KEMT
Department of Electronics and Multimedia Telecommunications

Biometrické systémy bezpečnosti

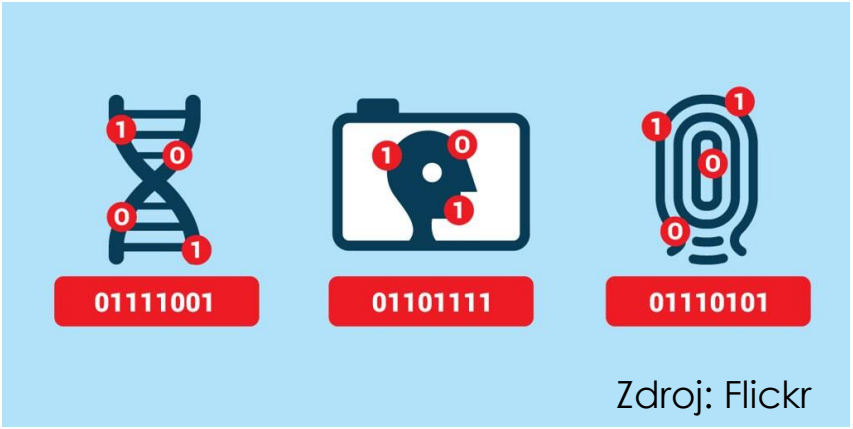
DOC. ING. MATÚŠ PLEVA, PHD.

Obsah

- *Zabezpečenie* komunikácie človek-stroj *s využitím biometrie*.
- Biometrická *identifikácia* a *verifikácia*.
- *Parametre* biometrických systémov.
- Prehľad skúmaných *fyziologických* biometrických znakov.
- Vybrané *behaviorálne* biometrické znaky a vývoj v tejto oblasti.
- Výskum v oblasti *multimodality* v biometrických systémoch.
- *Pokračovanie výskumu* v oblasti akustickej analýzy a multimodálnych technológií.

Definícia biometrie

- Slovo ***biometria*** pochádza z gréckych slov:
  - *biós - βιός – život,*
  - *metrikós - μετρικός – merací, meraný*.
- Biometria - meranie a analýza unikátnych *fyziologických* a *behaviorálnych* charakteristík *živých organizmov*.
- Pri *komunikácii človek-stroj sa zameriame na charakteristiky človeka - primárny používateľ* biometrického systému bezpečnosti.



Zdroj: Flickr

Aplikácie biometrických systémov

- bankové služby
- hraničné kontroly
- zdravotnícke elektronické služby
- platobné terminály/služby
- kontrola vstupu do objektu
  - firma, byt, garáž, telocvičňa, záujmový útvar, atď.
- letiskové bezpečnostné služby

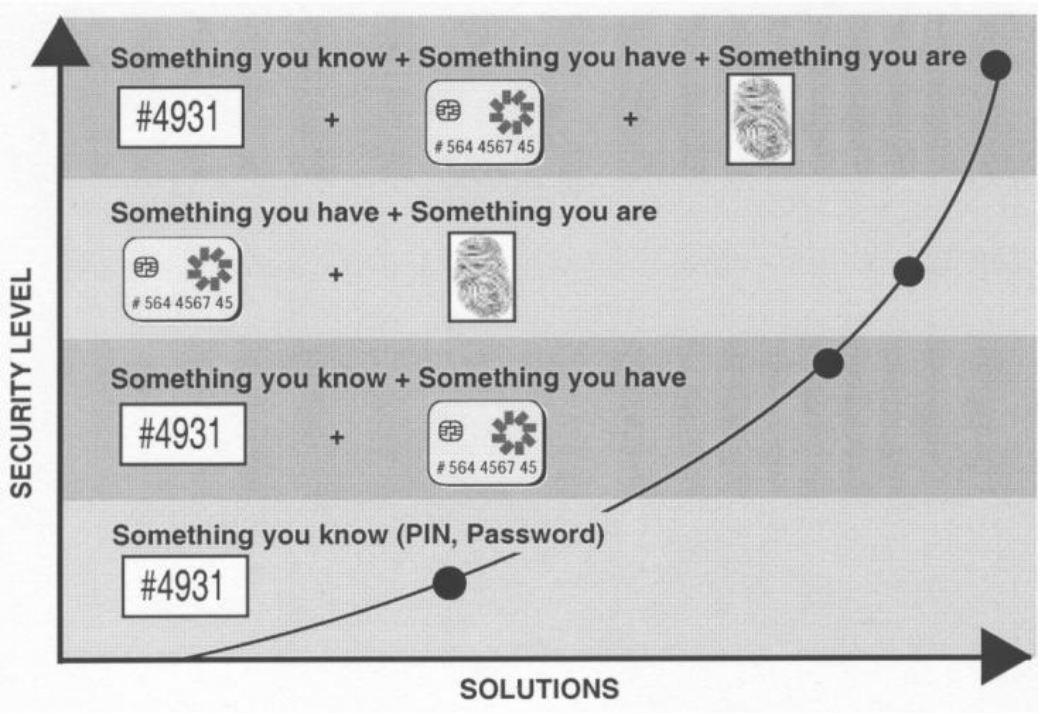
Zdroj: WikiCommons

Scarfo, P. Biometrics at the ATM (2017) Biometric Technology Today, 2017 (1), pp. 9-11. DOI: 10.1016/S0969-4765(17)30015-2

Aplikácie biometrických systémov

- forenzné systémy a kriminalistika
- lotériové terminály
- vernostné systémy
- systémy na dištančné vzdelávanie
  - a preskúšavanie/testovanie (či už vzdelávacie alebo certifikačné)
- mobilné telefóny a prístup k údajom v nich

Zvyšovanie zabezpečenia komunikácie človek-stroj



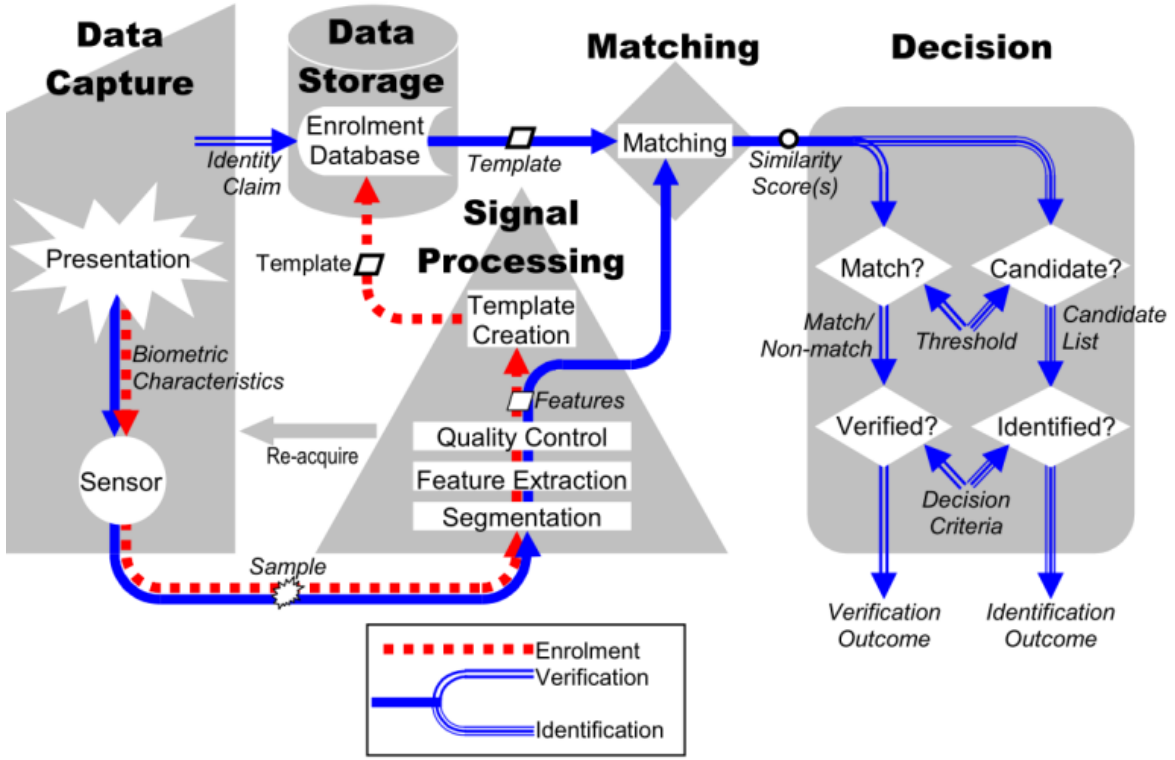
CSE 190 Topics in CSE: Introduction to Biometrics with Dr. David Kriegman

Ľudia sú identifikovaní na základe toho čo:

- **Majú** (ID karta, pas, rodný list, kľúče, platobná karta, atď.) - token,
- **Vedia** (heslo, PIN, meno, rodné číslo, atď.),
- **Sú** (biometrické fyziologické znaky ľudského tela alebo správania - behavior)

Základné pojmy

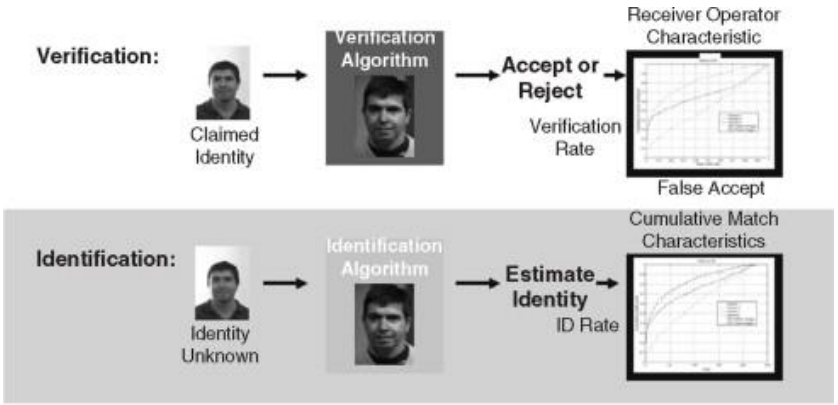
- ***Pravý***, oprávnený, známy používateľ - genuine
- ***Nepravý***, neoprávnený, neznámy používateľ, útočník, *podvodník* – impostor
- *Segmentácia, kontrola kvality, liveness detection*
- **Extrakcia *príznakov*** (features)
- **Výpočet/*trénovanie* modelu/vzoru** – (template creation)
- **Zaradenie do databázy (DB)** - enrollment, pridanie medzi pravých/známych/genuine
- **Porovnávanie** (matching) získaných znakov s jedným (***verifikácia***, 1:1) alebo viacerými (***identifikácia***, 1:N) modelmi/vzormi



ISO/IEC19794-1 Information technology—Biometric data interchange formats —Part 1: Framework

Autentifikácia vs Identifikácia

- **autentifikácia/verifikácia** - metóda *one2one* (1:1)
  - porovnanie *proklamovanej identity so zosnímanou osobou a jej biometrickými znakmi z databázy.*
  - *Výsledkom je binárne rozhodnutie **prijatie** alebo **zamietnutie** vstupu na základe **prahovej hodnoty** skóre/pravdepodobnosti*.
  - Hodnotí sa miera chybovosti a používa sa metrika FAR (False acceptance rate), FRR (False rejection rate), EER (Equal Error Rate).
  - *Rýchlejší* autentifikačný proces v rozsiahlych databázach.
- **Identifikácia** - *one2many* (1:N)
  - *Porovnávaním biometrických znakov používateľa so všetkými známymi modelmi/vzormi z databázy*.
  - Vyhodnocuje najpodobnejšiu identitu - presnosť (Accuracy).
  - Pomalší proces a nemusí vyhodnocovať autenticitu používateľa.



Wenyi Zhao, Rama Chellappa, *Face Processing*, Academic Press, 2006, Pages 547-575.

Vlastnosti biometrických systémov Biometrické znaky majú byť:

- **Univerzálne** (universality) - každý zdravý človek by mal daný znak mať,
- **Rozlíšiteľné**/unikátne (distinctiveness) - rozdiely v danom znaku medzi rôznymi osobami,
- **Trvalé**/stále (permanence) - znaky by sa nemali rýchlo meniť, pričom samozrejme úrazmi a starnutím dochádza k ich zmenám,
- **Snímateľné** (collectability) - znaky by malo byť možné relatívne jednoducho merať, snímať.

Zdroj: Flickr

Vlastnosti biometrických systémov Biometrický systém má mať dobrú:

- **Výkonnosť**/spoľahlivosť (performance) - či daný biometrický znak je relatívne rýchlo a jednoducho snímateľný, parametrizovateľný a porovnateľný s uloženou databázou s vysokou spoľahlivosťou.
- **Prijateľnosť**/akceptovateľnosť (acceptability) - ako je (alebo by mohol byť) daný systém akceptovaný/prijatý používateľmi, či daný biometrický znak nie je nepríjemné a zdĺhavé zosnímať, či sa budú pri používaní cítiť komfortne a podobne.
- **Neklamnosť**/nespochybniteľnosť (circumvention) - systém by mal byť ťažké oklamať, či spochybniť identitu, ktorú prijal za pravú/autentickú.
- **Bezpečnosť** – schopnosť systému odolať útoku na niektorú časť systému a prípadne zabrániť zneužitiu ukradnutých dát.

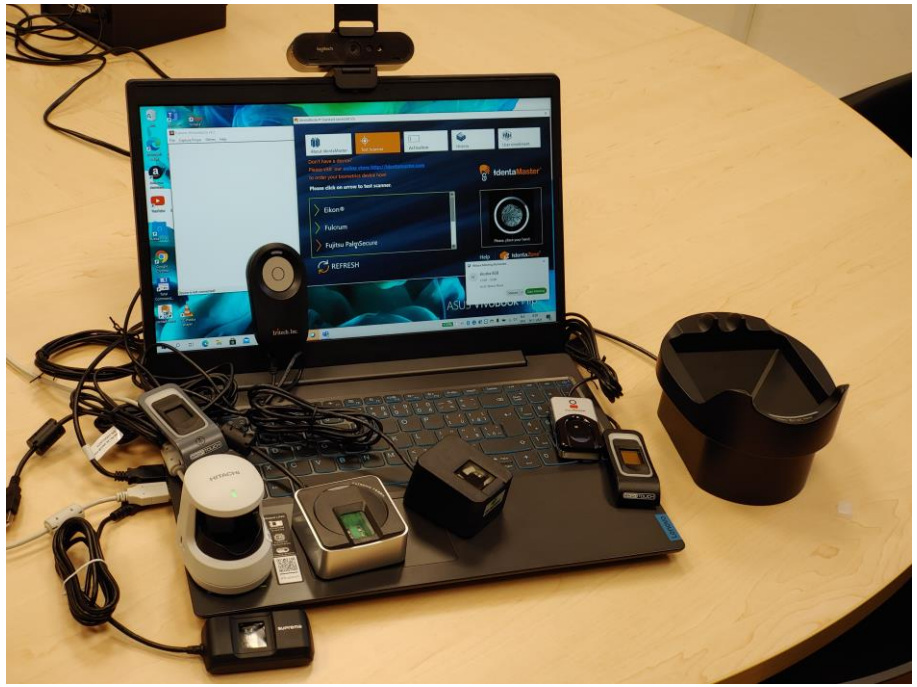
Zdroj: WikiCommons

Statická vs Kontinuálna autentifikácia

- ***Statická*** – overenie identity len pri vstupe do chráneného systému
- ***Kontinuálna*** – biometrická analýza beží počas celého času v chránenom systéme a keď pravdepodobnosť že nejde o pravého/genuine používateľa narastie nad určitý prah je vyzvaný na jednorázové dodatočné overenie identity. Môže byť sledovaná tvár, hlas, pohyby myšou, dynamika písania na klávesnici a iné.

Fyziologické/anatomické biometrické znaky

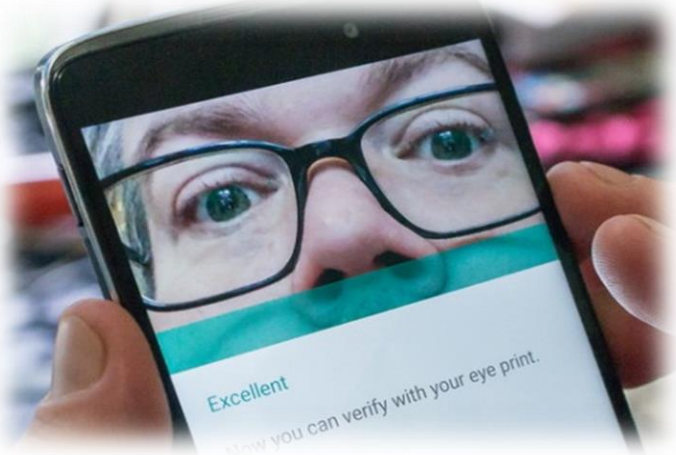
- **Tvár** – optický snímok (2D/3D) ale aj termálne emisie,
- **Oko**, dúhovka (iris), očné pozadie (rohovka - retina), žilky na oku,
- ***Tvar*** ucha, nosa, prstov, nohy, odltačok zubov, fotka širokého úsmevu, RTG zubov,
- ***Odtlačok prsta*** *(Fingerprints) a* ***odtlačok dlane*** *(Palmprints) – štruktúra kože na prstoch, dlani, nohe (deti) – senzor existuje optický, kapacitný, ultrazvukový, tlakový, termálny, laserový, atď.,*
- Štruktúra **krvného riečišťa** *dlane, prsta, zápästia - Palm/Finger/Wrist vein,*
- Geometria/tvar ruky - *Hand geometry,*
- *Telesný pach či vôňa, bakteriálny odtlačok - body odor,*
- ***DNA, ...***
  - zmena parametrov starnutím - vek, výška, hlas, hmotnosť, veľkosť chodidla, špeciálne znaky (tetovania, jazvy, atď.)



Fotka z ***laboratória KEMT*** na výuku biometrických systémov, financované z ***KEGA 009TUKE-4/2019*** *Zodp. riešiteľ:* ***Pleva***

Dostupnosť biometrických senzorov

- *Facial* & thermal emissions – camera (built-in) & thermo camera (expensive)
- *Eye* features as *iris* or *retina* – cell phone built in camera
- *Fingerprints & Palmprints – external sensors for higher EER (Equal Error Rate) – not accurate built in portable scanners,* (price for sensor on the picture ~$130)

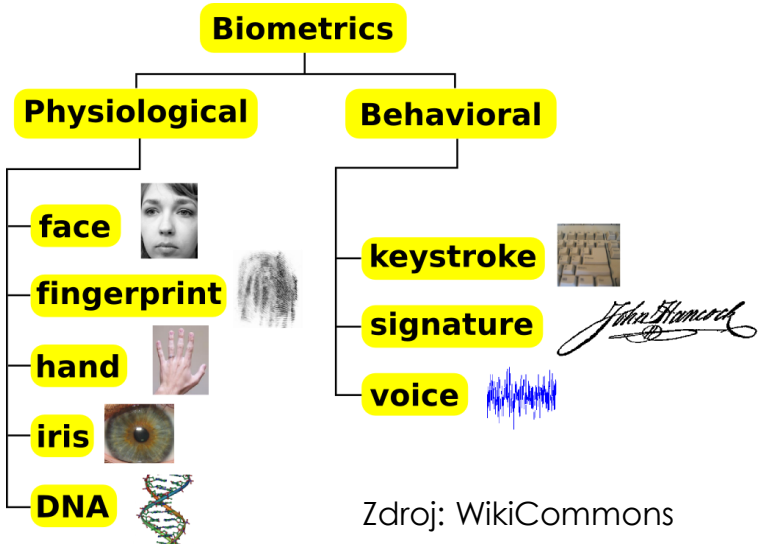


Dostupnosť biometrických senzorov

- *Palm vein* - the composition of vein in the palm of the right hand is a very accurate biometric feature (price ~ $400)
- *Hand geometry* - the geometry of the hand and fingers is the most widespread way of simple authentication when checking entry to exclusive areas, usually after entering your access code (~$2,000)
- *Skin pores & wrist/hand veins* - these new technologies are just in development and the sensors are not off-the-shelf

Behaviorálne biometrické znaky
Parametre správania

- Vlastnoručný ***podpis*** (statický, dynamický, dyn. + tlak),
- ***Hlasový*** *odtlačok – Voiceprint,*
- **Chôdza** – *Gait,*
- *Gestá,* ***pohyby pier,***
- ***Klávesová*** *dynamika - Keystroke dynamics,*
- ***Pohyby myšou,***
- ***Pohyby očí****, Pupilárny/zrenicový reflex na svetlo,*
- ***EKG*** *(el. sig. srdca), HR (heart rate - tep),* ***EEG*** *(el. mozgová aktivita),* ***EMG*** *(el. svalová aktivita),*
- ***Spôsob používania*** *mobilného telefónu: touch,* accelerometer, gyroscope, magnetometer, proximity, ambient lighting, gravity, pressure sensor, location, user activity, call data, SMS, app usage, browser history, phone status, secondary camera, stylometry (txt analysis) (*Eglitis, T., Guest, R. and Deravi, F., 2020. Data Behind Mobile Behavioural Biometrics–a Survey. IET Biometrics*.)



Zdroj: WikiCommons

Statická vs kontinuálna autentifikácia

- ***Statická*** – jednorazové overenie identity pri vstupe do chráneného systému.
- ***Kontinuálna*** – biometrická *analýza beží počas celého času* v zabezpečenom systéme, ak pravdepodobnosť že nejde o pravého/genuine používateľa narastie nad určitý prah je vyzvaný na jednorazové *dodatočné* overenie identity. Môže byť sledovaná tvár, hlas, pohyby myšou, dynamika písania na klávesnici a iné.

Chybovosť biometrických systémov – pri verifikácii ide o binárnu klasifikáciu

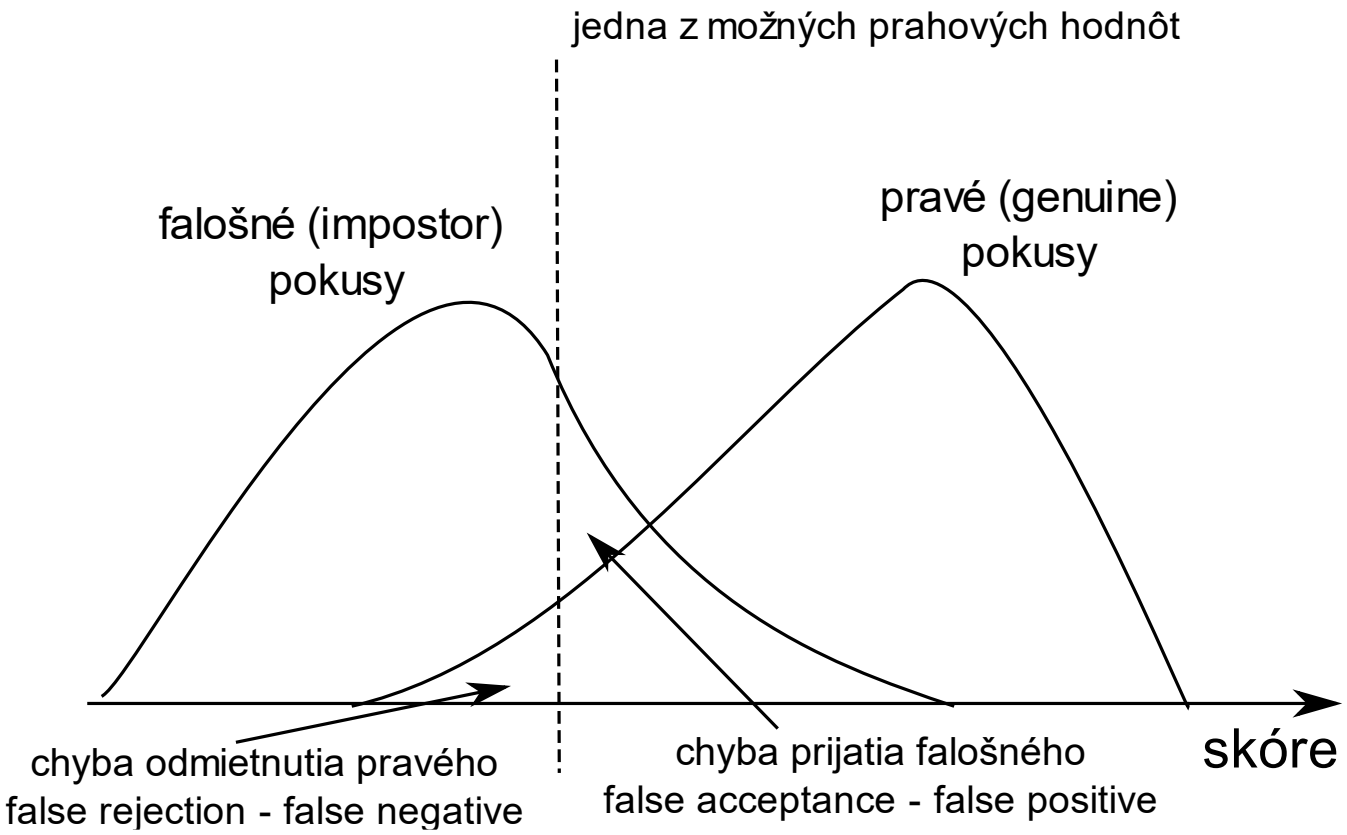
Prístup pre:	známeho (genuine)	cudzieho (impostor)
povolený (accept)	*True* Positive (TP/TA)	**False** Positive (FP/FA)
zamietnutý (reject)	**False** Negative (FN/FR)	*True* Negative (TN/TR)

Confusion matrix
Konfúzna matica

False rejection rate (**FRR**)
alebo False alarm probability
FN: Nesprávne zamietnutie oprávnenej osoby
Pomer nesprávne zamietnutých:
FRR = *FN/(TP+FN)*

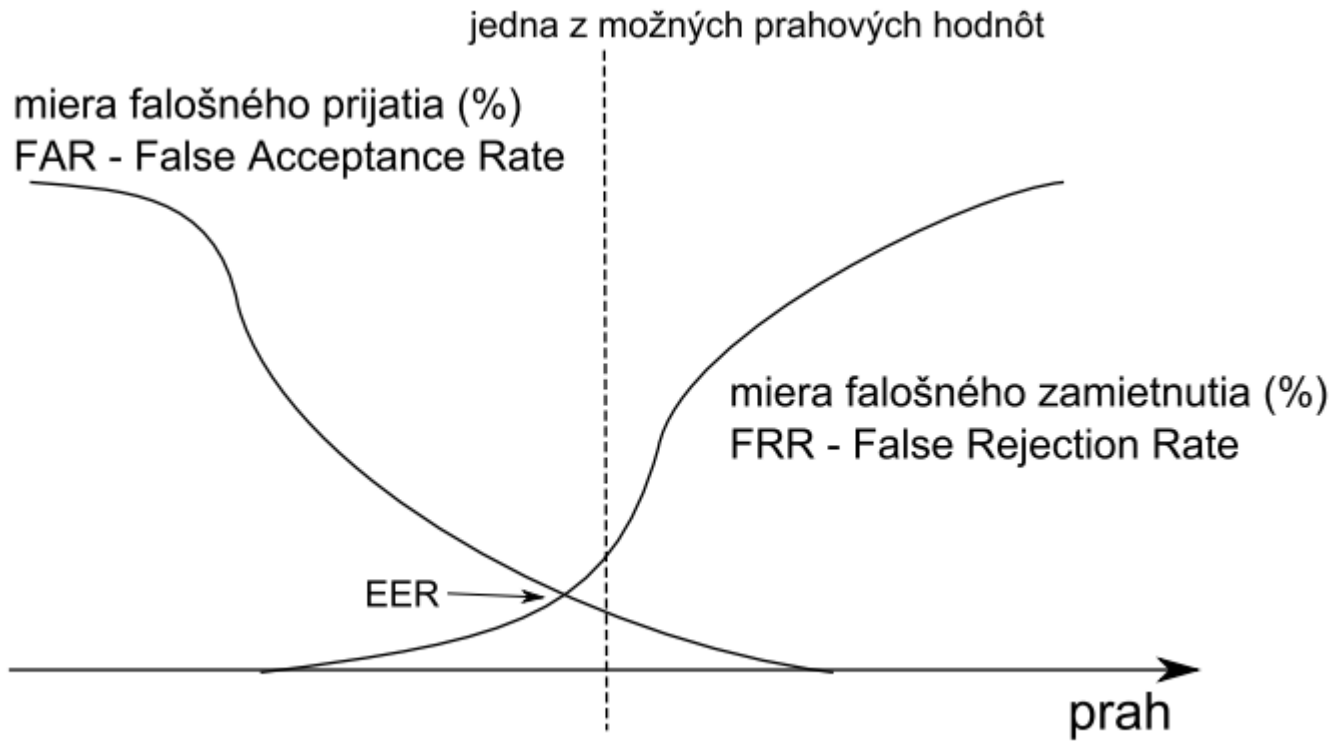
False acceptance rate (**FAR**)
alebo Miss probability
FP: Falošné prijatie/vpustenie
Pomer falošne prijatých:
FAR = *FP/(FP+TN)*

Histogram výskytu skóre pri verifikácii



EER

Aby sme dokázali porovnať rôzne autentifikačné systémy (1:1), bez ohľadu na to na akú bezpečnosť/prah je systém pri akceptácii identity nastavený, bol zvolený parameter EER (Equal Error Rate) teda percento chybovosti systému v bode kedy FRR a FAR sú zhodné, či inak povedané chybovosť systému v bode kedy pravdepodobnosť vpustenia falošného (impostor) používateľa - podvodníka je rovnaká ako pravdepodobnosť nevpustenia používateľa s pravou identitou (genuine). Samozrejme systém pri svojom chode môže mať inak nastavenú prahovú hodnotu a neznamená to že pri systéme s EER 5% má používateľ automaticky očakávať že ho systém s 5% pravdepodobnosťou nevpustí. Administrátor môže prah na akceptovanie identity nastaviť tak, že pravdepodobnosť nevpustenia bude len 1% ale samozrejme pravdepodobnosť vpustenia cudzej/nepravej identity sa zvýši na povedzme 8 či 15%.


jedna z možných prahových hodnôt
miera falošného prijatia (%)
FAR - False Acceptance Rate
miera falošného zamietnutia (%)
FRR - False Rejection Rate
EER
prah

- **FAR** (False acceptance rate) - percento falošne prijatých identít (do systému bol vpustený používateľ s falošnou identitou - impostor/podvodník), niekedy sa označuje aj ako False Match Rate - FMR či False Positive Rate - FPR (pozri obrázok 2.1).

- **FRR** (False rejection rate) - percento nesprávne zamietnutých identít (používateľovi s pravou identitou (genuine) bol prístup zamietnutý), niekedy sa označuje aj ako False Non-Match Rate - FNMR či False Negative Rate - FNR.

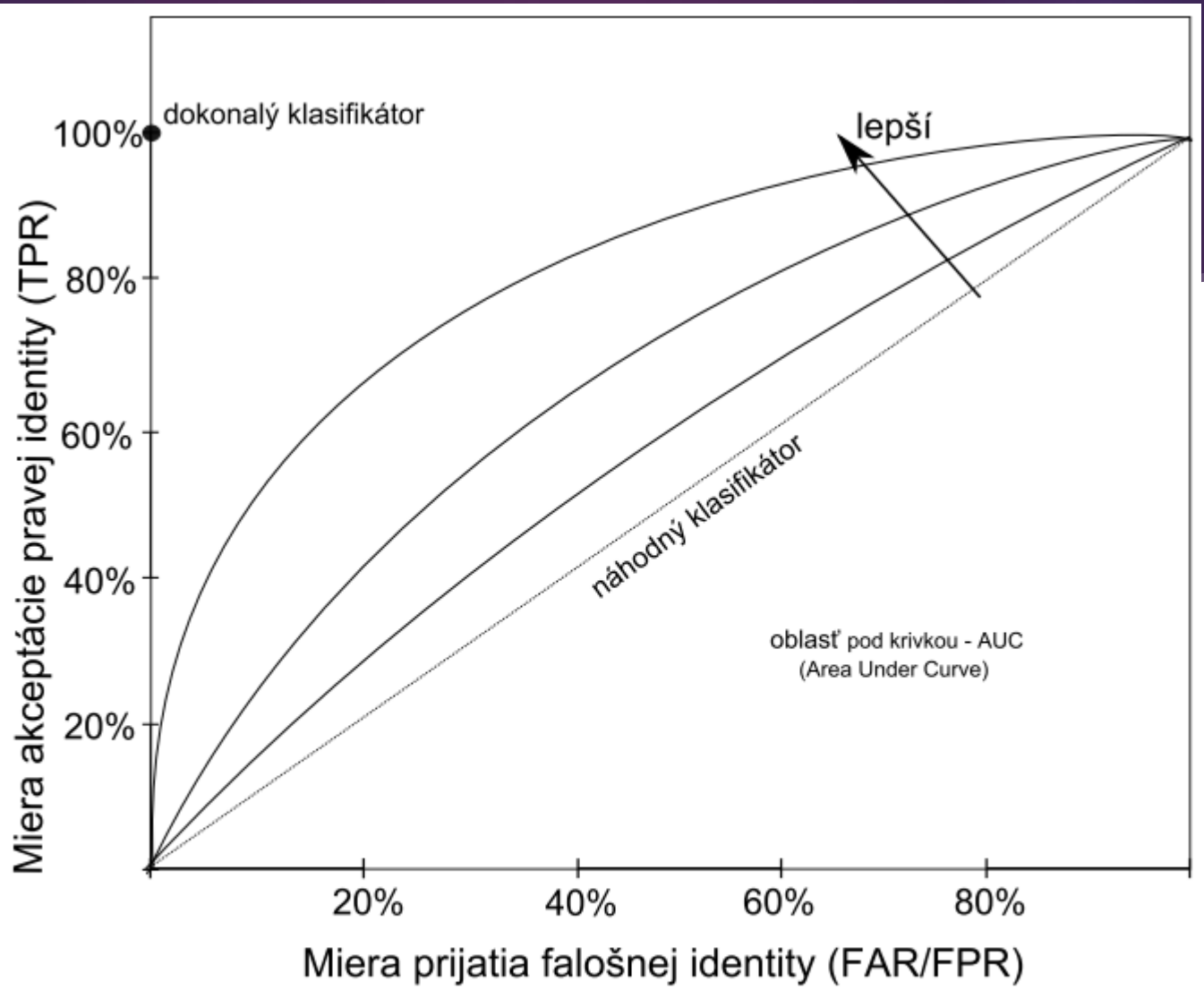
- FTD (Failure to Detect) + FTC (Failure to Capture) [6] - percento chybovosti pri snahe detegovať (FTD) biometrický objekt (napríklad tvár, prst a podobne) alebo spracovať zo získanej snímky/záznamu (sample) vhodné parametre (FTC) kvôli jej zlej kvalite, expozícii, šumu, špine a podobne.

- FTP (Failure to Process) + FTE (Failure to Enroll rate) - percento chybovosti pri zaradení do databázy - môže byť problém so získaním dát zo senzora (FTC), alebo je napríklad daný biometrický znak pri zosnímaní poškodený (môže byť aj špinou na prstoch, zakrytou tvárou, atď.), alebo nie je dostatok vzoriek na zaradenie do databázy (FTP), väčšinou na zvýšenie presnosti systému požadujeme niekoľko úspešne získaných a kvalitných vzoriek.

- FTA (Failure to Acquire rate) - percento chybovosti prí získaní dát v procese verifikácii/identifikácie - opäť môže ísť o problém pri získavaní dát (senzor, biometrický znak, kvalita, atď.) prípadne systémová chyba algoritmu či modelu v databáze získaného napríklad v iných podmienkach (svetelných, akustických, vlhkosť, hmla, atď.).

ROC

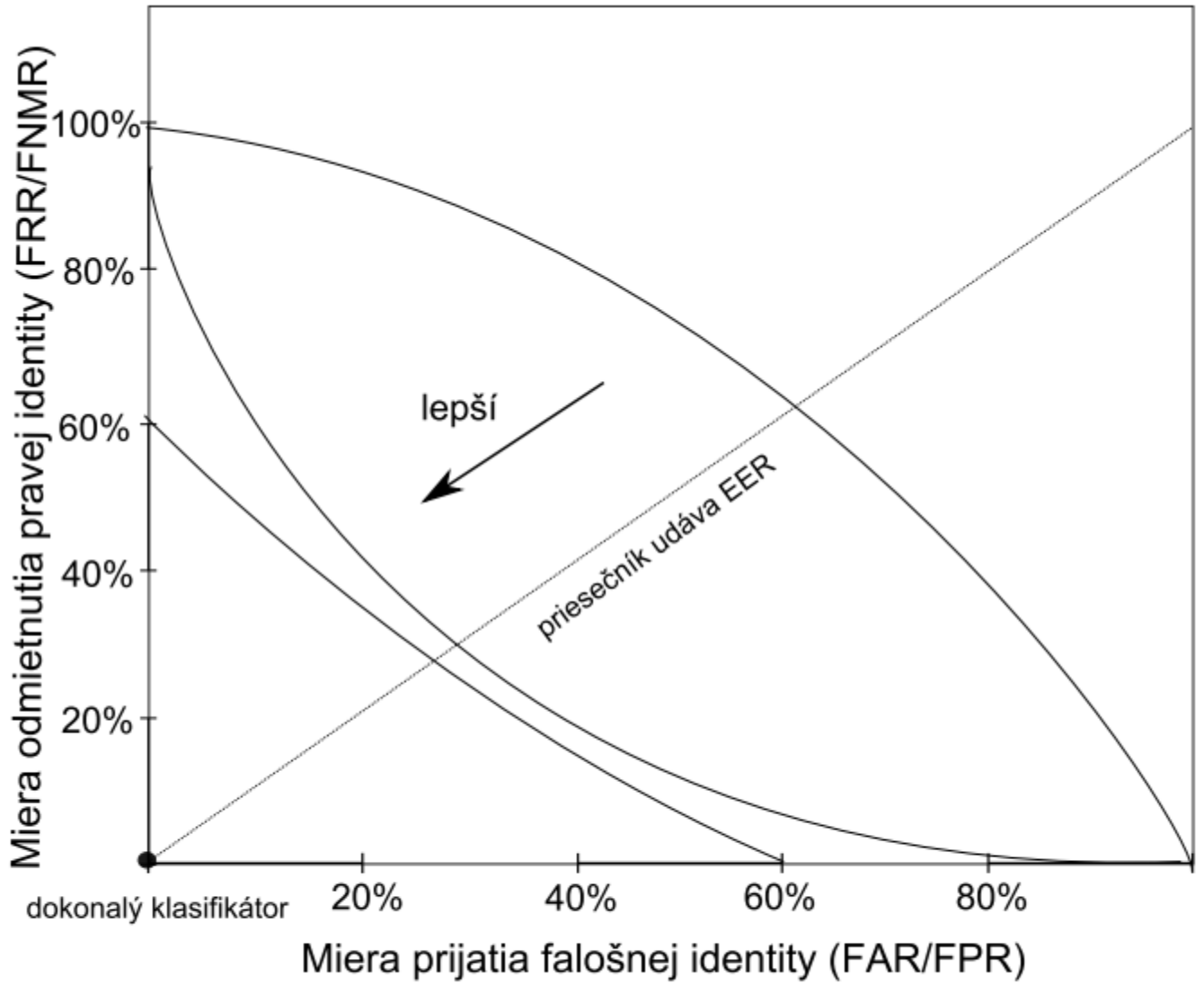
- receiver operating characteristic curve



Obr. 2.3 ROC krivka - operačná charakteristika binárneho klasifikátora

DET

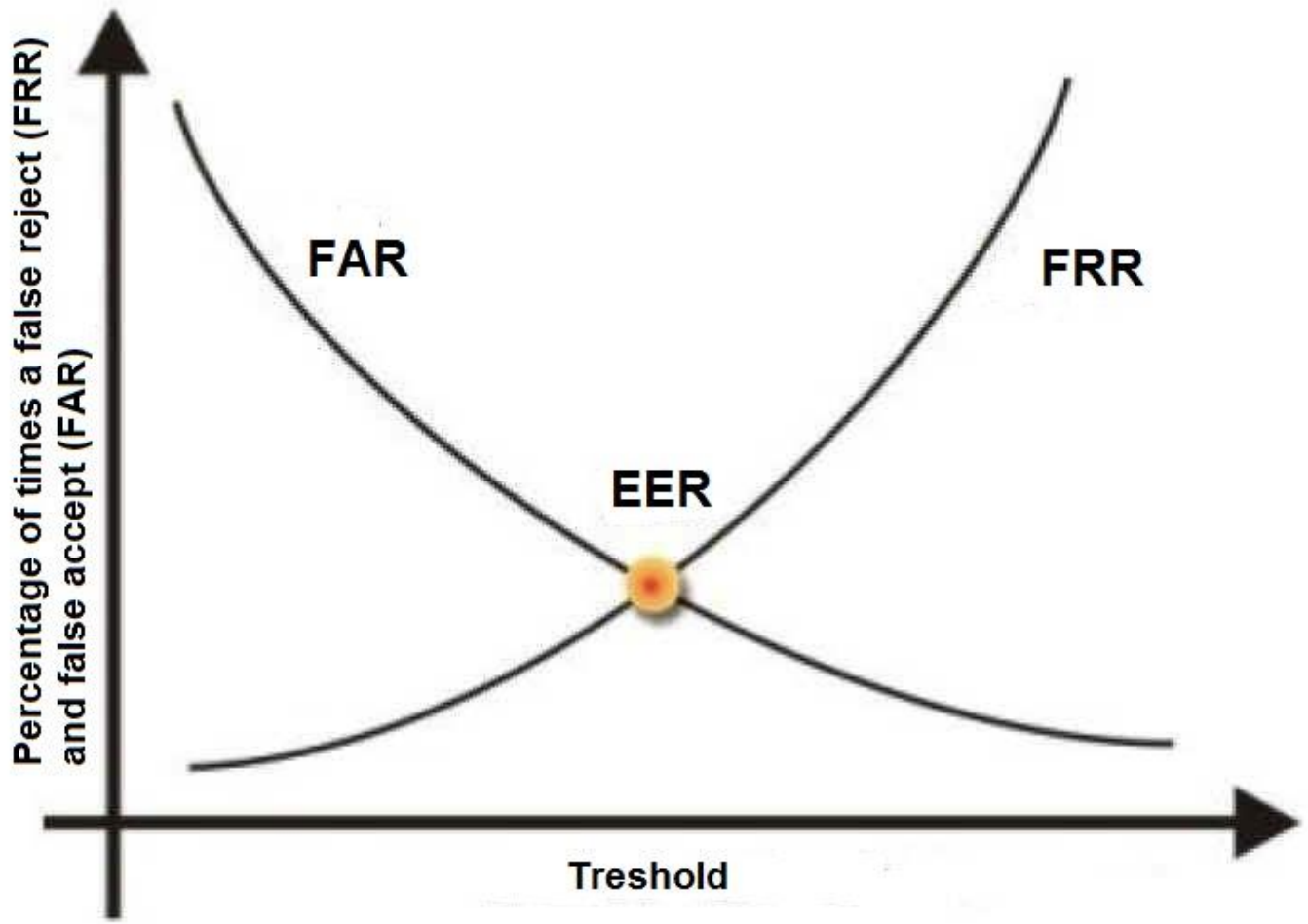
- **Detection error tradeoff**



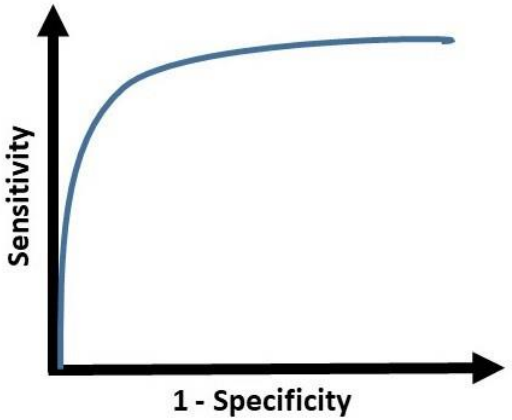
Obr. 2.4 DET krivka - kompromis detekčnej chyby

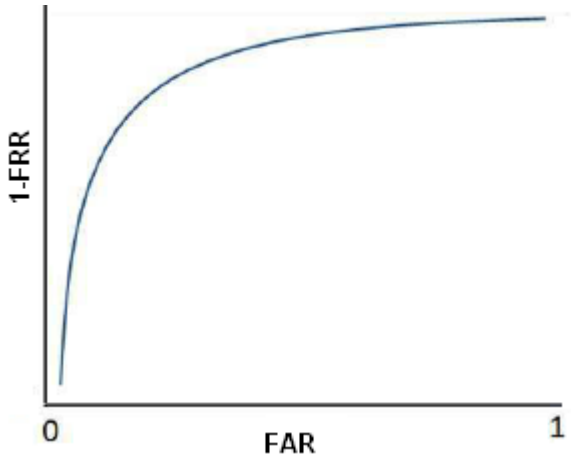
Error rates in biometric systems

- For authentication purposes: FRR, FAR, EER
  - False rejection & False acceptance rate depends on threshold, so for threshold when FAR=FRR the error rate is called Equal Error Rate
- For identification purposes: Accuracy = percentage of correctly recognized person

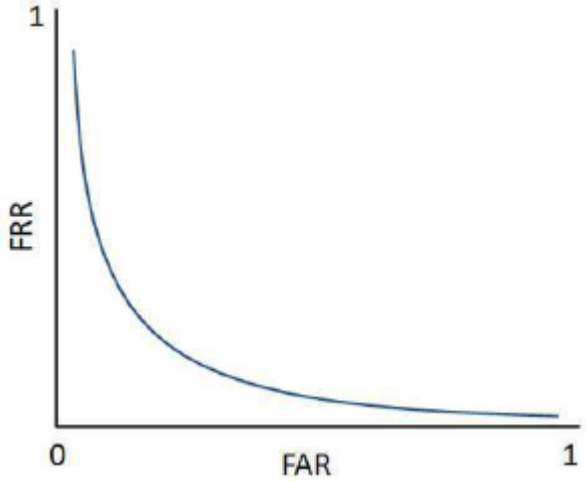


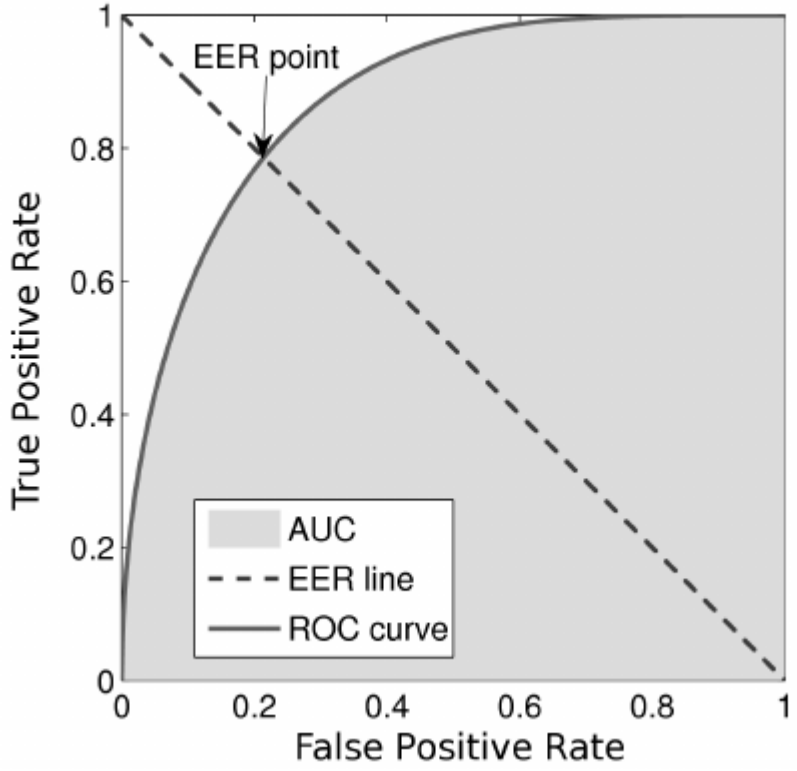
Error rates in biometric systems

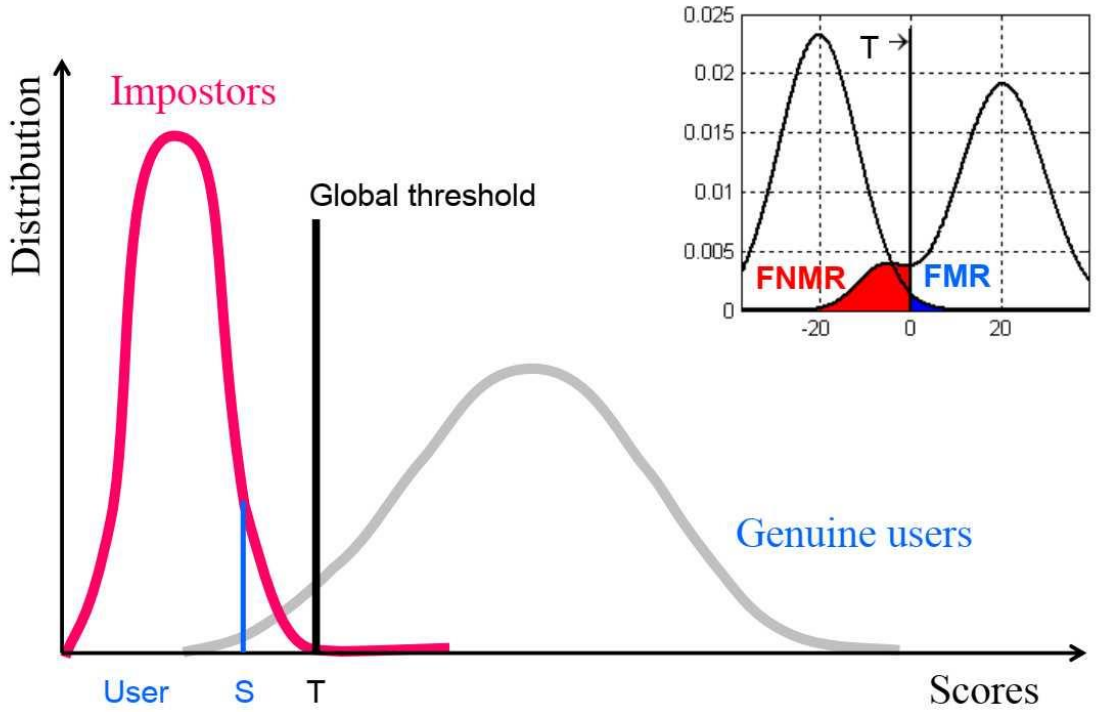




- Receiver operating characteristics (ROC) curves provide critical performance insights for the evaluation of an authentication algorithm.







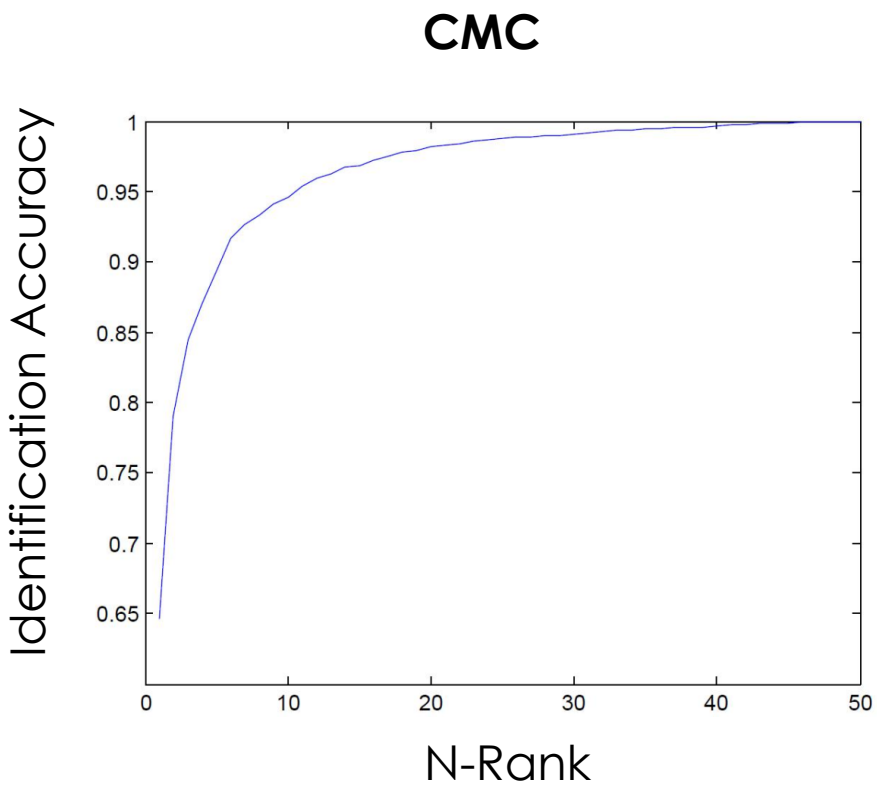
Daniel Novák: Biometrics. Introduction.
Slides from
https://cw.fel.cvut.cz/b191/courses/a6m33bio/start

Miery pri identifikácii

Cumulative Match Characteristic

Kumulatívna krivka zhody

- N-Rank – pravdepodobnosť že sa daná osoba bude nachádzať v liste TOP N nájdených uložených vzorov z DB
- closed-set identification

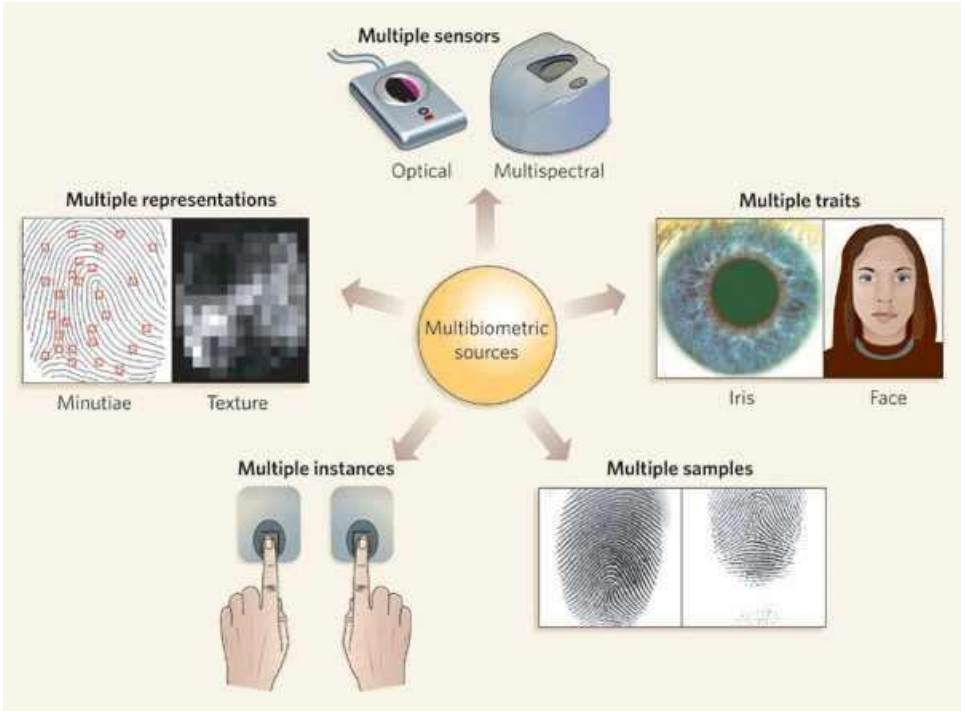


Multimodalita v interakcii človek stroj

- Multimodalita – vstup alebo výstup je prezentovaný viacerými komunikačnými kanálmi
- Podľa symetrickosti
  - **Symetrická** = rovnaké modality na vstupe aj výstupe. Napr. reč a gestá
  - **Asymetrická** = iné typy/počet modalít na vstupe a na výstupe
- Podľa typu multimodálnosti
  - **Alternatívna** – možnosť použiť jednu z možných modalít, napr. buď reč alebo písanie textu
  - **Sekvenčná** – jednotlivé modality nasledujú po sebe, nie súčasne. Napr. kombinácia dotykového displeja a hlasových povelov v aute
  - **Simultánna** – jednotlivé modality je možné použiť súčasne. Napr. súčasný vstup pomocou hlasu a gest.

Výskum v oblasti multimodality v biometrických systémoch

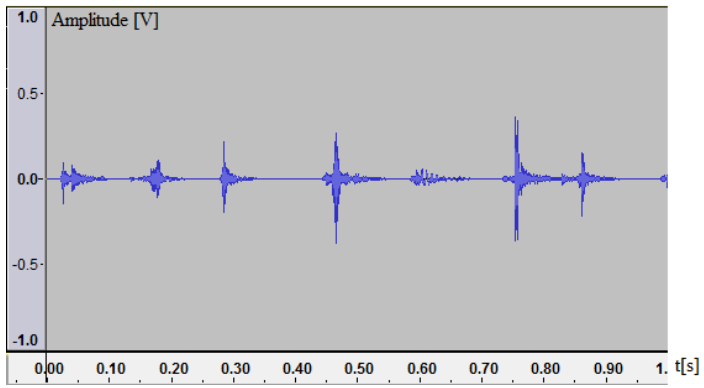
- Biometrický systém môže využívať **viacero modalít**:
  - Senzorov
  - Čŕt (napr. oko, tvár)
  - Vzoriek
  - Jednotiek (napr. pravé a ľavé oko, viac prstov, ...)
  - Reprezentácií
  - Algoritmov
- **Fúzia modalít** môže byť na rôznych úrovniach:
  - *Pred klasifikáciou (senzory, príznaky, ...)*
  - *Po klasifikácii (dynamická voľba klasifikátora, fúzia skóre, ...)*
- *Pri biometrickom systéme môže byť obťažujúce pre používateľa ak potrebuje viac interakcií pri prístupe.*



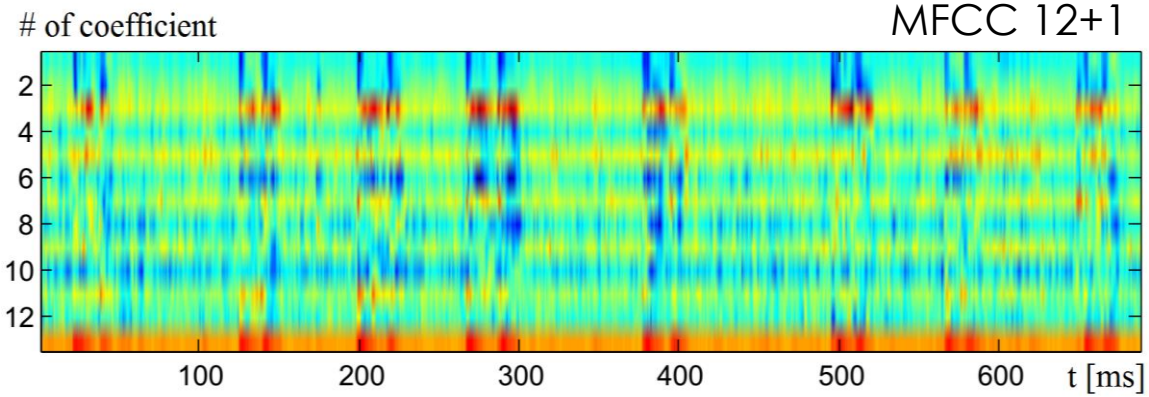
Anil K Jain. Biometric recognition. Nature, 449 (7158) : 38–40, 2007.

Výskum v oblasti multimodality klávesovej dynamiky

- Klávesová dynamika, resp. dynamika stláčania kláves na klávesnici počas písania frázy alebo voľného textu - *keystroke dynamics*.
- Na základe oslovenia výskumníkov (P. Bours) z NTUT NISLab (Norwegian Information Security Laboratory) Gjøvik sme začali analýzu nahrávok DB:
  - DB sa nahrávala v 4 sedeniach (sessions) po 25 napísaní frázy „password“,
  - 40 mužov a 10 žien, zaznamenané boli pohyby kláves a audiovizuálny záznam.



MFCC 12+1



TUKE Speech Lab and NISLab joint research in Keystroke Dynamics / Matúš Pleva, Patrick Bours - 2016. In: IWBF 2016. – Limassol, Cyprus

Výskum v oblasti multimodality klávesovej dynamiky

- **Časová analýza** z údajov ovládača klávesnice.
- Scaled Manhattan Distance (SMD) z 8 trvaní stlačenia klávesy a 7 latencií - to jest 15 hodnôt template T (t_i).
  - kde μ_i a σ_i sú ich stredné hodnoty a štandardné odchýlky

$$d(T,t) = \sum_{i=0}^{15} \frac{|\mu_i - t_i|}{\sigma_i}$$

- Získaná Equal Error Rate (EER) pri úlohe *verifikácie* bola **12,8%** pri jednej trénovacej a 3 testovacích sessions, čo kleslo na 9,91% keď sa použili 3 sessions na natrénovanie template a 1 sessions na testovanie.
- V úlohe *identifikácie* bola časová analýza horšia, presnosť **56,7%** pri jednej trénovacej session resp. 64,6% pri troch v porovnaní s akustickou analýzou ***90,62%*** *a* 97,03%.

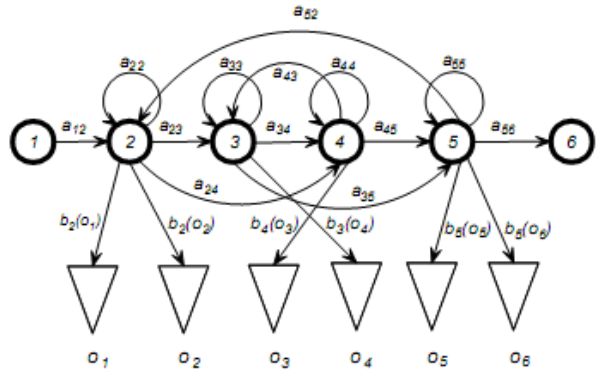
Static audio keystroke dynamics / Patrick Bours, Eva Kiktová, Matúš Pleva - 2015. In: Communications in Computer and Information Science : Multimedia Communications, Services and Security. Vol. 566 (2015), p. 159-169.

BEST PAPER of the conference MCSS 2015, Krakow

Výskum v oblasti multimodality klávesovej dynamiky

- **Zvuková (audio) analýza** – extrakcia rôznych typov *príznakov*, nakoniec najlepšie výsledky dávali MFCC (Mel-kepstrálne frekvenčné koeficienty) 39 koef. (25ms Ham. okno, 10ms krok).
- Na *vyhodnotenie* pravdepodobnosti bol použitý HMM (Skryté Markovove modely) kde najlepšie výsledky dával plne ergodický 3 stavový model.
- **Identifikácia**: najlepší 256 zmesový model trénovaný na 75 % náhodne zvolených nahrávkach dosiahol **99,33%** presnosť, pri použití *1* trénovacej session dosiahol systém *90,62%* presnosť (cross-validated) a pri použití *3 session* ***97,03%***. Zaujímavosťou je, že ak sa posledná session použila ako jediná na tréning tak systém dosiahol presnosť len 88,93 %.

$$Mel=2595*\log_{10}(1+Hz/700)$$



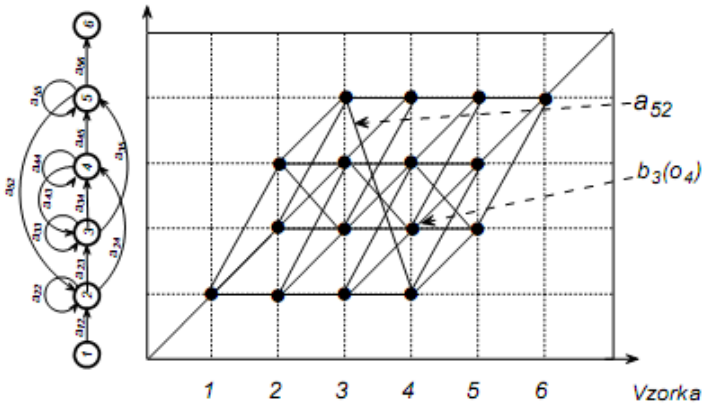
Acoustical user identification based on MFCC analysis of keystrokes / Matúš Pleva ... [et al.] - 2015. In: Advances in Electrical and Electronic Engineering. Vol. 13, no. 4 (2015), p. 309-313. - ISSN 1336-1376
Efficient acoustic detector of gunshots and glass breaking / Martin Lojka ... [et al.] - 2016. In: Multimedia Tools and Applications. Vol. 75, no. 17 (2016), p. 10441-10469.

Výskum v oblasti multimodality klávesovej dynamiky

- **Zvuková (audio) analýza** – MFCC (Mel-kepstrálne frekvenčné koeficienty) 39 koef., HMM (Skryté Markovove modely) 256 mix ergodický 3 stavový model.
- **Verifikácia**: výsledky boli *horšie ako pri časovej analýze* a tak bol navrhnutý *inovačný kalibračný proces* vyčlenením 1 užívateľa (1 z 50).

$$Log(prob_{calibrated}) = \frac{Log(prob_{actual})}{Log(prob_{calibration\_user})} \times 50$$

# of test sessions	EER [%] audio calibrated	EER [%] no calibration
3 (1 train sess.)	**14.34**	21.1
1 (3 train sess.)	**8.99**	19.1

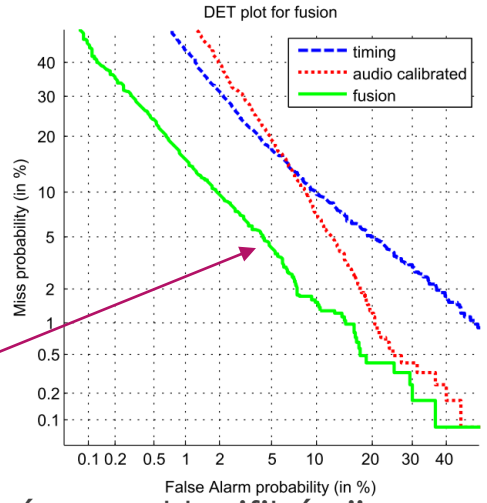


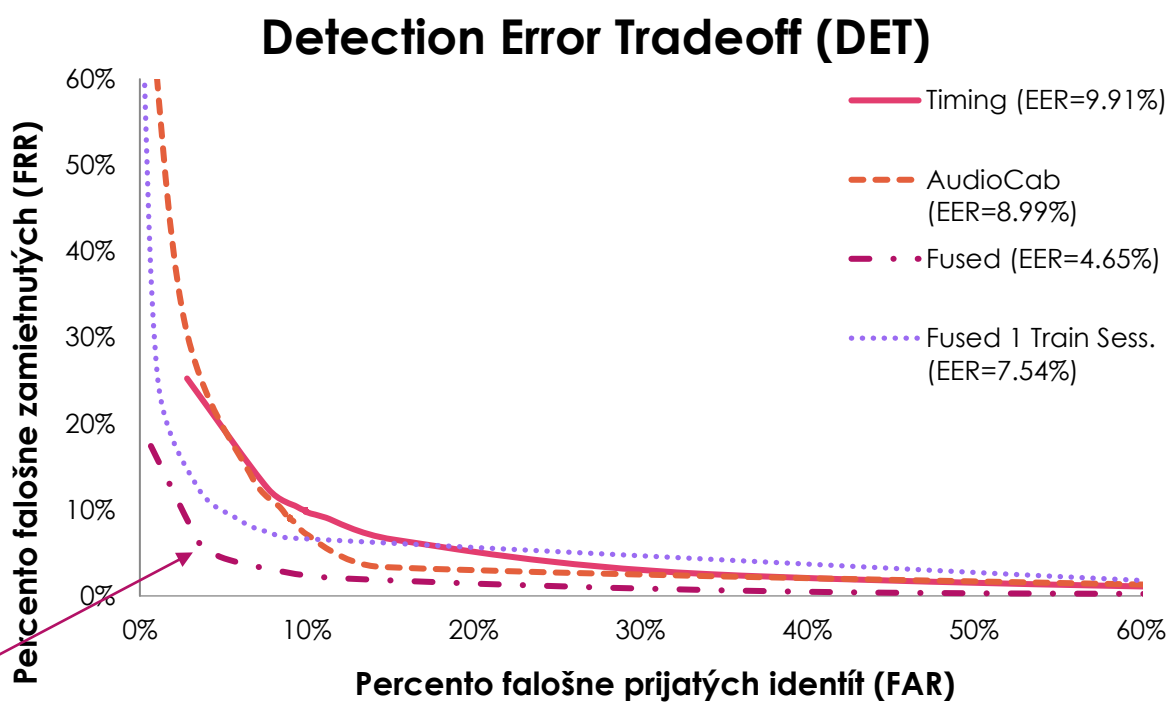
ergodický model

Acoustical keystroke analysis for user identification and authentication / Matus Pleva ... [et al.] - 2016. In: Radioelektronika 2016. - Danvers : IEEE, 2016 p. 386-389.

Výskum v oblasti multimodality klávesovej dynamiky

- **Fúzia časovej a audio analýzy** pre potreby *verifikácie* používateľa.
- Vhodná voľba algoritmu fúzie a porovnanie fúzovacieho algoritmu so široko uznávaným **Bosaris** toolkitom (fúzované *EER 4,71%* pri 3 trénovacích session, *7,3%* pri jednej).
- Použitý alg. lineárnej fúzie skóre po klasifikácii s hľadaním váhovacích parametrov fúzie na DEV DB a evaluáciou na EVA DB, potom sme množiny vymenili a vykreslený je priemerný dosiahnutý EER kde sme dosiahli ***4,65%*** *a* ***7,54%.***





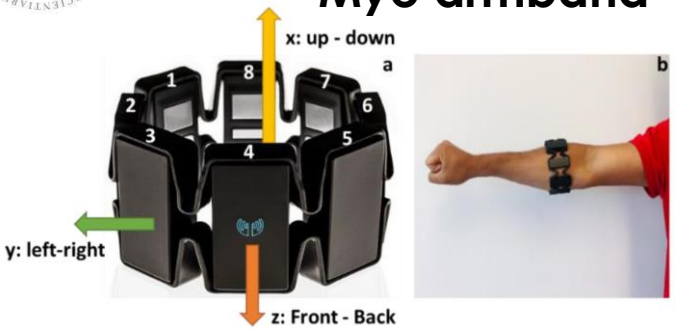
Improving static audio keystroke analysis by score fusion of acoustic and timing data / Matúš Pleva ... [et al.] - 2017. In: Multimedia Tools and Applications. Vol. 76, no. 24 (2017), p. 25749-25766.
Using Current Biometrics Technologies for Authentication in E-learning Assessment / Matúš Pleva ... [et al.] - 2016. In: ICETA 2016. - Danvers : IEEE, 2016 p. 269-274.

Pokračujúci výskum v oblasti akustickej analýzy a multimodality v biometrii

- V spolupráci s ÚI SAV nový projekt VEGA 2/0165/21 Technológie automatického spracovania reči na pomoc v krízových situáciách, zástupca zodpovedného riešiteľa z rezortu školstva – *analýza reči, kašľa a emócií v telefónnej komunikácii a hľadanie príznakov respiračných ochorení.*
- Bola v spolupráci s katedrou KPI TUKE navrhnutá *inovatívna mutlimodálna DB* s využitím EMG Myo náramkov na sledovanie svalovej aktivity pri písaní na klávesnici, vytvorená aplikácia na súčasný zber dát (časy z klávesnice, 2xMyo EMG/IMU, zvuk, video) - spoločný článok na medzinárodnú IEEE konferenciu CogInfoCom 2021 a nórsku konferenciu NISK 2021.
- V rámci pokračovania spolupráce s NTUT Gjøvik bol Patrick Bours *pozvaný ako zahraničný expert* projektu INDIGO Inteligentné dátové infraštruktúry pre digitálnu spoločnosť ITMS: 313011T571, pozvaný ako plenárny rečník IEEE konferencie Radioelektronika 2022 organizovanej TUKE.

https://developerblog.myo.com/

Myo armband



Bangaru, S.S.; Wang, C.; Aghazadeh, F. Data Quality and Reliability Assessment of Wearable EMG and IMU Sensor for Construction Activity Recognition. *Sensors* **2020**, *20*, 5264. https://doi.org/10.3390/s20185264

NTNU CCIS
Center for Cyber and Information Security

Ďakujem za pozornosť

doc. Ing. Matúš Pleva, PhD.

matus.pleva@tuke.sk

Tel: +421 55 602 2294

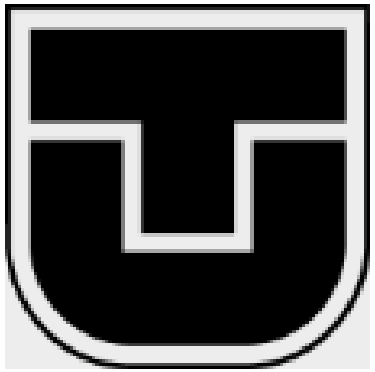
Němcovej 32, dv. 519,

KEMT, FEI, TUKE,

Košice

KEMT

Department of Electronics and Multimedia Telecommunications



Nedostatky biometrických systémov

- Sú drahšie ako použitie tokenov (heslo, ID karta, ...).
- Pri problémoch s nasnímaním biometrických dát systém nie je schopný vyhodnotiť autenticitu.
- Databázy s biometrickými dátami môžu byť ukradnuté.
- Nie sú bezchybné – kto je zodpovedný za chybu?
- Pri chorobe alebo zranení je množstvo biometrických znakov dočasne alebo trvalo poškodených.

Spoľahlivosť, bezpečnosť, štandardizácia

- Ako môžeme zdieľať získané dáta z rôznych senzorov s rôznymi databázami a systémami? Existuje štandardizácia?
- Ako sú biometrické dáta ukladané a prenášané? Je môžné ich ukradnúť a zneužiť? – šifrovanie, cancelable/revocable biometrics, blockchain?
- Ako zabrániť zneužitiu biometrických dát? spoofing -> liveness detection
- Ako je biometrický systém odolný voči hackerom?

Doplňujúce informácie

Iné biometrické techniky

- *Ľahká/jemná biometrika (**Soft biometrics**) - je to oblasť biometrie, ktorá skúma menej komplexné charakteristiky anatómie ľudského tela alebo aj správania, ktoré môžu dopĺňať tradičné biometrické znaky a pomôcť potvrdiť či vyvrátiť identitu ako je napríklad: výška postavy, hmotnosť tela, vek, pohlavie, etnikum, váha, farba očí či pleti, jazvy, tetovania aj s ich umiestnením na tele, prítomnosť zarastenej brady a jej tvar, okuliare, make-up/nalíčenie (aj chemický typ líčenia), použité oblečenie (s prípadnou pachovou stopou), prízvuk v hlase či rečová vada, fyziologické vady a podobne.*
- ***Multimodal biometrics*** – Multimodálny systém využíva viacero senzorov / algoritmov / vzoriek / jednotiek (pravé a ľavé oko, viac prstov, ...) / čŕt, je potrebné riešiť *fúziu* väčšinou rôznych *výstupných pravdepodobností*
- ***Biometrics in the Wild*** – Dáta získané vonku z veľkých vzdialeností, senzorov s nízkym rozlíšením alebo bez spolupráce subjektu znižujú schopnosť identifikovať osobu