



UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Počítačová biometria

Charakteristiky biometrických systémov

J. Majerník, L. Urbanská, A. Kačmariková

V-AR-24-25

Aplikácia biometrických systémov

Existuje niekoľko **dôvodov** na používanie biometrickej autentifikácie v závislosti od **účelu** a úrovne zabezpečenia, ktoré sú požadované systémami alebo technológiami

Medzi takéto dôvody patria okrem iného:

- výrazne nižšie **riziko krádeže identity** v porovnaní s inými technológiami a/alebo systémami autentifikácie, pretože sa používajú jedinečné ľudské biometrické znaky a atribúty
- pri autentifikácii do informačného systému **nie je potrebné si pamätať** žiadne informácie
- hackeri nevedia jednoduchým spôsobom zneužiť biometrickú autentifikáciu
- **nie je možné zdieľať** biometrické informácie s inou osobou



Problémy personálnej identity

- **Privátny** vs. **verejný** sektor
- vývoj biometrie môže priniesť rôzne **polemiky**, pokiaľ ide o osobnú povahu a zosúladenie s osobnou identitou

Na škodu
všetkých
občanov?

Veriť
predajcom?

Dôveryhodné
organizácie a vláda?

Kompetencia
a etika?

Želané alebo
nechcené?

Naozaj také
spoľahlivé?



Problémy personálnej identity

- praktická aplikácia si vyžaduje zváženie mnohých **otázok** ...
- v každom prípade si musíme byť viac vedomí **spôsobu**, akým sa technológia používa, než „**verit**“ samotnej technológii
(dôraz sa kladie na jej bezpečné a etické používanie)

**národná
a medzinárodná
bezpečnosť**

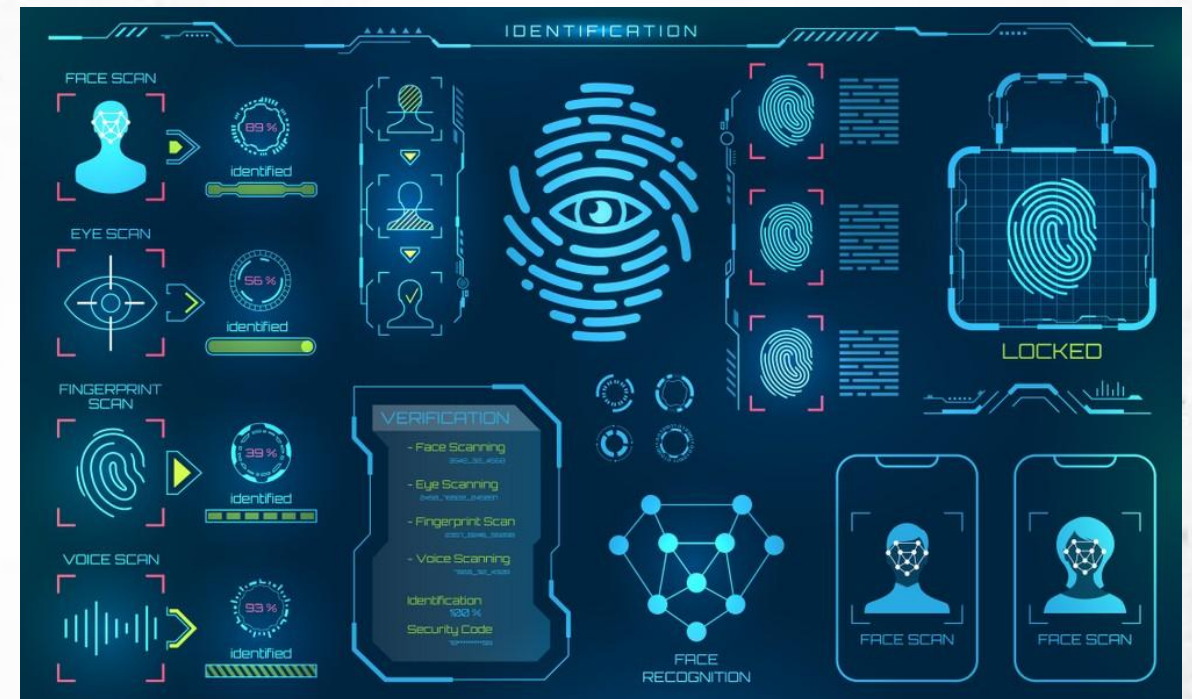


Najlepšia biometrická technika?

BEST

Ktorá biometrická technika je najlepšia?

- neexistuje celkovo „**najlepšia**“ biometria
- rôzne techniky majú výhody aj nevýhody v závislosti od aplikácie a okolností ich použitia



Najlepšia biometrická technika?

Fyzicky znečistené
alebo abrazívne
prostredie

-
Problémy pre
kontaktnú
techniku

Veľké zmeny
osvetlenia alebo
vlhkosti

-
Problémy
s technikami
závislými od
kamier

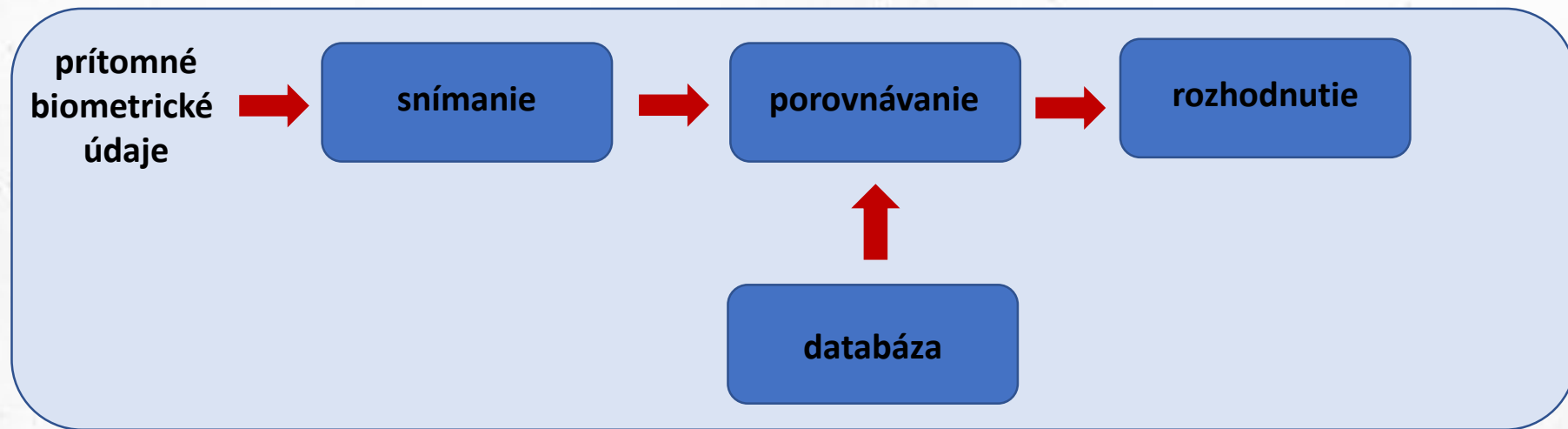
Nadmerne
hlučné
prostredie

-
Problémy so
zvukovými
technikami

- potrebné zohľadniť aj používateľskú základňu, špeciálne situácie, požiadavky na prevádzkový výkon atď.
- ... **neexistuje** najlepšia biometria, iba **optimálna** biometrická technika pre danú situáciu

Biometrické spracovanie

Prevádzka biometrického systému



Biometrické spracovanie

Ideálny biometrický systém predpokladá:

- všetci členovia populácie **majú** charakteristiku, ktorú biometria identifikuje
(tváre, odtlačky prstov, dúhovky očí atď.)
- každý biometrický identifikátor **sa líši** od všetkých ostatných v kontrolovanej populácii
- biometrické identifikátory **sa nemenia** za podmienok, v ktorých sú zhromažďované
- systém **odoláva** protiopatreniam



Charakteristiky biometrických systémov

Výkonnosť a **spoľahlivosť** biometrického systému sú kľúčovým faktorom pre vývoj aj aplikáciu. Biometrický autentifikačný systém by vždy prijímal **správne rozhodnutia**, avšak v skutočnosti sa vyskytujú **určité chyby**.

Vo všeobecnosti sa **presnosť fyziologickej** biometrie považuje za vyššiu ako **behaviorálnej** biometrie.

Štatistiky výkonnosti overovacích systémov sa líšia od tých, ktoré sú určené pre identifikačné aplikácie.



Charakteristiky biometrických systémov

Ako by sme mohli merať presnosť biometrického systému?

Ako porovnávať rôzne systémy?

...

- napr. skontrolovať biometrické výkonnostné charakteristiky „poskytované“ vývojármi/dodávateľmi...



Charakteristiky biometrických systémov

Výkonnosť biometrických autentifikačných systémov sa zvyčajne prezentuje z hľadiska **miery chybovosti rozhodovania** (presnosti):

- **miera falošných prijatí** (FAR - *false acceptance rate*)
 - **najzávažnejšia** chyba biometrického zabezpečenia
 - miera pravdepodobnosti, že biometrický bezpečnostný systém nesprávne akceptuje pokus o prístup neoprávnenej osoby (neodmietne nelegitímnu osobu)

$$\text{FAR} = \frac{\text{Počet falošne úspešných pokusov}}{\text{Celkový počet nelegitímnych pokusov}}$$

Charakteristiky biometrických systémov

- **miera falošných odmietnutí** (FRR - *false acceptance rate*)
 - situácia, v ktorej nie je možné identifikovať oprávnenú osobu
 - miera pravdepodobnosti, že biometrický bezpečnostný systém nesprávne odmietne pokus o prístup oprávnenej osoby (neoverenie oprávnenej osoby)

$$\text{FRR} = \frac{\text{Počet falošných odmietnutí}}{\text{Celkový počet legítimných pokusov}}$$

čím nižšie FAR a FRR,
tým lepší biometrický
systém
v „dokonalom“ systéme
by boli
obe miery nulové

Charakteristiky biometrických systémov

FAR



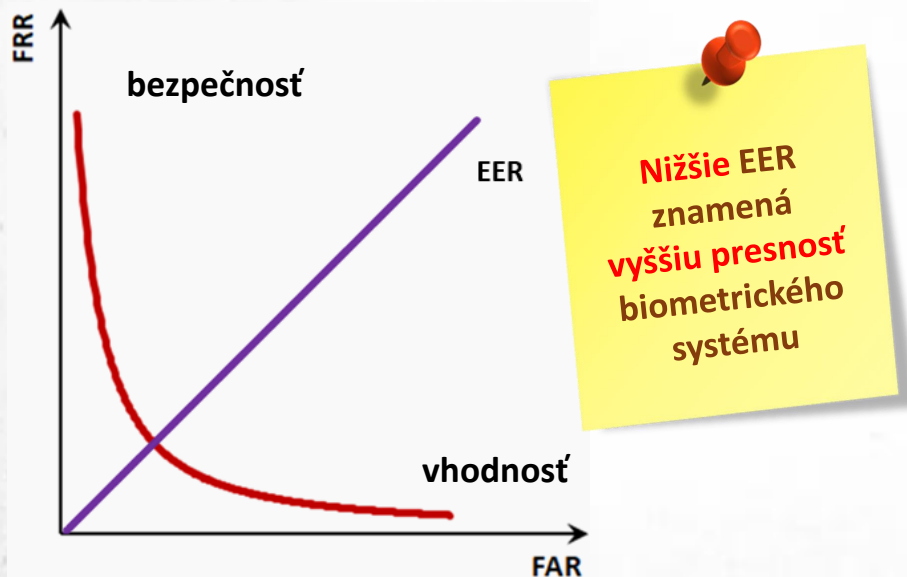
FRR



Charakteristiky biometrických systémov

- **miera rovnakej chybovosti (EER)**

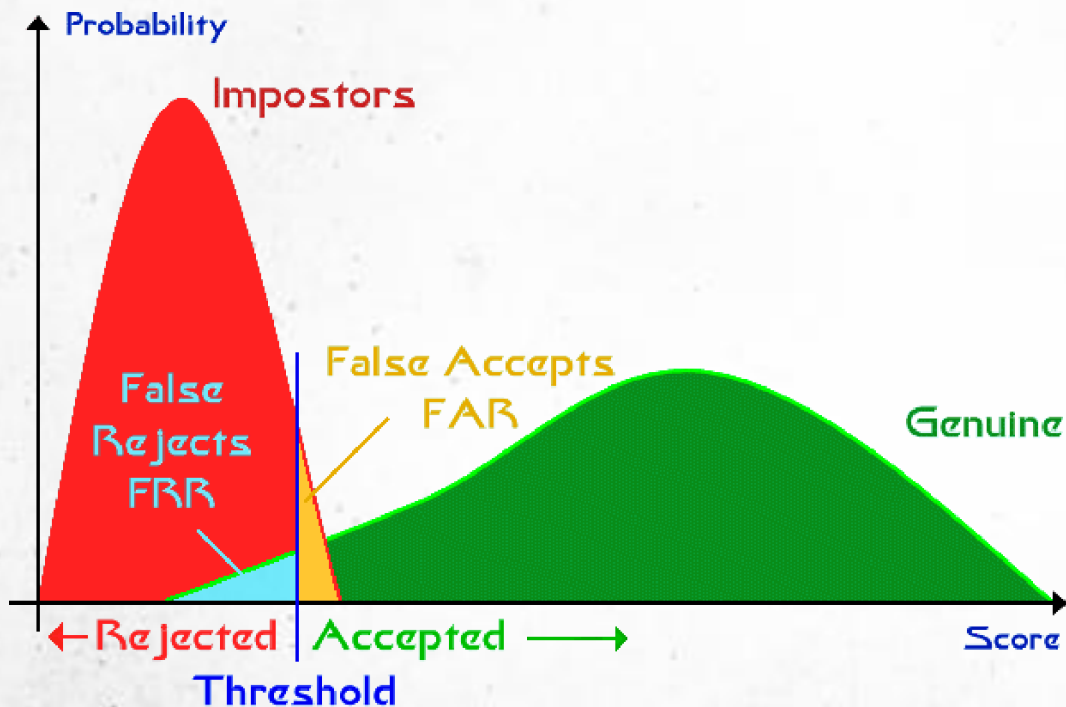
- miera chybovosti dosiahnutá na prahovej úrovni biometrického systému, kde sú miera falošného prijatia (FAR) a miera falošného odmietnutia (FRR) rovnaké
- rôzne spôsoby zobrazenia



- napr. krivka ROC (*Receiver Operating Characteristic*)
- graficky znázorňuje vzťah medzi dvoma protichodnými chybami systému pri meniacom sa prahu citlivosti

Charakteristiky biometrických systémov

- biometrické systémy majú schopnosť upraviť citlivosť (prah) miery chybovosti (t. j. systémy je ťažké porovnávať)
- miera falošného prijatia (FAR) a miera falošného odmietnutia (FRR) sa tiež nazývajú **falošná zhoda (FM)**, resp. **falošná nezhoda (FNM)**



- rozdiel je v tom, že FAR a FRR sú chyby na úrovni systému, ktoré zahŕňajú vzorky, ktoré sa nepodarilo získať alebo porovnať

Charakteristiky biometrických systémov

Výkon biometrického systému sa zhorší v prípade **nesprávnej registrácie osoby**.

Príklady meraní:

- **miera neúspešného zápisu/registrácie** (FTR - *failure to enrol rate*)
 - nastáva z dôvodu neschopnosti systému generovať opakovateľné šablóny pre konkrétnu časť populácie
 - môže nastať, ak osoba nemá daný biometrický prvok, osoba nedokáže vytvoriť obraz dostatočnej kvality počas zápisu alebo osoba nedokáže spoľahlivo zhodovať svoju šablónu v niekoľkých pokusoch v čase overenia

Charakteristiky biometrických systémov

- **miera neúspešného získania** (FTA - *failure to acquire rate*)
 - nastáva u osoby, keď systém nedokáže zachytiť alebo lokalizovať biometrické údaje s dostatočnou úrovňou kvality
 - závisí od prahovej úrovne nastavenej biometrickým systémom a môže sa zmeniť v dôsledku úpravy prahových úrovní rôznych vstupných biometrických údajov



Charakteristiky biometrických systémov

Predikcia miery falošných prijatí, miery falošných odmietnutí, priepustnosti systému, prijatia používateľmi a úspor nákladov na operačné systémy z testovacích údajov je **náročná úloha**.

Z pohľadu používateľov sú otázky:

„Je tento systém jednoduchší, rýchlejší, priateľskejší a pohodlnejší ako alternatívy?“

Tieto otázky sú veľmi špecifické, pokiaľ ide o aplikáciu, technológiu a marketing.

Charakteristiky biometrických systémov

- **nie je možné** tvrdiť, že jedna biometrická charakteristika je najlepšia pre všetky aplikácie, populácie, technológie a administratívne politiky
- **niektoré biometrické** charakteristiky sú však pre akúkoľvek konkrétnu aplikáciu jednoznačne **vhodnejšie ako iné**
- je potrebné pochopiť **technické faktory**, ale aj presný **kontext nasadenia**, aby bolo možné predpovedať prevádzkové dôsledky
(premenné prostredia interagujú s ľudskými premennými)



UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť



jaroslav.majernik@upjs.sk

lenka.urbanska@upjs.sk

andrea.kacmarikova@upjs.sk