TP C11

VERIFICATEURS biométriques
Introduction

http://www.biometrics.org/bc2008/
http://www.cse.msu.edu/biometrics/
http://pagesperso-orange.fr/fingerchip/index.htm
http://www.itl.nist.gov/iad/894.03/nigos/mbark.html
http://el.el.obs.utcluj.ro/site/Biometrics_2005.pdf
http://www.bromba.com/faq/biofaqe.htm
http://www.cse.ust.hk/svc2004/

TABLE DES MATIÈRES

• Securitee en e –World (“monde electronique”)

À l'ère de la connectivité électronique universelle ⇒ *e-World:*

⇒ *e-commerce* ⇒ *e-banking*

⇒ *e-shop* ⇒ *e-mail*

⇒ *e-phone* ⇒ *e-government ……*

- De plus en plus d'autres activités sont liées à l' Internet
- Internet, des difficultés et des problèmes de développement : ⇒ viruses, hackers, les vols sur l'ordinateur, accès non autorisés
- Ces questions touchent la prospérité et la productivité des entreprises et des particuliers

La sécurité est de plus en plus importante

- Une solution est l'authentification : message et vérification de l'utilisateur
- En fait, il y a un besoin croissant pour identifier les individus dans l'e- monde :
  - Cette personne peut accéder au système ?
  - Est-ce que cette personne a le droit de faire cette offre ?
- Un grand défi :

  L'authentification de l'utilisateur (vérification de l'identité)
- L'ordinateur peut identifier des individus spécifiques .

Une fois le développement de la technologie est de plus en plus, la fraude authentification positive est crucial !

- **L'authentification de l'utilisateur est basé sur trois méthodes**:
  1. Que j'ai ? (carte , clé, ...)
  2. Que sais-je ? (code PIN, ...)
  3. Quoi suis-je? (caractéristiques biométrique)

Biométrie

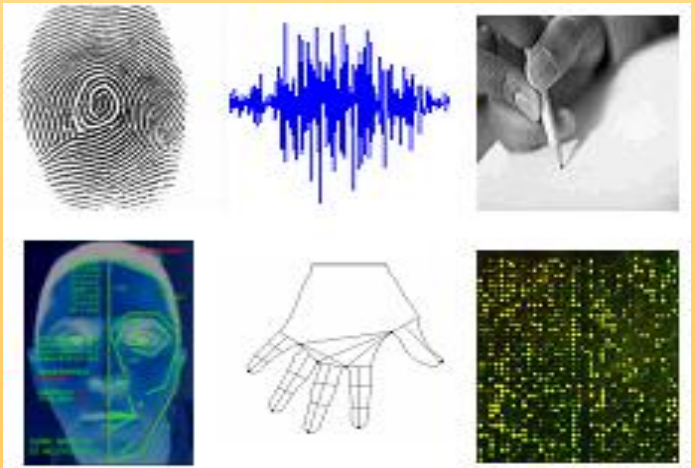
“La Biometrie « est un ensemble de méthodes automatisées de reconnaître une personne sur la base de caractéristiques physiologiques ou comportementales » comme le Consortium biométrique défini

Biometrie ⇒ ***bios*** **(**vie**)** et ***metron*** (mesure)

Les éléments biométriques :

physiologique:empreintes digitales, visage, iris, de la main, de l'ADN,...

Comportemental: la voix , la démarche, la signature, ...



- Toute caractéristique physiologique ou comportemental peut être utilisé comme un vérificateur biométrique tant qu'elle satisfait aux exigences suivantes [1]:

- **L'universalité-** que tout le monde doit avoir cette fonctionnalité
- **Caractère distinctif** - caractéristiques pour deux personnes pour être suffisamment distincte pour permettre la différenciation ;
- **Permanence** - fonction invariante une longue période de temps
- **Mesurabilité** - indique que la caractéristique biométrique peut être quantitativement mesurables

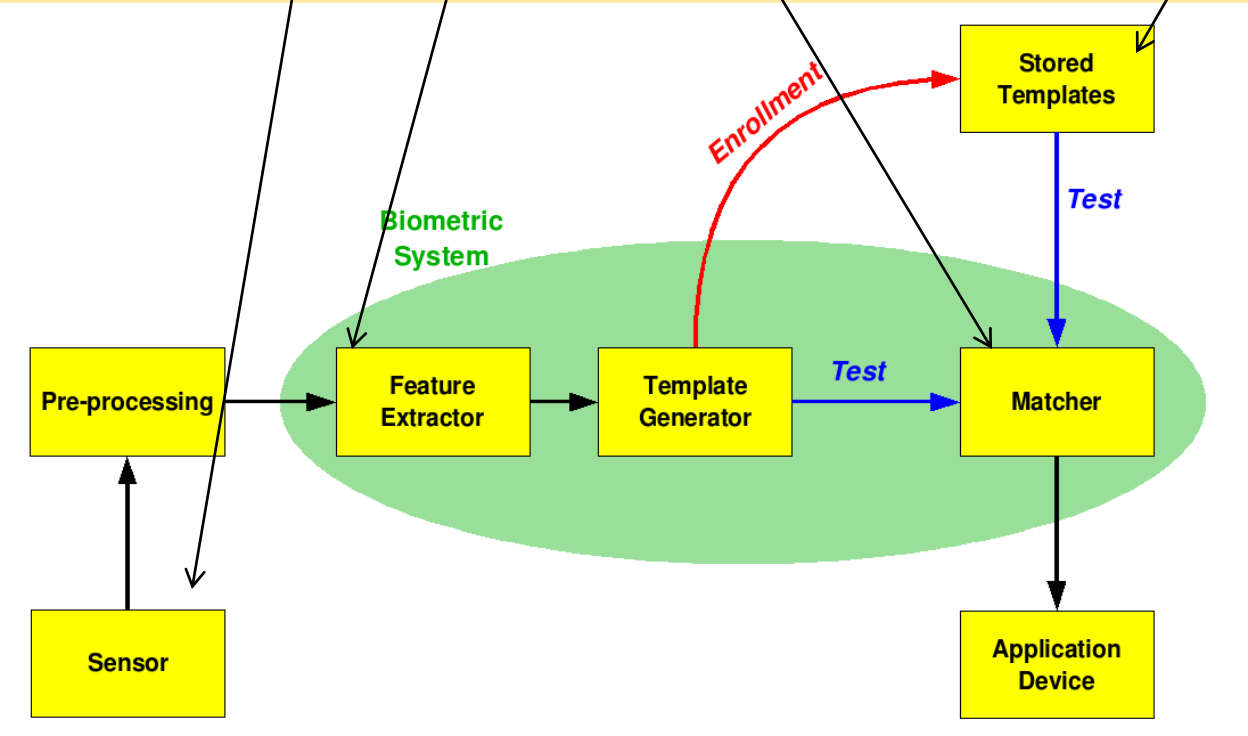
- Pour les systèmes pratiques sont encore nécessaires certaines exigences supplémentaires , à savoir :

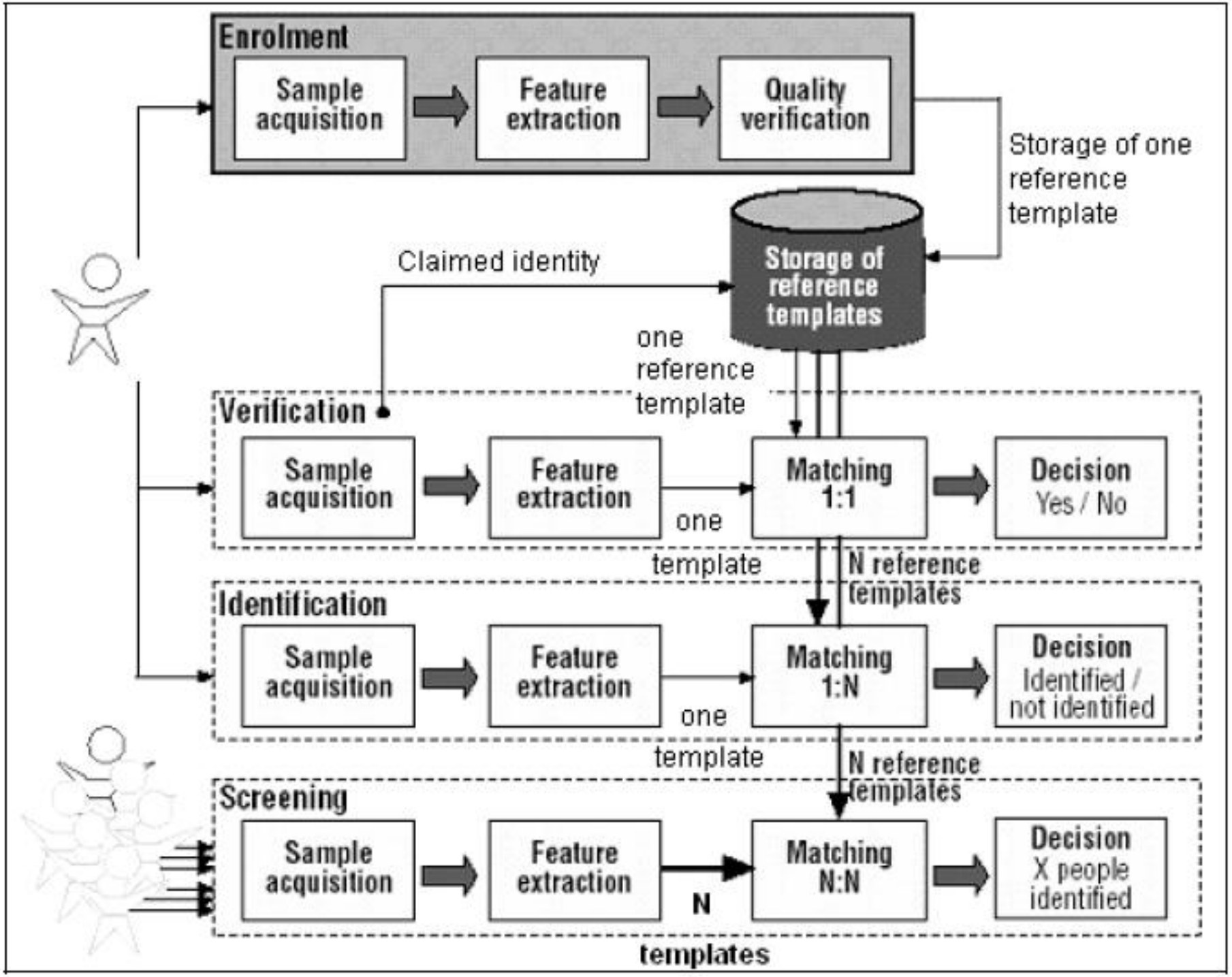
- **Performance** - qui se réfère à la précision tangible de reconnaissance, la vitesse, la robustesse et les ressources nécessaires pour atteindre un niveau de performance donné;
- **Acceptabilité** - indique la mesure dans laquelle la caractéristique biométrique est acceptée par les utilisateurs;
- **Résistance à la fraude** - indique la facilité avec laquelle un système peut être escroqué .

SYSTEMES BIOMETRIQUES – SB

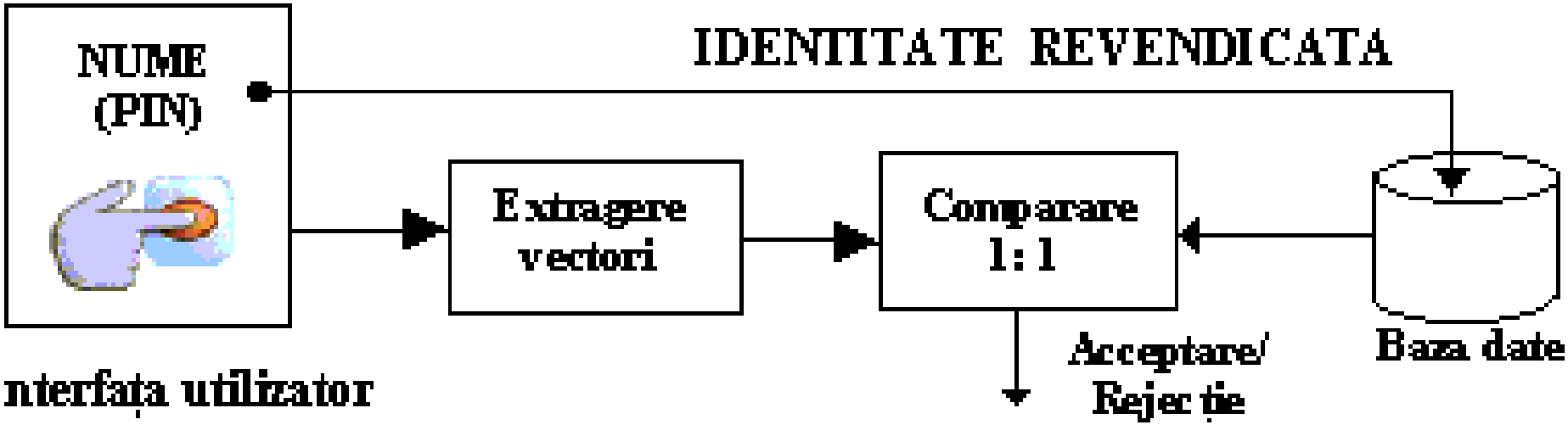
ELEMENTS:

- Capteur ;
- Module d'extraction de caractéristiques;
- Module de comparaison ;
- Base de données biométriques.

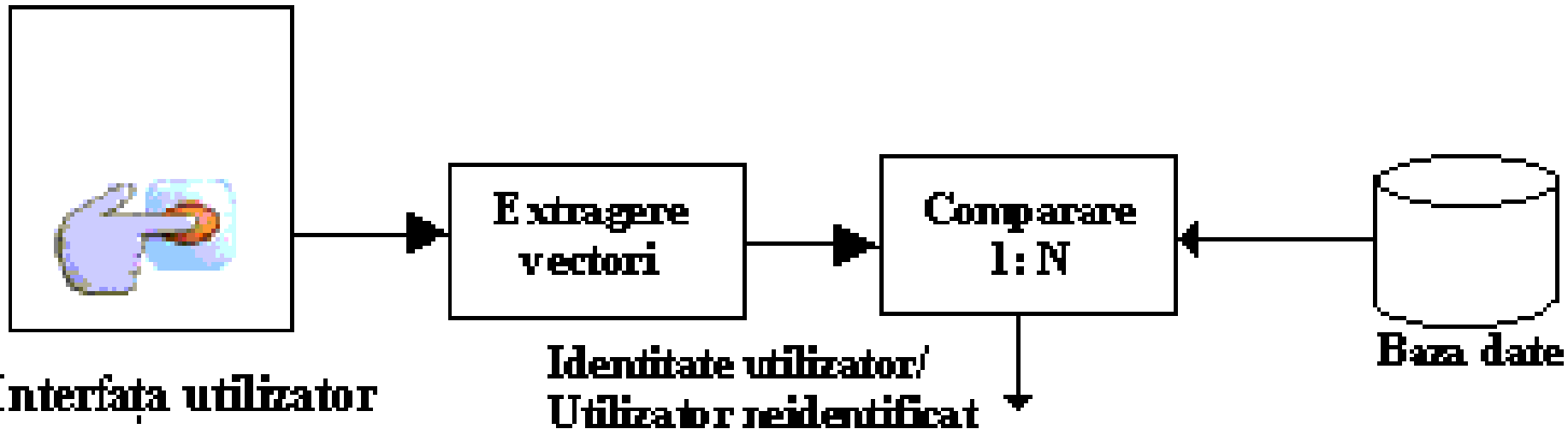



Enrolment
Sample acquisition
Feature extraction
Quality verification
Storage of one reference template
Storage of reference templates
Claimed identity
one reference template
Verification
Sample acquisition
Feature extraction
Matching 1:1
Decision Yes / No
one template
N reference templates
Identification
Sample acquisition
Feature extraction
Matching 1:N
Decision Identified / not identified
one template
N reference templates
Screening
Sample acquisition
Feature extraction
Matching N:N
Decision X people identified
N templates

VERIFICARE



IDENTIFICARE



Caractéristiques et taxonomie des systèmes biométriques

Systèmes de reconnaissance biométrique peuvent fonctionner en: MODE positive ou négative .

1. **Mode positive** : La reconnaissance positive décide si la personne qui affirme l'identité est vraiment cette personne .

   Le but: éviter que plusieurs utilisateurs d'utiliser la même identité

2. **Mode négative:** doit prouver que l'utilisateur n'est pas celui qu'il prétend qu'il est (SB SEULEMENT !)

   Le but : empêcher une personne d'avoir plusieurs identités.

• Les systèmes et les applications biométriques peuvent être classés comme suit:

- **Coopérative ou non coopératifs** - se réfère au comportement de l'imposteur en interaction avec le système (ex. vocale) ;

- **Fréquent ou rarement utilisé** - la fréquence avec laquelle les utilisateurs enregistrés sont soumis à reconnaissance biométrique ;

- **Caché/visible** - l'utilisateur est informé ou non qui fait l'objet de la reconnaissance biométrique ;

- **Avec ou sans aide** - indique comment le processus d'acquisition biométrique de données a lieu ;

- **SB publiques ou privés** - Les utilisateurs du système sont des clients ou des employés d'une entreprise ;

- **L'environnement d'exploitation standard ou non-standard** - désigne l'environnement dans lequel le système fonctionne ;

- **Ouvert ou fermé** - montre comment il est utilisé le motif biométrique d'une personne pour une ou plusieurs applications

Brève histoire de la biométrie

Egypte antique (BC) - ont été utilisée des principes de base de la vérification biométrique dans les situations usuelles de bureau/commerce (opérations agricoles , diverses procédures judiciaires) . Les caractéristiques biologiques utilisés : cicatrices , mensurations , la couleur des yeux, taille ou l'apparence de la peau .

Chine - (XIV siècle, Joao de Barros) - commerçants chinois utilisaient une forme de biométrie par impression sur du papier , de palme et semelle de leurs enfants , trempée dans l'encre , résolvant ainsi le problème des enfants de distinguer les uns des autres

France - (fin du XIX sec) - méthodes anthropométriques d'Alphonse Bertillon (1880) , utilisés pour identifier les criminels et de l'expertise judiciaire. Bertillon a remarqué que certains éléments du corps demeurent quant fixe : la longueur des doigts , le diamètre du crâne , l'hauteur , les cicatrices , les tatouages ou d'autres caractéristiques personnelles (discrédité en 1903)

Angleterre (1893) - Richard Edward Henry de Scotland Yard a commencé à utiliser les empreintes digitales

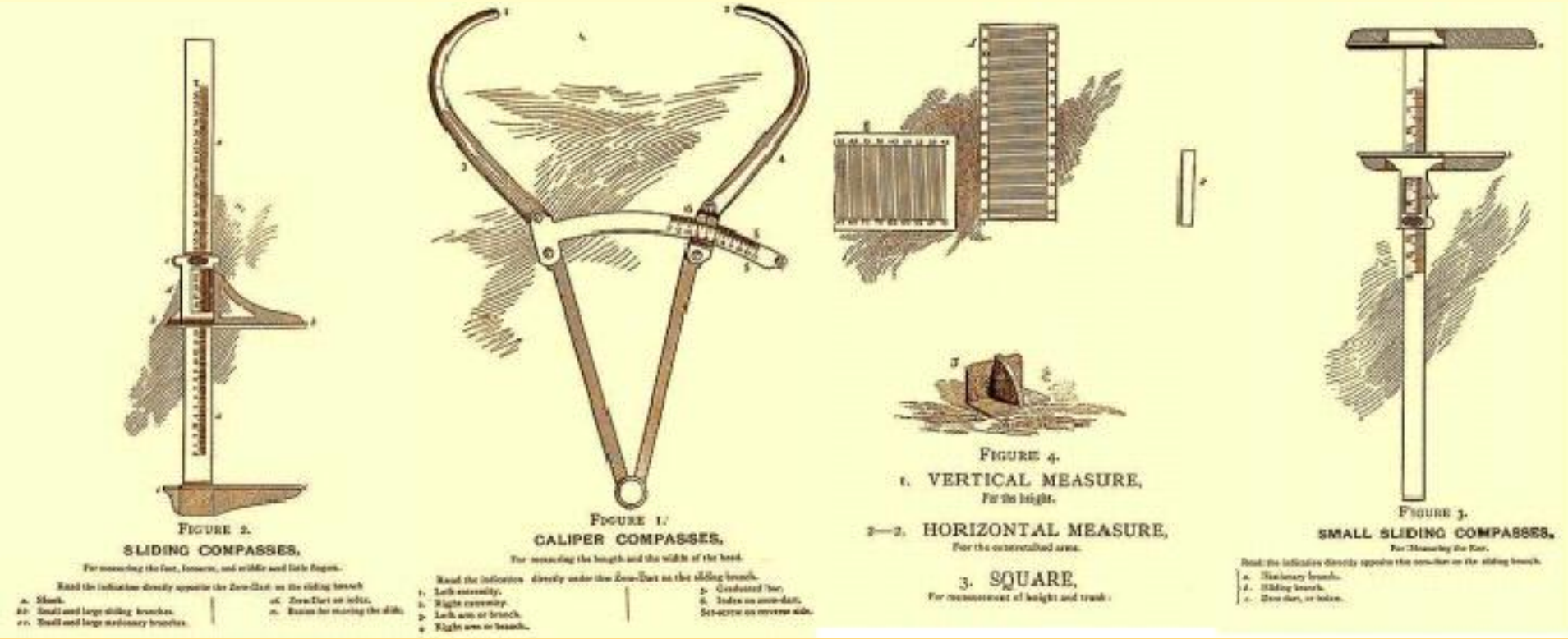


FIGURE 2.
SLIDING COMPASSES.

FIGURE 1.
CALIPER COMPASSES.

FIGURE 4.
1. VERTICAL MEASURE,
For the height.
2—2. HORIZONTAL MEASURE,
For the cranial area.
3. SQUARE,

FIGURE 3.
SMALL SLIDING COMPASSES.

Les instruments utilisés pour les mesures anthropométriques

Les mesures anthropométriques

Reconnaissance biométrique automatisée

- **Système d'identification automatique basé sur les empreintes digitales -1960**
- **Système d'identification du locuteur - 1969**
- **Reconnaissance de visages par ordinateur -1977**
- **Identification basée sur la rétine -1978**
- **Vérification de la signature automatique -1983**
- **Dynamique de frapper le clavier -1985 –**
- **Reconnaissance de l'iris -1993**
- **Identification automatique en utilisant l'impression de la paume -1998 .**

Il n'y a pas de vérificateur biométrique parfaite est choisie en fonction de l'application:

•***L'application nécessite une vérification ou d'identification***? Si une application nécessite l'identification d'un objet dans une grande base de données a besoin d'un facteur biométrique évolutive et bonne netteté (ex empreintes digitales, de l'iris ou de l'ADN.);

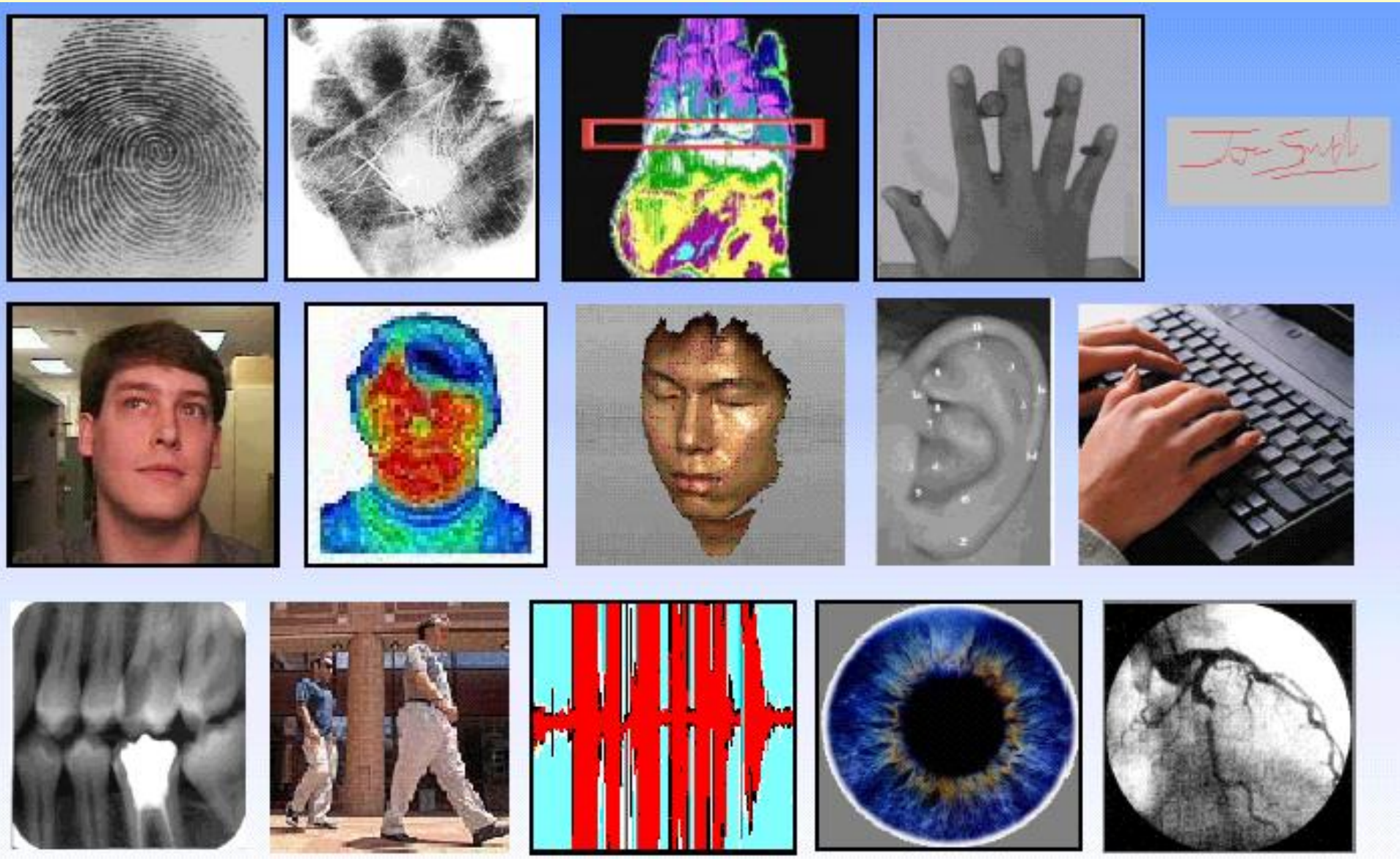
•***Quelles sont les habitudes d'utilisation de l'application?*** L'application est assisté (semi-automatique) ou sans aide (entièrement automatique);

•***Quelles sont les exigences de stockage d'application?*** Les applications accédant à des bases de données à distance pour faire de la reconnaissance nécessite des modèles plus petits;

•***Quelle est l'importance des exigences de performance***? Ainsi, une application qui nécessite une grande précision a besoin d'un facteur biométrique a haute distinction.

•***Quelles sont les caractéristiques biométriques acceptables pour les utilisateurs?*** Les applications commerciales les plus populaires ont les attributs suivants: coopératives, visibles, fermes et privés, avec utilisation fréquente l'inscription et la reconnaissance sans aide contrôlée, fonctionnant dans un environnement standard.

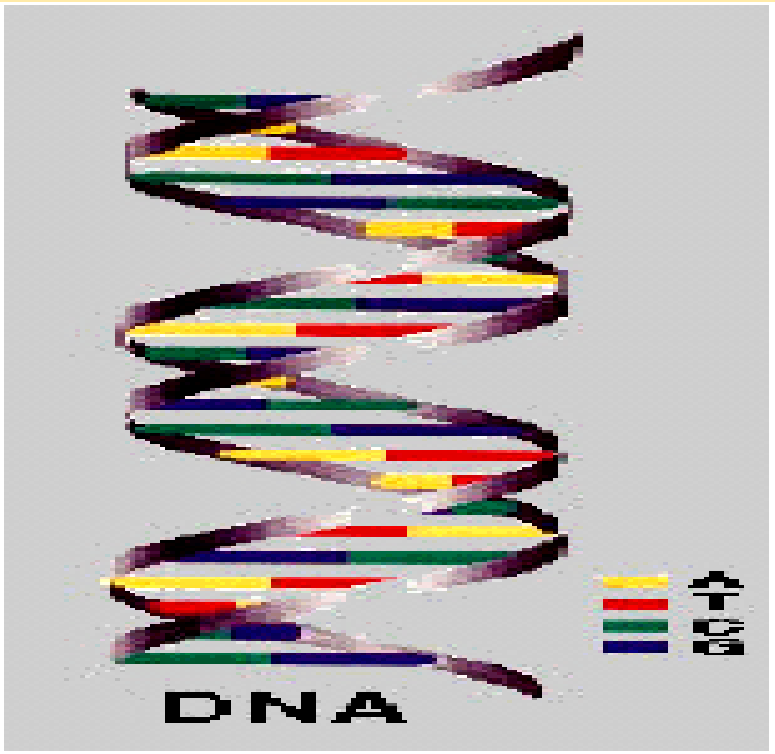
VERIFICATEURS BIOMETRIQUES

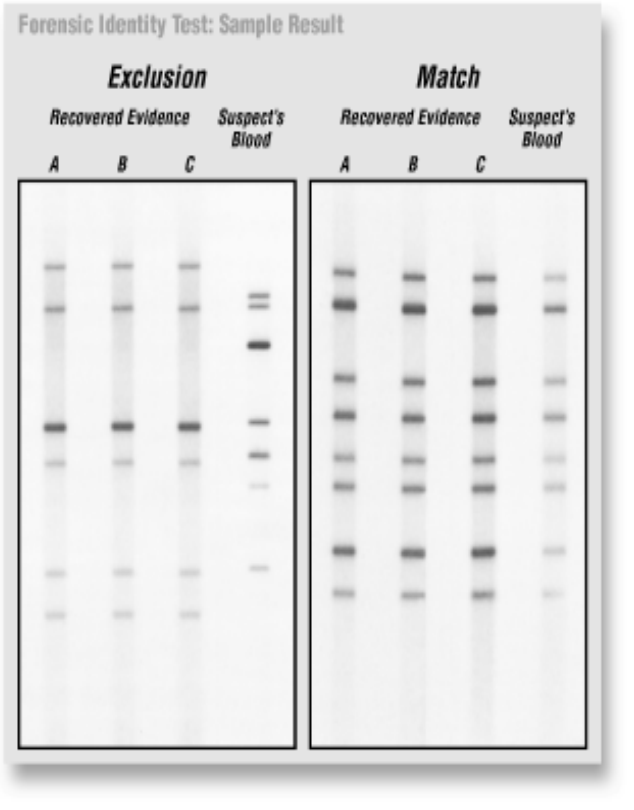


ADN – L'acide désoxyribonucléique - est un code à une dimension unique de son identité , à l'exception des jumeaux identiques (monozygotes) de motifs qui ont d'ADN identiques .

ADN *est utilisé spécifiquement pour les demandes de reconnaissance des personnes judiciaires et de médecine légale .*

Limitations: indique la contamination et de la sensibilité d' un échantillon d'ADN; peut être facilement volé et ensuite utilisé pour un usage particulier; insuffisante pour des applications en temps réel ;
soulève des questions de violation de la vie privée .



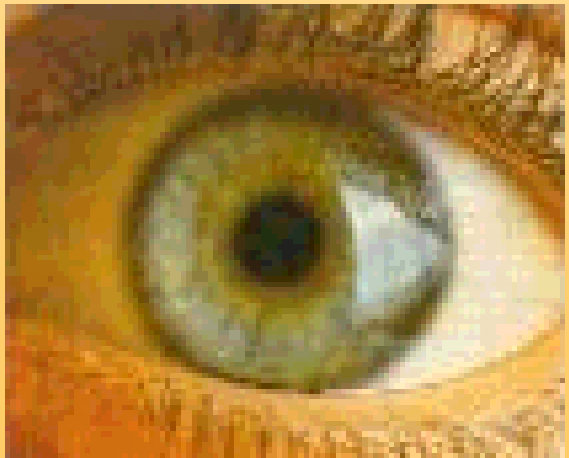


Le visage - est l'un des facteurs biométriques les plus acceptées ;

- Les approches les plus courantes est la méthode consistant à :
  - La forme et la position relative des différents attributs du visage (yeux, nez, les lèvres, le menton, les sourcils);
  - Dans l'analyse globale de l'image de visage , qui est l'image du visage comme une combinaison de canonique pondéré.
  - La reconnaissance faciale est un défi dans le développement de techniques de reconnaissance spécifiques qui peuvent être tolérants aux effets de l'âge, les expressions faciales, les variations de l'environnement et les changements dans l' angle de la face dans l'image, le degré d'éclairage , etc.
  - Le déguisement est une des difficultés d'applications sans assistance .

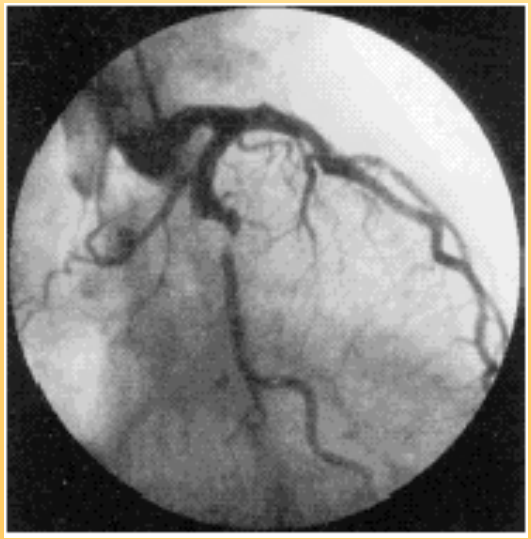
Iris - texture visuelle de l'iris humain est déterminé par le processus chaotique morphogénétique qui se développe en l'embryon et est pensé pour être distincte à chaque personne et chaque oeil et stable avec l'âge ;

- L'iris est un diaphragme qui traverse l'avant de la lentille et est la couleur qui entoure la pupille ;
- Une image de l'iris est un motif complexe constitué de plusieurs éléments distinctifs (ligaments , des arches , des sillons , des crêtes, des bagues, des taches de rousseur, etc.) ;
- Iris capture d'image implique la collaboration de l'enregistrement de l'utilisateur dans la zone centrale de l'image et d'un équilibre minutieux luminosité, mise au point, la résolution et le contraste ;
- La technologie de reconnaissance de l'iris est considérée comme étant faite avec une grande précision et la vitesse , et les systèmes actuels sont devenus efficaces et à prix raisonnable ;
- Difficultés de l’enrôlement (FTE -7 %)



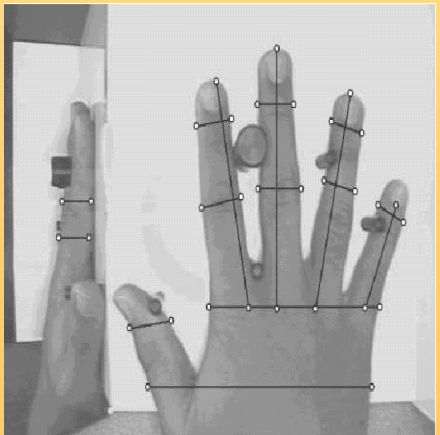
Rétine Scan - vascularisation rétinienne a une structure riche et sont soupçonnés d'être caractéristique a chaque individu et de chaque œil ;

- Il est censé être le facteur biométrique la plus sûre , car il est pas facile de changer ou de copier le système vasculaire rétinien ;
- L'acquisition implique également la coopération du sujet, le contact visuel et un dispositif avec peu d'effort de l'utilisateur ;
- Ces difficultés affectant la rétine de l'acceptation par le public ;
- La vascularisation de la rétine peut divulguer certaines conditions de santé (par exemple, hypertension), Qui est un autre facteur qui pourrait porter atteinte a la vie privée et de créer un obstacle à l' acceptation par le public .



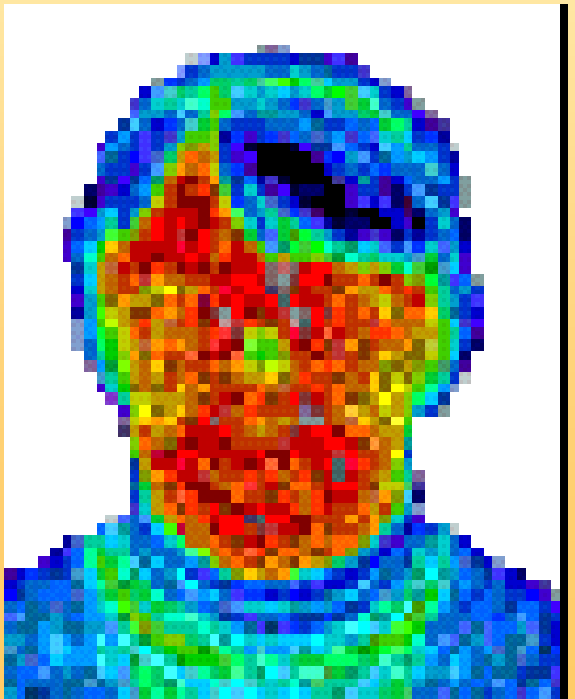
La forme de la main et des doigts - la forme et la longueur de la main et des doigts sont relativement invariant, mais pas très distinctif;

- Ce vérificateur a été utilisé dans l'un des premiers systèmes automatisés biométriques depuis les années 60 ;
- La technique est simple, peu coûteux, facile à utiliser et les conditions environnementales (humidité, robustes anomalies individuelles)
- Le système nécessite la coopération du sujet et de face et le côté avant de l' appareil portatif
- L'image est faite des mesures de la forme, la taille de la paume , la longueur et l'épaisseur des doigts .
- Les besoins de stockage caractéristiques main sont réduits (9 octets)
- En raison de distinction limitées les systèmes basé sur la géométrie de la main sont utilisés typiquement de vérification et ne sont pas appropriées pour d' applications de l'identification;
- Difficulté d'utilisation : la période de croissance, certaines maladies , des bijoux



Thermogrammes infrarouges (visage , les mains et les veines)

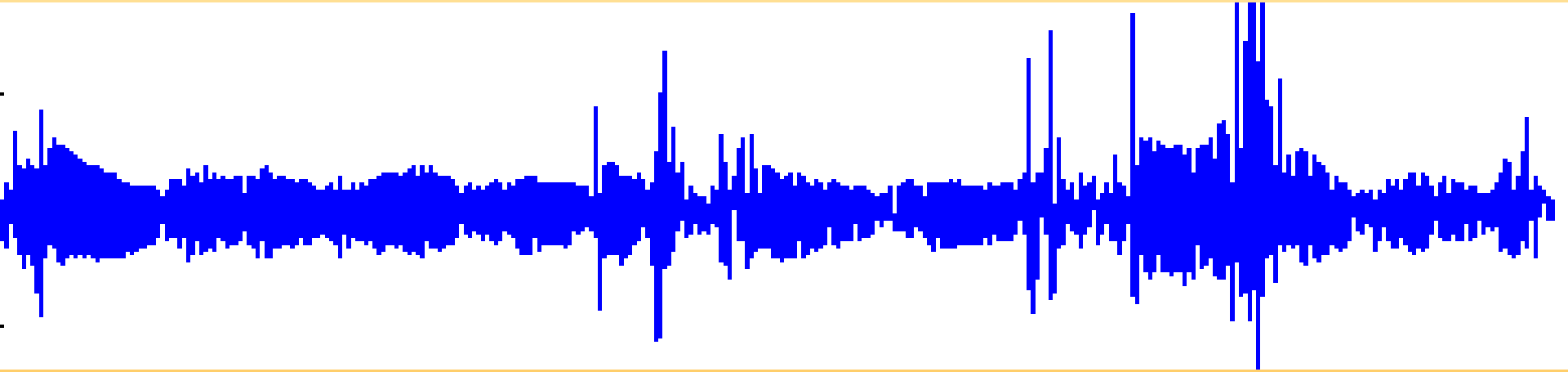
- Le schéma de la chaleur rayonnée par le corps humain est une caractéristique individuelle et peut être capturée par une caméra infrarouge d'une manière semblable à une image ;
- La technologie base sur les thermogrammes est non invasive et peut être utilisé pour reconnaître caché pendant la nuit ;
- Le défit de cette technologie doit faire face apparaît dans des environnements non contrôlés où les objets dégagent de la chaleur dans le voisinage du corps et affectent de manière décisive acquisition d'image ;
- Une technologie connexe est l'utilisation d'images infrarouges capturés à proximité de balayer la structure de la veine ;
- Les capteurs infrarouges ont des prix prohibitifs .



La Voix - est considéré comme un facteur biométrique largement acceptée, facile et peu coûteux acquis ;

- La voix d'une personne dépend de certaines caractéristiques personnelles physiologiques invariants (de l'appareil vocal, cordes vocales, de la bouche, de la langue, de la cavité nasale, les lèvres), mais aussi certains comportements, qui varie avec l'âge, la santé, les émotions .
- Il est possible dans les applications nécessitant la reconnaissance d'une personne par téléphone, mais pas considéré comme suffisamment distincts pour permettre l'identification des individus à partir d'une grande base de données d'utilisateurs ;

Problèmes: la variabilité/imitation de la voix pourraient induire en erreur les systèmes de reconnaissance



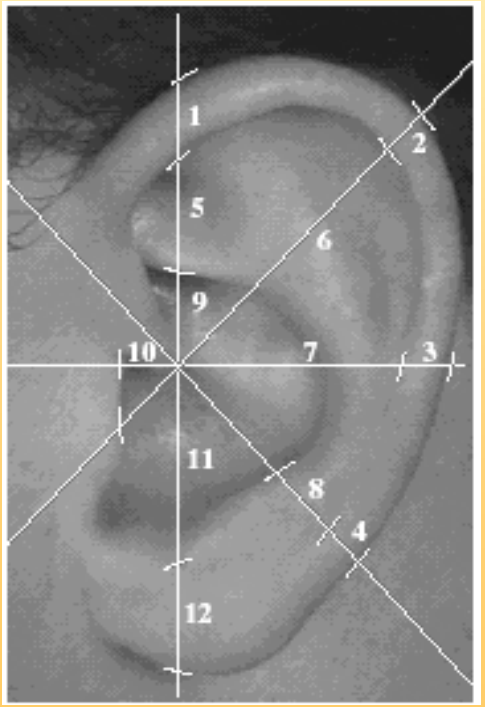
La Signature - est une façon simple et concrète dans laquelle une personne dirige sa main après un certain chemin qui est caractéristique - Est-ce un facteur biométrique comportementale qui change au fil du temps et est influencée par l'état physique et émotionnel de ceux qui signent ;

- Signatures des individus varie beaucoup: même les signatures successives varie considérablement ;
- Signature est acceptable dans de nombreuses opérations gouvernementales, juridiques et commerciales comme moyen de vérification;
- Problème: les contrefacteurs peuvent se reproduire signatures de tromper le système de vérification automatique

- **L'oreille** - la taille , la forme et la structure du cartilage de l'oreille se distinguent par des personnes différentes ;

- Une des caractéristiques de l'oreille ne sont pas prévu pour être un seul individu , il a donc le fort caractère distinctif ;

- Les approches de la reconnaissance des personnes est basées sur la comparaison des distances entre les différents points de référence de l'oreille



D' autre vérificateurs biométriques : marche, odeur, dynamique du typage

Comparison des verifications biometriques

Identificateur Biométrique	Universalite	Distinctivite	Permanence	Colectabilite	Performance	Acceptance	Surete
ADN	+	+	+	-	+	-	-
Oreille	0	0	+	0	0	+	0
Face	+	-	0	+	-	+	+
Thermogramme faciale	+	+	-	+	0	+	-
Eimpreinte	0	+	+	0	+	0	0
Marche	0	-	-	+	-	+	0
Geometrie de la maine	0	0	0	+	0	0	0
Veines de la maine	0	0	0	0	0	0	-
Iris	+	+	+	0	+	-	-
Typage	-	-	-	0	-	0	0
Odeur	+	+	+	-	-	0	-
Retine	+	+	0	-	+	-	-
Signature	-	-	-	+	-	+	+
Voix	0	-	-	0	-	+	+

+ Grande ; 0 Moyen; - Reduit

SB. Performances

- Deux échantillons des mêmes caractéristiques biométriques, prises de la même personne, ne sont pas exactement les mêmes a cause de:

- Capteur ;
- des changements de caractéristiques biométriques ;
- les conditions environnementales;
- l'interaction de l'utilisateur avec le capteur.

- Le réponse d'un SB est une réponse de similarité – s, qui quantifie les similitudes entre l'entrée et le modèle;

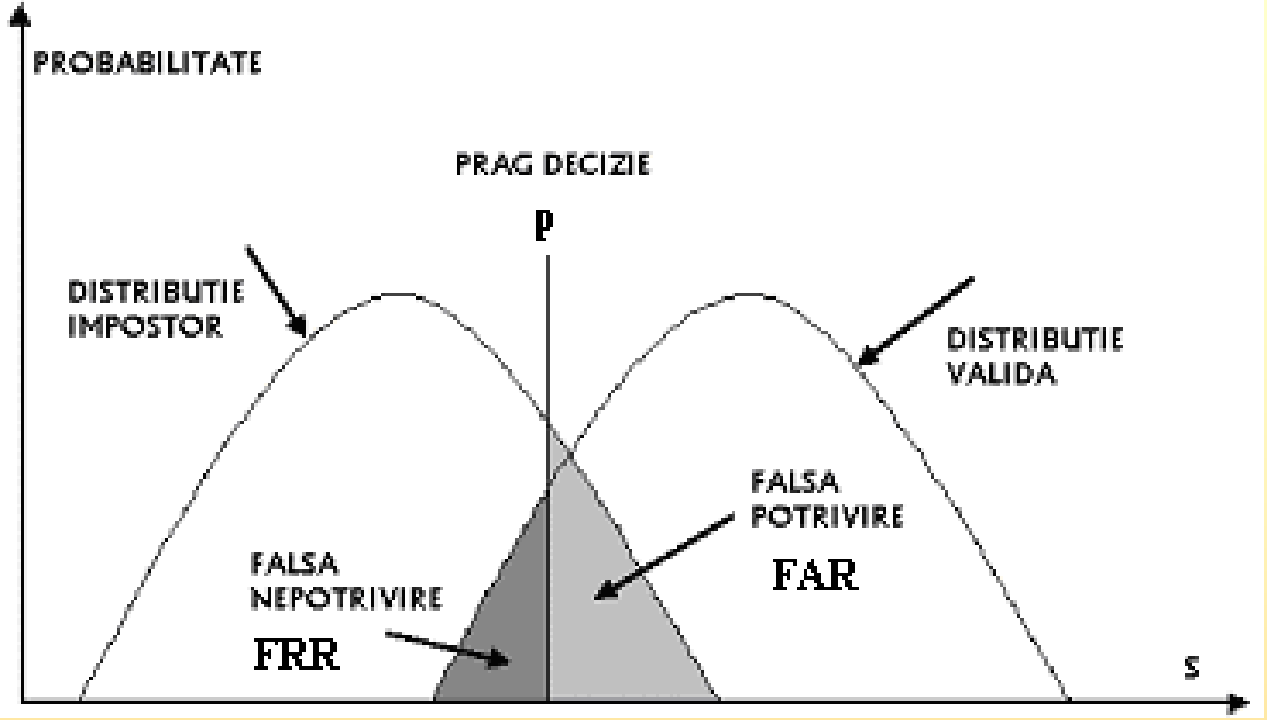
- La de décision est pris par un comparaison de **s** a un seuil a priori établie ;

Les Erreurs de systèmes de vérification biométrique :

- ***Le taux de fausse correspondance/acceptation (FAR)***
- ***Le taux de fausse inadéquation/rejet (FRR)***

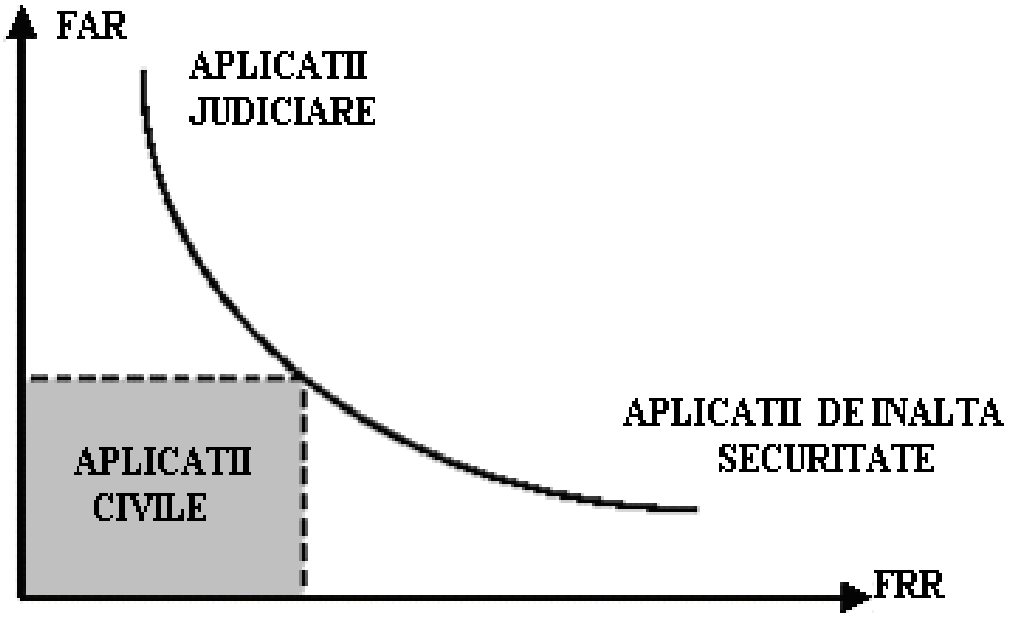
Hypothèses :H0 : XI ≠ XM - vecteurs sont des personnes différentes ;
H1: XI = - XM vecteurs proviennent de la même personne

Décision: D0 : la personne est pas qui prétend être ;
D1 : la personne est qui prétend être.



Les Erreurs de systèmes de vérification biométrique

Points de fonctionnement typiques pour différentes applications



Caracteristique biometrique	EER	FAR	FRR	Parametres de Test (conditions)	Test
Face	-	1 %	10 %	Différent d'éclairage intérieur / extérieur	FRVT (2002)
Eimpreinte	-	1 %	0.1 %	Les données fournies par le gouvernement américain	FpVTE (2003)
	2%	2 %	2 %	Spins ou de distorsion exagérée peau	FVC (2004)
Forme de la maine	1%	2 %	0.1 %	Avec anneaux et mauvaise position	(2005)
Iris	0.01 %	0.0001 %	0.2 %	Les meilleures conditions	NIST (2005)
Voce	6%	2 %	10 %	Texte indépendant, multilingue	NIST (2004)

Le niveau actuel de la performance des systèmes unimodale (taux d'erreur)

EER= Error to Enroll Rate; FAR= False Acceptance Rate; FRR= False Rejection Rate; Face Recognition Vendor Tests (FRVT); Fingerprint Verification Competition (FVC); National Institute of Standards and Technology (NIST)

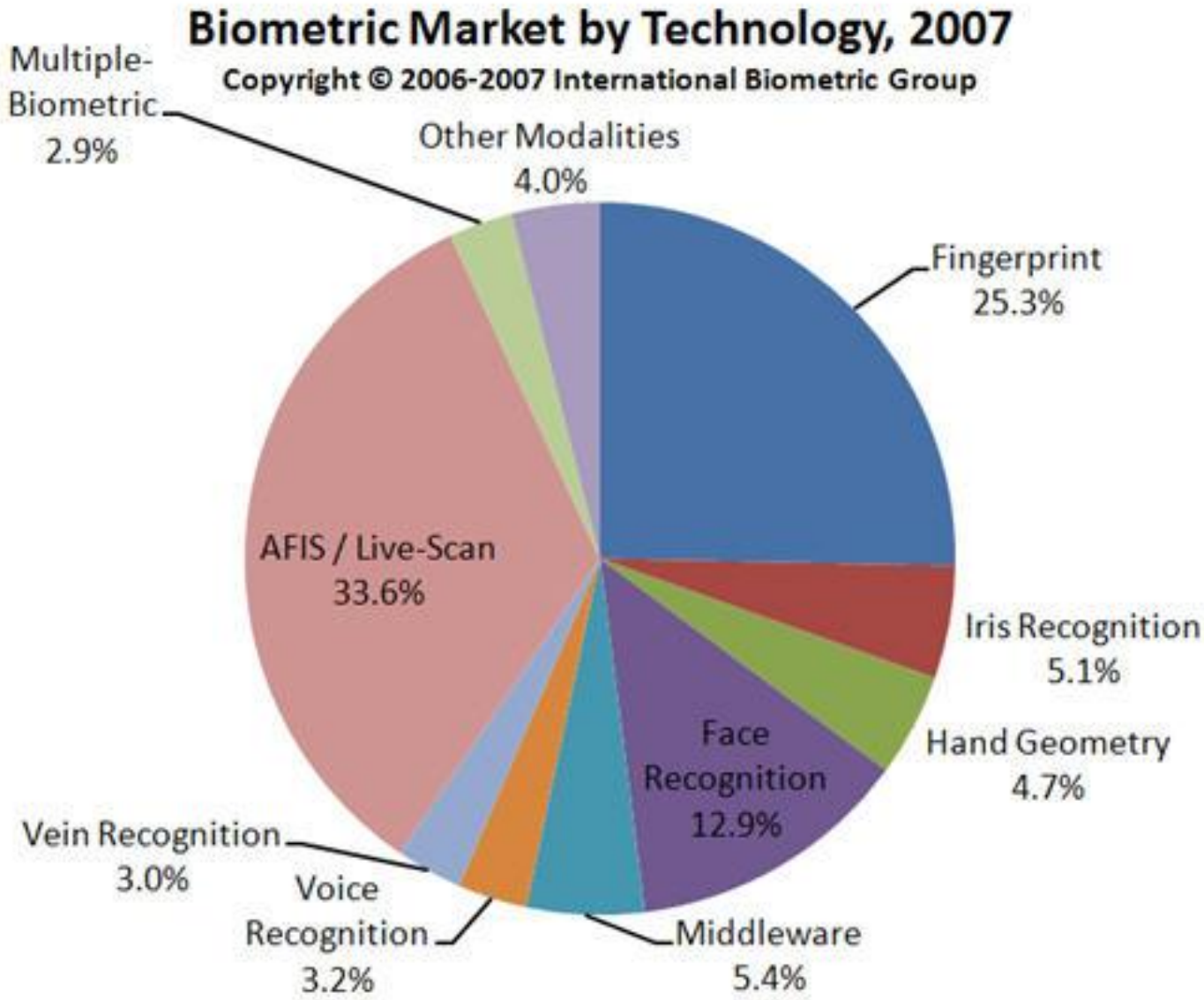
- Un afflux d'environ 300.000 passagers par jour (dans les aéroports de New York) à utiliser des cartes d'identité biométriques pour l'authentification, il y avait 6.000 de faux rejets par jour si elles utilisent des empreintes digitales, face - 45.000, 30.000 - voix!

	Empreinte	Maine	Iris	Face	Voix	Signature	Retine
Minim	100 bytes	9 bytes	256 bytes	84 byte	1 Kb	500bytes	96 bytes
Maxim	2 Kb	-	2 Kb	2.5 Kb	3 Kb	-	
Typic	300 bytes	9 bytes	512 bytes	2 Kb	1 Kb	1kb	96 bytes

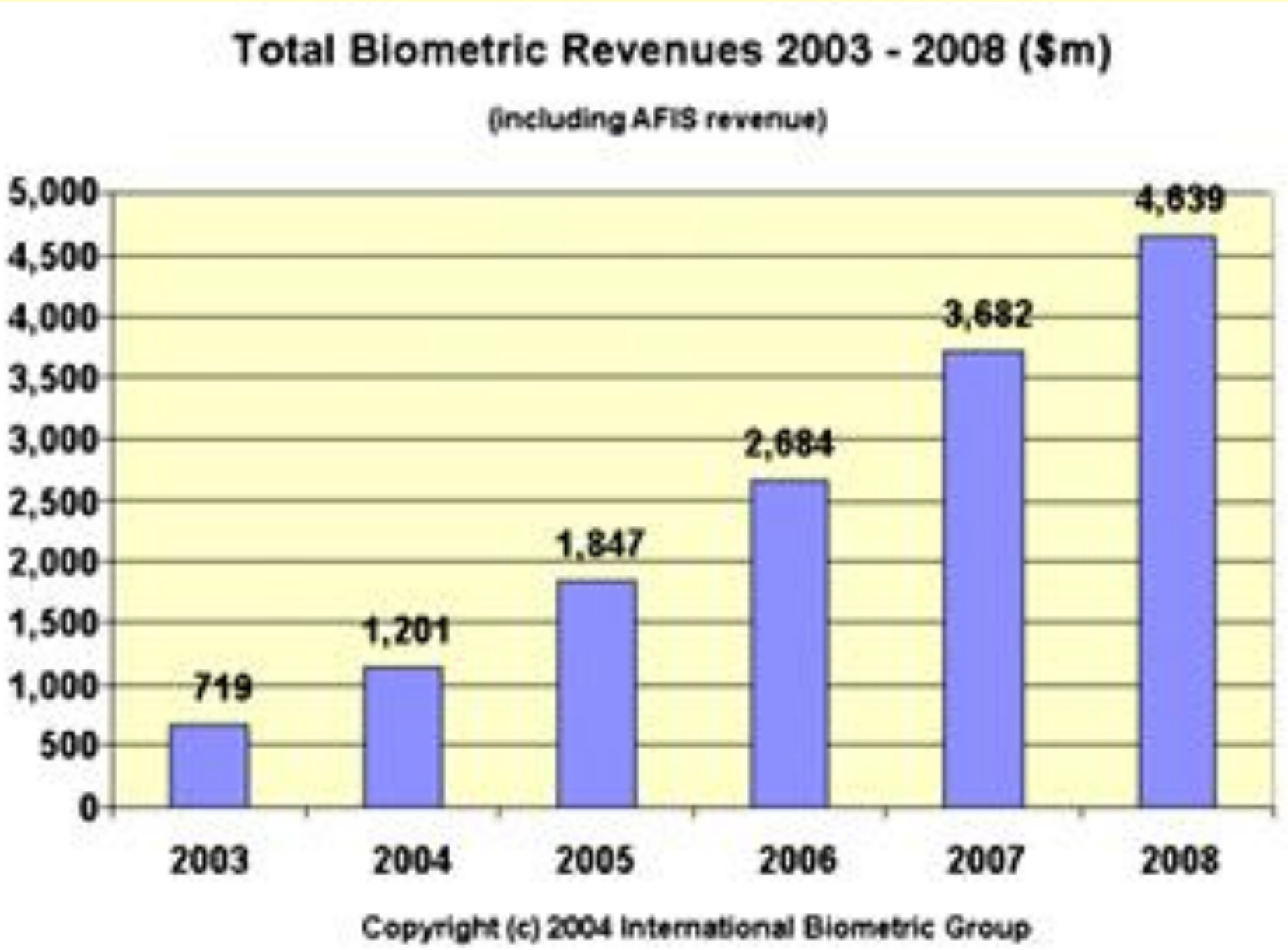
Les dimensions approximatives des différents modèles de VB

Systeme	Temps de transaction (sec)			Temps + temps introduction PIN
	Moyen	Median	Minim	
Face	15	14	10	Non
Empreinte (optic)	9	8	2	Non
Empreinte (chip)	19	15	9	Non
Maine	10	8	4	Oui
Iris	12	10	4	Oui
Veines	18	16	11	Non
Voix	12	11	10	Non

Vitesse de transaction des Systèmes biométriques



Marché pour le VB la plus répandue


Total Biometric Revenues 2003 - 2008 ($m)
(including AFIS revenue)
5,000
4,500
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
719
1,201
1,847
2,684
3,682
4,639
2003
2004
2005
2006
2007
2008
Copyright (c) 2004 International Biometric Group

NORMES BIOMETRIQUES

L'objectif: soutenir l'interopérabilité des systèmes et des applications biométriques mis au point par des fabricants différents et de permettre l'échange de données biométriques;

ANSI -Technical Committee M1, **Biometrics**

ISO/IEC - Joint Technical Committee 1 (JTC1)
- SC 37 Biometrics;
-SC68 Passports&Drivers Licenses

BioAPI Consortium – a proposée la conception d'une API (Application Program Interface) pour les systèmes biométriques afin d'améliorer la compatibilité dans un large éventail de technologies biométriques et de faciliter la communication entre les systèmes mis en place

NIST - (National Institute of Standards and Technology) prin specificațiile ***NIST 6529-A/2004,*** numit CBEFF (Common Biometric Exchange Formats Framework), promovează interoperabilitatea aplicațiilor și SB.

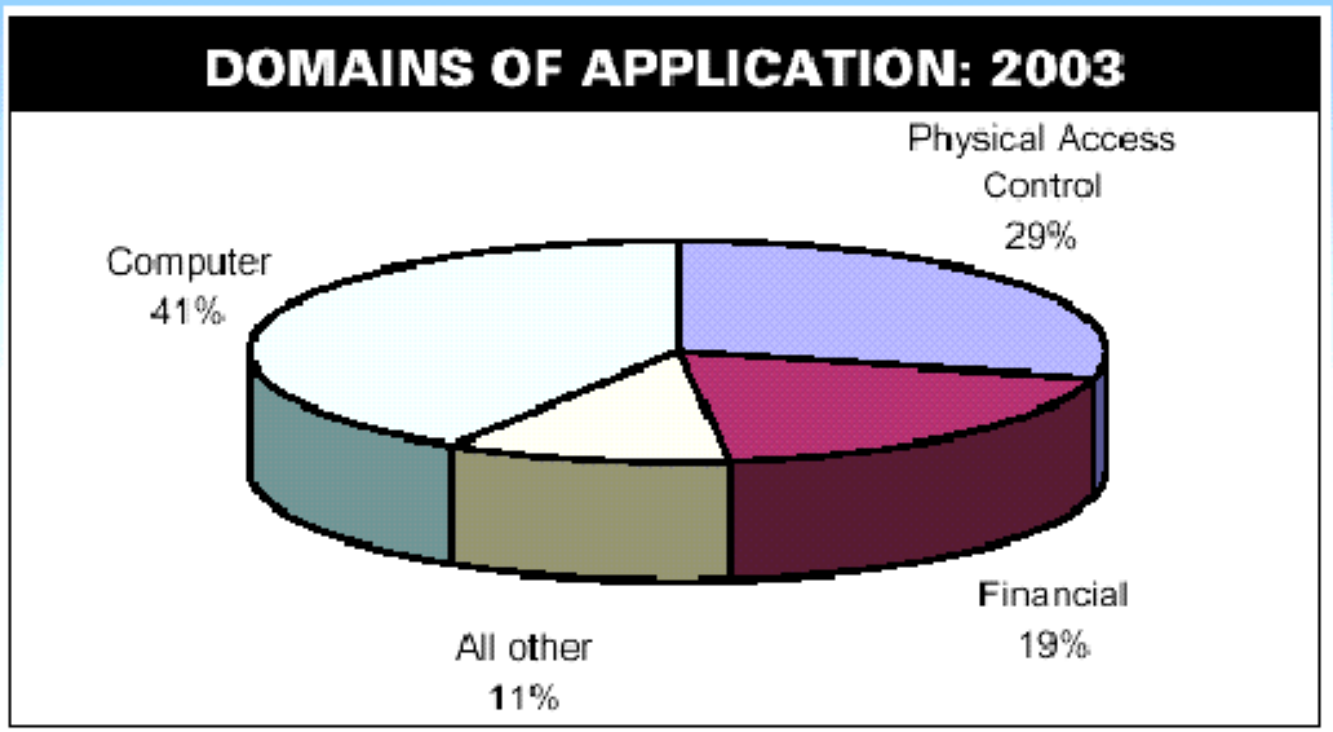
NORMES (ex.)

- ANSI/INCITS 358-2002, Information Technology: BiometricApplication Programmers Interface (BioAPI) Standard
- ANSI/INCITS 377-2004, Information Technology: Finger Pattern Data Interchange Format
- ANSI/INCITS 378-2004, Information Technology: Finger Minutiae Data Interchange Format
- ANSI/INCITS 379-2004, Information Technology: Iris Image Interchange Format
- ANSI/INCITS 385-2004, Information Technology: Face Recognition Format for Data Interchange

APLICATIONS de la BIOMETRIE

- Services financiers
- Police / justice
- Applications gouvernementales
- Immigration et Voyage
- e-Commerce et téléphone
- Contrôle d'accès PC / Réseau / "sur place"
- Transactions - ATM
- Identification des criminels
- Identification des citoyens

Domains of Application



Domaines d'application des SB

SYSTEMES MULTIMODALES

LIMITES DES SYSTÈMES unimodale

- manque d'universalité de certaines fonctionnalités

-(Échec d'enregistrement - ~ 4% empreintes digitales, de l'iris ~ 7%);

- Noisy signaux captés par les capteurs en raison de l'utilisation incorrecte par les clients et les conditions ambiantes (humidité, la saleté, la poussière, etc.)

- sécurité des capteurs utilisées

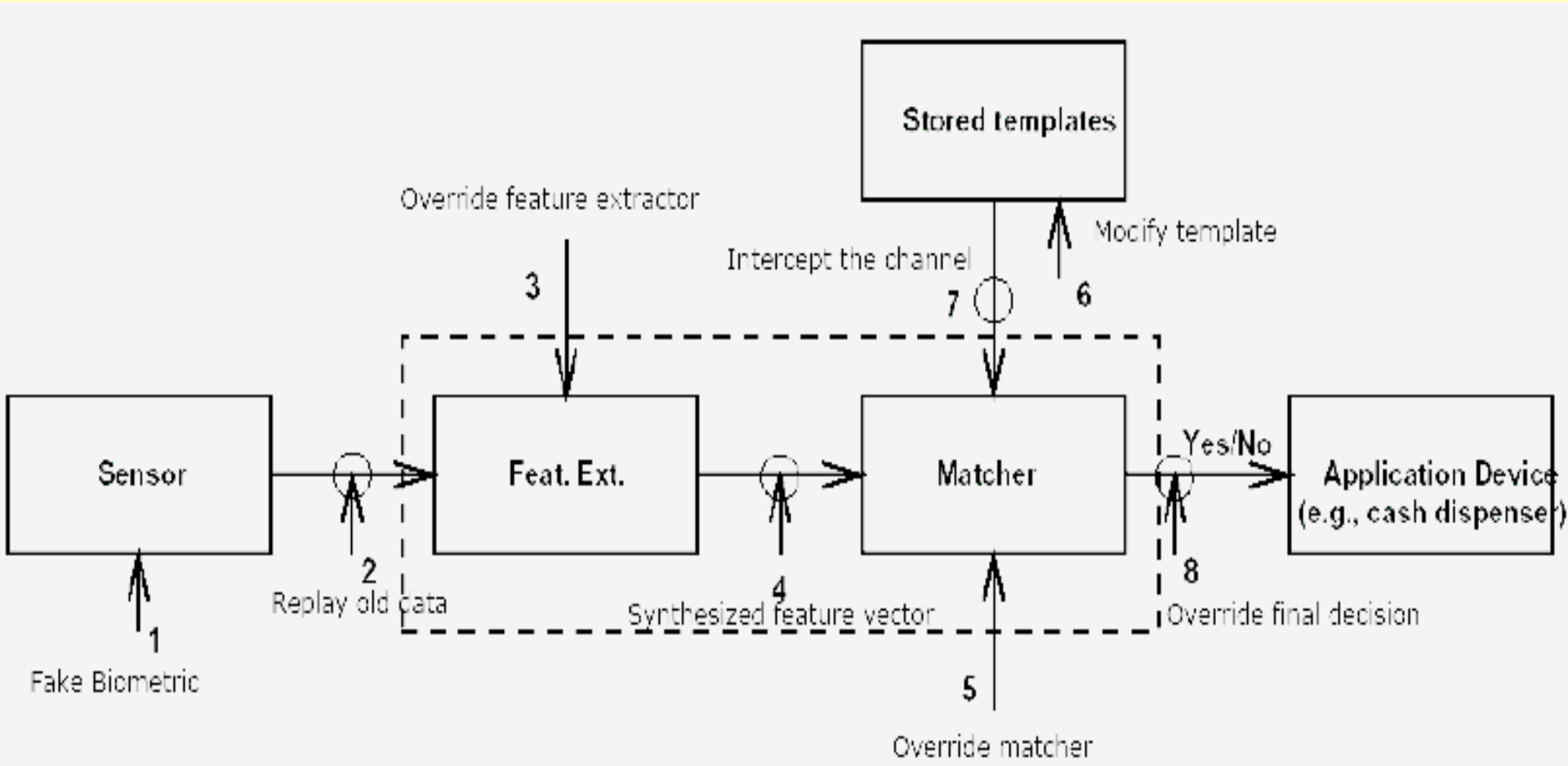
- Limitation de la discrimination en raison de la variabilité biométrique "in-class" assez grand "interclasses" réduit;

- La performance de reconnaissance des systèmes sont limités supérieur à un certain niveau;

- Taux d'erreur inacceptables pour les systèmes biométriques unimodales;

- manque de permanence et de la variabilité temporelle des caractéristiques biométriques;

- possibilités de fraude / clonage



Potential Attack Points (*Ratha et al.*)

Clone volontaire de l'empreinte

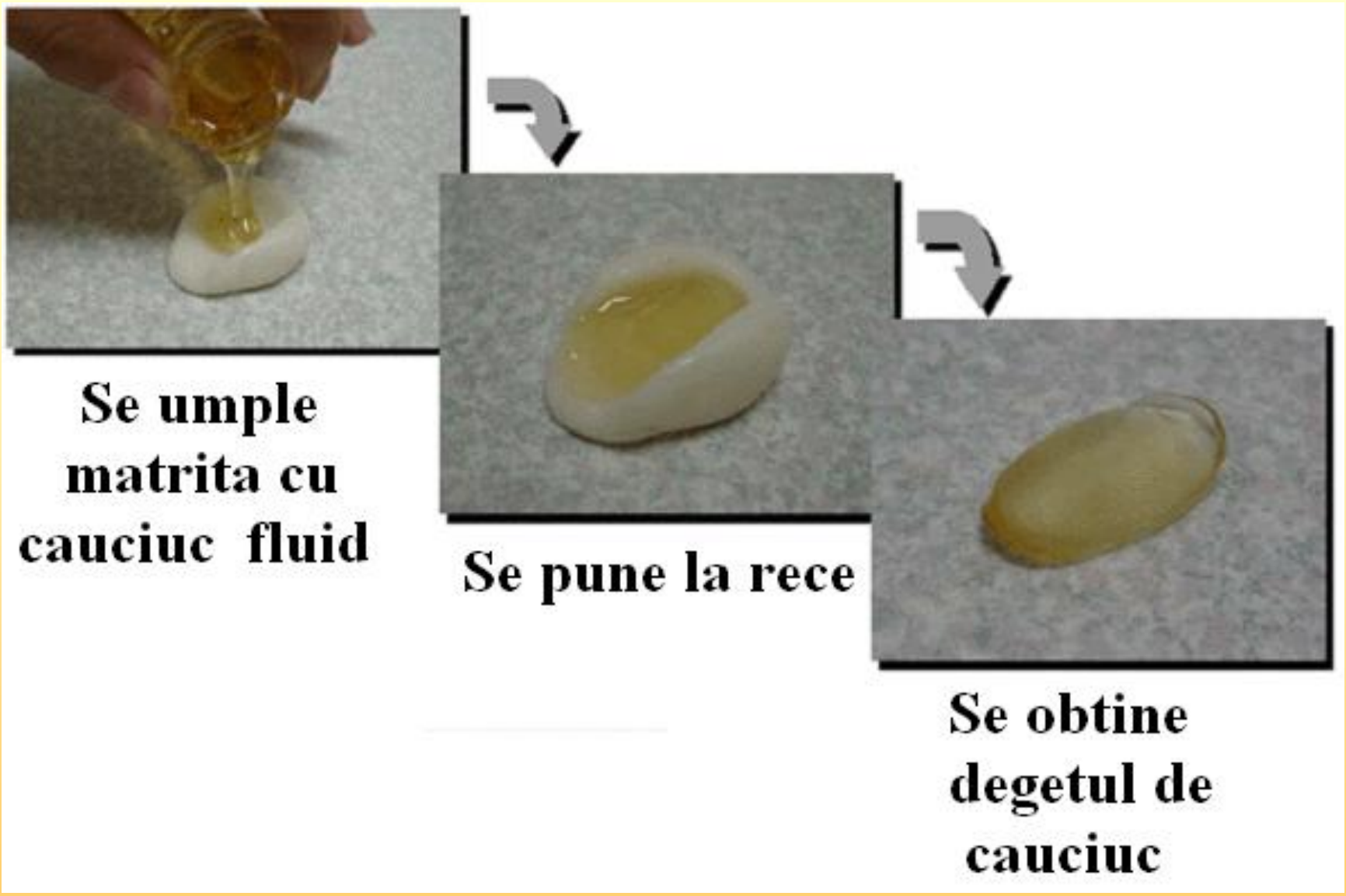
(méthode Matsumoto)

Plasticul se inmoaie in apa calda

Se imprima amprenta

Se obtine matrita

Operatiile dureaza ~10 min.



Le clone a été testé sur 11 types de capteurs capacitifs et optiques qui ont réussi à "tromper" !!!

Biométrie Multimodale

Les principales caractéristiques d'un système biométrique multimodal:

a) l'architecture - la séquence dans laquelle les différentes caractéristiques sont acquisition

b) les sources d'information - utilisées pour surmonter les systèmes des limites

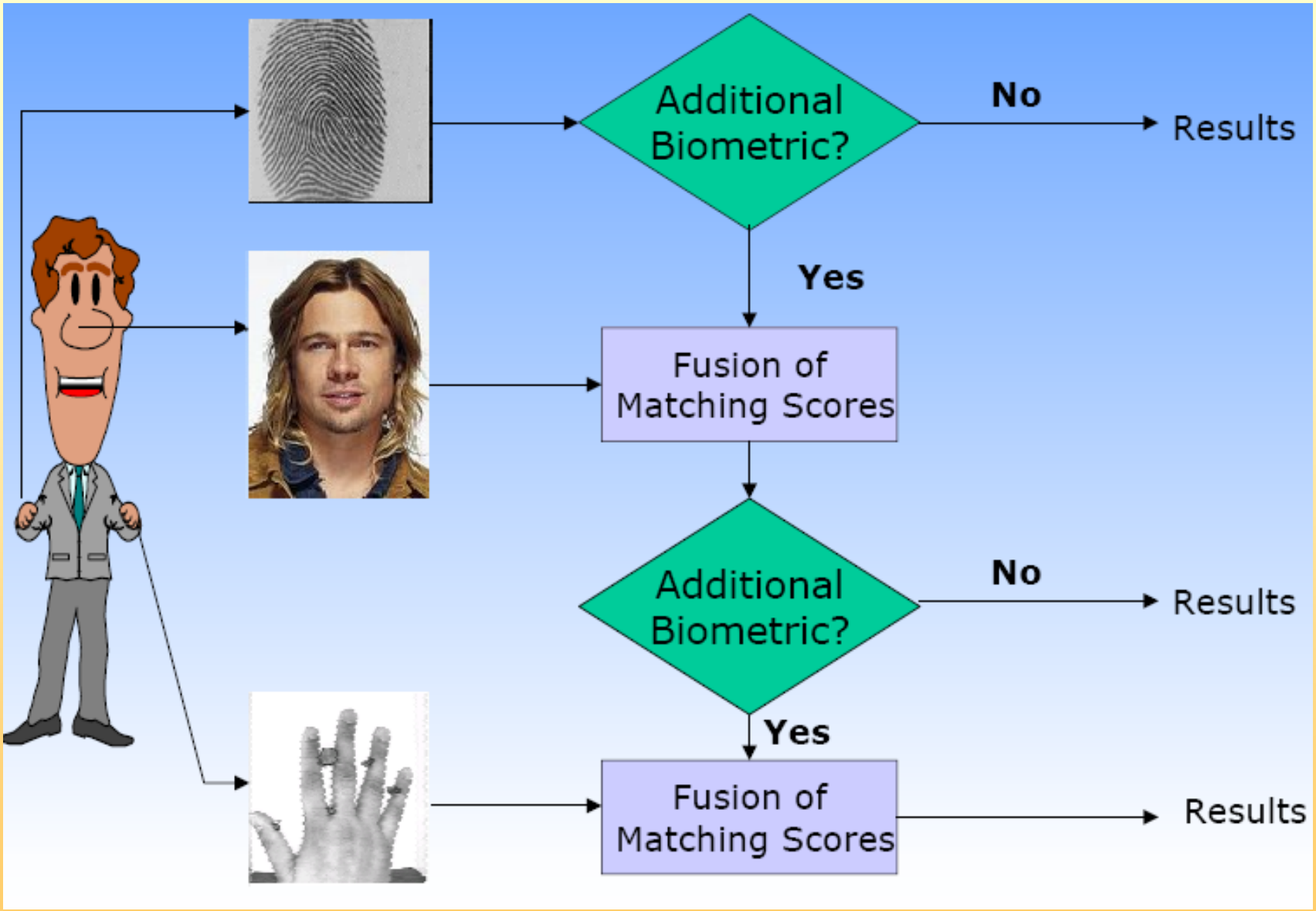
c) les niveaux de fusion - (capteurs, les caractéristiques d'extraction, de comparer les paramètres, décision)

d) **la méthodologie** utilisée pour intégrer plus de vérificateurs

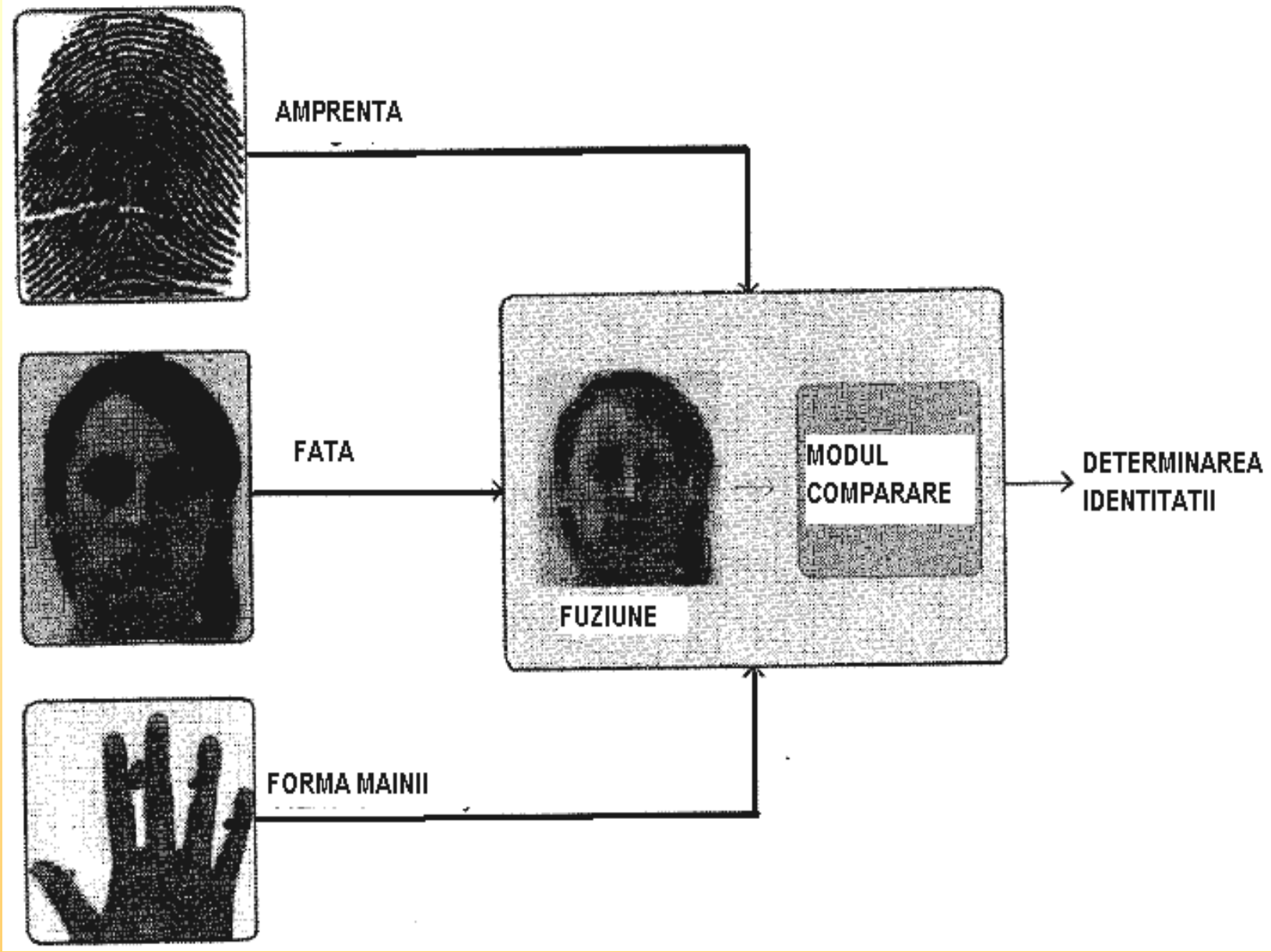
- architecture: parallèle/ série(cascade)

- système biométrique multimodales série sont recommandée pour application de sécurité réduite (ATM, ..)
- parallèle est recommandée en applications au niveau élevée de sécurité (militaire, espace,...)
- combinassions architecture parallèle sérielle (structure hiérarchique)

SYSTEME BIOMETRIQUES MULTIMODALES EN CASCADE

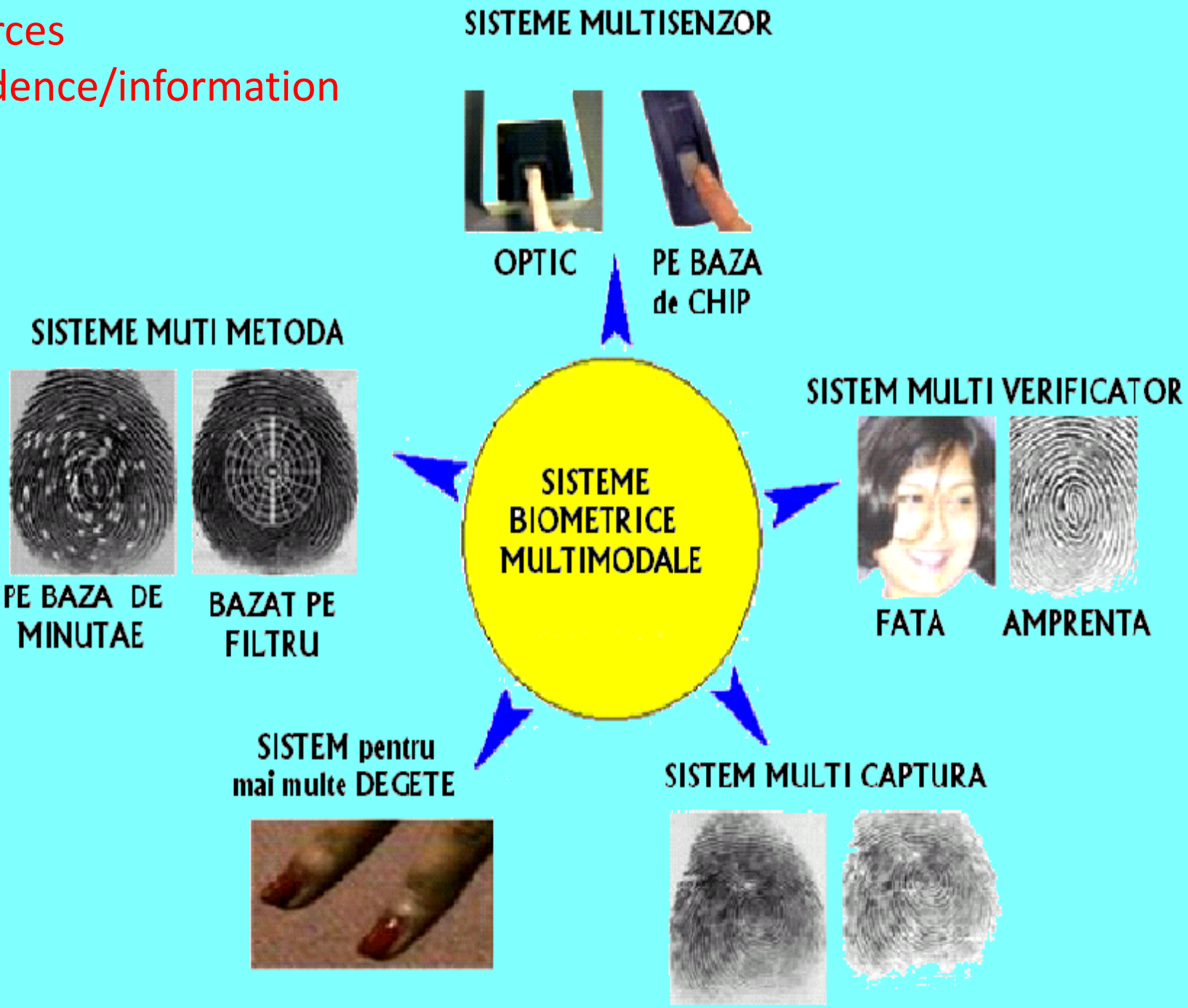


Cascaded Multimodal Biometric System (after Jain et al.)



En mode cascade les captures biométriques sont traitée simultanément pour établir l'identité

- sources d'evidence/information



Sources d' informations multi biométriques

Information biométrique multimodal peut provenir de diverses sources:

Multi-capteur - la même caractéristique biométrique est capturée à l'aide de divers capteurs pour extraire des informations à partir de différentes images enregistrées (spatiales);

Multi-algorithme - le même enregistrement de caractéristique biométrique est traité en utilisant divers algorithmes. Par exemple, même la capture d'empreintes digitales peut être traitée par un algorithme basé sur la texture et minuties (des détails de base) la réalisation d'un système d'amélioration de la performance;

Multi-instance (caractéristique) - utilisé bon nombre des mêmes traits caractéristiques biométriques (par exemple, l'index de la main droite et à gauche de l'iris des deux yeux.)

Multi-échantillonnage - même la capture de capteur multiples traits biométriques de même afin de capturer la variabilité d'un trait ou d'obtenir une représentation plus complète du trait;

Multimodal - captures combinent différents traits biométriques pour établir l'identité;

Hybride - intègre un sous-ensemble des scénarios ci-dessus.

Biometric features
Voice, Face, Lips movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand geometry
Fingerprint, Voice, Hand geometry
Voice, Hand geometry
Facial theromogram, Face
Iris, Face
Palm print, Hand geometry
Ear form, Voice
Voice, Lips movement

Caractéristiques biométriques qui sont appropriés pour les systèmes multimodal multi- checker

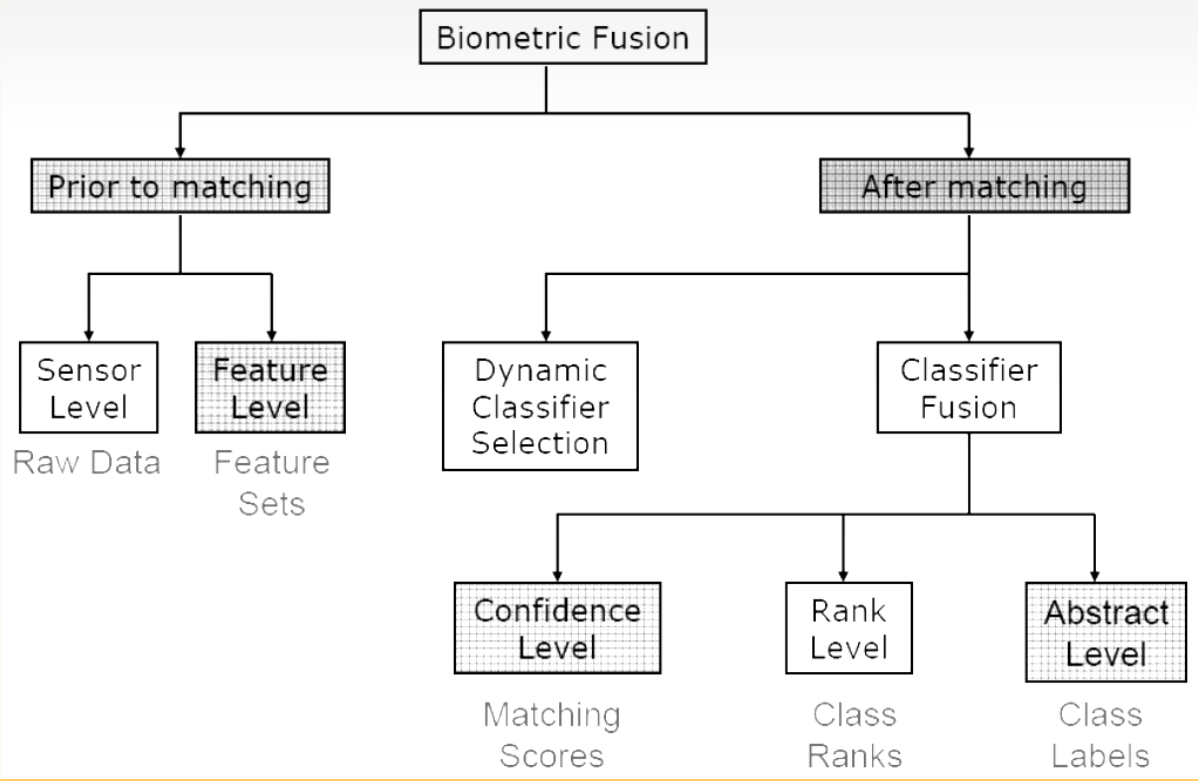
Les niveaux auxquelles on peut faire la fusion dans les systèmes biométriques multi vérificateur sont au niveau :

1 *modules capteurs* – on combine les echantions de la sortie des capteurs;

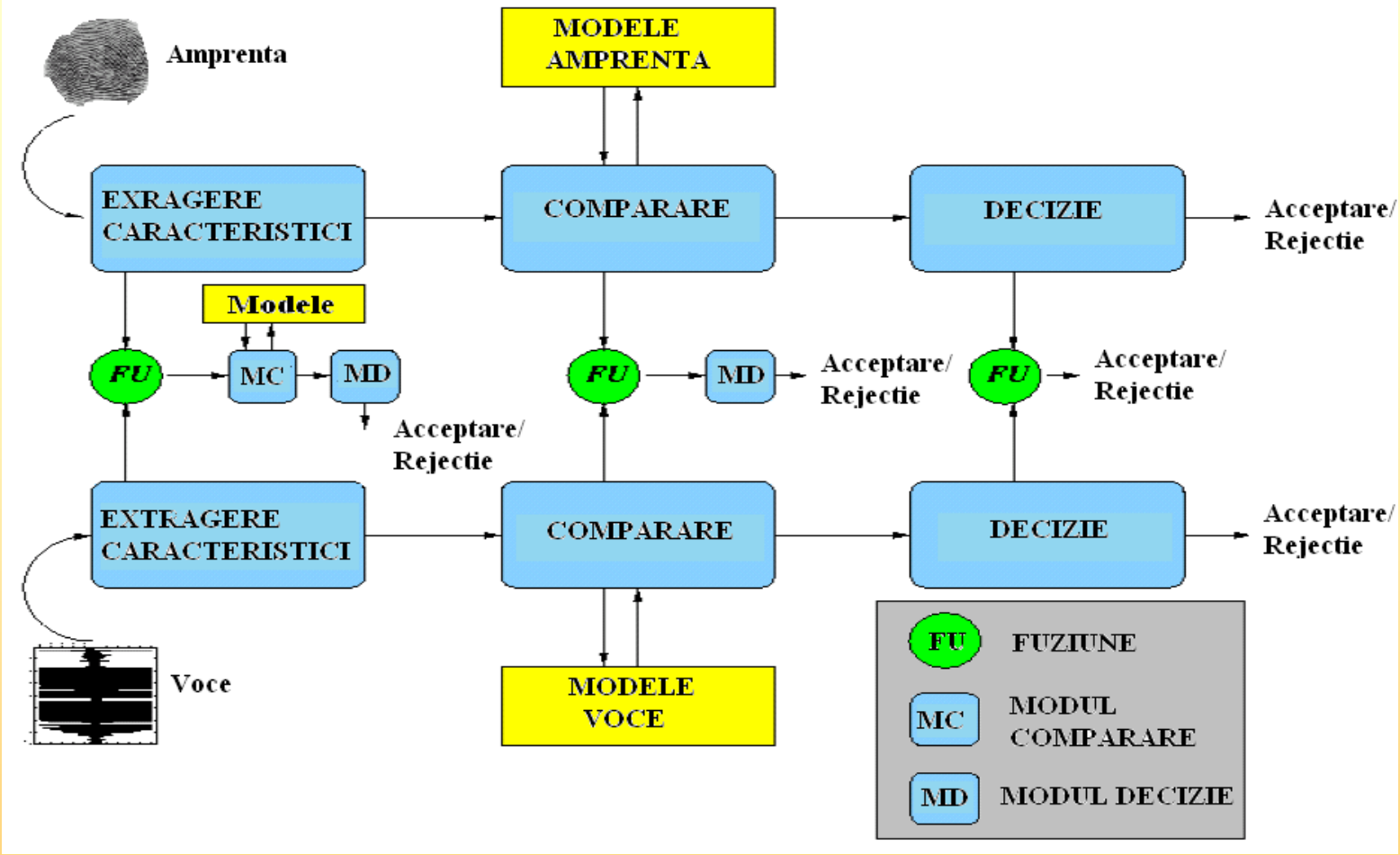
2. *modules d' extractions des caractéristiques* – on combine les caractéristiques extraites de chaque capteur;

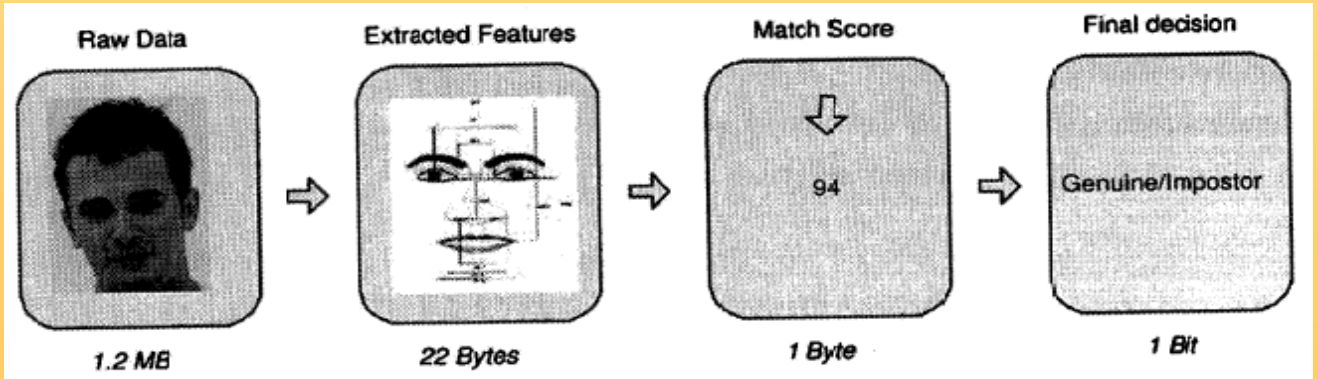
3. *modules de comparaison des paramètres* - on combine les résultats des comparaisons;

4. *modules de décision* – on combine les décisions d' identité;



NIVEAUX de FUSION





TECHNIQUES de NORMALISATION

• Scorurile de ieşire de la modulele de comparare furnizate prin diferite modalităţi sunt heterogene, prin urmare, este necesară normalizarea scorurilor

• Min-Max (MM): Mapeaza scorurile brute în intervalul [0,1], Max (S) şi min (S), fiind punctele de sfârşitul intervalului scorul, în general, furnizate de distribuitori:

$$n = \frac{s - min(S)}{max(S) - min(S)}$$

•Z-scor (ZS): Prin utilizarea acestei metode, scorurile sunt transformate într-o distribuţie cu medie de 0 şi abaterea standard de 1.

$$n = \frac{s - mean(S)}{std(S)}$$

Tanh (TH): Metoda constă în una din tehnicile statistice robuste şi mapează scorurile în intervalul [0,1]:

$$n = \frac{1}{2}\left[\tanh\left(0.01 \frac{s - mean(S)}{std(S)} \right) + 1 \right]$$

Adaptiva (AD): suprapunerea rezultatelor distribuţiilor autentice şi impostor în erori a caracteristicilor biometrice individuale (această regiune oferind c centrul său şi lăţimea sa W). O procedură de normalizare adaptiva care creste nivelul de separare a distribuţiilor originale şi impostor este utilizată, în timp ce scorurile se mapeaza in gama [0,1]:

$$n_{AD} = f(n_{MM})$$

Caracteristiques Biometriques SOFT (slabe)

- Orice trasatura care oferă unele informaţii despre identitatea unei persoane, dar nu furnizează dovezi suficiente pentru a determina cu exactitate identitatea
- verificatorii slabi ai identităţii umane: sex, culoarea pielii, culoarea parului, etnie, inaltime, culoare ochi, greutate etc.

Ethnicity, Skin Color, Hair color
(Sub-Saharan African, Indian, Southern European and Northwest European)

http://anthro.palomar.edu/adapt/adapt_4.htm
© Corel Corporation, Ottawa, Canada

Eye color

Weight

http://www.laurel-and-hardy.com/goodies/home6.html © CCA

CONCLUSIONS

Avantages des VB :

–Elimine/réduit les fraude;

–Agrandi la sécurité;

–Ne peut pas être facile transférée, oublie, perdue ou copiée;

–Convenable pour utilisateur;

Désavantages :

–Aucun vérificateur n’est pas optime (dépend d’ application);

–Ne peut pas être remplacée si se perte;

– Intégration difficile en system;

–Susceptible a passée l’ intimité;