TECHNICKÁ UNIVERZITA V KOŠICIACH

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Katedra elektroniky a multimediálnych telekomunikácií

Biometrické systémy bezpečnosti

Vysokoškolská učebnica

2021 **doc. Ing. Matúš PLEVA, PhD.**

TECHNICKÁ UNIVERZITA V KOŠICIACH

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Katedra elektroniky a multimediálnych telekomunikácií

doc. Ing. Matúš PLEVA, PhD.

Biometrické systémy bezpečnosti

Biometric security systems

Vysokoškolská učebnica

Recenzenti: *prof. Ing. Dušan Levický, CSc.*
doc. Ing. Roman Jarina, PhD.

Vydavateľ: Technická univerzita v Košiciach
Rok: 2021
ISBN: 978-80-553-3834-7
Vydanie: prvé
Dostupné online: `http://biometria.web.tuke.sk/BSB-ucebnica.pdf`
Rozsah: 120 strán

Poďakovanie

Chcem poďakovať celému kolektívu Katedry elektroniky a multimediálnych telekomunikácií, ale obzvlášť kolegom a kolegyniam z Laboratória rečových a mobilných technológií, s ktorými som na väčšine projektov a výskumných úloh úzko spolupracoval.

V neposlednom rade som vďačný *Bohu* za to, že mi po celú dobu dával silu, inšpiráciu a úžasnú rodinu. Týmto ďakujem mojim rodičom aj mojej *manželke Danke* a *synom Jankovi, Paľkovi a Jožkovi*, ktorí mi po celý čas robili radosť, akceptovali viac času stráveného v práci a tým mi dávali veľké množstvo energie a chuti do tejto práce.

Táto práca je výsledkom poznatkov získaných aj zapojením do projektov COST IC1106 - Integrating Biometrics and Forensics for the Digital Age (člen MC), CA16101 - MULTI-modal Imaging of FOREnsic SciEnce Evidence - tools for Forensic Science (člen MC), KEGA 009TUKE-4/2019 - Inovácia obsahu a príprava učebných textov pre predmet Biometrické systémy bezpečnosti (zodpovedný riešiteľ), VEGA 1/0753/20 - Robustné rečové technológie metódami hlbokého učenia (zástupca zodpovedného riešitela), APVV SK-TW-2017-0005 - Deep Learning for Advanced Speech Enabled Applications - Hlboké učenie pre pokročilé rečové aplikácie (vedúci zodpovedný riešiteľ medzinárodného projektu), VEGA 1/0075/15 - Vybrané aspekty bezpečnosti v moderných telekomunikáciách, VEGA 1/0386/12 - Bezpečnosť v moderných telekomunikačných sieťach, VEGA 1/0065/10 - Bezpečnosť telekomunikačných sietí a systémov budúcich generácií, VEGA 1/4054/07 - Bezpečnosť multimediálnych telekomunikácií a projekt 7. rámcového programu INDECT č. 218086 - Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment.

Abstrakt

Táto práca sa zaoberá spôsobmi, ako môže byť zabezpečená komunikácia človeka so strojom, pričom bezpečnosť je dosahovaná meraním fyziologických anatomických parametrov daného človeka alebo meraním jeho správania. Používateľ takéhoto systému, ktorý je oprávnený na prístup do neho alebo je mu známy sa volá pravý používateľ (genuine) a používateľ, ktorý je systému neznámy respektíve sa pokúša vstúpiť s cudzou identitou sa volá útočník (impostor). Oblasť biometrických systémov skúma rôzne spôsoby ako môže byť používateľ pri prístupe do systému preskúmaný bez toho aby si musel pamätať heslo alebo vlastniť nejaký identifikačný predmet (token). Biometrické bezpečnostné systémy nielen urýchľujú komunikáciu ľudí v modernej dobe, ale hlavne prinášajú vyššiu dôveru v komunikáciu na diaľku, čo je možné a niekedy aj nutné masívne využívať aj v moderných výukových systémoch.

V tejto práci sú dopodrobna rozpracované rôzne spôsoby snímania biometrických fyziologických (anatomických) aj behaviorálnych parametrov ľudského používateľa informačného systému. Sú definované rôzne rozdelenia biometrických systémov, spôsoby ich hodnotenia aj porovnávania, a sú načrtnuté moderné trendy výskumu a vývoja v tejto oblasti. Dôležitou časťou je kapitola o multimodálnych biometrických systémoch, kde autor prispel svojou vedeckou prácou, ktorej výsledky sú prezentované v prestížnych medzinárodných vedeckých fórach. Na záver sú predstavené spôsoby zabezpečenia, štandardizácie a rozvoja biometrických systémov v európskom právnom priestore.

Kľúčové slová

biometria, bezpečnosť, EER, FAR, FRR, multimodalita, behaviorálne znaky, fyziologické znaky, biometrické systémy bezpečnosti

Abstract

This work deals with ways in which human-machine communication can be ensured, while safety is achieved by measuring the physiological / anatomical parameters of a given person or by measuring his behavior. A user of such a system who is authorized to access it or is familiar with it is called a genuine user and a user who is unknown to the system or is trying to enter with a stolen identity is called an attacker or impostor. The field of biometric systems explores various ways in which a user can be examined when accessing a system without having to remember a password or have a token. Biometric security systems not only accelerate people's communication in modern times but mainly bring greater confidence in distance communication, which is possible and sometimes necessary to use massively in modern educational systems.

In this work, various methods of sensing biometric physiological (anatomical) and behavioral parameters of the human user of the information system are elaborated in detail. Different divisions of biometric systems, methods of their evaluation and comparison are defined, and modern trends in research and development in this area are outlined. An important part the chapter on multimodal biometric systems is where the author contributed his scientific work, the results of which are presented in prestigious international scientific forums. Finally, the ways of securing, standardization and development of biometric systems in the European legal area are presented.

Keywords

biometrics, security, EER, FAR, FRR, multimodality, behavioral traits, physiological traits, biometric security systems

Obsah

Abstrakt a kľúčové slová **v**

Zoznam obrázkov **ix**

Zoznam tabuliek **xiii**

Zoznam skratiek **xiv**

Slovník pojmov **xx**

Úvod **23**

1 Základy biometrie **26**

1.1 Úvod do biometrických systémov 26

1.2 Aplikačné oblasti biometrických technológií 27

1.3 Výhody a nevýhody biometrických bezpečnostných systémov 31

1.3.1 Detekcia autentickosti biometrického znaku 32

1.3.2 Spoľahlivosť biometrického znaku 32

1.3.3 Elektronické zdravotnícke služby a využitie biometrických technológií 33

1.3.4 Použiteľnosť biometrických systémov 34

2 Analýza, modelovanie a interpretácia biometrických údajov **35**

2.1 Základné bloky biometrického systému 35

2.1.1 Zhodnotenie kvality 36

2.1.2 Extrakcia biometrických parametrov 37

2.1.3 Modelovanie biometrických referencií 37
2.1.4 Interpretácia výsledku biometrického skúmania 38
2.2 Rozdiel medzi autentifikáciou a identifikáciou 38
2.3 Hodnotenie biometrických systémov 41
2.3.1 Vyhodnotenie chybovosti autentifikácie na základe parametra EER 44
2.3.2 Vyhodnotenie pomocou ROC a DET kriviek 45
2.3.3 Vyhodnotenie presnosti identifikácie 46
2.3.4 Statická a kontinuálna verifikácia 48
2.3.5 Základné bloky biometrického systému 49

3 Súčasné biometrické technológie 51
3.1 Fyziologické biometrické znaky a ich snímanie 51
3.2 Behaviorálne biometrické prvky v komunikácii človeka so strojom . . . 65

4 Multimodálna biometria 71
4.1 Definícia a rôzne typy multimodálnych systémov 71
4.2 Príklad multimodálneho biometrického systému analýzy dát z používania klávesnice 73
4.2.1 Kalibrácia pri akustickej analýze používania klávesnice 75
4.2.2 Fúzia výsledkov časovej a akustickej analýzy používania klávesnice 75
4.2.3 Efekt použitia multimodálnej časovej a akustickej analýzy používania klávesnice 76

5 Zabezpečenie biometrických údajov a systémov 79
5.1 Zneužitie biometrických dát 79
5.2 Možnosti zabezpečenia biometrických dát 80
5.3 Moderné trendy v oblasti bezpečnosti biometrických systémov ako celku 80
5.4 Biometrický systém využívajúci užitočne skresľujúce transformácie . . . 81

6 Biometrické aplikácie v európskom právnom priestore 82
6.1 Vízový informačný systém 83
6.2 Schengenský informačný systém 85

6.3 EuroDac - Európska daktyloskopická databáza 86
6.4 Zintenzívnenie cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti (prümské rozhodnutie) 86
6.5 Spoločná európska služba porovnávania biometrických údajov (CS-sBMS) 87

7 Štandardizácia v biometrii **88**

8 Záver **90**

Literatúra **93**

Addendum **119**

Zoznam obrázkov

2.1 Komponenty biometrického systému podľa ISO/IEC JTC 1/SC 37 Biometrics Standing Document 11, Part 1 [1]. 36

2.2 Histogram/distribúcia skóre/podobnosti pri viacerých pokusoch (napríklad Hammingova vzdialenosť prijatej vzorky od uloženého vzoru) pravých (genuine) a falošných (impostor) identít s ich aktuálnou prahovou hodnotou systému. 41

2.3 Hľadanie EER - prahu na x-ovej osi miery zhody, kedy je rovnosť medzi chybovosťou falošného prijatia - FAR a falošného odmietnutia - FRR. . 44

2.4 ROC krivka - operačná charakteristika binárneho klasifikátora. 46

2.5 DET krivka - kompromis detekčnej chyby. 47

3.1 Vybavenie biometrickými senzormi laboratória KEMT. Na obrázku je možné vidieť snímače odtlačkov prstov: DigitalPersona Eikontouch 510 a 710 + U.4500, GreenBit DactyID20, Futronic FS88H, Suprema Biomini Slim 2S; snímač dúhovky: IriSchield-USB MK2120U; snímač krvného riečišťa prsta: Hitachi H1; snímač krvného riečišťa dlane Fujitsu PalmSecure a kamera Logitech Brio 4k Pro. 52

3.2 Tvar ucha a prislúchajúci odtlačok ucha [2]. 53

3.3 Fotka zubov detského chrupu (foto z pxhere.com/cs/photo/420056 pod licenciou Creative Commons). 54

3.4 Typický senzor na snímanie dúhovky infračerveným svetlom s prisvietením na blízko - kameru je potrebné držať stabilne približne 5-10 cm od očnej buľvy po dobu cca 3 sekúnd, pričom reflexný povrch pomáha subjektu sledovať vlastný odraz oka. 55

3.5 Kroky pri spracovaní dúhovky [3] infračervenou kamerou: segmentácia (nájdenie dúhovky), normalizácia transformáciou kruhu rôznej šírky na pásik štandardnej šírky (plus detekcia masky prekrytia) a nakoniec zakódovanie informácie do vzoru s použitím binárnej masky, kde je dúhovka prekrytá viečkom. 56
3.6 Biometrický kapacitný snímač odtlačku prsta DigitalPersona Eikontouch 710 (obraz odtlačku prsta autora bol začiernený). 57
3.7 Biometrický optický snímač odtlačku prsta Futronic FS88H (obraz odtlačku prsta autora bol začiernený). 58
3.8 Rôzne vrstvy príznakov - markantov (minutiae) - hľadaných v papilárnych líniách [4] ako hlavné znaky (core - trojuholníky), konce a rozdvojenia papilárnych línií (štvorce) a póry v papilárnych líniách (ovály), ktoré sú dostupné iba pri snímkach s vysokým rozlíšením. 59
3.9 Verifikácia odtlačku prsta zosnímaného vľavo s nájdenými markantami a porovnanie zhody s markantami (minutiae) uloženými vo vzore (template), pričom je vidno nájdenie spoločného vzoru vpravo. Obrázok je z demo verzie od firmy Neurotechnology s názvom VeriFinger SDK 12.0 voľne dostupnej na webe: www.neurotechnology.com/download.html . . 60
3.10 Biometrický snímač krvného riečišťa dlane s nástavcom (PalmSecure with guide) aby dlaň bola stabilizovaná vo vhodnej vzdialenosti a primerane otvorená od firmy Fujitsu. Dá sa použiť aj bez nadstavby a snímať krvné riečište dlane bezkontaktne. 61
3.11 Biometrický snímač krvného riečišťa prsta od japonskej firmy Hitachi H1 - dáta sú prenášané šifrovane - preto aj obraz zo snímača je na obrazovke len ako binárny šum. 62
3.12 Snímka z biometrického snímača krvného riečišťa prsta a následné spracovanie obrazu [5]. 62

4.1 Príklady multimodálnych dát z rôznych senzorov, čŕt (dúhovka a tvár), vzoriek, jednotiek, reprezentácií / algoritmov / príznakov použitých na rovnakú vzorku [6]. 72

4.2 DET krivka výsledkov autentifikácie pre 3 tréningové sedenia (75 slov) pomocou zvukovej analýzy bez kalibrácie (AudioNoCab), iba s použitím časovacej analýzy (Timing), kalibrovaných zvukových výsledkov (AudioCab), fúzia kalibrovaného kalibrovaných výsledkov zvukovej analýzy a výsledkov časovej analýzy (Fused), a nakoniec to isté pre 1 trénovaciu (25 slov) a 3 testovacie sedenia - sessions (Fused 1 Train Sess.). 77

Zoznam tabuliek

2.1 Konfúzna matica binárnych rozhodnutí verifikačného / autentifikačného biometrického systému, kde *True* sú správne rozhodnutia a **False** sú nesprávne / chybné rozhodnutia. 42

4.1 Výsledky najlepšieho výsledku pre úlohu autentifikácie v EER pri použití *najlepšieho akustického modelu* a *fúzie* s príslušným časovým vzorom (rovnaká trénovacia / testovacia session) využitím lineárnej fúzie a najlepšej fúzie z balíka Bosaris toolkit. 76

6.1 Tabuľka prístupových práv do centrál biometrických databáz európskeho spoločenstva. (Prepravcovia majú prístup iba k rozhraniu potvrdzujúcemu platnosť víz(1) a ETIAS(2) autorizácie cestujúceho.) 83

6.2 Tabuľka prístupových práv do centrál biometrických databáz európskeho spoločenstva po splnení špeciálnych podmienok týkajúcich sa hľadanej osoby. 84

Zoznam skratiek

3D	*Three-dimensional space/model*
AAL	*Ambient Assisted Living*
ABIS	*Automated Biometric Identification System*
ADSL	*Asymmetric Digital Subscriber Line*
AFIS	*Automated Fingerprint Identification System*
ANSI	*American National Standards Institute*
API	*Application Programmable Interface*
ASR	*Automatic Speech Recognition*
ASVspoof	*Automatic Speaker Verification: Spoofing and Countermeasures Challenge*
AUC	*Area Under Curve*
BSI	*British Standards Institution*
CC	*Candidate Count*
CENELEC	*European Committee for Standardization in Electrical Engineering*
CERN	*Organisation européenne pour la recherche nucléaire - European Organization for Nuclear Research*
CSR	*Continuous Speech Recognition*
CS-sBMS	*Central SIS Shared Biometric Matching Service*
CMC	*Cumulative Match Characteristic Curve*
CNN	*Convolutional Neural Network*
COST	*European Cooperation in Science and Technology*
COST IC	*COST project in the field of ICT*
DARPA	*Defense Advanced Research Projects Agency*
dB	*deci–Bell*
DB	*DataBase*
DET	*Detection error tradeoff*
DIN	*Deutsche Industrie-Norm*
DRNN	*Deep Recurrent Neural Network*

DM	*Dialogue Management*
DNA	*DeoxyriboNucleic Acid*
DNN	*Deep Neural Networks*
DTD	*Document Type Definition*
EER	*Equal Error Rate*
EIT	*European Institute of Innovation and Technology*
ELRA	*European Language Resource Agency*
ECG/EKG	*Electrocardiogram*
EC/EK	*European Commission*
ECRIS-TCN	*European Criminal Record Information System for Third Country Nationals*
EEG	*Electroencephalogram - monitoring of the brain el. activity*
EER	*Equal Error Rate*
EES	*European Entry/Exit System*
EMG	*Electromyography*
ETIAS	*European Travel Information Authorisation System*
ETSI	*European Telecommunications Standards Institute*
EU/EÚ	*European Union*
euLISA	*European Agency for management of large-scale IT systems*
EURODAC	*European Dactyloscopy - EU fingerprint DB*
FA	*False Acceptance = False Positive (FR)*
FAR	*False Acceptance Rate, Type II error*
FEI	*Fakulta elektrotechniky a informatiky*
FMR	*False Match Rate*
FNMR	*False Non-Match Rate*
FN	*False Negative = False Rejection (FR) = False Non-Match (FNM)*
FNIR	*False Negative Identification-error Rate*
FNR	*False Negative Rate*
FP	*False Positive = False Acceptance (FA) = False Match (FM)*
FPIR	*False Positive Identification-error Rate*

FPR	*False Positive Rate*
FR	*False Rejection = False Negative (FN) = False Non-Match (FNM)*
FRR	*False Rejection Rate, Type I error*
FTA	*Failure to Acquire*
FTC	*Failure to Capture*
FTD	*Failure to Detect*
FTE	*Failure to Enroll*
FTF	*Failure to Find*
FTP	*Failure to Process*
GB	*GigaBytes*
GMM	*Gaussian Mixture Models*
GUI	*Graphic User Interface*
HCI	*Human - Computer Interaction*
HMM	*Hidden Markov Model*
HRI	*Human - Robot Interaction*
HTK	*HMM Toolkit*
HTK	*HMM Toolkit*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transfer Protocol*
IAAD	*Iris-recognition-at-a-distance*
ICT	*Information and Communication Technologies*
ID	*Identification - Identity Document*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
INDECT	*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*

IVR	*Interactive Voice Response*
IWBF	*International Workshop on Biometrics and Forensics*
JISC	*Japanese Industrial Standards Committee*
JRC	*Joint Research Centre*
JTC / SC	*Joint Technical Committee / Subcommittee*
KEGA	*Kultúrna a edukačná grantová agentúra MŠVVaŠ SR*
k-NN	*k-Nearest Neighbors algorithm*
LDC	*Linguistic Data Consortium*
LM	*Language Model*
LPC	*Linear Predictive Coding*
LVCSR	*Large Vocabulary Continuous Speech Recognition*
MASPER	*Multilingual and Crosslingual Speech Recognition*
MC	*Management Committee of COST action*
MFCC	*Mel Frequency Cepstral Coefficients*
MFL	*Master Label File*
MIT	*Massachusetts Institute of Technology*
MLP	*Multi-layer Perceptron*
MPEG	*Moving Picture Experts Group*
NFC	*Near-Field-Communication*
NIR	*Near Infrared Light*
NIST	*National Institute of Standards and Technology*
NLG	*Natural Language Generation*
NLP	*Natural Language Processing*
NLU	*Natural Language Understanding*
NTUT	*Norges teknisk-naturvitenskaplige universitet - Norwegian University of Science and Technology*
one2many	*Identifikácia na základe porovnania 1:N*
one2one	*Verifikácia na základe porovnania 1:1*
ORCID	*Open Researcher and Contributor ID*
P2P	*Peer-to-peer*

PCM *Pulse-code modulation*

PDF *Probability Density Function*

PIN *Personal Identification Number*

PLR *Pupillary Light Reflex*

PSD *Power Spectrum Density*

PSTN *Public Switched Telephone Network*

QA *Quality Assurance*

QG-MSVM *Q-Gaussian multi-class support vector machine*

ROC *Receiver Operating Characteristic*

RTF *Room Transfer Function*

RNN *Recurrent Neural Network*

RTG *Radioisotope Thermoelectric Generator*

SIS *Schengen Information System*

SMD *Scaled Manhattan Distance*

SNR *Signal to Noise Ratio*

STM *Sclite Segment Time Mark - file format*

STR *Short tandem repeat sequences in DNA*

SVM *Support Vector Machines*

TCP *Transmission Control Protocol*

TN *True Negative = True Rejection (TR)*

TNR *True Negative Rate*

TEOAE *Transient Evoked OtoAcoustic Emission*

TP *True Positive = True Acceptance (TA)*

TPR *True Positive Rate*

TTS *Text-To-Speech*

UAT *User Acceptance Testing*

UBM *Universal Background Model*

URI *Uniform Resource Identifier*

URL *Uniform Resource Locator*

USD *United States Dollar - currency*

UTF-8	*8-bit UCS/Unicode Transformation Format*
VEGA	*Vedecká grantová agentúra MŠVVaŠ SR a SAV*
VIS	*Visa Information System*
VSE	*Východoslovenská energetika*
W3C	*World Wide Web Consortium*
WAV	*Waveform Audio*
XML	*E*x*tensible* M*arkup* L*anguage*

Slovník pojmov

access control	*kontrola prístupu do zabezpečeného systému*
accuracy	*presnosť, pri evaluácii algoritmu identifikácie*
age estimation	*odhad veku*
anti-spoofing	*brániť sa maskovaniu/napodobenine biometrického znaku/totožnosti*
audio	*zvuk, zvukový*
autentifikácia	*verifikácia deklarovanej/proklamovanej identity*
autentizovať	*overenie pravosti, synonymum autentifikácie*
evaluácia	*vyhodnotenie systému, ocenenie, vyčíslenie*
enroll	*registrácia nového záznamu/modelu/vzoru do DB*
facial expression	*spätná väzba*
fingerprints	*odtlačky prstov*
finger vein	*obraz krvného riečišťa prsta*
fonéma	*základná rečová jednotka*
flow control	*riadenie toku dát*
frame	*rámec, skupina vzoriek / bytov*
genuine	*skutočný/pravý/nefalšovaný subjekt/používateľ*
identifikácia	*nájdenie najpodobnejšieho zo známych*
impostor	*podvodník, nepravý/falšovaný subjekt/používateľ*
iris	*obraz dúhovky oka*
keystroke dynamics	*dynamika stláčania kláves*
koartikulácia	*akustický prechod medzi fonémami*
logs	*logy - logovacie súbory - textový záznam o činnosti*
minutiae	*markanty - charakteristické znaky na papilárnych líniách získaných z odtlačkov prstov*

multilinguality	*viacjazykovosť*
neutral	*nestranný, nezaujatý, v neutrálnej polohe*
palm vein	*obraz krvného riečišťa dlane*
sample	*vzorka*
handwritten signature	*vlastnoručný podpis*
smartcard	*karta s magnetickým prúžkom alebo čipom*
streaming	*kontinuálny prenos multimediálneho prúdu dát*
template	*vzor*
treshold	*prah citlivosti/rozhodnutia*
update	*aktualizácia*
voiceprints	*hlasové odtlačky*
waveform	*typ krivky / vlny*
workshop	*pracovné stretnutie*

Úvod

Dnešná doba sa vyznačuje prudkým rozširovaním digitálnych technológií do všetkých oblastí ľudského života. Kvôli pandemickým opatreniam sa ľudia stávajú zajatcami svojich domovov a interpersonálna komunikácia prebieha hlavne pomocou elektronických zariadení spájaných digitálnymi sieťami a celosvetovou sieťou Internet.

Pri komunikácii dvoch ľudí, ktorí sa navzájom poznajú, nie je takou veľkou otázkou overenie identity, väčšinou sa používatelia poznajú pri prvom pohľade na obraz na displeji alebo po krátkom úvodnom dialógu. Rozpoznávanie identity - resp. jej verifikácia funguje väčšinou na základe našich spomienok na tvár danej osoby, alebo na jej typický hlas či vyjadrovanie. Do hry teda vstupuje analýza a porovnávanie obrazov, kde náš mozog berie automaticky do úvahy aj rôzne osvetlenie či otočenie, grimasu či gestikuláciu. Pri hlase porovnáva nielen farbu daného hlasu, ale aj slová, ktoré daný človek bežne vyslovuje, prípadne ako ich zvykne spájať, prípadne téma a obsah danej konverzácie, ktorá môže obsahovať iné dôverné informácie, ktoré zužujú množinu ľudí, ktorí by na druhej strane mohli byť.

Ak by nás pri konverzácii mal identifikovať počítač, nedokázal by zatiaľ takto komplexne zhodnotiť situáciu a vychádzal by z mnohých známych fyzických znakov - napríklad obraz tváre, alebo nášho správania - ako hovoríme, o čom hovoríme a farbu nášho hlasu, ktorá je mimochodom tiež ovplyvnená našim fyzickým stavom (chorobou, emóciami, atď.). Ak napríklad pristupujeme cez elektronickú komunikáciu do banky, môžeme aj hovoriť s človekom na druhej strane, ale napriek tomu môže počítač na základe nášho hlasu pomôcť operátorovi potvrdiť našu deklarovanú identitu, ktorú sme na začiatku uviedli (číslom zákazníka prípadne menom, priezviskom a dátumom narodenia).

Keďže komunikácia na diaľku cez elektronické komunikácie sa stáva v súčasnosti nielen štandardom, ale dokonca preferovaným spôsobom, kvôli našej bezpečnosti či zdraviu, je mimoriadne dôležité venovať sa oblasti identifikácie (nájdenia najlepšej zhody) alebo autentifikácie (verifikácie deklarovanej/proklamovanej identity) aj vo výskume a výuke moderných technických študijných odborov.

Na Technickej univerzite v Košiciach (TUKE) už desiatky rokov existuje výskumná skupina (laboratórium) zaoberajúca sa rečovými a mobilnými technológiami v telekomunikáciách na Katedre elektroniky a multimediálnych telekomunikácií (KEMT) v rámci Fakulty elektrotechniky a informatiky (FEI). Téma identifikácie človeka pri prístupe cez dátovú sieť aj pomocou jeho biometrických znakov zostane navždy interdisciplinárnou témou, pretože nielen v oblasti senzorov, ale aj v oblasti spracovania, prenosu, zabezpečenia a komunikácie sú potrebné nielen informatické, elektronické, chemické, optické a matematické metódy, ale je potrebná aj medicína, biológia a iné humanitné odbory ako psychológia či skúmanie vnímania (kognitívne vedy) pri evaluácii akceptovateľnosti danej technológie širokou verejnosťou z rôznych vekových či sociálnych kategórií.

Na katedre KEMT po zavedení nového študijného programu Počítačové siete, ktorý vychádzal z histórie študijných programov Multimediálne komunikačné technológie a Smartelektronika inžinierskeho stupňa, bol predmet Biometrické systémy bezpečnosti logickým a veľmi dôležitým prvkom na doplnenie vedomostí študentov v aplikovaní bezpečnosti prístupu do informatických systémov s využitím biometrických údajov používateľa. Autor tejto práce momentálne takisto rieši projekt KEGA: Inovácia obsahu a príprava učebných textov pre predmet Biometrické systémy bezpečnosti (009TUKE-4/2019), zameraný na dobudovanie materiálov pre tento predmet a rozvinutie materiálového zabezpečenia laboratória reálnymi biometrickými senzormi, s ktorými sa rozvíja aj výskum v rámci záverečných prác, ale aj medzinárodná spolupráca.

Táto práca má ambíciu sa ďalej rozširovať a prehlbovať ponúkané poznatky o nové výsledky aj zo záverečných prác pod vedením autora a vydať neskôr rozsiahlejšiu vedeckú prácu v tejto oblasti.

Táto práca na úvod ponúka základné rozdelenie biometrických systémov, ich defi-

níciu, základné sledované parametre pri biometrických systémoch aj senzoroch, možné aplikácie biometrických systémov, spôsoby ich zabezpečenia a kritické zhodnotenie súčasného stavu.

V ďalšej časti sa autor venuje spôsobom ako sa budujú biometrické systémy identifikácie a verifikácie používateľa, ako sa systémy hodnotia, aký je medzi nimi rozdiel v prístupe aj v technológii. Dôkladne je vysvetlený spôsob vyhodnotenia chybovosti a matematických parametrov, na základe ktorých je možné rôzne biometrické systémy identifikácie a autentifikácie porovnávať.

V ďalšej kapitole o najvýznamnejších biometrických technológiách sú dopodrobna predstavené súčasné fyziologické a behaviorálne metódy snímania parametrov človeka pri prístupe do elektronického systému. Doplnené sú fotkami z Laboratória biometrických systémov bezpečnosti s reálnymi funkčnými senzormi a ich využití pri zapojení na laboratórne počítačové vybavenie, získané vďaka financovaniu z projektu KEGA 009TUKE-4/2019.

V kapitole o multimodálnych biometrických systémoch sú najprv vysvetlené základy týchto technológií a ich členenie a potom je dopodrobna rozobratý vedecký prínos autora do tejto oblasti, ktorý vznikol v spolupráci s nórskym vedeckým tímom, vďaka medzinárodnému projektu COST IC1106 - Integrating Biometrics and Forensics for the Digital Age, v ktorom bol autor aktívnym členom a zároveň slovenským zástupcom v riadiacej komisii.

Na záver sú predstavené hlavné biometrické aplikácie v európskom priestore, ďalej v neposlednom rade hlavné výzvy v oblasti zabezpečenia biometrických systémov, technologické trendy a biometrické štandardizačné orgány.

Kapitola 1

Základy biometrie

1.1 Úvod do biometrických systémov

Každodenná interakcia medzi ľuďmi sa stáva stále viac digitálnou a ako medzičlánok v tejto komunikácii vstupuje nejaká forma informatického systému (stroja), pričom je potrebné overenie identity druhej strany spoľahlivým a dôveryhodným spôsobom. V tejto práci sa zameriame na spôsoby overenia identity používateľa v komunikácii človek - stroj pomocou jeho biometrických znakov, ktoré vychádzajú z jeho fyziologickej a anatomickej stavby tela a jeho správania (behavior). Pri pojme biometria sa niekedy chápe, že ide o akékoľvek meranie parametrov nejakého živého organizmu, pričom okrem človeka sa berú do úvahy aj zvieratá alebo rastliny. Pre účely tejto práce sa obmedzíme na parametre vzťahujúce sa k človeku a jeho komunikácii so strojom.

Moderné zariadenia osobnej potreby sú stále zabezpečené fyzickými zámkami, heslami alebo kľúčmi, pričom tieto musia byť zabezpečené voči strate, krádeži, či zabudnutiu. Preto ďalším logickým krokom je, aby prístupovým kľúčom do systému bolo niečo, čo je pre daného človeka - pravého vlastníka (genuine) - charakteristické a nemôže to stratiť, prípadne nie je jednoduché to skopírovať a o prístup do systému sa pokúsiť podvodom (impostor). Ďalším problémom je, že zariadenia, ktoré sa takto zamykajú obsahujú ešte viac našich súkromných dát, ktoré môžu pomôcť cudzej osobe nás identifikovať či podstrčiť inému systému našu identitu bez nášho vedomia. Naše dáta sa však nenachádzajú iba v bezpečných trezoroch zamknutých na kľúč, ale naše

digitálne dáta sa nachádzajú vo virtuálnych trezoroch a na sieťových úložiskách, o ktorých fyzickom umiestnení ani ako používateľ nemáme vedomosť a musíme dôverovať výrobcovi alebo nejakej bezpečnostnej autorite. Prístup k týmto dátam by však mal byť možný aj po znehodnotení či strate zariadenia, z ktorého sme pôvodne dáta nahrávali a otázka autentifikácie - teda verifikácie identity pôvodného vlastníka (genuine) je práve oblasťou, kde môže biometria zohrať dôležitú úlohu.

Biometrický systém je technológia, ktorá používa informácie o osobe za účelom jej identifikácie či potvrdenia deklarovanej/proklamovanej identity (verifikácia resp. sa hovorí aj autentifikácia či autentizácia). Aby bol systém efektívny, snaží sa zhromažďovať také informácie o osobe, ktoré by mali byť čo najviac unikátne. Informácie môžu byť fyziologického (je potrebné ich merať senzormi) či behaviorálneho (správanie) charakteru.

Slovo *biometria* pochádza z gréckych slov *bio* $\beta\iota o$ - *život* a *metrikós* $\mu\varepsilon\tau\rho\iota\kappa\acute{o}\varsigma$ - *merať*. V slovenčine používame pojem *biometria* na vednú oblasť a *biometrika* na meranie živých organizmov [7].

1.2 Aplikačné oblasti biometrických technológií

Hlavnými aplikáciami biometrických technológií sú v súčastnosti:

- bankové služby,
- hraničné, imigračné a azylové kontroly,
- zdravotné elektronické služby,
- platobné terminály/služby,
- kontrola vstupu do objektu (firma, byt, garáž, telocvičňa, záujmový útvar, atď.) alebo chráneného počítačového systému,
- letiskové bezpečnostné služby,
- kriminalistika a bezpečnostné zložky,

- forenzné a súdne systémy,
- automatizované systémy kontroly premávky (rýchlostná kontrola s fotkou),
- lotériové terminály,
- vernostné systémy,
- knižničné a školiace systémy,
- školy,
- systémy na vzdialené preskúšavanie/testovanie (či už školské alebo certifikačné),
- mobilné telefóny a prístup k údajom v nich,
- registrácia pri voľbách a iných verejných hlasovaniach,
- registrácia na diaľku (digital onboarding),
- registrácia do podporných mechanizmov (sociálne dávky, a podobne).

Výhodou biometrických systémov je, že je ťažšie ich oklamať alebo ukradnúť voči bežným bezpečnostným predmetom ako sú smartcards, rodný list, občiansky preukaz, kľúče (klasické do zámkov či USB elektronické kľúče), PIN, platobná karta, mobil a podobne. Môžu byť jednoduchšie na používanie a nemusia vyžadovať nosenie dodatočných bezpečnostných predmetov či pamätanie zložitých informácií - keďže jednoduché heslo/PIN (napríklad nbu123, 0000, heslo01 a podobne) nám neposkytuje požadované zabezpečenie. Identifikácia biometrickou metódou môže byť aj rýchlejšia - zlomok sekundy (napr. odtlačok prsta) voči zdĺhavému zadávaniu hesiel a PIN kódov (niekedy posielaných vo forme SMS správy).

Biometrické systémy neslúžia len na identifikáciu používateľov, ale aj na *vzdialené zavedenie / registráciu (enrollment) nového používateľa s využitím jeho biometrických znakov*, bez osobnej návštevy pobočky. Zvykne sa to nazývať aj ako "digital onboarding"[1] a súčasťou je aj identifikácia a verifikácia pravosti existujúcich identifikačných

[1] `https://www.innovatrics.com/digital-onboarding-toolkit/`

kariet daného používateľa. Identifikačných kariet použiteľných v danej krajine existuje často veľké množstvo ako vodičský preukaz, rôzne verzie občianskych preukazov, či preukazov sociálneho či zdravotného poistenia. Väčšinou je súčasťou aplikácie napríklad naskenovanie občianskeho preukazu plus nasnímanie tváre, hlasu či odtlačkov prstov priamo z mobilného telefónu. Daná aplikácia skontroluje pravosť daného dokladu a porovná jeho identifikačné biometrické znaky s tými, ktoré boli pri procese naživo zosnímané. Ďalšou dôležitou funkciou je skontrolovanie, či osoba s danými biometrickými znakmi už nie je registrovaná s iným dokladom, čo pomáha zamedziť duplikovaným úverom.

Zaujímavými aplikáciami sú aj *hľadanie podobných tvárí* v množstve hodín z rôznych sledovacích kamerových záznamov, na jednoduchšiu identifikáciu podozrivých osôb [2]. Takéto systémy sú schopné spracovať stovky hodín kamerových záznamov v minútach a zobraziť najvyskytovanejšie tváre s linkami na časy v jednotlivých videách na manuálne skontrolovanie. Zaujímavou vlastnosťou je aj nájdenie podobných tvárí, ktoré sa dajú použiť na získanie dôveryhodných svedeckých výpovedí, ak svedkovia správne identifikujú správnu osobu z množiny poskytnutých podobných fotiek.

Môžeme povedať, že ľudia môžu byť identifikovaní na základe toho, čo:

- **majú** - *something you have* (ID, pas, rodný list, kľúče, iné tokeny, atď.),
- **vedia** - *something you know* (heslo, PIN, meno, rodné číslo, atď.),
- **sú** - *something you are* (biometrické znaky ľudského tela, teda znaky, ktoré dokážeme odmerať).

Ak sa používajú v systéme identifikácie položky z dvoch alebo viacerých týchto skupín, hovoríme o dvojfaktorovej alebo multifaktorovej verifikácii [8].

Keď hovoríme o biometrických znakoch, ktoré sú využiteľné pre účely automatizovaných systémov, hľadáme hlavne znaky, ktoré sú:

- **univerzálne** (universality) - každý zdravý človek by mal daný znak mať (ide hlavne o ich polohu na ľudskom tele, kde samozrejme aj to, že daný znak tam

[2] `https://www.innovatrics.com/face-recognition-solutions/`

nie je, predstavuje dôležitú informáciu - chýbajúce tetovanie, prípadne strata končatiny či prsta),

- **rozlíšiteľné/unikátne** (distinctiveness) - malo by byť možné nájsť rozdiely v danom znaku/charakteristike medzi rôznymi osobami,
- **trvalé/stále** (permanence) - znaky by sa nemali rýchlo meniť, pričom samozrejme úrazmi a starnutím môže dochádzať k ich miernym zmenám,
- **snímateľné** (collectability) - znaky by malo byť možné relatívne jednoducho merať, snímať - senzory by mali byť dostupné a jednoducho rozšíriteľné.

Vzhľadom na praktickú použiteľnosť biometrických systémov sa berú do úvahy aj parametre ako:

- **výkonnosť/spoľahlivosť** (performance) - či daný biometrický znak je relatívne rýchlo a jednoducho snímateľný, parametrizovaný a porovnaný s uloženou databázou.
- **prijateľnosť/akceptovanie** (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.
- **nespochybniteľnosť/neklamnosť** (circumvention) - systém by malo byť ťažké oklamať, či spochybniť identitu, ktorú prijal za pravú/autentickú.

Samozrejme pri výskume sa tieto parametre berú do úvahy až v neskorších fázach. Pri výskume v oblasti biometrie a aj iných oblastiach platí, že je niekedy nutné skúmať aj navonok bláznivé a neuskutočniteľné nápady, ktoré sa ale časom môžu stať oveľa reálnejšími. Stáva sa, že napríklad na základe prvých poznatkov príde nejaký výrobca so senzorom, bez ktorého by systém bol v praxi nepoužiteľný. Alebo sa zvýši kvalita dostupných senzorov, takže sa spoľahlivosť systému zmení z nepoužiteľného na sľubný, a podobne.

1.3 Výhody a nevýhody biometrických bezpečnostných systémov

Nevýhodu biometrických systémov môže byť, že biometrické znaky sa môžu počas života meniť či stratiť/zničiť (po úraze alebo schválne). Nie je možné ich delegovať na druhú osobu v prípade, že je dotyčný používateľ indisponovaný. Biometrické systémy bezpečnosti sú väčšinou finančne nákladnejšie na spustenie, údržbu aj beh zvoleného riešenia. V prípade problémov pri snímaní biometrických údajov môže systém zhoršovať akceptáciu používateľmi systému (user acceptance level). Databáza, ktorá obsahuje biometrické údaje, môže byť ukradnutá alebo narušená vložením cudzích biometrických údajov pod falošnou identitou, čo používateľ systému nemusí identifikovať. Biometrické systémy nie sú 100%-tné a tak nemusia byť všeobecne akceptované. Bezpečnosť dát pri prenose medzi senzorom, systémom spracúvajúcim údaje a biometrickou databázou musí byť zabezpečený voči prieniku či kopírovaniu útočníkom, ale na druhej strane štandardizácia je potrebná na zlacnenie a rozšírenie danej technológie.

Obavy zostávajú napríklad aj z ukradnutia biometrických znakov osoby a jej replikovanie na účely nabúrania do iného systému. V jednoduchosti povedané, ak používate to isté heslo na rôznych systémoch s rôznym stupňom zabezpečenia a dôležitosti, môže sa stať, že niekto získa vaše heslo z databázy miestnej parkovacej služby a použije ho na prienik do vášho bankového konta či bytu. V prípade hesla je obrana jednoduchá, a teda zmena hesla vo všetkých systémoch, na ktoré si spomeniete, a hlavne tých, ktorých prelomením by došlo k najväčšej škode. Pri biometrických údajoch je situácia skomplikovaná tým, že vaše biometrické znaky si väčšinou nemôžete po ich krádeži zmeniť a tým pádom všetky systémy, ktoré ich používajú, sú už pre vás nedostatočne bezpečné a potrebujete v nich svoje uložené biometrické údaje zmazať a použiť iné biometrické údaje (iné prsty pri odtlačkoch a podobne). Teda budete musieť používať len tie biometrické znaky, ku ktorých krádeži a replikovaniu nedošlo.

Krádež biometrických údajov sa stáva bežnou súčasťou útokov na osobnú identitu [9]. Je veľké množstvo spôsobov ako získať napodobeninu/repliku odtlačkov prstov,

tváre, hesiel či PIN kódov a podobne. Nie je mojím cieľom priblížiť podobné techniky, skôr chcem upozorniť na to, aby sme necítili falošnú istotu pri ich používaní, a že s pridaním ďalšieho modernejšieho zabezpečenia by sme nemali strácať ostražitosť.

1.3.1 Detekcia autentickosti biometrického znaku

Ostražitosť pri používaní akýchkoľvek bezpečnostných systémov je vždy na mieste, a preto je veľkou témou aj detekcia autentickosti biometrického znaku, či detekcia živosti objektu (liveness detection, fraud / spoofing attack detection), ktorá poskytuje dodatočnú kontrolu pri systémoch vyžadujúcich vyššie zabezpečenie (trezor, hraničná kontrola, atď.) a snaží sa eliminovať možnosť použitia repliky biometrického znaku (umelého odtlačku prsta, fotky, makety ruky, silikónovej masky, neživých častí tela, a podobne). Tieto systémy sa snažia napríklad získať údaje nekonvenčným spôsobom (ktoré ešte útočníci nepoznajú alebo nevedia tak ľahko oklamať) - napríklad využitie infra kamery (termálne emisie) namiesto bežnej kamery pri rozpoznávaní tváre, či doplnenie o 3D kameru či senzor vzdialenosti, ktorý je schopný identifikovať, či ide o 3D model tváre alebo len 2D plochý model - teda napríklad fotku. Prípadne sú kamerou sledované pohyby tváre, mimických svalov, pohyb dúhovky v oku či jej reakcia na svetlo, a tým je dokázaná živosť objektu. Prí snímaní z kamery dokonca existujú techniky detekcie, či sa nezmenila kamera (napríklad v telefóne) podľa šumu optického snímača typického pre konkrétny výrobok [10] napriek tomu že je to rovnaký typ aj séria.

1.3.2 Spoľahlivosť biometrického znaku

S každou novou technológiou časom môže prísť spôsob, ako systém oklamať. Zaujímavým fenoménom je napríklad syntéza reči, ktorá donedávna neumožňovala dosiahnuť hlas podobný nejakej osobe do takej miery, že by bol schopný oklamať povedzme počas telefónneho hovoru osobu či biometrický systém na druhej strane linky. V súčasnej dobe však už existujú systémy využívajúce hlboké neurónové siete, ktoré podobný dialóg sú schopné zvládnuť [11] a podobne existujú systémy na zmenu tváre vo videu nahraným bezpečnostnou kamerou.

Opäť ale recipročne existujú výskumníci, ktorí pracujú na systémoch detekcie takýchto falošných hlasov a tvárí v záznamoch, keďže poznáme algoritmy ako je tento proces vykonaný [12].

Všetko je ale vo veľmi dynamickom vývoji a myslím, že v čase vydania tejto publikácie, je ťažko podľa záznamu zverejneného povedzme anonymne na internete, so stopercentnou istotou tvrdiť, kto bol na ňom zachytený. Všetko sa to odvíja od toho, aký prospech dokáže prípadnému útočníkovi nahrávka/hlas poskytnúť a prostriedkov, ktoré je na to ochotný/schopný v danom čase a priestore vynaložiť. Tým ale samozrejme nechcem spochybniť originalitu nejakých konkrétnych záznamov.

1.3.3 Elektronické zdravotnícke služby a využitie biometrických technológií

Treba podotknúť, že elektronické zdravotnícke služby majú zvláštne postavenie v biometrii, pretože už teraz ukladajú veľké množstvo biometrických údajov avšak za iným účelom. Slúžia momentálne hlavne na archiváciu a spracovanie biometrických dát a informácií o zdravotnom stave (napr. RTG zubov, EKG, DNA vzorky, atď.).

V súčasnosti sú ale tieto údaje čoraz väčším bezpečnostným rizikom pre pacientov, keďže v prípade uniknutia týchto informácií je možné falšovanie identity v niektorých systémoch. Takže je trošku paradoxné, že v súčasnosti sa uvažuje nad ochranou biometrických dát pacientov biometrickými systémami využívajúcimi jednak biometrickú identifikáciu autorizovaných osôb (teda hlavne lekárov ošetrujúcich daného pacienta), ale aj pomocou biometrických údajov pacienta, aby nebolo možné zasahovať do zdravotnej dokumentácie a záznamov bez vedomia pacienta.

O podobnom zabezpečení sa uvažuje napríklad v pôrodniciach, aby nebolo možné po uložení biometrických znakov dieťaťa hneď po pôrode bez vedomia matky zasahovať do jeho identifikačných biometrických údajov a tým pádom aby nebolo možné dieťa zameniť [13].

Samozrejme problémom je, ak pacient, ktorý má takto zabezpečené zdravotné údaje, potrebuje urgentnú pomoc a nie je schopný udeliť súhlas. V tomto prípade sa už ráta s filtrovaním údajov nevyhnutných na urgentnú zdravotnú starostlivosť a jej

sprístupnenie záchranným zložkám hneď po identifikácii osoby (či už pomocou biometrických údajov alebo povedzme občianskeho preukazu či blízkych ľudí v jeho blízkosti) aj bez jej aktuálneho súhlasu. Tento súhlas môže byť udelený povedzme vopred počas pravidelných kontrol. Tento prístup samozrejme v určitých indikáciách môže pomôcť pacientovi zachrániť život správnou voľbou medikamentov. Na druhej strane to môže byť opäť možnosť ako sa neautorizovaná osoba získa prístup k biometrickým údajom, keďže sú ľahšie dostupné.

1.3.4 Použiteľnosť biometrických systémov

V používaní moderných technológií, ku ktorým biometrické technológie patria, však podľa môjho názoru musíme pristupovať aj s určitou mierou dôvery a odvahy, inak by sme sa mohli báť používať aj telefón, banku a jej platobnú kartu, verejnú dopravu či piť vodu z vodovodu, pretože pomaly každý aspekt nášho života je aj kvôli inováciám a uľahčeniu ľudskej práce týmito technológiami ovplyvňovaný.

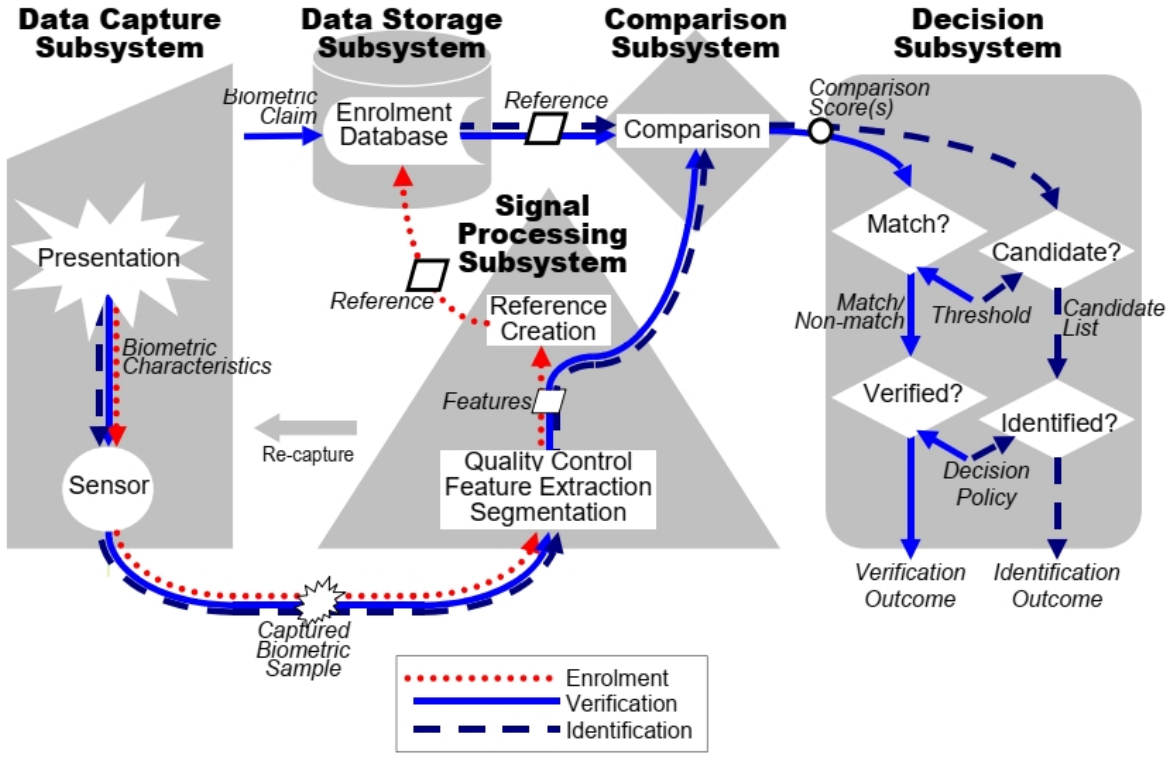
Jedným zo spôsobov ako napriek nedokonalosti systému je možné zvýšiť jeho dôveryhodnosť je, že po niekoľkých neúspešných autentifikáciách systém vyžaduje počkať nejaký čas pred ďalším pokusom a tento čas sa exponenciálne zvyšuje.

Kapitola 2

Analýza, modelovanie a interpretácia biometrických údajov

2.1 Základné bloky biometrického systému

Biometrické algoritmy obsahujú automatizované metódy, ktoré umožňujú *biometrickému systému* automaticky rozpoznať jednotlivca/používateľa podľa jeho anatomických/behaviorálnych čŕt [14]. Biometrická analýza pozostáva zo sekvencie automatizovaných operácií vykonávaných biometrickým systémom na overenie alebo identifikáciu používateľa. Na Obrázku 2.1 môžeme vidieť všeobecný model biometrického systému so základnými blokmi priamo z návrhu ISO/IEC štandardu 19794-1 [1]. V rámci analýzy biometrických údajov je potrebné najprv *zhodnotenie kvality* (Quality control) snímky/záznamu (sample), vylepšenie snímky/záznamu (sample), *extrakciu* hľadaných biometrických *parametrov* (features) z danej snímky/záznamu (sample), klasifikáciu/indexovanie parametrov - *vytvorenie modelu/vzoru* (reference), *hľadanie najlepšej zhody* (comparison) a pri multimodálnom biometrickom systéme aj *fúzia* (viď. kapitola 4, ako aj kompresné algoritmy, ktoré sa často používajú na zníženie úložného priestoru a šírky pásma [15].



Obr. 2.1 Komponenty biometrického systému podľa ISO/IEC JTC 1/SC 37 Biometrics Standing Document 11, Part 1 [1].

2.1.1 Zhodnotenie kvality

Prvým krokom po samotnej extrakcii biometrickej snímky (sample) je kontrola, či obsahuje to čo očakávame. Teda ak chceme mať snímku tváre, hľadáme na obrázku tvár (ak ich je viacero potrebujeme ich oddeliť - segmentovať), ak ide o hlas tak vo zvukovom zázname hľadáme hlasovú / rečovú aktivitu, pri extrakcii dúhovky hľadáme oko a viečka a podobne. Väčšinou v tomto kroku systém pracuje s obrazovými dátami, ale môžu to byť aj časovo premenné signály jednej (hlas) alebo aj viacerých dimenzií (EMG - viac senzorov sníma svalovú aktivitu napríklad zápästia). Podľa typu signálu je rôzny aj spôsob ich spracovania. Pri časovo premenných signáloch dochádza najprv k extrakcii rôznych typov príznakov, často ide o frekvenčnú analýzu (FFT, MFCC, ...).

Výsledkom fázy zhodnotenia kvality môže byť, že je vzorka odmietnutá a požaduje sa opätovné zosnímanie. Teda alebo je snímok z rôznych dôvodov nízkej kvality, alebo

nezachytáva očakávanú entitu - tvár, oko, prst a podobne. Táto chyba sa zvykne nazývať aj Failure to Detect (FTD). Ak tam síce daná entita je, ale senzor ju nebol schopný z nejakých dôvodov zachytiť v požadovanej kvalite, potom hovoríme o Failure to Capture (FTC). Môže to byť spôsobené špinou, osvetlením, nevhodnou rotáciou a podobne.

2.1.2 Extrakcia biometrických parametrov

Dôležitým krokom pri spracovaní komplexných dát, čo väčšinou biometrické snímky sú, je extrakcia vhodných parametrov, ktoré sa ďalej používajú pri vytvorení vzoru (template) či modelu (model). V súčasnosti sú aj moderné prístupy vo forme hlbokých neurónových sietí, kde extrakcia dôležitých informácií je urobená vo viacerých vrstvách neurónovej siete a tá sama vlastne hľadá tie podstatné vlastnosti z daných dát. Klasickým prístupom je hľadanie vhodných parametrov, ktoré sú v prípade biometrického systému čo najpodobnejšie v rámci snímok toho istého používateľa - intrapersonálna korelácia, a čo najrozličnejšie ak ide o rôznych používateľov - interpersonálna diskriminácia / odlišnosť. Ak potom tieto parametre alebo príznaky umiestnime v n-dimenzionálnom priestore snažíme sa nájsť miesta, kde sú zoskupené parametre patriace jednému používateľovi a zároveň sa snažíme nájsť diskriminačnú čiaru/y, ktorou ich oddelíme od druhého či všetkých ostatných používateľov. Tieto diskriminatívne procesy sú väčšinou vykonávané algoritmami ako SVM (support vector machine) či k-NN (k-Nearest Neighbors). Modernými prístupmi sú samozrejme neurónové siete, ktoré však vyžadujú mať veľké množstvo dát, na ktorých sa učia. To je však práve doménou dnešnej doby, keď dáta sú masívne zbierané prakticky všade a najviac asi v našom mobilnom telefóne.

2.1.3 Modelovanie biometrických referencií

Ako už bolo spomenuté, extrahované príznaky sa v kroku enrollment (zaradenia do DB) použijú na vytvorenie vzoru (template) alebo natrénovanie modelu vo všeobecnosti nazývanej referencie (reference). Ak chceme získanú snímku porovnať s dátami už uloženého používateľa, tak dochádza v tomto kroku k porovnávaniu získaných parametrov s uloženou referenciou. V rámci daného porovnania systém vyhodnotí určitú

mieru podobnosti či pravdepodobnosti, že daná vzorka je od toho istého používateľa ako uložená referencia. Natrénovanie modelu väčšinou vyžaduje viacero vektorov parametrov, a hovoríme o ňom väčšinou pri vzorkách zbieraných vo viacerých časových okamihoch za sebou, ako napríklad zvukové dáta. Pre vytvorenie vzoru väčšinou potrebujeme jeden alebo niekoľko snímkov (samples). Napríklad pri tvári je dobré aby daný vzor pokrýval viacero pohľadov. Pri vzorke dúhovky ale napríklad môže stačiť jedna snímka a preto nehovoríme o modeli, ktorý sa väčšinou trénuje väčším množstvom vektorov parametrov.

2.1.4 Interpretácia výsledku biometrického skúmania

Po porovnaní referencie s prijatými vzorkami je potrebné nejakým spôsobom interpretovať výsledok, teda mieru podobnosti či pravdepodobnosť, ktorú daný algoritmus vyhodnotí. Toto je niekedy práve najnáročnejšia časť celého systému, ako si vysvetlíme v ďalších kapitolách. Pri niektorých úlohách je táto podobnosť natoľko jednoznačným faktorom, že je možné navrhnúť jednoduchý prah (threshold) nad ktorým budeme považovať daného užívateľa za pravého / oprávneného (genuine). Niekedy však systém môže vyhodnotiť podobnosť či pravdepodobnosť v iných medziach pri každom pokuse. Napríklad pri porovnaní s množinou viacerých referencií z databázy dostaneme hodnoty medzi 10 až 200, a pri druhej vzorke zas pri porovnaní s rovnakou množinou medzi -20 až 20. Ak nejde o systémovú chybu dizajnu daného algoritmu, tak je potrebné urobiť dodatočnú kalibráciu, ktorá prispôsobí hodnoty do podobných medzí, aby mohol byť nejaký prah stanovený. Samozrejme čím je systém kvalitnejší, tak tým častejšie sa stáva, že daná hodnota podobnosti/skóre je pri pravom (genuine) užívateľovi nad stanoveným prahom, a pri porovnaní s viacerými referenciami bude najvyššia pri referencii, ktorá patrí danému používateľovi.

2.2 Rozdiel medzi autentifikáciou a identifikáciou

V biometrických systémoch sa na **autentifikáciu** používa metóda **one2one** (1:1) teda porovnanie zosnímaných biometrických znakov s proklamovanou/deklarovanou identi-

tou a jej biometrickými referenciami z databázy. V tomto prípade nedochádza k porovnaniu s modelmi/vzormi iných používateľov, čo môže viditeľne urýchliť autentifikačný proces v rozsiahlych databázach.

Autentifikácia je overenie deklarovanej identity a jej výsledkom je binárne rozhodnutie *prijatie* alebo *zamietnutie* vstupu. Táto metóda však vyžaduje, aby sa používateľ nejakým spôsobom najprv sám identifikoval - deklaroval či proklamoval svoju identitu - čo môže byť prakticky realizované vložením používateľského mena (alebo napríklad aj kliknutím na meno v zozname pri prihlásení do operačného systému), načítaním ID karty, či NFC (near field communication) zamestnaneckej karty alebo vyslovením svojho mena a priezviska. Táto metóda teda môže byť pre používateľa komplikovanejšia a viac zdĺhavá, čo môže ovplyvniť akceptáciu danej technológie používateľmi (user acceptance). Rozhodnutie o prijatí či zamietnutí je systémom vydané na základe prahu, ktorý ovplyvňuje následne mieru bezpečnosti a pohodlnosti pri používaní, čo bude podrobnejšie vysvetlené pri FRR, FAR a EER hodnotách neskôr.

Ako teda bolo spomenuté, autentifikácia v biometrických systémoch vyžaduje najprv deklarovanie identity používateľom. Ak však má byť systém jednoduchší na používanie, používa sa aj metóda **one2many** (1:N), čo by sa dalo porovnať s **identifikáciou** osoby porovnávaním jej biometrických údajov so všetkými známymi vzormi z databázy, čo však môže byť zdĺhavý proces ak ide o väčšie databázy, takže nemusí byť výhodou.

Výstupom systému one2many je identita najpravdepodobnejšieho vzoru z databázy (nie rozhodnutie o prijatí ako pri autentifikácii) a prípadne aj s jeho pravdepodobnosťou. Pritom by sa mala brať do úvahy aj možnosť, že sa objaví používateľ, ktorý v databáze nie je (open set), ale môže byť s niekým z databázy podobný. Preto ak ide o prístupový systém, tak by malo byť dodatočným rozhodnutím prijatie alebo odmietnutie vstupu do zabezpečeného systému. V prípade nového a teda neznámeho používateľa bude teda pravdepodobne systém schopný nájsť najbližšiu identitu z databázy, aj keď možno s nízkou pravdepodobnosťou, ale to ho predsa samozrejme nemôže oprávniť na vstup do systému. Preto sa tiež objavuje pojem nájdenie neznámeho/podvodníka (impostor matching) a nájdenie známeho (genuine matching) používateľa.

Pojem identifikácia sa aj kvôli týmto postupom *niekedy v praxi používa* aj na systém,

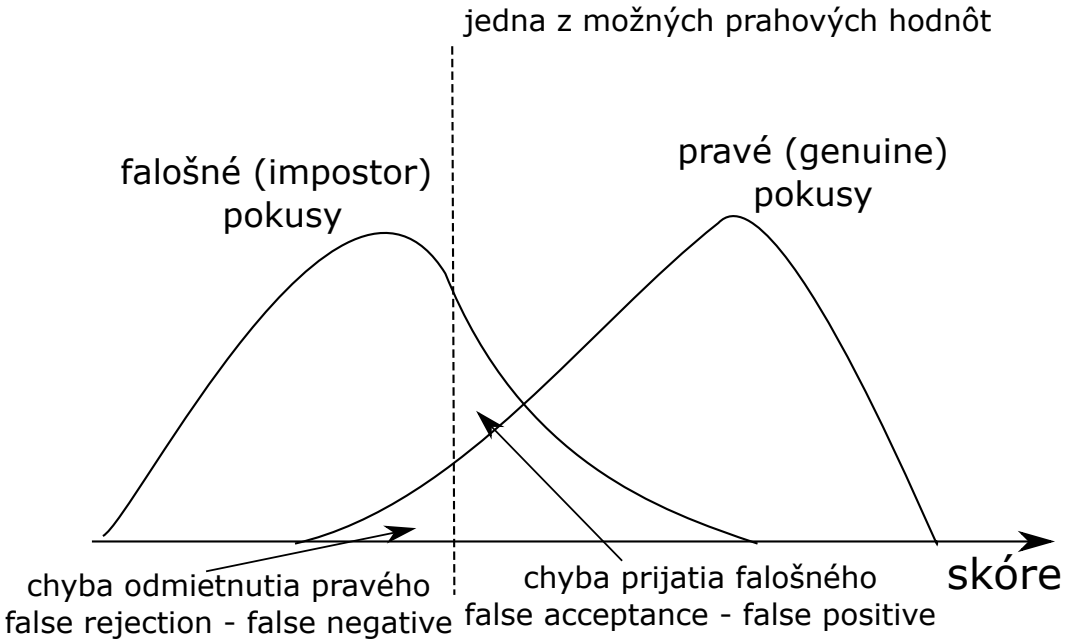
ktorý vykonáva *viacnásobnú verifikáciu* používateľa, ktorý nedeklaroval svoju identitu a teda verifikuje jeho vzorku so všetkými modelmi v databáze. Výsledkom môže byť, že verifikačný mechanizmus vyhodnotí viacero záznamov v databáze ako pravdepodobne zhodné alebo žiadny záznam nevyhodnotí ako zhodný. Samozrejme veľkosťou databázy rastie výpočtová náročnosť takéhoto systému.

Algoritmus *identifikácie neznámeho / negatívna identifikácia* teda nehľadá identitu používateľa, ktorého nepozná, ale má len povedať, že daný používateľ sa v databáze známych nenachádza (closed set). Vykonáva teda viacnásobnú verifikáciu a zisťuje či pri niektorom modeli neprekročila porovnávaná vzorka nastavený prah. Pri nájdení známeho (genuine matching) môžeme predpokladať, že neznáma osoba nemá do systému fyzicky prístup, prípadne to môže byť systém, ktorý sa len pokúša nájsť najpodobnejšiu identitu - napríklad systém, ktorý prispôsobí nastavenia sedadla/zrkadiel v aute, a teda identifikácia s cudzím profilom nespôsobí žiadnu ujmu novému ani identifikovanému používateľovi systému.

Pri one2many systémoch však existujú riešenia, ktoré umožňujú nastaviť prahovú hodnotu na základe skúseností z identifikácie a autentifikácie s využitím rozsiahlych biometrických databáz, pričom daný systém nielen nájde identitu, ale je schopný aj povedať, či bude daná identita prijatá/verifikovaná/autentifikovaná a či teda nejde o neznámeho používateľa, ktorý sa len svojimi biometrickými znakmi na niekoho z databázy podobá (open set).

Takéto systémy v praxi fungujú väčšinou s viac dôveryhodnými biometrickými znakmi ako sú krvné riečište prsta, odtlačok prsta atď. a sú prakticky viacnásobnou verifikáciou, nie identifikáciou. Ako však už bolo spomenuté, čím viac používateľov prehľadávaná databáza obsahuje, tým je systém nájdenia/identifikácie výpočtovo náročnejší, a preto aj majú tieto systémy prísnejšie obmedzenia na počet používateľov, ktorí budú v databáze uložení. Väčšinou platí že algoritmus, ktorý je schopný na danom výpočtovom systéme vykonávať one2many identifikáciu N používateľov, dokáže vykonávať namiesto nich v tom istom čase desaťnásobok, teda $10 \cdot N$ autentifikácií typu one2one.

2.3 Hodnotenie biometrických systémov



Obr. 2.2 Histogram/distribúcia skóre/podobnosti pri viacerých pokusoch (napríklad Hammingova vzdialenosť prijatej vzorky od uloženého vzoru) pravých (genuine) a falošných (impostor) identít s ich aktuálnou prahovou hodnotou systému.

Pri biometrickom systéme, ktorého prioritnou úlohou je verifikácia, ide o binárne rozhodnutie či bude na základe nastaveného prahu používateľ prijatý resp. prístup bude *povolený* (positive / accept / match) alebo bude prístup *zamietnutý* (negative / reject / non-match).

Ak jeho rozhodnutie bolo správne, hodnotíme ho ako pravdivé (true) alebo nepravdivé (false) ako je vidieť na Obrázku 2.2. Z týchto stavov môžeme vytvoriť jednoduchú konfúznu maticu (confusion matrix) rozhodnutí / pozorovaní po skončení testovania (viď Tabuľku 2.1), kde *genuine* - je známy používateľ, ktorý má byť prijatý a *impostor* - je útočník, ktorý nemá byť prijatý. Je vidieť, že sa v praxi používa veľké množstvo pojmov a preto nie je jednoduché sa v nich pri cudzojazyčnej literatúre orientovať.

V procese verifikácie či autentifikácie používateľa pri biometrických systémoch je možné vyčísliť aj presnosť: $Accuracy = (TN + TP)/(TP + FN + TN + FP)$, tento údaj však *nie je* pre verifikačný systém smerodajný, keďže *nie je* jasné aké typy chýb

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)

Tabuľka 2.1 Konfúzna matica binárnych rozhodnutí verifikačného / autentifikačného biometrického systému, kde *True* sú správne rozhodnutia a **False** sú nesprávne / chybné rozhodnutia.

robí a teda na aký účel môže byť použitý. Preto pri *verifikácii / autentifikácii sa tento údaj nevyčísluje ani neudáva* a pojem Accuracy - *presnosť* alebo *precíznosť* sa používa **iba** na vyhodnotenie procesu *identifikácie* z biometrických údajov.

Medzi hlavné atribúty kvality (QA - Quality Assurance) *verifikačných* biometrických systémov patria:

- **FAR** (False acceptance rate) - percento / pomer falošne prijatých identít (do systému bol prijatý/akceptovaný používateľ s falošnou identitou - impostor / podvodník), niekedy sa označuje aj ako False Match Rate - FMR či False Positive Rate - FPR / fall-out.

  $$FAR = FMR = FPR = FP/(TN + FP) \tag{2.1}$$

  kde FP je False Positive (neprávom prijatý/akceptovaný) a TN je True Negative (správne zamietnutý) - teda sledujeme len rozhodovanie systému vzhľadom k neznámemu / falošnému používateľovi či útočníkovi (impostor).

- **FRR** (False rejection rate) - percento / pomer 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.

  $$FRR = FNMR = FNR = FN/(TP + FN) \tag{2.2}$$

  kde FN je False Negative (známy používateľ bol nesprávne zamietnutý) a TP je True Positive (právom prijatý/akceptovaný) - teda sledujeme len rozhodovanie systému vzhľadom k známemu používateľovi (genuine).

- *FTD* (Failure to Detect) + *FTC* (Failure to Capture) [16] - percento / pomer 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 / pomer chybovosti pri zaradení / registrácii 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 / pomer chybovosti prí získaní dát v procese verifikácii/identifikácie - ide o sumu predošlých chýb, takže 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.).

$$FTA = FTD + FTC + FTP \tag{2.3}$$

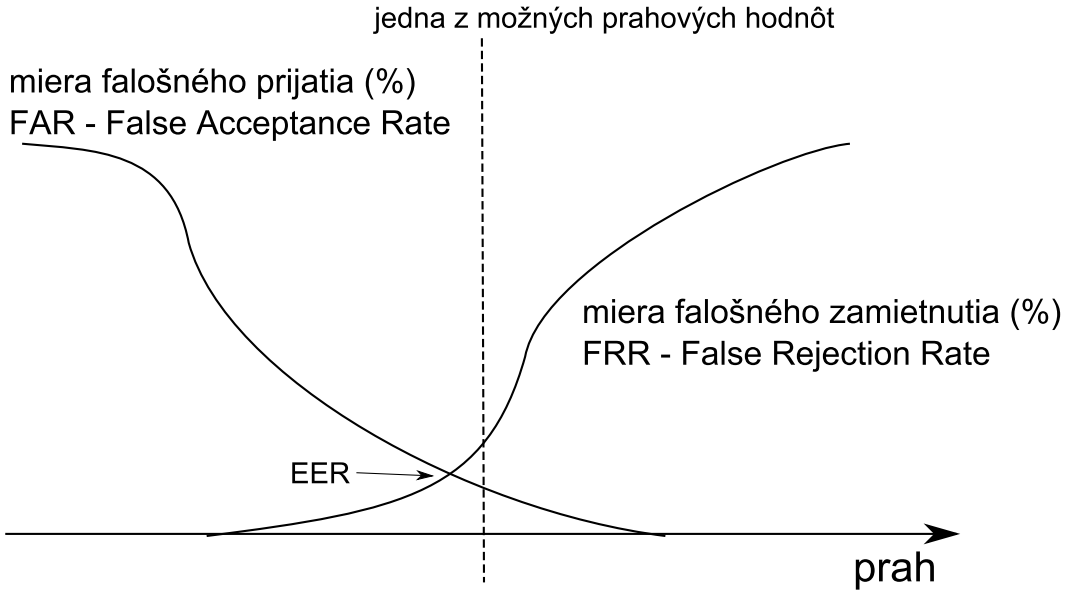
Dôležitou súčasťou biometrických systémov je evaluácia kvality zosnímanej biometrickej vzorky, pričom rozhodnutie o tom, že vzorka nie je dostatočne kvalitná je mimoriadne dôležité, ak má systém obsahovať kvalitné dáta. Kvalitné dáta prispievajú ku kvalitnej databáze, ktorá nebude produkovať zbytočné chyby a podobne kvalitná vzorka porovnávaná s databázou prinesie oveľa spoľahlivejší výsledok [17, 18]. Praktickým opatrením je, že po detegovaní nekvalitnej vzorky je používateľ vyzvaný na opakovanie snímania.

V systémoch s vysokou mierou bezpečnosti, kde prijatie falošnej identity môže spôsobiť veľkú škodu, sa preferuje nastaviť prah systému na čo najnižší FAR (povedzme $0,001\%$), ale s akceptovateľným FRR. Pričom v systémoch, kde je dôležitejšia plynulosť pri autentifikácii a prípadné narušenie identity nespôsobí veľkú škodu, je uprednostnené pre pohodlie/akceptáciu systému od používateľov čo najnižší FRR, ale s akceptovateľným FAR (povedzme $0,1\%$). Hodnoty FAR a FRR sú si nepriamo úmerné (väčšinou

nelineárne), teda zmenou jednej k lepšiemu sa druhá zhorší a naopak. Zmeny FAR a FRR je možné dosiahnuť nastavovaním *prahu* (treshold) pre matematický algoritmus vyhodnotenia podobnosti, či zhody, s biometrickými znakmi uloženej deklarovanej identity.

2.3.1 Vyhodnotenie chybovosti autentifikácie na základe parametra 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 pri zvolenom prahu zhodné (viď. Obrázok 2.3), či inak povedané chybovosť systému pri takom prahu (treshold), kedy pravdepodobnosť prijatia falošného (impostor) používateľa - podvodníka je rovnaká ako pravdepodobnosť neprijatia používateľa s pravou identitou (genuine). Niekedy sa objavuje aj pojem crossover error rate (CER) s rovnakým významom ako EER.



Obr. 2.3 Hľadanie EER - prahu na x-ovej osi miery zhody, kedy je rovnosť medzi chybovosťou falošného prijatia - FAR a falošného odmietnutia - FRR.

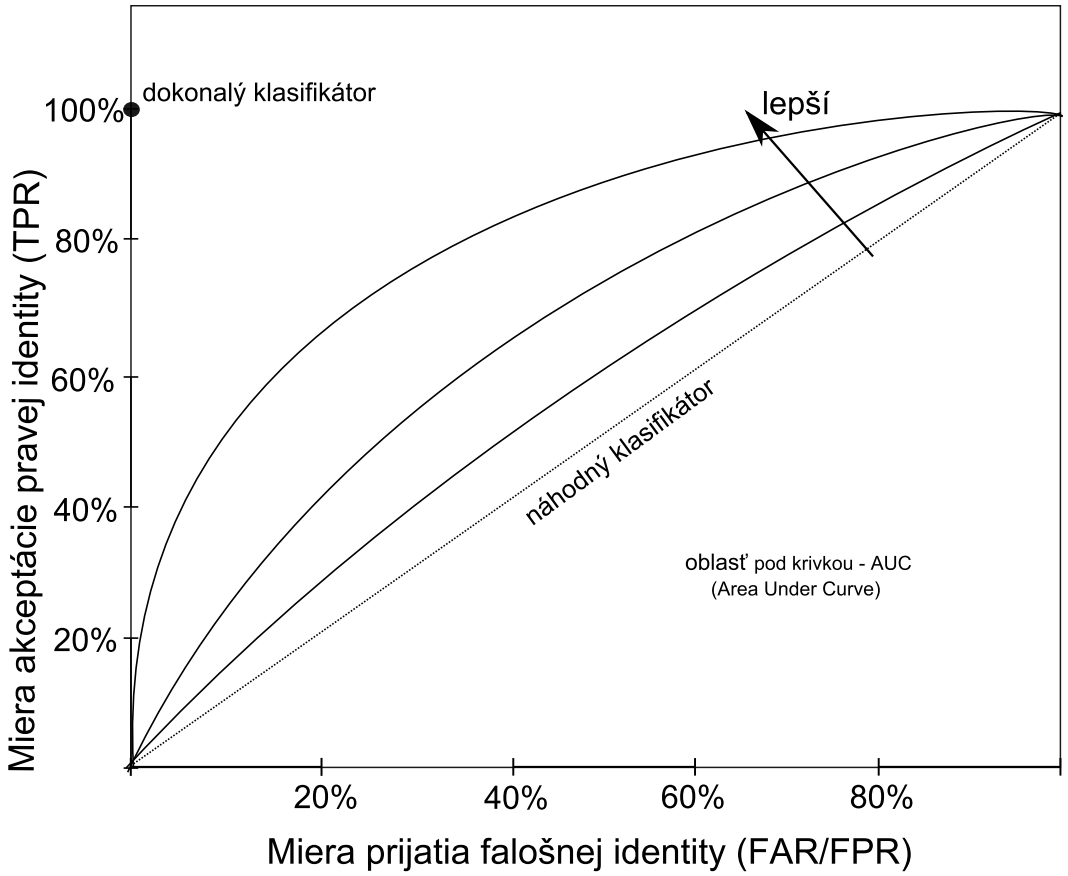
Samozrejme biometrický systém pri reálnom nasadení môže mať inak nastavenú

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 neprijatia bude len 1%, ale samozrejme pravdepodobnosť prijatia cudzej/nepravej identity sa zvýši na povedzme 8 či 15%.

2.3.2 Vyhodnotenie pomocou ROC a DET kriviek

Medzi krivkami, ktoré sa používajú na vizualizáciu kvality biometrického systému patrí aj ROC (receiver operating characteristic) krivka, ktorá sa používa hlavne v oblasti strojového učenia a dolovania dát [19]. ROC krivka vyhodnocuje schopnosť prijať pravého používateľa (genuine), a používa sa na nájdenie kompromisu medzi dosiahnutou mierou pozitívnej detekcie (TPR / hit rate / recall / detection power / 1-FRR / sensitivity) a akceptovanou mierou prijatia nepravého (impostor) používateľa (FAR / FPR / fall-out / 1-specificity) pri zmene detekčného prahu (viď. Obrázok 2.4). Presečník priamky medzi 100% (alebo 1) na x-ovej a y-ovej osi s ROC krivkou je bod ERR. V hodnotení klasifikátora sa berie niekedy do úvahy oblasť pod ROC krivkou - nazývaná ako Area Under Curve - AUC, pričom ak je to jedna, je to perfektný klasifikátor a ak je 0,5 tak je to náhodný klasifikátor.

Ďalšou často používanou krivkou je DET (Detection error tradeoff - kompromis detekčnej chyby), ktorá ako názov napovedá, je určená na nájdenie kompromisu medzi detekčnými chybami. Z názvu teda vyplýva, že berie do úvahy len chyby a to konkrétne: mieru chyby prijatia falošnej identity (FAR/FMR) a mieru chyby odmietnutia pravej identity (FRR/FNMR). Z DET krivky je možné určiť parameter EER, pretože ide o priesečník DET krivky daného systému s priamkou v 45 stupňovom uhle (kedy sú chyby/hodnoty z oboch súradníc totožné) ako to je možné vidieť na ukážke DET krivky 2.5. Krivka nemusí začínať a končiť na osiach grafu, vyhodnocujú sa len zmysluplné hodnoty prahov pre daný systém a jednotlivé systémy (v našom grafe sú tri) môžeme spoločne zakresliť do grafu a porovnať. Jednotlivé systémy môžeme porovnať aj podľa ich výkonnosti/chybovosti v priesečníku s EER, kde majú hodnotu približne 33, 37 a 64 percent.



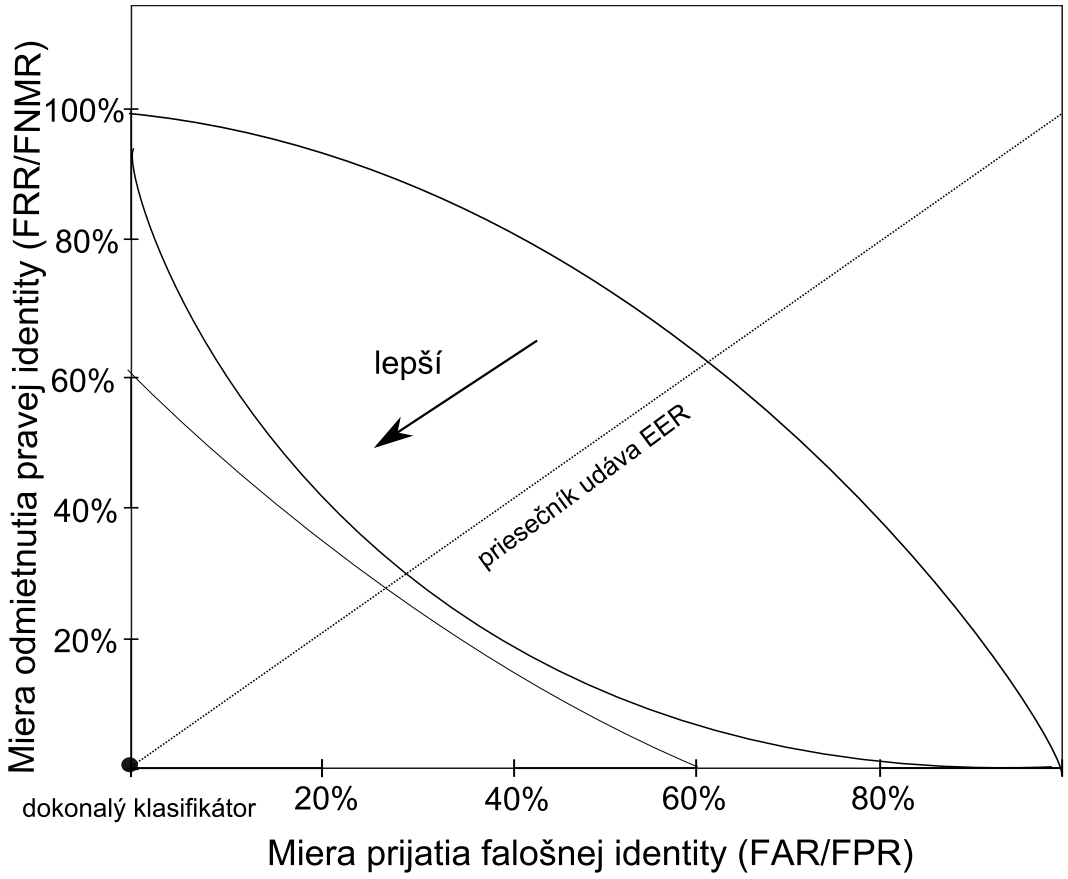
Obr. 2.4 ROC krivka - operačná charakteristika binárneho klasifikátora.

2.3.3 Vyhodnotenie presnosti identifikácie

Pri systémoch na identifikáciu používateľa (*1:N*) sa na porovnanie úspešnosti systémov používa parameter *Accuracy* - presnosť, teda s akou pravdepodobnosťou systém nájde správnu osobu z množiny známych N identít v databáze. Počíta sa ako pomer počtu správnych identifikácií (M - Match) ku všetkým vykonaným pokusom, ktoré sa počas testovania vykonajú - povedzme X. Teda $Accuracy = \frac{M}{X}$. To môžeme vyjadriť aj ako pomer počtu všetkých pokusov X mínus počet chýb substitúciou S (zamenením) a počtu všetkých pokusov X. Ak chceme *Acccuracy* vyjadriť v percentách, tak tento pomer vynásobíme 100 ako vo vzorci 2.4.

$$Accuracy = \frac{X - S}{X} \cdot 100\% \tag{2.4}$$

Pri systémoch identifikácie je ešte zaujímavé ak je systém schopný označiť vzorku



Obr. 2.5 DET krivka - kompromis detekčnej chyby.

ako neznámu, teda že vzorka s najvyšším skóre podobnosti má to skóre pod stanovenou prahovou hodnotou, kedy sa dá s vysokou pravdepodobnosťou prehlásiť, že daná vzorka sa v databáze nenachádza. Volá sa to aj hľadanie na otvorenej množine (open set).

Jednou z možností je použitie algoritmu autentifikácie na vzorku s najvyššou pravdepodobnosťou, pričom by sme skúsili otestovať, že by daný používateľ prehlásil, že je to jeho identita. Daný postup je však možné použiť iba v prípade, že algoritmy identifikácie a autentifikácie sú rôzne a produkujú iné hodnoty pravdepodobnosti a teda sa informácie navzájom dopĺňajú. Možné to je hlavne pri multimodálnych systémoch, kde napríklad jedna modalita má lepšie výsledky pri identifikácii (obraz) a druhá pri autentifikácii používateľa (hlas). Respektíve ide o rôzne modality pri snímaní toho istého biometrického znaku - zvuk klávesnice a časy stlačení/pustenia kláves získané priamo z ovládača klávesnice.

Niekedy sa pojem *identifikácia* používa aj na *viacnásobnú verifikáciu*, a to v prí-

pade, že zosnímaná vzorka je algoritmom verifikácie overená so všetkými používateľmi v databáze. Niekedy zase je používateľ verifikovaný len s N najlepšími kandidátmi, ktorí prekročili stanovený prah. Výsledkom teda môže byť od *0* po N kandidátov. Tento postup sa používa aj v prípade, že sú napríklad biometrické vzorky nekvalitné, ako napríklad pri forenznom skúmaní a podobne.

V prípade identifikácie s N najlepšími kandidátmi na výstupe existujú ďalšie spôsoby kvantifikácie chýb ako:

- *Failure to Find* (FTF) - počet nenájdených používateľov medzi prvými N kandidátmi,
- *Candidate Count* (CC) - maximálny počet kandidátov, ktorých chceme poskytovať obsluhe systému - nazývame aj *Top-K*,
- *False Negative Identification-error Rate* (FNIR) pravdepodobnosť falošne negatívnej chyby pri identifikačnej funkcii, teda pravdepodobnosť, že hľadaný objekt bude mať nízke skóre a neobjaví sa medzi *Top-K* kandidátmi,
- *False Positive Identification-error Rate* (FPIR) pravdepodobnosť falošne pozitívnej chyby pri identifikačnej funkcii, teda pravdepodobnosť, že nehľadaný objekt bude mať vysoké skóre a objaví sa medzi *Top-K* kandidátmi
- *Cumulative Match Characteristic Curve* (CMC) je krivka kumulatívnych akceptácií, ktorá má na x-ovej osi počet kandidátov (CC), a na y-ovej počet nájdených oprávnených (genuine) nad stanoveným skóre - teda testuje sa nad takzvanou uzavretou skupinou (closed set) [20] a teda nikto z hľadaných nie je mimo databázy. Jej názov je odvodený od faktu, že na y-ovej osi je suma pravdepodobností výskytov hľadanej identity na *1.* až *k.-tom* mieste (kde x=k), čo sa niekedy nazýva aj *Top-k rank* skóre.

2.3.4 Statická a kontinuálna verifikácia

Pri statickej verifikácii [21] sa používateľ autorizuje na vstup do systému raz (heslo, odtlačok prsta, smartcard a iné), pri kontinuálnej verifikácii [22] je sledované jeho

správanie počas práce/pobytu v systéme/zariadení a v prípade, že dôjde k nezvyklému správaniu (sledovať sa môže pohyb myšou, chôdza, tvár, používanie klávesnice, a iné) je používateľ vyzvaný na dodatočnú statickú autentifikáciu. Práve kombinácia statickej verifikácie pomocou hesla so sledovaním klávesovej dynamiky (keystroke dynamics) a kontinuálnej pomocou pohybu myšou je jedna z najčastejších kombinácií pri využívaní korporátnych informačných systémov.

Základnými prvkami biometrického systému sú:

- senzory,
- algoritmy spracovania biometrických dát a získania ich parametrov,
- algoritmy porovnávania vzorov,
- databáza modelov/vzorov.

2.3.5 Základné bloky biometrického systému

Interakciu biometrického systému s jeho používateľom tvorí hlavne:

- **vloženie záznamu používateľa (enrollment)** do databázy - vytvorenie modelu/vzoru či šablóny používateľa (pri overenej identite iným spôsobom - osobne, ID kartou a podobne), alebo jeho *zaregistrovanie*,
- **identifikácia** - automatické rozpoznávanie používateľa - nájdenie najpodobnejšieho zo známych používateľov,
- **autentifikácia** - automatická verifikácia prehlasovanej / proklamovanej / deklarovanej identity.

Biometrický systém môže pracovať lokálne alebo vzdialene. V prípade vzdialeného prístupu sa zosnímanie biometrických údajov deje mimo miesta, kde je systém, ktorý dáta vyhodnocuje fyzicky umiestnený, alebo ide o prístup do virtuálneho informačného systému - napríklad internet banking či e-learning. Nevýhodou vzdialeného prístupu je, že správca systému nemusí mať kontrolu nad použitými biometrickými senzormi,

ich kvalitou či modifikáciou. Pri vzdialenom prístupe je takisto ťažšie overiť či identifikovaný objekt súhlasí s identifikáciou a či nekoná povedzme pod nátlakom, či dokonca posmrtne.

Ľahká/jemná biometria (*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 [19] 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.

Biometrics in the Wild – Dáta získané vonku, z veľkých vzdialeností, senzorov s nízkym rozlíšením alebo bez spolupráce subjektu, znižujú schopnosť identifikovať osobu a tieto dáta sú označované ako “wild” alebo divoké. Takisto algoritmy a súťaže, ktoré sa na tieto dáta využívajú nesú väčšinou toto označenie.

Kapitola 3

Súčasné biometrické technológie

Pod pojmom biometrické technológie v tomto prehľade rozumieme hlavne ľudské črty a nezarátame pod živé organizmy v tejto práci zvieratá alebo rastliny. Samozrejme aj pri týchto živých organizmoch sa stretávame s pojmom biometria, ale keďže tento výskum je zameraný hlavne na interakciu človek - stroj (human computer interaction - HCI), nebudeme sa inými živými organizmami zaoberať.

3.1 Fyziologické biometrické znaky a ich snímanie

Medzi fyziologické či anatomické biometrické znaky zaraďujeme hlavne tie, ktoré je možné zosnímať z fyzického biologického ľudského tela, ktoré môže byť statické, teoreticky človek nemusí už byť nažive a teda je možné ho zosnímať aj posmrtne pri forenznej analýze. Radíme sem hlavne:

- Body odor - *telesný pach či vôňa* - typická pre daný metabolizmus vytvára špecifickú biologickú (je ovplyvnená stresom, chorobami, potravou) aj bakteriálnu stopu (hovorí sa aj o *bakteriálnej DNA* - tá je ovplyvnená celým metabolizmom - teda vplýva na ňu aj stres, lieky, potrava, atď.). Samotné odlišovanie ľudí podľa pachu síce patrí k najstarším v histórii, ale okrem použitia vycvičených psov sme zatiaľ nenašli vhodné elektronické senzory, z ktorých by sme boli schopní pach merať v takom množstve príznakov, aby bola identita rôznych ľudí rozlíšiteľná [23, 24]. Zaujímavým trendom je ale snímanie bakteriálnej stopy zo slín či vý-

Obr. 3.1 Vybavenie biometrickými senzormi laboratória KEMT. Na obrázku je možné vidieť snímače odtlačkov prstov: DigitalPersona Eikontouch 510 a 710 + U.4500, GreenBit DactyID20, Futronic FS88H, Suprema Biomini Slim 2S; snímač dúhovky: IriSchield-USB MK2120U; snímač krvného riečišťa prsta: Hitachi H1; snímač krvného riečišťa dlane Fujitsu PalmSecure a kamera Logitech Brio 4k Pro.

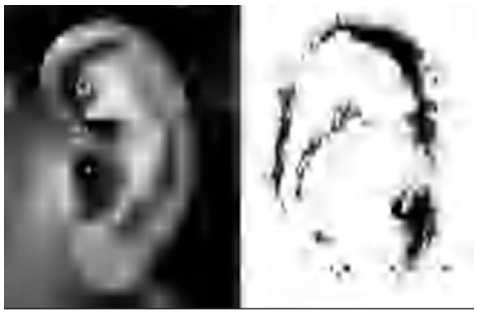
lučkov, opäť ale je to skôr doména forenznej vedy ako kontroly prístupu do elektronických systémov. Zaujímavosťou je schopnosť vycvičiť psov aj na detekciu vírusu Covid-19 z pachu človeka aj deň po jeho infikovaní[1].

- *Tvár* - fyzikálne črty tváre, môže sa snímať z viacero uhlov, problematická pri prvých systémoch sa javila detekcia "živosti"(liveness detection) [25, 26, 27], kde sa vývojári snažili zabrániť nabúraniu systémov použitím fotografie či dokonca 3D modelu alebo silikónovej masky [28, 29]. Pri snímaní sa preto pridali senzory, ktoré prípadne pomáhajú rozpoznať tvár aj pri zmene osvetlenia ako snímanie

[1] `https://unric.org/en/finland-first-in-europe-to-use-dogs-to-detect-covid-19/`

termálnych emisií, infra kamera s infra prisvetlením, meranie hĺbky (depth camera), ktorá odhalí, že nejde o 3D tvár, ale plochu [30, 29], algoritmy detekcie rastra na fotke, detekcia pohybu tváre z videa a podobne. V súčasnosti sa kvôli pandémii pracuje na algoritmoch, ktoré by boli schopné rozpoznať tváre aj pri zakrytí rúškom [31] či moslimským nikábom [32]. Pri rozpoznávaní podľa tváre sa musí brať do úvahy aj mejkap/nalíčenie (make-up), zmena strihu, fúzy, okuliare a podobne. V súčasnosti ku vyššiemu využitiu systémov na rozpoznávanie tváre prispel vývoj v oblasti hlbokých neurónových sietí (deep neural networks - DNN) [33, 12] a veľkých dát.

- *Ucho* - foto snímka ucha [34, 35, 36], prípadne aj odtlačok ucha (earprint - viď Obrázok 3.2) zosnímaný podobne ako odtlačok prsta z pevného povrchu [2]. Vznikla dokonca štúdia porovnávajúca snímky z tvrdšieho a mäkšieho povrchu (earmark) [37]. Pri foto snímke ucha vzniká pri praktickom využití problém s vlasmi, ktoré môžu ucho zakrývať, a nie každý je ochotný pokrývku hlavu, či vlasy odhaliť, takže pre praktické využitie je to používateľsky menej prijateľná alternatíva. V poslednej dobe sa dokonca objavila moderná metóda *Transient Evoked OtoAcoustic Emission* (TEOAE), ktorá meria akustickú odpoveď na click stimul (podnet na zvuk klinutia) z vonkajšieho zvukovodu [38]. Toto meranie sa robí in-ear slúchadlom so zabudovaným mikrofónom, ktorý meria odpoveď či ozvenu zvukovodu na klik podnet, čo určite tiež nie je príjemné pre používateľa.



Obr. 3.2 Tvar ucha a prislúchajúci odtlačok ucha [2].

- *Tvar prstov* na ruke [39], ruky [40], či tvar nohy [41, 42]. Pri tvare myslíme, že

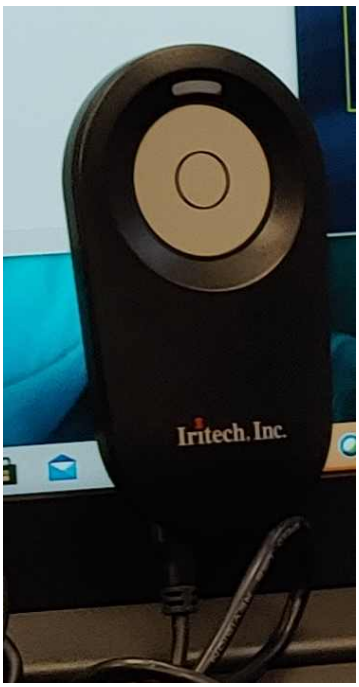
nejde o detailnú fotku alebo odtlačok, kde by boli aj papilárne línie na koži, ale skôr ide o obrysy, ktoré nám definujú čiernobiely tvar. Tvar ruky je práve široko rozšírený pri komerčných systémoch, kde nejde o vysokú bezpečnosť, ale skôr o čo najmenej obťažujúca kontrola vstupu, napríklad do fitness centra pre platiacich zákazníkov s permanentkou. Pri chodidle sa dokonca uvažovalo aj o senzoroch tlaku pri snímaní počas chôdze z podložky, pričom by distribúcia tlaku chodidla na podložku bola vstupným údajom na identifikáciu takže vo výsledku nejde o presný tvar chodidla ako v predošlých systémoch, ale skôr niečo ako stopa v tvrdšom blate naboso [43]. Pri prstoch existovali výskumy aj snímajúce tvar lôžka nechtu [44, 45].

- *Zuby* - odtlačok zubov [46, 47], prípadne RTG chrupu [48, 49, 50] či dokonca odtlačok pier [51] predstavuje spoľahlivú metódu identifikácie avšak nie je príliš vhodná kvôli potrebným senzorom a radiácii. Pri odtlačku zubov je opäť hygienický problém a nedostupnosť jednoduchého elektronického senzora. Napriek tomu sa objavili pokusy identifikácie pomocou fotky zubov zo "širokého úsmevu"(napríklad ako je na Obrázku 3.3, takže je vidieť predné rady zubov (približne 8 hore a 8 dole) [52].

Obr. 3.3 Fotka zubov detského chrupu (foto z pxhere.com/cs/photo/420056 pod licenciou Creative Commons).

- *Oko* - ľudské oči majú množstvo parametrov, ktoré môžu byť zosnímané, aj keď používateľská akceptovateľnosť týchto technológií je veľmi odlišná. Možno naj-

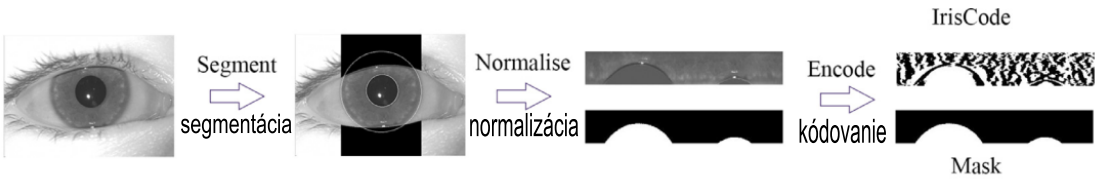
viditeľnejším znakom je dúhovka (iris), ktorá už dávno patrí k jednej z najrozšírenejších biometrických znakov [3, 53], pričom sa sníma aj posmrtne [54]. Jej výhoda je, že je u skoro každého vždy dobre viditeľná, ničím sa nezakrýva (keď je človek pri vedomí a nemá tmavé okuliare) a nie je tak obťažujúce ju zosnímať. Samozrejme kvalitná snímka môže byť časovo náročnejšia kvôli pohybu dúhovky, zaostreniu kamery a široko rozšíreným infra-snímaním (viď. Obrázok 3.4), kvôli kompenzácii rôznych svetelných podmienok a zúženia pri bežnom osvetlení (pupilárny svetelný reflex). Existujú však aj projekty snímania dúhovky na diaľku



Obr. 3.4 Typický senzor na snímanie dúhovky infračerveným svetlom s prisvietením na blízko - kameru je potrebné držať stabilne približne 5-10 cm od očnej buľvy po dobu cca 3 sekúnd, pričom reflexný povrch pomáha subjektu sledovať vlastný odraz oka.

(long range či iris-recognition-at-a-distance IAAD - cca 1 až 60 metrov) [3], kde sa používa NIR (near infrared light) kamera. Pri infra snímaní sa pracuje väčšinou s čiernobielym kruhovou snímkou, ktorá sa transformuje na vodorovný pásik a tento je porovnávaný s uloženým vzorom. Podobne ako pri iných druhoch optického snímania je potrebné zistiť - detegovať dúhovku, percento jej prekrytia viečkom s vytvorením binárnej masky (ktorá sa používa aj pri porovnaní s data-

bázou - aby sa porovnávala len viditeľná časť - viď. Obrázok 3.5), a vyhodnotenie či je snímka vhodná na použitie.

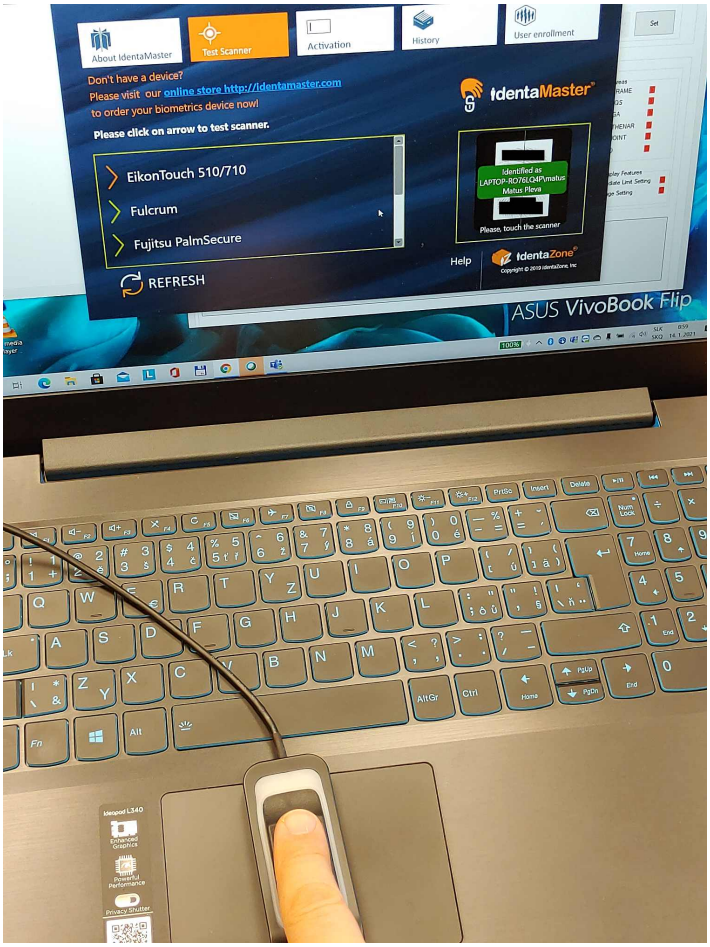


Obr. 3.5 Kroky pri spracovaní dúhovky [3] infračervenou kamerou: segmentácia (nájdenie dúhovky), normalizácia transformáciou kruhu rôznej šírky na pásik štandardnej šírky (plus detekcia masky prekrytia) a nakoniec zakódovanie informácie do vzoru s použitím binárnej masky, kde je dúhovka prekrytá viečkom.

Existujú však aj očné kontaktné šošovky, ktoré menia farbu a prípadne aj tvar dúhovky, a preto je z pohľadu vyššej bezpečnosti výhodnejšie použitie snímky sietnice (retina), ktorá však už vyžaduje komplikovanejšie a pre používateľa nepríjemnejšie a dlhšie trvajúce snímanie [55, 56, 57]. Aj sietnica však môže byť ovplyvnená chorobou, podobne ako viditeľné žilky na očnej buľve (sclera vein patterns) okolo dúhovky, ktoré tiež môžu byť použité ako biometrický znak [58].

- *Odtlačok prstov* (atrament, kapacitný ako na Obrázku 3.6, optický ako na Obrázku 3.7, piezoelektrický, termálny, ultrazvukový senzor [59], laserový 3D) patrí k úplne najlepšie pokrytej vedeckej oblasti v biometrii [60, 61] a aj najmasívnejšie využívanou praktickou aplikáciou, a preto by bol témou na samostatnú knihu. Pre systémy identifikácie používateľa na základe odtlačkov prstov existuje zaužívaný anglický názov Automatic Fingerprint Identification Systems so skratkou AFIS.

  Spomenieme teda, že hlavne vďaka zatiaľ najlepším parametrom z pohľadu kombinácie univerzálnosti, nespochybniteľnosti a teraz už aj lepšej používateľskej prijateľnosti než v minulosti, patrí stále aj k najdynamickejšie sa rozvíjajúcim odvetviam. Vďaka rozvoju medzinárodnej dopravy a biometrických pasov aj identifikačných preukazov existujú štátne aj nadnárodné agentúry s rôznym prístupom

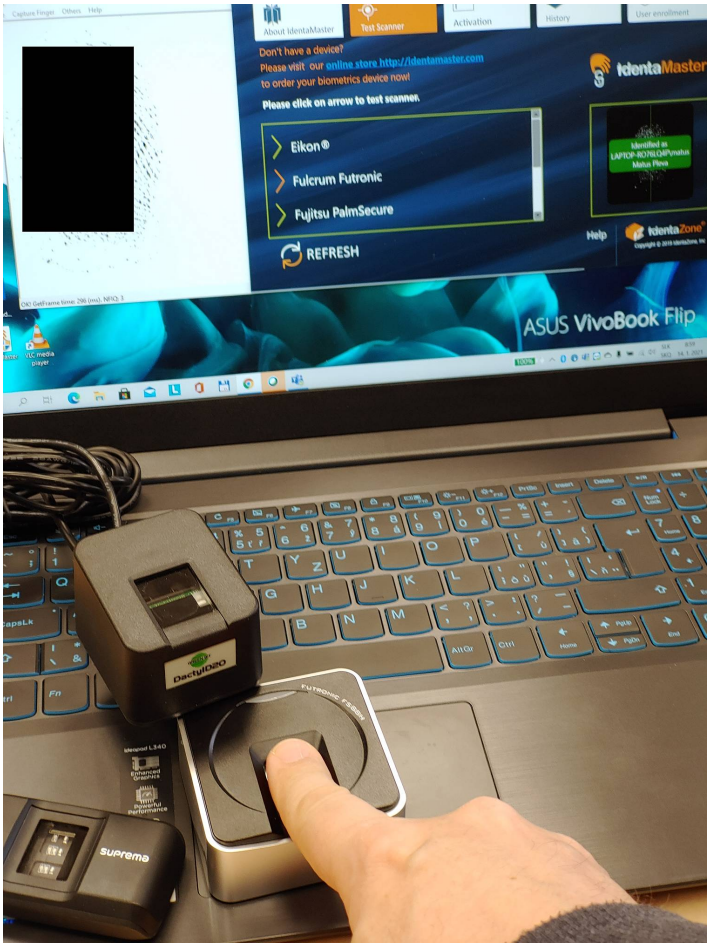


Obr. 3.6 Biometrický kapacitný snímač odtlačku prsta DigitalPersona Eikontouch 710 (obraz odtlačku prsta autora bol začiernený).

do rozsiahlych databáz odtlačkov prstov.

V oblasti detekcie živosti či falšovania [62] tiež patrí k najlepšie pokrytým oblastiam aj vďaka stále vyvíjaným a vylepšovaným senzorom snímania odtlačkov prsta, prstov či celej ruky.

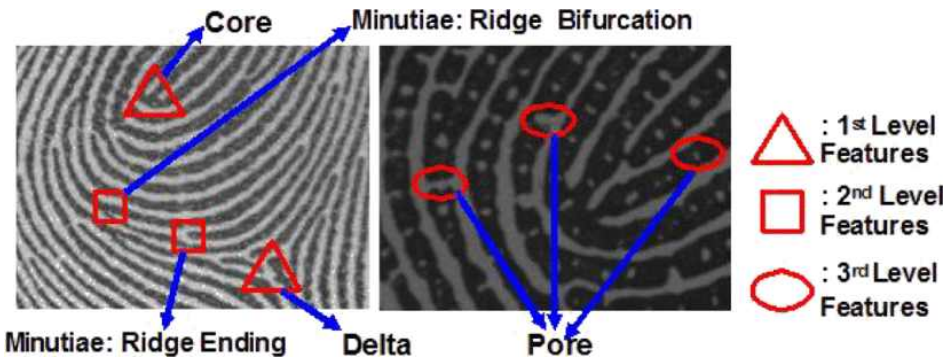
Jedným z nových a veľmi sľubných prístupov pre obdobie pandémie je aj bezdotykový laserový 3D skener [63] vyvíjaný v DG Joint Research Centre v talianskej Ispre. Zaujímavosťou a zároveň aj základnou slabinou tohto biometrického znaku je, že pre niektoré vekové skupiny kvalita zosnímaných odtlačkov doteraz rozšírenými senzormi nie je vhodná [64]. Najproblematickejšie sú deti do 4 rokov (znaky na prste sú ešte vo vývoji) a starší ľudia nad 65 rokov (koža degraduje



Obr. 3.7 Biometrický optický snímač odtlačku prsta Futronic FS88H (obraz odtlačku prsta autora bol začiernený).

a dehydruje), pričom moderné metódy už sú schopné pracovať pri zachovaní určitých odporúčaní s odtlačkami detí v skupine 6 až 12 rokov [64], ale spoľahlivosť je najvyššia medzi 12-tym a 65-tym rokom veku. Pri zohľadňovaní veku sa berie do úvahy aj model predikcie rastu prsta a evolúcie markantov na odtlačku prsta počas rokov.

Zaujímavosťou je, že pri súčasnom masívnom presadzovaní hlbokých regresných [65] a konvolučných neurónových sietí (DRNN a CNN), sa tieto uplatnili v oblasti odtlačkov prstov iba na hľadanie markantov v zosnímanom odtlačku (predspracovanie a parametrizácia ako je na Obrázku 3.8) [66, 67], ale pre efektívne hľadanie zhody s uloženými vzormi sa používajú klasické algoritmy ako napríklad Q-Gaussian multi-class support vector machine (QG-MSVM) [68]. Pri odtlač-

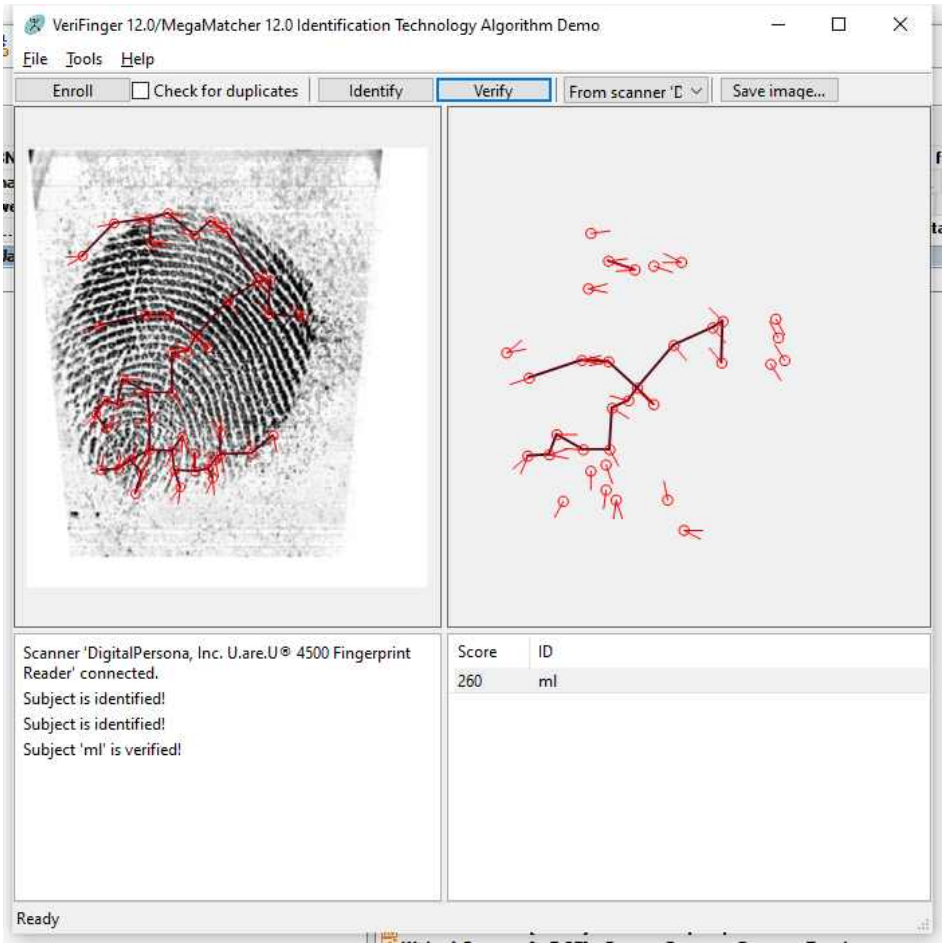


Obr. 3.8 Rôzne vrstvy príznakov - markantov (minutiae) - hľadaných v papilárnych líniách [4] ako hlavné znaky (core - trojuholníky), konce a rozdvojenia papilárnych línií (štvorce) a póry v papilárnych líniách (ovály), ktoré sú dostupné iba pri snímkach s vysokým rozlíšením.

koch prstov je dôležité spomenúť, že základným postupom je hľadanie markantov (minutiae) v papilárnych líniách a ich vzájomnej polohy ako je názorne vidieť na Obrázku 3.9. Z týchto dát vzniká model či vzor (template), ktorý sa porovnáva s nájdenými bodmi.

- *Odtlačok celej dlane* [69, 70] či nohy sa používa pri deťoch a dospievajúcich do 12 rokov [71], keď sa odtlačky prstov ešte vyvíjajú a nie sú vždy dostatočne spoľahlivé na jednoznačnú identifikáciu, napríklad v pôrodnici [72, 73]. Pri otlačku dlane sa podobne ako pri odtlačku prsta používajú aj pokročilejšie techniky snímania ako napríklad ultrazvukový senzor [74], 3D ultrazvukový obraz [75] a multimodálna fúzia so snímkou tvaru ruky (hand shape / geometry) [76, 77], ktorá sa v minulosti používala v iných multimodálnych systémoch na podporu iných znakov (napr. reči [78]).

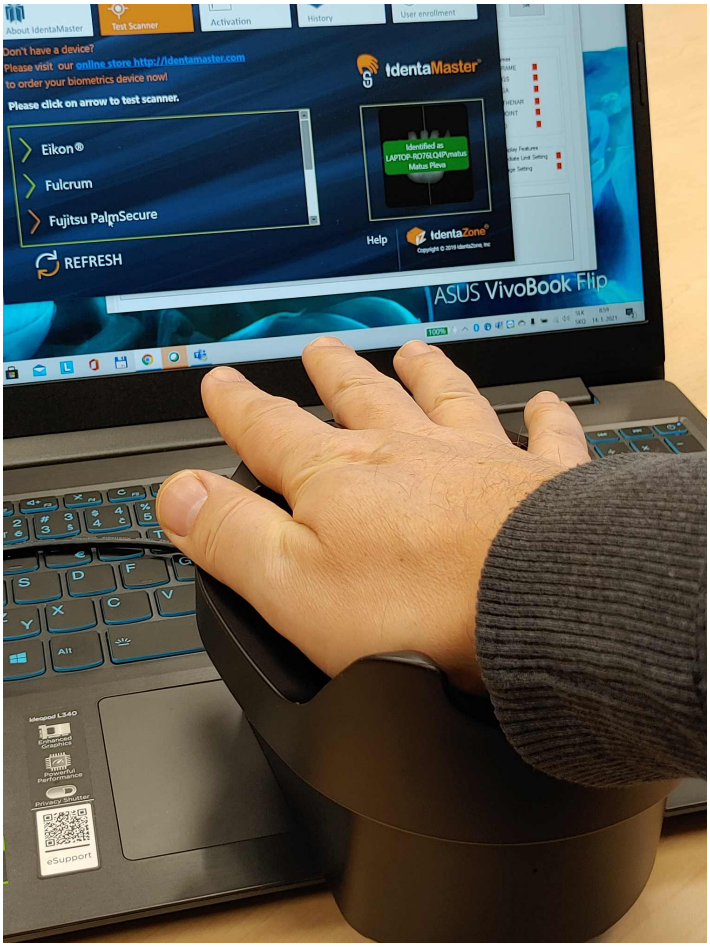
- *Krvné riečište* prstov [79, 80], zápästia a dlane (wrist/hand veins) [81], sníma štruktúrna krvného riečišťa pod kožou pomocou infra kamery ako môžete vidieť aj na Obrázku 3.10 pri snímaní dlane. Snímanie krvného riečišťa prsta je tvarom senzora podobné ako snímanie odtlačku prsta (viď. Obrázok 3.11), čo môže byť používateľsky prijateľná verzia pre snímanie biometrických znakov starších ľudí po 65 roku, keď štruktúra kože degraduje [82, 83]. Ukážka obrázku z optického



Obr. 3.9 Verifikácia odtlačku prsta zosnímaného vľavo s nájdenými markantami a porovnanie zhody s markantami (minutiae) uloženými vo vzore (template), pričom je vidno nájdenie spoločného vzoru vpravo. Obrázok je z demo verzie od firmy Neurotechnology s názvom VeriFinger SDK 12.0 voľne dostupnej na webe: www.neurotechnology.com/download.html

senzora a extrahovaných vzorov krvného riečišťa môžete vidieť na Obrázku 3.12. Z pohľadu výskumu ide o atraktívnu oblasť aj kvôli dostupnosti voľných toolkitov aj databáz hlavne z rakúskej Salzburskej univerzity [84].

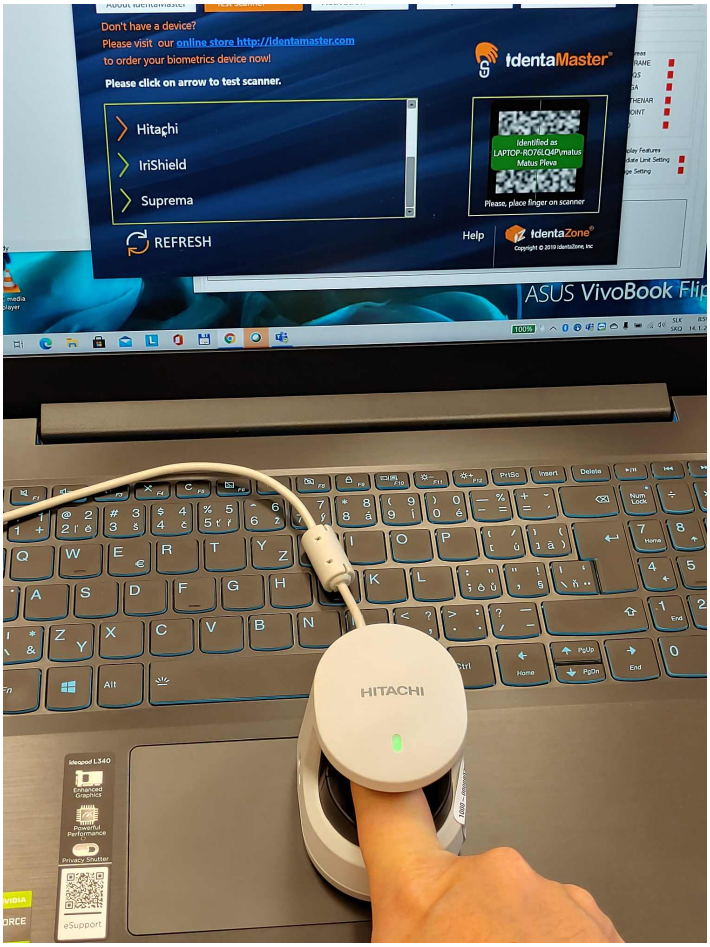
Snímanie krvného riečišťa dlane bolo implementované aj do mobilného telefónu LG G8S, vďaka čomu je možné telefón odomknúť bez fyzického dotyku, keď je položený na stole a preto je odomknutie tvárou problematické. Medzi používateľmi však nebolo veľmi obľúbené, keďže je potrebné ruku dať do správnej polohy nad telefónom a kamere trvá, kým obraz správne zosníma, čo vyžaduje od použí-



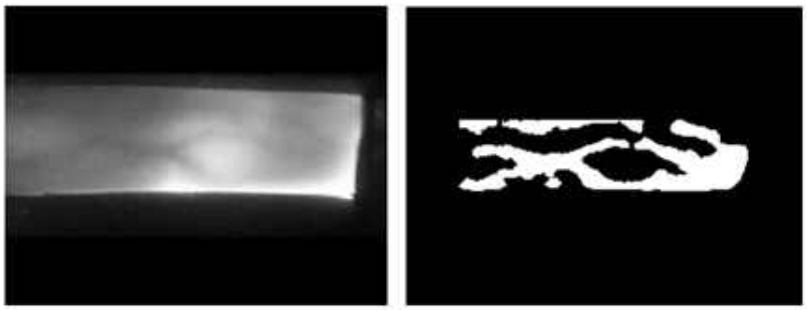
Obr. 3.10 Biometrický snímač krvného riečišťa dlane s nástavcom (PalmSecure with guide) aby dlaň bola stabilizovaná vo vhodnej vzdialenosti a primerane otvorená od firmy Fujitsu. Dá sa použiť aj bez nadstavby a snímať krvné riečište dlane bezkontaktne.

vateľa trpezlivosť aj zácvik. Na druhej strane bezkontaktné biometrické snímače naberajú v pandemickej situácii na dôležitosti, keďže ich netreba pravidelne dezinfikovať, pričom ide už o existujúcu a overenú technológiu zo širokou podporou výrobcov senzorov aj autentifikačných biometrických systémov [85]. Existuje už aj snímanie krvného riečišťa v 3D, pričom tretím rozmerom je snímanie hĺbky danej cievy pod kožou pomocou fotoakustickej tomografie, kde sa používa pulzujúci laser spolu s ultrazvukovým detektorom [86].

- *Póry na koži* je možné snímať opticky alebo laserom pri veľmi detailnej snímke alebo snímke s vysokým rozlíšením, pričom snímka môže byť z rôznych častí tela ako tvár [87], okolie očí [88], dlaň [74] či nos [89], nielen z odtlačku prsta. Snímanie



Obr. 3.11 Biometrický snímač krvného riečišťa prsta od japonskej firmy Hitachi H1 - dáta sú prenášané šifrovane - preto aj obraz zo snímača je na obrazovke len ako binárny šum.



Obr. 3.12 Snímka z biometrického snímača krvného riečišťa prsta a následné spracovanie obrazu [5].

pórov a ich textúru pri odtlačku prsta sa však často používa na detekciu živosti či pokusu o zosnímanie falošného odtlačku prsta [90].

- Tvar a detailná snímka nosa [91, 92] prípadne 3D snímka nosa [93] patria vlastne k detailnejšiemu snímku tváre, takže podobne ako iné črty tváre by sme ho mohli zaradiť k rozpoznávaniu tváre. Rovnako ako oči, ucho, snímka zubov a podobne dokáže pomocou moderných systémov snímania dosiahnuť samostatnú detekčnú či autentifikačnú presnosť [92].

- *DNA* - zloženie deoxyribonukleovej kyseliny resp. vzory opakovania krátkych tandemových sekvencií (short tandem repeat sequences - STR - väčšinou minimálne 13-tich) [94] ako spoľahlivý biometrický identifikátor sa používa už od počiatku 21. storočia. Keďže snímanie a analýza je časovo (typicky len analýza STR trvá okolo 3 hodín) a prístrojovo náročná, pri používaní DNA sa na identifikáciu osoby používali hlavne vo forenzných aplikáciách. V súčasnosti však už existujú prístupy schopné vykonať analýzu STR za 14 minút. Existujú na trhu už aj mobilné analyzátory DNA do 1000 USD[2] pripojiteľné k laptopu. Takže je možné, že v najbližšej dobe bude existovať aj DNA test na počkanie a bude možné ho použiť v kritickej infraštruktúre. Otázkou je potom len spôsob odobratia vzorky a možné oklamanie podhodenou falošnou DNA vzorkou.

- Odhad či presné meranie fyzických parametrov (*antropológia*) ako vek [95, 96], výška (z videa postavy) [97, 98, 99], hmotnosť (možné odmerať napríklad pri nástupe do lietadla, alebo zo zdravotnej dokumentácie), veľkosť chodidla, pohlavie [95], farba kože [100, 101], očí, chýbajúce zuby, špeciálne znaky (tetovania [102], následky zranení, jazvy (môže byť na odtlačku prsta [103]), choroby, atď.) sa používa pri multimodálnej biometrii v kombinácii so špecifickejšími znakmi a ich snímanie či odhad radíme do oblasti mäkkej - *soft biometrie*.

Pri anatomických či fyziologických znakoch dochádza ku zmene parametrov starnutím - vek, výška, hlas, hmotnosť, veľkosť chodidla, špeciálne znaky (tetovania [104],

[2] `https://nanoporetech.com/products/comparison`

The University of California news `https://news.ucsc.edu/2018/01/nanopore-genome.html`

jazvy [87], atď.), telesný pach, tvár, atď., ale aj úrazmi či chorobou. Prakticky každý biometrický znak môže byť týmito faktormi viac či menej ovplyvnený. Týka sa to aj behaviorálnych znakov, ktoré sú tiež vlastne tvorené ľudskými anatomickými prvkami ako ústa, pľúca, nohy, a iné.

Pri *snímaní* biometrických znakov *kamerou* dochádza k týmto hlavným komplikáciám či faktorom, ktoré ovplyvňujú ich úspešnosť [8]:

1. *natočenie* - pri snímaní tváre, prsta, ucha prípadne oka je samozrejme dôležité správne natočenie objektu a kamery, keďže obyčajná kamera (nie 3D) sníma prakticky kolmý priemet obrazu z daného uhla, snímka teda pri natočení môže byť deformovaná a nie úplne viditeľná;

2. *veľkosť/priblíženie* - objekt je samozrejmé nastaviť na vzdialenosť ktorá:

   - umožní kamere správne zaostriť - nie príliš blízko,
   - rozlíšenie bude dostatočné na získanie potrebných parametrov - nie príliš ďaleko,
   - nespôsobí deformáciu vplyvom zakrivenia šošovky - podľa typu šošovky a veľkosti objektu
   - umožní zosnímanie celého biometrického prvku - teda bude vidieť celé ucho, oko, tvár, postavu a podobne;

3. *osvetlenie* (angl. illumination) - zmena osvetlenia môže byť dôležitým faktorom hlavne pri členitejších objektoch ako je tvár či ucho, ďalším faktorom je aj svetlo v pozadí objektu, ktoré môže spôsobiť podexponovanie biometrického prvku, ktorý nás zaujíma.

4. *prekrytie* (angl. occlusions) - objekt môže byť čiastočne alebo úplne zakrytý, napríklad rúško na tvári, ruka, okuliare, šatka, závoj, fanúšikovské pomaľovanie, pančucha, a podobne.

Pri niektorých biometrických senzoroch sú tieto problémy riešené tým, že je presne stanovená poloha snímaného objektu, pričom sú aj presné formy (väčšinou plastové),

kde umiestniť tvár/prst/dlaň/oko a senzor prípadne má aj vlastný zdroj svetla (môže byť aj infra), ktorý zabezpečí aj správne osvetlenie.

3.2 Behaviorálne biometrické prvky v komunikácii človeka so strojom

Behaviorálne znaky vychádzajú zo *správania sa* používateľa informačného systému a mohli by sme predpokladať, že poskytujú automaticky aj detekciu živosti (liveness detection), keďže neživý používateľ by nemal vykazovať znaky nejakého správania. Nie je to však pravda, behaviorálne biometrické znaky čelia iným typom útokov a to napodobňovaním správania, či záznamom a opätovným prehraním záznamu pôvodného používateľa (replay attack). Pri snímaní a spracovaní jednotlivých biometrických znakov alebo ich vzoriek sa výskum tiež orientuje na detekciu pravosti danej vzorky, teda detekciou, či správanie je generované autentickým používateľom alebo ho niekto napodobuje [105].

Výber používaných behaviorálnych biometrických prvkov:

- *Podpis* písaný rukou (handwritten signature) môže byť statický - odtlačok pera na papieri [106, 107], dynamický 2D - pri tomto type je druhým rozmerom snímanie pohybov pera počas podpisovania [108] či snímanie pohybu prsta po dotykovej obrazovke [109, 110], dynamický 3D - okrem snímania pohybu senzor sleduje aj tlak pera na podložku [111], či dokonca podpisovanie vo vzduchu [112]. V súčasnosti existujú veľké databázy podpisov a na ich spracovanie sa používajú už aj hlboké neurónové siete [113].

  Treba poznamenať, že čo sa týka univerzálnosti, existujú ázijské krajiny, kde existuje zvyklosť namiesto podpisu používať pečiatku (Tajvan), prípadne je problém pri negramotných ľuďoch.

  V našom prostredí sa takisto stretávame s novým trendom zavádzania jednoduchšieho písma (napríklad Comenia script [114]), ktoré sa niekedy označuje ako nespojité, ale v skutočnosti existuje aj sa vyučuje aj jeho spojitá varianta, spája-

nie však nie je povinné ako pri spojitom písme. Vyznačuje sa veľkou podobnosťou písanej a tlačenej formy, čím sa znižuje počet znakov, ktoré sa dieťa potrebuje naučiť písať aj čítať.

V skutočnosti sa podobné písma vo svete používajú a nepredstavujú problém pri rozpoznávaní identity človeka, ktorý text písal, pretože vždy obsahujú nejaké typické ťahy rukou [115]. Problém však môže byť pri tomto znaku jeho stálosť, pretože písmo sa časom vyvíja [116] aj podľa toho, nakoľko ho daný človek vo svojom živote využíva, čo je v súčasnej dobe naozaj veľkou otázkou.

Pri skúmaní podpisu často prichádza do úvahy aj skúmanie originality papiera a atramentu, prípadne mikroskopické skúmanie rýh vytvorených tlakom na papier. To je však už skôr otázkou forenznej analýzy ako prístupového biometrického systému, kde sa používateľ podpisuje pri pokuse o autentifikáciu. Zaujímavosťou je detekcia rôznych chorôb ako Parkinsonov syndróm zo zmien správania, čo sa dá detegovať aj pri podpise [117].

- *Klávesová dynamika*, alebo sledovanie časovania stlačenia a pustenia klávesy pri písaní na klávesnici (keystroke dynamics) - dynamika pri používaní klávesnice [118]. Takisto ide o veľmi dobre pokrytú výskumnú oblasť. Rozpoznať používateľa sa väčšinou snažíme tak, že píše vopred dohodnuté heslo [119] alebo PIN [120, 121] a jeho písanie je v trénovacej databáze pokryté, ale existujú už aj prístupy schopné rozpoznať používateľa aj na základe voľne písaného textu [122, 123]. Samozrejme existujú aj prístupy, ktoré snímajú ďalšie modality ako tlak na klávesy [124, 125], zvuk kláves [126], pohyb ruky (extrahované z videa alebo gyro či EMG senzora). Pri mobilných zariadeniach je možné popri stlačených virtuálnych klávesách zaznamenávať ešte mnoho ďalších parametrov, ktoré ponúkajú súčasné mobilné telefóny ako akcelerometer, gyroskop, tlak na obrazovku, a podobne [127, 128]. Klávesová dynamika sa dá používať aj pri kontinuálnom monitorovaní správania používateľa počas skúšania na diaľku [129, 130], čo je tiež pri pandémii novou výzvou.

- *Pohyby myšou* (mouse movements / gestures), alebo typické pohyby myšou či

správanie počas práce s počítačom či iným informatickým systémom [131, 132, 133]. Keďže myš sa používa väčšinou spolu s klávesnicou, je to ideálny pár na multimodálnu biometriu [22, 134], napríklad aj pre kontrolu autenticity študenta pri prístupe do e-learning platformy [135]. Niekedy sa používa model správania sa s myšou na kontinuálnu autentifikáciu a pri podozrení (ak klesne skóre pod definovaný prah) je používateľ vyzvaný na dodatočnú autentifikáciu.

- *Hlasový odtlačok* (voiceprint) alebo tiež rozpoznávanie rečníka (speaker verification, speaker identification) je jedným z najrozšírenejších behaviorálnych znakov v praktických aplikáciách [136, 137, 138]. Ako pri iných znakoch aj reč sa môže degradovať vekom [139, 140, 141], ale aj zdravotným stavom, únavou, momentálnymi emóciami [142, 143] a podobne. Ako doplnok sa používa aj snímanie dychu pred a po hlasovom odtlačku, kde aj zo zvuku dýchania (breathing) je možné namodelovať vzorku daného používateľa [144]. V súčasnosti je najväčšou výzvou detekcia podhodenia nahrávky daného používateľa útočníkom (impostor) [145] hlavne u textovo závislých systémoch [146]. Najväčšou prichádzajúcou hrozbou však je možnosť rýchlej syntézy reči daného rečníka vo vysokej kvalite pomocou neurónových sietí [147, 148]. V tejto oblasti ale existuje vynikajúca medzinárodná súťaž na detekciu týchto útokov ASVspoof[3] (Automatic Speaker Verification: Spoofing and Countermeasures Challenge), ktorá publikuje každý rok nové databázy rečníkov a aj rôznych typov útokov na týchto rečníkov a základných spôsobov (baselines) ich detekcie [149].

- *Chôdza* (gait) je biometrický znak rozpoznávaný väčšinou z dohľadových kamier [150, 151]. Využíva sa hlavne vo forenzných aplikáciách hľadania podozrivých osôb z kamerových záznamov, keď tvár nie je viditeľná. Skúma sa chôdza, celkové držanie tela, a pohyb tela aj jednotlivých končatín pri chôdzi [152]. V poslednej dobe existujú aj výskumy na detekciu pohlavia z chôdze [153] či využitia neurónových sietí [154]. Existujú výskumy identifikácie používateľa aj pomocou nositeľných (wearable) senzorov, či už v mobile, inteligentných hodinkách alebo

[3] `https://www.asvspoof.org/`

senzorov svalovej aktivity (EMG) [155, 156].

- *Gestá* (gesture) typické pri dialógu, hádke, prípadne pri znakovej reči. Podobne ako pri chôdzi existujú prístupy detekcii gest z obrazu / kamery / 3D kamery či Kinect senzora [157], ale aj zo senzorov svalovej aktivity (EMG), ale aj v spolupráci s EKG a EEG senzormi [158, 159]. Zaujímavosťou je rozlišovanie používateľa podľa virtuálneho úderu päsťou pred seba ako pri boxovaní [160], pričom dáta boli snímané z akcelerometra smart náramku, alebo virtuálny hod loptičkou pri používaní VR (virtual reality) headsetu - náhlavnej súpravy [161]. V literatúre sa pojem gesto používa aj s spojitosti s akýmkoľvek opakovaným vzorom ako napríklad s gestami myšou - čo je vlastne sledovanie používania myši, gestami na dotykovej obrazovke - teda pohyb prstom po dotykovej obrazovke a podobne. Preto je dôležité pri štúdiu tejto oblasti rozlišovať gestá, ktoré súvisia s celými rukami, nohami či ramenami.

- *Srdcová elektrická aktivita* snímaná ako EKG (elektro kardio graf) - anglicky ECG, môže byť v súčasnosti snímaná aj pomocou nositeľných inteligentných zariadení (smart wearables) ako hodinky či fitness náramky, ktoré síce väčšinou ponúkajú hlavne snímanie srdcovej frekvencie, ale už sú na trhu aj modely so zabudovaným snímaním EKG (Withings Scanwatch, Apple Watch, Samsung Galaxy Watch 3, Fitbit Sense a iné[4]). Rozpoznávanie osoby podľa EKG už bolo skúmané aj predtým [162, 163], ale týmto posunom sa dostalo do novej fascinujúcej fázy ak by sme boli schopní dáta z hodiniek analyzovať biometrickým systémom [164].

- *Mozgová elektrická aktivita* snímaná ako EEG (electroencephalogram), síce nepríde v súčasnosti ako vhodný systém na rozpoznávanie používateľa, keďže bežne dostupné snímacie zariadenia sú komplikované na správnu inštaláciu na hlavu aby získané dáta boli vhodné na spracovanie [165]. Podobne ako pri gestách sa pojem EEG biometrics nevťahuje automaticky na rozpoznávanie používateľa [166], ale skôr na získavanie dát o mozgových vlnách ako takých [167].

[4] `https://www.reviewsbreak.com/best-ecg-smartwatch/`

- *Reakcia zrenice oka* na zmenu svetelných podmienok - anglicky pupillary light reflex (PLR) je parametrom, ktorý môže byť použitý ako doplnok k rozpoznávaniu dúhovky na identifikáciu pokusu oklamať biometrický systém umelou/vytlačenou dúhovkou [168] alebo z neživého oka [169]. Zaujímavosťou ale je snaha len na základe pohybu dúhovky v reakcii na svetlo identifikovať používateľa, pričom podľa autorov ide o jeden z najbezpečnejších behaviorálnych znakov, pretože tento reflex nie sme schopní nijako vôľovo ovládať [170]. Snímanie je možné aj pomocou smart telefónu alebo VR headsetu. Samozrejme z daného reflexu je možné identifikovať veľa rôznych chorôb a poškodení mozgu na základe rôznych vlnových dĺžok použitého svetla a tak je táto oblasť takisto bohato vedecky pokrytá.

- *Sledovanie pohybu oka* prípadne mikropohybov - anglicky Eye tracking prípadne Micro-movements of the Eye [171] sa používa na identifikáciu používateľa počas používania zabezpečeného systému. Používa sa aj v kombinácii s klávesovou dynamikou [172] či na diagnostiku rôznych neurologických ochorení ako schizofrénia [173, 174], Parkinsonova choroba [175], roztrúsená skleróza [176], demencia, autizmus [177] či dyslexia [178].

- *Pohyby pier* (lip movement) - rozpoznávanie používateľa podľa pohybov pier môžeme vnímať ako súčasť rozpoznávania podľa tváre, avšak pri tvári rozpoznávame statický obraz a pri pohyboch pier sledujeme typické správanie používateľa pri vyslovení slov, čo je často kombinované s identifikáciou podľa hlasového odtlačku [179, 180] takisto v multimodálnych biometrických systémoch.

- *Používanie mobilného telefónu* (cell phone usage) je široká oblasť pokrývajúca veľké množstvo dát a senzorov, ktoré je možné získať a jeho používateľovi ako: používanie dotykovej obrazovky (touch), senzor zrýchlenia (accelerometer), gyroskop - senzor zmeny polohy voči gravitačnej sile (gyroscope), magnetometer - senzor magnetického poľa, senzor priblíženia telefónu k telu / uchu (proximity), osvetlenie okolia (ambient lighting), senzor smeru gravitácie (gravity), senzor tlaku (pressure sensor), senzor polohy (location), poloha získaná zo zoznamu dostupných bezdrôtových sietí (WLAN - wireless LAN - WiFi, BPAN - Bluetooth

personal area network, NFC - Nier field communication) a ich SSID a MAC adries, aktivita používateľa pri používaní telefónu (user activity), protokol volaní (call data), protokol krátkych správ (SMS), protokol používania aplikácií v smartphone (app. usage), história prezerania webových stránok (browser history), stav telefónu a jeho nabíjanie počas dňa (phone status), sekundárna selfie kamera (secondary camera), analýza písaného textu a voľby opráv z ponúknutých návrhov predikcie z ovládača klávesnice (stylometry) [181, 182].

Vďaka analýze týchto dát sa stáva mobilný telefón jedným z hlavných moderných prostriedkov spoľahlivého identifikovania a autentifikovania používateľa, a to sme ešte nezahrnuli biometrické senzory, ktoré tieto telefóny majú priamo zabudované ako senzor odtlačkov prstov, tváre, krvného riečišťa dlane, hlasového odtlačku a podobne. Ďalšou možnosťou je zber dát z priamo pripojených zariadení k telefónu ako sú smart hodinky, smart band náramok, smart ring (inteligentný prsteň[5]) a mnohé iné, ktoré už dokážu zbierať množstvo biometrických údajov o danej osobe a dopĺňať dáta pre multimodálne biometrické systémy opísané v ďalšej kapitole.

[5]Titanový Oura Ring z fínskeho Oulu ponúka prepojenie s fitness aplikáciou cez Bluetooth so 7 dňovou výdržou batérie `https://ouraring.com/` pri kontinuálnom meraní srdcového tepu, teploty, aktivity a vodotesnosť do 100 hĺbky.

Kapitola 4

Multimodálna biometria

4.1 Definícia a rôzne typy multimodálnych systémov

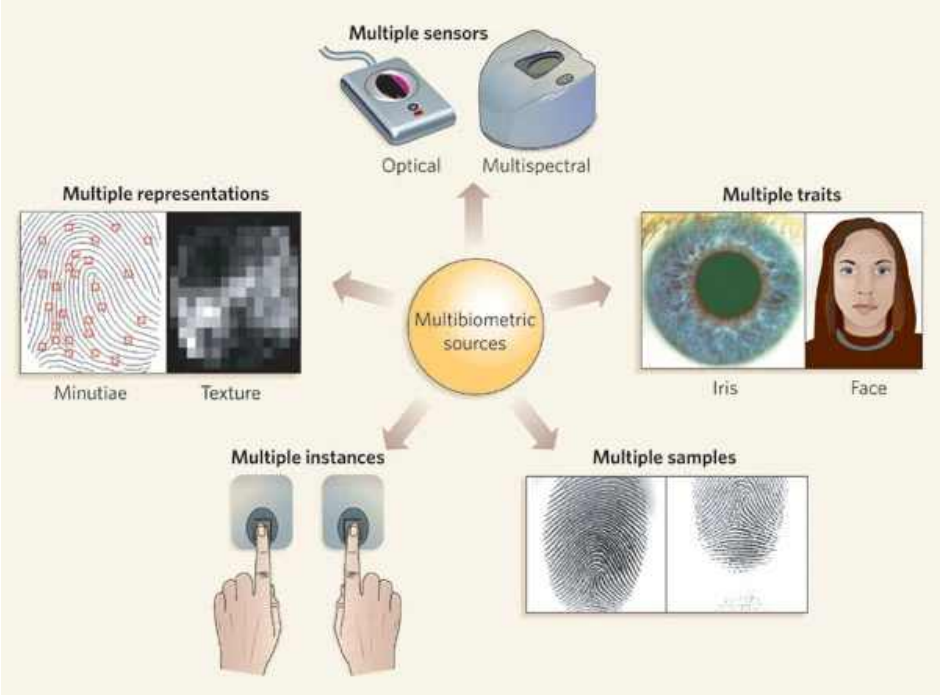
Multimodálny biometrický systém môžeme definovať biometrický systém, ktorý sa rozhoduje na základe viacerých vstupov či kombinácií vstupov a následne musí vykonať viac rozhodnutí.

Vo všeobecnosti môžeme povedať, že multimodálny systém môže využívať viac:

- senzorov - napríklad tvár a hlas, kde teda berieme do úvahy rôzne senzory, [183] ako kamera a mikrofón, alebo napríklad odtlačok prsta a podpis,
- algoritmov - v tomto prípade ide o jednu vzorku zosnímanú jedným senzorom, ktorú ale spracujú rôzne algoritmy na porovnanie s databázou, pričom môže ísť aj o rôzne algoritmy extrakcie príznakov,
- vzoriek - ide o prípad, keď napríklad tá istá tvár sa spracuje z rôznych snímok tej istej kamery/senzora (viď Obrázok 4.1) [6],
- jednotiek (pravé a ľavé oko, viac prstov jednej ruky, ukazováky oboch rúk, a podobne) - ak je zosnímaných viacero prstov tej istej ruky, ale tým istým senzorom, môže to byť aj pravé a ľavé oko, teda každá z jednotiek má vlastný model v databáze a tento prístup má zabezpečiť spoľahlivejšiu identifikáciu, ale je samozrejme

viac obťažujúci pre používateľa,

- čŕt - existujú senzory, ktoré snímajú odtlačok prsta, ale zároveň sú schopné zosnímať aj krvné riečište prsta (vylepšený senzor od firmy Hitachi, podobný tomu na Obrázku 3.11 - v tomto prípade sám senzor dodáva kombinované príznaky extrahované zo snímok z oboch senzorov), prípadne póry kože, každý zo znakov má vlastný model, spôsob extrakcie a algoritmus porovnávania príznakov.



Obr. 4.1 Príklady multimodálnych dát z rôznych senzorov, čŕt (dúhovka a tvár), vzoriek, jednotiek, reprezentácií / algoritmov / príznakov použitých na rovnakú vzorku [6].

Problémom multimodálnych systémov je, že je potrebné si zvoliť a vhodne vyladiť informačnú fúziu na rôznych vrstvách [184]:

- pred-klasifikačná vrstva:
  - na úrovni *senzorov* - senzory dodajú kombinovanú vzorku
  - na úrovni *príznakov* extrahovaných zo vzoriek - výstupom je len jedna sada príznakov

- vrstva po klasifikácii:
  - dynamická *voľba klasifikátora* - vyberie napríklad spoľahlivejší z dostupných
  - *fúzia skóre* klasifikátorov na základe:
    - skóre (vyššia hodnota, Borda count, logistická regresia)
    - abstrakcie (väčšinové hlasovanie, model znalostí o správaní, vážené hlasovanie na základe Dempsterovej-Shaferovej teórie dôkazov, pravidlo AND a pravidlo OR, a podobne)
    - merania či spoľahlivosti (neurónové siete, k-NN, SVM, rozhodovacie stromy, normalizácia + lineárna kombinácia + prahovanie, a podobne).

4.2 Príklad multimodálneho biometrického systému analýzy dát z používania klávesnice

Téma multimodálnej fúzie je podrobnejšie opísaná na prípadovej štúdii medzinárodného vedeckého výskumu, ktorý začal v roku 2015 na konferencii IWBF International Workshop on Biometrics and Forensics v Gjøviku, na ktorého programe sa zúčastnili Ing. Pleva (autor tejto práce) spolu s kolegyňou Ing. Kiktovou, vďaka výstupom z výskumu zameraného na akustickú detekciu výstrelov vo verejných priestranstvách. Počas konferencie boli oslovení Patrickom Boursom z Nórskej vedecko-technickej univerzity, ktorý pracoval na identifikácii a verifikácii používateľa na základe snímania časov pohybov kláves na klávesnici (bez snímania dynamiky stlačenia) a počas vytvárania databázy bola vytvorená pomocou webkamery aj akustická stopa. Prvým krokom bola implementácia zvykovej identifikácie [185] a neskôr aj autentifikácie používateľa na základe zvuku klávesnice [186]. Neskôr pracovali na kalibrácii, fúzii aj normalizácii skóre, aby bol vytvorený prvý multimodálny biometrický systém na detekciu používateľa na základe fúzie výsledkov analýzy časových a akustických dát z klávesnice [21].

Získané dáta o časoch z klávesnice boli použité na výpočet trvania a latencie pre všetkých 100 napísaných slov každého z 50 účastníkov. Na vytvorenie šablóny bolo použité jedno sedenie (25 slov) a krížovou validáciou boli testované zvyšné tri

sedenia (sessions). Podobne bolo testované aj použitie troch sedení na vytvorenie šablóny a iba jednej na testovanie v podobnom nastavení [187]. Výkonnosť systému bola hodnotená z hľadiska autentifikácie aj identifikácie. Šablóna používateľa pozostávala zo strednej a štandardnej odchýlky pre každé z 8 trvaní stlačenia klávesy pre jedno slovo a 7 latencií medzi klávesami slova "password"[188].

Použitá metrika vzdialenosti bola Scaled Manhattan Distance (SMD), pretože ide o najvýkonnejšiu metriku vzdialenosti podľa Killourhy a Maxion [189]. Ak je šablóna označená $T = ((\mu_1, \sigma_1), (\mu_2, \sigma_2), \ldots, (\mu_{15}, \sigma_{15}))$ a vstup testu je označený $t = (t_1, t_2, \ldots, t_{15})$, potom sa SMD rovná:

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

V prístupe pre akustickú analýzu sme zvolili metódy úspešne otestované pri podobnej úlohe akustickej analýzy zvukových udalostí ako MFCC (Mel-Frequency Cepstral Coefficients) príznaky a Hidden Markov Model (HMM), pričom sme ale použili jeden až sedem stavové ergodické modely (možný aj návrat do ľubovoľného predošlého skrytého stavu) [190]. Už prvé výsledky akustickej analýzy ukázali zaujímavé zistenia pri úlohe identifikácie:

1. Najvyššiu mieru presnosti identifikácie (99,35%) dosiahli modely, ktoré boli trénované na 75 náhodne vybraných slov/realizácií. Pri časovej analýze bolo dosiahnutých pre jednu testovaciu sadu maximálne 64,6% presnosti.

2. Pre prax realistickejší scenár s použitím 25 trénovacích slov bola presnosť identifikácie približne na úrovni 90,62% po krížovej validácii. Pri časovej analýze to bolo iba 56,7%.

3. Najlepší výsledok 92,91% pri trénovaní 25 slovami bol dosiahnutý, ak bola pri trénovaní použitá nahrávka v poradí druhého sedenia. A najhoršia zase (88,93%) pri trénovaní posledným sedením, kde bolo napísaných 25 slov. To by mohlo znamenať, že pri prvom sedení sa používatelia ešte zoznamujú so systémom a najlepší stereotyp dosiahnu pri druhom sedení. Pri štvrtom už pravdepodobne je stereotyp písania najviac odlišný od prvých sedení - používateľ už píše dané slovo

napríklad neprirodzene rýchlo, alebo sa už tešil na splnenie úlohy a nesústredil sa tak na slová samotné.

4. V úlohe identifikácie dosahovala akustická analýza výrazne lepšie výsledky než časová analýza.

4.2.1 Kalibrácia pri akustickej analýze používania klávesnice

Pri úlohe verifikácie či autentifikácie proklamovanej / deklarovanej identity vznikol problém, ak malo byť skóre získané z akustickej analýzy a porovnania s uloženým modelom prahované podľa presne stanoveného prahu na binárny klasifikátor prijatia či zamietnutia proklamovanej identity. Skóre z akustickej analýzy totiž bolo silne závislé od testovacej nahrávky. Bolo vyskúšaných veľa spôsobov normalizácie skóre (podľa dĺžky, priemernej amplitúdy, tichých oblastí, redukcie šumu a iné), ale nič neprinieslo očakávané výsledky a pri trénovaní 75 slovami a testovaní 25 slovami bol EER (Equal Error Rate) približne na úrovni 19,1% voči 11,7% pri použití časovej analýzy.

Nakoniec bola úspešne využitá autorova idea kalibrácie zvukovej nahrávky pomocou univerzálneho modelu, pričom bol inšpirovaný prístupom používaným pri identifikácii rečníka podľa hlasu, kde sa používa univerzálny background model (UBM) pozadia. Tu bolo skóre normalizované s použitím porovnania so skóre kalibračného modelu. V praxi by daný model mohol byť nahraný pri inštalácii systému a klávesnice, pričom by zohľadňoval lokálne akustické podmienky, zvuk danej klávesnice a podobne. S využitím kalibrácie bola dosiahnutá miera chybovosti EER 11,6% čo bolo dokonca lepšie ako pri časovej analýze. Pri viac realistickom modeli, kde sa použilo 25 slov na trénovanie, dosiahla lepšie výsledky časová analýza pri EER 14,4% voči 16,6% pri kalibrovanej akustickej analýze.

4.2.2 Fúzia výsledkov časovej a akustickej analýzy používania klávesnice

Ako už ale bolo povedané, finálny problém multimodálnych systémov je fúzia skóre z analýzy rôznych modalít. Lineárnou kombináciou, kalibráciou a prahovaním skóre sa

podarilo autorovi tento multimodálny systém vyladiť na úroveň, ktorá znížila výsledné EER skoro na polovicu.

Na porovnanie výsledkov sme použili široko uznávaný Bosaris[1] toolkit [191] používaný na porovnanie výkonnosti systémov na identifikáciu / autentifikáciu rečníka [192] alebo Query by Example Search on Speech - teda vyhľadávanie v reči podľa akustickej ukážky [193, 194]. Polovicu testovacej sady (50 slov) sme použili ako vývojovú podmnožinu pre modelovanie parametrov fúznych funkcií a aplikovali sme ju na zvyšok testovacej sady. Potom sme kvôli krížovej validácii vystriedali všetky kombinácie skupín a priemerný EER je uvedený v Tabuľke 4.1.

počet test. slov	Časová analýza EER	Kalibrovaná audio EER	Navrhnutá fúzia EER	Bosaris najlepšia fúzia EER
25	9,91%	8,99%	**4,65%**	4,71%
75	12,08%	14,34%	7,54%	**7,30%**

Tabuľka 4.1 Výsledky najlepšieho výsledku pre úlohu autentifikácie v EER pri použití *najlepšieho akustického modelu* a *fúzie* s príslušným časovým vzorom (rovnaká trénovacia / testovacia session) využitím lineárnej fúzie a najlepšej fúzie z balíka Bosaris toolkit.

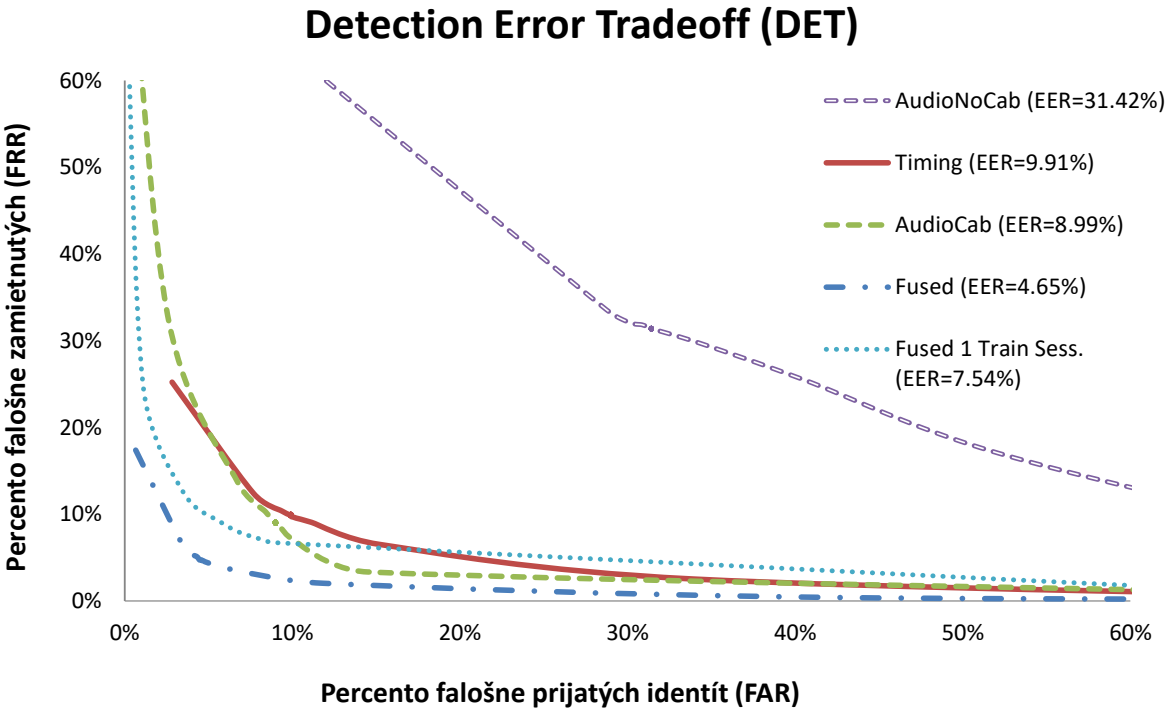
Treba poznamenať, že pri využití kalibrácie jedným náhodným používateľom boli testy vykonané na zvyšných 49 používateľoch a tak priemerné výsledky nemusia sedieť s výsledkami časovej analýzy bez kalibrácie.

4.2.3 Efekt použitia multimodálnej časovej a akustickej analýzy používania klávesnice

Z údajov prezentovaných na Obrázku 4.2 je zrejmé, že autorom navrhnutá fúzia časovej analýzy a kalibrovaných výsledkov zvukovej analýzy poskytuje lepšie výsledky ako ostatné porovnávané systémy a takisto, že navrhnutý spôsob fúzie je postačujúci na výrazné zlepšenie výsledkov multimodálneho systému (4,65% EER) v porovnaní

[1] `http://sites.google.com/site/bosaristoolkit`

s jedno modálnym - čisto akustickým (8,99% EER) alebo systémom postaveným len na časovej analýze (9,91% EER). V prípade, že chceme použiť len 25 slov na trénovanie, je schopný multimodálny systém dosiahnuť 7,30% EER pričom unimodálny systém založený na časovej analýze 12,08% EER a akustický systém s kalibráciou 14,34% EER.



Obr. 4.2 DET krivka výsledkov autentifikácie pre 3 tréningové sedenia (75 slov) pomocou zvukovej analýzy bez kalibrácie (AudioNoCab), iba s použitím časovacej analýzy (Timing), kalibrovaných zvukových výsledkov (AudioCab), fúzia kalibrovaného kalibrovaných výsledkov zvukovej analýzy a výsledkov časovej analýzy (Fused), a nakoniec to isté pre 1 trénovaciu (25 slov) a 3 testovacie sedenia - sessions (Fused 1 Train Sess.).

Počas následných experimentov s daným systémom boli testované aj rôzne klávesnice, a pokiaľ ide o časovú analýzu, ukázalo sa, že zmena hardvéru nemá zásadný vplyv na výkon systému pri úlohe autentifikácie. V ďalšom výskume s NTUT Gjøvik uvažujeme aj o skúmaní vplyvu rôznych šumov pozadia počas písania a fúziu s analýzou dynamiky práce s počítačovou myšou [22].

V súčasnosti spolupracujeme s kolegami z katedry KPI FEI TU na tvorbe databázy,

ktorá by obsahovala pre daný problém až 5 modalít - časovanie kláves, zvuk klávesnice, obraz z kamery nad klávesnicou, EMG dáta z MYO náramku [195] a gyroskopických dát o pohybe zápästia z MYO náramku.

Kapitola 5

Zabezpečenie biometrických údajov a systémov

Jednou z kľúčových vlastností biometrických systémov je, ako dokážu zabezpečiť citlivé osobné údaje s ktorými pracujú, ktorými sú okrem informácií o vašej identite (meno, priezvisko, dátum narodenia, bydlisko a podobne) hlavne vaše biometrické dáta. Tieto dáta sa môžu ukladať do databázy v rôznej podobe a ich zabezpečenie je jedným z kľúčových prvkov spoľahlivosti aj dôveryhodnosti celého biometrického systému.

5.1 Zneužitie biometrických dát

Jednou z najväčších obáv pri biometrických systémoch je krádež identity - teda použitie databázy používateľov na autentifikovanie sa nielen do daného biometrického systému, ale hlavne aj do iných, ktoré daný používateľ používa a sú pre neho omnoho dôležitejšie ako systém, z ktorého k úniku dát došlo ako napríklad banka, prístup do databázy fotiek, založenie úveru v cudzom mene, či iné narušenie súkromia.

Biometrický systém ako celok je možné napadnúť v každom jeho bloku ako je snímanie vzorky, extrakcia príznakov, prenos dát, databáza príznakov či vzorov, porovnávací algoritmus či len v bode prenosu / zobrazeniu konečného binárneho rozhodnutia či je autor oprávnený na vstup alebo nie.

5.2 Možnosti zabezpečenia biometrických dát

Jednou možnosťou je zabezpečiť všetky časti systému silným šifrovacím mechanizmom [196], ktorý zamedzí ovplyvňovaniu či kopírovaniu prenášaných či spracovávaných dát.

Inou koncepciou je silná dôveryhodná národná autorita, ktorá jediná by ukladala aj porovnávala získané biometrické dáta a poskytovala výsledok inštitúcii, ktorej by ste dali povolenie na spracovanie vašich dát - snímanie a odoslanie biometrických dát na porovnanie do centrálneho autentifikačného systému [197].

Dôležitým rozdielom je, že pri tomto koncepte lokálna inštitúcia nemá právo ukladať vaše biometrické dáta ani žiadne s nimi spojené modely či vzory viažúce sa na vašu identitu. Samozrejme vyššie nároky sú na overenie spoľahlivosti prístupu danej inštitúcie do centrálneho systému, zabezpečenie celého prenosu. Centrálny autentifikačný register by napríklad v prípade poruchy alebo nedostupnosti dátového prenosu odstavil všetky autentifikačné systémy v zemi.

5.3 Moderné trendy v oblasti bezpečnosti biometrických systémov ako celku

Je technologickým trendom decentralizovať verifikačné procedúry aj preto, aby nemohlo dôjsť k narušeniu integrity databázy, napríklad vložením falošných vzoriek. Jednou z technologických výziev je integrácia blockchain technológie do biometrických systémov [198, 199], kde každá transakcia je chránená vložením digitálneho podpisu, ktorý je nemožné bez poškodenia štruktúry denníka zmazať. Tým pádom je možné každú manipuláciu vystopovať. Spolu s metódami steganografie a šifrovania [200] sa navrhujú aj moderné medicínske systémy na spoľahlivú identifikáciu pacienta na základe jeho biometrických znakov [201].

5.4 Biometrický systém využívajúci užitočne skresľujúce transformácie

Ďalšou zaujímavou oblasťou je aj nový smer zrušiteľnej / odvolateľnej biometrie (cancelable [202] alebo revocable biometrics [203]), kde je biometrická vzorka po zosnímaní odfiltrovaná špecifickou matematickou procedúrou používajúcou množinu skresľujúcich (distortion) parametrov, ktorá prípadne vyžaduje nejaký tajný sekundárny vstup (napríklad PIN zadaný používateľom, ktorý systém nikde neukladá). Následne je výstup z nej spracovávaný bežným biometrickým algoritmom na vytvorenie modelu/vzorky a uložený do databázy.

Táto procedúra však musí zabezpečiť, že ak vzorky z databázy uniknú, tak nebudú v iných systémoch použiteľné (kvôli neznámej množine skresľujúcich parametrov, tajného sekundárneho vstupu, či aj pre nový systém neznámemu algoritmu skreslenia), ale zároveň, že vzorka/model nebude znehodnotený natoľko, že by bol nepoužiteľný na algoritmy verifikácie či identifikácie v pôvodnom systéme. Nejde teda o proces podobný šifrovaniu, ktorý má zabezpečiť, aby zašifrované dáta vyzerali ako náhodné.

Kapitola 6

Biometrické aplikácie v európskom právnom priestore

Hlavnými európskymi informačnými systémami, ktoré využívajú biometriu, sú:

- Visa informačný systém - Visa Information System (VIS),
- Schengenský informačný systém - Schengen Information System (SIS II)
- a EURODAC.

Tieto systémy sú v kompetencii Európskej agentúry pre prevádzkové riadenie rozsiahlych informačných systémov v oblasti slobody pohybu, bezpečnosti a spravodlivosti - European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (euLISA)[1]. Táto agentúra je podľa nedávnych právnych predpisov tiež poverená vývojom a prevádzkou európskeho systému cezhraničného vstupu / výstupu pre bezvízový styk občanov tretích krajín (European Entry/Exit System - EES[2]), európskeho systému autorizácie cestovných informácií pre bezvízový styk (visa-exempt non-EU nationals) pre momentálne 62 krajín mimo EÚ (European Travel Information Authorisation System - ETIAS[3]) a európskeho informačného systému registrov trestov pre štátnych príslušníkov tretích krajín, ale aj občanov krajín

[1] https://www.eulisa.europa.eu/Pages/default.aspx

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

[3] https://www.schengenvisainfo.com/etias/

EÚ (European Criminal Record Information System for Third Country Nationals - ECRIS-TCN).

Databázy týchto biometrických systémov sú centralizované a prísne strážené, pričom členské štáty majú lokálne kópie len biometrických vzorov/modelov (templates) nie čistých dát (fotiek, či odtlačkov prstov a podobne). V prípade potreby kontaktujú národné kontaktné centrum pre daný systém so špecifickou požiadavkou. V tabuľke 6.1 a 6.2[4] môžete vidieť, kto je oprávnený do daných databáz pristupovať.

Prístup oprávnených osôb z odd.:	SIS	VIS	EuroDac	EES	ETIAS
udeľovanie víz (konzul) a imigračné	•	•		•	
pohraničné kontroly (pozemné, pobrežné, vzdušné, letiskové a iné)	•	•	•	•	•
udeľovanie azylu	•	•	•		
polícia	•				
colné a kontrola tovaru	•				
justícia	•				
register áut, lodí a lietadiel	•				
osobní prepravcovia		•		•(1)	•(2)

Tabuľka 6.1 Tabuľka prístupových práv do centrál biometrických databáz európskeho spoločenstva. (Prepravcovia majú prístup iba k rozhraniu potvrdzujúcemu platnosť víz(1) a ETIAS(2) autorizácie cestujúceho.)

6.1 Vízový informačný systém

Vízový informačný systém - Visa Information System (VIS)[5] slúži hlavne na uchovávanie a verifikáciu identít občanov tretích krajín (mimo Európskej únie), kde sa registrujú odtlačky prstov (všetkých 10) a odtlačok tváre - takzvaný „mugshot“. Spracuje približne

[4] `https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190205_security-union-eu-information-systems_en.pdf`

[5] `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14517`

Prístup v špecifickom rozhraní:	SIS	VIS	EuroDac	EES	ETIAS
iné národné autority		•		•	•
Europol	•	•	•	•	•
Eurojust	•				
Európska hraničná a pobrežná stráž	•	•	•		•
Európska podporná azylová kancelária			•		

Tabuľka 6.2 Tabuľka prístupových práv do centrál biometrických databáz európskeho spoločenstva po splnení špeciálnych podmienok týkajúcich sa hľadanej osoby.

60 miliónov žiadostí o víza ročne (za rok 2018). Podľa aktuálnej regulácie sa neodoberajú odtlačky prstov deťom mladším ako 12 rokov, ale je v príprave už nová regulácia na snímanie odtlačkov prstov deťom od 6 rokov.[6]

Hlavným účelom vízového informačného systému (VIS) je zlepšiť vykonávanie spoločnej vízovej politiky, konzulárnej spolupráce a konzultácií medzi ústrednými vízovými orgánmi prostredníctvom:

- uľahčenia postupu pri podávaní žiadosti o vízum;
- zabránenia „nakupovaniu víz“;
- uľahčenia boja proti podvodom;
- uľahčovania kontrol na hraničných priechodoch vonkajších hraníc a na vnútroštátnych územiach;
- pomoci pri identifikácii osôb, ktoré nespĺňajú požiadavky na vstup, pobyt alebo pobyt na štátnych územiach;
- uľahčenia uplatňovania nariadenia Dublinského dohovoru - hlavne identifikovanie krajiny, ktorá je zodpovedná za preskúmanie žiadosti o azyl štátneho príslušníka tretej krajiny, a za posúdenie uvedenej žiadosti;

[6] `https://publications.jrc.ec.europa.eu/repository/bitstream/JRC110173/jrc_fingerprint_children_elderly_study_v.final.pdf`

- prispievania k predchádzaniu hrozbám pre vnútornú bezpečnosť krajín EÚ.

Každý súbor žiadosti o víza je vo VIS uložený najviac päť rokov. Iba krajina, ktorá záznam vytvorila, má právo na doplnenie alebo vymazanie údajov, ktoré do VIS vložila. Pri hraničnej kontrole majú pracovníci prístup do VIS za účelom overenia totožnosti osoby a/alebo pravosti víza a/alebo toho, či daná osoba spĺňa požiadavky na vstup, pobyt v EÚ alebo pobyt na vnútroštátnom území. Ak sa na základe tohto vyhľadávania vo VIS nájdu údaje o držiteľovi víza, príslušné orgány môžu nahliadnuť do určitých údajov v súbore so žiadosťou.

6.2 Schengenský informačný systém

Tento systém slúži na výmenu informácií o trestnej činnosti, jej objektoch a jej páchateľoch, pričom sa v nejakej forme zdieľajú aj ich biometrické dáta. Keďže v rámci Schengenského priestoru je voľný pohyb ľudí a tovaru, je dôležité aby, krajiny boli schopné medzi sebou rýchlo zdieľať informácie o ukradnutých autách, tovaroch, či hľadaných osobách. Do databázy sa evidujú ale aj stratené osoby alebo tovar, údaje o stratených deťoch, teroristoch, falšovaných/odcudzených identitách, bezpečnostné previerky a podobne.

Do systému má prístup 30 krajín (štáty EÚ, Veľká Británia, a asociované krajiny EÚ - Švajčiarsko, Nórsko, Island, Lichtenštajnsko) plus Europol a Eurojust, pričom eviduje informácie o EÚ občanoch aj občanoch mimo EÚ.

V SIS II sa zdieľajú okrem odtlačkov prstov všetkých prstov aj čiastočné odtlačky prstov, v Amerike nazývané latent fingerprints, v Európe ich nazývame aj fingermarks. Pri odtlačkoch prstov je možné mať k dispozícii kompletný odtlačok, ktorý sa sníma väčšinou prerolovaním prsta namočeného v atramente cez papier (rolled) alebo len priložením na skener (flat). Zdieľajú sa aj odtlačky dlaní (palm prints) prípadne fotky tvárí (facial images - mugshots) či DNA.

Podľa štatistických údajov agentúry bolo v roku 2019 nájdených 283 713 zhôd medzi hľadanou osobou a položkou v databáze pri 6,6 miliónoch prístupov ročne[7].

[7]SIS II - 2019 - Statistics - factsheet `doi.org/10.2857/579595` novšie je možné nájsť na `https:`

Začiatkom roku 2018 agentúra eu-LISA úspešne spustila platformu SIS Automated Fingerprint Identification System (AFIS). SIS AFIS spĺňa požiadavky komunity orgánov činných v trestnom konaní v rámci Európskeho spoločenstva a poskytuje na úrovni EÚ pokročilý nástroj umožňujúci identifikáciu hľadaných osôb iba pomocou ich odtlačkov prstov.

6.3 EuroDac - Európska daktyloskopická databáza

EuroDac je databáza cudzincov žiadajúcich o azyl v krajine EÚ (občania mimo krajín EÚ). Táto databáza je podľa jej názvu vyslovene biometricky zameraná, keďže eviduje hlavne odtlačky prstov. Podľa jej štatistických údajov za rok 2019[8] EuroDac spracoval cca 916 tisíc súborov odtlačkov prstov z čoho 592,69 tisíc súborov odtlačkov zo žiadostí na medzinárodnú ochranu ľudí 14 a viac rokov (kategória 1), 111,76 tisíc ľudí prichytených pri nelegálnom prestupe hraníc členských štátov EÚ (opäť len 14 a viac ročných) - 2. kategórie, 211,6 tisíc ľudí nad 13 rokov nájdených ilegálne na území členského štátu EÚ (kategória 3), 449 súborov odtlačkov prstov zaslaných orgánmi činnými v trestnom konaní členského štátu na účely prevencie, odhaľovania alebo vyšetrovania teroristických trestných činov alebo iných závažných trestných činov (kategória 4). Europol nepredložil žiadne odtlačky prstov (kategória 5) v roku 2019.

6.4 Zintenzívnenie cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti (prümské rozhodnutie)

Predchodcom centrálnych informačných systémov bolo takzvané rozhodnutie alebo *dohovor z Prüm*[9], ktoré vzniklo v roku 2005 a zaväzovalo signatárske krajiny (Belgicko,

//www.eulisa.europa.eu/our-publications/reports.

[8]Eurodac - 2019 Statistics - factsheet http://doi.org/10.2857/77253 novšie je možné nájsť na https://www.eulisa.europa.eu/our-publications/reports.

[9]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:jl0005

Nemecko, Španielsko, Francúzsko, Luxembursko, Holandsko a Rakúsko) k spolupráci policajných a justičných orgánov v boji proti terorizmu a cezhraničnej trestnej činnosti. V rámci neho vznikli národné databázy a mechanizmy cezhraničného prístupu k nim na báze P2P (peer to peer - jeden na jedného). Poskytovali prístup k DNA profilom, daktyloskopickým údajom (odtlačky prstov rôzneho druhu), a evidencii vozidiel. Okrem biometrických dát poskytuje sieť údaje v súvislosti s významnými podujatiami, informácie s cieľom predchádzať teroristickým trestným činom a ďalšie opatrenia na zintenzívnenie cezhraničnej policajnej spolupráce.

Čo sa týka osobných údajov, tak tie je možné poskytnúť len vtedy, ak sa dotknuté osoby považujú za hrozbu pre verejný poriadok a bezpečnosť alebo ak panuje presvedčenie, že pri podujatiach spáchajú trestný čin. Tieto údaje možno použiť len v súvislosti s podujatím, na ktoré boli poskytnuté, a po tom, čo poslúžili svojmu účelu, ale najneskôr po roku od ich dodania, sa vymažú[10].

6.5 Spoločná európska služba porovnávania biometrických údajov (CS-sBMS)

Nová služba, na ktorej intenzívne pracujú rôzne EÚ inštitúcie pod názvom CS-sBMS Central SIS Shared Biometric Matching Service vznikla nariadením Európskeho parlamentu a Európskej rady 2019/817 a 2019/818 z mája 2019[11]. Pričom pod Central SIS sa myslí centrálna databáza Schengenského informačného systému, Backup SIS je jej záložná kópia a National SIS sú jej národné kópie obsahujúce len modely a vzory, nie čisté dáta. CS-sBMS má však poskytovať aj unifikované rozhranie k vyhľadávaniu v databázach VIS, EuroDac, EES a ECRIS, ale až po dokázaní, že v národnom registri záznam nebol nájdený a že je právny dôvod vyhľadávať v spomenutých databázach.

[10] `https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=LEGISSUM:jl0005&from=EN`

[11] `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817`

Kapitola 7

Štandardizácia v biometrii

Potreba štandardizácie prichádza pri každom technologickom systéme, ktorý sa rozšíri do viacerých krajín a poskytuje ho viacero výrobcov. Biometrické systémy od svojho počiatku patria k systémom, ktoré okrem zabezpečenia dát požadovali aj ich zdieľanie na forenzné účely. Napriek tomu štandardizácia je stále veľkou výzvou, pretože jednotlivé krajiny sa držia lokálnych štandardov kvôli spätnej kompatibilite národných systémov s historickými dátami.

Vďaka integrácii Slovenska do Európskej únie a Schengenského priestoru je novou výzvou aj celoeurópsky systém kontroly identity pri vstupe a opúšťaní tohoto priestoru, hlavne pre obyvateľov z iných krajín.

V súčasnosti existuje komisia ISO/IEC JTC 1/SC 37[1] [204], ktorá má na starosti štandardizáciu všeobecných biometrických technológií a podporu výmeny údajov (interoperability) medzi aplikáciami a systémami. Pracuje v oblasti štandardizácie súborov; návrh spoločných používateľských rozhraní biometrických aplikácií; formáty výmeny biometrických údajov; súvisiace biometrické profily / vzory / modely; uplatňovanie porovnateľných hodnotiacich kritérií na biometrické technológie; metodiky testovania a podávania správ o výkonnosti a cezhraničné a spoločenské aspekty.

Medzi medzinárodné štandardizačné orgány patria [205]:

- ISO - International Organization for Standardization,
- IEC - International Electrotechnical Commission and

[1] `https://www.iso.org/committee/313770.html`

- ITU - International Union of Telecommunications.

Na regionálnej (nadnárodnej) úrovni poznáme napríklad [205]:

- ETSI - European Institute for Standardization in Telecommunications,
- CENELEC - European Committee for Standardization in Electrical Engineering,
- CEN - Comité Européen de Normalisation - ang. European Committee for Standardization.

Na národnej úrovni sú známe [205]:

- BSI - British Standards Institution,
- ANSI - American National Standards Institute,
- DIN - Deutsche Industrie-Norm,
- GOST (Gosstandart) - vydávaný Euroázijskou radou pre normalizáciu, metrológiu a certifikáciu (EASC) Spoločenstvo nezávislých štátov - štáty z bývalého Zväzu sovietskych socialistických republík (ZSSR),
- JISC - Japanese Industrial Standards Committee,
- Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky - vydáva Slovenské technické normy: STN, alebo
- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví - vydáva České technické normy: ČSN (pôvodne československá státní norma).

Zaujímavosťou je, že v niektorých štátoch vydávajú normy výhradne štátne inštitúcie a úrady a niekde aj záujmové združenia ako napríklad W3C[2] medzinárodné združenie, ktoré sa zaoberá tvorbou štandardov pre prostredie Worl Wide Web a vzniklo na akademickej pôde MIT - Massachusettského technologického inštitútu v spolupráci s Európskou organizáciou pre jadrový výskum CERN a s podporou Európskej komisie EC a americkej Agentúry pre výskum pokročilých obranných projektov DARPA [206].

[2] `http://www.w3.org`

Kapitola 8

Záver

V tejto učebnici je zhrnutá problematika biometrických systémov pre rozhranie človek - stroj, zhodnotením súčasných technológií, načrtnutím moderných trendov a bude určite inšpiráciou pre získanie prehľadu v odbore biometrických systémov aj pre skúmanie nových smerov a poznatkov.

Práca sa nezaoberá inými odbormi merania živých systémov ako rastliny či živočíchy, na čo sme pri skúmaní pojmu biometria tiež narazili. Podobne oblasť forenznej vedy, ktorá skúma mnoho ďalších stôp po živých organizmoch a hľadá ich živé či neživé zdroje by predstavovala príliš široký záber, a preto sa práca sústredila na témy, ktorým sa autor počas svojej vedeckej práce podrobnejšie venoval.

Práca poskytuje dôležitý prínos v oblasti biometrie v rozhraní človek - stroj a vedecký prínos prezentovaný hlavne v oblasti multimodálnej biometrie poskytuje výborný základ na ďalšie budovanie takýchto systémov a medzinárodnej spolupráce na pracovisku autora alebo v iných spolupracujúcich organizáciách.

Poznatky využité pri výskume a prezentované v tejto práci sú výsledkom dlhoročnej práce autora v oblasti spracovania signálov [194], bezpečnosti/biometrie a rozhrania človek - stroj [207] aj človek - robot (hlavne rečového rozhrania) [208, 209], detekcie akustických signálov [210], spracovania rečových dát [211] a vychádzajú z najvýznamnejších publikácií autora, ako napríklad:

- Pleva, M., et al.: Improving static audio keystroke analysis by score fusion of acoustic and timing data, 2017. In: Multimedia Tools and Applications, 76 (24),

p. 25749–25766, 2017. (IF = 1.346, CC journal, Q1),

- Vavrek, J., et al.: Weighted Fast Sequential DTW for Multilingual Audio Query-by-Example Retrieval, 2018. In: Journal of Intelligent Information Systems, 51 (2), p. 439-455, (IF = 1.294, CC journal, Q1),

- Lojka, M., Pleva, M., et al.: Efficient acoustic detector of gunshots and glass breaking. In: Multimedia Tools and Applications, 75 (17), p. 10441-10469, 2016, (IF = 1.346, CC journal, Q1),

- Ondáš, S., et al.: Service Robot SCORPIO with Robust Speech Interface, In: International Journal of Advanced Robotic Systems. Vol. 10 (3), 11p, Open Access, ISSN 1729-8806, 2013. (IF = 0.821, CC journal, Q3),

- Ondáš, S., et al.: Pediatric Speech Audiometry Web Application for Hearing Detection in the Home Environment, 2020, Electronics, 9 (6), p. 994. (IF = 2.412, CC journal, Q2 JCR), výsledok spolupráce s UPJŠ v Košiciach,

- Shivarov, N., et al.: A Case Study on Human-Robot Interaction of the Remote-Controlled Service Robot for Elderly and Disabled Care. (2019) Computing and Informatics, 38 (5), pp. 1210-1236. (IF = 0.496, CC journal, Q3), výsledok medzinárodnej spolupráce s Bulharskou Akadémiou vied v Sofii,

- Liao, Y.F., et al.: Formosa Speech in the Wild Corpus for Improving Taiwanese Mandarin Speech Enabled Human-Computer Interaction, (2020) Journal of Signal Processing Systems, 92 (8), pp. 853-873. (IF = 1.013, CC journal, Q3), výsledok medzinárodného projektu s National Taipei University of Technology,

- Pleva, M., et.al.: Implementing English speech interface to Jaguar robot for SWAT training. In: SAMI 2017: IEEE, pp. 105-110, prvotná publikácia výsledkov mesačnej stáže v CAVS, MSU, US,

- Bours, P., Kiktová, E., Pleva, M.: Static Audio Keystroke Dynamics, IEEE MCSS conference 2015, *best paper of the conference*, LNCS Vol. CCIS-566, pp. 159-169, 2015,

- Pleva, M., Juhár, J.: TUKE-BNews-SK: Slovak Broadcast News Corpus Construction and Evaluation, LREC 2014, Reykjavik, ELRA, pp. 1709-1713, 2014 - súhrn prínosov autora v oblasti rečových databáz v slovenčine.

Poznatky z tejto práce sú využité vo vyučovaní predmetov Biometrické systémy bezpečnosti, ale aj Operačné systémy (spôsoby autentifikácie používateľa a prístupových práv) a Princípy počítačového inžinierstva, ktoré autor takisto zabezpečuje.

Táto vysokoškolská učebnica bude ďalej rozširovaná a dopĺňaná do formy monografie vhodnej ako výukový materiál pre predmet Biometrické systémy bezpečnosti, ktorý autor garantuje, zabezpečuje po stránke prednášok, cvičení aj spolupráce s praxou a medzinárodnej spolupráce. V rámci prednášok pravidelne pozýva expertov z firiem ako napríklad Innovatrics, Crayonic, medzinárodnej vedeckej inštitúcie Joint Research Center (DG-JRC) Directorate E - Space, Security and Migration, Cyber and Digital Citizens' Security Unit európskej komisie, Slovenskej akadémie vied a samozrejme aj Norwegian University of Science and Technology.

V najbližšej budúcnosti autor pracuje v spolupráci s inými pracoviskami univerzity TUKE (KPI, KKUI, KMTI) [212, 213], Norwegian University of Science and Technology na pokračovaní výskumu a Joint Research Center v oblasti multimodálnej biometrie a jej využitia v dobe pandémie, dištančnej výuky, bezdotykových systémov a hľadania nových spôsobov merania a vyhodnocovania rôznych biometrických znakov.

Literatúra

[1] WG 4 Convener. Standing Document 14-4 (SD 14-4) January 2010, Roadmap for SC 37/WG 4 — Biometric Functional Architecture and Related Profiles. *ISO/IEC JTC 1/SC 37 N 3701*, pages 1–6, 2010.

[2] AM Curiel López de Arcaute and J Granell Navarro. La huella de oreja como método de identificación. *Acta Otorrinolaringológica Española*, 57(7):329 – 332, 2006.

[3] Kien Nguyen, Clinton Fookes, Raghavender Jillela, Sridha Sridharan, and Arun Ross. Long range iris recognition: A survey. *Pattern Recognition*, 72:123–143, 2017.

[4] David Zhang, Feng Liu, Qijun Zhao, Guangming Lu, and Nan Luo. Selecting a reference high resolution for fingerprint recognition using minutiae and pores. *IEEE Transactions on Instrumentation and Measurement*, 60(3):863–871, 2011.

[5] David Mulyono and Horng Shi Jinn. A study of finger vein biometric for personal identification. In *2008 International Symposium on Biometrics and Security Technologies*, pages 1–8, 2008.

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

[7] Miloš Oravec and Ľuboš Omelina. *Biometria – učebné texty*. RT systems, 2013. ISBN: 978-80-970519-6-9.

[8] Marek Loderer and Jarmila Pavlovičová. *Biometria – Rozpoznávanie ľudských tvárí*. FELIA s.r.o., 2016. ISBN 978-80-89824-06-9.

[9] Dušan Levický. *Základy kybernetickej bezpečnosti*. Elfa, Košice, 2020.

[10] Chang-Tsun Li. Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 5(2):280–287, 2010.

[11] Pavol Partila, Jaromir Tovarek, Gokhan Hakki Ilk, Jan Rozhon, and Miroslav Voznak. Deep learning serves voice cloning: How vulnerable are automatic speaker verification systems to spoofing trials? *IEEE Communications Magazine*, 58(2):100–105, 2020.

[12] Yomna Safaa El-Din, Mohamed N Moustafa, and Hani Mahdi. Deep convolutional neural networks for face and iris presentation attack detection: survey and case study. *IET Biometrics*, 9(5):179–193, 2020.

[13] Abhinav Kumar and Sanjay Kumar Singh. Recent advances in biometric recognition for newborns. *The Biometric Computing: Recognition and Registration*, page 235, 2019.

[14] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1):4–20, 2004.

[15] Yi Chen and Jean-Christophe Fondeur. Biometric algorithms. In Stan Z. Li and Anil K. Jain, editors, *Encyclopedia of Biometrics*, pages 156–161. Springer US, Boston, MA, 2015.

[16] Metod Rybár. Biometrics - introduction to biometrics. Innovatrics, s.r.o., 2020. Innovatrics Academy e-learning course `https://learn.innovatrics.com`.

[17] Javier Hernandez-Ortega, Javier Galbally, Julian Fierrez, Rudolf Haraksim, and Laurent Beslay. Faceqnet: Quality assessment for face recognition based on deep learning. In *2019 International Conference on Biometrics (ICB)*, pages 1–8. IEEE, 2019.

[18] Javier Galbally, Rudolf Haraksim, Pasquale Ferrara, Laurent Beslay, and Elham Tabassi. Fingerprint quality: Mapping nfiq1 classes and nfiq2 values. In *2019 International Conference on Biometrics (ICB)*, pages 1–8. IEEE, 2019.

[19] Stan Z. Li and Anil Jain, editors. *ROC Curve*, pages 1131–1131. Springer US, Boston, MA, 2009.

[20] Naser Damer, Alexander Opel, and Alexander Nouak. Cmc curve properties and biometric source weighting in multi-biometric score-level fusion. In *17th International Conference on Information Fusion (FUSION)*, pages 1–6. IEEE, 2014.

[21] Matúš Pleva, Patrick Bours, Stanislav Ondáš, and Jozef Juhár. Improving static audio keystroke analysis by score fusion of acoustic and timing data. *Multimedia Tools and Applications*, 76(24):25749–25766, 2017.

[22] Soumik Mondal and Patrick Bours. A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing*, 230:1–22, 2017.

[23] Martin D Gibbs. Biometrics: body odor authentication perception and acceptance. *ACM SIGCAS Computers and Society*, 40(4):16–24, 2010.

[24] Revathi Rajan, N Fakhuruddin, N Hassan, and M Nasimul. Chemical fingerprinting of human body odor: an overview of previous studies. *Malaysian Journal of Forensic Sciences*, 4(1):33–38, 2013.

[25] Avinash Kumar Singh, Piyush Joshi, and Gora Chand Nandi. Face recognition with liveness detection using eye and mouth movement. In *2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014)*, pages 592–597. IEEE, 2014.

[26] Yasar Abbas Ur Rehman, Lai Man Po, and Mengyang Liu. Livenet: Improving features generalization for face liveness detection using convolution neural networks. *Expert Systems with Applications*, 108:159–169, 2018.

[27] Enas A Raheem, Sharifah Mumtazah Syed Ahmad, and Wan Azizun Wan Adnan. Insight on face liveness detection: A systematic literature review. *International Journal of Electrical and Computer Engineering*, 9(6):5865, 2019.

[28] Ishan Manjani, Snigdha Tariyal, Mayank Vatsa, Richa Singh, and Angshul Majumdar. Detecting silicone mask-based presentation attack via deep dictionary learning. *IEEE Transactions on Information Forensics and Security*, 12(7):1713–1723, 2017.

[29] Sushil Bhattacharjee, Amir Mohammadi, and Sébastien Marcel. Spoofing deep face recognition with custom silicone masks. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–7. IEEE, 2018.

[30] Nesli Erdogmus and Sebastien Marcel. Spoofing face recognition with 3d masks. *IEEE transactions on information forensics and security*, 9(7):1084–1097, 2014.

[31] Mohamed Loey, Gunasekaran Manogaran, Mohamed Hamed N Taha, and Nour Eldeen M Khalifa. A hybrid deep transfer learning model with machine learning methods for face mask detection in the era of the covid-19 pandemic. *Measurement*, 167:108288, 2020.

[32] Abdulaziz Ali Saleh Alashbi and Mohd Shahrizal Sunar. Occluded face detection, face in niqab dataset. In *International Conference of Reliable Information and Communication Technology*, pages 209–215. Springer, 2019.

[33] Yaman Akbulut, Abdulkadir Şengür, Ümit Budak, and Sami Ekici. Deep learning based face liveness detection in videos. In *2017 international artificial intelligence and data processing symposium (IDAP)*, pages 1–4. IEEE, 2017.

[34] Miloš Oravec, Jarmila Pavlovičová, Dominik Sopiak, Vojtěch Jirka, Marek Loderer, Ľuboš Lehota, Marek Vodička, Matej Fačkovec, Matej Mihalik, Martin Tomík, and Jozef Gerát. Mobile ear recognition application. In *2016 International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 1–4. IEEE, 2016.

[35] Ayman Abaza, Arun Ross, Christina Hebert, Mary Ann F Harrison, and Mark S Nixon. A survey on ear biometrics. *ACM computing surveys (CSUR)*, 45(2):1–35, 2013.

[36] Arun Ross and Ayman Abaza. Human ear recognition. *Computer*, 44(11):79–81, 2011.

[37] Aythami Morales, Moises Diaz, Gloria Llinas-Sanchez, and Miguel A Ferrer. Earprint recognition based on an ensemble of global and local features. In *2015 International Carnahan Conference on Security Technology (ICCST)*, pages 253–258. IEEE, 2015.

[38] Yuxi Liu and Dimitrios Hatzinakos. Earprint: Transient evoked otoacoustic emission for biometrics. *IEEE Transactions on Information Forensics and Security*, 9(12):2291–2301, 2014.

[39] Wenxiong Kang and Qiuxia Wu. Pose-invariant hand shape recognition based on finger geometry. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(11):1510–1521, 2014.

[40] Nicolae Duta. A survey of biometric technology based on hand shape. *Pattern Recognition*, 42(11):2797–2806, 2009.

[41] Andreas Uhl and Peter Wild. Footprint-based biometric verification. *Journal of Electronic Imaging*, 17(1):011016, 2008.

[42] Rohit Khokher, Ram Chandra Singh, and Rahul Kumar. Footprint recognition with principal component analysis and independent component analysis. *Macromolecular Symposia*, 347(1):16–26, 2015.

[43] Takahiro Takeda, Kazuhiko Taniguchi, Kazunari Asari, Kei Kuramoto, Syoji Kobashi, and Yutaka Hata. Biometric personal authentication by one step foot pressure distribution change by load distribution sensor. In *2009 IEEE International Conference on Fuzzy Systems*, pages 906–910. IEEE, 2009.

[44] Amioy Kumar, Shruti Garg, and Madasu Hanmandlu. Biometric authentication using finger nail plates. *Expert systems with applications*, 41(2):373–386, 2014.

[45] Roman Rak, Václav Matyáš, Zdeněk Říha, et al. *Biometrie a identita člověka (ve forenzních a komerčních aplikacích)*. Grada Publishing as, 2008.

[46] Shaik Kamal Sha, B Vengal Rao, M Sirisha Rao, KV Halini Kumari, Sudarshan Kumar Chinna, and Divya Sahu. Are tooth prints a hard tissue equivalence of finger print in mass disaster: A rationalized review. *Journal of pharmacy & bioallied sciences*, 9(Suppl 1):S29, 2017.

[47] Nidhi Gupta, Kiran Jadhav, BR Ahmed Mujib, and Vikram S Amberkar. Is re-creation of human identity possible using tooth prints? an experimental study to aid in identification. *Forensic science international*, 192(1-3):67–71, 2009.

[48] Phen-Lan Lin, Yan-Hao Lai, and Po-Whei Huang. Dental biometrics: Human identification based on teeth and dental works in bitewing radiographs. *Pattern Recognition*, 45(3):934–946, 2012.

[49] Hong Chen and Anil K Jain. Dental biometrics: Alignment and matching of dental radiographs. *IEEE transactions on pattern analysis and machine intelligence*, 27(8):1319–1326, 2005.

[50] Kailai Zhang, Ji Wu, Hu Chen, and Peijun Lyu. An effective teeth recognition method using label tree with cascade network structure. *Computerized Medical Imaging and Graphics*, 68:61–70, 2018.

[51] Michał Choraś. The lip as a biometric. *Pattern Analysis and Applications*, 13(1):105–112, 2010.

[52] Dong-Ju Kim, Jeong-Hoon Shin, and Kwang-Seok Hong. Teeth recognition based on multiple attempts in mobile device. *Journal of Network and Computer Applications*, 33(3):283–292, 2010.

[53] Maria De Marsico, Alfredo Petrosino, and Stefano Ricciardi. Iris recognition through machine learning techniques: A survey. *Pattern Recognition Letters*, 82:106–115, 2016.

[54] Aidan Boyd, Shivangi Yadav, Thomas Swearingen, Andrey Kuehlkamp, Mateusz Trokielewicz, Eric Benjamin, Piotr Maciejewicz, Dennis Chute, Arun Ross, Patrick Flynn, et al. Post-mortem iris recognition—a survey and assessment of the state of the art. *IEEE Access*, 8:136570–136593, 2020.

[55] Ishan Nigam, Mayank Vatsa, and Richa Singh. Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, 26:1–35, 2015.

[56] Fahreddin Sadikoglu and Selin Uzelaltinbulat. Biometric retina identification based on neural network. *Procedia Computer Science*, 102:26–33, 2016.

[57] Ryszard S Choraś. Retina recognition for biometrics. In *Seventh International Conference on Digital Information Management (ICDIM 2012)*, pages 177–180. IEEE, 2012.

[58] Zhi Zhou, Eliza Yingzi Du, N Luke Thomas, and Edward J Delp. A new human identification method: Sclera recognition. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 42(3):571–583, 2012.

[59] Jessica Liu Strohmann, Changting Xu, Yipeng Lu, and Hrishikesh Panchawagh. Ultrasonic biometric authentication system with contact gesture sensing. In *2020 IEEE International Ultrasonics Symposium (IUS)*, pages 1–3. IEEE, 2020.

[60] Anush Sankaran, Mayank Vatsa, and Richa Singh. Latent fingerprint matching: A survey. *IEEE Access*, 2:982–1004, 2014.

[61] Daniel Peralta, Mikel Galar, Isaac Triguero, Daniel Paternain, Salvador García, Edurne Barrenechea, José M Benítez, Humberto Bustince, and Francisco Herrera. A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Information Sciences*, 315:67–87, 2015.

[62] Emanuela Marasco and Arun Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys (CSUR)*, 47(2):1–36, 2014.

[63] Javier Galbally, Laurent Beslay, and Gunnar Böstrom. 3D-FLARE: A touchless full-3D fingerprint recognition system based on laser sensing. *IEEE Access*, 8:145513–145534, 2020.

[64] Javier Galbally, Rudolf Haraksim, and Laurent Beslay. A study of age and ageing in fingerprint biometrics. *IEEE Transactions on Information Forensics and Security*, 14(5):1351–1365, 2019.

[65] Zhenshen Qu, Junyu Liu, Yang Liu, Qiuyu Guan, Chunyu Yang, and Yuxin Zhang. Orienet: A regression system for latent fingerprint orientation field extraction. In Věra Kůrková, Yannis Manolopoulos, Barbara Hammer, Lazaros Iliadis, and Ilias Maglogiannis, editors, *Artificial Neural Networks and Machine Learning – ICANN 2018*, pages 436–446, Cham, 2018. Springer International Publishing.

[66] L. N. Darlow and B. Rosman. Fingerprint minutiae extraction using deep learning. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 22–30, 2017.

[67] Y. Tang, F. Gao, J. Feng, and Y. Liu. Fingernet: An unified deep network for fingerprint minutiae extraction. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 108–116, 2017.

[68] Mohamed Hammad, Yashu Liu, and Kuanquan Wang. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access*, 7:26527–26542, 2019.

[69] Eryun Liu. Infant footprint recognition. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 1653–1660, 2017.

[70] Pratichi Basak, Saurabh De, Mallika Agarwal, Aakarsh Malhotra, Mayank Vatsa, and Richa Singh. Multimodal biometric recognition for toddlers and pre-school

children. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 627–633. IEEE, 2017.

[71] Anil K Jain, Sunpreet S Arora, Lacey Best-Rowden, Kai Cao, Prem Sewak Sudhish, and Anjoo Bhatnagar. Biometrics for child vaccination and welfare: Persistence of fingerprint recognition for infants and toddlers. *arXiv preprint arXiv:1504.04651*, 2015.

[72] Wei Jia, Hai-Yang Cai, Jie Gui, Rong-Xiang Hu, Ying-Ke Lei, and Xiao-Feng Wang. Newborn footprint recognition using orientation feature. *Neural Computing and Applications*, 21(8):1855–1863, 2012.

[73] Riti Kushwaha, Neeta Nain, and Gaurav Singal. Detailed analysis of footprint geometry for person identification. In *2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pages 229–236. IEEE, 2017.

[74] Antonio Iula. Ultrasound systems for biometric recognition. *Sensors*, 19(10):2317, 2019.

[75] Donatella Nardiello, Michele Calia, and Antonio Iula. An improved ultrasound system for biometric recognition based on 3d palmprint. In *2016 IEEE International Ultrasonics Symposium (IUS)*, pages 1–4. IEEE, 2016.

[76] Antonio Iula, Gabriel Hine, Alessandro Ramalli, and Francesco Guidi. An improved ultrasound system for biometric recognition based on hand geometry and palmprint. *Procedia Engineering*, 87:1338–1341, 2014.

[77] Ajay Kumar, David CM Wong, Helen C Shen, and Anil K Jain. Personal verification using palmprint and hand geometry biometric. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 668–678. Springer, 2003.

[78] Peter Varchol, Dušan Levický, and Jozef Juhár. Multimodal biometric authentication using speech and hand geometry fusion. In *2008 15th International Conference on Systems, Signals and Image Processing*, pages 57–60. IEEE, 2008.

[79] Yi Liu, Jie Ling, Zhusong Liu, Jian Shen, and Chongzhi Gao. Finger vein secure biometric template generation based on deep learning. *Soft Computing*, 22(7):2257–2265, 2018.

[80] Rig Das, Emanuela Piciucco, Emanuele Maiorana, and Patrizio Campisi. Convolutional neural network for finger-vein-based biometric identification. *IEEE Transactions on Information Forensics and Security*, 14(2):360–373, 2018.

[81] Jie Cao, Mingyang Xu, Weisong Shi, Zhifeng Yu, Abdulbaset Salim, and Paul Kilgore. Mypalmvein: a palm vein-based low-cost mobile identification system for wide age range. In *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, pages 292–297. IEEE, 2015.

[82] Yutthana Pititheeraphab, Nuntachai Thongpance, Hisayuki Aoyama, and Chuchart Pintavirooj. Vein pattern verification and identification based on local geometric invariants constructed from minutia points and augmented with barcoded local feature. *Applied Sciences*, 10(9):3192, 2020.

[83] Kashif Shaheed, Hangang Liu, Gongping Yang, Imran Qureshi, Jie Gou, and Yilong Yin. A systematic review of finger vein recognition techniques. *Information*, 9(9):213, 2018.

[84] Christof Kauba, Bernhard Prommegger, and Andreas Uhl. *OpenVein—An Open-Source Modular Multipurpose Finger Vein Scanner Design*, pages 77–111. Springer International Publishing, Cham, 2020.

[85] Goh Kah Ong Michael, Tee Connie, Andrew Beng Jin Teoh, and G Chetty. A contactless biometric system using palm print and palm vein features. *Advanced Biometric Technologies*, pages 155–177, 2011.

[86] Ye Zhan, Aditya Singh Rathore, Giovanni Milione, Yuehang Wang, Wenhan Zheng, Wenyao Xu, and Jun Xia. 3d finger vein biometric authentication with photoacoustic tomography. *Appl. Opt.*, 59(28):8751–8758, Oct 2020.

[87] Anil K Jain and Unsang Park. Facial marks: Soft biometric for face recognition. In *2009 16th IEEE International Conference on Image Processing (ICIP)*, pages 37–40, 2009.

[88] Damon L Woodard, Shrinivas J Pundlik, Jamie R Lyle, and Philip E Miller. Periocular region appearance cues for biometric identification. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, pages 162–169, 2010.

[89] Shangling Song, Kazuhiko Ohnuma, Zhi Liu, Liangmo Mei, Akira Kawada, and Tomoyuki Monma. Novel biometrics based on nose pore recognition. *Optical Engineering*, 48(5):057204, 2009.

[90] Diwakar Agarwal and Atul Bansal. Fingerprint liveness detection through fusion of pores perspiration and texture features. *Journal of King Saud University - Computer and Information Sciences*, 2020.

[91] Adrian Moorhouse, Adrian N Evans, Gary A Atkinson, J Sunf, and Melvyn L Smith. The nose on your face may not be so plain: using the nose as a biometric. *IET Conference Proceedings*, pages 3–3(1), 2009.

[92] Niv Zehngut, Felix Juefei-Xu, Rishabh Bardia, Dipan K Pal, Chandrasekhar Bhagavatula, and Marios Savvides. Investigating the feasibility of image-based nose biometrics. In *2015 IEEE international conference on image processing (ICIP)*, pages 522–526. IEEE, 2015.

[93] Hassen Drira, Boulbaba Ben Amor, Anuj Srivastava, and Mohamed Daoudi. A riemannian analysis of 3d nose shapes for partial human biometrics. In *2009 IEEE 12th International Conference on Computer Vision*, pages 2050–2057. IEEE, 2009.

[94] Erica L Romsos and Peter M Vallone. Rapid pcr of str markers: Applications to human identification. *Forensic Science International: Genetics*, 18:90–99, 2015.

[95] Bartłomiej Hebda and Tomasz Kryjak. A compact deep convolutional neural network architecture for video based age and gender estimation. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 787–790. IEEE, 2016.

[96] Zhipeng Ji, Congyan Lang, Kai Li, and Junliang Xing. Deep age estimation model stabilization from images to videos. In *2018 24th International Conference on Pattern Recognition (ICPR)*, pages 1420–1425. IEEE, 2018.

[97] Fukun Yin and Shizhe Zhou. Accurate estimation of body height from a single depth image via a four-stage developing network. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 8267–8276, 2020.

[98] Ondrej Kainz, František Jakab, Miroslav Michalko, Roman Vápeník, and Dávid Cymbalák. Kinect as a tool in estimation of selected human body dimensions. In *2016 International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 157–163. IEEE, 2016.

[99] Aleš Deák, Ondrej Kainz, Miroslav Michalko, and František Jakab. Estimation of human body height from uncalibrated image. In *2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 1–4. IEEE, 2017.

[100] Pierluigi Carcagnì, Marco Del Coco, Dario Cazzato, Marco Leo, and Cosimo Distante. A study on different experimental configurations for age, race, and gender estimation problems. *EURASIP Journal on Image and Video Processing*, 2015(1):37, 2015.

[101] Yuefeng Huang, Xinyu Ao, and Yongping Li. Real time face detection based on skin tone detector. *International Journal of Computer Science and Network Security*, 9(7):71–77, 2009.

[102] Rishi Gupta, Sandeep Kumar, Pradeep Yadav, and Sumit Shrivastava. Identification of age, gender, & race smt (scare, marks, tattoos) from unconstrained facial images using statistical techniques. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pages 1–8. IEEE, 2018.

[103] Kresimir Delac and Mislav Grgic. A survey of biometric recognition methods. In *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*, pages 184–193. IEEE, 2004.

[104] Miguel Nicolás-Díaz, Annette Morales-González, and Heydi Méndez-Vázquez. Deep generic features for tattoo identification. In Ingela Nyström, Yanio Hernández Heredia, and Vladimir Milián Núñez, editors, *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, pages 272–282, Cham, 2019. Springer International Publishing.

[105] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Presentation attacks in signature biometrics: types and introduction to attack detection. In *Handbook of Biometric Anti-Spoofing*, pages 439–453. Springer, 2019.

[106] Moises Diaz, Miguel A Ferrer, Donato Impedovo, Muhammad Imran Malik, Giuseppe Pirlo, and Réjean Plamondon. A perspective analysis of handwritten signature technology. *ACM Computing Surveys (CSUR)*, 51(6):1–39, 2019.

[107] Moises Diaz-Cabrera, Aythami Morales, and Miguel A Ferrer. Emerging issues for static handwritten signature biometric. *Advances in Digital Handwritten Signature Processing. A Human Artefact for e-Society*, pages 111–122, 2014.

[108] Raul Sanchez-Reillo, Helga C Quiros-Sandoval, Ines Goicoechea-Telleria, and Wendy Ponce-Hernandez. Improving presentation attack detection in dynamic handwritten signature biometrics. *IEEE Access*, 5:20463–20469, 2017.

[109] Ramon Blanco-Gonzalo, Oscar Miguel-Hurtado, Aitor Mendaza-Ormaza, and Raul Sanchez-Reillo. Handwritten signature recognition in mobile scenarios:

Performance evaluation. In *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, pages 174–179. IEEE, 2012.

[110] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. Benchmarking desktop and mobile handwriting across cots devices: The e-biosign biometric database. *PloS one*, 12(5):e0176792, 2017.

[111] Christian Hook, Juergen Kempf, and Georg Scharfenberg. New pen device for biometrical 3d pressure analysis of handwritten characters, words and signatures. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 38–44, 2003.

[112] Gonzalo Bailador, Carmen Sanchez-Avila, Javier Guerra-Casanova, and Alberto de Santos Sierra. Analysis of pattern recognition techniques for in-air signature biometrics. *Pattern Recognition*, 44(10-11):2468–2478, 2011.

[113] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. Do you need more data? the deepsigndb on-line handwritten signature biometric database. In *2019 International Conference on Document Analysis and Recognition (ICDAR)*, pages 1143–1148. IEEE, 2019.

[114] Iva Košek Bartošová and Eliška Třečková. The new writing system Comenia Script in the Czech Republic. *Procedia-Social and Behavioral Sciences*, 112:1255–1262, 2014.

[115] Martin Rajnoha, Radim Burget, and Malay Kishore Dutta. Handwriting Comenia Script recognition with convolutional neural network. In *2017 40th International Conference on Telecommunications and Signal Processing (TSP)*, pages 775–779. IEEE, 2017.

[116] Javier Galbally, Marcos Martinez-Diaz, and Julian Fierrez. Aging in biometrics: An experimental analysis on on-line signature. *PloS one*, 8(7):e69897, 2013.

[117] Clayton R Pereira, Danilo R Pereira, Gustavo H Rosa, Victor HC Albuquerque, Silke AT Weber, Christian Hook, and João P Papa. Handwritten dynamics

assessment through convolutional neural networks: An application to parkinson's disease identification. *Artificial intelligence in medicine*, 87:67–77, 2018.

[118] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. *Computers & Security*, 83:151–166, 2019.

[119] Sowndarya Krishnamoorthy, Luis Rueda, Sherif Saad, and Haytham Elmiligi. Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning. In *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, pages 50–57, 2018.

[120] Bhaveer Bhana and Stephen Flowerday. Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security*, page 101925, 2020.

[121] Baljit Singh Saini, Navdeep Kaur, and Kamaljit Singh Bhatia. Keystroke dynamics based user authentication using numeric keypad. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pages 25–29. IEEE, 2017.

[122] Junhong Kim, Haedong Kim, and Pilsung Kang. Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. *Applied Soft Computing*, 62:1077–1087, 2018.

[123] Junhong Kim and Pilsung Kang. Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features. *Pattern Recognition*, 108:107556, 2020.

[124] Alexey E Sulavko, Alexander V Eremenko, and Alexander A Fedotov. Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure. In *2017 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, pages 1–7. IEEE, 2017.

[125] Anbiao Huang, Shuo Gao, Junliang Chen, Lijun Xu, and Arokia Nathan. High security user authentication enabled by piezoelectric keystroke dynamics and machine learning. *IEEE Sensors Journal*, 20(21):13037–13046, 2020.

[126] Vladyslav Loboda and Grzegorz Kolaczek. Sound and keystroke dynamics analysis for user authenticity verification. In *2019 IEEE 14th International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, pages 551–558. IEEE, 2019.

[127] Hyungu Lee, Jung Yeon Hwang, Dong In Kim, Shincheol Lee, Sung-Hoon Lee, and Ji Sun Shin. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. *Security and Communication Networks*, 2018, 2018.

[128] Hyungu Lee, Jung Yeon Hwang, Shincheol Lee, Dong In Kim, Sung-Hoon Lee, Jaehwan Lee, and Ji Sun Shin. A parameterized model to select discriminating features on keystroke dynamics authentication on smartphones. *Pervasive and Mobile Computing*, 54:45–57, 2019.

[129] Senthil Kumar AV and M Rathi. Keystroke dynamics: A behavioral biometric model for user authentication in online exams. In *Biometric Authentication in Online Learning Environments*, pages 183–207. IGI Global, 2019.

[130] Saurabh Singh et al. Keystroke dynamics for continuous authentication. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 205–208. IEEE, 2018.

[131] Zach Jorgensen and Ting Yu. On mouse dynamics as a behavioral biometric for authentication. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 476–482, 2011.

[132] Nan Zheng, Aaron Paloski, and Haining Wang. An efficient user verification system via mouse movements. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 139–150, 2011.

[133] Bassam Sayed, Issa Traoré, Isaac Woungang, and Mohammad S Obaidat. Biometric authentication using mouse gesture dynamics. *IEEE Systems Journal*, 7(2):262–274, 2013.

[134] Kyle O Bailey, James S Okolica, and Gilbert L Peterson. User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*, 43:77–89, 2014.

[135] Gianni Fenu, Mirko Marras, and Ludovico Boratto. A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113:83–92, 2018.

[136] Stefan Billeb, Christian Rathgeb, Herbert Reininger, Klaus Kasper, and Christoph Busch. Biometric template protection for speaker recognition based on universal background models. *IET Biometrics*, 4(2):116–126, 2015.

[137] Finnian Kelly, Andrzej Drygajlo, and Naomi Harte. Speaker verification with long-term ageing data. In *2012 5th IAPR international conference on biometrics (ICB)*, pages 478–483. IEEE, 2012.

[138] Andrzej Drygajlo and Rudolf Haraksim. Biometric evidence in forensic automatic speaker recognition. In *Handbook of Biometrics for Forensic Science*, pages 221–239. Springer, 2017.

[139] Andreas Lanitis. A survey of the effects of aging on biometric identity verification. *International Journal of Biometrics*, 2(1):34–52, 2010.

[140] Yuri Matveev. The problem of voice template aging in speaker recognition systems. In *International Conference on Speech and Computer*, pages 345–353. Springer, 2013.

[141] Rohan Kumar Das, Sarfaraz Jelil, and SR Mahadeva Prasanna. Exploring session variability and template aging in speaker verification for fixed phrase short utterances. In *Interspeech*, pages 445–449, 2016.

[142] Dongdong Li, Yingchun Yang, and Weihui Dai. Cost-sensitive learning for emotion robust speaker recognition. *The Scientific World Journal*, 2014, 2014.

[143] Milan Rusko, Marian Trnka, Sakhia Darjaa, Tim H Stelkens-Kobsch, and Michael Finke. Weaknesses of voice biometrics-sensitivity of speaker verification to emotional arousal. In *25th International Congress on Sound and Vibration, 8.-12. Juli 2018, Hiroshima, Japan*, 2018.

[144] Li Lu, Lingshuang Liu, Muhammad Jawad Hussain, and Yongshuai Liu. I sense you by breath: Speaker recognition via breath biometrics. *IEEE Transactions on Dependable and Secure Computing*, 2017.

[145] Hemant A Patil and Madhu R Kamble. A survey on replay attack detection for automatic speaker verification (asv) system. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pages 1047–1053. IEEE, 2018.

[146] Zhizheng Wu, Sheng Gao, Eng Siong Cling, and Haizhou Li. A study on replay attack and anti-spoofing for text-dependent speaker verification. In *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific*, pages 1–5. IEEE, 2014.

[147] Mingrui Yuan and Zhiyao Duan. Spoofing speaker verification systems with deep multi-speaker text-to-speech synthesis. *arXiv preprint arXiv:1910.13054*, 2019.

[148] Yi Xie, Cong Shi, Zhuohang Li, Jian Liu, Yingying Chen, and Bo Yuan. Real-time, universal, and robust adversarial attacks against speaker recognition systems. In *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1738–1742, 2020.

[149] Massimiliano Todisco, Héctor Delgado, and Nicholas Evans. Constant q cepstral coefficients: A spoofing countermeasure for automatic speaker verification. *Computer Speech & Language*, 45:516–535, 2017.

[150] James Eric Mason, Issa Traore, and Isaac Woungang. Facets and promises of gait biometric recognition. In *Biometric-Based Physical and Cybersecurity Systems*, pages 233–253. Springer, 2019.

[151] Jasvinder Pal Singh, Sanjeev Jain, Sakshi Arora, and Uday Pratap Singh. A survey of behavioral biometric gait recognition: Current success and future perspectives. *Archives of Computational Methods in Engineering*, pages 1–42, 2019.

[152] Patrick Connor and Arun Ross. Biometric recognition by gait: A survey of modalities and features. *Computer Vision and Image Understanding*, 167:1–27, 2018.

[153] Amer G Binsaadoon and E-SM El-Alfy. Enhanced method for recognizing gender in smart environments from gait biometric. *Smart Cities Symposium 2018*, 2018.

[154] Akarsh Pokkunuru, Kalvik Jakkala, Arupjyoti Bhuyan, Pu Wang, and Zhi Sun. Neuralwave: Gait-based user identification through commodity wifi and deep learning. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pages 758–765. IEEE, 2018.

[155] Maria De Marsico, Alessio Mecca, and Silvio Barra. Walking in a smart city: Investigating the gait stabilization effect for biometric recognition via wearable sensors. *Computers & Electrical Engineering*, 80:106501, 2019.

[156] Yao Guo, Raffaele Gravina, Xiao Gu, Giancarlo Fortino, and Guang-Zhong Yang. Emg-based abnormal gait detection and recognition. In *2020 IEEE International Conference on Human-Machine Systems (ICHMS)*, pages 1–6. IEEE, 2020.

[157] Yann Maret, Daniel Oberson, and Marina Gavrilova. Real-time embedded system for gesture recognition. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 30–34. IEEE, 2018.

[158] Jiayuan He and Ning Jiang. Biometric from surface electromyogram (semg): Feasibility of user verification and identification based on gesture recognition. *Frontiers in Bioengineering and Biotechnology*, 8:58, 2020.

[159] Shin Hochul, Lee Kideok, Lee Hyeonchang, Jong Man Lee, Bong Seop Song, and Jae Won Lee. Biometric authentication using gesture, August 4 2020. US Patent 10,733,274.

[160] Guan-Cheng Liang, Xiang-Yu Xu, and Jia-Di Yu. User-authentication on wearable devices based on punch gesture biometrics. In *ITM Web of Conferences*, volume 11, page 01003. EDP Sciences, 2017.

[161] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. Task-driven biometric authentication of users in virtual reality (vr) environments. In *International conference on multimedia modeling*, pages 55–67. Springer, 2019.

[162] Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Deep-ECG: convolutional neural networks for ECG biometric recognition. *Pattern Recognition Letters*, 126:78–85, 2019.

[163] João Ribeiro Pinto, Jaime S Cardoso, André Lourenço, and Carlos Carreiras. Towards a continuous biometric system based on ECG signals acquired on the steering wheel. *Sensors*, 17(10):2228, 2017.

[164] Qingxue Zhang, Dian Zhou, and Xuan Zeng. Heartid: A multiresolution convolutional neural network for ECG-based biometric human identification in smart health applications. *Ieee Access*, 5:11805–11816, 2017.

[165] Audrey Aldridge, Eli Barnes, Cindy L Bethel, Daniel W Carruth, Marianna Kocturova, Matus Pleva, and Jozef Juhar. Accessible electroencephalograms (EEGs): A comparative review with OpenBCI's Ultracortex Mark IV headset. In *2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pages 1–6, 2019.

[166] Min Wang, Jiankun Hu, and Hussein A Abbass. BrainPrint: EEG biometric identification based on analyzing brain connectivity graphs. *Pattern Recognition*, page 107381, 2020.

[167] Su Yang and Farzin Deravi. On the usability of electroencephalographic signals for biometric recognition: A survey. *IEEE Transactions on Human-Machine Systems*, 47(6):958–969, 2017.

[168] Adam Czajka. Database of iris printouts and its application: Development of liveness detection method for iris recognition. In *2013 18th International Conference on Methods & Models in Automation & Robotics (MMAR)*, pages 28–33. IEEE, 2013.

[169] Mateusz Trokielewicz, Adam Czajka, and Piotr Maciejewicz. Presentation attack detection for cadaver iris. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10. IEEE, 2018.

[170] Shilin Yan, Shan Chang, Jiacheng Wang, and Shanila Azhar. Using pupil light reflex for fast biometric authentication. In *Proceedings of the ACM Turing Celebration Conference-China*, pages 139–143, 2020.

[171] Lena A Jäger, Silvia Makowski, Paul Prasse, Sascha Liehr, Maximilian Seidler, and Tobias Scheffer. Deep eyedentification: Biometric identification using micromovements of the eye. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, pages 299–314. Springer, 2019.

[172] Daniel L. Silver and Adam Biggs. Keystroke and eye-tracking biometrics for user identification. In Hamid R. Arabnia, editor, *Proceedings of the 2006 International Conference on Artificial Intelligence, ICAI 2006, Las Vegas, Nevada, USA, June 26-29, 2006, Volume 2*, pages 344–348. CSREA Press, 2006.

[173] Juraj Kacur, Jaroslav Polec, Eva Smolejova, and Anton Heretik. An analysis of eye-tracking features and modelling methods for free-viewed standard stimulus: Application for Schizophrenia detection. *IEEE Journal of Biomedical and Health Informatics*, 24(11):3055–3065, 2020.

[174] Agostina J Larrazabal, CE García Cena, and César Ernesto Martínez. Video-oculography eye tracking towards clinical applications: A review. *Computers in biology and medicine*, 108:57–66, 2019.

[175] Daniel Jansson, Alexander Medvedev, Hans Axelson, and Dag Nyholm. Stochastic anomaly detection in eye-tracking data for quantification of motor symptoms in Parkinson's disease. In *Signal and Image Analysis for Biomedical and Life Sciences*, pages 63–82. Springer, 2015.

[176] Christy K Sheehy, Alexandra Beaudry-Richard, Ethan Bensinger, Jacqueline Theis, and Ari J Green. Methods to assess ocular motor dysfunction in multiple sclerosis. *Journal of Neuro-ophthalmology*, 38(4):488–493, 2018.

[177] Jiannan Kang, Xiaoya Han, Jiajia Song, Zikang Niu, and Xiaoli Li. The identification of children with autism spectrum disorder by SVM approach on EEG and eye-tracking data. *Computers in biology and medicine*, 120:103722, 2020.

[178] Mélodie Vidal, Jayson Turner, Andreas Bulling, and Hans Gellersen. Wearable eye tracking for mental health monitoring. *Computer Communications*, 35(11):1306–1311, 2012.

[179] Robert W Frischholz and Ulrich Dieckmann. Biold: a multimodal biometric identification system. *Computer*, 33(2):64–68, 2000.

[180] Hasan Ertan Çetingül, Engin Erzin, Yücel Yemez, and A Murat Tekalp. Multimodal speaker/speech recognition using lip motion, lip texture and audio. *Signal processing*, 86(12):3549–3558, 2006.

[181] Teodors Eglitis, Richard Guest, and Farzin Deravi. Data behind mobile behavioural biometrics – a survey. *IET Biometrics*, 9(6):224–237, 2020.

[182] Ahmed Mahfouz, Tarek M Mahmoud, and Ahmed Sharaf Eldin. A survey on behavioral biometric authentication on smartphones. *Journal of information security and applications*, 37:28–37, 2017.

[183] Meryem Regouid, Mohamed Touahria, Mohamed Benouis, and Nicholas Costen. Multimodal biometric system for ECG, ear and iris recognition based on local descriptors. *Multimedia Tools and Applications*, 78(16):22509–22535, 2019.

[184] Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12):2270–2285, 2005.

[185] Matus Pleva, Eva Kiktova, Jozef Juhar, and Patrick Bours. Acoustical user identification based on MFCC analysis of keystrokes. *Advances in Electrical and Electronic Engineering*, 13(4):309–313, 2015.

[186] Matus Pleva, Eva Kiktova, Peter Viszlay, and Patrick Bours. Acoustical keystroke analysis for user identification and authentication. In *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pages 386–389, 2016.

[187] Patrick Bours, Eva Kiktová, and Matúš Pleva. Static audio keystroke dynamics. In Andrzej Dziech, Mikołaj Leszczuk, and Remigiusz Baran, editors, *Multimedia Communications, Services and Security*, pages 159–169, Cham, 2015. Springer International Publishing.

[188] Salil P Banerjee and Damon L Woodard. Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7(1):116–139, 2012.

[189] Kevin S Killourhy and Roy A Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pages 125–134, 2009.

[190] Eva Kiktova, Martin Lojka, Matus Pleva, Jozef Juhar, and Anton Cizmar. Comparison of different feature types for acoustic event detection system. In *International Conference on Multimedia Communications, Services and Security*, pages 288–297. Springer, 2013.

[191] Niko Brümmer and Edward de Villiers. The Bosaris toolkit: Theory, algorithms and code for surviving the new DCF. *arXiv preprint arXiv:1304.2865*, 2013.

[192] Ondrej Novotný, Pavel Matejka, Oldrich Plchot, Ondrej Glembek, and Lukáš Burget. Analysis of speaker recognition systems in realistic scenarios of the SITW 2016 challenge. *Interspeech 2016*, pages 828–832, 2016.

[193] Luis J Rodriguez-Fuentes, Amparo Varona, Mikel Penagarikano, Germán Bordel, and Mireia Diez. GTTS systems for the SWS task at MediaEval 2013. In *Working Notes Proceedings of the MediaEval 2013 Workshop, Barcelona, Spain, October 18-19, CEUR-WS. org, ISSN 1613-0073*, 2013.

[194] Jozef Vavrek, Peter Viszlay, Martin Lojka, Jozef Juhár, and Matúš Pleva. Weighted fast sequential DTW for multilingual audio Query-by-Example retrieval. *Journal of Intelligent Information Systems*, 51(2):439–455, 2018.

[195] Md Abdur Rahim and Jungpil Shin. Hand movement activity-based character input system on a virtual keyboard. *Electronics*, 9(5):774, 2020.

[196] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters*, 31(8):733 – 741, 2010. Award winning papers from the 19th International Conference on Pattern Recognition (ICPR).

[197] Charles A Shoniregun and Stephen Crosier. *Securing biometrics applications*. Springer, 2008.

[198] Paco Garcia. Biometrics on the blockchain. *Biometric Technology Today*, 2018(5):5–7, 2018.

[199] Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana, and Ruben Vera-Rodriguez. Blockchain and biometrics: A first look into opportunities and challenges. In *International Congress on Blockchain and Applications*, pages 169–177. Springer, 2019.

[200] Dušan Levický. *Aplikovaná kryptografia*. Elfa, Košice, 2018.

[201] AH Mohsin, AA Zaidan, BB Zaidan, OS Albahri, AS Albahri, MA Alsalem, and KI Mohammed. Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. *Computer Standards & Interfaces*, 66:103343, 2019.

[202] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015.

[203] Zhe Jin, Andrew Beng Jin Teoh, Thian Song Ong, and Connie Tee. Generating revocable fingerprint template using minutiae pair representation. In *2010 2nd International Conference on Education Technology and Computer*, volume 5, pages V5–251. IEEE, 2010.

[204] Farzin Deravi. Biometrics standards. In *Advances in biometrics*, pages 473–489. Springer, 2008.

[205] Mladen Trikoš, Ivan Tot, Jovan Bajčetić, Komlen Lalović, Boriša Jovanović, and Dušan Bogićević. Biometric security standardization. In *2019 Zooming Innovation in Consumer Technologies Conference (ZINC)*, pages 17–20. IEEE, 2019.

[206] Martin Sarnovský, Karol Furdík, and Erika Školová. *Riadenie IT Prostredia*. Technická univerzita v Košiciach, 2015. Online na `http://people.tuke.sk/martin.sarnovsky/rip_skripta/Riadenie%20IT%20Prostredia.html`.

[207] Stanislav Ondáš, Eva Kiktová, Matúš Pleva, Mária Oravcová, Lukáš Hudák, Jozef Juhár, and Július Zimmermann. Pediatric speech audiometry web application for hearing detection in the home environment. *Electronics*, 9(6):994, Jun 2020.

[208] Stanislav Ondas, Jozef Juhar, Matus Pleva, Anton Cizmar, and Roland Holcer. Service robot SCORPIO with robust speech interface. *International Journal of Advanced Robotic Systems*, 10(1):3, 2013.

[209] Matus Pleva, Jozef Juhar, Anton Cizmar, Christopher Hudson, Daniel W Carruth, and Cindy L Bethel. Implementing English speech interface to jaguar robot for swat training. In *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 105–110. IEEE, 2017.

[210] Martin Lojka, Matúš Pleva, Eva Kiktová, Jozef Juhár, and Anton Čižmár. Efficient acoustic detector of gunshots and glass breaking. *Multimedia Tools and Applications*, 75(17):10441–10469, 2016.

[211] Matúš Pleva and Jozef Juhár. TUKE-BNews-SK: Slovak broadcast news corpus construction and evaluation. In *LREC*, pages 1709–1713, 2014.

[212] Štefan Korečko, Matus Pleva, Markus Hoff Skudal, and Patrick Bours. EMG input data collection for multimodal keystroke analysis. In *Proceedings of CogInfoCom 2021 - 12th IEEE International Conference on Cognitive Infocommunications*, pages 205–210, 2021.

[213] Markus Hoff Skudal, Matus Pleva, Štefan Korečko, Patrick Bours, and Daniel Hladek. Comparing natural and strong typing behavior for keystroke dynamics multimodal database collection. In *Proceedings of NISK 2021 - Norwegian Information Security conference, Trondheim*, pages 1–4, 2021.

Addendum

Pracovný e-mail autora: Matus.Pleva@tuke.sk

Pracovný Skype ID: ivrtuke

WWW stránka univerzity: http://www.tuke.sk

WWW stránka fakulty: http://fei.tuke.sk

WWW stránka katedry: http://kemt.fei.tuke.sk

Claritive ResearcherID: http://www.researcherid.com/rid/H-7209-2012

ORCID profile: http://orcid.org/0000-0003-4380-0801

Google scholar:

http://scholar.google.sk/citations?user=TgWS5vUAAAAJ

ResearchGate: http://www.researchgate.net/profile/Matus_Pleva2/

Scopus author ID:

https://www.scopus.com/authid/detail.uri?authorId=21834757800

Publons profile: https://publons.com/author/1399351/

IEEE*Xplore* profile: https://ieeexplore.ieee.org/author/37063036000

SpringerLink profile:

https://link.springer.com/search?query=matus+pleva

Semantic Scholar profile:

https://www.semanticscholar.org/author/Matus-Pleva/9721935

LinkedIn: http://sk.linkedin.com/pub/matus-pleva/59/211/1a0/

Na vytvorenie tohoto dokumentu bol použitý *pdf*$\mathcal{CS}$LaTeX, typograficky orientovaný programovací jazyk implementovaný v klaudovej službe *Overleaf*.

Poďakovanie: Táto publikácia je jedným z výstupov riešenia projektu Inovácia obsahu a príprava učebných textov pre predmet Biometrické systémy bezpečnosti (KEGA 009TUKE-4/2019) a bola realizovaná z prostriedkov tohto projektu.

Vydavateľ: Technická univerzita v Košiciach
Rok: 2021
ISBN: 978-80-553-3834-7
Vydanie: prvé
Dostupné online: `http://biometria.web.tuke.sk/BSB-ucebnica.pdf`
Rozsah: 120 strán