

Curs 12

VERIFICATORI BIOMETRICI PREZENTARE GENERALA

<https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security>

CUPRINS

- Securitate si biometrie
- Sisteme biometrice (SB)
- Scurt istoric al biometriei
- Verificatori biometrici (VB)
- Performantele sistemelor biometrice
- Standardizarea biometrica
- Aplicatii ale biometriei
- Sisteme multimodale
- Concluzii

- **Securitatea in e –World (“lumea electronica”)**

In era conectivitatii electronice universale ⇒ e-World:

⇒ e-commerce

⇒ e-banking

⇒ e-shop

⇒ e-mail

⇒ e-phone

⇒ e-government

- Din ce in ce mai multe activitati sunt legate de **INTERNET**

- Dezvoltarea Internet-ului intampina dificultati si probleme:

⇒ Virusi

⇒ Hackeri

⇒ Furturi pe computer

⇒ Accese neautorizate ...

- *Aceste probleme afecteaza prosperitatea si productivitatea firmelor si persoanelor*

Securitatea devine din ce in ce mai importanta

- O solutie este **autentificarea**: verificarea mesajului si a utilizatorului
- De fapt este o nevoie crescanda de identificare a **indivizilor** in e-world:
 - **POATE AVEA ACEASTA PERSOANA acces in sistem ?**
 - **ARE ACEASTA PERSOANA DREPT de a face aceasta tranzactie?**

O mare provocare:

Autentificarea utilizatorilor (verificarea identitatii)

- Calculatorul poate identifica anumite persoane.

O data ce dezvoltarea tehnologiilor de fraudare este in crestere
Autentificarea pozitiva este cruciala !

Autentificarea utilizatorului se bazeaza pe 3 metode:

- 1.Ce am (card, cheie,...)**
- 2. Ce stiu (cod, PIN,...)**
- 3. Ce sunt/ce fac (caracteristici biometrice)**

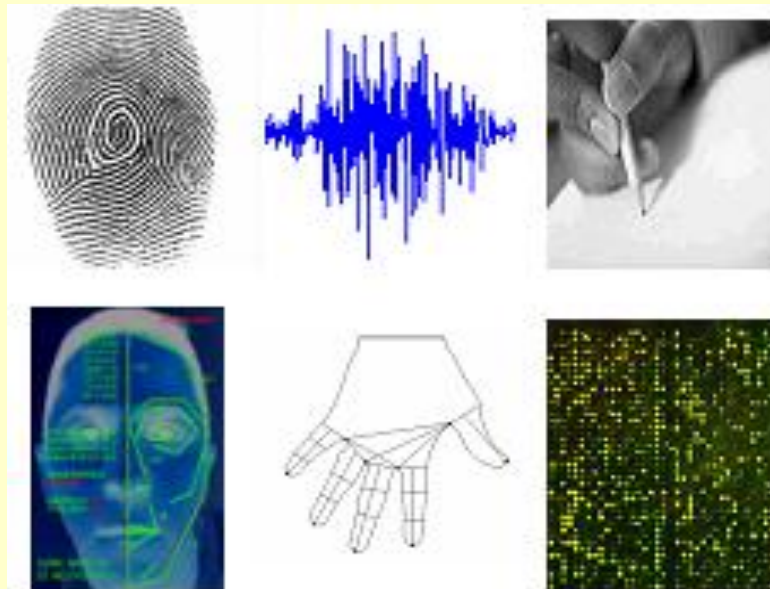
BIOMETRIA

“**Biometria** reprezintă un set de metode automate de recunoaștere a persoanelor pe baza caracteristicilor fiziologice sau comportamentale”
conform definiției Consorțiului Biometric

Biometrie $\Rightarrow$ *bios* (viață) și *metron* (măsură)

Caracteristici biometrice :

- fiziologice: amprenta, fata, iris, mâna, ADN,...
- comportamentale : voce, mers, semnătură,...



Orice caracteristică fiziologică sau comportamentală poate fi folosită ca verificador biometric atâta timp cât satisface următoarele cerințe [1]:

- **universalitate** – adică fiecare persoană trebuie să posede această caracteristică ;
- **distinctivitate** – caracteristicile pentru două persoane să fie suficient de distincte pentru a permite diferențierea lor;
- **permanență** - caracteristica să fie invariantă pe o perioadă cât mai lungă de timp;
- **colectabilitate** – indică faptul că respectiva caracteristică biometrică poate fi și măsurabilă cantitativ.

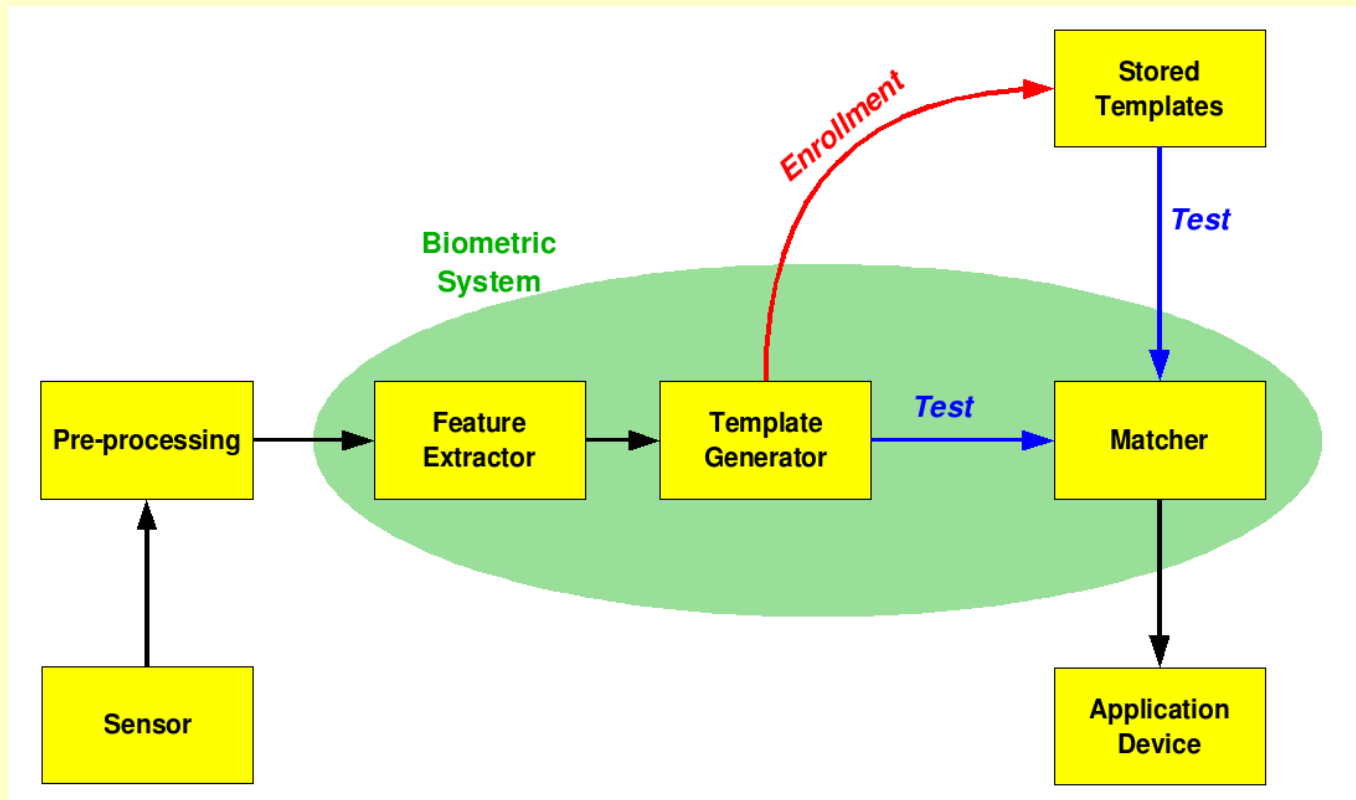
Pentru sistemele practice mai sunt necesare câteva cerințe în plus și anume:

- **performanța** – care se referă la precizia de recunoaștere tangibilă, viteză, robustețe, precum și la resursele necesare pentru a atinge un anumit nivel de performanță;
- **acceptabilitatea** – indică gradul în care respectiva caracteristică biometrică se impune a fi acceptată de utilizatori;
- **rezistența la fraudare** – indică facilitatea cu care un sistem poate fi fraudat.

SISTEME BIOMETRICE – SB

ELEMENTELE:

- senzorul ;
- modulul de extragere al vectorilor specifici ;
- modulul comparator ;
- baza de date biometrice .

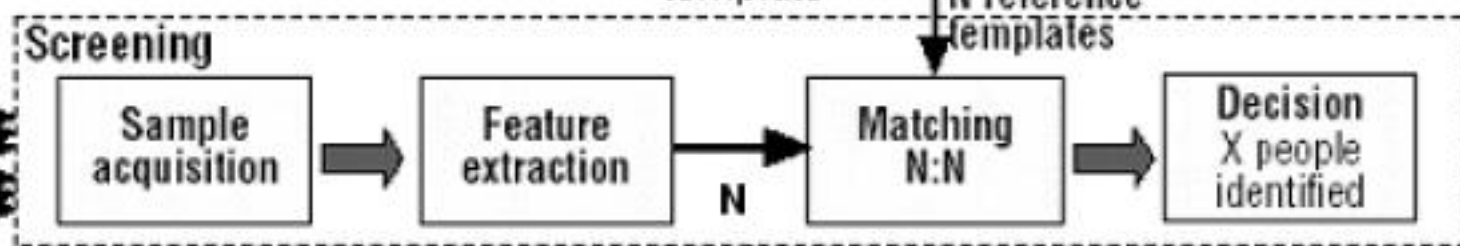
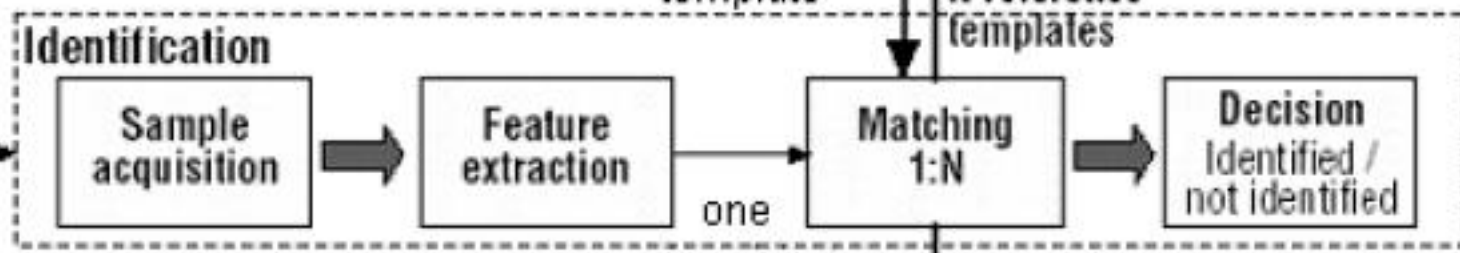
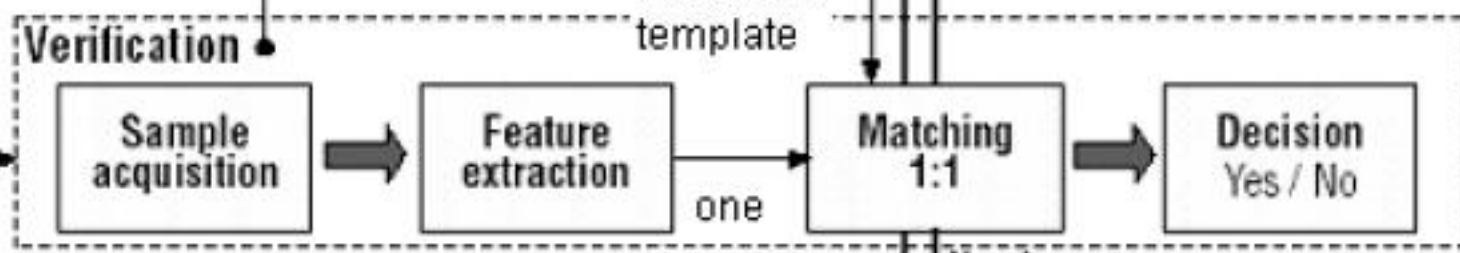




Storage of one reference template



Claimed identity



templates

Caracteristicile și taxonomia sistemelor biometrice

Sistemele de recunoaștere biometrică pot opera în mod :

pozitiv sau negativ.

1. *Recunoașterea pozitivă* stabilește dacă persoana care-și revendică identitatea este într-adevăr acea persoană.

- **Scopul:** de a preveni ca mai mulți utilizatori să folosească aceeași identitate

2. *Recunoașterea negativă* trebuie să dovedească faptul că utilizatorul nu este cine revendică el că ar fi. (NUMAI pentru SB !)

- **Scopul:** de a preveni ca o persoană să aibă mai multe identități.

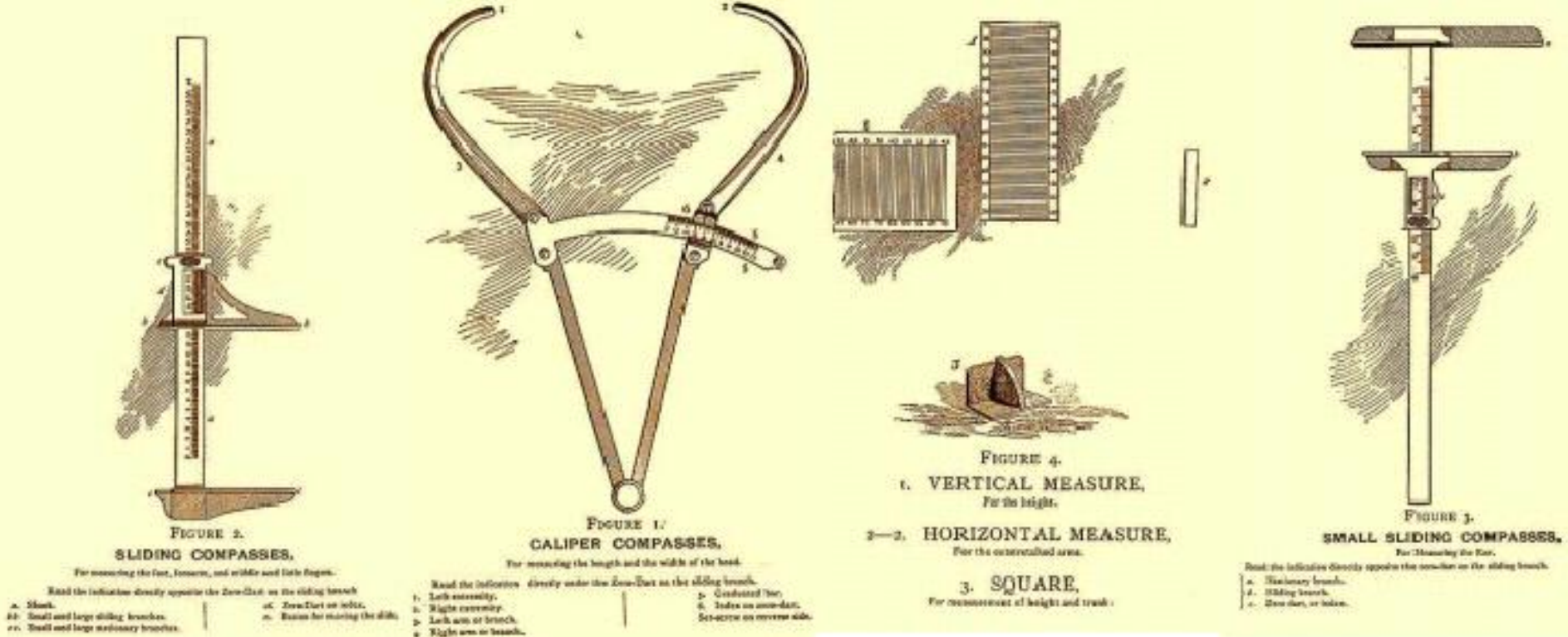
- **Sistemele si aplicatiile biometrice pot fi clasificate astfel:**
 - **cooperante sau necooperante** - se referă la modul de comportare al impostorului în interacțiune cu sistemul (ex. Voce);
 - **utilizate frecvent sau rar** - indică frecvența cu care utilizatorii înregistrați sunt subiectul recunoașterii biometrice;
 - **ascunse/vizibile** - utilizatorul este informat sau nu că este subiectul unei recunoașteri biometrice;
 - **asistate sau neasistate** - indică modul cum se desfășoară procesul achiziției datelor biometrice;
 - **publice sau private** –se referă la utilizatorii sistemului care sunt clienții sau angajații unei firme;
 - **mediul de operare standard sau nestandard** - se referă la condițiile de mediu în care operează sistemul;
 - **deschise sau închise** - arată modul cum este utilizat tiparul biometric al unei persoane pentru una sau mai multe aplicații.

Scurt istoric al biometriei

Egiptul antic (B.C.)- se foloseau principiile de bază ale verificării biometrice în situațiile uzuale de afaceri (tranzacții agricole, diverse proceduri legale). Caracteristicile biologice folosite: cicatrici, măsurarea corpului, culoarea ochilor, înălțime sau aspectul tenului.

China - (sec.XIV-lea, Joao de Barros) - comercianții chinezi foloseau o formă de biometrie prin imprimarea pe hîrtie a palmei și tălpii copiilor lor, muiate în cerneală, prin acest mod rezolvând problema de a-și distinge copiii unii de alții.

Franta – (sfârșitul sec. al XIX-lea) - metodele antropometrice ale lui **Alphonse Bertillon** (1880), utilizate în identificarea criminalilor și în expertizele judiciare. Bertillon a sesizat ca anumite elemente ale corpului rămân aproximativ fixe: lungimea degetelor, diametrul craniului, înălțimea, cicatrici, tatuaje sau alte caracteristici personale (discreditat în 1903)



Instrumente folosite pentru masuratori antropometrice

Anglia (1893) - Richard Eduard Henry de la Scotland Yard a demarat folosirea amprentei digitale



Masuratori antropometriche

Sisteme automate de recunoaștere biometrică

- Sistemul automat de identificare pe baza amprenteii -1960
- Sistemul de identificare a vorbitorului - 1969
- Recunoașterea feței cu ajutorul calculatorului -1977
- Identificarea pe baza retinei -1978
- Verificarea automată a semnăturii –1983
- Dinamica tastării -1985
- Recunoașterea pe baza irisului -1993
- Identificarea automată utilizând amprenta palmară -1998.

NU EXISTA VB perfect, se alege in functie de aplicatie :

Aplicația necesită verificare sau identificare?

Dacă o aplicație necesită identificarea unui subiect dintr-o bază mare de date are nevoie de un factor biometric scalabil și cu bună distinctivitate (ex. amprente, iris sau ADN);

Care sunt modurile de utilizare ale aplicației?

Aplicația este asistată (semi-automată) sau neasistată (complet automată);

Care sunt cerințele de stocare pentru aplicație?

Aplicațiile care accesează baze de date aflate la distanță pentru a face recunoașterea, necesită modele de dimensiuni reduse;

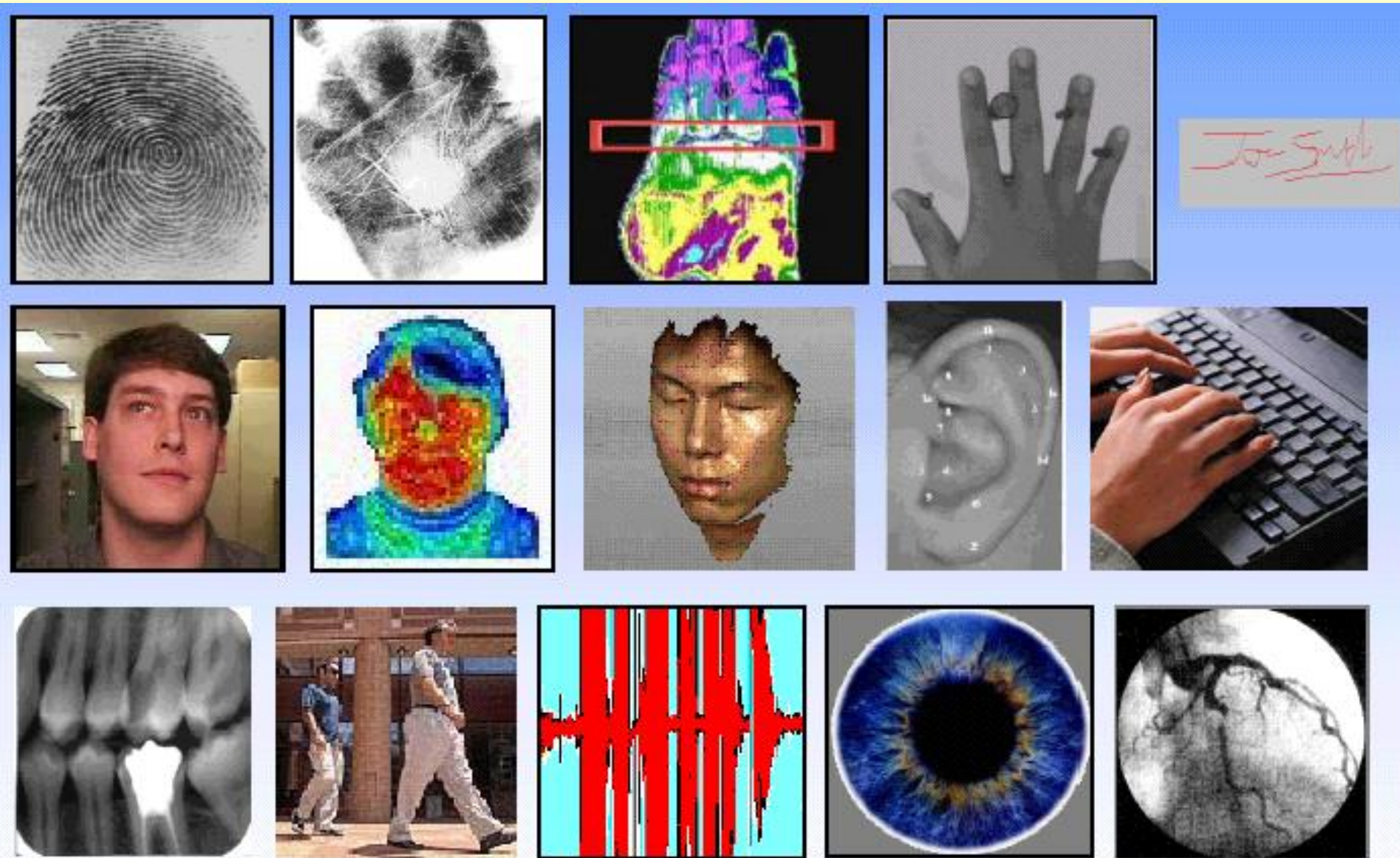
Cât de importante sunt cerințele de performanță?

Astfel, o aplicație care necesită acuratețe foarte mare are nevoie de un factor biometric cu distinctivitate cât mai mare.

Care caracteristici biometrice sunt acceptabile pentru utilizatori?

• Cele mai populare aplicații comerciale au următoarele attribute: *cooperante, vizibile, închise și private, cu utilizare frecventă, înrolare controlată și recunoaștere neasistată, operând într-un mediu standard.*

VERIFICATORI BIOMETRICI

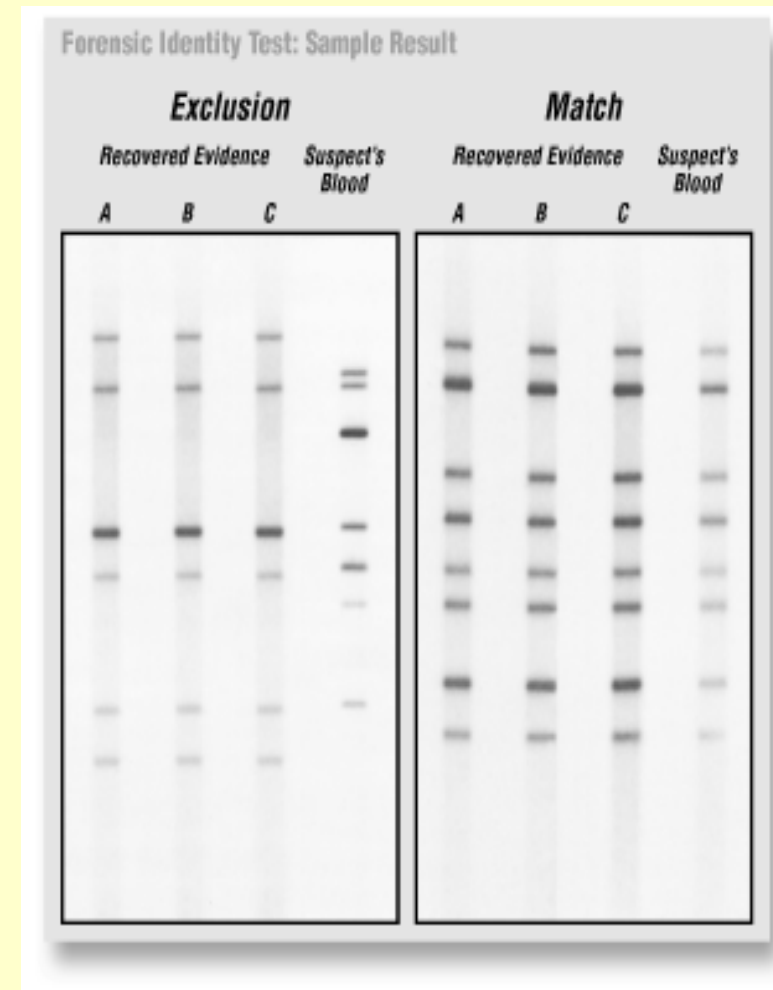
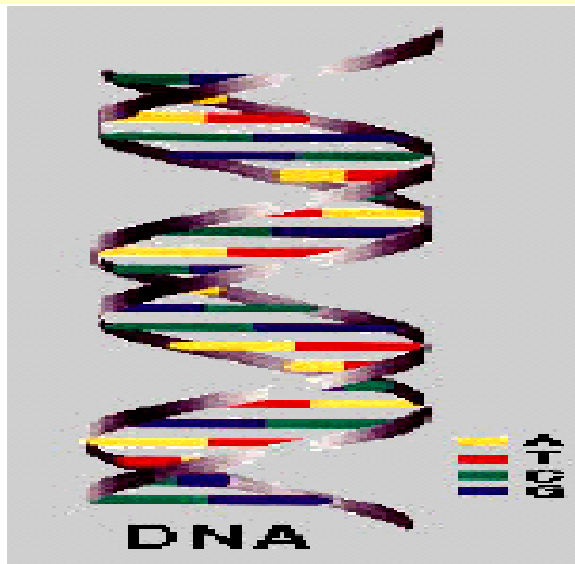


ADN – Acid dezoxiribonucleic - este un cod unidimensional unic pentru identitatea cuiva, exceptând gemenii identici (monoziagoți) care au tipare ADN identice.

ADN-ul este folosit în mod special la aplicațiile judiciare și criminalistice pentru recunoașterea de persoane.

Limitari:

- contaminarea și sensibilitatea indică faptul că o probă ADN poate fi ușor furată și apoi utilizată cu un anumit scop;
- inadecvat pentru aplicații în timp real;
- ridică probleme de încălcare a intimității.



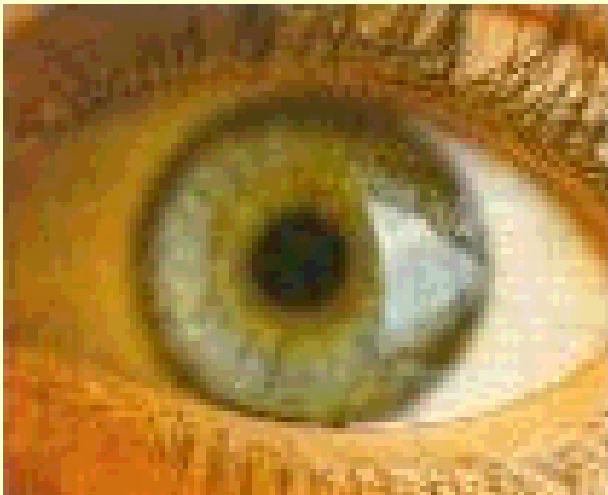
Fața - reprezintă unul dintre cei mai acceptați factori biometrici;

- Abordările cele mai uzuale ale metodei constau fie în:
 - forma și localizarea relativă a diferitelor attribute faciale (ochi, nas, buze, bărbie, sprâncene);
 - fie în analiza globală a imaginii feței, care reprezintă fața ca o combinație de imagini faciale canonice ponderate.
- Recunoașterea feței este o provocare în dezvoltarea unor tehnici de recunoaștere specifice, care să poată fi tolerante la efectele cauzate de vârstă, expresii faciale, variații în mediul înconjurător și variații ale unghiului feței în poză, grad de iluminare etc.
- Deghizarea este una din dificultățile aplicațiilor neasistate.



Irisul - textura vizuală a irisului uman este determinată de procesul morfogenetic haotic care se dezvoltă în stadiul embrionar și este considerat a fi distinct pentru fiecare persoană și fiecare ochi și stabil cu vârsta;

- Irisul reprezintă o diafragma care se întinde peste partea anterioară a cristalinului și este partea colorată care înconjoară pupila;
- O imagine de iris este un model complex format din mai multe caracteristici distinctive (ligamente, arce, brazde, creste, inele, pistrui etc.);
- Captarea imaginii irisului implică și colaborarea din partea utilizatorului, pentru înregistrarea lui în zona centrală a imaginii și o atentă echilibrare a luminozității, focalizării, rezoluției și contrastului;
- Tehnologia de recunoaștere a irisului este considerată a fi făcută cu o mare acuratețe și viteză, iar sistemele actuale au devenit eficiente și rezonabile ca preț;
- Dificultăți la înrolare (FTE ~7%)



Amprenta digitala

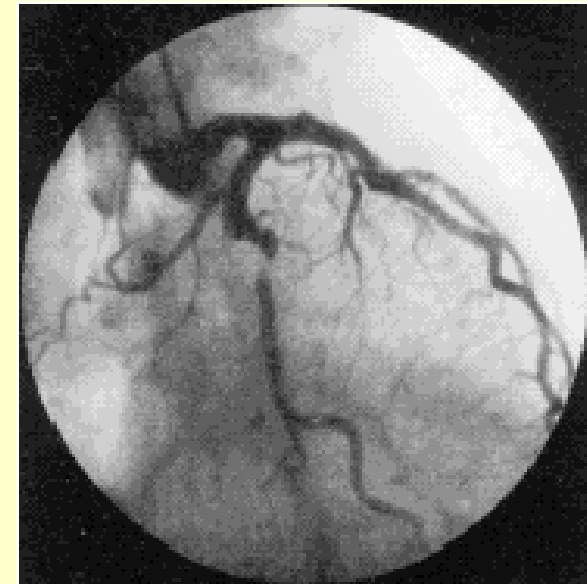
- O amprentă digitală este o amprentă lăsată de creștăturile unui deget uman. Recuperarea amprentelor digitale parțiale de la locul unei infracțiuni este o metodă importantă a științei criminalistice.
- Umezeala și grăsimea de pe un deget dau naștere la amprente pe suprafețe precum sticla sau metalul.
- Una dintre metodele cu rezultate foarte bune de recunoaștere, totuși având un mare număr de dificultăți la înrolare. Sunt puse la punct mai multe metode de recunoaștere pe baza de amprenta



- <https://en.wikipedia.org/wiki/Fingerprint>

Scanarea retinei - Vasculatura retinei are o structură bogată și se consideră a fi caracteristică fiecărui individ și fiecărui ochi;

- Se presupune a fi cel mai sigur factor biometric, de vreme ce nu este deloc ușor a schimba sau a copia vasculatura retinei;
- Achiziția imaginii implică de asemenea cooperarea subiectului, contactul dispozitivului cu ochiul și un anumit efort din partea utilizatorului;
- Aceste dificultati afectează acceptarea factorilor biometrici retinali de către public;
- Vasculatura retinei poate dezvălui anumite afecțiuni ale sănătății (de ex. hipertensiune), acesta fiind un alt factor care poate leza intimitatea și poate crea o piedică în calea acceptanței publice.



Forma mâinii și a degetelor – forma și lungimea mâinii și a degetelor sunt relativ invariante, deși nu foarte distinctive;

- Acest verficator s-a utilizat la unul dintre primele sisteme biometrice automate încă din anii '60;

- Tehnica este simplă, ieftină, ușor de utilizat și robustă la condiții de mediu (umiditate, anomalii individuale).

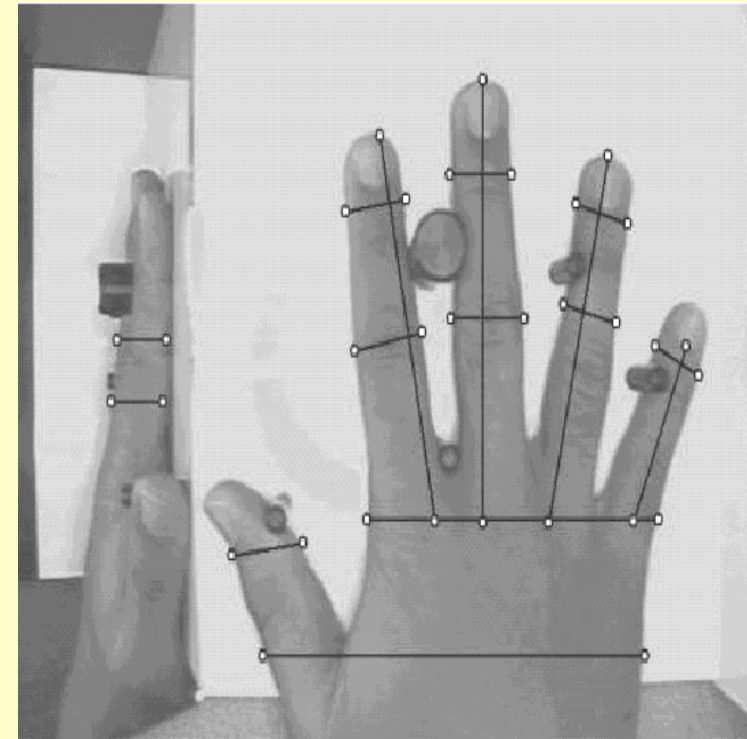
- Sistemul necesită cooperarea subiectului și captează imagini frontale și laterale ale mâinii ținute în fața dispozitivului

- Pe imagine se fac măsurători ale formei, mărimii palmei, lungimii și grosimii degetelor.

- Nevoile de stocare ale caracteristicii mâinii sunt reduse (9 octeți)

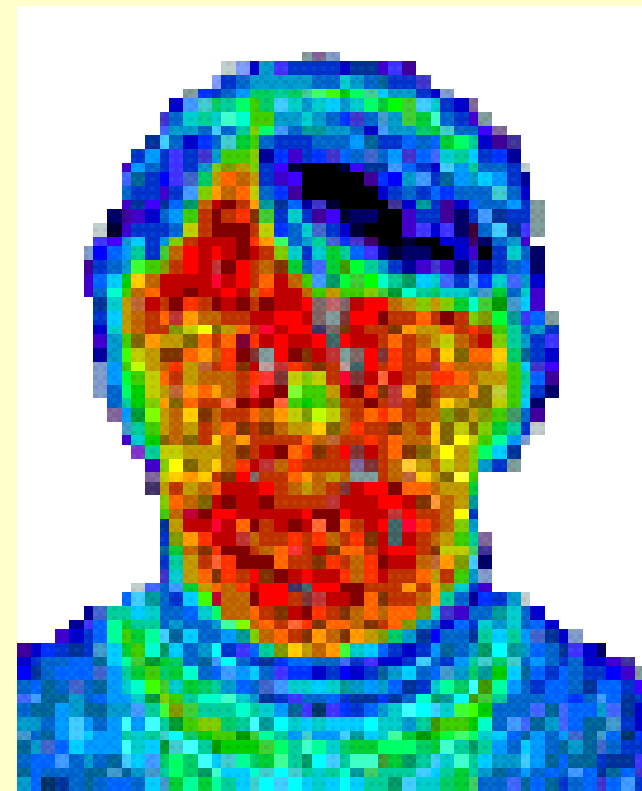
- Datorită distinctivității limitate, sistemele bazate pe geometria mâinii sunt utilizate în mod tipic pentru verificare și nu sunt adecvate pentru aplicații de identificare;

- probleme în utilizare: în perioada de creștere, unele boli, bijuterii



Termograme în infraroșu (faciale, ale mâinilor și venelor)

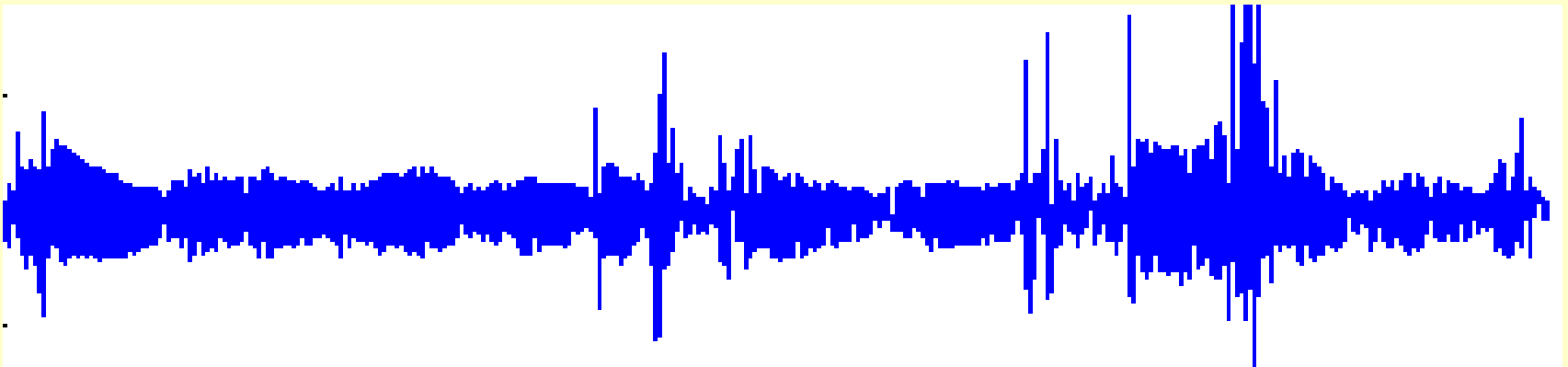
- Tiparul căldurii radiate de corpul uman este o caracteristică individuală și poate fi capturată de o cameră în infraroșu într-un mod asemănător cu o fotografie;
- Tehnologia bazată pe termograme este neinvazivă și poate fi utilizată pentru recunoaștere ascunsă și pe timp de noapte;
- Solicitări la care trebuie să facă față tehnologia apare în medii necontrolate, unde alte obiecte emană căldură în vecinătatea corpului și pot afecta în mod hotărâtor achiziția imaginii;
- O tehnologie înrudită este utilizarea imaginilor în infraroșu captate din apropiere pentru a scana structura venelor;
- Senzorii în infraroșu au prețuri prohibitive.



Vocea - este considerat un factor biometric unanim acceptat, usor si ieftin de achizitionat;

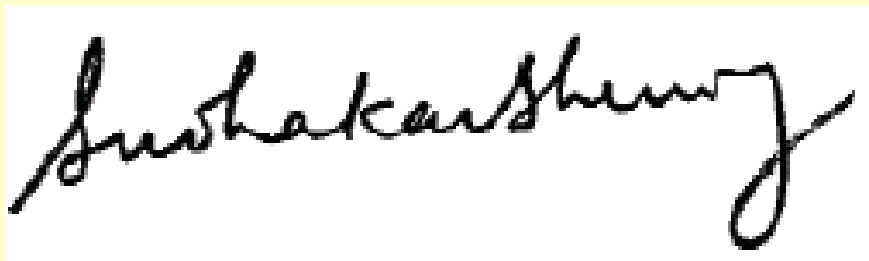
- Vocea unei persoane este dependentă de anumite *caracteristici fiziologice* personale invariante (tract vocal, corzi vocale, gură, limbă, cavitate nazală, buze), dar și de unele *comportamentale*, care diferă cu vârsta, starea de sănătate, emoții.
- Este fezabilă în aplicații care necesită recunoașterea unei persoane prin telefon, dar nu se consideră a fi suficient de distinctă pentru a permite identificarea indivizilor dintr-o bază de date cu multi utilizatori;

Probleme: variabilitatea/imitarea vocii și poate induce în eroare sistemele de recunoaștere.



Semnătura – este o formă simplă și concretă a felului în care o persoană își dirijează mâna după o anumită traiectorie care îi este caracteristică;

- este un factor biometric comportamental care se schimbă în timp și este influențată de starea fizică și emoțională a celui care semnează;
- semnăturile unor persoane variază foarte mult: chiar și semnături succesive diferă semnificativ;
- semnătura este considerată acceptabilă în multe tranzacții guvernamentale, legale și comerciale ca metodă de verificare;
- **probleme:** falsificatorii pot reproduce semnăturile pentru a induce în eroare sistemul automat de verificare.

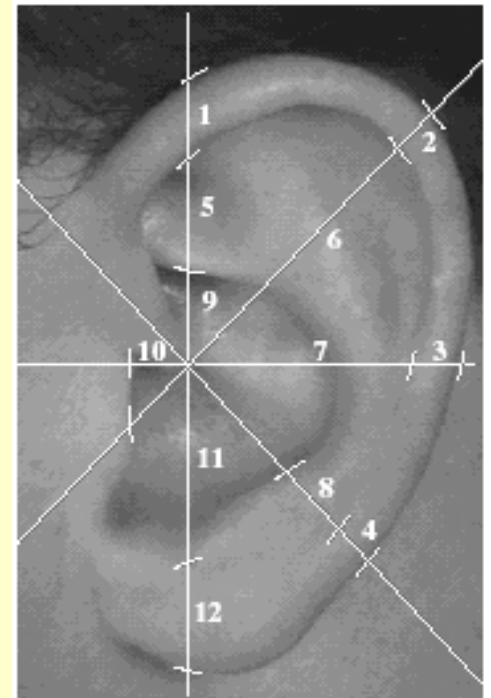
A sample handwritten signature in black ink on a white background. The signature is cursive and appears to read 'Sushakar Shetty'.

Urechea - dimensiunea, forma urechii și structura cartilagiilor sunt distinctive pentru diferitele persoane;

- Caracteristicile unei urechi nu sunt de așteptat să fie unice la oricare individ, deci nu are mare distinctivitate;
- Abordările de recunoaștere a persoanelor folosind urechea se bazează pe compararea distanței diverselor puncte de referință localizate pe ureche.

ALTI VERIFICATORI BIOMETRICI :

- MERSUL
- MIROSUL
- DINAMICA TASTARII



Comparație a verificatorilor biometrici

Identificator Biometric	Universalitate	Distinctivitate	Permanență	Colectabilitate	Performanță	Acceptanță	Siguranță
ADN	+	+	+	-	+	-	-
Ureche	0	0	+	0	0	+	0
Față	+	-	0	+	-	+	+
Termogramă facială	+	+	-	+	0	+	-
Amprentă	0	+	+	0	+	0	0
Mers	0	-	-	+	-	+	0
Geometria mâinii	0	0	0	+	0	0	0
Venele mâinii	0	0	0	0	0	0	-
Iris	+	+	+	0	+	-	-
Tastare	-	-	-	0	-	0	0
Miros	+	+	+	-	-	0	-
Retina	+	+	0	-	+	-	-
Semnătură	-	-	-	+	-	+	+
Voce	0	-	-	0	-	+	+

+ Mare ; 0 Medie; - Redusă

Sisteme biometrice. Performante

Două eșantioane ale aceleiași caracteristici biometrice, prelevate de la aceeași persoană, nu sunt perfect identice datorită :

- *senzorului;*
- *modificărilor caracteristicii biometrice;*
- *condițiilor ambiente;*
- *interacțiunii utilizatorului cu senzorul.*

- Răspunsul unui SB este un rezultat de **similitudine – s**, care cuantifică asemănarea dintre intrare și model, iar decizia se ia comparând **s** cu un **prag p** a priori stabilit;

Erorile sistemelor de verificare biometrice :

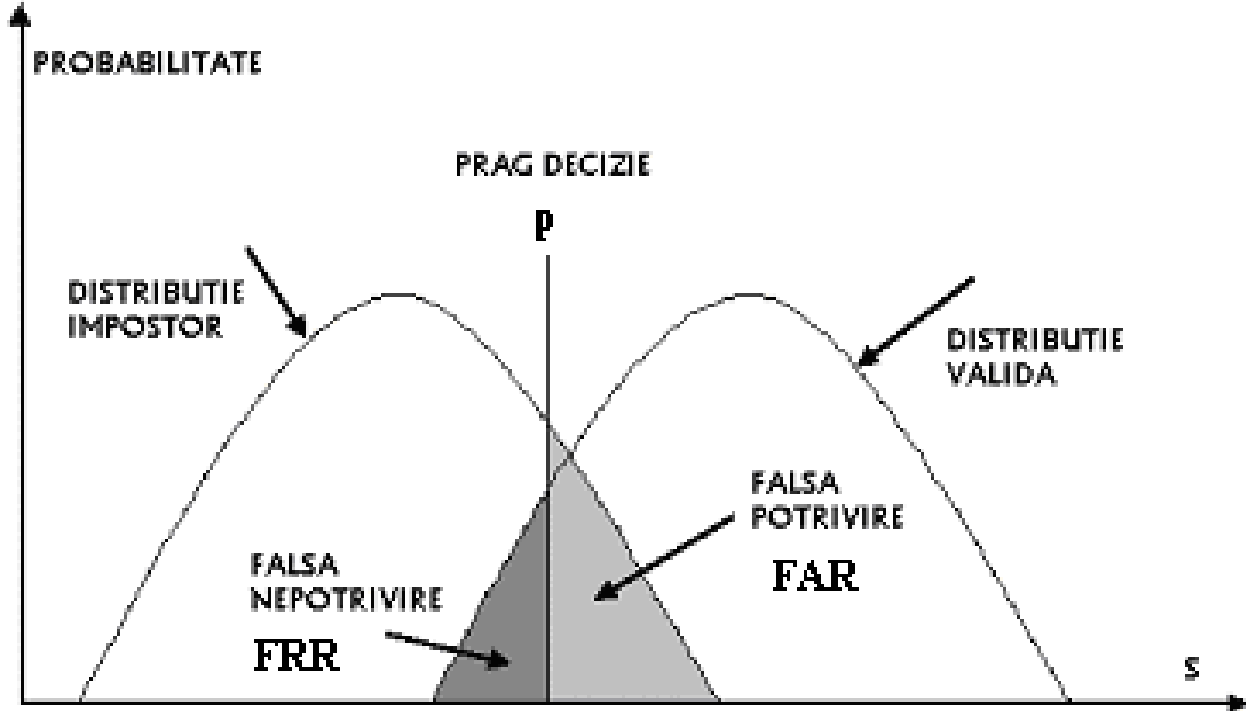
- **rata de falsă potrivire/acceptare (FAR)**
- **rata de falsă nepotrivire/respingere (FRR)**

Ipoteze : $I_0: X_I \neq X_M$ - vectorii sunt de la persoane diferite;

$I_1: X_I = X_M$ - vectorii sunt de la aceeași persoană;

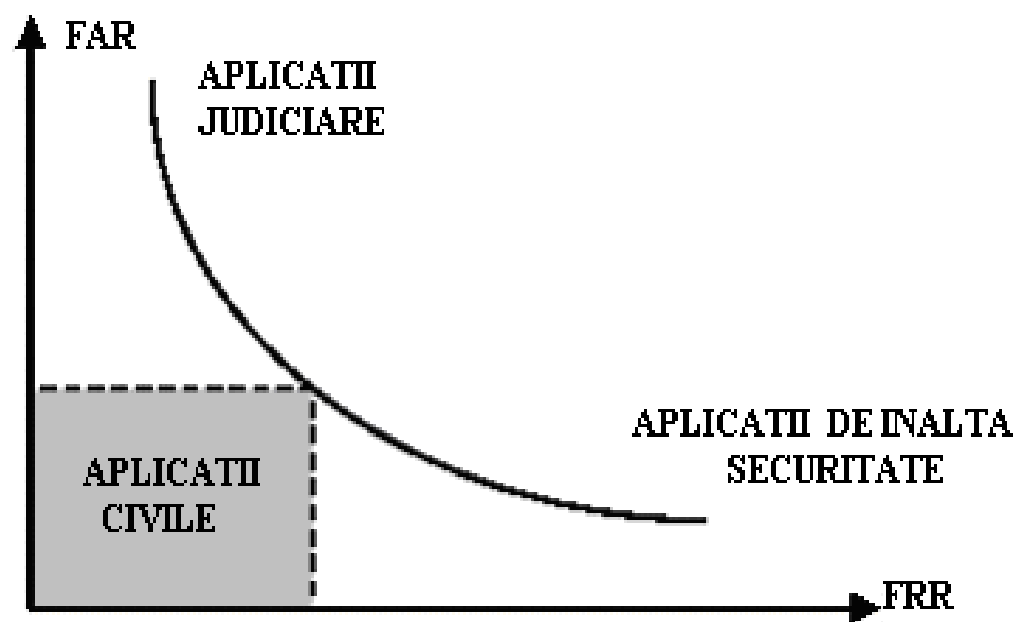
Decizia : D_0 : persoana nu este cine pretinde că este;

D_1 : persoana este cine pretinde că este.



Erorile SB de verificare

Punctele de operare tipice la diferite aplicații



Caracteristica biometrica	EER	FAR	FRR	Parametrii de Test (conditii)	Test
Fata	-	1 %	10 %	Iluminare diferita interior/exterior	FRVT (2002)
Amprenta Digitala	-	1 %	0.1 %	Date furnizate de US Government	FpVTE (2003)
	2%	2 %	2 %	Rotatii sau distorsiuni exagerate ale pielii	FVC (2004)
Forma Mainii	1%	2 %	0.1 %	Cu inele si pozitii improprii	(2005)
Iris	0.01 %	0.0001 %	0.2 %	Cele mai bune conditii	NIST (2005)
Voce	6%	2 %	10 %	Independent de text , multilingual	NIST (2004)

Nivelul actual al performantelor sistemelor unimodale (rate de erori)

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)

- La un flux de pasageri de aproximativ **300.000** pe zi (în aeroporturile din New York) la utilizarea cardurilor de identificare biometrice pentru autentificare ar exista **6.000** de false rejecții zilnic dacă s-ar utiliza amprenta digitală, **30.000** în cazul feței și **45.000** pentru voce !

	Amprentă	Forma mâinii	Iris	Față	Voce	Semnătură	Retină
Minim	100 bytes	9 bytes	256 bytes	84 byte	1 Kb	500bytes	96 bytes
Maxim	2 Kb	-	2 Kb	2.5 Kb	3 Kb	-	
Tipic	300 bytes	9 bytes	512 bytes	2 Kb	1 Kb	1kb	96 bytes

Dimensiunile aproximative ale modelelor pentru diferiți VB

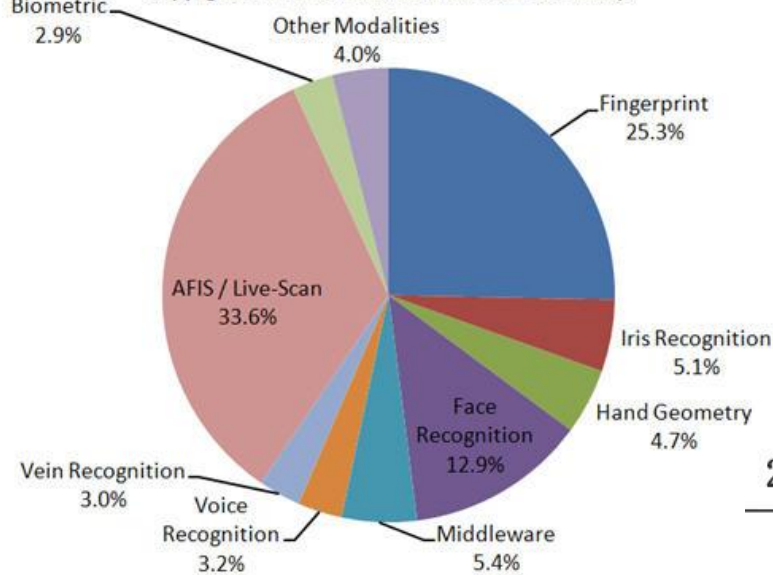
Sistem	Timpul tranzacției (sec)			Timpul include introducerea PIN
	Mediu	Median	Minim	
Față	15	14	10	Nu
Amprentă (optic)	9	8	2	Nu
Amprentă (chip)	19	15	9	Nu
Mână	10	8	4	Da
Iris	12	10	4	Da
Vene	18	16	11	Nu
Voce	12	11	10	Nu

Biometric Technology Types Features Overview

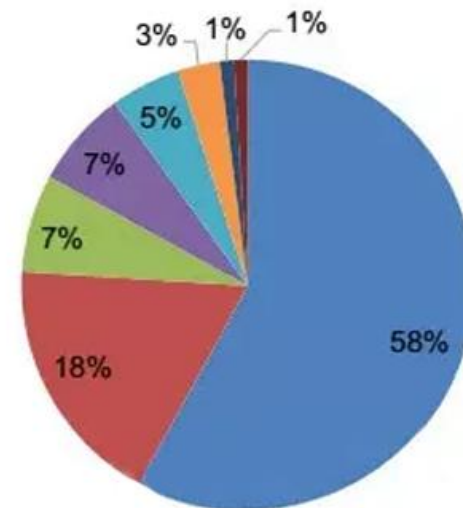
Features	 Facial Recognition	 Iris Scanning	 Fingerprint Identification	 Voice Verification
Accuracy	Medium-low	High	High	Medium
Attack's precaution	Medium	Very high	High	Medium
Verification time	About 3 seconds	Less than 5 seconds	Less than 3 seconds	About 5 seconds
Devices Required	Camera	Camera	Scanner	Microphone
Interference	Lighting, glasses, hair, moving, age	Lighting, inaccurate eye positioning in relation to the device	Dryness, dirt, deep injury, age	Noise, cold symptoms

Biometric Market by Technology, 2007

Copyright © 2006-2007 International Biometric Group

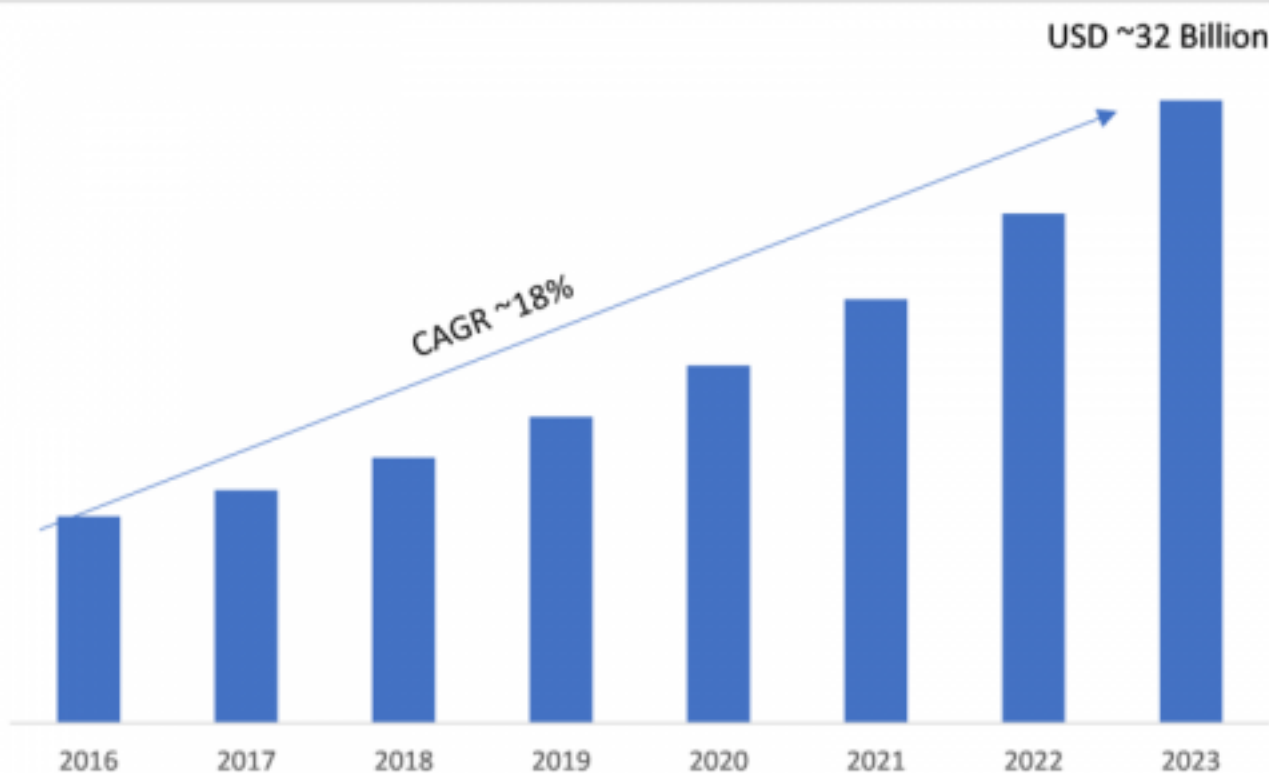


2015 global biometric market structure



- Fingerprint recognition
- Face recognition
- Iris recognition
- Palmpoint recognition
- Voice recognition
- Vein recognition
- Note recognition
- other

Piata celor mai raspanditi VB

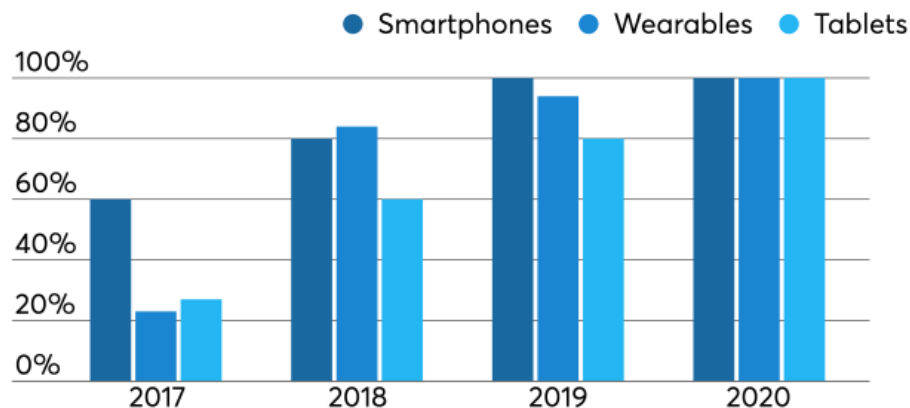


$$CAGR = \left(\frac{\text{Valoare finala}}{\text{Valoare initiala}} \right)^{\left(\frac{1}{\text{Nr de ani}} \right)} - 1$$

- Rata compusa de crestere anuala (*Compound Annual Growth Rate*) este rata de crestere anuala medie a unei investitii pe o perioada data mai mare de un an

Bio metrics

By 2020, it is expected that 100% of mobile devices will rely on some type of biometric safeguard



Source: Statista

STANDARDIZAREA BIOMETRICA

Scopul: pentru a sprijini *interoperabilitatea* sistemelor și aplicațiilor biometrice dezvoltate de diverși producători și pentru a permite *schimbul de date* biometrice ;

ANSI -Technical Committee M1, **Biometrics**

ISO/IEC - Joint Technical Committee 1 (JTC1)

- SC 37 Biometrics;

- SC68 Passports&Drivers Licenses

BioAPI Consortium – a **propus proiectarea unui API** (Application Program Interface) pentru sisteme biometrice cu scopul de a imbunatati compatibilitatea intr-o gama larga de tehnologii biometrice si a facilita comunicarea intre sistemele implementate

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.

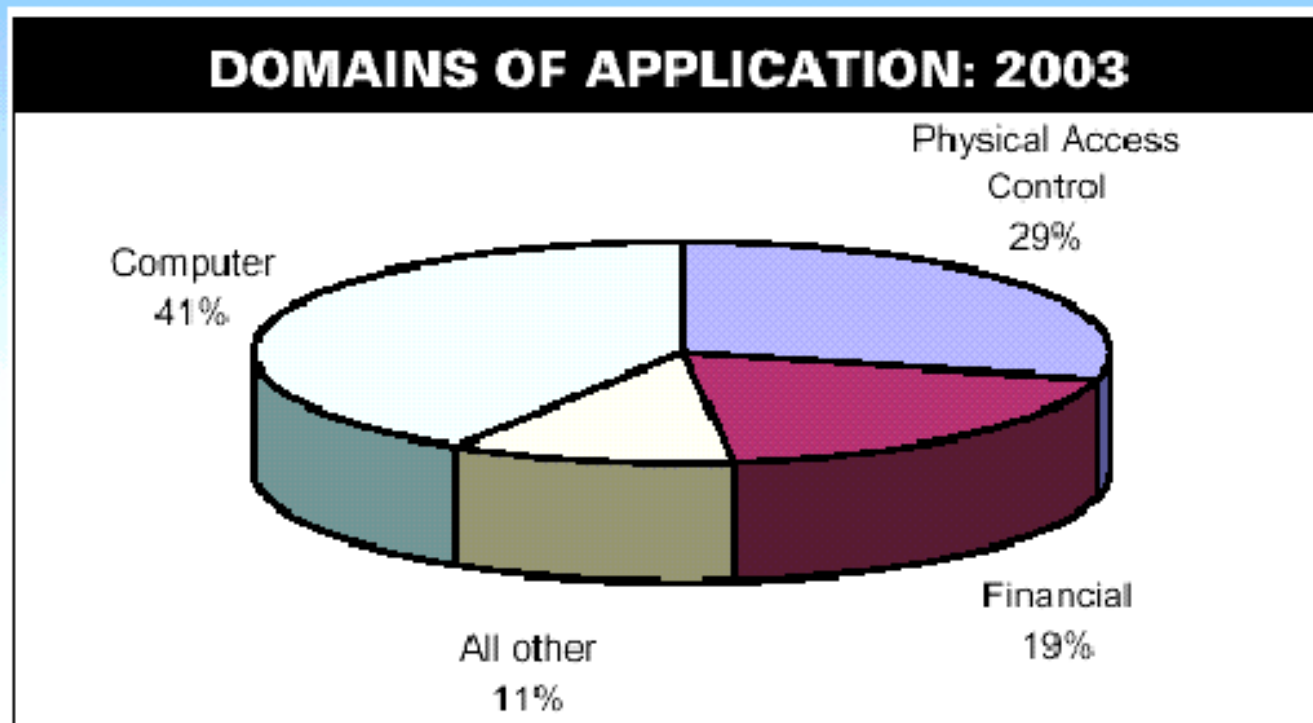
Standarde (ex.)

- 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

APLICATII ALE BIOMETRIEI

- Servicii financiare
- Aplicarea legii/judiciare
- Aplicatii guvernamentale
- Imigrare si calatorii
- e-Commerce si telefonie
- Control acces PC/ Network/ "on-site"
- Tranzactii - ATM
- Identificarea criminalilor
- Identificarea cetatenilor

Domains of Application

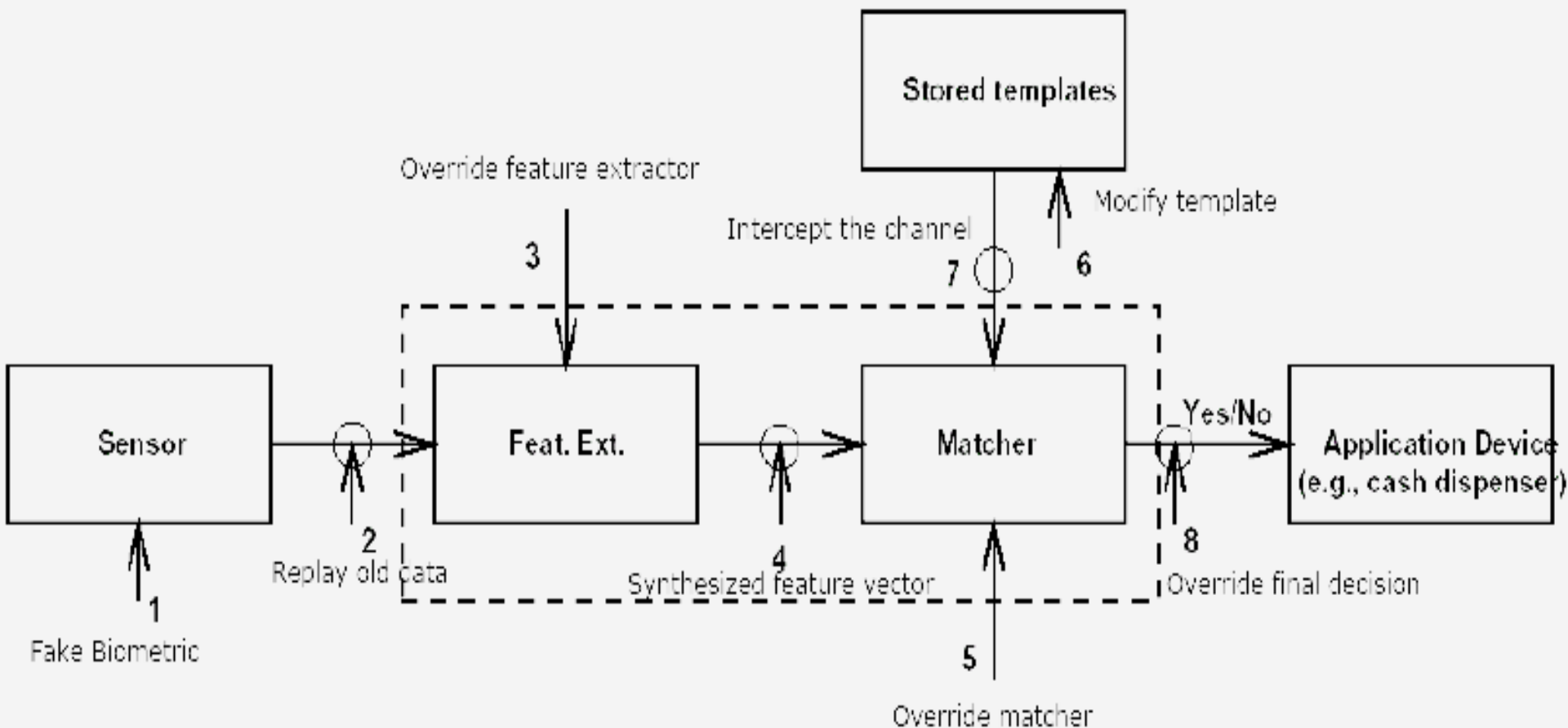


Domenii de aplicare a SB

SISTEME MULTIMODALE

LIMITELE SISTEMELOR UNIMODALE

- lipsa de universalitate a unor caracteristici
(Failure to enroll - amprenta digitala ~ 4%, iris ~ 7%);
- semnale zgomotoase captate de la senzori datorită folosirii incorecte de către clienți și a condițiilor ambientale (umiditate, murdărie, praf etc.)
- siguranța senzorilor folosiți;
- limitarea discriminării sistemelor biometrice datorită unei variabilități “in-class” destul de mari și “inter-class” reduse;
- performanțele de recunoaștere ale sistemelor sunt limitate superior la un anumit nivel;
- rate de erori inacceptabile pentru sistemele biometrice unimodale ;
- lipsa de permanență și variabilitatea în timp a caracteristicilor biometrice;
- posibilitati de fraudare/clonare;



Potential Attack Points (*Ratha et al.*)

Clonarea voluntara a amprente (metoda Matsumoto)



**Plasticul se
inmoaie in apa
calda**



**Se imprima
amprenta**



**Se obtine
matrita**

Operatiile dureaza ~10 min.



**Se umple
matrita cu
cauciuc fluid**



Se pune la rece



**Se obtine
degetul de
cauciuc**

Clona a fost testata pe 11 tipuri de senzori optici si capacitivi pe care a reusit sa-i "păcălească" !!!

Biometrie Multimodala

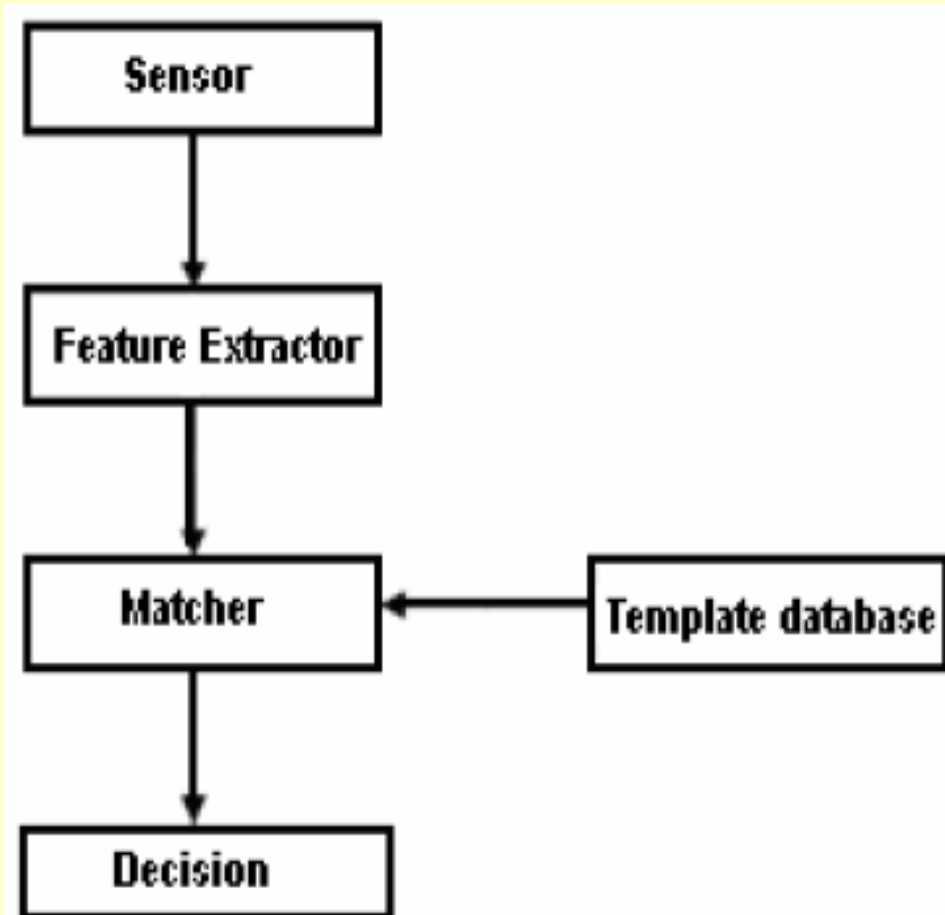
Principalele caracteristici ale unui sistem biometric multimodal :

a) **arhitectura** - secventa in care diferitele caracteristici sunt achizitionate

b) **sursele de evidenta** – folosite pentru a depasi limitarile sistemelor unimodale

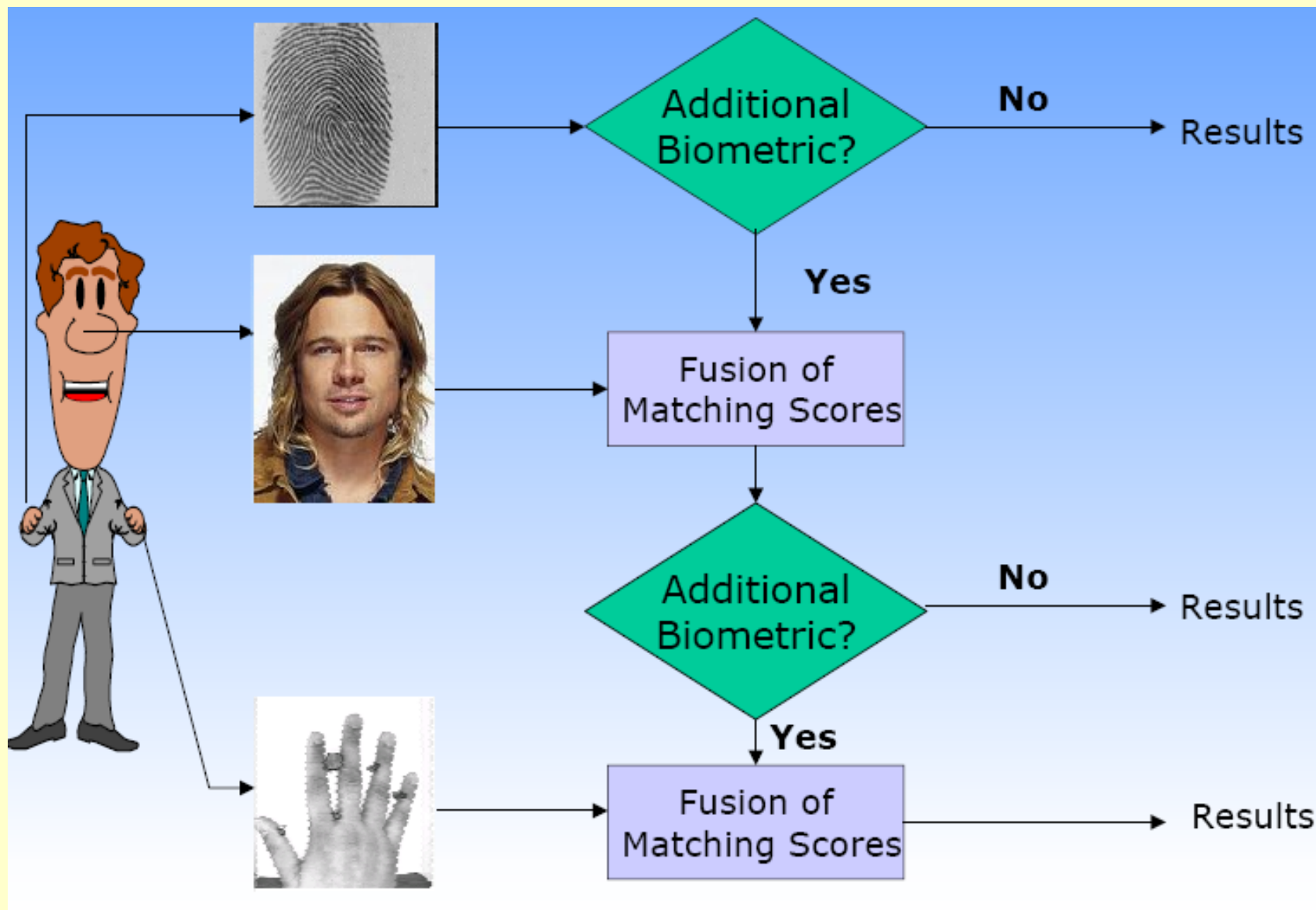
c) **nivelele de fuziune** - (senzori, extragere caracteristici, comparare parametrii, decizie)

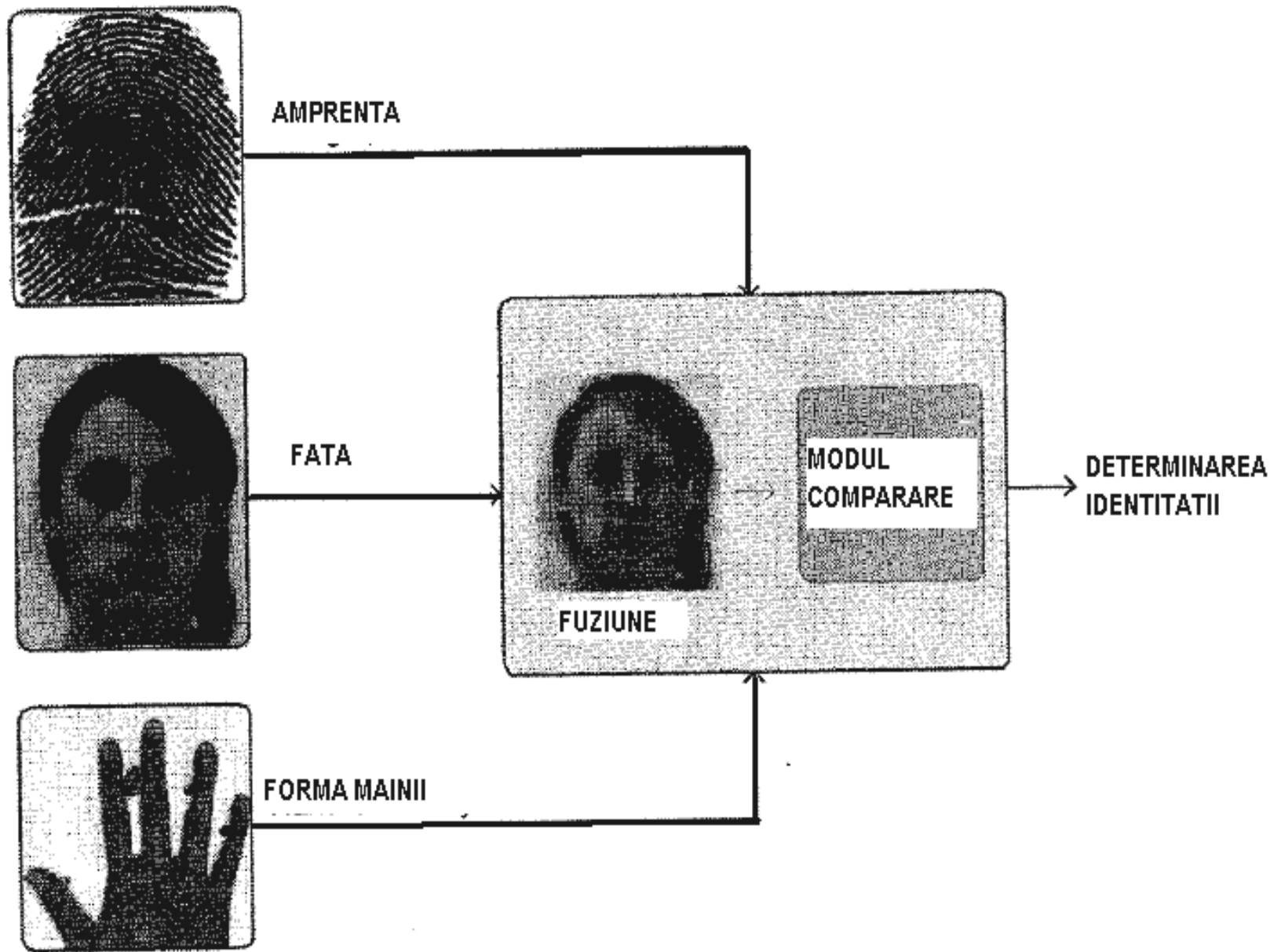
d) **metodologia** folosita pentru a integra mai multi verificatori



- arhitectura: paralela / seriala (cascada)
- sistemele biometrice multimodale seriale sunt este recomandate pentru aplicatii de securitate mai redusa (ATM, ..)
- - paralel este recomandat în aplicații cu un nivel ridicat de securitate (militară etc, spațiu)
- combinatia arhitecturii paralele și seriale (structură ierarhică)

SISTEME BIOMETRICE MULTIMODALE CASCADATE





In modul de operare paralel capturile biometrice sunt procesate simultan pentru a stabili identitatea

- sursele de evidenta

SISTEME MULTISENZOR

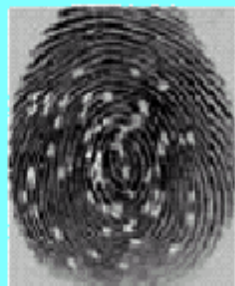


OPTIC



PE BAZA
de CHIP

SISTEME MUTI METODA



PE BAZA DE
MINUTAE



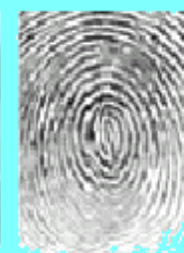
BAZAT PE
FILTRU

SISTEME BIOMETRICE MULTIMODALE

SISTEM MULTI VERIFICATOR

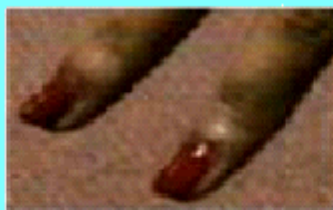


FATA

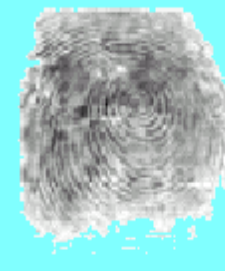


AMPRENTA

SISTEM pentru mai multe DEGETE



SISTEM MULTI CAPTURA



Surse multibiometrice de informatii

Informatia biometrica multimodala poate proveni din diferite surse :

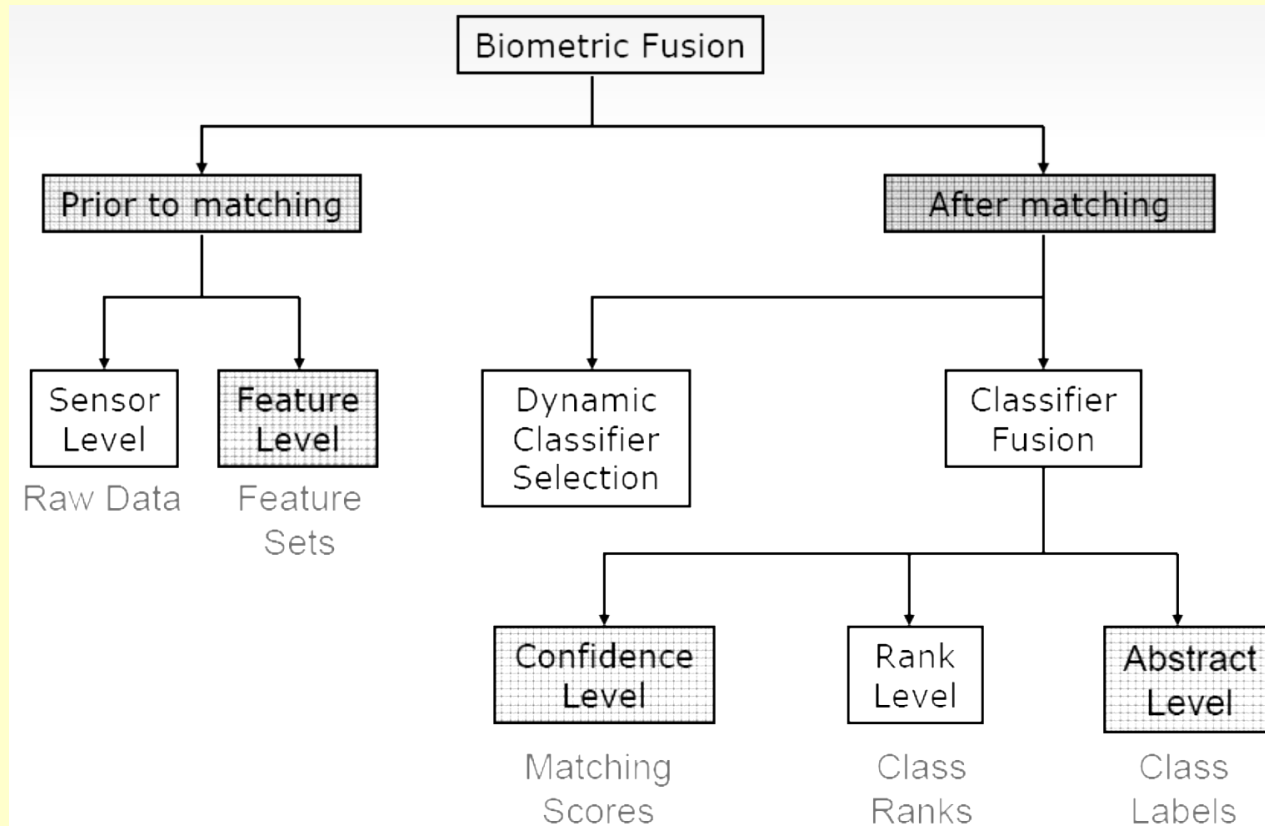
- **multi-sensor** – aceeași trasatură biometrică este captată folosind diferiți senzori pentru a extrage diferite informații din imaginile înregistrate (spatial);
- **multi-algorithm** – aceeași înregistrare a unei trasaturi biometrice este procesată folosind diferiți algoritmi. De exemplu, aceeași captură a unei amprente poate fi prelucrată prin algoritmi bazati pe texturi și pe minutiae (detalii de bază) realizând o îmbunătățire a performanțelor sistemului;
- **multi-instanta** (-caracteristica) – se utilizează mai multe caracteristici ale aceleiași trasaturi biometrice (ex. indexul de la mână dreaptă și stângă, irisul de la ambii ochi)
- **multi-sample** – același senzor face capturi multiple ale aceleiași trasaturi biometrice cu scopul de a surprinde variabilitatea unei trasaturi sau de a obține o reprezentare cât mai completă a trasaturii ;
- **multimodale** – combină capturile diferitelor trasaturi biometrice pentru stabilirea identității;
- **hibride** – integrează un subset a scenariilor mai sus enumerate.

Caracteristici
Voce, Față
Voce, Mișcarea buzelor
Voce, Față, Mișcarea buzelor
Amprentă, Față
Amprentă, Față, Voce
Amprentă, Față, Geometria mâinii
Amprentă, Voce, Geometria mâinii
Voce, Geometria mâinii
Termogramă facială, Față
Iris, Față
Amprenta palmară, Geometria mâinii
Ureche, Voce

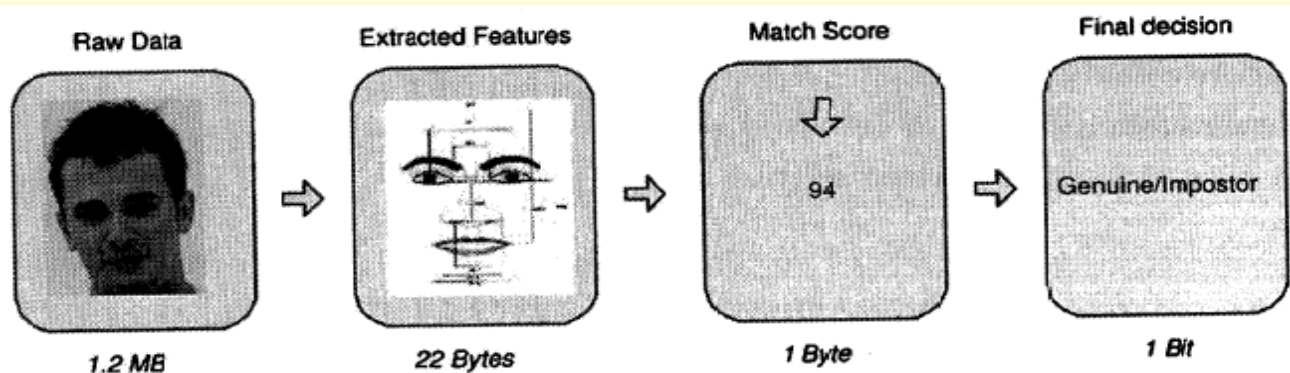
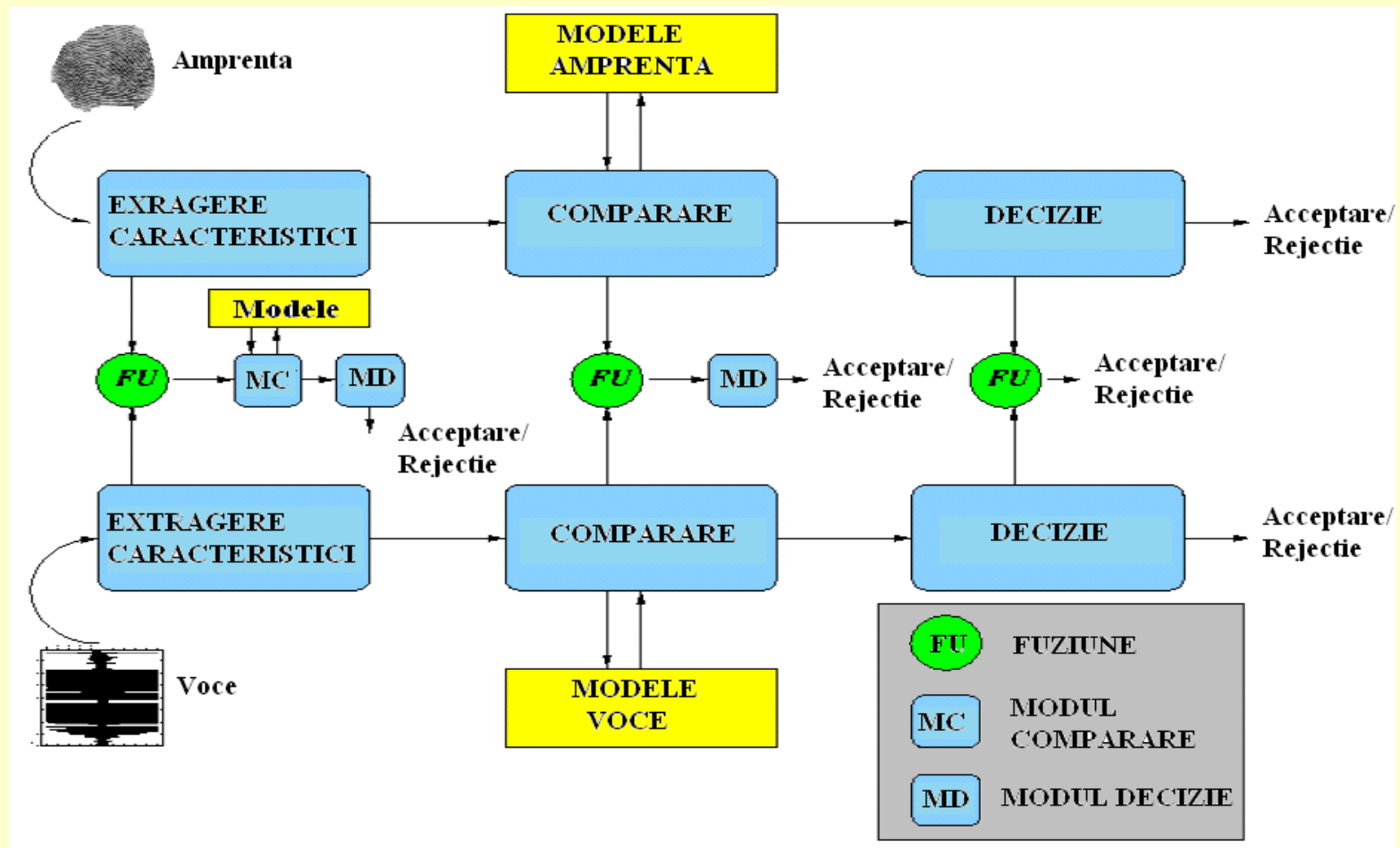
Caracteristici biometrice care se pretează
la sistemele multimodale/multi-verificator

Nivelele la care se poate face **fuziunea** în sistemele biometrice multi-verificator sunt la nivelul :

1. *modulelor senzorialor* - se combină eşantioanele de la ieşirile senzorilor;
2. *modulelelor de extragere a caracteristicilor* - se combină caracteristicile extrase de la fiecare verificador;
3. *modulelor de comparare a parametrilor* - se combină rezultatele comparărilor;
4. *modulelor de decizie* – se combină deciziile de identitate;



NIVELE de FUZIUNE



TEHNICI de NORMALIZARE

- Scorurile de ieșire de la modulele de comparare furnizate prin diferite modalități sunt heterogene, prin urmare, este necesară normalizarea scorurilor
- **Min-Max (MM)**: Mapează scorurile brute în intervalul [0,1], Max (S) și min (S), fiind punctele de sfârșitul 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 distribuție cu medie de 0 și abaterea standard de 1.

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

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

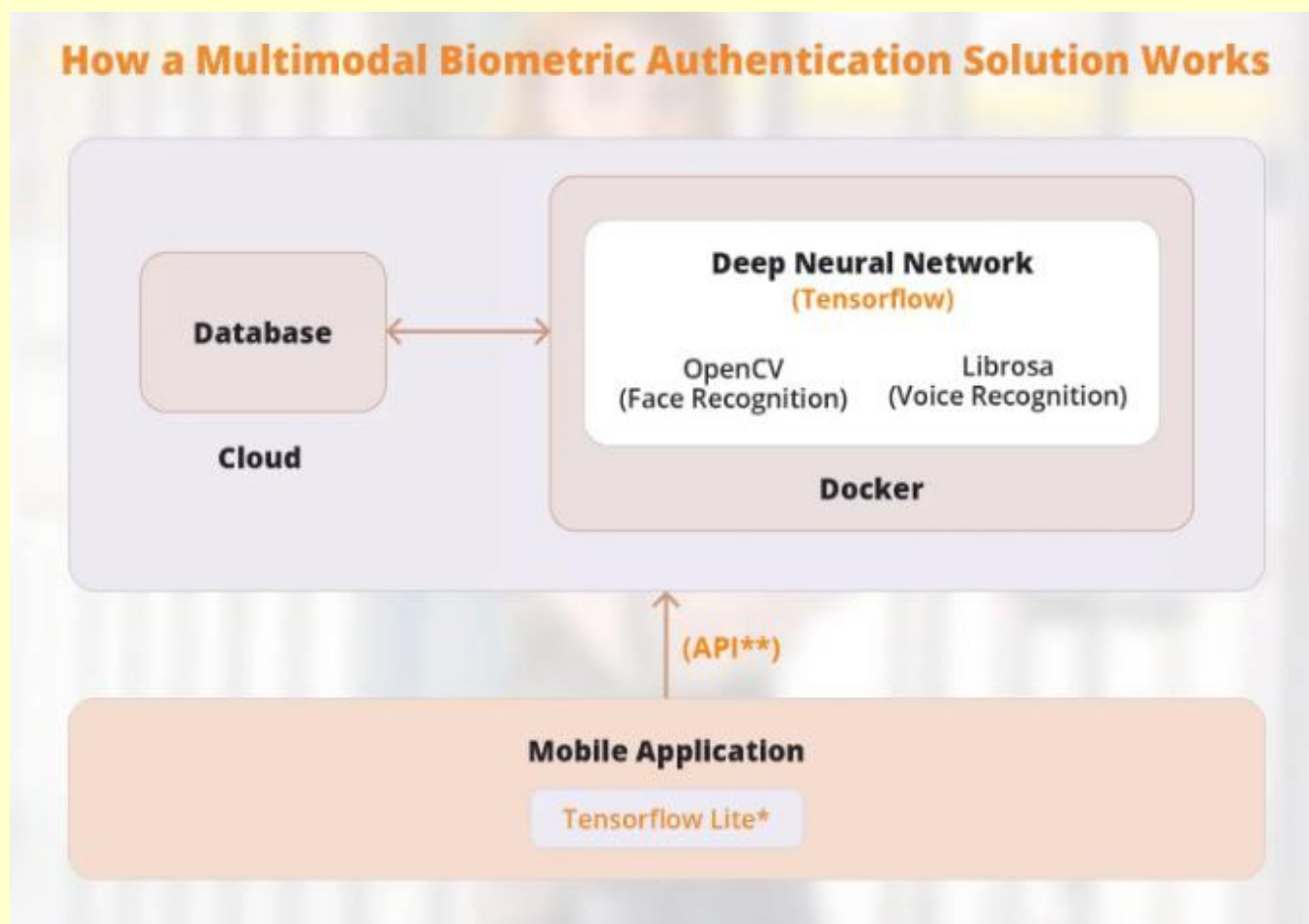
$$n = \frac{1}{2} \left[\tanh\left(0.01 \frac{s - \text{mean}(S)}{\text{std}(S)}\right) + 1 \right]$$

Adaptiva (AD): suprapunerea rezultatelor distribuțiilor autentice și impostor în erori a caracteristicilor biometrice individuale (această regiune oferind centrul său și lățimea sa W). O procedură de normalizare adaptivă care crește nivelul de separare a distribuțiilor originale și impostor este utilizată, în timp ce scorurile se mapează în gama [0,1]:

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

CUM FUNCȚIONEAZĂ SOLUȚIILE DE AUTENTIFICARE BIOMETRICĂ MULTIMODALĂ?

- Fiecare formă de tehnologie biometrică are avantajele și dezavantajele sale. De asemenea, nu toate sunt eficiente în mod universal.
- Pentru a îmbunătăți acuratețea și eficiența tehnologiei de autentificare biometrică, este important să se sporească securitatea cu soluții multimodale de recunoaștere biometrică.



- Rețelele neuronale în aplicațiile mobile pot fi dificil de dezvoltat și implementat. Rețelele neuronale pot fi integrate în aplicații folosind TensorFlow Lite, dar există diverse limitări.
- Antrenarea modelelor de rețele neuronale folosind biblioteca TensorFlow poate fi de ajutor. Va trebui proiectata cu atenție arhitectura aplicației în prealabil și să se ia în considerare aceste cerințe
- Dacă nu este posibilă o aplicație nativă, acest proces poate fi descărcat în cloud pentru a procesa datele ca API în repaus. Cu toate acestea, acest lucru implică resurse de rețea suplimentare și necesită o conexiune la internet.
- Există Nvidia Docker care poate simplifica implementarea sistemului, în timp ce un furnizor de servicii (cum ar fi AWS) poate oferi un canal de comunicare neîntrerupt, putere de calcul pentru rețelele neuronale și o interfață convenabilă pentru scalarea sistemului.

Caracteristici Biometrice SOFT (“slabe”)

- Orice trasatura care oferă unele informații despre identitatea unei persoane, dar nu furnizează dovezi suficiente pentru a determina cu exactitate identitatea
- verifcatorii slabi ai identității 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

CONCLUZII

Avantajele VB :

- Elimina/ reduce fraudele;
- Sporeste securitatea;
- Nu pot fi usor transferate, uitate, pierdute sau copiate;
- Convenabile pentru utilizator ;

Dezavantaje :

- Niciun verificator nu este optim (depinde de aplicatie);
- Nu pot fi inlocuiti daca se pierd;
- Integrare dificila in sistem;
- Susceptibile la incalcarea intimitatii;

Biometria bazată pe AI

- Biometria se referă la măsurarea și analiza statistică a caracteristicilor biologice unice ale unei persoane. Când este cuplată cu inteligența artificială (AI), în special cu învățarea automată (Machine Learning - ML) și învățarea profundă (Deep Learning - DL), aceste sisteme devin mult mai **precise, rapide și adaptabile** în identificarea și verificarea persoanelor.

Cum funcționează biometria cu AI?

AI-ul revoluționează biometria în două moduri principale:

Extracția Caracteristicilor (Feature Extraction):

- În loc să măsoare doar puncte fixe (cum ar fi creștăturile clasice ale amprentelor), algoritmi DL pot învăța să extragă mii de **caracteristici subtile** și **modele complexe** din datele brute (imagini, sunet, video).

Potrivirea și Recunoașterea (matching and recognition):

- AI-ul folosește modele complexe pentru a compara datele biometrice culese cu șabloanele stocate. Aceste modele pot gestiona **variațiile mari** (de exemplu, o persoană care îmbătrânește, schimbările de iluminare, sau expresiile faciale) mult mai eficient decât algoritmi tradiționali.

Tipuri cheie de biometrie îmbunătățită de AI

- AI-ul este aplicat la aproape toate formele de biometrie, dar cele mai notabile includ:

Tipul Biometric	Caracteristici Măsurate	Rolul AI
Recunoașterea Facială	Geometria feței, textură, mișcarea mușchilor	Găsește fețele în mulțime, recunoaștere sub diverse unghiuri/iluminări, detectează măștile/spoofing-ul (fețe false).
Recunoașterea Amprentelor	Modele de creste, puncte caracteristice (minutiae)	Îmbunătățește calitatea imaginii amprente, potrivire mai rapidă în baze de date masive.
Recunoașterea Irisului/Retinei	Modele unice ale irisului, vase de sânge	Identifică cu precizie extremă, chiar și la distanță sau sub ochelari.
Recunoașterea Vocii (Voice)	Frecvența, tonul, ritmul vorbirii	Verificare pe baza intonației și a modului de vorbire (nu doar a cuvintelor), detectarea înregistrărilor sau a vocilor sintetizate.
Biometria Comportamentală	Stilul de tastare, mersul, mișcarea mouse-ului	Stabilește un profil unic de interacțiune (de exemplu, pentru detectarea fraudei online).
Recunoașterea Venei	Modelul venelor sub-dermice	Recunoaștere foarte sigură, dificil de falsificat, AI-ul îmbunătățește detectarea.

Avantajele AI în Biometrie

Precizie Sporită: rate de eroare (False Acceptance Rate - FAR și False Rejection Rate - FRR) mult mai mici.

Viteză: Potrivirea și căutarea în baze de date mari se fac aproape instantaneu.

Securitate Anti-Spoofing: Algoritmii AI, în special Deep Learning, excelează în detectarea încercărilor de fraudă (de exemplu, folosind o fotografie 2D în loc de o față vie, cunoscută ca Liveness Detection).

Adaptabilitate: Sistemele pot învăța continuu din noi date, îmbunătățind performanța în timp.

Fuziunea multi-modală: AI-ul poate combina date din mai multe surse biometrice (de exemplu, fața și vocea) pentru o rată de precizie aproape perfectă.

Provocări și Preocupări Etice

Deși este un domeniu promițător, biometria cu AI aduce și provocări:

Biasul algoritmic: Sistemele AI pot reflecta și amplifica biasurile din datele de antrenament. De exemplu, unele sisteme de recunoaștere facială au performanțe mai slabe pentru anumite grupuri demografice (cum ar fi persoanele cu pielea mai închisă la culoare sau femeile).

Confidențialitatea datelor: Datele biometrice sunt extrem de sensibile. Stocarea, securitatea și Reglementarea lor (cum ar fi GDPR) sunt critice.

Eroare Zero: Deși AI-ul a redus drastic erorile, nicio tehnologie nu este 100% perfectă, iar o greșeală (mai ales o identificare greșită) poate avea consecințe semnificative.

Aplicații Curente

Biometria cu AI este utilizată pe scară largă în:

- **Acces Dispozitive:** Deblocarea smartphone-urilor (Face ID).
- **Securitatea Frontierelor:** Scanarea facială și a irisului în aeroporturi.
- **Servicii Financiare:** Verificarea identității pentru plăți și deschiderea de conturi.
- **Sisteme de Supraveghere:** Monitorizarea zonelor publice și căutarea persoanelor dispărute/suspecte.