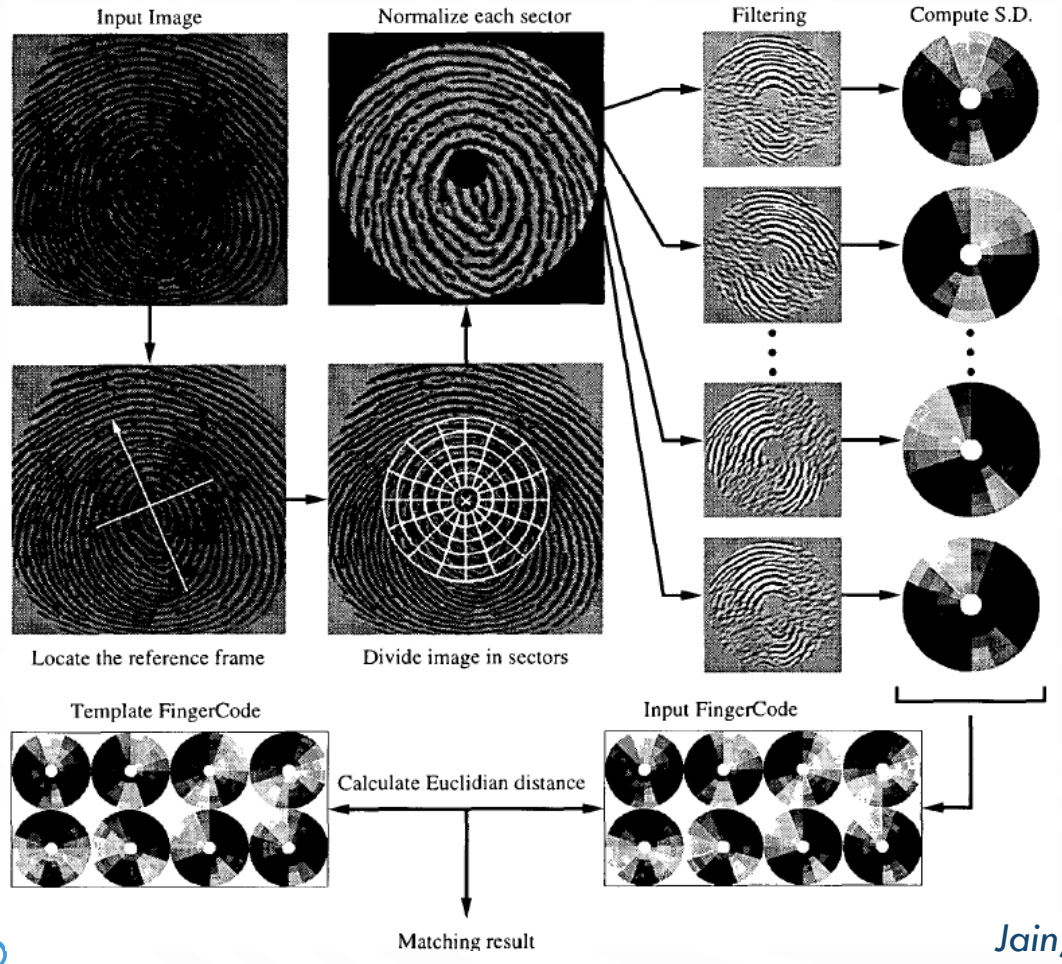
- De nombreux algorithmes existent
- 2 types principaux :
  - Basés sur l'étude des minuties :
    - Comparaison de l'emplacement et de l'orientation des minuties
    - Souvent utilisés pour les contrôles gouvernementaux (standards)
  - Basés sur l'étude du pattern général :
    - Comparaison de la configuration générale

ALGORITHMES DE COMPARAISON D'EMPREINTES

- Etude des minuties
  1. Numérisation de l'image
  2. Filtrage
  3. Evaluation de la qualité (score)
  4. Constitution d'un squelette (chaque trait = 1 pixel)
  5. Extraction d'une structure caractéristique
  6. « Gabarit » basé sur un ensemble suffisant et fiable de minuties
     - Nombre minimum : 14 minuties environ vs 100 détectées, 40 par sécurité
     - Une minutie : 16 octets



ALGORITHMES DE COMPARAISON D'EMPREINTES



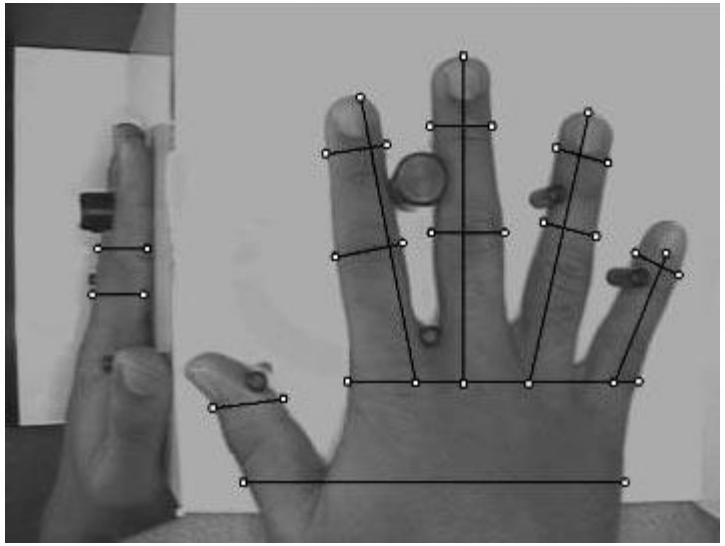
- Point de référence : Point de courbure maximale des crêtes dans l'image
- Axe de référence : Axe de symétrie locale au point de référence
- Filtrage avec filtres de Gabor (8 directions) pour capturer les caractéristiques globales et locales
- Calcul de l'écart type dans chaque secteur
- Obtention d'un FingerCode

Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (CVPR' 1999). FingerCode: a filterbank for fingerprint representation and matching.

PROBLÈMES

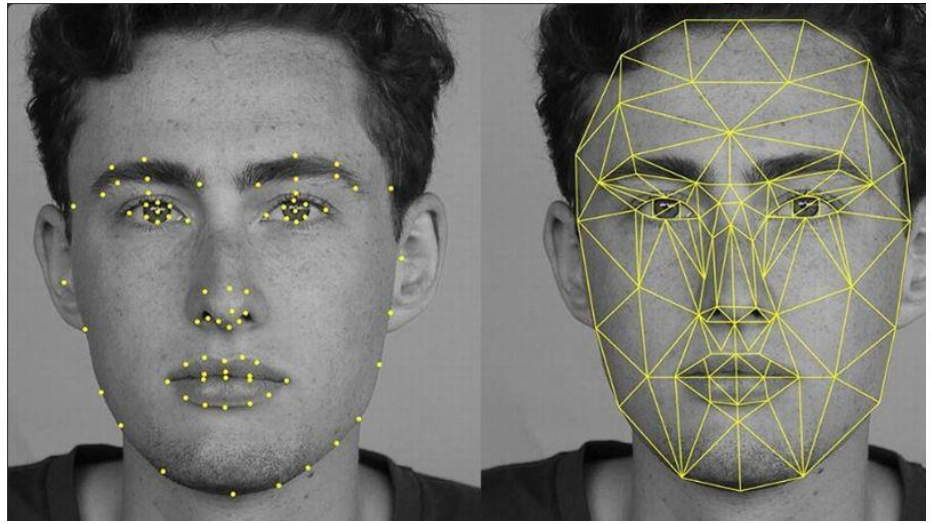
GÉOMÉTRIE DE LA MAIN

- Capture des 2 côtés de la main par la caméra
- Caractéristiques géométriques de la silhouette de la main (une dizaine d'octets)
- Plus vieille modalité biométrique



RECONNAISSANCE FACIALE

- Basée sur les caractéristiques géométriques du visage
  - Locales
  - Globales
- Beaucoup d'algorithmes utilisés (2D ou 3D)

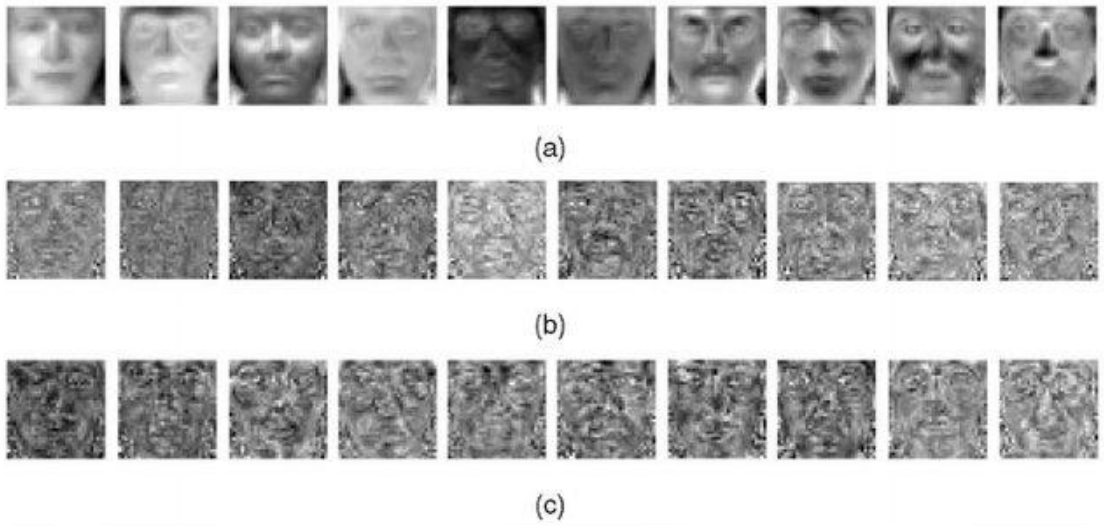


Method category	Sample algorithms: year first appeared in the literature
Local, holistic, and hybrid	Principal component analysis (Eigenfaces): 1991 Modular Eigenfaces: 1994 Linear discriminant analysis (Fisherfaces): 1997 Independent component analysis (ICA): 2002 Local binary pattern (LBP): 2006 Scale-invariant feature transform (SIFT): 2006 Speeded-up robust features (SURF): 2009 Learning-based descriptor (LBD): 2010
Appearance- and model-based	3D morphable model: 1999 Active appearance model (AAM): 2000 Eigen light field: 2004 Associate–predict model (APM): 2011
Geometry- and template-based	Dynamic link architecture (DLA): 1993 Elastic bunch-graph matching (EBGM): 1997 Trace transform (TT): 2003 Kernel methods: 2002 Simulated annealing for 3D face recognition: 2009
Template-matching, statistical, and neural networks	Probabilistic decision-based neural network (PDBNN): 1997 Genetic algorithm–evolutionary pursuit (EP): 1998 Wavelet packet analysis (WPA): 2000 Sparse representation (SR): 2009 Partial least squares (PLS): 2013 Hybrid deep learning (HDL): 2013 Discriminant face descriptor: 2014 DeepFace deep neural network: 2014 Deep hidden identity features (DeepID): 2014 FaceNet embedding: 2015

BASE D'ENTRAINEMENT

EIGEN/FISHER/LAPLACIAN FACES

- But : Prendre en compte les informations importantes qui permettront de reconnaître un visage parmi d'autres
- Approche : Représenter un visage comme une combinaison linéaire d'un ensemble d'images
- Méthodes utilisées :
  - Eigenfaces : Analyse en composantes principales (ACP)
  - Fisherfaces : Analyse discriminante linéaire de Fisher (FLDA/LDA)
  - Laplacianfaces : Projection avec préservation du voisinage (LPP)



EIGEN/FISHER/LAPLACIAN FACES

- Exemple : Etapes du calcul des eigenfaces
  - Constitution d'une base d'images de référence/d'apprentissage
  - Images chargées sous forme de matrices puis transformées en vecteurs

$$\{I_1, I_2, \ldots, I_M\}, \text{where } I_k = \begin{bmatrix} p^k_{1,1} & p^k_{1,2} & \cdots & p^k_{1,N} \\ p^k_{2,1} & p^k_{2,2} & \cdots & p^k_{2,N} \\ \vdots & & & \\ p^k_{N,1} & p^k_{N,2} & \cdots & p^k_{N,N} \end{bmatrix}_{N \times N}$$

$$\text{and } 0 \leq p^k_{i,j} \leq 255.$$

$$\Gamma_k = \begin{bmatrix} p^k_{1,1} \\ p^k_{1,2} \\ \vdots \\ p^k_{1,N} \\ p^k_{2,1} \\ p^k_{2,2} \\ \vdots \\ p^k_{2,N} \\ \vdots \\ p^k_{N,1} \\ p^k_{N,2} \\ \vdots \\ p^k_{N,N} \end{bmatrix}_{N \times 1}$$

$$, \text{where } k = 1, \ldots, M \text{ and } p^k_{i,j} \in I_k$$

EIGEN/FISHER/LAPLACIAN FACES

- Exemple : Etapes du calcul des eigenfaces
  - Calcul du visage moyen $\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i$
  - Calcul des caractéristiques propres par soustraction du visage moyen $\Phi_i = \Gamma_i - \Psi$
  - Calcul de la matrice de covariance

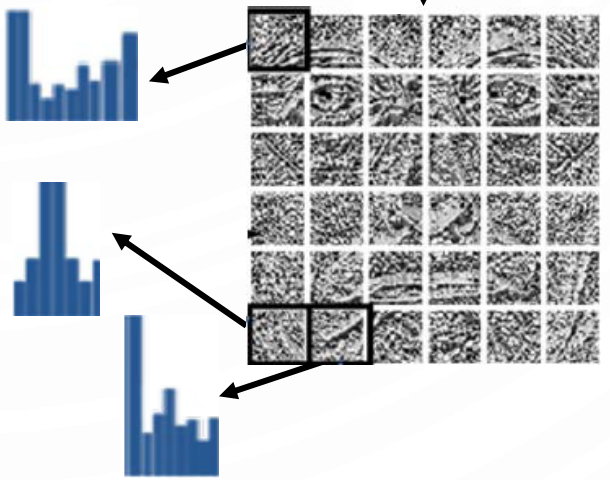
$$C = \frac{1}{M}\sum_{i=1}^{M}\Phi_i\Phi_i^T = AA^T, \text{ where } A = [\Phi_1\Phi_2 \ldots \Phi_M]$$

  - Calcul des vecteurs propres u_k (visages propres = eigenfaces) de la matrice de covariance
  - Projection de l'image à tester dans l'espace des visages propres (combinaison linéaire)
  - Différence entre l'image à tester (après soustraction du visage moyen) et cette image projetée
  - Comparaison à un seuil

LOCAL BINARY PATTERNS HISTOGRAMS

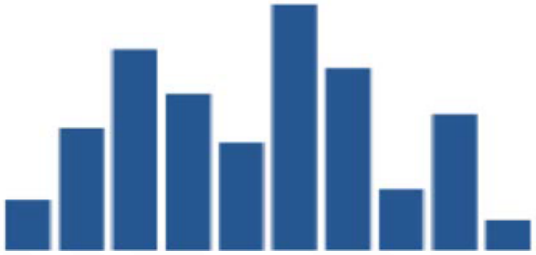
Segmentation

Extraction de caractéristiques



Un histogramme
par région de
motifs binaires locaux (LBP)

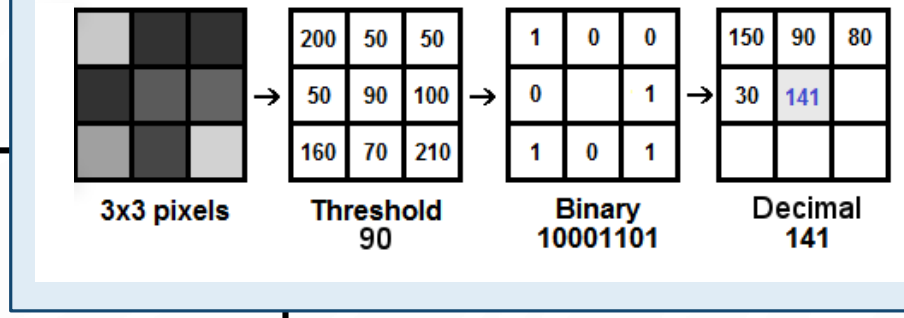
Concaténation

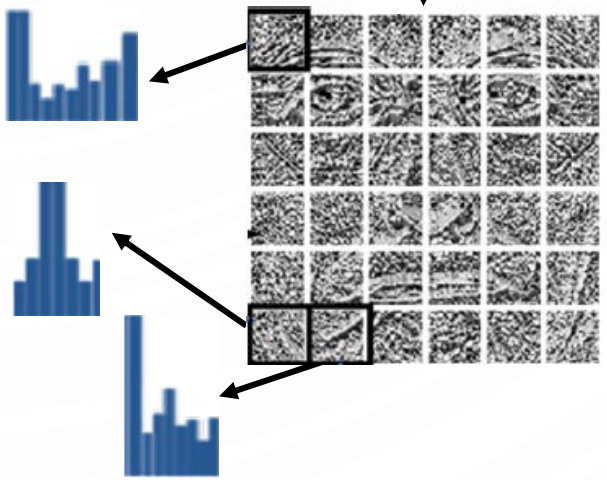


Modèle final
(template)

LOCAL BINARY PATTERNS HISTOGRAMS

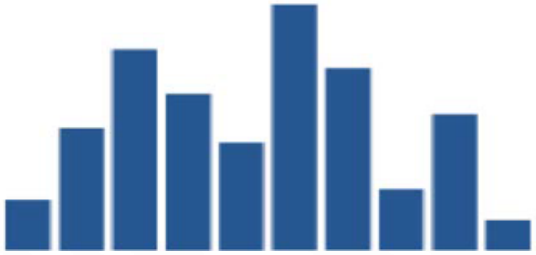
Segmentation





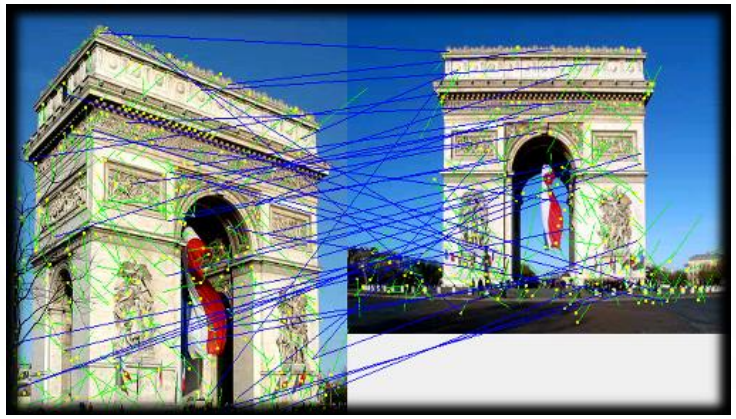
Un histogramme par région de motifs binaires locaux (LBP)

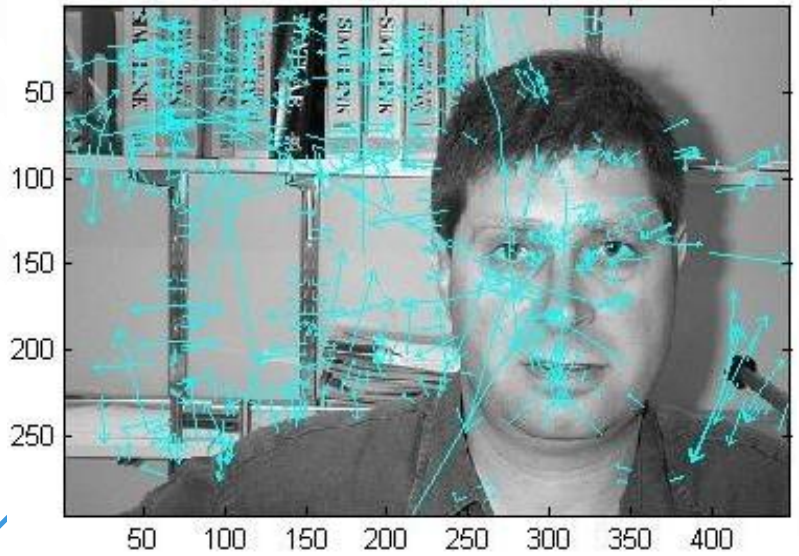
Concaténation

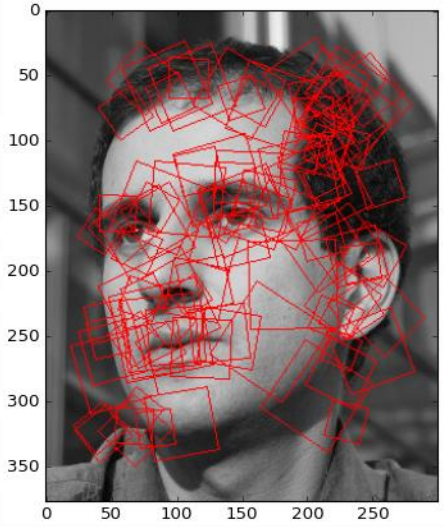


Modèle final (template)

SIFT/SURF

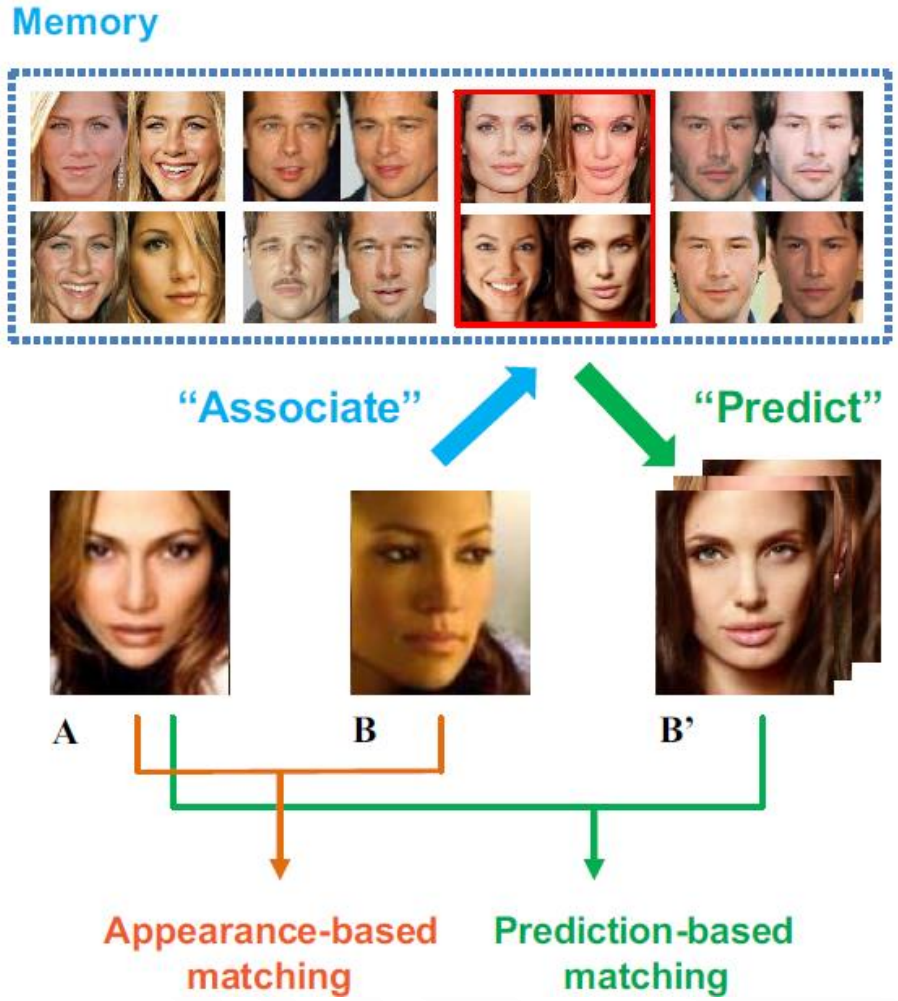




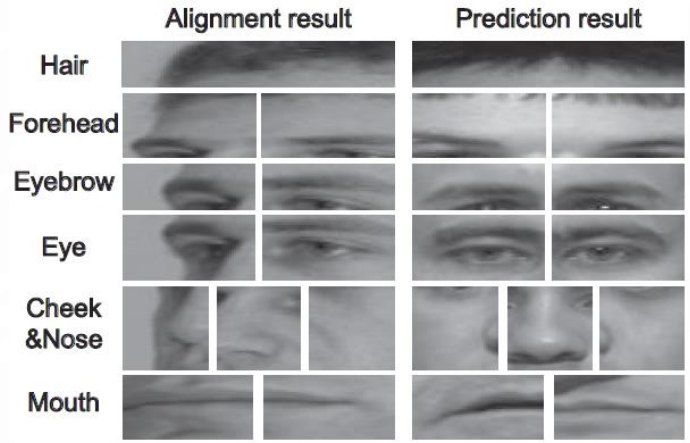


- But : Détecter et identifier les éléments similaires entre différentes images numériques
- Informations numériques dérivées de l'analyse locale d'une image
- Caractérisent le contenu visuel de cette image de la façon la plus **indépendante** possible **de l'échelle, du cadrage, de l'angle d'observation et de l'exposition**
- 2 photographies très différentes = descripteurs très différents eux aussi (pouvoir discriminant)
- SIFT : protégé aux États-Unis par un brevet détenu par l'université de la Colombie-Britannique

APPEARANCE vs PREDICTION BASED MATCHING



- Différentes prises de vue (pose, expression, luminosité…)
- Méthodes basées :
  - Apparence : comparaison directe
  - Prédiction : Association avec identité générique similaire
- Généralement : éléments du visage (pas visage en entier)



Yin, Q., Tang, X., & Sun, J. (2011). An associate-predict model for face recognition.

DEEPFACE DEEP NEURAL NETWORK

- Entrainé sur 4 millions d'images mises en ligne par les utilisateurs de Facebook
- Très grande efficacité (taux de précision : 97,25%)
- Etapes :
  - Détection du visage dans l'image
  - Alignement du visage détecté
  - Représentation de l'image au travers du CNN
  - Classification de l'image à l'aide de vecteurs caractéristiques (classifieur)

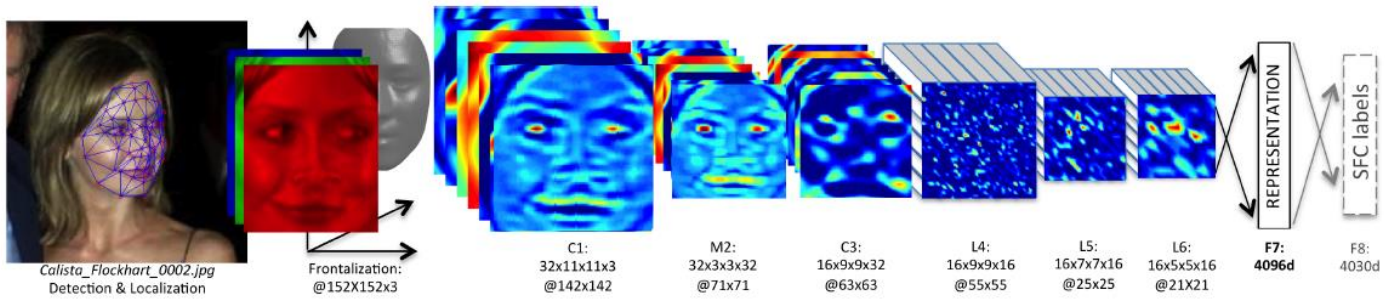


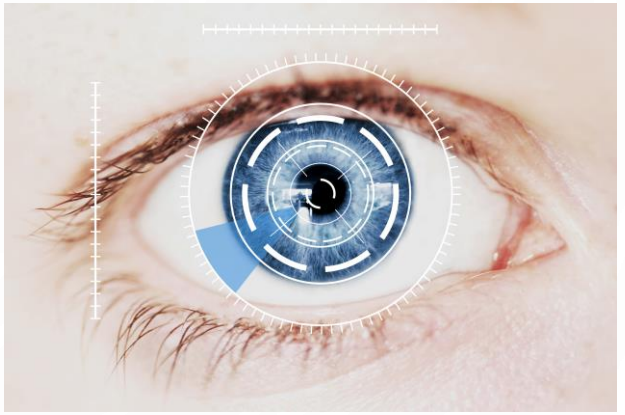
Figure 2. **Outline of the *DeepFace* architecture**. A front-end of a single convolution-pooling-convolution filtering on the rectified input, followed by three locally-connected layers and two fully-connected layers. Colors illustrate feature maps produced at each layer. The net includes more than 120 million parameters, where more than 95% come from the local and fully connected layers.

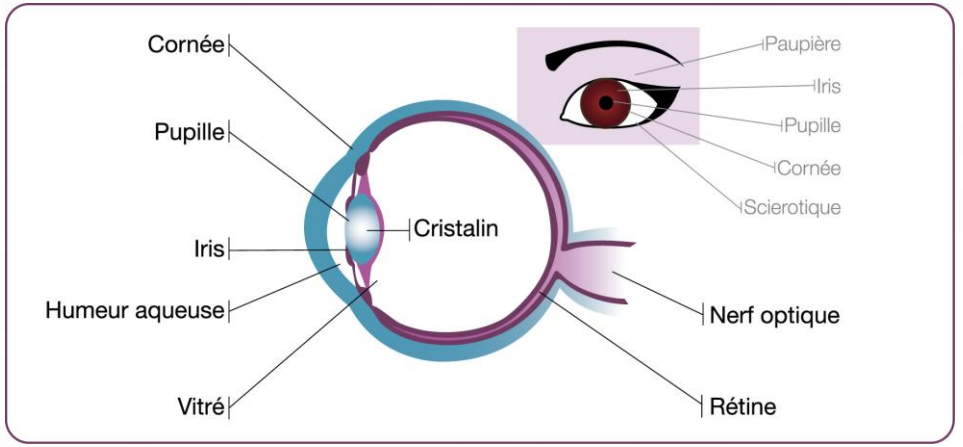
Facebook AI Research - DeepFace

PROBLÈMES

RECONNAISSANCE DE L'IRIS

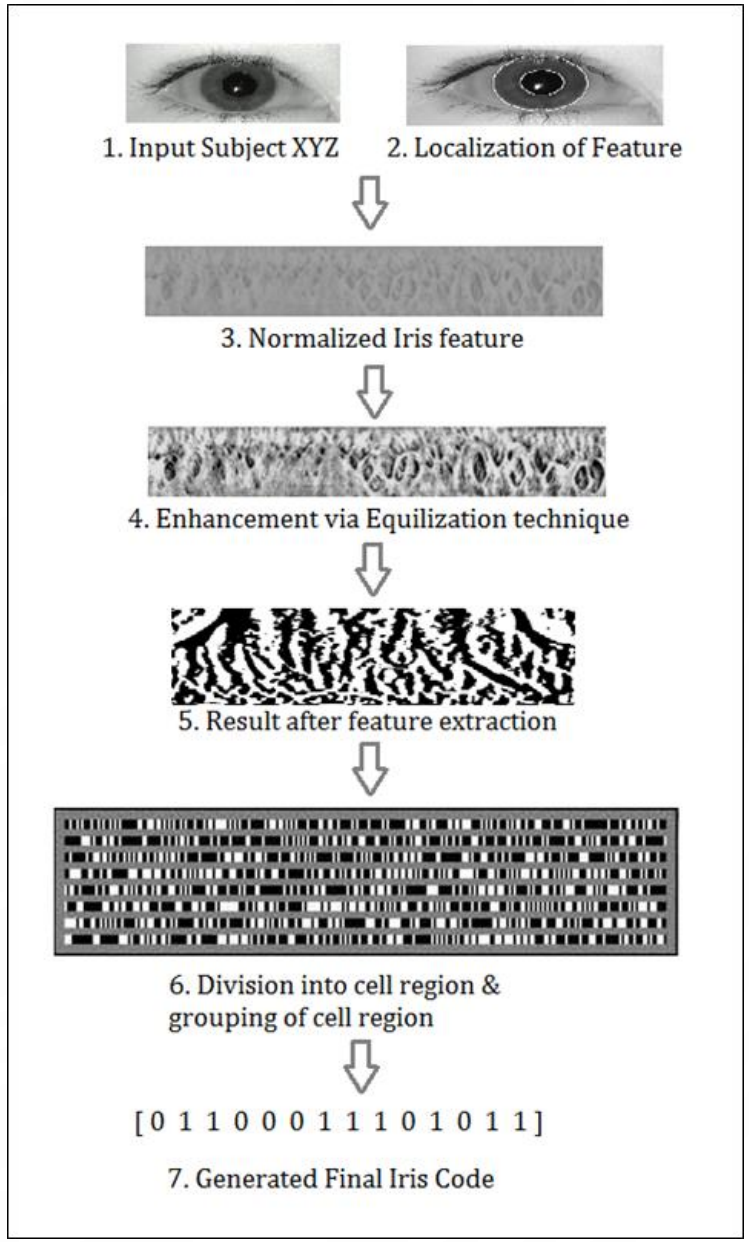
- Images acquises avec proche infrarouge
- Seulement la structure (ou motif) est utilisée (pas la couleur) :
  - Collerette autour de la pupille
  - Taches pigmentaires (taches de rousseur ou les grains de beauté)
  - Cryptes (ce sont de petits creux)
  - Couronne ciliaire (enchevêtrement de tubes fins formant un petit renflement)
  - Sillons ou pupille contrôlés suivant leur taille
- A ne pas confondre avec :
  - La rétine
  - Les veines sur les yeux
  - La cornée



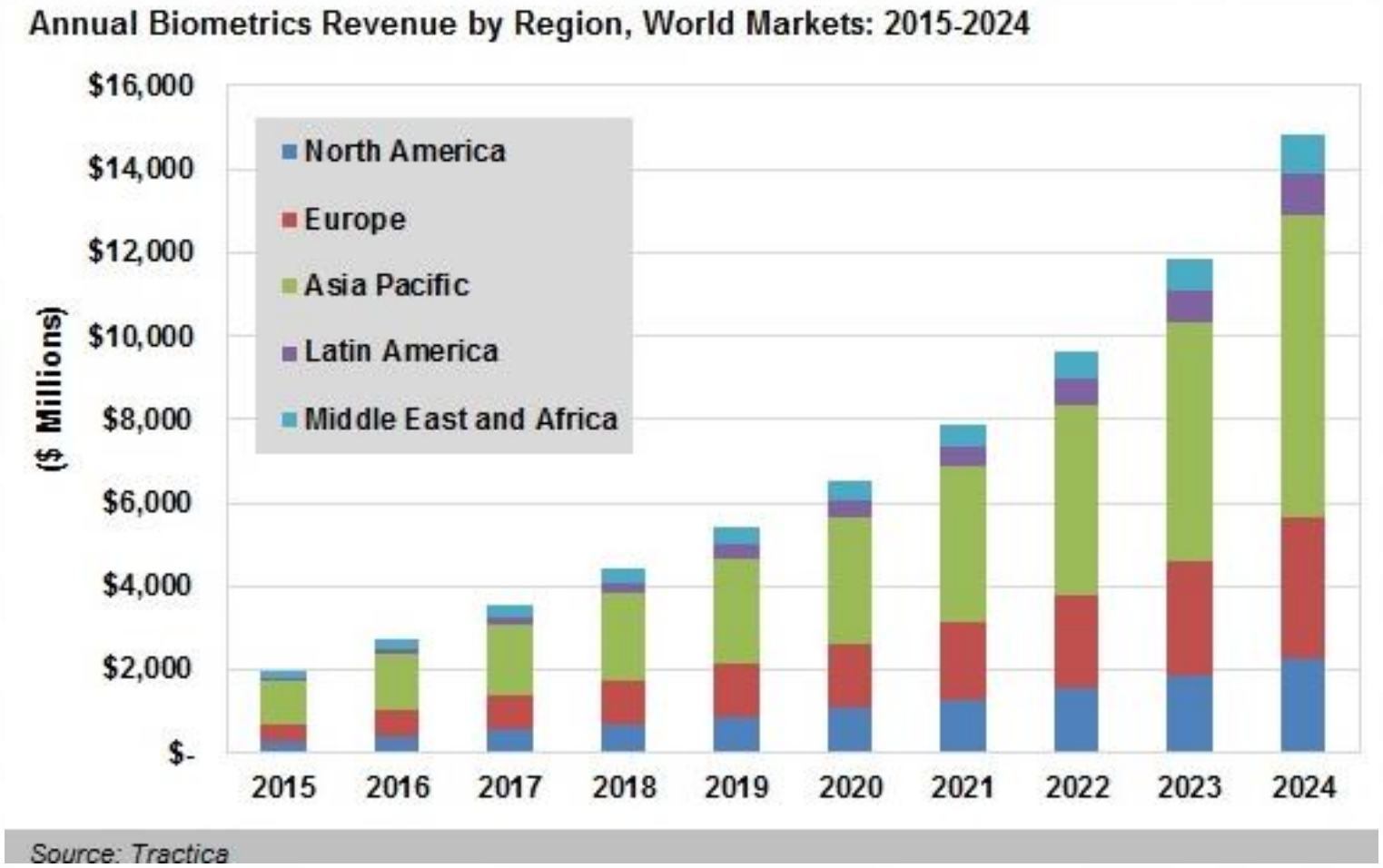


RECONNAISSANCE DE L'IRIS

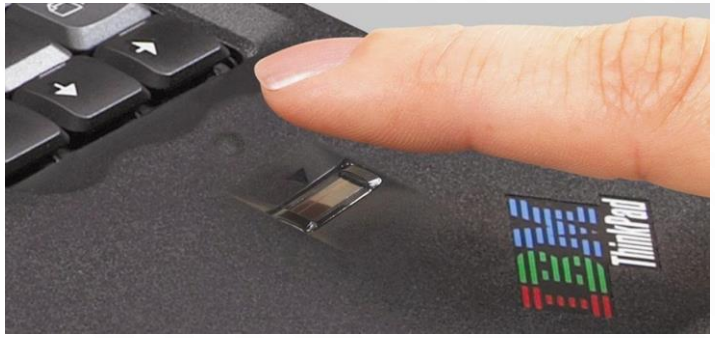
- Algorithme du Pr. John Daugman
  - Structure = iris code
  - Très bonnes performances
- Problème : acquisition
  - Cible en mouvement
  - Beaucoup de reflets
  - Trop foncé difficile à détecter
  - Paupière fermée
  - Lentilles



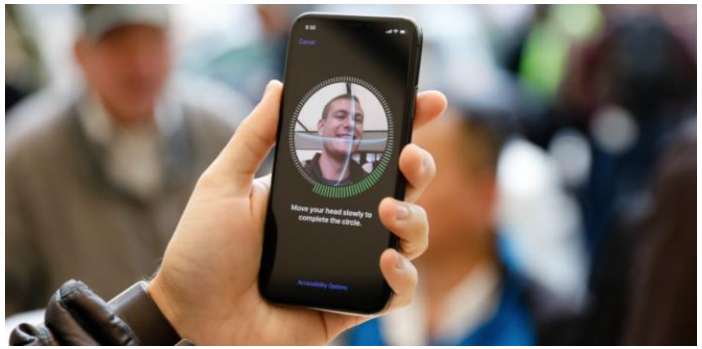
MARCHÉ DE LA BIOMÉTRIE



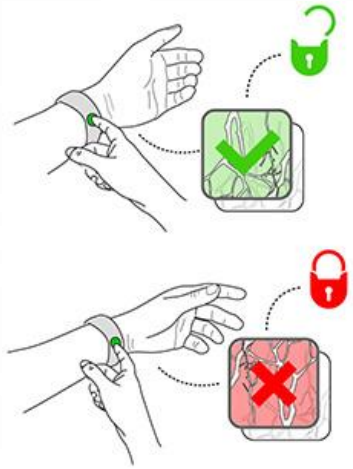
ORDINATEURS ET TÉLÉPHONES

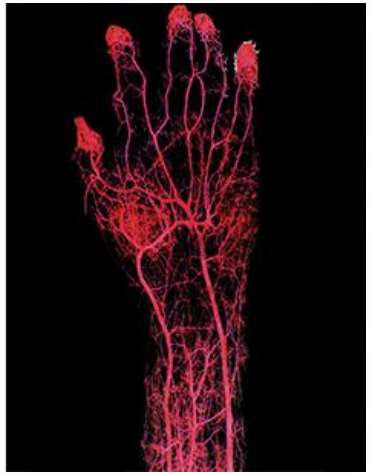


- Capteurs d'empreintes :
  - Zone où poser le doigt en façade
    - Premiers capteurs
  - Zone où faire glisser le doigt en façade
    - Les plus utilisés
  - Capteur sous l'écran
    - En cours de développement
    - Plutôt lent
- Reconnaissance faciale de plus en plus utilisée



AUTRES APPLICATIONS



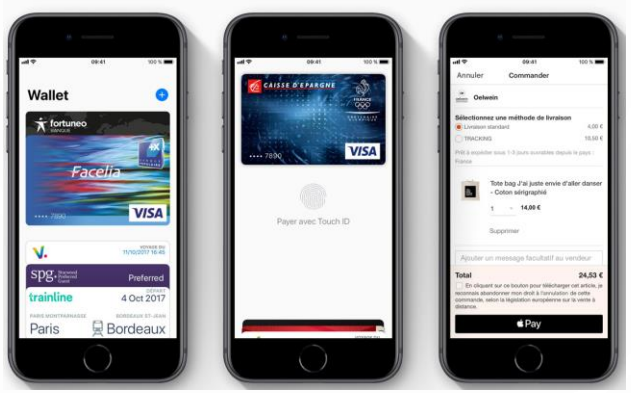


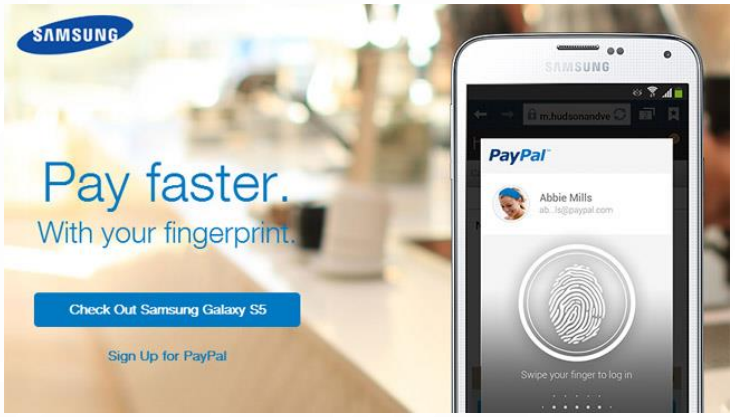
AUTRES APPLICATIONS

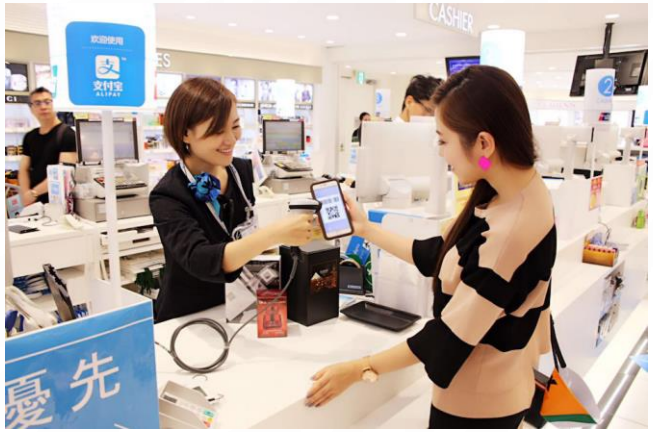
AUTRES APPLICATIONS

E-PAIEMENT

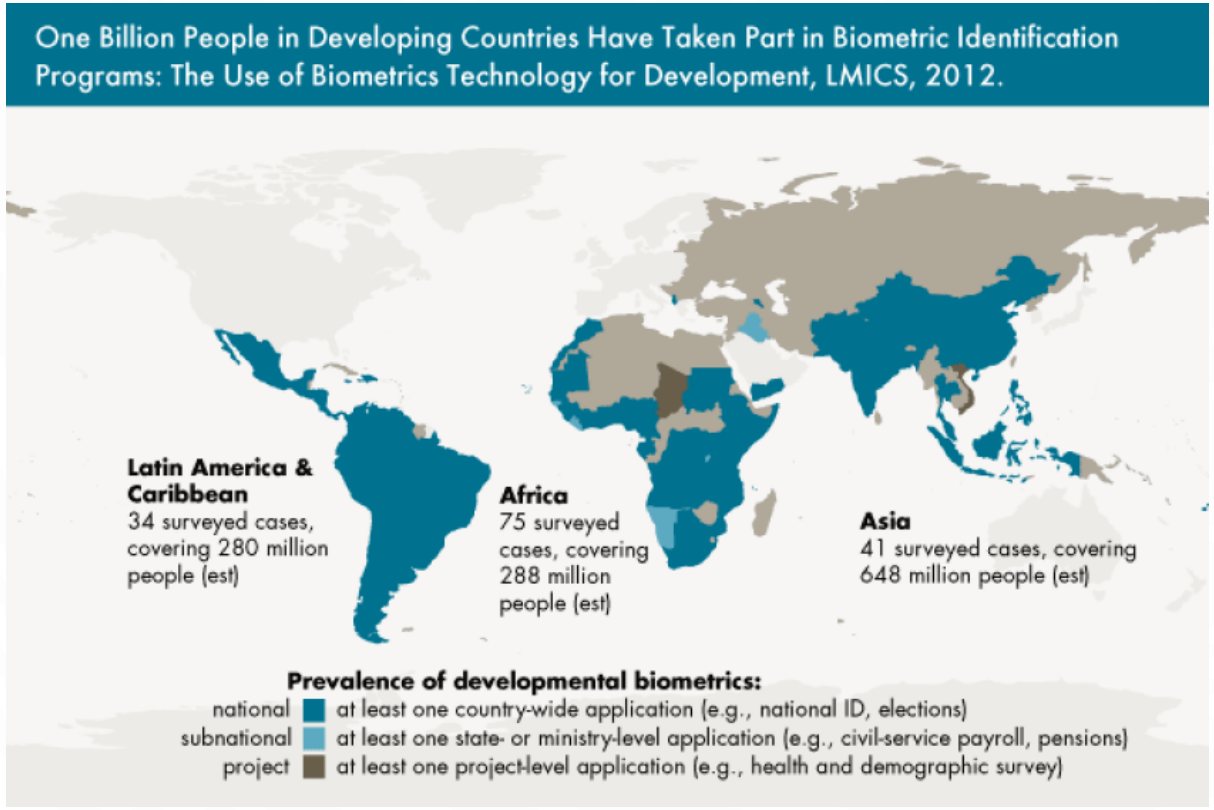
- Payer avec son empreinte digitale
- Pay-by-touch (2008, US)
- Apple Pay (2014, iPhone 6)
- Alipay/WeChat Pay (2015, Chine)
- Paylib/Samsung Pay/Google Pay (2017)







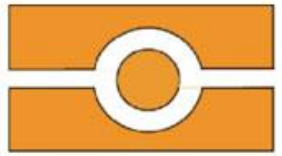
APPLICATIONS GOUVERNEMENTALES



DOCUMENTS OFFICIELS

- Puce sans-contact dans le passeport avec données écrites
- Passeport optique → électronique → biométrique
- En France :
  - Photographie numérisée
  - 2 empreintes digitales
  - Application DELPHINE
- Données biométriques des voyageurs collectées
  - Lors de la demande de visa
  - Lors de leur entrée sur le territoire

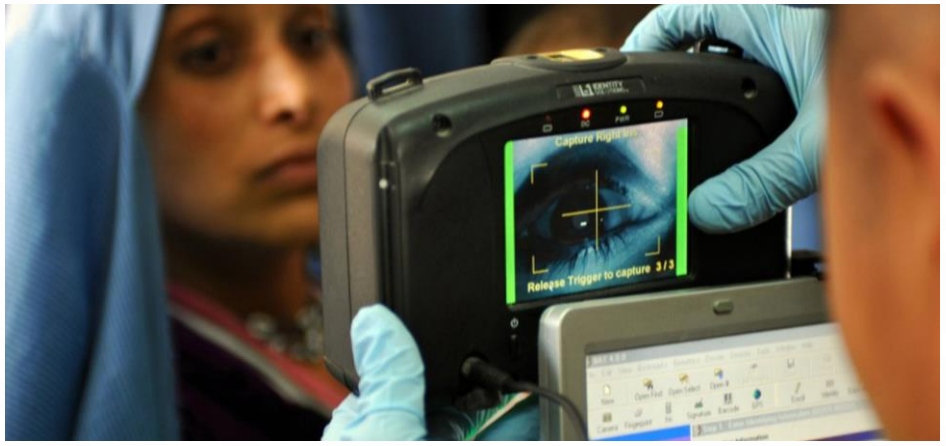
The below is the universal RFID e-passport logo which is being used to identify passport locations which require e-passport scanning.



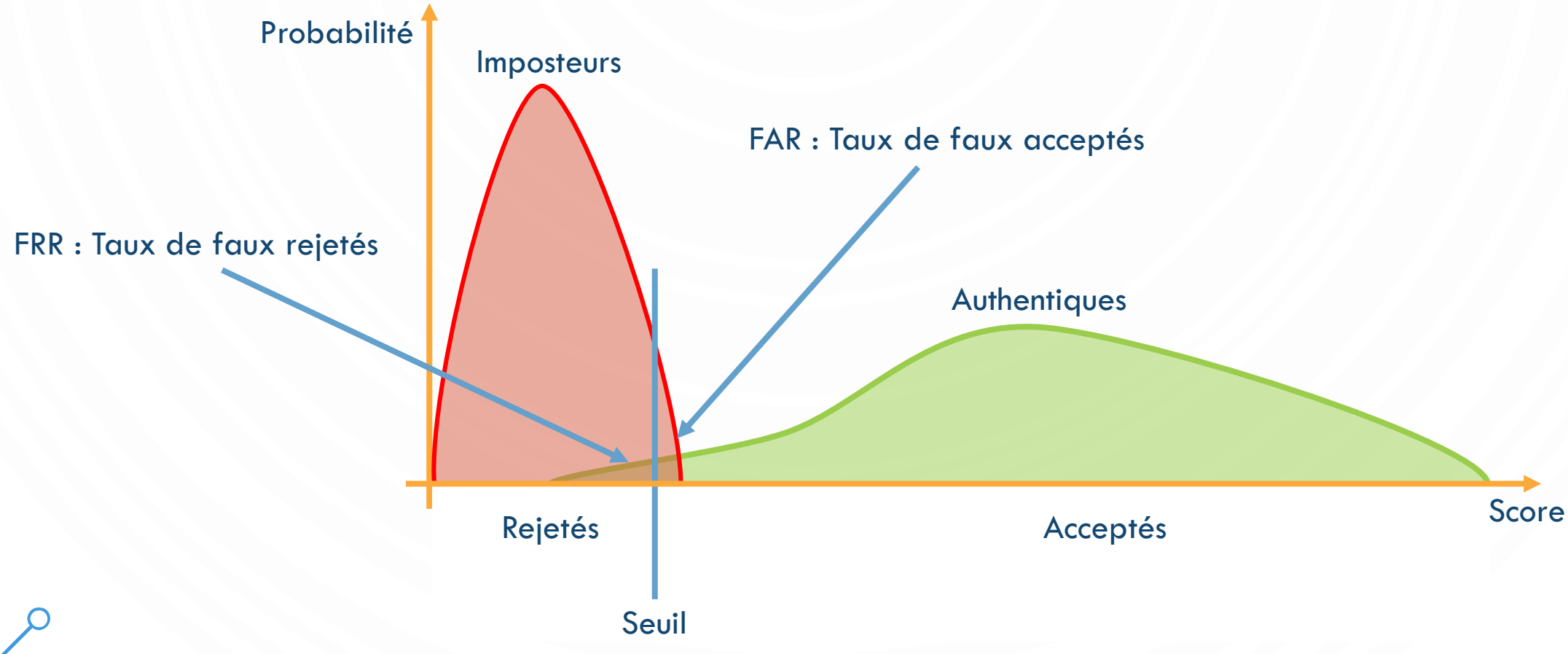
As of 2008, 45 countries are using e-passports, and more are expected to follow suit.

FORCES DE L'ORDRE

- Bases de données biométriques :
  - USA/FBI : 77 millions d'empreintes digitales (2014)
  - Autralie : 6,3 millions d'empreintes digitales, 837000 échantillons d'ADN (2013)
  - Grande-Bretagne : 5,5 millions d'empreintes digitales, 3,4 millions d'échantillons d'ADN
  - France : 4,8 millions d'empreintes digitales, 2,5 millions d'échantillons d'ADN
- Essor des achats de matériel biométrique + efficacité

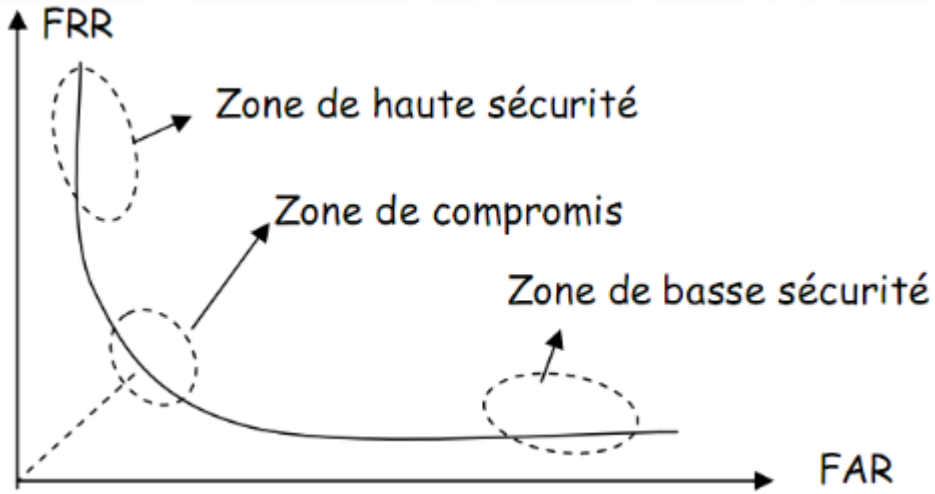


PERFORMANCE



PERFORMANCE

- Compromis entre le FAR et le FRR
- FAR bas = Peu de succès d'attaque
  - Moins tolérant aux attaques avec des données proches
  - Moins tolérant lors de l'authentification (même si légitime)
  - Augmente le FRR
- FRR bas = Facile à utiliser
  - Utilisateur légitime toujours reconnu
  - Plus tolérant si données altérées
  - Plus facile à attaquer
  - Augmente le FAR
- Haute sécurité = plus d'erreurs
- Sécurité préférée à confort d'utilisation
  - FRR = 1%
  - FAR ≤ 0,1%

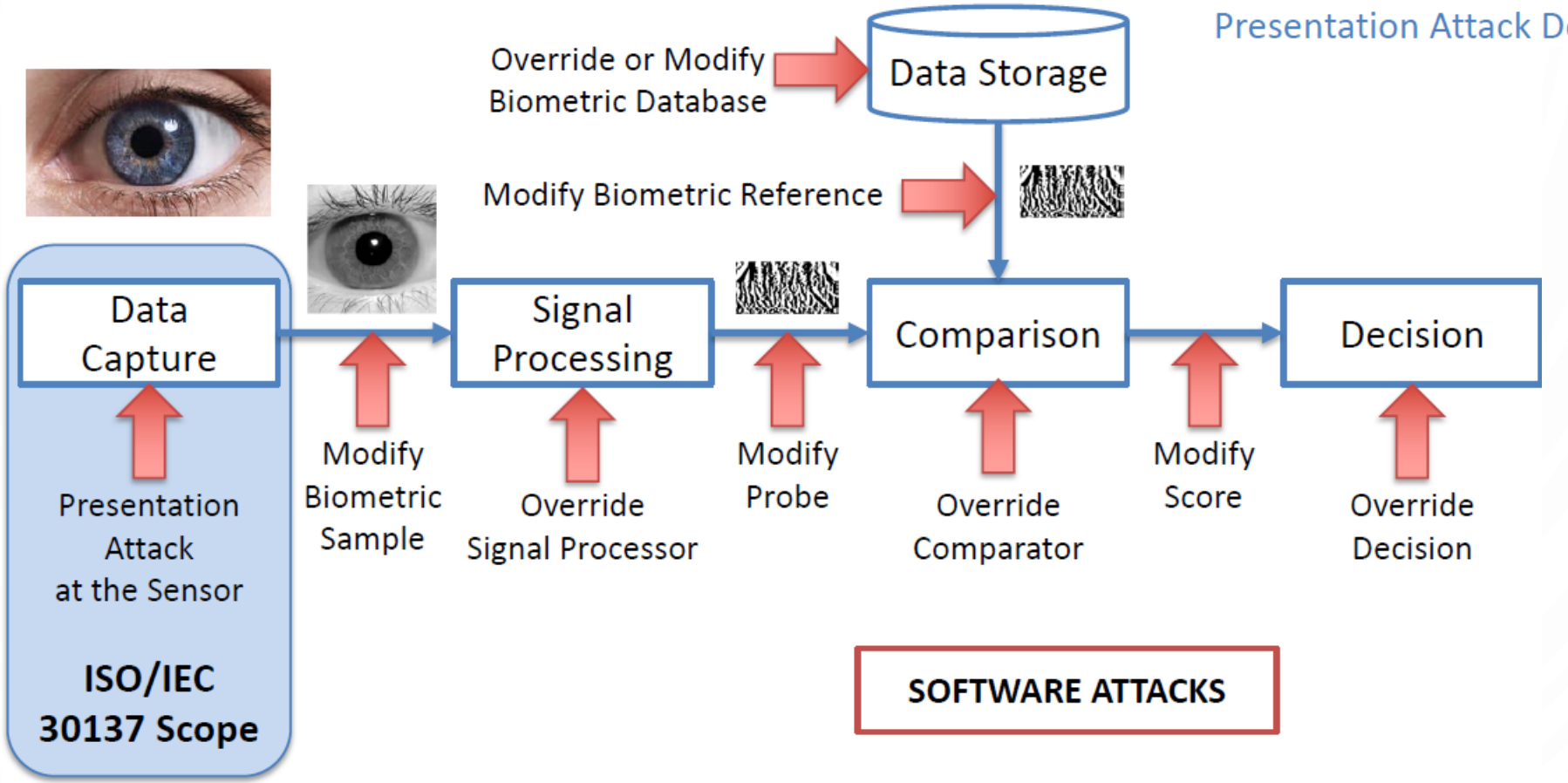


USURPATION DE TRAITS BIOMÉTRIQUES

- Information biométrique souvent publique
- Très simple à acquérir, surtout grâce avec Internet
  - ADN : juste besoin de résidus organiques
  - Visage : une simple photo
  - Iris : photo haute résolution
  - Empreintes digitales : empreintes laissées sur une surface
  - Voix : enregistrement

VULNÉRABILITÉS À ≠ NIVEAUX

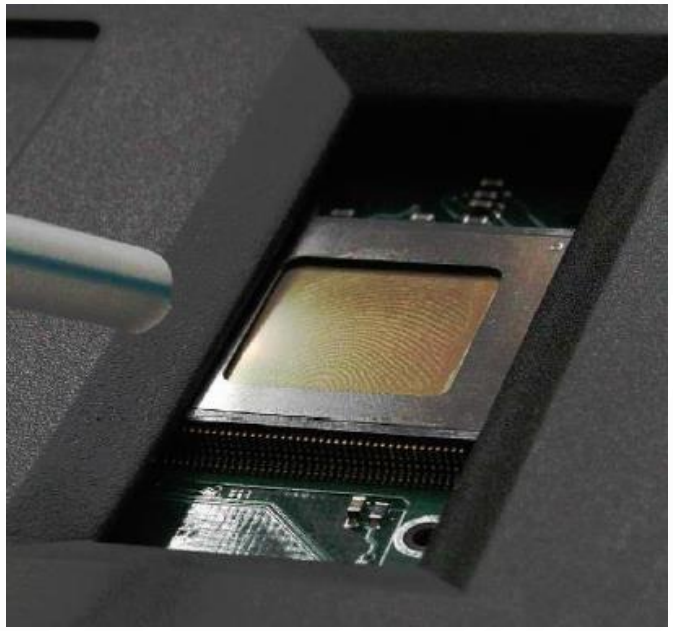
[ISO/IEC 30137 on Biometric Presentation Attack Detection]



ATTAQUES PAR PRÉSENTATION

- **Définition** : Présentation à un sous-système de capture de traits biométriques avec l'objectif d'interférer avec le fonctionnement du système biométrique
- **Imposteur** : L'attaquant tente de correspondre aux traits d'une personne enrôlée dans le système
- **« Correcteur » d'identité** : L'attaquant tente d'éviter d'être apparié à sa propre référence biométrique (par exemple, pour échapper à une entrée de la liste noire)

USURPATION D'EMPREINTES



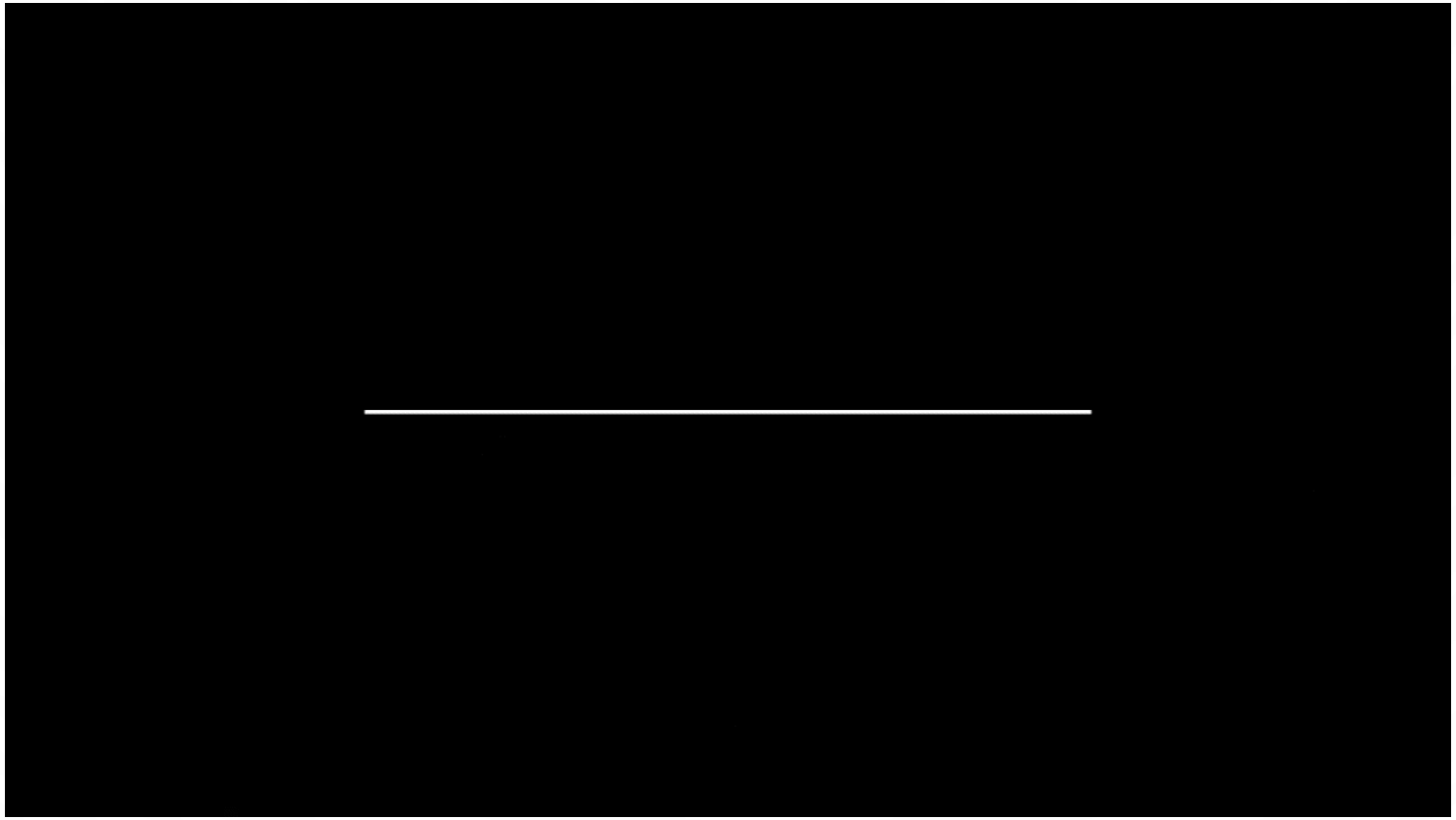
- Présence de vie difficile à détecter :
  - Un doigt coupé peut être maintenu en vie (chirurgie)
  - Greffe complète d'un main (et donc des empreintes !)
- Différents niveaux :
  - Sans effort : empreinte laissée sur le capteur
  - Faux/copies : photocopie de l'empreinte, faux doigt en gélatine ou en latex, fine couche avec l'empreinte collée sur le doigt
  - Doigt original : coupé, en amenant une personne décédée…

USURPATION D'EMPREINTES

- Difficile de fabriquer un faux doigt/empreintes ?
  - Avec coopération :
    - Facile de fabriquer un moule
    - Informations sur internet et dans des articles
  - D'après une empreinte :
    - Difficile de savoir quel doigt c'est
    - Besoin d'acquérir une bonne image
  - Différents matériaux possibles (gélatine, silicone, gomme, colle, latex…)

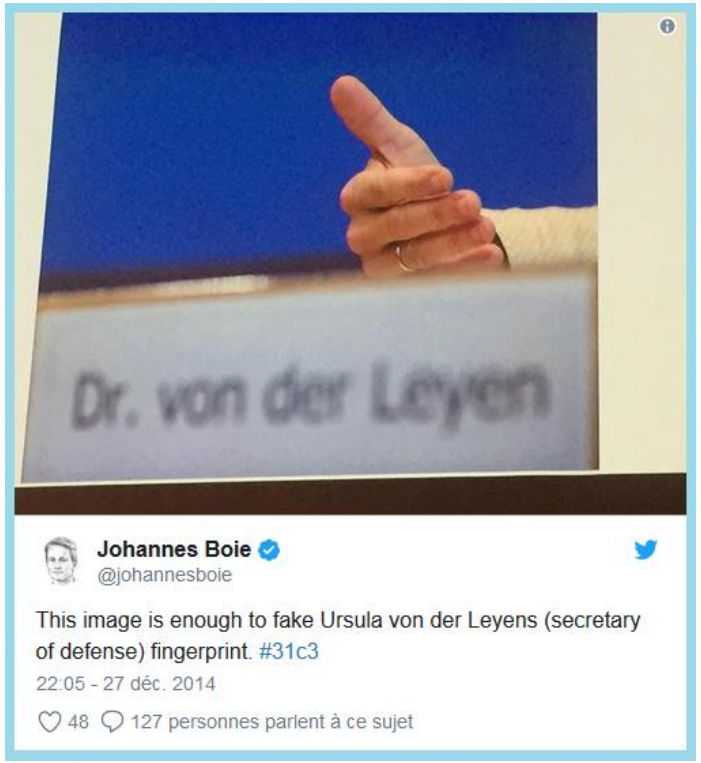
USURPATION D'EMPREINTES

- 2013 : Piratage du système TouchID de l'iPhone 5s, puis 6
  - Par le German Chaos Computer Club



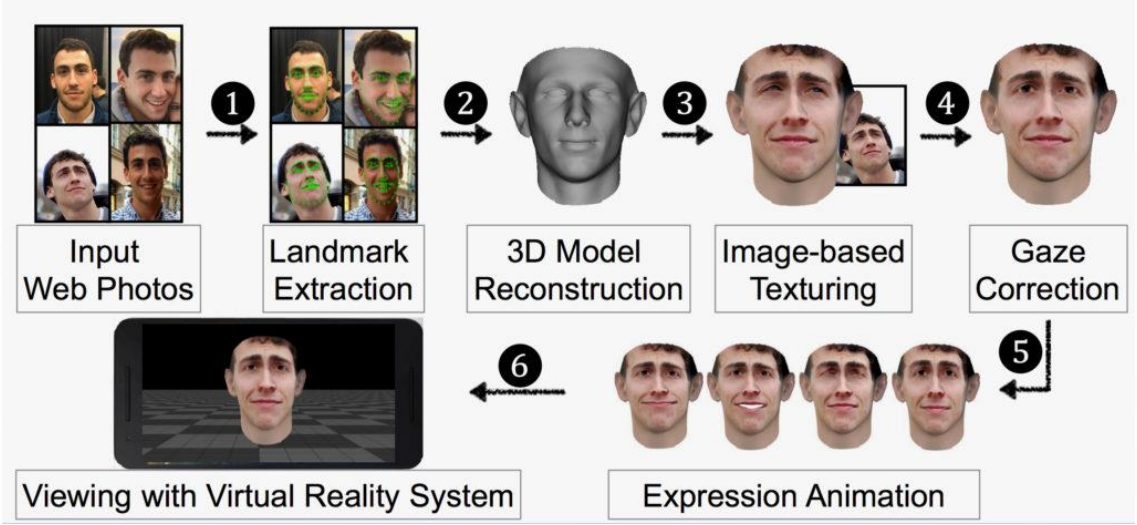
USURPATION D'EMPREINTES

- 2017 : Vol d'empreintes d'après les selfies ?
  - Mise en garde du Pr. Isao Echizu (National Institute of Informatics, Japon)
  - En particulier, « V de la victoire » (index et majeur)
  - Facile si :
    - Distance réduite avec l'appareil (< 3 mètres)
    - Bonnes conditions de luminosité (pleine lumière)
    - Bon angle
  - Plus difficile si filtres utilisés
  - Contre-mesures :
    - Film transparent à base d'oxyde de titane pour cacher ses empreintes sur les photos
    - Résolution plus élevée sur les capteurs d'empreintes
    - Sensibilité aux pulsations cardiaques et à la pression sanguine



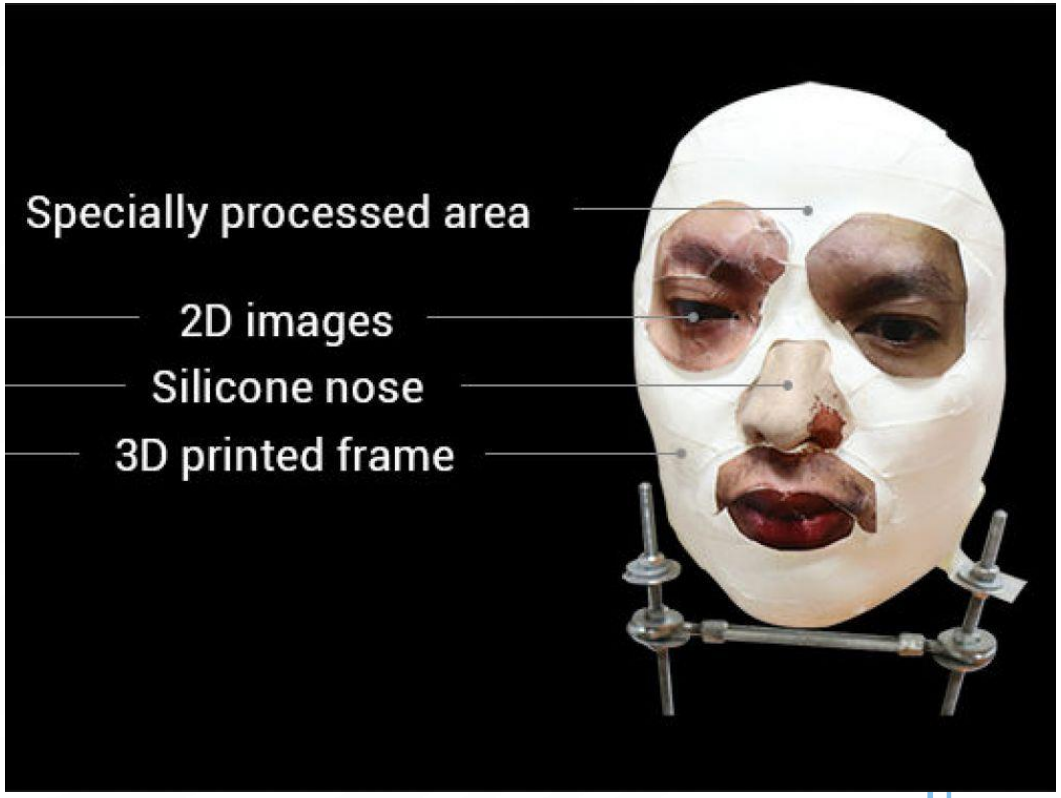
USURPATION DE VISAGE

- 2016 : Systèmes de reconnaissance faciale déjoués
  - Chercheurs de l'Université de Chapel Hill (CA, USA)
  - Photographies de 20 bénévoles, récoltées sur les réseaux sociaux
  - Construction d'un modèle 3D du visage
  - Amélioration du rendu, ajout d'expressions…
  - Intégration dans téléphone (réalité virtuelle)
  - Système qui déjoue 4/5 systèmes biométriques testés
  - 55 à 85% de réussite
  - Contre-mesures :
    - Impossible de reproduire les signaux humains
    - Caméra infra-rouge
    - Projecteur de lumière structurée



USURPATION DU VISAGE

- 2017 : Piratage du système Face ID de l'iPhone X
  - Par Bkav Corporation (Vietnam)

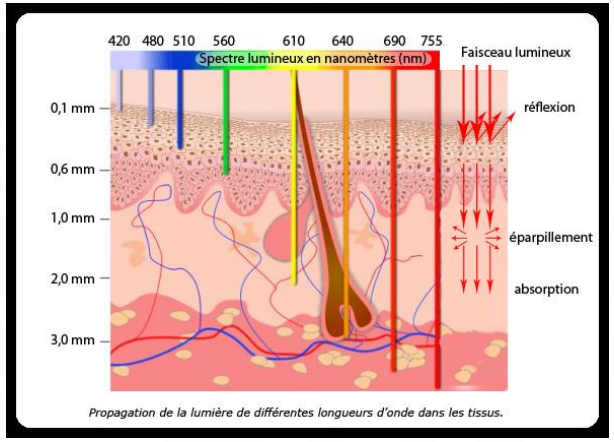


USURPATION D'IRIS

- 2017 : Piratage du système d'identification par lecture de l'iris du smartphone Galaxy S8 de Samsung
  - (Toujours) par le German Chaos Computer Club

DÉTECTION DU VIVANT

- Détection de la chaleur
- Détection des battements du cœur
- Oxymètre de pouls (rythme cardiaque + oxygène dans le sang)
- Distorsion de la peau
- Absorption de la lumière par la peau
- Clignement des yeux
- Micro-mouvements
- Texture du visage (photo vs réelle)
- Changement de la pupille suivant la lumière (réflexe photomoteur)
- Différence entre un globe oculaire vivant ou mort détectable par DL



Propagation de la lumière de différentes longueurs d'onde dans les tissus.

SYSTÈMES MULTI-BIOMÉTRIQUES

- Avantages
  - Meilleures performances
  - Robustesse accrue face aux défaillances des capteurs individuels
  - Diminution du nombre de cas où le système n'est pas en mesure de prendre une décision
  - Différents niveaux de sécurité
- Différents niveaux de fusion
  - Fusion des modalités biométriques
  - Fusion au niveau du score
  - Fusion au niveau de la décision

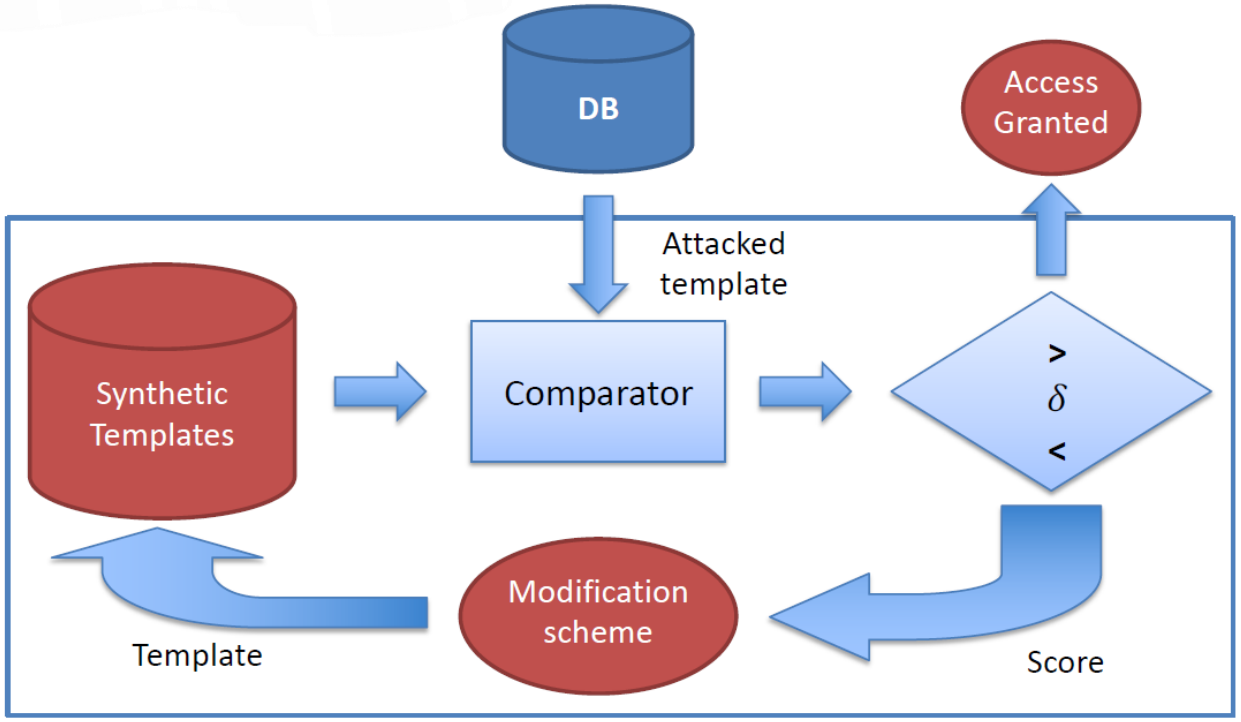
Peut être difficile à mettre en place **mais** réduit l'espace de stockage et meilleure sécurité

ATTAQUES HILL CLIMBING

- Le *hill-climbing* une méthode générale qui prend en entrée trois objets :
  - Une configuration
  - Une fonction qui pour chaque configuration donne un ensemble de configurations voisines,
  - Une fonction-objectif qui permet d'évaluer chaque configuration.
- A partir de la configuration initiale, évaluation des solutions voisines, et choix de la meilleure de celles-ci
- Recommencement de l'opération jusqu'à arriver à une position meilleure que les positions voisines (optimum local).

Wikipédia

ATTAQUES HILL CLIMBING

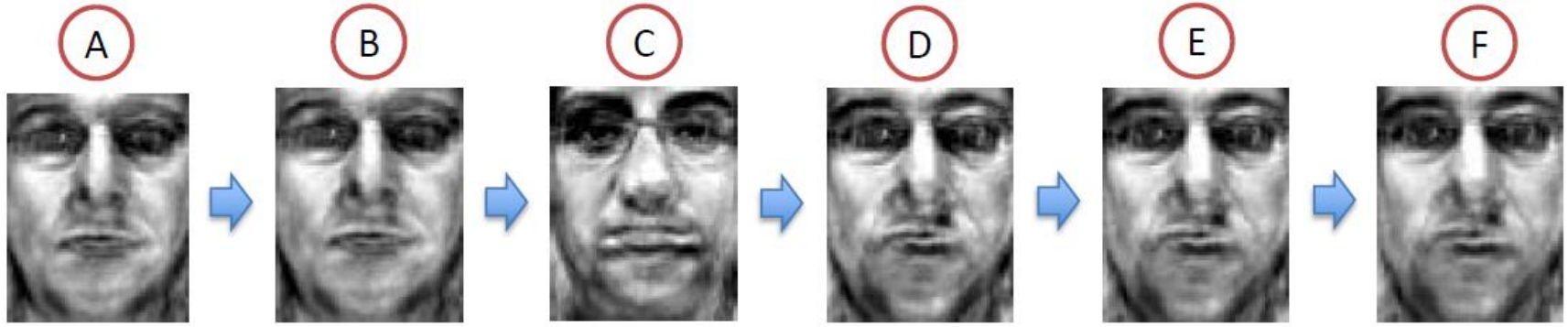


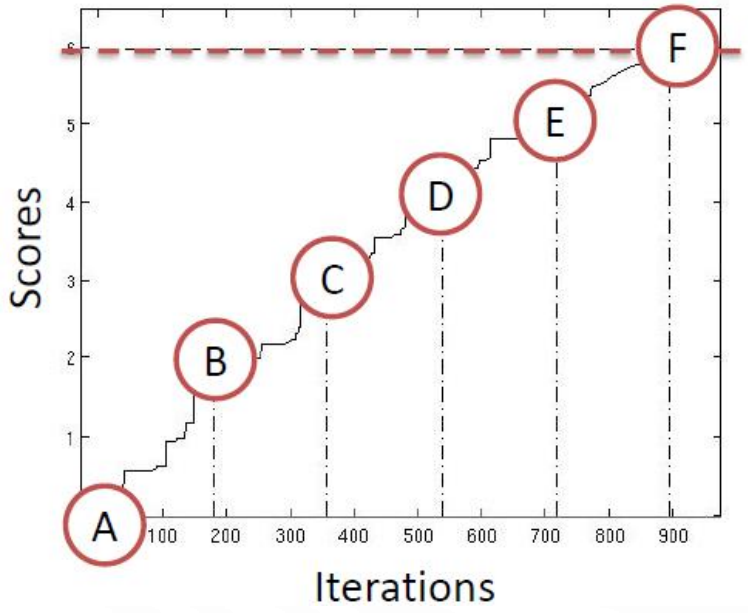
Dr. Marta Gomez-Barrero

- Attaques basées sur l'analyse du score
- Adaptation itérative du modèle synthétique
- Si le score **augmente** : on **retient** la modification
- Si le score **baisse** : on **rejette** la modification

Approximation du modèle pour déjouer le système **mais** pas reconstruction…

ATTAQUES HILL CLIMBING





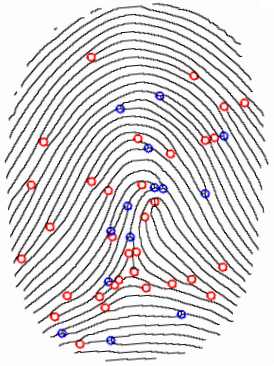
Verification Threshold

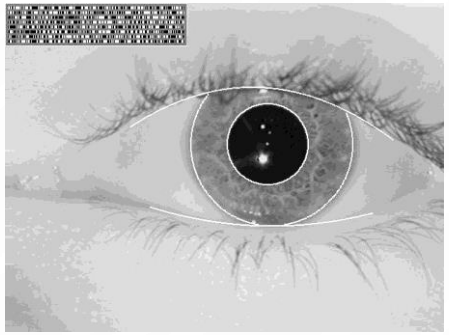
The attack was successful, and we only needed access to the scores

Target: Enrolled Sample

ATTAQUES D'INVERSION

- Croyance : Les modèles stockés ne révèlent aucune information sur les caractéristiques biométriques

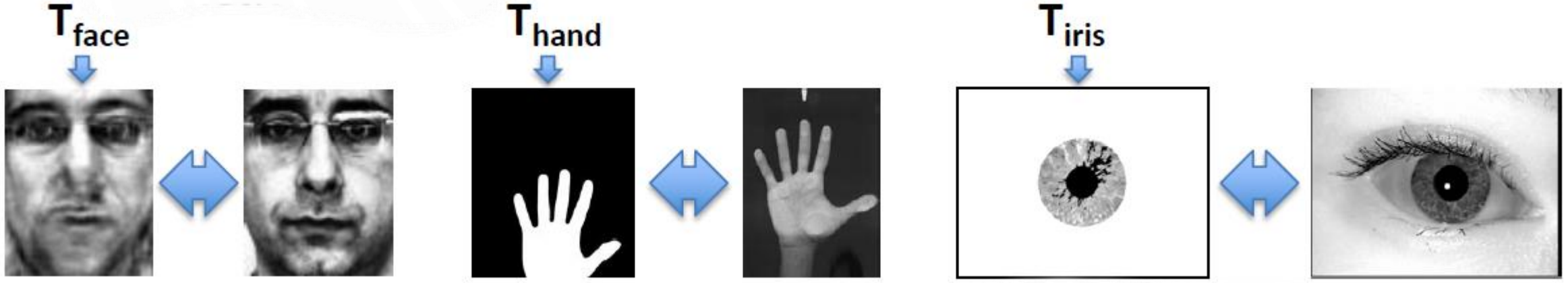




- C'est faux ! Des échantillons biométriques peuvent être retrouvés en analysant les modèles stockés de manière insécurisée…

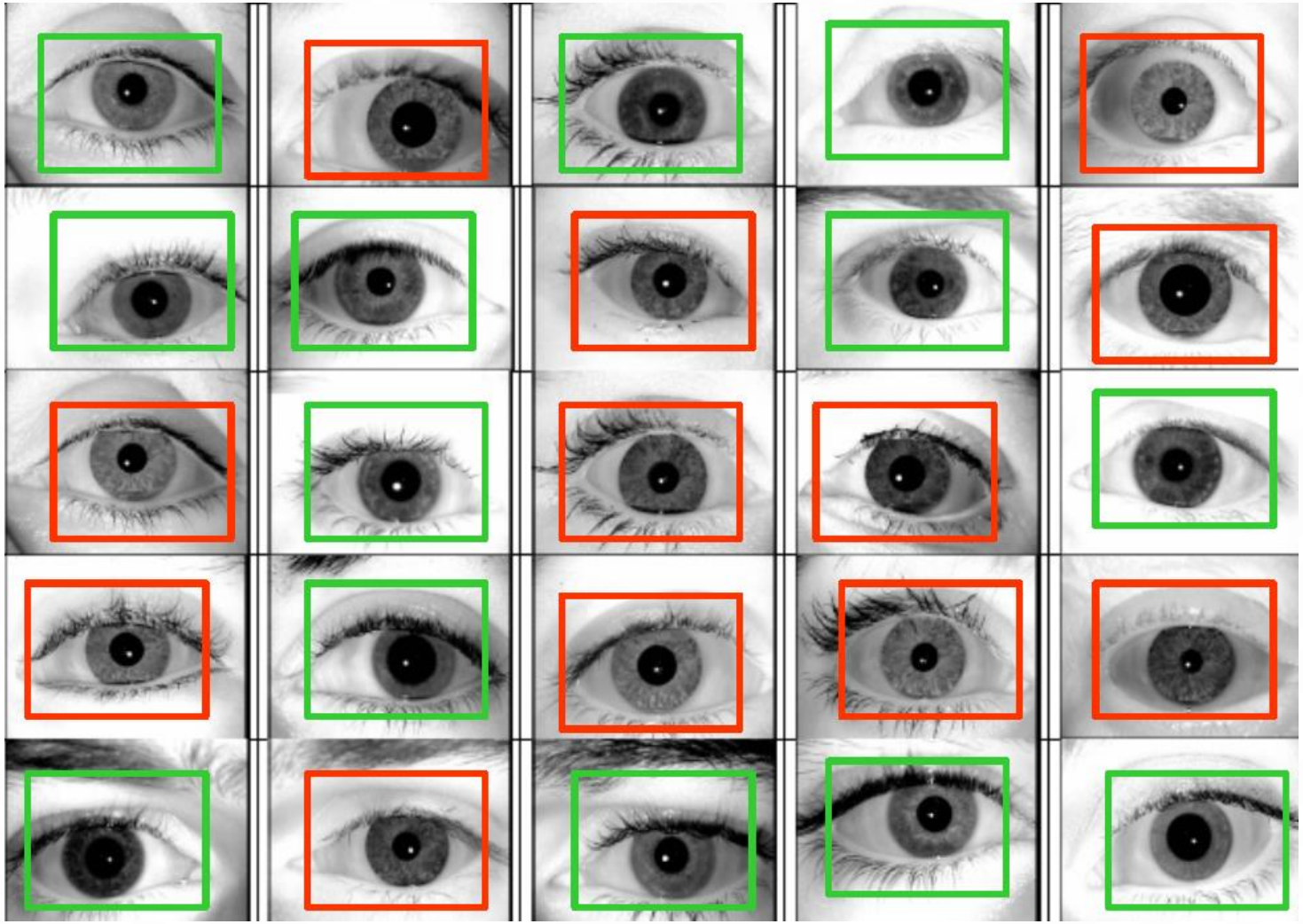
ATTAQUES D'INVERSION

- En utilisant les algorithmes précédents, basés sur le Hill Climbing, reconstruction des échantillons biométriques possible !



Gomez-Barrero, M., Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2012). Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm.
Gomez-Barrero, M., Galbally, J., Morales, A., Ferrer, M. A., Fierrez, J., & Ortega-Garcia, J. (2014). A novel hand reconstruction approach and its application to vulnerability assessment.

ATTAQUES D'INVERSION

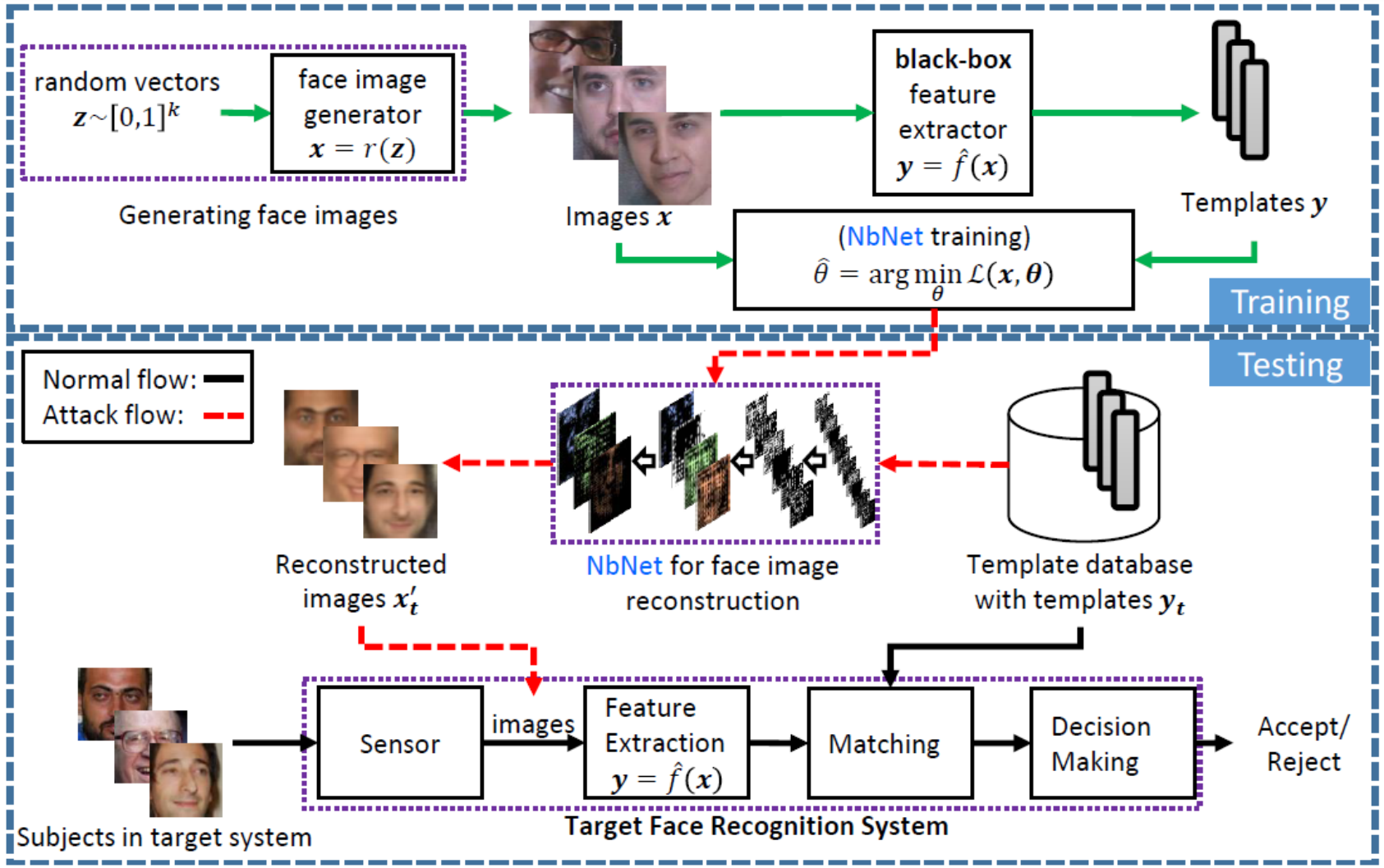


ATTAQUES D'INVERSION : DEEP LEARNING

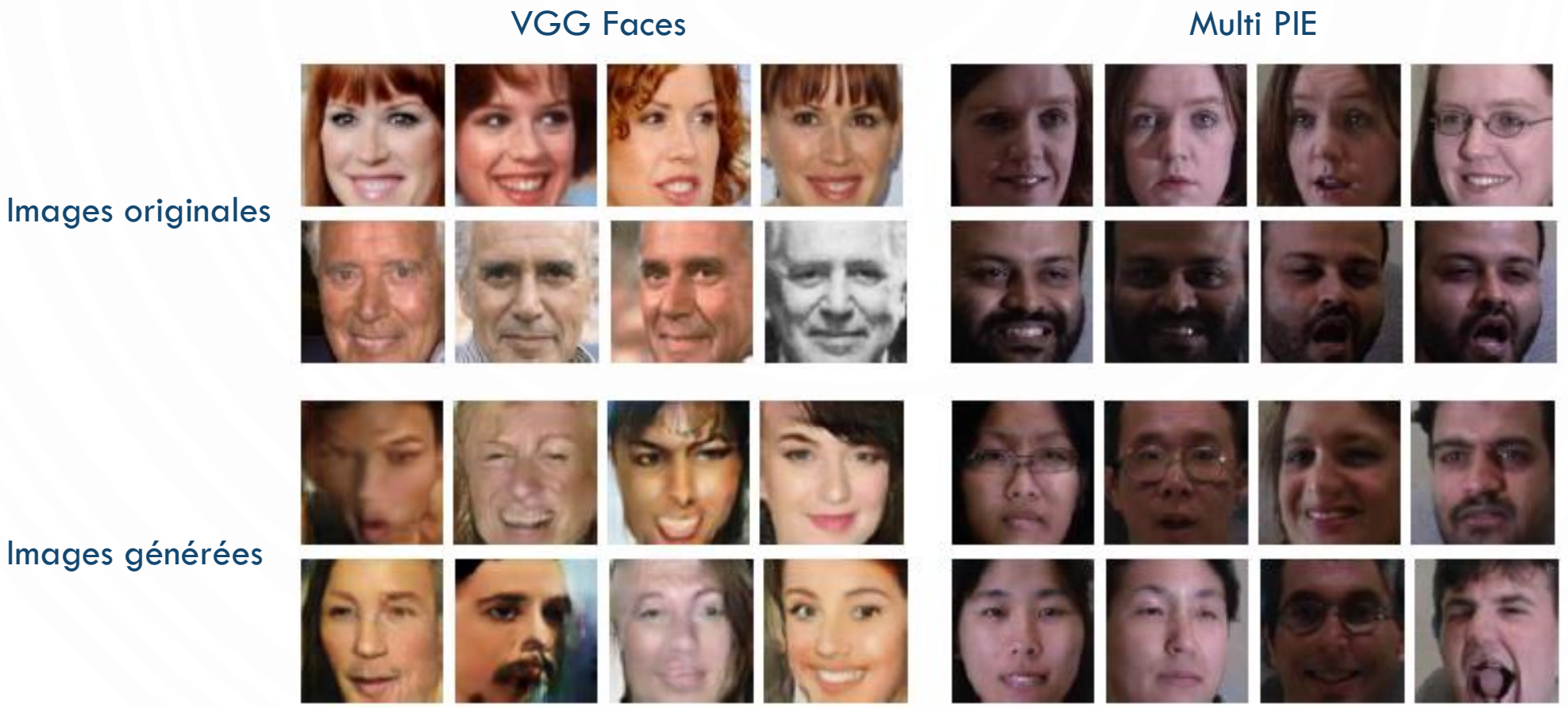
- Aussi vulnérable aux attaques d'inversion…
- Un réseau déconvolutionnel de « bon voisinage » (NbNet) peut être utilisé pour reconstruire les modèles de visages de FaceNet
- Taux de succès entre 73% et 95%, selon les bases d'images

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering.
Mai, G., Cao, K., Pong, C. Y., & Jain, A. K. (2018). On the Reconstruction of Face Images from Deep Face Templates.

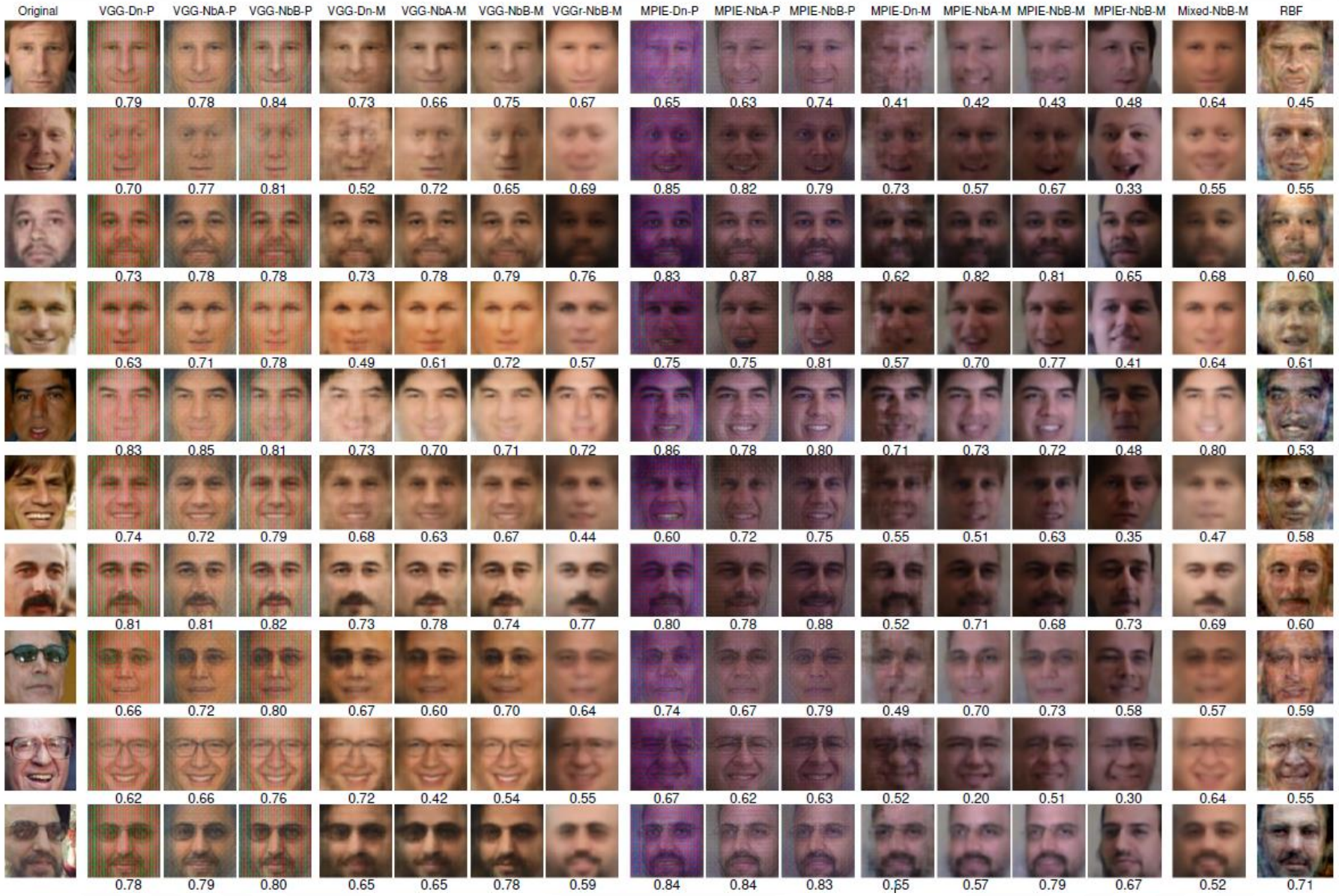
ATTAQUES D'INVERSION : DEEP LEARNING



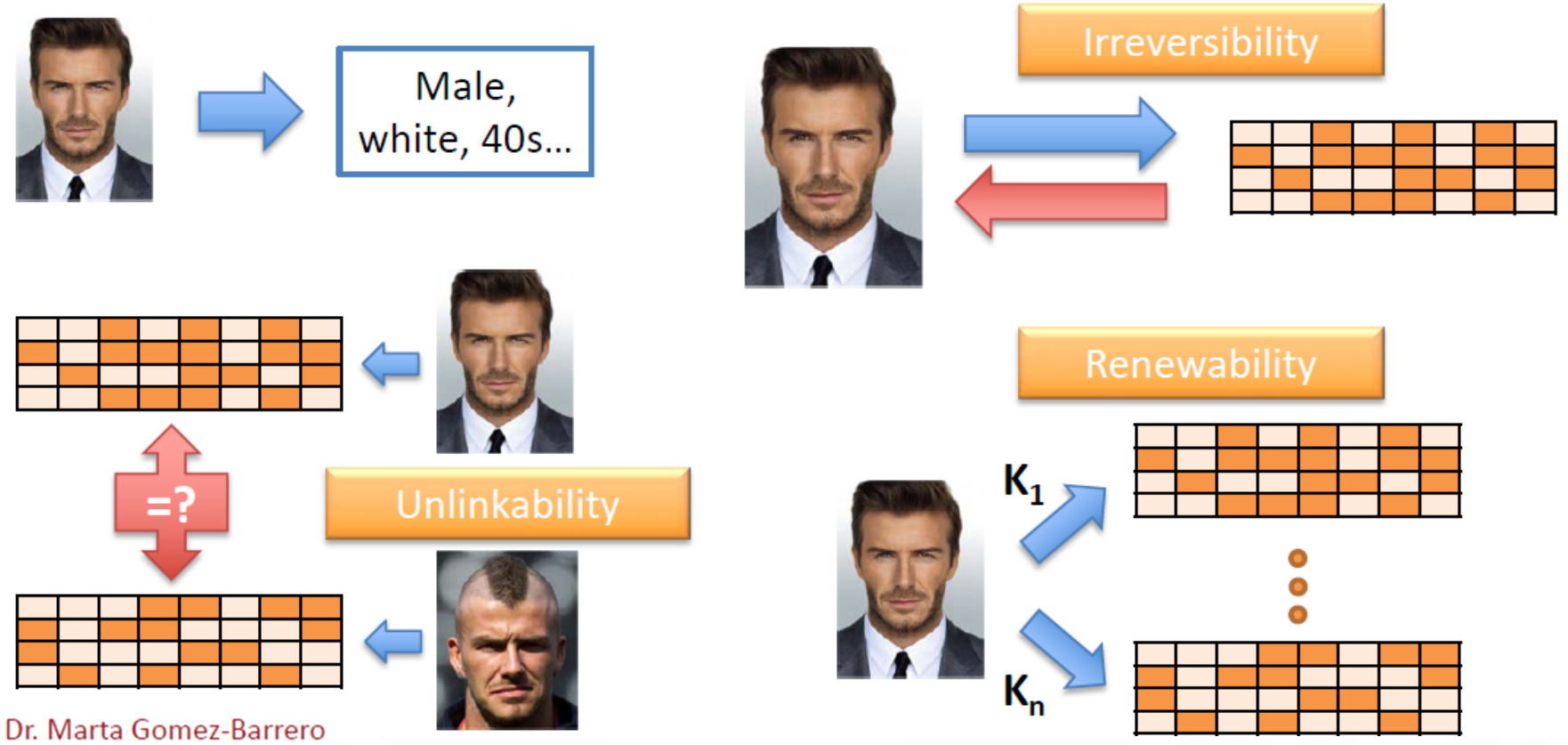
ATTAQUES D'INVERSION : DEEP LEARNING



ATTAQUES D'INVERSION : DEEP LEARNING



PROTECTION DES MODÈLES



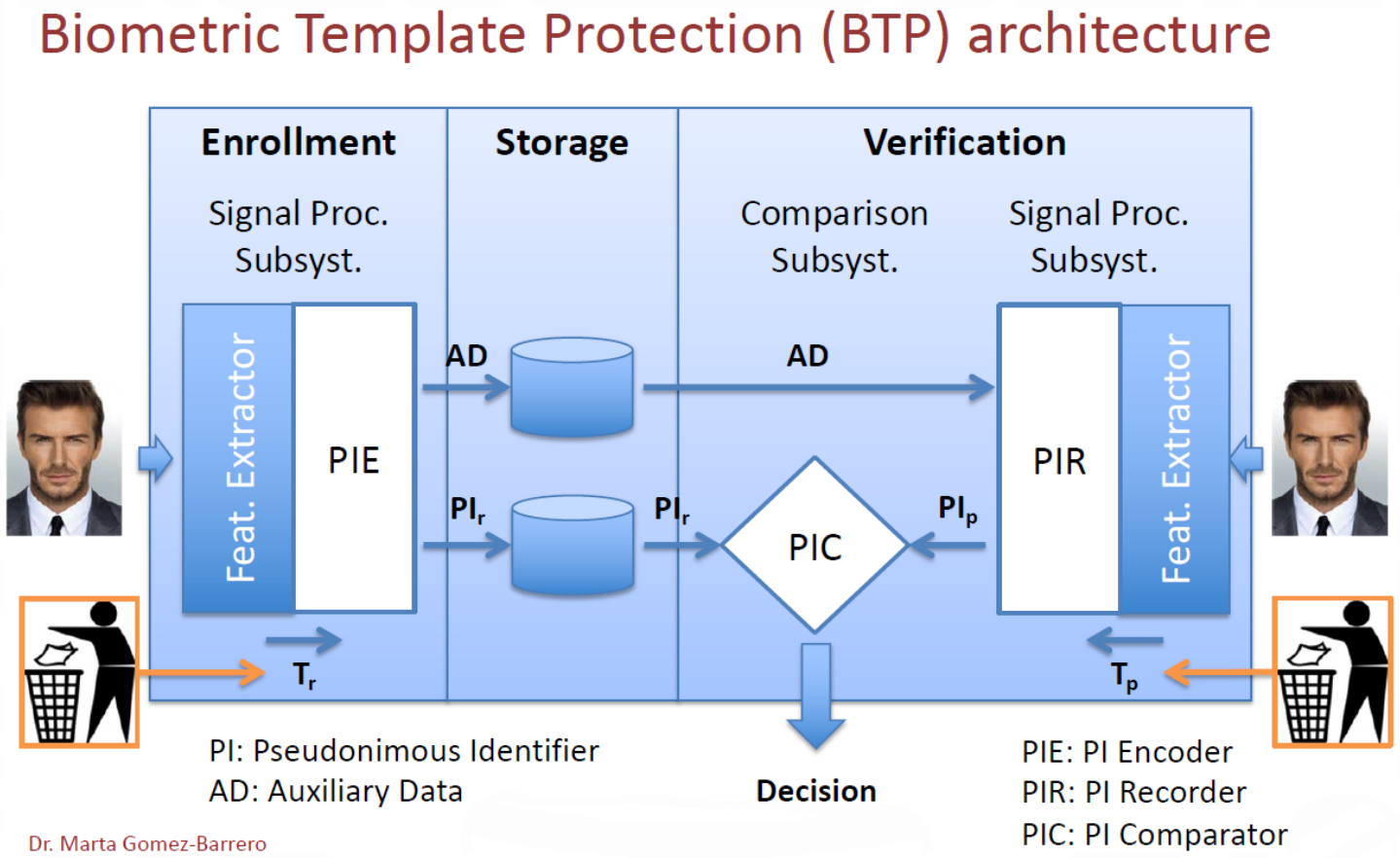
Irréversibilité + Renouvelabilité + Incompatibilité
(+ Précision + Taille du modèle + Temps de vérification)

BIOMÉTRIE vs CRYPTOGRAPHIE

- Faut-il chiffrer les modèles biométriques ? Utiliser une fonction de hachage ?
- Différence entre les mots de passe et les données biométriques :
  - Données biométriques fortement influencées par le bruit
  - Fonctions cryptographiques (à sens unique) très sensibles au bruit
- Cryptographie : 2 inconvénients principaux
  - Chiffré sécurisé seulement tant que la clé de déchiffrement n'est pas connue de l'attaquant.
  - Modèle déchiffré à chaque tentative d'authentification, car la comparaison ne peut être effectuée directement dans le domaine chiffré (sauf si chiffrement homomorphe)

BIOMÉTRIE vs CRYPTOGRAPHIE

- Solution : Stocker le modèle chiffré et la clé de déchiffrement dans un environnement sécurisé au sein d'une carte à puce ou une puce sécurisée.

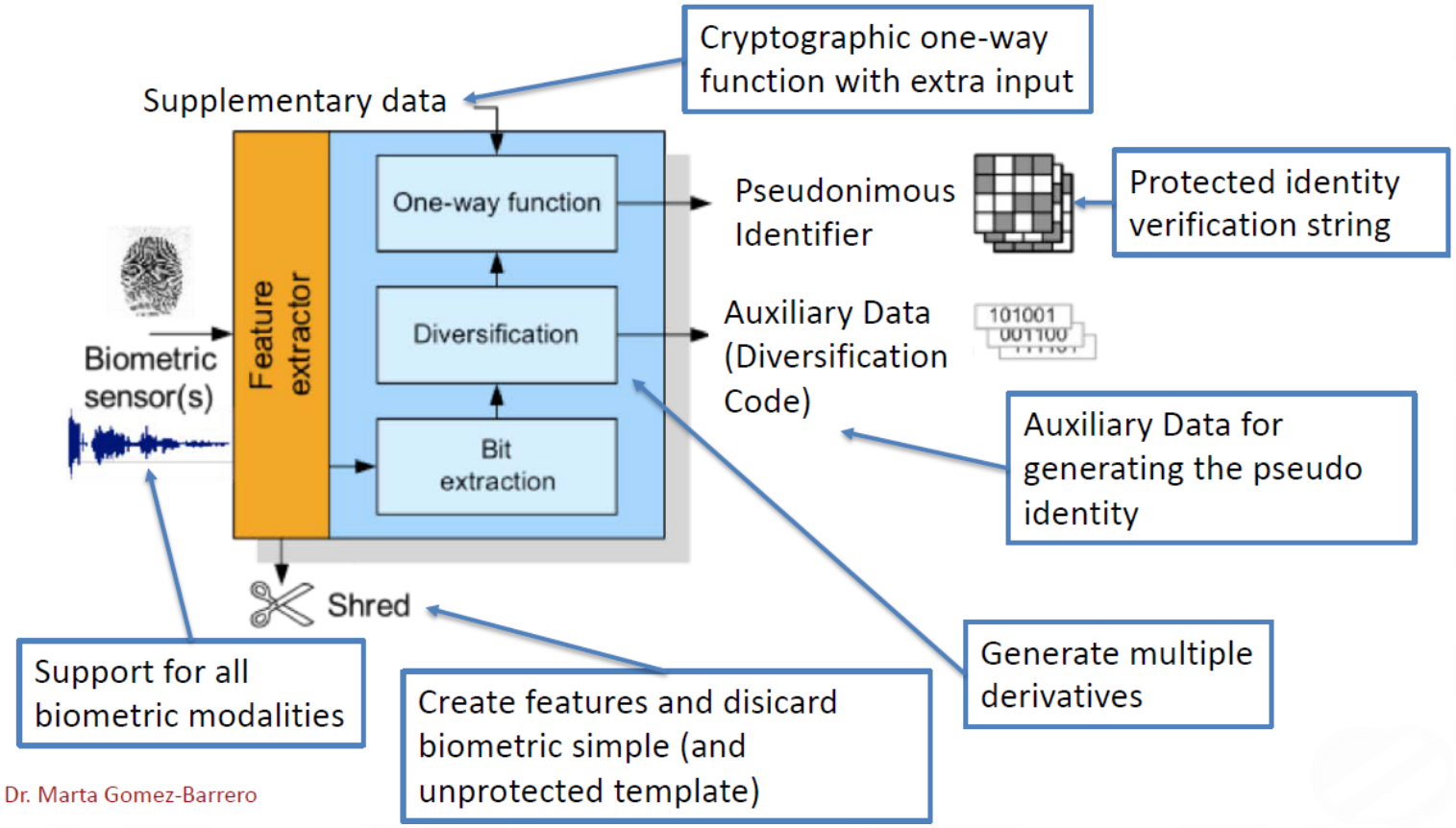


IDENTIFIANT PSEUDONYME (PI)

- Conversion en deux étapes des échantillons biométriques capturés en modèles protégés
- Pour une protection permanente :
  - Stockage, transmission et comparaison protégés
- Impossible de récupérer l'échantillon biométrique d'origine du modèle protégé
- Un modèle représente des données d’identification **pour une application seulement**

IDENTIFIANT PSEUDONYME (PI)

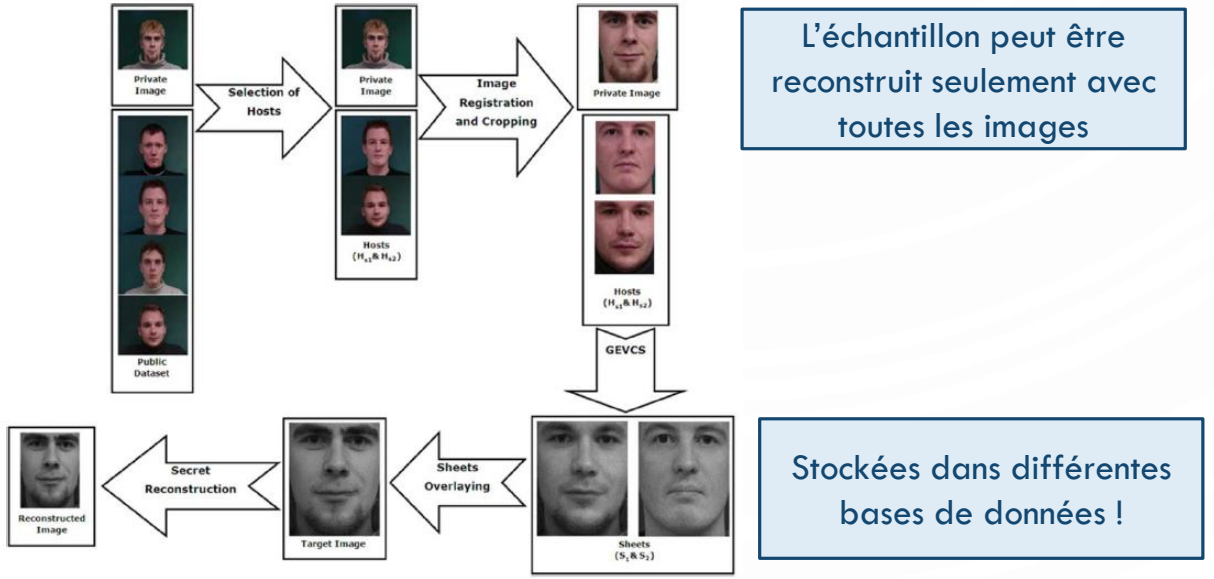
Pseudonymous Identifier Encoder (PIE)



Dr. Marta Gomez-Barrero

BIOMÉTRIE ANNULABLE

- **Distorsions intentionnelles et reproductibles** basées sur des transformations qui fournissent une comparaison de modèles biométriques dans le domaine protégé
- 2 types :
  - Transformations non réversibles des données biométriques ou modèles non protégés
  - Mélange avec données auxiliaires pour dériver une version déformée du modèle biométrique



L'échantillon peut être reconstruit seulement avec toutes les images

Stockées dans différentes bases de données !

Ross, A., & Othman, A. (2011). Visual cryptography for biometric privacy.

CRYPTOBIOMÉTRIE

- Combinaison de clés cryptographiques avec des versions des modèles biométriques d'origine pour obtenir des modèles sécurisés.
- Dans la plupart des cas : données auxiliaires générées
- Schémas avec attache à la clé (« ***Key binding*** »)
  - Combinaison de la clé avec le modèle biométrique.
- Schémas de génération de la clé (« ***Key generation*** »)
  - Clé et modèle biométrique générés directement à partir des données brutes
- Dans les 2 cas : Vérification = Application d'un algorithme aux données biométriques pour retrouver la clé

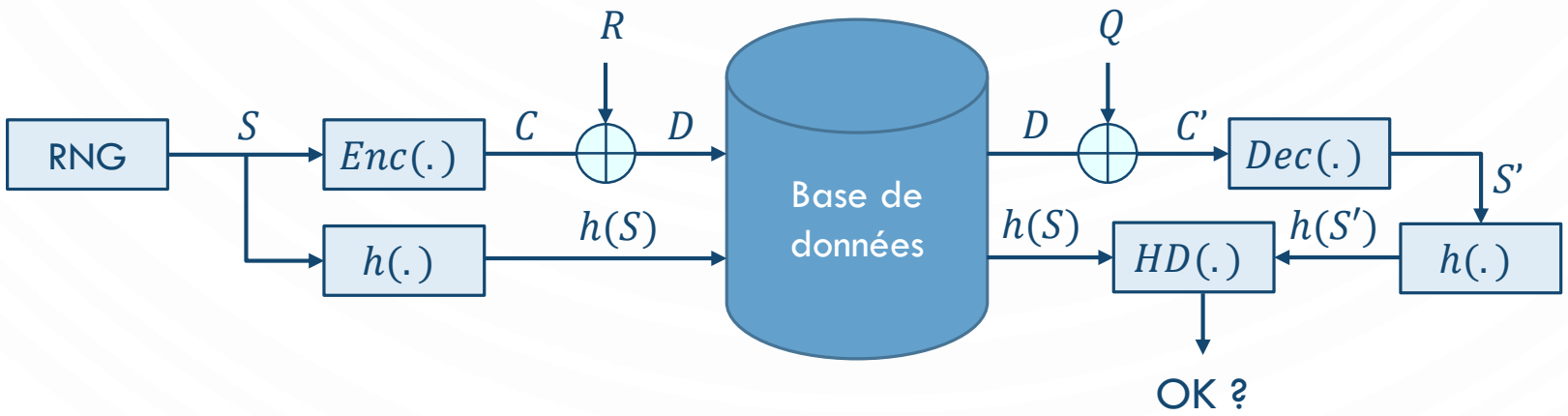
CRYPTOBIOMÉTRIE – « FUZZY COMMITMENT »

ENROLLEMENT

- R vecteur associé aux données biométriques à stocker
- Génération aléatoire de S et chiffrement $C = Enc(S)$
- Fonction de hachage appliquée à S pour obtenir $h(S)$
- Génération des données additionnelles (publiques) $D = C \oplus R$
- Stockage de D et $h(S)$ dans la base de données

VÉRIFICATION

- Q vecteur associé aux données biométriques à comparer
- Récupération de D dans la base de données
- Calcul de $C' = Q \oplus D = Q \oplus C \oplus R$
- Déchiffrement $S' = Dec(C')$
- Fonction de hachage appliquée à S' pour obtenir $h(S')$
- Comparaison de $h(S)$ et $h(S')$



Juels, Ari, and Martin Wattenberg. "A fuzzy commitment scheme."

CHIFFREMENT HOMOMORPHE ET BIOMÉTRIE

- Protection du modèle basée sur le chiffrement homomorphe
  - Méthode générale
  - Pas d'altération des performances
  - Protection permanente : toutes les opérations réalisées dans le domaine chiffré
  - Irréversibilité et non-associativiré
  - Renouvelabilité sans réacquisition
- Problèmes
  - Limitation du nombre d'opérations dans le domaine chiffré (capacité de stockage…)
  - Clé secrète + Modèle protégé = modèle compromis !

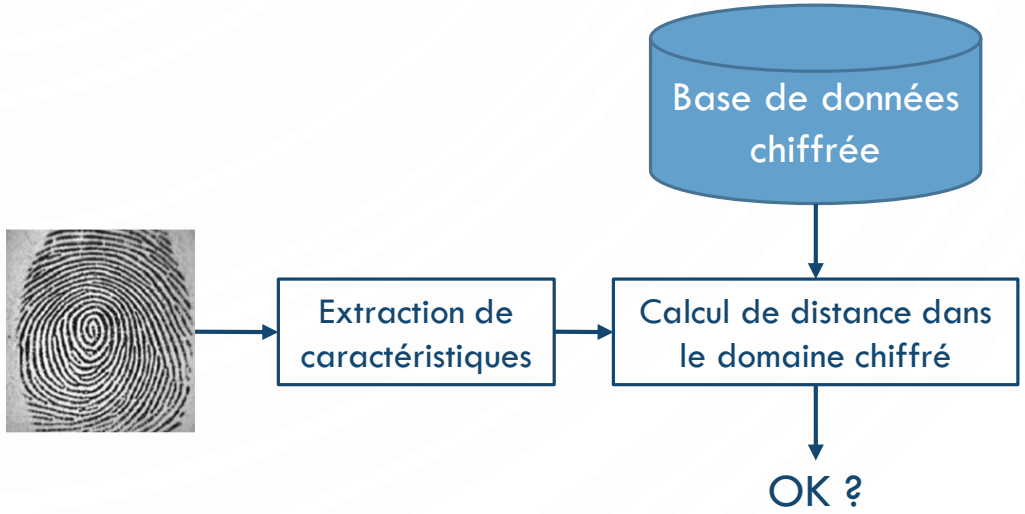
Fontaine, Caroline, and Fabien Galand. "A survey of homomorphic encryption for nonspecialists."

CHIFFREMENT HOMOMORPHE ET BIOMÉTRIE

- Implémentation pratique en utilisant le cryptosystème de Paillier
- Basé sur l'hypothèse suivante (*Decisional Composite Residuosity Assumption*)
  - Soit un nombre composé n et un entier z, il est difficile de savoir s'il existe un entier y tel que $z \equiv y^n \bmod n^2$.
- Homomorphisme additif :
  - $Dec(m_1' \cdot m_2' \bmod n^2) = m_1 + m_2 \bmod n$

    Produit de 2 chiffrés — Somme de 2 clairs
  - $Dec\left((m_1')^l \bmod n^2\right) = m_1 \cdot l \bmod n$

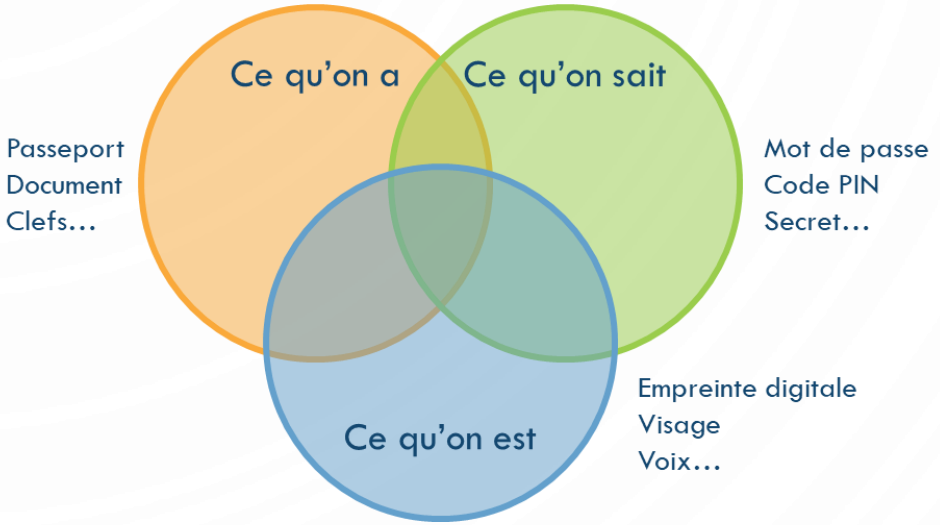
    Exponentiation d'un chiffré et d'un clair — Produit de 2 clairs



Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes."

OUVERTURE : AUTHENTIFICATION PLURI-FACTEURS

- Combinaison de plusieurs facteurs d'authentification, suivant le niveau de sécurité requis
- Par exemple, smartphone LG V30 avec :
  - Lecture faciale
  - Reconnaissance vocale
  - Lecteur d'empreintes digitales
  - Données stockées sur le téléphone



CONCLUSION

- Enjeux de sécurité liés au stockage des données biométriques :
  - Bases de données contenant des informations personnelles souvent piratées
  - Par exemple : Office of Personnel Management (USA) piraté en 2015
    - Vol des empreintes digitales de 5,6 millions employés du gouvernement
    - Usurpation d'identité
  - Plus sûr de stocker les données sur le système plutôt que chez un fournisseur de services
  - Chiffrement des données nécessaires
- Analyse de protection de la vie privée :
  - Analyser l'impact de l'utilisation d'une donnée biométrique (information personnelle) sur la vie privée d'un individu
  - S'assurer qu'une donnée biométrique est utilisée de manière appropriée, pour un usage précis (et connu de l'utilisateur)
  - Loin d'être le cas…

CONCLUSION : PROTECTION DE LA VIE PRIVÉE

- Exemple : enrôlement à l'insu de la population
  - Système avec reconnaissance faciale
    - Caméra CCTV développée en 2012 par Hitachi Hokosuai Electric (Japon)
      - Scan de 36 millions de visages par seconde
      - Reconnaissance instantanée si déjà filmé
      - Base de données avec visages pré-indexés
      - Echec de reconnaissance seulement si :
        - Taille < 40x40 pixels
        - Visage pas de face
    - Surveillance à l'aéroport de Dubaï en 2018
      - Utilisation de 80 caméras en passant sous un tunnel dans un aquarium virtuel
  - Système avec reconnaissance d'iris
    - Développé en 2014 par l'Université Carnegie Mellon (PA, USA)
    - Scanner l'iris d'un individu dans un foule à une distance de 10 mètres


TRTWORLD

SYSTÈMES DE VIDÉOSURVEILLANCE

PAULINE PUTEAUX – LIRMM, UNIV. MONTPELLIER/CNRS

HMIN407 – SÉCURITÉ INFORMATIQUE : ENJEUX ET FACETTES

LE 30/01/19

MOTIVATIONS

- Dissuasion
- Observation
- Surveillance
- Collecte de renseignements
- Evaluation d'un incident probable et intervention connexe
- Evaluation d'un incident en cours et intervention connexe
- Analyse judiciaire après l'incident
- Analyse des éléments de preuve après l'incident

MOTIVATIONS

- Nombreux clients :
  - Milieux financiers et banquiers
  - Transport
  - Industrie
  - Commerce au détail
  - Éducation
  - Services publics
  - Importance des secteurs publics et parapublics

MARCHÉ DE LA VIDÉOSURVEILLANCE

MOTEURS

- Evénements (attentats)
- Criminalité locale
- Nouvelles technologies
- Fiabilité des systèmes
- Consentement de la population

FREINS

- Protection de la vie privée
- Efficacité des systèmes (prévention)
- Absences de normes
- Coûts importants

BASES TECHNIQUES

- Eclairage
  - Source lumineuse nécessaire (soleil ou lumière artificielle)
  - Lumière normale ou infrarouge, suivant le type d'application
  - Infrarouge utilisé si :
    - Surveillance discrète
    - Conditions d'éclairage difficiles

BASES TECHNIQUES

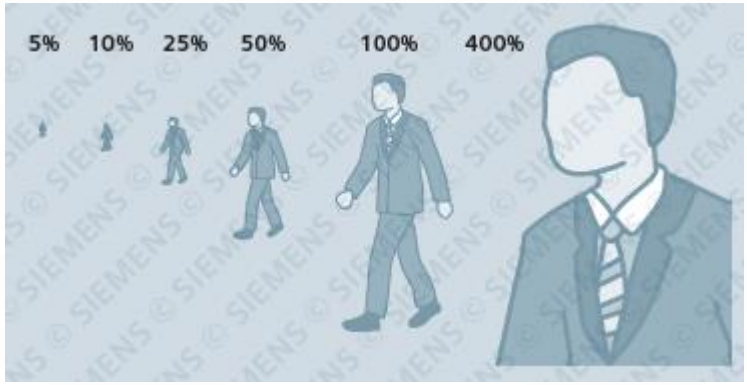
- Objectif responsable de :
  - La définition du **champ de vision** (partie de la scène à enregistrer + niveau de détails)
  - Le contrôle de **quantité de lumière** qui atteint le capteur via l'objectif pour éclairer correctement l'image
  - La **mise au point** par déplacement de lentilles de l'objectif ou modification de l'écart entre l'objectif et le capteur
- Trois types de champs de vision

A gauche : Grand angle
Au centre : Normal
A droite : Téléobjectif

- Trois types d'objectifs : fixe, foyer progressif ou zoom

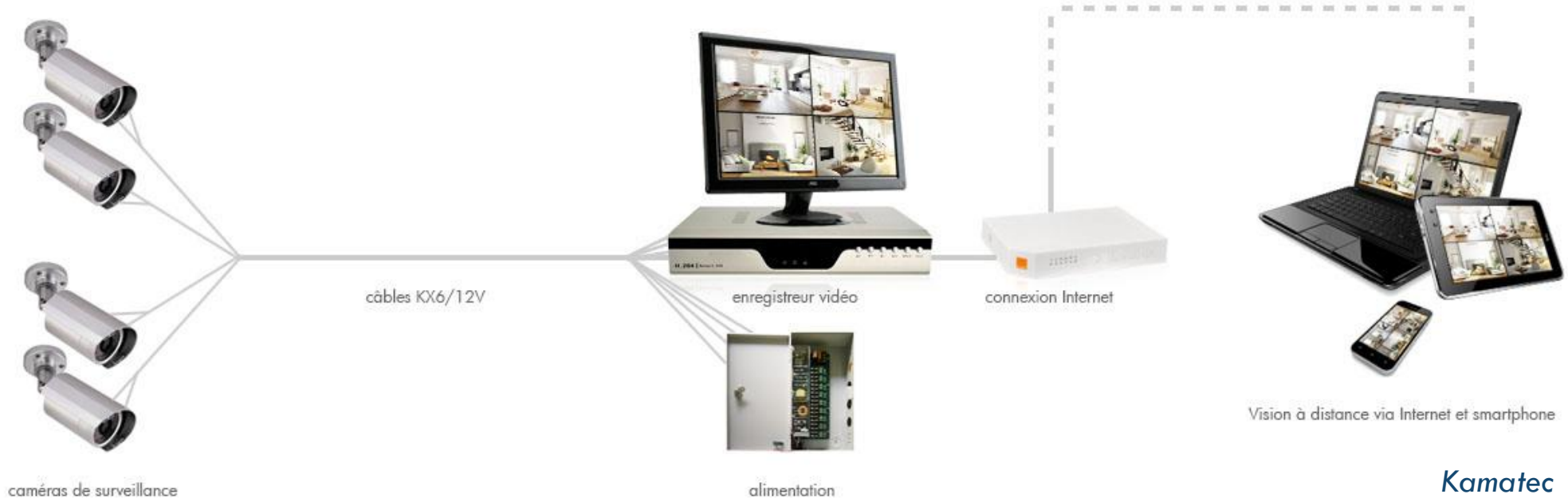
BASES TECHNIQUES

- Norme DIN EN 20132-7 (Avril 2013) : ≠ niveaux de définition et classification d'objets
  - **Surveiller** : cible d'observation pas inférieure à 5% de la hauteur de l'image (ou supérieure à 80mm par pixel)
  - **Détecter** : cible d'observation pas inférieure à 10% de la hauteur de l'image (ou supérieure à 40mm par pixel)
  - **Observer** : cible d'observation équivalente à 25% de la hauteur de l'image (ou supérieure à 16mm par pixel)
  - **Reconnaître** : cible d'observation pas inférieure à 50% de la hauteur de l'image (ou supérieure à 8mm par pixel)
  - **Identifier** : cible d'observation pas inférieure à 100% de la hauteur de l'image (ou supérieure à 4mm par pixel)
  - **Examiner** : cible d'observation pas inférieure à 400% de la hauteur de l'image (ou supérieure à 1mm par pixel)



VIDÉOSURVEILLANCE IP

- Flux vidéo transmis sous protocole Internet (IP) à travers des réseaux informatiques



Kamatec

VIDÉOSURVEILLANCE IP

- Avantages et inconvénients

- Numérique de A à Z
- Architecture souple et extensible
- Matériel non propriétaire
- Diminution des coûts pour des systèmes à nombreuses caméras
- Aucune perte de conversion analogiques/numériques

- Exige une infrastructure réseau
- Requiert des compétences en réseautique
- Gestion difficile des systèmes
- Sécurité et fiabilité du réseau

VIDÉOSURVEILLANCE INTELLIGENTE

- Analyse automatisée de la vidéo
  - Identification des objects
  - Analyse de comportements / d'attitudes spécifiques
- Transformation en données dont le traitement permet de poser une action
- Usages possibles :
  - Sécurité/Surveillance
  - Opérations/Marketing

VIDÉOSURVEILLANCE INTELLIGENTE

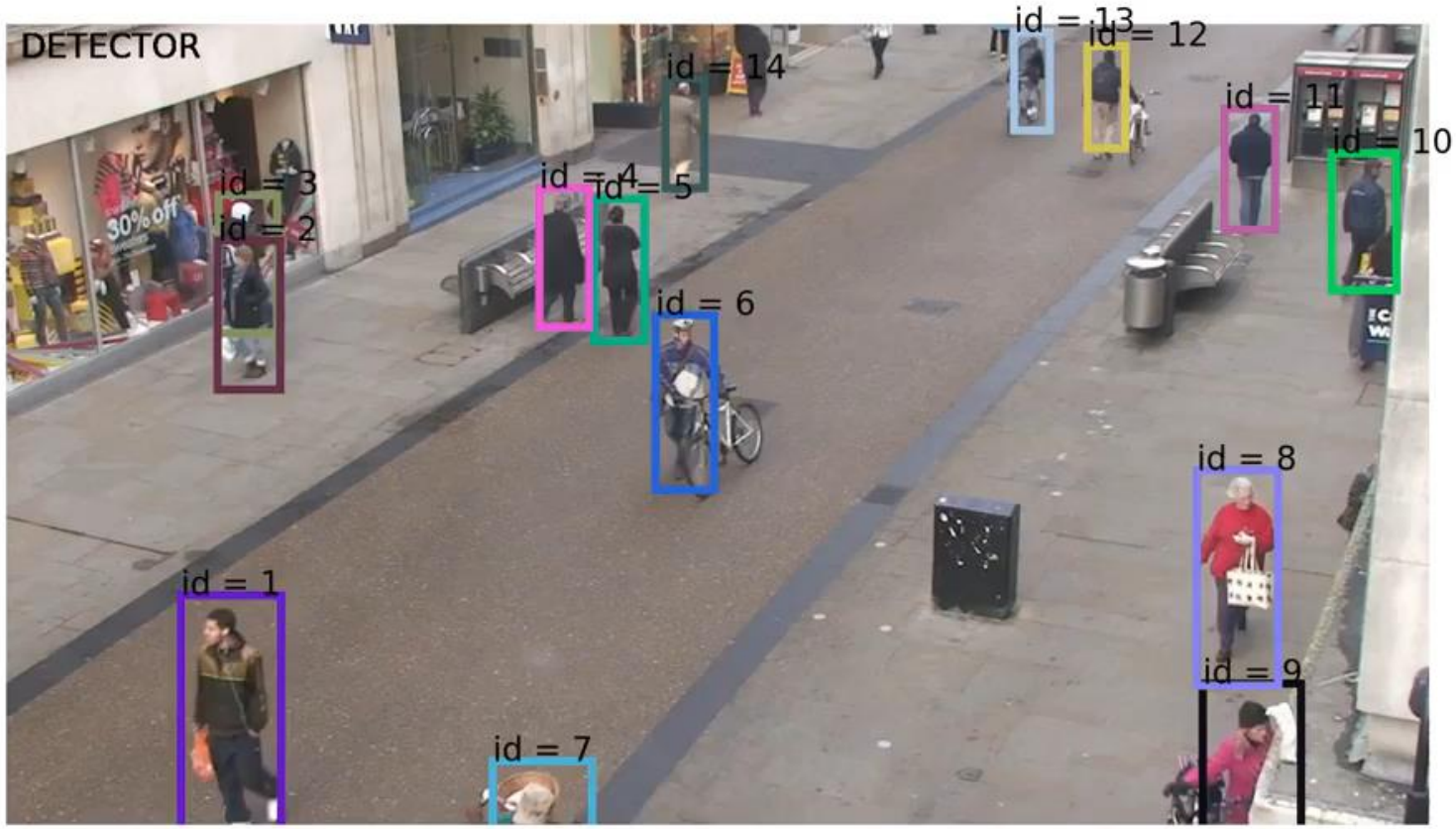
- Beaucoup d'avantages
  - Fonctionne 24h/24 et 7j/7
  - Déclenchement d'alarmes pour intervention
  - Réduction de la bande passante et de l'archivage
  - Assistance au personnel de surveillance
  - Suivi d'activité d'une scène possible
  - Accélération de la recherche dans les séquences archivées

SEGMENTATION D'OBJETS EN MOUVEMENT

- Segmentation des pixels qui diffèrent de l'arrière-plan d'un point de vue statistique

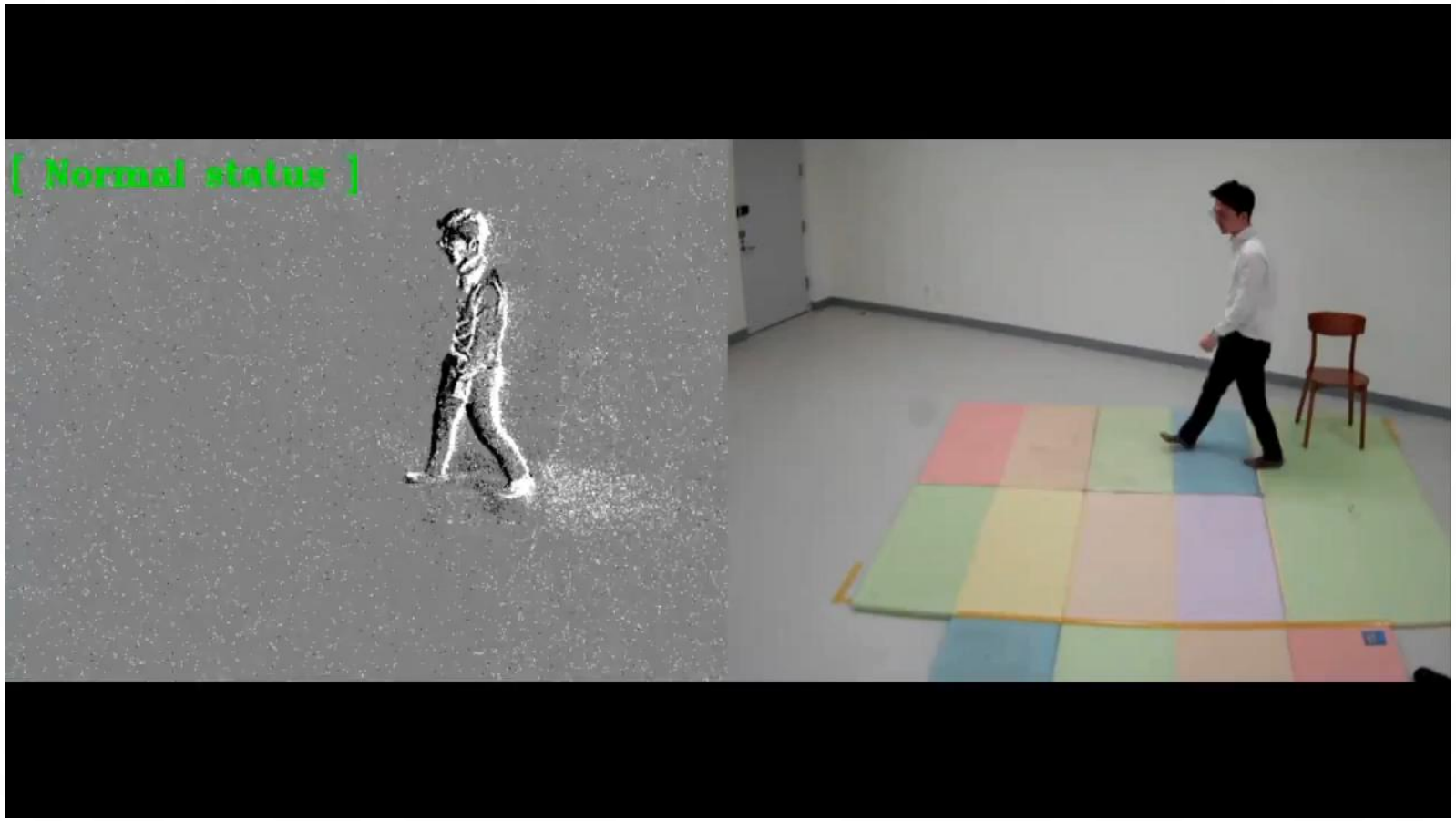
Joao Faro, Real-time Video Surveillance System with Adaptive Background

SUIVI ET CLASSIFICATION D'OBJETS

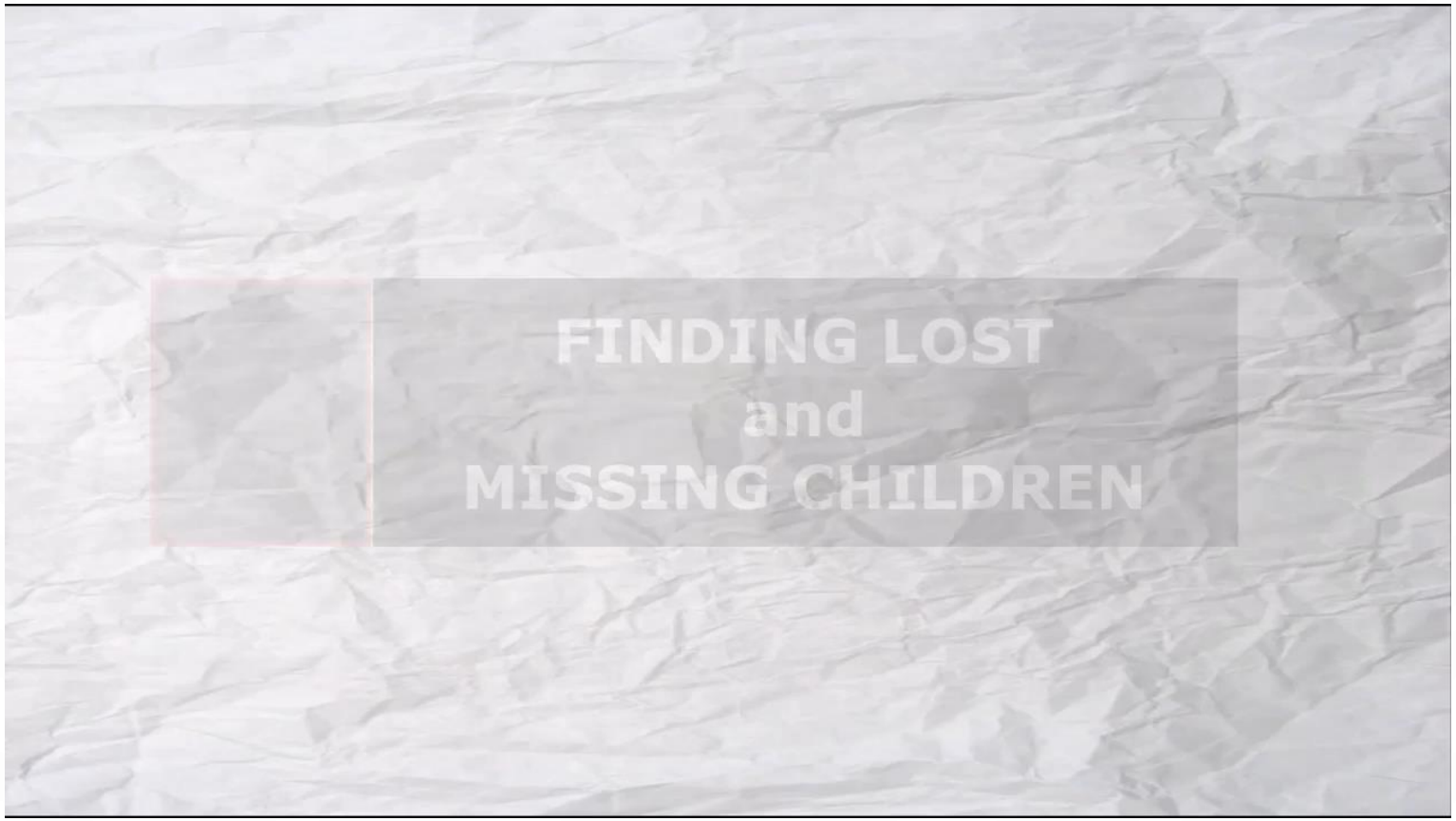


DÉTECTION ET RECONNAISSANCE DE PLAQUES

RECONNAISSANCE DE COMPORTEMENTS



RETROUVER UN ENFANT PERDU



DÉTECTION D'INTRUSION

DÉTECTION D'OBJET ABANDONNÉ

COMPTAGE D'OBJETS

PROBLÈMES

- Pour la segmentation
  - Ombrages
  - Arrière-plan en mouvement (dynamique)
    - Feuillage, drapeaux, fontaines, fumée…
    - Fausses alarmes

Source:http://figment.csee.usf.edu/~sfefilat/data/papers/ThAT4.2.pdf

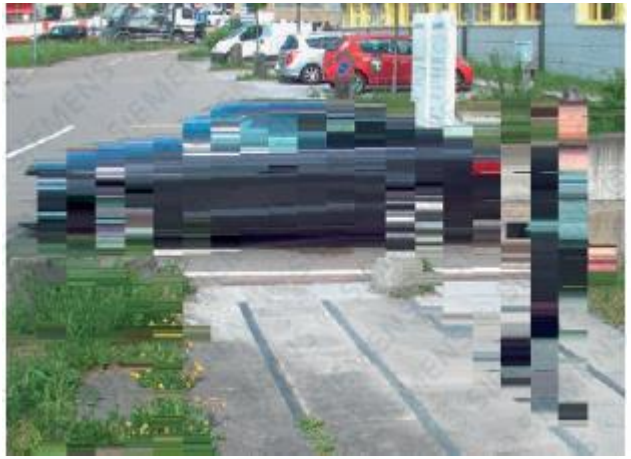
Source:
http://portfolio.ecs.soton.ac.uk/20/3/irp_report_ieee.pdf

PROBLÈMES (ET DÉFIS !)

- Pour le suivi et la classification
  - Occlusions
  - Piétons qui rampent ou qui transportent des objets
  - Objets fractionnés ou agglutinés
- Généraux
  - Faux objets : reflets dans vitres ou flaques d'eau,
  - Nuit
  - Conditions météo difficiles

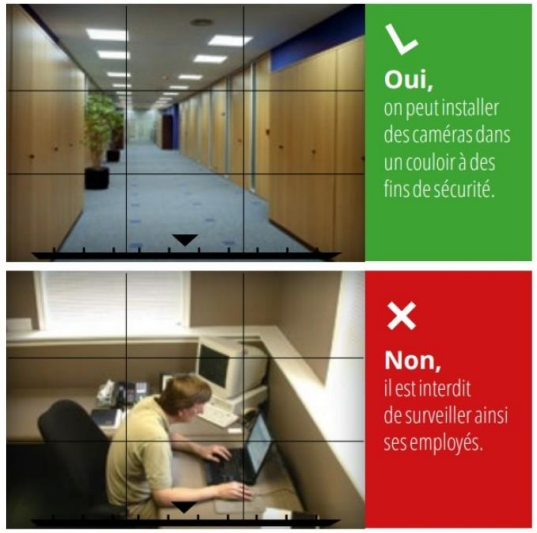
PROTECTION DE LA VIE PRIVÉE

- Objectifs
  - Les données doivent être disponibles lorsqu'elles sont nécessaires
  - Les programmes et les données doivent être protégés contre les accès non autorisés
- Méthodes
  - Chiffrement partiel



RÉGLEMENTATION

- Règles de base
  - Interdit de filmer dans un lieu public (sauf autorisation préfectorale)
  - Dans un lieu privé : soumise à autorisation de la CNIL
  - Installation justifiée par motivations de sécurité des lieux et des personnes
  - Si enregistrement des données : déclaration à la CNIL
  - Besoin du consentement des personnes filmées



RÉGLEMENTATION

- Information du public
  - Sur la voie publique : panneaux avec le symbole d'une caméra
  - Lieux publics/privés : pancartes ou affiches indiquant :
    - Que les lieux sont sous vidéosurveillance
    - Le nom du responsable
    - Les modalités d'exercice du droit à l'image
    - Le nom du destinataire des images
  - Entreprise :
    - Information personnelle (courrier) et collective des salariés
    - Information du CE (si plus de 10 employés)

RÉGLEMENTATION

SANCTIONS

- Droit de demander réparation pour violation de son image et de sa vie privée
- Responsable risque un an d'emprisonnement et une amende de 45 000 € (article 226-1 du Code Pénal)

Vidéosurveillance excessive : mise en demeure de l'Institut des techniques informatiques et commerciales (ITIC)

24 juillet 2018

Le 2 juillet, la Présidente de la CNIL a mis en demeure l'Institut des techniques informatiques et commerciales de mettre en conformité son système de vidéosurveillance.

L'Institut des techniques informatiques et commerciales (l'ITIC) est une école privée d'enseignement supérieur qui délivre des formations de niveau bac +2 à bac +5 dans le secteur économique tertiaire. Il compte entre 600 et 800 étudiants inscrits chaque année et emploie une dizaine de salariés et 60 enseignants.

En février 2018, la CNIL a procédé à un contrôle dans les locaux de l'école situés à Paris.

Elle a constaté :

- qu'un système de vidéosurveillance y était installé et que certaines des caméras filmaient en permanence l'ensemble des salles de cours et des lieux de vie des étudiants ;
- que l'une de ces caméras filmait en continu le poste de travail d'une employée ;
- que les images étaient conservées au-delà d'un mois, qui était la durée maximale prévue par l'école ;
- que les personnes filmées n'étaient pas correctement informées ;
- que les images issues de la vidéosurveillance n'étaient pas suffisamment sécurisées, le système ne permettant pas de s'assurer qu'aucun tiers non autorisé n'accède aux images.

MERCI POUR VOTRE ATTENTION !