Aspekty biometrické identifikace osob s využitím rozpoznávání tváře

Aspects of biometric identification of people with usage of face recognition

Svozil Lukáš

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš SVOZIL**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Aspekty biometrické identifikace osob s využitím rozpoznávání tváře**

Zásady pro vypracování:

1. **Proveďte rešerši současného stavu řešení biometrické identifikace osob s využitím rozpoznávání tváře.**
2. **Možnosti použití rozpoznávacích systémů.**
3. **Zhodnocení používaných algoritmů.**
4. **V závěru práce zhodnoťte identifikační systém IRIS 2200, jímž ústav disponuje a naznačte další vývoj.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Křeček a kol. : Příručka zabezpečovací techniky, Blatná: Blatenská tiskárna, 2003, ISBN 80-902938-2-4**
2. **Vít, V., Kuba, P.: Televizní technika, 1. vyd., nakladatelství BEN, 2002, ISBN 80-86056-88-0**
3. **SONKA M., HLAVAC V., BOYLE R. Image Processing, Analysis, and Machine Vision. 2.vyd. PWS Publishing, Pacific Grove, 1999. ISBN 0-534-95393-X.**
4. **HLAVÁČ V., SEDLÁČEK M. Zpracování signálů a obrazů. Praha: Vydavatelství ČVUT, 2000. ISBN 80-01-03110-1.**
5. **Http://web.mvcr.cz/archiv2008/casopisy/kriminalistika/2003/03_01/hinner.html [online]. 2003 [cit. 2009-02-03]. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/casopisy/kriminalistika/2003/03_01/hinner.html>.**
6. **Http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf [online]. 2008 [cit. 2008-02-03]. Dostupný z WWW: <http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf>.**

Vedoucí bakalářské práce: **Ing. Rudolf Drga**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Bakalářská práce bude řešit problematiku hodnocení současného stavu řešení biometrické identifikace osob s využitím rozpoznávání tváře. Hodnoceny budou jednotlivé možnosti. Závěr práce bude tvořit zhodnocení identifikačního systému IRIS 2200, jímž ústav disponuje.

Klíčová slova: Biometrie, Biometrická identifikace, Rozpoznávání tváře, Identifikace tváře, Verifikace tváře, Biometrická šablona

ABSTRACT

This bachelor thesis deals with summarizing of present state of biometrical identification of people using a face recognition. Individual possibilities will be evaluated. The end of the thesis is about summarizing of identification system IRIS 2200, which is available at our department.

Keywords: Biometrics, Biometrical identification, face recognition, face identification, face verification, biometric template

Na tomto místě bych rád poděkoval svému vedoucímu bakalářské práce panu ing. Rudolfovi Drgovi, za jeho odborné rady, připomínky a konzultace. Dále bych chtěl poděkovat své rodině a přítelkyni za podporu po celou dobu během mých studií.

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/a jsem seznámen/a 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.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Jednou u nejvíce probíraných otázek dnešní doby je bezpečnost. Snažíme se co nejúčinněji zabezpečit nejen své domy, automobily. Mnohem vyšší poptávka je v komerční a státní sféře. Je potřeba efektivně zabezpečit rozsáhlé komplexy podniků, státní budovy, finanční domy. Stranou nezůstává ani doprava a celní kontroly. Zejména tyto dva úseky se staly po 11. Září 2009 nejčastěji spojovanou oblastí s pojmem bezpečnost.

Biometrické systémy na tomto poli sehrávají velmi důležitou roli. Mezi nejvíce používané systémy patří verifikace duhovky, identifikace otisku prstů a také verifikace obličeje. V této práci se budu zabývat právě zmíněnou biometrickou metodou verifikace obličeje. Rozpoznávání podle tváře lidé využívají odnepaměti. Nejprve samozřejmě nešlo o počítačovou metodu, ale o přirozenou schopnost lidí rozeznat své blízké a známé osoby. O počátcích automatizovaného rozpoznávání tváře se bavíme v 60. letech 20. století. Tento vývoj byl velmi závislý na vývoji výpočetní a snímací techniky. Největší pokrok se udál za posledních 15 let. Za tuto dobu si již našel své místo v komerční bezpečnosti, kde s touto metodou začalo experimentovat.

Verifikace obličeje má velmi široké spektrum využití. Kontrola vstupu do budov, monitorování veřejného prostranství, při kterém nás může systém upozornit na zájmovou osobu ve snímaném prostoru, celní kontroly, biometrické pasy atd. Využití tohoto systému samozřejmě závisí na kvalitě použitého zařízení a programu na rozpoznávání obličeje. Vývoj této biometrické metody je však ještě ve svých počátcích a většinou probíhá pouze jen zkušební provoz těchto systémů.

Dále se budu zabývat jednotlivými druhy přístupu k počítačovému rozpoznávání tváří. Mezi nejvíce prozkoumané algoritmy patří LDA, PCA, EBGM.

V praktické části bakalářské práce zhodnotím systém Access Vision 4 a porovnám jej s jiným biometrickým zařízením a to čtečkou otisku prstů V- Pass. Zhodnocení budu provádět pro FRR, neboli pravděpodobnost chybného odmítnutí, o kterém se v práci taky zmiňuji.

I. TEORETICKÁ ČÁST

1 BIOMETRIE

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. behaviorálních charakteristik. Pojem biometrika je odvozený z řeckých slov "bios" a "metron". První znamená "život", druhé pak "měřit, měření". Kdybychom se chtěli držet doslovného překladu, zněla by biometrie jako "měření živého". V přeneseném významu jde ovšem o měření a rozpoznávání určitých charakteristik člověka.[3]

Obr. 1. Biometrie[13]

1.1 Historie biometrie

Aniž by si to lidé uvědomili, podstatu biometrie využívali od nepaměti. V dávných dobách žili v malých komunitách a společenstvích, kde neměli sebevětší problém se vzájemně rozeznat. Využívali totiž tzv. vizuální biometrickou identifikaci, kterou samozřejmě využíváme i my nyní. Jedná se totiž o základní vlastnost, která je přirozená každému člověku. Nejen tvář, ale také rozdílný hlas, fyzické proporce, nebo výrazné zranění a handicapy byly nápomocny lidem rozeznat totožnost obyvatele stejného území.

Tyto metody přestávaly být úspěšné při větší migraci osob, kdy bylo již nemožné znát všechny lidi. Vznikla nutnost bezpečně rozpoznat a identifikovat osoby jinými metodami.

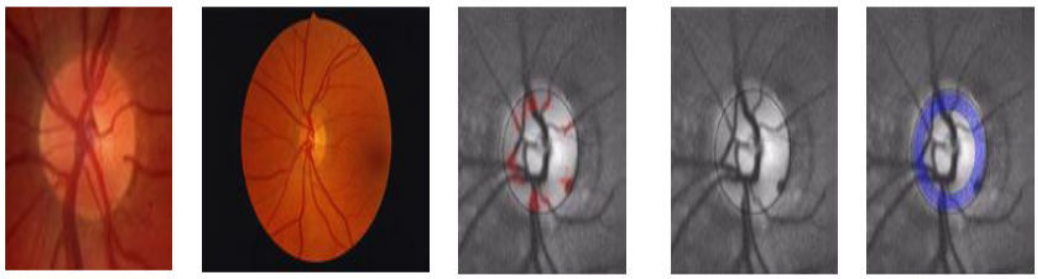
První zmínky o tzv. komerčním využití biometrické identifikaci pocházejí z doby faraona vládnoucího v Egyptě. Při vyplácení mezd zde byli lidé identifikováni, aby nedošlo k vícenásobnému vydání odměny týž osobě. Rozpoznáváni byli podle fyzických proporcí, podle barvy očí a různých zranění.

Obyvatelé Babylónu a Persie zase používali obdobu dnešní daktyloskopie. Pro identifikaci používali otisk palce na hliněnou tabulku, kterým stvrzovali obchodní a kupní smlouvy.

Nás bude v první řadě zajímat novodobá historie využití biometrie k identifikaci osob v komerční oblasti. Pro tuto oblast je velmi důležitý nástup výpočetní techniky ve 20. století a její využití v jednotlivých oblastech biometrické identifikace.

V 70. letech 20. století byla daktyloskopie poprvé realizována na počítačích. V dnešní době probíhá snímání otisků prstů v převážné většině na výpočetní technice. Nejprve byla tato technologie využívána pouze pro soudní praxi, policejní a bezpečnostní účely, ovšem později se uplatnila také v systémech kontroly vstupu do objektů a budov.

Další metodou, která byla v roce 1980 nově použita, je identifikace pomocí struktury sítnice.



Obr. 2. Identifikace pomocí struktury sítnice[3]

Verifikace obličeje, které se budeme více věnovat v dalších kapitolách, patří mezi „mladší“ využívané metody. Další techniky na sebe nenechali dlouho čekat a také si vydobyly své postavení v biometrických oborech. S obrovským rozšířením a vývojem výpočetní techniky v 90. letech 20. století nastal velký rozmach a rozvoj biometrických metod. V dnešní době by bylo nemožné si bez výpočetní techniky biometrickou identifikaci vůbec představit.

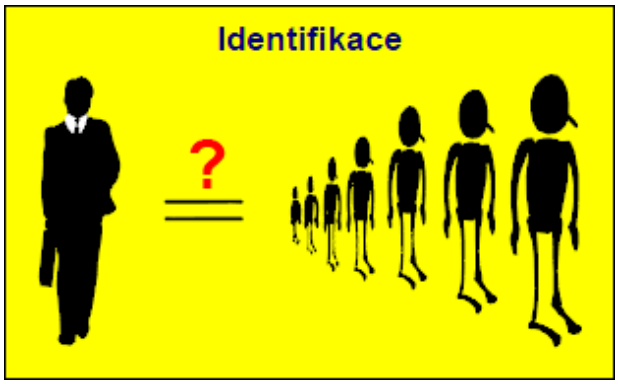
1.2 Základní pojmy v biometrii

V oboru biometrie se setkáváme se spoustou cizojazyčných výrazů, které mají převážně původ v anglickém jazyce. Tyto výrazy je třeba správně překládat do češtiny, aby nedocházelo k nesprávnému pochopení daného pojmu a tím i nesprávnému porozumění

dané problematiky. Pojem biometrie jsme si osvětlili v předešlém textu, tak se nyní zaměříme na výrazy identifikace, verifikace, rekognoskace a autentizace.

1.2.1 Identifikace

Pochází z anglického slova „identification“. Jedná se o proces, kdy se biometrické systém pokouší určit totožnost neznámého jedince. Biometrická informace je sejmuta a porovnávána se všemi uloženými vzorky (šablonami). Princip je znám jako one-to-many.[3]



Obr. 3. Identifikace[14]

1.2.2 Verifikace

V anglickém jazyce verification. Označuje nám proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku s již dříve zapsaným (tzv. šablonou neboli template). Jedná se o tzv. princip one-to-one.[3]

Obr. 4. Verifikace[14]

1.2.3 Rekognoskace (rozpoznávání)

V anglickém překladu recognition. Nazýváme jím druhový termín, který nutně nemusí znamenat identifikaci ani verifikaci. Jedná se o rozpoznávání člověka použitím vhodné tělesné vlastnosti. [3]

1.2.4 Autentizace

Authentication překládáme jako autentizace a jedná se o pojem, který lze sloučit s termínem rozpoznávání. Ovšem na konci procesu v tomto případě získá uživatel určitý status, např. oprávněný/neoprávněný atd.[3]

2 KRITÉRIA PRO BIOMETRICKOU IDENTIFIKACI

Biometrické identifikační systémy pracují s předem určenými biologickými, nebo behaviorálními vlastnostmi lidí. Aby technologie byla efektivní, systémy i měřené biometrické vlastnosti osob musí splňovat aspekty, bez nichž by měření bylo nemožné či nepřijatelné.

2.1 Biometrické kritéria uživatelů

Máme tím na mysli biologické a behaviorální kritéria, které jsou vyžadovány jednotlivými biometrickými metodami.

- Jedinečnost: je základem všech biometrických systémů, bez které by nemohly fungovat. Jedná se o unikátní vlastnosti lidí, které jsou u každého člověka jedinečné, originální a u jiného jedince se nevyskytují ve stejných hodnotách.
- Univerzálnost: Myslíme tím, že se vlastnost musí vyskytovat u co největšího počtu lidí, aby bylo možné provádět biometrické měření danou metodou.
- Trvalost: Vybíráme takové vlastnosti, které jsou během času stálé a neměnné.
- Měřitelnost: Tyto vlastnosti musí být měřitelné za použití stejných technických prostředků.
- Uživatelská přijatelnost

2.2 Kritéria biometrických systémů

Také dané biometrické systémy a aplikace musí splňovat podmínky, aby byly v praxi efektivní. Tyto kritéria rozdělíme:

- Operační
- Finanční
- Technické

2.2.1 Operační kritéria

Jsou důležité pro uživatele, ať už ojedinělé, nebo zejména ty, kteří používají biometrické aplikace každý den (při příchodu do práce), či několikrát denně (při přihlašování do počítače, systému atd.).

Patří sem především:

- **Uživatelská přijatelnost** – Nejdůležitější vlastností Biometrického systému. Celý proces identifikace/verifikace musí být přijatelný pro vysoký počet lidí po stránce osobní, společenské, sociální, náboženské, politické, etické, atd.
- **Spolehlivost** – Snímání, ukládání a uchování biometrické informace musí být kdykoliv zopakovatelné se stejnými výsledky.
- **Praktičnost** – Uživatel by měl být průběhem co nejméně obtěžován a zdržován. Celý proces by měl jednoduchý, jasný a zřetelný, nevyžadující přílišnou pozornost.

2.2.2 Finanční kritéria

Finanční záležitosti vždy patřili a patřit budou faktorem, který rozhodne o případném nákupu zařízení. Zákazník by však měl brát na zřetel i následné provozní náklady.

Zajímají nás tyto faktory:

- Pořizovací cena technologie
- Cena instalace
- Náklady spojené s uvedením do provozu – školení, trénink
- Cena následných upgradů, nových modifikací
- Cena logistické podpory a provozu
- Cena návazných systémů (počítačových, fyzické ostrahy, atd.)
- Cena dalších zamýšlených zařízení, budoucího rozvoje systému
- Cena obsluhy zařízení [1]

2.2.3 Technická kritéria

Mezi nejčastější vyhodnocovací kritéria v oblasti biometrické identifikace obvykle patří následující charakteristiky:

- Minimální čas zpracování/vyhodnocení identifikačních charakteristik
- Přijatelná chybovost
- Odolnost
- Efektivnost
- Výkonnost
- Standardizace (kompatibilita s ostatními systémy)
- Skladovatelnost identifikačních charakteristik
- Požadovaný prostor pro uložení a zpracování identifikačních charakteristik
- Přesnost
- Jednoduchost [1]

3 MĚŘENÍ SPOLEHLIVOSTI BIOMETRICKÝCH SYSTÉMŮ

Pokud budeme vybírat zařízení biometrické identifikace, zjistíme, že na trhu je jich spousta druhů, které se od sebe na první pohled neliší. Rozhodovat se můžeme mezi různými biometrickými metodami, nebo zařízeními pracujícími na stejném fyzikálním principu, avšak od odlišného výrobce. Je potřeba zhodnotit velké množství faktorů, které nám pomohou vybrat tu nejlepší možnost. Kritéria, kterými budeme porovnávat jednotlivé systémy, můžeme rozdělit na hlavní a vedlejší. Mezi vedlejší zařadíme rychlost zpracování samotného porovnání, kapacitní možnosti (počet realizovaných identifikací/verifikací v určité časové jednotce), uživatelskou přijatelnost, cenu, bezporuchovou spolehlivost zařízení, odolnost vůči opotřebování atd.

Jelikož biometrické zařízení jsou systémy především bezpečnostní, tak hlavním kritériem je správné rozpoznání oprávněného uživatele a správné odmítnutí neznámé osoby. Mohou nastat případy, kdy systém nerozpozná osobu, která má oprávnění pro vstup do daného objektu. Opačným případem je, když systém vpustí do objektu neoprávněnou osobu.

V praxi poté pracujeme s pravděpodobností obou zmíněných negativních a tedy nežádoucích jevů. V průběhu let byly zavedeny dva základní pojmy:

- **Pravděpodobnost chybného odmítnutí** (autorizované osoby) biometrickým zařízením, v anglickém překladu **False Rejction Rate (FRR)**. Používá se také pojem Type Error Rate (chyba 1. typu).
- **Pravděpodobnost chybného přijetí** (neoprávněné osoby), označována též **False Acceptance Rate (FAR)**, nebo ekvivalentně Type II Error Rate (chyba 2. typu).

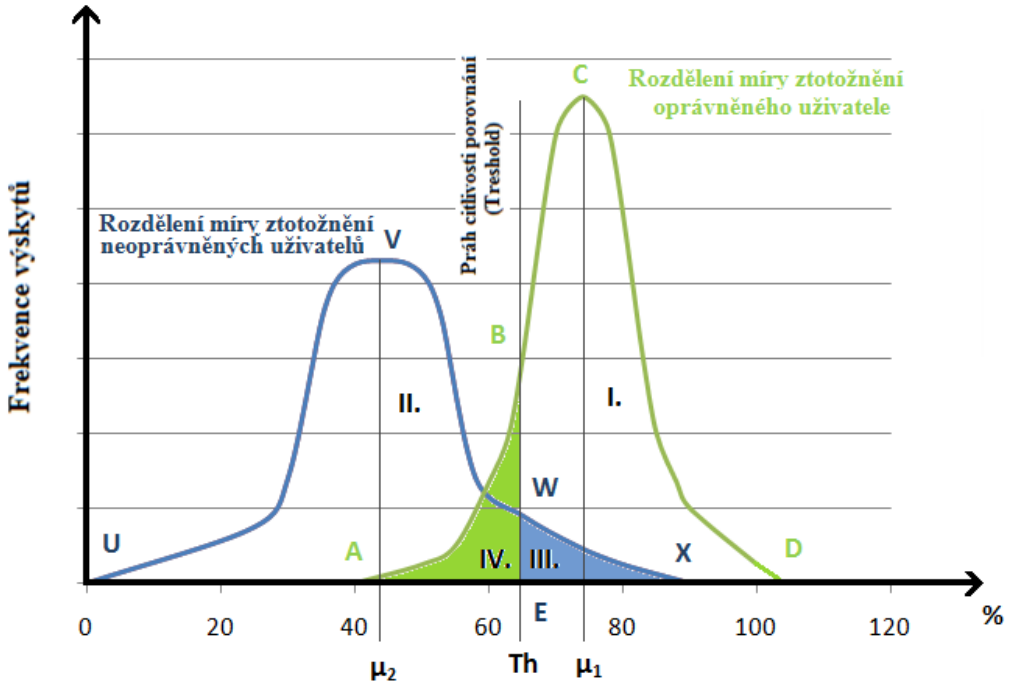
Biometrické metody identifikace/verifikace jsou založeny na statistickém vyhodnocování podobnosti biometrického vzoru a biometrické šablony. Při každém snímání biometrického vzorku nejsou zaznamenávány absolutně stejné hodnoty, stejné markanty pořizovaných charakteristik. V důsledku se pak i obě porovnávané šablony nepatrně liší. Míra ztotožnění je pak pokaždé odlišná a závisí především na každé biometrické aplikaci a jejím technickým řešením. [1]

V praxi je pak možné pro každé konkrétní zařízení graficky vyjádřit závislost četnosti míry ztotožnění osob, které se podrobují identifikaci nebo verifikaci. Tyto závislosti jsou

graficky zpracovány v Obr. 5. pro dvě skupiny osob, kterým odpovídají dvě křivky rozdělení.

První křivkou procházející (procházející postupně body A, B, C, D) je rozdělení četností výsledků porovnání jednoho a téhož oprávněného uživatele, který se násobně podrobil identifikačnímu/verifikačnímu procesu.

Aplikace má nastavený určitý práh citlivosti (přímka EB, kolmá na osu x), který společně s oběma křivkami rozděluje plochu do čtyř oblastí, označených I. Až IV. Oprávněný uživatel, jenž má výsledek porovnání vyšší než práh citlivosti, je aplikací akceptován; v opačném případě je odmítnut. Neoprávnění uživatelé, jež mají výsledek porovnání vyšší než citlivostní práh, jsou rovněž aplikací akceptováni. Při hodnotě nižší jsou taktéž odmítáni, stejně jako oprávnění uživatelé. [1]



Obr. 5. Výsledek porovnání – míra ztotožnění

O čtyřech oblastech mžeme tedy říci:

- Oblast, která je dána plochou $P_{E,\ B,\ C,\ D,\ E}$ představuje korektní akceptaci oprávněného uživatele, tj. uživatel s aplikací spokojen, protože byl správně rozpoznán.
- Oblast PU, V, W, E, U znamená korektní odmítnutí neoprávněného uživatele, který je ovšem nespokojen, protože se mu nepodařilo proniknout do aplikace.
- PW, X, E, W je oblastí nekorektního odmítnutí neoprávněného uživatele. Ten je spokojen, protože překonal aplikaci. Nespokojený je ale správce aplikace, protože k bezpečnostnímu incidentu.
- Oblast P A, B, E, A vyjadřuje oblast nekorektního odmítnutí oprávněného uživatele. Uživatel není spokojen, protože aplikace není spolehlivá a nerozpoznala jej. Odmítnut musí být pouze neoprávněný uživatel.

O tom, zda je uživatel oprávněný, rozhoduje míra ztotožnění biometrických vzorků. [1]

3.1 Pravděpodobnost chybného odmítnutí (False Rejection Rate- FRR)

Pravděpodobnost chybného odmítnutí, nebo také Chyba I. druhu je jedním z bezpečnostních kritérií biometrických systémů. Udává pravděpodobnost, s jakou bude zařízení chybovat a neidentifikuje/neverifikuje oprávněného uživatele, přestože uživatel má v aplikaci již uloženou svou biometrickou šablonu. Z tohoto důvodu je uživatel nucen opakovaně se identifikovat/verifikovat.

Pravděpodobnost chybného odmítnutí je dána vztahem:

$$FRR=(N_{FR}/N_{EIA}).100\ [\%] \qquad FRR=(N_{FR}/N_{EVA}).100\ [\%] \qquad (1)$$

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).

Z bezpečnostního hlediska tato chyba nemá v osobních aplikacích velký význam. K žádnému bezpečnostnímu ohrožení nedojde, pouze se může stát, že oprávněné osoby

nejsou rozpoznány. Jde spíše o nežádoucí jev pro uživatele. Ti poté musejí opakovat proces identifikace, přestože mají garantovaný vstup. S rostoucím počtem FRR klesá u zákazníků důvěra v zařízení, jelikož identifikace se může stát obtěžujícím procesem. Jiný význam má však FRR v policejních a soudních praxích, kde se jedná o závažný nežádoucí jev. Pachatel, který má být identifikován, je systémem milně nerozpoznán, tudíž vypadá z okruhu vyšetřovaných osob.

3.2 Pravděpodobnost chybného přijetí (False Acceptance Rate – FAR)

V literatuře ji můžeme objevit také pod názvem Chyba II. Druhu. Jestliže FRR nemá na bezpečnost v komerčním sektoru veliký význam, tak u FAR je to právě naopak. Jedná se o situaci, kdy biometrické zařízení nesprávně vyhodnotí cizí osobu jako registrovanou v systému a vpustí ji do objektu, nebo aplikace, přestože tato k tomu nemá oprávnění. Může se jednat o pachatele, kterému byla milně přiřazena biometrická šablona již zavedeného uživatele. V mnohých případech jsou útoky na systémy cílené a promyšlené, o to je situace nebezpečnější, když je systém oklamán. Pravděpodobnost chybného přijetí je závažným nedostatkem, který může mít nedozírné následky, ať už finančního, společenského nebo jiného charakteru.

Pravděpodobnost chybného přijetí FAR je dána vztahem:

$$FAR=(N_{FA}/N_{IIA}).100\ [\%] \qquad FAR=(N_{FA}/N_{IVA}).100\ [\%] \qquad (2)$$

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)

V policejních a soudních aplikacích má FAR opět trochu odlišný význam. Dojde-li milně k identifikování nesprávné osoby, pro tuto mohou vzniknout nepříjemnosti. Také případné vyšetřování celého případu by se mohlo uchýlit klamným směrem.

3.3 Přesnější výpočty chybovosti

Výpočet FRR a FAR předpokládá, že počty chyb i počty pokusů o identifikaci/verifikaci jsou vyrovnané. Nyní si uvedeme přesnější metody pro výpočet pravděpodobnosti chyb.

3.3.1 Failure to Enroll Rate (FTE nebo FER)

Jedná se o skutečnost, kdy uživatel nemůže být zaregistrován do biometrického systému. Tento fakt se týká lidí s určitým deficitem, jako je například chybějící prst, slepota atd. FER udává poměr osob, u kterých selhal proces sejmutí vlastnosti. Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti, která se snímá. Lze poté určit i tzn. osobní FER (Personál FER) udávající vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání. V případě, že byla uživateli správně sejmuta biometrická vlastnost, avšak systém ho chybně odmítl i po mnoha identifikačních/verifikačních pokusech, mluvíme o tzv. Koeficientu selhání přístupu FTA (Failure To Acquire). Abychom získali spolehlivé statistické údaje, je nutno provést velké množství pokusů o sejmutí biometrické vlastnosti. Pravděpodobnost neúspěchu sejmutí vlastnosti konkrétní osoby se vypočte podle vzorce. [3]

FER(n) = počet neúspěšných pokusů o zápis u 1 osoby/celkový počet pokusů o zápis u 1 osoby

Čím více pokusů provedeme, tím lepší hodnoty nám vycházejí. Celkové FER pro N účastníků (uživatelů) je definován jako průměr z FER (n) podle vzorce. [3]

$$FER = \frac{1}{N} \cdot \sum_{n-1}^{N} FER(n) \tag{3}$$

Čím více uživatelů se bude započítávat, tím přesnější hodnoty nám budou vycházet.[3]

3.3.2 False Identification Rate (FIR)

Koeficient FIR udává pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně přiřazena k některému referenčnímu vzorku. Přesná definice závisí na principu, kterým se přiřazuje pořízený vzorek k referenčnímu, jelikož se často stává, že po srovnávacím procesu vyhovuje více než jeden referenční vzorek, tzn., překračuje rozhodovací práh. [3]

3.3.3 False Match rate (FMR)

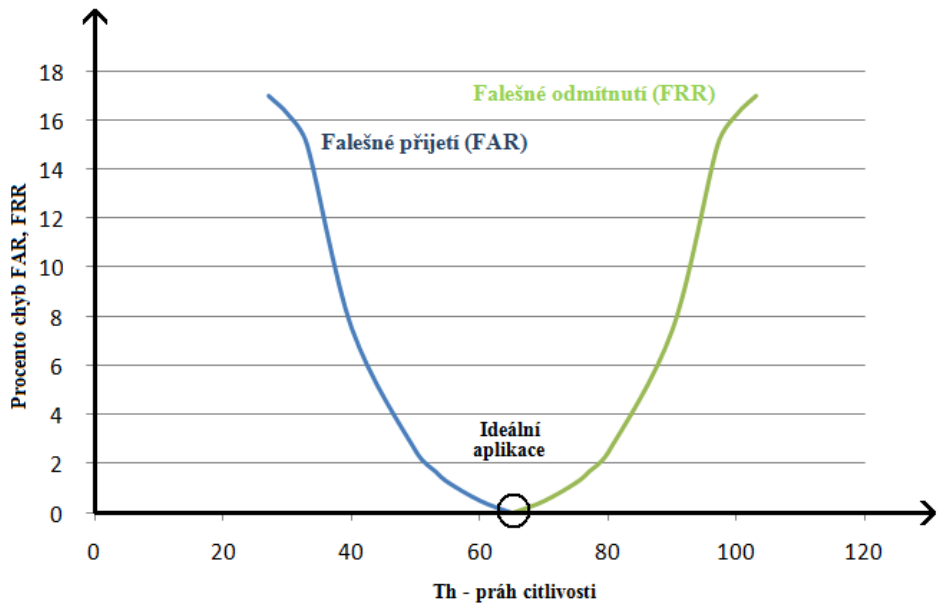
Koeficient FIR udává poměr neoprávněných osob, které jsou nesprávně rozpoznány jako akreditované během srovnávacího procesu. Porovnáme-li ho s koeficientem FAR, liší se v tom, že na rozdíl od FAR se do FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Znamená to tedy, že koeficienty FAR a FRR jsou více závislé na způsobu používání biometrického zařízení, tzn., nesprávně rozpoznané biometrické vlastnosti tyto koeficienty zhoršují. [3]

3.3.4 False Non-Match Rate (FNMR)

Koeficient FNMR udává poměr toho, že oprávněné osoby jsou nesprávně nerozpoznány během srovnávacího procesu. V porovnání s FRR se liší v tom, že se nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. [3]

3.4 Vztah FRR a FAR

Pokud budeme uvažovat o aplikaci, která nebude vykazovat žádné falešné odmítnutí, ani žádné falešné přijetí, můžeme mluvit o tzv. ideální aplikaci (viz. Obr. 5). Jednalo by se tedy o rovnost mezi FRR a FAR. Takové aplikace ovšem v praxi nemáme. [3]

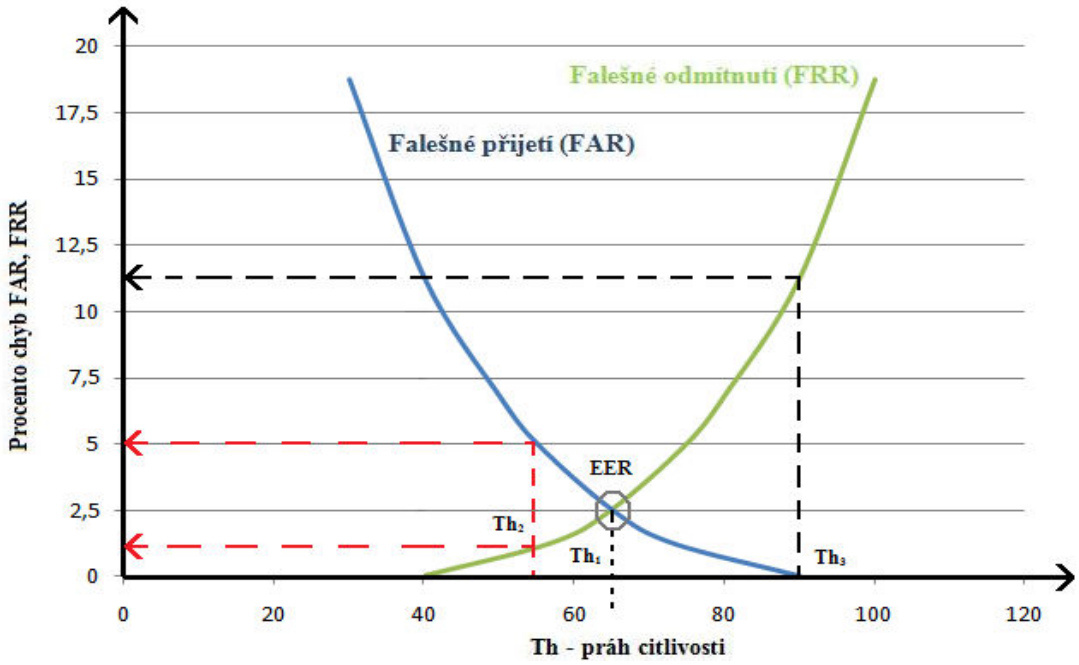


Obr. 6. Ideální biometrická aplikace

Důležitým pojmem při měření efektivnosti (výkonnosti) biometrických systémů je tzv. křížový koeficient, udávající, s jakou pravděpodobností při jakém nastavení hranice rozhodování nastane jev FAR a FFR současně (tzn. FAR=FFR). Křížový koeficient EER (Equal error rate) je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR. [3]

Je-li FAR koeficientem bezpečnosti a FRR koeficientem komfortu, je zřejmé, že ve chvíli kdy jsou v rovnováze, je v rovnováze i celkové nastavení systému (viz Obr. 6).

Z Obr. 6 je zřejmé, že se křivky FAR a FRR chovají významově proti sobě. Jestliže budeme požadovat žádné falešné přijetí osoby, nastavíme FAR na hodnotu 0. V tom případě se nám změní i FRR na hodnotu zhruba 11,9% (viz Obr. 6). Pokud nastavíme citlivost na 54, dostaneme hodnoty FAR= 5% a FRR= 1,25%.



Obr. 7. Reálná biometrická aplikace

3.4.1 Receiver Operating Characterics (ROC)

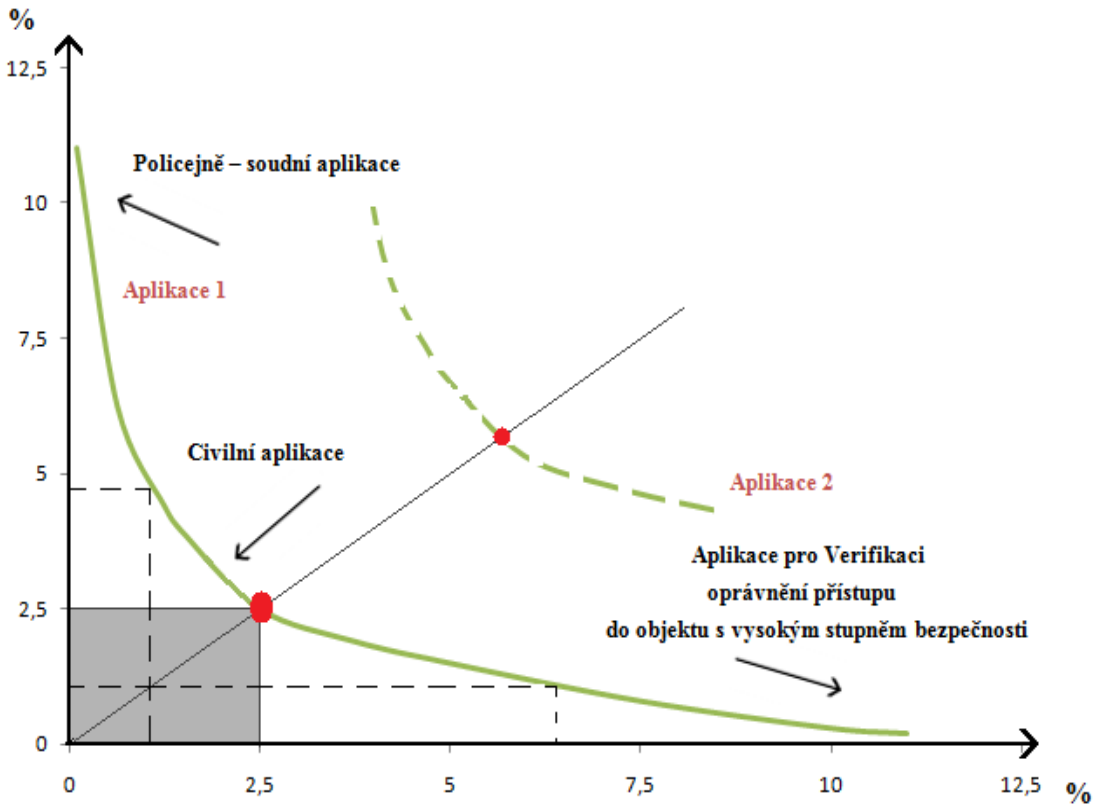
Pomocí křivky ROC můžeme snáze a objektivně porovnávat kvalitu jednotlivých, biometrický systémů. Jedná se o graf, ze kterého vyčteme vzájemný vztah

pravděpodobností chybného přijetí a chybného odmítnutí. Equal Error Rate (ERR) je nazýván bod, kde se protínají křivky FRR a FAR.

Pro bod ERR platí:

$$FRR=FAR \tag{4}$$

Jak už bylo řečeno, tato záležitost slouží pouze pro srovnání biometrických aplikací. V praxi ERR nastavujeme podle požadavků uživatele, pro které je systém instalován. Obyčejní uživatelé ocení spíše nižší práh citlivosti pro přijatelnější pracovní vlastnosti. Naopak bankovní a vládní instituce popřípadě vojenské objekty budou požadovat na prvním místě vysokou bezpečnost. Znamená to že FRR se sníží a Far zvýší. Fakt, že dojde k nerozpoznání oprávněného uživatele je přijatelnější než chybné vpuštění cizí osoby.



Obr. 8. Reciving Operating Characteristics – Závislost FAR a FRR.

4 VERIFIKACE OBLIČEJE

Identifikace osob pomocí rozpoznávání obličeje, je biometrická metoda, kterou lidé využívají odnepaměti. Schopnost rozpoznat své přátele, členy rodiny, spolužáky, kolegy v práci, sousedy, považujeme za zcela přirozenou. Jedná se o automatický proces, při kterém náš mozek porovnává obraz uložený v paměti s předlohou, kterou má před sebou. Celý tento proces, můžeme říci identifikační, trvá jen zlomek vteřiny. Osoby nám velmi blízké jsme schopni rozpoznat z fotografií pořízených za velmi špatných světelných podmínek.

Obr. 9. 3D model obličeje[13]

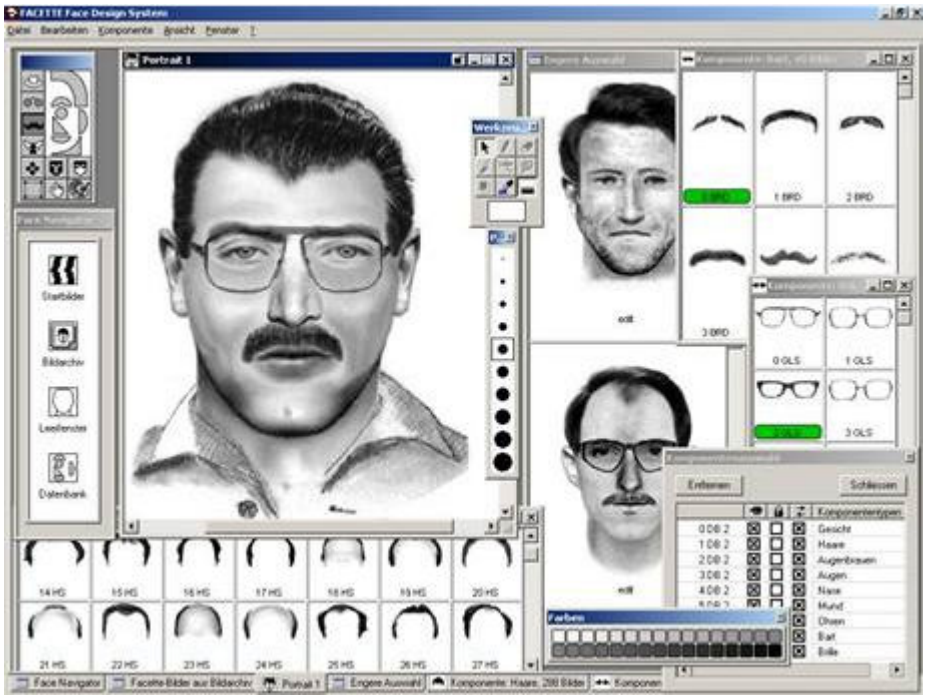
4.1 Historie identifikace osob na základě rozpoznání tváře

Identifikací osob podle tváře se již po desetiletí velmi intenzivně zabývá policie. V policejní a soudní praxi používáme spíše pojem portrétní identifikace, přičemž se jedná o samostatnou vědní disciplínu. První zmínky o použití obdoby této současné

kriminalistické metody nacházíme již kolem roku 1880 ve Francii. Většího rozkvětu se portrétní identifikace dočkala ve 20. století, kdy byla tato metoda podrobněji vědecky zkoumána. I proto bylo nalezeno hned několik způsobu identifikace a jejich vývoj byl docela rychlý. V první polovině minulého století profesionální kreslíř sestavoval obraz podle výslechu obětí, nebo svědků. V 60. letech, byla využívána tzv. metoda skládaného portrétu. Na podsvětlenou desku byly přikládány folie jednotlivých částí tváře (oči, nos, ústa, obočí, uši, atd…).

Obr. 10. Skládaný portrét používaný v 60. Letech[15]

Portrétní identifikace byla značně ovlivněna, tak jako i jiné vědní disciplíny, nástupem výpočetní techniky. Začaly se používat standardizované softwary, které jsou neustále zdokonalovány.



Obr. 11. Program pro tvorbu podoby pachatele[15]

Ve stínu portrétní identifikace se postupně začala od 60. let 20. století vyvíjet pozdější počítačová metoda rozpoznávání obličeje, která byla dobře využitelná v komerční oblasti. Její vývoj byl závislý na kvalitě výpočetní techniky. Za posledních 15 let se na poli rozvoje biometrické metody rozpoznávání tváře udál obrovský pokrok. Význam této metody neobyčejně vzrostl po 11. září 2001.

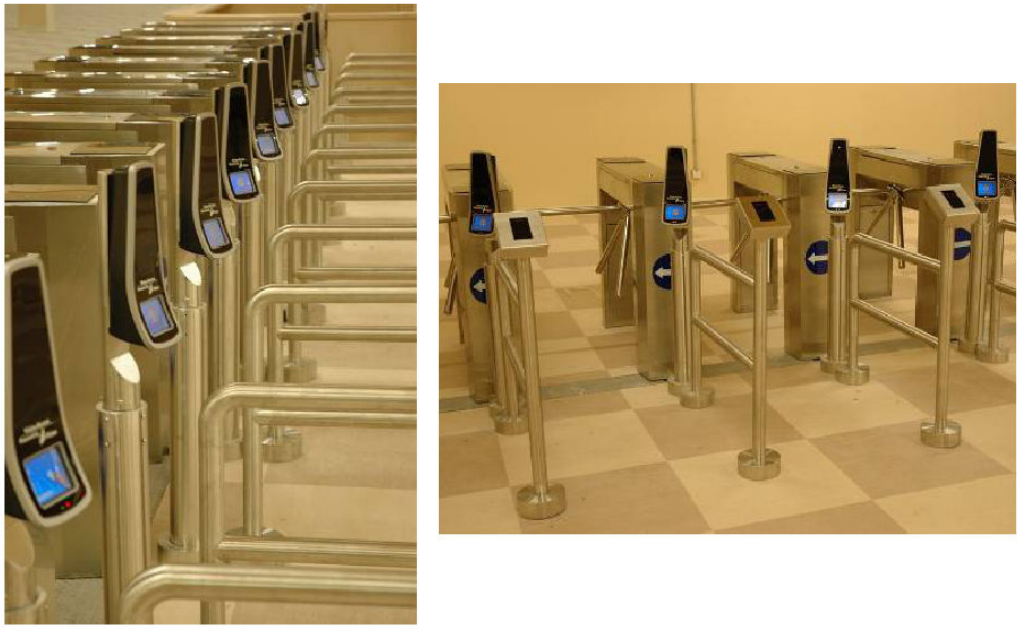
Jak už bylo řečeno tak portrétní identifikace se používá v policejní a soudní praxi. Jedná se o zpětné zhotovení tváře podezřelé osoby. Metoda biometrické identifikace osob nazvána rozpoznávání obličeje má v praxi zcela jiný význam. Jedná se o okamžité počítačové rozpoznání obličeje osob, na snímané scéně, ze kterého je okamžitě vyvozen důsledek.

4.2 Využití rozpoznávání tváře v praxi

Rozpoznávání obličeje se mezi biometrickými metodami řadí k mladším metodám identifikace osob. Jak již bylo řečeno v předchozí kapitole, velkým zlomem v poptávce po verifikaci tváře byl teroristický útok ze dne 11. 9. 2001. Důvodem byla nezbytnost nějakým způsobem zvýšit bezpečnost v hromadné dopravě, zejména v leteckém provozu, v ochraně státních i soukromých budov, při mapování veřejné scény před vandalismem, zločinci a samozřejmě zvýšení bezpečnostních požadavků při celní kontrole, která jsou úzce spjata

s již zmíněným leteckým provozem. Rozpoznání obličeje by mohlo zastávat v těchto opatřeních velmi důležitou roli. Metoda verifikace tváře má oproti jiným systémům biometrické identifikace několik výhod avšak prozatím i nedostatků. Hlavním záporem je úspěšnost či neúspěšnost verifikace. Někteří výrobci udávají úspěšnost správné identifikace i 90%, avšak v konečném součtu všech systémů to nevypadá příliš růžově. Systémy jsou zatím ve větší míře převážně v testovacím provozu. Vhodnou variantou je skloubení této biometrické metody s jinými bezpečnostními opatřeními, jako je použití čipových karet, hesel atd.

Pokud se zaměříme na předpoklady, které by v budoucnu měli upřednostňovat použití verifikace obličeje, na první pohled značným faktem je pasivní charakter systému. Máme tím na mysli, že není potřeba vyvíjet speciální aktivitu vedoucí k prokázání totožnosti, jako u jiných rozpoznávacích metod. Kamery umístěné u vstupů do chráněných prostor budov a objektů nevyžadují žádný fyzický kontakt se zařízením a verifikace trvá jen pár vteřin.



Obr. 12. Kontrola vstupu[13]

Lidé si mohou tento způsob identifikace velmi rychle osvojit, neboť jim ubude každodenní složitější proces prokazování své identity. Také přímý kontakt se zařízením (např. otisky

prstů, nebo obraz krevního řečiště), se po čase může stát pro mnohé uživatele obtěžujícím procesem. Tady se dostáváme k další výhodě. Při snímání otisků prstů, je potřeba často čistit snímač, tento druh údržby u kamer samozřejmě odpadá. Neposlední výhodou je fakt, že k systémům identifikace osob na základě tváře můžeme použít již stávající CCTV. Kamery mají všestranné využití. Nejen že poskytuje obrazový záznam, ale dokáže nás upozornit na zájmovou osobu ve snímaném prostoru. Tato skutečnost je důležitá zejména ve forezní praxi.

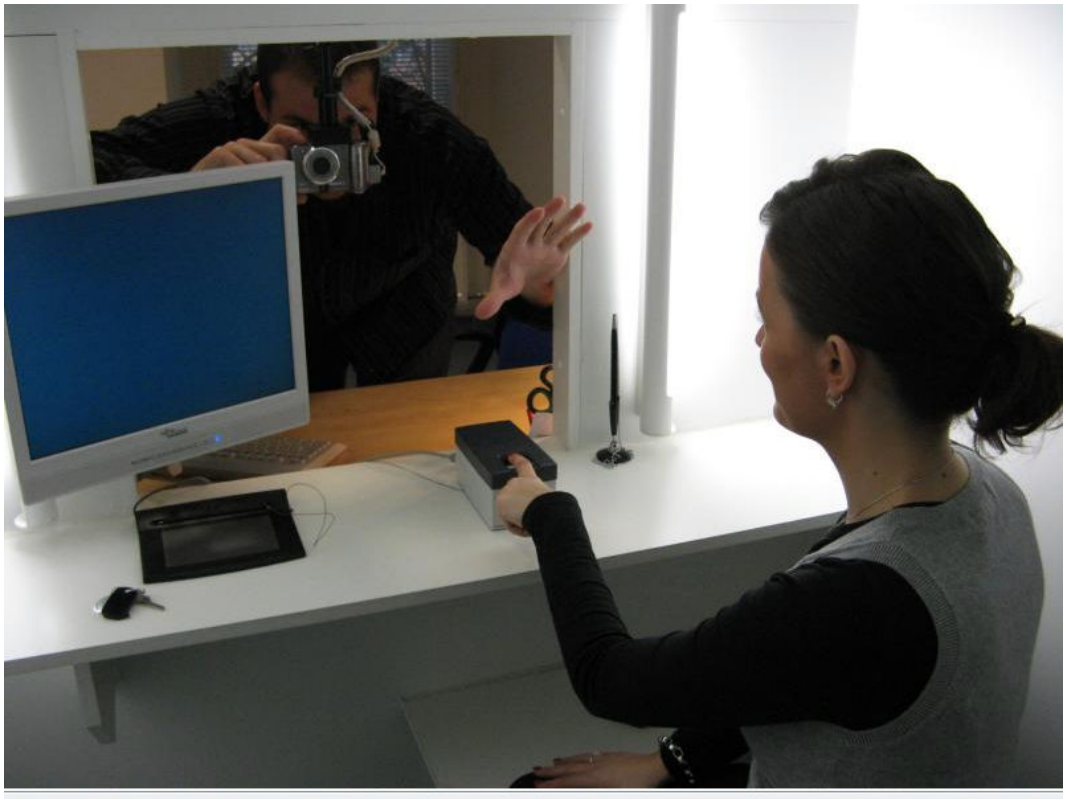
Obr. 13. Kamera snímající prostor[8]

Také je potřeba zmínit, že některým lidem může být pocit, že jsou natáčeni velmi nepříjemný. Samozřejmě, v prostoru si většina z nás kamer ani nepovšimne, ale pokud jsou umístěné u vstupu do budov, či objektu může nastat problém. Proces, při kterém je osoba zjevně snímána z menší vzdálenosti, například u turniketu při vstupu do chráněného prostoru, se může zdát některým z nás velmi nepříjemné. Lidem připadá obraz jejich tváře uložený v systému, jako mnohem větší vpád do soukromí, než uložené data krevního řečiště či otisku prstu. Spousta z nás také nemá ráda, když jsou fotografováni, nebo obecně když na ně míří objektiv. Tento pocit vyvolává taky identifikační proces, který se pro tyto

osoby stává velmi nepříjemným. Těchto negativních reakcí je naštěstí zanedbatelné minimum.

4.2.1 Celní kontroly

Dnešní svět s sebou nese stálou hrozbu teroristických útoků a nelegální migrace osob po celém světě. Je to dáno současným moderním stylem života na naší planetě, který nese jméno Globalizace. Vzdálenosti mezi jednotlivými zeměmi a kontinenty se stávají díky letecké dopravě zanedbatelným pojmem. Celní kontroly jsou proto jedny z hlavních preventivních opatření, které mohou zamezit páchání trestné činnosti. Vysoké požadavky na bezpečnost, kvalitní identifikaci totožnosti a rychlost odbavení ke všem těmto aspektům může značně přispět biometrická metoda verifikace tváře.



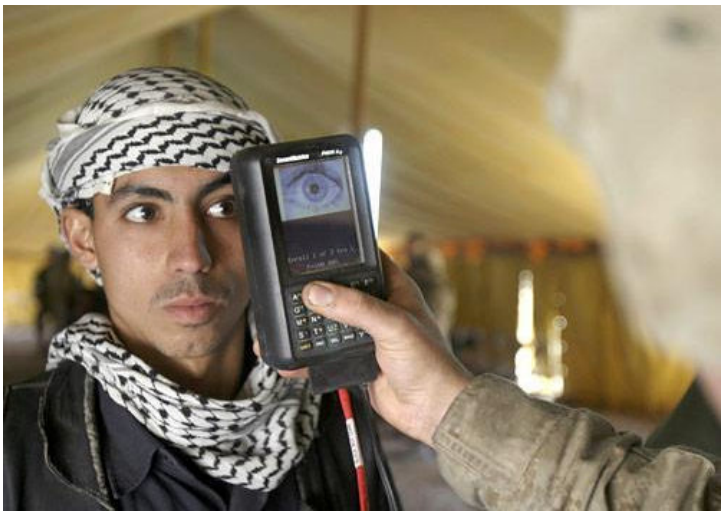
Obr. 14. Ukládání biometrické šablony[19]

Biometrické identifikace osob s využitím rozpoznávání tváře používá zatím malý počet cestujících. Jedná se o dobrovolníky, kteří pravidelně využívají mezinárodní letecké linky.

Jejich odměnou je rychlost a pohodlí při odbavování. Tento druh identifikace může být na letištích použit v mnoha různých aplikacích. Jedna z možností je mapování odbavovacího prostoru zavazadel. Při odložení zavazadla je pořízena fotka majitele a ta je poté porovnána s osobou, která kufr vyzvedává. Zpětně můžeme také zkrátit čas nalezení zavazadla, které bylo odevzdáno k odbavení podezřelou osobou. Dochází také k případům, kdy se záměrně zamění osoby v transitním prostoru a nastoupí do jiného letadla. Této ilegální migraci lze zabránit snímáním tváře těsně při vstupu do letadla, kde bude obličej porovnán s předlohou získanou při odbavení. Velké problémy by ovšem jistě způsobil systém, který by nebyl plně spolehlivý. Mohlo by se stát, že jednou za čas by byl některý z cestujících milně označen za černého pasažéra, to by mu jistě způsobilo přinejmenším nepříjemnosti.

Zaměstnanci na letištích jsou další skupinou, která využívá verifikaci obličeje k přístupu do jednotlivých částí letiště. Prvním letištěm, které začalo využívat verifikaci obličeje při celní kontrole svých zaměstnanců, bylo v roce 2002 australské Sydney. Systém porovnával obličej osoby s fotografií v pasu. Úspěšný provoz systému však neměl příliš dlouhé trvání. Dva zaměstnanci asijského původu se rozhodli, že systém prověří. Vyměnili si pasy a pokusili se verifikovat. Systém je oba bez problému vpustil, čímž hodně utrpěl na dobré pověsti.

Pásmo Gazy každodenně překračuje více jako 50 tisíc lidí cestujících za prací do sousední země. Zde jsou využívány biometrické systémy geometrie ruky, verifikace duhovky a rozpoznání tváře. Všechny údaje se ukládají na identifikační čipové karty jednotlivce.



Obr. 15. Celní kontrola[3]

4.2.2 Ochrana vstupů do budov, a další možné aplikace

Vysoké nároky na bezpečnost vyžadují samozřejmě v první řadě banky, finanční budovy hotely, kasina atd. Banky a finanční instituce využívají rozpoznávání obličeje pro kontrolu vstupu a pohybu osob v objektu. Jedná se o klasické režimové opatření, kdy má každý zaměstnanec odlišné oprávnění vstupu do různých prostor (trezor, pokladna, archív, atd.). Použitím biometrické identifikace odpadá riziko odcizení čipových karet, klíčů, nebo jiných tokenů, které by pachateli umožnili vstup do střežených prostor.

Obr. 16. Kontrola vstupů do kanceláří[13]

Herna a kasina využívají identifikaci tváře k odhalení problémových návštěvníků. Všechny prostory těchto provozoven jsou monitorovány. Osoba, se kterou jsou problémy, je zpětně vyhledána na záznamu a její tvář je uložena do systému. Při její další návštěvě je obsluha upozorněna kamerovým systémem na přítomnost nežádoucí osoby. Herny a kasina, které spolu vzájemně spolupracují, si předávají informace o těchto nežádaných klientech. Z toho vyplívá, navštíví-li tato osoba jiný podnik, jeho personál je již při jejím vstupu upozorněna systémem a může podniknout patřičné kroky k udržení pořádku.

Stejnou aplikaci využívají i obchodní řetězce, které si zrovna tak předávají biometrické informace o zlodějích v prodejnách. Krádež může být odhalena až po zavírací době. To ovšem není problém k vytvoření fotografie recidivisty. Na toho bude bezpečnostní agentura upozorněna při jeho další návštěvě v jedné z provozoven obchodního řetězce.

Hotely mohou využívat nejen již zmíněné režimové opatření, nebo upozornění na tzv. problémové osoby. Dalším velmi efektivním využitím rozpoznáním tváře je upozornění personálu na recepci na stálé klienty. Aplikace upozorní obsluhu recepce, že přichází

pravidelný host. Na monitoru mu prozradí jméno osoby, jeho nejčastější požadavky a další potřebné informace. Zavedení klientů do takového registru lze ovšem jen po domluvě s hostem. Nejedná se o bezpečnostní aplikaci, ale jde o další velmi užitečné využití verifikace obličeje.

Mezi výše uvedené stálice na požadavky vysoké bezpečnosti můžeme zařadit i menší subjekty, které začínají velmi výrazně vystupovat z pozadí. Máme tím na mysli sociální a zdravotní zařízení jako jsou školy, školky, jesle, nemocnice, lékárny atd. Možná se ptáte proč zrovna školky a školy? Odpověď je prostá a jednoduchá, stačí, když se podíváme několik měsíců zpět. Otřesný případ pobodání několika dětí a zaměstnanců školy šíleným útočníkem v Belgii. Dalšími důvody jsou stále častější únosy dětí ze školek jedním z rodičů, nebo nedej bože psychicky narušeným člověkem. Záměrem je nainstalovat kontrolu vstupu do objektů školek. Byly by uloženy šablony rodičů a příbuzných, kteří mohou děti vyzvednout. Všichni ostatní by se do zařízení vůbec nedostali a odpadlo by i milné vpuštění cizí osoby do budovy zaměstnancem školky, jak tomu bylo právě v Belgii.

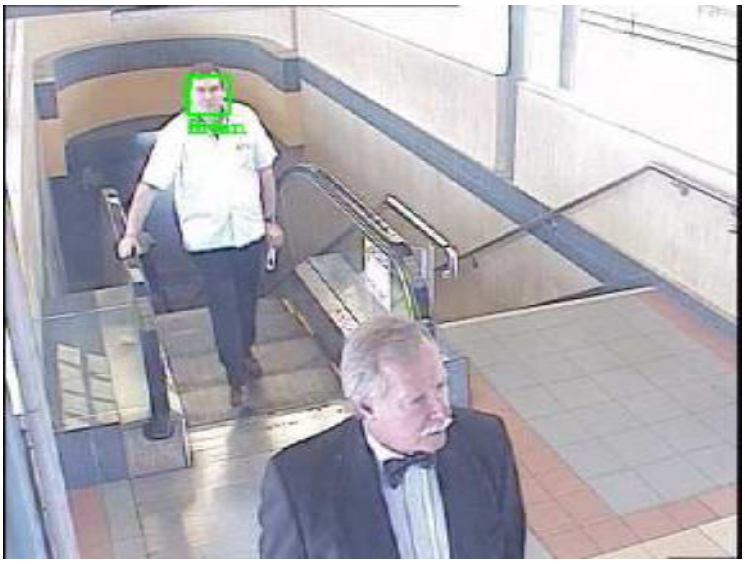
Nemocnice a lékárny jsou mnohdy obrovským komplexem budov, kde se pohybuje velké množství personálu. Je zde uloženo obrovské množství nejen medikamentů a chemikálií, ke kterému by měli mít přístup jen oprávnění zaměstnanci. Příchod do těchto citlivých prostorů jako jsou operační sály, lékárny atd. je zabezpečena režimovým opatřením.

Všechny výše zmíněné možnosti využití verifikace obličeje jsou oblasti, kde se v budoucnu očekává nasazení tohoto biometrického systému. Jeho výhod, jež jsme si uvedli, je nespočet. Plnému nasazení, jako samostatnému systému kontroly vstupu, zatím brání fakt, že systémy nejsou propracované k plné spolehlivosti. Vyskytují se případy, kdy je milně vpuštěna cizí osoba jako například na letišti v Sydney. V některých provozech nemusí tato skutečnost znamenat větší ohrožení, avšak pro spolehlivost systému kontroly vstupu je tento fakt absolutně nepřijatelný. V současnosti se nabízí využití systému v kombinaci s jinou bezpečnostní metodou, jakou je třeba zadání hesla, či použití čipové karty atd.

4.2.3 Dynamické snímání scény

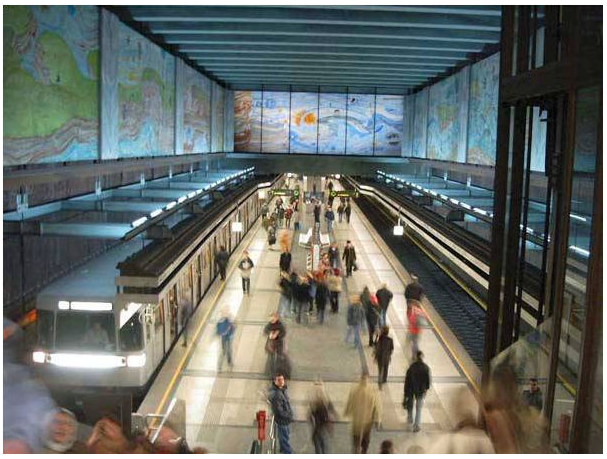
Dynamické monitorování scény není v bezpečnostní a policejně-soudní praxi žádnou novinkou. Kamerové systémy střeží většinu měst po celé Evropě. Slouží především k monitorování dopravy, k udržení pořádku v ulicích před vandaly, chuligány a k potlačení kriminality jako takové. Personál na dispečinku vyhodnocuje dění na monitorech a

vyvozuje z něj důsledky. Aplikace umožňující rozpoznávání tváře pozvedává dynamické monitorování prostoru na mnohem vyšší úroveň a přináší nové možnosti. Tato oblast biometrické identifikace je nejbouřlivěji se vyvíjející oblastí.



Obr. 17. Monitorování veřejné scény[16]

Tyto aplikace mají velice široké spektrum využití. Monitorování dopravních uzlů, jako jsou nádraží, letiště, přístavy, je jednou z možností. Vhodným umístěním kamer na místa jako jsou turnikety, eskalátory, schodiště docílíme monitorování obrovského množství lidí. Aplikace schopná rozpoznat tváře v davu lidí velmi rychle ponese své ovoce. Dispečink bude upozorněn, jestliže se ve snímaném prostoru objeví zájmová osoba. Do systému musí být samozřejmě předem vloženy šablony hledaných osob, ať už teroristů, vrahů, zločinců, či pohřešovaných lidí.



Obr. 18. Snímání veřejných dopravních uzlů[8]

V roce 2006 byl v Německu spuštěn testovací projekt, který monitoroval právě pohyb cestujících na vlakovém nádraží v Mohuči. Tento dopravní uzel byl upřednostněn z důvodu, že zde panují velmi dobré světelné podmínky, které jsou důležité pro správnou identifikaci osob podle tváře. Šest kamer bylo umístěno nad hlavní nádražní schodiště, kudy denně projde až 20 000 lidí. V databázi zájmových osob je zatím 200 dobrovolníků, kteří se do projektu přihlásili. Snímky všech ostatních lidí, kteří nejsou v databázi, byly po 48 hodinách mazány z důvodu ochrany osobních dat.

Monitorování davu při demonstracích, sportovních zápasech či při jiných shromážděních je další možnost využití aplikace rozpoznávání tváře na dynamicky snímané scéně. Při protestech nebo na demonstracích se velmi často objevují tytéž problémové osoby. Jedná se především o stoupence krajní pravice, kteří velmi často porušují zákon.

Fotbalové zápasy se již dlouhou dobu potýkají s problémovými fanoušky. Ne ve všech zemí se s tímto nešvarem dokázali organizátoři vypořádat. Zdárným příkladem je Česká Republika, kde se odpovědnost za chuligány přehazuje mezi policií a majiteli klubů. Policie pravidelně monitoruje sektory s těmito fanoušky. Materiálu s fotografiemi chuligánů je tedy spousta. Stačilo by se vydat směrem k biometrické identifikaci a využití aplikace rozpoznání obličeje. Současný prodej lístků na jméno zaměstnává velké množství personálu a pro samotné fanoušky je příliš zdlouhavý a nepříjemný. Kamery umístěné nad vchodem do stadionu by rozhodly, který fanoušek smí a nesmí na fotbalová utkání. Vzorným příkladem je fotbalový klub PSV Eindhoven, který využívá právě identifikace problémových fanoušků pomocí kamery.

Obr. 19. Monitorování problémových fanoušků[20]

4.2.4 Kreditní karty, řidičské průkazy a ostatní doklady

Vydávání nového dokladu, či jeho duplikátu je v USA provázeno bezpečnostními opatřeními. Využívá se právě identifikace totožnosti osob na základě rozpoznání obličeje. Cílem je zamezit ilegálnímu vydání nových dokladů. Spousta lidí se snaží podvodně získat např. řidičský průkaz, který jim byl zabaven. Celou situaci stěžuje fakt, že státy unie nepoužívají jednotnou centrální počítačovou evidenci dokladů. Fotografie tak zůstává jediným způsobem jak datově propojit jednotlivé systémy. Tvář osoby, která se uchází o vydání nového dokladu, je porovnávány s ostatními snímky v databázi. Porovnají se tedy všechny šablony tváří a zjistí se, zda již tato osoba nemá tento doklad vydána.

Fotografie z řidičského průkazu se také začíná využívat v souvislosti s rychlostními přestupky řidičů, zaznamenaných kamerovým systémem. Jako usvědčující důkaz slouží fotografie auta s čitelnou SPZ a časem pořízení snímku. V databázi vozidel je poté vyhledán majitel vozidla a vyzván k uhrazení pokuty. Vlastníci automobilů sebrání, mnohdy však oprávněně, že tento přestupek nespáchali oni. Není totiž prokazatelné, kdo automobil řídil. Začal se tedy používat systém dvou kamer, kdy ta první snímá vozidlo s SPZ a druhá zachycuje obličej řidiče. Podle tohoto snímku je nalezen skutečný viník přestupku v databázi řidičů.

Obr. 20. Zaznamenávání dopravních přestupků[21]

Přístup do bankomatů se provádí pomocí čipové karty a zadání pin kódu. Nová technologie využívá verifikaci tváře. Na kartě obsahující mikročip je uložena biometrická předloha tváře majitele účtu. Kamera umístěná v bankomatu porovná vzor tváře se snímaným obličejem osoby, která se pokouší přihlásit do systému. Informace se porovnávají přímo mezi bankomatem a kartou, během logování uživatele. Data tedy není potřeba přenášet do systému, čímž se zabrání jejich zneužití. Tato aplikace však ještě není plně zavedena do praxe. Zatím se pouze spekuluje, zda by splnila přísné bezpečnostní kritéria, jelikož nejslabším místem je komunikace mezi kartou a databází, která může být nabourána.

V poslední době se u nás hovoří velmi často o biometrickém pasu. Jedná se o cestovní pas, který je kombinací papírového a elektronického pasu. Elektronický pas navíc obsahuje naše biometrické šablony. V současnosti jsou standardizované především otisk prstu, verifikace duhovky a digitální mapa tváře. Všechny citlivé údaje jsou uloženy na RFID čipu.

4.2.5 Přihlašování do výpočetní techniky

Biometrická identifikace rozpoznávání tváře se širokému množství lidí dostalo do podvědomí především díky instalaci této bezpečnostní aplikace do notebooků. Výpočetní technika využívala nejdříve klasické přístupové hesla do systémů, později biometrickou

identifikaci otisku prstu. Nyní se rozšířila již zmíněná metoda verifikace obličeje uživatele webovou kamerou umístěnou přímo v notebooku. Při přihlášení porovná šablony s biometrickými daty s osobou před monitorem. Tato novinka vzbudila velké ohlasy, které byly ve většině převážně negativní.

Instalovaný software nebyl ve většině případů na úrovni, která by uživateli ulehčovala přihlašování do systému, ale spíše naopak. Největším problémem byli různé světelné podmínky při přihlašování, které poté oprávněného uživatele vyhodnocovali jako osobu neznámou. Dalším problémem byla bezpečnostní odolnost. Mnohdy stačilo k přihlášení do systému vložit před objektiv kvalitní fotografii uživatele. Některé systémy kontrolovaly, zda se objekt před kamerou hýbe, či nikoliv. Mělo se tím zamezit triku s obrázkem uživatele vloženým před monitor. Tento bylo možné prolomit pouhým pohybováním obrázku.

Obr. 21. Přihlašování do Windows pomocí verifikace obličeje[22]

Z tohoto důvodu se mohlo stát, že u uživatelů těchto aplikací nastala nedůvěra v tento druh biometrické identifikace. Problémem však není metoda verifikace obličeje, ale kvalita softwaru dodávaného do zařízení. Prodejcům šlo spíše o novinku, která jejich produkt vyzdvihne na trhu, než o kvalitní prvek bezpečnosti, který by samozřejmě neúnosně zvedl

prodejní cenu. Metoda rozpoznávání tváře se užívá v oblastech s mnohem vyššími požadavky na bezpečnost, než je logování se do systému výpočetní techniky mezi řadovými uživateli, s velmi uspokojivými výsledky. Já osobně bych však tento druh autentizace do výpočetní techniky neodepisoval, jelikož výrobci budou systém neustále zdokonalovat.

5 PROCES ROZPOZNÁVÁNÍ OBLIČEJE

Problematika procesu počítačového rozpoznávání tváří je velmi rozsáhlá oblast, ve které se ukrývá nemalé množství postupů, metod, mající jediný cíl, pravdivě rozpoznat obličej. Zjednodušeně se dá říci, že rozpoznávání obličeje je porovnávání sejmutého obrazu kamerou s obrazem tváře, který je uložen v databázi biometrického systému. Avšak samotný děj rozpoznávání tváří je spletitý celek složený z přesně definovaných kroků:

- Detekce tváře v prostoru
- Přesná lokalizace hlavy
- Rozpoznávání důležitých markantů v obličeji
- Proces identifikace

5.1 Druhy rozpoznávání obličeje

Biometrické systémy rozpoznávání obličeje pracují nejčastěji na základě tří principů:

- Verifikace
- Identifikace
- Srovnávání šablon

5.1.1 Verifikace obličeje

Vyhledávání 1:1, tedy snaha o nalezení referenčního obličeje, jehož identita je již potvrzena, k našemu hledanému obličeji. Jelikož se nám nabízí hned celá řada různých verifikačních algoritmů založených na rozdílných metodách, máme tedy potřebu zhodnotit tyto metody podle nějakého verifikačního poměru. Verifikační poměr tedy bude poměr mezi správným počtem povolených přístupů oproti poměru chybně povolených přístupů, tedy podvodnými (podvrženými) přístupy. Dobré verifikační systémy balancují mezi těmito dvěma hodnotami, kde jejich konkrétní hodnoty závisí na konkrétním použití a stupni bezpečnosti. Verifikační poměr pro konkrétní úlohu bývá zakreslen pomocí grafu, který se nazývá ROC křivka.[2]

5.1.2 Identifikace obličeje

Jedná se o porovnávací proces 1:N, kde srovnáváme hledaný obraz s tváří, oproti všem referenčním obličejům uloženým nejčastěji v databázi a snažíme se určit podobnost mezi těmito obrazy. Tento proces bývá nejčastěji realizován tím způsobem, že se hledaný obraz uloží do databáze (nejčastěji ve formě vektoru) a má tedy nejvyšší podobnost s hledaným obličejem. Identifikační proces je uzavřený proces, který porovnává různé vlastnosti obrazu a je individuální pro většinu databází. Testované rysy obličeje musí být nejprve normalizované, tedy pootočeny a zarovnány podle os tak, aby bylo možné je porovnat s dalšími obličeji. Výsledkem je tedy míra podobnosti pro každé srovnání, které jsou později seřazeny sestupně tak, aby bylo možné jednoduše projít podobné obličeje od nejvíce odpovídajících, až po ty nejméně podobné.[2]

5.1.3 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.[2]

5.2 Rozdělení přístupu rozpoznávání obličeje

V dnešní době je známo spousta metod a technik přístupu, které využívají automatizované systémy rozpoznávání obličeje. Jejich rozčlenění do různých kategorií závisí na úhlu pohledu, například pokud budeme mít na mysli časové kritérium, rozlišíme statické a dynamické snímky, přičemž poslední jmenovaný můžeme rozložit na jednotlivé statické obrazy. Co se týče formy zpracování obrazu, známe 2D (dvourozměrné) a 3D (třírozměrné) obrazy. Barevné spektrum nám vyčlení obrazy černobílé, barevné, infračervené, případně jejich různou kombinaci. Čelní pohled, boční pohled, obecný pohled a jejich kombinace jsou rozděleny na základě způsobu snímání.

V literatuře se setkáváme nejčastěji se dvěma způsoby rozdělení. První rozčlenění je velmi přehledné a jednoduché:

- Geometrický přístup (založený na rysech tváře)
- Fotometrický přístup (založený na vhledu tváře)

Druhý způsob rozdělení je více podrobný:

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

5.2.1 Strukturální způsob

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. [2]

5.2.2 Holistický způsob

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). [2]

5.2.3 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. [2]

5.2.4 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.[2]

6 LOKALIZACE HLAVY

Prvním důležitým krokem v procesu rozpoznávání obličejů je správná identifikace oblasti hlavy a tváře na fotografii, nebo ve snímané scéně. K této problematice můžeme nejen v literatuře, ale především na internetu naleznout velké množství informací. Já uvedu jen příklad několika algoritmů. Ve většině případů se používá kombinace více algoritmů. I samotný proces lokalizace a rozpoznávání obličeje se v některých případech pojí do jednoho celku.

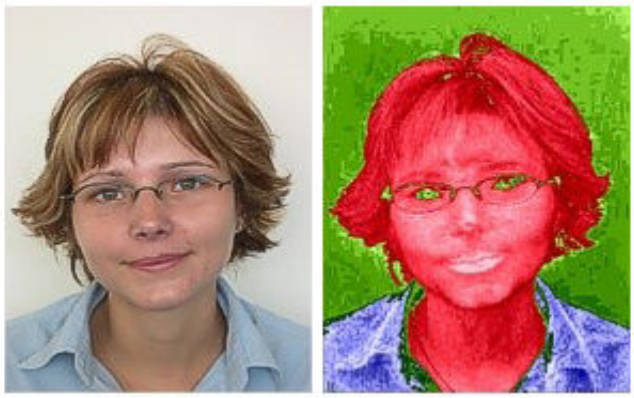
6.1 Strukturální metody

Jedná se o metodu, která vychází z antropologických znalostí a hledání identifikačních markantů. Tato metoda byla a stále je používaná ve forezních aplikacích. Známe několik popsaných antropometrických bodů, přičemž se jedná o vnitřní a vnější koutky oka, vnější horizontální body rtů, bod přechodu nosu v čelo, bod špičky nosu. Zjednodušeně lze říct, že se zaměřujeme na dominantní části obličeje, kterými jsou oblasti očí, nosu a úst (rtů). Uši se nevyužívají, jelikož ne vždy je poloha hlavy v takové pozici, ve které by bylo možné tuto techniku využít. Navíc je zde i spousta faktorů znemožňující použít tuto metodu, jako například dlouhé vlasy, nebo pokrývka hlavy, která by ve valné většině zmařili identifikaci.

Jestliže budeme hledat charakteristické markanty manuálně, nebudeme mít sebevětší problém nalézt ty správné body. Jenže v dnešní době potřebujeme rozeznávací systémy plně automatizované, jelikož obrovské množství dat nelze zvládnout zpracovat ručně v požadovaném časovém úseku. Tady právě nastává oříšek v podobě nekvalitního snímku. Tato metoda má problémy rozeznat obrázky horší kvalit, jelikož charakteristických markantů, na které se zaměřuje, není mnoho.

6.2 Detekce obličeje pomocí barvy kůže

Lokalizace tváře ve snímaném prostoru prováděná pomocí detekce barvy kůže, je další využívanou metodou nejen díky své rychlosti rozpoznávání. Na světě je několik etnických ras s rozdílnou barvou pleti.



Obr. 22. Detekce obličeje pomocí barvy kůže[4]

Existuje však mezi nimi jistá podobnost v prostoru počítačového vidění, která umožňuje detekovat všechny tyto skupiny. Tato skutečnost je dána tím, že obličej je barevně odlišný od svého pozadí. Pokud budeme tuto aplikaci využívat při vstupu do budovy, při celní kontrole, atd., kde jsou statické kamery, můžeme připravit ideální pozadí pro verifikaci, které bude jednoduché a kontrastní.

Obr. 23. Rozpoznání obličeje s různorodým pozadím[4]

Problém nastává v okamžiku, pokud pozadí má stejnou barvu jak obličej, což je případ dynamického snímání prostoru nejen ve venkovních podmínkách. Z tohoto důvodu se

technika detekce kůže kombinuje s jinými algoritmy. Hlavní výhodou této techniky je nezávislost na natočení hlavy vůči kameře a na změnu světelných podmínek.

6.3 Detekce pomocí kontur Tváře

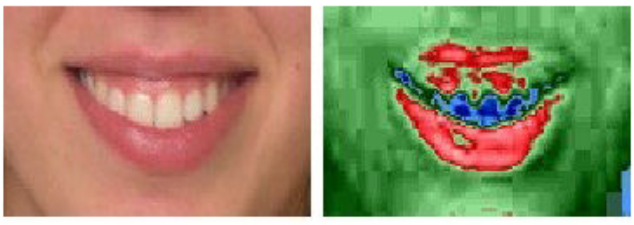
Lokalizace obličeje pomocí kontur je další metodou využívající charakteristické znaky lidské tváře. Kontury neboli obrysy nám tedy detekují hranice hlavy. Tato technika využívá k detekování hran metodu energetických křivek. V literatuře se objevuje pod názvy snakes, neboli „hady“, či aktivní kontury. Tato technika vyžaduje apriorní znalosti tvaru hlavy. Proces lokalizace probíhá tak, že hady přikládáme na jednotlivé snímky. Křivky se deformují pomocí vnitřní, vnější a obrazové síly. Vnější síly jsou vytvořeny počátečním umístěním hadů. Obrazové síly směřují směrem k hraně objektům, tudíž tvarují přiloženou křivku a vnitřní síly kontroluj í celý průběh. Při procesu se had tvaruje až k hraně objektu, tedy do pozice s minimální celkovou energií.

6.4 Detekce úst (rtů)

Detekce úst je poněkud problematickou oblastí. Jak jistě víme, ústa nemají pevně daný tvar. Ten se neustále mění podle nálady, či jiných podnětů. Nevýhodou je její citlivost na rušivé podněty. Máme dvě možnosti, které lze využít k lokalizaci rtů. Tou první je metoda již zmíněných hadů.

Nejprve podle polohy očí zjistíme pravděpodobnou oblast, kde se vyskytují rty. Tady použijeme metodu výše popsaných aktivních kontur.

Další možností je využití barevné odlišnosti stejně jako u detekce celého obličeje, rty i ústa mají jiné barvu než okolní kůže. Stejným způsobem jako u implementování kontur zjistíme pravděpodobnou oblast výskytu úst.



Obr. 24. Detekce úst[4]

6.5 Detekce očí

Obrysy oči a rtů jsou určovány pomoci poměrného umístění vzhledem k hranicím hlavy. Oči mají obecně stabilní strukturu a tvar skládající se z duhovky a vička. Tento fakt nabízí možnost jejich hledání pomocí pevného vzoru (šablony), podobně jako u modelu hlavy. Pomoci rastru obličeje se provede prohledávací fáze v celém obrazu. [4]

7 ROZPOZNÁVÁNÍ OBLIČEJE

Jak jsem již uvedl, úkolem lokalizace obličeje je najít samotný objekt tváře např. na snímku. Při rozpoznávání se algoritmy zaměřují již na charakteristické markanty na obličeji a nacházejí mezi nimi rozdíly.

7.1 Lineární analýza

Většina základních metod pro rozpoznávání je založena na lineárních vzhledových klasifikátorech, jsou to analýzy hlavních komponent a diskriminační analýza. Obrazová data o rozměrech X a Y mohu být reprezentována pomocí vektoru respektive pomocí bodu ve vysoko-rozměrném prostoru. Možností projekce vektoru na bázové vektory získáme projekční koeficienty, které jsou základním typem reprezentace tváře v obraze. Můžeme tedy porovnávat obličeje a určit tak míru podobnosti, například určením kosinu mezi vektory testovaného a referenčního vektoru. Klasifikační metody můžeme považovat za transformaci z obrazového vektoru do projekčního vektoru. [2]

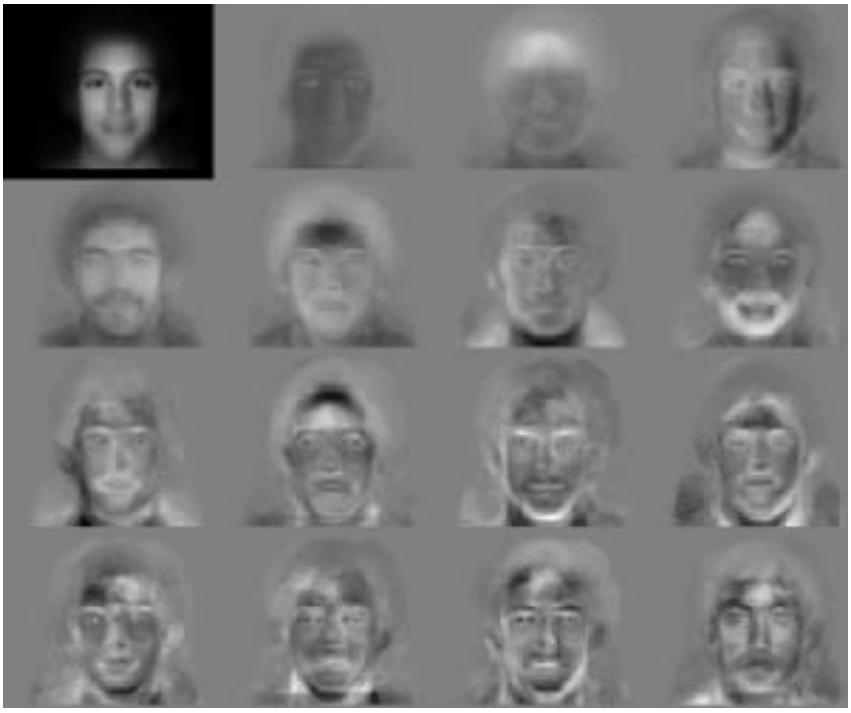
7.1.1 Analýza hlavních částí (PCA - Principal Components Analysis)

Algoritmus použit pro rozpoznávání obličeje byl v roce 1991 popsán pány Turkem a Pentlandem. PCA se stala platformou pro mnohé ostatní metody, nebo se používá v kombinaci s jinými algoritmy, k dosažení lepších výsledků. Jelikož využívá automatizovanou extrakci rysů, je vhodné jej použít u velkých kolekcí dat.

Jedná se o metodu prezentace lidského obličeje lineární transformací z původní, nebo průměrné tváře. Snímky, které jsou uložené v databázi v podobě biometrické informace, budou zprůměrovány v jeden průměrný obličej. Ten je poté převeden na tzv. eigenfaces, nebo také normalizovaná tvář (matice jasových úrovní).

Obr. 25. Metoda PCA[17]

Eigenfaces využívají markantní charakteristiky lidské tváře, které jsou důležité pro počítačové rozpoznávání. Tyto informace jsou následně uloženy v databázi rozpoznávacích softwarů. V procesu identifikace tváře, zjišťujeme odchylky vektorů původního obrázku od eigenfaces, což urychluje proces rozpoznávání. Nepotřebujeme tedy potom mít uložen objemný obrázek, ale pouze číselné hodnoty, což urychlí vyhledávací proces v databázi.



Obr. 26. PCA- vlevo nahoře průměrný obličej tváří[3]

7.1.2 Lineární diskriminační analýza (LDA - Linear Discriminant Analysis)

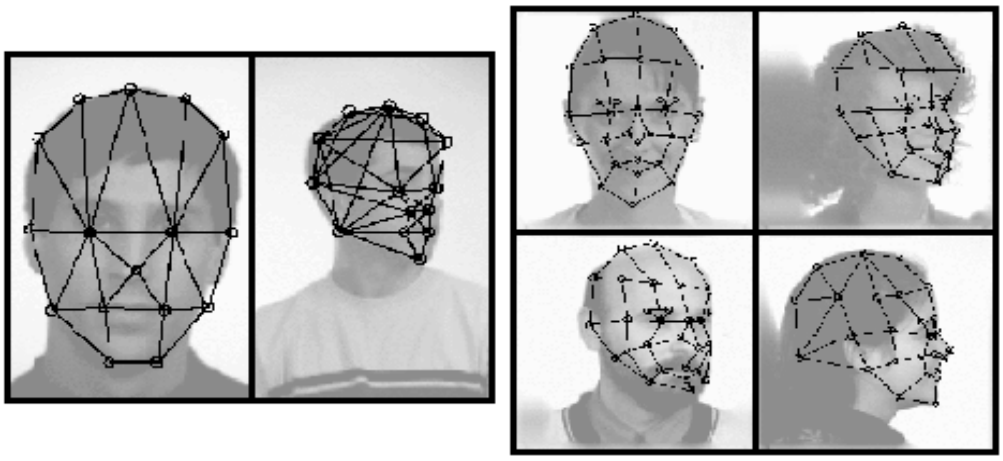
Metoda LDA pracuje stejně jako PCA ve vektorové oblasti. Naší pozorností jsou body ve vektorovém prostoru, které se snažíme rozdělit do jedné a více skupin. Členíme je podle diskriminačních funkcí. Každá kategorie zvolených bodů je odlišná od těch ostatních, přičemž se snažíme, aby tyto rozdíly byly maximální. Naopak v dané skupině se snažíme diference minimalizovat. V praxi to pro nás znamená, že vzniknou třídy různých typů obličejů. Ve skupině budou tváře velmi podobné.

Obr. 27. Metoda LDA[3]

Fisherova lineární diskriminační funkce (FLD) je jedna z nejznámějších a nejpřesnějších lineárních metod. FLD pracuje s osobitými znaky skupin, z kterých pomocí různých statistik vyčlení obrazy do korespondujících tříd.

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

Předešlé dva algoritmy využívají lineární charakteristiky, tudíž nemohou reagovat na nelineární podněty. Máme na mysli především osvětlení obličeje, pozice hlavy a výraz tváře. Tady přichází na řadu EBGM. Jedná se o metodu, při níž jsou na obličeji definovány uzlové body, které po spojení vytvoří souřadnicovou síť nazývanou elastický srovnávací diagram. Na povrch tváře je přiložena souřadnicová síť, která je doformována podle zakřivení obličeje.

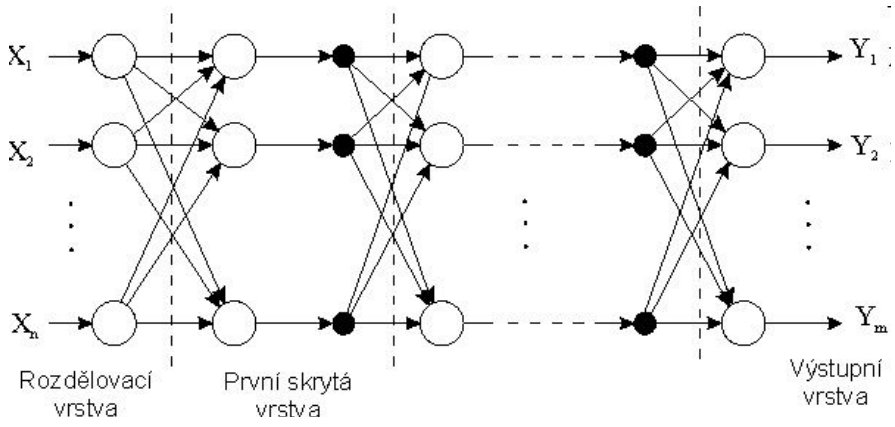


Obr. 28. Elastický srovnávací diagram[18]

Lidská tvář neustále mění svůj výraz, nejčastěji v oblasti úst, kdy dochází k různému zakřivení rtů. Dochází tedy k změně odstínů šedi v oblasti a geometrickým modifikacím. Síť se přesto stále bude kopírovat tvář a reprezentovat její křivky. EBGM může mít problémy s definování významných charakteristik, jako jsou oči, ústa a nos. Tento problém se řeší využitím metod PCA a LDA.

7.3 Neuronové sítě

V literatuře se objevují také pod anglický názvem Artifacial Neural Network – ANN. Neuronové sítě využívají vlastnosti, které je podstatně zvýhodňují oproti jiným metodám. Většina programů pracuje podle přesně definovaného postupu. V praxi však nastává spousta různorodých situací, při kterých je vhodné využít pokaždé jiný typ algoritmu, jež bude mít v daném momentě nejvíce efektivní výsledek. Dalším aspektem je fakt, že programy si v praxi musí poradit i s neúplnými, nebo nekvalitními daty, které ovšem mohou být jedinou dostupnou informací. Řešením těchto problémů mohou být právě metody neuronových sítí. ANN mají ojedinělou schopnost „učit se“, což je její základní vlastností.



Obr. 29. Neuronové sítě[4]

Umělá neuronová síť je prostředkem pro zpracování komplexních dat, využívajícím ke své práci množství propojených procesorů a výpočetních cest. ANN jsou inspirovány architekturou lidského mozku – jsou schopny se učit a analyzovat rozsáhlé a komplexní množiny dat, které mnohem lineárnější algoritmy jen těžko zvládnou.[1]

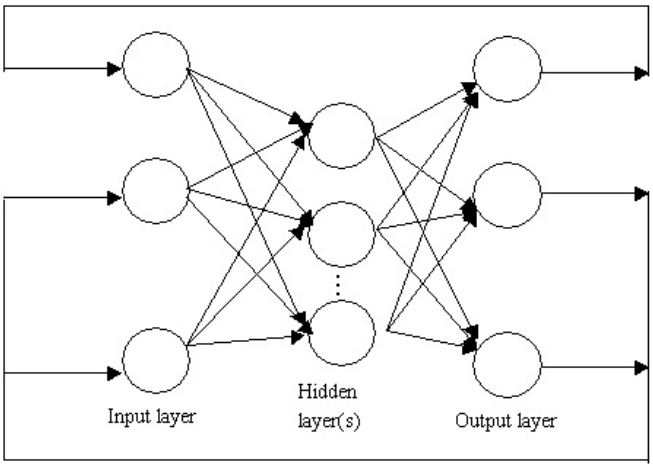
7.3.1 Princip neuronových sítí

Umělá neuronová síť funguje tak, že vytváří spojení mezi mnoha různými procesními prvky, z nichž každý je analogický se samostatným neuronem v biologickém mozku. Tyto neurony mohou být fyzicky konstruovány nebo simulovány digitálním počítačem. Každý neuron dostává mnoho vstupních signálů. Poté, na základě vnitřního vyvažovacího systému, jež zohledňuje váhy jednotlivých akcí, produkuje jednotlivý výstupní signál, který je typicky zasílán jako vstup jinému neuronu. Neurony jsou těsně spojeny a organizovány do různých vrstev. Vstupní vrstva dostává vstupní údaje, výstupní vrstva vytváří finální výstup. Mezi tyto dvě vrstvy je obvykle vložena jedna nebo více skrytých vrstev. Tato struktura neumožňuje předvídat ani znát přesný tok dat. [1]

7.3.2 Učení ANN

Na počátku jsou všechny neurony bez jakýchkoliv „vědomostí“. Je potřeba je zaškolit pro danou problematiku. Uvedeme si dvě známé taktiky učení ANN. První je self-arganizing ANN, nebo můžeme říci taky samoorganizující se. Tyto sítě jsou vystavovány velkému množství dat a směřuje se k odhalení zákonitostí a souvislostí v těchto datech. [1]

Druhou možností je učení Back-propagation, neboli zpětně šířící se. Trénování sítě probíhá tak, že vytvoříme soubor tréninkových dat a síť tento soubor několikrát po sobě zpracovává. Tréninkový soubor se skládá z dvojic vstupních a výstupních vzorů. Výstupní vzor může být považován za kategorii, do které má být správně zařazen vstupní vzor. Síť přijme na vstupní vrstvě vstupní vzor, ten sítí projde přes skrytou vrstvu na výstupní, na které se objeví jako výstupní vzor. Tento výstup je porovnán se správným výstupním vzorem načteným z tréninkového souboru. Informace o odchylce je sítí šířena směrem od výstupní vrstvy k vrstvě vstupní a jsou podle ní upravovány váhy sítě tak, aby až síť bude stejnou dvojici vzorů číst příště, byla odchylka na její výstupní vrstvě menší.



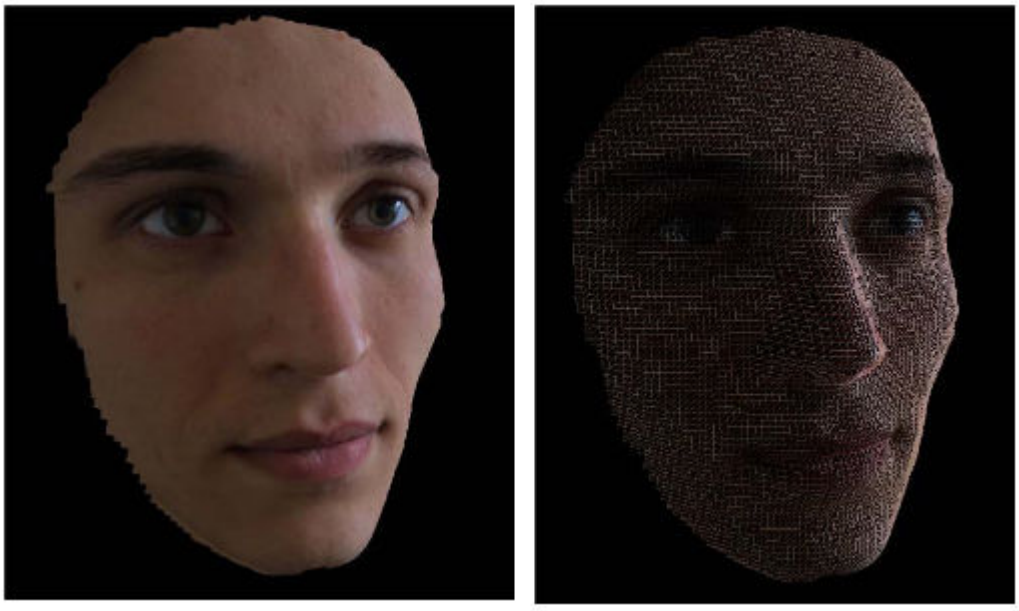
Obr. 30. Neuronové sítě[4]

Poté, co se síť správně naučí tréninkový soubor, může byt testována na jiném souboru dvojic vstupních a výstupních vzorů, abychom zjistili, jak dobře se síť naučila zobecňovat. U některých typů dat není výhodné, aby se síť naučila tréninkový soubor co nejpřesněji, protože potom si pamatuje tyto data příliš specificky a to ji bráni v zobecňování neznámých dat. [4]

7.4 3D model obličeje

3D, neboli trojrozměrné zpracování tváře je další možností přístupu k zpracování lidského obličeje. Mnohdy se můžeme setkat s otázkou který přístup je vhodnější, 2D či 3D. Pro obě metody najdeme řadu výhod i nevýhod. Záleží jen, kterým pohledem budeme danou problematiku zkoumat. 2D metoda má výhodu v jednodušším snímání biometrické šablony. Můžeme uložit lidskou tvář zachycenou, nejen z kvalitní fotografie, ale také

například kamerovým systémem. Zastánci tohoto přístupu uvádějí také tuto metodu jako přijatelnější pro počítačové zpracování.



Obr. 31. 3D model tváře[13]

Oproti tomu můžeme uvézt, že 3D snímání obsahuje mnohem více informací o dané tváři. Uložení trojrozměrné šablony nebude však možné z dynamického záznamu či z jakékoliv fotografie. Je potřeba použít speciální jednotku, kterou uložíme biometrickou šablonu do databáze systémů.

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. [5]

II. PRAKTICKÁ ČÁST

8 HODNOCENÍ SYSTÉMU A4 VISION

V praktické části se nyní budu zabývat systémem A4 Vision jímž ústav disponuje. Mým cílem je provézt porovnání tohoto systému s dalším biometrickým zařízením, otiskem prstů. Zaměřím se na pravděpodobnost chybného odmítnutí, neboli FRR – False Rejection Rate. FRR udává pravděpodobnost, s jakou bude zařízení chybovat a neidentifikuje/neverifikuje oprávněného uživatele, přestože uživatel má v aplikaci již uloženou svou biometrickou šablonu. Z tohoto důvodu je uživatel nucen opakovaně se identifikovat/verifikovat. Tato charakteristika je důležitá zejména pro osoby, které využívají systém každý den. Pokud by měly problémy se verifikovat, přestože mají povolen přístup např. do budovy, tento systém by pro ně nebyl přínosem, ale spíše přítěží. Provedu tedy měření pro obě zařízení a budu se snažit porovnat již zmíněnou pravděpodobnost FRR obou systémů.

Obr. 32. A4 Vision

Pravděpodobnost chybného odmítnutí je dána vztahem:

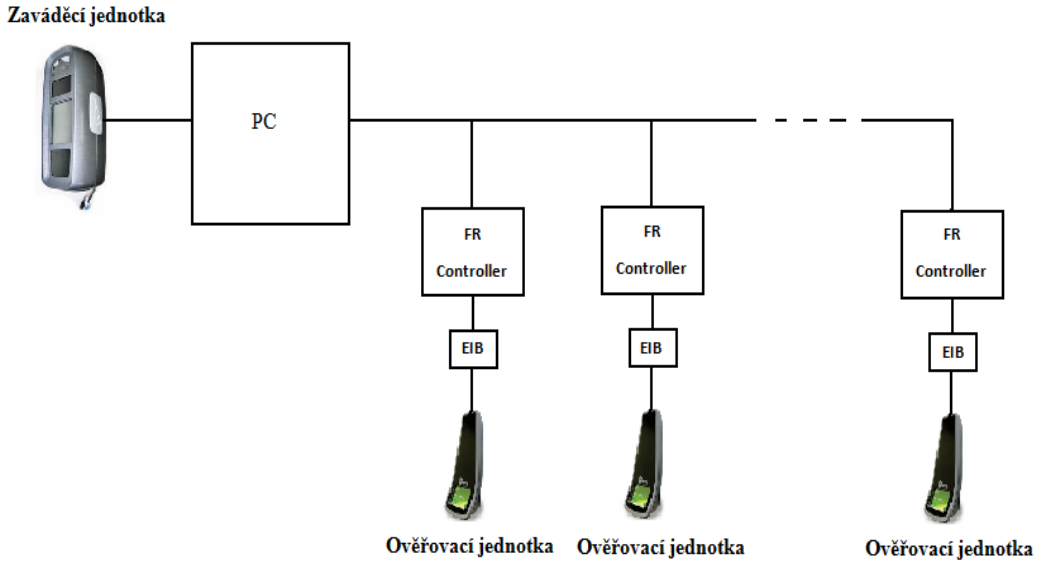
$$FRR=(N_{FR}/N_{EIA}).100\ [\%] \qquad FRR=(N_{FR}/N_{EVA}).100\ [\%] \qquad (5)$$

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).

Obr. 33. Access Vision 4[13]



Obr. 34. Schéma zapojení systému A4 Vision

PC	Personal Computer
EIB	Easy Install Box
FR Controler	Průmyslový počítač

9 MĚŘENÍ FRR SYSTÉMU A4 VISION

A4 Vision je zařízení určené pro kontroly vstupu osob. Jedná se o systém, který identifikuje uživatele podle 3D modelu obličeje. Výrobce prezentuje systém jako velice přesný, spolehlivý, zejména v otázce FRR. Právě na tuhle problematiku provedu měření a porovnám jej s jiným biometrickým systémem a to systémem otisku prstů.

9.1 Jednotlivá zařízení A4 Vision

9.1.1 Technická specifikace systému A4 Vision

- Čas identifikace <1 sec
- Čas verifikace <1 sec
- Čas zavedení 3 – 5 sec
- Max počet zařízení 10000
- Max počet uživatelů 4000

9.1.2 Zaváděcí jednotka

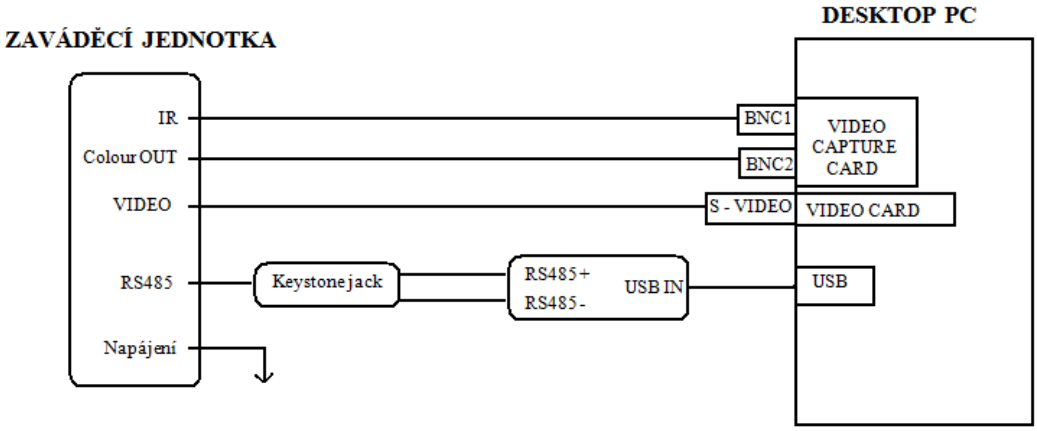
Jedná se o zařízení, kterým zavádíme biometrické šablony do databáze systému. Bývá umístěna na místě nepřístupném pro veřejnost. Odborná obsluha jej používá k zavádění nových šablon pro oprávnění ke vstupu.

Obr. 35. Zaváděcí jednotka[13]

Zaváděcí jednotka obsahuje barevnou kameru, projektor, LCD display, infračervenou kameru. Projektor vysílá infračervené světlo. Infračervená kamera zaznamenává na obličeji až 40000 bodů jak ve vertikální, tak v horizontální linii. Tyto body poté vytvoří tzv. mesh, neboli 3D síť. Z té se poté zpracují charakteristické znaky tváře.

Při ukládání šablony do systému je potřeba dodržet především vzdálenost obličeje od zaváděcí jednotky, sundat si brýle, popřípadě odstranit si spadené vlasy do tváře a sundat čepici.

- Rozměry 102 x 285 x 153 mm
- Napájení 12V
- Hmotnost 1.6 Kg



Obr. 36. Schéma zapojení zaváděcí jednotky do PC

9.1.3 Optická jednotka FRO

Optická, nebo také můžeme říci ověřovací jednotka, bývá umístěna na místech, jako jsou vstupy do budov, objektů, kanceláří atd. pro kontrolu osob. Jedná se o bezdotykové zařízení přichycené na pevnou podložku.

Při pokusu o verifikaci/identifikaci je opět potřeba dodržet vzdálenost obličeje od zaváděcí jednotky, sundat si brýle, popřípadě odstranit si spadené vlasy do tváře a sundat čepici.

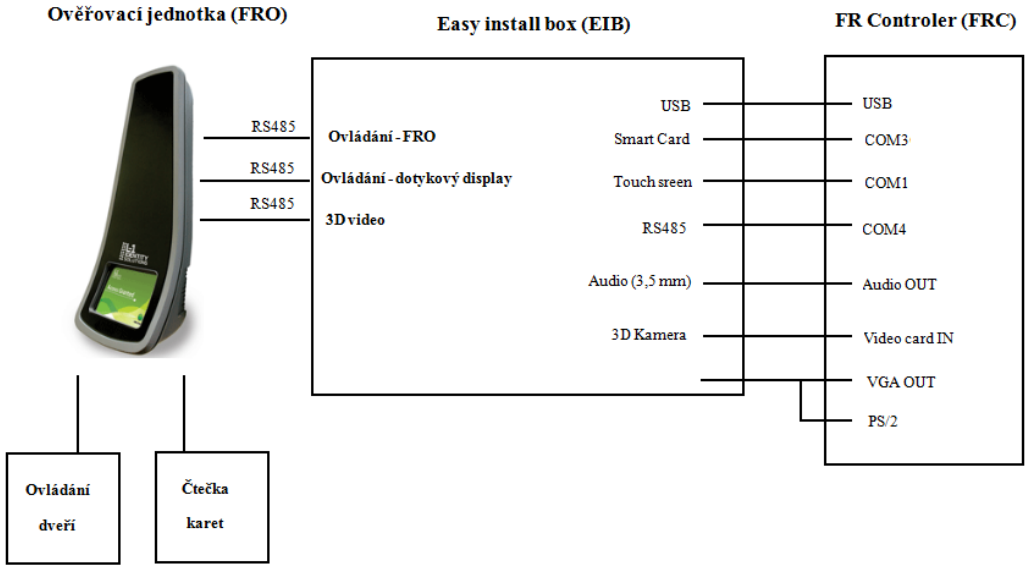
Obr. 37. FRO[13]

- Rozměry 90 x 227 x 80 mm
- Napájení 12V
- Hmotnost 0.8 Kg
- Horizontální snímací úhel 17° 30´
- Vertikální snímací úhel 13° 30´
- Vzdálenost obličeje pro snímání >500 mm
- Pracovní teplota od 15°do 30°C

Proces identifikace:

- FRO vypíše identifikační hlášení
- Testovaná osoba přistoupí k optické jednotce FRO
- Detektor pohybu v jednotce vyhodnotí přítomnost osoby – „someone is here“
- FRO akusticky informuje obsluhu o zahájení procesu rozpoznání – „start of recognition“
- Provede se skenování obličeje a následně rozpoznání
- Pokud je identifikace pozitivní vypíše se hláška – „identification positive“

- Pokud je vstup odmítnut – „Object not recognized“



Obr. 38. Schéma zapojení ověřovací jednotky s EIB a FRC

9.2 Měření

Měření jsem provedl celkem pro tři osoby. Každé osobě byla uložena její biometrická šablona v systému A4 Vision. Poté každý uživatel provedl 200 identifikačních pokusů. Snímání je po nastudování manuálu bezproblémové. Nejdůležitější je dodržení vzdálenosti tváře od snímací jednotky. Identifikace trvá, jak je uvedeno v manuálu od výrobce několik vteřin. Pouze při nedodržení podmínek pro snímání tváře systém nahlásí chybu. Jak jsem již uvedl, prováděl jsem měření na zjištění FRR.

Při měření systém chybně nerozpoznal celkem v 11 případech z 600 pokusů o identifikaci. Velké množství chybných odmítnutí zaznamenal uživatel č. 2. Přestože sejmutá šablona byla stejných kvalit jako u ostatních uživatelů, byla dodržena předepsaná vzdálenost a měření probíhalo za stejných podmínek. Výsledky měření jsou v Tab.1., viz níže.

A4 Vision			
Uživatel	Pokusů	Chybná identifikace	FRR
1	200	3	1,5%
2	200	6	3%
3	200	2	1%
celkem	600	16	**1,8%**

Tab. 1. Měření FRR systému A4 Vision

9.3 Měření FRR čtečky prstů V-Pass

Jedná se o čtečku prstů používanou pro kontrolu vstupu do objektů, nebo budov. Nejprve je nutno opět uložit biometrickou šablonu. Šablona může být uložena jednak v paměti čtečky, která je pro 200 uživatelů, nebo v paměti připojeného PC přes USB port. Já jsem pracoval s pamětí čtečky. Uložení šablony bylo rychlou a jednoduchou záležitostí.

Obr. 39. Čtečka otisku

Prstů [23]

- Rozměry 130x 50 x 65 mm
- Napájení 12V
- Čas identifikace <2 sec
- Čas zavedení <3 sec
- Max počet uživatelů 200

9.3.1 Měření

Opět jsem provedl 200 pokusů o identifikace pro všechny tři uživatele. Čtečka prstů byla přesnější, znatelné to bylo zejména u uživatele č. 2. Chybné odmítnutí uživatele nastalo celkem ve 3 případech. Výsledky měření jsou v Tab.2., viz níže.

V - Pass			
Uživatel	Pokusů	Chybná identifikace	FRR
1	200	2	1%
2	200	1	0,5%
3	200	0	0%
celkem	600	3	**0,5%**

Tab. 2. *Měření FRR systému V – Pass*

9.4 Závěr měření

Co se týče měření, výsledky byly znatelně příznivější pro čtečku prstů, která dosáhla hodnoty FRR 0,5%, oproti tomu A4 Vision dosáhl hodnoty FRR 1,8%. Zaměříme - li se více na zařízení Access Vision můžeme konstatovat, že větší problém s identifikací byl pouze u uživatele č. 2. I přesto, že zařízení Access Vision 4 je pomyslnou špičkou v oblasti rozpoznávání obličejů, čtečka prstů byla přesnější. Rozpoznávání obličeje je náročnější, co

se týče zavádění šablony. Pokud se nám nepodaří správně sejmout 3D podobu tváře, budeme mít problémy při procesu rozpoznávání.

ZÁVĚR

Cílem této práce bylo zhodnotit současný stav biometrické metody rozpoznávání obličeje pomocí kamer. Nejprve jsem objasnil pojem biometrie a obecně biometrické metody, používané v bezpečnostní praxi. Verifikace tváře patří mezi „mladší“ biometrické metody, avšak i přes tento handicap je již poměrně hojně využívanou. Převážně se však jedná pouze o testovací a zkušební provozy. Potenciální využití je však velmi široké. Počínaje uplatněním v systémech kontroly vstupu přes celní kontroly a tím pádem i letištní prevenci, dále dynamické snímání veřejných prostranství, kasin, obchodních řetězců atd. Meze fantazie využití se zde nekladou.

V současné době je však problémem funkčnost systému. Při použití tokenů, hesel a čipových karet máme zajištěnou 100% úspěšnost. Verifikace obličeje však podobných výsledků nedosahuje. I když některé systémy jsou velmi kvalitní, vždy je zde nějaká míra chybovosti. Mám tím na mysli pravděpodobnost FRR a FAR. FAR je velmi závažná z bezpečnostního hlediska, kdežto FRR je nepřijatelná z uživatelského pohledu.

Uplatnění by tato metoda mohla najít při dynamickém snímání veřejného prostranství, kdy nikoho „fyzicky“ neobtěžuje a přitom může upozornit na zájmové osoby ve snímaném prostoru. Dalo by se říci, že nemůže napáchat znatelné škody. Oproti tomu při použití na letištích, celním odbavení, při kontrole vstupu do budov a jejich částí bych byl ovšem opatrnější. Pokud by systém do objektu pustil osobu neoprávněnou, jak se tomu mnohdy může stát (FAR), mohlo by to mít závažný dopad na danou instituci, či podnik. Jednou z možností jak zavádět verifikaci tváře jako systém kontroly vstupu by mohla být jeho kombinace s jinou metodou, např. využitím hesla, tokenů, atd.

V praktické části jsem hodnotil systém rozpoznávání obličeje Access Vision 4 se systémem snímáče otisku prstů V – Pass. Zaměřil jsem se na porovnání těchto zařízení z pohledu uživatele, jinými slovy, měřil jsem charakteristiku FRR. Výsledek mého měření vyzněl lépe pro snímač otisku prstů V - Pass. U A4 Vision nastaly potíže především v situacích, kdy uživatel nedodržel předepsanou vzdálenost od ověřovací jednotky. Jelikož na oblast rozpoznávání obličejů je zaměřena obrovská pozornost a provádí se intenzivní výzkum, jistě dojde k zdokonalení metod rozpoznávání a k odstranění některých současných problémů.

V dalších letech se dá předpokládat opět velký pokrok na poli rozpoznávání obličejů. Algorimy se stávají stále přesnější a ne jinak tomu bude nadále. V budoucnu se budeme s touto oblastí setkávat jistě častěji a jen další vývoj nám ukáže, jestli se tato velmi zajímavá biometrická metoda natrvalo uplatní v bezpečnostní praxi jako samostatná plnohodnotná metoda.

ZÁVĚR V ANGLIČTINĚ

This bachelor thesis deals with summarizing of present state of biometrical identification of people using a face recognition. Individual possibilities will be evaluated. The end of the thesis is about summarizing of identification system IRIS 2200, which is available at our department.

The aim of this thesis was to summarize the present state of biometrical method of the face recognition using the video cameras. At first I generally defined the term Biometry and biometrical methods used in security systems. Face verification belongs among younger biometrical methods, despite this handicap it is used quite often. The usage is mainly in testing and experimental areas. Potential usage of this method is wide, you can use it in the systems of checking the enters, customs control including airport security, dynamic monitoring of public places, casinos, supermarket chains etc. You can use it in many other ways.

At the present time there is a problem with system utility. When we use tokens, passwords and smart cards there is is 100% success. Face verification doesn´t reach the same goals. Even though some systems are of a very good quality, there is always some kind of mistake, by this I mean FRR and FAR probability. FAR is very important because of security, FRR is not acceptab from the user´s point of view.

This method should be used in dynamic monitoring of public places, when no people are bothered physically and during this it can warn about interesting people in sensing place. It can be said that no apparent mistakes will be done. As opposed to the usage of this method at the airports, customs controls and checking of entries into buildings and their parts. I suggest we should be much more careful in this case. If the system enables the entry of unauthorised person, it may happen when we use FAR, it may have serious consequences for the institution or the company. One of the possibilities how to implement face verification as a system for checking the entry should be it´s combination with another method, e.g. using of password, tokens etc.

In the practical part I summarized the system of the face verification called Access Vision 4 with the system of fingerprints sensoring called V-Pass. I was mainly interested in comparing these two devices from the user´s point of view, in other words, I measured FRR characteristics. The better result was in V-Pass. In A4 Vision there were problems in

situations, in which the user did not follow the specified distance from the testing unit. There is a great attention paid to the area of face recognition and intensive research is conducted. For sure the methods will be improved and present problems will be solved.

In a next few years a big progress in the area of face recognition is supposed to happen. Algoritms are becoming more precise and it will continue. In the future we will meet this area more often and next research will show us how this interesting method will be applied in security profession as an individual fully-fledged method.

SEZNAM POUŽITÉ LITERATURY

[1] RAK, Roman, et al. Biometrie a identita člověka : ve forezních a komrčních aplikacích. 2008. vyd. Praha : Grada Publishing, a.s., 2008. 644 s. ISBN 978-80-247-2365-5.

[2] ČÁSTEK, Petr. Face recognition. Master Degree Programme (x), FIT VUT [online]. 2008 [cit. 2009-03-23]. Dostupný z WWW: <http://www.feec.vutbr.cz/EEICT/2008/sbornik/02-Magisterske%20projekty/08-Grafika%20a%20multimedia/02-xcaste01.pdf>.

[3] ŠČUREK, Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Oddělení bezpečnosti osob a majetku [online]. 2008 [cit. 2009-03-15]. Dostupný z WWW: <http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf>.

[4] MICHALÍK, Marek. Algoritmy pro rozpoznání obličeje. Bakalářská práce [online]. 2008 [cit. 2009-05-02]. Dostupný z WWW: <https://www.stag.utb.cz/apps/stag/dipfile/index.php?download_this_unauthorized=9103>.

[5] Třetí pól [online]. 2009. 2009 , 2009 [cit. 2009-05-07]. Dostupný z WWW: <http://www.tretipol.cz/index.asp?clanek&view&501>.

[6] Www.novinky.cz [online]. 2006. 2006 [cit. 2009-03-11]. Dostupný z WWW: <http://www.novinky.cz/zahranicni/evropa/98126-nemecko-zkousi-program-na-identifikace-tvari-v-davu.html>.

[7] Kriminalistické metody : Portrétní identifikace [online]. 9.12.2007 , 9.12.2007 [cit. 2009-04-12]. Dostupný z WWW: <http://www.specialista.info/view.php?nazevclanku=kriminalisticke-metody-portretni-identifikace&cisloclanku=2007120004>.

[8] JANDA, Martin. Dá se odhalit tvář teroristy?. 21 století [online]. 2006 [cit. 2009-04-12]. Dostupný z WWW: <http://www.21stoleti.cz/view.php?cisloclanku=2006121929>.

[9] KRÁTKÝ, Michal, SKOPAL, Tomáš, SNÁŠEL, Václav. Efektivní vyhledávání v kolekcích obrázků tváří. Katedra informatiky, VŠB-Technická univerzita Ostrava 17. listopadu 15, 708 33 Ostrava [online]. 2004 [cit. 2009-04-19]. Dostupný z WWW: <http://www.cs.vsb.cz/kratky/courses/2003-04/dis/reference/effface.pdf>.

[10] DELAC, Kresimir, GRGIC, Mislav, STEWART BARTLETT, Marian. Recent Advances in Face Recognition,. Recent Advances in Face Recognition [online]. 2008 [cit. 2009-04-15]. Dostupný z WWW: <http://www.booksaio.net/ebooks/recent-advances-in-face-recognition>.

[11] ZHAO, W., CHELLAPPA, R., KRISHNASWAMY, A. Discriminant analysis of principal components for face recognition. Discriminant analysis of principal components for face recognition [online]. 2005 [cit. 2009-04-03]. Dostupný z WWW: <http://reference.kfupm.edu.sa/content/d/i/discriminant_analysis_of_principal_compo_34371.pdf>.

[12] GRGIC, Mislav, DELAC, Kresimir. FACE RECOGNITION HOMEPAGE [online]. 2005. 2005 [cit. 2009-02-04]. Dostupný z WWW: <http://www.face-rec.org/>.

[13] ČÁSTEK, Petr. FACE RECOGNITION. FACE RECOGNITION [online]. 2008 [cit. 2009-03-23]. Dostupný z WWW: <http://www.feec.vutbr.cz/EEICT/2008/sbornik/02-Magisterske%20projekty/08-Grafika%20a%20multimedia/02-xcaste01.pdf>.

[13] www.sofim.cz

[14] DRAHANSKÝ, Martin. Přehled biometrických systémů a testování jejich spolehlivosti. VUT Brno [online]. 2007 [cit. 2009-04-23]. Dostupný z WWW: <http://data.security-portal.cz/clanky/113/odborne_prednasky/Prezentace.pdf>.

[15] Nakreslete zločince a pošlete ho za mříže. Technet.cz [online]. 2008 [cit. 2009-03-12]. Dostupný z WWW: <http://technet.idnes.cz/nakreslete-zlocince-a-poslete-ho-za-mrize-f14-/tec_technika.asp?c=A080505_151953_tec_technika_kuz>.

[16] MALINKA, Kamil. Autentizace uživatelů. Fakulta informačních technologií [online]. 2008 [cit. 2009-03-01]. Dostupný z WWW: <http://isildur.ics.muni.cz/~kamil/KIB/slajdy/prednaska6.pdf>.

[17] FRITSCH, Lukáš. METODA PCA A JEJÍ IMPLEMENTACE V JAZYCE C++. CVUT v Praze [online]. 2005 [cit. 2009-04-04]. Dostupný z WWW: <http://dsp.vscht.cz/konference_matlab/MATLAB07/prispevky/fritsch_l/fritsch_l.pdf>.

[18] WISKOTT, Laurenz, et al. Face Recognition by Elastic Bunch Graph Matching. Institute for Neural Computation [online]. 1999 [cit. 2009-02-26]. Dostupný z WWW: <http://www.face-rec.org/algorithms/EBGM/WisFelKrue99-FaceRecognition-JainBook.pdf>.

[19] Www.brno.cz [online]. 2008. 2005 [cit. 2009-04-26]. Dostupný z WWW: <http://www.brno.cz/galerie/obrazky/1236679899-v.jpg>.

[20] KOMÁNKOVÁ, Jana. Reflex : Hooli gans! [online]. 2004. 2004 [cit. 2009-05-07]. Dostupný z WWW: <http://images.google.com/imgres?imgurl=http://www.reflex.cz/images/imgdb/original/phpLm8e2A.jpg&imgrefurl=http://www.reflex.cz/Clanek16591.html&usg=__f0Nxmy9EU0XzrwnkpZNywQ5Znnk=&h=426&w=639&sz=103&hl=cs&start=10&um=1&tbnid=clYgWoIJRXCUdM:&tbnh=91&tbnw=137&prev=/images%3Fq%3Dmonitorov%25C3%25A1n%25C3%25AD%2Bfanou%25C5%25A1k%25C5%25AF%26hl%3Dcs%26client%3Dopera%26rls%3Dcs%26sa%3DN%26um%3D1>.

[21] www.dipol.com

[22] http://images.techtree.com/ttimages/story/82558_veriface.jpg

[23] www.sourcesecurity.com

[24] Křeček a kol. : Příručka zabezpečovací techniky, Blatná: Blatenská tiskárna, 2003, ISBN 80-902938-2-4

[25] Vít, V., Kuba, P.: Televizní technika, 1. vyd., nakladatelství BEN, 2002, ISBN 80-86056-88-0

[26] SONKA M., HLAVAC V., BOYLE R. Image Processing, Analysis, and Machine Vision. 2.vyd. PWS Publishing, Pacific Grove, 1999. ISBN 0-534-95393-X

[27] HLAVÁČ V., SEDLÁČEK M. Zpracování signálů a obrazů. Praha: Vydavatelství ČVUT, 2000. ISBN 80-01-03110-1.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ANN Artifacial Neural Network – Neuronové sítě

CCTV Closed Circuit Television – Uzavřený televizní okruh

FAR False Acceptance Rate - Pravděpodobnost chybného přijetí

FER Failure to Enroll Rate Skutečnost kdy uživateli nemůže být zaveden do systému

FIR False Identification Rate

FMR False Match rate

FNMR False Non-Match Rate

FRC Průmyslový počítač

FRO Optická jednotka (Ověřovací jednotka)

FRR False Rejection Rate - Pravděpodobnost chybného odmítnutí

FTE Skutečnost kdy uživateli nemůže být zaveden do systému

LDA Linear Discriminant Analysis - Lineární diskriminační analýza

PC Personal computer – Osobní počítač

PCA Principal Components Analysis - Analýza hlavních částí

SPZ Státní poznávací značka

SEZNAM OBRÁZKŮ

SEZNAM TABULEK