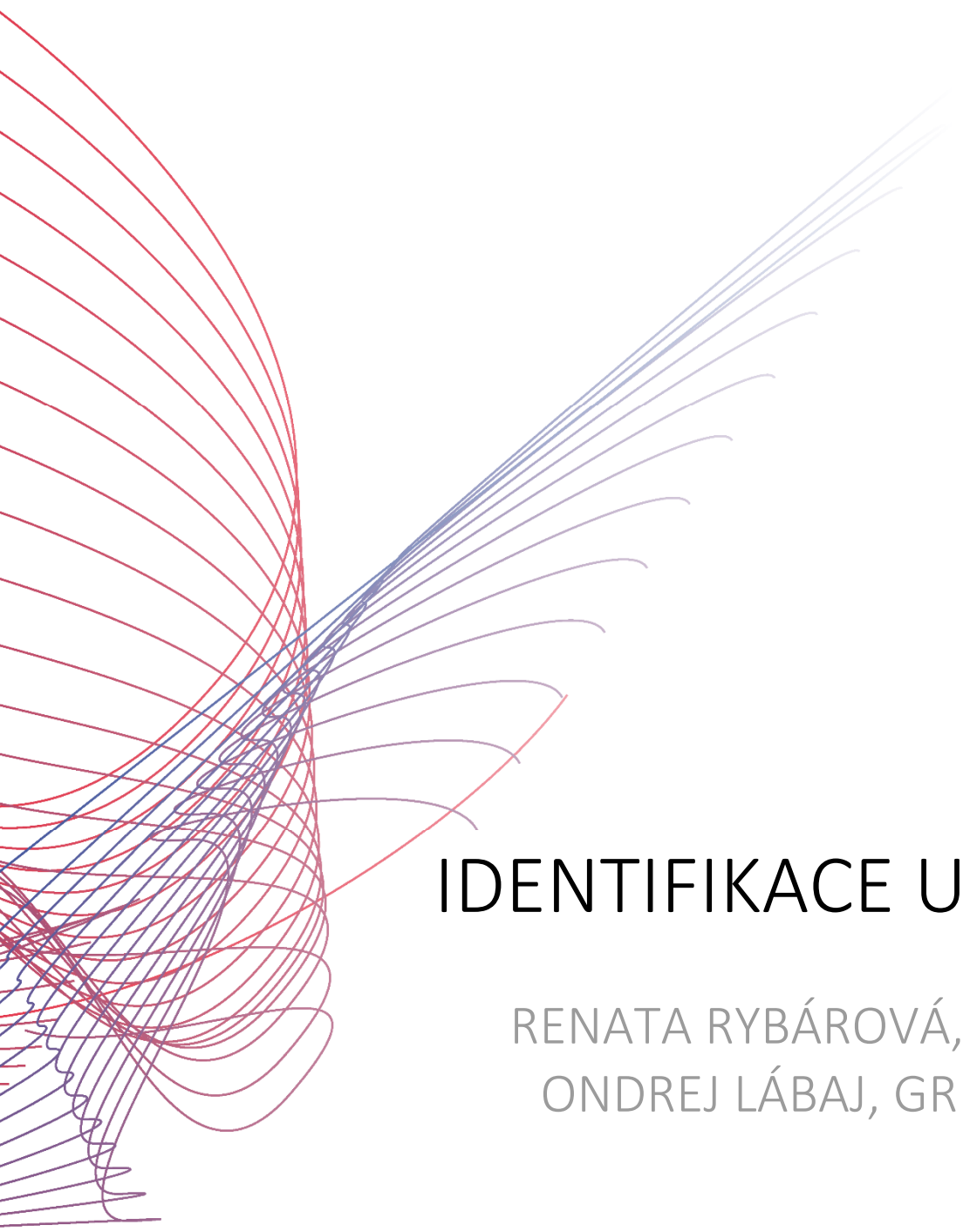
en
cs de
sk es

TECH
pedia



IDENTIFIKACE UŽIVATELŮ

RENATA RYBÁROVÁ, JURAJ KAČUR,
ONDREJ LÁBAJ, GREGOR ROZINAJ

Název díla: Identifikace uživatelů
Autor: Renata Rybárová, Juraj Kačur, Ondrej Lábaj, Gregor Rozinaj
Přeložil: Pavel Bezpalec
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 224352084
Tisk: (pouze elektronicky)
Počet stran: 45
Edice (vydání): 1. vydání, 2017

ISBN 978-80-01-06236-4

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering

http://www.techpedia.eu

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor.
Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
	Výhody
	Nevýhody

ANOTACE

Identifikace uživatele, autorizace a autentifikace zabezpečují, že k systému budou mít přístup jen oprávnění uživatelé a akceptují se jen příkazy, které budou autorizované. Identifikace hovořícího má za cíl základní identifikaci možných uživatelů začleněných do databáze systému. Tato funkce může být vhodná pro úlohy vycházející z identifikace, jako např. aktivace osobního profilu. Detekce tváře může poskytnout bezpečnější identifikaci založenou na tváři uživatele, která poskytuje více charakteristických prvků. Ty mohou být použité na parametrizaci v porovnání s hlasovou identifikací. Navíc, rozpoznávání 3D tváře ještě více rozšiřuje možnosti extrakce příznaků pro přesnější identifikaci v rámci skupiny uživatelů. Může být proto použitá pro vysoký stupeň autentifikace (a autorizace) pro nejnáročnější aplikace (např. přihlášení se do banky atd.).

CÍLE

Hlavním cílem tohoto výukového kurzu je seznámit studenty se základy identifikace, autentifikace a autorizace uživatele. Studentovi jsou představeny základní principy identifikace hovořícího, identifikace uživatele na základě 2D a 3D rozpoznávání tváří, autentifikačních metod a autorizace uživatele.

LITERATURA

[1] Abate, Andrea F.; Nappi, Michele; Riccio, Daniel; Sabatino, Gabriele. 2D and 3D face řečognition: A survey In: Pattern Řečognition Letters, Volume 28, Issue 14, 15 October 2007, Pages 1885–1906. available at www.sciencediřečt.com [http://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; Pavlovicová, 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; Pavlovicová, 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 Identifikace uživatelů

Identifikace uživatele je jedním z klíčových prvků zabezpečujících, aby systém nebo aplikace vykonávaly jen příkazy, které jsou skutečně oprávněné. Nejpoužívanější typ autentifikace nebo ověřování je heslo. Ale s rozvojem informačních technologií a algoritmů na ochranu bezpečnosti, systémy a aplikace začínají používat autentifikaci na základě biometrických údajů.

Použití biometrie účinně eliminuje případná rizika spojená s méně pokročilými technologiemi, které jsou založené na tom, co člověk má nebo zná oproti tomu, čím člověk skutečně je [1]. Jedná se o velmi atraktívní a populární technologii, protože může být integrovaná do libovolné aplikace nebo systému vyžadujícího bezpečnostní kontroly nebo kontrolu přístupu.

Identifikace hovořícího poskytuje základní identifikaci možných uživatelů nacházejících se v okolí systému. Metoda detekce tváře si klade za cíl poskytnout spolehlivou identifikaci založenou na tvářích uživatelů, které obsahují mnohem více charakteristik v porovnání s identifikací na základě hlasu, které mohou být parametrizované. Navíc rozpoznávání 3D tváře dále rozšiřuje možnosti získávání (extrakce) příznaků, aby se přesněji identifikovaly konkrétní osoby. Proto může být použitý pro nejvyšší úroveň autentifikace (i autorizace nebo povolení) pro nejnáročnější aplikace (např. přihlášeni do bankovního účtu, atd.) Z bezpečnostních důvodů je možné autentifikaci pomocí rozpoznávání 3D tváře rozšířit o další metody jako například sledování pohybu očí nebo rozpoznání duhovky. Tento přístup může simulovat multiúrovňovou autentifikaci (přihlášení pomocí biometrie a bezpečnostního klíče – tokenu), potřebnou na autentifikaci nejvyšší úrovně.

Biometrie mají též svoje nevýhody. Rozpoznání duhovky je extrémně přesné, ale drahé z pohledu implementace a ne příliš akceptované lidmi. Otisky prstů jsou spolehlivé a neinvazivní, ale nejsou vhodné pro nespolupracující jedince. Naopak, rozpoznávání tváří se zdá být rozumným kompromisem mezi spolehlivostí a společenskou přijatelností [1].

2 Identifikace hovořícího

2.1 Identifikace hovořícího – přehled

Identifikace hovořícího je součástí širšího konceptu rozpoznávání řečníka. Skládá se ze dvou podobných avšak rozdílných úloh: identifikace a verifikace hovořícího. Cílem první úlohy je určit, kdo ze zvolené (uzavřené) skupiny lidí získané ve fázi trénování hovoří, přičemž druhá úloha má potvrdit, zda je hovořící skutečně ten, za koho se vydává.

V případě nízkého skóre systém může identifikaci odmítnout (nebyl to nikdo ze skupiny). Takováto úloha se nazývá též problém uzavřené skupiny (v trénovací množině je konečný počet hovořících).

Na druhé straně verifikace potvrzuje, zda je daný hovořící skutečně ten, za koho se deklaroval, např. pomocí hesla, na základě svého hlasového vzorku.

Vzhledem k tomu, že je na světě je mnoho lidí, potenciálních útočníků, jejichž řeč nemůže být současně uložena v databázi, se tento problém označuje za problém otevřené skupiny. V této úloze je důležitý model všeobecného hovořícího, na základě kterého se správně určí prahy zamítnutí nesprávného uživatele.

Úloha rozpoznávání řečníka je velmi komplexní a problematická kvůli mnoha aspektům, které budou později vysvětleny. Tomuto problému výzkumné týmy věnují již více než 40 let a tato oblast není stále uzavřená. S pokrokem dostupných technologií se i oblasti aplikace rozpoznání řečníka stále rozšiřuje např. do následujících oblastí:

- Kriminalistika
- Přirozená a neinvazívní metoda získání a zpracování biometrických dat, např. pro kontrolu přístupu k službám nebo datům
- Automatická indexace řečových databází
- Herní průmysl
- Pomůcky pro postižené

Řešení problému identifikace v sobě zahrnuje 3 základní oblasti výzkumu:

- **extrakce příznaků** řeči vhodných pro identifikaci
- **normalizaci příznaků** kompenzujících řečníkovu variabilitu a změnu prostředí
- **klasifikace a rozhodování** na základě extrahovaných příznaků

Identifikace hovořícího se dále dělí na dvě velké skupiny, a to textově závislý a textově nezávislý systém. Textově závislý systém očekává určité promluvy, na

základě kterých vykoná rozhodnutí. Na druhé straně textově nezávislé systémy pracují nezávisle na konkrétní promluvě. U textově závislých systémů lze očekávat vyšší úspěšnost identifikace při dané délce promluvy. Ty totiž mohou bezpečně zahrnout i specifické koartikulační efekty.

2.2 Vlastnosti řečových signálů

Řečový signál je fyzicky tvořen hlasovými orgány, které jsou ale ovládané mozkovou činností jedince. Oba dva aspekty úzce souvisí s daným jedincem, proto obě aktivity vnášejí do řečového signálu specifické vlastnosti hovořícího; proto se i řečový signál označuje jako biometrický.

I když je primární úlohou řečového signálu přenos řečové informace, obsahuje v sobě též dodatečné informace např. specifické pro hovořícího, které jsou dané velikostí, tvarem a tuhostí jednotlivých hlasových orgánů, náladou, zdravotním stavem, vzděláním, povahou, původem, zvyky atd.

Způsob zakódování těchto informací do řečového signálu není úplně známý, stejně jako i samotný matematický popis této operace. Proto je poměrně náročné separovat a extrahovat jednotlivé příznaky pro zvolenou oblast zpracování řeči (rozpoznávaní řeči, identifikace hovořícího, atd.). Navíc řeč obsahuje velkou variabilitu hovořícího způsobenou různými vlivy, např. náladou, fyzickým stavem, chorobou, atd. Nakonec signál může být značně degradovaný přítomností šumů a vlivem nahrávacích zařízení a prostředí, v němž k nahrávání došlo.

Modifikace signálu, které nejsou způsobené řečníkem (zařízení, prostor, atd.) se označují jako změny relace. Tyto změny mají významný vliv na úspěšnost identifikace a proto musí být ošetřeny. To platí zejména v případech, kdy se podmínky nahrávání neshodují s podmínkami nasazení.

2.3 Extrakce příznaků řeči

S ohledem na množství problémů naznačených v předchozím textu a k vlastnostem řeči, bylo nalezeno mnoho metod parametrizujících řeč. Dobré příznaky pro identifikaci však musí splňovat následující vlastnosti:

- Diskriminativnost mezi hovořícími
- Robustnost vůči šumům pozadí
- Necitlivost vůči vlivům nahrávacích zařízení a prostředí
- Musí potlačit variabilitu hovořícího
- Musí být lehko získatelné

Protože existuje mnoho rozdílných příznaků, které sledují parametry různých fyzikálních vlastností, dělí se příznaky pro identifikaci hovořícího do několika úrovní:

- Akustické
- Prozodické
- Příznaky vyšší úrovně

Na akustické úrovni se extrahují příznaky z krátkých časových intervalů (10-30ms), které mají za cíl popsat akustickou stránku zvuku. Obvykle se jedná o modifikované obálky spektra apod. Takové příznaky tedy souvisí s fyzickými vlastnostmi hlasových orgánů jedince. Navíc tyto příznaky zahrnují různé psychoakustické fenomény, tak jako to dělá sluchový systém člověka. To zvyšuje robustnost vůči šumům a vlivu prostředí. V současnosti nejpoužívanější a nejúspěšnější jsou *Melovy frekvenční kepstrální koeficienty* **(MFCC)**, *perceptuální lineární predikce* **(PLP)** a *kepstrální lineární predikční koeficienty* **(CLPC)**. MFCC a PLP se snaží vystihnout modifikovanou obálku spektra využívající psychoakustické principy jako je odlišné vnímané výšky tónu lidmi, kritická pásma, křivka shodné hlasitosti, atd. Tyto příznaky jsou schopné zachytit počet, polohu i tvar formantových frekvencí, které jsou nutné pro správný vjem zvuku. Proto jsou důležité zejména pro oblast rozpoznávání řeči. Při identifikaci řečníka však též hrají významnou úlohu, jelikož jsou schopné postihnout i menši změny formantových frekvencí v závislosti na hovořícím. Polohy formantových frekvencí se totiž neliší jen od hlásky ke hlásce, ale i mezi hovořícími. CLPC příznaky se na druhou stranu snaží popsat (odhadnout) parametry modelu produkce řeči, čím by bylo možné modelovat (určit) konkrétního hovořícího (jeho hlasový trakt). K zmíněným akustickým příznakům se často konstruují dynamické parametry, které mají za cíl vystihnout jejich vývoj v čase, který je též specifický pro konkrétní hovořící. Na to se používají diferenční nebo akcelerační koeficienty počítané z většího časového rámce.

Příznaky na prozodické úrovni se spíše zaměřují na charakter řeči, způsob hovoření, návyky při hovoření, fyzický a zdravotný stav, atd. Samozřejmě je tato informace rozprostřená v širším časovém úseku v rozmezí několika sekund. Nejvíc preferované rysy na této úrovni jsou: rytmus, dynamika řeči, rychlost hovoření,

modulace hlasivkové frekvenci, tvorba pauz, atd. Na druhé straně jsou tyto příznaky hůře extrahovatelné a kvantifikovatelné jako na akustické úrovni. Proto existuje vícero metod na jejich získání. Nejběžnější pro detekci hlasivkové periody jsou: *průměrná magnituda diferenční funkce* (**AMDF)**, autokorelační funkce, inverzní filtrování, apod. Pro dynamiku řeči je to průběh energie v čase atd. Samozřejmě kromě základních metod existuje množství jejich modifikací.

2.4 Klasifikace - algoritmus rozhodování

Po fázi extrakce příznaků a jejich případné normalizaci (bude popsaná v další části) následuje fáze klasifikace, resp. rozhodnutí, kde se určí, kterému hovořícímu dané příznaky řeči nejlépe odpovídají. Samozřejmě je možné v případě nízké důvěryhodnosti výsledku celý proces zamítnout. Existuje mnoho vhodných, prakticky použitelných klasifikačních metod, které se vzhledem k různé činnosti zpracování a komplexnosti dále dělí na více skupin se svými výhodami a negativy:

- **Ne parametrické metody** - nepředpokládají žádný model rozložení dat v prostoru. Jejich hlavním reprezentantem je metoda *K-nejbližších sousedů* **(KNN)**. KNN hledá K nejbližších příznaků v prostoru k neznámému a na jejich základě vytvoří výsledné rozhodnutí. Je to jednoduchá metoda, která při nedostatku dat obvykle dosahuje menší robustnost.

- **Parametrické metody** předpokládají známou distribuci, podle které jsou rozložená data v prostoru. Potom je potřeba už jen správně odhadnout parametry takových modelů na základě trénovacích dat. V případě malého množství dat dosahují vyšší robustnosti. Jejich hlavním reprezentantem je *směs Gaussových funkcí* **(GMM)**. Tento model předpokládá, že prostor je popsán kombinací Gaussových rozdělení.

- **Diskriminativní metody** se namísto co nejlepšího popisu rozložení dat v prostoru snaží nalézt rozhodovací funkci tak, aby se dosáhlo co nejmenší chyby rozhodování. V tomto případě dosahují i vyšší generalizační schopnosti. Mezi nejvýznamnější metody patří *neuronové sítě* **(NN)** a *systémy s podpůrnými vektory* **(SVM)**.

- **Generativní (popisné) metody** se snaží popsat data v prostoru a nerozdělovat je primárně do tříd. Pokud se podaří dokonale popsat rozložení dat, je s jejich pomocí teoretický možné konstruovat optimální klasifikátor (Bayesův). Mezi nejvýznamnější metody v této oblasti patří GMM.

Ukázalo se jako vhodné konstruovat modely všeobecných hovořících, které byli postaveny na velkém množství různých hovořících tak, aby pokrývaly širokou populaci. Ty je potom možné používat při stanovení prahů zamítnutí nebo pro adaptaci specifických modelů.

2.5 Kompenzace vlivu prostředí

Na potlačení vlivu změn prostředí (podmínek při trénovaní a testovaní: šumy, nahrávací zařízení, prostředí, atd.) a i samotného hovořícího bylo vyvinuto mnoho metod využívajících různé předpoklady a způsoby činnosti. Nejjednodušší metody normalizují příznaky např. tak, aby měly stejnou energii v měřených pásmech (ekvalizace). Často se to dělá odčítáním průměrného kepstra. Dále je možné využít fixně nastavené filtry, které mají za cíl zvýrazňovat modulační spektrum řeči, nebo pomocí tzv. relativní spektrální analýzy (RASTA). Sofistikovanější metody se snaží nalézt vhodnou transformaci mezi příznaky z trénovací fáze a aktuálně zpracovanými. Tento přístup se označuje za mapování příznaků. Je možné transformovat i celé modely hovořících tak, aby odpovídaly aktuálnímu rozložení dat. Toto se označuje jako syntéza modelů hovořících. Posledně jmenované metody pracují na základě aktuálních dat, proto je možná jejich adaptace v čase při změně prostředí. To si však vyžaduje podstatně složitější algoritmy zpracování signálů.

Méně sofistikovaná metoda, která ale dosahuje dobré výsledky je mít data/modely pro různé typy prostředí. Potom po správné detekci nejbližšího prostředí použít právě tato data nebo modely, čímž se dosáhne nejmenšího rozdílu mezi trénovacími a testovacími podmínkami, to vede k minimalizaci chybovosti.

Pro získání ucelenějšího a podrobnějšího přehledu o technologiích a metodách použitých pro oblast rozpoznávání řečníka viz např. [2].

3 Rozpoznání tváře

Tvář se postupně stává nejatraktivnější biometrií a systémy rozpoznání tváře pro identifikaci osob jsou stále více využívané ve velkém množství aplikací. Vývoj algoritmů a metod rozpoznávání též umožňuje využít systémy na identifikaci a verifikaci v komerční oblasti. Avšak tyto systémy nedosahují porovnatelné výsledky v nekontrolovaných a neomezených podmínkách. Rozpoznávání tváří za těchto podmínek je stále náročný problém, navzdory nedávným pokrokům v této oblasti.

Biometrické systémy pro identifikaci osob, které jsou vyvinuté několika společnostmi, dosahují vysokou přesnost v rozpoznávání tváří. Většina z těchto aplikací musí splňovat [3]:

- dokáže rozpoznat několik tváří z jednoho video záběru nebo jednoho obrázku
- vysokou úspešnost rozpoznávání
- nezávislost na světelných podmínkách
- stabilitu při změně výrazu tváře nebo pózy
- rozpoznání v reálném čase, atd.

Existuje několik faktorů, které mohou ovlivnit výkon a přesnost systému pro rozpoznávání tváří [1]:

- **Osvětlení** - změny osvětlení v důsledku vlastností odrazivosti kůže a díky vnitřnímu řízení kamery. Některé 2D metody plní dobře úlohu rozpoznávání jen při malých změnách osvětlení.
- **Změna pózy -** ovlivňuje proces autentifikace, protože představuje deformaci objektu. Detekční metody by měly řešit problém s ohledem na různé úhly pohledu na umístěný objekt (např. výhled z bezpečnostních kamer). Na druhé straně jsou rozpoznávací algoritmy relativně robustné co se týče výrazu tváře (s výjimkou některých extrémních výrazů jako výkřik).
- **Doba zpoždění** - je též důležitým faktorem, zahrnujícím změny ve tváři člověka během určité dlouhé doby. Všeobecně je tento problém těžko řešitelný vzhledem k ostatním problémům.

3.1 Metody rozpoznávání tváře

Systémy rozpoznávání tváři spadají do dvou kategorií: verifikace a identifikace.

Verifikace tváře odpovídá shodě 1:1. V tomto procesu se obraz tváře, kterého identita se ověřuje, porovnává s šablonami snímků tváře.

Naopak identifikace tváře je 1:N problém. Obraz tváře je porovnaný se všemi obrazovými šablonami v databázi tváří pro stanovení identity tváře.

V případě, že nevíme, zda je testovaná tvář v databázi systému, postup je následující. Obrázek s tváří je porovnán se všemi obrazy tváří v databázi a vyhodnotí se pravděpodobnost shody pro každou z nich. Všechny tyto pravděpodobnosti jsou numericky seřazeny: nejvyšší hodnota je jako první. V případě, že je pravděpodobnost vyšší jak nastavená prahová hodnota, systém informuje o výsledku [1].

Vybrané základní metody 2D rozpoznání tváře:

- Lineární/nelineární projekční metody
    - *Principal Component Analysis* (**PCA**) - metoda založená na PCA se nazývá „eigenface“. Hlavní myšlenkou PCA je rozložit datový prostor na lineární kombinaci malého počtu základních funkcí, které jsou ortogonální, a které reprezentují maximální variaci směrů v trénovací sadě [4].
    - *Kernel Principal Component Analysis* (**KPCA**) - je metoda nelineární extrakce příznaků. KPCA může získat sadu příznaků, které jsou vhodnější pro kategorizaci než konvenční PCA. KPCA je široko používaný v případě rozpoznání tváře s výrazem a při různých světelných podmínkách [4].
    - *Linear Discriminant Analysis* (**LDA**) – byla navržena jako lepší alternativa k PCA. Poskytuje rozlišení mezi třídami, zatímco PCA se zabývá vstupními daty v celém svém rozsahu bez toho, aby věnovala pozornost základní struktuře. Ve skutečnosti spočívá hlavní cíl LDA v nalezení báze vektorů, které poskytují nejlepší rozlišení mezi třídami. LDA se snaží maximalizovat rozdíly mezi třídami, čím se minimalizují rozdíly v rámci své třídy [1].
    - *Discriminant Common Vectors* (**DCV**) - hlavní myšlenka DCV spočívá ve shromažďování podobnosti mezi prvky ve stejné třídě a vyloučení jejich odlišnosti [1].
- Neuronové sítě – je nelineární řešení, používá se i v jiných oblastech rozpoznávání vzorů. Výhodou neuronových klasifikátorů proti lineárním je, že se může snížit počet nesprávných zařazení mezi sousedními třídami. Základní myšlenkou je, aby se brala do úvahy síť s neuronem pro každý pixel v obraze. Avšak, vzhledem k rozměrům vzorů, nejsou neuronové sítě přímo trénované se vstupnými obrazy. Před procesem trénování se používají techniky snižující počet rozměrů.

- Systémy iterovaných funkcí (*iterated function systems - IFS)* – teorie IFS byla vyvinuta především v oblasti kódování obrazu a nedávno byla rozšířena i na indexování obrazu. Fraktální kód obrázku je neměnný vzhledem k široké sadě globálních transformací, jako je rotace, kontrastní škálování, atd. IFS obrazu tváře se používá při trénování neuronových sítí, kde se používá jako klasifikátor [1].

3.2 Extrakce příznaků

Některé algoritmy rozpoznáváni tváře jsou založené na příznacích extrahovaných z obrazu tváře člověka - nazývaných tvářové příznaky. Například algoritmus může analyzovat relativní polohu, velikost, a/nebo tvar očí, nosu, úst, lícních kostí a čelisti. Tyto příznaky jsou potom použity při hledaní odpovídajících příznaků ve skupině snímků. Ostatní algoritmy normalizují galérii snímků tváře a potom komprimují data tím, že ukládají jen data v obraze, které jsou užitečné pro rozpoznání tváře. Testovaný obraz se potom porovná s údaji o tváři.

Před získáním příznaků jsou obrázky/snímky předzpracované a normalizované.

Jako součást předzpracování je snížení rozměrů všech vstupních snímků na definovanou velikost. Též je možno aplikovat **CLAHE** (*contrast limited adaptive histogram equalization)* - kontrastově omezenou adaptivní ekvalizaci histogramu. Normalizované snímky mohou být maskované tak, aby se vynechalo pozadí a ponechala jen oblast tváře.

Hlavním cílem procesu normalizace je minimalizovat nekontrolované variace, které se vyskytují v průběhu získáváni snímků a na udržování odchylek pozorovaných v tvářových příznacích mezi jednotlivci.

Velkou změnu v obraze může způsobit změna pózy.

Extrakce příznaků zahrnuje snížení množství prostředků potřebných k popisu velkého souboru dat. Při rozpoznání tváře se vykonává analýza velkého množství dat. Analýza s velkým počtem proměnných všeobecně vyžaduje velké množství paměti a výpočetní síly. Extrakce příznaků se vztahuje ke snížení proměnných a dat.

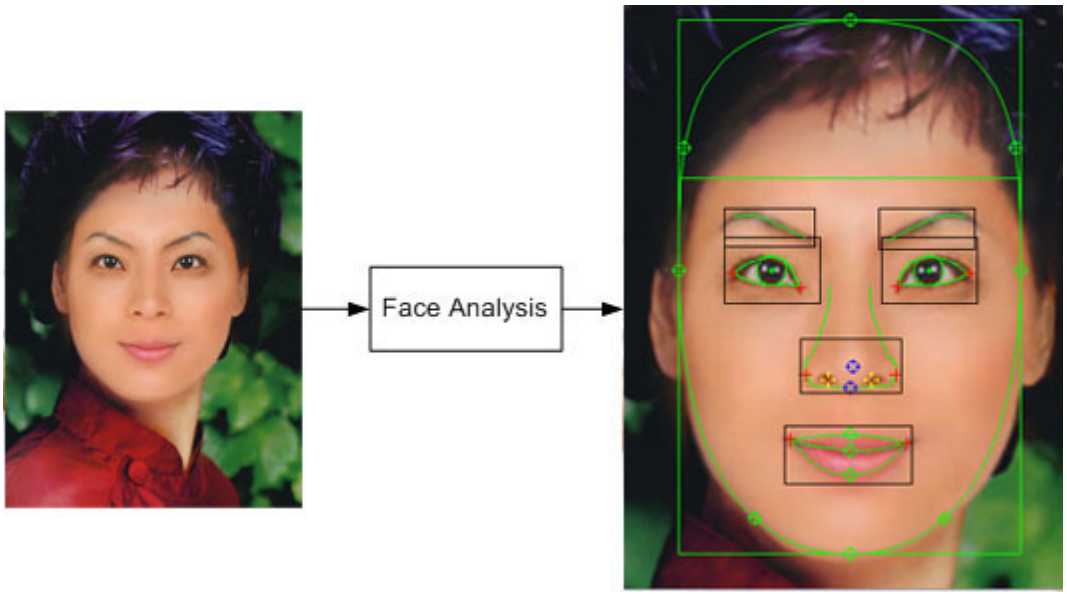
Při extrakci příznaků se nejčastěji využívají metody založené na detekci hran. Velmi dobré výsledky se dosahují i při lokálních binárních vzorech (*local binary patterns* - **LBP**).

Detekce hran je název pro sadu matematických metod. Hlavním cílem je detekovat body v digitálním obraze, kde se prudce mění jas. Tyto obrazové body s ostrou změnou jasu jsou obvykle uspořádané do sestavy zakřivených čar pojmenovaných hrany.

Nejčastěji používané funkce na detekci hran jsou Sobelův operátor (nazývaný též Sobelův filtr), Prewittův operátor nebo Gaborův filtr.

Příznaky se mohou získat z předzpracovaných snímků tváří pomocí LBP histogramu. LBP histogramy se považují za jedny z nejlepších příznaků pro

rozpoznávání tváří, když je k dispozici jen limitované množství vzorků a mohou být lehce vypočítány v reálném čase [5] (Obr. 2.1).



Obr. 2.1 – Příklad získaných příznaků

3.3 Klasifikace tváří

Systém rozpoznávání tváří pracuje obvykle ve dvou fázích. První fáze je proces trénování a druhý je klasifikace uživatelů. Moderní metody rozpoznávání tváře správně fungují, pokud je k dispozici ve fázi trénování až 10 snímků jedné osoby. Mnoho různých technik bylo vyvinuto pro rozpoznání tváře jen z jednoho obrazu dané osoby. Trénovací fáze by měla být plně automatizovaná a uživatelé ji musí být schopni ovládat. Tréninkový proces používá algoritmy shlukování (clustering algoritmy).

Hlavním cílem všech shlukovacích (clustering) algoritmů je vytvořit shluk (cluster) nebo třídu ve vstupním datovém souboru. Existuje mnoho algoritmů shlukování. Tyto algoritmy mohou být rozděleny do dvou skupin: rozdělovací a hierarchické algoritmy [5].

Jako příklad shlukovacího algoritmu můžeme uvést K-means algoritmus. Dalším algoritmem na vytvoření shluků je tzv. samo organizující se mapa - *self-organizing map* (**SOM**), patřící k neuronovým sítím nebo algoritmus prostorového shlukování založený na hustotě prvků (*density-based spatial clustering of applications with noise* - **DBSCAN**).

Pro klasifikaci příznaků získaných z tváří můžeme uvést dva způsoby v závislosti na počtu trénovacích snímků a počtu identit použitých v rámci systému:

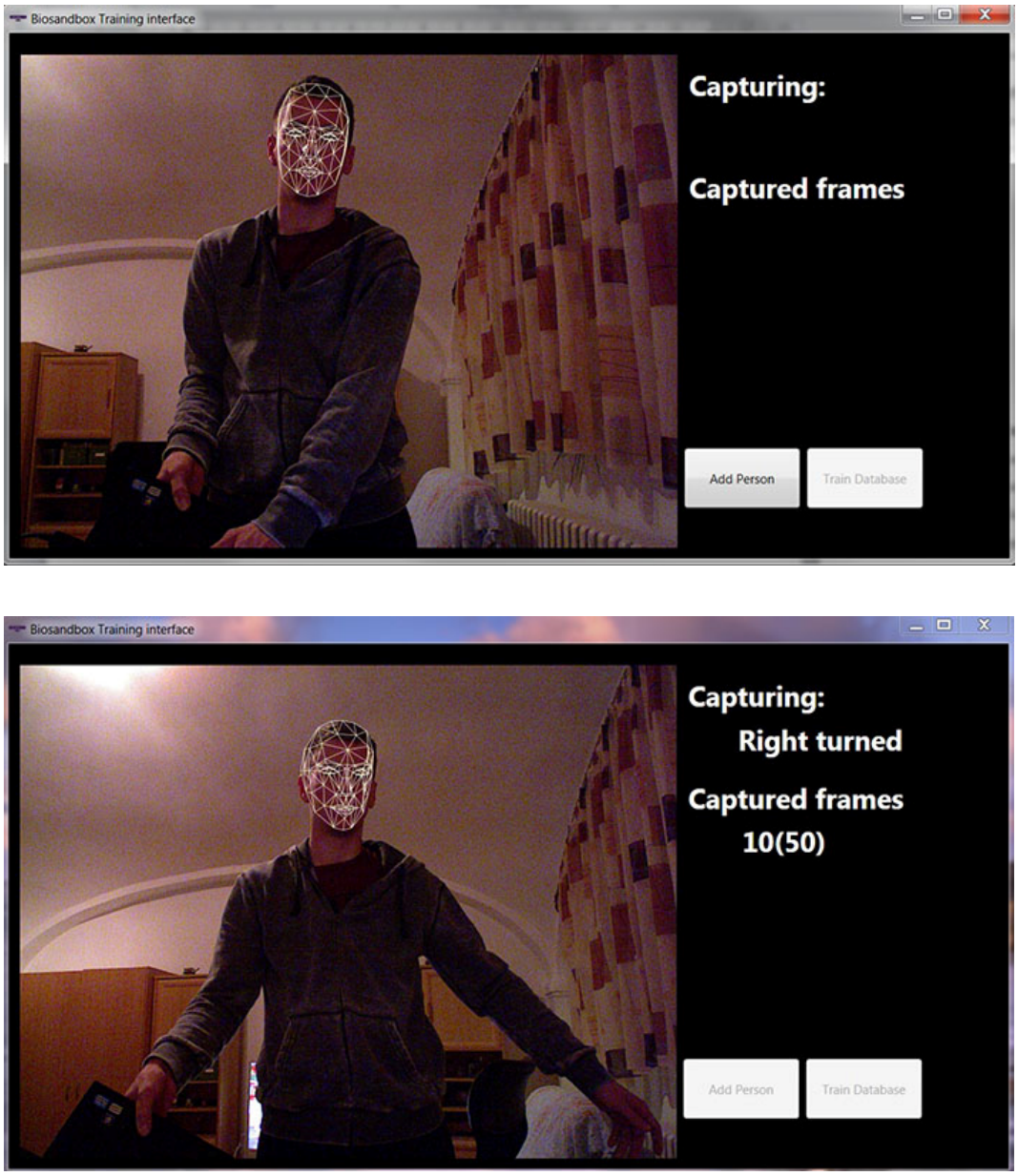
- Systémy s podpůrnými vektory (Support Vector Machines) - používají se jen, když je v systému relativně malý počet identit. Hlavní nevýhodou této metody je časově náročné trénování modelu, když se použije větší počet vzorků.
- Systémy na bázi K-nejbližších sousedů (K-Nearest Neighbour) - tento algoritmus může být použit v distribuovaném systému. Trénování se vykonává jednoduše vložením příznaku do databáze [5].

3.4 Lokalizace a rozpoznání tváře

Biometrické systémy, konkrétně systémy rozpoznávání tváře, jsou široce využívané v mnoha různých typech aplikací. Typickým příkladem takové aplikace je v současné době inteligentní TV se systémem rozpoznávání tváří. Rozpoznávání tváří ve smart TV se používá na autentifikaci uživatele. Na základě toho mohou být poskytnuty personalizované služby nebo doporučeny různé programy. Systémy rozpoznávání tváří by měly pracovat v reálném čase a měly by být schopny rozpoznat jednu nebo více identit/osob. Většina z těchto systémů má v sobě zahrnuto též grafické uživatelské rozhraní pro automatický proces trénování (Obr. 2.2).

Obvykle 2D úloha rozpoznávání tváří vyžaduje zpracování vstupu z fotoaparátu nebo kamery. Hlavní proces rozpoznávání tváří se skládá z těchto částečných úloh:

- Získání vstupního obrazu - čte obraz z kamery, převede ho do formátu požadovaného systémem a odevzdá ho dále ke zpracování
- **lokalizace tváře** - lokalizuje tváře v obraze a přiradí jim souřadnice. Lokalizační algoritmus je určen v závislosti na použitém fotoaparátu/kameře.
- **trénovací proces** – využívá shlukovací algoritmy jako např. K-means
- **předzpracování** lokalizovaných tváři zahrnuje optimalizaci histogramu
- **normalizace** – např. změna rozměrů obrázku
- **získávání příznaků** – získává příznaky z předzpracovaných tváří, např. LBP využití
- **klasifikace tváří** (v obraze) – využívá metody jako Support Vector Machines nebo K-Nearest Neighbor Distance Matching
- **sledování tváři** (v obraze) - Obvykle se sledují jen tváře z přední strany, protože drtivá většina metod rozpoznávání tváří je spolehlivá jen při práci s čelním snímkem tváře. Jakmile je tvář rozpoznaná, začne sledování, což výrazně šetří výpočetní zdroje a umožňuje sledovat objekt i po změnách pózy [3]. Takže informace o rozpoznaném uživateli se pošle jako výstup ze systému.

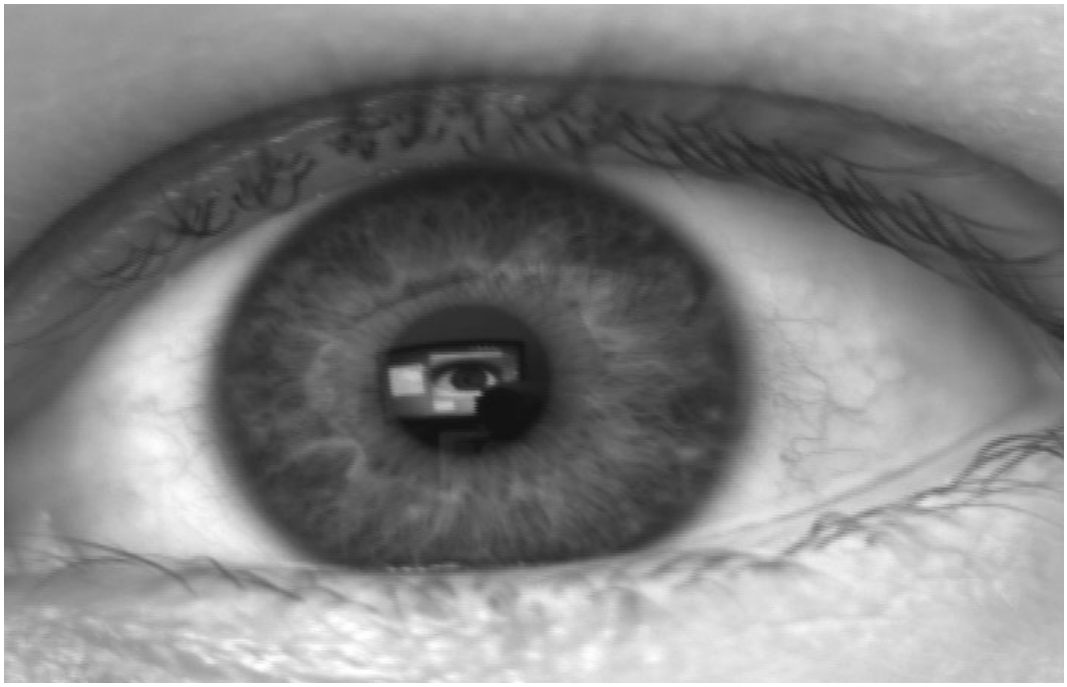


Obr. 2.2 – Príklad trénovacího GUI u systému s rozpoznáním tváře

3.5 Rozpoznání duhovky

Duhovka je jednou z nejpopulárnějších biometrických charakteristik. Kombinace bezdotykového snímání, časové stability a vysoké přesnosti rozpoznávání umožňuje použití v bezpečnostních aplikacích.

Bylo dokázáno, že přesnost rozpoznávání duhovky závisí na kvalitě zachyceného obrazu oční duhovky a předzpracování obrazu. **NIR** (*near infrarred*) snímací kamera je doporučená na snížení negativního vlivu osvětlení (viz Obr. 2.3). Použití NIR umožňuje přidat extra světelný zdroj bez vlivu na pohodlí snímání.



Obr. 2.3 – Příklad snímání obrazu kamerou Guppy F-038B NIR

Identifikace založená na rozpoznání duhovky se skládá z lokalizace duhovky, extrakce příznaků a klasifikace. Jeden z nejúspěšnějších systémů dosahuje přesnost 100% v řízených podmínkách. Ale proces lokalizace a normalizace pro aplikace ve skutečném životě je potřeba zlepšit. Tento systém používá Gaborův filtr na extrakci příznaků, kde jsou filtrované signály kvantované do dvou úrovní. Tímto postupem se získají řetězce binárních čísel (příznaky). Porovnáním nejbližších vzorků pomocí metody KNN a Hammingové vzdálenosti dostáváme rozpoznání duhovky.

4 Rozpoznání 3D tváře

Rozpoznávání tváří na základě 2D přístupu je běžný a přirozený postup. 3D přístup k rozpoznávání tváře dosahuje všeobecně vyšší bezpečnosti než 2D přístup k rozpoznávání tváří.

Techniky založené na 3D rozpoznávání tváře by měly splňovat několik náležitosti, jako je robustnost s ohledem na změny osvětlení, stejně jako i na změnu polohy, natočení a úpravy původního modelu v rámci absolutní vztažné soustavy [1].

4.1 Metody rozpoznání 3D tváře

3D rozpoznání tváře v porovnání s 2D rozpoznáváním tváře využívá větší tok informací o charakteristikách tváře. Oba dva přístupy však potřebují základní předzpracování, jako je normalizace obrazu tváře, otočení do neutrální polohy atd. Přidaná informace nejen o 2D tváři, ale i hloubková analýza nabízí bohatý zdroj informací, které nejsou zachycené v 2D obrazech. Hlavni výhody 3D oproti 2D analýze tváře jsou:

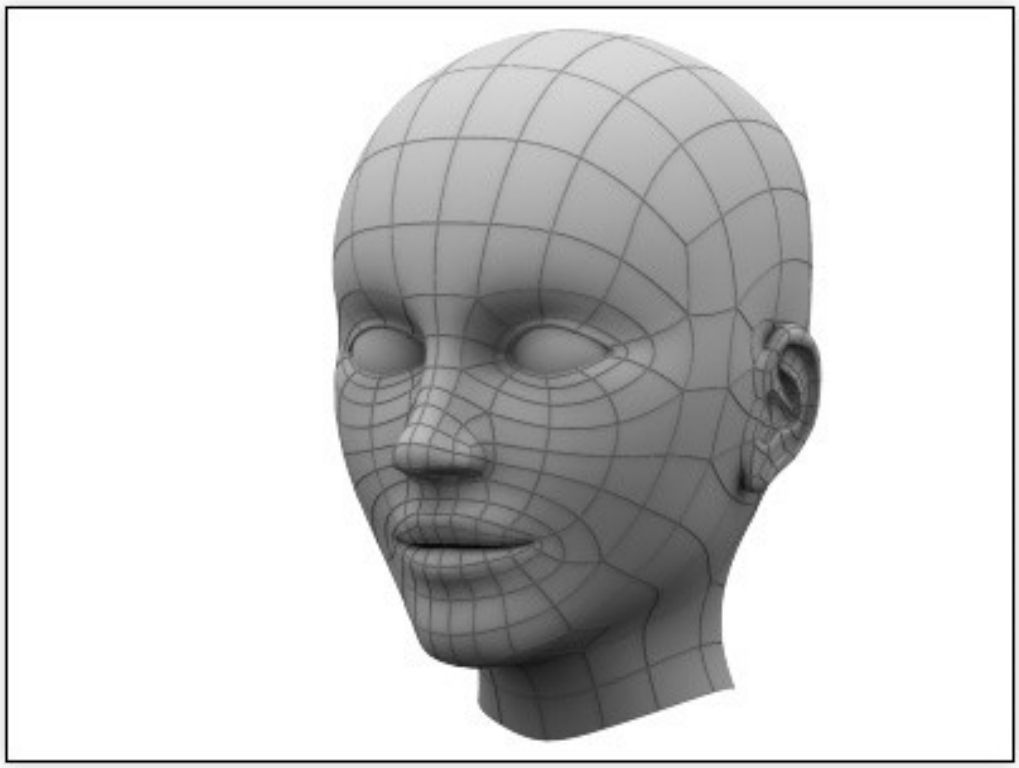
- není ovlivněn změnami osvětlení nebo použitím kosmetiky
- méně citlivé na změny vzhledu
- lehčeji se zvládá změna pózy
- projektivní povaha 2D obrazu
- zjednodušuje detekci tváře a tvářových příznaků, odhaduje pózu

Vybrané základní metody na 3D detekci tváře:

- 3D rozpoznání tváře na principu analýzy povrchu - tento přístup je založen na klasickém 3D rozpoznávání objektů (viz Obr. 3.1). Existují různé typy metod rozpoznávání založené na
  - použití místně zakřivených prvků, které jsou nezávislé na otočení (např. křivka profilu tváře)
  - použití párování bod-bod (polygon několika významných bodů tváře)

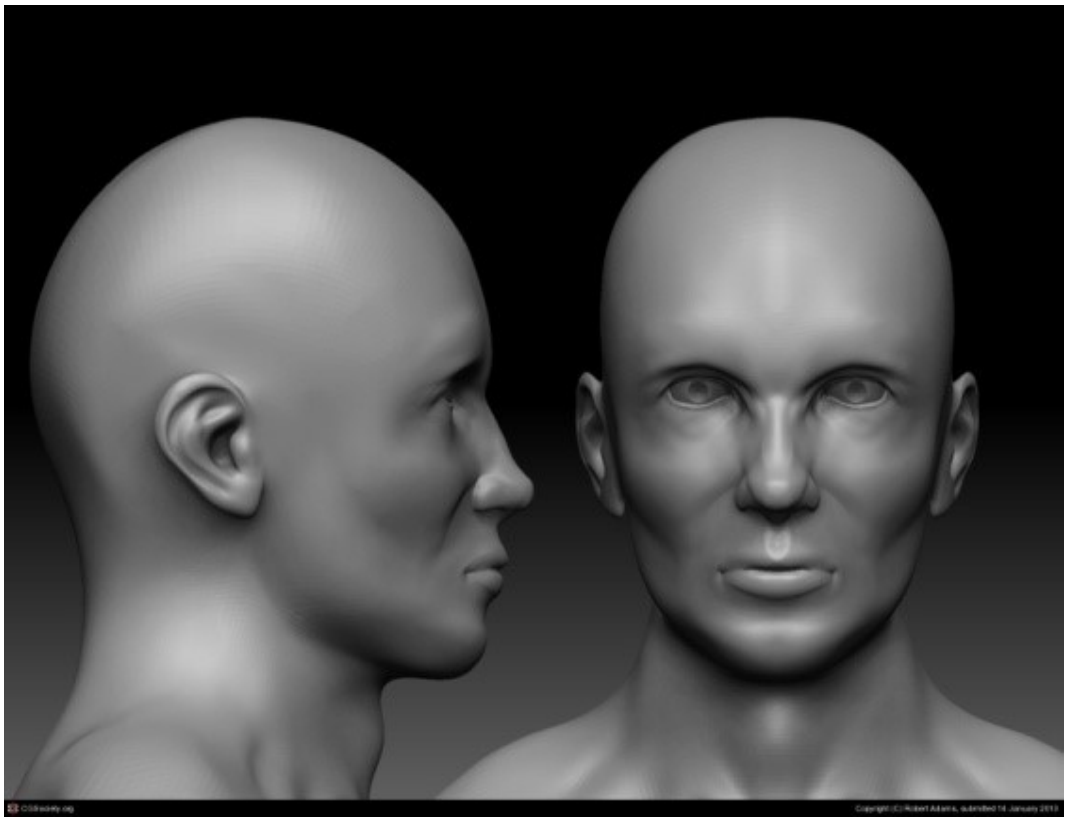
Obr. 3.1 – 3D rozpoznání tváře na principu analýzy povrchu

- 3D rozpoznání tváře na principu analýzy vzhledu - tato metoda se zaobírá technikou „eigenfaces“ a „fisherfaces“. Požaduje se přesné zarovnání snímače a obrázků v databázi. Tvářové příznaky jako jsou oči, ústa, atd. jsou lokalizované a využité pro rozpoznání. Tato metoda se dá lehko implementovat a není časově náročná (Obr. 3.2).



Obr. 3.2 – 3D rozpoznání tváře na principu analýzy vzhledu

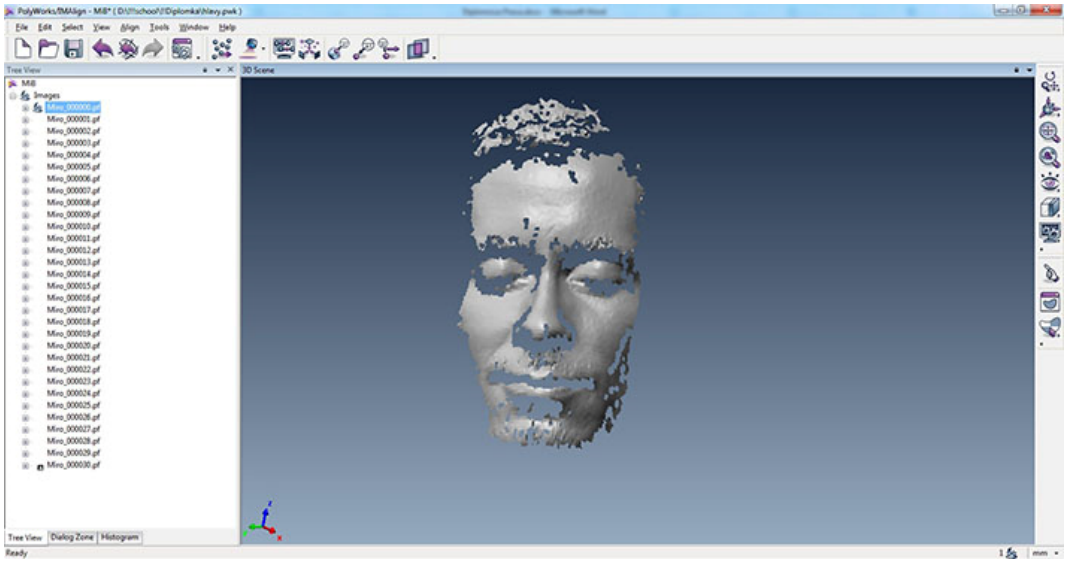
- 3D rozpoznání tváře na principu analýzy modelu - tato metoda je založená na metodě analýzy syntézou. Vytvoří se 3D model tváře s označenými a popsanými parametry, který se porovnává s modely v databázi. Tato metoda není vhodná pro aplikace v reálném čase (Obr. 3.3).



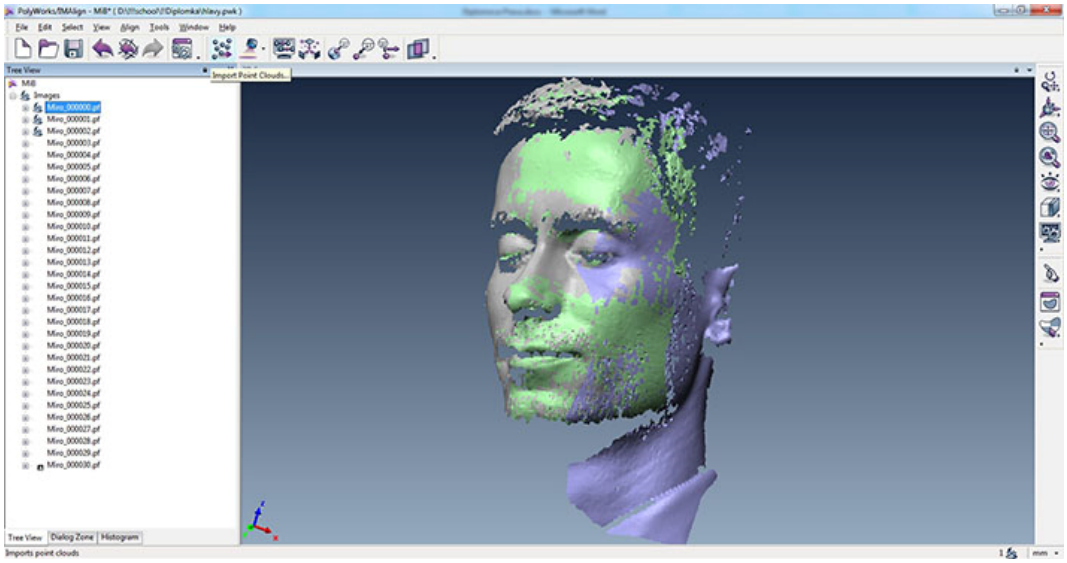
Obr. 3.3 – 3D rozpoznání tváře na principu analýzy modelu

4.2 Předzpracování a registrace dat

Na začátku celého procesu se zachytí 3D maska povrchu tváře (příklad vytvoření 3D tváře je na obrázcích Obr. 3.4. - Obr. 3.6). Existuje několik různých způsobů jak dosáhnout zachycení 3D povrchu tváře, například stereo kamery, hloubková kamera, laserová kamera, optické nebo laserové snímače, atd.



Obr. 3.4 – Jeden sken



Obr. 3.5 – Více skenů vytvářejících tvář

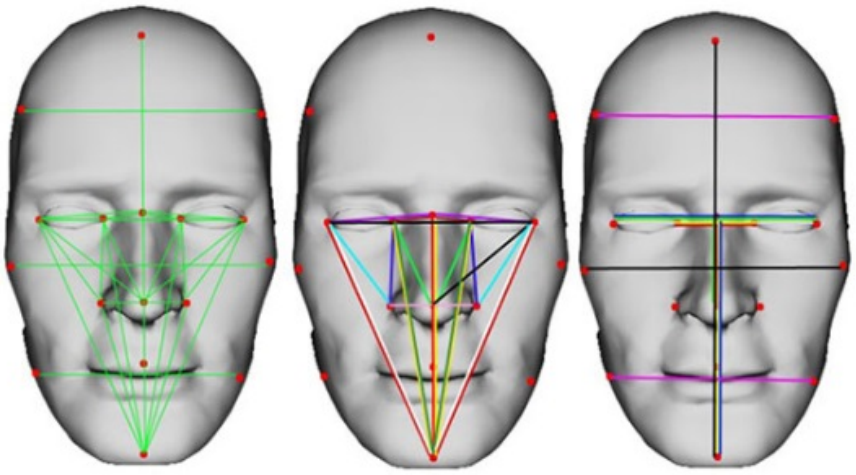
Obr. 3.6 – Výsledný 3D model tváře

Z celého získaného snímku je potřebná jen tvář. Vzhledem k tomu je potřebné ořezání tváře. Každá tvář je ohraničená obdélníkem, který se skládá ze 4 bodů na hlavě. Boční hrany se skládají z bodů, jejichž pozice je nejvíce vlevo a vpravo. Nejvyšší bod je horní okraj a spodní okraj obsahuje nejnižší bod. Ořezání je potom založené na obdélníku vytvořeném 4 body.

Zachycené údaje jsou následně předzpracovány pomocí algoritmů na extrakci příznaků.

Účelem extrakce příznaků je získat kompaktní informace z obrázků, které jsou důležité pro rozlišování mezi obrazy tváří různých lidí a jsou stabilní z pohledu fotometrických a geometrických variaci v obraze.

Jako příznaky možno použít body tváře (vrchol hlavy, čelo, oči, brada, nos, ústa, atd.) a vzdálenosti mezi těmito vybranými body v 3D Euklidovském prostoru (viz Obr. 3.7).



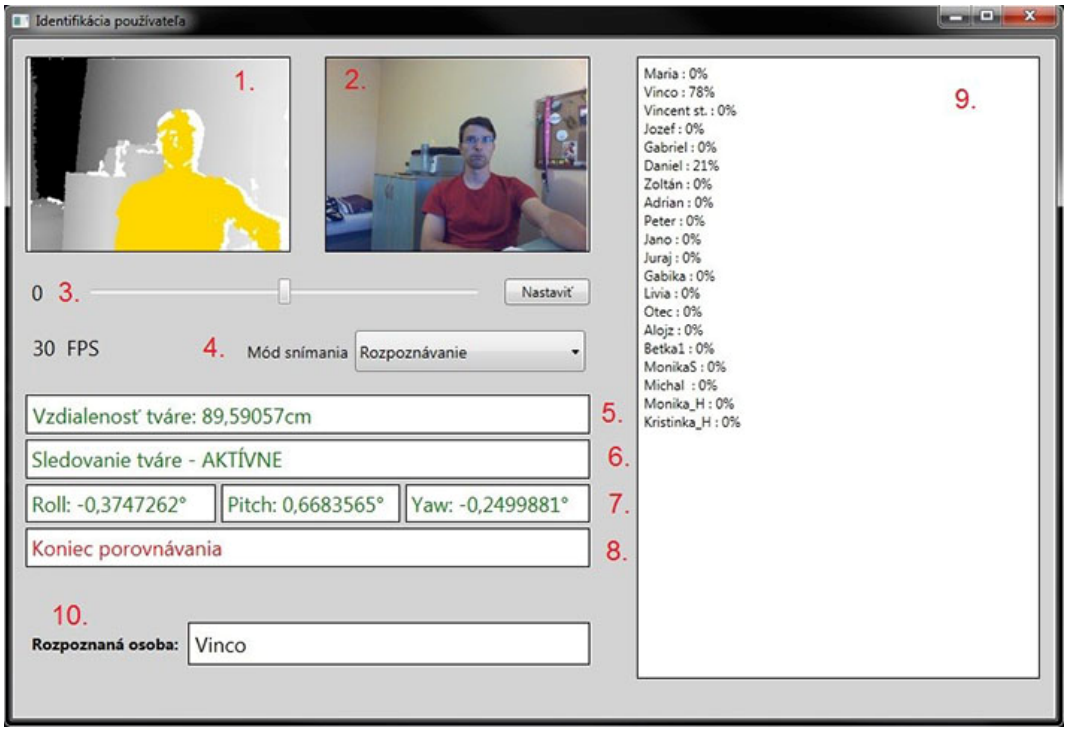
Obr. 3.7 – Příklad tvářových příznaků

4.3 Aplikace pro rozpoznání 3D tváře

3D rozpoznání tváře možno též použít v mnoha aplikacích, například na zabezpečený přístup do systému nebo rozpoznání uživatele pro Smart TV a umožnění online nakupování (např. může být povoleno jen pro rodiče a ne pro děti, atd.).

Úloha 3D rozpoznávání tváří vyžaduje stejně jako 2D rozpoznávání tváří vstup z kamery. Pro 3D rozpoznávání tváře je potřeba zachytit 3D povrch tváře. Hlavní proces rozpoznávání tváří se skládá z následujících částečných procesů:

- **3D snímání povrchu tváře** - existuje několik různých způsobů na realizaci této úlohy, například stereo kamery, laserové nebo hloubkové kamery (např. Kinect senzor Kinect), atd.
- **předzpracování** – zachycené údaje jsou následně předzpracovány
- **získávání příznaků** - účelem extrakce příznaků je získat kompaktní informace z obrázků, které jsou důležité pro rozlišování mezi obrazy tváří různých lidí a jsou stabilní, pokud jde o fotometrické a geometrické variace v obrazech
- **měření vzdálenosti** - poslední krok rozpoznávání 3D tváře je měření vzdálenosti mezi 3D povrchem tváře uživatele a 3D tváří uloženou v databázi. Existuje několik technik na měření vzdálenosti. Nejjednodušší způsob je měření lokální a globální vzdálenosti dvou tváří, kde je potřeba správně a velmi přesně určit body tváře (oči, nos, ústa, brada, uši, atd.) a měření jejich vzdálenosti od zavedených metrik. Sofistikovanější metody jsou metody nejbližšího souseda nebo Support Vector Machine atd.



Obr. 3.8 – Příklad GUI v aplikaci 3D rozpoznání tváří

5 Autentifikace

Přístupová bezpečnost systému je navrhovaná tak, aby umožnila přístup jen autorizovaným uživatelům, jejichž identitu je nutno předem ověřit. V zásadě se jedná o tři odlišné kroky, konkrétně identifikaci, autentifikaci a autorizaci [6].

Identifikace – je krok, při kterém se uživatel prokáže tzv. tokenem nebo identifikačním řetězcem, např. ve tvaru e-mailové adresy nebo tel. čísla.

Autentifikace – po přijetí identifikačního tokenu musí identifikovaný uživatel poskytnout důkaz o své identitě.

Autorizace – povoluje nebo zakazuje uživateli přístup k požadovanému obsahu a vykonání postupnosti akcí, na základě jeho oprávnění.

Uživatele systému je možné autentifikovat na základě toho, že něco znají (memometrics), něco rozpoznají (cognometrics), něco vlastní nebo čím jsou charakterističtí (biometrics). Při všech třech způsobech systém s uživatelem sdílí tajemství (tzv. authentication key). Během registrace se uživatel a systém dohodnou, co bude tím tajemstvím. V případě biometrie systém během registrace zaznamená digitální reprezentaci některého aspektu uživatelovy fyziologie nebo chování.

Obr. 4.1 – Možnosti autentifikace uživatele

5.1 Typy autentifikačních mechanizmů

Následující kapitola diskutuje autentifikační mechanismy, seskupené do kategorií podle způsobů jmenovaných v úvodu předešlé kapitoly.

Biometrics - charakteristika uživatele

Biometrie je porovnávání anatomické, fyziologické a behaviorální charakteristiky osoby.

Biometrické autentifikační mechanizmy spadají do dvou základních kategorií:

- **Behaviorální biometrie** - založená např. na pohybech uživatele při manipulaci s myší počítače, zpožděním nebo dynamikou úderů do klávesnice nebo dynamice podpisu.
- **Fyziologická charakteristika** - založená na otiscích prstů, hlasu, zorniček nebo sítnice, charakteristice rysů, tváře, ruky nebo geometrii prstů nebo dokonce tvaru ucha.

Biometrické technologie je složité mezi sebou porovnávat. Každá z nich má různý rozsah přesnosti, spolehlivosti a použitelnosti. I přes těžkosti při jejich vzájemném porovnávání však je možno definovat, jakou váhu má přesnost proti použitelnosti apod. V případě použitelnosti je jednoduchou biometrickou metodou například rozpoznávání tváře. Naopak metody, které vyžadují natočení některé části těla k senzoru (rozpoznávání sítnice), a tedy jsou méně komfortní pro použití, dokážou produkovat mnohem přesnější výsledky.

Testování biometrie je komplikovaný proces, který vyžaduje objektivní porovnání. Biometrická autentifikace proto není jednoduchý proces typu ano/ne, ale zahrnuje komplikovanou statistickou analýzu údajů, získaných ze senzorů v reálném čase.

Na světě existuje několik soukromých i veřejných testovacích laboratoří, které prosazují nastavení standardů této oblasti, jako například *National Institutes of Standards and technology* (**NIST**) nebo The International Biometric Group [6].

Memometrics - znalost něčeho

V tomto případě jde o generování náhodných sekvencí znaků nebo čísel, které jsou nazývané heslem (pokud jde o slovo), PINem (pokud jde o číselné vyjádření) nebo tzv. frází (passphrase; pokud jde o více jako jedno slovo). Hesla však mohou mít podobu sémantického tvaru.

Typy hesel:

- náhodné heslo – v současnosti je asi nejpopulárnějším autentifikačním mechanismem náhodné heslo. Hesla mají velký potenciál být dostatečně

bezpečnými. To ale nemusí platit v nekontrolovaném prostředí, jakým je webové prostředí. Uživatelé si z důvodu lehčího zapamatování volí heslo sami, i když systém dokáže nabídnout silnější heslo. Systémem nabídnuté heslo však často skončí zapsané na papíře, neboť je problematické si ho zapamatovat. Poskytovatelé web aplikací proto preferují uživatelem stanovené heslo [7].

- sémantické hesla – sémantická hesla jsou založená na tvorbě tajemství na základě deduktivního procesu. Tento proces sestává ze zadávání otázek s cílem získat přesnou odpověď, kterou vyžaduje (Obr. 4.2). Teoreticky mohou mít uživatelé s vyvoláním hesla menší problém, jelikož kognitivní hesla jsou založená na vyvolání známého faktu, který si uživatel musí pamatovat. Návrh bezpečnostních systémů založených na tomto způsobu není vůbec triviální [8].

Obr. 4.2 – Základné principy sémantických hesel

Cognometrics - rozpoznání něčeho uživatelem

Idea grafické autentifikace je založená na vizuální paměti uživatele. Vědecké studie poukazují na fakt, že lidská bytost má obrovské a prakticky neomezené možnosti pamatovat si obrázky [9].

Grafické kódy si získávají na popularitě hlavně v případě mobilních technologií, např. pro odblokování mobilního telefonu. Existují dva hlavní principy:

- **grafické kódy založené na rozpoznávání** - uživatel vybere cílový obrázek z rušivých elementů ve scéně. Při tomto přístupu, který je založený na čistě vizuální paměti, se využívá schopnost rozpoznat předtím viděný objekt mezi množstvím ostatních.
- **grafické kódy založené na pozici** - uživatel při tomto principu musí nakreslit obrazec, obvykle do mřížky, kde se vyžaduje vizuálně-prostorová paměť a přesný pohyb.

Vlastnictví

Autentifikace může být založená na něčem, co uživatel vlastní. Tímto objektem je tzv. token. Dobrým příkladem tokenu je SecureID od RSA Security na Obr. 4.3 [15]

Obr. 4.3 – Příklad tokenu: Bezpečnostní ID – RSA Security

Token prostřednictvím šifrovací funkce, která kombinuje zámek a tajný klíč, vytváří numerický kód, zobrazovaný na LCD displeji. Na autentifikaci použije vlastník SecureID zobrazené číslo. Autentifikační server taktéž pozná tajemství uložené v uživatelově tokenu, stejně jako i čas a den. Na základě těchto znalostí autentifikační server vykoná stejnou šifrovací funkci. Pro úspěšnou autentifikaci se propočítaná hodnota musí shodovat s hodnotou, kterou vložil uživatel.

Jiným příkladem je autentifikační token, který disponuje **USB** (*Universal Serial Bus*) rozhraním. Takovýto typ tokenu typicky obsahuje soukromý klíč, veřejný klíč a certifikát vydaný certifikační autoritou. Bezpečnostní systém vyšle tokenu tzv. výzvu (challenge), čímž se ověří správnost soukromého klíče. V dalším kroku systém ověří proti databázi, zda jméno na certifikátu koresponduje s autorizovanou identitou, které je umožněn vstup.

Tokeny mohou být poskytované ve formě software nebo hardware.

Nevýhodou hardwarového tokenu je potřeba mít ho u sebe vždy, je-li potřeba autentifikovat se vůči systému a je samozřejmě potřeba nosit u sebe všechny tokeny, pokud uživatel disponuje více přístupy.

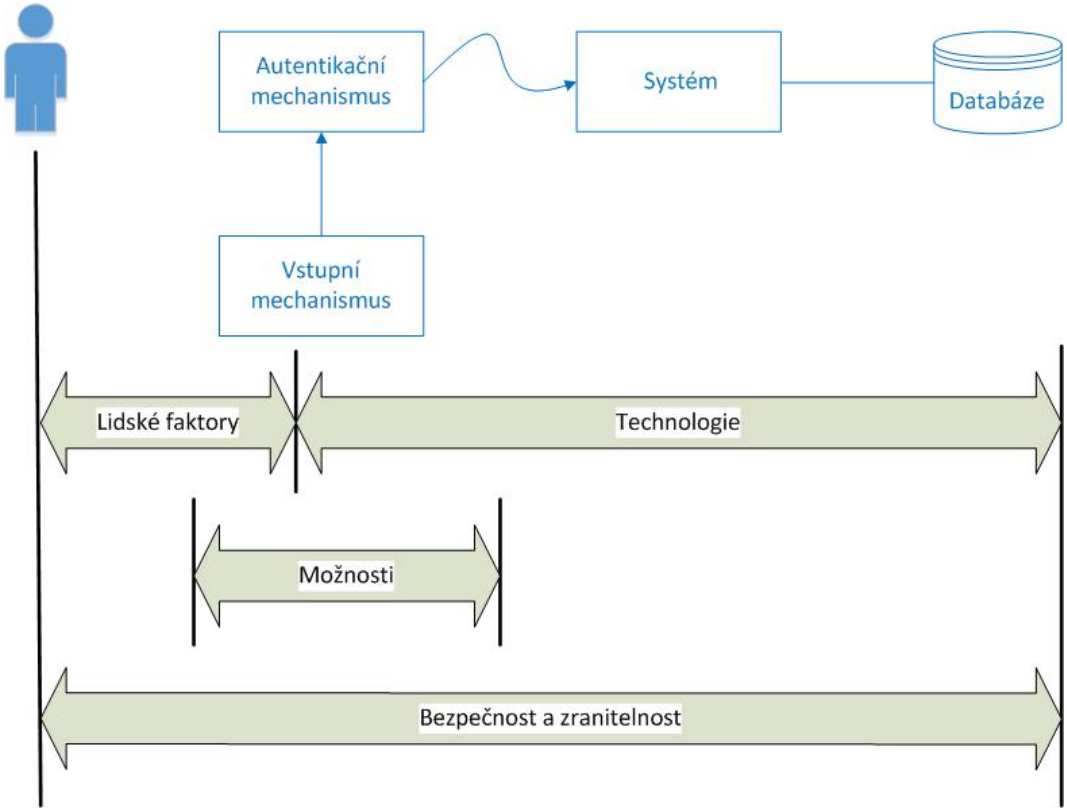
Softwarové tokeny tyto problémy řeší uložením klíčů na osobní zařízení, jako je například přenosný počítač (laptop). V tomto případě může uživatel přistupovat do systému jen ze zařízení, na kterém se tokeny nacházejí. Kromě jiného je použití softwarových tokenů zranitelné na kompromitovaném zařízení, kde se nacházejí.

5.2 Lidský faktor v procesu autentifikace

Několik autentifikačních scénářů využívá metodu šifrování veřejného klíče (public key cryptography). Například uživatel vlastní tzv. smart kartu, která je nositelem veřejného klíče a odpovídajícího soukromého klíče (private key). Na autentifikaci uživatele posílá systém náhodnou výzvu (challenge). Uživatel podepíše výzvu svým soukromým klíčem a posílá výsledek systému, který ověří podpis veřejným klíčem. Tímto způsobem dokáže systém verifikovat, zda je uživatel držitelem správného soukromého klíče a to bez potřeby přijmout tento klíč. Namísto potřeby ukládání veřejného klíče do soboru na vzdáleném systému dokáže smart karta předložit podepsanou výzvu a certifikát veřejného klíče, který byl podepsaný třetí stranou. V tomto případě jde o tzv. **PKI** (*Public Key Infrastructure*), normu vycházející ze specifikací ITU-T.

Jednou z možností autentifikačních systémů založených na PKI je, že uživatel musí při použití smart karty nejprve autentifikovat sebe sama do lokálního systému (typicky program na počítači nebo mobilním zařízení) obvykle s použitím hesla a až následně se smart karta použije na autentifikaci vzdáleného systému, prostřednictvím PKI. Vzdálený systém se spoléhá na to, že smart karta je spolehlivá. Věří prohlášení smart karty, že subjekt byl náležitě autentifikovaný. Jde o příklad tranzitivní důvěry.

Obr. 4.4 znázorňuje entity zahrnuté v autentifikačním procesu. V každém kroku tohoto procesu dokáže potenciální útočník získat přístup k autentifikačnímu klíči.



Obr. 4.4 – Entity zahrnuté v autentifikačním procesu

Oblastí zranitelnosti je však vstupní mechanizmus a uživatel. V případě autentifikace založené na znalosti (hesla, PINu…) si musí uživatelé pamatovat tajemství, což některým lidem jednoduše nevyhovuje nebo je to pro ně složité. Toto tajemství lidé obvykle vysloví někdy nechtíc nebo si ho zapíší, případně ho např. blízký rodinný příslušník zjistí, pokud není dostatečně silné. Uživatelé ale mnohokrát svoje heslo vědomě sdílejí s někým, koho dobře znají, jelikož si neuvědomují konsekvence z toho plynoucí. Další z možností je zachycení hesla na vstupu, způsobem *man-in-the-middle*, pokud nejde o zabezpečenou přenosovou cestu. Man in the middle (zkratka **MITM**, z angličtiny „člověk uprostřed“ nebo „člověk mezi“) patří mezi nejznámější problémy v informatice a kryptografii. Jeho podstatou je snaha útočníka odposlechnout komunikaci mezi účastníky tak, že se stane aktívním prostředníkem. V dnešní době není podstatné, aby byl fyzicky přítomný mezi dvěma komunikujícími body, protože síťový přenos se dá lekce přesměrovat.

Bezpečnost není možné řešit výhradně jen technickým způsobem, vzhledem k tomu, že uživatelé tvoří její integrální část [10].

6 Autorizace

Autorizace je ověření oprávnění subjektu při vstupu (do sítě nebo služby), na základě přístupových práv. Kromě toho definuje, ke kterým informacím může identifikovaný a autentifikovaný uživatel přistupovat a jaké akce může vykonat.

6.1 Model autorizace

Modely řízení přístupu (Obr. 5.1) se používají na uplatňování pravidel a účelů stanoveného bezpečnostního pravidla a definují, za jakých podmínek je možné přistupovat k prostředkům systému a jeho službám, tj. objektu. V současnosti se využívá několik hlavních modelů řízení přístupu [11]:

- *Discretionary Access Control* (**DAC**) – dovoluje vlastníkovi objektu definovat, kdo může a kdo nemůže přistoupit k tomuto objektu. Tento model se proto někdy nazývá i *Identity-Based Access Control* (**JENC**).

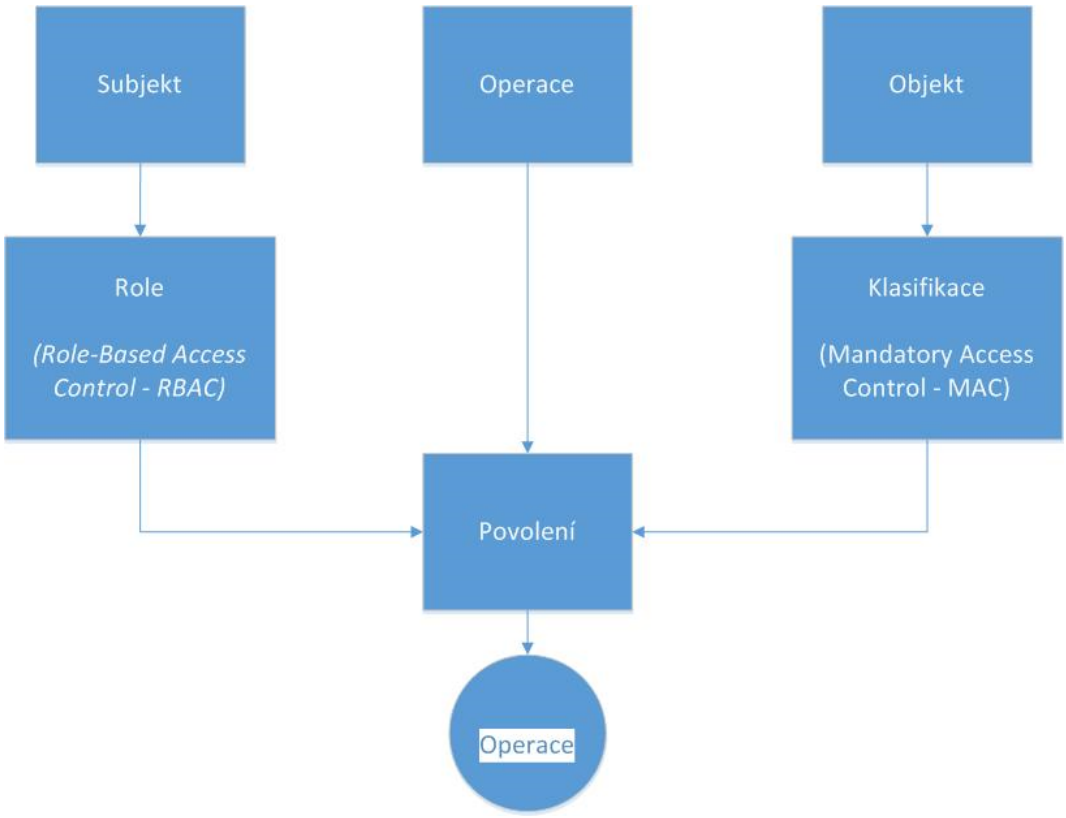
- *Mandatory Access Control* (**MAC**) – používá na určení toho, ke komu může subjekt (uživatel) přistupovat tzv. klasifikace. Subjekt tedy může přistoupit ke všem objektům, jejichž úroveň oprávnění je nižší nebo rovná než klasifikace objektu. Tento model se někdy nazývá i jako kontrola přístupu založená na pravidlech (rule-based access control).

- *Role-Based Access Control* (**RBAC**) – je nejrozšířenějším modelem. Používá na přidělení oprávnění subjektům role a skupiny. Uživatel tak může přistupovat k objektům na základě rolí, které má v oprávnění a též na základě své skupiny. Velkou výhodou a tím, co provádí tento model nejrozšířenějším je, že ve většině případů stačí modifikovat role a ne uživatele samotné.

- **Task Based Access Control** (**TBAC**) – je modelem, při kterém se kontroluje počet přistoupení uživatele k objektu. Pokud uživatel tohoto čísla dosáhne, jeho další přístup je zamítnut.

- **Attribute Based Access Control** (**ABAC**) – je model, který na přidělení oprávnění využívá atributy uživatele. Atributy jsou v tomto případě vlastnosti asociované s konkrétní entitou (Subjekt, Zdroje, Prostředí). Pokud za atributy považujeme i role, tak RBAC je možné taktéž modelovat prostřednictvím ABAC.

Všechny zmíněné modely je možno využívat i v kombinaci. Povolení závisí na subjektu – uživateli, který hodlá přistoupit k objektům a operacím, které si přeje uživatel vykonat.



Obr. 5.1 – Autorizační model

6.2 Pravidla správy přístupu

Jednou z nejpoužívanějších technik řízení přístupu (Obr. 5.2) je tzv. přístupová matice. Řádky matice představují možnosti uživatele a sloupce reprezentují objekty. Tato technika se často označuje i jako seznam řízení přístupu (*Access Control List* - **ACL**).

Kontrola přístupu v závislosti od obsahu je další rozšířenou technikou, při které může jeden uživatel přistoupit k detailnějším informacím nebo datům objektu jako jiný uživatel. Toto rozhodnutí může záviset na faktorech, jako například věk, použitý terminál, místo odkud přistupuje, IP adresa z jaké přistupuje, čas apod.

Obr. 5.2 – Správce řízení přístupu

6.3 Přístupová práva

Rozhodovací proces při přijetí požadavku na přístup do konkrétního systému/aplikace, jej informačního obsahu může v určitých krocích záviset na přístupových právech, uspořádaných do soboru tzv. povolení. Pravidla přidělování povolení vycházejí ve všeobecnosti z modelů popsaných v části 5.1 Model autorizace.

Příklad.

V systému je použitý RBAC model a definované tři role:

- administrátor
- vlastník skupiny
- uživatel v skupině

V tomto případě Administrátor přiděluje vlastníkovi skupiny nebo členovi přístupová práva vstupu ke konkrétním aplikacím.

Vlastník skupiny dále definuje, ke kterým aplikacím může konkrétní člen skupiny v roli Uživatele vstupovat. Pokud Administrátor předtím přidělil Vlastníkovi skupiny práva na přidávání, modifikaci a mazání obsahu v konkrétní aplikaci, může tato práva dále přidělit členovi skupiny, který se zároveň může stát i přispěvatelem obsahu, tj. vystupovat i v roli Vlastníka dat. Příkladem takovýchto aplikací je služba sdíleného multimédiálního obsahu.

Člena skupiny reprezentuje rola Uživatele dat a rola Vlastníka dat. Rozdíl mezi oběma dvěma rolemi je vlastnictví konkrétního informačního obsahu např. ve formě sdíleného videa v konkrétní aplikaci. Pokud uživatel systému v některé z aplikací takovýto obsah vytvoří, nabude zároveň roli Vlastníka dat a nad konkrétním obsahem a jeho možnostmi sdílení sám rozhoduje, znovu však v rámci kompetencí stanovených Vlastníkem skupiny. Člen skupiny v roli Vlastníka dat má možnost rozhodovat jen o akci a vztahu v rámci svých kompetencí.