Návrh systému na rozpoznávání osob prostřednictvím biometrie obličeje

System design for face recognition by face biometric

Jiří Gábrlík

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří GÁBRLÍK**
Osobní číslo:	**A08325**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh systému na rozpoznávání osob prostřednictvím biometrie obličeje**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na biometrické systémy.**
2. **Proveďte analýzu současného stavu dostupných biometrických systémů na rozpoznávání obličeje pro bezpečnostní účely.**
3. **Navrhněte možností inovace systému dostupnými prostředky s ohledem na snížení pořizovacích a udržovacích nákladů.**
4. **Vypracujte inovativní postup za pomocí vývojového diagramu.**
5. **Navrhněte hardwarové řešení biometrického systému.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Rak, R., et al., Biometrie a identita člověka ve forenzních a komerčních aplikacích, Grada, 2008**
2. **Ščurek, R., Biometrické metody identifikace osob v bezpečnostní praxi, skripta VŠB TU, Ostrava 2008**
3. **Oppel, A., Databáze bez předchozích znalostí, Computer Press, a.s., 2006**
4. **MATYÁŠ, Václav. Principy a technické aspekty autentizace. Data Security Management, Praha, Tate International. ISSN 1211 -8737, 2007, vol. XI, no. 1, s. 10 -16.**
5. **Svozil, L., Aspekty biometrické identifikace osob s využitím rozpoznávání tváře, bakalářská práce, UTB ve Zlíně, 2009**

Vedoucí bakalářské práce: **Ing. Pavel Neckář**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

V bakalářské práci se student nejprve zaměří na rešeršní část práce, ve které bude porovnávat dostupné systémy na biometrii obličeje pro bezpečnostní účely. Na základě zjištěných informací student navrhne možnosti inovací tohoto systému dostupnými prostředky s ohledem na snižování nákladů. V praktické části se student zaměří na vypracování inovativního postupu při rozpoznávání obličeje využitím vývojových diagramů, na jejichž základě sestaví hardwarové řešení tohoto systému.

Klíčová slova: Biometrie, Rozpoznání obličeje, Identifikace obličeje, Přístupový systém

ABSTRACT

In this thesis student will focused on the exploration of facts, which will compare the available systems on the facial biometrics for security purposes. From this facts student will propose the possibility of innovation in biometric system based on reducing prices. In the practical part, student will focus on developing innovative procedure for face recognition using flowcharts, based on this student will prepare the configuration of hardware solution for facial biometric system.

Keywords: Biometrics, Face recognition, Face identification, Access system

Na tomto místě bych rád poděkoval svému vedoucímu bakalářské práce panu Ing. Pavlu Neckářovi za jeho odborné vedení, rady a konzultace, které mi poskytoval během řešení mé bakalářské práce a paní Ing. Kateřině Sulovské za její rady z oblasti biometriky.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době je stále více důležité chránit svá data, informace a celkově své soukromí včetně možností přístupů. Nejčastěji je použito hesel, kódů, pinů, přístupových karet a tokenů. V posledních letech přibyly biometrické prvky, které poskytují výhody nepřenositelnosti bioinformace, člověk s sebou nemusí nosit množství přístupových prvků, které mohou být poškozeny, ztraceny nebo dokonce odcizeny a následně zneužity, ale biometrické rysy člověka jsou specifické již od jeho narození.

Bakalářská práce se zaměřuje na problematiku biometrických přístupových systémů založených na rozpoznávání lidského obličeje. Současné přístupové systémy využívající biometrii obličeje jsou vysoce spolehlivé, dle nastavených kritérií, ale jejich finanční nákladnost může odrazovat od jejich aplikace. Cílem této práce je navržení inovativního biometrického systému na principu rozpoznávání lidské tváře s ohledem právě na snížení pořizovacích, respektive výrobních a udržovacích nákladů.

V bakalářské práci jsou rozebrány algoritmy pro detekci, lokalizaci a samotné rozpoznání lidského obličeje. Detekce a lokalizace obličeje je důležitá pro rozhodnutí a specifikaci, kde se na snímku přesně nachází obličej. K detekci a lokalizaci obličeje jsou vztaženy porovnávací metody založené na barvě pleti, vlastnostech prostředí nebo pohybu obličeje. Pro rozpoznání obličeje jsou popsány algoritmy PCA, LDA, EBGM a 3D model. Na základě vlastností a využitelnosti jednotlivých algoritmů je navržen inovativní systém.

V doporučení pro budoucí vývoj softwarové části je navrhnut systém obsahující aplikaci algoritmů a postupů pro identifikaci uživatele. Názorný postup poskytuje vývojovým diagram v kapitole 9. Využita je kombinace dvou ze zmíněných algoritmů a celý proces identifikace je doplněn o prvek ne-biometrického charakteru.

Navrhovaný systém vychází z konceptu, který jsem vytvořil podle možností hardwarové náročnosti a „vytěžitelnosti“ systému. Cílem hardwarového řešení bylo snížit výrobní a pořizovací cenu přístupového biometrického systému tak, aby byla výrazně nižší než cena podobných zařízení porovnaných v kapitole 5 a systém se tak stal dostupnějším. Použité technické prostředky jsou vybrány s ohledem na plnění účelu, kompatibilitu a finanční nákladnost.

I. TEORETICKÁ ČÁST

1 DEFINICE BIOMETRIE

Biometrie je automatická metoda autentizace založená na rozpoznávání jedinečných biologických charakteristik subjektu - živé osoby. Metoda vychází z přesvědčení, že některé biologické charakteristiky (morfologické, fyziologické) jsou pro každého živého člověka jedinečné a neměnitelné. [1]

1.1 Biometrie a základní pojmy

Biometrie (biometric) je vědní obor zabývající se studií a zkoumáním živých organismů (bio-), především člověka, a měřením (metric) jeho biologických (anatomických a fyziologických) vlastností a také jeho chováním, tzn. behaviorálními charakteristikami. Pojem biometrika je odvozený z řeckých slov "bios" a "metron". První znamená "život", druhé pak "měřit, měření". Biometrika se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností, tedy měření a rozpoznávání určitých biologických a behaviorálních charakteristik člověka. [2]

1.1.1 Verification (ověření,verifikace)

Označuje proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku s již dříve zapsaným. Jedná se o tzv. princip one-to-one. [2]

1.1.2 Identification (identifikace)

Biometrický systém se pokouší pomocí nastavených procesů určit totožnost neznámého jedince. Biometrická informace je sejmuta a porovnávána se všemi uloženými vzorky. Princip je znám jako one-to-many. [2]

1.1.3 Recognition (rozpoznávání)

Označuje proces verifikace nebo identifikace na základě porovnání známých rysů z databáze s rysy získanými z digitálního snímku člověka.

1.1.4 Authentication (autentizace, legalizace)

Pojem, který lze sloučit s termínem rozpoznávání. Ovšem na konci procesu v tomto případě získá uživatel určitý status, např. oprávněný/neoprávněný. [2]

1.2 Historie biometriky

Ze všech dnes používaných biometrických technologií je nejznámější a také nejstarší metodou otisk prstu. Znalost o existenci papilárních linií na lidské kůži se objevuje u celé řady civilizací. Na území dnešního státu Indiana byly nalezeny kameny s rytými obrazy, tzv. "petroglyfy", znázorňující lidskou ruku s vyznačenými papilárními liniemi. Vytvořily je indiánské kmeny obývající tato území v období několika tisíc let před naším letopočtem. [3]

Moderní historie biometrie se datuje od roku 1882, kdy antropolog a šéf oddělení identifikace pachatelů pařížské policie Alphonse Bertillion hledal nějaký způsob, který by mu umožnil identifikovat již jednou odsouzené zločince. Především jeho zásluhou se biometrie stala reálným předmětem studia. Problém s opakovaně vězněnými zločinci tkvěl v tom, že při každém novém zatčení udávali nové falešné jméno a úřady nebyly sto jim jejich opakovanou recidivitu prokázat. Bertillion vynalezl metodu, která spočívala v měření fyzických znaků člověka a byla po něm nazvána bertilionáž. Uvědomil si, že některé charakteristické tělesné rysy jako je velikost lebky nebo délka prstů zůstanou stále stejné, i když si dané osoby změní jméno, přiberou na váze nebo si nechají ostříhat, či narůst vlasy. První praktické základy daktyloskopické identifikace položil sir William James Herschel. Úředník žijící v Indii měl za úkol vyplácení důchodů velkému počtu penzionovaných indických vojáků, kteří neměli žádné osobní doklady a které z pohledu Evropana nemohl rozeznat. Protože se Herschel domníval, že se důchod vyplácí i osobám, které již zemřely, zavedl nový výplatní systém. Každá vyplácená osoba musela příjem peněz potvrdit otiskem ukazováku a prostředníku pravé ruky na výplatní listinu. Zabránil tak podvodům a zároveň nasbíral množství materiálu ke zkoumání. Svoji metodu navrhl k využití ve věznicích, kde by zamezila záměnám těžkých zločinců za tzv. lehké případy. Jeho návrhy však byly označeny za výplody fantazie a nikdy nebyly akceptovány. Na problematice otisků prstů pracovalo mnoho dalších význačných osobností, mimo jiné český přírodovědec Jan Evangelista Purkyně, který jako první popsal jednotlivé typy charakteristických kreseb papilárních linií na koncových článcích prstů a klasifikoval je do devíti různých vzorů. [3]

Přes počáteční problémy a odmítání se nakonec technika otisků prstů dočkala uznání a i po nástupu nových technologií, jako je DNA či oční duhovka, zůstává dodnes nejpoužívanější metodou při identifikaci a ověřování identity osob. [3]

První pokusy identifikace osob na základě snímku obličeje pocházejí z šedesátých let. Tehdy byl vyvinut poloautomatický systém, který prováděl identifikaci na základě významných rysů, které byly vyznačeny administrátorem. Významný posun byl zaznamenán v sedmdesátých letech, kdy bylo zautomatizováno vyhledávání některých významných rysů (barva vlasů, šířka rtů). V roce 1988 byla poprvé využita metoda PCA (principal component analysis) v klasifikační fázi identifikace. Tato technika lineární algebry byla významným milníkem a je využívá dodnes. V roce 2001 byl vyvinut systém, který byl schopen práce v reálném čase. [4]

2 EFEKTIVNOST BIOMETRICKÝCH SYSTÉMŮ

Efektivnost biometrických systémů je udávána procentuální mírou pravděpodobnosti selhání zařízení. Patří sem koeficient nesprávného vyhodnocení odmítnutí žadatele (FRR) a koeficient nesprávného vyhodnocení přijetí žadatele (FAR).

2.1 Chybné odmítnutí žadatele – FRR (False Rejection Rate)

Koeficient chybného odmítnutí žadatele je označován jako chyba I. druhu. Nerozpoznání uživatele způsobuje zamezení přístupu osoby, která je oprávněná, v systému registrovaná a přístup má mít povolen. Tato chyba pouze snižuje komfort verifikace/ identifikace a neohrožuje bezpečnost chráněného objektu.

$$FRR = \frac{N_{FR}}{N_{EIA}} \cdot 100\ [\%] \tag{1}$$

$$FRR = \frac{N_{FR}}{N_{EVA}} \cdot 100\ [\%] \tag{2}$$

N_{FR} - počet chybných odmítnutí (Number of False Rejection).
N_{EIA} - počet pokusů oprávněných osob o identifikaci (Number of Enrolle Identification Attemps).
N_{EVA} - počet pokusů oprávněných osob o verifikaci (Number of Enrolle Verification Attemps)

2.2 Chybné přijetí žadatele – FAR (False Acceptance Rate)

Koeficient chybného přijetí žadatele je označován jako chyba II. druhu. Jde o povolení přístupu osobě, která nemá v systému uloženou svou biometrickou šablonu, tudíž nemá mít ani přístup do objektu nebo aplikace. Důvodem může být mylné přiřazení biometrické šablony jiného žadatele nebo úspěšné cílené oklamání systému pachatelem. Takové selhání systému vytváří oproti chybnému odmítnutí uživatele vážné bezpečnostní riziko.

$$FAR = \frac{N_{FA}}{N_{IIA}} \cdot 100\ [\%] \tag{3}$$

$$FAR = \frac{N_{FA}}{N_{IVA}} \cdot 100\ [\%] \tag{4}$$

N_{FA} - počet chybných přijetí (Number of False Acceptance).

N_{IIA} - počet pokusů neoprávněných osob o identifikaci (Number of Ipostor Identification Attemps)

N_{IVA} - počet pokusů neoprávněných osob o verifikaci (Number of Impostor Verification Attemps)

3 DRUHY BIOMETRICKÝCH IDENTIFIKACÍ

3.1 Otisk prstu

Identifikace na základě otisku prstu je jednou z nejznámějších a nejvíce publikovaných biometrických metod. Otisk prstu se používá pro identifikaci celá století, a to hlavně pro svou jedinečnost a stálost v čase. [2]

Princip identifikace pomocí otisku prstů je založen na tvaru povrchu kůže. Vnitřní povrch prstů obsahuje vyvýšené, drobné, brázdovité útvary, které vytvářejí různé vzory. Jsou to **smyčky, přesleny a oblouky**. Důležité je to, s jakou frekvencí se vyskytují. Při porovnávání otisků prstů se sleduje jak přítomnost identifikačních bodů (markantů), tak i jejich umístění v daném otisku. Otisk prstu obsahuje v průměru 75-175 identifikačních bodů. V praxi není stanoven přesný počet bodů nutný k rozlišení mezi dvěma otisky. [5]

Obr. 1 Struktury otisku prstu
- smyčky, přesleny, oblouky [9]

3.2 Geometrie ruky

Biometrické systémy založené na verifikaci geometrie ruky jsou používány v různorodých aplikacích, včetně docházkových systémů, kde jsou poměrně velmi rozšířené. Pro mnoho biometrických projektů je verifikace geometrie ruky obvykle prvním systémem, o kterém se při návrhu uvažuje. [5]

Zařízení pro rozeznávání geometrie ruky využívají jednoduchého principu měření a tří-dimensionálního snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce pomocí CCD kamery. Na obrazu ruky lze najít přes 31 000

polohových bodů a provést 90 různých měření vzdáleností. Doba verifikace je 1 až 2 sekundy. [2]

3.3 Oční duhovka

Duhovka je barevná část oka, jejíž zabarvení odpovídá množství pigmentu uvnitř svaloviny. Duhovka se vyvíjí během prenatálního růstu plodu a její vzorkování je náhodné, tudíž jedinečné pro každého člověka. Žádný člověk, ani dvojčata, nemají obě duhovky stejné, což činí tyto systémy nejpřesnějšími ze všech. Snímání duhovky vyžaduje velice kvalitní digitální kameru a infračervené osvětlení oka. Během snímání se duhovka mapuje do fázových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Tyto informace pak slouží k vytvoření duhovkové mapy a šablony pro identifikaci. Při verifikačním procesu se porovnává mapa duhovky verifikované osoby s referenční pomocí testu statistické nezávislosti. [2]

3.4 Sítnice oka

Pro rozpoznávání osoby dle její sítnice se používá obraz struktury cév na pozadí lidského oka v okolí slepé skvrny. Sítnice je světlo-citlivý povrch na zadní straně oka a je složena z velkého množství nervových buněk. Pro získání obrazu se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém. Verifikace sítnice je velice přesnou metodou identifikace. Aby mohlo dojít k verifikaci, musí se uživatel dívat do přesně vymezeného prostoru. Při tomto procesu není možné používat brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast používání a její použití se shrnuje na oblasti vůbec nejvyššího stupně zabezpečení. [2]

3.5 Žilní řečiště

Jedná se o jednu z nejnovějších metod rozpoznávání jedince. Tato technologie se vyznačuje obtížností falšování. Technologie spočívá ve snímání hřbetu ruky nebo prstů speciální kamerou v infračerveném světle. Tak lze získat černobílý obraz stromové struktury žil, které tvoří zřetelný vzorec. Struktura krevního řečiště se navíc v dospělém věku příliš nemění, je velice výrazná a její jedinečnost i mezi jednovaječnými dvojčaty prokázaly vědecké studie. Výhodou je také bezkontaktní princip. Snímání probíhá tak, že

zdroj (pole LED diody) prosvítí ruku a na základě různé absorpce záření krevních cév a ostatních tkání se vytvoří obraz pomocí snímací CCD kamery. Obraz je dále digitalizován a zpracováván za cílem vyextrahování sítě cév. Ukládají se důležité vlastnosti jako: body a úhly větvení cév a tloušťka cév. [2]

3.6 Hlas

Verifikace lidského hlasu je definováno jako elektronická metoda positivní identifikace osoby pomocí rozšířené analýzy digitálního "otisku hlasu". Tvar hlasivek, ústní dutiny, jazyka a zubů způsobují, že rezonance vokálního traktu je u různých osob dostatečně odlišná. [5]

Jednou z nejúspěšnějších technik pro ověřování hlasu je porovnávání vzorků pomocí analýzy signálů řeči. Dynamické, stejně jako okamžité spektrální znaky zřejmě hrají významnou roli ve vnímání řeči. Některé ověřovací technologie zakládají své autentizační rozhodnutí na analýze vět. Věta má více akustické informace než jednoduché slovo; více informace umožňuje vyšší kvalitu srovnávacího procesu pro absolutní shodu. Slova bývají krátká a neobsahují dostatečnou akustickou informaci, která by spolehlivě odlišila mluvčího. Věty zná pouze autentický mluvčí a mohou jimi být i množiny slov, které je mluvčí schopen vyslovit opakovaně test za testem. [5]

Uživatelé si často vytvářejí svoje vlastní tajné autentizační věty a bezpečnost systému je částečně rozšířena, protože neoprávnění uživatelé neví, kterou větu použít, natož jakým hlasem ji vyslovit. Charakteristickým příznakem současných systémů pro verifikaci hlasu je, že verifikace může být za určitých okolností (nastydnutí, šum okolí, atd.) mnohem komplikovanější než u jiných biometrik. Avšak vzhledem k významu této biometrické techniky, lze předpokládat její významný rozvoj. [5]

3.7 Ušní boltec

Identifikace člověka využívající biometrii ušního boltce je založená na individuálním tvaru a morfometrické stavbě ušního boltce každého jedince. Obecně existují tři metody biometrické identifikace podle ušního boltce:

1. Podle morfometrických vztahů – geometrie ušního boltce, ve 2D nebo 3D formě
2. Podle otisku struktur ušního boltce – tato metoda ale pro praxi není příliš "komfortní", její využití je ve forenzní oblasti
3. Podle termogramu ušního boltce – termografického snímku, mapujícího rozložení tělesné teploty na ušním boltci

Použitelnou metodou pro komerční využití, tak aby byla komfortní pro uživatele, je identifikace podle morfometrických vztahů – geometrie ušního boltce. V tomto případě je uživateli ušní boltec nasnímán speciálním optickým snímacím zařízením ze vzdálenosti cca 0,5 – 1 m. Data zanesená na snímku (morfometrické vztahy – rozměry, tvary, položení významných bodů, křivky apod.) jsou pak vyhodnocena a v závislosti na použitém typu algoritmu porovnána s příslušnou databází. [2]

3.8 Obličej

Metody identifikace pomocí obličeje jsou popsány podrobněji v následující kapitole.

4 PRINCIPY ROZPOZNÁVÁNÍ OBLIČEJE

Zde jsou uvedeny některé metody, které se v současnosti používají k verifikaci/identifikaci osob podle obličeje. Tento proces je ovlivněn řadou aspektů, jako jsou změny osvětlení-natočení, rotace, stíny. Tyto rušivé vlivy jsou celkem snadno normalizovatelné, závažnější problémy představují morfologické změny způsobené stárnutím a výrazy způsobené emocemi.

Existují dva základní přístupy rozpoznávání obličeje

- Geometrický- založený na rysech tváře
- Fotometrický- založený na vzhledu obrazu tváře

Podrobnější způsob dělení přístupů rozpoznávání obličeje

- Strukturální přístup
- Holistický přístup
- Znalostní metody
- Srovnávání šablon

Strukturální přístup

Rozpoznávání jednotlivých dominantních částí obličeje (oči, ústa, …) předkládaného vzoru, změření antropometrických veličin, jejich normalizace vzhledem k předpokládaným rušivým vlivům, porovnání s databází známých fotografií použitím klasifikačních algoritmů, statistické rozhodnutí o relativní podobnosti s takto vybranou množinou obrazů. [6]

Holistický přístup

Identifikace vzorku pomocí globálních reprezentací opět s následným statistickým vyhodnocením relativní pravděpodobnosti. Příznačné pro tento přístup jsou kombinace metody backpropagation (metoda zpětného učení neuronové sítě), základní analýzy komponent (PCA) a dekompozice jedinečných hodnot (SVD). [6]

Znalostní metody

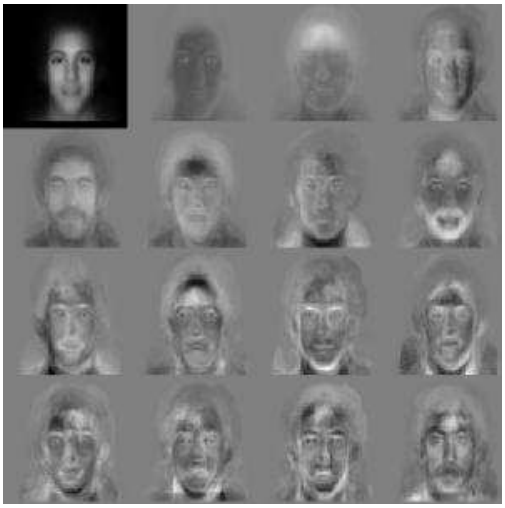
Tvář je prohledávána na základě předem daných pravidel, pomocí kterých je popsána „typická tvář“. Pravidly se vyjadřují vztahy mezi různými částmi obličeje. Tato metoda vyžaduje velmi precizní lokalizaci a popis jednotlivých příznaků, což vede k nutnosti použití složitých a robustních algoritmů. Z tohoto důvodu tyto metody zpravidla nedosahují požadovaných výsledků. [6]

Srovnávání šablon

Hledání na základě korelace obrazu s přednastavenými šablonami buď celého obličeje a jeho částí. Nevýhodou tohoto přístupu je nutnost vytvořit a mít uloženy v paměti jednotlivé šablony, které je potřeba většinou ručně vytvořit, což je velmi pracné a časově náročné. [6]

4.1 Analýza hlavních částí (PCA - Principal Components Analysis)

Každou tvář lze rozdělit na tzv. eigenfaces (vzory tváří - matice jasových úrovní) a poté jde opět složit (viz. Obr. 2). Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo - hash. Metoda využívá normalizovaných obrázků, které se vyznačují standardizovaným umístěním očí, uší a dalších významných bodů. Metoda PCA provede redukci nepotřebných příznaků, což znamená, že jsou odebrány příznaky, které jsou korelované s jinými příznaky. Počet příznaků se tak výrazně sníží (zhruba na tisícinu), a tak je usnadněna klasifikace i uložení jinak velkých databází. Vlastní klasifikace je založena na některé z obvykle využívaných klasifikačních technik – například na metodě nejbližšího souseda. [7]



Obr. 2 Standardní eigenfaces
používané pro rozložení obrazu [7]

4.2 Lineární diskriminační analýza (LDA - Linear Discriminant Analysis)

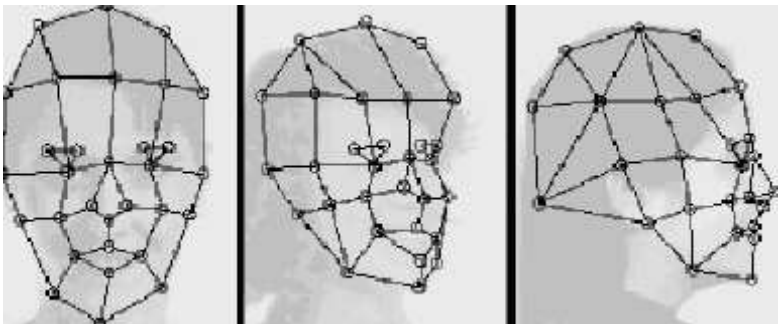
LDA je metoda, kdy se třídí pořízené obrazy tváří do skupin. Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině, každý blok snímků reprezentuje jednu třídu (viz Obr. 3). [2]

Obr. 3 Příklad šesti tříd užitím LDA [7]

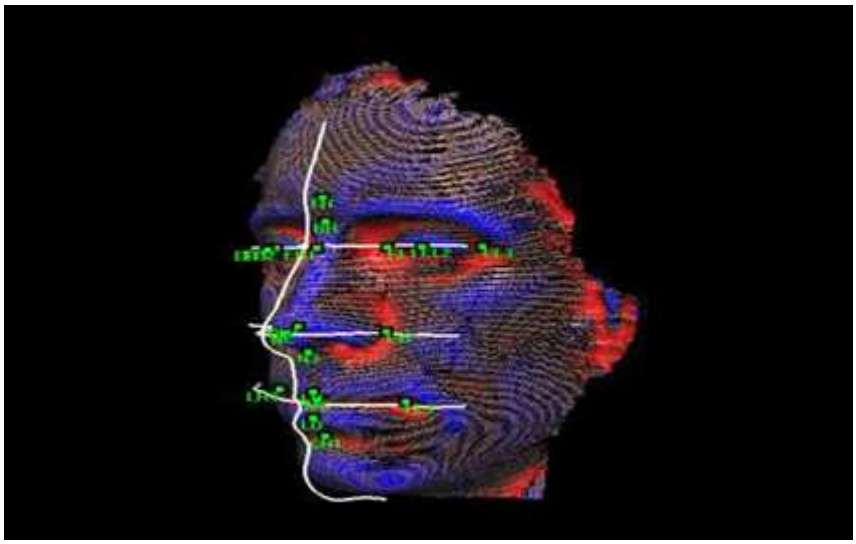
4.3 Elastický srovnávací diagram (EBGM - Elastic bunch graph matching)

Metoda EBGM byla vyvinuta, jelikož předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení). Princip je takový, že na obličeji se definují uzlové body, které se poté propojí a tím definují linie tváře v prostoru a vznikne souřadnicová síť obličeje (viz. Obrázek). Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou. [2]

FRR: <1%; FAR: 0,1%, Čas verifikace: 3 sekundy, Míra spolehlivost: střední



Obr. 4 Síť vytvořená elastickým mapováním [7]



Obr. 5 Obraz zpracovaný počítačem [7]

4.4 3D model obličeje

Další metodou verifikace obličeje je vytvoření jeho 3D modelu. Pořízení galerie autorizovaných osob je nákladná metoda, při níž se využívá 3D laserový scanner. Lidská tvář je deformovanou plochou v 3D prostoru. Tato metoda je založena na morfingu a tzv. fittingu („lícování“) – deformaci tohoto modelu obličeje, který zakóduje tvar a strukturu v rámci parametrů modelu a na algoritmu, který obnoví tyto parametry z jednotlivého obrazu obličeje. Databáze známých vzorů obličejů se vytváří 3D snímačem, nebo aproximací fotografií z několika úhlů pohledu obličeje (například trojdílné policejní fotografie). Pro identifikaci obličeje je z modelu použit tvar a texturové parametry, které jsou odděleny od obrazových parametrů, jako je poloha a osvětlení. [7]

4.5 Neuronové sítě

Neuronová síť je jedním z výpočetních modelů používaných v umělé inteligenci. Jejím vzorem je chování odpovídajících biologických struktur. Skládá se z umělých neuronů, jejichž předobrazem je biologický neuron. Neurony jsou vzájemně propojeny a navzájem si předávají signály a transformují je pomocí určitých přenosových funkcí. Neuron má libovolný počet vstupů, ale pouze jeden výstup. [8]

Formální neuron je v podstatě jednoduchá jednotka, která ohodnotí - vynásobí všechny vstupy jejich vahami (váhy se mění během učení - odtud plyne adaptace sítě) a takto získané hodnoty sečte. Výslednou hodnotu dosadí do přenosové funkce neuronu a výstup této funkce je i výstupem z neuronu, který slouží jako vstup do neuronů dalších. [8]

5 BIOMETRICKÁ ZAŘÍZENÍ SOUČASNÉHO TRHU

V kapitole jsou porovnána tři přístupová zařízení využívající biometrii obličeje, které jsou v současné době trendem na českém trhu. Souhrnné vlastnosti porovnávaných zařízení jsou následně obsaženy v tabulce (Tab. 1). Významnou částí u porovnávaných systémů je identifikace uživatele pomocí obličeje, ale i podpora dalších přístupových metod nebo jejich kombinace.

5.1 Suprema D-station

D-station je zařízení od korejské společnosti Suprema, které vyniká tím, že umožňuje k autentizaci uživatele využít více biometrických vlastností najednou, a to díky Multi-Biometrickému režimu MBFT (Multi-Biometric Fusion Technology). Následně jsou systémem nabízeny režimy Ultra Speed a Twin.

Technickou platformu tvoří tříjádrový procesor Tri-CPU o výkonu 1,4 GHz (2x 400 MHz + 1x 667 MHz), který je nutný pro rychlé zpracování několika vstupních dat najednou. Komunikace s uživatelem probíhá přes širokoúhlý 5,0” WVGA dotykový LCD s pozorovacím úhlem 140°. Snímání obličejů je realizováno pomocí vestavěné kamery s rozlišením 1,3 megapixelů. D-Station disponuje vnitřní pamětí 1 GB, kterou lze rozšířit o SD kartu. Z komunikačních rozhraní to jsou Wi-Fi, TCP/IP, RS232 a RS485, USB a dále 4 TTL vstupy a Wiegand pro komunikaci s RFID (Radio Frequency Identification) kartami. Zajímavostí je akcelerometr, který slouží k indikaci neoprávněné manipulaci se zařízením. Napájecí napětí 12V DC je přiváděno pomocí PoE - Power over Ethernet (napájení zajištěno síťovou složkou), což snižuje množství kabeláže. Kapacita zařízení je 400 000 uživatelů pro identifikaci (1:1) a 20 000 pro verifikaci (1:N).

Multi-Biometric Fusion Technology (MBFT)

V MBFT režimu probíhá autentizace na základě rozpoznání uživatelova obličeje a jeho otisků dvou prstů. Zaručena je maximální míra správnosti autentizace, důvodem je doplnění celého systému dvěma senzory na otisky prstů. Podporováno je snímaní obou otisků prstů i obličeje současně. To následně přispívá k vyšší rychlosti celého procesu.

Ultra Speed

Ultra Speed režim využívá ke zjištění identity osob pouze snímače otisků prstů, ale opět oba současně. Celý proces rozpoznání osoby je následně rychlejší než MBFT.

Twin

Režim Twin dokáže zpracovat současně dva otisky prstů, ale od dvou nezávislých uživatelů. Systém autentizuje dvě různé osoby v jeden okamžik. Je tedy vhodný jako přístupové zařízení do firem, kde se například střídají směny s větším počtem lidí. D-Station v režimu Twin, pak rychle odbaví dva zástupy najednou.

Výsledná volba systému autentizace (MBFT, Ultra Speed nebo Twin) vychází z předpokladů pořizovatele na rychlost a kvalitu identifikace. Vhodnost je založena na vysoké flexibilitě využití tohoto systému.

Obr. 6 Suprema D-station [10]

5.2 EFG Aktion AFT-500

AFT-500 terminál je od české firmy EFG CZ spol. s r.o. a kromě systému pro rozpoznávání obličejů má i integrovaný snímač RFID karet. Procesorem je zde TI DM CPU 600 MHz. Na předním panelu je umístěn 3,5” TFT displej s rozlišením 240x320 DPI. Displej však není dotykový, a proto je vedle něj umístěna kapacitní klávesnice s 16 tlačítky. Paměť je tvořena SD kartou s kapacitou 4GB, která je schopna pojmout až 70 000

snímků. AFT-500 umožňuje kombinovat několik přístupových metod. Uživatel může být autentizován pomocí jednotlivých metod nebo jejich kombinacemi:

- biometrií obličeje
- RFID karty
- PINu a biometrií obličeje
- RFID karty a biometrií obličeje

Každá z metod distribuovaná systémem vytváří určité okolnosti a podmínky pro správnou identifikaci, které se samozřejmě liší rychlostí. Je třeba volit kompromis mezi rychlostí a bezpečností podle použití systému. Kapacita zařízení je 500 osob, ale existuje možnost navýšení této kapacity na 1400 osob. Detekci a identifikaci obličeje lze provádět do vzdálenosti 80 cm od kamery. Výstupem terminálu jsou relé 1x NC/NO/C, pro komunikaci to jsou rozhraní Ethernet, USB a Wiegand 26bit/34bit. Zařízení je zkonstruováno pod krytím IP54 pro použití ve venkovních prostorech, kde lze očekávat vyšší možnost kontaktu s vodou.

Obr. 7 EFG Aktion AFT-500 [12]

5.3 Comfis iFace 303

Vstupní terminál iFace 303 opět od české firmy, tak jako terminal D-Station využívá metod rozpoznávání obličeje a otisku prstu uživatele. Navíc umožňuje i verifikaci pomocí RFID nebo hesla. U tohoto zařízení ale není možné jednotlivé metody kombinovat. Systémové vybavení iFace 303 disponuje procesorem ZK Multi-Bio CPU 630MHz, 4,3“ dotykovým TFT displejem a pamětí 256 MB. Ke snímání obličeje používá infračervenou kameru s vysokým rozlišením, díky níž je možná identifikace i v tmavém prostředí. Kapacita zařízení umožňuje pojmout 700 obličejů, 5 000 otisků prstů a 10 000 ID karet. Stejně jako D-Station také nabízí komunikaci přes rozhraní RS232, RS485, TCP/IP/, USB, Wiegand 26bit, Wi-Fi a GPRS. Stejně tak i napájecí napětí 12V DC je přiváděno pomocí PoE. Záložní baterie o kapacitě 2000mAh dokáže udržet zařízení v chodu až na 4h běžného provozu. Pomocí funkce webserver umožňuje správu systému prostřednictvím internetového prohlížeče.

Obr. 8 iFace 303 [11]

5.4 Porovnání parametrů jednotlivých zařízení

	EFG Aktion AFT-500	Comfis iFace 303	Suprema D-Station
Kapacita obličejů	500	700	10 000
Doba ověření [s]	≤ 1	≤ 2	≤ 1
Displej [’’]	3,5	4,3	5,0
Možnosti identifikace	Obličej/ Pin a obličej/ Karta/ Karta a obličej	Obličej/ RFID/ otisk prstu/ heslo	Obličej a 2 otisky prstů/ 2 otisky prstů/ 1 otisk prstu
Procesor	TI DM CPU 600MHz	Multi-Bio CPU 630MHz	Tri-CPU 1,4GHz
Napájecí napětí [V]	12	12	12
Proudový odběr [A]	0,5	3	0,5
Provozní teplota [°C]	0 – 40	0 – 45	-20 – 50
Rozměry [mm]	200 x 115 x 95	193,6 x 165,2 x 86	143 x 82 x 35
Cena bez DPH [Kč]	18 900	27 000	39 900

Tab. 1 Porovnání parametrů jednotlivých zařízení

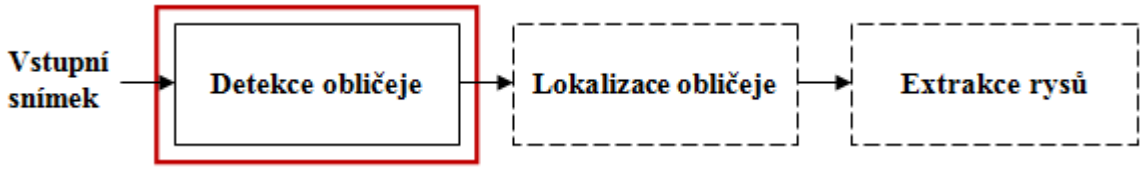
Jednou z důležitých vlastností při výběru autonomních vstupních terminálů je kapacita obličejů, které je schopno zařízení rozpoznat. Nejnižší kapacitu obličejů nabízí Aktion AFT-500, jak již bylo zmíněno, lze tuto paměť zvětšit z původních 500 až na 1400. I přesto ale tato kapacita nemusí být dostatečná pro některé aplikace, například v podniku s větším počtem zaměstnanců. Dalším důležitým parametrem je rychlost autentizace. Ta je u všech zařízení kratší než 2 sekundy a srovnatelná, přestože D-Station disponuje procesorem se třemi jádry o celkovém výkonu více než dvojnásobném oproti zmíněným konkurentům. S lepšími technickými parametry vystupuje D-Station. Jeho celkové konstrukční provedení disponuje malou velikostí a použitelností ve velkém rozmezí teplot. Výhody tohoto zařízení nemusí vyvážit rozdíl cen a lepší variantou se může stát i Aktion AFT-500 s navýšenou kapacitou obličejů na 1400. Oproti iFace 303 navíc umožňuje kombinovat

metody autentizace. Problémovou částí u Supremy lze považovat technickou podporu, protože se jedná o výrobek z Korey, zatímco oba konkurenti pochází z ČR. Přínosem u systému iFace 303 může být Wi-Fi modul a správa pomocí internetového prohlížeče.

II. PRAKTICKÁ ČÁST

6 ALGORITMY PRO DETEKCI OBLIČEJE

V praxi používané algoritmy biometrickými systémy pro detekci obličejů využívají odlišné postupy. Obecně ale platí, že nejdříve je na vstupním snímku nutné detekovat rozpoznávaný obličej, aby mohl být následně lokalizován. Některé algoritmy používají pro detekci i lokalizaci obličeje téměř totožné metody, tudíž obě fáze probíhají v jednom kroku.



Obr. 9 Posloupnost algoritmů- detekce obličeje

6.1 Metody detekce obličeje

Metodu detekce obličeje je potřeba volit v závislosti na prostředí, kde bude využívána. Každá metoda má své výhody i nevýhody. Záleží také, jestli je detekce prováděna na statických nebo pohyblivých snímcích.

6.1.1 Detekce ve stálém prostředí

Detekce obličeje je prováděna z fotografií, které jsou pořizovány za stálého osvětlení a s pozadím stále stejné barvy. Ideální je místnost bez oken, ve které sluneční světlo nemůže ovlivňovat intenzitu nastaveného umělého osvětlení. Za takovýchto podmínek je detekce obličeje na fotografii usnadněna.

Výhoda: Snadná detekce obličeje

Nevýhoda: Těžko udržitelné světelné podmínky z hlediska praktičnosti.

6.1.2 Detekce podle barvy pleti

Metoda detekuje obličej na základě barvy lidské pleti. Systém na snímku vyhledává souvislou plochu, která má podobnou barvu jako lidská pleť. Systém rozhodování je

podřízen chybě, která vyvstává na základě odlišnosti barvy lidské pleti, rozptyl barev vychází od téměř bílé až po hodně tmavou v závislosti na lidské rase, a proto je těžké nastavit optimální barvu detekce. Velkou roli hraje také barva pozadí. Světlé pozadí může splývat se světlou pletí a tmavé pozadí s tmavou pletí, proto následná detekce neutvoří kvalitní obraz obličeje. Pro zmírnění nedostatků této metody by bylo vhodné používat pozadí, které je nejvíce barevně odlišné od lidské pleti.

Výhoda: Při optimální barvě pozadí spolehlivá detekce.

Nevýhoda: Neexistuje univerzální barva lidské kůže.

6.1.3 Detekce na základě pohybu

Detekování obličeje z časově reálného videa využívá například pohybu celé hlavy oproti jejímu pozadí. Systém se zaměřuje na změnu přibližně stále stejné plochy obrazu. Obličej může být z videa detekován také pomocí očí. V důsledku mrkání očí dojde současně ke změně obrazu na dvou místech obrazu ve vodorovné ose.

Výhoda: Umožňuje spolehlivou detekci.

Nevýhoda: Nelze použít u fotografií.

7 ALGORITMY PRO ROZPOZNÁNÍ OBLIČEJE

V předchozí kapitole je nastíněná problematika detekce obličeje. Součástí postupu rozpoznání obličeje je hned po jeho detekci lokalizace a extrakce rysů obličeje, které systém dělají jedinečným.

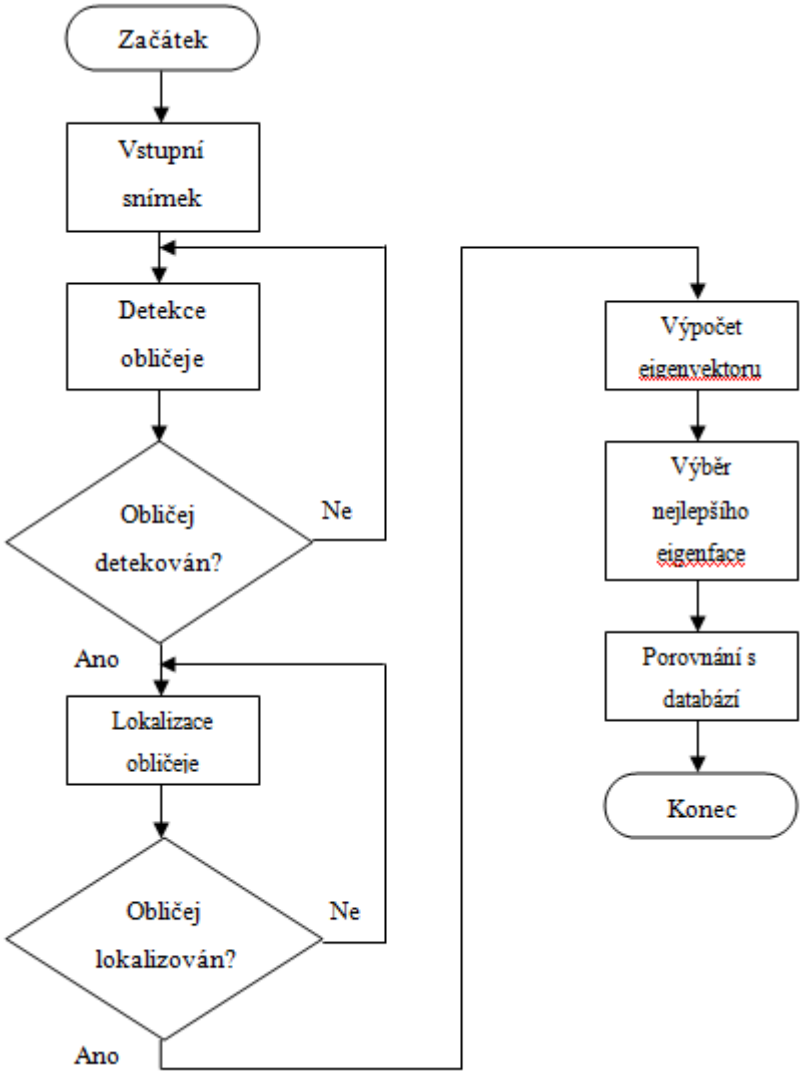
Obr. 10 Posloupnost algoritmů- lokalizace obličeje a extrakce rysů

7.1 Algoritmus PCA

Základem správné funkce tohoto algoritmu je databáze několika snímků každého uživatele, přičemž na každém snímku má uživatel odlišný výraz a snímky jsou pořízeny při různém osvětlení. Po samotné detekci a lokalizaci uživatelova obličeje dochází k výpočtu eigenvektorů obličeje, které zohledňují hlavní rysy obličeje a tvoří eigenfaces. Každý obličej je tvořen lineární kombinací eigenfaces. Následně se vybere nejlepší eigenface a ten je porovnán s databází.

Eigenvektor- informace o jednotlivých rysech obličeje

Eigenface- soubor eigenvektorů tvořící celý obličej



Obr. 11 Vývojový diagram algoritmu PCA

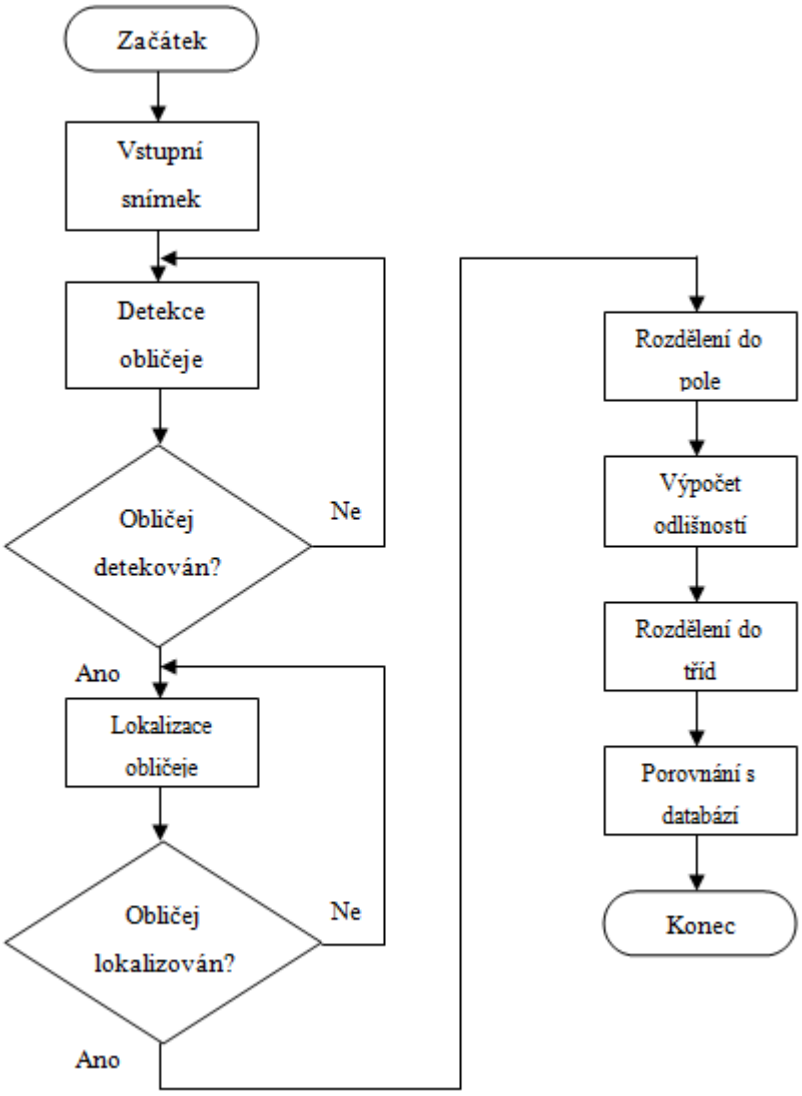
7.2 Algoritmus LDA

Algoritmus využívá v části rozpoznání obličeje několik snímků každého uživatele. Snímky by se měli lišit úhlem natočení obličeje, výrazem obličeje, nasvětlením scény a barvou pozadí. V případě, že uživatel nosí brýle, tak i snímky s brýlemi a bez nich. Snímky se řadí do dvourozměrného pole podle intenzity a dělí do tříd podle míry podobnosti. Podobnost se určuje podle očí, úst, vlasů, brady nebo jejich kombinací a klasifikují se podle míry odlišnosti:

- malé změny
- výrazné změny v horizontálním směru, tj. vertikální hrany

- výrazné změny ve vertikálním směru, tj. horizontální hrany
- výrazné změny v různých částech

Cílem je, aby snímky v každé třídě si byly co nejvíce podobné a jednotlivé třídy aby se od sebe co nejvíce lišily.

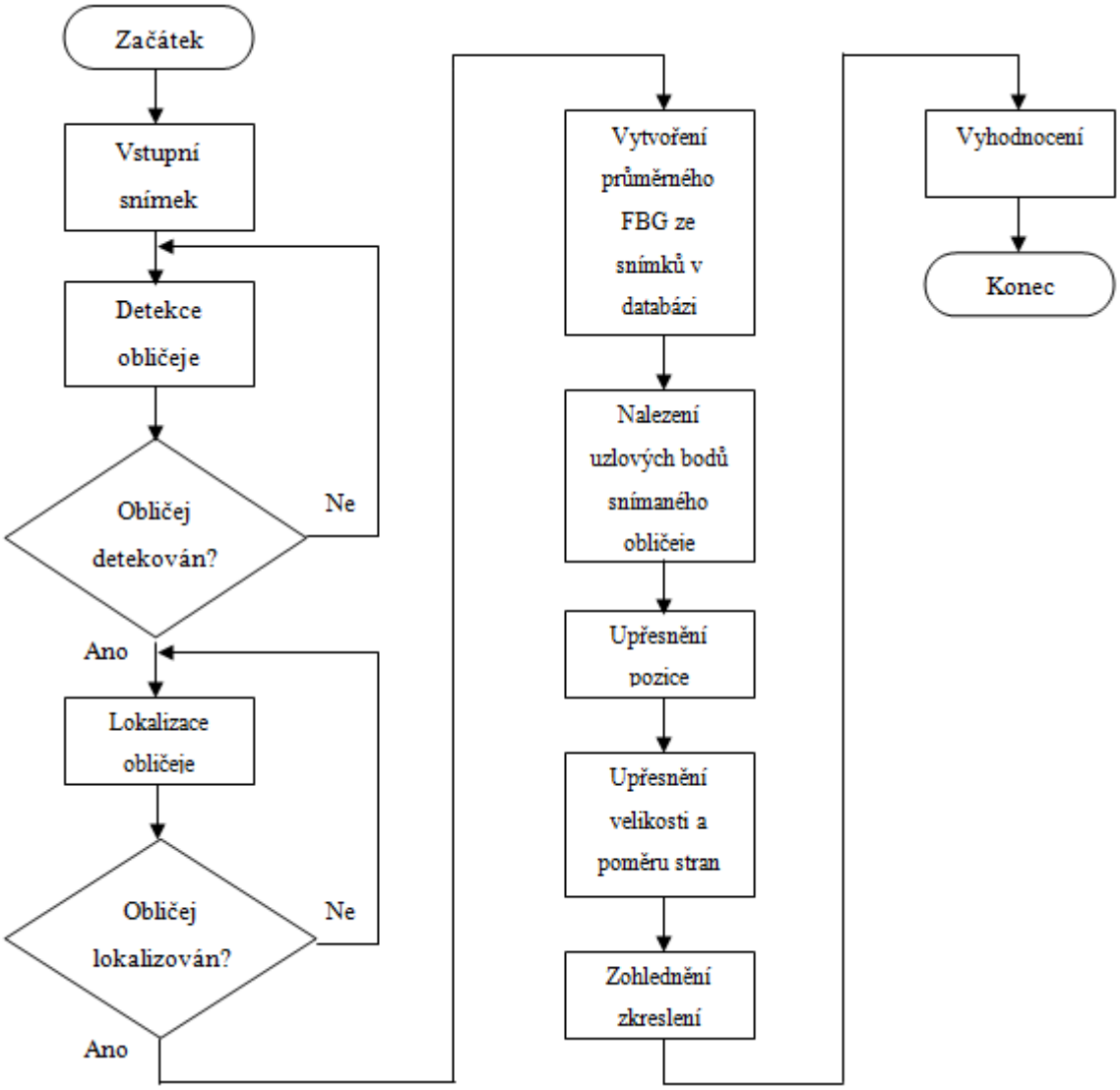


Obr. 12 Vývojový diagram algoritmu LDA

7.3 Algoritmus EBGM

Na rozdíl od předchozích dvou algoritmů není algoritmus EBGM závislý na osvětlení snímaného obličeje. V každém obličeji jsou nalezeny uzlové body, které mohou být reprezentovány například koutky úst, očí, špičkou nosu nebo horním a dolním okrajem uší. Ze všech obličejů v databázi se vytvoří FBG (face bunch graph), který obsahuje různé

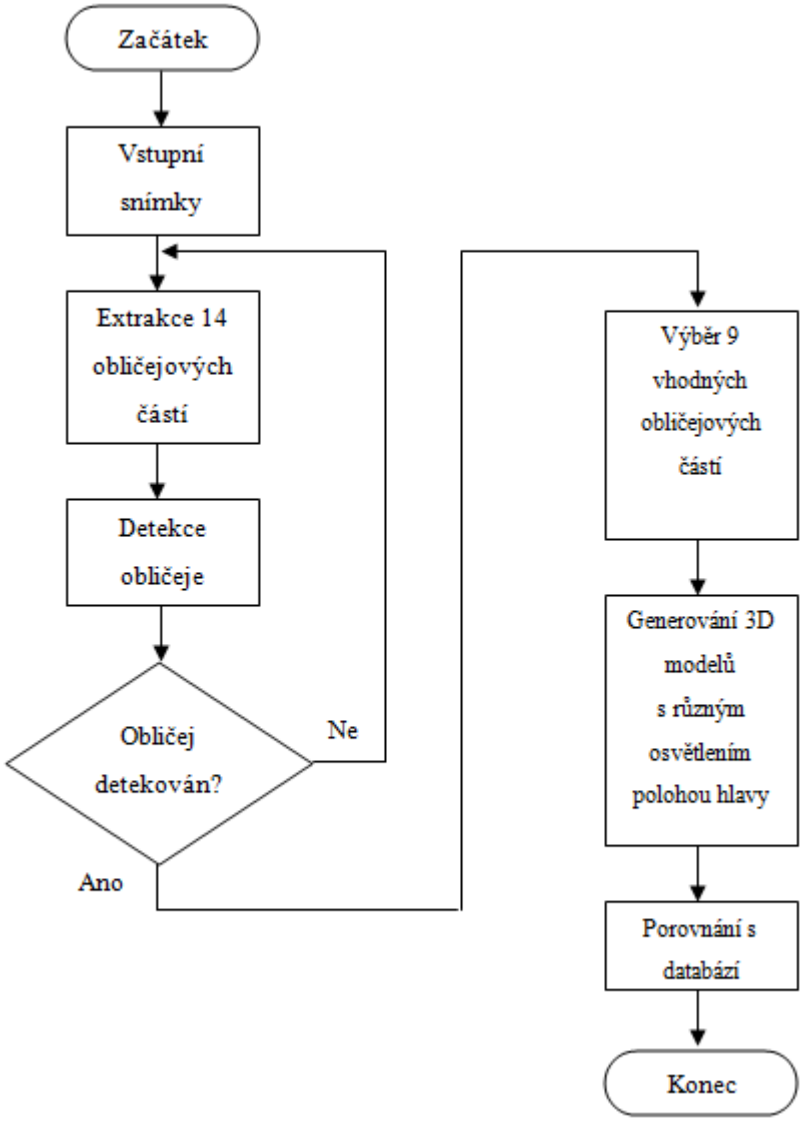
pozice těchto uzlových bodů. Cílem metody je najít na snímku obličeje uzlové body, které jsou shodné s uzlovými body některého snímku z FBG. Postup se skládá ze čtyř základních fází. V první fázi se hledá přibližná pozice obličeje. Z FBG se vytvoří průměrný graf obličeje a porovnává se podobnost se snímaným obličejem ve čtvercích o ploše 4 pixely a následně 1 pixel. V dalším kroku dochází k upřesnění pozice a velikosti a to tím způsobem, že se zkontroluje podobnost na pozicích o ± 3 pixely v horizontální i vertikální ose a v každé z těchto osmi pozic se ověří dvě různé velikosti se shodnou pozicí. Varianta s nejlepší shodou se použije v dalším kroku pro upřesnění velikosti a poměru stran. V poslední fází se zohledňuje možné lokální zkreslení.



Obr. 13 Vývojový diagram algoritmu EBGM

7.4 3D model obličeje

Metoda 3D modelu obličeje využívá jako vstupní informace 3 fotografie - přední pohled, poloviční profil a úplný profil uživatele. Aby byl obličej vůbec detekován, musí se z těchto fotografií extrahovat 14 obličejových oblastí, které obsahují jednoznačné prvky obličeje, jako jsou oči, ústa, nos. Po detekci obličeje dochází k vygenerování 3D modelu obličeje, který slouží k samotnému rozpoznávání. Modelů se generuje několik, a to s různým osvětlením a různým natočením hlavy. Všechny 3D modely jsou v rozlišení 58x58 bodů a jsou složeny z 9 ze 14 již zmíněných obličejových částí. Použijí se jen ty nejvhodnější, tedy nejsouvislejší.



Obr. 14 Vývojový diagram pro 3D model obličeje

7.5 Srovnání algoritmů

Algoritmus PCA je v dnešní době považován za efektivní a spolehlivý způsob rozpoznávání obličeje. Pro jeho správnou funkci potřebuje mít databázi alespoň se 3 až 4 snímky každého uživatele. Aby stejné spolehlivosti dosáhl i algoritmus LDA, potřebuje takových snímků mnohem více, a to asi pětinásobek, protože na snímcích by měl být kromě jiného výrazu a osvětlení také jiný úhel natočení obličeje a odlišná barva pozadí. Pro vyšší počet snímků je potřeba i větší kapacita databáze. Navíc práce s vyšším počtem snímků bývá zpravidla pomalejší. Jak již bylo zmíněno, obě metody jsou hodně závislé na osvětlení, při kterém jsou snímky pořizovány. Rychlost rozpoznání závisí na použité databázi a hardwaru. Algoritmus EBGM dosahuje při rozpoznávání vysoké spolehlivosti, dokonce vyšší než PCA. Problém metody spočívá v nepřesné lokalizaci uzlových bodů. Vhodnost použití vychází z kombinace algoritmu EBGM s algoritmem PCA. Metoda rozpoznávání obličeje na základě jeho 3D modelu je ze všech uvedených metod finančně nejnákladnější, protože k nasnímání obličeje je potřeba buď laserový skener, nebo zařízení pro snímání předního pohledu, polovičního profilu a úplného profilu současně.

8 INOVATIVNÍ SYSTÉM

Na základě zjištěných informací o současných přístupových systémech, používaných algoritmech a jejich nedostatcích, je zde popsán návrh inovativního řešení přístupového systému s ohledem na snížení pořizovacích a udržovacích nákladů. U většiny objektů, které využívají přístupové biometrické systémy je běžné, že jimi mají opatřeno více než jeden vstup, a to razantně zvyšuje cenu celého přístupového systému.

8.1 Snížení pořizovacích nákladů

Celý inovativní systém je založen na tom, že jednotlivé přístupové terminály nejsou autonomní a využívají jednodušší hardware. Nevýhodou autonomních terminálů je, že i když jich je v objektu použito více, každý z nich má svou vlastní databázi a pracují nezávisle na sobě. Oproti tomu neautonomní terminály, které jsou součástí inovativního systému, vlastní databázi nemají a využívají centrální databázi, která je realizována pomocí jednoho serveru umístěného uvnitř střeženého objektu. Přístupové terminály jsou se serverem umístěným v serverovně objektu propojeny pomocí sítě Ethernet. Využitím centrální databáze dochází jednak ke zvýšení efektivity vyhodnocování přístupů, protože systém neustále přijímá informace o všech žádostech o přístup a hlavně dochází ke snížení pořizovacích nákladů. Jednotlivé terminály nemusí mít velkou kapacitu vnitřní paměti na ukládání snímků a také výkonný procesor na jejich zpracování. Zpracování a uložení snímků probíhá na zmíněném centrálním serveru s databází. Další možností, jak snížit pořizovací náklady, je aplikace levnějšího displeje. Je zbytečné, aby displej na přístupovém terminálu byl dotykový a s úhlopříčkou 4,0“ nebo 5,0“. Primární funkcí displeje je zobrazovat polohu snímaného obličeje, aby uživatel věděl, jestli je objektivem zabírán správně. Místo dotykového displeje je terminál doplněn o klasickou tlačítkovou klávesnici, která také plní přístupovou funkci z ohledu vložení PINu. Toto řešení obsahující menší displej s nižším rozlišením a tlačítkovou klávesnici sníží pořizovací náklady oproti dotykovému displeji s vysokým rozlišením.

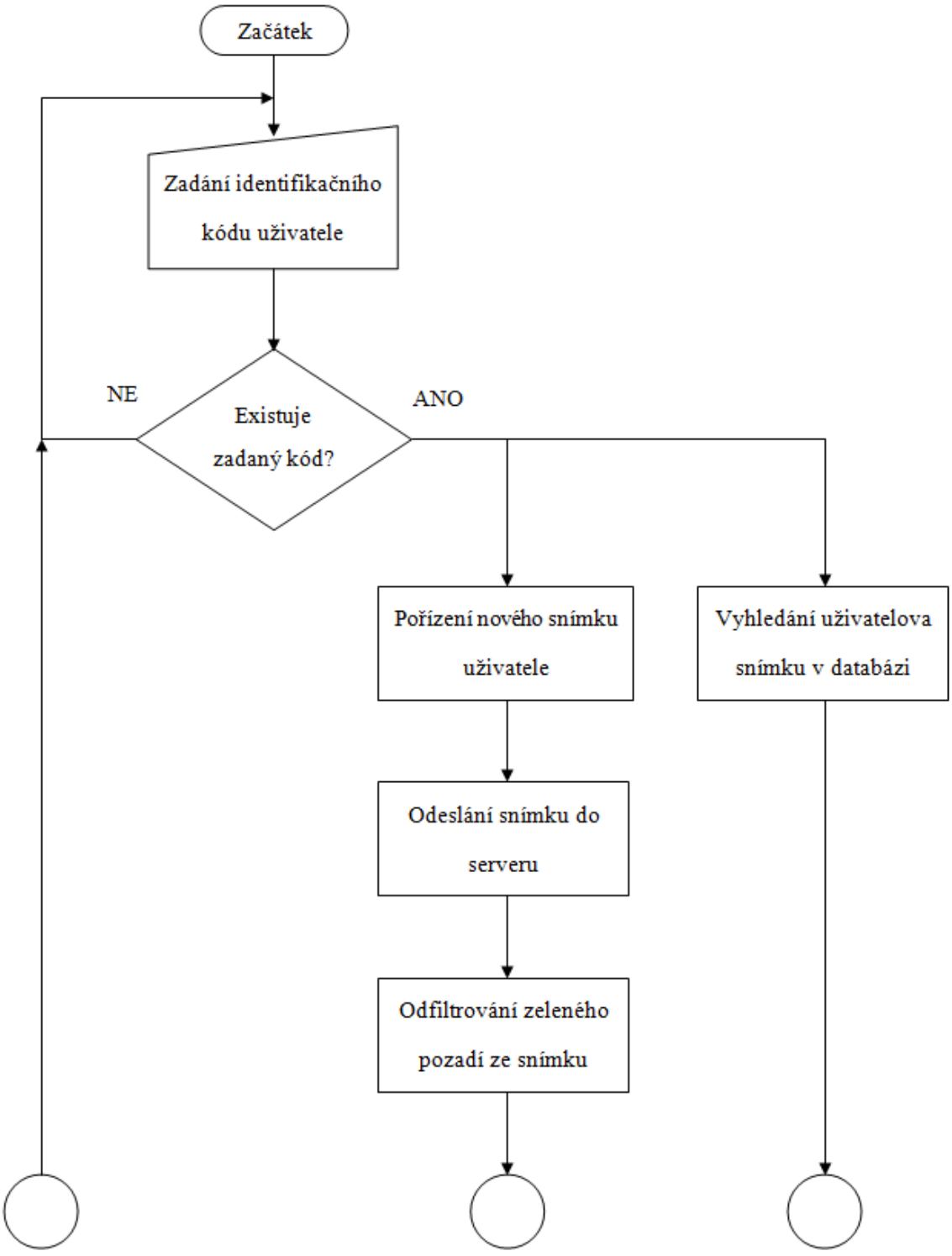
8.2 Snížení udržovacích nákladů

Snížení udržovacích nákladů je dosaženo tím, že odpadá nutnost spravovat databázi každého terminálu zvlášť, ale správa se provádí pouze na centrálním serveru. V případě

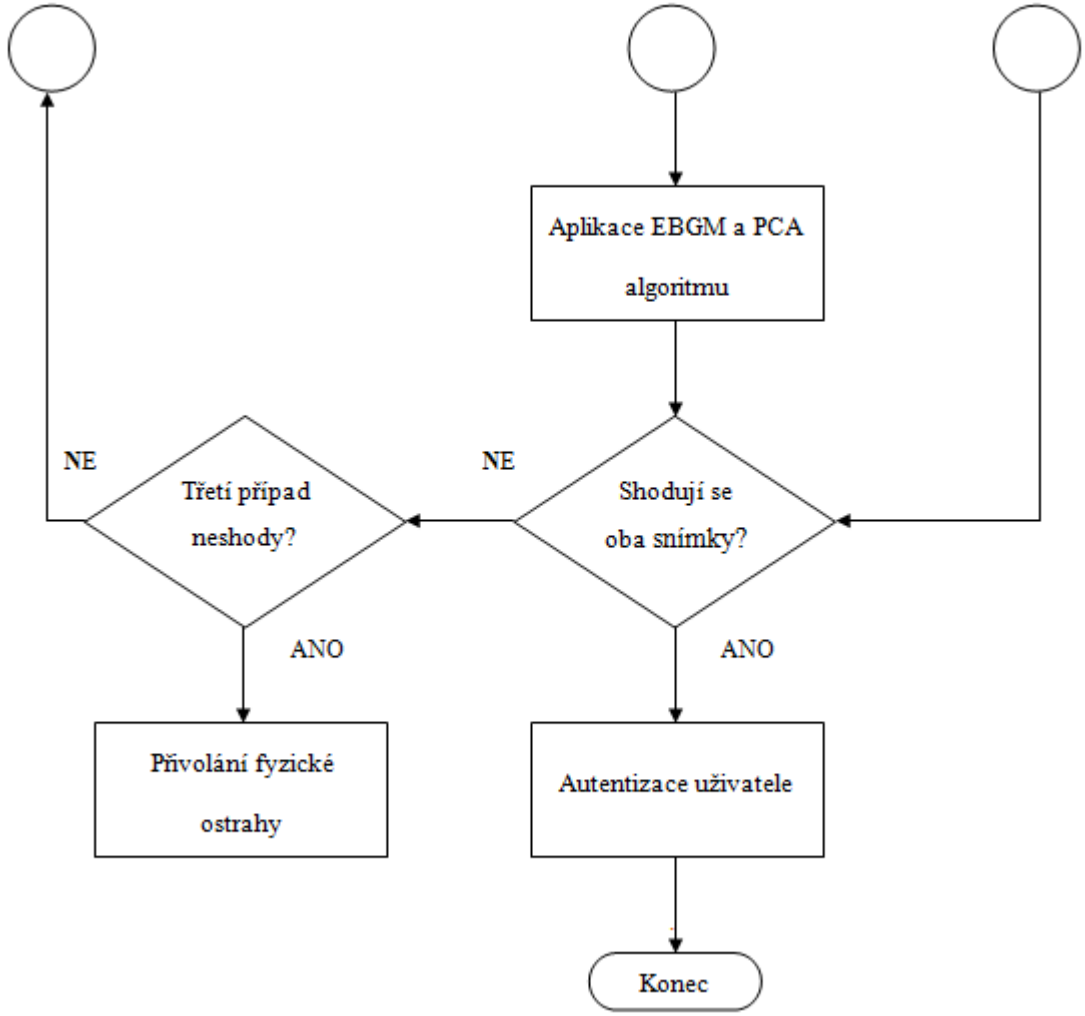
požadavku na rozšíření systému o další přístupový terminál, stačí přístupový terminál jen připojit a nakonfigurovat. Žádná manipulace s databází není nutná.

9 ŘEŠENÍ INOVATIVNÍHO SYSTÉMU

9.1 Vývojový diagram



Obr. 15 Vývojový diagram inovativního systému- 1/2



Obr. 16 Vývojový diagram inovativního systému- 2/2

9.2 Popis systému

9.2.1 Prostředí

Základním předpokladem pro správnou funkci navrhovaného systému je stálost prostředí, ve kterém jsou pořizovány snímky uživatelů. Jedná se o barvu pozadí a osvětlení. Barva pozadí by měla být taková, aby její kontrast s barvou pletí člověka byl co největší, a to bez ohledu na rasu. Jako vhodné se jeví odstíny zelené barvy z důvodu nebiologického kožního pigmentu. Dále je nutné, aby osvětlení celé scény včetně pozadí bylo neměnné a osvětlovalo dané místo se stálou intenzitou a jasem světla. Jen za výše zmíněných podmínek je zaručena barevná stálost pozadí, bez ohledu na denní dobu. Místo, kde bude probíhat autentizace, by mělo být bez přístupu vnějšího světla, tudíž bez oken a s plnými dveřmi, nebo odděleno od okolí tak, aby bylo zamezeno ovlivnění jiným osvětlením, než k tomu určeným.

9.2.2 Proces autentizace

Pokud jsou podmínky prostředí splněny, může dojít k procesu autentizace uživatele. V prvním kroku zadá uživatel do terminálu pomocí klávesnice svůj identifikační kód. Po zadání identifikačního kódu systém zajistí vyhledání potřebných informací v databázi (existence uživatele, přístupová práva). V případě, že uživatel zadá identifikační kód a systém jej vyhodnotí jako neplatný, může se jej pokusit zadat znovu. Pokud ale uživatel se zadaným kódem existuje, má již v databázi uložen svůj zpracovaný snímek. Snímek se ihned připraví k porovnání, zatímco ve stejný okamžik proběhne snímání obličeje uživatele. Nově pořízený snímek se odešle na server k softwarovému zpracování. V první řadě se z něj odfiltruje stejný odstín zelené barvy, jako má pozadí na fotografii. Tím vznikne pouze obraz obličeje a vlasů uživatele. Na takto vyextrahovaný obličej se aplikuje kombinace algoritmů EBGM a PCA (viz kapitola 7) a výsledek se porovná s již nalezeným, stejnou metodou zpracovaným snímkem, který je v databázi přiřazen uživateli na základě jeho identifikačního kódu. Pokud je splněna míra shody obou snímků, uživatel je identifikován a je mu například umožněn vstup. V opačném případě dojde k opětovnému snímání obličeje a celý proces porovnání se provede znovu. Nedojde-li k potřebné shodě, systém uživateli po třetím pokusu nepovolí přístup a na místo například přivolá fyzickou ostrahu pro vyřešení situace. Míra shody snímku z databáze a porovnávaného snímku se

bude zřejmě pokaždé trochu lišit a nebude stoprocentní. Lze proto míru shody nastavit na určitý počet procent, například na 70% a výrazně tím eliminovat chybné odmítnutí žadatele FRR (viz kapitola 2), protože se jedná o identifikaci, kdy se uživatel nejprve prokazuje identifikačním kódem a systém umožňuje předběžně vyhledání dané osoby v databázi.

9.2.3 Význam identifikačního kódu uživatele

Pokud by nebylo vyžadováno zadání identifikačního kódu uživatele, systém by musel uživatele verifikovat, a to tak, že by nově pořízený snímek porovnal se všemi snímky ve své databázi a na základě shody rozhodl o identitě. Oproti této variantě se navrhovaný systém jeví jako přesnější, spolehlivější a hlavně rychlejší, protože v jeden okamžik probíhá pořizování snímku i vyhledání uloženého snímku v databázi.

10 HARDWAROVÉ ŘEŠENÍ SYSTÉMU

Cílem navrhovaného hardwarového řešení bylo snížit výrobní a pořizovací ceny přístupového biometrického systému. Zvolené komponenty byly voleny s ohledem na plnění účelu, kompatibilitu a finanční nákladnost.

10.1 Procesorové vybavení řídicího systému

Procesor pro řízení celého terminálu je realizován osmibitovým mikrokontrolérem AVR ATmega128-16 AU od firmy Atmel. Jeho úkolem je ovládat kameru pro pořízení snímku a následně snímek poslat na server pomocí ethernetového řadiče. Lze do něj uložit program o velikosti 128kB. Instrukční sada procesoru nabízí 120 instrukcí.

- Taktovací kmitočet: 0 - 16 MHz
- RAM: 4 kB
- Napájecí napětí: 4.5 - 5.5 V
- Proudový odběr: 1,1 mA
- Pouzdro: TQFP 64
- Cena: **od 178 Kč bez DPH**

Obr. 17 ATmega128-16AU[13]

10.2 Ethernetový řadič

Na základě adekvátní komunikace terminálu se serverem bylo vybráno rozhraní Ethernet. V důsledku správné komunikace systému je nutno použít ethernetový řadič, který takové spojení zajistí. Pro kompatibilitu s vybraným procesorem se jako vhodný jeví řadič Nano SocketLAN. Komuniace mezi procesorem a řadičem může probíhat přes rozhraní UART nebo SPI, kterým obě zařízení disponují. Řadič umožňuje komunikaci na Ethernetu typu 10/100BaseT. Propojení serveru s přístupovými terminály je realizováno UTP kabelem s konektorem RJ-45.

- Napájecí napětí: 3,3 V
- Proudový odběr: 150 mA
- Cena: **785 Kč bez DPH**

Obr. 18 Řadič pro ethernet [14]

10.3 Kamera

Navrženou kamerou je model JK301. Malá barevná kamera s rozlišením 380 TV řádků, kódováním PAL a senzorem CMOS 1,3“. Počet pixelů 682x528. Výstupní rozhraní je CINCH.

- Napájecí napětí: 9 V
- Proudový odběr: 30 mA
- Cena: **699 Kč bez DPH**

10.4 Displej

Pro zobrazování výstupu z kamery je užitý barevný displej typu LCD-25 o rozměru 2,5“ a rozlišení 320x240 pixelů. Součástí modulu je deska plošných spojů s elektronikou pro zpracování obrazu. Obě části jsou propojeny Flex kabelem. Vstupním rozhraním je CINCH.

- Napájecí napětí: 12 V
- Cena: **789 Kč bez DPH**

10.5 Klávesnice

Pro zadávání identifikačního kódu uživatele je zvolena 16-ti tlačítková membránová klávesnice. Obsahuje číslice 0-9 a 6 funkčních kláves, kterým lze podle potřeby naprogramovat různé funkce, například mazání při chybném zadání kódu.

- Cena: **133 Kč bez DPH**

Obr. 19 Membránová klávesnice [15]

10.6 Server

Server v navrhovaném systému tvoří nedílnou součást přístupového systému, jelikož uchovává celkovou databázi informací pro správné vyhodnocení přístupu a vytváří

podmínky pro správnou funkčnost přístupových terminálů. Proto je důležité, aby byl v provozu 24 hodin denně a měl více než jeden pevný disk. Více pevných disků umožňuje vytvořit RAID pro vyšší ochranu dat na něm uložených. Požadavky na výkonnost serveru se můžou lišit podle konkrétní aplikace systému, záleží, jestli bude server využit i k jiným účelům, než jen ke komunikaci s terminály. Server Dell T110 je svým výkonem plně dostatečný pro navrhovaný systém. Řadič disků PERC S100 umožňuje RAID 5, který je odolný vůči poruše jednoho disku.

- Procesor: Intel® Xeon X3450 Processor (2,66 GHz)
- RAM: 2x 2 GB
- Pevné disky: 4x 500 GB
- Cena: **34 500 Kč bez DPH**

10.7 Dodatečné informace

Ve výsledku musí celý přístupový systém vyhovovat normě ČSN EN 50133 a všem jejím požadavkům. V případě, že by aplikace zařízení vyžadovala nepřetržitý provoz systému (norma jej nevyžaduje), je vhodné doplnit terminály o záložní zdroje energie. Stejně tak by se musel zajistit chod serveru instalací UPS zdroje nebo dieselového agregátu.

ZÁVĚR

Prvním bodem bakalářské práce bylo vypracovat literární rešerši zaměřenou na biometrické systémy. V této části jsem objasnil pojem biometrie, její základní pojmy, historii a popsal v praxi nejpoužívanější biometrické metody. Stručně je zde popsána i problematika spolehlivosti biometrických systémů a to chybné přijetí uživatele FAR a chybné odmítnutí uživatele FRR, které mají velký význam při výběru biometrického systému. Zatímco FAR znamená vážnou bezpečnostní hrozbu pro střežený objekt, FRR vážný problém není, ale je nepříjemný z pohledu uživatele.

Následně jsou v bakalářské práci porovnány tři přístupové systémy založené na biometrii obličeje, které jsou v současné době k dostání na českém trhu. Všechny tyto systémy nabízí autentizaci uživatele podle jeho obličeje. Ostatními parametry se ale liší. Některé umožňují dokonce kombinovat dvě přístupové metody právě pro snížení míry FAR. Vlastnosti těchto zařízení, včetně pořizovacích cen, jsou shrnuty v tabulce (Tab. 1). Právě vysoká cena může odrazovat od aplikace těchto systémů.

Jedním z cílů praktické části práce proto bylo navrhnout možnosti inovace systému, respektive vypracovat inovativní systém s ohledem na snížení pořizovacích a udržovacích nákladů. Základem bylo porovnat použitelnost algoritmů pro detekci, lokalizaci a rozpoznání obličeje na snímku. Inovace systému spočívá v aplikaci dvou vybraných algoritmů v návaznosti na uživatelův identifikační kód, čímž je umožněna identifikace, nikoliv verifikace. To přispívá ke zvýšení spolehlivosti systému. Důležitým kritériem rozpoznávání obličejů tímto systémem je stálost osvětlení a barva pozadí na snímku, která musí být co nejvíce odlišná od barvy pleti. Barva pozadí se následně ze snímku odfiltruje a vznikne pouze obraz hlavy a obličeje, na který se aplikují zmíněné dva algoritmy. Vše je znázorněno ve vývojovém diagramu v kapitole 9.

Nutnost snížení pořizovací ceny systému, vedlo k použití levnějších hardwarových prvků, které však plní potřebný účel. Hlavním rozdílem oproti třem porovnávaným systémům je v použití systému využívajícím databázi na centrálním serveru, s ohledem k použité funkci není na systém kladena vysoká náročnost na hardware ke zpracování a ukládání dat. Tím odpadá potřeba paměti o velké kapacitě a výkonného procesoru. Velký dotykový displej je nahrazen menším LCD panelem doplněným o klávesnici. Zvolená varianta účelně plní funkci přístupového systému a snižuje pořizovací a udržovací náklady.

Bezpečnostní systémy na principu rozpoznávání obličejů jsou poměrně nová záležitost a jejich uplatnění se teprve začíná nacházet. V příštích letech se dá předpokládat vývoj a zdokonalování těchto systémů, které povede k širšímu uplatnění. Jednou z užitečných aplikací by mohly být bankomaty, kde by po zadání PINu sloužili k potvrzení identity uživatele.

ZÁVĚR V ANGLIČTINĚ

The first point of the thesis was to base on exploration of facts focused on biometric systems. The first section was explained the concept of biometrics, technical biometric terms, history and the practical biometric methods. Briefly are described issues of the reliability of biometric systems, false acceptance by the FAR and false rejection by the FRR which have a great importance in choosing a biometric system. While the FAR means a serious threat to the security guarding, FRR isn't a serious problem but it is annoying for a users.

Then the thesis compares three access systems based on facial biometrics that are currently available on the Czech trade. All these systems offer authentication by the face. Other parameters of these systems are different. Some systems even allow two access methods specifically for reducing the FAR. The characteristics of these devices, including acquisition prices, are summarized in the table (Table 1). A high price may discourage the application of these systems.

One of the targets of practical part therefore was to propose the possibility of innovation system, or develop an innovative system with a view to reducing price and maintenance price. The basis was to compare the applicability of algorithms for detection, localization and recognition of faces in an image. Innovation system is in the application of the two selected algorithms in response to a user identification code thereby it making identification possible, but not verification. It contributes to increase system reliability. Next important criterion for face recognition was stable lighting and background color of the image, which must be much different from the color of skin. The background color from image is filtered and after that is created only the one image of the head and the face; the previous two algorithms are applied on it. Everything is shown in the flowchart in Chapter 9.

In order to reduce the price of the system it is necessary to use cheaper hardware which can perform the required purpose. The main difference compared with the three compared systems is that the proposed system uses a database on a central server so it doesn't need to powerful hardware for data processing and storage. This eliminates the main demand for large capacity of memory and powerful processor. Large touch screen is replaced by a

smaller LCD panel accompanied by keyboard. This option also performs the purpose and is cheaper.

Security systems based on face recognition is a relatively new issue and their using is just starting to appear. In coming years we can expect development and improvement of these systems leading to widespread application. One of useful applications may be ATM, where can be used to confirm user identity after insert a PIN.

SEZNAM POUŽITÉ LITERATURY

[1] *Logica.cz* [online]. 2010 [cit. 2011-03-23]. Biometrie. Dostupné z WWW: <http://www.logica.cz/we-do/security/biometrie/>.

[2] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. [s.l.] : [s.n.], 2008 [cit. 2011-03-23]. Dostupné z WWW: <http://www.fbi.vsb.cz/miranda2/export/sites-oot/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf>.

[3] Historie biometrik a jejich využití ve výpočetní technice *[online]. 2003 [cit. 2011-03-22]. Historie biometrik a jejich využití ve výpočetní technice. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm>.*

[4] *Autentizační metody založené na biometrických informacích* [online]. 18.11.2010 [cit. 2011-03-22]. Autentizační metody založené na biometrických informacích. Dostupné z WWW: <http://access.feld.cvut.cz/view.php?nazevclanku=autentizacni-metody-zalozene-na-biometrickych-informacich&cisloclanku=2010110002>.

[5] *Biometrika* [online]. 2010 [cit. 2011-03-22]. Biometrika. Dostupné z WWW: <http://www.nula.wz.cz/biometrika/>.

[6] ČÁSTEK, Petr. *Face recognition* [online]. [s.l.], 2008. 4 s. Oborová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z WWW: <http://www.feec.vutbr.cz/EEICT/2008/sbornik/02-Magisterske%20projekty/08-Grafika%20a%20multimedia/02-xcaste01.pdf>.

[7] Biometrické metody v bezpečnostní praxi (2). *3POL* [online]. 2006, č. 5, [cit. 2011-03-22]. Dostupný z WWW: <http://3pol.cz/501-biometricke-metody-v-bezpecnostni-praxi-%282%29>.

[8] MORÁVEK, Petr. *Identifikace obličeje osoby snímané kamerou* [online]. [s.l.], 2010. 80 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[9] *Science.howstuffworks.com* [online]. 2008 [cit. 2011-05-16]. How Fingerprinting Works . Dostupné z WWW: <http://science.howstuffworks.com/fingerprinting1.htm>.

[10] *Visitelecom.itrademarket.com* [online]. 2011 [cit. 2011-05-16]. FINGERPRINT - SUPREMA D-STATION, X-STATION. Dostupné z WWW: <http://visitelecom.itrademarket.com/2529824/fingerprint-suprema-d-station-x-station.htm>.

[11] *Comfis.cz* [online]. 2010 [cit. 2011-05-16]. IFace 303. Dostupné z WWW: <http://www.comfis.cz/produkty/pristupove-a-dochazkove-terminaly-a-jejich-prislusenstvi/multimedialni-pristupove-a-dochazkove-terminaly/iface-303>.

[12] *Shop.efg.cz* [online]. 2010 [cit. 2011-05-16]. AFT-500. Dostupné z WWW: <http://shop.efg.cz/z19476-aft-500>.

[13] *Digikey.com* [online]. 2011 [cit. 2011-05-16]. Avr atmega32. Dostupné z WWW: <http://search.digikey.com/scripts/DkSearch/dksus.dll?vendor=0&keywords=avr+atmega32>.

[14] *Pandatron.sk* [online]. 2010 [cit. 2011-05-16]. Nano SocketLAN. Dostupné z WWW: <http://www.pandatron.sk/?shop&sla=2&pn=90016&tx=nano_socketlan>.

[15] *Vpcentrum.prodejce.cz* [online]. 12.8.2010 [cit. 2011-05-16]. VP centrum elektronika. Dostupné z WWW: <http://www.vpcentrum.prodejce.cz/p-7368/k-1174/univerzalni-membranova-klavesnice-16-tlacitek/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCD Charge-Coupled Device.

DNA Deoxyribonukleová kyselina.

EBGM Elastic Bunch Graph Matching- Elastický srovnávací diagram.

FAR False Acceptance rate- Chybné přijetí žadatele.

FBG Face Bunch Graph.

FRR False Rejection Rate- Chybné odmítnutí žadatele.

GPRS General Packet Radio Service.

LCD Liquid Crystal Display.

LDA Linear Discriminant Analysis - Lineární diskriminační analýza.

LED Light-Emitting Diode.

MBFT Multi Biometric Fusion Technology.

PAL Phase Alternating Line.

PCA Principal Components Analysis- Analýza hlavních částí.

PIN Personal Identification Number

RFID Radio Frequency Identification.

SPI Serial Peripheral Interface

SVD Singular Value Decomposition- dekompozice jedinečných hodnot.

TFT Thin-Film Transistor.

TQFP Thin Quad Flat Pack.

UART Universal asynchronous receiver/ transmitter.

UPS Uninterruptible Power Supply.

UTP Unshielded twisted pair.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK