

BIO – Biometrické systémy

Úvod do biometrických systémů

Tomáš Goldmann , 2024

na základě přednášky Martina Drahanského

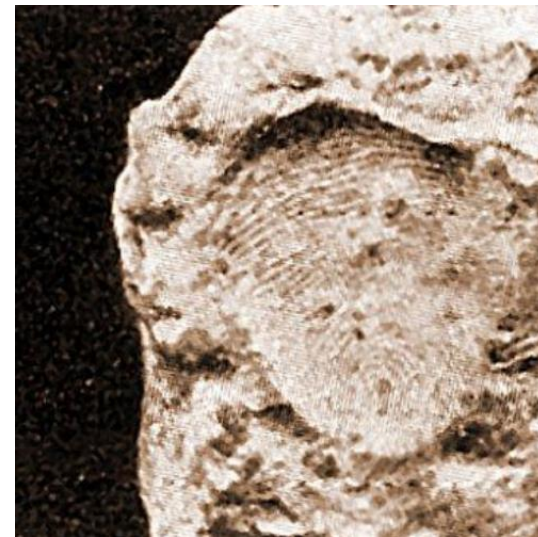
- ❑ Pojem biometrie je složen ze dvou řeckých slov ze slov „bios“ (život) a „metron“ (měřítko)
- ❑ Měření a analýza biologických rysů
- ❑ Široké spektrum aplikací (spotřebitelská elektronika, zabezpečení kritické infrastruktury, ..)
- ❑ Biometrické metody můžeme rozdělit na **neautomatické** a **automatické**
- ❑ S biometrií se setkáváme denně:
 - Rozpoznávání obličeje
 - Rozpoznávání hlasu
 - ...



- ❑ **500 let před naším letopočtem** – Potvrzování obchodních transakcí otiskem prstů do hliněných tabulek
- ❑ **14. století** – Otisky prstů použité pro verifikaci obchodních partnerů



<https://blog.humanode.io/evolution-of-biometrics>



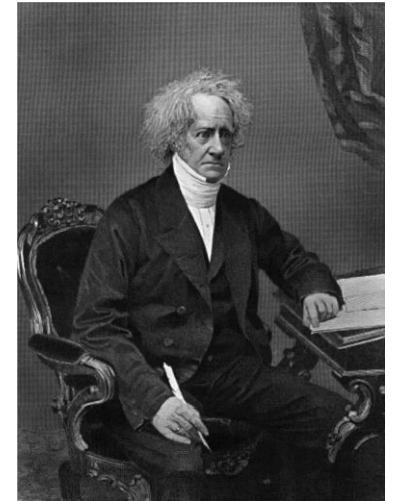
<https://time.graphics/event/143559>

- ❑ **1858** - W.J. Herschel – Využíval otisky prstů a dlaně na zadní straně kontraktů zaměstnanců

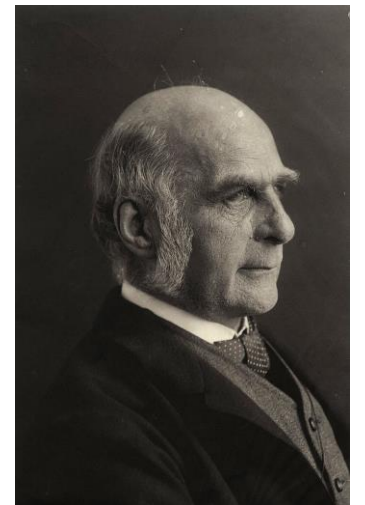


<https://blog.humanode.io/evolution-of-biometrics>

- ❑ **1865** - Francis Galton - Studie o dědičnosti fyzických vlastností („Hereditary talent and character“)
- ❑ **1869** - Francis Galton - Spoluzakladatel eugeniky
- ❑ **1875** - Francis Galton - Zakladatel výzkumu dvojčat



W.J. Herschel



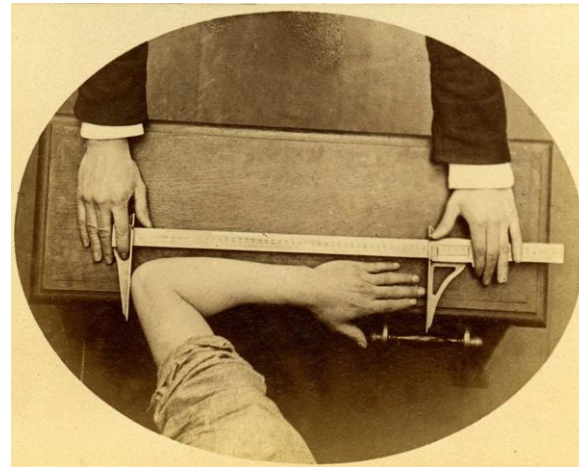
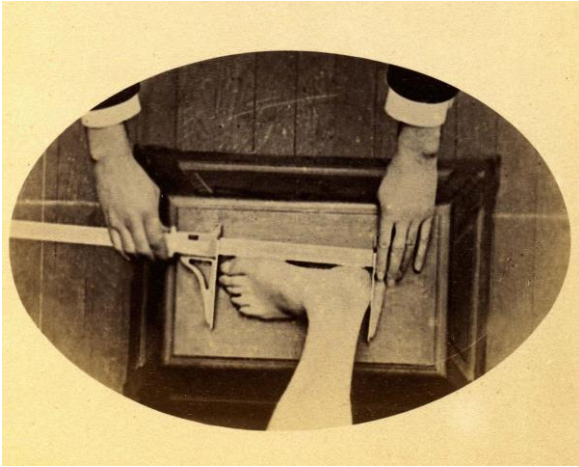
F. Galton

- ❑ **1880** - Francis Galton - Zavedení antropometrie



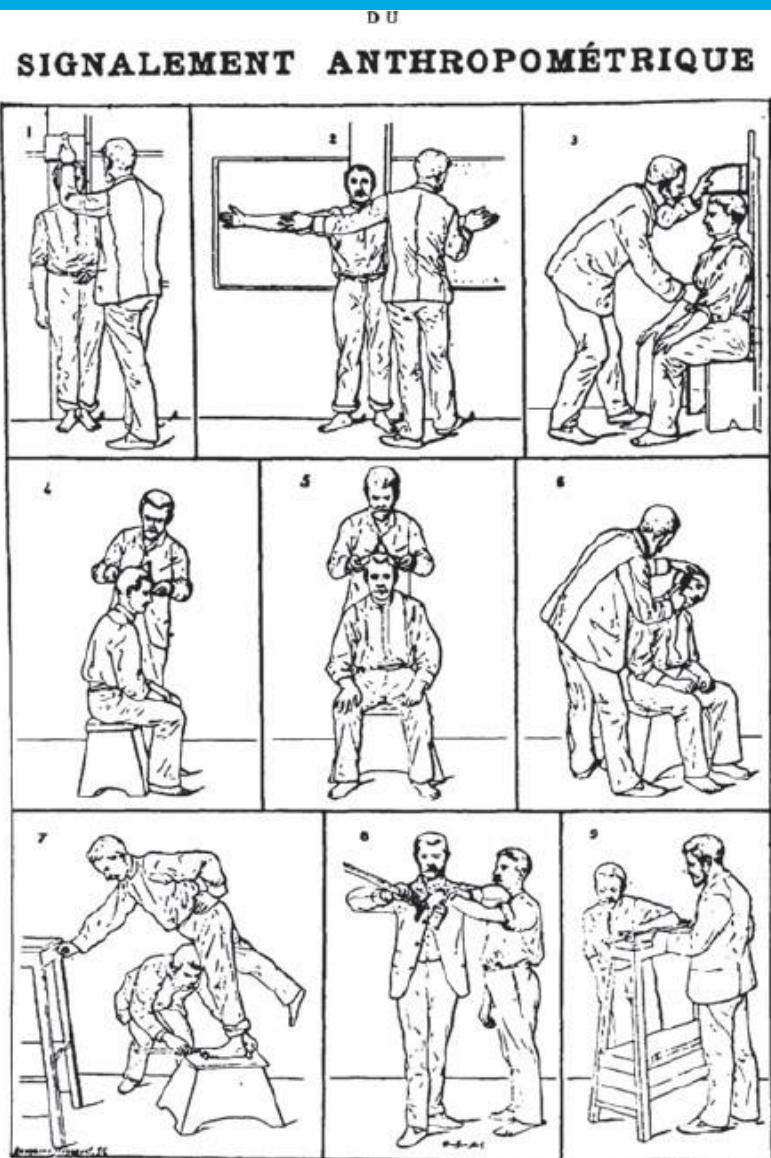
❑ 1879 -1883 – První pokusy s tzv. Bertillonovou metodou

- Louis Alphonse Bertillon – policista antropolog, kriminolog, fotograf a kriminalista, průkopník kriminalistické fotografie
- Využití antropometrie jako identifikačního systému (pro měření bylo použito 11 tělesných rozměrů)
- Později se přidaly k antropometrickým měřením otisky prstů -> vytlačily Bertillonovou metodu



- ❑ **Antropometrie** je vědní disciplína zabývající se měřením a studiem rozměrů lidského těla.
- ❑ Antropometrické rozměry jsou u většiny lidí stabilní od 20. roku života (výjimky: zdravotní stav, životní styl, hormonální vlivy)

- ☐ 1. Tělesná výška
- ☐ 2. Délka natažené paže
- ☐ 3. Výška v sedu
- ☐ 4. Délka hlavy
- ☐ 5. Šířka hlavy
- ☐ 6a. Délka pravého ucha
- ☐ 6b. Šířka pravého ucha
- ☐ 7. Délka levé nohy
- ☐ 8a. Délka lev. prostředníčku
- ☐ 8b. Délka levého malíčku
- ☐ 9. Délka levého předloktí



Height,	Head length,	L. Foot,
Outer Arms,	Head width,	L. Mid. F.
Trunk,	B. Ear. Length,	L. L. F.
	Cheek,	L. Fore A.

Name	
Alias	
Alias	
Crime	
Age	Height
Weight	Build
Hair	Eyes
Born	Beard
Complexion	
Occupation	
Date of arrest	
Officer	

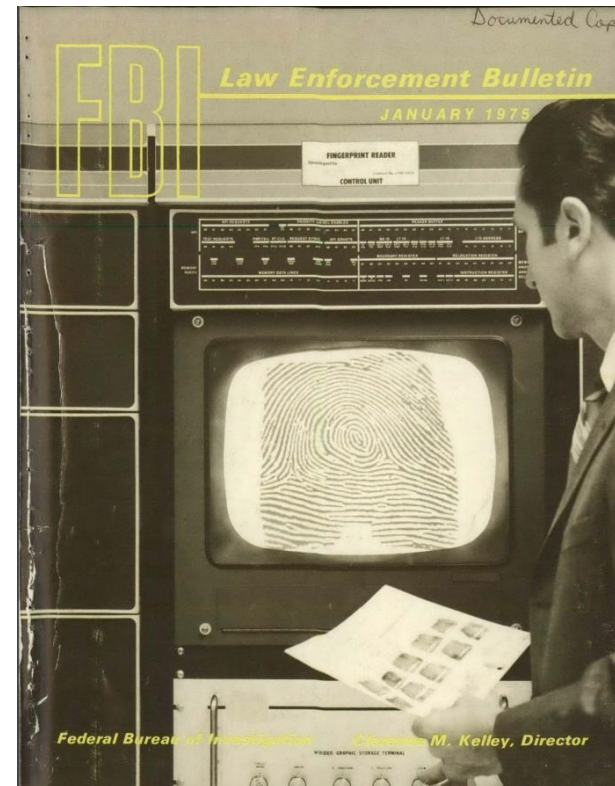
St. L. Detect. Dept. St. Louis, Mo.

- ❑ **léta 1890** - Argentina: Zavedení daktyloskopie jako identifikačního systému
- ❑ **1892** – Argentina: První vyřešený případ s využitím otisků prstů

- ❑ **1892** – Británie: F. Galton- kniha „Finger Prints “ (<https://galton.org/books/finger-prints/index.htm>)
- ❑ **1893** – Británie: Scotland Yard zavedl Galtonův systém do policejní služby jako doplněk Bertinollovy metody

- ❑ **1900 – Nahrazení Bertinollovy metody a zavedení Henryho systému**
 - Edward Henry – Definoval systém jak klasifikovat a uchovat informace o otiscích prstů

- ❑ 1924 - Založení oddělení identifikace otisků u FBI
- ❑ 1936 - Frank Burch - představil koncept využití duhovky pro identifikaci
- ❑ 1965 - Použití systému AFIS s 810 tisíci otisky prstů
- ❑ 1970 – Automatické rozpoznávání podle otisků prstů
- ❑ 1971 - První článek k rozpoznávání obličeje
- ❑ 1974 - První použití rozpoznávání na základě geometrie ruky
- ❑ 1985 – Leonard Flam and Aran Safir - Představení konceptu, že duhovka je pro každého člověka jedinečná
- ❑ 1996 – Použití rozpoznávání podle geometrie ruky při olympiádě v Atlant
- ❑ 1999 - Nasazení IAFIS (Integrated Automated Fingerprint Identification System)
- ❑ 2011 – NGI (Next Generation Identification)
- ❑ 2013 – Představení Apple Touch ID
- ❑ 2018 – Mastercard se senzorem otisků prstů



- ❑ **Biometrie** (IT) je automatické rozpoznávání jednotlivců na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a charakteristického *chování* (např. podpis, chůze).

- ❑ *ISO/IEC JTC 1/SC37 omezuje rozsah výrazu „jednotlivec“ na lidskou bytost.

- ❑ **Biometrická charakteristika** (biometric characteristic) - biologická a behaviorální charakteristika jednotlivce, které mohou být detekovány a ze kterých lze pro účely automatického rozpoznávání jednotlivců získat rozlišující opakovatelné biometrické rysy

- ❑ Biometrické rysy

- ❑ Biometrická šablona

❑ Biometrické charakteristiky

- Fyziologické rysy
- Behaviorální

❑ Identita

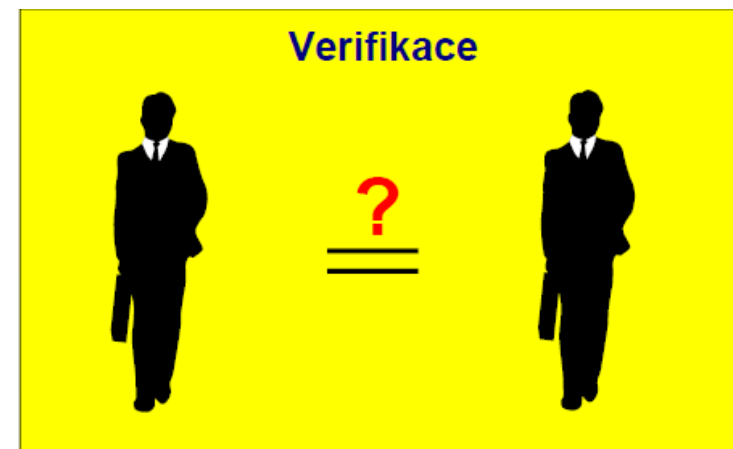
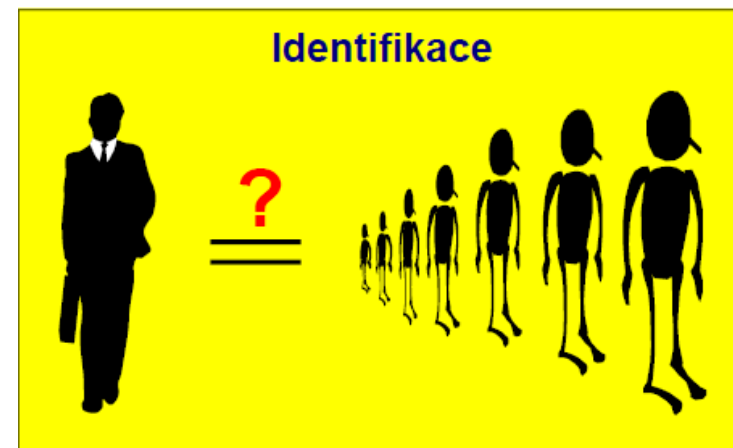
- **Fyzická identita** – fyzická charakteristika člověka.
- **Elektronická identita** – spojena s digitálním světem.
- Příklad: Přihlašovací údaje k e-mailovému účtu nebo bankovní aplikaci.

❑ Identifikace

- Porovnání 1:N
- **Praktický příklad:** Využití rozpoznání obličeje v letištních bezpečnostních systémech, kde je obličej cestujícího porovnán s databází známých identit.

❑ Verifikace

- Porovnání 1:1
- **Praktický příklad:** Odemčení mobilního telefonu pomocí otisku prstu, kde je otisk prstu porovnán s uloženým otiskem.



❑ Autentizace

- **Potvrzení identity** - Autentizace je proces ověření totožnosti osoby na základě jejich jedinečných biologických charakteristik.

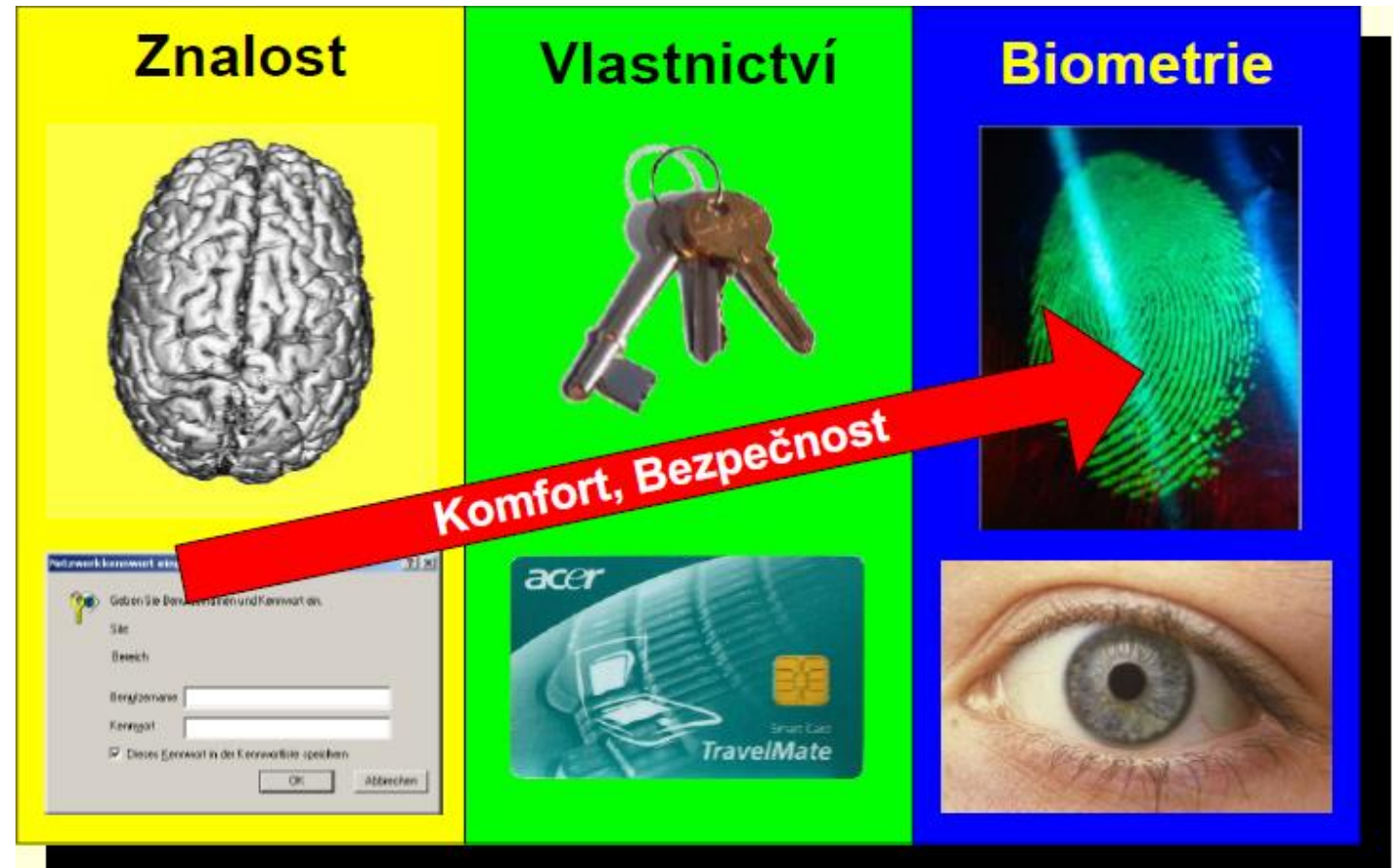
❑ Autorizace

- **Oprávnění k akci** - Autorizace je proces, který následuje po autentizaci. Znamená přidělení oprávnění k provedení určité akce nebo přístupu k určitému zdroji. Jinými slovy, po ověření identity je osoba oprávněna k vykonání specifických činností.

❑ **Identita** z latinského slova „idem“ (totéž)

❑ Je založená na:

- něčem co víme („we know“)
- něčem co máme („we have“)
- něčem co jsme („we are“)



❑ Něco co víme

- Tajné tlačítko / páčka
- Předepsaný postup
- Heslo
- PIN

❑ Idea: **Náhodná** a **lehce** zapamatovatelná informace.

❑ Nebezpečí: Získání této tajné skutečnosti nepovolanou osobou.



"Your logon password is XB#2D940. Write it down and don't lose it again."

<https://www.netsec.news/how-long-does-it-take-a-hacker-to-brute-force-a-password-in-2023/>

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years



HIVE
SYSTEMS

> Learn more about this at hivesystems.com/password

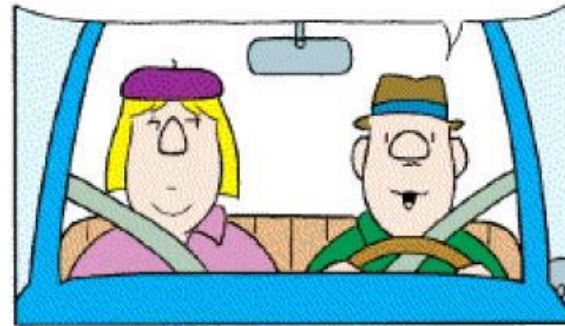
12x RTX 4090

THE BORN LOSER®



by Art & Chip Sansom

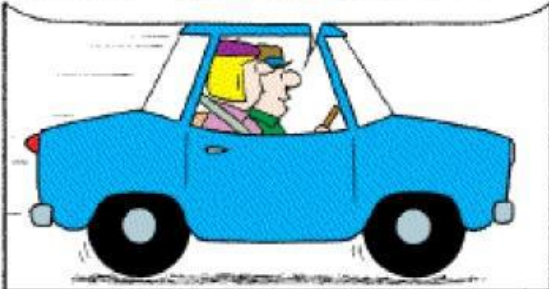
"I GOT OUR NEW ATM CARD TODAY!"



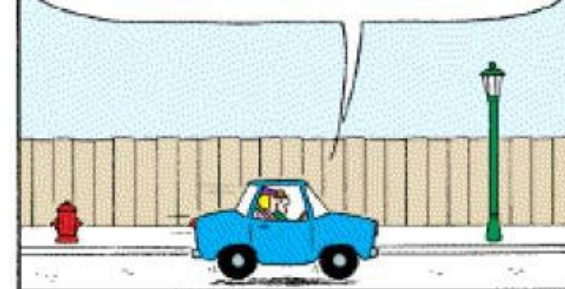
YOU DID? OH, GOODIE!
I CAN'T WAIT TO USE IT!



"I HAD TO SELECT A SECRET PIN
CODE FOR THE NEW ATM CARD!"



"AFTER GIVING IT A LOT OF THOUGHT, I
FINALLY SETTLED ON ONE!"



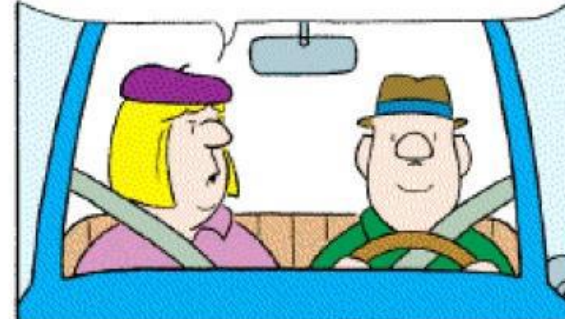
LET ME GUESS...
IT'S OUR INITIALS?
OUR PHONE NUMBER?
OUR ANNIVERSARY?
OUR ADDRESS?



HA! ANY CRIMINAL
COULD EASILY CONNECT
THOSE WITH US! I
CAME UP WITH A
CODE NO ONE
WOULD THINK TO
ASSOCIATE WITH US!



"ALL RIGHT, ALREADY! WHAT IS IT?"



313715!



www.coffin.com
© 2000 by NEA, Inc.
Art & Chip Sansom

❑ **Klíčová myšlenka:** Identifikace prostřednictvím něčeho, co vlastníme a ostatní ne.

❑ **Co vlastníme (fyzické identifikátory)**

- **Klíč:** Fyzický nebo digitální pro přístup
- **Čipová karta (Smart karta):** Elektronická karta s integrovaným čipem
- **Token:** Fyzické zařízení pro dvoufaktorovou autentizaci
- **RFID-Tag:** Bezkontaktní technologie pro identifikaci

❑ **Něco co máme**

- Klíč
- Čipovou (smart) kartu
- Token
- RFID-Tag

❑ **Rizika fyzické identifikace:**

- **Zcizení vlastnictví neoprávněnou osobou:**
 - Krádež (může trvat déle, než si uvědomíme, že byl majetek ztracen).
 - Nelegální kopie nebo neoprávněné přečtení informací z karty, tokenu či RFID.

❑ **Klíčová myšlenka:** Naše tělo a chování samo o sobě slouží jako identifikační klíč.

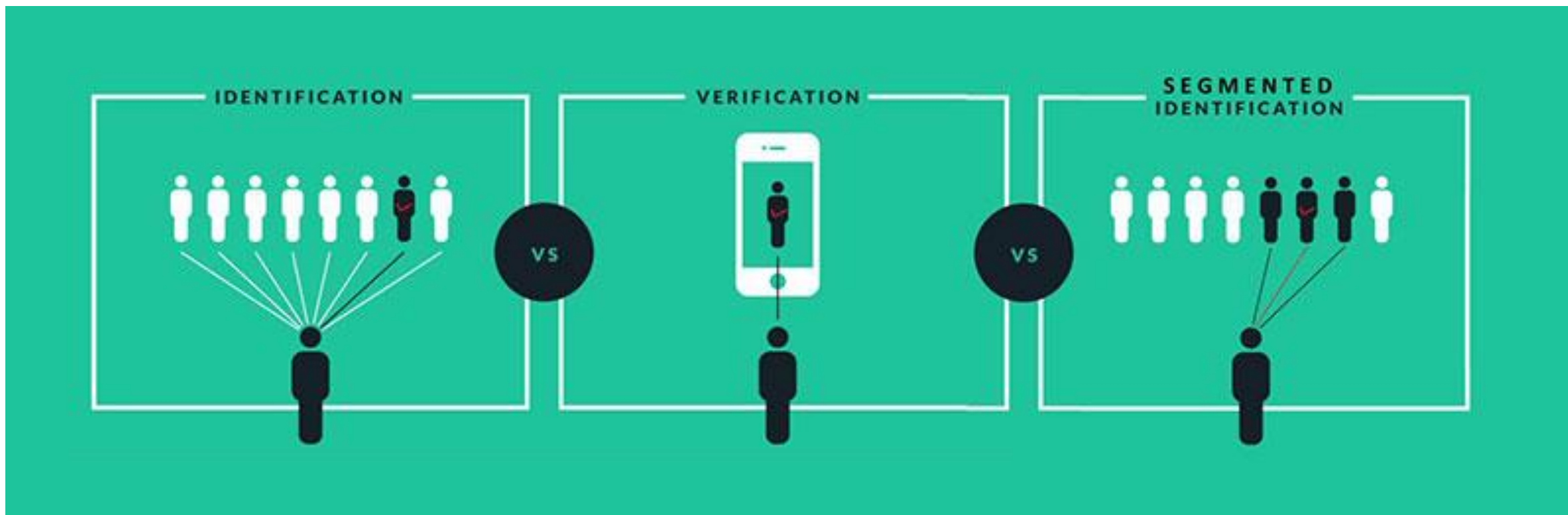
❑ **Co nás definuje (biometrické identifikátory)**

- **Vzhled:** Obličejové rysy, barva očí, struktura pokožky
- **Pohyby:** Chůze, gestikulace, dynamika pohybů
- **Chování:** Rytmus řeči, reakce na různé podněty
- **Projevy v různých situacích:** Emoce, výrazy tváře, rozhodování ve stresových podmínkách

❑ **Rizika biometrické identifikace:**

- Využití kopie biometrických údajů pro vytvoření falešné identity.
 - **Příklad:** Kopie otisku prstu zanechaná na skle v restauraci.
 - **Příklad:** Fotografie obličeje pořízená během dovolené, využita k neautorizované identifikaci.

- ❑ Segmented identification (spíš marketingový pojem)



- ❑ Klíčový proces v biometrických systémech
 - **Identifikace jednotlivce porovnáním jeho biometrických údajů s mnoha záznamy v databázi**

- ❑ Možné výsledky
 - Identita potvrzena
 - Nenalezeno
 - Skupina nejpravděpodobnějších kandidátů

- ❑ Příklady použití
 - Automatizované daktyloskopické identifikační systémy (AFIS)
 - Databáze žadatelů o azyl
 - Registrace nových uživatelů v systémech

- ❑ Právní a etické otázky
 - Regulace a normy týkající se biometrické identifikace
 - EU ACT o AI

- ❑ Klíčový proces v biometrických systémech
 - Verifikace identity porovnáním aktuálních biometrických údajů s jediným uloženým vzorkem.

- ❑ Možné výsledky
 - Potvrzeno
 - Nepotvrzeno

- ❑ Příklady použití
 - Přístupové systémy (např. odemykání telefonu nebo počítače pomocí otisku prstu či rozpoznání obličeje)
 - Biometrické platební systémy (potvrzení platby pomocí biometrie)
 - Vstupní kontrola na pracovištích (ověření zaměstnance při vstupu)

- ❑ Proces, kterým systém potvrzuje autentičnost (hodnověrnost) identity uživatele.
- ❑ Použití v biometrických systémech
 - Identifikace (1:N) - Zjištění identity uživatele porovnáním aktuálního vzorku s databází referenčních vzorků.
 - Verifikace (1:1) - Ověření, zda uživatel je tím, za koho se vydává, porovnáním aktuálního vzorku s jedním referenčním vzorkem
- ❑ Příklady použití
 - Přístupové systémy
 - Kontrola vstupu do zabezpečených prostor pomocí biometrie (otisk prstu, rozpoznání obličeje).
 - Daktyloskopické systémy
 - Použití otisků prstů pro identifikaci nebo verifikaci osob.
- ❑ Časté zaměňování pojmů:
 - Autentizace je proces potvrzení identity uživatele.
 - Autorizace určuje, jaká oprávnění má ověřený uživatel.
 - Verifikace je metoda autentizace formou 1:1 porovnání.
 - Identifikace je metoda autentizace formou 1:N porovnání.

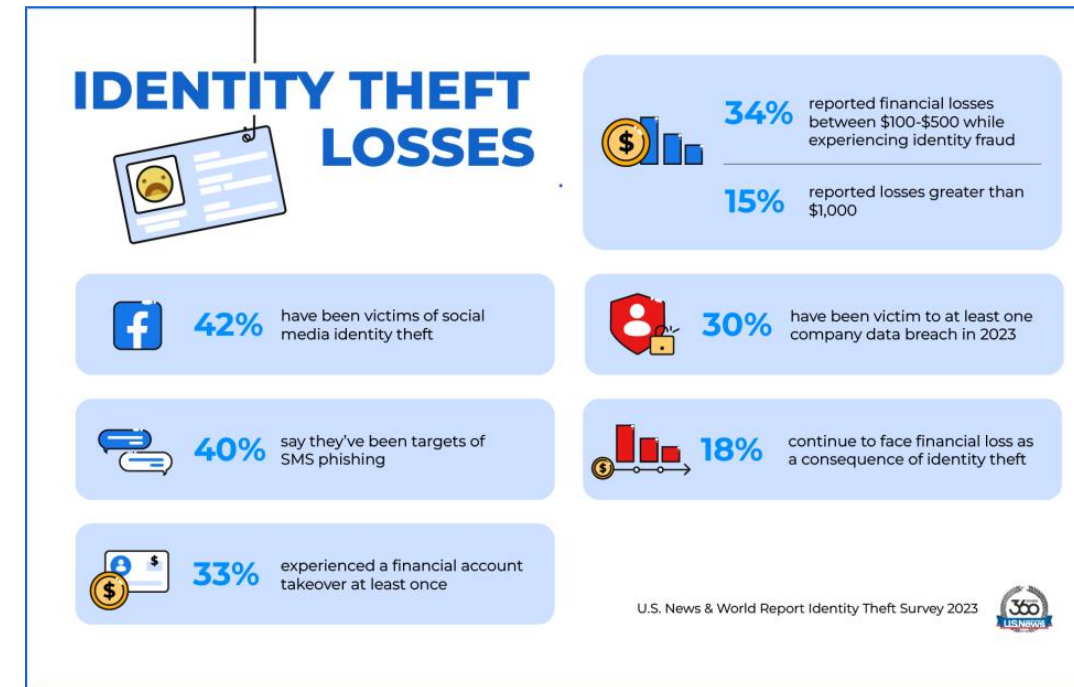
- ❑ V dřívějších dobách se lidé v menších komunitách znali mezi sebou.
- ❑ S růstem populace a nárůstem mobility jsme se začali spoléhat na dokumenty a tajemství, které nám slouží k určení identity.
- ❑ Identifikace a verifikace osob jsou dnes klíčovými součástmi infrastruktury v různých sektorech, jako je bankovníctví, hraniční kontrola nebo právní systém.

- ❑ Otázky spojené s identitou jednotlivce:
 - Je tato osoba skutečně tou, za kterou se vydává? (Verifikace)
 - Byl tento žadatel u nás již někdy dříve? (Identifikace)
 - Má mít tento uživatel přístup k našemu systému? (Autorizace)

- ❑ Žijeme nyní v globální společnosti, ve které se vyskytují všehoschopní a nebezpeční jedinci, kterým nemůžeme již věřit na základě předložených osobních dokladů (problematika falešné identity).

❑ Krádež identity-„Identity Theft“

- Zloději identity odcizí kreditní kartu, zjistí PIN (např. datum narození), zcizeným PINem provedou úspěšně autentizaci a vyberou z bankomatu peníze
- V roce 2021 se stalo USA přibližně 23,9 milionů krádeží identit



<https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey>

❑ Výhody:

- Vysoká úroveň bezpečnosti - Jedinečné biometrické údaje je obtížné padělat nebo kopírovat.
- Pohodlí pro uživatele - Není nutné si pamatovat hesla nebo nosit identifikační karty.
- Rychlost a efektivita - Okamžité ověření identity v reálném čase.
- Snížení rizika podvodů - Těžší neoprávněný přístup díky jedinečnosti biometrických dat.
- Univerzální použitelnost - Využití napříč různými odvětvími jako bankovníctví, zdravotnictví či bezpečnost.
- Zlepšení uživatelské zkušenosti - Jednodušší a intuitivnější proces autentizace.
- Snadná integrace - Kompatibilita s existujícími systémy a bezpečnostními protokoly.
- Dlouhodobá nákladová efektivita - Snížení nákladů na správu hesel a obnovu přístupových údajů.

❑ Nevýhody:

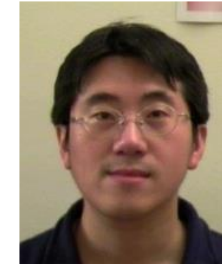
- Obavy o soukromí - Sběr a ukládání biometrických údajů může vést k narušení osobního soukromí.
- Možnost zneužití dat - Kompromitované biometrické údaje nelze změnit jako heslo nebo PIN, což zvyšuje riziko jejich zneužití.
- Chyby při identifikaci - Falešně pozitivní (nesprávné potvrzení identity) a falešně negativní (nesprávné odmítnutí identity) výsledky mohou způsobit problémy.
- Technologické omezení - Kvalita snímačů a okolní podmínky (světlo, hluk) mohou ovlivnit přesnost rozpoznání.
- Vysoké počáteční náklady - Implementace a údržba biometrických systémů může být finančně náročná.
- Etické a právní otázky - Různé legislativy a normy mohou omezovat použití biometrických technologií.
- Hygienické obavy - Sdílená zařízení (např. snímače otisků prstů) mohou představovat zdravotní riziko.
- Technické překážky u některých uživatelů - Fyzické vlastnosti nebo zdravotní stav mohou bránit přesnému snímání (např. opotřebené otisky prstů, jizvy).
- Akceptace uživateli - Někteří lidé mohou mít odpor nebo nedůvěru k používání biometrie.

- ❑ Hlavní výzvou pro biometrii je navrhnout biometrický systém, který kombinuje použitelnost, škálovatelnost a přesnost.

- ❑ Metriky přesnosti (více 2. přednáška):
 - **FAR (False Acceptance Rate)** – Míra falešného přijetí: Procento případů, kdy systém chybně akceptuje neautorizovanou osobu jako správnou.
 - **FRR (False Rejection Rate)** – Míra falešného odmítnutí: Procento případů, kdy systém nesprávně odmítne autorizovanou osobu.
 - **EER (Equal Error Rate)** – Míra rovnovážné chyby: Bod, kde se FAR a FRR rovnají. Nižší EER znamená vyšší přesnost systému.
 - **TAR (True Acceptance Rate)** – Míra správného přijetí: Procento případů, kdy systém správně identifikuje autorizovanou osobu (doplňuje FRR).
 - **FMR (False Match Rate)** – Míra nesprávné shody: Podobná FAR, ale specificky se zaměřuje na nesprávné párování biometrických vzorků.
 - **FNMR (False Non-Match Rate)** – Míra nesprávné neshody: Procento případů, kdy systém chybně neidentifikuje shodné biometrické vzorky.

- ☐ Mezitřídní a vnitrotřídní variabilita
- ☐ Segmentace
- ☐ Zašuměný vstup
- ☐ Výkonnost systému (chyby, rychlost, náklady)
- ☐ Jednoznačnost biometrické vlastnosti
- ☐ Fúze více biometrických vlastností
- ☐ Rozšiřitelnost
- ☐ Útoky na biometrický systém
- ☐ Otázky privátních dat

- ❑ **Vnitrotrídní variabilita (Intra-Class Variability)** - Rozdíly v biometrických vzorcích téže osoby při různých měřeních.
- ❑ Příčiny:
 - Fyzické změny: Stárnutí, zdravotní stav, zranění.
 - Podmínky snímání: Osvětlení, úhel, vzdálenost, kvalita snímače.
 - Dočasné faktory: Mimika, nálada, únava, prostředí.
- ❑ Může vést k **falešně negativním výsledkům** (systém nepozná oprávněného uživatele).



https://www.researchgate.net/figure/Intra-class-variation-associated-with-an-individuals-face-image-Due-to-change-in-pose_fig5_50315614

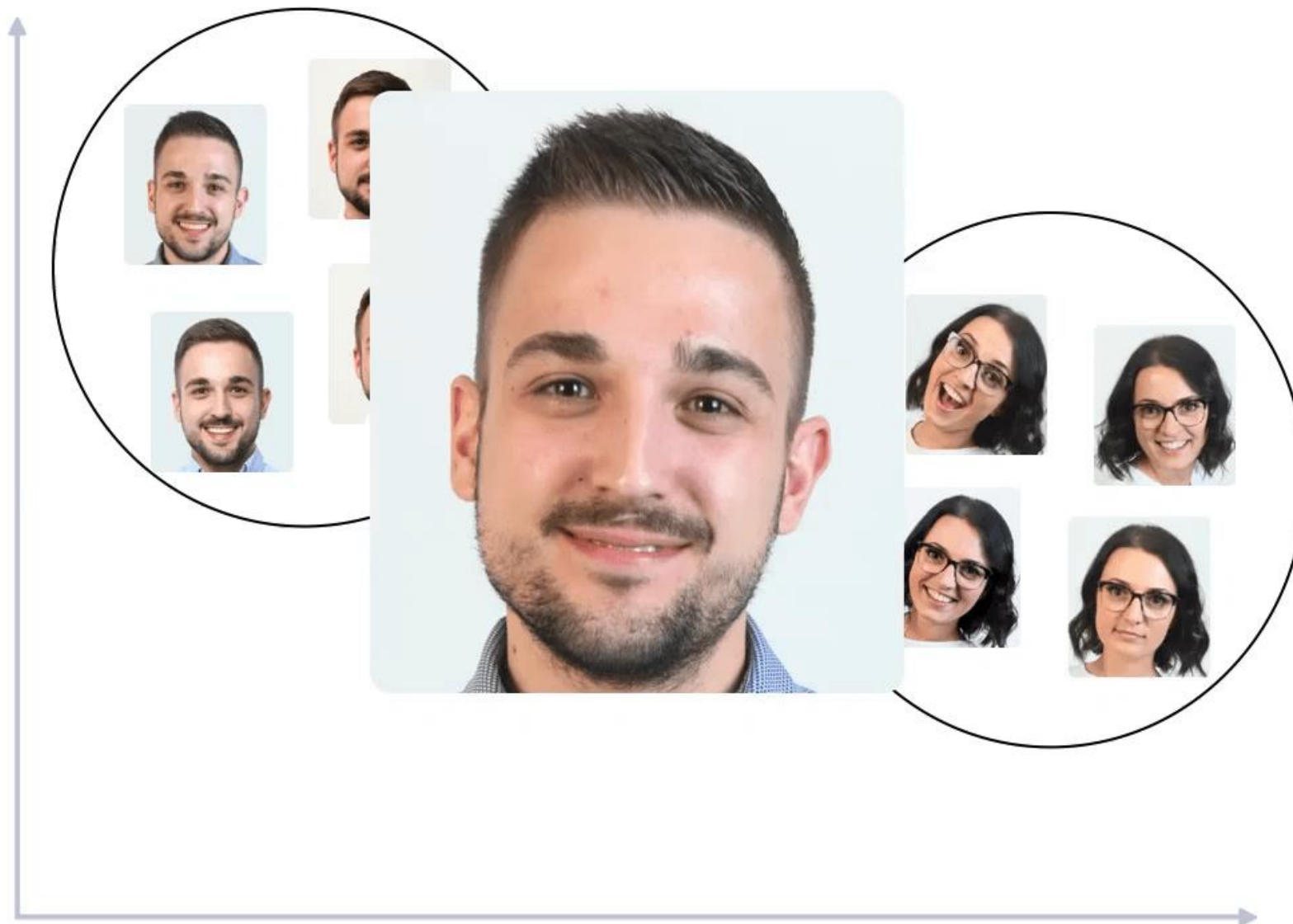
- ❑ **Mezitřídní variabilita (Inter-Class Variability)** - Rozdíly mezi biometrickými vzorci různých osob.
- ❑ Požadavky:
 - Vzorky různých osob by měly být co nejvíce odlišné.
- ❑ Nízká mezitřídní variabilita může vést k **falešně pozitivním výsledkům** (systém zamění neoprávněnou osobu za oprávněnou).



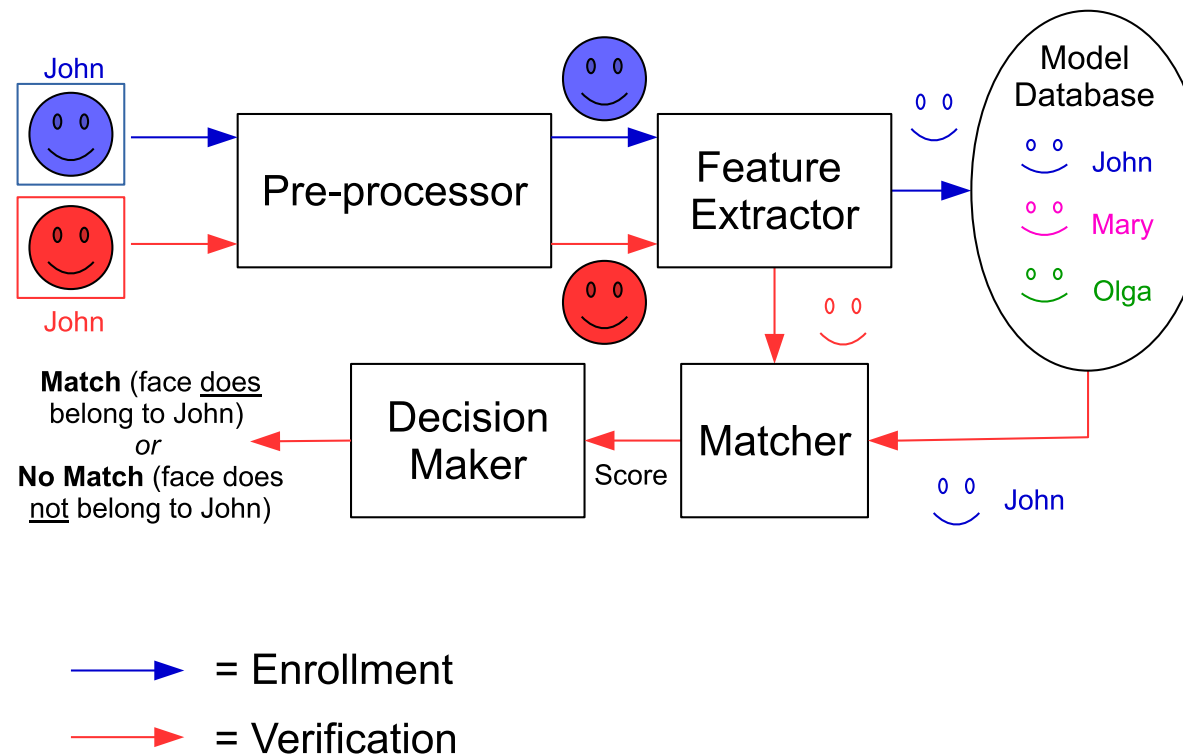
Dataset: 23 Pairs of Identical Twins Face Image Data

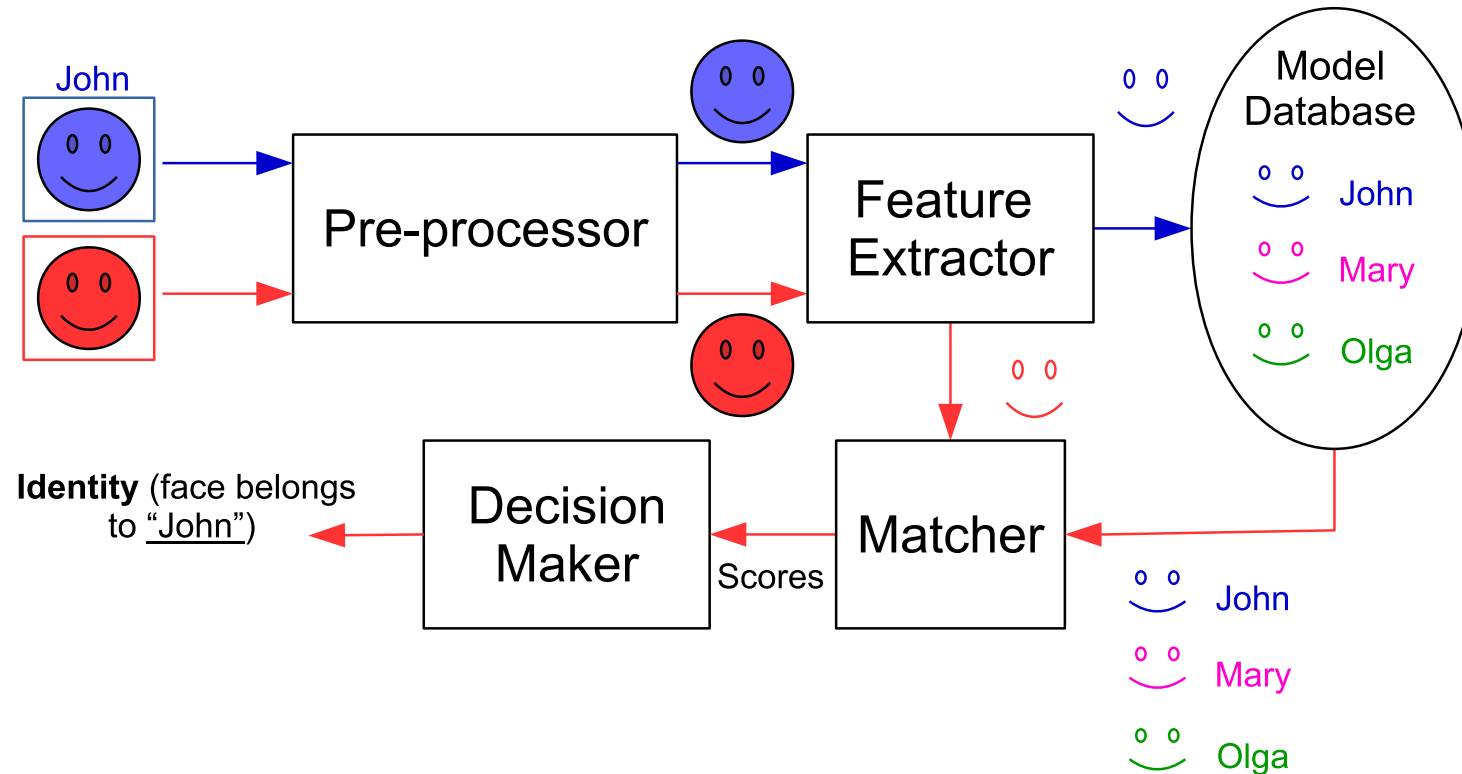


- ❑ **Cíl v biometrických aplikacích: Minimalizovat vnitrotřídní variabilitu a maximalizovat mezitřídní variabilitu.**
- ❑ Vývoj algoritmů, které jsou odolné vůči změnám u téže osoby a citlivé na rozdíly mezi různými osobami.
- ❑ Příklady
 - **Rozpoznávání otisků prstů:**
 - Vnitrotřídní variabilita: Suchá nebo vlhká pokožka, drobná poranění.
 - Mezitřídní variabilita: Podobné vzory papilárních linií u různých osob.
 - **Rozpoznávání obličeje:**
 - Vnitrotřídní variabilita: Různé výrazy, osvětlení, stárnutí.
 - Mezitřídní variabilita: Vysoká podobnost mezi příbuznými nebo dvojčaty.
 - **Rozpoznávání hlasu:**
 - Vnitrotřídní variabilita: Nachlazení, stres, emoční stav.
 - Mezitřídní variabilita: Podobné hlasové charakteristiky u různých osob.

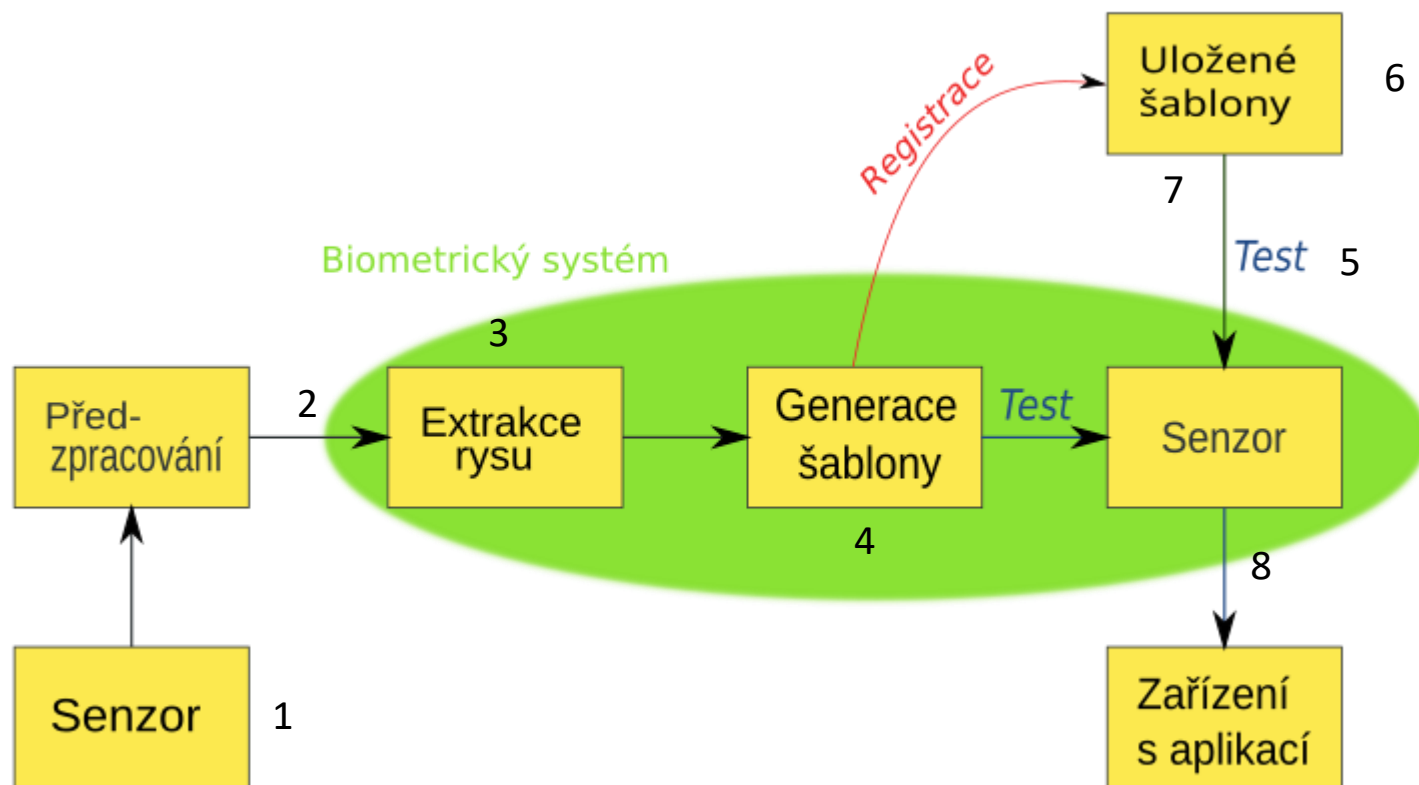


- ❑ **Registrace (*enrollment*)** – je proces zachycení biometrických dat, zpracování, vytvoření biometrické šablony a následné uložení do databáze.
- ❑ **Rozpoznání (*recognition*)** – Nově nasnímaná biometrická data jsou porovnána s databází zaregistrovaných dat
 - V případě verifikace rozhodneme, zdali se jedná o stejnou osobu.
 - V případě identifikace rozhodneme, které identitě náleží vstupní biometrická data.





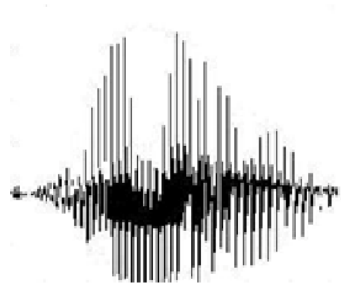
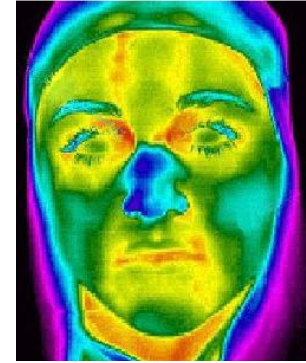
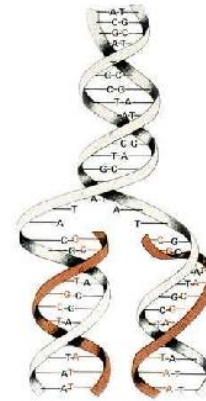
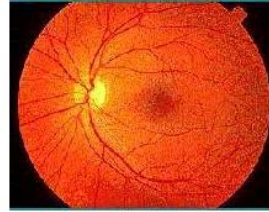
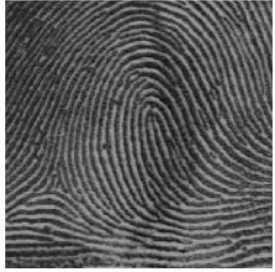
—————> = Enrollment
 —————> = Identification



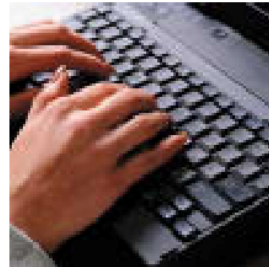
1. Podvrh biom. charakteristik
2. Replikace starých dat
3. Modifikace extraktoru
4. Syntetický vektor rysů
5. Změna porovnání
6. Modifikace šablony
7. Blokování kanálu
8. Změna výsledku

BIO

Biometrické charakteristiky



Uudag



Fyziologické rysy, které se s časem výrazně nemění (např. otisky prstů, tvar obličeje).

- ❑ **Jedinečné pro každého jednotlivce** - Každý člověk má odlišné biometrické vzorce, což zajišťuje vysokou úroveň bezpečnosti (např. duhovka, sítnice).
- ❑ **Snímatelné a analyzovatelné** - Statické charakteristiky lze jednoduše zachytit pomocí specializovaných zařízení (kamery, skenery).
- ❑ **Odolnost vůči dočasným změnám** - Na rozdíl od behaviorálních charakteristik nejsou statické biometrické údaje ovlivněny náladou, zdravím nebo prostředím.
- ❑ **Vysoká přesnost** - Díky své stálosti a jedinečnosti poskytují velmi přesné výsledky, ideální pro dlouhodobé ověřování identity.
- ❑ **Použití v různých sektorech** - Uplatnění v oblastech, kde je potřeba vysoká úroveň zabezpečení, jako je bankovníctví, kriminalistika, či hraniční kontrola.
- ❑ **Technologická omezení** - Kvalita snímače a podmínky (osvětlení, vlhkost) mohou ovlivnit přesnost, ale při správném nastavení jsou velmi spolehlivé.



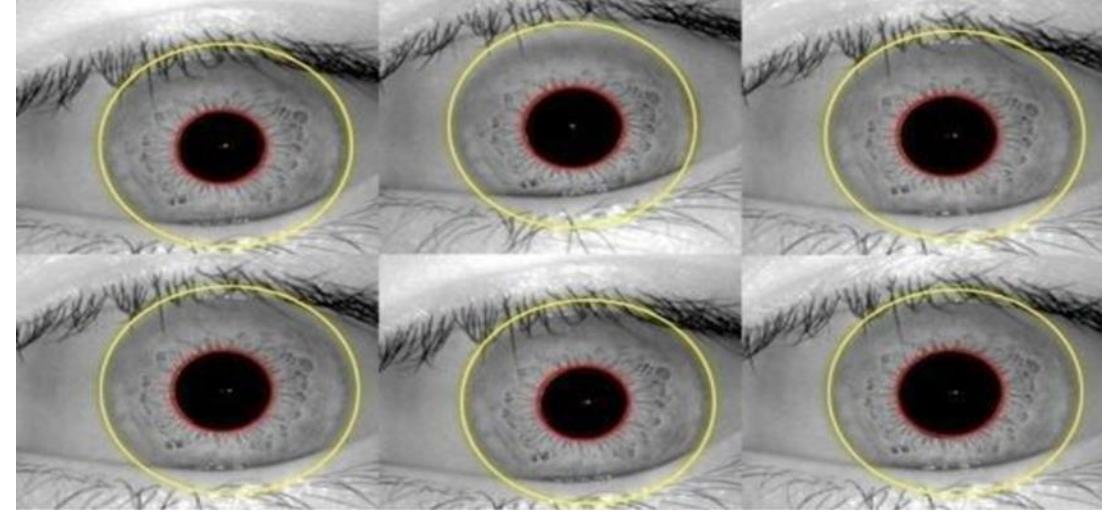
☐ Anatomické (fyzické) charakteristiky:

- Otisk prstu
- Obličej
- Duhovka oka
- Sítnice oka
- Geometrie ruky
- Dlaň
- Termogram obličeje
- Termogram ruky
- Dentální obraz
- Podpis
- Tvar ucha
- Snímek nehtu
- DNA

- ❑ Dynamické charakteristiky vycházejí z jedinečných vzorců chování jednotlivce, např. rytmus chůze, dynamika podpisu, způsob psaní.
- ❑ **Proměnlivé v čase** - Tyto charakteristiky se mohou měnit v závislosti na fyzickém stavu, emocích, únavě nebo prostředí (např. změny hlasu při nachlazení).
- ❑ **Měření procesu, ne jen výsledku** - Dynamické biometrické metody sledují nejen výsledek (např. podpis), ale také způsob, jakým je akce prováděna (rychlost, tlak při podpisu).
- ❑ **Riziko falešných pozitiv/negativ** - Vzhledem k proměnlivosti mohou dynamické biometrické systémy někdy poskytnout méně přesné výsledky ve srovnání se statickými metodami.
- ❑ **Využití ve vícefaktorové autentizaci** - Často se kombinují s jinými biometrickými metodami pro zvýšení bezpečnosti (např. rozpoznávání hlasu + heslo).
- ❑ Příklady
 - **Rozpoznávání hlasu:** Sleduje jedinečné vzorce hlasového projevu.
 - **Dynamika psaní na klávesnici:** Měří rychlost a rytmus při psaní.
 - **Způsob chůze:** Analyzuje vzorce pohybu a chůze.

❑ Dynamické vlastnosti (chování):

- Hlas / Řeč
- Gestikulace obličeje
- Podpis (dynamika)
- Dynamika stisku kláves
- Pohyby rtů
- Chůze
- *Zužování duhovky*



https://www.researchgate.net/figure/Iris-localization-Daugman-1994_fig2_305443076

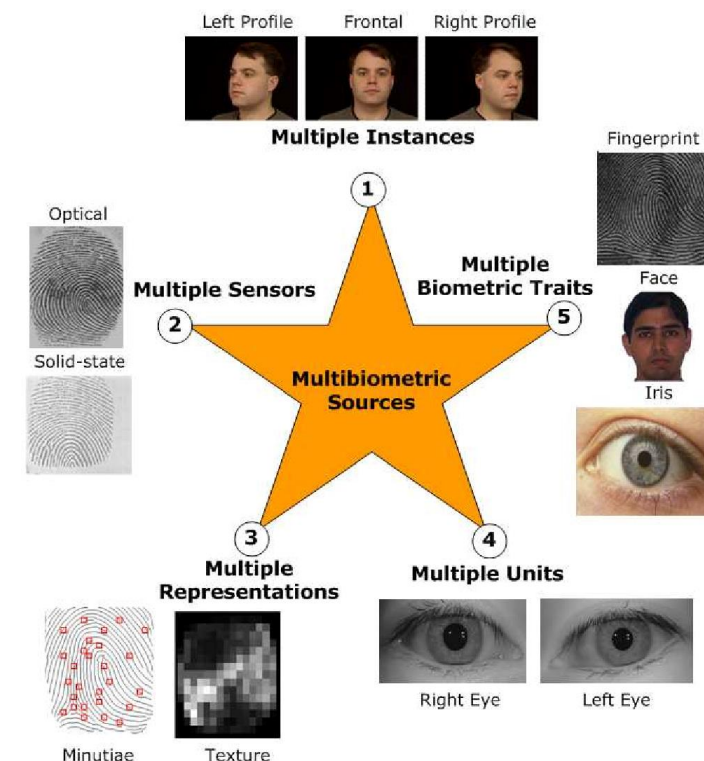
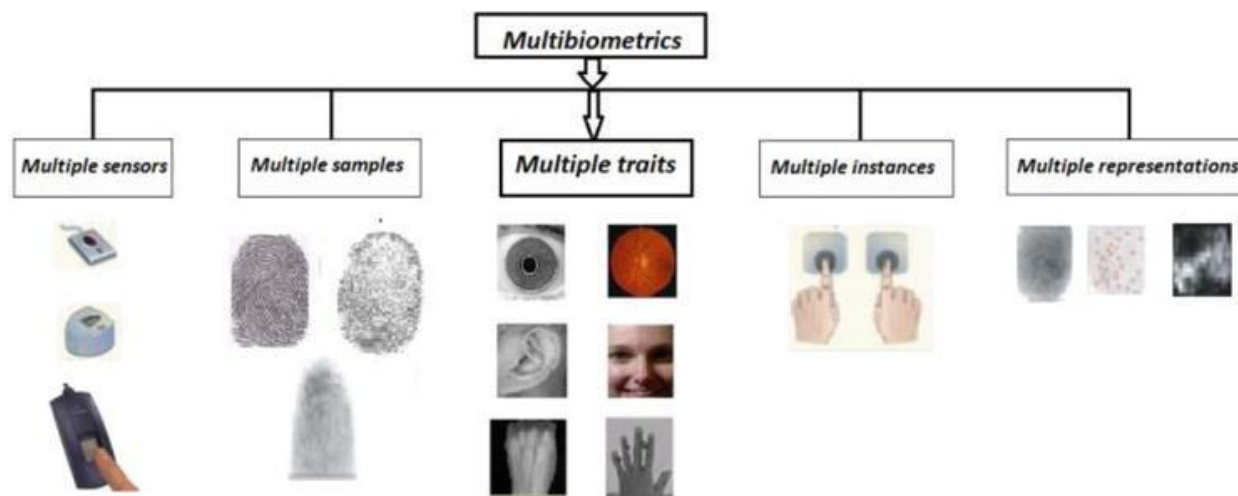
❑ Unimodální biometrický systém

- Používá pouze 1 biometrickou vlastnost
- Nižší spolehlivost

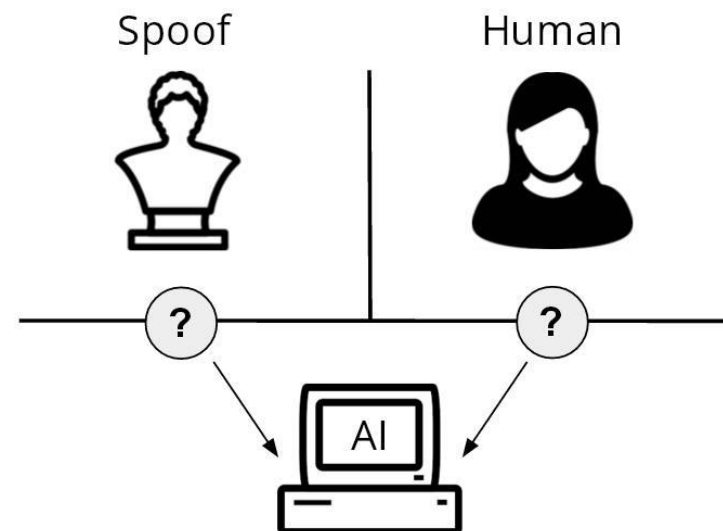


❑ Multimodální biometrický systém

- Použití buď více příznaků jedné vlastnosti
 - Příklad: Statické a dynamické vlastnosti podpisu
- Použití více biometrických vlastností
 - Příklad: Rozpoznávání obličeje v kombinaci s duhovkou
- Zvýšení spolehlivosti rozpoznání
- Více robustní vůči falšování a pokusům o útok
- Vyšší nároky na systém



- ❑ Proces, který ověřuje, zda biometrické údaje pocházejí od skutečné, živé osoby, nikoli z podvržených zdrojů (fotografie, video, 3D modely).
- ❑ Cíl - Zabránit útokům, které se snaží oklamat biometrické systémy pomocí neživých nebo falešných materiálů.
- ❑ Podobnost s Turingovým testem
 - Detekce živosti lze přirovnat k Turingovu testu v biometrických systémech – cíl je podobný, ověřit, zda interagujeme se skutečným člověkem (živou bytostí) a nikoli s podvrženým systémem (např. simulace nebo záznam).
- ❑ Typy detekce živosti
 - Pasivní
 - Aktivní
 - Hybridní



Forenzní	Vládní	Komerční
Identifikace mrtvol	Národní ID karty ATM	Bankomaty
Krim. vyšetřování	Řidičský průkaz Registrace voličů	Kontrola přístupu Počítačový login
Určení rodičovství	Sociální dávky	Mobilní telefony
Ztracené děti	Hraniční kontroly	e-Komerce Smart karty



<https://www.pathologyoutlines.com/image/forensicsidentificationNinivirtualmg7-1.png>



<http://www.airport-business.com/2020/11/contactless-biometrics-access-control-hygienic-frictionless-experience/>

- ❑ Univerzalita (*Universality*) – Popisuje, jak je dostupná biometrická charakteristika dostupná pro jednotlivé osoby.
- ❑ Jedinečnost (*Uniqueness*) - Jak dobře separuje jednotlivé osoby od sebe.
- ❑ Konstantnost (*Permanence*) – Vyjadřuje, jak je biometrická charakteristika stabilní v čase.
- ❑ Získatelnost (*Collectability*) - Jak je biometrická charakteristika snímatelná.
- ❑ Výkonnost (*Performance*) - Značí jak přesně, rychle a robustně lze nasnímat bio. charakteristiku.
- ❑ Akceptace (*Acceptability*) - Vyjadřuje míru ochotny lidí si nechat nasmínat bio. charakteristiku.

- ❑ Bezpečnost proti falšování (*Circumvention*) – Vyjadřuje, jak je složité oklamat biometrický systém.
- ❑ Finanční náklady na pořízení

- ❑ **Entropie** - míra nejistoty nebo rozmanitosti v biometrických údajích. > entropie -> vyšší bezpečnost

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Keystrokes	low	low	low	medium	low	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermogram	high	high	low	high	medium	high	high

❑ Další aspekty:

- Použitelnost
- Údržba
- Dostupnost
- Provedení
- Anonymita
- Distribuovatelnost

❑ Spolehlivost

- Osvětlení / Teplota
- Make-up
- Zranění / Operace
- Čepice / Brýle
- Sestřih / Vousy
- Stárnutí

Typy útoků:

„*Low-Force-Attack*“ -napodobení podpisu, hlasu

„*Brute-Force-Attack*“ -použití speciálních technik

- ❑ Spolehlivá a automatická identifikace / verifikace osob se stává nutností; Příklady: národní identifikační karty, hraniční kontrola, přístupové systémy, e-Shopping ...
- ❑ Neexistuje žádná náhrada za biometrii, ve smyslu spolehlivé identifikace / verifikace osob.
- ❑ Biometrické senzory jsou laciné a některé z nich jsou i velmi kompaktní (pro mobilní telefony a laptopy).
- ❑ Některé biometrické systémy nejsou úplně dostatečně přesné, spolehlivé nebo bezpečné pro některé využití.
- ❑ Je třeba testování biometrických systémů na rozsáhlých databázích.
- ❑ Biometrie může vylepšit ochranu našeho soukromí, ale jsou nutné vládní předpisy a směrnice.

❑ Nutný výzkum především v následujících oblastech:

- Nové reprezentace
- Porovnávací algoritmy
- Efektivní indexování v databázi
- Multimodální biometrické systémy
- Detekce živosti
- Ochrana šablon
- Vylepšení chybových hranic
- Nutné další investice a mnoho práce

Děkuji za pozornost!

Dotazy?

- ❑ Použité zdroje: Prezentace k 1. přednášce BIO (Martin Drahanský), další viz. poznámky