



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

DEPARTMENT OF BIOMEDICAL ENGINEERING

ROZPOZNÁVÁNÍ OBLIČEJE

FACE RECOGNITION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Richard Maňkoš

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Radim Kolář, Ph.D.

BRNO 2016

Diplomová práce

magisterský navazující studijní obor Biomedicínské a ekologické inženýrství
Ústav biomedicínského inženýrství

Student: Bc. Richard Maňkoš

ID: 147814

Ročník: 2

Akademický rok: 2015/16

NÁZEV TÉMATU:

Rozpoznávání obličejů

POKYNY PRO VYPRACOVÁNÍ:

1) Prostudujte a stručně charakterizujte publikované metody pro rozpoznávání obličejů. Dále se seznámte s principem metod pro detekci obličejů v obraze a zvolenou metodu ověřte pomocí existující implementace. 2) Zvolte vhodnou metodu či metody pro rozpoznávání a podrobněji je popište. 3) Navrhněte způsob pro komplexní snímání videosekvencí vhodných pro rozpoznávání obličejů. Při návrhu uvažte různé faktory (např. směr pohledu, vzdálenost, změnu vzhledu, emoce). 4) Realizujte měření videosekvencí dle předchozího bodu alespoň pro 20 osob. 5) Implementujte vybranou metodu pro rozpoznávání obličejů. 6) Metodu otestujte a získané výsledky dostatečně diskutujte. 7) Navrhněte a otestujte rozšíření metody pro videosekvence.

DOPORUČENÁ LITERATURA:

- [1] NIXON, M. a A. AGUADO. Feature Extraction and Image Processing, Elsevier, 2005.
- [2] DRAHANSKÝ, M., F. ORSÁG, a M. DOLEŽEL. Biometrie, Brno Computer Press, 2011.

Termín zadání: 8.2.2016

Termín odevzdání: 20.5.2016

Vedoucí práce: doc. Ing. Radim Kolář, Ph.D.

Konzultant diplomové práce:

prof. Ing. Ivo Provazník, Ph.D., předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato diplomová práce se zabývá rozpoznáváním obličeje v digitálním obraze. První část se věnuje popisu biometrie a stručně charakterizuje nejčastěji využívané biometrické metody. Ve druhé části je popsán postup pro rozpoznání obličeje v obraze. Podrobněji je popsána metoda detekce Viola-Jones a metoda rozpoznávání PCA, která bude implementována v Matlabu. Poslední, praktická část je věnovaná popisu návrhu snímání videosekvencí, implementací metody PCA do Matlabu a diskuzi dosažených výsledků .

KLÍČOVÁ SLOVA

Biometrie, detekce obličeje, Viola-Jones, rozpoznávání obličeje, PCA, videosekvence

ABSTRACT

This diploma thesis deals with face recognition in digital pictures. The first part describes biometry and, shortly, characterizes biometrical methods which are the most oftenly used. In the second part is described the approach of face recognition in a picture. Specifically, it is described the method for face detection - Viola-Jones and method for face recognition - PCA, which will be implemented in Matlab. The last part, which is practical, describes the scheme for video-sequence recording, implementation of the PCA method in Matlab and discussion of the achieved results.

KEYWORDS

Biometry, face detection, Viola-Jones, face recognition, PCA, video-sequence

MAŇKOŠ, R. *Rozpoznávání obličeje*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2016. 49 s., Diplomová práce. Vedoucí práce: doc. Ing. Radim Kolář, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Rozpoznávání obličeje jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne

.....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu semestrální práce doc. Ing. Radimu Kolářovi, Ph.D za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé semestrální práce.

V Brně dne

.....

(podpis autora)

OBSAH

Zoznam obrázkov	viii
Zoznam tabuliek	x
Úvod	1
1 Biometria	2
1.1 Pojmy identifikácia, verifikácia, biometrický systém a charakteristika biometrických vlastností	3
1.2 Meranie výkonnosti biometrických metód	4
1.3 Stručný prehľad základných biometrických identifikačných metód používaných v bežnej praxi	8
2 Detekcia a Rozpoznanie tváre	12
2.1 Detekcia tváre v snímku	12
2.1.1 Viola-Jones detektor	13
2.1.2 KLT algoritmus na sledovanie tváre.....	18
2.2 Normalizácia tváre	19
2.3 Metódy rozpoznania tváre pomocou podobnosti obrazových dát	19
2.3.1 PCA (Principal Component Analysis) - Eigenfaces	20
2.3.2 LDA (Linear Discriminant Analysis)	25
2.3.3 LBP (Local Binary Pattern)	26
2.3.4 ICA (Independent Component Analysis)	27
2.4 Metódy rozpoznania tváre na základe topologických vlastností tváre ...	27
2.4.1 ASM a AAM metóda.....	28
3 Praktická časť	30
3.1 Detekcia tváre	30
3.2 Návrh snímania videosekvencií	31
3.3 Vytvorenie databáze tvárí	32
3.4 Vytvorenie databázy videí	33
3.5 Implementácia metódy rozpoznávania tváre do programovacieho prostredia Matlab	35
4 Testovanie programu	40

5	Diskusia	44
6	Záver	49
	Literatúra	50
	Zoznam skratiek	53
	Príloha	54

ZOZNAM OBRÁZKOV

Obr. 1.1 Biometrický systém. [1]	3
Obr. 1.2 Chyby FMR vs. FNRM a FAR vs. FRR. [1]	6
Obr. 1.3 Závilosti EER, ZeroFMR a ZeroFNMR. [1]	7
Obr. 1.4 Príklad ROC krivky. [1]	8
Obr. 1.5 Papilárne línie. A - papilárne línie tvoria jednoduché oblúky; B - papilárne línie tvoria slučku, ktorá vedie vľavo; C - papilárne línie tvoria kruhové, oválne, špirálne, dvojslučkové obrazce; D - papilárne línie tvoria slučku vedúcu vpravo. Prevzaté z [4]	8
Obr. 1.6 Lokalizovanie dúhovky a jej piktografický popis. Prevzaté z [3]	9
Obr. 1.7 Počítačové spracovanie biometrických dát tváre. [3]	10
Obr. 1.8 Ruka snímaná CCD kamerou a príklad merania vzdialeností.[3]	11
Obr. 1.9 Biometrické charakteristiky podpisu. [5]	11
Obr. 2.1 a) slabé klasifikátory; b) silný klasifikátor. [8].....	14
Obr. 2.2 Príklad výpočtu sumy ľubovoľného obdĺžnika pomocou integrálneho obrazu. (w – šírka požadovaného trojuholníka; h – výška požadovaného trojuholníka) [9]	16
Obr. 2.3 Základné typy Haarových príznakov. [8]	17
Obr. 2.4 Blokovaný diagram – KLT algoritmus	18
Obr. 2.5 Detegovaná tvár s vyznačenými príznakmi. [17]	19
Obr. 2.6 Prevedenie obrazu z 2D priestoru do 1D priestoru.....	21
Obr. 2.7 Trénovacia sada obrázkov tvári. [15]	22
Obr. 2.8 Priemerná tvár. [15].....	22
Obr. 2.9 Prvých 9 eigenfaces. [15]	24
Obr. 2.10 Základný LBP operátor. [19].....	26
Obr. 2.11 Klasifikácia založená na LBP histogramoch. [20]	27
Obr. 2.12 Geometrické vlastnosti tváre (biela farba) používané pri experimentoch rozpoznania. [11]	28
Obr. 2.13 Metóda AAM – iteratívne mapovanie modelu na testovací obrázok. [1]	29
Obr. 3.1 Správne detegovaná tvár.....	30
Obr. 3.2 Chybná detekcia	30
Obr. 3.3 Zlyhanie detekcie.....	31
Obr. 3.4 Príklad obrázkov v databáze.....	33

Obr. 3.5 Snímka videa zo scény1	34
Obr. 3.6 Snímka videa zo scény2	34
Obr. 3.7 Vývojový diagram programu.....	35
Obr. 3.8 Grafické užívateľské prostredie vytvoreného programu	36
Obr. 3.9 GUI po nahratí dát	37
Obr. 3.10 Rozpoznaná osoba	38
Obr. 3.11 Graf početnosti zhody fotiek z databázy s osobou na videu.....	39
Obr. 5.1 Tieň na tvári pri použití bodového zdroja svetla nad osobou.....	45
Obr. 5.2 Detegované vypínače svetiel	45
Obr. 5.3 Vľavo obrázok získaný orezaním videa pri statickej polohe osoby, vpravo obrázok získaný priamo z videa.....	46

ZOZNAM TABULIEK

Tabuľka 4.1 : Výsledky rozpoznávacieho procesu scény1	40
Tabuľka 4.2 : Úspešnosť správneho rozpoznania u scény1.....	41
Tabuľka 4.3 Výsledky rozpoznávacieho procesu scény1	42
Tabuľka 4.4 Úspešnosť správneho rozpoznania u scény2.....	42

ÚVOD

V súčasnej dobe sa na identifikáciu a verifikáciu osôb čoraz častejšie používajú biometrické metódy. Ich výhodou je, že biometrické vlastnosti typické pre každú osobu sa nedajú stratiť a sú neustále dostupné. Jednou z biometrických metód je aj rozpoznávanie tváre, ktorej sa bude táto diplomová práca venovať.

Rozpoznanie tváre sa hojne využíva hlavne v kriminalistike, napríklad pri hľadaní kriminálnikov, podozrivých teroristov alebo stratených detí. V súčasnosti sa k riešeniu využívajú mnohé metódy, avšak všetky majú okrem výhod aj svoje limitácie. Niektoré z nich budú popísané v tejto diplomovej práci. Spoločnou vlastnosťou všetkých metód je postup, akým k rozpoznaní tváre dochádza. Prvým krokom je detekcia polohy tváre v snímku, za ňou nasleduje extrakcia príznakov, a posledným krokom je klasifikácia alebo vyhodnotenie podobnosti hľadanej tváre.[18]

Nasledujúci text diplomovej práce je členený do piatich základných častí. Kapitola 1 popisuje základné informácie o biometrii. Druhá kapitola sa zaoberá procesom rozpoznávania tváre, kde je charakterizovaná jedna metóda detekcie a niekoľko základných metód rozpoznania tváre. Tretia kapitola je zameraná na praktickú časť diplomovej práce. Je v nej popísaný postup vytvorenia foto-databáz, video-databáz a implementácia metódy rozpoznania tváre v programovacom prostredí Matlab. Štvrtá kapitola je venovaná dosiahnutým výsledkom práce. Posledná, piata kapitola, obsahuje diskusiu k výsledkom a predkladá možnosti zdokonalenia programu.

1 BIOMETRIA

Slovo biometria je gréckeho pôvodu a skladá sa zo slov „bios“ a „metron“. Prvé zo slov znamená život a druhé znamená meradlo. V doslovnom preklade ide teda o akési „meranie života“. V IT oblasti je biometria charakterizovaná ako automatické rozpoznávanie ľudských jedincov na základe ich charakteristických anatomických rysov a behaviorálnych rysov.

Anatomické (statické) vlastnosti :

- Odtlačok prstu
- Tvár
- Dúhovka oka
- Sietnica oka
- Geometria ruky
- DNA
- Dentálny obraz
- Termogram ruky

Behaviorálne (dynamické) vlastnosti :

- Hlas / reč
- Mimika tváre a pohyb pier
- Podpis (dynamická) forma
- Chôdza
- Dynamika stláčania kláves

U anatomických fyzických vlastností je jeden pevný rys jednou konkrétnou biometrickou vlastnosťou, kde zároveň táto biometrická vlastnosť nie je ľahko ovplyvniteľná človekom a je vždy prítomná.

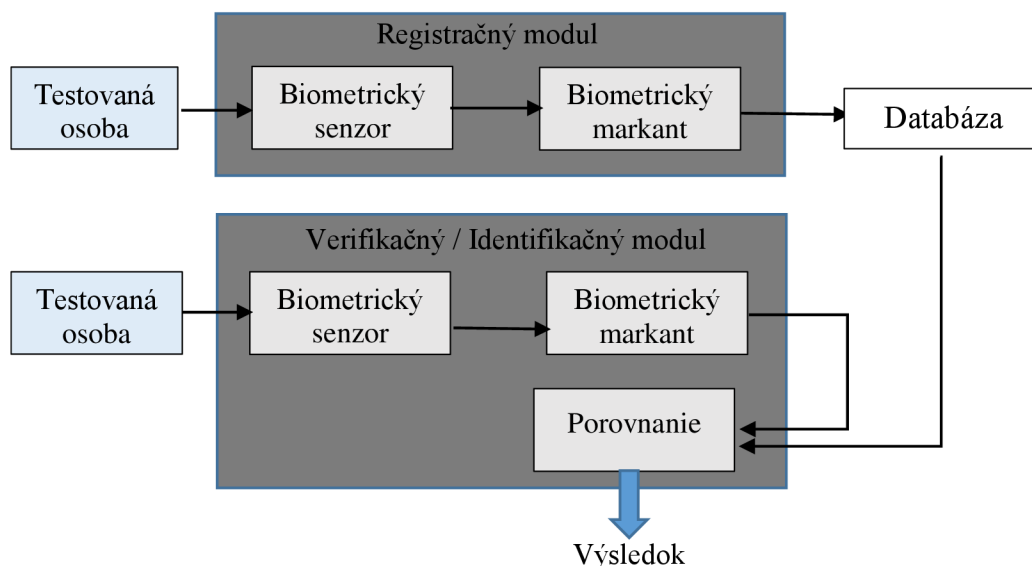
Dynamické vlastnosti sú spojené s určitou akciou užívateľa a biometrická vlastnosť je v tomto prípade pomerne ľahko ovplyvniteľná – každé nasnímanie danej biometrickej vlastnosti môže viesť k odlišnej sade biometrických vzoriek.[1]

1.1 Pojmy identifikácia, verifikácia, biometrický systém a charakteristika biometrických vlastností

Identifikácia je proces, pri ktorom sa porovnáva jedna nasnímaná biometrická vzorka so všetkými referenčnými šablónami, ktoré boli uložené v databáze. Ide o porovnanie jednej k mnoho, 1:N. Výsledkom tohto procesu je rozpoznanie totožnosti majiteľa nasnímaného vzorku.

Verifikácia je proces, pri ktorom sa porovnáva jedna nasnímaná šablóna s jednou šablónou uloženou v databáze, ktorá patrí preverovanej osobe. Ide o porovnanie jedna k jednej, 1:1. Výsledkom tohto procesu má byť zistenie, či snímaná osoba je skutočne tá, za ktorú sa vydáva. Verifikačný proces je omnoho rýchlejší a z pohľadu výkonnosti biometrickej aplikácie aj omnoho jednoduchší ako proces identifikácie. [2]

Biometrický systém sa skladá z dvoch modulov, a to z registračného modulu a verifikačného/identifikačného modulu. Zjednodušený model systému je zobrazený na obrázku Obr. 1.1. V súvislosti s biometrickými vlastnosťami sa biometrické systémy môžu rozdeliť na unimodálne a multimodálne. Unimodálne systémy používajú len jednu biometrickú vlastnosť. Ich cena je nižšia, no majú nižšiu spoľahlivosť. Multimodálne systémy využívajú buď viac príznakov jednej biometrickej vlastnosti (napr. statické a dynamické vlastnosti podpisu), alebo viac biometrických vlastností. Ich cena je vyššia, avšak sú spoľahlivejšie a robustnejšie k falšovaniu.



Obr. 1.1 Biometrický systém. [1]

Biometrický senzor slúži k získaniu biometrického vzorku a k jeho následnému prevedeniu do digitálnej podoby. Pojmom „biometrický markant“ sa označujú extrahované rysy z biometrického vzorku na vstupe. Biometrické rysy, ktoré získame v registračnom module sú následne uložené v databáze, naopak biometrické rysy získané vo verifikačnom/identifikačnom module sa neukladajú, ale porovnávajú sa s rysmi uloženými v databáze. Po porovnaní sa získa výsledok, ktorého hodnota závisí na nájdení alebo nenájdení zhody, poprípade na operačnom móde (verifikácia alebo identifikácia). [1]

Pri rozhodovaní o nasadení konkrétneho biometrického systému je dôležitým kritériom *charakteristika biometrických vlastností*. Medzi základné charakteristiky radíme tieto [1]:

- Univerzálnosť – každá jedna osoba by mala mať túto vlastnosť
- Jedinečnosť – biometrická vlastnosť nesmie byť rovnaká pre žiadne dve osoby
- Konštantnosť – vlastnosť zostáva nemenná v čase
- Získateľnosť – biometrická vlastnosť je kvantitatívne merateľná
- Výkonnosť – biometrická vlastnosť sa nesmie zmeniť ani zostarnúť
- Akceptácia – ochota ľudí nechať si nasnímať biometrickú vlastnosť
- Odolnosť proti falšovaniu – jednoduchosť vytvorenia falzifikátu danej biometrickej vlastnosti
- Finančné náklady na zaobstaranie systému

1.2 Meranie výkonnosti biometrických metód

V procese identifikácie alebo verifikácie môže biometrický systém dospieť k chybnému záveru, a preto je nutné každý systém dôkladne otestovať. Následne je možné vysloviť relevantný záver o kvalite a funkčnosti daného systému a porovnať ho s inými typmi biometrických systémov.

Medzi parametre, ktoré hodnotia výkonnosť jednotlivých systémov patrí :

- Miera chybného prijatia
- Miera chybného odmietnutia
- Miera chybnnej zhody
- Miera chybnnej nezhody
- Miera vyrovnanania chýb
- Miera neschopnosti nasnímať

- Miera neschopnosti zaregistrovať
- Miera neschopnosti porovnať

Miera chybného prijatia – FAR (False Acceptance Rate) udáva pravdepodobnosť chybného prijatia neoprávnenej osoby systémom, ktorý tým umožní vstup potenciálnemu útočníkovi. V literatúre sa zvykne označovať aj ako chyba 2. typu a je definovaná ako

$$FAR = \frac{N_{FA}}{N_{IIA}} \text{ alebo } FRR = \frac{N_{FA}}{N_{IVA}}, \quad (1.1)$$

kde N_{FA} znamená počet chybných prijatí, N_{IIA} počet pokusov neoprávnených osôb o identifikáciu, N_{IVA} počet pokusov neoprávnených osôb o verifikáciu. [2]

Miera chybného odmietnutia – FRR (False Rejection Rate) udáva pravdepodobnosť, s ktorou systém nerozpozná oprávneného užívateľa alebo osobu, ktorá má v aplikácii uloženú svoju biometrickú šablónu. Označuje sa aj ako chyba 1. typu a je definovaná ako

$$FRR = \frac{N_{FR}}{N_{EIA}} \text{ alebo } FRR = \frac{N_{FR}}{N_{EVA}}, \quad (1.2)$$

kde N_{FR} znamená počet chybných odmietnutí, N_{EIA} počet pokusov oprávnených osôb o identifikáciu, N_{EVA} počet pokusov oprávnených osôb o verifikáciu. [2]

Miera chybnnej zhody – FMR (False Match Rate) udáva podiel chybne akceptovateľných osôb. Je definovaný ako

$$FMR(T) = \int_T^1 p(s|H_1) ds, \quad (1.3)$$

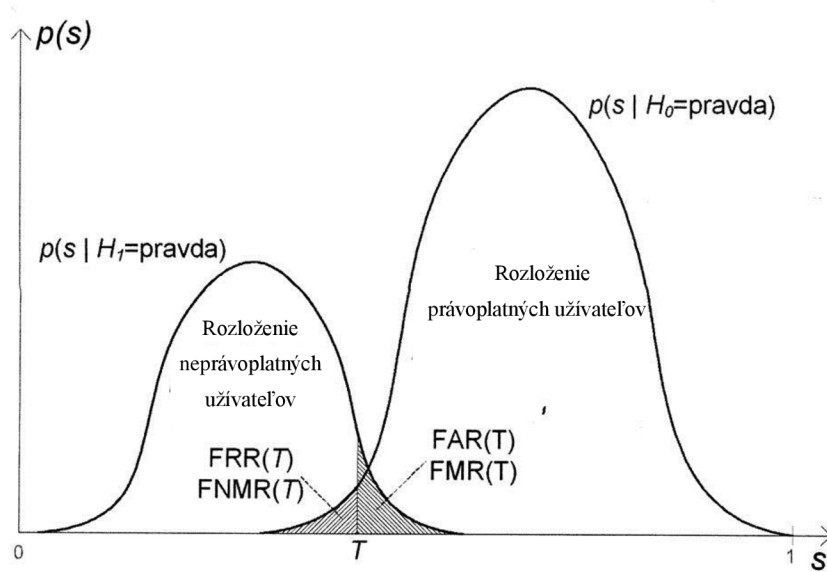
kde T je rozhodovací prah, H_1 je výrok, ktorý znamená, že vzor a šablóna pochádzajú od rôznych osôb, p je pravdepodobnostná hustota, ktorá udáva, že výrok v zátvorke je pravdivý a s je skóre porovnania. [1]

Miera chybnnej nezhody – FNMR (False Non-Match Rate) udáva podiel chybne neakceptovaných osôb a je definovaný ako

$$FNMR(T) = \int_0^T p(s|H_0) ds, \quad (1.4)$$

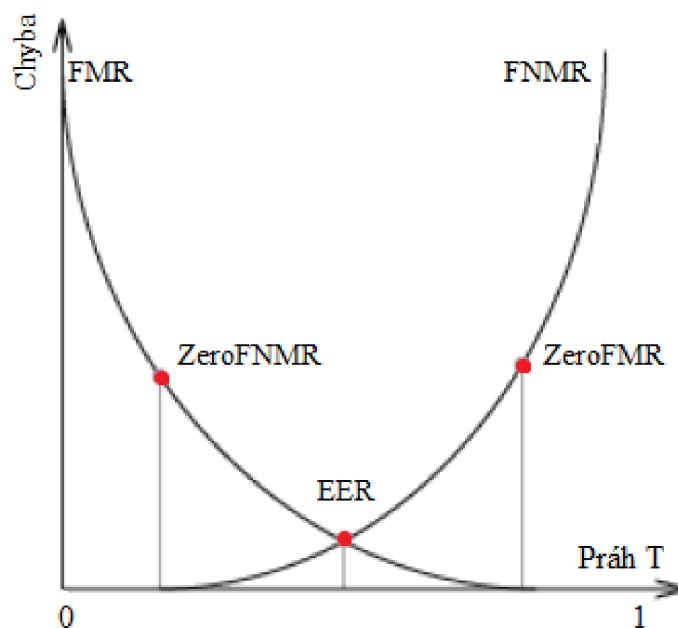
kde T je rozhodovací prah, H_0 je výrok, ktorý znamená, že vzor a šablóna pochádzajú od rovnakej osoby, p je pravdepodobnostná hustota, ktorá udáva, že výrok v zátvorke je

pravdivý a s je skóre porovnania.



Obr. 1.2 Chyby FMR vs. FNMR a FAR vs. FRR. [1]

Miera vyrovnania chýb – EER (Equal Error Rate) je určená podmienkou $FMR(T) = FNMR(T)$. Keďže sú FMR a FNMR krivky diskkrétne funkcie, nie je EER možné určiť presne. Je však možné nájsť oblasť, v ktorej sa obe chybové miery zhodujú. Pri nastavení prahu T na hodnotu EER bude systémom chybné prijatý a chybné odmietnutý rovnaký počet osôb. Podľa spôsobu použitia systému je následne možné tento prah nastavovať. S pojmom EER sa spája ešte charakteristika ZeroFMR, čo je dolná hranica FNMR ($FMR=0$) a ZeroFNMR, čo je dolná hranica FMR ($FNMR=0$). Závislosti sú zobrazené na Obr. 1.3.



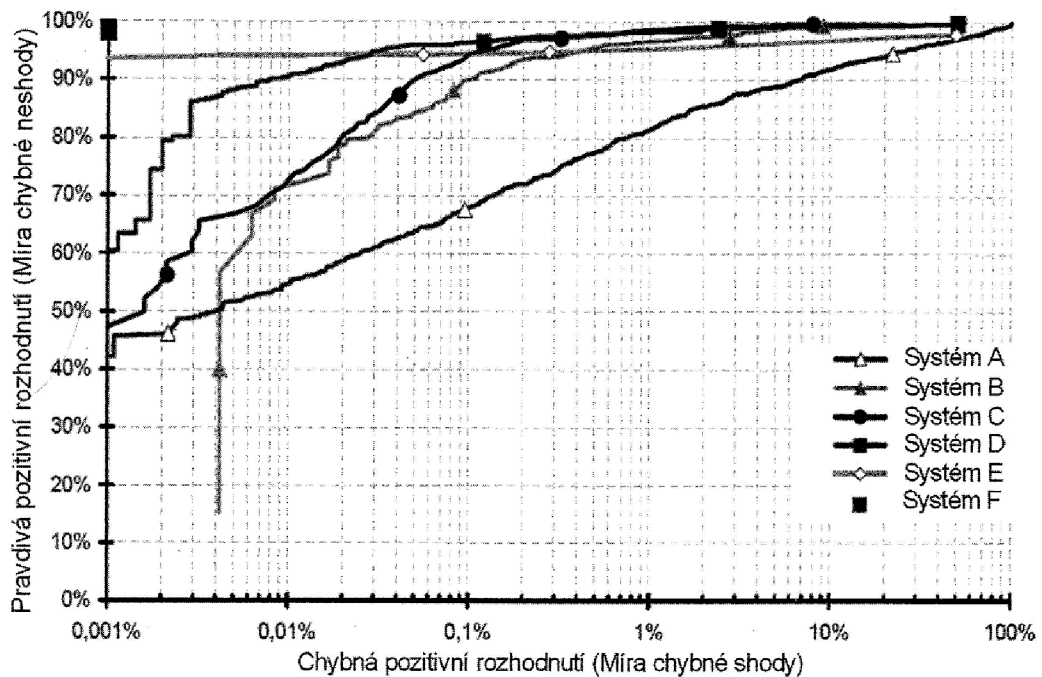
Obr. 1.3 Závislosti EER, ZeroFMR a ZeroFNMR. [1]

Miera neschopnosti nasnímať – FTA (Failure To Acquire) slúži predovšetkým k hodnoteniu kvality senzoru použitého v biometrickom systéme. Udáva podiel chybných záznamov daného senzoru v prípade, že je biometrická charakteristika prítomná. Čím je hodnota FTA vyššia, tým je daný senzor menej vhodný na snímanie danej biometrickej charakteristiky.

Miera neschopnosti zaregistrovať – FTE (Failure to Enroll) udáva percentuálny podiel užívateľov, ktorých biometrické charakteristiky sa nie je systém schopný naučiť. FTE teda hodnotí schopnosť algoritmu pracovať aj s nekvalitnými biometrickými charakteristikami.

Miera neschopnosti porovnať – FTM (Failure To Match) udáva percentuálny podiel biometrických charakteristík získaných zo senzoru, ktoré nemohli byť porovnané alebo spracované. Táto miera udáva neschopnosť systému spraviť rozhodnutie, a teda po porovnaní sa nedosiahne žiaden výsledok.

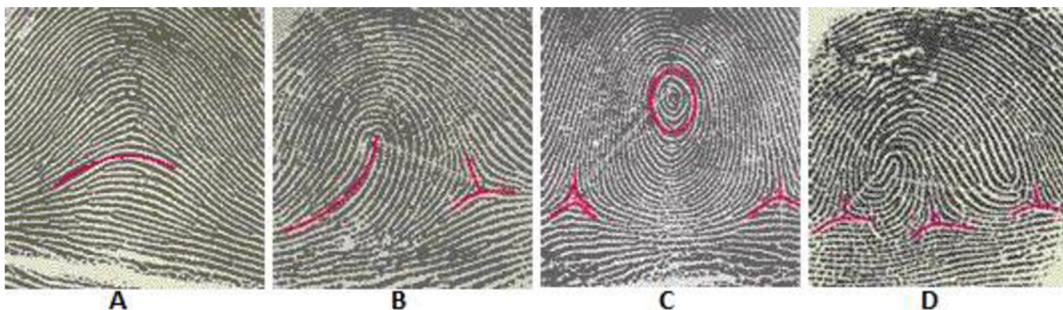
V súčasnej dobe sa ako štandard pri popise výkonnosti daného systému používajú ROC krivky (z angl. Receiver Operating Curve), ktoré predstavujú detekčnú schopnosť funkcie FMR vzhľadom k FNMR, poprípade FAR/FRR. Príklad ROC krivky je zobrazený na Obr. 1.4 .Obr. 1.4 Príklad ROC krivky. [1]



Obr. 1.4 Príklad ROC krivky. [1]

1.3 Stručný prehľad základných biometrických identifikačných metód používaných v bežnej praxi

Odtlačok prsta - považuje sa za symbol biometrickej identifikácie a je uznávaný ako celosvetový štandard policajno-súdnej a bezpečnostne komerčnej identifikácie. Táto metóda je založená na obrazoch papilárnych línií, ktoré sú pre každú osobu unikátne. Poznáme 3 základné typy papilárnych obrazcov – oblúky, slučky a víry. Príklady obrazcov papilárnych línií sú zobrazené na Obr. 1.5.

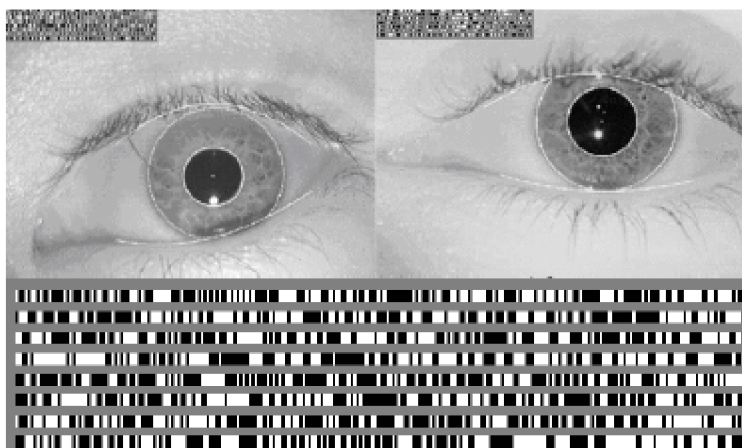


Obr. 1.5 Papilárne línie. A - papilárne línie tvoria jednoduché oblúky; B - papilárne línie tvoria slučku, ktorá vedie vľavo; C - papilárne línie tvoria kruhové, oválne, špirálne, dvojslučkové obrazce; D - papilárne línie tvoria slučku vedúcu vpravo. Prevzaté z [4]

V samotnom procese identifikácie pomocou algoritmu sa však využíva prítomnosť markantov, ktoré sa nachádzajú v jednotlivých papilárnych líniách. Medzi ne patrí napríklad línia, rozvetvená línia, oko, hák alebo výbežok.

Snímanie v súčasnosti neprebieha len pomocou klasického kriminalistického spôsobu pomocou daktyloskopie čierne, ale aj opticko-elektronickými čipmi pre priame snímanie. [2][3]

Očná dúhovka – je farebná časť oka, ktorá sa nachádza okolo zreničky. Jej sfarbenie a štruktúra sú geneticky závislé, no rozloženie jednotlivých farebných štruktúr, ktoré sú podobné snehovej vločke, je náhodné a časovo nemenné. Táto biometrická metóda patrí medzi najpresnejšie, pretože dokáže odlíšiť aj jednovaječné dvojčatá, a dokonca ani jeden človek nemá obe dúhovky rovnaké. Na snímanie sa používa kvalitná digitálna kamera a infračervené osvetlenie oka. Princípom je mapovanie dúhovky počas snímania do fázorových diagramov. Tie obsahujú informácie o pozícii, počte a orientácii špecifických plošiek a slúžia na vytvorenie dúhovkovej mapy (viď Obr. 1.6) .[3]

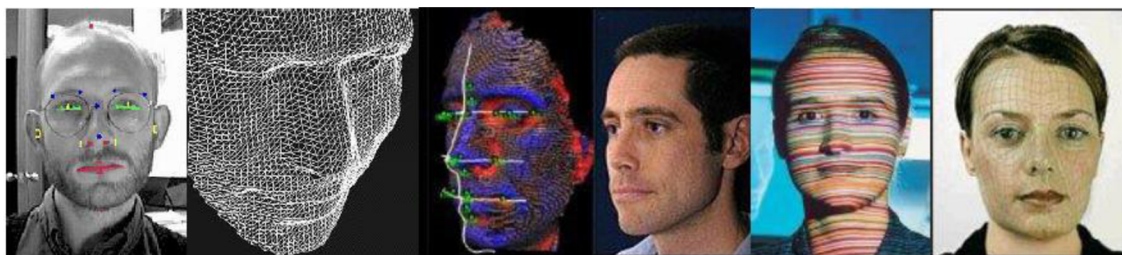


Obr. 1.6 Lokalizovanie dúhovky a jej piktografický popis. Prevzaté z [3]

Očná sietnica – princípom je zmapovanie drobných žiliek a ciev v sietnici, ktoré zostávajú u každého človeka počas celého života takmer nemenné. Pri snímaní sa využíva zdroj svetla s nízkou intenzitou žiarenia a opto-elektrický systém. Vzhľadom k tomu, že sietnica obsahuje dostatočne veľké množstvo špecifických anatomických bodov, má táto metóda vysokú identifikačnú presnosť. Nevýhodou je to, že vyžaduje od užívateľa aby sa díval do presne vymedzeného priestoru, čo môže byť pre niektoré osoby nepríjemné. [2][3]

Tvár – identifikácia alebo verifikácia tváre je v súčasnosti jednou z najviac

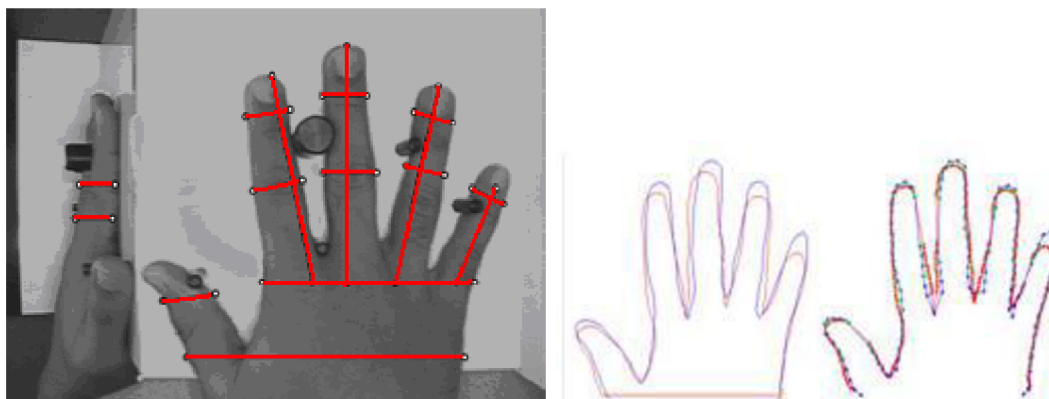
skúmaných metód. Jej využitie má z hľadiska bezpečnosti veľký význam napríklad na letiskách, štadiónoch alebo vlakových staniciach, kde by sa mohli v dave ľudí nájsť osoby, ktoré sú podozrivé z trestnej činnosti. Rozpoznanie tváre je založené na porovnaní nasnímaného obrazu s obrazom, ktorý je uložený v centrálnej databáze, pričom sa využíva poloha opticky významných miest na tvári (nos, ústa, oči,...). Nevýhodou je vplyv viacerých faktorov na účinnosť detekcie tváre a následnú verifikáciu alebo identifikáciu. Najvýznamnejším faktorom je vplyv osvetlenia a uhol, z ktorého je osoba nasnímaná. Príklad počítačového spracovania je na Obr. 1.7.



Obr. 1.7 Počítačové spracovanie biometrických dát tváre. [3]

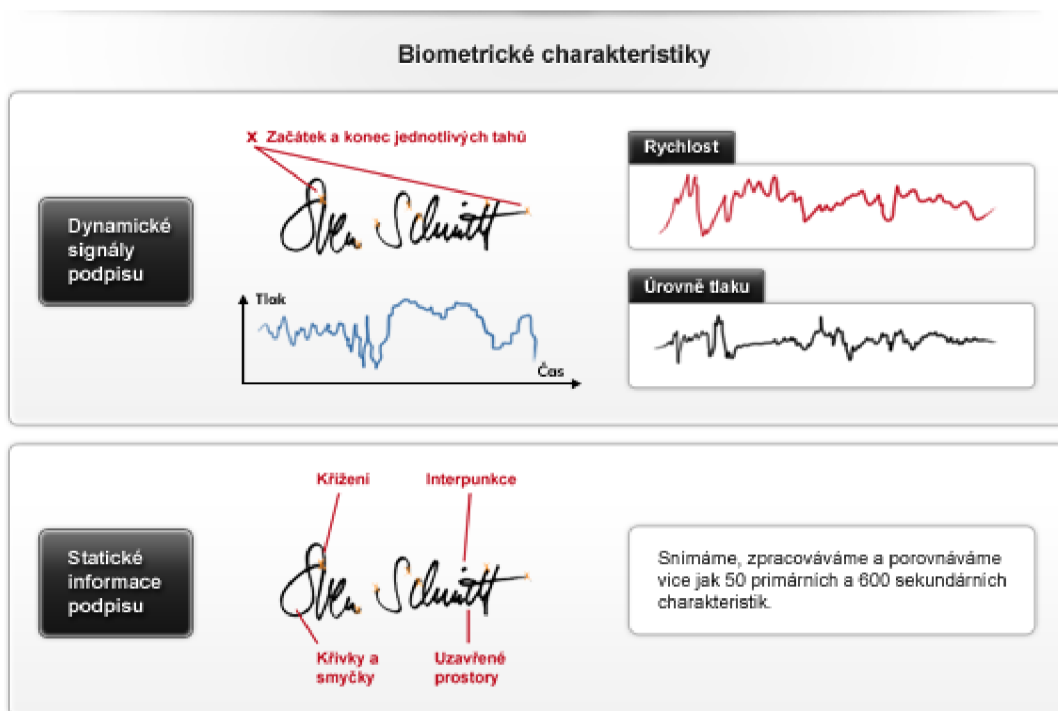
DNA – obsahuje obrovské množstvo informácií o každej osobe a už malá časť z nich je dostačujúca na identifikáciu osoby. Štruktúra DNA je rozdielna pre každú osobu s výnimkou jednovaječných dvojčiat. Využíva sa najmä v policajnej praxi a pri potvrdzovaní otcovstva. Na identifikáciu v reálnom čase sa zatiaľ pre náročnosť a zdĺhavosť získavania DNA odtlačku nepoužíva.

Geometria ruky – metóda je založená na dvoj alebo trojrozmernom meraní dĺžky alebo šírky jednotlivých prstov, kĺbov alebo kostí (Obr. 1.8). Začiatky používania tohto princípu pri automatizovanej bezpečnostne-komerčnej identifikácii osôb sa datujú už na 70. roky 20. storočia. Nevýhodou je však nie príliš unikátna biometrická vlastnosť, a preto je jej použitie závislé na očakávanom stupni bezpečnosti, ktorej sa chce dosiahnuť.



Obr. 1.8 Ruka snímaná CCD kamerou a príklad merania vzdialeností.[3]

Podpis – táto biometrická metóda využíva jedinečnosť kombinácie anatomických a behaviorálnych vlastností človeka. V súčasnosti sa nevyužíva len statický obraz podpisu, ale spracovávajú sa aj dynamické charakteristiky pri jeho písaní (Obr. 1.9), a to rýchlosť písania, tlak na podložku, smer podpisu a ďalšie relačné charakteristiky. Výhodou tohto systému je, že dynamiku podpisu sa z obrázku naučiť nedá, a preto je odolný voči falšovaniu. [3]



Obr. 1.9 Biometrické charakteristiky podpisu. [5]

2 DETEKCIA A ROZPOZNANIE TVÁRE

Rozpoznávanie tváre si získalo veľkú pozornosť v posledných 15-tich rokoch kvôli zvýšenému počtu komerčných a kriminalisticko-súdnych aplikácií, ktoré vyžadovali spoľahlivé overenie totožnosti človeka (napríklad pri overovaní prístupu, kontrole a sledovaní ľudí na verejných priestranstvách, bezpečnosti transakcií a interakcie človeka s počítačom) a dostupnosť lacných snímacích zariadení.

Napriek tomu, že existuje viacero spoľahlivejších biometrických metód, ako napríklad biometria odtlačku prsta alebo dúhovky, na rozvoj metód rozpoznania tváre sa v súčasnosti kladie veľký dôraz kvôli jej výhodám. Medzi ne patria hlavne neinvazívnosť a vysoká účinnosť aj v prípade, že snímaná osoba si nie je vedomá systému rozpoznávania osôb. [10]

Vo väčšine prípadov sa pri rozpoznávaní tváre postupuje podľa tejto schémy [1] :

- 1) Detekcia tváre v snímku
- 2) Normalizácia nájdenej tváre, ktorá zahŕňa napríklad kompenzáciu osvetlenia
- 3) Extrakcia príznakov
- 4) Vyhodnotenie podobnosti nasnímaného obrázku s obrázkami uloženými v databáze

2.1 Detekcia tváre v snímku

Detekcia tváre je prvým krokom potrebným pri procese rozpoznávania tváre. Pri zhotovovaní algoritmu je nutné brať v úvahu rôzne situácie – snímanie za rôzneho osvetlenia, rozdiel vo farbe pleti, rozmeroch, pozícii a orientácii tváre, poprípade, či sa na snímku nejaká tvár nachádza.

V súčasnosti existuje viacero metód na detekciu, a podľa spôsobu riešenia tohto problému ich možno rozdeliť do štyroch skupín :

1. Znalostné metódy → Knowledge-based methods
2. Metódy invariantných rysov → Feature invariant approaches
3. Metódy založené na porovnávaní šablón → Template matching methods
4. Metódy založené na vzhľade → Appearance-based methods

Znalostné metódy – sú založené na definovaných pravidlách, ktoré popisujú ako vyzerá skutočná ľudská tvár. Tieto pravidlá väčšinou určujú vzájomné vzťahy medzi

jednotlivými časťami tváre. Znalostné metódy sú určené predovšetkým na lokalizáciu tváre. Nevýhodou je robustnosť a zložitosť algoritmov, ktoré väčšinou nedosahujú požadované výsledky.

Metódy invariantných rysov - cieľom týchto algoritmov je nájsť v obraze štrukturálne rysy tváre, ktoré sú v obraze viditeľné pri rôznych svetelných podmienkach alebo rôznej orientácii tváre. Medzi rysy ktoré sa využívajú patria napríklad oči, ústa, nos alebo farba pokožky. Tieto metódy sa využívajú hlavne na lokalizáciu tváre a ich výhodou je jednoduchá implementácia, ktorá poskytuje kvalitné výsledky.

Metódy založené na porovnávaní šablón – princíp týchto metód je založený na korelácii medzi vstupným obrazom a šablónami, ktoré sú uložené v databáze. Táto databáza obsahuje šablóny, ktoré popisujú buď celú tvár alebo popisujú jednotlivé časti tváre samostatne. Metódy sa používajú na lokalizáciu a aj na detekciu tváre. Nevýhodou je nutnosť rozsiahlej databáze pre dosiahnutie čo najlepších výsledkov.

Metódy založené na vzhľade – model tváre sa získava v procese učenia z trénovacej množiny, ktorá obsahuje rôzne typy tvárí. Tieto modely sú následne použité pri detekcii, kde sa porovnáva vstupný snímok s modelom. Metódy založené na vzhľade dosahujú veľmi dobré výsledky a používajú sa hlavne na detekciu. [6] [7]

2.1.1 Viola-Jones detektor

Prvý krát bol detektor Viola-Jones predstavený v roku 2001 P. Violom a M. Jonesom. Jedná sa o objektový detektor pracujúci so šedo-tónovými obrazmi, ktorý patrí medzi metódy založené na vzhľade a je jedným z najčastejšie používaných detektorov na detekciu tváre. Skladá sa z troch častí :

- Haarove príznaky
- Integrálny obraz
- AdaBoost algoritmus

Medzi výhody tohto algoritmu patrí jeho rýchlosť, značná nezávislosť na osvetlení a dostatočná spoľahlivosť.

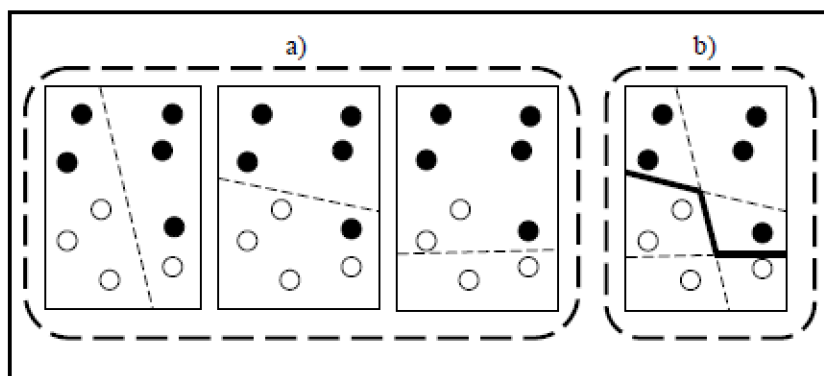
Základom pre realizáciu tohto detektoru je trénovacia množina, na ktorej sa bude algoritmus učiť. Táto trénovacia množina musí obsahovať negatívne a pozitívne vzory. V tomto prípade sú pozitívne vzory snímky, na ktorých sa tvár vyskytuje a negatívne vzory sú snímky, ktoré tvár neobsahujú.

A. AdaBoost algoritmus

Tento klasifikačný algoritmus vychádza z metódy strojového učenia zvanej boosting, ktorej cieľom je zlepšenie klasifikačnej presnosti ľubovoľného algoritmu strojového učenia. Základom je využitie slabých klasifikátorov $h_t(x)$, vybraných z množiny klasifikátorov H . Lineárnou kombináciou slabých klasifikátorov vznikne nelineárny silný klasifikátor $H(x)$. Na vstup algoritmu prichádza tréningová množina S , zložená z dvojice x_i a y_i , kde x_i je získaná hodnota príznaku a y_i je trieda odpovedajúca príznaku i , a môže nadobúdať hodnoty -1 a 1. Na rozdiel od boostingu využíva AdaBoost váhenie tréningovej množiny váhami D_t . Tie sú na začiatku nastavené rovnomerne a následne prebehne proces učenia, ktorý sa skladá z nasledujúcich krokov [9]:

1. Výber slabého klasifikátora s najmenšou chybou klasifikácie pri váhach D_t
2. Overenie, či nedošlo k prekročeniu hodnoty 0,5 u chyby klasifikátora
3. Výpočet koeficientu slabého klasifikátora v lineárnej kombinácii $H(x)$
4. Aktualizácia jednotlivých váh D_t

Princíp vzniku silného klasifikátora z lineárnej kombinácie slabých klasifikátorov je zobrazený na Obr. 2.1.



Obr. 2.1 a) slabé klasifikátory; b) silný klasifikátor. [8]

Matematický popis procesu učenia klasifikačného algoritmu AdaBoost:[9]

1. Vstup :

$$S = \{(x_1, y_1), \dots, (x_m, y_m)\}, \quad (2.1)$$

počet interácií T

2. Inicializácia váh:

$$D_1(i) = \frac{1}{m} \quad (2.2)$$

3. Cyklus pre $t = 1, \dots, T$:

a. Výber klasifikátorov na základe váženej trénovacej chyby

$$\varepsilon_j = \sum_{i=1}^m D_t(i) I[y_i \neq h_j(x_i)] \quad (2.3)$$

$$h_t = \operatorname{argmin}_{h_j \in H} \varepsilon_j$$

b. Ak

$$\varepsilon_t = 0 \text{ alebo } \varepsilon_t \geq \frac{1}{2} \quad (2.4)$$

potom koniec cyklu

c. Nastavenie

$$\alpha_t = \frac{1}{2} \log\left(\frac{1 - \varepsilon_t}{\varepsilon_t}\right) \quad (2.5)$$

d. Úprava váh

$$D_{t+1}(i) = \frac{D_t(i) e^{-\alpha_t y_i h_t(x_i)}}{Z_t} \quad (2.6)$$

kde

$$Z_t = \sum_{i=1}^m D_t(i) e^{-\alpha_t y_i h_t(x_i)}, \quad (2.7)$$

4. Výstup

$$H(x) = \text{sign} \left(\sum_{t=1}^T \alpha_t h_t(x) \right) \quad (2.8)$$

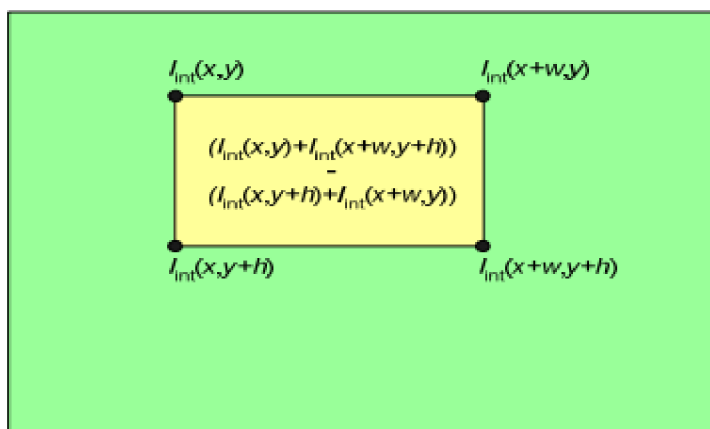
B. Integrálny obraz

Integrálny obraz sa využíva na jednoduchý a rýchly výpočet hodnôt príznakov zo vstupného obrazu. Aby sa pre každú hodnotu príznaku vstupného obrazu nemusela počítať suma hodnôt pixelov odpovedajúcich danému príznaku, je originálny obraz prevedený na integrálny. V ňom sú kumulatívne sčítané hodnoty pixelov vo všetkých radoch a stĺpcoch naľavo od pozície aktuálneho pixelu, a teda napríklad pixel umiestnený v pravom dolnom rohu má hodnotu súčtu intenzít všetkých pixelov v obraze.

Jednotlivé hodnoty integrálneho obrazu sa získajú riešením nasledujúcej rovnice :

$$\begin{aligned} s(x, y) &= s(x, y - 1) + I(x, y), \\ I_{int}(x, y) &= I_{int}(x - 1, y) + s(x, y), \end{aligned} \quad (2.9)$$

kde $s(x,y)$ znamená kumulovaný súčet hodnôt v riadku obrazu, $I(x,y)$ sú hodnoty intenzít jednotlivých pixelov vstupného obrazu a I_{int} predstavuje jednotlivé hodnoty integrálneho obrazu. Zároveň platí, že $s(x,0)=0$ a $I_{int}(0,y)=0$.



Obr. 2.2 Príklad výpočtu sumy ľubovoľného obdĺžnika pomocou integrálneho obrazu. (w – šírka požadovaného trojuholníka; h – výška požadovaného trojuholníka) [9]

Ako je možné vidieť na Obr. 2.2, na výpočet sumy ľubovoľného obdĺžnika postačujú dve operácie sčítania a jedna operácia odčítania. Tým sa výpočet hodnôt jednotlivých príznakov výrazne zjednoduší. [9]

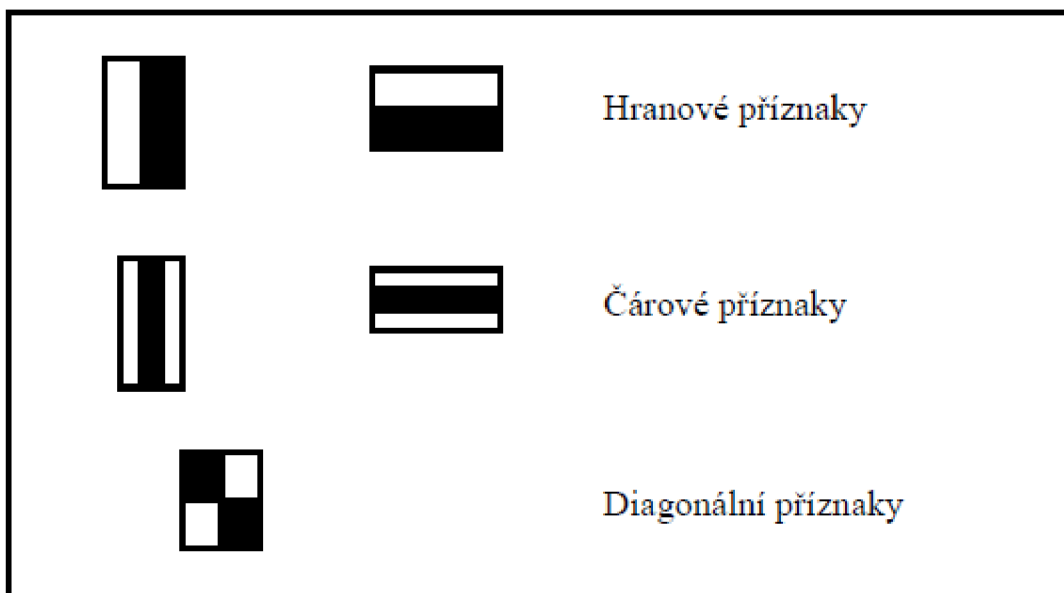
C. Haarove príznaky

Haarove príznaky sú obdĺžnikové oblasti, ktoré sú využité ako vstup do klasifikačného algoritmu. Jednotlivé príznaky sú použité na celý vstupný obraz, pričom postupne dochádza k zmene veľkosti príznakov od veľkosti 1x1 až na veľkosť odpovedajúcu vstupnému obrazu.

Hodnota príznaku sa získava odčítaním sumy intenzít i pixelov obrazu pod čiernou časťou oblasti ($I(x_b, y_b)$) od sumy intenzít j pixelov obrazu pod svetlou časťou ($I(x_w, y_w)$) [8]:

$$f(x) = \sum_{w=1}^i I(x_w, y_w) - \sum_{b=1}^i I(x_b, y_b) \quad (2.10)$$

Na Obr. 2.3 sú zobrazené tri základné typy Haarových príznakov.

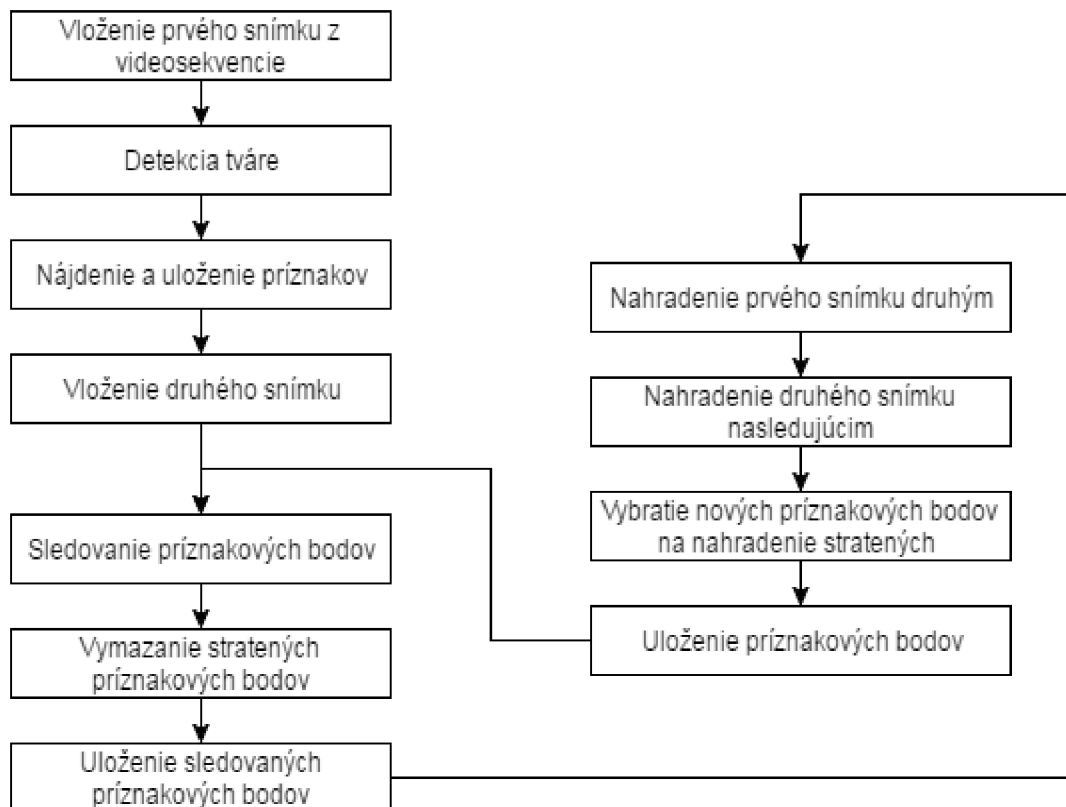


Obr. 2.3 Základné typy Haarových príznakov. [8]

2.1.2 KLT algoritmus na sledovanie tváre

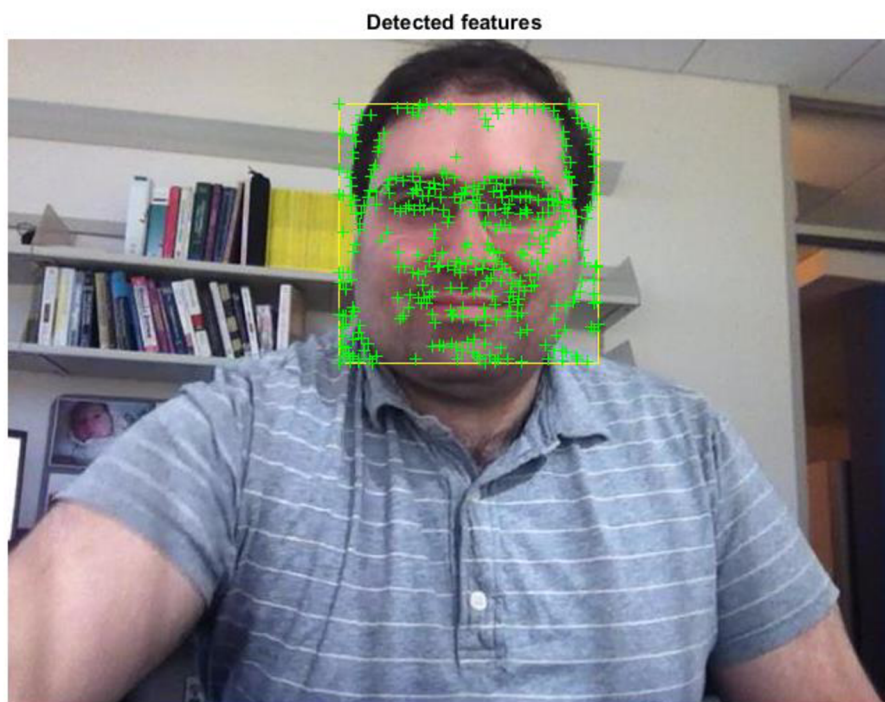
Pri videosekvenciách by bolo využitie objektového detektora popísaného v kapitole 2.1.1 na každú jednu snímku výpočtovo veľmi náročné a takisto málo spoľahlivé v prípade, že osoba na videu pootočí alebo nakloní hlavu. Preto sa na sledovanie tváre vo videu využíva Kanade-Lucas-Tomasi algoritmus, známy aj ako KLT algoritmus.

Princíp fungovania takéhoto sledovacieho algoritmu je zobrazený na blokovom diagrame (Obr. 2.4).



Obr. 2.4 Blokový diagram – KLT algoritmus

Vstupom je prvý snímok videa, na ktorý sa aplikuje Viola-Jones detektor. Týmto sa získa výrez v ktorom sa nachádza tvár. V ďalšom kroku sa v tomto výreze identifikujú príznakové body, ktoré bude možné spoľahlivo sledovať. V zdroji [17] sa ako štandard využívajú tzv. „good features to track“ navrhnuté Shi a Tomasi. Posledným krokom je sledovanie nájdených príznakových bodov naprieč všetkými snímkami vo videu. Na Obr. 2.5 je zobrazená detegovaná tvár s identifikovanými príznakovými bodmi.



Obr. 2.5 Detegovaná tvár s vyznačenými príznakmi. [17]

2.2 Normalizácia tváre

Úlohou normalizácie je v prípade rozpoznávanie tváre vhodne predspracovať výrez, ktorý obsahuje detegovanú tvár a zvýšiť tým spoľahlivosť porovnávaní. Medzi typické úlohy patrí napríklad zníženie vnútrotriednej variability a zvýšenie medzitriednej variability [1]. Typy normalizácie, ktoré sa v procese rozpoznávania môžu využiť sú napríklad:

- Zmena veľkosti obrázka
- Vyrezanie tváre z pozadia
- Zarovnanie význačných bodov
- Jasová kompenzácia – ekvalizácia histogramu
- Ďalšie typy normalizácie, ku ktorým patrí napríklad potlačenie vplyvu účesu, okuliarov, atď.

2.3 Metódy rozpoznania tváre pomocou podobnosti obrazových dát

Najdôležitejšou úlohou pri procese rozpoznávania je vyriešiť otázku, kto je osoba, ktorá sa nachádza na danom snímku. Podľa prístupu, s akým sa k riešeniu tejto otázky

pristupuje, sa dajú metódy rozpoznania tváre rozdeliť do dvoch hlavných kategórií, a to na metódy rozpoznania tváre pomocou **podobností obrazových dát** a metódy rozpoznania tváre na základe **topologických vlastností tváre**.

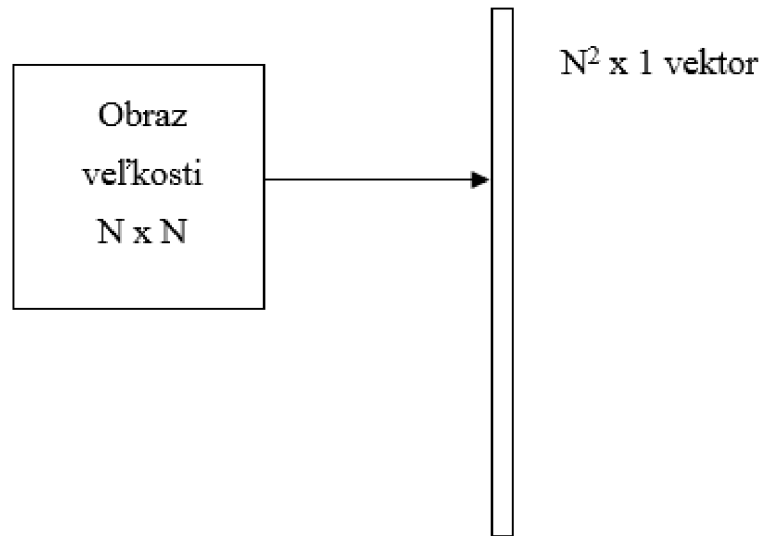
Metódy rozpoznania tváre modelujú variabilitu rôznych tvárí tým, že analyzujú ich štatistické vlastnosti na základe veľkého množstva tréningových obrázkov. Patria sem štatistické metódy ako PCA (z angl. Principal Component Analysis, inak nazývaná aj ako metóda Eigenfaces) a LDA (z angl. Linear Discriminant Analysis, v inej literatúre aj ako Fisherfaces), alebo metódy založené na strojovom učení – neurónové siete, či SVM (z angl. Support Vector Machines). [1]

2.3.1 PCA (Principal Component Analysis) - Eigenfaces

PCA, alebo aj analýza hlavných komponent je jedna z najčastejšie používaných metód na rozpoznanie tváre. Ako prvý ju použili Kirby a Sirovich [14] na obrazy tváre a dokázali, že PCA je optimálna kompresná schéma, ktorá minimalizuje strednú kvadratickú odchýlku medzi originálnym obrazom a jeho rekonštrukciou pre ľubovoľný stupeň kompresie. Následne Turk a Pentland [14] popularizovali využiteľnosť PCA, keď ju využili na výpočet základných vektorov podpriestoru (ktoré nazvali eigenfaces) pre databázu snímok tváre a premietli snímky z databázy do komprimovaného podpriestoru. Eigenfaces sú vlastne vlastné vektory kovariančnej matice vypočítanej z obrazov tvárí v tréningovej množine, ktoré boli prevedené do vektorovej podoby. [6] [14]

Výpočet eigenfaces

V prvom kroku sú prevedené vstupné obrazy z dvojdimenzionálneho priestoru do vektorovej podoby, takže matica o veľkosti $N \times N$ sa zmení na vektor o veľkosti N^2 (Obr. 2.6). V prípade, že by bol vstupný obraz veľkosti 256×256 , výsledný vektor by mal veľkosť 65 536.



Obr. 2.6 Prevedenie obrazu z 2D priestoru do 1D priestoru

Z týchto vektorov sa následne zostrojí matica tak, že sa vektory poskladajú vedľa seba. Počet riadkov bude v tomto prípade N^2 a počet stĺpcov bude rovný celkovému počtu obrázkov. Skupina obrázkov bude teda popísaná ako množina bodov vo viacdimezióálnom priestore. Hlavná myšlienka analýzy hlavných komponent je nájsť vektory, ktoré najlepšie popisujú distribúciu obrázkov tváří v celom obrazovom priestore. Tieto vektory definujú podpriestor obrázkov tváre, ktorý sa nazýva „face space“. Každý vektor má dĺžku N^2 , popisuje obraz rozmerov $N \times N$ a je lineárnou kombináciou obrazov tváří. Keďže sú vektory podobné ľudskej tvári a sú to vlastné vektory kovariančnej matice korešpondujúcej s originálnymi snímkami tváre, nazývajú sa eigenfaces.

Nech bude tréningová sada snímkov tváre $\Gamma_1, \Gamma_2, \Gamma_3, \dots, \Gamma_M$. Príklad takejto sady, ktorá sa skladá z 20 obrázkov je na Obr. 2.7.



Obr. 2.7 Trénovacia sada obrázkov tvári. [15]

Potom bude priemerná tvár všetkých tvári, zobrazená na Obr. 2.8, definovaná ako

$$\Psi = \frac{1}{M} \sum_{n=1}^M \Gamma_n \quad (2.11)$$



Obr. 2.8 Priemerná tvár. [15]

Pre centrovanie dát sa od každého obrázku z trénovacej sady odčíta priemerná hodnota

$$\phi_i = \Gamma_i - \Psi \quad (2.12)$$

Takto vznikne súbor veľmi veľkých vektorov, ktoré sú vstupom pre metódu analýzy hlavných komponent. PCA hľadá množinu ortonormálnych vektorov u_n , ktoré najlepšie popisujú distribúciu dát. Nájdené vektory u_k sú v tomto prípade vlastné vektory (eigenvektors) a skalárne hodnoty λ_k sú vlastné hodnoty (eigenvalues) kovariančnej matice, ktorá je daná nasledujúcim vzťahom :

$$C = \frac{1}{M} \sum_{n=1}^M \phi_n \phi_n^T = AA^T, \quad (2.13)$$

kde matica $A = [\phi_1 \ \phi_2 \ \dots \ \phi_M]$. Kovariančná matica C má rozmery $N^2 \times N^2$, a teda určenie N^2 vlastných vektorov a vlastných čísel je takmer neriešiteľná otázka. Preto je potrebné vytvoriť výpočtovo realizovateľnú metódu na nájdenie vlastných hodnôt.

Uvažujme vlastné vektory v_i z $A^T A$ tak, že

$$A^T A v_i = \mu_i v_i \quad (2.14)$$

Prenásobením oboch strán A dostaneme

$$A A^T A v_i = \mu_i A v_i \quad (2.15)$$

Z čoho môžeme vidieť, že $A v_i$ sú vlastné vektory $C = A A^T$.

Podľa tejto analýzy môže byť skonštruovaná matica o rozmeroch $M \times M$

$$L = A^T A, \quad (2.16)$$

kde

$$L_{m,n} = \phi_m^T \phi_n, \quad (2.17)$$

a následne môže byť nájdených M vlastných vektorov v_l z matice L . Tieto vektory určujú lineárnu kombináciu M obrázkov tváre z trénovacej množiny na formovanie eigenfaces u_l :

$$u_l = \sum_{k=1}^M v_{l,k} \phi_k, \quad l = 1, \dots, M \quad (2.18)$$

Na Obr. 2.9 Je možné vidieť prvých 9 eigenfaces odvodených zo vstupných snímok zobrazených na Obr. 2.9.



Obr. 2.9 Prvých 9 eigenfaces. [15]

Touto analýzou sa zjednodušili výpočty z rádov počtu pixelov v snímku (N^2) na počet obrázkov v trénovacej množine (M). [13]

Rozpoznávanie tváre

Testovaný obrázok tváre (Γ) je transformovaný na jeho eigenface komponenty pomocou jednoduchej operácie

$$\omega_k = u_k^T(\Gamma - \Psi) \quad (2.19)$$

pre $k = 1, \dots, M$.

Váhy formujú vektor $\Omega^T = [\omega_1, \omega_2, \dots, \omega_M]$, ktorý popisuje príspevok jednotlivých eigenface pri reprezentácii vstupného obrazu.[13] Po tomto procese už stačí len rozhodnúť, ktorá tvár z trénovacej sady sa najviac podobá neznámej tvári. Na rozhodnutie sa využíva zistenie vzdialenosti medzi trénovacími eigenfaces Ω a eigenface neznámeho obrázku Ω^T . Najčastejšie sa využíva Euklidovskej vzdialenosti :

$$e_r = \min_l ||\Omega^T - \Omega||, \quad (2.20)$$

ale využíva sa aj Hammingovej vzdialenosti alebo Mahalanobisovej vzdialenosti.[15]

Výhody PCA metódy [18]:

- Rozpoznávanie je jednoduché a efektívne v porovnaní s ďalšími prístupmi.
- Kompresia dát je dosiahnutá ich reprezentáciou do nízko-dimenzionálneho podpriestoru.
- Údaje intenzít sú použité priamo pre učenie a rozpoznanie bez významného nízko-úrovňového alebo stredno-úrovňového spracovania.

Nevýhody PCA metódy [18]:

- Metóda je veľmi citlivá na mierku (veľkosť danej tváre), a preto je nutné nízko-úrovňové predspracovanie rozmerov vstupných obrázkov.
- Schopnosť rozpoznávania sa znižuje menením pózy a osvetlenia.
- Pri extrémnej zmene výrazu tváre, polohy hlavy alebo použitím prevleku sa tiež schopnosť rozpoznávania znižuje.
- Pri veľkom množstve tréningových fotiek je učiaci proces časovo náročný, čo sťažuje možnosť aktualizácie databáze.

2.3.2 LDA (Linear Discriminant Analysis)

Táto metóda sa v literatúre zvykne nazývať aj ako *Fisherfaces*. Princíp je podobný ako pri rozpoznávaní pomocou metódy PCA, kde je opäť cieľom čo najviac zredukovať priestor tváří pre hľadanie vzorov. Nový priestor sa vytvára tak, aby separoval čo najviac body, ktoré popisujú rovnakú osobu od bodov ostatných osôb. Nevýhodou tejto metódy je, že môže dôjsť k preučeniu - adaptácii systému na osoby, ktoré sa zúčastnili procesu učenia a v prípade novej osoby nie je možné predpovedať, či jej obraz bude od ostatných dostatočne separovaný. [1]

Postup rozpoznania tváre využitím LDA [16] :

- 1) Ako prvé je potrebné zaradiť snímky v tréningovej množine do niektorej z vytvorených tried, označených C .
- 2) Z tried sa vypočíta priemerný vektor μ podľa vzťahu

$$\mu = \frac{1}{C} \sum_{i=1}^C \mu_i \quad (2.21)$$

- 3) V ďalšom kroku sa zistí počet prvkov v rámci tried, M .
- 4) Vypočíta sa rozptyl medzi maticami a rozptyl v rámci matice. Na výpočet rozptylu v rámci matice sa využije vzťah

$$S_w = \sum_{i=1}^c \sum_{j=1}^M (Y_j - \mu_i)(Y_j - \mu_i)^T, \quad (2.22)$$

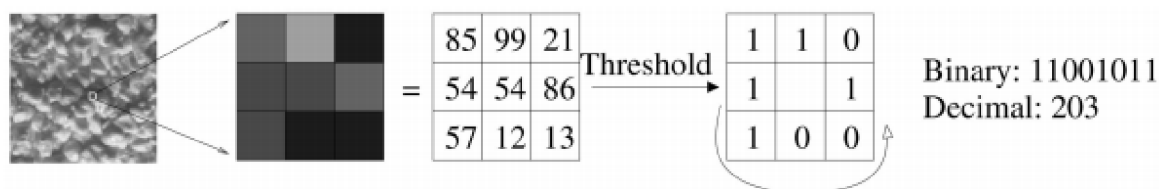
a na výpočet rozptylu medzi maticami sa využije rovnica

$$S_b = \sum_{i=1}^c (\mu_i - \mu)(\mu_i - \mu)^T \quad (2.23)$$

- 5) Vypočíta sa pomer rozptylu medzi triedami k rozptylu v rámci triedy.
- 6) Výpočet vlastnej hodnoty a príslušného vlastného vektoru.
- 7) Normalizácia vlastného vektoru.
- 8) Výpočet váhy a Euklidovskej vzdialenosti.

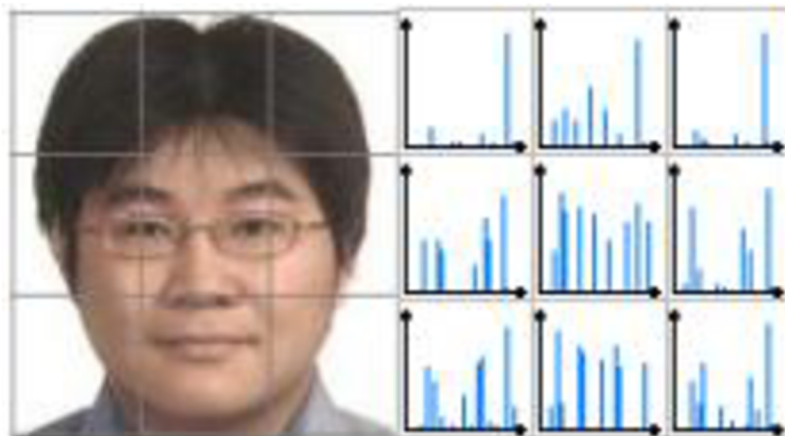
2.3.3 LBP (Local Binary Pattern)

Rozpoznanie tváre na základe LBP bolo navrhnuté v [19]. LBP operátor priradí štítok každému pixelu v obrázku tým, že sa prahuje susedstvo 3x3 okolo centrálného pixelu, ktorého hodnota je prahová. Výsledkom tohto prahovania je binárne číslo. Princíp je zobrazený na Obr. 2.10.



Obr. 2.10 Základný LBP operátor. [19]

Následne sa k popisu textúry využije histogram vytvorený z daných štítkov. Pre snímok tváre platí, že sa rozdelí na niekoľko regiónov, a kombinácia LBP histogramov (Obr. 2.11) sa využije k popisu tváre. Ku klasifikácii tvári do skupín sa využíva chí-kvadrát. Výhodou tejto metódy je hlavne jej robustnosť voči zmenám osvetlenia.[20]



Obr. 2.11 Klasifikácia založená na LBP histogramoch. [20]

2.3.4 ICA (Independent Component Analysis)

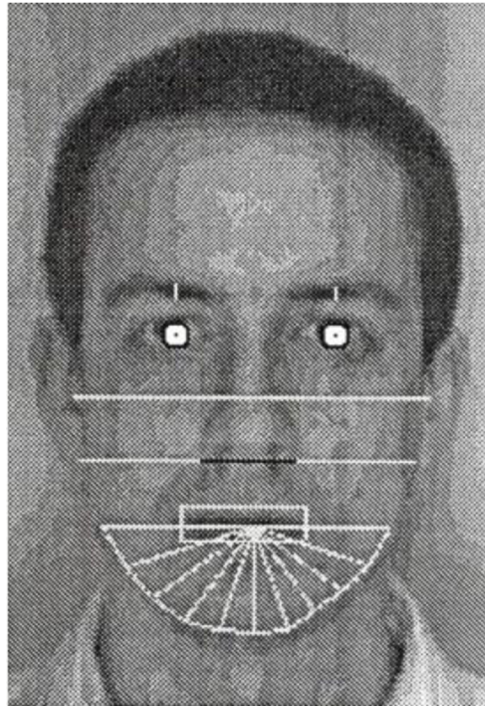
Metóda nezávislých komponent sa využíva k transformácii viacdimenzionálneho náhodného vektoru na jeho komponenty. Tieto komponenty by mali byť od seba čo najviac štatisticky nezávislé. Dôležitým princípom odhadu ICA je maximálna negaussovskosť, ktorá vyplýva z centrálneho limitného teorému. Používa sa na nájdenie základných faktorov alebo komponentov z viacdimenzionálnych štatistických dát. Jej cieľom je poskytnúť nezávislý rozklad a reprezentáciu obrazu, čo znamená, že by mala byť využívaná k minimalizácii štatistickej závislosti medzi dvoma základnými vektormi.

V [21] sa píše, že pokiaľ existujú nezávislé základné obrázky so štatisticky nezávislými hodnotami koeficientov, tak má metóda ICA lepšiu úspešnosť rozpoznania v porovnaní s metódou PCA, pretože metóda PCA berie v úvahu len momenty druhého rádu a nekoreluje dáta. Na druhej strane metóda ICA poskytuje efektívnejšiu reprezentáciu dát, pretože využíva štatistiku vyššieho rádu a identifikuje nezávislé zdrojové komponenty z ich lineárneho kríženia. [21]

2.4 Metódy rozpoznania tváre na základe topologických vlastností tváre

Tieto metódy sú založené na tom, že sa najprv snažia identifikovať a extrahovať zo vstupného snímku výrazné rysy tváre, ako sú napríklad ústa, nos, oči. Následne sú vypočítané geometrické vzťahy medzi týmito nájdenými bodmi tváre, čím sa redukuje vstupný obraz tváre na vektor geometrických vlastností. Príklad takýchto geometrických vlastností tváre je zobrazený na Obr. 2.12. Na porovnanie snímok a klasifikáciu sa využívajú štandardné štatistické metódy využívané na rozpoznanie

vzorov. Patria sem metódy ASM (Active Shape Model), AAM (Active Appearance Model) a EBGM (Elastic Bunch Graph Matching).



Obr. 2.12 Geometrické vlastnosti tváre (biela farba) požívané pri experimentoch rozpoznania. [11]

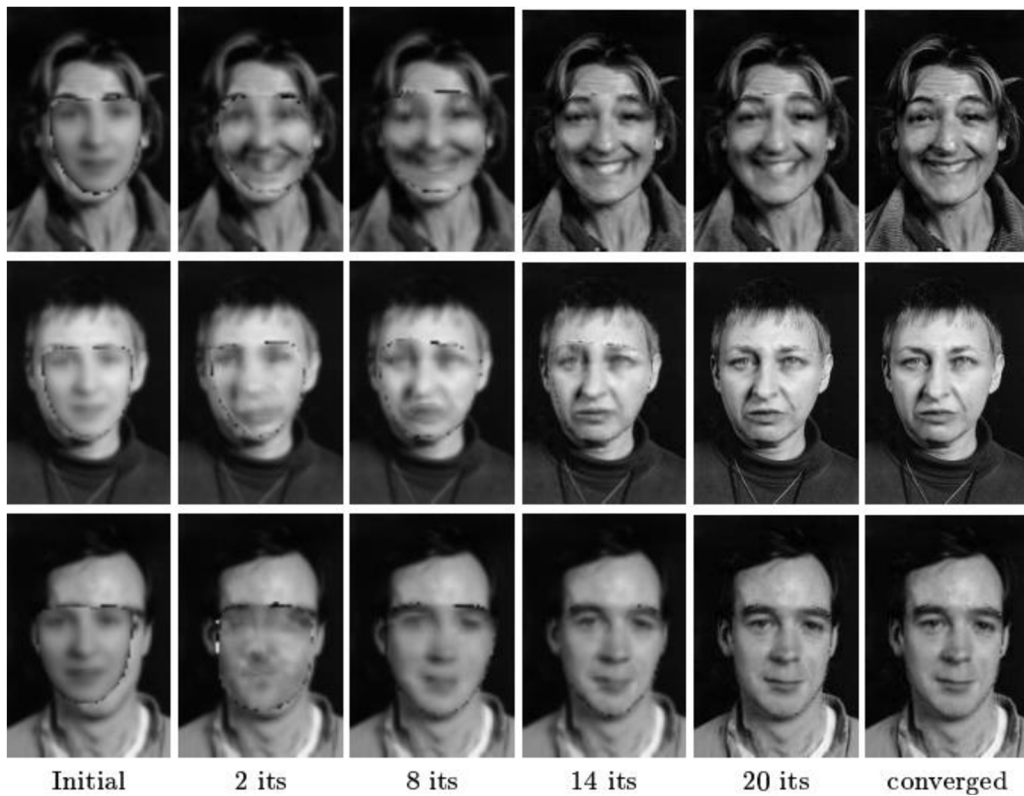
Hlavnou výhodou týchto modelov je ich robustnosť voči zmenám v polohe tváre, osvetlení a veľkosti snímanej tváre. Nevýhodou je však zložitá extrakcia príznakov a fakt, že osoba, ktorá vytvára túto techniku musí sama rozhodnúť, ktoré príznaky sú dôležité.[11]

2.4.1 ASM a AAM metóda

Tieto metódy fungujú na princípe aktívnej šablóny, ktorá sa skladá z niekoľkých významných bodov umiestnených na tvári (kútik oka, ušný lalok atď.). Body je nutné v rámci predspracovania najprv ručne označiť na každom snímku z trénovacej množiny a následne si model šablóny zapamätá vzájomnú polohu týchto bodov, poprípade aj informácie o textúre v ploche ohraničenej jednotlivými bodmi.

Rozdiel medzi AAM a ASM je v tom, že šablóna u metódy ASM sa skladá len z jednotlivých bodov a hrán medzi nimi, ktoré sú potom iteratívne namapované na hranový obraz vstupného snímku. Až po získaní výsledného tvaru šablóny je deformovaná aj textúra. Na druhej strane šablóna u metódy AAM obsahuje okrem

bodov a hrán aj informácie o textúre, ktoré sú následne pri procese iterácie šablóny používané spoločne (viď Obr. 2.13) a obvykle dosahujú lepšie výsledky ako metóda ASM. Rozpoznávanie identity je možné porovnaním referenčnej a extrahovanej šablóny. [1]



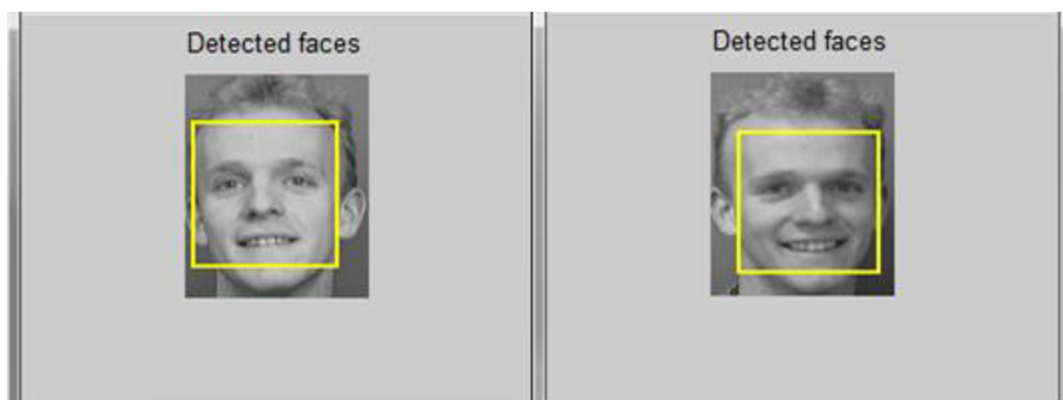
Obr. 2.13 Metóda AAM – iteratívne mapovanie modelu na testovací obrázok. [1]

3 PRAKTICKÁ ČASŤ

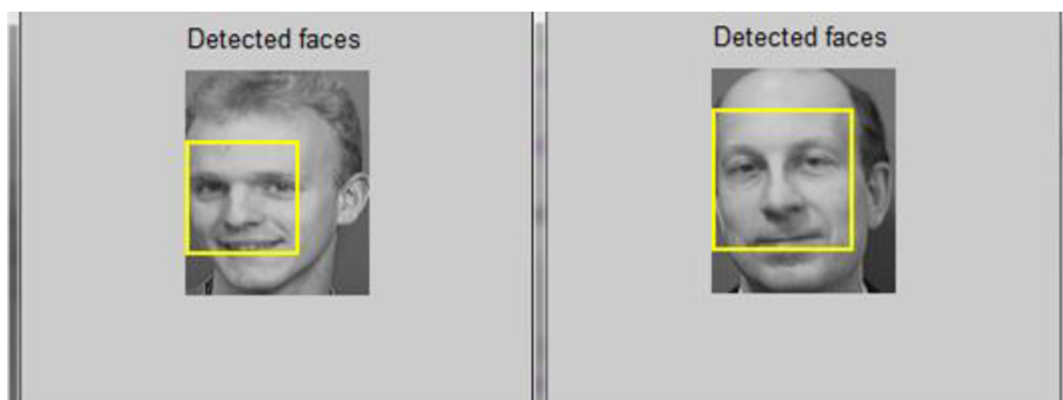
3.1 Detekcia tváre

V praktickej časti bola overená funkčnosť algoritmu na detekciu tváre Viola-Jones, ktorý je podrobnejšie popísaný v kapitole 2.1.1. Algoritmus bol implementovaný do programovacieho prostredia Matlab a otestovaný na sade snímok z databázy AT&T Laboratories Cambridge. Databáza obsahuje 10 rôznych snímok 40-tich subjektov. U niektorých subjektov boli obrázky nasnímané v rozdielnom čase, pri zmenenom osvetlení, zmene výrazu tváre (otvorené/zavreté oči, úsmev/bez úsmevu) a detailoch tváre (okuliare/bez okuliarov). Všetky obrázky boli snímané voči tmavému pozadiu.

Z nasledujúcich obrázkov je možné vidieť nedostatky Viola-Jones detektoru, kde sa potvrdilo, že je detekcia závislá na osvetlení a hlavne smeru pohľadu snímanej osoby. Príklad správnej detekcie je zobrazený na Obr. 3.1, príklad chybné detekcie na Obr. 3.2 a príklad, kde detektor nedokázal tvár detegovať vôbec na Obr. 3.3.



Obr. 3.1 Správne detegovaná tvár



Obr. 3.2 Chybná detekcia



Obr. 3.3 Zlyhanie detekcie

3.2 Návrh snímania videosekvencií

V tejto kapitole je navrhnutý postup a špecifiká snímania videosekvencií, ktoré boli realizované pri riešení diplomovej práce.

Vzhľadom k tomu, aby bol vytvorený systém s vysokou presnosťou a rýchlosťou rozpoznania tváre pri využití súčasných algoritmov, bolo nutné presne definovať požiadavky na zariadenie snímajúce scénu, podmienky, za ktorých sa bude snímať, a chovanie sa osôb, ktoré budú snímané.

Snímacie zariadenie

- Fotoaparát Canon PowerShot G15
- Svetelnosť F1.8 – 2.8
- Najvyššie rozlíšenie fotografií - 12 Mpx
- Najvyššie rozlíšenie pri natáčaní videa – full HD formátu H.246 a QuickTime MOV
- rýchlosť snímania cca 30 snímok za sekundu

Zobrazovacie zariadenie

- Lenovo Z570
- Procesor: Intel® Core™ i5 – 2430M CPU @ 2.40GHz
- Pamäť RAM : 4 GB
- Operačný systém: Windows 7
- Verzia Matlabu : R2014a

Podmienky snímania

- konštantné osvetlenie miestnosti
- použitie bieleho svetla na prisvetlenie
- statické pozadie
- snímanie len jednej osoby
- scéna bude u každého subjektu totožná

Odporúčané nastavenia

- počítač s pamäťou RAM aspoň 4 GB
- Matlab od verzie R2012a do verzie R2014b

Správanie sa snímaných osôb

- osoby spolupracujú so snímacím zariadením – pre detekciu tváre je nutný približne priamy pohľad osoby na kameru, pri následnom trekovaní je možné uhol pohľadu meniť
- štandardný výraz tváre je neutrálny, ale v priebehu snímania sa môže zmeniť pre zistenie funkčnosti rozpoznávacieho systému
- scenár, podľa ktorého sa budú subjekty pohybovať je u každého subjektu totožný

Scenár1 – osoba vchádza do miestnosti a približuje sa ku snímačej kamere, ktorá je výške 1,8m a pozerá sa do objektívu. Počas tohto okamihu by malo dôjsť k identifikácii osoby, ktorej by bol umožnený/neumožnený prístup do zabezpečenej oblasti.

Scenár2 – osoba prechádza vedľa kamery, ktorá je vo výške 1,8m. Táto scéna by mala simulovať snímame v nejakej kontrolovanej oblasti, kde by bolo nutné mať obraz o tom, kto do danej miestnosti vošiel.

3.3 Vytvorenie databáze tvárí

Prvým krokom pre rozpoznanie tváre z videosekvencií je získanie trénovacej množiny obrázkov zo snímanej skupiny subjektov. Na vytvorení databázy sa podieľalo 17 osôb. Pre vyššiu úspešnosť identifikácie sa vytvorilo viac fotiek od každého subjektu. Tie musia byť orezané tak, aby bola viditeľná len tvár subjektu, ktorá by mala mať rovnaké rozmery, ako tvár detegovaná využitím detektoru Viola-Jones. To je možné spraviť dvoma spôsobmi :

- a) Orezaním fotografií manuálne – toto riešenie je veľmi pracné, a keďže je algoritmus použitý v tejto diplomovej práci veľmi náchylný na veľkosť tváre na snímku, je aj veľmi náročné vyrezať tvár tak, aby bolo výsledné rozpoznanie algoritmu úspešné.
- b) Využitie programu vytvoreného v Matlabe – program vytvorený v tejto diplomovej práci využíva algoritmus Viola-Jones a následne na sledovanie tváre algoritmus KLT. Po aplikácii týchto algoritmov sa do programu uložia súradnice bodov v každom snímku videa, kde sa nachádza tvár. Následne už stačí detegovanú tvár len vykresliť a uložiť ako obrázok. Toto riešenie je jednoduchšie, omnoho rýchlejšie a vykazuje lepšie výsledky ako ručné orezávanie.

Príklad niektorých fotiek z databázy, ktoré boli získané druhou popísanou metódou sú zobrazené na Obr. 3.4.



Obr. 3.4 Príklad obrázkov v databáze

Orezanie fotiek je pri metóde PCA dôležitý faktor a pri nedodržaní presných rozmerov orezanej tváre rozpoznávací algoritmus nebude účinný.

3.4 Vytvorenie databázy videí

Keďže zadaním diplomovej práce bola implementácia rozpoznávacej metódy na videosekvencie, bolo nutné vytvoriť si databázu videí. Tie boli snímané v rozlíšení 640x480 px, pretože samotný proces rozpoznávania je výpočtovo veľmi náročný.

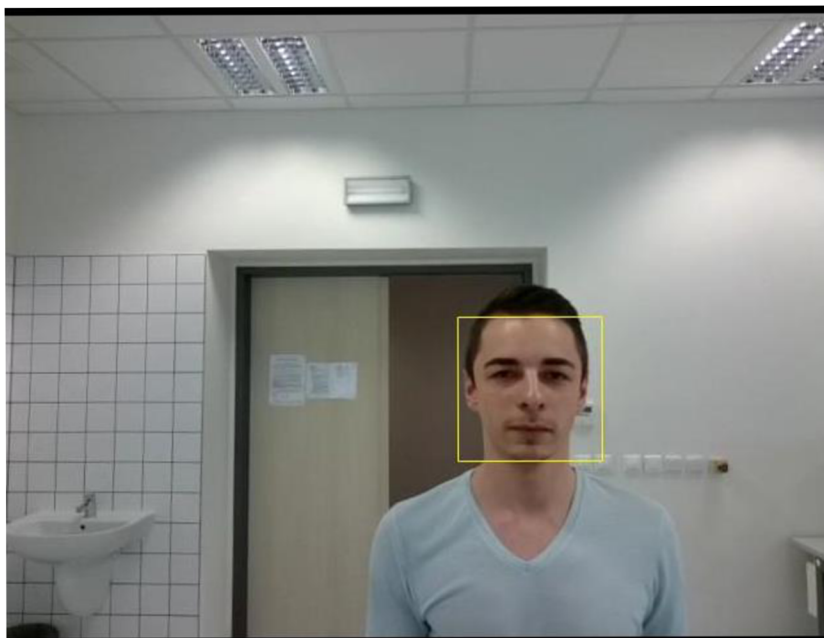
Natočené videá boli pred samotným uložením do databázy orezané na vhodnú dĺžku tak, aby bola sledovaná osoba vo vhodnej vzdialenosti. Na orezanie videí sa použil online nástroj pre rezanie videí dostupný z [22]. Jeho výhodou je, že odpadá nutnosť inštalovať software do vlastného počítača, a takisto je tam mnoho doplnkových nástrojov pre úpravu videí, ako napríklad konvertovanie do iných formátov, otáčanie videa, vyrezanie len určitej záujmovej časti videa, odstránenie zvukov z videa, alebo zmena rozlíšenia videa. Nevýhodou je, že po orezaní sa video skonvertuje na jeden z 5-tich dostupných formátov. V prípade vytvárania tejto databázy bol využitý formát mp4.

Jednotlivé videá sa začínajú pri priamom pohľade osoby do fotoaparátu vo vzdialenosti približne 2 metrov od snímacieho zariadenia, aby mohol algoritmus Viola-Jones jednoznačne identifikovať tvár danej osoby a aby nájdená tvár bola v dostatočnej kvalite. Dĺžka videí trvá jednotky sekúnd a je závislá od rýchlosti chôdze danej osoby. Dĺžka videa by pri použití počítača s pamäťou RAM 4GB nemala presiahnuť dĺžku 4-5 sekúnd, z dôvodu výpočtovej náročnosti implementovanej metódy v Matlabe a plynulosti programu. V prípade výkonnejšieho počítača by bolo možné použiť aj dlhšie videá vo vyššom rozlíšení. Príklad jedného snímku videa zo scény1 je na Obr. 3.5 a príklad snímku zo scény2 je na Obr. 3.6.

Vytvorené boli dve databázy videí. V prvej sú videá, ktoré zobrazujú prvú scénu. Natočených je 17 osôb, pričom niektoré osoby majú viac ako jedno video. Príkladom sú osoby, ktoré nosia dioptrické okuliare. Tie boli natočené s nimi a aj bez nich. Niektoré

osoby sa zúčastnili natáčania po nejakom časovom úseku od natočenia prvého videa, a boli tak nasnímané pre testovacie účely znova, poprípade so zmeneným výrazom tváre.

V druhej databáze sú videá, ktoré zobrazujú scénu2. Obsahuje 12 videí.



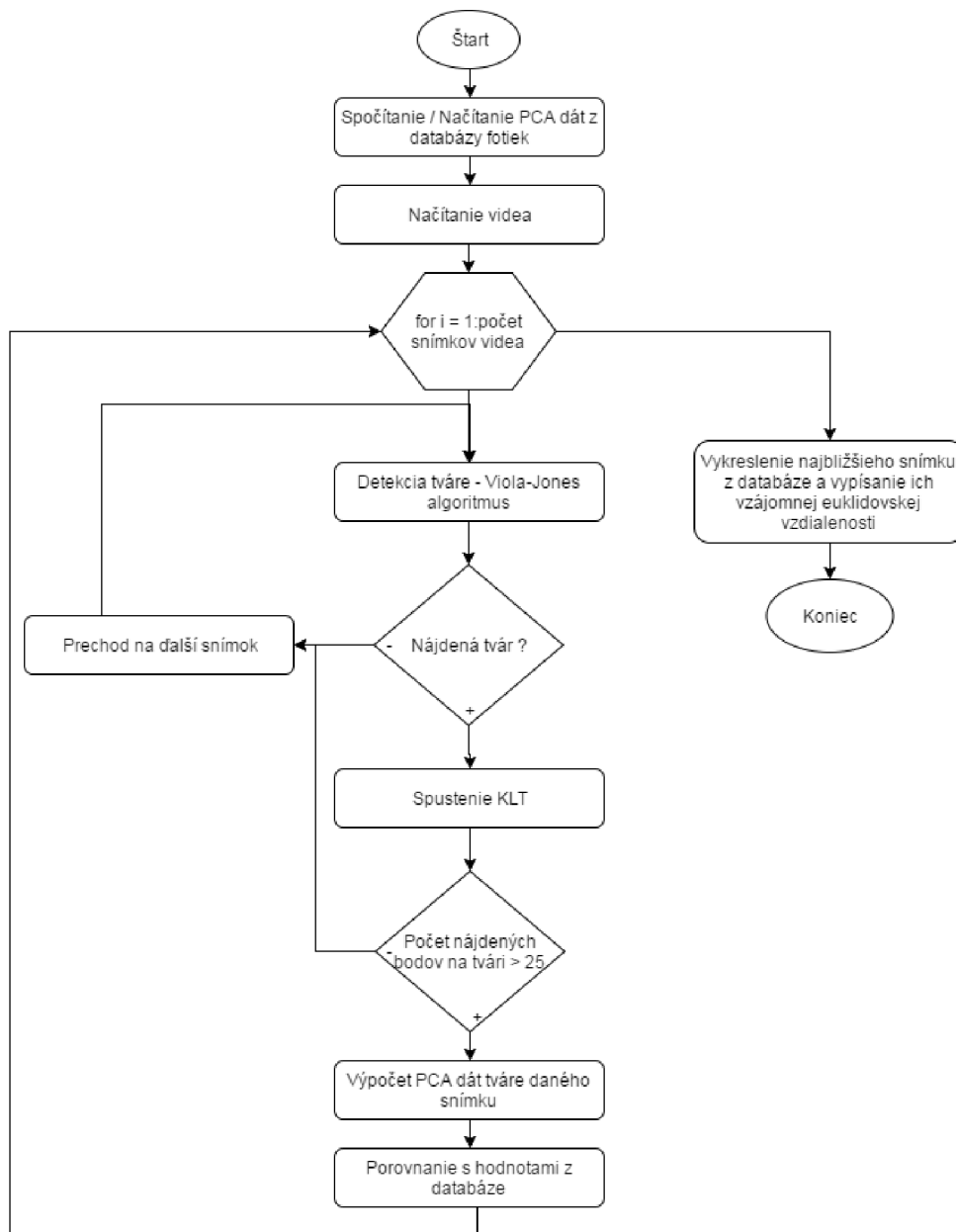
Obr. 3.5 Snímka videa zo scény1



Obr. 3.6 Snímka videa zo scény2

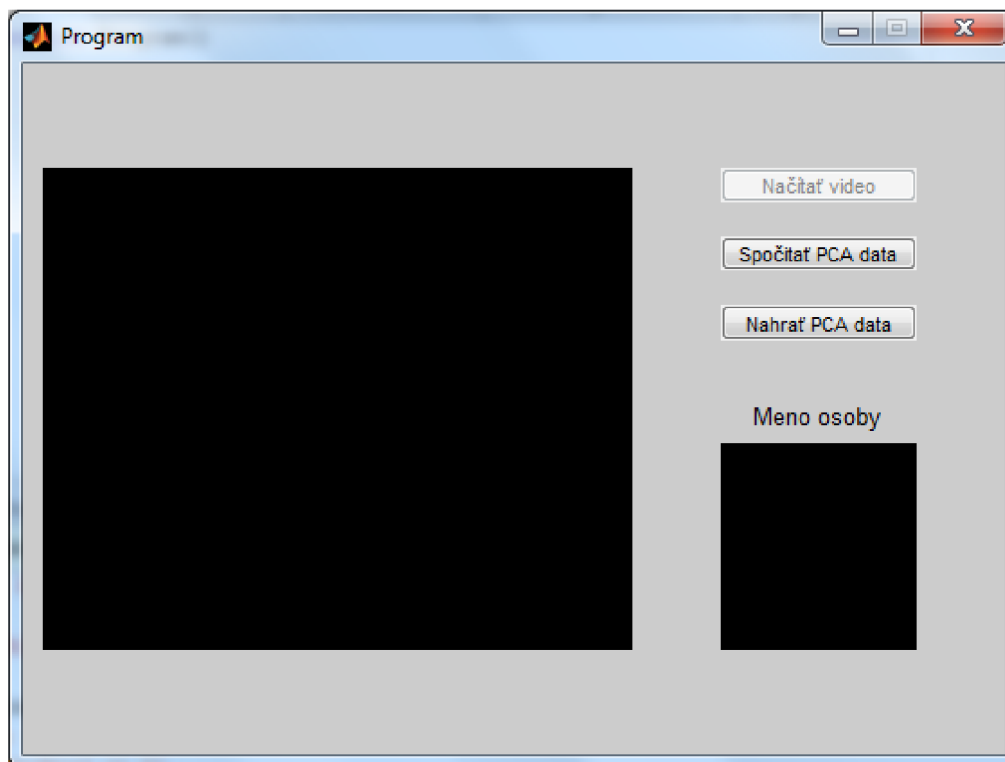
3.5 Implementácia metódy rozpoznávania tváre do programovacieho prostredia Matlab

Súčasťou diplomovej práce bolo vhodné implementovať vybranú metódu rozpoznávania tváre do programovacieho prostredia Matlab a otestovať ju na vytvorenej databáze videí. Pre túto úlohu bola vybratá metóda PCA, od ktorej sa mnohé ďalšie metódy odvíjajú. Princíp metódy je podrobne popísaný v kapitole 2.3.1. Pre znázornenie, ako vytvorený program pracuje, bol vytvorený vývojový diagram, ktorý je zobrazený na Obr. 3.7.



Obr. 3.7 Vývojový diagram programu

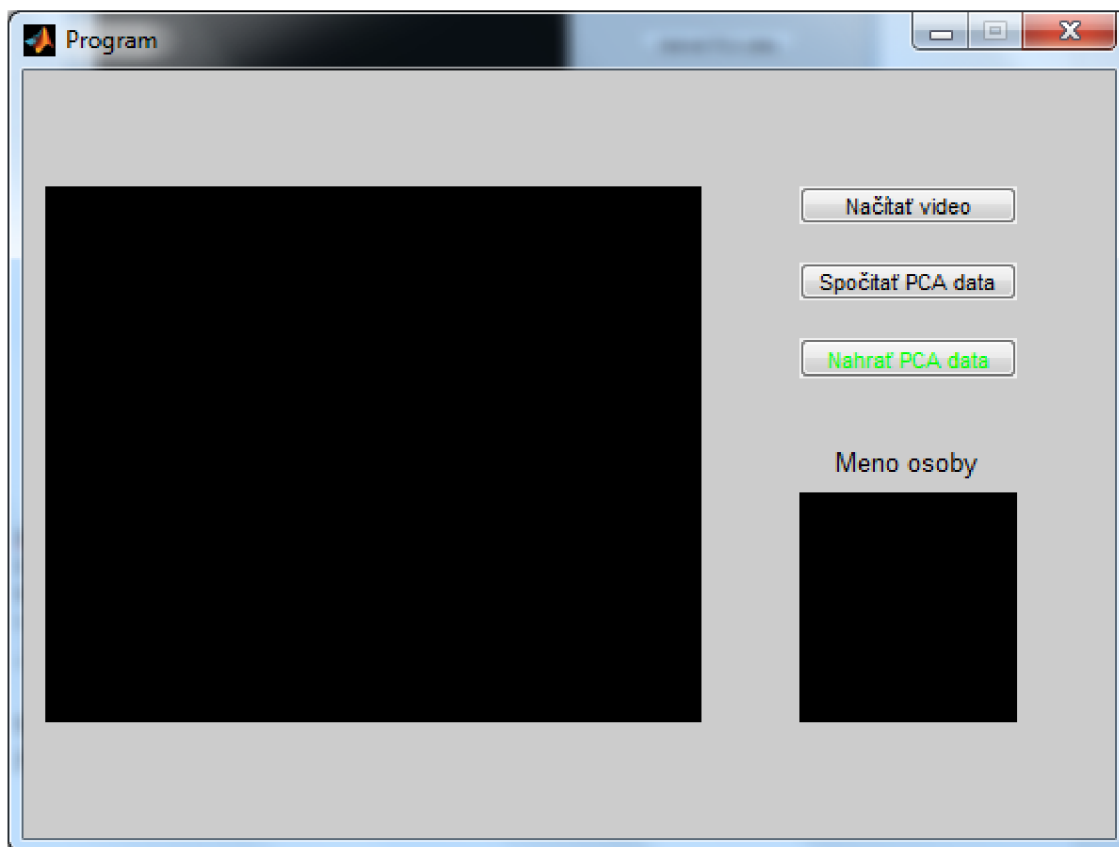
Pre jednoduchšie používanie a testovanie bolo vytvorené grafické užívateľské prostredie – GUI, ktoré sa otvorí po spustení skriptu s názvom „Program“. Okno užívateľského prostredia po spustení je zobrazené na Obr. 3.8.



Obr. 3.8 Grafické užívateľské prostredie vytvoreného programu

V prvom kroku si užívateľ môže zvoliť, či chce spočítať „eigenfaces“ z databázy snímok. Ak áno, klikne na tlačidlo „Spočítať PCA data“. Užívateľovi je povolené vybrať si z ľubovoľnej databázy, ktorú má v počítači vytvorenú. Spočítané hodnoty sa následne uložia ako súbor *PCAData.mat*. V prípade, že tento súbor už bol vytvorený, a snímky v databáze sa nemenili, je možné si hodnoty len načítať. V tom prípade sa klikne na „Nahrať PCA data“.

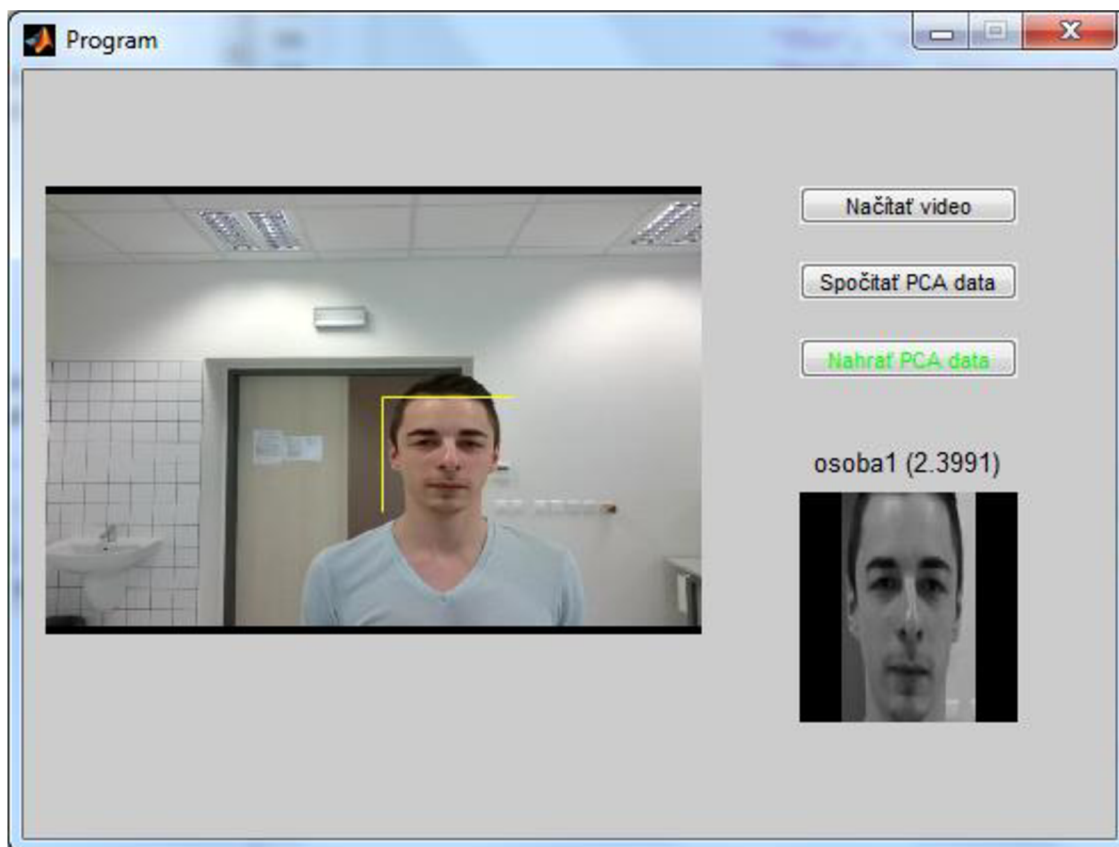
Po spočítaní, alebo nahratí PCA dát sa sprístupní tlačidlo „Načítať video“ a text na tlačidlo „Nahrať PCA data“ sa sfarbí do zelena, čo má značiť, že dáta sú nahrané. Opäť je možné načítať ľubovoľné video z databázy. Obrázok GUI-čka po nahratí dát je na Obr. 3.9.



Obr. 3.9 GUI po nahratí dát

Po načítaní videa sa spustí na pozadí celý proces analýzy videa. Najdlhším procesom je načítanie videa, pretože jednotlivé snímky videa sa nahrávajú do štruktúry, odkiaľ budú neskôr pri analýze volané. Keďže sú snímky farebné, tento proces potrebuje dostatočne veľkú pamäť RAM. Po načítaní sa spustí na prvom snímku detektor Viola-Jones. Ak sa deteguje tvár a má dostatočný počet bodov pre spustenie sledovacieho algoritmu KLT, detekcia tváre sa na nasledujúcom snímku nerobí. Ak sa počet sledovaných bodov zmenší pod 25, znova sa spustí detektor tváre. Na každom snímku, kde bola tvár detegovaná sa zistia súradnice polohy hlavy v rámci daného snímku. Tieto kroky sa robia v pozadí, pretože sú výpočtovo náročné, a video by pri priebežnom načítaní snímok nadmieru sekalo.

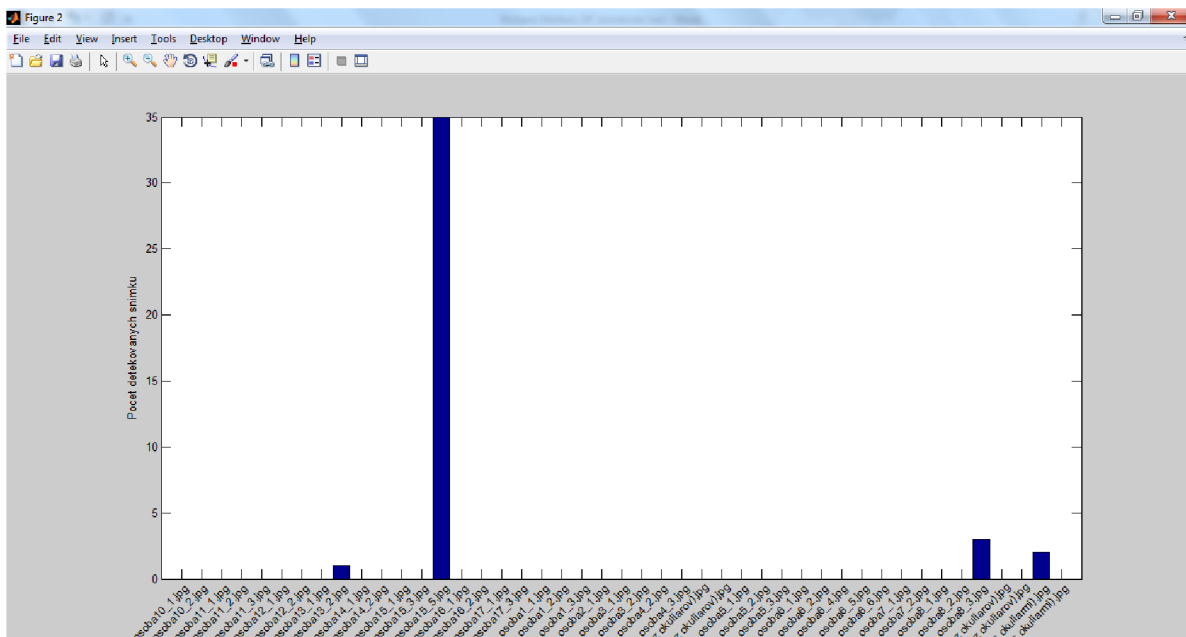
Po získaní súradníc tváre, môže byť aplikovaná metóda PCA aj na jednotlivé snímky videa a výsledné hodnoty sa nakoniec porovnajú na základe euklidovskej vzdialenosti s hodnotami snímok v databáze. Osoba, ktorá bola najčastejšie identifikovaná za osobu na videu sa vykreslí. Nad ňu sa vypíše, o ktorú osobu sa jedná, a aká bola jej priemerná euklidovská vzdialenosť k danej tvári. Vzdialenosť sa počíta ako priemerná hodnota z euklidovských vzdialeností identifikovanej osoby.



Obr. 3.10 Rozpoznaná osoba

Výsledkom činnosti programu je aj vytvorenie grafu, kde sa zobrazí početnosť, koľkokrát bola fotka z databázy označená ako daná osoba na videu. Tento graf sa vytvára z celého videa. Príklad je možné vidieť na Obr. 3.11.

Keďže testovacích osôb bolo pri scénke1 sedemnášť a pri scénke2 dvanášť, databáza obsahuje mnoho fotiek tvári. Preto je vhodné pre prehľadnosť grafu použiť napríklad pri scénke1 len snímky z priameho pohľadu osôb do snímacieho zariadenia. Ináč by nebolo na osi x-ovej možné rozoznať, o ktorú osobu sa jedná.



Obr. 3.11 Graf početnosti zhody fotiek z databázy s osobou na videu

Po skončení rozpoznávacieho procesu sa ešte uložia hodnoty euklidovských vzdialeností pre každý jeden snímok videa do tabuľky v Exceli pod názvom „*DistancaMatica.xls*“. Každý riadok v tabuľke vyjadruje jeden snímok z videa a stĺpce vyjadrujú osoby v poradí, ako sú uložené v databáze. Tento súbor by mohol slúžiť pre náhľad, aké sú rozdiely vo vzdialenostiach medzi tvárou na videu a jednotlivými osobami.

4 TESTOVANIE PROGRAMU

Testovanie programu bolo prevedené na vlastne vytvorených videách a snímkach, ktorých vytvorenie bolo popísané v kapitole 3.3 a 3.4. Ako prvé boli otestované videá pri priamom pohľade testovaných osôb do snímacieho zariadenia. Počet eigenfaces bol po testovaní v programe nastavený na hodnotu $0,2 \times \text{celkový počet snímkov v databáze}$, kde vykazoval proces rozpoznania najlepšie výsledky.

Z prvého testovania boli vytvorené tabuľky 4.1 a 4.2.

Tabuľka 4.1 : Výsledky rozpoznávacieho procesu scény1

video	Najčastejšie rozpoznaná tvár osoby	Priemerná euklidovská vzdialenosť k najčastejšie rozpoznanej osobe	Druhá najčastejšie rozpoznaná osoba
osoba1	osoba1	4,87	osoba15
osoba1_2	osoba8	9,31	osoba15
osoba2	osoba2	3,17	osoba8
osoba3	osoba3	3,28	-
osoba4	osoba4	4,82	osoba11
osoba4_2	osoba11	6,59	osoba4
osoba5	osoba5	8,30	osoba3
osoba5_2	osoba5	9,00	osoba3
osoba6	osoba6	3,28	osoba7
osoba6_2	osoba6	6,43	osoba7
osoba6_3	osoba6	2,93	osoba14
osoba7	osoba7	5,45	osoba1
osoba8	osoba8	2,56	osoba15
osoba9	osoba9	7,49	osoba15
osoba9_2	osoba9	6,75	osoba10
osoba10	osoba10	4,81	osoba8
osoba11	osoba11	3,71	osoba1
osoba12	osoba12	5,79	-
osoba13	osoba13	4,15	osoba14
osoba14	osoba14	3,68	-
osoba15	osoba15	7,28	osoba8
osoba15_2	osoba15	3,44	osoba8
osoba16	osoba16	3,69	-
osoba17	osoba17	3,13	osoba12

V prvej tabuľke je možné vidieť, že program rozpoznal nesprávne osobu len na videu s názvom „osoba1_2“ a „osoba4_2“. V prípade videa „osoba1_2“ program identifikoval na ako druhú najčastejšie rozpoznajú „osobu15“, čo stále nie je osoba, ktorá sa na videu nachádzala. Tento fakt mohol byť spôsobený hlavne tým, že toto

video sa natáčalo v iný deň, a v inej miestnosti ako ostatné a tvár osoby bola inak osvetlená ako v momente, keď sa tvorili fotky do databázy. Ako je možné vidieť aj najmenšia priemerná euklidovská vzdialenosť má najväčšiu hodnotu v tabuľke. Z tabuľky 4.3 sa ukazuje úspešnosť rozpoznania tohto videa len ako 38,71%, čo je najmenšia hodnota v tabuľke. Z tabuľky je ďalej možné vyčítať, že pri videu „osoba4_2“ je priemerná euklidovská vzdialenosť nesprávne rozpoznanej osoby menšia, ako pri ostatných videách, kde bolo rozpoznanie správne. U piatich správne rozpoznaných osôb je hodnota vzdialenosti vyššia. Táto chyba mohla vzniknúť z dôvodu približne rovnakých črt tváre daných osôb.

Tabuľka 4.2 : Úspešnosť správneho rozpoznania u scénky 1

Video	Správne rozpoznaná osoba (počet snímok)	Chybné rozpoznaná osoba (počet snímok)	Celkový počet snímok videa	Úspešnosť správneho rozpoznania (%)
osoba1	45	3	48	93,75
osoba1_2	12	19	31	38,71
osoba2	28	22	50	56,00
osoba3	36	0	36	100,00
osoba4	44	10	54	81,48
osoba4_2	31	20	51	60,78
osoba5	47	7	54	87,04
osoba5_2	29	10	39	74,36
osoba6	46	7	53	86,79
osoba6_2	30	15	45	66,67
osoba6_3	34	5	39	87,18
osoba7	37	10	47	78,72
osoba8	44	1	45	97,78
osoba9	50	5	55	90,91
osoba9_2	39	20	59	66,10
osoba10	38	6	44	86,36
osoba11	36	1	36	100,00
osoba12	49	0	49	100,00
osoba13	43	10	53	81,13
osoba14	58	0	58	100,00
osoba15	27	22	49	55,10
osoba15_2	35	6	41	85,37
osoba16	32	0	32	100,00
osoba17	28	7	35	80,00

Tabuľka 4.2 zobrazuje, na koľkých snímkach videa bola osoba identifikovaná správne a na koľkých bola zamenená s inou osobou. Z týchto hodnôt bola následne vypočítaná percentuálna úspešnosť programu. Najnižšia úspešnosť bola pri nesprávne identifikovanom videu „osoba1_2“ s hodnotou 38,71%. Úspešnosť 100% bola

dosiahnutá pri testovaní videí štyroch osôb. Celková priemerná úspešnosť rozpoznávania z celej databázy vyšla 81,43%.

Druhé testovanie bolo prevedené na databáze videí pomenovanej „scénka2“. Výsledky sú zobrazené v tabuľkách 4.3 a 4.4. Počet výsledných eigenfaces bol nastavený na hodnotu 0,8 x celkový počet snímok v databáze.

Tabuľka 4.3 Výsledky rozpoznávacieho procesu scénky1

video	Najčastejšie rozpoznaná tvár osoby	Priemerná euklidovská vzdialenosť k najčastejšie rozpoznanej osobe	Druhá najčastejšie rozpoznaná osoba
osoba1	osoba1	12,86	osoba9
osoba4	osoba4	14,48	osoba11
osoba5	osoba5	22,69	osoba6
osoba6	osoba6	16,58	osoba12
osoba7	osoba6	16,28	osoba7
osoba8	osoba7	19,50	osoba6
osoba9	osoba12	22,22	osoba1
osoba10	osoba10	12,35	osoba12
osoba11	osoba14	23,39	osoba8
osoba12	osoba12	15,20	osoba10
osoba13	osoba6	15,63	osoba1
osoba14	osoba6	21,08	osoba14

Z tabuľky 4.3 je možné vyčítať, že program označil osobu na videu za nesprávnu v 50-tich percentách.

Tabuľka 4.4 Úspešnosť správneho rozpoznania u scénky2

Video	Správne rozpoznaná osoba (počet snímok)	Chybne rozpoznaná osoba (počet snímok)	Celkový počet snímok videa	Úspešnosť správneho rozpoznania (%)
osoba1	9	19	28	32,14
osoba4	20	5	25	80,00
osoba5	10	2	12	83,33
osoba6	11	12	23	47,83
osoba7	5	38	43	11,63
osoba8	0	39	39	0,00
osoba9	5	36	41	12,20
osoba10	23	22	45	51,11
osoba11	2	13	15	13,33
osoba12	4	8	12	33,33
osoba13	0	37	37	0,00
osoba14	11	14	25	44,00

Podľa hodnôt vypočítaných z tabuľky 4.4 bola celková úspešnosť programu pre rozpoznanie tvárí na scénke2 len 38,02%.

U videí „osoba8“ a „osoba13“ nedošlo k rozpoznaní správnej osoby ani na jednom snímku. V prípade osoby13 to mohlo byť spôsobené tým, že daná osoba a aj osoba s ktorou si ju systém zamenil boli blondíny a mali približne rovnaké črty tváre. U osoby8 mohlo byť spôsobené nízkym rozlíšením detegovanej tváre, ktorá sa následne podobala na osobu7

5 DISKUSIA

Scénka1

Z výsledkov testovania programu je možné vidieť, že algoritmus na rozpoznanie tváre pri danej databáze snímok tváre pracoval pri čelnom pohľade spoľahlivo. Správne označiť osobu sa mu nepodarilo len v dvoch prípadoch, a to pri druhom videu osoby1, ktoré však bolo natáčané v iný deň, ako ostatné videá, a takisto v inej miestnosti. Pri detailnejšom pohľade na detegovanú tvár je možné vidieť, že tvár je osvetlená ináč, ako na ostatných videách, a potvrdzuje to teoretický predpoklad, že metóda PCA je veľmi citlivá na zmenu osvetlenia.

V druhom prípade chybného rozpoznania sa prejavila chyba metódy PCA, ktorá nezohľadňuje vnútrotriednu variabilitu. Pri detailnejšom preštudovaní výsledkov sa zistilo, že osoba11 bola rozpoznaná na videu 19-krát, čo bola najvyššia hodnota. Daná osoba vo videu však mala v databáze až 4 snímky tváre (fotografie s okuliarmi a fotografie bez okuliarov), a počet, koľkokrát ich algoritmus na celom videu rozpoznať je 31-krát, čo je viac, ako tvár, ku ktorej osobu na videu prirovnal. Túto chybu by bolo možné odstrániť využitím metódy LDA, kde sa vytvoria triedy, v ktorých je viac fotiek patriacich jednej osobe, a následne sa pracuje s nimi.

Pre dodržanie konštantného osvetlenia pri všetkých osobách, bola miestnosť zatemnená a využívalo sa umelé osvetlenie. Toto riešenie však nebolo úplne správne, pretože bodové žiariče pri chôdzi osvetľovali osobu vždy ináč, a na tvári sa vytvárali tieň. Riešením by mohlo byť konštantné prísvetľovanie osoby spredu, poprípade jeden silný bodový žiarič umiestnený na stene pred osobou, ktorý by nevytváral na tvári pri chôdzi tieň. Príklad vytváraného tieňa pod nosom je na Obr. 5.1. Odstránenie chyby meniaceho sa osvetlenia tváre by mohlo zabezpečiť, že tvár osoby v databáze by bola rovnaká v každej vzdialenosti osoby od snímacieho zariadenia. To by malo za následok zvýšenie úspešnosti rozpoznávacieho procesu.



Obr. 5.1 Tieň na tvári pri použití bodového zdroja svetla nad osobou

Druhým zásadným bodom pre úspešné rozpoznávanie bolo dodržať mierku rozpoznávanej tváre. Pri ručnom orezávaní fotiek pre získanie tváre do databázy bolo rozpoznávanie nepresné a výsledná fotka, ktorá mala vždy najväčšiu zhodu, bola tá, ktorá bola orezaná najpodobnejšie výrezu, ktorý deteguje algoritmus Viola-Jones. Preto bolo prístupné k získavaniu fotiek do databázy vyrezaním fotiek priamo zo snímok videí.

Ďalším dôležitým bodom, ktorý uberá na úspešnosti rozpoznávacieho procesu je pozadie za osobou. Snahou bolo snímať osobu pri vchode do miestnosti cez dvere, kde by sa dostala k snímaciemu zariadeniu. To sa ukázalo ako zlé riešenie, pretože pri chôdzi sa neustále menila poloha hlavy, a teda aj pozadie nasnímané za osobou. Túto chybu by bolo možné odstrániť orezaním tváre a odstránením pozadia, poprípade by mohlo byť snímacie zariadenie umiestnené oproti stene, na ktorej by sa nenachádzal žiaden objekt. V našom prípade sa vedľa osoby hlavy nachádzali vypínače svetiel, ktoré svojím usporiadaním pripomínali detekčnému algoritmu tvár, čo opäť viedlo ku skresleniu konečných výsledkov. Obrázok chybného detekcie tváre je na Obr. 5.2.



Obr. 5.2 Detegované vypínače svetiel

Faktorom ovplyvňujúcim úspešnosť rozpoznávania bola aj vzdialenosť osoby od snímacieho zariadenia na začiatku rozpoznávacieho procesu. Pri vzdialenosti viac ako 2 m bolo rozlíšenie snímky tak malé, že detekčný algoritmus síce tvár zaregistroval, avšak na danej tvári nebolo možné identifikovať žiadne detaily. Preto boli videá orezané a začiatok každého videa je približne v čase, kedy je už možné tvár rozpoznať. Riešením tohto problému by bolo natáčanie videa vo vyššom rozlíšení. K tomu by však bolo nutné pri využití vytvoreného algoritmu použiť výkonnejší počítač s väčšou pamäťou RAM. Na počítači s pamäťou 16 GB bolo možné spustiť aj video v HD kvalite, kde je rozlíšenie tváre väčšie aj pri väčšej vzdialenosti.

Úspešnosť vytvoreného programu je ťažké porovnať s inými metódami, pretože boli testované na iných videách. Je však možné spomenúť výsledok z článku [23], kde bola využitá metóda „Probabilistic Appearance Manifold“. Výsledok úspešnosti metódy bol definovaný ako podiel počtu snímok, kde bola identita správne rozpoznaná a počtu snímok vo všetkých testovaných videách. Úspešnosť popísanej metódy vyšla 92,1%. V [24] využitím metódy ARMA (z anglického autoregressive and moving average) dosiahli pri testovaní ich databázy úspešnosť rozpoznania viac než 90%. Úspešnosť metódy PCA použitej v tejto diplomovej práci je 81,43%.

Scénka2

Scénka2 bola natočená kvôli otestovanie algoritmu na bočných pohľadoch. Tu však algoritmus zlyhal vo väčšine prípadov. V tomto prípade bola snaha vytvoriť databázu fotiek tváří orezaním videí, kde osoba otáčala hlavou najprv do jednej a potom do druhej strany. Tieto videá však boli natočené v inej polohe snímacieho zariadenia, ako pri samotnom natáčaní videosekvencií. To spôsobilo iné osvetlenie tváre, ktoré ovplyvnilo aj samotné rozpoznanie (Obr. 5.3).



Obr. 5.3 Vľavo obrázok získaný orezaním videa pri statickej polohe osoby, vpravo obrázok získaný priamo z videa

Následne sa použil spôsob rovnaký ako pri získavaní fotiek pri prvej scénke, avšak tváre na jednotlivých snímkach sú značne rozmazané a v mnohých prípadoch kvôli chybnjej detekcii neúplné. Preto je databáza kombináciou databázy k scénke1, fotografií tvári vystrihnutých pri statickom natáčaní pohybov hlavy a niektorých fotiek, ktoré mali dostatočnú kvalitu pri získaní z videí pre scénku1.

Ako bolo spomenuté v predchádzajúcom odseku, problémom bola aj detekcia tváre, kde algoritmus Viola-Jones zlyháva pri väčšom naklonení tváre voči snímaciemu zariadeniu. Tento nedostatok by bolo možné odstrániť orezaním časti videa, kde by už algoritmus nebol schopný tvár detegovať. Avšak už samotná tvár, ktorú je pri natočení algoritmus ešte schopný detegovať je v mnohých prípadoch zle definovaná.

Rozpoznávacía úspešnosť metódy pri naklonení hlavy je veľmi nízka. Okrem vyššie spomínaných faktorov sa na zlom výsledku podieľal aj fakt, že nebolo možné natočiť úplne rovnaké videá pre každú osobu, pretože každá osoba mala inú rýchlosť chôdze, alebo vykonala inú trasu k snímaciemu zariadeniu. Pri rýchlej chôdzi fotoaparát nie vždy stihol osobu správne zaostriť a aj preto mohla byť tvár na videu rozmazaná.

Vytvorený program v prostredí Matlab

Program vytvorený v programovacom prostredí Matlab je vytvorený s ohľadom na výpočtové možnosti počítača, na ktorom bolo rozpoznávanie testované. Dôvodom, prečo rozpoznávanie tváre na video-sekvenciách prebieha na pozadí spusteného algoritmu je ten, že samotné operácie načítania a detekcie tváre sú výpočtovo náročné. Pri načítaní vždy len jedného snímku videa a následnej detekcii tváre by bolo prehrávanie videa pri danej konfigurácii počítača pomalé a zasekané.

Zhodnotenie

V závere je možné zhodnotiť, že metóda PCA nie je pre rozpoznanie tváre vo videu ideálna. Je ovplyvnená osvetlením tváre, ktoré sa však za normálnych okolností pri pohybe osoby mení. Takisto sa mení aj poloha tváre a pozadie za tvárou, ktoré by bolo pri statických fotografiách konštantné. Preto by bolo vhodnejšie využiť napríklad metódu ICA, ktorá by nemala byť na osvetlení až tak závislá, poprípade využiť spojenie metódy PCA s inou metódou, napríklad LDA, ktorá zohľadňuje vnútrotriednu variabilitu. To by však tiež nevyriešilo otázku chybnjej detekcie tváre pri väčšom naklonení tváre voči snímaciemu zariadeniu. A teda princíp vytvorený v tejto diplomovej práci nedokáže úspešne riešiť rozpoznanie tváre pri jej natočení o dostatočný uhol voči snímaciemu zariadeniu.

Ďalšou možnosťou, ako by sa dal program vylepšiť, by bolo zistenie prahu maximálnej euklidovskej vzdialenosti, kde po jeho prekročení by systém označil osobu ako neznámu. Program v tejto diplomovej práci identifikuje každú osobu a zisťuje len podobnosť najbližšej osoby. To by pri verifikačnom systéme bolo nedostačujúce, a nedochádzalo by tak k odmietnutiu cudzích osôb.

Ako samotný verifikačný prístroj na vpustenie osoby do kontrolovaného pásma by bolo aj po zavedení prahu 2D rozpoznávanie tváre metódou PCA nepostačujúce, pretože by na oklamanie systému bola dostatočná vytlačená fotografia danej osoby. Vhodnejšia by bola preto napríklad metóda 3D rozpoznania tváre.

6 ZÁVER

Úlohou tejto diplomovej práce bolo naštudovať si rôzne metódy rozpoznania tváre, ktoré sa v súčasnosti používajú, vyskúšať si implementáciu algoritmu na detekciu a rozpoznanie tváre a vytvoriť databázu videí, ktoré budú následne využité pri testovaní algoritmu slúžiaceho na rozpoznanie tváre.

Prvá kapitola bola venovaná teoretickému popisu biometrie, ku ktorej patrí aj samotné rozpoznanie tváří. Boli v nej vysvetlené najčastejšie používané pojmy, stručne charakterizované biometrické metódy, ktoré sa v súčasnosti najčastejšie využívajú, a takisto popísané parametre využívajúce sa na hodnotenie výkonnosti biometrického systému.

Druhá kapitola sa zaoberala teoretickým popisom procesu rozpoznávania tváre. Jednou z najdôležitejších častí rozpoznávania tváre je samotná detekcia. V práci bol vybraný detektor Viola-Jones, ktorý bol aj podrobnejšie popísaný. Metód na rozpoznanie tváre je mnoho a niektoré z nich boli v práci stručne popísané. Podrobnejšie bola popísaná metóda PCA, ktorá je následne implementovaná do programovacieho prostredia Matlab.

Tretia kapitola je praktická a je v nej ukážka detekcie implementovaného algoritmu Viola-Jones na snímkach z databáze AT&T. Potvrdilo sa, že úspešnosť detekcie tohto algoritmu je závislá na smeru pohľadu snímanej osoby. Pri tvárach, kde sa snímané osoby pozerali priamo do kamery bola detekcia bezchybná, avšak pri zväčšovaní uhlu natočenia hlavy voči kamere sa detekčná účinnosť algoritmu znižovala. Následne bol popísaný návrh snímania videosekvencií, na ktorých bola otestovaná metóda PCA pre rozpoznanie tváre. Výsledky testovania sú popísané v kapitole 4.

Posedná, priata kapitola sa zaoberá diskusiou k výsledkom práce a zhodnotení celkovej funkčnosti použitej metódy. Táto metóda patrí medzi staršie, avšak na statických snímkach dosahovala pomerne kvalitné výsledky, a pre svoju rýchlosť bola vybraná na implementáciu v tejto diplomovej práci. Pri pohybe osôb vo videách sa však prejavili jej limitácie, ktorými sú hlavne potreba konštantného osvetlenia a rovnakej polohy hlavy ako na testovacích snímkach. Využitie tejto metódy v praxi je hlavne kvôli spomínaným limitáciám obmedzené, a bolo by možné ju využiť v systémoch, kde nie je kladený veľký dôraz na presnosť.

LITERATÚRA

- [1] DRAHANSKÝ, M., ORSÁG, F. *Biometrie*. Vyd. 1. Brno: Computer press a.s., 2011, s. 294. ISBN 978-80-254-8979-6.
- [2] RAK, R., MATYÁŠ, F., ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Vyd. 1. Praha: Grada, 2008, s. 631. ISBN 978-80-247-2365-5.
- [3] ŠČUREK, R. *Biometrické metody identifikace osob v bezpečnostní praxi*. Studijní text. [online]. VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Oddělení bezpečnosti osob a majetku, 2008 [cit. 2015-12-09]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/040/.content/systems/resource/PDF/biometricke_metody.pdf
- [4] Daktyloskopia. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-12-09]. Dostupné z: <https://sk.wikipedia.org/wiki/Daktyloskopia>
- [5] *Signosoft s.r.o.* [online]. [cit. 2015-12-11]. Dostupné z: <http://www.signosoft.com/biometrickepodpisy.php>
- [6] MING-HSUAN YANG, D.J. KRIEGMAN a N. AHUJA. Detecting faces in images: a survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence* [online]. **24**(1): 34-58 [cit. 2016-01-04]. DOI: 10.1109/34.982883. ISSN 01628828. Dostupné z: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=982883>
- [7] JURÁČEK, A. *Lokalizace obličejů ve video sekvencích v reálném čase*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 77 s. Vedoucí diplomové práce Ing. Miloslav Richter, Ph.D.
- [8] HAUSER, V. *Rozpoznávání obličejů v obraze*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2012. 60 s. Vedoucí diplomové práce Ing. Kamil Říha, Ph.D.
- [9] PŘINOSIL, J. a M. KROLIKOWSKI. Využití detektoru Viola-Jones pro lokalizaci obličejů a očí v barevných obrazech. *Elektrorevue*. 2008, (31): 1-16. ISSN 1213-1539.
- [10] TSALAKANIDOU, Filareti, Sotiris MALASSIOTIS a Michael G. STRINTZIS. *Face Recognition - Face Detection, Global Approaches for, Feature Based Techniques, Problems and Considerations, Conclusions and Future Developments* [online]. [cit. 2016-01-04]. Dostupné z: <http://encyclopedia.jrank.org/articles/pages/6741/Face-Recognition.html>
- [11] JAFRI, Rabia a Hamid R. ARABNIA. A Survey of Face Recognition Techniques. *Journal of Information Processing Systems* [online]. 2009, **5**(2): 41-68 [cit. 2015-12-29]. DOI: 10.3745/JIPS.2009.5.2.041. ISSN 1976-913x. Dostupné z: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.446.3828&rep=rep1&type=pdf>
- [12] LI, Chang-Tsun. *Handbook of research on computational forensics, digital crime, and investigation: methods and solutions* [online]. Hershey, PA: Information Science Reference, c2010, s. 53-78 [cit. 2015-12-29]. ISBN 1605668370. Dostupné z: https://www2.warwick.ac.uk/fac/sci/dcs/people/abhir_bhalerao/publications/face-recognition-chapter.pdf.

- [13] TURK, Matthew a Alex PENTLAND. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience* [online]. 1991, 3(1): 71-86 [cit. 2015-12-30]. DOI: 10.1162/jocn.1991.3.1.71. ISSN 0898-929x. Dostupné z: <http://www.face-rec.org/algorithms/PCA/jcn.pdf>
- [14] DRAPER, Bruce A., Kyungim BAEK, Marian Stewart BARTLETT a J.Ross BEVERIDGE. Recognizing faces with PCA and ICA. *Computer Vision and Image Understanding* [online]. 2003,91(1-2): 115-137 [cit. 2015-12-30]. DOI: 10.1016/S1077-3142(03)00077-8. ISSN 10773142. Dostupné z: http://www.cc.gatech.edu/~isbell/reading/papers/draper_cvui03.pdf
- [15] DUBSKÝ M. *Simulace biometrických zabezpečovacích systémů pracujících na principu rozpoznávání tváře*. VUT v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2008. 85 str. Diplomová práce. Vedoucí práce ing. Hicham Atassi.
- [16] MAHMUD, Firoz, Mst. Taskia KHATUN, Syed Tauhid ZUHORI, Shyla AFROGE, Mumu AKTAR a Biprodip PAL. Face recognition using Principle Component Analysis and Linear Discriminant Analysis. *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)* [online]. IEEE, 2015, : 1-4 [cit. 2016-01-04]. DOI: 10.1109/ICEEICT.2015.7307518. ISBN 978-1-4673-6676-2. Dostupné z: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7307518>
- [17] Face Detection and Tracking Using the KLT Algorithm. In: *MathWorks* [online]. United States [cit. 2016-05-15]. Dostupné z: <http://www.mathworks.com/help/vision/examples/face-detection-and-tracking-using-the-klt-algorithm.html?requestedDomain=www.mathworks.com>
- [18] KUMAR, Sanjeev a Harpreet KAUR. FACE RECOGNITION TECHNIQUES: CLASSIFICATION AND COMPARISONS. *International Journal of Information Technology and Knowledge Management* [online]. 2012, 5(2), 361-363 [cit. 2016-05-15]. ISSN 0973-4414. Dostupné z: http://www.csjournals.com/IJITKM/PDF%205-2/26_Sanjeev_Kumar.pdf
- [19] AHONEN, T., A. HADID a M. PIETIKAINEN. Face Description with Local Binary Patterns: Application to Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence* [online]. 2006, 28(12), 2037-2041 [cit. 2016-05-15]. DOI: 10.1109/TPAMI.2006.244. ISSN 0162-8828. Dostupné z: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1717463>
- [20] CHE-HUA, Yeh, Pei-Ruu SHIH, Kuan-Ting LIU, Huang-Ming CHANG a Ming OUHYOUNG. *A Comparison of Three Methods of Face Recognition for Home Photos* [online]. [cit. 2016-05-15]. Dostupné z: <http://www.cmlab.csie.ntu.edu.tw/~sakurawars/img/Poster2009.pdf>. National Taiwan University.
- [21] SOLANKI, Dhavalsinh V. a Ashish M. KOTHARI. A Survey on Face Recognition Techniques and its Applications. *Journal of Image Processing & Pattern Recognition Progress* [online]. 2014, 1(3), 1-6 [cit. 2016-05-17]. ISSN 2394-1995. Dostupné z: http://www.academia.edu/10065628/Face_Recognition_Techniques
- [22] Online Video Cutter. *123APPS* [online]. [cit. 2016-05-17]. Dostupné z: <http://online-video-cutter.com/>
- [23] KUANG-CHIH LEE, J. HO, MING-HSUAN YANG a D. KRIEGMAN. Video-based face recognition using probabilistic appearance manifolds. *2003 IEEE Computer Society*

- Conference on Computer Vision and Pattern Recognition, 2003. Proceedings*[online]. IEEE Comput. Soc, 2003, , I-313-I-320 [cit. 2016-05-20]. DOI: 10.1109/CVPR.2003.1211369. ISBN 0-7695-1900-8. Dostupné z: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1211369>
- [24] AGGARWAL, G., A.K.R. CHOWDHURY, R. CHELLAPPA a D. KRIEGMAN. A system identification approach for video-based face recognition. *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004* [online]. IEEE, 2004, , 175-178 Vol.4 [cit. 2016-05-20]. DOI: 10.1109/ICPR.2004.1333732. ISBN 0-7695-2128-2. Dostupné z: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1333732>
- [25] FileExchange: rotateXLabels(ax, angle, varargin). *MathWorks* [online]. [cit. 2016-05-20]. Dostupné z: <http://www.mathworks.com/matlabcentral/fileexchange/27812-rotate-x-axis-tick-labels/content/rotateXLabels.m>

ZOZNAM SKRATIEK

IT	Information technology
FAR	False Acceptance Rate – miera chybného prijatia
FRR	False Rejection Rate – miera chybného odmietnutia
FMR	False Match Rate – miera chybnnej zhody
FNMR	False Non-Match Rate – miera chybnnej nezhody
EER	Equal Error Rate – miera vyrovnania chýb
FTA	Failure to Acquire – miera neschopnosti nasnímať
FTE	Failure to Enroll – miera neschopnosti zaregistrovať
FTM	Failure to Match – miera neschopnosti porovnať
ROC	Receiver Operating Curve
PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
SVM	Support Vector Machines
ASM	Active Shape Model
AAM	Active Appearance Model
EBGM	Elastic Bunch Graph Matching
LBP	Local Binary Pattern
ICA	Independent Component Analysis
Mpx	Megapixel
HD	High-definition
2D	Dvojdimenziálny priestor
3D	Trojdimenziálny priestor
ARMA	Autoregressive and moving average
KLT	Kanade-Lucas-Tomasi algoritmus

PRÍLOHA

Príloha stručne popisuje funkcie v Matlabe vytvorené pre rozpoznanie tváre, ktoré sú súčasťou praktickej časti tejto diplomovej práce.

- `Program.m` – táto funkcia slúži na spustenie programu. Po spustení sa otvorí GUI, z ktorého sa volajú všetky ostatné funkcie
- `ImageRead.m` – funkcia slúži na načítanie snímok z databázy
- `VideoRead.m` – funkcia slúži na načítanie videa
- `KLT.m` - táto funkcia slúži na detegovanie tváre a jej následné sledovanie využitím algoritmu KTL. Vznikla úpravou funkcií voľne dostupných na stránke Matlabu
- `PCA.m` – funkcia slúži na výpočet vektorov podpriestoru PCA zo snímok v databáze a následne aj zo snímok tváre zistených vo videu
- `CalculatePCADData.m` - funkcia slúži k výpočtu eigenfaces
- `LoadPCADData.m` - funkcia slúži na načítanie súboru s uloženými hodnotami PCA analýzy vstupnej databáze
- `FaceRecognition.m` – funkcia slúži na vyhodnotenie podobnosti tváre na videu s tvármi v databáze
- `rotateXLabels.m` - táto funkcia slúži na natočenie popiskov v osi x a je prevzatá z [25]