Česká zemědělská univerzita v Praze

Technická fakulta

Spolehlivost rozpoznání obličeje pomocí smart kamerových systémů

Diplomová práce

Vedoucí diplomové práce: Ing. Veronika Hartová, Ph.D.

Diplomant: Bc. Josef Prachař

PRAHA 2018

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Josef Prachař

Obchod a podnikání s technikou

Název práce

Spolehlivost rozpoznání obličeje pomocí smart kamerových systémů

Název anglicky

Reliability of face recognition using smart camera systems

Cíle práce

Diplomová práce je tematicky zaměřena na spolehlivost současných kamerových smart technologií s funkcí rozpoznání obličeje.
Hlavním cílem je provést testování určených technologií a jejich následné zhodnocení.
Dílčí cíle diplomové práce jsou:
- vytvořit přehled řešené problematiky
- kvalitně zpracovat rešeržní část
- provést rozbor současných smart kamerových technologií
- provést sadu testování a měření spolehlivosti u kamer Netatmo
- provést finanční zhodnocení kamerových systémů s detekcí obličeje

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýzách odborných informačních zdrojů.

Praktická část práce je zaměřena na testování a zjištění spolehlivosti u kamerových smart technologií Netatmo.

Na základě rozboru teoretických poznatků a výsledků praktické části práce, budou formulovány závěry diplomové práce.

Doporučený rozsah práce

50 až 60 stran včetně grafů, obrázků a tabulek

Klíčová slova

smart technologie, kamerové systémy, spolehlivost, rozpoznání obličeje

---

Doporučené zdroje informací

GARDNER, J W. – AWADELKARIM, O O. – VARADAN, V K. *Microsensors, MEMS, and smart devices.* Chichester: Wiley, 2001. ISBN 0-471-86109-.

Makin, D.A. , Jenkins, G., Gaffney, M. Civilizing Surveillance Practices: The Pullman Police Department Public Safety Camera Monitoring Internship Program. Journal of Applied Security Research. ISSN: 19361610

Mehta, Y. , Pai, M.M.M. , Mallissery, S. , Singh, S. Cloud enabled air quality detection, analysis and prediction – A smart city application for smart health. 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016. ISBN: 978-150901365-4

RASCH, D. *Mathematische Statistik : eine Einführung für Studenten der Mathematik, Statistik, Biometrie und Naturwissenschaften.* HEIDELBERG: BARTH, 1995. ISBN 3-335-00370-5.

ŘÍHA, Z. – RAK, R. – MATYÁŠ, V. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada, 2008. ISBN 978-80-247-2365-5.

Saponara, S., Pilato, L., Fanucci, L. Exploiting CCTV camera system for advanced passenger services on-board trains. 2nd IEEE International Smart Cities Conference, ISC2 2016. ISBN: 978-150901845-1

Sidhu, R.S. , Sharad, M. Smart surveillance system for detecting interpersonal crime. 2016 International Conference on Communication and Signal Processing, ICCSP 2016. ISBN: 978-150900396-9

ZACH, J. – DRÁPELA, K. *Biometrie, biostatistika : vybrané části.* Brno: Mendelova zemědělská a lesnická univerzita, 1996. ISBN 80-7157-234-9.

Předběžný termín obhajoby

2017/18 LS – TF

Vedoucí práce

Ing. Veronika Hartová, Ph.D.

Garantující pracoviště

Katedra vozidel a pozemní dopravy

Elektronicky schváleno dne 13. 1. 2017

doc. Ing. Miroslav Růžička, CSc.

Vedoucí katedry

Elektronicky schváleno dne 23. 1. 2017

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 07. 07. 2017

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma: **Spolehlivost rozpoznávání obličeje pomocí smart kamerových systémů** vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

Prohlašuji, že tištěná i elektronická verze diplomové práce jsou totožné.

…….

Bc. Josef Prachař

Poděkování

Tímto bych rád poděkoval vedoucí mé diplomové práce paní Ing. Veronice Hartové, Ph.D., za vedení diplomové práce, ochotu, trpělivost a cenné rady, které mi poskytla během konzultací. Závěrem moje poděkování patří mé rodině za duševní podporu při psaní diplomové práce, jakož podporu při celém studiu.

Abstrakt

Diplomová práce se zabývá spolehlivostí rozpoznávání obličeje pomocí smart kamerových systémů. Tato diplomová práce je rozdělena do dvou hlavních částí – teoretická a praktická. Teoretická část této diplomové práce je rozdělena do několika částí. Jedna z částí je věnována seznámení se smart kamerami a jejich komponenty, další část se zabývá vysvětlení pojmu biometrie a identifikačních metod a poslední část je věnována kamerovému systému, jež při výkonu své práce využívá Policie České republiky. Praktická část je zaměřena na testování a zjištění spolehlivosti u kamerových smart technologií.

Klíčová slova: smart technologie, kamerové systémy, spolehlivost, rozpoznání obličeje

Summary

This diploma thesis deals with the reliability of face recognition using smart camera systems. This diploma thesis is divided into two main parts - theoretical and practical. The theoretical part of this diploma thesis is divided into several parts. One part is devoted to familiarization with smart cameras and their components, the next part deals with the explanation of the concept of biometrics and identification methods and the last part is devoted to the camera system used in the performance of its work by the Police of the Czech Republic. The practical part is focused on testing and detecting the reliability of camera smart technologies.

Keywords: smart technology, camera systems, reliability, face recognition

Obsah

Obsah 7
1 Úvod 1
2 Cíle práce 2
3 Metodika práce 3
4 Přehled řešené tématiky 4
4.1 Smart technologie 4
4.2 Smart kamery 4
4.3 Komponenty Smart kamer 6
4.3.1 Snímač obrazu 6
4.3.2 Procesor 7
4.3.3 Datová a programová paměť (energeticky nezávislá flash a RAM) 8
4.3.4 Vstupy a výstupy 9
4.3.5 Komunikační rozhraní 9
4.3.6 Konstrukce inteligentní kamery 10
4.3.7 Software a programování 10
4.3.8 Využití inteligentních kamer 11
4.4 Firmy zabývající se vývojem biometrických systémů 12
4.4.1 Morpho 12
4.4.2 Eyedea Recognition 13
4.5 Biometrie 14
4.5.1 Biometrické identifikační metody 18
4.5.2 Geometrie ruky 18
4.5.3 Otisk prstu 19
4.5.4 Geometrie tváře 20
4.5.5 Duhovka oka 23
4.5.6 Sítnice oka 24
4.5.7 Identifikace na základě chůze 25
4.5.8 Behaveometrika 26
4.6 Autorizace obličejové biometrie 26

4.6.1 Identifikace osoby dle vnějších znaků 27
4.6.2 Klasická identifikace pomocí portrétu využívaná bezpečnostními složkami ... 28
4.6.3 Bezpečností a policejně-forenzní aplikace 29
4.7 Kriminalistická identifikace osob u Policie České republiky 31
4.8 Příklady kamerových systémů využívaných Policií České republiky 32
4.8.1 Městský kamerový dohlížecí systém 32
4.8.2 Kamerové systémy v policejních vozech 33
4.8.3 Ochrana letiště - zajištění zvýšení bezpečnosti na letišti Václava Havla Praha 35
4.8.4 Čtyři česká letiště dostanou moderní bezpečnostní prvky za půl miliardy 35
5 Praktická část práce 37
5.1 Použitá zařízení 37
5.1.1 Kamera Netatmo NSC01-EU 37
5.1.2 Síťová bezpečnostní kamera - Edimax IC-7113W 39
5.1.3 Otočná IP kamera - D-Link DCS-5030L 40
5.2 Výsledky měření 42
5.2.1 Multikriteriální analýza dat 45
5.2.2 Parametry pro konečné hodnocení 45
6. Závěr 48
Seznam literatury 50
Seznam obrázků 54
Seznam tabulek 55
Seznam grafů 55

1 Úvod

Metody rozpoznávání obličeje jsou velmi obtížnou disciplínou, která lidstvo provází již od pravěkých dob, kdy lidé neměli k dispozici takové autorizační prostředky, jako mají lidé k dispozici v dnešní době. Identifikace pomocí rozpoznávání obličeje je velmi úzce spojená s bezpečností. Již v pravěkých dobách byli lidé nuceni v rámci bezpečnosti vlastní či bezpečnosti smečky rozeznat přítele od nepřítele. K tomuto účelu využívali právě identifikaci pomocí rozpoznávání obličeje. Tato vlastnost je u člověka vyvíjena od prvního okamžiku po narození, kdy je dítě schopno bez bližší souvislosti zřetelně rozeznat tváře. Jako první je schopno novorozeně rozeznat od všech ostatních matku, s níž je velmi blízkém kontaktu od narození. [1,2]

Identifikace a její metody se v průběhu času neustále vyvíjela a zdokonalovala se. Od počátečných primitivních metod až po současné modernější metody. V průběhu času se metody identifikace osob začaly dělit podle nejrůznějších kritérií. V současné době je možné osobu identifikovat nejen podle tváře, ale také podle také podle jeho vlastnictví (záznam na matrice, osobní údaje, identifikační průkazy), tak podle znalosti člověka (rodinná historie, přezdívky, rodinný stav, hesla), a v neposlední řadě také podle dalších biometrických a behaviorálních metod (otisk prstu, DNA, styl chůze, sken duhovky či sítnice, geometrie ruky, styl písma). [1,3]

V současné bezpečnostní situaci se stává identifikace osob jednou z hlavních priorit a na toto odvětví kladen čím dál tím větší důraz. Je kladen důraz na rychlejší, komplexnější a co nejpřesnější identifikaci podezřelé osoby v davu a zabránění tak případně katastrofy v podobě útoku na osoby či majetek. Čím dál více se využívají kamerové systémy, které se neustále vyvíjí, jsou propojovány s nejrůznějšími databázemi bezpečnostních složek. Jsou schopné identifikovat podezřelé chování a upozornit na ně příslušné bezpečnostní složky. [1,2]

Kamer a kamerových systémů je v současné době velké množství. Otázkou zůstává, jak moc jsou kvalitní? Dokážou plnit svou úlohu na 100%? Jaké kamerové systémy jsou dostupné v České republice? Jsou kamerové systémy používané bezpečnostními složkami stejně kvalitní jako systémy, jež jsou používané v soukromém sektoru? Těmito otázkami se bude zabývat praktická část této diplomové práce. [2]

2 Cíle práce

Cílem diplomové práce je zaměřit se na spolehlivost současných kamerových smart technologií s funkcí rozpoznání obličeje. Hlavním cílem je provést testování určených technologií a jejich následné hodnocení. Dílčí cíle diplomové práce je vytvořit přehled řešené problematiky, provést rozbor současných smart kamerových technologií, provést sadu testování a měření spolehlivosti kamer Netatmo a provést finanční hodnocení kamerových systémů s detekcí obličeje. Další cíl diplomové práce je seznámení s historií identifikace osob a zejména vědní disciplíně zvaná Biometrie. Zde jsou popsány vědní obory identifikace osob např. otisku prstu - daktyloskopie, geometrie tváře, identifikace na základě chůze aj., kriminalistické metody, které používá Policie ČR.

Dílčí cíle:

- Vytvořit přehled řešené problematiky
- Zaměření se na spolehlivost současných kamerových smart technologií s funkcí rozpoznání obličeje.
- Představení dvou firem se sídlem v České republice, které se zabývají vývojem biometrických systémů, které pomáhají firmám a společnostem v nejrůznějších odvětvích při ochraně osob či majetku.
- Zaměření se na obor Biometrie, jehož náplní je studium a zkoumání živých organismů (obzvláště pak člověka).
- Představení některých kriminalistických metod používaných Policií ČR.
- zjistit spolehlivost kamery Netatmo s funkcí rozpoznávání obličejů.
- Provést finanční zhodnocení třech kamer s funkcí detekce obličeje.

3 Metodika práce

Teoretická část této diplomové práce bude vycházet především z knižních publikací, dále pak z internetových zdrojů a přístupných skript. Teoretická část bude rozdělena do dvou hlavních částí. První část řešené problematiky v teoretické části této diplomové práce bude zaměřena na objasnění pojmů smart kamer, jejich konstrukci a části. Dále bude v této první části představeno využití smart kamer a budou zde představeny dva zástupci firem zabývající se vývojem a inovacemi softwarů pro identifikaci osob a předmětů. Druhá část řešené problematiky v teoretické části této diplomové práce bude zaměřena na objasnění pojmu biometrie, představení některých biometrických metod identifikace osob, vysvětlení a přestavení autorizace obličejové biometrie a jejího využití ve forenzních a bezpečnostních aplikacích a v poslední řadě zde budou přestaveny ukázky kamerových systémů, které při své práci využívá Policie České republiky.

V praktické části bude provedeno měření ve vestibulu kancelářských prostor nejmenované firmy, kde se každodenně pohybuje 12 zaměstnanců této firmy. Měření bude probíhat od rána v čase docházky pracovníků do zaměstnání až do večerních hodin. První týden bude kamera volně zapnuta za účelem uložení jednotlivých obličejů zaměstnanců. Samotné měření pak proběhne kontinuálně po dobu 3 měsíců. Na základě získaných dat bude provedeno vyhodnocení a budou stanoveny závěry, jak vysoká je spolehlivost konkrétní kamery a to jak za standardního osvětlení nebo za šera či tmy. Následně bude provedena multikriteriální analýza dat, kdy budou porovnány tři nejprodávanější výrobky společnosti Alza v určité cenové relaci. Závěrem bude provedeno vyhodnocení a stanoveno pořadí těchto třech výrobků.

4 Přehled řešené tématiky

Tato kapitola shrnuje kompletně celý přehled řešené problematiky této diplomové práce. Kapitola je rozdělena do tří hlavních částí. První část je věnována smart technologiím, potažmo smart kamerám, především pak popisu co to smart kamery vůbec jsou a dále pak jejich komponentům a druhům. Tato část se také věnuje představení firem, které se vývojem těchto kamer zabývají. Druhá část je věnována biometrii. Zde je věnována pozornost vysvětlení pojmu biometrie, dále jsou zde představeny některé vybrané metody identifikace osob a také druhy identifikace, kterou jsou využívané bezpečnostními složkami. Poslední kapitola je věnována představení kamerových systémů, které využívá při své práci Policie České republiky.

4.1 Smart technologie

Smart technologie neboli inteligentní technologie jsou technologie, které zahrnují aplikace logické i fyzické ve všech formátech. Schopností těchto technologií je automatické přizpůsobení se a modifikace své chování tak, aby technologické senzory, jež poskytují konečná data pro analýzy, byly kompatibilní s prostředím a smysly věcí. Smart technologie jsou schopné učení se, využívání nově nabitých zkušeností ke zlepšení svého výkonu, či předpokládání, myšlení a úvahách o dalších krocích, mají také schopnost být soběstačné a nezávislé. [1]

4.2 Smart kamery

Jako smart kamery jsou označovány ty kamery, které se vyznačují schopností přijímat obrazy a zároveň dávají smysl dění v přijímaných obrazech. V jistých případech jsou smart kamery schopny provádět jisté úkony za osobu, jež kameru užívá. Jako smart kameru je možné označit kupříkladu takovou kameru, která je nastavena na snímání pohybu u vstupu do budovy a při nepovoleném vstupu či podezřelém pohybu je schopna spustit poplach či uživatele o podezřelém pohybu či nepovolnému vstupu informovat pomocí emailu či sms zprávy. Smart kamery jsou schopné vyhodnotit situaci (v tomto případě nepovolený vstup či podezřelý pohyb) a přijmout adekvátní opatření (spuštění poplachu či odeslání zprávy uživateli). [2]

I přesto, že se tento popis může jevit jako technická definice pojmu smart kamery, není tomu tak. V současné době existuje velké množství definic pojmu smart kamera, které však nemusí být technicky korektní. Mnoho současných definic smart kamery definuje jako přístroje se zabudovanou schopností zpracování obrazu. Avšak tuto skutečnost lze aplikovat na prakticky téměř všechny v současnosti používané kamery či fotoaparáty. Dle publikace Smart Cameras je vlastnost, která odděluje inteligentní kamery od kamer neinteligentních skutečnost, že jsou schopné generovat prostřednictvím vestavěného obrazového procesoru primární vstup či výstup. Pro účel této diplomové práce lze inteligentní kamery definovat jako zabudovaný systém vidění, který je schopen extrahovat ze zachycených obrazů informace specifické pro určitou aplikaci. Spolu s touto vlastností jsou inteligentní kamery schopné vygenerovat popis dané události či učinit rozhodnutí, která jsou v automatizovaných a inteligentních systémech používána. [2]

V definice uvedené výše je několik důležitých aspektů, které jsou vysvětleny v bodech níže:

- „vision systém“ znamená, že kamera je schopna zachytit pohyb či objekt vyfotografovat. Slovo vision v tomto kontextu označuje vlastnost, kdy kamera není schopná zachytit pouze světlo viditelné, ale i ostatní barevná spektra, mezi která řadíme infračervené spektrum či tepelné snímání. Pojem „systém“ v této definici znamená, že všechny komponenty zabudované ve smart kameře nemusí být nutně její součástí.
- „usazení“ interpretuje schopnost smart kamery fungovat automaticky a autonomně prostřednictvím využívání všech zabudovaných komponentům jako jsou paměť, mikroprocesor, komunikační rozhraní či napájení
- „generace rozhodnutí či popisu událostí“ definuje primární funkci smart kamery jakožto přístroje, jež není schopný pro uživatele pouze zhotovovat fotografie či videa, ale je schopný stanovit zdali došlo k předem definované události a pracovat s touto událostí dál. [2]

Není pravidlem, že kamery či fotoaparáty, které mají zabudované zpracování obrazu, bývají označovány jako inteligentní. Hlavním kritériem při posuzování zdali lze kameru označit jako inteligentní je obrazové zpracování. Velké množství kamer určených pro spotřebitele má v sobě zabudované složité zpracování obrazu a signálů, které má energii k dokončení funkcí, mezi které jsou řazené například automatické zaostření či vyvážení bílé barvy nebo automatické ostření a komprese obrazu. Kdežto primárním účelem inteligentních

kamer je generace popisu zachycených rozhodnutí a událostí a pro další přístroje v automaticky řízeném systému. Tento účel inteligentních kamer je zjevný především ve dvou nejrozšířenějších oblastech využití, které jsou video sledování a průmyslově strojnímu sledování. Díky tomu, že každá inteligentní kamera obsahuje v každé jednotce inteligentní procesory, jsou takové kamery vhodné zejména tam, kde je třeba sledovat či zajistit větší objekty pomocí rozloženého vidění, kde kamery musí pracovat asynchronně a nezávisle. [2,3]

4.3 Komponenty Smart kamer

Smart kamery většinou obsahují níže uvedené komponenty, které tvoří základní části, ne vždy je musí obsahovat všechny. Jedná o část prvků snímání a digitalizace, dále pak výpočetní část, vstupy a výstupy a v neposlední řadě také komunikační rozhraní. [3,4]

4.3.1 Snímač obrazu

Snímač obrazu je přístroj, který je tvořen soustavou jednoduchých foto senzorů, které jsou schopné přenést komplexní obrazovou informaci na elektrický signál. Tyto snímače bývají nejčastěji používány v zařízeních na zachycení komplexní obrazové informace, mezi které se řadí například digitální fotoaparáty a kamery či nejrůznější typy skenerů. První elektrické kamery sloužící k zachycení obrazu, využívali k jeho zachycení a k následnému převodu na elektrický signál snímač elektronky, který byl zanedlouho nahrazen křemíkovými mikročipy na bázi CCD či později pak CMOS. Oba dva tyto snímače obrazu pracují na stejné bázi, oba dva jsou určené k zachycení obrazu a k jeho následnému převodu do elektrické informace. Obrazy a věrnosti barev z obou těchto snímačů jsou takřka totožné a ani jeden z nich nepřevyšuje ten druhý. Jediný rozdíl mezi těmito dvěma snímači je v jejich výrobě a provozních parametrech. [5]

Jednotlivé fotobuňky, nacházející se v CCD senzoru jsou analogové – pasivní. Generace elektrického náboje probíhá až poté, co světlo na fotobuňku dopadne, což se projeví jako změna napětí na kontaktu jednotlivé fotobuňky. Po změření a zpracování ovládacím obvodem je výsledný produkt v podobě digitální informace spolu s elektrickou podobou obrazu, jež dopadl na celou plochu senzoru soustavy fotobuněk. Největším omezením CCD senzoru nejsou finanční prostředky či nákladná výroba, ale některá omezení, mezi které patří hlavně rychlost. [5]

Oproti tomu v obrazovém čipu CMOS se nacházejí aktivní jednotlivé fotobuňky, jež jsou vyrobeny polovodičovou technologií CMOS. Jednotlivé fotobuňky v tomto čipu mají svou vlastní fotodiodu, přes kterou je periodicky veden elektrický impuls, jehož změna parametrů nastává vždy po dopadu světla na fotodiodu. Následně nastává velmi podobný proces jako v případě CCD senzoru. Obrazový čip CMOS má stejně jako CCD senzor své výhody i nevýhody. Jelikož se jedná o složitější strukturu obrazového senzoru, je samotná výroba náročnější což znamená vyšší finanční náklady. Avšak oproti CCD senzoru je obrazový čip CMOS mnohem rychlejší, což je v případě obrazového zpracování velmi zásadní a důležitý faktor. [5]

Výkon snímače obrazu lze hodnotit několika hledisky. Mezi tři nejčastější posuzované parametry patří dynamický rozsah, citlivost při slabém světle a odstup šum-signál. [5]

Barevné snímače obrazu lze rozdělit do několika základních typů, které se liší v principu separace samostatných barev. Všechny barevné snímače musí splňovat stejnou podmínku a to, že vždy musí sestavit jeden plnobarevný bod ze tří základních barev, jež jsou modrá, zelená a červená, neboli RGB. [5]

4.3.2 Procesor

Centrální procesorová jednotka, neboli CPU je soubor elektronických obvodů nacházejících se uvnitř počítače, jež na základě návodu provádějí sadu základních aritmetických, logických, vstupních a výstupních operací a jejich následnou kontrolu. Pojem centrální procesová jednotka je používám od počátku 60. let. [6]

Centrální procesorová jednotka v průběhu let změnila svou formu a způsob implementace, avšak její základní funkce zůstaly takřka stejné. Jedna z hlavních součástí centrální procesorové jednotky se nazývá aritmetická logická jednotka neboli ALU. Hlavním úkolem této jednotky je realizovat logické a aritmetické operace, a dále pak registry procesorů. Tyto procesory pak odesílají operace do aritmetické logické jednotky, které následně pak výsledky jednotlivých operací ukládají. Další hlavní součástkou centrální procesorové jednotky je řídící jednotka, která řídí načítání dat z paměti a vykonáváním těchto úkonů řídí činnost aritmetické logické jednotky, nejrůznějších registrů a dalších důležitých součástí. [6]

Často bývá v chytrých kamerách používán, tzn. digitální signálový procesor, neboli DSP. Tento procesor je specializovaný mikroprocesor, jehož architektura je optimalizovaná pro nutné provozní nároky pro digitální zpracování signálu. Mezi hlavní cíle digitálního signálového procesoru je zpravidla komprese komunálních reálných analogových signálů, měření či filtrování, či provádět algoritmy zpracování digitálního signálu. Tyto procesory jsou díky své speciální paměťové výstavbě schopny načítání více instrukcí či dat najednou. [7]

4.3.3 Datová a programová paměť (energeticky nezávislá flash a RAM)

Energeticky nezávislá flash je typ počítačové paměti, kdy je možné načíst již uložené informace rovněž poté, co bylo zařízení vypnuto a opětovně zapnuto. Opak energeticky nezávislé paměti je tzv. volitelná paměť, která pro uchování dat a zabránění jejich smazání potřebuje stálý výkon. Jako příklad energeticky nezávislé je možné uvést flash paměti, FRAM paměť, většina počítačových paměťových zařízeních na magnetické bázi jako SSD pevné disky či pevné disky. Tento druh paměti bývá velmi často využíván jako druhotné úložiště nebo jako prostředek k dlouhodobému ukládání dat. V současné době je nejrozšířenější primárním úložištěm volatelní paměť RAM. Znamená to, že vše, co je v této paměti uloženo je v okamžiku vypnutí počítače ztraceno. Většina těchto forem nezávisle volatelných pamětí není z důvodu ceny a či nižšího výkonu nebo horší odolnosti zápisu, vhodná k použití jako primárná paměti. V tomto případě je lepší použití volatelní paměti s nahodilým přístupem. Ukládání dat je možné rozdělit na elektronicky a mechanicky adresované systémy. Jako příklad elektronicky adresovaného systému můžeme uvést nejrůznější paměti pro čtení. Tyto paměti jsou oproti mechanicky adresovaným systémům, mezi které řadíme například pevné či optické disky, které jsou pomalé a mají nízkou cenu za jeden bit, dražší, ale zato rychlejší. [8]

Jak již bylo řečeno výše, paměť RAM je volitelná polovodičová paměť určená pro takřka okamžitý zápis a čtení jakékoliv buňky nacházející se v paměti. Paměť RAM má neomezený počet zápisů a čtení, avšak po vypnutí napájení této paměti dochází k zapomenutí dat. Z tohoto důvodu je nutné data a informace, jež mají být zachovány, ukládat na nevolitelné paměti jako jsou nejrůznější druhy disků či flash pamětí. [9]

4.3.4 Vstupy a výstupy

Inteligentní kamera se díky digitálním výstupům přibližuje standardním senzorům. Toto přiblížení je důvod, proč jsou inteligentní kamery stejně provedeny. Jedná se především o otevřené konektory PNP či NPN, jen v sobě mají ochranu proti přepólování či proti poškození vzniklé napěťovou špičkou, které může vzniknout při spínání indukční zátěže a pracovní napětí o velikosti do 30 V. Aby mohly být synchronizované snímané obrazy se stavem procesu, je nutné mít digitální vstupy. Aby byl snímaný objekt kvalitně sejmut, je nutné ho sejmout v určité poloze. Kameru je možné spustit několika způsoby, například pomocí signálu z řídicího systému či prostřednictvím čidla přiblížení. U inteligentních kamer nebývají často galvanicky odděleny vstupy a výstupy od napájecího napětí, stejně jako nebývají odděleny navzájem. Inteligentní kamery bývají nejčastěji využívány stejně jako běžné senzory lokálně, umístěním na zařízení, které má jedno napájení, kde není riziko velkého rozdílu potenciálu. Vzhledem k neustále minimalizaci inteligentních kamer často výrobci přistupují k odklonu od v průmyslové elektronice používaných norem. Jsou proto vyráběny i kamery, jež mají vstupy a výstupy na úrovni TTL. Tyto kamery potřebují k tomu, aby mohly být připojeny do průmyslového provozu galvanicky oddělený převodník úrovní a napájení z externích zdrojů. Jsou i kamery, kde jsou vstupy a výstupy zcela vynechány a je třeba je nahradit I / O připojení ke komunikačnímu rozhraní, což instalaci inteligentní kamery velmi prodražuje. [4]

4.3.5 Komunikační rozhraní

Komunikační rozhraní u inteligentních kamer zastává hned pár důležitých funkcí. Jednou z nedůležitějších funkcí rozhraní je připojení k HMI zařízení. Pomocí HMI zařízení, jež je v dnešní době používáno jako standardní používaný modelu PC, je možné inteligentní kameru nastavit či naprogramovat. Aby mohla být daná úloha pohodlně a rychle zpracována, je třeba, aby snímky zachycené HMI probíhaly v reálném čase. Vzhledem k tomu, že rychlost přenosu musí být relativně velká, bývá jako základní komunikační rozhraní využíván Ethernet. [4]

Mezi další funkce komunikačního rozhraní může být zařazen přenos dat do nadřazeného řídící systému. Dále pak ke komunikačnímu rozhraní může být připojen modul, díky kterému je možné rozšířit počty vstupů a výstupu. Komunikační rozhraní může v případě potřeby komunikace mezi více kamerami sloužit jako jakýsi zprostředkovatel komunikace

mezi nimi. V neposlední řadě bývá toto rozhraní používáno k servisu, při výměně firmwaru a dalších účelech. [4]

4.3.6 Konstrukce inteligentní kamery

Konstrukce inteligentní kamery po mechanické stránce není prozatím standardizována. Konstrukce inteligentní kamery se v současné době velmi podobá běžné průmyslové kameře, avšak s tím rozdílem, že inteligentní kamera má více připojovacích míst. Mezi tyto místa patří místo pro vstup a výstup výše zmiňovaného komunikačního rozhraní. Inteligentní kamery bývají mnohými výrobci doplňovány o vestavěný kruhový LED osvětlovač, který je zobrazen na obr. 1, který se však hodí pouze pro plnění nejjednodušších úkolů stojového vidění. [4]

Obrázek 1 - *Inteligentní kamera se zabudovaným LED osvětlením*

[10]

4.3.7 Software a programování

Do inteligentní kamery není možné instalovat kterýkoliv existující software, což je dáno především úzkou souvislostí mezi technickými prvky, mezi které patří omezený rozsah paměti, mikroprocesor, počty vstupů a výstupů či připojení snímacího čipu. Oproti standardním video senzorům by měla inteligentní kamery dokázat zpracovat pokud možno či nejširší počet úkolů strojního vidění. [4]

Software inteligentních kamer, jež plní běžné úkoly strojního vidění, by měl být schopen provádět několik základních operací. Mezi tyto operace patří zpracování (objevení hran a jejich převod do vektorů, či analýza jasu nebo vyhledávání kontrastních předmětů) a měření obrazu (určení vzdálenosti v obraze ve vektorech). Dále pak četba textu a čárových či maticových identifikačních kódů, manipulace s hardwarem inteligentní kamery (obsluha komunikačního rozhraní, vstupů a výstupů či správa snímacího čipu. V neposlední řadě je to pak při složitějších úkolech zpracování dat, kde jsou při zpracování využívaný statistické či matematické postupy a možnost sestavení uživatelského programu. [4]

U inteligentních kamer existují dva způsoby řešení plnění těchto úkolů. Jsou výrobci inteligentních kamer, které je uživateli dodávají pouze s operačním systémem. Další potřebné nástroje jsou uživateli dodány jako knihovna funkcí pro obecný jazyk pro programování, kde má uživatel možnosti prostřednictvím tohoto využití těchto funkcí si program pro daný úkol napsat sám, přeložit ho a implementovat do paměti programu inteligentní kamery. I přes veškeré snahy dodavatelů knihoven doplňovat je nejrůznějšími simulátory či jinými prostředky, jež konečnému uživateli mají usnadnit práci, tak je vždy výsledek závislý na programovacích schopnostech programátora. U složitějších systémů se při programování používají grafická vývojová prostředí, která jsou zobrazována na PC, jež je k systému připojeno. Toto prostředí kooperuje s firmwarem inteligentní kamery a uživateli tak umožňuje využívat nástrojů či senzorů, jež jsou orientovány na základní operace, které probíhají při řešení úkolů strojového vidění. Uživatel zde může nalézt nástroje určené k detekci kontrastního rozhraní či kontrastních předmětů, nebo pro nastavení chování komunikačního rozhraní, vstupů či výstupů. Působení nástroje obrazu a výstup obrazu je nejzřejmější ve vývojovém prostředí, kdy je jejich výsledek interpretován ve formě logické hodnoty jako výsledek inspekce. Výstupem této inspekce může být výsledek dobrý / vadný. Následný inspekční program je sestaven pomocí seřazení nástrojů do tabulky případně do vývojového diagramu. Aby mohl uživatel v tomto vývojovém prostředí vytvořit aplikační program, nepotřebuje k tomu žádné znalosti programování. Uživatel se tak může zaměřit na získávání důležitých a spolehlivých informací o prověřované vlastnosti zobrazeného předmětu. [4]

4.3.8 Využití inteligentních kamer

Inteligentní kamery mají v současné době čím dál tím větší využití. Je to především z důvodu jejich rostoucímu výkonu a schopnosti spolupráce v síti. Inteligentní kamery jsou v současné využívány v mnoha odvětvích a oborech. V průmyslu zastávají úlohy a úkoly,

které v minulosti byly schopné zastávat pouze velké systémy strojového vidění. Dalším využitím v průmyslovém odvětví je nahrazení standardních senzorů přiblížení právě inteligentními kamerami. Inteligentní kamera je schopná v jedné operaci provést najednou kontrolu správnosti výšky hladiny, dále pak zdali je správně nasazen uzávěr a nalepená etiketa. [4]

Dalšími odvětvími, kde jsou inteligentní kamery využívány je komerční a bezpečnostní průmysl. Velkou výhodou využití inteligentních kamer je fakt, že pracoviště, kde monitorování probíhá, není závislé na místě a umožňuje tak realizovat i vzdálený monitoring prostoru. [11]

Inteligentní kamerové systémy jsou používány zajištění bezpečnosti osob a majetku a jsou využívány všemi bezpečnostními složkami. Tyto systému jsou implementovány a využívány na letištích, v bankách, v institucích, kde probíhají práce s penězi, na nádražích, na veřejných prostranstvích, v obchodních centrech, na finančních úřadech, při různých akcích, kde se shromažďuje velké množství lidí a dalších podobných institucí. [11]

4.4 Firmy zabývající se vývojem biometrických systémů

Existuje několik firem, které se zabývají vývojem biometrických systémů, které pomáhají firmám a společnostem v nejrůznějších odvětvích při ochraně osob či majetku. Níže budou představeny dvě z těchto firem.

4.4.1 Morpho

Společnost Morpho začala svou činnost již v roce 1924 pod názvem Sagem. V průběhu času prošla firma vývojem, nejrůznějšími fúzemi a změnami názvů. V současné době působí v 55 zemích celého světa. K zemím, ve kterých společnost Morpho působí, patří například Francie, Albánie, Rakousko, Argentina, Kanada, Čína, Kolumbie, Německo, České republika, Mexiko, Peru a další. Firma se zabývá řešením pro personalizaci a inteligentní karty, které podporují také řešení nejen biometrická, ale také řešení pro rozvoj bezpečnosti nejrůznějších transakcí a vývoj IT. [12]

V České republice firma Morpho působí od roku 1995. Sídlo české pobočky se nachází na severu Moravy ve městě Ostrava a pracuje zde více než 200 vysoce kvalifikovaných pracovníků. Česká pobočka zajišťuje personifikaci, výrobu a následným

plněním a balením nejrůznějších druhů karet, jako jsou karty bankovní, zdravotní, pojišťovací nebo přepravní. Česká pobočka společnosti Morpho se pyšní vlastním vývojovým centrem a týmem, jež se zabývá efektivním řešením personalizace a digitalizací procesů pro karty. Prostřednictvím odbornosti české pobočky mohly být oblasti karet a dalších nositelných materiálů realizované speciální inovační projekty, mezi které patří Style2Pay, 3D karta či specializované biometrické projekty určené pro speciálně pro nejrůznější finanční instituce. [13]

V globálu se společnost Morpho zabývá inovacemi v oboru biometrických řešení ve třech oblastech. Těmito oblastmi jsou občanská identita (výdej bezpečných průkazů totožnosti, sčítání lidu a registr občanů – biometrický registr občanů), veřejná bezpečnost (podpora v oblasti vymáhání práv, usnadnění cestování osob na letištích, bezpečný vstup a přístup k veřejným budovám či do kritických míst infrastruktury) a v neposlední řadě také v oblasti digitálního zabezpečení (bezpečnost transakcí, plateb, bezpečnost v oblasti zdravotní péče a online ověřování). [12]

4.4.2 Eyedea Recognition

Společnost Eyedea Recognition s. r. o. vznikla jako universitní spin-off na Českém učení Technickém v Praze v roce 2006. Je to technologická společnost, jejíž hlavní náplní je vývoj a dodávání rozvinutých softwarových nástrojů určených k analýze obrazu, jež je založena na metodách pro strojové učení a umělé inteligence. Jejím hlavním zaměřením je vývoj softwarů určených k detekci a rozpoznávání objektů nacházejících se na snímcích. Společnost Eyedea Recognition s. r. o. se angažuje v několika oblastech rozpoznávání a identifikace objektů (osoby i věci). [14]

Mezi produkty firmy Eyedea Recognition patří například Eyeface SDK jež je specializuje na rozeznávání a hodnocení obličejů z hlediska pohlaví a věku. Tento systém je velmi často používám například při měření sledovanosti a zásahu reklamních ploch, počítání osob na snímku či v záběru a v dalších podobných směrech. [15]

Dalším produktem zabývajícím se rozpoznávání obličeje je forenzní software Eyeidentity. Tento software slouží k detekci obličejů na snímcích i videozáznamech. Tento software není závislý na světle, postoji osoby či obličejovém výrazu, díky podobnostní metrice dokáže rozeznat osobu z milionu zaznamenaných osob. Software podporuje většinu již existujících formátů obrazu a videa. Uživatel tohoto systému je oprávněn ke správě

databáze osob, dále pak ke zpracování obrazových a videozáznamů z probíhajících případů a zadání porovnání s databází. Tento software je velmi často využívám bezpečnostními složkami, mezi které patří Europol, Francouzská policie či Policie České republiky. [16]

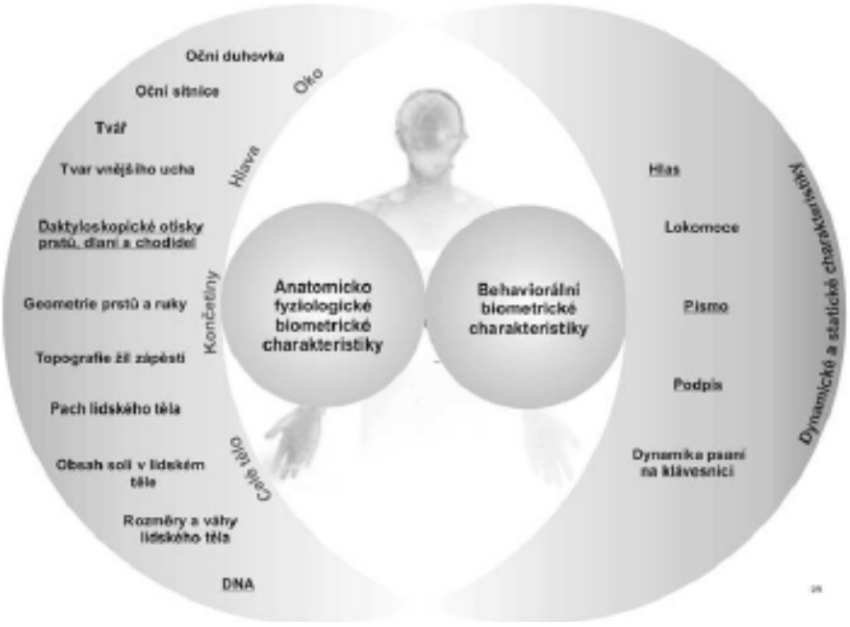
Další oblastí využití softwarů této firmy je identifikace vozidel, kdy jsou softwary schopny rozeznat o jakou kategorii, typ, výrobce a barvu vozidla se jedná. Na to je navázán software na čtení poznávacích značek vozidel. [15]

V neposlední řadě se firma zabývá také softwary na detekci zorniček a analýzy pohybu oka, což umožňuje například postiženým osobám ovládat jejich počítač pouze pomocí pohybu oka. Dalšími softwary jsou softwary na pro detekci obsahu videa či software, jež sledují neoprávněné užití obrázků daného klienta nacházejícího se na internetu. [15]

4.5 Biometrie

Biometrie je obor, jehož náplní je studium a zkoumání živých organismů (obzvláště pak člověka) a měří jejich anatomických a fyziologických vlastností včetně jejich behavioristických charakteristik. Behavioristické vlastnosti nejsou v praxi využívané tak často, jako vlastnosti anatomické a fyziologické, jež znázorňuje obr. 2. Tyto celkové charakteristiky jsou snímány, zpracovávány, vyhodnocovány a následně uchovávány v procesu verifikace a identifikace. [17,29, 34,37]

Obrázek 2 - *Dva druhy základních přístupů k členění biometrické identifikace*



[18]

Anatomické a fyziologickými vlastnosti jsou vlastnosti vztahující se k tělesnému tvaru. Pro verifikaci či identifikaci jsou využívány vlastnosti založené na vědeckých poznatcích o lidském těle. Mezi tyto vlastnosti je možno zařadit rozpoznávání obličeje, topografii žil na zápěstí, lidský pach, obsah soli v lidském těle, váha a rozměr lidského těla, DNA, otisky prstů, rozpoznávání duhovky či sítnice nebo například geometrii rukou. [18,34,36]

Oproti tomu behavioristické vlastnosti jsou vlastnosti vztahující se k projevům chování člověka a jsou unikátní a nestále v čase. Odborníci do behavioristických vlastností řadí také hlas člověka, chůzi a pohyb lidského těla jako celku i jeho částí či styl a dovednost psaní. Při identifikaci či verifikaci prostřednictvím psaní se rozlišujeme několik způsobů identifikace. Jedná se o podpis osoby, styl psaní souvislého textu či o dynamiku psaní na počítačové klávesnici. [18,38]

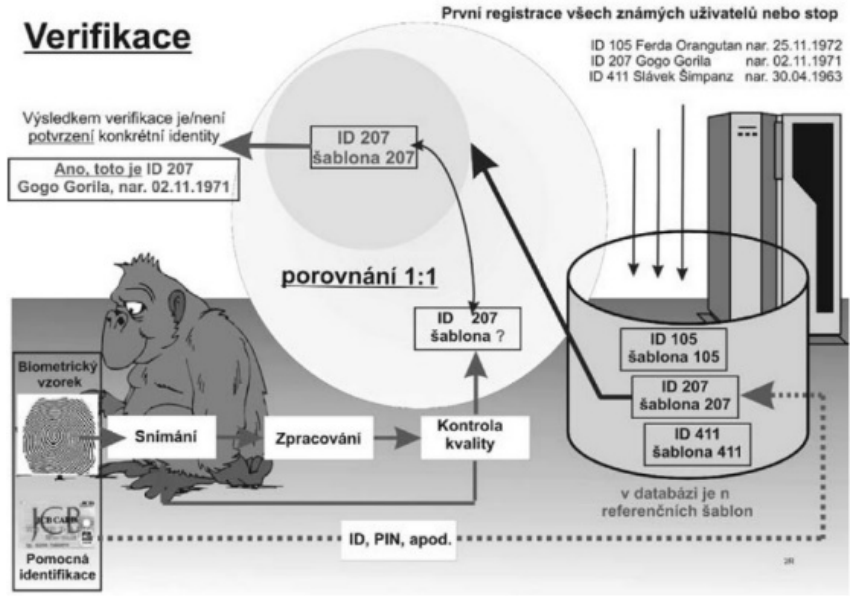
Biologické vlastnosti k rozeznávání člověka byly využívány již v historii. Lidé se v historii poznávaní podle charakteristických znaků ve tváři, či pomocí otisků dlaní v jeskyních, které soužily jako jakýsi podpis autora kresby či sdělení. Na konci 60. let se díky vývoji počítačových technologií začalo stávat biometrické rozeznávání osob více automatizovaným. V praxi jsou k identifikaci osoby používány biologické vlastnosti mnohem častěji než vlastnosti behavioristické. [17,32]

Rozpoznávání (recognition), tento pojem nemusí nutně znamenat verifikaci či identifikaci. Týká se to spíše rozpoznáváním osoby dle použití určité a vhodné tělesné vlastnosti. Může se jednat například o rozpoznávání otisků prstů, kdy ověřujeme shodu dvou lidských otisků prstu či o rozpoznávání obličeje nebo ručně psané rozpoznávání, kdy je autor rozpoznávám dle konkrétního rukopisu. A v neposlední řadě je možné také hovořit o iris rozpoznáváním, jež pro identifikaci osoby používá matematické techniky rozpoznávání vzoru jedné či dvou kostek očí osoby zobrazených na obrazových snímcích. [17,19]

Ověřování neboli verifikace je pojem označující proces kontroly pravosti. Je to proces, během kterého se biometrický systém snaží potvrdit totožnost prokazující se osoby se vzorkem zapsaným v minulosti v databázi. Hovoříme zde o principu one-to-one. Tento proces je obdobou procesu identifikace, avšak s tím rozdílem, že je rychlejší, hardwarově nenáročný a jednodušší. Postup verifikace je velmi jednoduchý, kdy je nejprve biologický vzorek snímán, následně je vytvořena šablony. Nasnímaný vzorek následně prochází kontrolou kvality a v konečné fázi je porovnán se šablonou patřící subjektu uloženou v databázi. Na

základě vyhodnocení porovnání snímku biologického vzorku a šablony dojde k rozhodnutí. Celý proces je znázorněn na obr. 3. [17,18,32]

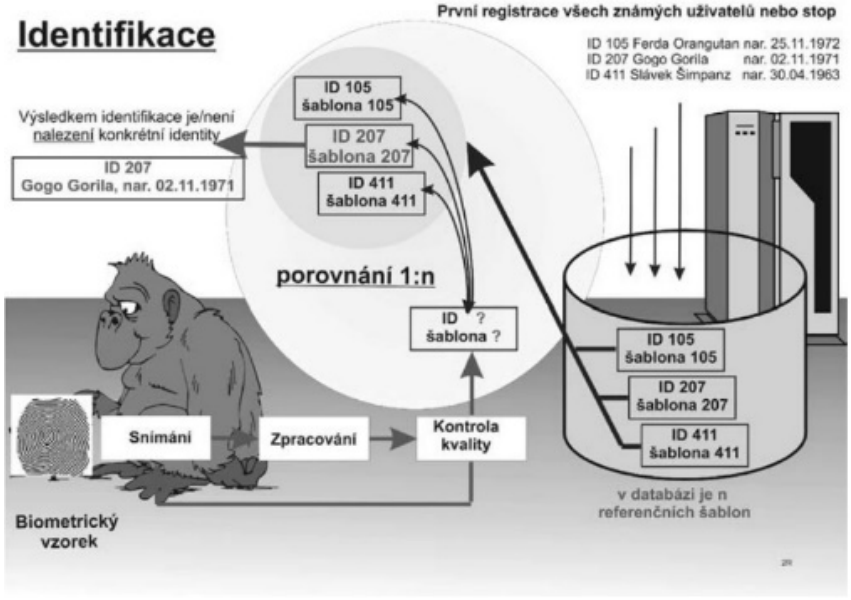
Obrázek 3 - *Verifikace*



[18]

Identifikace je pojem, jenž označuje proces, kdy se biometrický systém snaží ztotožnit neznámou osobu. Jejím cílem je snaha zjistit, zdali nově nasnímaný vzorek odpovídá některé z šablon v databázi. Jedná se o princip one-to-many, kdy je vzorek nasnímán, následně je vytvořena šablona, stejně jako u verifikace i zde dochází ke kontrole kvality snímku vzorku a porovnání se všemi uloženými šablonami v databázi. Na základě vyhodnocení dochází k rozhodnutí. Celý popis identifikace je znázorněn na obr. 4. [17,18]

Obrázek 4 - *Proces identifikace*



[18]

Můžeme rozlišit dva druhy identifikace a to pozitivní a negativní. Pozitivní identifikace si klade za cíl potvrzení totožnosti osoby, za kterou se daný vzorek vydává. V zásadě pozitivní identifikace spočívá v nalezení shody šablony a zkoumaného vzorku. V případě, že ke shodě dojde, je osobě přístup povolen. V případě nenalezení shody je osobě přístup zamítnut. Kdežto cílem negativní identifikace je ztotožnění osoby a určení, že tato osoba není ta osoba, za kterou se vydává. V případě, že je v databázi nalezena shoda s touto osobou, je této osobě přístup zamítnut. V opačném případě, pokud daná osoba nebyla v databázi nalezena, je jí přístup povolen. [18]

Autorizace je proces, který je možné spojit s procesem rozpoznávání. Rozdíl mezi autorizací a rozpoznáváním je ten, že při autorizaci dochází na konci tohoto procesu k přidělení dané určitého statusu (oprávněn / neoprávněn). Existují tři základní metody autorizace. Jedná se o autorizaci pomocí hesla, kdy je heslo použito jako prostředek pro přístup do systému. Autorizace heslem je v současné době nejvyužívanějším procesem na světě. Další metodou autorizace je autorizace prostřednictvím předmětu, kdy každý uživatel vlastní speciální předmět neboli token, jímž se musí při vstupu či přihlášení do systému prokázat. Poslední metodou autorizace je biometrická autorizace, kdy je pro identifikaci osoby využíván individuální tělesný znak. Mezi tyto znaky řadíme například otisk prstu, sítnice oka, duhovku oka či lidský hlas. [17,18]

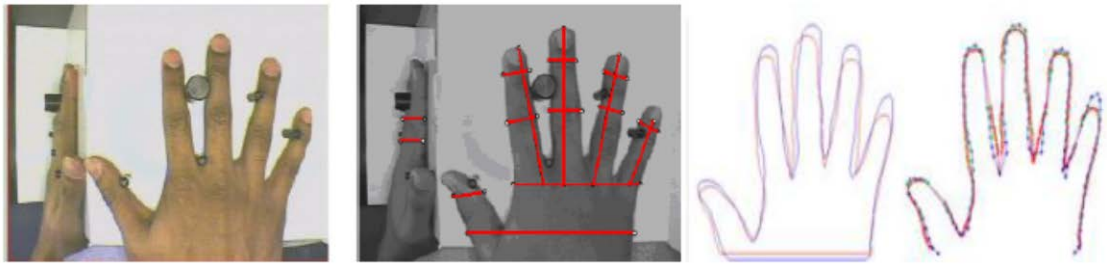
4.5.1 Biometrické identifikační metody

V této podkapitole jsou vysvětleny některé vybrané biometrické identifikační metody, které jsou v bezpečnostní praxi nejvyužívanější a nejznámější. Tyto identifikační metody vycházejí z hypotézy, že mnoho vlastností a charakteristik jsou pro každého jedince specifické a v průběhu času také minimálně proměnné. Při volbě vhodné vlastnosti sloužící k identifikaci osoby, je důležité brát ohled i na hlediska jako je ochota jedince pro snímání určité vlastnosti, nenáročná získatelnost dané vlastnosti a v neposlední řadě i cena snímání. Biometrické identifikační metody využívají dvou různých vlastností a to anatomických a behaviorálních. Výhody anatomických vlastností při identifikaci je jejich neměnnost, nezávislost na aktivitě prováděné subjektem a také jejich neustálá přítomnost. Behaviorální metody identifikace se projevují až při konkrétní činnosti a díky tomu se může projevit jejich nestálost při nejrůznějších procesech autorizace, což je jejich nevýhoda. [20,34,36]

4.5.2 Geometrie ruky

Tato biometrická identifikační metoda je považována za nejstarší automatizovaný bezpečnostně-komerční proces identifikace osoby. Tuto identifikační metodu vyvinul a následně si jí nechal i patentovat David Sidlauskas v roce 1985. Podstatou pro metodu identifikaci osoby podle geometrie ruky je jednoduchý princip měření ruky, sestávají se z dvou či třírozměrného snímání délky, tloušťky, šířky a povrchu ruky. K tomuto snímání je používána speciální podložka s 5 polohovými kolíky a CCD kamerou, jež je znázorněno na obr. 5. [17,29,35]

Obrázek 5 - *Ruka se zrcadly, jež je snímána CCD kamerou a příklad měření vzdálenosti*



[17]

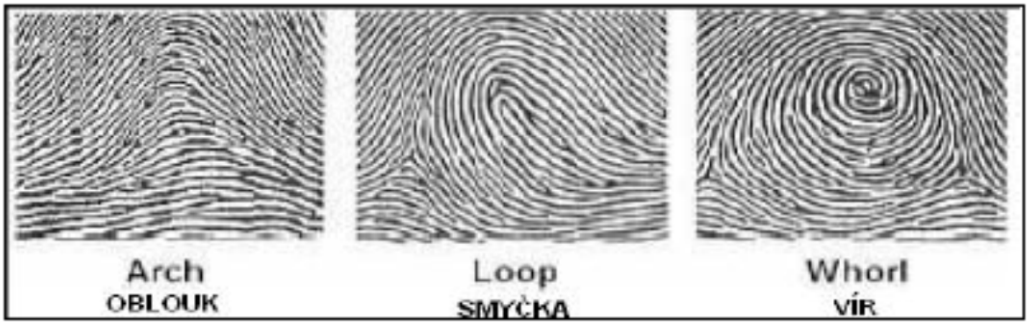
Na snímku ruky je možné dohledat až 31 000 polohových bodů a realizovat až 90 nejrůznějších měření vzdálenosti. Vybraná měření se následně ukládají do 9ti bitového

souborů, díky čemuž jsou tyto systémy výhodné z hlediska nízkého využití systémové paměti. Nejčastěji se tato metoda verifikace používá jako docházkový či přistupový systém. [17]

4.5.3 Otisk prstu

Tato metoda identifikace osoby je jednou z nejznámějších biometrických metod. Je uznávána jako celosvětový standard identifikace v bezpečnostně-komerční a policejně-soudní sféře a to hlavně pro svou jedinečnost a stálost v čase. Tato metoda se stala velmi využívanou především pro svou poměrnou jednoduchost v získávání vzorků, pro použitelnost na velké části lidské populace, četnost vzorků (člověk má standardně 10 prstů) a v neposlední řadě má tato metoda již velkou policejní databázi. Otisk prstu se skládá z drobných rýh vytvářející různé a vzory (oblouk, smyčka a vír), které jsou pro každého člověka jedinečné, jež je zobrazeno na obr. 6. Tato metoda se začala k identifikaci osoby používat již na konci 19. století, kdy byly nalezeny a definovány některé charakteristické body prstu sloužící k identifikaci osoby, panem Franciscem Galtonem. [17,31,39]

Obrázek 6 - ***vzory otisků prstu***



[17]

Existuje několik metod snímání otisků prstů. Otisky prstů se mohou snímat například klasickou metodou za pomocí inkoustu a papíru, jež se používá výhradně ve forenzní sféře a při policejních vyšetřováních. Principem této metody je rolování celého prstu na papíře tak, aby byl získán celý otisk prstu, prakticky se dá říci od nehtu k nehtu. Důležité je získat co nejvíce použitelné markanty, který následně pomohou zvýšit rychlost a přesnost identifikace. Další metodou snímání otisků prstů je snímání statické. Tato metoda je jednou z nejběžnějších a nejpoužívanějších metod, kdy osoba bez jakéhokoliv jiného pohybu přitiskne svůj prst na senzor. Velkou výhodou této metody je její rychlost a jednoduchost. Nevýhodou však může být přílišný tlak prstu, při kterém může dojít k poškození či dokonce přelomení snímací

čočky. Dalšími nevýhodami je pak pootočení prstu a následná deformace pokožky při pokládání prstu, či zašpinění senzoru nebo zanechání latentního otisku. [17,36]

Jakmile jsou otisky prstů sejmuty jakoukoliv z výše zmiňovaných metod, přichází na řad zpracování sejmutých otisků (obrazů). Zpracování sejmutých obrazů má několik kroků. Jako první krok je nutné zvýšit kvalitu sejmutého otisku, tak aby odpovídal požadované úrovni v bloku předzpracování obrazu, což v praxi znamená úpravu jasu, morfologické operace. Poté následují detekce markantů a papilárních linií (neboli rysů otisku). Celý proces je zakončen tzv. klasifikací rysů, na jejímž základě je určen výsledek autorizace. [17,18,20]

4.5.4 Geometrie tváře

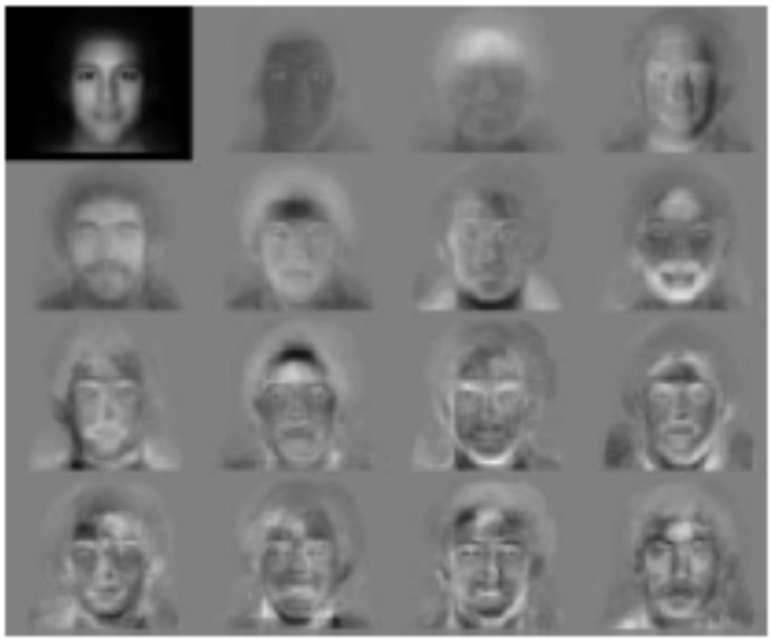
Identifikace osoby na základě biometrie tváře je nejpřirozenější a zároveň nejobtížnější a nejvíce zkoumanou metodou identifikace. Tato metoda identifikace má svůj počátek v 60. letech 20. století. Velkou výhodou identifikace na základě biometrie tváře je fakt, že kontrolovaná osoba častokrát ani netuší, že je prověřována. Tuto metodu identifikace využívají ve velké míře především bezpečnostní složky zejména z důvodů preventivních například na letištích, kdy pomocí ní mohou být odhaleny potenciálně nebezpečné nebo hledané osoby. [18,37,38]

V principu je identifikace osoby na základě jeho tváře založena na srovnání obrazu sejmutého kamerou s obrazem uloženým v některé databázi. K přesné identifikaci osoby jsou použity následující parametry – tvar obličeje a umístění výrazných tvarů na tváři jako je nos, pusa, obočí či oči. Vzhledem k tomu, že obraz může bát v mnoha případech diskriminován nějakou určitou funkcí, nebývá uschována přesná poloha rtů, nosu či očí, ale spíše jejich vzdálenost od sebe jako je vzdálenost mezi nosem a rty nebo mezi obočími, či například velikost úhlu mezi okem a špičkou nosu. [17,18,31]

Existuje několik metod identifikace člověka. Mezi nejznámější z nich patří identifikace na základě měření geometrických vlastností a identifikace na základě porovnávání šablon. Identifikaci na základě geometrických vlastností můžeme rozdělit na dva hlavní přístupy. Jedná se přístupy geometrický, jež je založen na rysech obličeje a fotometrický, které se zakládá na vzhledu obličeje. Existuje mnoho algoritmů, podle kterých je možné obličej identifikovat z nich jsou nejlépe probádané a prostudované tři. Jedná se o PCA neboli analýzu hlavní části, LDA což je zkratka pro lineární diskriminační analýzu a EBGM neboli elastický srovnávací diagram. [17,32]

PCA neboli analýza hlavní části je jaká si matematická operace na základě které jsou vytvořeny alba tzv. eigenfaces neboli normalizovaných vzorů tváří. Prostřednictvím této metody je možné každou tvář rozdělit a následně jí opětovně složit, jak je ukázáno na obr. 7. Každému z těch eigenfacesů je přiděleno číslo, které je pak ukládáno namísto obrázku. [17,29,33]

Obrázek 7 - *Standardní vzory tváří využívané k rozložení obrazu*



[17]

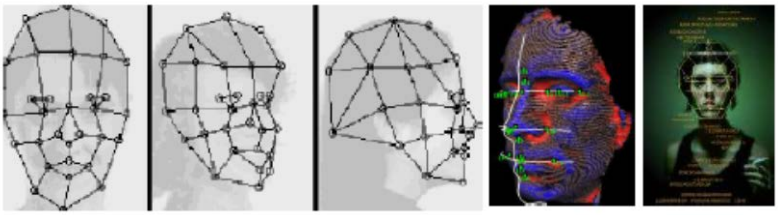
LDA neboli lineární diskriminační analýza je analýza, kdy jsou pořízené snímky selektovány do určitých skupin tváří. Hlavním cílem této analýzy je minimalizace rozdílů v jednotlivých skupinách a maximalizace rozdílů mezi těmito skupinami, kdy je v každé skupině snímků reprezentována jedna třída, jak ukazuje obr. 8. [17,34]

Obrázek 8 - *Příklad šesti skupin vytvořených na základě LDA analýzy*

[17]

A posledním algoritmem je EBGM neboli elastický srovnávací diagram. Tento diagram byl vyvinut na základě toho, že jak analýza PCA tak LDA nejsou schopny analyzovat nelineární charakteristiky, mezi které se řadí například výraz tváře, pozice hlavy či osvětlení místnosti či prostoru. EBGM využívá vydefinovaných uzlových bodů na obličeje, kterou jsou následně spojeny a díky tomu je možné tvář identifikovat v prostoru. Tímto propojením uzlových bodů vzniklá jakási souřadnicová síť, viz obr. 9. Celý proces snímání je nastaven tak, že na systém na základě filtrů uzlových bodů na obličeji reaguje na zachycené obličeje a porovnává je s databází a následně shody či neshody vyhodnocuje. Tento diagram se doporučuje vzhledem k problematice lokalizace orientačních bodů umístěných na obličeji kombinovat s předchozími analýzami. [17,33,38]

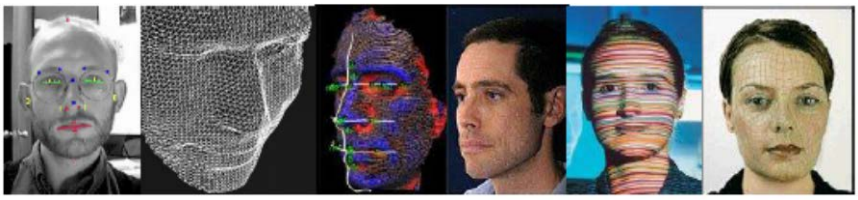
Obrázek 9 - *Síť vytvořena pomocí elastického mapování a vs. obraz, jež zpracoval počítač*



[17]

Využití geometrické metody k identifikaci osob je v současné době neustále se rozšiřující a moderní princip identifikace. V současné době je velmi hojně využívána na místech, kde by se mohli nacházet hledané či pohřešované osoby, viz obr. 10. Mezi tyto místa patří již několikrát zmiňované letiště, nádraží, náměstí či rušné ulice. [17,33]

Obrázek 10 - *Ukázky zpracování biometrických dat pomocí počítače*



[17]

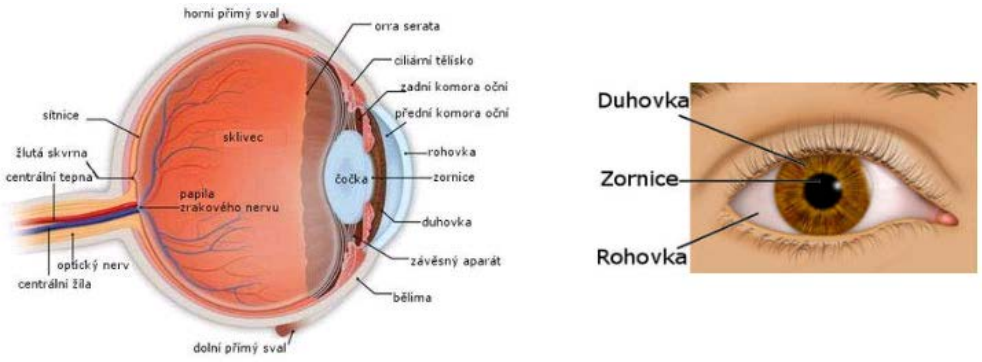
Ač je metoda identifikace na základě geometrie obličeje velmi oblíbená na místech s větší koncentrací lidí, není vždy 100% spolehlivá. Například při použití této metody ve venkovních podmínkách, může dojít k chybné či negativní identifikace až v 80 % případů. Na

vině je hned několik faktorů. Patří mezi ně už samotné prostředí nebo dále pak úhel 45 stupňů, ze kterého jsou fotografie pořizovány. Mezi další vlivy ovlivňující pozitivní identifikaci patří proměnlivost osvětlení, která je způsobena různorodostí a odlišností oblečení. V těchto případech se nemusí podařit najít shodu fotografie s obrázkem v databázi až ve 40 % případů. Technologie identifikace osoby podle geometrie obličeje může v mnoha případech velmi pomoci, ale fotografie musí být foceny dle určitých specifik, jako je třeba zachycení celého obličeje. Je třeba také zajistit dostatečné množství pracovníků, kteří budou schopni zpracovat a přiřadit snímek hledané osoby s fotografií uloženou v databázi. [17,33]

4.5.5 Duhovka oka

Identifikace osoby pomocí duhovky oka je relativně mladá metoda identifikace. Jako první si nechal automatický systém pro identifikaci pomocí duhovky patentovat v roce 1994 Úřad pro jadernou bezpečnost, který tehdy vedl Dr. John Daugman. Duhovka, jež se nachází mezi rohovkou a čočkou, viz obr. 11, je sval regulující zaostřování oka neboli velikost čočky na základě toho, jak intenzivní světlo na oko dopadá. Za zabarvení duhovky je zodpovědný meletoninův pigment a jeho množství ve svalovině. I když zabarvení duhovky může být dědičné, tak její vzorkování nikoliv, to je zcela náhodné a vyvíjí se v průběhu prenatálního růstu plodu. Tímto je zaručena její jedinečnost (dokonce i u dvojčat) na rozdíl od metody rozpoznávání tváře. Tato velmi unikátní vlastnost je tato metoda jedna z nepřesnějších metod identifikace člověka na světě. [17,32,35]

Obrázek 11 - *Průřez oka*

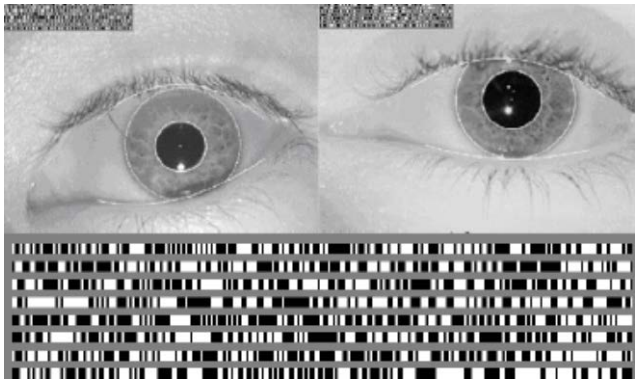


[20]

Aby mohlo být snímání duhovky kvalitní a identifikace mohla být uskutečněna, je zapotřebí velice kvalitní digitální kamery a infračerveného osvětlení oka. Duhovka je během

snímání mapována do fázorových diagramů, jež v sobě ukrývají informace týkající se četnosti, orientace a pozic specifických plošek. Na základě zpracování těchto informací vzniká mapa a šablona sloužící k identifikaci osoby, viz obr. 12. [17,37]

Obrázek 12 - *Lokalizace duhovky a její piktografické znázornění*



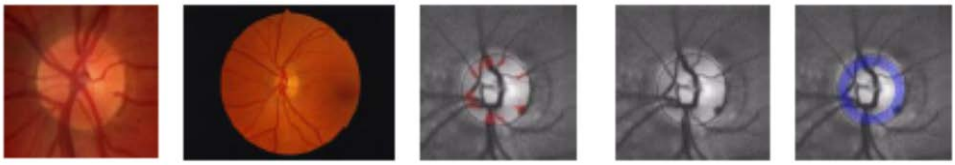
[17]

I při této metodě, stejně jako u jiných metod dochází k ověřování informace, zdali skenovaná oblast vykazuje známky živého organismu. Pro tyto účely bývá použito několik testů. Mezi něž testy patří změna osvětlení v průběhu skenování, sledování dalších jiných pohybů v oku, test odrazivosti sítnice či bývají použity dvě kamery, pomocí kterých je vytvořen 3D obraz, který je následně ověřován, zdali je pravý či nikoliv. [20,29]

4.5.6 Sítnice oka

Tento druh identifikace využívá strukturu krevních žilek a cév nacházející se na pozadí lidského oka. Kdy každá z žilek, které jsou v oku, má při správném osvětlení oproti sítnici samotné jinou odrazivou vlastnost, díky které může docházet k identifikaci, viz obr. 13. K získání obrazu struktury žil a cév v sítnici je využíván infračervené světlo (světelný zdroj s nízkou zářivou intenzitou) a opto-elektrickým systémem. Při použití světla s touto vlnovou délkou se stane sítnice takřka průhlednou a obraz utváří až odraz žilní a cévní sítě v choroidu, který lze naleznout za sítnicí, a který vytváří následný snímek, jež je možné použít při identifikaci. Ten je následně porovnáváno s obrazem v databázi. Struktura obrazu krevních žil a cév je získávána pomoci speciální optické kamery. Aby mohlo k identifikaci dojít, je třeba, aby se uživatel díval do určitého prostoru (někdy až 10 – 15 sekund), což pro něj může být často velmi nekomfortní a nepříjemné a v případě, že uživatel nosí brýle, tak i nemožné. Vzhledem k těmto důvodům není tato metoda identifikace příliš rozšířená a je využívána především v institucích s nejvyšším stupněm zabezpečení. [17,18,20,33]

Obrázek 13 - *Sítnice s charakteristickými parametry*



[17]

4.5.7 Identifikace na základě chůze

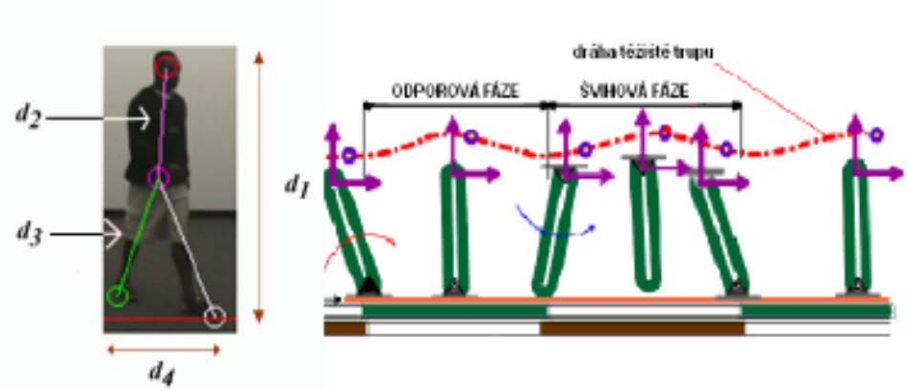
Jedná se o jeden z nově vznikajících okruhů identifikace či verifikace člověka. Podobně jako je tomu u otisku prstů či duhovky oka, i tato vlastnost je pro každého člověka jedinečná, stálá a v průběhu času relativně neměnná. Mezi hlavní výhodou tohoto druhu identifikace oproti jiným metodám, je její bezkontaktnost a fakt, že není nijak intrusivní, tudíž není pro člověka tolik nepříjemná. [17,20]

Hlavním rozlišovacím znakem u této metody identifikace je dynamický stereotyp celého těla (stejný způsob identifikace využívá například identifikace na základě písma, pouze s tím rozdílem, že zkoumá dynamický stereotyp ruky). [20]

Tato metoda identifikace má velký význam například při pokusech o identifikaci trestních činů, během kterých jsou pachatele zcela maskováni a není tak možné využit jiné metody, jako ideální případ může posloužit přepadení banky či klenotnictví. Vzhledem ke stále častějšímu nasazování průmyslových kamer na rušná a frekventovaná místa (letiště, náměstí, nádraží), nachází i zde tato metoda identifikace svůj význam a uplatnění. Jelikož v současné době prozatím neexistuje databáze, na základě které by mohly být nálezy srovnávány se snímky získanými z kamerových systémů, je uplatněné této metody zatím pouze čistě forenzního charakteru. [17]

Tato metoda identifikace je postavena na porovnávání křivek drah opisující určité body nacházející se na lidském těle, neboli těžiště. Identifikace osoby na základě chůze vyhodnocuje, buď trajektorii pohybu daných bodů jakou jsou například klouby dolních končetin, či další těžiště nebo na základě úhlových změn, ke kterým dochází ve velkých kloubech dolních končetin. Vlastnosti jsou vybírány vždy tak, aby byly v čase co nejvíce neměnné. Vzhledem k jedinečnosti pohybových svalových kosterních systému a dynamického stereotypu tato metoda vhodná pro porovnání 1 : 1 k identifikaci, viz obr. 14. [17]

Obrázek 14 - *Vytváření drah těžiště trupu*



[17]

České kriminalistka a její výzkum v této oblasti se může pyšnit umístěním na předních místech ve vývoji této metody identifikace. [17]

4.5.8 Behaveometrika

Behaveometrika je speciální druh identifikace, při které jsou sledování a analizovány vlastnosti člověka. Nejedná se však o fyzické vlastnosti člověka, nýbrž například styl psaní na klávesnici, kdy bývá zkoumána rytmika a četnost úderů, dále pak zkoumání pohybu myší či hlasové ověřování. Systémy určené k identifikaci osob na základě stylu písma či monitoringu na základě pohybu myší jsou velmi zajimavé v tom, že uživateli nestačí pouze autorizace, ale systém sleduje a zkoumá i průběh práce a tím umožňuje průběžnou kontrolu. Tento systém pozná, zdali v průběhu práce k počítači neusedla jiná než oprávnění osoba. [17,29]

Dalšími odvětvími, kterými se tato metoda identifikace zabývá je zkoumání již zmiňovaných stylů chůze, či stylů gest či jiných znaků. Velkou výhodou této metody je nekontaktnost a také možnost jejího využití na velkou vzdálenost. U některých odvětví této metody existuje riziko chybné identifikace, jelikož jsou vlastnosti, které se v průběhu času mohou změnit. [17,34]

4.6 Autorizace obličejové biometrie

Rozpoznávání osob na základě obličejové biometrie je metoda stará a známá, co existuje lidstvo. Již tísíciletí je tato metoda identifikace založena na intuici. Lidé jsou schopni na základě tváře rozpoznat osoby sobě blízké, kolegy v práci, či své kamarády. Proces

identifikace osob na základě obličeje provádí náš mozek automaticky a během zlomku vteřiny, kdy je schopen porovnat tvář, kterou osoba vidí s předlohou uloženou v něm. Idenfikace osoby na základě obličejové biometrie se začala vědecky zkoumat až ve 20. a 21. století. [18,36]

Metodu identifikace na základě obličejové metody již více jak jedno století velmi často využívají při své práci nejrůznější policejní složky. Vzhledem k tomu, že je portét obličeje osoby jednou z nejdůležitějších částí popisu osoby, bylo proto bezpečnostními složkami vyvinuto několik metod rozeznávání lidského obličeje. [18,37]

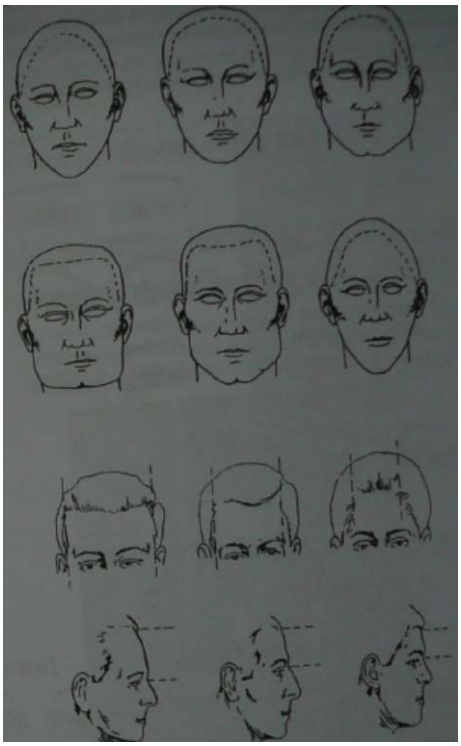
4.6.1 Identifikace osoby dle vnějších znaků

Práce bezpečnostních složek nebo kriminální policie klade velký důraz na co nejvýstižnější správný popis osoby. Tento popis bezpečnostním složkách nebo kriminální policii pomáhá nejen při úkonech při vyřešetřování tresné činnosti, ale například i při hledání pohřešované osoby, osoby v pátrání či při idetifikaci pachalete nebo nalezené mrtvoly. [18]

Věda, jež se zabývá popisem lidského těla a hodnocením jeho znaků, je nazývána antropoligie. Z antropologického hlediska můžeme hodnotit stav lidského těla z pohledu somatometrického (antropometrického) či somatoskopického. Pohled somatometrický využívá k ohodnocení stavu lidského těla nejrůznější objektivní pomůcky, jež jsou vyjádřeny mírami (míry délky, hmotnost, úhly a jiné). Kdežto pohled somatoskopický hodnotí stav lidského těla dle vývoje člověka, velikosti částí těla či dle chybějícího některého ze základních znaků. V běžné praxi se tyto dvě metody popisu osoby často doplňují. Na obr. 15 se nacházejí ukázky různých tvarů a znaků obličeje. [18]

V 80tých letech 19. století se o rozvoj kriminalistické somatometrie zasloužil pařížský kriminalista Alphonse Bertillon, jež zavedl v registru zločinců pořádek, tak že vypracoval systém rozdělení registrace osob dle 11 tělesných měr, jež byly zaznamenány na jedné kartě, kterou bylo v kartotéce díky zavedenému jednoduchému systému v kartotéce zločinců velmi snadno dohledat. Tyto údaje byly následně doplněny popisem, jež často obsahovaly zvláštní charakteristku dané osoby. [18]

Obrázek 15 - *Ukázka různých znaků obličeje*



[18]

Úřední popis osoby je, na rozdíl od toho laického, prováděn proškolenou osobou dle jednotného systému. Touto proškolenou osobou bývá často kriminální technik, který při sestavování portrétu osoby využívá i technických pomůcek, jako jsou různá měřidla, vzorníky barev, tvarů očí či vzorník vlasový. Tento popis je zaznamenáván do úředného záznamu, kde jsou jednotlivé popisované prvky uváděny v logickém sledu za sebou (například obočí – hustota a tvar, oči – tvar, vzdálenost, horní víčko, dále pak výška, váha či přibližný věk). [18]

4.6.2 Klasická identifikace pomocí portrétu využívaná bezpečnostními složkami

Při sestavování portrétu se zaměřuje na dvě takové hlavní věci, a to konkrétně na všeobecný popis, jako je tvar obličeje, plnost obličeje nebo barva, ať už se bavíme o barvě plati, očí či vlasů. A druhou věcí jsou vlastnosti doplňkové, mezi které mohou patřit různá neobvyklá znaménka, jizvy, pihy, kosmetické vady a další. [18]

Při popisu jednotlivých částí je důležité uvádět jejich detaily. Při popisu vlasů je třeba uvést jejich barvu, ta je určena buď subjektivním posouzením osoba, která popis udává, či pomocí porovnání se vzorníkem barevnosti vlasů, kde se nachazejí barvy od světlé plavé, přes

hnědou až po černou. U zrzavých či prošedivělých až bílých vlasů je třeba být, vzhledem k nejasnosti původní barvy, při popisu obezřetný. Konkrétně u šedých vlasů je do popisu uváděn stupeň prošedivnění. Dále je při popisu vlasů dobré uvést jejich tvar, délku, střih (vlasy sčesané dozadu, dopředu, kde se nacházela pěšinka, účes) či charakteristiku (krátké, dlouhé, vlnité, kudrnaté, rovné), hojnost (plešatost a její stupně, řídké vlasy, husté vlasy). Pozor je třeba si dávat při popisu vousů. Zde jsou popisovány stejné charakteristické znaky jako u vlasů, tzn. délka, barva, hustota či například tvar. [18]

U dalších částí obličeje jako jsou rty, oči, nos, zuby jsou nejčastějšími popisovanými charakteristikami jejich barva, tvar, vzdálenost od sebe či jiného bodu na obličeji, proporcionalita ke zbytku tváře. [18]

Další části těla a jejich vlastnosti se popisují většinou v případě, kdy jsou něčím nápadné či nezvyklé. U rukou a paží to může být jejich délka, zdali byly svalnaté či naopak slabé, podoba či deformace nehtů, či chybějí prst nebo jeho deformaci či nepravidelnost. Stejně jako ruce jsou popisovány i nohy, kdy bývá odhadována jejich velikost či jakákoliv deformace či nezvyklé znamená, jako třeba tetování. Pokud hovoříme o nohou, tak nesmíme opomenout i chůzi a její styl, pokud byl něčím výjimečný. [18]

Dále může být brát zřetel i na způsob řeči, pokud byl něčím zvlášním, například zde můžeme hovořit o šišlání, ráčkování a dalších vadách řeči. Také v tomto případě může být uvedeno, jakým jazykem popisovaná osoba hovořila. Při popisu je třeba uvádět jakákoliv jiná další zvláštní znamení, kterých si člověk všimne. Všechny tyto věci následně pak pomohou při pátrání po popisované osobě a mohou vést je jejímu dřívějšímu nalezení. [18]

4.6.3 Bezpečností a policejně-forenzní aplikace

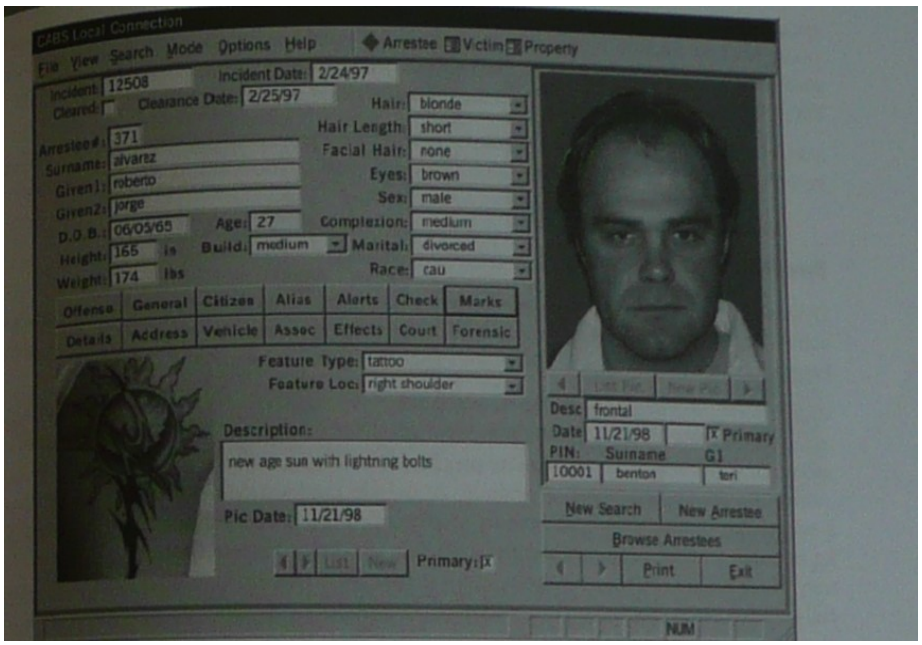
Spojení vidění pomocí počítačů a rozpoznávání obličejů osob markantně změnilo a přineslo zcela nový způsob práce bezpečnostních složek a to zejména v oblasti zpracování snímků osob (statických tváří osob) a monitorování zájmové scény (je již dynamické). [18]

V minulosti probíhala idenfikace osob na základě statického snímku (fotografie, portrét, skica a další) pouze manuálně, kdy porovnávání s kartotékou probíhalo lidským činitelem, který prohlédl a porovnával snímek se snímky v kartotéce jeden po druhém. V současné identifikačně-forenzní praxi je vše již automatizováno. U hodnocení tváře jsou zpracovány pouze dílčí klasifikace markantů v obličeji, mezi které řadíme oči, uši, nos, bradu,

obočí, či ušní boldce a další části obličeje. Dalé jsou těmto částem přírazeny určité popisy, číselné markanty a jsou charakterizovány kontrury tváře (oválná, kulatá, hranatá). Avšak nejsou vytvořeny klasifakční vzorce obličeje jako celku, který by se stával z jednotlivých markatnů, jejich geometického tvaru či jejich vzdálenosti, stejně tak jako je tomu například u dalktyloskopie. [18]

Softwary, které vyvíjejí společnost pro zpracování identifikace statických tváří, jsou schopné vyhodnotit až 15 milionů tváří za jednu minutu, kdežto liský mozek na vyhodnocení jedné tváře potřebuje až 20 milisekund. Softwary v roce 2002 byly tak 5000x rychlejší ve zpracování tváře nežli lidský mozek. Navíc další věcí je fakt, že neextistuje žádný mozek na světě, který by dokázal zpracovat takové množství tváří a zároveň si k nim přiřadit další údaje jako je jméno, příjmení či bydliště nebo datum narození, viz obr. 16. [18]

Obrázek 16 - *Příklad softwaru pro identifikaci osob*



[18]

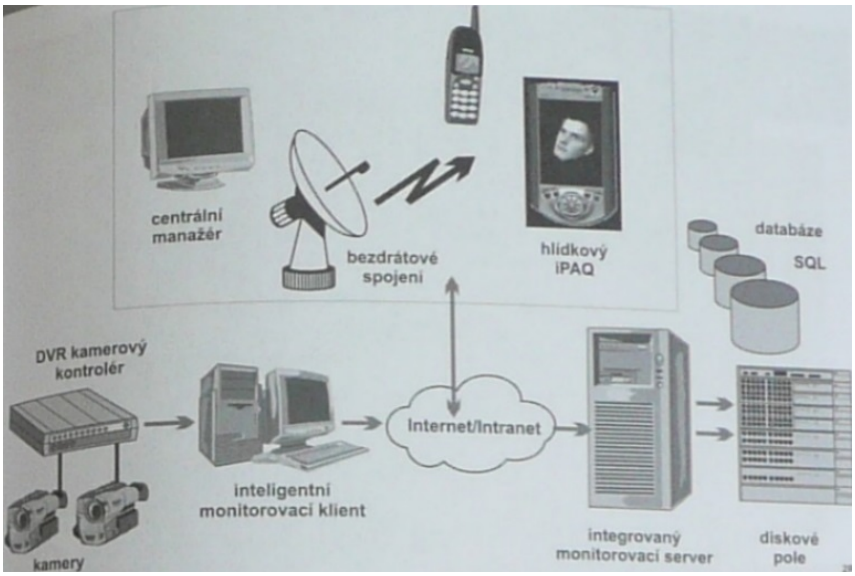
Rozpoznávání osob na základě snímku a jeho následné konfontace dalších osob, mezi kterými se nachází pachatel je v současné době běžnou forenzní praxí. [18]

Dynamický způsob monitorování neoboli monitorování zájmové scény v kombinaci se softwarem na rozpoznávání obličejů se v policejně-bezpečností praxi stal novým operativním nástrojem při jejich práci. Kamery, které monitovorání zajišťují přenáší záznam v reálném čase. V 80. letech 20. století začaly být místa a prostory s vysokým počtem trestních činů

nebo s vysokou hrozbou tresné činnosti preneventivně monitorovány pomocí CCTV (uzavřených televizních okruhů). Záznamy z těcho uzavřených televizních okruhů jsou shomažďovány v monitorovacích či operačních centrálách. [18]

Tyto autonomní systémy jsou nejčastěji využívané na veřejných místech, v dopravě, na místech s vyšším výskytem prostitutek či kapesních zlodějů, v obchodních domech či k hledání hledaných osob či terotisků nebo pachatelů trestné činnosti. Získané obrazové záznamy jsou pak vyhodnocovány operačními důstojníky. Napojení monotorivacích systémů na softwary pro rozpoznávání obličejů dávají operačním důstojníků nástroj pro rychlou reakci v případě, že se na záznamu nachází zájmová osoba nacházející se v databázi. [18]

Obrázek 17 - *Dynamický monitorovací systém a jeho infrastruktura*



[18]

4.7 Kriminalistická identifikace osob u Policie České republiky

Kriminalistická identifikace je proces, jež si klade za cíl určit vztah a souvislost mezi kriminalisticky relevatní událostí, kriminalistickými stopami a objekty, které stopy zanechaly. Tento druh identifikace se snaží vztah a souvislosti mezi těmito 3 věcmi indiviualizovat. Kriminalistická identifikace se opírá o fakt, že není možné, aby existovaly dva objekty, které by byly naprosto totožné a mohly tak zanechávat naprosto stejné stopy. Všechny objekty se mezi sebou liší svými vlastnosti, jako je například váha, výška či barva očí nebo vlasů. [18]

Kriminalistická identifikace je možná pouze v tom případě, zanechal-li po sobě objekt jakoukoliv po určitý čas relevantně neměnnou kriminalistickou stopu. [18]

4.8 Příklady kamerových systémů využívaných Policií České republiky

Policie České republiky využívá při výkonu své práce nejrůznější kamerové systémy. Tyto systémy jí pomáhají nejen pří řešení nejrůznějších přestupků či trestních činů, ale také při dokumentaci jejich práce a zároveň i jakýsi záznam jejich práce a zásahů pro případ, že by se je někdo pokusil uplatit či obvinit z jiného činu. [22]

4.8.1 Městský kamerový dohlížecí systém

Jednou z hlavních funkcí městskch kamerových dohlížecích systémů je prevence, tzn. tvorba bezpečných zón ve městech. Tyto systémy jsou nejčastěji instalovány na místech s velkou koncentrací osob. Mezi taková místa řadíme nejrůznější společenské, kulturní či komerční instituce, náměstí, centra měst, parkoviště, nádraží, ale také například sídliště. Tento dohlížecí systém je velmi přínosný v případech ochrany bezpečnosti osob nebo majetku, odhalování přestupků či trestních činů a taky dohlíží na dodržování závazných právních předpisů týkajících se ochrany veřejného majetku. [21]

Aby mohl být městský kamerový dohlížení systém provozován, je nutné aby se řídil zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů a byl také v souladu se zákonem č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů a zákonem č. 101/2000 Sb., o ochraně osobních dat, ve znění pozdějších předpisů. Tento kamerový dohlížecí systém musí sledovat pouze prostranství veřejného charakteru. Definice a charakteristka veřejných prostranství je specifikována v § 34 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů. Těmito prostory se rozumí veškeré ulice, náměstí, tržnice, chodníky, parky a ostatní veřejná zeleň, dále pak prostory, určené k obecnému užívání, což znamená, že jsou přístupná všem občanům bez jakýchkoliv omezení a ohledu na vlastnictví. [21]

Městský dohlížecí kamerový systém sloužit jako pomoc při koordinaci všech složek Integrovaného záchranného systému v situacích, kdy je závažněji ohrožena občanská bezpečnost. Obrazové záznamy z těchto systémů nejsou určené pro širokou veřejnost, nýbrž slouží výhradně po přesně vymezené potřeby Policie České republiky a Městské případně Obecní policie. Pro manipulaci se zařízením městského kamerového dohlížecího je vždy určena pověřená, řádně proškolená a kompetentní obsluha, která zabrání případnému vstupu

neoprávněné osoby. O monitorování veřejného prostranství musí být všichni občané a návštěvníci daného místa řádně informovani. [21]

Policie České republiky má v nezbytných případech pro plnění svých úkolů, nazákladě§ 79 zákona o Policii České republiky, opravnění zpracovat citlivé i osobní údaje osob bez jejich souhlasu. Těmito úkoly je myšlena především zajištění veřejného pořádku a ochrana osob a majetku. Dle § 62 má v nezbytných případěch Policie České republiky také pravomoc pořizovat obrazové, zvukové či jiné záznamy osob či věcí, které se pohybují nebo jsou umístěny na veřejných prostranství. V případě, že jsou k získávání těchto záznamů naistalovaný stálé kamerové systémy, je povinností Policie České republiky o této skutečenosti dostatečně informovat veřejnost. Způsob, jak bude Policie České republiky o této skutečnosti veřejnost informovat je vzhledem k tomu, že není zákonem upravena, na jejím uvážení. [21]

4.8.2 Kamerové systémy v policejních vozech

Mezi standardní vybavení policejních vozů by měly patřit i tzv. lokalizační a záznamová zařízení, který by měly policistům pomáhat při výkonu jejich služby v oblasti bezpečnosti, prevence či řešení nejrůznějších rizik. Vozidla jež jsou vybavena lokalizačními a záznamovými zařízeními jsou pro policisty velmi prospěsný systému. Tyto systémy zefektivňují a usnadňují policistům jejich práci. [22]

Lokalizační a záznamové zařízení zahrnují radiostanici s GPS, dále pak navigaci a datalogy. Pod pojem datalog patř záznamníky dat, dále pak kamery spolu s videoservery, kde jsou ukládana pořízená data z kamer a neposlední řadě PC s monitorem a dalšími potřebnými komponenty. Pořízením těchto zařízení byla sjednocena komunikační platforma Policie České republiky s ostatními složkami Integrovaného záchranného systému a tím zvýšena kvalita koordinace při závažných a mimořádných událostech. [22]

Pomocí GPS jsou schopni operační důstojníci, na základě grafického znázornění hlídkových vozů včetně provozních informací o vozidle, rychleji a snadnější poslat na místo nejbližší hlídku a zrychlit tak dojezdové časy. Další velkou výhodou umístění GPS navigace v policejních autech je i lepší orientace na neznámém místě, čímž se opět zrychlí dojezdový čas na místo. Posádky hlídkových vozů díky GPS navigaci mohou dojezdový čas lépe odhadnou a nejsou tak závislý pouze na informaci od operačního důstojníka. V případě širšího

opatření jako je pronáslednování vozidla, či nasazení hlídek z více krajů, může být jejich koordinace jednodušší a tím se zvýší účinnost využití dostupných hlídek. [22]

Kamery umístění za a před policejním vozidelem jsou schopné pořizovat záznamy, jež jsou následně použity při operativním rozhodování policejní hlídky. Tyto záznámy si mohou policisté přehrát přímo ve vozidle. Pořízené záznamy slouží mimo jiné také k zachycení nejrůznějších dopravních přestupků (jízda na červenou, nerespektování dopravního značení, předjíždění v místech, kde to není povoleno, držení a užívání smart telefonů, dokumentace děje nehody a další situace). Dalším využitím kamer umístěních v policejních vozech může být dokumentace ostatních přestupků či trestních činů ať už se jedná o majetek, občanské soužití či veřejný pořádek. V neposlední řadě kamery slouží k zachycení a zadokumentování jednolivých zákroků policejních hlídek, které dávájí jak policistům, tak občanům určitou jistotuv dokazování protiprávního jednání. Tyto záznamy slouží jako nezpochybnitelný důkaz při uplatnění pravomocí policejních hlídek směrem k občanům. [22]

Počítačové termíny s dotykovým displejem slouží policejním hlídkám nejen k využítím map a již zmiňovému zkráceni dojezdového času, ale především budou mít díky těmto terminálům přístup do informačního systému Policie České republiky. Přístup do systémů hlídky umožňuje policejní hlídce v průběhu výkonu služby získat informace osobám či vozidlům, díky kterým budou hlídky schopny určit správnou taktiku dalšího postupu. Dostupnost informačního systému ve vozidlech policejních hlídek, jim pomáhá také při pátrání po osobách, věcech či vozidlech. Ukázka terminálu s dotykovým displejem a kamerou viz obr. 18 a 19. [22]

Obrázek 18 - *Ukázky podoby počítačového terminálu s dotykovým displejem a kamery*

Je třeba podotknout, že ne každý policejní vůz je těmito lokalizačními a záznamovými systémy vybaveno. Auto na jednotlivé kraje a útvary přicházejí od výrobce bez těchto systémů, pouze s připravenou kabeláží. Jaký systém bude do konkrétního policejního vozidla nainstalován, je závislé na finančních prostředcích krajů a útvarů. Každý policejní vůz je však vždy vybaven radiostanicí s GPS.

4.8.3 Ochrana letiště - zajištění zvýšení bezpečnosti na letišti Václava Havla Praha

Vzhledem k členství České republiky v Schengenském prostoru představují naše mezinárodní letiště jediné vnější hranice, na nichž probíhá kontrola osob vstupujících do České republiky, potažmo celého Schengenského prostoru. S ohledem na počet cestujících, kteří prochází Letištěm Václava Havla Praha, se jedná o jednoznačně nejvíce frekventované letiště na území České republiky. Z tohoto vyplývá nezbytnost pečlivého monitoringu osob, které tímto letištěm procházejí. Kromě faktické nezbytnosti provést řádné zabezpečení letiště vychází tato nutnost i z mezinárodních závazků přijatých Českou republikou. S ohledem na mezinárodní závazky i prosté množství cestujících a multietnicitu osob procházejících letištěm Václava Havla Praha může případný bezpečnostní incident, ke kterému nebude v důsledku nedostatečné reakce řádně přistupováno, způsobit mezinárodní incident. Toto se týká jak problematiky řádné kontroly cestujících, tak i nastavení odpovídajících postupů, jak odhalit a reagovat na bezpečnostní hrozby. Popis výchozí situace, resp. navrhované řešení a opatření ke zvýšení bezpečnosti letiště Václava Havla Praha, plně koresponduje s obsahem Usnesení Vlády České republiky ze dne 20. března 2013 č. 200 o Strategii České republiky pro boj proti terorismu od roku 2013. [23]

4.8.4 Čtyři česká letiště dostanou moderní bezpečnostní prvky za půl miliardy

Česká republika investuje 550 milionů korun na zvýšení bezpečnosti čtyř mimopražských mezinárodních letišť. Na řadu se dostala poté, co skončil projekt na zvýšení bezpečnosti Letiště Václava Havla v Praze, což přišlo na 187 milionů korun.

Z podprojektů plánovaných pro pražské letiště fungují všechny kromě systému detekce obličejů - zatím je jen v pilotním provozu. Venkovní prostory pražského letiště například nyní hlídají brány s kamerami, které snímají registrační značky aut. Systém je schopen rozpoznávat vozidla v pátrání. [24]

5 Praktická část práce

Praktická část zahrnuje informace o použitých měřících zařízení, testování spolehlivosti těchto zařízení a jejich následné vyhodnocení. Praktická část také obsahuje multikriteriální analýzu dat, kde jsou jednotlivé zvolené kamery porovnány a z tohoto porovnání jsou udělány závěry a zhodnocení.

5.1 Použitá zařízení

V této kapitole se nachází zařízení, které bylo v průběhu práce a procesu měření využito. Nachází se zde jejich zevrubný popis i případný způsob využití a také pracovní podmínky, které jsou stanovené výrobcem.

- **Kamera Netatmo NSC01-EU**
- **Síťová bezpečnostní kamera - Edimax IC-7113W**
- **Otočná IP kamera - D-Link DCS-5030L**

5.1.1 Kamera Netatmo NSC01-EU

Kamera Netatmo má funkci rozpoznávání obličejů, vše je zaznamenáváno ve Full HD kvalitě. Zvuk i obraz je přenášen pomocí internetu a vše je možné sledovat v mobilní aplikaci a to i v reálném čase. Zaznamenává jak ve dne, tak v noci.

Rozměry:
45 × 45 × 155 mm

Materiál:
Odolný hliníkový kryt
Matný černý plast (infračervené světlo)
Pro vnitřní použití

Kamera:
Video senzor: 4 Mpx
Rozlišení: až 1920 × 1080 px

Připojení:
Ethernet RJ-45 port: 10/100 Mbits
Wireless: Wi-Fi 802.11 b/g/n (2.4G)

Úložiště:
Paměťová karta MicroSD o velikosti maximálně 32 GB
8GB karta MicroSD Class 10 součástí balení

Požadavky:
Připojení k internetu
Mobilní aplikace pro telefon s iOS (verze 8 a vyšší) nebo s Androidem (verze 4.3 a vyšší)
Webová aplikace pro nejnovější verze prohlížečů Firefox, Safari, Chrome a Internet Explorer

Obsah balení:
1× Welcome kamera
1× USB kabel
1× napájecí adaptér
1× 8GB micro SD karta

Cena 5499,- Kč. – zdroj CZC.cz [26]

Obrázek 19 - *Kamera Netatmo s funkcí rozpoznávání obličejů NSC01-EU*

[26]

5.1.2 Síťová bezpečnostní kamera - Edimax IC-7113W

Kamera Edimax se dá použít jak ve dne tak v noci, má schopnost detekce pohybu. Veškerá činnost je monitorována přes aplikaci v mobilním telefonu přes internetové připojení. Disponuje 8 LED diodami a je otočná v osách X a Y.

Rozměry

Výška 11,6 cm
Hloubka 12,8 cm

Parametry a specifikace

Použití - Vnitřní
Maximální rozlišení 1280 × 720 px
Typ snímače CMOS
Komprese videa MJPEG, H.264
Šířka 11,2 cm

Vstupy a výstupy

Rozhraní RJ-45 LAN, MicroSD/SDHC slot, Napájecí jack, Wifi
Slot pro paměťovou kartu SDHC, MicroSD

Funkce

Noční vidění - Ano
Ovládání přes aplikaci - Windows Phone
Funkce - Detekce pohybu
Rotace - Ne

Cena 3290,-Kč – zdroj Alza.cz [27]

Obrázek 20 - *Síťová bezpečnostní kamera Edimax IC-7113W*

[27]

5.1.3 Otočná IP kamera - D-Link DCS-5030L

Kamera D-Link se dá použít jak ve dne, tak v noci. Veškerá činnost je monitorována a oznámena přes aplikaci v mobilním telefonu přes internetové připojení. Disponuje 10 LED diodami a je otočná v osách X a Y. Kamera zaznamenává jak zvuk, tak pohyb.

Rozměry

Šířka - 11,64 cm
Výška - 10,91 cm
Hloubka - 13,36 cm

Parametry a specifikace

Použití - Vnitřní
Napájení - Adaptér
Maximální rozlišení - 1280 × 720 px
Typ snímače - CMOS
Komprese videa - MJPEG, H.264

Vstupy a výstupy

Rozhraní - RJ-45 LAN, MicroSD/SDHC slot, Wifi
Slot pro paměťovou kartu - MicroSD
Maximální velikost paměťové karty - 128 GB

Funkce

Noční vidění - Ano
Maximální dosvit nočního vidění - 5 m
Ovládání přes aplikaci - Google Android, Apple iOS
Funkce - Digitální zoom, Detekce pohybu, Detekce zvuku, Zasílání e-mail notifikací, Vestavěný mikrofon, Cloud platforma
Rotace - Ano

Video: Zorný úhel - 170 °

Cena 2999,- Kč. – zdroj CZC.cz [28]

Obrázek 21 - *Otočná IP kamera - D-Link DCS-5030L*

[28]

5.2 Výsledky měření

Měření bylo provedeno na kameře Netatmo - kamera s funkcí rozpoznávání obličejů, zlato/bílá - NSC01-EU.

Probíhalo ve vestibulu kancelářských prostor firmy, která si nepřeje být jmenována. Každodenně se ve vestibulu pohybuje 12 subjektů (zaměstnanců). Pracovní doba je klouzavá, kdy někteří zaměstnanci přicházejí již od 6:00 hod. a někteří v práci zůstanou až do 22:00 hod. Tato kamera byla nainstalována na docházkový systém firmy. Byla sepnuta a do mobilního telefonu byla nainstalována aplikace pro přístup na cloud dané kamery Netatmo. Kamera se musela první týden nechat volně běžet bez sběru dat, jelikož se musela učit a ukládat jednotlivé obličeje zaměstnanců. Měření probíhalo kontinuálně a to od 24. 8. 2017 až do 30. 11. 2017. Měření bylo zaměřeno na spolehlivost této kamery a to jak za standardního osvětlení vestibulu kanceláří s pomocí umělého osvětlení a tak za šera bez zapnutí umělého osvětlení. Také byla pozorována míra chybné identifikace, kdy kamera vyhodnotila pohyb a učila se nové tváře, ale v místnosti nebyla přítomna žádná osoba. Tato situace nastávala většinou v noci za tmy, kdy zavanul průvan a rozhýbal závěsy a záclony, které byly v zorném úhlu kamery a vytvořily mylnou představu přítomnosti člověka.
identifikace neživého:

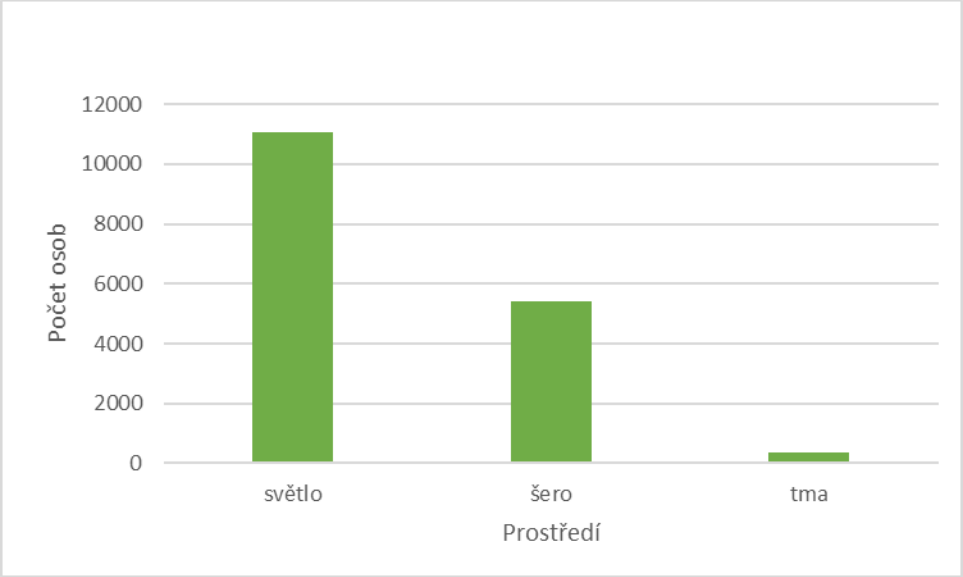
- kytka
- stín
- jiná část těla
- závěsy, aj….

špatně přiřazený obličej:

- záměna obličeje uživatelů, které jsou uloženy v kameře

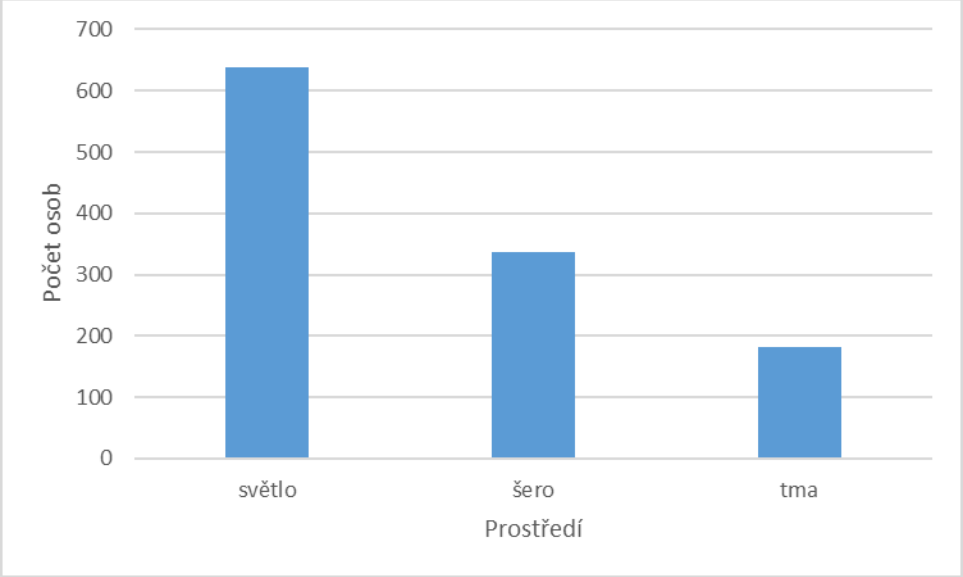
Z grafu č. 1 je patrné, že během světla došlo k nejvyššímu počtu správně přiřazených osob. Za šera byly tyto výsledky nižší a za tmy byl počet správně přiřazených osob nejnižší. Je však důležité vzít potaz, že jsou v tomto grafu uvedeny absolutní hodnoty úspěšných indentifikací. Ze získaných dat bylo zjištěno, že během světla byl pohyb osob nejvyšší - přibližně jedenáct tisíc zaznamenaných průchodů, v případě šera byl pohyb osob oproti pohybu za světla přibližně poloviční – přibližně pět tisíc průchodů. Za tmy docházelo k minimální detekci osob. Zaznamenaný trend odpovídá předpokládané docházce zaměstnanců.

Graf 1 - *Správně přiřazený obličej*



V grafu č. 2 lze vidět pokračování trendu z grafu č. 1. Hlavním rozdílem je podstatné zvýšení množství detekcí v případě tmy. To lze přisuzovat problémům v kvalitě obrazu. Tento problém lze indentifikovat již z toho grafu absolutních hodnot.

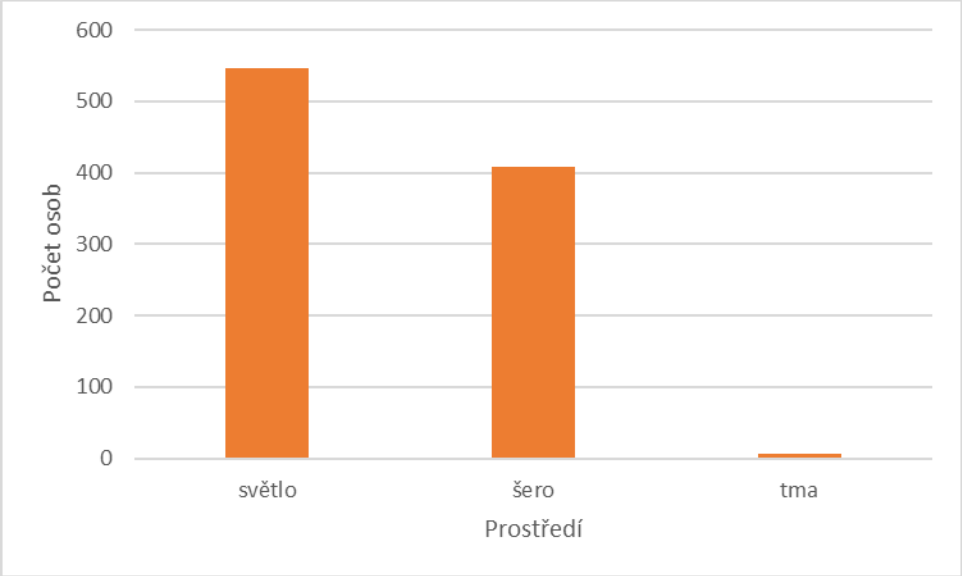
Graf 2 - *Přiřazení neživého objektu*



Na grafu č. 3 je znázorněn počet špatně přiřazených obličejů (záměna osob) k osobám z databáze za různých světelných podmínek. Z grafu výplývá, že za světla došlo k přibližně pětseti padesáti záměnám, za šera k přibližně čtyř stům záměnám a za tmy k nepatrnému

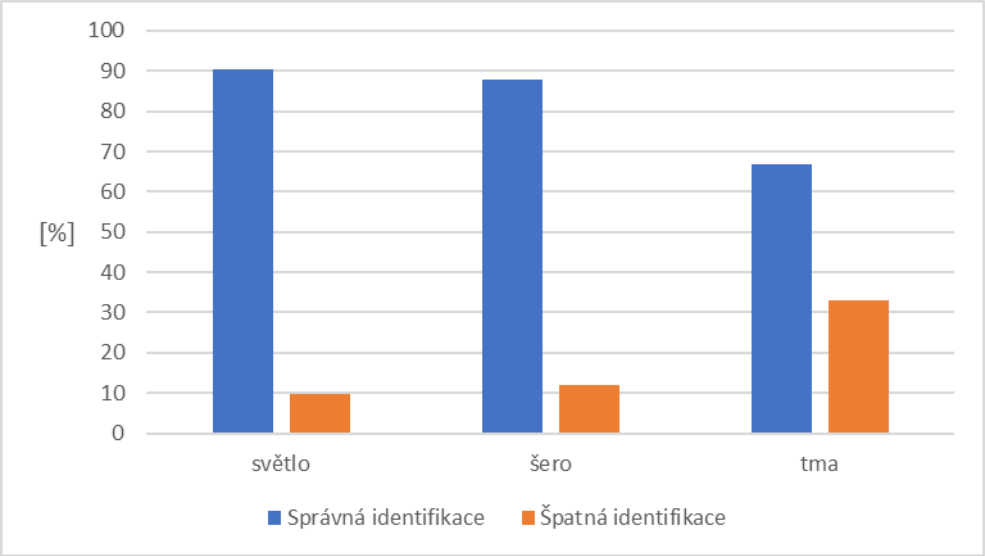
množství záměn. Toto je způsobeno především tím, že za světla a šera byl pohyb osob neúměrně vyšší pohybu za tmy.

Graf 3 - *Záměna osob*



Na grafu č. 4 je v modrých sloupcích znázorněn poměr úspěšných identifikací vzhledem k celkovému počtu identifikací v procentech. Je zde vidět, že za světla byla úspěšnost nejvyšší – dosáhla přibližně 90%, za šera byla dosažena úspěšnost srovnatelná s hodnotou dosaženou za světla – opět přibližně 90% a za tmy došlo ke značnému poklesu úspěšnosti – přibližně 65%. Na oranžových sloupcích je znázorněn inverzní pohled na zkoumanou problematiku. Je zde vidět, že chybovost za světla a šera dosahuje srovnatelných hodnot – přibližně 10% a za tmy dochází k podstatnému zhoršení detekčních schopností – přibližně 35% chybných detekcí z celkového počtu zjištěných detekcí osob. Tento graf má podstatně vyšší vypovídající hodnotu. To je zapříčiněno přepočtem absolutních hodnot detekcí osob do hodnot relativních. Při této úpravě dojde k zohlednění celkového počtu detekcí osob za daných světelných podmínek a je tak možné skutečné porovnání naměřených hodnot.

Graf 4 - *Chybovost identifikace*



5.2.1 Multikriteriální analýza dat

Také nazývána jako vícekriteriální analýza variant či též vícekriteriální hodnocení variant, kdy je množina posuzovaných variant popsána konkrétním výčtem všech prvků. Jedná se o postup podporující komplikovaná rozhodnutí, při kterých je potřeba posoudit varianty více hledisek. Jednotlivá hlediska jsou vyjadřována ve formě kritérií. Obvyklým cílem vícekriteriálního rozhodování je vybrat jednu z množiny posuzovaných variant, případně seřadit varianty podle výhodnosti dle daných preferencí. [25]

5.2.2 Parametry pro konečné hodnocení

V tabulce č. 1 jsou vypsané jednotlivé parametry vybraných kamer. Kamery byly vybrány na základě dat o prodejích, které poskytla firma Alza. Tyto systémy jsou neprodávanějšími za poslední 4 roky.

Tabulka 1 - *Parametry pro konečné hodnocení*

	D-Link DCS-5030L	Edimax IC-7113W	Netatmo NSC01-EU
Rozlišení	1280x720	1280x720	1920x1080
Úhel záběru	94,36°	78°	130°
Provedení kamer	otočná	otočná	neotočná
Kapacita Micro SD	128 GB	32 GB	32 GB
Cena	2 999 Kč	3 290 Kč	5 499 Kč

Z níže uvedené tabulky byly v tabulce č. 2 zhodnoceny jednotlivá kritéria a určeny váhy pro konečné zhodnocení. Váhy jsou uvedeny v pravém sloupci tabulky. Váhy byly přiděleny dle důležitosti parametru. Nevětší důležitost byla přidělena parametru rozlišení, dále byl důležitý úhel záběru, cena, paměťová kapacita a na posledním místě provedení kamer. V dalším kroku bylo potřeba určit pořadí v řádku, jak se jednotlivé kamery umístily. Z prvního řádku je patrné, že pokud byly stejné hodnoty u jednoho parametru, bylo nutné bodové hodnocení rozdělit.

Tabulka 2 - *Multikriteriální analýza parametrů*

parametry	D-Link DCS-5030L	Edimax IC-7113W	Netatmo NSC01-EU	Váhy
Rozlišení	2,5	2,5	1	1
Úhel záběru	2	3	1	2
Provedení kamer	1,5	1,5	2	5
Kapacita Micro SD	1	2,5	2,5	4
Cena	1	2	3	3

Další postup byl takový, že se vždy vydělila hodnota parametru váhami v daném řádku a vyšly výsledné hodnoty, viz. Tabulka č. 3. V posledních dvou řádcích už je spočítán a určen výsledek multikriteriální analýzy dat. Bylo potřeba udělat sumu jednotlivých sloupců a dle výsledků přiřadit jednotlivým kamerám pořadí. Nejlepší se rovnalo nejnižšímu přiřazenému číslu. Tedy na prvním místě se umístila kamera Netatmo NSC01-EU, na druhém D-Link DCS-5030L a na posledním Edimax IC-7113W.

Tabulka 3 - *Výsledek multikriteriální analýzy dat*

parametry	D-Link DCS-5030L	Edimax IC-7113W	Netatmo NSC01-EU
Rozlišení	2,5	2,5	1
Úhel záběru	1	1,5	0,5
Provedení kamer	0,3	0,3	0,4
Kapacita Micro SD	0,25	0,625	0,625
Cena	0,333333333	0,666666667	1
Suma	4,383333333	5,59	3,53
Pořadí	**2.**	**3.**	**1.**

Na základě porovnání všech dostupných dat a provedené analýzy lze konstatovat, že nejspolehlivější výrobek je kamera Netatmo NSC01-EU. I přesto že z porovnávaných výrobků je tato kamera nejdražší, vyplatí se investovat větší částku do pořízení tohoto výrobku z důvodu spolehlivosti aj. aspektů.

6. Závěr

Měření bylo realizováno na kameře Netatmo - NSC01-EU s funkcí rozpoznávání obličejů. Testování bylo provedeno ve vestibulu firmy, kam každý den dochází do zaměstnání v čase od 6:00 hod. do 22:00 hod., 12 subjektů (zaměstnanců). Do mobilního telefonu byla nainstalována aplikace pro přístup na cloud dané kamery Netatmo. První týden kamera byla kamera zapnuta bez sběru dat za účelem uložení jednotlivých obličejů zaměstnanců. Následně bylo provedeno měření kontinuálně po dobu cca 3 měsíců za standardního osvětlení vestibulu kanceláří s pomocí umělého osvětlení a tak za šera bez zapnutí umělého osvětlení. Také byla pozorována míra chybné identifikace, kdy kamera vyhodnotila pohyb a učila se nové tváře, ale v místnosti nebyla přítomna žádná osoba. Tato situace nastávala většinou v noci za tmy, kdy zavanul průvan a rozhýbal závěsy a záclony, které byly v zorném úhlu kamery a vytvořily mylnou představu přítomnosti člověka. Kamera identifikovala neživé předměty jako např. kytku, stín, závěsy nebo jinou část těla.

Samotné měření ukázalo, že během světla došlo k nejvyššímu počtu správně přiřazených osob. Za šera byly tyto výsledky nižší a za tmy byl počet správně přiřazených osob nejnižší. Při vyhodnocení bylo důležité vzít v potaz, že během světla byl pohyb osob nejvyšší - přibližně jedenáct tisíc zaznamenaných průchodů, v případě šera byl pohyb osob oproti pohybu za světla přibližně poloviční – přibližně pět tisíc průchodů. Za tmy docházelo k minimální detekci osob. Zaznamenaný trend odpovídá předpokládané docházce zaměstnanců. V případě detekce neživého objektu je podstatné zvýšení množství detekcí v případě tmy. To lze přisuzovat problémům v kvalitě obrazu. V případě počtu špatně přiřazených obličejů (záměna osob) k osobám z databáze za různých světelných podmínek bylo zjištěno, že za světla došlo k přiblížně pětseti padesáti záměnám, za šera k přibližně čtyř stům záměnám a za tmy k nepatrnému množství záměn. Toto je způsobeno především tím, že za světla a šera byl pohyb osob neúměrně vyšší pohybu za tmy. Co se týče poměru úspěšných identifikací vzhledem k celkovému počtu identifikací v procentech, bylo zjištěno, že za světla byla úspěšnost nejvyšší – dosáhla přibližně 90%, za šera byla dosažena úspěšnost srovnatelná s hodnotou dosaženou za světla – opět přibližně 90% a za tmy došlo ke značnému poklesu úspěšnosti – přibližně 65%.

V konečném multikriteriálním hodnocení byly porovnány jednotlivé parametry tří nejprodávanějších výrobků za poslední 4 roky, na základě dat o prodejích, které poskytla

firma Alza. Klady byly přiděleny dle důležitosti parametru. Nevětší důležitost byla přidělena parametru rozlišení, dále byl důležitý úhel záběru, cena, paměťová kapacita a na posledním místě provedení kamer. Na základě porovnání všech dostupných dat a provedené analýzy bylo konstatováno, že nejspolehlivější výrobek je kamera Netatmo NSC01-EU. I přesto že se jedná o výrobek nejdražší. Závěrem je nezbytné zdůraznit, že v této diplomové práci byly porovnány výrobky levnější a dostupné pro běžného uživatele. Špičkový kamerový systém s funkcí rozpoznání a identifikace ať již osob, registračních značek vozidel používaných například Policií ČR jsou v cenové relaci milionů korun.

Seznam literatury

[1] IGI Global Disseminator of knowledge. *www.igi-global.com* [online]. USA: IGI Global, 2018 [cit. 2017-12-01]. Dostupné z: https://www.igi-global.com/dictionary/smart-technology/38186.

[2] NABIL BELBACHIR, Ahmed. *Smart Cameras*. Ilustrované vydání. neznáme: Springer Science & Business Media, 2009. ISBN 9781441909534.

[3] Smart camera. *Wikipedia* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://en.wikipedia.org/wiki/Smart_camera

[4] HAVLE, Ing. Otto, CSc., MBA. Přehled trhu: inteligentní kamery. *Automa* [online]. **2009**(5) [cit. 2018-02-25]. Dostupné z: http://automa.cz/cz/casopis-clanky/prehled-trhu-inteligentni-kamery-2009_05_39009_4959/

[5] Snímač obrazu. *Wikipedie* [online]. 2016 [cit. 2017-12-04]. Dostupné z: https://sk.wikipedia.org/wiki/Sn%C3%ADma%C4%8D_obrazu

[6] Central processing unit. *Wikipedie* [online]. 2016 [cit. 2017-12-10]. Dostupné z: https://en.wikipedia.org/wiki/Central_processing_unit

[7] Digital signal processor. *Wikipedie* [online]. 2017 [cit. 2017-12-10]. Dostupné z: https://en.wikipedia.org/wiki/Digital_signal_processor

[8] Non-volatile memory. *Wikipedie* [online]. 2017 [cit. 2017-12-10]. Dostupné z: https://en.wikipedia.org/wiki/Non-volatile_memory

[8] RAM. Wikipedia [online]. 2017 [cit. 2017-12-10]. Dostupné z: https://cs.wikipedia.org/wiki/RAM

[10] Cafago. *Cafago* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.cafago.com/cs/p-s1420eu.html

[11] HORÁK, Martin. *IP kamery a jejich využití v průmyslu komerční bezpečnosti*. Zlín, 2007. Bakalářská práce. Universita Tomáše Bati ve Zlíně.

[12] About Morpho | Leader in Biometrics and Digital Identity. *Idemia* [online]. 2017 [cit. 2018-02-15]. Dostupné z: https://www.morpho.com/en/about-us

[13] Morpho in the Czech Republic. *Idemia* [online]. 2017 [cit. 2018-02-15]. Dostupné z: https://www.morpho.com/en/country/morpho-czech-republic

[14] Eyeidea recognition. *Eyedea Recognition s. r. o.* [online]. 2018 [cit. 2018-02-15]. Dostupné z: http://www.eyedea.cz/cs/about-us/

[15] Eyeidea recognition. *Eyedea Recognition s. r. o.* [online]. 2018 [cit. 2018-02-15]. Dostupné z: http://www.eyedea.cz/cs/products/

[16] FORENZNÍ SOFTWARE PRO ROZPOZNÁVÁNÍ OBLIČEJŮ. *Eyedea Recognition s. r. o.* [online]. 2018 [cit. 2018-02-15]. Dostupné z: http://www.eyedea.cz/cs/eyedentity/

[17] Mgr. Ing. ŠČUREK Radomír, Ph.D. *Biometrické metody identifikace osob v bezpečnostní praxi.* 2008.

[18] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA a kolektiv. *Biometrie a identita člověka*. neznámé: Grada, 2008. ISBN 8024723654.

[19] Iris recognition. *Wikipedia* [online]. 2018 [cit. 2018-01-09]. Dostupné z: https://en.wikipedia.org/wiki/Iris_recognition

[20] BENEŠ, R. *Autentizační metody založené na biometrických informacích* [online]. Brno: Vysoké učení technické v Brně, 2010 [cit. 2017-12-29]. Dostupné z: http://access.feld.cvut.cz/view.php?nazevclanku=autentizacni-metody-zalozene-na-biometrickych-informacich&cisloclanku=2010110002

[21] KONÍČEK, JUDr. Tomáš. *Městské kamerové dohlížecí systémy*.

[22] Více jak 150 policejních vozů je vybaveno profesionální technikou. *Policie České republiky* [online]. 2015 [cit. 2018-01-20]. Dostupné z:

http://www.policie.cz/clanek/vice-jak-150-policejnich-vozu-je-vybaveno-profesionalni-technikou.aspx

[23] Úřad vlády ČR [online]. 2018 [cit. 2018-01-31]. Dostupné z:

https://www.vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-

na-zadost/Priloha_6_Material_2.pdf

[24] Idnes.cz zprávy [online]. 2018 [cit. 2018-01-30]. Dostupné z:

https://zpravy.idnes.cz/letiste-bezpecnost-schillerova-babis-praha-fe1-/domaci.aspx?c=A180130_112845_domaci_jn

[25] Vícekriteriální analýza variant. *Wikipedie* [online]. 2017 [cit. 2017-9-03]. Dostupné z: https://cs.wikipedia.org/wiki/V%C3%ADcekriteri%C3%A1ln%C3%AD_anal%C3%BDza_variant#Pojmy

[26] CZC.cz [online]. 2018 [cit. 2018-03-20]. Dostupné z:

https://www.czc.cz/netatmo-kamera-s-funkci-rozpoznavani-obliceju-zlato-bila/178141/produkt

[27] Alza.cz [online]. 2018 [cit. 2018-03-20]. Dostupné z:

https://www.alza.cz/edimax-ic-7113w-d3970032.htm?kampan=adpla_produkty_PC-doplnky

[28] CZC.cz [online]. 2018 [cit. 2018-03-20]. Dostupné z:

https://www.czc.cz/d-link-dcs-5030l/215484/produkt

[29] [CGY96] Cox, I. J., Ghosn, J., Yianilos P.N.: „Feature-based Face Recognition Using Mixture Distance“, CVPR ’96, str. 209–216, 1996.

[30] [KoM93] Kotek Z., Mařík V. a kol: „Metody rozpoznávání a jejich aplikace”, Academia Praha, 1993, str. 195, ISBN 80-200-0297-9.

[31] [LKP96] Lee, C. H., Kim, J. S., Park, K. H.: „Automatic Human Face Location in a Complex Background“, Paterrn Recognition, vol. 29, str. 1877–1889, 1996.

[32] [BHK97] Belhumeur, P. N., Hespanha, J. P., Kriegman, D. J.: „Eigenfaces vs. Fisherfacs: Recognition using Class Specific Linear Projection“, IEEE Trans. PAMI, vol. 19, str. 711–720, 1997.

[33] [LiK02] Lixin Fan, Kah Kay Sung: „A Combined Feature-texture Similarity Measure for Face Alignment Under Varying Pose“, School of Computing National University of Singapore, 2002.

[34] [Luc99] Lu, C. Y., Zhang, C. S.: „PCA-base Symmetry Detection”, Chinese Journal of Electronics, in Chinese, vol. 27, č. 5, 1999.

[35] [VAO94] Valentin, D., Abdi, H., O'Toole, A. J.: „Connectionist Models of Face Processing: A Survey", Pattern Recognition, vol. 27, str. 1209–1230, 1994.

[36] [ZYL97] Zhang, J., Yan, H., Lades M.: „Face Recognition: Eigenface, Elastic Matching and Neural Nets", Proc. IEEE, vol. 85, str. 1423–1435, 1997.

[37] [Aka92] Ali N. Akansu and Richard A. Haddad: „Multiresolution Signal Decomposition: Transforms, Subbands, and Wavelets", Academic Press, San Diego, CA, 1992.

[38] [BBH93] Jonathan N. Bradley, Christopher M. Brislawn and Tom Hopper: „The FBI wavelet/scalar quantization standard for grey-scale fingerprint image compression", In Visual Info. Process II, volume 1961 of Proc. SPIE, str. 293–304, Orlando, FL, April 1993. SPIE.

[39] [www04] Kosz, D.: „New numerical methods of fingerprint's recognition based ona mathematical description of arrangement of dermatoglyphics and creation of minutiae", 2018 [cit. 2017-12-01]. Dostupné z: www.optel.com.pl/software/english/method.htm.

Seznam obrázků

Obrázek 1 - *Inteligentní kamera se zabudovaným LED osvětlením* 10

Obrázek 2 - *Dva druhy základních přístupů k členění biometrické identifikace* 14

Obrázek 3 - *Verifikace* 16

Obrázek 4 - *Proces identifikace* 17

Obrázek 5 - *Ruka se zrcadly, jež je snímána CCD kamerou a příklad měření vzdálenosti* 18

Obrázek 6 - *vzory otisků prstu* 19

Obrázek 7 - *Standardní vzory tváří využívané k rozložení obrazu* 21

Obrázek 8 - *Příklad šesti skupin vytvořených na základě LDA analýzy* 21

Obrázek 9 - *Síť vytvořena pomocí elastického mapování a vs. obraz, jež zpracoval počítač* 22

Obrázek 10 - *Ukázky zpracování biometrických dat pomocí počítače* 22

Obrázek 11 - *Průřez oka* 23

Obrázek 12 - *Lokalizace duhovky a její piktografické znázornění* 24

Obrázek 13 - *Sítnice s charakteristickými parametry* 25

Obrázek 14 - *Vytváření drah těžiště trupu* 26

Obrázek 15 - *Ukázka různých znaků obličeje* 28

Obrázek 16 - *Příklad softwaru pro identifikaci osob* 30

Obrázek 17 - *Dynamický monitorovací systém a jeho infrastruktura* 31

Obrázek 18 - *Ukázky podoby počítačového terminálu s dotykovým displejem a kamery* 34

Obrázek 23 - *Kamera Netatmo s funkcí rozpoznávání obličejů NSC01-EU* 38

Obrázek 24 - *Síťová bezpečnostní kamera Edimax IC-7113W* 40

Obrázek 25 - *Otočná IP kamera - D-Link DCS-5030L* 41

Seznam tabulek

Tabulka 1 - *Parametry pro konečné hodnocení* 46

Tabulka 2 - *Multikriteriální analýza parametrů* 46

Tabulka 3 - *Výsledek multikriteriální analýzy dat* 47

Seznam grafů

Graf 1 - *Správně přiřazený obličej* 43

Graf 2 - *Přiřazení neživého objektu* 43

Graf 3 - *Záměna osob* 44

Graf 4 - *Chybovost identifikace* 45