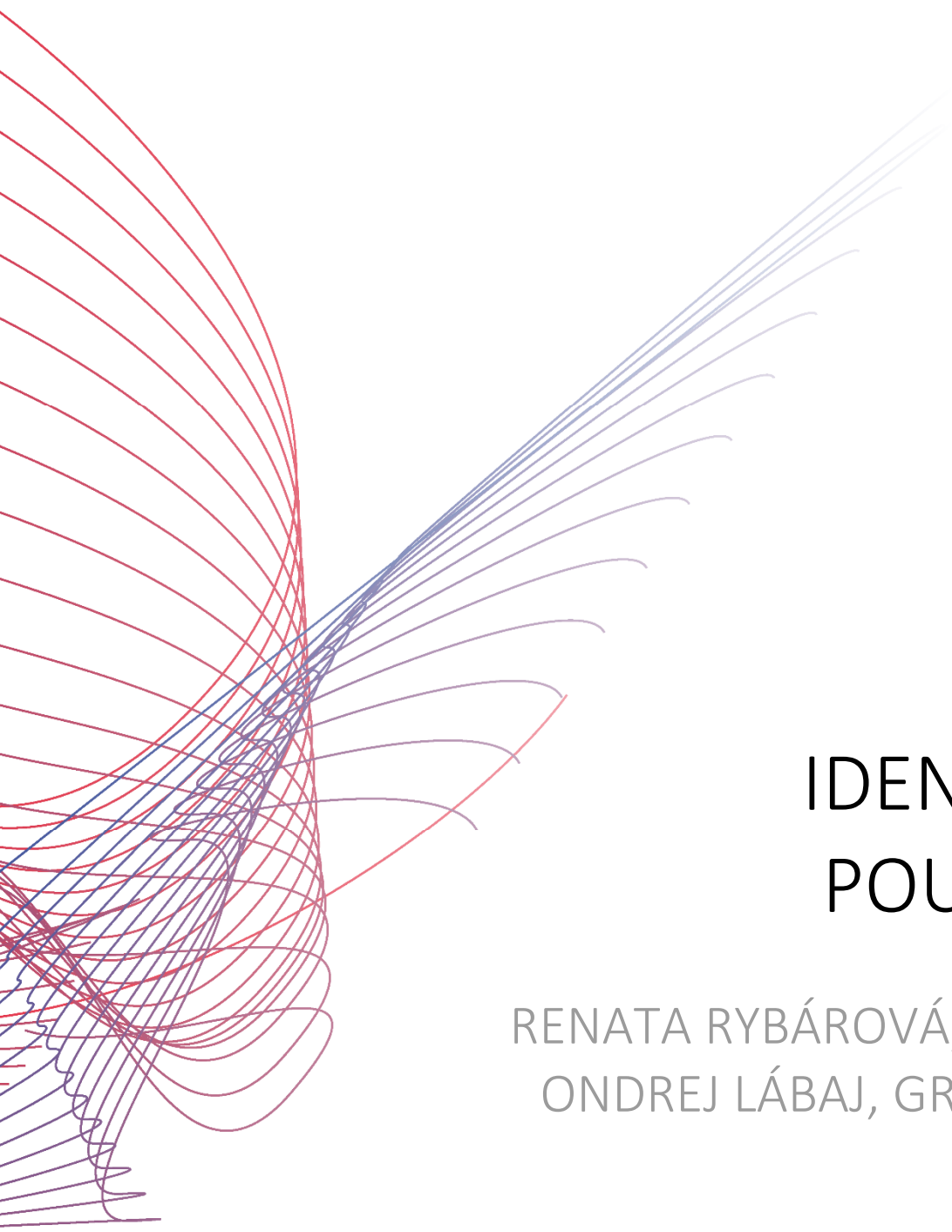
en
cs de
sk es

TECH
pedia



IDENTIFIKÁCIA POUŽÍVATEĽA

RENATA RYBÁROVÁ, JURAJ KAČUR,
ONDREJ LÁBAJ, GREGOR ROZINAJ

Názov: Identifikácia používateľa

Autor: Renata Rybárová, Juraj Kačur, Ondrej Lábaj, Gregor Rozinaj

Vydalo: České vysoké učení technické v Praze

Fakulta elektrotechnická

Kontaktná adresa: Technická 2, Praha 6, Česká republika

Tel.: +420 224352084

Tlač: (iba elektronická)

Počet strán: 45

Edícia (vydanie): 1. vydanie, 2017

ISBN 978-80-01-06240-1

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
	Výhody
	Nevýhody

ANOTÁCIA

Identifikácia používateľa, autorizácia a autentifikácia zabezpečujú, že k systému budú mať prístup iba oprávnení používatelia a akceptujú sa iba príkazy, ktoré budú autorizované. Identifikácia hovoriaceho má za cieľ základnú identifikáciu možných používateľov začlenených do databázy systému. Táto funkcia môže byť vhodná pre úlohy vychádzajúce z identifikácie, ako napr. aktivácia osobného profilu. Detekcia tváre môže poskytnúť bezpečnejšiu identifikáciu založenú na tvári používateľa, ktorá poskytuje viac charakteristických prvkov. Tie môžu byť použité na parametrizáciu v porovnaní s hlasovou identifikáciou. Navyše, rozpoznávanie 3D tváre ešte viac rozširuje možnosti extrakcie príznakov pre presnejšiu identifikáciu v rámci skupiny používateľov. Môže byť preto použitá na vysoký stupeň autentifikácie (a autorizácie) pre najnáročnejšie aplikácie (napr. prihlásenie sa do banky atď.).

CIELE

Hlavným cieľom tohto výučbového kurzu je oboznámiť študentov so základmi identifikácie, autentifikácie a autorizácie používateľa. Študentovi sú predstavené základné princípy identifikácie hovoriaceho, identifikácie používateľa na základe 2D a 3D rozpoznávania tvári, autentifikačných metód a autorizácie používateľa.

LITERATÚRA

[1] Abate, Andrea F.; Nappi, Michele; Riccio, Daniel; Sabatino, Gabriele. 2D and 3D face recognition: A survey In: Pattern Recognition Letters, Volume 28, Issue 14, 15 October 2007, Pages 1885–1906. available at www.sciencedirect.com.

[2] T. Kinnunen, H. Li, An overview of text-independent speaker recognition: from features to supervectors, Speech communication, Vol. 52, pp. 12-40, Elsevier, 2010

[3] Probst, Michael; Schumann, Sebastian; Rozinaj, Gregor; Minarik, Ivan; Rybárová, Renata; Oravec, Miloš. EVALUATION: Final Multimodal Interface for User/Group-Aware Personalisation, Deliverable 5.5.1, available at http://www.hbb-next.eu/index.php/documents, Decmber 2013.

[4] Bán, Jozef; Féder, Matej; Oravec, Miloš; Pavlovičová, Jarmila. Face Recognition of Images Corrupted by Transmission Errors. In: Redžúr 2012: proceedings; 6th International Workshop on Multimedia and Signal Processing. April 11, 2012, Vienna, Austria. Bratislava: Nakladateľstvo STU, 2012. pp. 15-18, ISBN 978-80-227-3686-2

[5] Rozinaj, Gregor; Minarik, Ivan; Rybárová, Renata; Pavlovičová, Jarmila; Mármol, Félix Gómez; Tormo, Ginés Dólera, Gülbahar, Mark; Schumann, Sebastian. DESIGN AND PROTOCOL: Final User ID, Profile, Application Reputation Framework, Deliverable 3.4.1, available at http://www.hbb-next.eu/index.php/documents, Decmber 2013.

[6] Schneier, Bruce. Sensible Authentication, ACM Queue 1, Volume 1 Issue 10, February 2004. Pages 74.

[7] McCue, A. Is Your Cat a Target for Password-Stealing Hackers?, Silicon.com, 11 August 2004.

[8] Haskett, J.A., Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms In Communications of the ACM 27, 1984.

[9] Madigan, A. Picture Memory - Memory and Cognition: Essays in Honour of Allan Paivio Erlbaum, 1983.

[10] Cranor, L.F.; Garfinkel, S. Security and Usability, O'Reilly, August 2005. ISBN 0-596-00827-9.

[11] Vacca, J.R. Computer and Information Security Handbook, Morgan Kaufmann, 2009. ISBN 978-0-12-374354-1.

[12] Gattiker, U. E. The Information Security Dictionary, KLUWER ACADEMICPUBLISHERS, 2004. ISBN 1-4020-7927-3.

Obsah

1 Identifikácia používateľa

Identifikácia používateľa je jedným z kľúčových prvkov zabezpečujúcich, aby systém alebo aplikácia vykonávali len príkazy, ktoré sú skutočne oprávnené. Najpoužívanejší typ autentifikácie alebo overovania je heslo. Ale s rozvojom informačných technológií a algoritmov na ochranu bezpečnosti, systémy a aplikácie začínajú používať autentifikáciu na základe biometrických údajov.

Použitie biometrie účinne eliminuje prípadné riziká spojené s menej pokročilými technológiami, ktoré sú založené na tom, čo človek má alebo vie oproti tomu než čím človek v skutočne je [1]. Jedná sa o veľmi atraktívnu a populárnu technológiu, pretože môže byť integrovaná do ľubovoľnej aplikácie alebo systému vyžadujúceho bezpečnostné kontroly alebo kontrolu prístupu.

Identifikácia hovoriaceho poskytuje základnú identifikáciu možných používateľov nachádzajúcich sa v okolí systému. Metóda detekcie tváre si kladie za cieľ poskytnúť spoľahlivú identifikáciu založenú na tvárach používateľov, ktoré obsahujú oveľa viac charakteristík v porovnaní s identifikáciou na základe hlasu, ktoré môžu byť parametrizované. Navyše rozpoznávanie 3D tváre ďalej rozširuje možnosti získavania (extrakcie) príznakov, aby sa presnejšie identifikovali konkrétne osoby. Preto môže byť použitý pre najvyššiu úroveň autentifikácie (aj autorizácie alebo povolenia) pre najnáročnejšie aplikácie (napr. prihlásenie do bankového účtu, atď.) Z bezpečnostných dôvodov je možné autentifikáciu pomocou rozpoznávania 3D tváre rozšíriť o ďalšie metódy ako napríklad sledovanie pohybu očí alebo rozpoznanie dúhovky. Tento prístup môže simulovať multi-úrovňovú autentifikáciu (prihlásenie pomocou biometrie a bezpečnostného kľúča - tokenu), potrebnú na autentifikáciu najvyššej úrovne.

Biometrie majú tiež svoje nevýhody. Rozpoznanie dúhovky je extrémne presné, ale drahé z pohľadu implementácie a nie príliš akceptované ľuďmi. Odtlačky prstov sú spoľahlivé a neinvazívne, ale nie sú vhodné pre nespolupracujúcich jedincov. Naopak, rozpoznávanie tvárí sa zdá byť rozumným kompromisom medzi spoľahlivosťou a spoločenskou akceptáciou [1].

2 Identifikácia hovoriaceho

2.1 Identifikácia hovoriaceho - prehľaď

Identifikácia hovoriaceho je súčasťou širšieho konceptu rozpoznávania rečníka. Skladá sa z dvoch podobných ale predsa len rozdielnych úloh: identifikácia a verifikácia hovoriaceho. Prvá úloha má za cieľ určiť kto zo zvolenej (uzavretej) skupiny ľudí získanej vo fáze trénovania rozpráva, pričom druhá úloha má potvrdiť či je hovoriaci skutočne ten, za koho sa vydáva.

V prípade nízkeho skóre systém môže identifikáciu odmietnuť (nebol to nikto zo skupiny). Takáto úloha sa volá aj problém uzavretej skupiny (v trénovacej množine je konečný počet hovoriacich).

Na druhej strane verifikácia potvrdzuje či je daný hovoriaci skutočne ten za koho sa deklaroval napr. pomocou hesla, na základe svojej hlasovej vzorky.

Pretože na svete je veľa ľudí, potenciálnych útočníkov, ktorých reč nemôže byť súčasne nahratá v databáze, sa tento problém označuje za úlohu otvorenej skupiny. Pri tejto úlohe je dôležitý model všeobecného hovoriaceho na základe ktorého sa správne určia prahy zamietnutia nesprávneho používateľa.

Úloha rozpoznávania rečníka je veľmi komplexná a problematická kvôli viacerým aspektom, ktoré budú vysvetlené ďalej. Tomuto problému sa venujú výskumné tímy už viac ako 40 rokov a táto oblasť stále nie je uzavretá. S pokrokom dostupných technológií sa aj oblasti aplikácie rozpoznania rečníka stále rozširuje napr. aj do nasledovných sfér:

- Kriminalistika
- Prirodzená a neinvazívna metóda získania a spracovania biometrických dát napr. pre kontrolu prístupu k službám alebo dátam
- Automatická indexácia rečových databáz
- Hrací priemysel
- Pomôcky pre postihnutých

Riešenie problému identifikácie v sebe zahŕňa 3 základné oblasti výskumu:

- **Extrakcia príznakov** reči vhodných pre identifikáciu
- **Normalizácia príznakov** kompenzujúca rečníkovu variabilitu a zmenu prostredia
- **Klasifikácia a rozhodovanie** na základe extrahovaných príznakov

Identifikácia hovoriaceho sa ďalej delí na 2 veľké skupiny, a to textovo závislú a textovo nezávislú. Textovo závislý systém očakáva určité prehovorenie, na základe ktorého vykoná rozhodnutie. Na druhej strane textovo nezávislé systémy pracujú nezávislé od konkrétneho vyhovorenia. Pri textovo závislých systémoch sa dá očakávať vyššia úspešnosť identifikácie pri danej dĺžke prehovorenia. Tie totiž môžu bezpečne postihnúť aj špecifické koartikulačné efekty.

2.2 Vlastnosti rečových signálov

Rečový signál je fyzicky tvorený hlasovými orgánmi, ktoré sú ale ovládané mozgovou činnosťou jedinca. Obidva aspekty úzko súvisia s daným jedincom, preto obidve aktivity vnášajú do rečového signálu špecifické vlastnosti hovoriaceho; preto sa aj rečový signál označuje ako biometrický.

I keď primárnou úlohou rečového signálu je prenos rečovej informácie, ten v sebe obsahuje aj dodatočné informácie napr. špecifické pre hovoriaceho, ktoré sú dané veľkosťou, tvarom a tuhosťou jednotlivých hlasových orgánov, náladou, zdravotným stavom, vzdelaním, povahou, pôvodom, zvykmi, atď.

Spôsob zakódovania týchto informácií do rečového signálu nie je úplné známy ako aj samotný matematický opis takejto operácie. Preto je pomerne náročné separovať a extrahovať jednotlivé príznaky pre zvolenú oblasť spracovania reči (rozpoznávanie reči, identifikácia hovoriaceho, atď.). Navyše reč obsahuje veľkú variabilitu hovoriaceho spôsobenú rôznymi vplyvmi, napr. náladou, fyzickým stavom, chorobou, atď. Nakoniec signál môže byť značne degradovaný prítomnosťou šumov a vplyvom nahrávacích zariadení a prostredí, kde k nahrávaniu došlo.

Modifikácie signálu, ktoré nie sú spôsobené rečníkom (zariadenia, priestor, atd.) sa označujú ako zmeny relácie. Tieto zmeny majú významný vplyv na úspešnosť identifikácie a preto musia byť ošetrené. To platí najmä v prípadoch, keď sa podmienky nahrávania nezhodujú s podmienkami nasadenia.

2.3 Extrakcia príznakov reči

Vzhľadom na množstvo problémov spomenutých v predošlom texte a vlastnosti reči, bolo nájdených veľa metód parametrizujúcich reč. Dobré príznaky pre identifikáciu však musia spĺňať nasledovné vlastnosti:

- Diskriminatívnosť medzi hovoriacimi
- Odolnosť voči šumom pozadia
- Necitlivosť voči vplyvom nahrávacích zariadení a prostredí
- Musia potláčať variabilitu hovoriaceho
- Musia byť ľahko získateľné

Pretože existuje veľa rozdielnych príznakov, ktoré sledujú parametre rôznych fyzikálnych vlastností, príznaky pre identifikáciu hovoriaceho sa delia do viacerých úrovní:

- Akustické
- Prozodické
- Príznaky vyššej úrovne

Na akustickej úrovni sa extrahujú príznaky z krátkych časových intervalov (10-30 ms), ktoré majú za cieľ opísať akustickú stránku zvuku. Zvyčajne sa jedná o modifikované obálky spektra a pod. Takéto príznaky teda súvisia s fyzickými vlastnosťami hlasových orgánov jedinca. Navyše tieto príznaky v sebe zhŕňajú rozličné psychoakustické fenomény, tak ako to robí sluchový systém človeka. To zvyšuje odolnosť voči šumom a vplyvu prostredia. V súčasnosti najpoužívanejšie a najúspešnejšie sú *Melovo frekvenčné kepstrálne koeficienty* **(MFCC)**, *perceptuálna lineárna predikcia* **(PLP)** a *kepstrálne lineárne predikčné koeficienty* **(CLPC)**. MFCC a PLP sa snažia vystihnúť modifikovanú obálku spektra využívajúc psychoakustické princípy ako odlišné vnímanie výšky tónu ľuďmi (iná frekvenčná stupnica ako Hz), kritické pásma, krivka rovnakej hlasitosti, atď. Tieto príznaky sú schopné zachytiť počet, polohu aj tvar formantových frekvencií, ktoré sú nevyhnutné na správny vnem zvuku. Preto sú dôležité najmä pre oblasť rozpoznávania reči. Pri identifikácií rečníka však tiež hrajú významnú úlohu, keďže sú schopné vystihnúť aj menšie zmeny formantových frekvencií v závislosti od hovoriaceho ku hovoriacemu. Polohy formantových frekvencií sa totiž nelíšia len od hlásky ku hláske ale aj medzi hovoriacimi. CLPC príznaky sa na druhú stranu snažia opísať (odhadnúť) parametre modelu produkcie reči, čím by bolo možné modelovať (určiť) konkrétneho hovoriaceho (jeho hlasový trakt). K spomenutým akustickým príznakom sa často konštruujú dynamické parametre, ktoré majú za cieľ vystihnúť ich vývoj v čase, ktorý je tiež špecifický pre konkrétnych hovoriacich. Na to sa používajú diferenčné alebo akceleračné koeficienty počítané z väčšieho časového rámca.

Príznaky na prozodickej úrovni sa skôr zameriavajú na charakter reči, spôsob hovorenia, návyky pri hovorení, fyzický a zdravotný stav, atď. Samozrejme táto

informácia je rozprestretá v širšom časovom úseku v rozmedzí niekoľkých sekúnd. Najviac preferované črty na tejto úrovni sú: rytmus, dynamika reči, rýchlosť hovorenia, modulácia hlasivkovej frekvencie, tvorba páuz, atď. Na druhej strane tieto príznaky sú ťažšie extrahovateľné a kvantifikovateľné ako na akustickej úrovni. Preto existuje viacero metód na ich získanie. Najbežnejšie sú pre detekcie hlasivkovej periódy: *priemerná magnitúda diferenčnej funkcie* (**AMDF)**, autokorelačná funkcia, inverzné filtrovanie, a pod.. Pre dynamiku reči je to priebeh energie v čase atď. Samozrejme okrem základných metód existuje množstvo ich modifikácií.

2.4 Klasifikácia- algoritmus rozhodovania

Po fáze extrakcie príznakov a ich prípadnej normalizácií (bude opísaná v ďalšej časti) nasleduje fáza klasifikácie, resp. rozhodnutia, kde sa určí ktorému hovoriacemu dané príznaky reči najlepšie zodpovedajú. Samozrejme je možné zamietnuť urobiť rozhodnutie v prípade nízkej dôveryhodnosti výsledku. Existuje veľa vhodných, prakticky použiteľných klasifikačných metód, ktoré sa vzhľadom na rôznu činnosť spracovania a komplexnosť ďalej delia do viacerých skupín so svojimi výhodami a negatívami:

- **Neparametrické metódy**- tieto nepredpokladajú žiaden model rozloženia dát v priestore. Ich hlavným reprezentantom je metóda *K najbližších susedov* (**KNN**). KNN hľadá K najbližších príznakov v priestore k neznámemu a na základe nich urobí výsledné rozhodnutie. Je to jednoduchá metóda, ktorá pri nedostatku dát zvyčajne dosahuje menšiu robustnosť.

- **Parametrické metódy** predpokladajú známu distribúciu, podľa ktorej sú dáta v priestore rozložené. Potom je potrebné už len správne odhadnúť parametre takýchto modelov na základe trénovacích dát. V prípade malého množstva dát dosahujú vyššiu robustnosť. Ich hlavným reprezentantom je *zmes Gaussových funkcií* **(GMM)**. Tento model predpokladá, že priestor je opísaný kombináciou Gaussových rozdelení.

- **Diskriminatívne metódy** namiesto čo najlepšieho opisu rozloženia dát v priestore sa snažia nájsť rozhodovaciu funkciu tak, aby sa dosahovala, čo najmenšia chyba rozhodovania. Usilujú sa maximalizovať aj robustnosť pre nevidené dáta. V takomto prípade dosahujú aj vyššiu generalizačnú schopnosť. Medzi najvýznamnejšie metódy patria *neurónové siete* **(NN)** a *systémy s podpornými vektormi* **(SVM)**.

- **Generatívne (opisné) metódy** sa snažia popísať dáta v priestore a nerozdeľovať ich primárne do tried. Ak sa podarí dokonale opísať rozloženie dát, je pomocou nich teoretický možné skonštruovať optimálny klasifikátor (Bayesov). Medzi najvýznamnejšie metódy v tejto oblasti patrí GMM.

Ukázalo sa ako vhodné konštruovať modely všeobecných hovoriacich, ktoré boli postavené na veľkom množstve rôznych hovoriacich tak, aby pokrývali širokú populáciu. Tie je potom možné používať pri stanovení prahov zamietnutia alebo pre adaptáciu špecifických modelov.

2.5 Kompenzácia vplyvu prostredia

Na potlačenie vplyvu zmien prostredia (podmienok pri trénovaní a testovaní: šumy, nahrávacie zariadenia, prostredie, atď.) a aj samotného hovoriaceho bolo vynájdených veľa metód využívajúcich rôzne predpoklady a spôsoby činnosti. Najjednoduchšie metódy normalizujú príznaky napr. tak, aby mali rovnakú energiu v meraných pásmach (ekvalizácia). Často sa to robí odčítaním priemerného kepstra. Ďalej je možné využiť fixne nastavené filtre, ktoré majú za cieľ zvýrazňovať modulačné spektrum reči, alebo pomocou tzv. relatívnej spektrálnej analýzy (RASTA). Sofistikovanejšie metódy sa snažia nájsť vhodnú transformáciu medzi príznakmi z trénovacej fáze a aktuálne spracovanými. Tento prístup sa označuje za mapovanie príznakov. Je možné transformovať aj celé modely hovoriacich tak, aby zodpovedali aktuálnemu rozloženiu dát. Toto sa označuje ako syntéza modelov hovoriacich. Posledne spomenuté metódy pracujú na základe aktuálnych dát preto je možná ich adaptácia v čase pri zmene prostredia. To si však vyžaduje podstatne zložitejšie algoritmy spracovania signálov.

Menej sofistikovanejšia metóda, ktorá ale dosahuje dobré výsledky je mať dáta/modely pre rôzne typy prostredí. Potom po správnej detekcií najbližšieho prostredia použiť práve tieto dáta alebo modely, čím sa dosiahne najmenší rozdiel medzi trénovacími a testovacími podmienkami, čo vedie k minimalizácií chybovosti.

Pre získanie ucelenejšieho a podrobnejšieho prehľadu o technológiách a metódach použitých pre oblasť rozpoznávania rečníka viď napr. [2].

3 Rozpoznanie tváre

Tvár sa postupne stáva najatraktívnejšou biometriou a systémy rozpoznania tváre pre identifikáciu osôb sú stále viac využívané vo veľkom množstve aplikácií. Vývoj algoritmov a metód rozpoznávania tiež umožňuje využiť systémy na identifikáciu a verifikáciu v komerčnej oblasti. Avšak tieto systémy nedosahujú porovnateľné výsledky v nekontrolovaných a neobmedzených podmienkach. Rozpoznávanie tvárí za týchto podmienok je stále náročný problém aj napriek nedávnym pokrokom v tejto oblasti.

Biometrické systémy pre identifikáciu osôb, ktoré sú vyvinuté niekoľkými spoločnosťami, dosahujú vysokú presnosť v rozpoznávaní tvárí. Väčšina z týchto aplikácií musí spĺňať [3]:

- Dokáže rozpoznať niekoľko tvárí z jedného video záberu alebo jedného obrázku
- Vysokú úspešnosť rozpoznávania
- Nezávislosť od svetelných podmienok
- Stabilitu pri zmene výrazu tváre alebo pózy
- Rozpoznanie v reálnom čase, atď.

Môžeme vidieť, že je niekoľko faktorov, ktoré môžu ovplyvniť výkon a presnosť systému pre rozpoznávanie tvárí [1]:

- **Osvetlenie** - zmeny osvetlenia v dôsledku vlastností odrazivosti kože a vďaka vnútornej kontrole kamery. Niektoré 2D metódy plnia dobre úlohu rozpoznávania len pri malých zmenách osvetlenia.
- **Zmena pózy -** ovplyvňuje proces autentifikácie, pretože predstavuje deformáciu objektu. Detekčné metódy by mali riešiť problém s ohľadom na rôzne uhly pohľadu na umiestnený objekt (napr. výhľad z bezpečnostných kamier). Na druhej strane sú rozpoznávacie algoritmy relatívne robustné čo sa týka výrazu tváre (s výnimkou niektorých extrémnych výrazov ako výkrik).
- **Doba oneskorenia** - je tiež dôležitým faktorom, zahŕňajúcim zmeny v tvári človeka počas určitej dlhej doby. Všeobecne je tento problém ťažko vyriešiť vzhľadom na ostatné problémy.

3.1 Metódy rozpoznávania tváre

Systémy rozpoznávania tvári spadajú do dvoch kategórií: verifikácia a identifikácia.

Verifikácia tváre zodpovedá zhode 1:1. V tomto procese sa obraz tváre, ktorého identita sa overuje, porovnáva s šablónami snímok tváre.

Naopak, identifikácia tváre je 1: N problém. Obraz tváre je porovnaný so všetkými obrazovými šablónami v databáze tvárí pre stanovenie identity tváre.

V prípade, že nevieme, či testovaná tvár je v databáze systému, postup je nasledujúci. Obrázok s tvárou je porovnaný so všetkými obrazmi tvárí v databáze a vyhodnotí sa pravdepodobnosť zhody pre každú z nich. Všetky tieto pravdepodobnosti sú numericky zoradené: najvyššia hodnota je ako prvá. V prípade, že pravdepodobnosť je vyššia ako nastavená prahová hodnota, systém nás informuje o výsledku [1].

Základné vybrané metódy 2D rozpoznania tvári:

- Lineárne/nelineárne projekčné metódy
    - *Principal Component Analysis* (**PCA**) - metóda založená na PCA sa volá „eigenface“. Hlavnou myšlienkou PCA je rozložiť dátový priestor na lineárnu kombináciu malého počtu bázových funkcii, ktoré sú ortogonálne a ktoré reprezentujú maximálnu variáciu smerov v trénovacej sade [4].
    - *Kernel Principal Component Analysis* (**KPCA**) - je metóda nelineárnej extrakcie príznakov. KPCA môže získať sadu príznakov, ktoré sú vhodnejšie pre kategorizáciu než konvenčné PCA. KPCA je široko používaný v prípade rozpoznania tváre s výrazom a pri rôznych svetelných podmienkach [4].
    - *Linear Discriminant Analysis* (**LDA**) – bola navrhnutá ako lepšia alternatíva k PCA. Poskytuje rozdelenie medzi triedami, zatiaľ čo PCA sa zaoberá vstupnými dátami v celom ich rozsahu bez toho, aby venovala pozornosť základnej štruktúre. V skutočnosti hlavný cieľ LDA spočíva v nájdení bázy vektorov, ktoré poskytujú najlepšiu diskrimináciu medzi triedami. LDA sa snaží maximalizovať rozdiely medzi triedami, čím sa minimalizujú rozdiely v rámci svojej triede [1].
    - *Discriminant Common Vectors* (**DCV**) - hlavná myšlienka DCV spočíva v zhromažďovaní podobnosti medzi prvkami v rovnakej triede a vylúčením ich odlišnosti [1].
- Neurónové siete – je nelineárne riešenie, používa sa aj v iných oblastiach rozpoznávania vzorov. Výhodou neurónových klasifikátorov oproti lineárnym je tá, že sa môže znížiť počet nesprávnych zaradení medzi susednými triedami. Základnou myšlienkou je, aby sa brala do úvahy sieť s neurónom pre každý pixel v obraze. Avšak, vzhľadom na rozmery vzorov, neurónové siete nie sú

priamo trénované so vstupnými obrazmi. Pred procesom trénovania sa používajú techniky znižujúce počet rozmerov.

- Systémy iterovaných funkcií (*iterated function systems - IFS)* – IFS teória bola vyvinutá predovšetkým v oblasti kódovania obrazu a nedávno bola rozšírená na indexovanie obrazu. Fraktálny kód obrázku je nemenný vzhľadom na širokú sadu globálnych transformácií ako je rotácia, kontrastné škálovanie, atď. IFS obrazu tváre sa používa pri trénovaní neurónových sietí, kde sa používa ako klasifikátor [1].

3.2 Extrakcia príznakov

Niektoré algoritmy rozpoznávania tváre sú založené na príznakoch extrahovaných z obrazu tváre človeka - nazývaných tvárové príznaky. Napríklad algoritmus môže analyzovať relatívnu polohu, veľkosť, a/alebo tvar očí, nosa, úst, lícnych kostí a čeľuste. Tieto príznaky sú potom použité pri hľadaní zodpovedajúcich príznakov v skupine snímok. Ostatné algoritmy normalizujú galériu snímok tváre a potom komprimujú dáta tým, že ukladajú iba dáta v obraze, ktoré sú užitočné pre rozpoznanie tváre. Testovaný obraz sa potom porovná s údajmi o tvári.

Pred získaním príznakov sú obrázky/snímky predspracované a normalizované.

Ako súčasť predspracovania je zníženie rozmerov všetkých vstupných snímok na definovanú veľkosť. Tiež je možné aplikovať **CLAHE** (*contrast limited adaptive histogram equalization)* - kontrastovo obmedzená adaptívna ekvalizácia histogramu. Normalizované snímky môžu byť maskované tak, aby sa vynechalo pozadie a ponechala sa iba oblasť tváre.

Hlavným cieľom procesu normalizácie je minimalizovať nekontrolované variácie, ktoré sa vyskytujú v priebehu získavania snímok a na udržiavanie odchýlok pozorovaných v tvárových príznakoch medzi jednotlivcami.

Veľkú zmenu v obraze môže spôsobiť zmena pózy.

Extrakcia príznakov zahŕňa zníženie množstva prostriedkov potrebných k popisu veľkého súboru dát. Pri rozpoznaní tváre sa vykonáva analýza veľkého množstva dát. Analýza s veľkým počtom premenných všeobecne vyžaduje veľké množstvo pamäte a výpočtovej sily. Extrakcia príznakov sa vzťahuje k zníženiu premenných a dát.

Pri extrakcii príznakov sa najčastejšie využívajú metódy založené na detekcií hrán. Veľmi dobré výsledky sa dosahujú aj pri lokálnych binárnych vzoroch (*local binary patterns* **LBP**).

Detekcia hrán je názov pre sadu matematických metód. Hlavným cieľom je detekovať body v digitálnom obraze, kde sa prudko mení jas. Tieto obrazové body s ostrou zmenou jasu sú obvykle usporiadané do zostavy zakrivených čiar pomenovaných hrany.

Najčastejšie používane funkcie na detekciu hrán sú Sobelov operátor (nazývaný tiež Sobelov filter), Prewittov operátor alebo Gaborov filter.

Príznaky sa môžu získať z predspracovaných snímok tvárí pomocou LBP histogramu. LBP historgramy sa považujú za jedny z najlepších príznakov pre

rozpoznávanie tvárí, keď je k dispozícií iba limitované množstvo vzoriek a môžu byť ľahko vypočítané v reálnom čase [5] (Fig. 2.1).

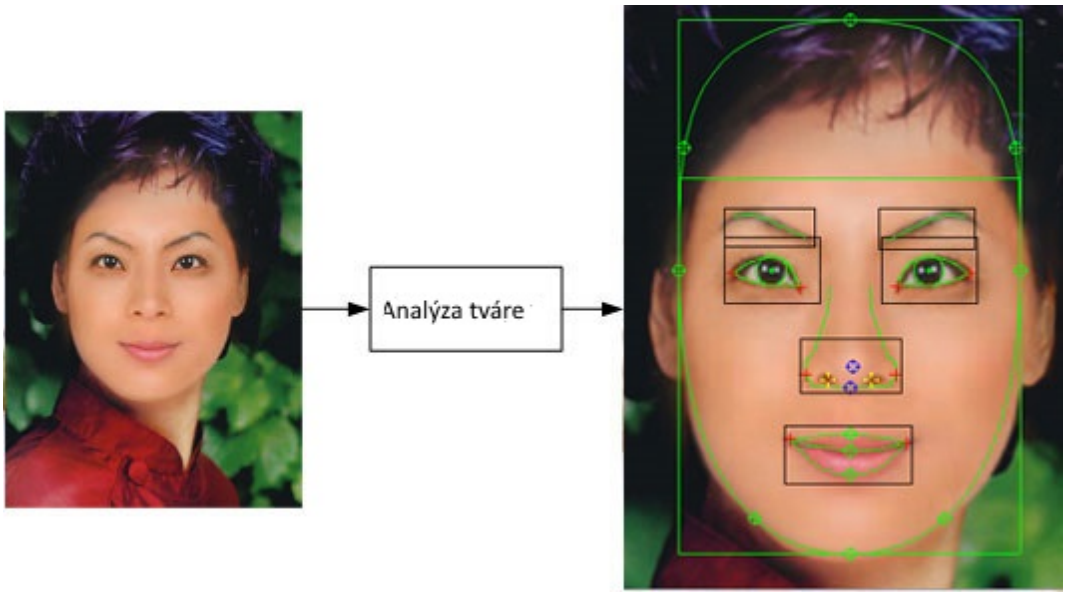


Fig. 2.1 – Príklad získaných príznakov

3.3 Klasifikácia tvárí

Systém rozpoznávania tvárí pracuje zvyčajne v dvoch hlavných fázach. Prvá fáza je proces trénovania a druhý je klasifikácia používateľov. Moderné metódy rozpoznávania tváre správne fungujú ak je k dispozícii vo fáze trénovania až 10 snímok jednej osoby. Veľa rôznych techník bolo vyvinutých pre rozpoznanie tváre iba z jedného obrazu danej osoby. Trénovacia fáza by mala byť plne automatizovaná a používatelia ju musia byť schopní ovládať. Tréningový proces používa algoritmy zhlukovania (clustering algoritmy).

Hlavným cieľom všetkých zhlukovacích (clustering) algoritmov je vytvoriť zhluk (cluster) alebo triedu vo vstupnom dátovom súbore. Existuje mnoho algoritmy zhlukovania. Tieto algoritmy môžu byť rozdelené do dvoch skupín: deliace a hierarchické algoritmy [5].

Ako príklad zhlukovacieho algoritmu môžeme spomenúť K-means algoritmus. Ďalším algoritmom na vytvorenie zhlukov je tzv. samorganizujúca mapa - *self-organizing map* (**SOM**), patriaca k neurónovým sieťam alebo algoritmus priestorového zhlukovania založený na hustote prvkov (*density-based spatial clustering of applications with noise* - **DBSCAN**).

Pre klasifikáciu príznakov získaných z tvárí môžeme spomenúť dva spôsoby v závislosti od počtu trénovacích snímok a počtu identít použitých v rámci systému:

- Systémy s podpornými vektormi (Support Vector Machines) - používajú sa iba keď sa v systéme uvažuje relatívne malý počet identít. Hlavnou nevýhodou tejto metódy je časovo náročné trénovanie modelu, keď sa použije väčší počet vzoriek.
- Systémy na báze K najbližších susedov (K-Nearest neighbour) - tento algoritmus môže byť ľahko použitý v distribuovanom systéme. Trénovanie sa vykonáva jednoducho vložením príznaku do databázy [5].

3.4 Lokalizácia a rozpoznanie tváre

Biometrické systémy, konkrétne systémy rozpoznávania tváre, sú široko využívané v mnohých rôznych typoch aplikácií. Typickým príkladom takejto aplikácie v súčasnej dobe je inteligentná TV so systémom rozpoznávania tvárí. Rozpoznávanie tvárí v smart TV sa používa na autentifikáciu používateľa. Na základe toho môžu byť poskytnuté personalizované služby alebo odporučené rôzne programy. Systémy rozpoznávania tvárí by mali pracovať v reálnom čase a mali by byť schopné rozpoznať jednu alebo viac identít/osôb. Väčšina z týchto systémov má v sebe zahrnuté tiež grafické užívateľské rozhranie pre automatický proces trénovania (Fig. 2.2).

Obvykle 2D prístup rozpoznávania tvárí vyžaduje spracovanie vstupu z fotoaparátu alebo kamery. Hlavný proces rozpoznávania tvárí sa skladá z týchto čiastkových úloh:

- Získanie vstupného obrazu - číta obraz z kamery, prevedie ho do formátu požadovaného systémom a odovzdá ho ďalej na spracovanie
- **Lokalizácia tváre** - lokalizuje tváre v obraze a priradí mu súradnice. V závislosti na použitom fotoaparáte/kamere je určený lokalizačný algoritmus.
- **Trénovací proces** – využíva zhlukovacie algoritmy ako napr. K-means
- **Predspracovanie** lokalizovaných tvári zahŕňa optimalizáciu histogramu
- **Normalizácia** – napr. zmena rozmerov obrázku
- **Získavanie príznakov** – získava príznaky z predspracovaných tvári, napr. LBP využitie
- **Klasifikácia tvári** (v obraze) – využíva metódy ako Support Vector Machines alebo K-Nearest neighbor distance matching
- **Sledovanie tvári** (v obraze) - zvyčajne sa sledujú iba tváre z prednej strany, pretože drvivá väčšina metód rozpoznávania tvárí je spoľahlivá len pri práci s čelným snímkom tváre. Akonáhle je tvár rozpoznaná, začne sledovanie, čo výrazne šetrí výpočtové zdroje a umožňuje sledovať objekt aj po zmenách pózy [3]. Takže informácia o rozpoznanom používateľovi sa pošle ako výstup zo systému.

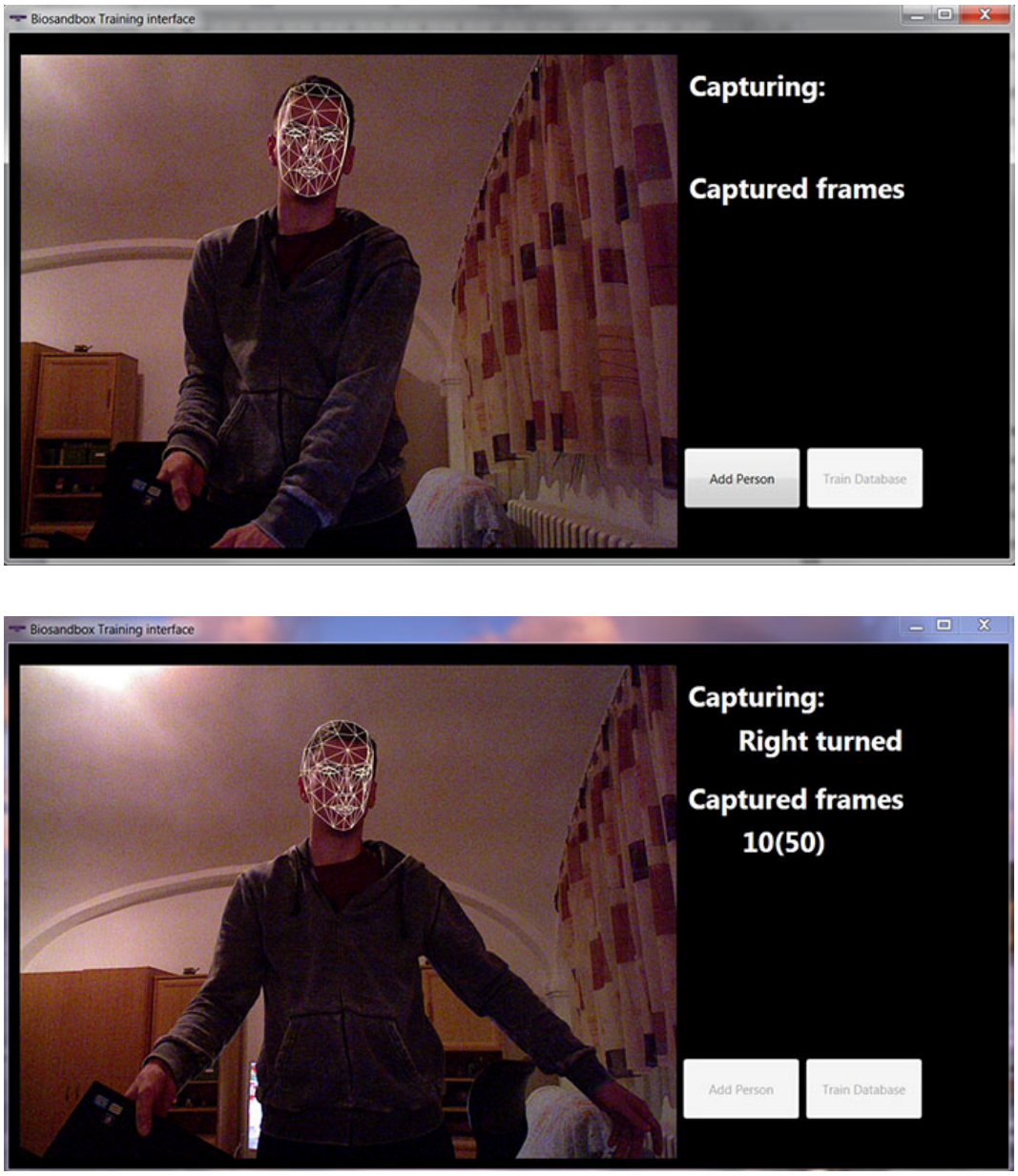


Fig. 2.2 – Príklad trénovacieho GUI pri systéme s rozpoznaním tváre (GUI ponúka možnosť pridať nového používateľa stlačením tlačidla ‘Add Person‘, trénovanie databázy stlačením tlačidla ‘Train Database‘. Na obrazovke vidieť stav nahrávania – ‚Capturing‘ a množstvo zachytených rámcov – ‚Captured frames‘.)

3.5 Rozpoznanie dúhovky

Dúhovka je jedným z najpopulárnejších biometrických charakteristík. Kombinácia bezdotykového snímania, časovej stability a vysokej presnosti rozpoznávania umožňujú použitie v bezpečnostných aplikáciách a iných dozorných zložkách.

Bolo dokázané, že presnosť rozpoznávania dúhovky závisí na kvalite zachyteného obrazu očnej dúhovky a predspracovania obrazu. **NIR** (*near infrarred*) snímacia kamera je odporúčaná na zníženie negatívneho vplyvu osvetlenia (pozri obr. 2.3). Použitie NIR umožňuje pridať extra svetelný zdroja bez vplyvu na pohodlie snímania.

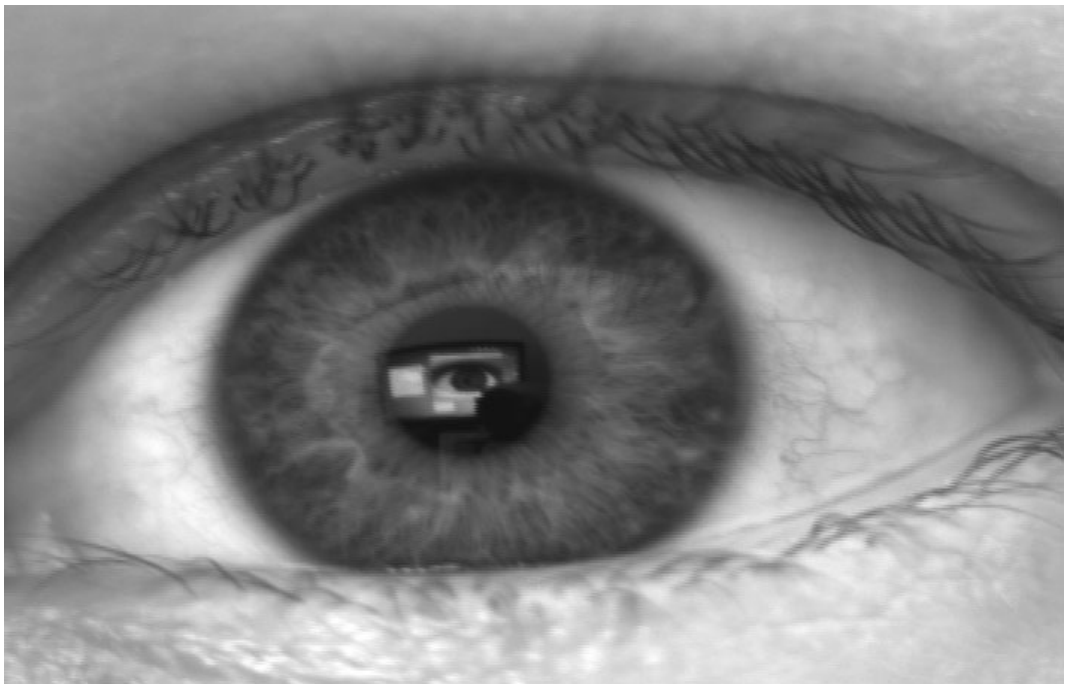


Fig. 2.3 – Príklad snímania obrazu kamerou Guppy F-038B NIR

Identifikácia založená na rozpoznaní dúhovky sa skladá z lokalizácie dúhovky, extrakcie príznakov a klasifikácie. Jeden z najúspešnejších systémov dosahuje presnosť 100% v kontrolovaných podmienkach. Ale proces lokalizácie a normalizácie pre aplikácie v skutočnom živote je potrebné zlepšiť. Tento systém používa Gaborov filter na extrakciu príznakov, kde sú filtrované signály kvantované do dvoch úrovní. Týmto postupom sa získajú reťazce binárnych čísel (príznaky). Porovnaním najbližších vzoriek pomocou metódy KNN a Hammingovej vzdialenosti dostávame rozpoznanie dúhovky.

4 Rozpoznanie 3D tváre

Rozpoznávanie tvárí na základe 2D prístupu je bežný a prirodzený postup. Prístup 3D rozpoznávania tváre dosahuje všeobecne vyššiu bezpečnosť než 2D prístup pre rozpoznávanie tvárí.

Techniky založené na 3D rozpoznávaní tváre by mali spĺňať niekoľko náležitosti, ako je odolnosť s ohľadom na zmeny osvetlenia, rovnako ako aj na zmenu polohy, natočenia a úpravy pôvodného modelu v rámci absolútnej vzťažnej sústavy [1].

4.1 Metódy rozpoznania 3D tváre

3D rozpoznanie tváre v porovnaní s 2D rozpoznávaním tváre využíva väčší tok informácií o charakteristikách tváre. Obidva prístupy však potrebujú základné predspracovanie, ako je normalizácie obrazu tváre, otočenie do neutrálnej polohy atď. Pridaná informácia nielen o 2D tvári, ale aj hĺbková analýza ponúka bohatý zdroj informácií, ktoré nie sú zachytené v 2D obrazoch. Hlavné výhody 3D oproti 2D analýze tváre sú:

- Nie je ovplyvnený zmenami osvetlenia alebo použitím kozmetiky
- Menej citlivé na zmeny vzhľadu
- Ľahšie sa zvláda zmena pózy
- Projektívna povaha 2D obrazu
- Zjednodušuje detekciu tváre a tvárových príznakov, odhaduje pózu

Vybrané základné metódy na 3D detekciu tváre:

- 3D rozpoznanie tváre na princípe analýzy povrchu - tento prístup je založený na klasickom 3D rozpoznávaní objektov (viď obr. 3.1). Existujú rôzne typy metód rozpoznávania založené na:
    - Použitie miestne zakrivených prvkov, ktoré sú nezávislé od otáčania (napr. krivka profilu tváre)
    - Použitie párovania bod-bod (polygón niekoľkých významných bodov tváre)

Fig. 3.1 – 3D rozpoznanie tváre na princípe analýzy povrchu

- 3D rozpoznanie tváre na princípe analýzy vzhľadu - táto metóda sa zaoberá technikou „eigenfaces“ a „fisherfaces“. Požaduje sa presné zarovnanie snímača a obrázkov v databáze. Tvárové príznaky ako sú oči, ústa, atď. sú lokalizované a využité pre rozpoznanie. Táto metóda sa dá ľahko implementovať a nie je časovo náročná (obr. 3.2).

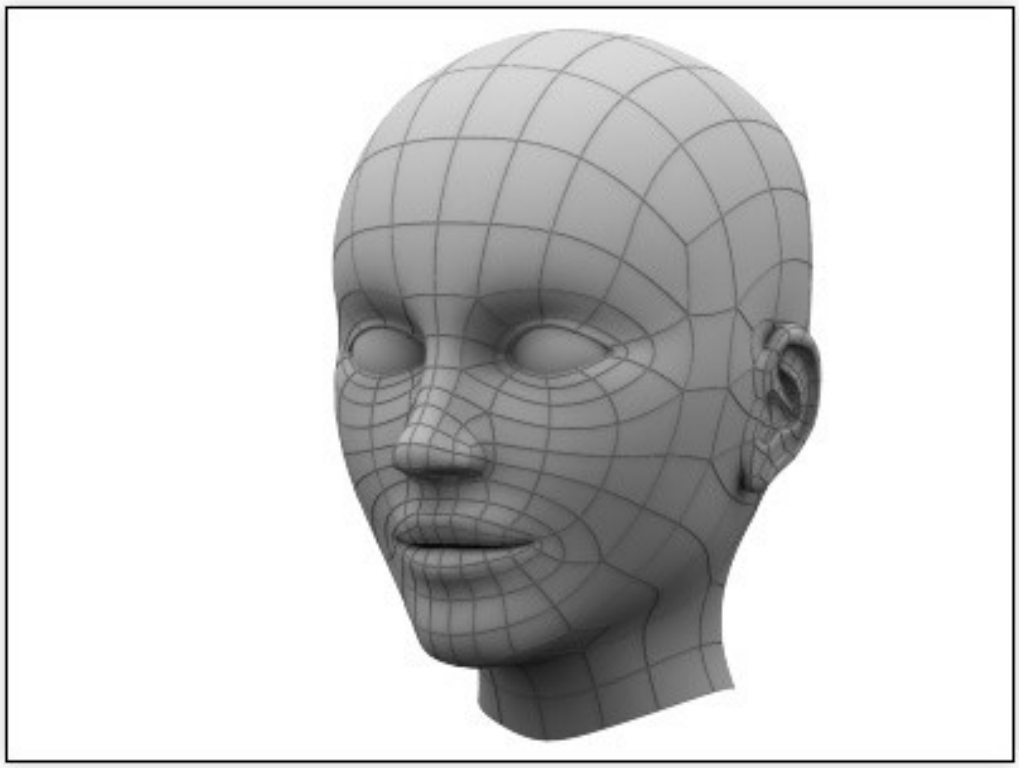


Fig. 3.2 – 3D rozpoznanie tváre na princípe analýzy vzhľadu

- 3D rozpoznanie tváre na princípe analýzy modelu **-** táto metóda je založená na metóde analýzy syntézou. Vytvorí sa 3D model tváre s označenými a popísanými parametrami, ktorý sa porovnáva s modelmi v databáze. Táto metóda nie je vhodná pre aplikácie v reálnom čase (Fig. 3.3).

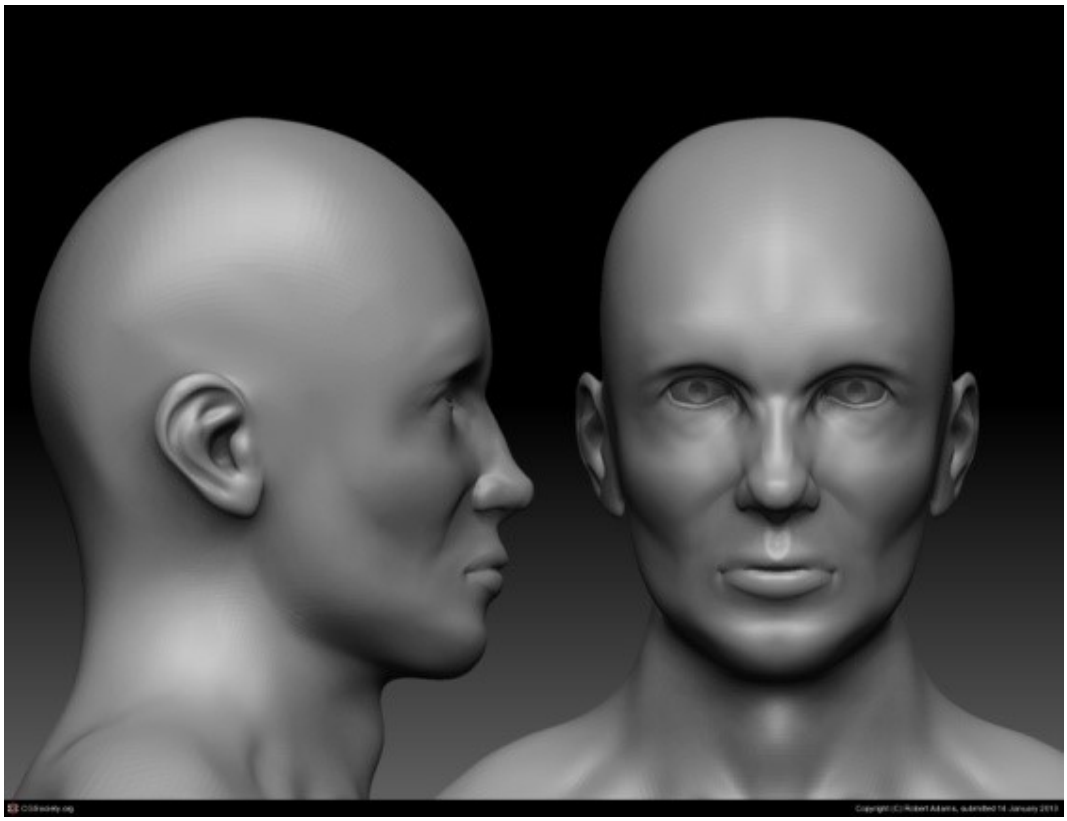


Fig. 3.3 – 3D rozpoznanie tváre na princípe analýzy modelu

4.2 Predspracovanie a registrácia dát

Na začiatku celého procesu sa zachytí 3D maska povrchu tváre (príklad vytvorenie 3D tváre je na obrázkoch obr. 3.4. - obr. 3.6). Existuje niekoľko rôznych spôsobov ako dosiahnuť zachytenie 3D povrchu tváre, napríklad stereo kamery, hĺbková kamera, laserová kamera, optické alebo laserové snímače, atď.

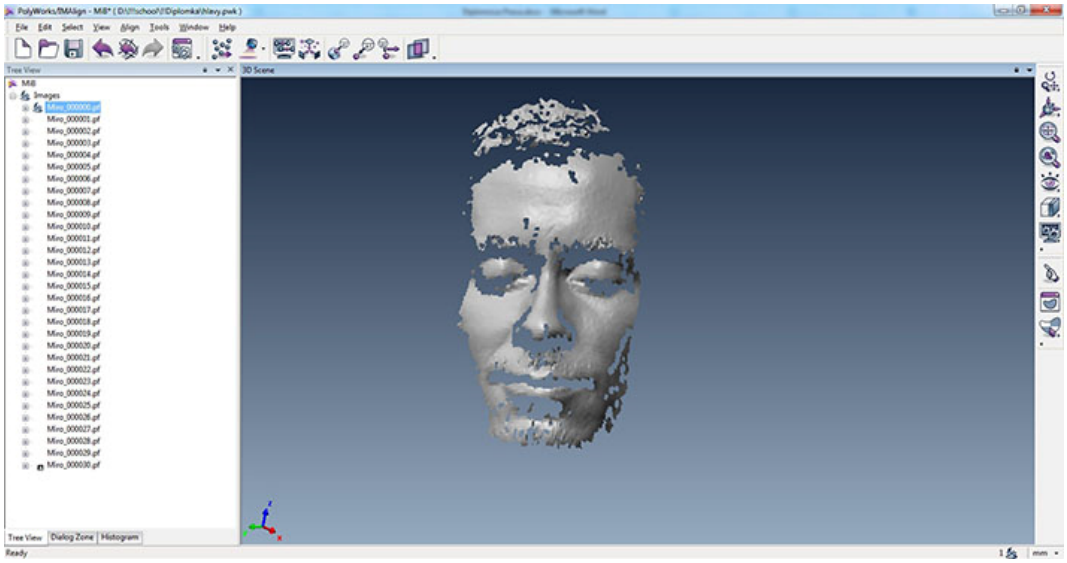


Fig. 3.4 – Jeden sken

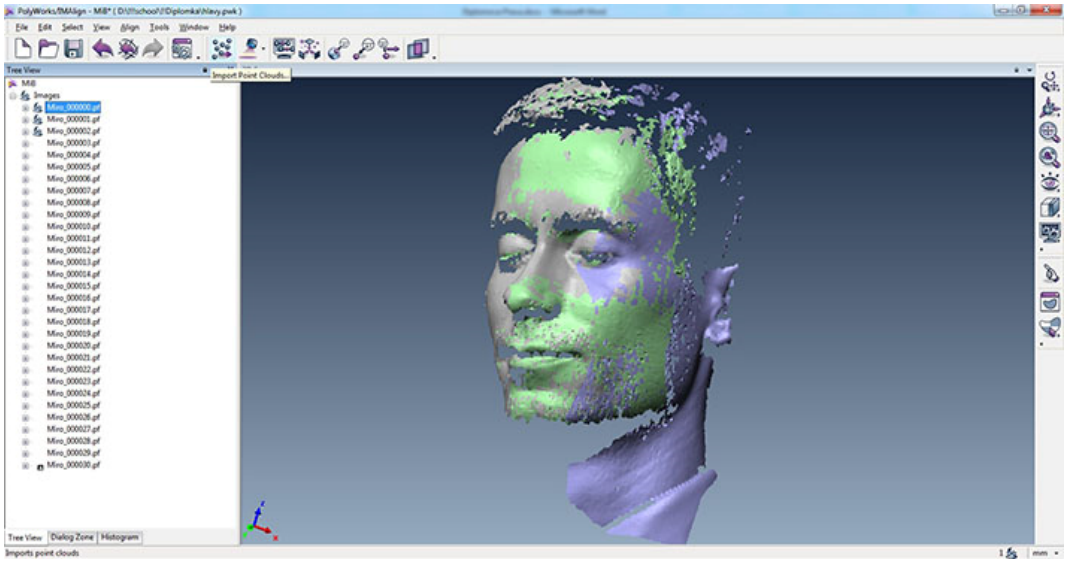


Fig. 3.5 – Viac skenov vytvárajúcich tvár

Fig. 3.6 – Výsledný 3D model tváre

Z celého nadobudnutého snímku je potrebná iba tvár. Vzhľadom k tomu je potrebné orezanie tváre. Každá tvár je ohraničená obdĺžnikom, ktorý sa skladá z 4 bodov na hlave. Bočné hrany sa skladajú z bodov, ktorých pozícia je najviac doľava a doprava. Najvyšší bod je horný okraj a spodný okraj obsahuje najnižší bod. Orezanie je potom založené na obdĺžniku vytvorenom 4 bodmi.

Zachytené údaje sú následne predspracované pomocou algoritmov na extrakciu príznakov.

Účelom extrakcie príznakov je získať kompaktné informácie z obrázkov, ktoré sú dôležité pre rozlišovanie medzi obrazmi tvárí rôznych ľudí a sú stabilné z pohľadu fotometrických a geometrických variácií v obraze.

Ako príznaky možno použiť body tváre (vrchol hlavy, čelo, oči, brada, nos, ústa, atď.) a vzdialenosti medzi týmito vybranými bodmi v 3D Euklidovskom priestore (viď obr. 3.7).

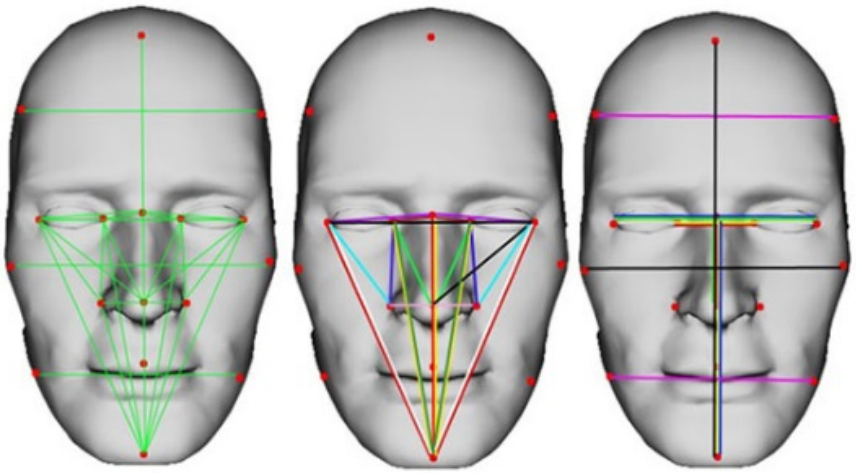


Fig. 3.7 – Príklad tvárových príznakov

4.3 Aplikácie pre rozpoznanie 3D tváre

3D rozpoznanie tváre možno tiež použiť v mnohých aplikáciách, napríklad na zabezpečený prístup do systému alebo rozpoznanie používateľa pre Smart TV a umožnenie online nakupovanie (napr. môže byť povolené len pre rodičov a nie pre deti, atď.).

3D prístup rozpoznávania tvárí vyžaduje rovnako ako 2D rozpoznávanie tvárí vstup z kamery. Pre 3D rozpoznávanie tváre je potrebné zachytiť 3D povrch tváre. Hlavný proces rozpoznávania tvárí sa skladá z nasledujúcich čiastkových procesov:

- **3D snímanie povrchu tváre** - existuje niekoľko rôznych spôsobov na realizáciu tejto úlohy, napríklad stereo kamery, laserové alebo hĺbkové kamery (napr. Kinect senzor Kinect), atď.
- **Predspracovanie** – zachytené údaje sú následne predspracované
- **Získavanie príznakov** - účelom extrakcie príznakov je získať kompaktné informácie z obrázkov, ktoré sú dôležité pre rozlišovanie medzi obrazmi tvárí rôznych ľudí a sú stabilné, pokiaľ ide o fotometrické a geometrické variácie v obrazoch
- **Meranie vzdialenosti -** posledný krok rozpoznávania 3D tváre je meranie vzdialenosti medzi 3D povrchom tváre používateľa a 3D tvárou uloženou vo vnútri databázy. Existuje niekoľko techník na meranie vzdialenosti. Najjednoduchší spôsob je meranie lokálnej a globálnej vzdialenosti dvoch tvárí, kde je potrebné správne a veľmi presne určiť body tváre (oči, nos, ústa, brada, uši, atď.) a meranie ich vzdialenosti od zavedených metrík. Sofistikovanejšie metódy sú metódy najbližšieho suseda alebo Support Vector Machine atď.

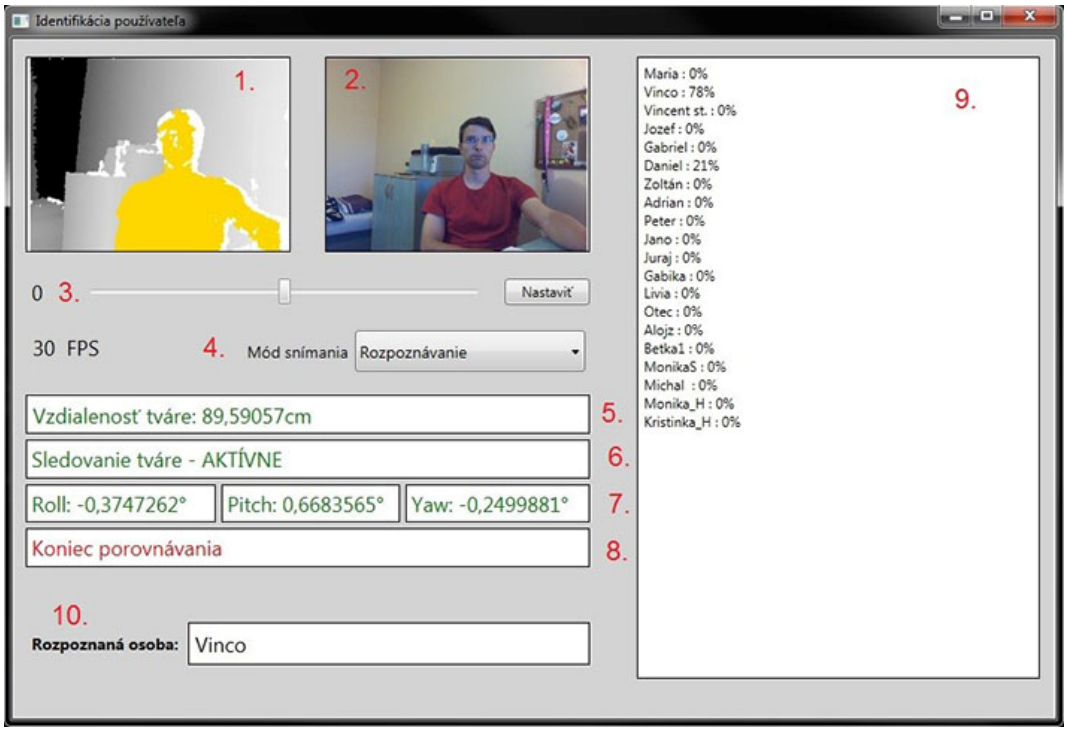


Fig. 3.8 – Príklad GUI v aplikácií 3D rozpoznania tvárí

5 Autentifikácia

Prístupová bezpečnosť systému je navrhovaná s ohľadom na to, aby umožnila prístup iba autorizovaným používateľom, ktorých identitu je predtým potrebné overiť. Jedná sa v zásade o tri odlišné kroky, konkrétne identifikáciu, autentifikáciu a autorizáciu [6].

Identifikácia – je krok, pri ktorom sa používateľ preukáže tzv. tokenom alebo identifikačným reťazcom, napr. v tvare e-mailovej adresy alebo tel. čísla.

Autentifikácia – po prijatí identifikačného tokenu musí identifikovaný používateľ poskytnúť dôkaz o svojej identite.

Autorizácia – Povoľuje alebo zakazuje používateľovi prístup ku požadovanému obsahu a vykonanie postupnosti akcií, na základe jeho oprávnení.

Používateľov systému je možné autentifikovať na základe toho, že niečo vedia (memometrics), niečo rozpoznajú (cognometrics), niečo vlastnia alebo čím sú charakteristickí (biometrics). Pri všetkých troch spôsoboch systém s používateľom zdieľajú tajomstvo (tzv. authentication key). Počas registrácie sa používateľ a systém dohodnú, čo tým tajomstvom bude. V prípade biometrie systém počas registrácie zaznamená digitálnu reprezentáciu niektorého aspektu používateľovej fyziológie alebo správania.

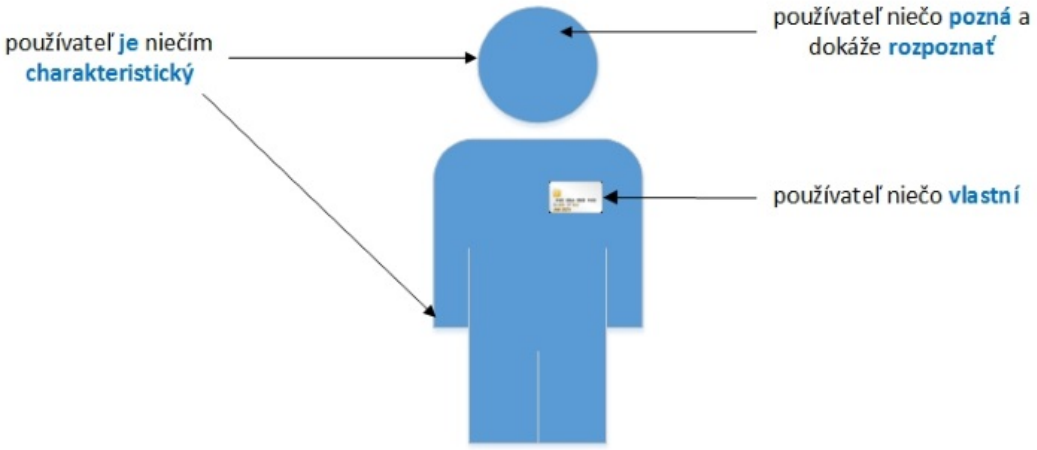


Fig. 4.1 – Možnosti autentifikácie používateľa

5.1 Typy autentifikačných mechanizmov

Nasledovná kapitola diskutuje o autentifikačných mechanizmoch, zoskupených do kategórií podľa spôsobov vymenovaných v úvode predošlej kapitoly.

Biometrics - charakteristika používateľa

Biometria je porovnávanie anatomickej, fyziologickej a behaviorálnej charakteristiky osoby.

Biometrické autentifikačné mechanizmy spadajú do dvoch základných kategórií:

- **Behaviorálna biometria** - založená napr. na pohyboch používateľa pri manipulácii s myšou počítača, latencii alebo dynamike úderov do klávesnice alebo dynamike podpisu.
- **Fyziologická charakteristika** - založená na odtlačkoch prstov, hlasu, zreničky alebo sietnice, rysovej charakteristike tváre, ruky alebo geometrii prstov alebo dokonca tvaru ucha.

Biometrické technológie je zložité medzi sebou porovnávať. Každá z nich má rôzny rozsah presnosti, spoľahlivosti a použiteľnosti. Aj napriek ťažkosti ich vzájomne porovnať však vieme povedať, akú váhu má presnosť verzus použiteľnosť a pod. V prípade použiteľnosti je jednoduchou biometrickou metódou napríklad rozpoznávanie tváre. Naopak metódy, ktoré vyžadujú nastavenie niektorej časti tela ku senzoru (rozpoznávanie sietnice), a teda sú menej komfortné na použitie, dokážu produkovať oveľa presnejšie výsledky.

Testovanie biometrie je komplikovaný proces, ktorý vyžaduje objektívne porovnanie. Biometrická autentifikácia preto nie je jednoduchý proces typu áno/nie, ale zahŕňa komplikovanú štatistickú analýzu údajov, získaných zo senzorov v reálnom čase.

Na svete exituje niekoľko súkromných aj verejných testovacích laboratórií, ktoré presadzujú nastavenie štandardov tejto oblasti, ako napríklad *National Institutes of Standards and technology* (**NIST**) alebo The International Biometric Group [6].

Memometrics - znalosť niečoho

V tomto prípade ide o generovanie náhodných sekvencií znakov alebo čísel, ktoré sú nazývané heslom (ak ide o slovo), PINom (ak ide o číselné vyjadrenie) alebo tzv. frázu (passphrase; ak ide o viac ako jedno slovo). Heslá však môžu mať je podobu sémantického tvaru.

Typy hesiel:

- Náhodné heslo – v súčasnosti je asi najpopulárnejším autentifikačným mechanizmom náhodné heslo. Heslá majú veľký potenciál byť dostatočne bezpečnými. To ale nemusí platiť v nekontrolovanom prostredí, akým je webové prostredie. Používatelia si z dôvodu ľahšieho zapamätania volia heslo sami, aj napriek tomu, že systém dokáže ponúknuť silnejšie heslo. Systémom ponúknuté heslo však často skončí zapísané na papieri, nakoľko je problematické si ho zapamätať. Poskytovatelia web aplikácií preto preferujú používateľom stanovené heslo. [7].

- Sémantické heslá – sémantické heslá sú založené na tvorbe tajomstva na základe deduktívneho procesu. Tento proces pozostáva zo zadávania otázok s cieľom získať presnú odpoveď, ktorú vyžaduje (Fig. 4.2). Teoreticky môžu mať používatelia s vyvolaním hesla menší problém, nakoľko kognitívne heslá sú založené na vyvolaní známeho faktu, ktorý si používateľ musí pamätať. Návrh bezpečnostných systémov založených na tomto spôsobe nie je vôbec triviálny [8].

Fig. 4.2 – Základné princípy sémantických hesiel

Cognometrics - rozpoznanie niečoho používateľom

Idea grafickej autentifikácie je založená na vizuálnej pamäti používateľa. Vedecké štúdie poukazujú na fakt, že ľudská bytosť má obrovské a prakticky neobmedzené možnosti pamätať si obrázky [9].

Grafické kódy si získavajú na popularite hlavne v prípade mobilných technológií, napr. pre odblokovanie mobilného telefónu. Existujú dva hlavné princípy:

- **Grafické kódy založené na rozpoznávaní** - používateľ vyberie cieľový obrázok z pomedzi množstva rušivých elementov v scéne. Pri tomto prístupe, ktorý je čisto založený na vizuálnej pamäti, sa využíva schopnosť rozpoznať predtým videný objekt medzi množstvom ostatných.
- **Grafické kódy založené na pozícii** - používateľ pri tomto prístupe musí nakresliť obrazec, zvyčajne do mriežky, kde sa vyžaduje vizuálno-priestorová pamäť a presný pohyb.

Vlastníctvo

Autentifikácia môže byť založená na niečom, čo používateľ vlastní. Týmto objektom je tzv. token. Dobrým príkladom tokenu je SecureID od RSA Security na Fig. 4.3. [15]

Fig. 4.3 – Príklad tokenu: Bezpečnostné ID – RSA Security

Token prostredníctvom šifrovacej funkcie, ktorá kombinuje zámok a tajný kľúč, vytvára numerický kód, zobrazovaný na LCD displeji. Na autentifikáciu použije vlastník SecureID zobrazené číslo. Autentifikačný server taktiež pozná tajomstvo uložené v používateľovom tokene, rovnako ako aj čas a deň. Na základe týchto znalostí autentifikačný server vykoná rovnakú šifrovaciu funkciu. Pre úspešnú autentifikáciu sa prepočítaná hodnota musí zhodovať s hodnotou, ktorú vložil používateľ.

Iným príkladom je autentifikačný token, ktorý disponuje **USB** (*Universal Serial Bus*) rozhraním. Takýto typ tokenu typicky obsahuje súkromný kľúč, verejný kľúč a certifikát vydaný certifikačnou autoritou. Bezpečnostný systém vyšle tokenu tzv. výzvu (challenge), čím sa overí správnosť súkromného kľúča. V ďalšom kroku systém voči databáze overí, či meno na certifikáte korešponduje s autorizovanou identitou, ktorej je umožnený vstup.

Tokeny môžu byť poskytované vo forme softvéru (*software* - **SW**) alebo hardvéru (*hardware* - **HW**).

Nevýhodou hardvérového tokenu je potreba mať ho pri sebe vždy, keď je potrebné autentifikovať sa voči systému a samozrejme potreba nosiť pri sebe všetky tokeny, ak používateľ disponuje viacerými prístupmi.

Softvérové tokeny tieto problémy riešia uložením kľúčov na osobné zariadenie, ako je napríklad prenosný počítač (laptop). V tomto prípade môže používateľ pristupovať do systému iba zo zariadenia, na ktorom sa tokeny nachádzajú. Okrem iného je použitie softvérových tokenov zraniteľné na kompromitovanie zariadenia, kde sa nachádzajú.

5.2 Ľudský faktor v procese autentifikácie

Viaceré autentifikačné scenáre využívajú metódy šifrovania verejného kľúča (public key cryptography). Napríklad, používateľ vlastní tzv. smart kartu, ktorá je nositeľom verejného kľúča a zodpovedajúceho súkromného kľúča (private key). Na autentifikáciu požívateľa posiela systém náhodnú výzvu (challenge). Používateľ podpíše výzvu svojím súkromným kľúčom a posiela výsledok systému, ktorý overí podpis verejným kľúčom. Týmto spôsobom dokáže systém verifikovať, či je používateľ držiteľom správneho súkromného kľúča a to bez potreby prijať tento kľúč. Namiesto potreby ukladania verejného kľúča do súboru na vzdialenom systéme dokáže smart karta predložiť podpísanú výzvu a certifikát verejného kľúča, ktorý bol podpísaný treťou stranou. V tomto prípade ide o tzv. **PKI** (*Public Key Infrastructure*), normu vychádzajúcu z ITU-T špecifikácií.

Jednou z možných ciest pri autentifikačných systémoch založených na PKI je, že používateľ musí pri použití smart karty najprv autentifikovať samého seba do lokálneho systému (typicky program na počítači alebo mobilnom zariadení) zvyčajne s použitím hesla a až následne sa smart karta použije na autentifikáciu do vzdialeného systému, prostredníctvom PKI. Vzdialený systém sa spolieha na to, že smart karta je spoľahlivá. Verí vyhláseniu smart karty, že subjekt bol náležite autentifikovaný. Ide o príklad tranzitívnej dôvery.

Fig. 4.4 znázorňuje entity zahrnuté v autentifikačnom procese. V každom kroku tohto procesu dokáže potenciálny útočník získať prístup ku autentifikačnému kľúču.

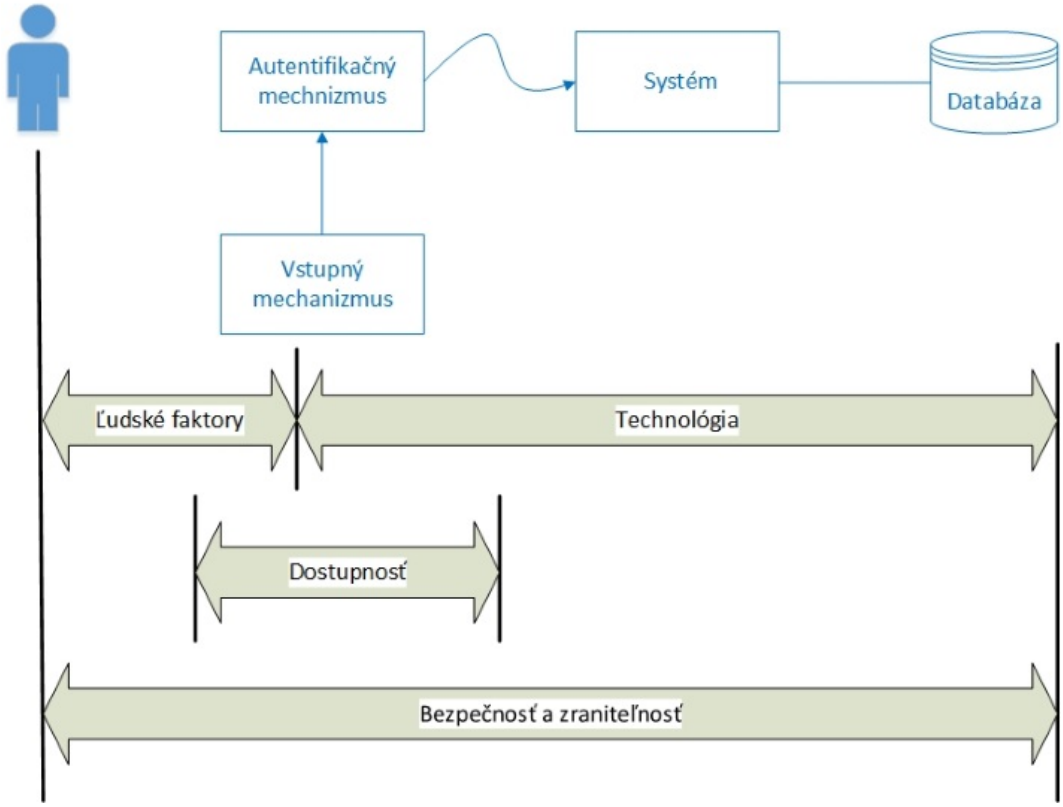


Fig. 4.4 – Entity zahrnuté v autentifikačnom procese

Oblasťou zraniteľnosti je však vstupný mechanizmus a používateľ. V prípade autentifikácie založenej na znalosti (hesla, PIN-u a pod.) si musí používateľa pamätať tajomstvo, čo niektorým ľuďom jednoducho nevyhovuje alebo je to pre nich zložité. Toto tajomstvo ľudia obyčajne vyslovia niekedy nechtiac alebo si ho zapíšu, prípadne ho napr. blízky rodinný príslušník zistí, ak nie je dostatočne silné. Používatelia ale mnohokrát svoje heslo vedome zdieľajú s niekým, koho dobre poznajú, nakoľko si neuvedomujú konzekvencie z toho plynúce. Ďalšou z možností je zachytenie hesla na vstupe, spôsobom *man-in-the-middle*, ak nejde o zabezpečenú prenosovú cestu. Man in the middle (skratka **MITM**, z angličtiny „človek uprostred“ alebo „človek medzi“) patrí medzi najznámejšie problémy v informatike a kryptografii. Jeho podstatou je snaha útočníka odpočúvať komunikáciu medzi účastníkmi tak, že sa stane aktívnym prostredníkom. V dnešnej dobe nie je podstatné, aby bol fyzicky prítomný v strede medzi dvoma komunikujúcimi bodmi, pretože sa sieťový prenos dá ľahko presmerovať.

Bezpečnosť všeobecne preto nie je možné riešiť výhradne len technickým spôsobom, nakoľko používatelia tvoria jeho integrálnu časť [10].

6 Autorizácia

Autorizácia je overenie oprávnení subjektu pri vstupe (do siete alebo služby) na základe prístupových práv. Okrem toho definuje, ku ktorým informáciám môže identifikovaný a autentifikovaný používateľ pristupovať a aké akcie môže vykonať.

6.1 Model autorizácie

Modely riadenia prístupu (Fig. 5.1) sa používajú na uplatňovanie pravidiel a účelov stanoveného bezpečnostného pravidla a definujú, za akých podmienok je možné pristupovať ku prostriedkom systému a jeho službám, t.j. objektu. V súčasnosti sa využíva niekoľko hlavných modelov riadenia prístupu [11]::

- *Discretionary Access Control* (**DAC**) – dovoľuje vlastníkovi objektu definovať, kto môže a kto nemôže pristúpiť ku tomuto objektu. Tento model sa preto niekedy nazýva aj *Identity-Based Access Control* (**IBAC**).

- *Mandatory Access Control* (**MAC**) – používa na určenie toho, ku čomu môže subjekt (používateľ) pristupovať tzv. klasifikácie. Subjekt teda môže pristúpiť ku všetkým objektom, ktorých úroveň oprávnenia je nižšia alebo rovná ako klasifikácia objektu. Tento model sa niekedy nazýva aj ako kontrola prístupu založená na pravidlách (rule-based access control).

- *Role-Based Access Conrol* (**RBAC**) – je najrozšírenejším modelom. Používa na pridelenie oprávnení subjektom role a skupiny. Používateľ tak môže pristupovať k objektom na základe rolí, ktoré má v oprávnení a tiež na základe svojej skupiny. Veľkou výhodou a tým, čo robí tento model najrozšírenejším je, že vo väčšine prípadov stačí modifikovať role a nie používateľov samotných.

- **Task Based Access Control** (**TBAC**) – je modelom, pri ktorom sa kontroluje počet pristúpení používateľa ku objektu. Ak používateľ toto číslo dosiahne, jeho ďalší prístup je zamietnutý.

- **Attribute based Access Control** (**ABAC**) – je model, ktorý využíva na pridelenie oprávnení atribúty používateľa. Atribúty sú v tomto prípade vlastnosti asociované s konkrétnou entitou (Subjekt, Zdroje, Prostredie). Ak za atribúty považujeme aj role, tak RBAC je možné taktiež modelovať prostredníctvom ABAC.

Všetky spomenuté modely je možné využívať aj v kombinácii. Povolenia závisia na subjekte – používateľovi, ktorý chce pristúpiť ku objektom a operácii, ktorú si želá používateľ vykonať.

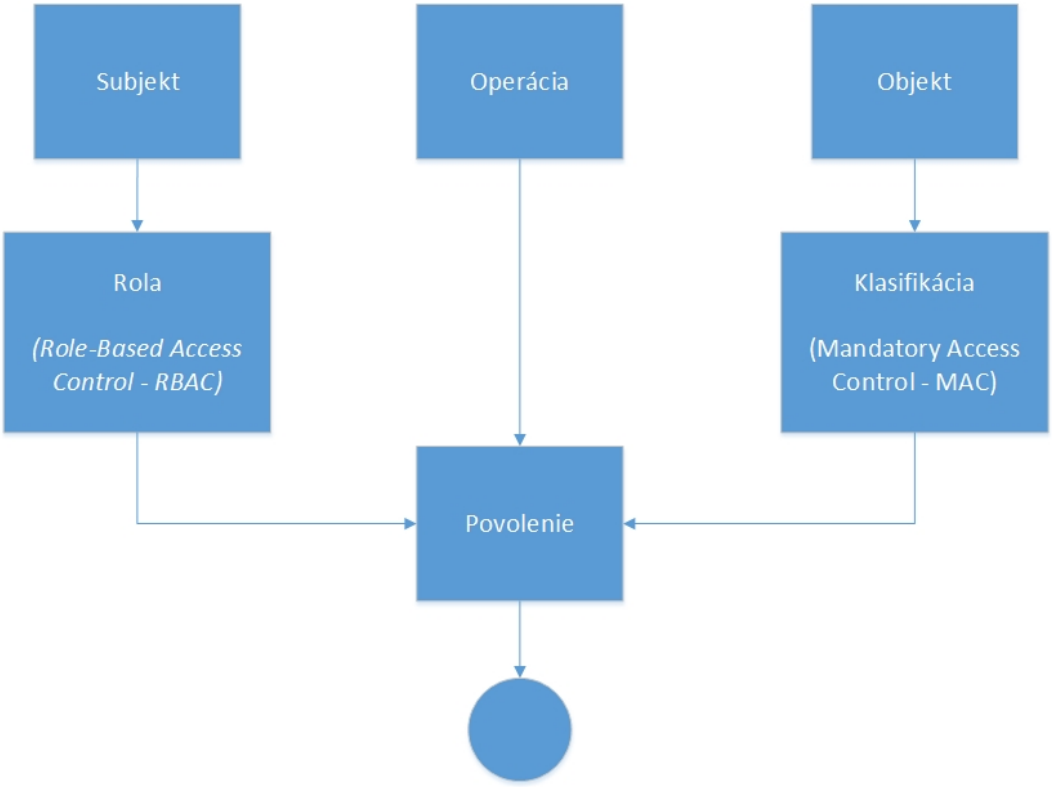


Fig. 5.1 – Autorizačný model

6.2 Pravidlá manažmentu prístupu

Jednou z najpoužívanejších techník riadenia prístupu (Fig. 5.2) je tzv. prístupová matica. Riadky matice predstavujú možnosti používateľa a stĺpce reprezentujú objekty. Táto technika sa často označuje aj ako zoznam riadenia prístupu (*Access Control List* - **ACL**).

Kontrola prístupu v závislosti od obsahu je ďalšou rozšírenou technikou, pri ktorej môže jeden používateľ pristúpiť k detailnejším informáciám alebo dátam objektu ako iný používateľ. Toto rozhodnutie môže závisieť na faktoroch, ako napríklad vek, použitý terminál, miesto odkiaľ pristupuje, IP adresa z akej pristupuje, čas a pod.

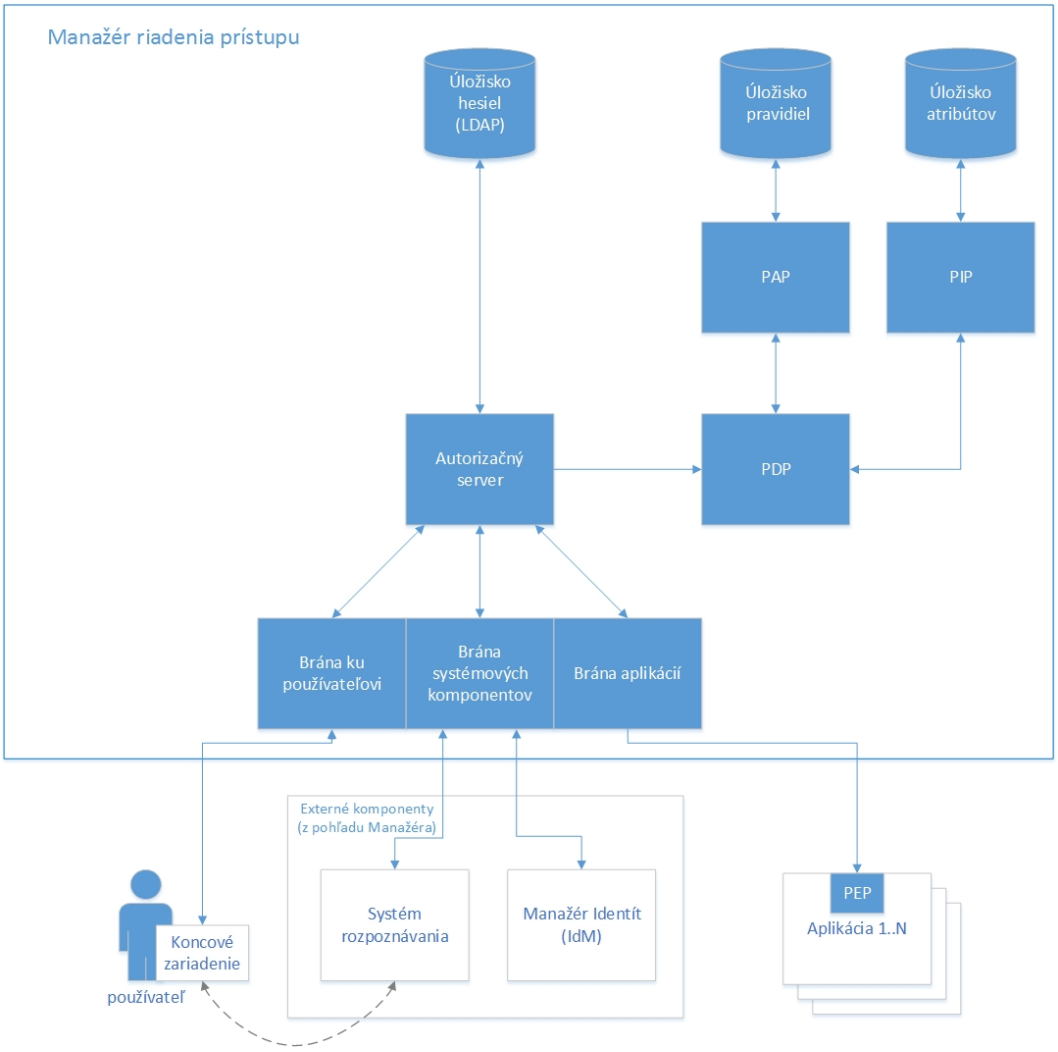


Fig. 5.2 – Manažér riadenia prístupu

6.3 Prístupové práva

Rozhodovací proces pri prijatí požiadavky na prístup do konkrétneho systému/aplikácie, jej informačného obsahu môže v určitých krokoch závisieť od prístupových práv, usporiadaných do súboru tzv. povolení. Pravidlá prideľovania povolení vychádzajú vo všeobecnosti z modelov opísaných v časti 5.1 Model autorizácie.

V systéme je použitý RBAC model a sú definované tri role:

- Administrátor
- Vlastník skupiny
- Používateľ v skupine

V tomto prípade Administrátor prideľuje Vlastníkovi skupiny alebo Členovi prístupové práva vstupu ku konkrétnym aplikáciám.

Vlastník skupiny ďalej definuje, ku ktorým aplikáciám môže konkrétny Člen skupiny v roli Používateľa vstupovať. Ak Administrátor predtým pridelil Vlastníkovi skupiny práva na pridávanie, modifikáciu a mazanie obsahu v konkrétnej aplikácii, môže tieto práva ďalej prideliť Členovi skupiny, ktorý sa zároveň môže stať aj prispievateľom obsahu, t.j. vystupovať aj v roli Vlastníka dát. Príkladom takýchto aplikácií je služba zdieľaného multimediálneho obsahu.

Člena skupiny reprezentuje rola Používateľa dát a rola Vlastníka dát. Rozdiel medzi obidvoma rolami je vlastníctvo konkrétneho informačného obsahu napr. vo forme zdieľaného videa v konkrétnej aplikácii. Ak používateľ systému v niektorej z aplikácií takýto obsah vytvorí, nadobudne zároveň rolu Vlastníka dát a nad konkrétnym obsahom a jeho možnosťami zdieľania sám rozhoduje, znovu však v rámci kompetencií stanovených Vlastníkom skupiny. Člen skupiny v roli Vlastníka dát má možnosť rozhodovať iba o akcii a vzťahu v rámci svojich kompetencií.