Testování spolehlivosti software určeného pro detekci osob

Bc. Lukáš Gabko, DiS.

Diplomová práce 2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

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

Jméno a příjmení:	**Bc. Lukáš Gabko, DiS.**
Osobní číslo:	**A17459**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Testování spolehlivosti software určeného pro detekci osob**
Téma anglicky:	**Testing Software Reliability Designed to Detect People**

Zásady pro vypracování:

1. **Vypracujte rešerši zaměřenou na způsoby detekce obličeje osob.**
2. **V rámci rešerše se orientujte na kamerové systémy používané v bezpečnostních technologiích, možnosti ukládání záznamu a export obrázků.**
3. **Proveďte analýzu trhu zaměřenou na softwarové nástroje vhodné pro detekci obličeje osob.**
4. **Otestujte spolehlivost dvou zvolených softwarových nástrojů určených pro detekci obličeje.**
5. **Proveďte diskuzi získaných výsledků a možnosti využití v bezpečnostní oblasti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, L. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeR-BuM, 2011. ISBN 978-80-87500-19-4.**
2. **LUKÁŠ, L. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeR-BuM, 2012. ISBN 978-80-87500-05-7.**
3. **LOVEČEK, T. a NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. 1. vyd. Žilina: Žilinská univerzita, 2008. ISBN 978-80-8070-8931.**
4. **KŘEČEK, S. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Crice-tus, 2006. ISBN 80-902938-2-4.**
5. **JAIN, A. K. a LI, Z. S. Handbook of Face Recognition, Springer-Verlag London, 2011. ISBN 978-0-85729-931-4.**
6. **GONG, S.Dynamic Vision: From Images to Face Recognition, Imperial College Press, 2005. ISBN 978-1860941818.**
7. **HORNÝ, Stanislav a Libor KRSEK. Úvod do multimédií. Vyd. 1. V Praze: Oeconomica, 2009, 157 s. ISBN 978-80-245-1608-0.**
8. **LONG, Ben a Sonja SCHENK. Velká kniha digitálního videa. Vyd. 1. Překlad Magdalena Kolínová. Brno: Computer Press, 2005, 478 s. ISBN 80-251-0580-6.**

Vedoucí diplomové práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 20. května 2019

Bc. Lukáš Gabko v. r.
podpis diplomanta

ABSTRAKT

V teoretické části diplomové práce jsou popsány kamerové systémy, princip činnosti kamer a jednotlivé komponenty kamerových systémů. Druhá kapitola je věnována způsobu detekce a rozpoznávání obličejů, jsou zde popsány v praxi používané metody. V první praktické části diplomové práce jsou uvedeni výrobci softwarových programů pro detekci obličejů s následným porovnáním v databázi osob a způsoby testování dle mezinárodního standardu. Druhá část je věnována testování vybraných softwarů se zaměřením na jejich spolehlivost dle předem definovaných scénářů. V poslední části diplomové práci je vedena diskuze nad výsledky spolehlivosti detekce a identifikace osob a možnosti aplikování těchto software v bezpečnostní oblasti.

Klíčová slova: kamera, detekce osob, identifikace osob, software

ABSTRACT

In the theoretical part of the thesis there is a description of camera systems, camera operation principle and individual components of camera systems. The second chapter is devoted to the method of face detection and recognition, the methods used in practice are described here. The first practical part of the thesis speaks about manufacturers of software programs for face detection with subsequent comparison in the database of persons and methods of testing according to the international standard. The second part is devoted to testing selected software with a focus on their reliability according to predefined scenarios. In the last part of the thesis there is a discussion over the results of reliability of detection and identification of persons and the possibility of applying these software in the security area.

Keywords: camera, detection of people, identification of people, software

Poděkování

Na tomto místě bych chtěl poděkovat doc. Mgr. Milanu Adámkovi, Ph.D. za vedení mé diplomové práce cenné rady a odborný dohled. Děkuji také Ing. Milanu Šindelovi za pomoc při gramatické a formální kontrole práce.

Poděkování patří i všem, kteří mě v průběhu celého studia podporovali, zejména mé rodině.

Motto: *„Bruslím tam, kde puk bude, nikoliv, kde je.“*

Wayne Gretzky – kanadský hokejista

OBSAH

ÚVOD

Rozpoznávat jednotlivé předměty, věci, osoby a vjemy patří k základním lidským schopnostem. Lidské smysly jsou uzpůsobeny k tomu, aby se člověk mohl správně orientovat a rozhodovat. Lidské oko nám v každodenní činnosti pomáhá snad ze všech smyslových orgánů nejvíce. Pomocí rohovky, čočky, tyčinek, čípků a ostatních částí dokážeme identifikovat značné množství objektů, skutečností, díky očnímu kontaktu můžeme komunikovat s okolím. Aniž bychom si to uvědomovali, tak ve skutečnosti pomocí vidění získáváme nové informace anebo si ověřujeme informace již získané. Vytváříme si různě důležité databáze v paměti, jež jsou mezi sebou vzájemně propojené a které se neustále plní novými daty a dochází k porovnání s daty již uloženými. Typický je příklad, kdy se náhodně střetneme s cizí osobou. Pomocí zraku dojde k načtení základních údajů o dotyčné osobě, jako jsou tvar obličeje, vlasy a jejich barva a další parametry člověka. Jaké informace o druhé osobě si do naší databáze mysli uložíme je značně individuální. Následně probíhá porovnání s databází uloženou v paměti. Výsledkem by mělo být označení, zda jsme již dotyčnou osobu viděli nebo ne. Ne vždy je však odpověď jednoznačná a stává se, že si sami nejsme jistí, zda jsme se s dotyčným již setkali nebo nikoliv. Nejistotu při rozhodování může vyvolat zapomnětlivost nebo osoba zásadně změnila vizáž anebo jsme potkali dotyčného coby jednoho z jednovaječných dvojčat…

Kolem roku 1970 dochází k digitálnímu zpracování obrazu a v následujících letech se vědci postupně zabývají 3D strukturou objektů. Postupně se oblast rozvíjí do více směrů, přičemž jedním z nich se stala detekce objektů a detekce osob. V roce 2019 se s rozpoznáváním předmětů a detekcí osob setkáváme každý den. Ať se již jedná o rozpoznání naší registrační značky na vozidle a její následné zobrazení na panelu spolu s aktuální rychlostí vozidla nebo detekci podezřelého zavazadla na veřejném prostranství anebo Face ID, které nám pomáhá bezpečně odemknout náš mobilní telefon identifikací našeho obličeje.

Základem pro další zpracování však zůstává kvalitní vstupní vizuální podklad (fotografie, video sekvence). Ačkoliv se přední výrobci kamerových systémů, digitálních fotoaparátů a mobilních telefonů předhánějí ve velikosti rozlišení u svých výrobků, není zatím v jejich silách dosáhnout kvality rozlišení zdravého lidského oka. Vědci odhadují, že jedno zdravé lidské oko má rozlišení 576 megapixelů, ale jen 7 megapixelů má pro člověka doopravdy význam. Podobné je to i se zmíněnými kamerami, ne všechny informace, které kamerovým systém získáme, jsou pro nás důležité nebo užitečné. Důvodem pro stále větší rozlišení je potřeba získat kvalitní obraz pro další zpracování, které pak následně probíhá. V této

souvislosti existuje celá řada video analytických softwarů, které dokážou setřídit data do ucelených celků tak, aby pro uživatele byly požadovaným přínosem, nebo nám pomáhají automatizovat některé procesy. (1)

Ve spojitosti se řešením bezpečnostní situace ve světě se v posledních letech často mluví o megatrendu umělé inteligenci (Artificial Inteligence). Umělá inteligence dokáže pomocí vysokého počítačového výkonu, objemu dat a algoritmů strojového učení zpracovávat a řešit složité problémy. Oblast rozpoznávání obličejů potažmo detekce předmětů nezůstala v této oblasti pozadu a umělou inteligenci ve svých algoritmech hojně využívá.

Bezpečnostní situace v České republice se neustále vyvíjí a mění. I když riziko spáchání teroristického činu zatím nebylo zaznamenáno, neznamenáno to, že by se radikálové na našem území nepohybovali. Míra kriminality v České republice má dlouhodobě klesající tendenci, ale objasněnost trestných činů se standardně pohybuje pod 50 % úspěšnosti. Dle mého názoru bude rozpoznávání obličejů s následným porovnáním v databázi (Face Recognition) v bezpečnostní problematice nabývat na svém významu nejen v boji proti terorismu, ale bude se využívat i při vstupech do objektů zvláštního významu či pro identifikaci osoby podezřelé ze spáchání trestné činnosti. (2) (3)

V teoretické části diplomové práce jsou popsány možnosti získávání podkladů pro detekci osob kamerovými systémy. Navazující část práce se zabývá jednotlivými algoritmy pro detekci obličejů a identifikaci osob. Praktická část diplomové práce je věnována analýze současných výrobců softwarů pro Face Recognition s následným testováním dvou samostatných programů a jednoho software, který je produktem výrobce kamerových systémů. V poslední části práce je vedena diskuze nad zjištěnými výsledky testování jednotlivých softwarů a jejich možná aplikace do průmyslu komerční bezpečnosti.

I. TEORETICKÁ ČÁST

1. KAMEROVÉ SYSTÉMY V BEZPEČNOSTNÍM PRŮMYSLU

Hlavním zdrojem vizualizačních dat je v průmyslu komerční bezpečnosti kamerový systém, jehož primárním úkolem je monitorovat snímanou scénu a následně potvrzovat vzniklé poplachové události. Jelikož současný technologický rozvoj udělal značný pokrok, tak i možnosti kamerových systémů se značně rozšířily. Díky specializovaným software dokážeme již na úrovni kamery detekovat změnu v obraze, zónovat snímanou scénu, trackovat objekty nebo vytvářet bezpečnostní koridory. Inovace se týkají nejen softwarové části, ale i sama kamera prošla značnou modernizací. Asi největší změnou je přechod z analogových kamerových systémů na síťové kamerové systémy označovány jako IP kamery.

1.1 Hlavní komponenty kamer

Mezi základní části analogových kamerových systémů patří objektiv a fotocitlivý prvek. U IP kamerových systémů patří mezi základní části i elektronická část. Objektiv spolu s ovládacími prvky pro zoom a clonou tvoří první část kamery a slouží k vytvoření obrazu snímané scény. Za objektivem je umístěn fotocitlivý prvek pro záznam obrazu. Pomocí senzoru dochází k převodu obrazu do elektrické podoby. IP kamerové systémy digitalizují získané informace ze snímače pomocí mikroprocesoru a elektronické části. Obě části taktéž komprimují data, ukládají je na média nebo přenášejí na záznamová zařízení či zobrazovací jednotky. (4)

1.1.1 Objektiv

Objektiv je složen z několika čoček a dalších součástí, které jsou uspořádány do optické osy. V případě, že dochází k ostření nebo zoomování, jednotlivé prvky objektivu se začnou pohybovat. Hlavní funkcí objektivu je promítnutí zmenšeného obrazu snímané scény na plochu fotocitlivého snímače kamery. Mezi hlavní parametry objektivu patří: ohnisková vzdálenost, světelnost, clona a hloubka ostrosti. (4) (5)

1.1.1.1 Ohnisková vzdálenost

Ohnisková vzdálenost, rovněž označována jako focus, je pomyslná vzdálenost za objektivem měřená od optického středu objektivu k rovině snímání. V této vzdálenosti se objekt ležící v nekonečné vzdálenosti zobrazí ostře.

Obrázek 1 – Ohnisková vzdálenost ve vztahu k úhlu záběru (6)

Ohniskovou vzdáleností se mění šířka a úhel záběru, přičemž všeobecně se dá konstatovat, že čím kratší je ohnisková vzdálenost, tím širší je úhel záběru. Podle typu snímače a ohniskové vzdálenosti se určují pozorovací úhly záběru snímané scény. Pomocí transfokátoru můžeme plynule měnit ohniskovou vzdálenost u některých objektivů. Podle toho jestli můžeme měnit ohniskovou vzdálenost, rozlišujeme tři typy objektivů. Pokud je od výrobce ohnisková vzdálenost pevně nastavena, mluvíme o objektivech s pevným ohniskem. V případě, že je možné ručně otáčet částí objektivu, jedná se o objektiv s proměnným ohniskem. Třetí možností je objektiv s elektronickou řízenou změnou ohniska, která je nastavitelná pomocí motorku. (4) (5)

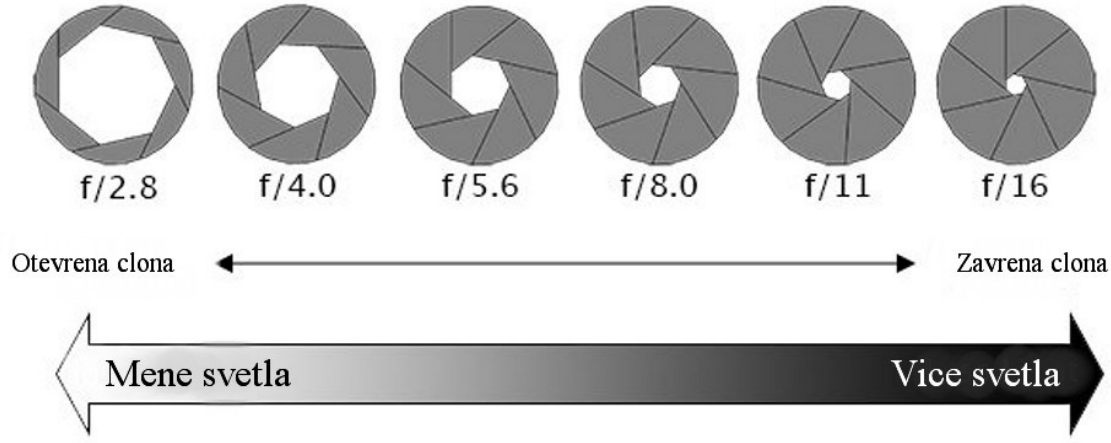
1.1.1.2 Světelnost

Světelnost objektivu je v podstatě maximální schopnost přijímat světlo, přičemž platí, že čím menší je číslo označující světelnost, tím je tato schopnost objektivu větší. Světelnost je dána nejmenším clonovým číslem objektivu, v technické dokumentaci označováno jako ***F***. Při zaznamenávání obrazu to znamená, že pokud je světelnost větší (menší clonové číslo ***F***), můžeme zkrátit čas uzávěrky a tím snížit možnost rozmazání snímku. (5)

1.1.1.3 Clona

K regulaci množství světla procházejícího objektivem s následným dopaden na fotocitlivý prvek používáme clonu. Tento mechanický prvek je tvořen kovovými lamelami, pomocí kterých lze měnit prstenec pro průchod světla. Velikost nastavení clony má přímí vliv na rozlišovací schopnost, což je kvalita s jakou je objektiv schopný vykreslit snímanou scénu. Postupným zavíráním clony se rozlišovací schopnost objektivu nejdříve zlepšuje, ale při

malém otevření clony se rozlišovací schopnost zhoršuje. Clonové číslo (f) vyjadřuje poměr ohniskové vzdálenosti a průměru otvoru clony. Čím menší clonové číslo je, tím menší jsou světelné ztráty v soustavě čoček a o kvalitnější objektiv se jedná. Clonové čísla se řídí geometrickou řadou 1; 1,4; 2; 2,8; 4; 5,6; 8; 11; 16; 22; 32. Podle způsobu ovládání lze clony rozdělit na objektivy s pevnou clonou, kde je nastavení clony stanoveno výrobcem a není možné ji měnit. U objektivu s manuálním nastavením clony si uživatel clonu koriguje dle vlastních požadavků. Třetí možností je řídit clonu automaticky, přičemž pro ovládání clony je využívána elektronika a servomechanismus. (4) (5)



Obrázek 2 – Nastavení clony (7)

1.1.1.4 Hloubka ostrosti

Hloubku ostrosti lze zjednodušeně definovat jako rozsah vzdáleností na scéně, kde se na výsledném snímku zdá vše ostré. Z pohledu fotografa lze o hloubce ostrosti mluvit tehdy, pokud pozorujeme fotografii o velikosti A4 ze vzdálenosti 38 centimetrů a tato scéna se zdá, zdravému oku, ostrá. Zavírání clony hloubku ostrosti zvyšuje, zatímco otevírání hloubku ostrosti snižuje. (8)

1.1.2 Fotocitlivé prvky

Světlo ze snímané scény prochází objektivem kamery a pomocí soustavy čoček dopadá na snímaný čip. Na čipu je dopadající světlo prostřednictvím fotocitlivého prvku přeměněno na elektrický proud. Elektronika v kameře převede elektrický proud na analogový nebo digitální obraz, který je možné dále zpracovávat či přenášet. (9)

V praxi se setkáváme s různými druhy fotocitlivých prvků, přičemž nejvíce rozšířenými jsou CCD senzor, Super CCD senzor, CMOS nebo DPS senzor. Na základě svého principu, konstrukce a technologie výroby se mění i získané technické parametry kamer.

1.1.3 Technické parametry kamer

S technologickým rozvojem výrobců a s požadavky zákazníků se mění i požadavky na jednotlivé technické parametry kamer. Dříve se sledovaly zejména parametry týkající se rozlišení, snímacího čipu, světelné citlivosti, poměru stran obrazu, dynamičnosti obrazu či napájení, tak v současnosti nás zajímají i funkcionality jako jsou automatické přepínání mezi denní a noční scénou, integrovaný IR přísvit, nástroje pro potlačení nepříznivých vlivů, kompresní metoda či automatické vyrovnání bílé barvy a další.

		1.0 MP	2.0 MP	3.0 MP	5.0 MP
Image Sensor		1/2.8" progressive scan CMOS			1/1.8" progressive scan CMOS
Aspect Ratio		16:9		4:3	
Active Pixels (H x V)		1280 x 720	1920 x 1080	2048 x 1536	2592 x 1944
Imaging Area (H x V)		4.8 mm x 2.7mm; 0.189" x 0.106"		5.12 mm x 3.84 mm; 0.202" x 0.151"	6.22 mm x 4.66 mm 0.245" x 0.183
IR Illumination (option) (High Power 850 nm LEDs)		30 m (98 ft) max. distance at 0 lux			
Minimum Illumination	3 - 9 mm lens:	0.04 lux (F1.3) in color mode; 0.008 lux (F1.3) in monochrome mode			N/A
	4.3 - 8 mm lens:	N/A			0.033 lux (F1.8) in color mode; 0.0066 lux (F1.8) in monochrome mode
	9 - 22 mm lens:	0.08 lux (F1.6) in color mode; 0.016 lux (F1.6) in monochrome mode			0.026 lux (F1.6) in color mode; 0.005 lux (F1.6) in monochrome mode
Image Rate (full resolution)		30 fps		30 fps (20 fps with WDR enabled)	30 fps
Dynamic Range		67 dB			83 dB
Dynamic Range (WDR enabled)		120 dB triple exposure (20 fps or less); 100 dB dual exposure (30 fps)			N/A
Resolution Scaling		Down to 768 x 432			Down to 1792 x 1344
Camera Operating Mode		N/A			

Obrázek 3 – Ukázka technických parametrů IP kamery společnosti Avigilon (10)

1.2 Analogové kamerové systémy

Analogové kamerové systémy jsou z pohledu historie v oblasti bezpečnostního průmyslu využívány již několik desítek let a prošly svým vývojem. I přes určitou technologickou zastaralost jsou díky své vyšší citlivosti, nižším nárokům na diskovou kapacitu a menším finančním nárokům stále v nabídce výrobců kamerových systémů. Základní složení komponentů samotné kamery je uvedeno v kapitole 1. 1, dále jsou v textu níže popsány možnosti přenosu analogového signálu, záznamová a zobrazovací zařízení.

1.2.1 Přenos analogového signálu

Nejběžnějším způsobem přenosu analogového video signálu na kratší vzdálenost (řádově stovky metrů) je použití koaxiálního kabelu s impedancí 75 ohmů. Pro propojování komponentů analogového kamerového systému v řádech jednotek kilometrů se využívá telekomunikačního kabelu se dvěma sadami vodičů (kroucený pár). Vysoká přenosová rychlost, velká vzdálenost, stabilita a odolnost proti elektromagnetickému rušení jsou největší výhody, které nabízí možnost přenášet signál prostřednictvím optického kabelu. V případech, kdy není možná pokládka metalických či optických kabelových tras, je vhodné přenášet informace pomocí bezdrátového přenosu a to na Českým telekomunikačním úřadem garantovaných frekvencích 10 GHz , 5,8 GHz a 2,4 GHz. Na velmi krátkou vzdálenost lze přenášet videosignál i přes infračervený přenos. (11)

1.2.2 Záznam obrazu

Pro potřeby forenzního zkoumání a vyhodnocování událostí je nutné mít k dispozici záznamové zařízení, na kterém bude možné uchovávat videosignál ze snímané scény. Pro analogové kamerové systémy je možné zaznamenávat obrazový signál na analogové záznamové zařízení anebo digitální záznamové zařízení. Za historický je považován záznam na VCR (Video Cassete Recorder), kdy pomocí změny elektrického signálu na magnetické pole došlo k uchování záznamu na fóliový pásek. Kapacita záznamu byla omezena velikostí délky kazety nebo nutnosti pravidelné výměny kazet. Digitální záznam videosignálu je možné ukládat pomocí přídavných karet PCI (Peripheral Component Interconnect) anebo DVR (Digital Video Recorder). Přídavné karty PCI se instalují do osobních počítačů a pomocí analogově – digitálního převodníku dochází k digitalizaci obrazu, který je následně ukládán na pevný disk osobního počítače. Digital Video Recordery jsou velmi podobné osobním počítačům a jejich hardwarové vybavení (procesor, operační paměť, základní deska, síťová karta, diskový řadič) spolu s digitalizací a multiplexováním dává předpoklad pro kvalitně zpracovaný a uložený záznam snímané scény. Do DVR je možné připojit 1, 2, 4, 8, 16 nebo 32 video vstupů. V případě, že je nutné videosignál „posílat“ po ethernetové síti mimo objekt, v němž je uloženo DVR, připojí se k DVR síťový prvek a následně může být videosignál zobrazen i několik kilometrů od místa instalace kamerového systému. Další možností uchování záznamu je video server, který převádí analogový signál na digitální a v případě, že je připojen síťový prvek je možné videosignál distribuovat po ethernetové síti dále. (9) (11)

1.2.3 Zobrazovací zařízení

Pro monitorování snímané scény v živém přenosu (on-line režim), ale i pro přehrávání událostí z historie se využívají zobrazovací jednotky neboli monitory. Analogový signál se zobrazuje na speciálních CRT (Carhode Ray Tube) monitorech, které jsou přizpůsobeny pro 24 hodinový provoz. Černobílé monitory jsou již téměř na všech místech nahrazeny barevnými monitory, čímž se zlepšila uživatelská přívětivost i vyhodnocovací možnosti. V případě, že je žádoucí zobrazovat na jednom monitoru více kamer, musí být do systému implementován prvek, který dokáže videosignál pro takové zobrazení upravit. Kamerový přepínač umožňuje ruční nebo automatické přepínání obrazu z kamer na obrazovku monitoru. Rozdělením obrazovky na čtyři stejné části docílíme možnosti monitorovat v jeden okamžik čtyři snímané scény. K zajištění takové funkcionality je nutné instalovat kvadrantový selektor, zkráceně kvadrátor. Pro jednoduché monitorování více kamer se rovněž využívá zobrazení obrazu v obraze, kdy je obraz z jedné kamery roztažen přes celý monitor a z dalších kamer je obraz zmenšen. K zobrazování snímané scény z kamerového systému s více videosignály se používá multiplexer, který je zároveň přímo propojen se záznamovým zařízením. Multiplexer se vyrábí ve variantách pro 4, 8 a 16 kamer a je již plně digitalizován. U rozsáhlých kamerových systémů s velkým množstvím kamer a zobrazovacích monitorů se k přepínání kamer na jednotlivé monitory používá křížové přepojovací pole. Pomocí tohoto zařízení si může operátor určovat, kterou kameru bude mít zobrazenou na jakém monitoru. Multiplexery a křížová přepojovací pole (video matice) jsou digitálními systémy a proto je možné zobrazovat informace nejen na CRT monitorech, ale i na LCD (Liquid Crystal Display) displejích. (11) (12)

Důležitým parametrem pro CRT monitory a LCD displeje je jejich rozlišení. U analogového videa rozlišujeme formáty PAL (Phase Alternation by Line) a NTSC (National Television System Committee) u digitálního video signálu se jedná o VGA (Video Graphics Array) a MPEG (Motion Picture Expert Group). U analogového formátu je rozlišení PAL 576 horizontálních řádků při 25 snímcích za sekundu. NTSC má nižší rozlišení a to 480 horizontálních řádků, ale dokáže za jednu vteřinu zobrazit 30 snímků. Při digitalizaci analogového videa je důležitým údajem počet pixelů, jež budou vytvořeny na jeden řádek analogového obrazu. U formátu PAL je definována rozlišení 704 x 572 pixelů a pro NTSC je to 704 x 480. U zobrazení analogového kamerového systému v průmyslu komerční bezpečnosti se využívá maximálního rozlišení zobrazovací jednotky pro současně čtyři kamery, čtvrtina celkového obrazu se označuje jako CIF (Common Intermediate Format).

Rozlišení pro VGA je vyjádřeno jako 640 x 480 pixelů a podobně jako u analogových zobrazovacích jednotek v průmyslu komerční bezpečnosti, tak i u VGA se sdílí maximální rozlišení pro čtyři kamery, takovou čtvrtinu označujeme jako rozlišení SIF (Standard Interchange Format). Jako čtyř násobek VGA se označuje rozlišení 1280 x 960 pixelů, což je počet pixelů v řádu jednotek milionů a v takovém případě mluvíme o megapixelovém rozlišení. Zobrazovací zařízení s vysokým rozlišením budou popsána v kapitole 1. 3. 4. (5) (11) (13) (14)

1.3 IP kamerové systémy

Nástupcem analogových kamerových systémů se potupně stávají IP kamerové systémy. Základní prvky takových kamerových systémů zůstávají stejné, jen jsou tyto systémy plně digitální a prošly technickou modernizací. Na úrovni kamery došlo k zásadní změně, přičemž zpracování obrazu do digitální podoby probíhá již v samotné kameře pomocí obrazového procesoru. Rovněž komprese dat je řešena na úrovni kamery. Kamera disponuje svým vlastním CPU (Central Processing Unit), DRAM (Dynamic Random Access Memory) a svou interní flash pamětí. Pro přenos dat po ethernetové nebo optické síti je kamera doplněna o patřičný konektor. Výjimkou nejsou ani kamery s integrovanou kartou pro bezdrátový přenos. V oblasti rozlišení kamer se v současné době pohybujeme na úrovni několika jednotek megapixel, ale na trhu lze najít i kamery s rozlišením přesahující 15 megapixel. Rovněž je možné zaznamenávat více snímků za jednu sekundu, kdy dnes je standardní zachytit za jednu sekundu 30 až 60 snímků. Další výhodou je kabeláž (datový síťový kabel), která může být použita jednak pro propojení jednotlivých komponentů kamerového systému, ale zároveň stejnou kabeláží lze přistupovat z osobního počítače do Internetu. Datovým síťovým kabelem lze kameru i napájet. Všechny síťové kamery mají v počítačové síti přidělenou vlastní IP adresu (statickou nebo dynamickou), což je výhodou při identifikaci případných problémů v nastavení či síti. (15)

I když kamery disponují velmi dobrou kompresí (přenáší se jen změny na snímané scéně) tak větší rozlišení a vyšší frekvence snímkování má vliv na diskovou kapacitu záznamových zařízení. Při 30 snímcích za sekundu a jednodenní archivaci je pro jednu kameru potřebné mít diskové pole v řádech desítek GB. V případě, že jsou data z IP kamery přenášena přes globálně otevřený Internet, je nutné věnovat zvýšenou pozornost samotnému zabezpečení jednak kamery, ale i celého datového síťového přenosu. Kybernetické útoky na jednotlivé zařízení se pravidelně objevují a výrobci musí na tyto situace pružně reagovat vydáváním

bezpečnostních záplat. Výše uvedené faktory mají také vliv na celkové finanční náklady spojené s modernizací nebo budováním nových kamerových systémů.

1.3.1 Základní konstrukční rozdělení IP kamer

Podle možnosti využití IP kamery je důležité zvolit vhodné konstrukční provedení samotné kamery. Jedním z kritérií pro vhodný výběr IP kamery je prostředí, ve kterém bude kamera instalována. Jedná se o vnitřní či venkovní prostředí a další dělení můžou ještě ovlivnit i faktory jako povětrnostní podmínky (např. mořské prostředí) nebo prostředí s vysokým nebezpečím exploze. Dle konstrukce samotné kamery lze obecně IP kamery rozdělit na statické (fixní) a otočné (Pan –Tilt – Zoom).

1.3.1.1 Fixní kamery

Do této kategorie se řadí kamery, které mají pevně stanovený úhel záběru, bez možnosti otáčení v horizontálním nebo vertikálním směru. Změna úhlu záběru snímané scény je možná pomocí zoomovacího objektivu. Bez patřičného krytu jsou fixní kamery označovány box kamerami a jsou instalovány přímo na stativ nebo držák. Výhodou je, že v rámci servisních prací je k nim velmi dobrý přístup, což je zároveň i nevýhoda, protože potencionální narušitel může s kamerou libovolně otáčet. Tyto kamery jsou instalovány převážně do vnitřního prostředí a do dostatečné výšky od země, aby případná sabotáž byla co nejvíce ztížena. Do venkovního prostředí se fixní kamery instalují v krytech zvaných bullet, které mají dostatečné IP krytí (odolnost elektrického zařízení proti vniknutí cizího tělesa a vniknutí kapalin), jsou vybaveny vyhříváním a integrovaným IR přísvitem. Přístup servisního technika do bullet kamery je již o něco složitější, ale to je zapříčiněno venkovním prostředím. Možnost manipulace narušitele s kamerou však zůstává. Třetím typem statické kamery je dle konstrukčního provedení dome kamera. Názve dome, znamená kupule a výhodou u těchto typů kamer je to, že není na první pohled patrné, jaký směr kamera monitoruje. Další výhodou je, že není možné s kamerou libovolně manipulovat a tím změnit snímanou scénu. V praxi se objevily případy, kdy se narušitelé snažili kopule rozbít fyzickou silou a proto je u těchto kamer uváděno i krytí proti vnějšímu mechanickému poškození IK (0 – 10 dle energie nárazu). (4) (16) (17)

Obrázek 4 – Konstrukční provedení fixních kamer

1.3.1.2 Otočné IP kamery

Hlavním rozdílem mezi otočnou kamerou a fixní kamerou je možnost měnit snímanou scénu otočnou kamerou ve třech možných variantách. Změna může probíhat v horizontální nebo vertikální ose a přibližování. Z anglického významu uvedených možností Pan – Tilt – Zoom se v praxi používá označení PTZ kamera. Kamery jsou nejčastěji v provedení dome a jsou určeny pro vnitřní i venkovní prostředí. Obrovskou výhodou je možnost monitorovat rozsáhlý prostor pomocí jedné kamery a operativně tak reagovat na vzniklou situaci. Kamera může být ovládána operátorem pomocí ovládacího pultu nebo kliknutím do obrazu snímané scény ve vyhodnocovacím software. PTZ kamery mají různé funkcionality, jako automatické trackování (otáčení) za objektem zájmu nebo na základě informací od poplachového systému se natočit do určitého místa (dle předem nastavených pozic). Určitou nevýhodou bylo, že otočné kamery se „neuměly podívat pod sebe“. Toto již bylo výrobci vyřešeno a nyní již nové PTZ kamery tímto problémem nedisponují. V případě použití zoomování dochází ke změně ohniskové vzdálenosti a operátor ztrácí celkový přehled o snímané scéně, což může způsobovat určité problémy. Multisenzorové panoramatické kamery mohou neustále monitorovat celou snímanou scénu a přitom je možné i zoomovat určité místo. Tato funkcionalita je zajištěna díky umístnění několik kamerových senzorů s proměnným ohniskem po konstrukčním obvodě kamery. Například multisenzorová panoramatická kamera od společnosti Axis modelové řady P3707-PE obsahuje čtyři kamerové senzory, jejichž umístnění na kruhové dráze lze upravovat tak, aby bylo možné monitorovat požadovaný prostor. Individuálně lze kamerové senzory naklánět v horizontálním úhlu od 108° do 54°. Rozlišení výše uvedeného typu panoramatické kamery

je 8 megapixelů. Z pohledu síťového provozu zabírá kamera jen jednu IP adresu a je možné kameru napájet pomocí datového síťového kabelu. (4) (18)

Obrázek 5 – Otočné IP kamery

1.3.2 Přenos síťového videa

Základní rozdělení přenosových tras videosignálu od kamery dále na záznamová a zobrazovací zařízení probíhá podobně jako u analogových kamerových systémů. Nejčastěji je přenos řešen pomocí metalických přenosových tras do vzdálenosti sto metrů (bez nutnosti instalace dalších síťových prvků) kroucenou dvou linkou. Tu tvoří osm samostatných měděných vodičů, které jsou barevně rozděleny do párů zakončených konektorem RJ - 45. Podle typu odolnosti proti rušení rozdělujeme metalickou kabeláž na UTP (Unshielded Twisted Pair), FTP (Foiled Twisted Pair), STP (Shielded Twisted Pair) a ISTP (Individual Shielded Twisted Pair). Rozdíl mezi jednotlivými typy kabelů je ve stínění, přičemž UTP nemá stínění, FTP má stínění celého kabelu fólií, STP je stíněn opletením a u ISTP je stíněn každý jednotlivý pár vodičů. Další členění strukturované kabeláže je podle šířky pásma a přenosové rychlosti. Označení Cat5e má šířku pásma 100 MHz a přenosovou rychlost 10 Mbps až 1 Gbps. Šířku pásma 250 MHz a rychlost přenosu 1 Gbps až 10 Gbps dosáhneme při použití kroucené dvoulinky označené jako Cat6. Až 10 Gbps s šířkou pásma 1200 MHz přeneseme pomocí Cat 7. Nově byla standardizována kategorie Cat8, která má šířku pásma 2000 MHz a přenosovou rychlost 40 Gbps. (17) (19) (20)

U IP kamerových systémů je možnost přenášet video signál i pomocí optických sítí a bezdrátovým přenosem.

K síťovému provozu kamerového systému, je nutné vybudovat kvalitní datovou infrastrukturu, jehož součástí jsou síťové switche, routery, šifrátory, firewally a další zařízení.

1.3.3 Záznam monitorované scény

Stejně jako u analogových kamerových systémů i u síťových systémů je důležitý záznam monitorované scény pro pozdější verifikaci poplachových událostí nebo jako důkazní materiál. Síťové záznamové zařízení, do kterého se ukládá záznam, se nazývá Network Video Recorder (dále jen NVR). Podle počtu připojených IP kamer je nutné volit i záznamové zařízení s dostatečným počtem digitálních vstupů. V současné době je možné instalovat NVR s 4, 8, 16, 32 nebo 64 digitálními vstupy, což umožňuje připojení stejného počtu IP kamer. V závislosti na počtu připojených IP kamer, rozlišení, kompresi, počtu snímků a doby archivace je nutné zvolit potřebnou diskovou kapacitu NVR. K orientačnímu výpočtu diskové kapacity jsou určeny různé softwarové nástroje, které jsou instalovány přímo v NVR nebo je možné použít aplikace třetích stran, jako je uvedeno na Obrázku 6.

Obrázek 6 – Výpočet úložiště záznamu pro jednu kameru (21)

Datové úložiště může být řešeno pevnými disky (HDD) nebo nezávislým vícenásobným diskovým polem (RAID). Pomocí NVR je možné po datové síťové kabeláži jednotlivé kamery napájet. K tomu je nutné, aby NVR podporoval napájení PoE (Power over Ethernet). Důležitým aspektem je možnost kombinovat výrobce jednotlivých prvků kamerového systému. Ne vždy je možné připojit do záznamového zařízení síťové kamery různých

výrobců, což může komplikovat budování nových nebo modernizaci stávajících kamerových systémů. Standardně je k záznamovému zařízení dodáváno i přívětivé uživatelsko-administrativní prostředí VMS (Video Management Systém), díky kterému je možné zobrazovat a konfigurovat celý systém. Možnost přístupu více uživatelů je umožněna díky síťovému provozu. Celá řada záznamových zařízení umožňuje přístup k datům pomocí mobilních aplikací, kdy si uživatel přes svůj chytrý mobilní telefon může prohlížet vybrané události. Vzdálený přístup do záznamového zařízení přes Internet představuje komfortní řešení servisních zásahů bez nutnosti fyzické přítomnosti technika. Využívání mobilní aplikace nebo vzdálený přístup přes síť Internet, představuje potencionální bezpečnostní riziko kamerového systému a je nutné nastavit patřičné šifrování přenosu informací nebo vytvoření šifrovaných VPN tunelů.

1.3.4 Zobrazovací jednotky

Síťové kamery svým rozlišením zvyšují možnost sledovat na snímané scény více detailů nebo monitorovat větší prostor. K zobrazení těchto informací je vhodné disponovat kvalitními zobrazovacími zařízeními, která dokážou vyobrazit detaily zachycené kamerami s vysokým rozlišením. Tyto požadavky splňují LCD displeje, plazmové displeje, LED nebo QLED zobrazovací zařízení.

U monitorů stolních počítačů mluvíme o rozlišení nad jeden megapixelů u Full HD rozlišení 1920 x 1080 pixelů. Jako standard QHD označujeme 2560 x 1440 pixelů a označení 4K má monitor s rozlišením 3840 x 2160 pixelů. Kromě monitorů ke stolním počítačům jsou pro lepší přehlednost a uživatelský komfort na dohledová centra instalovány i průmyslové televize. Rozlišení u televizí může být ve standardu Full HD, 2K (2048 x 1080) 4K nebo 8K (7680 x 4320). Tato profesionální zařízení jsou určena pro nepřetržitý provoz 24/7/365 a jsou instalovány jako samostatné části anebo sdružovány do monitorových stěn. V poslední době se na trhu objevují zadně projekční kostky, které jsou dodávány v rozlišení Full HD. Při instalaci monitorovacích stěn se k jejich ovládání dříve používaly multiplexery a křížová přepojovací pole (video matice). V současnosti jsou již instalovány speciální servery, které pomocí software (např. eyeCON V5) dokážou řídit zobrazení monitorovací stěny podle nejrůznějších požadavků uživatelů.

Dalšími parametry, kterými se u zobrazovacích jednotek zabýváme, je odezva a uhlopříčka monitorů či průmyslových televizí. Z pohledu energetické náročnosti je důležitá spotřeba

elektrické energie. Samotné jednotky rovněž vyzařují do prostoru energii a zvyšují teplotu v místnostech, tato skutečnost pak ovlivňuje návrh klimatizačních a vytápěcích jednotek.

1.3.5 Pokročilé funkce IP kamerových systémů

Plná digitalizace IP kamerových systémů dává možnost ke zlepšení některých parametrů a funkcionalit systému. Ať se již jedná o zlepšení snímání scény nebo o video analytické funkcionality na úrovni záznamového zařízení. Pro vylepšení obrazu, ve kterém se objevuje šum, se na úrovni kamery používá funkce DNR (Digital Noise Reduction). Světlo, jež působí kontrastně na snímanou scénu, činí značné problémy při vyhodnocování snímané scény. Pomocí funkce WDR (Wide Dynamic Range) je kamera schopná takové kontrasty, mezi zejména bílou a černou barvou, potlačit a obraz náležitě „vyladit“. Mezi funkcionality, které podporuje již samotná kamera, patří detekce objektů, překročení vytyčené linie, detekce střelby, odebrání objektu ze snímané scény nebo detekce změny pozice kamery. V případě nastavení některé z funkcí (ty jsou individuální dle výrobce) dochází k vytvoření poplachové události, která následně upozorní operátora na dohledovém centru nebo může spustit jinou událost anebo odeslat informaci na mobilní telefon. (4)

Video analytické funkce na úrovni zpracování záznamu jsou vyžadovány jednak v bezpečnostním průmyslu pro rychlé vyhledávání, ale i například pro ochranu měkkých cílů [1]. Dnešní software dokážou během několika sekund vyhledat v celodenním záznamu například osobu v červeném kabátě nebo označí místo, kde dochází k vysoké koncentraci osob na veřejném prostranství…

Mezi inteligentní funkce síťových kamerových systémů patří i detekce obličeje potažmo rozpoznávání osob na základě předem vytvořené databáze.

1.4 Hybridní kamerové systémy

Častým důvodem k budování hybridních kamerových systémů je potřeba částečné modernizace současného analogového kamerového systému nebo doplnění analogového kamerového systému o nové kamery. Možnost vytvoření hybridního kamerového systému skýtá použití hybridního DVR, který má v sobě vstupy určené pro analogové kamery, ale zároveň do něj můžeme připojit IP kamery. Pro připojení analogového kamerového systému do síťového kamerového systému můžeme použít i video enkodér, který je vybaven několika

[1] Označení míst s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům.

vstupy, digitalizátorem obrazu, obrazovým kompresorem a webovým serverem se síťovým rozhraním. (22)

1.5 Ukládání záznamu a export obrázků z kamerových systémů

Základní možnosti ukládání video signálu pro analogový a IP kamerový systém byl popsán v předcházejících kapitolách. Další alternativou může být uložení zaznamenávaného video na SD kartu. Pro tuto eventualitu je nutné, aby kamera byla vybavena slotem pro vložení SD karty. Kapacita takové záznamové karty se pohybuje od 8 GB do 512 GB. Výhodou je, že po vyjmutí SD karty z kamery je možné ji připojit do počítače a dále informace zpracovávat. Nutnost mít do každé kameře jednu SD kartu je považována za nevýhodu. Další možností, jak ukládat záznam z kamerového systému, je využití cloudového úložiště třetí strany. K tomu, aby bylo možné využít cloudové řešení je nutné být připojen do Internetu stabilním připojením a mít k dispozici dostatečnou kapacitu na cloudovém disku. Využití cloudového řešení pro větší objemy dat bývá zpoplatněno a tudíž se do cloudu ukládají jen určité části video sekvence, nejčastěji poplachové události a několik video sekvencí před a po poplachové události.

Pro další zpracování videa mimo záznamové zařízení nebo Video Management System je důležitý samotný formát videa. Z důvodu zachování integrity vyexportovaného videa může mít video svůj vlastní formát, který stanovuje výrobce. Jednotlivé segmenty videa jsou označovány hologramem, tak aby nemohlo dojít k manipulaci se záznamem. Záznam, který je vyexportován ve formátu výrobce, může být použit orgány činnými v trestním řízení jako důkazní materiál před soudem. Standardně je k exportovanému videu ještě předán i program pro přehrání videa ve formátu výrobce.

Pro potřeby dalšího zpracování systémy třetích stran nebo jen pro obrazové reporty, je možné video záznamy exportovat i v obecných formátech jako jsou.avi, .wmv, .mp4 atd. Tyto formáty jsou již volně přehratelné a je možné s nimi pracovat dále, například jako podklad pro detekci předmětů nebo osob. (13)

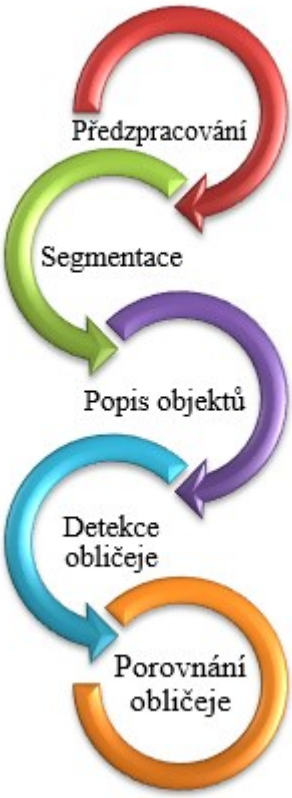
Ze záznamu je možné rovněž exportovat fotografie a to ve formátech .jpeg nebo .png. I tyto formáty je možné zpracovávat pro další účely uživatele.

Video sekvence nebo fotografie je možné exportovat na externí úložiště jako USB disky nebo harddisky. V případě síťového propojení se určená data mohou dále distribuovat na jiné servery nebo replikovat do různých databází k dalšímu zpracování.

2. ZPRACOVÁNÍ OBRAZU, DETEKCE A ROZPOZNÁVÁNÍ OBLIČEJE OSOB

Získané informace ze snímané scény můžeme dále digitálně zpracovávat. Jednou z možností dalšího zpracování je identifikace osob. Samotné identifikaci však musí předcházet určení, zda se osoba v obraze nachází. Dalším krokem je detekce a lokalizace obličeje osob. Následuje porovnání v předem připravené databázi a výstupem je výsledek s pozitivním nebo negativním oznámení o výskytu osoby v databázi. V druhé kapitole budou popsány způsoby zpracování obrazu, detekce obličeje osob s následným porovnáním v databázi osob. Celý popsaný proces se nazývá Face Recognition.

Po snímání a přenosu informací, které mají být dále digitálně zpracovávány, následuje proces převodu snímku do počítačového vidění. Takové zpracování obrazu má několik postupných fází. Na obrázku 7 je znázorněn postup zaměřený na detekci obličeje osob s následným porovnáním v databázi.



Obrázek 7 – Proces detekce a rozpoznávání obličeje osob

2.1 Předzpracování obrazu

V první fázi zpracování obrazu je důležité obrazovou informaci „očistit“ od optických chyb a šumů a zvýraznit části obrazu, které nesou důležité informace. Jedním ze způsobů je jasová transformace, která pomocí histogramu určuje výskyt četnosti jednotlivých hodnot jasu v obraze. Geometrickou transformací můžeme upravovat geometrické zkreslení obrazu. Filtrací pomocí Gaussova 2D filtru dokážeme eliminovat šum, který vzniká při snímání nebo přenosu dat. Další možností předzpracování je detekce hran, kdy za použití několika typů operátorů dokážeme v obraze zvýraznit ostré hrany. (23)

2.2 Segmentace

Jedná se o proces, při kterém dochází k dělení obrazu do jednotlivých částí (pixelů). Těmto částem je přidělen určitý index segmentu. Důvodem segmentace je oddělení důležitých částí obrazu od ostatních marginálních částí. V praxi se setkáváme s několika metodami segmentace, mezi které patří prahování, metoda vycházející z detekce hran, metoda orientovaná na regiony, znalostní metody a neuronové sítě. (14)

2.3 Popis objektů

V dalším kroku zpracování obrazu dochází k rozdělení nalezených obrazů do jednotlivých tříd. Objekty je možné rozdělit do čtyř základních tříd: dle barvy, umístnění, velikosti a tvaru. Barva je základní vlastností každého objektu a její výhodou je, že není závislá na pozici umístnění v obraze a její případné posunutí nebo změna úhlu pozorovatele objektu není problematické pro určení, o jakou barvu se jedná. V obraze objektu můžeme rozeznat, zda je některá barva dominantní nebo určit rozvržení barev. K určení polohy objektů v obraze se používá několik definic. Mezi základní definice patří určení polohy objektů jedním bodem nebo nalezení maximální a minimální polohy v horizontálním a vertikálním směru. Velikost objektů je možné určovat pomocí počtu pixelů, které ohraničují příslušný objekt. Pro složitější a přesnější výpočty velikosti objektů se používá metoda rotace konvexního mnohoúhelníku. Popsání tvaru objektů patří k nejtěžšímu, avšak nejdůležitějšímu úkolu, který je nutné při zpracování obrazu vyřešit. Velký problém pro rozpoznávání objektů v obraze podle tvaru je orientace a s tím spojený úhel, pod kterým je předmět pozorován. Pro určení tvaru objektů v obraze se používají různé šablony. Tvar objektů je možné popsat pomocí hraničních bodů nebo pomocí tvaru regionu. (24)

2.4 Detekce obličeje osob

Detekce obličejů osob prošla v posledních 20 letech významnou proměnou. Existuje nepřeberné množství metod a algoritmů, které jsou zaměřeny na identifikace obličeje člověka v obraze. Samotné rozdělení metod je možné podle více kritérií, ať se již jedná o formu zpracování obrazu ve 2D či 3D anebo dle způsobu snímání, kde rozlišujeme čelní pohledy, pohledy z boku nebo obecné pohledy. V následujících podkapitolách budou stručně popsány vybrané metody a algoritmy pro detekci obličeje. Na základě matematických způsobů modelování tváře může být detekce a lokalizace tváře rozdělena na statisticky orientované metody a znalostní metody. V praxi se používají různé kombinace metod pro co nejpřesnější detekci a lokalizaci obličeje. (25)

2.4.1 Metoda podprostoru

Cílem této metody je nalézt v obraze tváře obecné, a při tom markantní charakteristiky (ústa, nos, uši atd.) typické pro lidskou tvář. Jestliže tyto charakteristiky v obraze nalezneme, můžeme konstatovat, že na vyhodnocovaném snímku je obličeje. Každý obraz tváře je považován za vícerozměrný vektor a každý obrazový pixel odpovídá určité obrazové komponentě. Jestliže všechny charakteristiky tváře leží v stejném podprostoru více rozměrového prostoru, znamená to, že je tento podprostor dobrou reprezentací tváře, protože obsahuje společné rysy tváře. Detekce je pak detekcí podprostoru, v níž se tvář nalézá. V praxi a odborné literatuře se setkáváme s pojmem normalizovaný obraz tváře neboli eigenface [2]. Při normalizaci dochází k úpravám snímku v podobě změny měřítka, nalezení speciálních bodů na obličeji nebo určení prostorové orientace. Eigenface probíhá i na úrovni barevné škály, kdy dochází k úpravě obrazu do šedých odstínů nejen celého snímku, ale i určitých částí obličeje. Normalizované obrazce mají přibližně stejnou velikost i prostorovou orientaci a dochází k jejich efektivnějšímu porovnávání s dalšími obrazy. (25)

[2] Eigen – z německého „vlastní“

Obrázek 8 – Normalizované obrazce (26)

2.4.2 Metoda neuronových sítí

Detekce tváří pomocí neuronových sítí je považována za klasifikační problém o dvou třídách: první třídu tvoří obrazy tváře a druhá třída jsou obrazy, které naopak nejsou obrazy lidské tváře. Základním úkolem je pak naučit aplikace bezchybně rozpoznávat obrazy obou tříd. K tomu se připravují speciální vzorové knihovny s obrazy obou tříd. Pro neuronové sítě je poměrně těžké rozpoznávat obrazy druhé třídy, protože obrazů, jež nepředstavují podobu tváře, je obrovské množství. Detekce tváře pak záleží na kvalitě schopnosti rozeznávat právě obrazy druhé třídy. Z uvedeného vyplývá, že metoda neuronových sítí používaná pro detekci a rozpoznávání tváře v obraze má svá slabá místa. Vedou se proto intenzivní výzkumné práce jak metodu neuronových sítí efektivně doplnit o další metody, eliminující právě uvedené nedostatky. (25)

2.4.3 Metody založená na rozložení odstínů šedi v obraze

U tváří jednotlivých osob existují velké rozdíly mezi jejich vzhledy, ale i přesto lze určit obecná pravidla o distribuci odstínů šedé barvy v obraze za normálních světelných podmínek. I když dva jedinci mají rozdílný vzhled, tak lze konstatovat, že oblast očí je vždy tmavší než třeba oblast čela. Mezi nejznámější metody z této kategorie můžeme uvést metodu mozaiky, která vychází z přirozeného rozpoznávání tváří lidským mozkem. Výhodou metody mozaika je fakt, že dokáže na snímku detekovat malý nebo nevýrazný

obličej. Princip metody vychází z rozdělení oblastí do obrazových bloků ve čtvercové síti 4x4, přičemž v těchto blocích budou ležet oči, ústa, nos a líce atd. Jestliže se ve zpracovávaném obraze bude nacházet lidská tvář, pak právě v obrazových blocích nalezneme identifikující markanty (oči, ústa, nos, líce apod.), které vyhovují pravidlům distribuce odstínů šedé barvy. Postupně se vybírají jednotlivé obrazové bloky a zkoumá se, zda se v nich nalézají hledané markanty. Části, které zájmové markanty nemají, se vyřazují z dalšího zpracování. Obrazové bloky, které obsahují hledané markanty, se znovu rozdělí do sítě ještě detailnějších obrazových bloků (8x8). Pomocí metody detekce hran se definitivně určuje pozice očí, úst, nosu a líce. Metoda má několik možných variant dělení obrazových bloků s cílem zvýšit efektivitu zpracování obrazu. Snímky lidských tváří nejsou vždy pořizovány za konstantního osvětlení, ovlivňují je vrhané stíny samotnou distribucí odstínu šedé barvy. Obrazové bloky se pak zpracovávají pomocí adaptivního přizpůsobování. Zpracování touto metodou je pomalé a kombinuje se s dalšími metodami, aby výsledná kvalita byla co nejvyšší a zároveň doba zpracování co nejkratší. (27) (28)

2.4.4 Rozpoznávání obličejových obrysů

Obrys tváře neboli kontura je důležitou charakteristikou obličeje. Pokud se podaří korektně a přesně definovat obrys tváře, pak další detekce tváře je podstatně jednoduší. Často si však jistota správné detekce hrany tváře není příliš vysoká. Důvodem je fakt, že současné algoritmy na detekci hran mají svá omezení. Přesto však lze obrysů obličeje efektivně využít v kombinaci s dalšími přístupy. Detekce kontur lze využít k nalezení jednotlivých objektů v tváři, jako jsou oči, nos, ústa atd., jež jsou vstupními charakteristikami pro další metody, používané v procesu identifikace nebo verifikace tváře. Obrysy, kontury, hrany objektů lze obecně nalézt pomocí prahování, detekce hran, segmentace narůstáním oblastí, segmentací srovnání se vzorem apod. (25)

2.4.5 Metoda založená na informaci o barvách

Každý člověk má barvu svého obličeje různou, ale i tak lze definovat určité zásady, které diferencují obličej od barevně odlišného prostředí, což je základní myšlenka detekce a lokalizace obličeje na scéně. Rozložení barev v obličeji lidí stejné rasy je velice podobné a lze zde obecně najít typické oblasti s určitou barvou. Pro oblast očních důlků je typická barva stínů, zatímco nos je jinak barevně výrazný a ohraničený stíny. Pomocí barev lze tedy efektivně detekovat tvář na scéně. Při dobrých světelných podmínkách lze barvy dobře rozeznávat pomocí poměrně jednoduchých algoritmů. Problémy vznikají při velice jasném

nebo naopak temném osvětlení, při různých úhlech dopadajícího světla na tvář. V těchto podmínkách je těžké rozlišit různé barvy a to dokonce i tehdy, kdy se barvy lidských tváří výrazně od sebe liší. (25)

2.5 Rozpoznávání tváře

Rozpoznávání obličeje je proces, při kterém se na základě vstupních dat hledá identita osoby v databázi. Po načtení vstupních dat a předzpracování obrazu (oříznutí a normalizace) dojde k extrakci příznaků, což znamená extrahování vektoru pomocí zvoleného deskriptoru. Následuje přiřazení identity zvoleným klasifikátorem a vyhodnocení úspěšnosti.

2.5.1 Analýza hlavních částí - Principal Component Analysis

Algoritmus byl popsán v roce 1991 a stal se základem pro další metody rozpoznávání obličeje nebo se používá v kombinaci s jinými algoritmy. Jedná se o statistickou metodu prezentace lidské tváře v lineární transformaci (Karhunen - Loève Transform) nebo průměrné tváře. Snímky jsou uloženy v databázi v podobě biometrické informace. Následně dochází k zprůměrování snímku a k převodu na eigenface. Eigenfaces využívají markantní charakteristiky lidského obličeje, které jsou důležité pro počítačové rozpoznání. V procesu rozpoznání tváře se zjišťují odchylky vektorů původního obrázku od eigenfaces, což urychluje proces rozpoznávání. Pro zrychlení procesu rozpoznávání obličeje se neukládá celý obrázek, ale pouze číselná hodnota. (29) (30)

2.5.2 Lineární diskriminační analýza - Linear Discriminant Analysis

Metoda pracuje na principu vektorové oblasti, přičemž rozděluje jednotlivé body obrazce do jedné nebo více skupin. Toto členění probíhá na základě diskriminačních funkcí. Vzniklé skupiny obličejů se od sebe musí maximálně odlišovat, ale obličeje, které jsou součástí dané skupiny si maximálně podobné. Fisherova lineární diskriminační funkce je jedna z nejznámějších a nejpřesnějších lineárních metod, jenž pracuje s osobitými znaky skupin, z kterých pomocí různých statistik vyčlení obrazy do určených tříd. (29) (31)

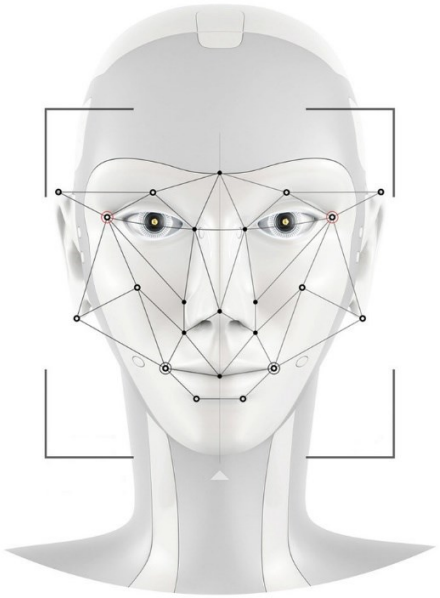
2.5.3 Rozpoznávání založené na geometrických tvarech a identifikačních markantech

Metoda vychází z definování geometrických a vizuálních charakteristik, které jsou určeny člověkem. Mezi základní identifikační markanty patří oči, nos, ústa a brada, protože tyto části obličeje vytváří konkrétní podobu lidské tváře a zároveň slouží i ke klasifikaci tváří.

Jedná se o charakteristiky určené vzdálenostmi a úhly mezi identifikačními markanty. Pracuje se s dvanácti základními antropologickými body a to:

- vnitřní koutky oka
- vnější koutky oka
- vnější horizontální body rtů
- bod přechodu nosu v čelo
- bod spodní hrany nosu – špičky
- body na chrupavce ucha
- body přechodu ušního lalůčku do tváře

Metody, které jsou založené na automatizovaném zpracování antropologických bodů, se často doplňují o další metody, protože se identifikační markanty se těžko vyhledávají v obrazech nízké kvality, nízkého rozlišení nebo při špatných světelných podmínkách. (27)



Obrázek 9 – Markanty obličeje (32)

2.5.4 Metoda optických toků

V případě, že je k dispozici sekvence snímků pohybu hlavy jedné osoby a je provedena detailní analýza dvojice snímků, jdoucích po sobě, je zřetelné, že dochází k dynamickým změnám. Mění se světelná intenzita mezi odpovídajícími body ve snímcích a zároveň dochází k prostorovému pohybu těchto bodů. Každý bod má svůj směr pohybu. Za určitou časovou jednotku navíc urazí určitou dráhu. Odpovídající si body mají i svou rychlost. Jedná se o změny intenzity a změny prostorové. Mezi dvěma snímky lze pak definovat rozdíly,

vyjádřené pomocí optického toku a ty využívat pro rozpoznávání pohybu a rovněž pro rozpoznávání tváře. Každá tvář má své specifické rozmístění bodů, které ji charakterizují. Optický tok tak určuje charakter i výraz tváře. Metoda optického toku je typicky využívána v úlohách rozpoznávání emocí, jejichž automatizované zpracovávání se již využívá v praxi. (25)

2.5.5 Neuronové sítě

Metody neuronových sítí, používané pro rozpoznání lidských tváří, lze rozdělit do dvou základních kategorií. V první kategorii jsou identifikační charakteristiky rozpoznávány nejrůznějšími metodami, a metoda neuronových sítí je použita pouze pro konečné rozpoznání tváří. Ve druhé kategorii metody neuronových sítí slouží pro jak určování jednotlivých identifikačních charakteristik, tak i pro závěrečné rozpoznávání. V minulosti bylo nejdříve charakterizováno 50 základních komponentů tváře, které se zobrazovaly do pětirozměrného prostoru s autokorelační neuronovou sítí. Ve druhém rozhodovacím procesu se používaly vícevrstvé rozhodovací mechanismy. Další možností je smíšená neuronová síť, která vyhodnocuje jednotlivé identifikační markanty a následně v nadřazené neuronové síti dochází ke klasifikaci tváří a určují se identifikačně-verifikační výstupy. (25)

Nejpodstatnější a nejzákladnější vlastností neuronových sítí je jejich učení. V trénování neuronové sítě je rozdíl mezi běžným využitím počítačů a využitím systémů, které pracují na principu neuronových sítí. Algoritmy uživatelských programů transformují množinu vstupních dat do množiny výstupních dat, tak jak je popsáno v kapitolách výše. U neuronových sítí však není potřebná algoritmizace řešení, ale je důležitá trénovací množina neuronových sítí a její následné učení za použití vzorců popisující řešení problematiky. (33)

2.5.6 Rozpoznávání obličeje na základě 3D snímků

Vnímání okolního světa v trojrozměrném prostoru poskytuje více informací, než vnímání prostoru v dvourozměrném prostoru. 3D možnost přináší větší možnosti rozpoznávání osob a to díky získání prostorového modelu lidského obličeje. Samotné získání 3D obrazu je však složitější než získání informací z dvourozměrného prostoru. Kamery používané v bezpečnostních oblastech i fotoaparáty získávají data v 2D prostoru a rovněž počítačové zpracování vstupního signálu je přizpůsobeno pro dvourozměrný prostor. Jednotlivé metody získávání informací z prostoru jsou však rozdílné, ale v posledních letech dochází k sjednocování těchto metod a postupů.

K získání 3D snímku se využívá snímací zařízení v podobě 2,5D skeneru. Rozdíl oproti 2D obrazu je v tom, že o snímaném bodu je navíc uchovávaná informace o jeho hloubce. Tímto způsobem jsou reprezentována data, ale tyto data nemohou být považována za 3D model, jelikož tímto způsobem nemohou být reprezentovány body, které leží na stejných souřadnicích, ale i v jiné hloubce. Většina zařízení, které tvoří 2,5D skener využívají ke své činnosti strukturovaně viditelné nebo infračervené světlo. Promítnutím jistého vzoru na 3D povrch a jeho snímání pod jiným úhlem vede k dostatečné tvorbě 2,5D obrazce. V případě, že některá místa nejsou vidět (z důvodu zákrytu), bude model v těchto místech obsahovat díry. Většinou bývá pořízeno více skenů z různých míst a ty se poté skládají do plného 3D modelu. Nasnímaná data lze reprezentovat například v podobě mraku bodů jako polygonální síť nebo hloubkovou mapu. (27)

Podobně jako u 2D snímků je nutné i 3D snímků získané obrazce normalizovat. Normalizace probíhá přes detekci klíčových bodů, jimiž jsou koutky očí a špička nosu. Pro detekci těchto bodů lze model transformovat do výchozí polohy, ve které lze předpokládat vysokou míru závislosti mezi dvěma modely stejného obličeje. Nejjednodušší je detekovat nos, protože se jedná o nejvíce vystouplou část obličeje směrem k snímacímu zařízení. Pro kompenzace hlavy je model rotován kolem os x a y, a jako nos je zvolen bod, který má souřadnice z v průměru nejnižší a tudíž se jedná o nejméně vzdálený bod. Další normalizace obrazu se provádí v oblasti hrubého zarovnání obličeje pomocí transformace trojice bodů v rovině. (27)

K porovnávání 3D obrazce s referenčním snímkem hledané osoby se například využívá metody podobnosti 3D modelů na základě algoritmu Iterative Closest Point. Algoritmus najde jemné zarovnání referenčního snímku a snímku hledané osoby a výsledná podobnost se pak určí na základě rozdílů tvarů zarovnaných 3D reprezentací (polygonálních sítí). Algoritmus nejprve vybere kontrolní body a poté iterativně transformuje testovací snímek proto to, aby všechny kontrolní body měly minimální vzdálenost od povrchu šablony. Tyto kontrolní body jsou vybírány v oblastech, kde dochází k malé změně u různých výrazů obličeje, ale tak, aby pokryly co možná největší plochu obličeje. Další možností metody jsou založené na tvaru a vzhledu obličeje nebo na podobnosti hloubkových map. (27)

2.6 Databáze a požadavky na snímky

Ve fázi rozpoznávání obličejů je kromě samotného získaného a normalizovaného snímku nutné mít k dispozici i databázi osob, ve které se budou osoby vyhledávat. Mezi základní

metody rozpoznání patří případ, kdy se ověřuje skutečnost, zda osoba, u které máme k dispozici aktuální snímek je ve skutečnosti osobou na snímku starém několik dnů, týdnů, měsíců nebo let. Typickým případem je situaci při letištní kontrole, kdy je nutné ověřit, že osoba, která se dostavila k pasové kontrole, je totožná s osobou uvedenou v cestovním pase nebo jiném cestovním dokladu. Takové porovnání se v odborné praxi označuje jako 1:1 (one-to-one). Dalším případem porovnání snímku je možnost konfrontovat aktuální snímek osoby s databází neurčitého počtu osob, přičemž výsledkem musí být informace, zda se osoba v databázi nachází či nikoliv. Pro příklad lze uvést situaci, kdy má přístup do uzavřené místnosti (objektu) několik desítek či stovek osob. Na vstupu do uzavřeného prostoru je instalována kamera, která snímá scénu a zasílá digitální snímky do záznamového zařízení. Následně je získaný snímek pomocí software porovnán s databází osob, které mají povolen vstup do uzavřeného prostoru. Po vyhodnocení porovnávacího procesu je určeno, zda se osoba na vstupu do uzavřeného prostoru v databázi oprávněných osob pro vstup nachází či nikoliv. O pozitivním nebo negativním nálezu osoby v databázi povolených osob je informován operátor, který postupuje dle stanovených postupů. Porovnání jedné osoby oproti databázi neurčitého počtu lidí se nazývá porovnáním 1:M (one-to-many). S případy, kdy je na snímané scéně velké množství osob (dav) a je nutné tyto osoby porovnat s databází se setkáváme poměrně často. Typickým případem může být vstup na fotbalový stadion, přičemž některé osoby mají na stadion zakázaný vstup a nesmějí se pohybovat ani v okolí stadionu. Pomocí kamerového systému lze monitorovat prostor kolem stadionu a na základě získaných snímků provádět dotazy do databáze, zda se nejedná o osoby, které by zde neměly být. Neoprávněných osob na snímané scéně muže být několik desítek, stejně tak i osob na „Black List“[3] v databázi může být velké množství. Pro takové porovnání se užívá označení M:M (many-to-many).

Pro efektivní měření výkonosti používaných rozpoznávacích algoritmů se v odborné literatuře a praxi užívají názvy False Match Rate a False Non Match Rate. False Match Rate (dále jen FMR) udává procento snímků, kdy došlo k nalezení osob v databázi, ale osoba ve skutečnosti v databázi nebyla. Přičemž False Non Match Rate (dále jen FNMR), je procento snímků, kde nedošlo k nalezení osoby v databázi, ale osoba v databázi byla. Z uvedených definic vyplývá, že ideální by bylo, kdyby byly obě hodnoty nulové.

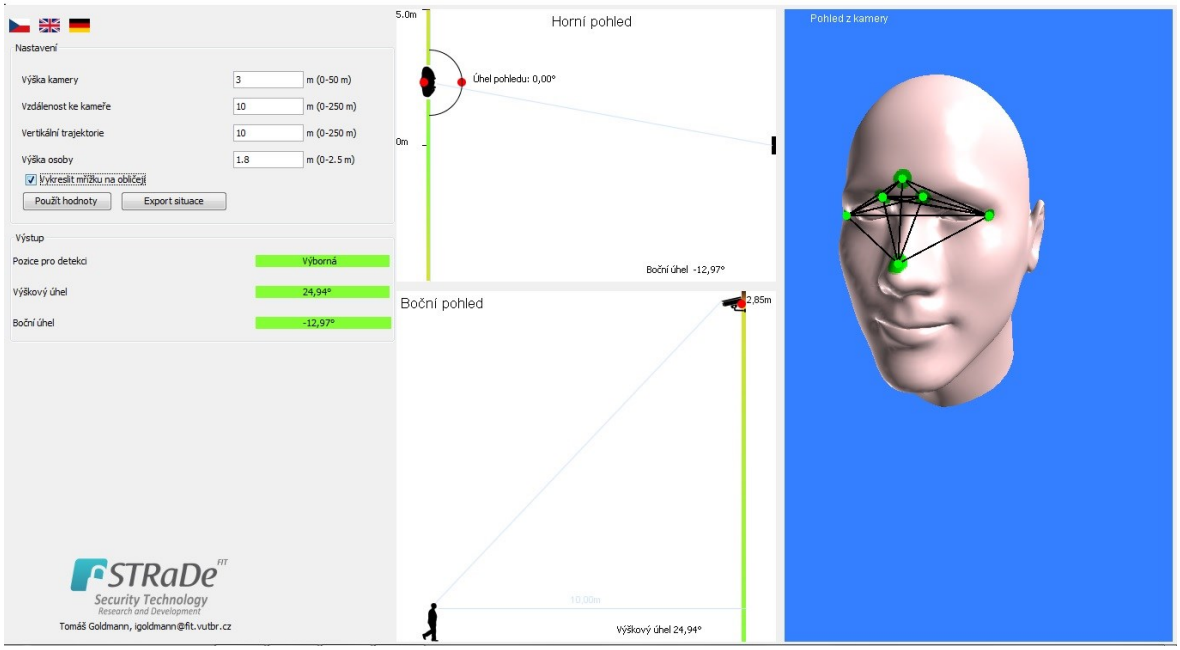
Výsledky Face Recognition závisí nejen na zvolených algoritmech, použitých databázích, ale i na kvalitě vstupních obrazců a rovněž i na kvalitě snímků, jež jsou uloženy v databázi,

[3] Black List – seznam nežádoucích osob

ve které se budou osoby vyhledávat. Pro všeobecné standardy týkající se biometrických informací je vydána mezinárodní norma ISO/IEC 19 794 Information Technology – Biometric data interchange formats. Norma ve své páté části klade požadavky i na fotografie, které mají být použity k rozpoznávání osob. V normě jsou rovněž klasifikovány požadavky na scénu (světelné podmínky), ve které je snímek pořízen, pozice snímajícího zařízení vůči snímané osobě nebo formát získaných vstupních dat. V rámci rozpoznávání obličeje jsou obecně za kvalitní snímky označovány Visa snímky (pasové fotografie) a takové snímky je vhodné využívat jako snímky referenční (uložené v databázi porovnávaných osob). Důležitá je rovněž kvalita snímku z pohledu jeho rozlišení a natočení obličeje. U jednotlivých výrobců softwarů pro Face Recognition se může požadavek na rozlišení lišit. Obecně lze konstatovat, že by snímek měl mít rozlišení minimálně 60 pixelů mezi očima osoby. Podobné je to i s natočením obličeje ve vertikální a horizontální poloze, přičemž natočení o více než 30 ° v horizontální a 15 ° ve vertikální rovině je označováno jako hraniční.

Obrázky určené k porovnání by měly splňovat požadavky na rozlišení a natočení obličeje i podmínky uvedené v normě ISO/IEC 19794, ale z praktického hlediska toto není možné vždy zajistit. Při některých situacích je možné snímanou scénu ovlivnit tak, abychom dosáhli co nejlepších vstupních dat pro další zpracování, ale ne vždy můžeme vytvořit bezpečnostní koridor nebo podobné opatření tak, abychom získali kvalitní vstupní data určená k porovnání.

Pro získání validních vstupních dat se často využívá kamerový systém za předpokladu, že kamerový systém bude disponovat kamerami s vyšším rozlišením. Instalační výška a úhel záběru rovněž ovlivňují výsledek snímání obličeje. Vysoké učení technické v Brně, Fakulta informačních technologií vyvinula aplikaci s názvem Head Viewer, pomocí které je možné určit výšku instalace a úhel záběru bezpečnostní kamery, přičemž je kladen důraz na co nejefektivnější detekci obličeje. V aplikaci je možné nastavit základní parametry kamery jako instalační výšku, vzdálenost osoby od kamery nebo výšku osoby. Po nastavení těchto kritérií je ihned k dispozici výstup, včetně hodnocení, zda je pozice bezpečnostní kamery pro detekci obličeje vhodná či nikoliv.



Obrázek 10 – Ukázka aplikace Head Viewer

II. PRAKTICKÁ ČÁST

3. SOFTWAROVÉ NÁSTOROJE PRO DETEKCI OSOB

Detekcí obličejů osob s následným porovnáváním v databázi osob se zabývají jednak samotní výrobci kamerových systémů, ale tato oblast je zajímavá i pro společnosti vyvíjející software. Tyto společnosti nabízejí své algoritmy jako software třetích stran, které běží na pozadí bezpečnostního systému a reagují pouze v případě přednastavených relací. Typickým případem je situace, kdy do prostoru vstupuje neautorizovaná osoba. Pomocí kamerového systému jsou získány snímky osoby, které jsou následně odeslány na server s nainstalovaným software pro Face Recognition, který provede porovnání a v případě, že je osoba umístněná na „Black List“, zašle tuto informaci operátorovi bezpečnostního systému. V současné době je na trhu dostupných několik desítek software, které jsou používány k Face Recognition (dále jen FR). Na obrázku 11 – Přehled výrobců software pro FR, jsou uvedeni vybraní představitelé tohoto segmentu.

P.č.	Název společnosti	Stát
1.	3Divi	USA
2.	Alchera	Jižní Korea
3.	AnyVision	Izrael
4.	Aware	USA
5.	Ayonix	Japonsko
6.	Camvi Technologies	USA
7.	Gemalto Cogent	Francie
8.	Cognitec Systems GmbH	Německo
9.	Dermalog	Německo
10.	Digital Barriers	Velká Británie
11.	Ever AI	USA
12.	Eyedea Recognition	Česká republika
13.	Glory Ltd	Japonsko
14.	Gorilla Technology	Čína
15.	Loginface Corp	Jižní Korea
16.	Hikvision Research Institute	Čína
17.	Idemia	Francie
18.	Imagus Technology Pty Ltd	Austrálie
19.	Incode Technologies	USA
20.	Innovatrics	Slovensko
21.	Alivia/Innovation Sys.	USA

P.č.	Název společnosti	Stát
22.	Megvii	Čína
23.	Microfocus	USA
24.	Microsoft Corporation	USA
25.	NEC Corporation	Japonsko
26.	Neurotechnology	Litva
27.	N-Tech Lab	Rusko
28.	Panasonic	Japonsko
29.	QuantaSoft	Česká republika
30.	Rank One Computing	USA
31.	Real Networks	USA
32.	Shenzhen Inst. Adv. Tech. CAS	Čína
33.	Smilart UG	Německo
34.	Tevian	Rusko
35.	TigerIT Americas LLC	USA
36.	TongYi Transportation Technology	Čína/Austrálie/VB
37.	Visidon	Finsko
38.	Vigilant Solutions	USA
39.	VisionLabs	Rusko
40.	Vocord	Rusko
41.	Zhuhai Yisheng Electronics Tech.	Čína

Obrázek 11- Přehled výrobců software pro FR

Rozhodně není pro budoucího uživatele jednoduché vybrat ten nejvhodnější software pro konkrétní aplikace. Samotní výrobci deklarují určité parametry svých algoritmů, jako jsou například FNMR, FMR, doba odezvy, určování pohlaví či věku, ale spolehlivost a přesnost udávaných výsledků je pro standardního zákazníka těžko ověřitelná. Za uznávanou mezinárodní autoritu, která se zabývá mimo jiné i testováním software pro FR, je National

Institute of Standards and Technology (dále jen NIST) sídlící ve Spojených státech amerických. Pro výrobce je možnost testování jejich produktů dobrovolná a není zavazující, avšak v odborných kruzích je testování u NIST vyžadováno a je garancí deklarovaných parametrů software. Zaměření jednotlivých testovacích scénářů pro testování software pro FR v laboratořích NIST jsou různá.

V roce 2014 proběhlo testování jednotlivých algoritmů se zaměřením na identifikaci osob označováno jako 1:M (one-to-many). Na obrázku 12 je seznam šestnácti dodavatelských nebo vývojových společností, které do testu dodaly celkem čtyřicet tři algoritmů pro FR.

Provider Name	Letter Code
3M/Cogent	A
Cognitec	B
Neurotechnology	C
Safran Morpho	D
NEC	E
Tsinghua University (EE - Prof. Wen)	F
Beijing Ivsign Technology Co. Ltd.	G
Chinese Academy of Sci. - Inst. Automation (Prof. Liu)	H
Chinese Academy of Sci - Inst. Computing Technology (Prof. Shan)	I
Toshiba Corporation	J
Tsinghua University (EE - Prof. Su)	L
HP / Virage	M
Zhuhai Yisheng Electronics Tech. Co. Ltd.	P
JunYu Technology Co. Ltd.	Q
Decatur Industries Inc.	S
Ayonix Inc. (JP)	T

Obrázek 12 – Dodavatelé testovaných algoritmů v roce 2014 (34)

Do výchozí databáze pro porovnání referenčních snímků bylo umístěno 1,6 milionu individuálních fotografií. Jako snímky určené k porovnání byly využity fotografie označovány jako Mugshots (fotografie z policejních databází pořízené při zadržení osob). Tyto fotografie byly v rozlišení 480 x 600 pixelů ve formátu JPEG. Dále bylo využito snímků z webových kamer v rozlišení 240 x 240 pixelů a fotografií označovaných jako VISA (pasové fotografie) s rozlišením 480 x 640 pixelů. Většina programů při porovnání výchozí fotografie oproti výchozí databázi určuje pořadí shody hledané fotografie oproti výchozí databázi. V případě, že hledaná fotografie je přiřazena na první místo, znamená to, že je nejvhodnějším kandidátem na shodu. Jelikož při testování NIST bylo známo, jaká osoba má být ve výchozí databázi nalezena, bylo bráno v potaz, na kterém místě (pořadí) bude hledaná osoba na fotografii zařazena. Nejlépe byla hodnocena situace, kdy hledaná osoba ve výchozí databázi byla první v pořadí, a nejhorší hodnocení bylo uděleno za padesáté pořadí. Při porovnání snímků z webových kamer, Visa fotografií a oproti

fotografiím s označením Mugshots dosáhly nejlepších výsledků algoritmy od společností NEC, Toshiba a Safran Morpho. Výsledky z těchto testů jsou uveřejněny na webových stránkách NIST pod označení NIST Interagency Report 8009. (34)

V dubnu roku 2015 byla pod označením NIST Interagency Report 8052 uveřejněna zpráva o výsledcích dalšího testování. Testování bylo zaměřeno na ověření spolehlivosti při určování, zda se jedná o muže či ženu, určení věku a etnického původu. Stanovení uvedených parametrů je zajímavé pro obchodní problematiku zejména z pohledu cíleného marketingu. Testování probíhalo v období od června 2012 do října 2013 a zúčastnilo se jej pouze šest výrobců (Cognitec, Neurotechnology, NEC Corporation, Tsingua Univerzity, Mitre a Zhuhai-Yisheng), kteří představili celkem třináct algoritmů. První část testu byla zaměřena na určení pohlaví z pasových fotografií, naskenovaných fotografií nebo skupinových digitálních fotografií. Celkem bylo testováno 951 766 obrazů, přičemž mužů na fotografiích bylo 472 762 a fotografií žen 479 004. Při určování mužů na fotografii byl dosažen nejlepší výsledek s hodnotou 97,9 % správného určení, u žen bylo nejlepší skóre 95,6 %. Naopak nejhorší výsledky dosáhl algoritmus s hodnotou 89,5% u mužů a 81,9% u žen. Dalším testem bylo určení rozsahu věku osob na fotografiích. Na obrázku 13 je tabulka, ve které je v prvním sloupci věkový rozsah testovaných osob, ve druhém sloupci je počet testovaných fotografií u žen, třetí sloupec se týká počtu fotografií u mužů. Následující sloupce jsou výsledky jednotlivých algoritmů, první číslo je procentuální vyjádření shody u žen a za lomítkem je procentuální vyjádření míry shody u mužů. Z tabluky je patrné, že největší problém pro určování věku osob na snímcích je u malých dětí ve věku 0 - 10 let a u lidí ve věku 81 – 90 let. Hodnoty u osob středního věku dosahují úspěšnosti přes 90 %.

Age Range	# Females	# Males	B30D	B31D	C30D	E30D	E31D	E32D	F30D	K10D	P30D
0–10	11141	11442	77.0 | 82.8	77.1 | 82.6	90.2 | 20.3	68.1 | 72.9	68.5 | 74.1	68.0 | 72.1	78.0 | 34.0	87.8 | 25.3	93.6 | 16.3
11–20	11067	10859	92.9 | 92.2	93.7 | 91.3	97.5 | 74.0	94.2 | 90.2	92.5 | 91.9	94.7 | 90.7	88.3 | 72.2	91.3 | 75.4	91.4 | 81.9
21–30	32966	36786	97.3 | 97.9	97.5 | 97.9	98.5 | 93.5	96.4 | 98.3	95.1 | 98.7	97.3 | 98.7	92.2 | 79.4	90.8 | 93.2	94.6 | 95.9
31–40	21848	27185	96.0 | 99.0	96.0 | 99.1	97.9 | 94.4	95.0 | 98.7	93.5 | 98.9	97.0 | 98.9	90.9 | 80.5	87.0 | 95.1	92.6 | 96.9
41–50	16330	18145	92.2 | 99.4	92.5 | 99.5	95.8 | 94.3	92.0 | 98.9	90.0 | 98.9	96.4 | 98.8	88.5 | 78.9	82.8 | 95.4	87.2 | 97.3
51–60	14376	12185	84.4 | 99.5	85.4 | 99.6	92.4 | 93.7	87.4 | 98.9	85.0 | 98.8	94.7 | 98.4	84.9 | 78.2	77.9 | 95.0	78.6 | 97.8
61–70	7320	5960	74.4 | 99.4	75.1 | 99.5	86.4 | 93.1	79.7 | 98.5	78.2 | 98.3	90.7 | 97.4	77.7 | 78.9	67.7 | 94.5	66.4 | 97.6
71–80	2579	1960	59.3 | 99.5	59.9 | 99.4	73.2 | 92.2	67.4 | 97.1	68.3 | 97.1	84.1 | 97.0	64.7 | 79.3	55.6 | 93.6	53.8 | 95.3
81–90	457	355	49.2 | 97.6	49.7 | 97.9	61.3 | 91.7	66.1 | 94.8	64.7 | 95.5	82.5 | 92.0	53.3 | 81.7	48.1 | 90.6	47.0 | 93.5

Obrázek 13 - Úspěšnost testovacích algoritmů dle rozsahu věku (35)

Určování etnického původu bylo dalším testem. Bylo testováno přibližně 1800 snímků osob ve věku 11 - 40 let, přičemž úkolem bylo určit jakého etnického původu osoba je. Zajímavostí je, že nejvíce algoritmů dosáhlo svých nejlepších výsledků u indického etnika,

zatímco u argentického, japonského a tchainwanského etnika měly algoritmy nejnižší shodu. Výsledky jednotlivých algoritmů jsou uvedeny na obrázku 14. (35)

	ARG	BRZL	CHIN	COL	DF	IND	ISRL	JPN	KOR	PERU	PHIL	POL	RUS	TWAN
B30D	95.0	97.7	96.4	96.4	99.0	97.2	97.8	90.0	94.4	97.2	97.9	98.1	97.6	94.1
B31D	95.3	97.8	96.7	96.7	99.0	97.7	98.0	90.1	94.3	97.6	98.1	98.2	97.7	94.0
C30D	93.3	95.0	89.2	94.6	96.7	98.1	96.4	82.9	83.6	95.4	92.8	97.3	96.8	81.5
E30D	91.2	96.6	96.4	95.0	97.2	97.8	96.6	95.1	95.6	96.8	97.7	97.5	96.9	96.1
E31D	89.8	97.0	94.4	94.7	96.1	96.9	95.8	96.7	94.9	96.9	97.6	97.7	96.6	96.8
E32D	93.9	97.2	96.6	95.5	97.6	98.4	97.3	95.8	95.8	97.5	98.0	98.1	97.6	97.1
F30D	80.9	86.4	80.8	86.2	83.6	82.5	87.1	84.3	81.7	86.2	78.6	89.8	87.8	76.1
K10D	86.8	91.2	89.6	87.0	88.1	94.6	94.5	85.5	86.0	90.1	90.9	92.6	91.4	88.4
P30D	90.8	95.0	93.2	93.8	96.1	96.0	95.3	89.2	90.5	95.0	95.3	94.5	94.8	88.9

Obrázek 14 – Testování etnického původu osob (35)

V listopadu roku 2018 pod označením NIST Interagency Report 8238 byly zveřejněny výsledky opakovaného testování zaměřené na rozpoznávání tváří s následnou identifikací. Jedná se o navazující test, který NIST uveřejnil pod označením NIST IR 8009 v roce 2014. Do testování bylo zahrnuto celkem 127 algoritmů od 39 komerčních vývojových společností a jedné univerzity. Byla vytvořena databáze, která obsahovala 30,2 milionů fotografií s 14,4 miliony osob, což bylo největší nezávislé a veřejné hodnocení uvedených algoritmů. Testování bylo zaměřeno na rychlost odezvy vloženého snímku oproti výchozí databázi, přesnost identifikace, ale i na rozpoznávání dvojčat. Pro samotné testování byly použity opět fotografie typu Mugshots ve stejném rozlišení jako v roce 2014, fotografie z webové kamery nižší kvality, fotografie pořízené video sekvencí a fotografie z „běžného života“ jak je ukázáno na obrázku 15.

Samotné scénáře a hodnocení testování algoritmů bylo stejné jako v roce 2014. Výsledky zahrnují i informace, jak si testované algoritmy vedly v porovnání s nejlepšími výsledky z roku 2014, čili zda dochází ke zkvalitnění vyvíjených algoritmů. Tady lze konstatovat, že výsledky z roku 2018 ukazují na stoupající výkonnost napříč všemi vývojovými společnostmi. Nejlepších výsledků v testování, dle NIST, dosáhly algoritmy od americké společnosti Microsoft Corporation, čínské Shanghai Yitu Technology a univerzitního algoritmu od Shenzhen Institutes of Advanced Technology Chine Academy of Sciences.

Obrázek 15 – Ukázka testovací sady fotografií (36)

Nejúspěšnější algoritmy z roku 2014 a to od společnosti NEC Corporation se se svými algoritmy umístily v první čtvrtině celkového pořadí. Společnost Safran Morpho se stala obchodní akvizicí pro společnost Idemia a její algoritmy se nacházely v celkovém pořadí do čtyřicátého místa. Výrobce software Toshiba se testování v roce 2018 nezúčastnil. Česká vývojová společnost Eyedea Recognition se se svými algoritmy v celkovém pořadí pohybovala okolo osmdesátého místa. O něco lépe dopadly slovenské algoritmy od společnosti Innovatrics, které obsadily pozice v přibližně polovině všech algoritmů. (36)

4. DETEKCE OSOB JAKO SOUČÁST KAMEROVÉHO SYSTÉMU

Společnost Panasonic Corporation se zabývá detekcí osob již od roku 1990. Nejdříve byl systém používán k rozpoznání registračních značek a v zábavném průmyslu. Postupně docházelo k vývoji jednotlivých algoritmů na takovou úroveň, že došlo k vzniku vlastního software určeného pro bezpečnostní průmysl. Produkt standardně detekuje obličeje, porovnává s jinými snímky, ganderově rozděluje osoby a určuje věk osob s tolerancí 10 let. Software s názvem FacePro je využíván na japonském mezinárodním letišti Narita International Airport.

Výrobcem je doporučeno, aby k snímání scény byly použity kamery Panasonic edice I-Pro Extreme s objektivy od společnosti Fujinon nebo Tamron. Důvodem doporučení je vzájemná kompatibilita jednotlivých prvků systémů a taky skutečnost, že kamery z uvedené edice provádějí základní zpracování již přímo na úrovni kamery. Následně je po datové infrastruktuře (šifrovaně) posílán jen nejlepší referenční snímek spolu s výsledky vypočítaného algoritmu, přičemž velikost takového balíčku nepřekročí desítky kb. Taková komprimace dat, spolu s vysokým výpočetním výkonem grafické karty serveru, umožňuje, porovnat za jednu sekundu třicet tisíc snímků.

Základní požadavky na hardware a software serveru:

CPU - Intel®, Xeon ® nebo CoreTM i7 series 3,40 GHz a vyšší řady

Paměť – 32 GB a více

Harddisk – 1 TB a více

Grafická karta – NVIDIA® QUADRO® P5000

Napájecí zdroj - 550 W a více

Operační systém - Microsoft® Windows® 10 Profesional RS4 (64 bit) nebo Microsoft Server® 2016 Standard Edition

Získané snímky je možné použít pro porovnání v relaci 1:1 nebo 1:M. Samozřejmostí je vytváření „Black List“ [4] seznamů, přičemž v základní variantě je možné do takového seznamu uložit až 10.000 snímků, rozšířená varianta umožňuje vložit na „Black List“ až 30.000 snímků. Velikost databáze získaných snímků není téměř omezena a může obsahovat miliony fotografií. Do FacePro je možné vkládat vlastní referenční snímky získané z jiných zdrojů nebo lze vytvořit referenční fotografii přímo systémem.

[4] Black List – seznam nežádoucích osob

Výrobce deklaruje spolehlivost produktu testováním v rámci National Institute of Standards and Technology (duben 2017). Výsledky hodnoty FNMR a FMR měly dosahovat téměř ideálních hodnot.

Pro správnou detekci osob a následné porovnání v databázích je nutné dodržet některé podmínky a to zejména výška instalované kamery. Tato výška by se měla pohybovat v rozmezí 2 – 2,5 metru. Snímaný prostor by měl mít neměnné světelné podmínky a měla by být vytvořena spolupracující scéna. Je doporučeno, aby se osoba pohybovala ve scenérii v přímém směru proti kameře nejméně 4 sekundy a bylo zachováno to, že obličej nebude otočen k vertikální ose o více než 30 ° a horizontálně o 45 °. Dále je možné detekovat i osoby se slunečními brýlemi a na konci roku 2018 již měl být systém na takové úrovni, že dokáže správně vyhodnotit i osoby s rouškou či šátkem přes obličej.

Obrázek 16 - Detekční možnosti osob (37)

Při praktické ukázce bylo ke snímání scény využito IP kamery Panasonic typ WV-S-1131 s čipem 1/2.8 MOS a 60 snímky za sekundu. Objektiv Fujinon YV 3.3 x 15SA-SA2 s focusem 8 – 50 mm byl zaostřen do vzdálenosti přibližně 6 metrů. Kamera byla umístěna na stativu v instalační výšce dvou metrů. Pomocí datového kabelu CAT 5e byla kamera napájena přes switch značky Zyxel s PoE. Switch byl následně připojen do serveru, který měl požadovanou specifikaci (viz výše).

Samotné testování probíhalo v prostorách administrativní budovy v ideálních klimatických a světelných podmínkách. Test byl zaměřen na ověření deklarovaných funkcionalit, zejména samotné detekce obličeje a vyhodnocení oproti databázi. Obslužný program měl vyvolat poplachovou událost v případě výskytu osoby z „Black List“. Jako referenční snímek pro „Black List“ byla použita pasová fotografie pořízena před přibližně pěti lety. Fotografie byla následně ještě vyfocena pomocí mobilního telefonu a až poté byla exportována jako

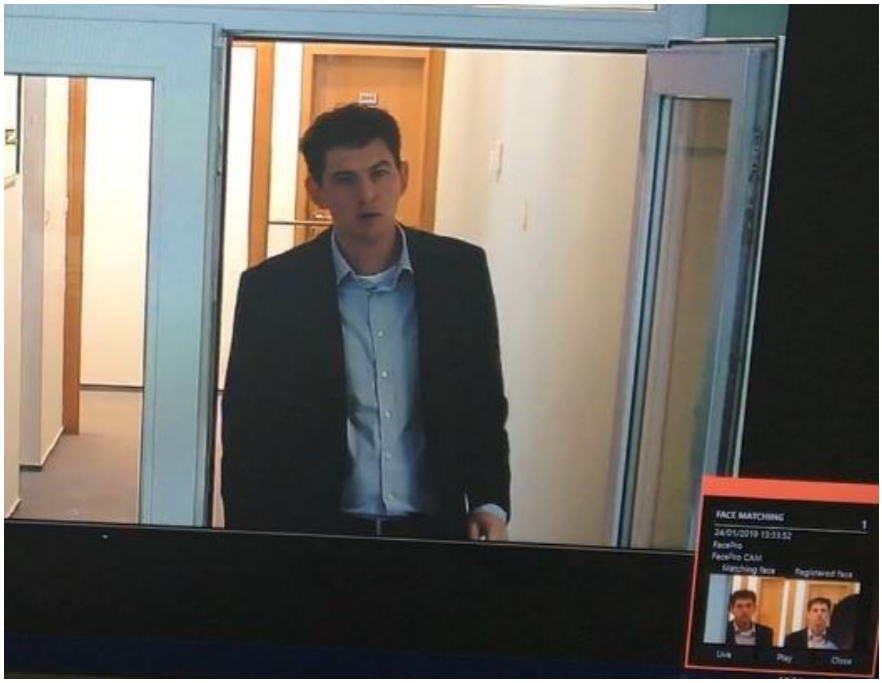
referenční snímek do databáze. Druhý referenční snímek osoby byl pořízen samotným kamerovým systém.

Obrázek 17 – Referenční foto – vlevo pasová, vpravo pořízená systémem

První test proběhl ve vzdálenosti přibližně 9 metrů s cílem identifikovat spolupracující osobu, která se bude přirozeně pohybovat směrem ke kameře. Na obrázku 18 – Detekce obličeje na 9 metrech je patrné, že systém detekoval obličej okamžitě, jakmile se osoba objevila v záběru. Tato skutečnost je signalizována modrým rámečkem. Zajímavostí je, že detekce obličeje proběhla přes skleněnou výplň dveří.

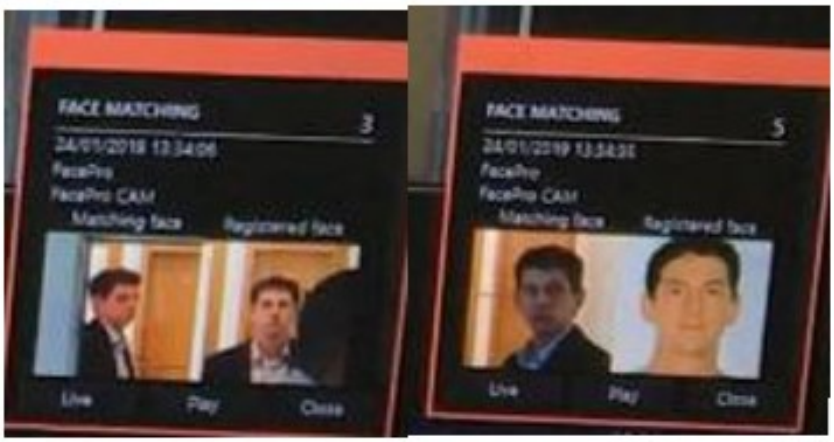
Obrázek 18 – Detekce obličeje na 9 metrech

K vyhodnocení hledané osoby, včetně znázornění poplachové informace, dochází přibližně po dvou sekundách od detekce obličeje, což může být zapříčiněno uzavřenou částí dveří a ke krátké ztrátě osoby ze záběru. Na obrázku 19 - Vizualizace hledané osoby je vidět snímaná scéna a vizualizace poplachové události. Za povšimnutí stojí fakt, že jako referenční snímek byl vybrán snímek, který pořídil samotný systém.



Obrázek 19 – Vizualizace hledané osoby

Další test byl zaměřen na schopnost systému detekovat obličej a porovnávat osobu, která je k objektivu kamery pootočena o 45 °. K testování bylo využito dvou vzdáleností a to šest a devět metrů. Lze konstatovat, že v obou vzdálenost dokáže systém obličej detekovat i z profilu, což bylo deklarováno výrobcem.



Obrázek 20 - Identifikace pod úhlem 45 ° na 6 a 9 metrech

Následný test byl zaměřen na osobu, která má nasazeny běžně používané sluneční brýle. Všechny parametry testu zůstaly stejné jako při předchozím testování. Systém dokázal detekovat obličej přibližně na sedmi metrech, ale ani při pokračující chůzi směrem k objektivu nedokázal software přiřadit k osobě porovnávanou osobu. Průchodových testů proběhlo více a s různými osobami, ale nepodařilo se spolehlivost této funkcionality ověřit.

Obrázek 21 - Detekce obličeje v brýlích

Poslední testovanou funkcionalitou byla detekce obličeje s následným porovnáním v databázi u osoby, která má částečně obličej zakrytý šátkem či rouškou. Všechny parametry testu zůstaly stejné jako při předchozím testování. Jelikož výrobce deklaroval tuto funkci uvést do distribuce až na konci roku 2018, nebylo jisté, zda bude funkcionalita již zakomponována do aktuálně používané verze FacePro (testování proběhlo v lednu 2019).

Obrázek 22 - Detekce osoby s šátkem

U tohoto testu se ukázalo, že pro detekci obličeje je stěžejní částí v obraze oblast nosu. Při prvním testu byl šátek přetažen i přes nos a nedošlo k detekci obličeje ani ve vzdálenosti tří metrů. V druhém testu byl šátek nasazen tak, aby nezakrýval nos a k detekci obličeje došlo přibližně na šesti metrech. V obou případech však nedošlo k porovnání zaznamenané osoby s osobou na „Black List“.

Ve výše popsaném se jednalo jen o základní testování deklarovaných funkcionalit systému a vzhledem k časovým, hardwarovým a licenčním možnostem výrobce nebylo možné udělat důkladnější testování a objektivně posoudit spolehlivost systému.

5. TESTOVÁNÍ SOFTWARE PRO FACE RECOGNITION

5.1 Testování jednotlivých software

Pro samotné uživatelské testování byly vybrány software od japonské společnosti NEC Corporation a izraelské společnosti AnyVision.

Společnost NEC Corporation vznikla již v roce 1899 a od začátku své činnosti se věnovala oblasti telekomunikací, následně vývojem osobních počítačů a v poslední období rovněž vývojem algoritmů pro detekci obličejů a rozpoznáváním osob. Její produkt Neo Face Watch je využíván na mezinárodním letišti Václava Havla v Praze k ověření biometrických údajů v cestovním dokladu.

Izraelská společnost AnyVision vznikla teprve v roce 2014, ale za tak krátké období se dokázala dostat mezi přední dodavatele software pro FR po celém světě. Za zmínku stojí instalace jejího produktu Better Tomorow na mezinárodním letišti v moskevském Domodědově, kde je aplikován systém pro kontrolu cestujících 1:1, ale i online vyhodnocování 1:M.

Na obrázku 23 jsou vypsány některé funkcionality testovaných software. Účelem testování nebylo ověřit všechny deklarované funkce, ale testování bylo zaměřeno primárně na ověření spolehlivosti detekce a identifikace osob 1:M na snímcích horší kvality.

Funkcionalita	Neo Face	Better Tomorrow
stanovení přibližného věku	✓	
identifikace pohlaví	✓	
natočení tváře horizontálně > 30°	✓	✓
natočení tváře vertikálně > 15°	✓	✓
identifikace osoby se slunečními brýlemi		✓
identifikace osoby se zakrytým obličejem		✓
identifikace osoby mladší než 15 let	✓	
určení etnické příslušnosti	✓	
trackování osob napříč systémem	✓	✓
uživatelské vytváření Black List	✓	✓
identifikace emocí (hněv, radost,…)	✓	
export dat	✓	✓
detekce předmětů		✓

Obrázek 23 - Přehled funkcionalit software

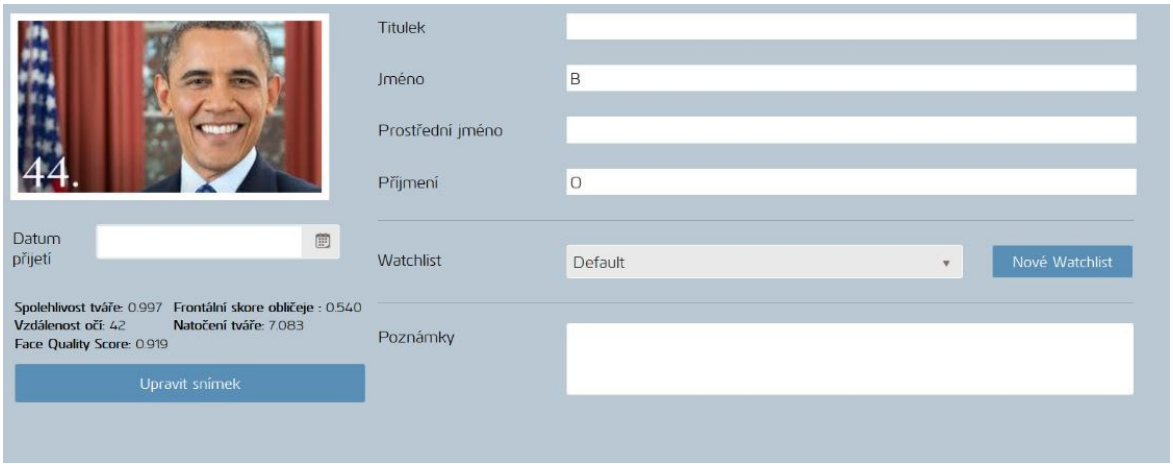
K testování byla využita databáze, ve které bylo použito cca 13 000 fotografií typu Mugshots. V databázi jsou zastoupeny muži a ženy ve věku 15 - 80 let a různých etnik, přičemž nejvíce zastoupeni jsou muži a ženy bělošského původu. Tato databáze je uvolněna pro potřeby vývojářů software určených k detekci obličejů s následným porovnáváním. Databáze je volně stažitelná z veřejných zdrojů.

Pro testování byly vytvořeny fotografie osob v různém prostředí tak, aby co nejvíce odpovídaly reálným podmínkám. Některé fotografie však byly záměrně pořízeny v situacích, kdy již bylo i pro člověka těžké určit, zda se skutečně jedná o osobu, která má být nalezena ve výchozí databázi. Kvalita fotografií odpovídala požadavkům dle normy ISO/IEC 19794, některé fotografie byly staženy z volně dostupných internetových zdrojů. U jedné sady fotografií došlo nejdříve k vyvolání z klasického kinematografického filmu a následně došlo k převedení do digitální podoby pomocí fotoaparátu na mobilním telefonu s rozlišením 12 Mpx, což mělo za následek celkové zhoršení kvality snímku.

Samotní výrobci software pro FR určují minimální nutnou hardwarovou a softwarovou konfiguraci klientských stanic a severů. Při testování software Neo Face Watch byla použita lokální pracovní stanice s procesorem Intel Core i7 2,00 GHz, RAM 8,00 GB a operační systém Windows 10. Pro produkt Better Tomorow byla využít systém klient – server, přičemž serverová část byla konfigurována s dvěma procesory Intel Xeon E5, grafická karta 4 x NVIDIA Tesla P40, RAM 256 GB. Klientská stanice měla procesor Intel Core i5 2,4 GHz, RAM 4,00 GB s operačním systémem Windows 7.

Oba produkty měly své vlastní přívětivé uživatelské prostředí, které se ovládalo velmi intuitivně, a i když byl produkt Better Tomorrow v anglické jazykové verzi, nebylo těžké se v programu orientovat a pohodlně pracovat. Nejdříve bylo nutné připojit se k výchozí databázi (databáze s 13 000 fotografiemi typu Mugshots). Následně byla do výchozí databáze (konkrétně do záložky s názvem Watch List[5]) nahrána referenční fotografie osoby, kterou budeme hledat. Po zadání povinných údajů, došlo k načtení snímku a k zhodnocení kvality fotografie. U programu Neo Face Watch jsou informace o načtené fotografii jako spolehlivost tváře, vzdálenost očí a další, tak jak uvedeno na obrázku 24.

[5] Watch List – seznam osob v databázi



Obrázek 24 – Ukázka referenčního snímku v Neo Face Watch

U produktu Better Tomorrow se uživatel musí smířit pouze s konstatováním, že se jedná o fotografii v horší kvalitě (obrázek 25), případně dojde k upozornění, že je fotografie nevhodná jako referenční snímek a je nutné vložit jinou fotografii.

Obrázek 25 – Ukázka referenčního snímku Better Tomorrow

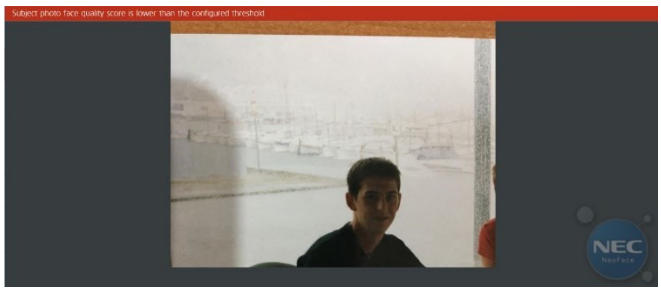
Po vložení referenčního snímku do Watch Listu byly postupně vkládány jednotlivé fotografie k identifikaci osoby na fotografiích, tedy jednalo se o testování 1:M. Aby bylo dosaženo korektního výsledku, tak byla nastavena hranice prahové hodnoty tzv. Thresholds na úroveň 0,45. To v praxi znamenalo, že v případě, pokud se fotografie neshodovala s referenčním snímkem alespoň na score 0,45 nebyla takové fotografii přiřazena žádné osobě a k identifikaci nedošlo. Prahovou hodnotu bylo možné zvyšovat i snižovat dle potřeby uživatele, ale v testování bylo vycházeno z doporučení výrobce.

Jak již bylo zmíněno, testování bylo zaměřeno na různé typy prostředí a situace. Vzhledem k rozsáhlosti testovaných dat není možné uveřejnit všechny vzniklé situace a jsou vybrány jen některé snímky a to zejména z mé osobní databáze nebo z volně dostupných otevřených zdrojů.

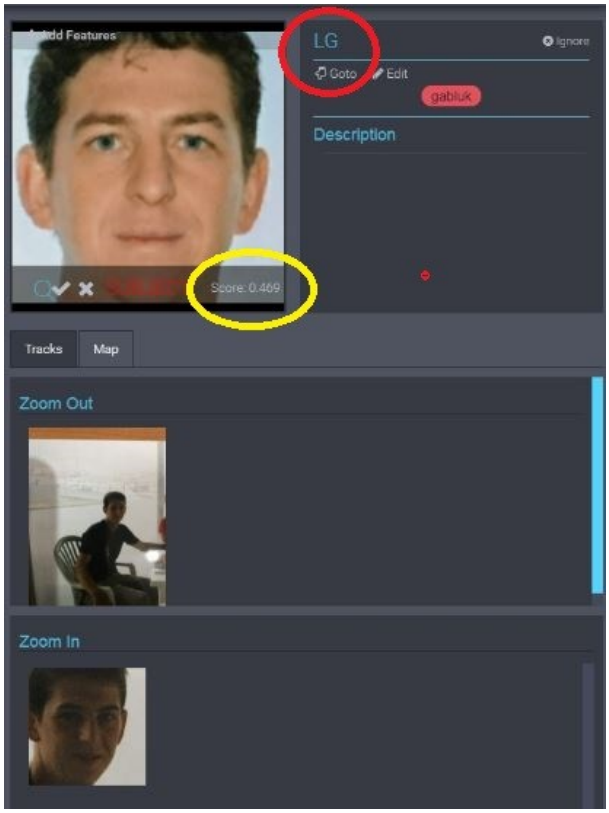
V prvním testu měly systémy detekovat sedícího muže ve věku 23 – viz levý snímek na obrázku 26. Jako referenční snímek byla použita pasová fotografie, na které je stejný muž ve věku 35 let (pravý snímek na obrázku 26), který byl do Watch Listu uložen pod jménem „LG“. Očekávaný výsledkem je takový, že levý snímek na obrázku 26 bude systémem detekován jako první kandidát na osobu s označením „LG“ a score shody se bude blížit hodnotě „1“ (čím vyšší číslo blížící se hodnotě „1“ v kolonce score, tím vyšší je pravděpodobnost, že se jedná o stejnou osobu). Kvalita obou snímku je snížena skutečností, že snímky byly nejdříve vyvolány a následně nafoceny pomocí fotoaparátu v mobilním telefonu.

Obrázek 26 – Vstupní a referenční snímky

Na obrázku 27 je ukázán výsledek algoritmus Neo Face Watch, který nedokázal fotografii vyhodnotit, přičemž konstatoval, že „Vzdálenost očí na fotografii je nižší, než nastavená prahová hodnota“. Tuto skutečnost potvrzuje druhý testovaný algoritmus, který správně přiřadil hledanou osobu „LG“, ale uvedené score (viz žluté kolečko na obrázku dole) se rovná 0,469 viz obrázek 28.



Obrázek 27 – Výsledek prvního testu - Neo Face Watch



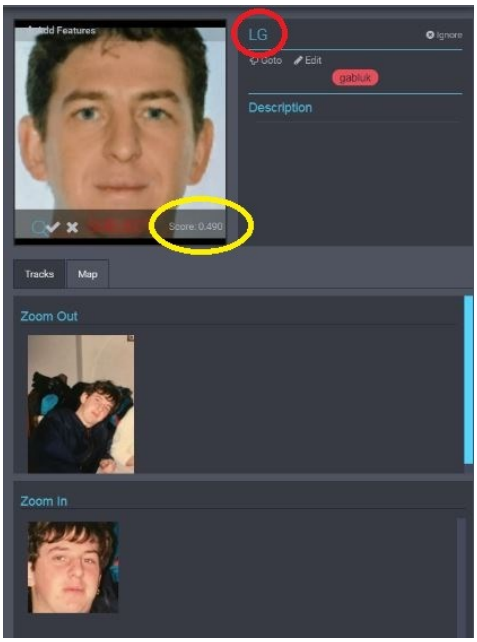
Obrázek 28 – Výsledek prvního testu - Better Tomorrow

V dalším testu byla testována stejná osoba, jen doba pořízení fotografie bylo ještě více v minulosti a hledané osobě bylo přibližně 19 let. Vyhodnocovaný snímek je na obrázku 29. Referenční snímek s označením „LG“ zůstal nezměněn. Očekávaný výsledek měl být stejný jako v prvním testu, tedy přiřazení osoby s názvem „LG“ a co nejvyšší score.

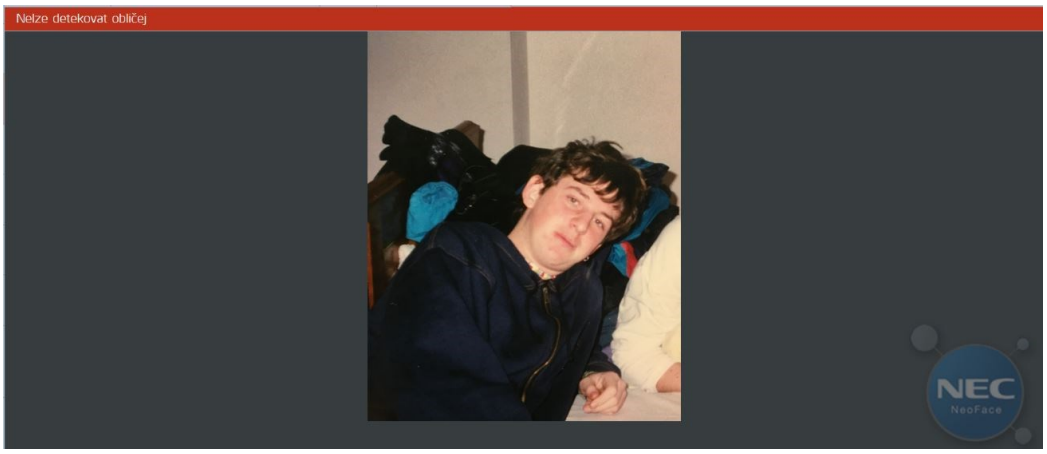
Obrázek 29 – Vstupní snímek pro druhý test

Program Better Tomorrow správně přiřadil hledanou osobu k osobě „LG“, přičemž score dosáhlo hodnoty 0,490 bodu. U produktu Neo Face Watch nedošlo k přiřazení hledané osobě

a algoritmus pro detekci tváří vyhodnotil, že „Nelze detekovat obličej“. Výsledky obou systémů jsou na obrázcích 30 a 31.



Obrázek 30 – Výsledek druhého testu – Better Tomorrow



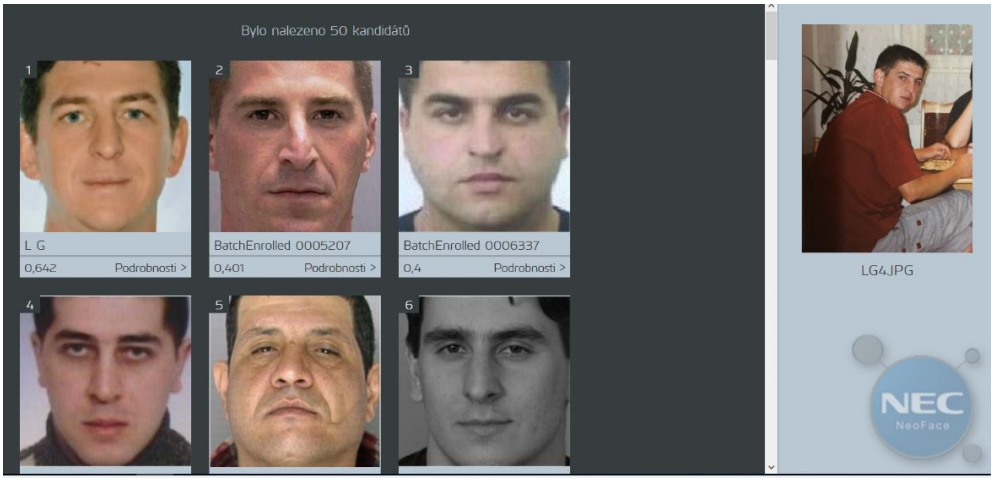
Obrázek 31 – Výsledek druhého testu – Neo Face Watch

Další test byl zaměřen na schopnost algoritmů správně identifikovat fotografii muže s pootočenou a lehce skloněnou hlavou viz obrázek 32, přičemž fotografie je opět vyvolána a následně nafocena pomocí mobilního telefonu.

Obrázek 32 – Vstupní foto pro třetí test

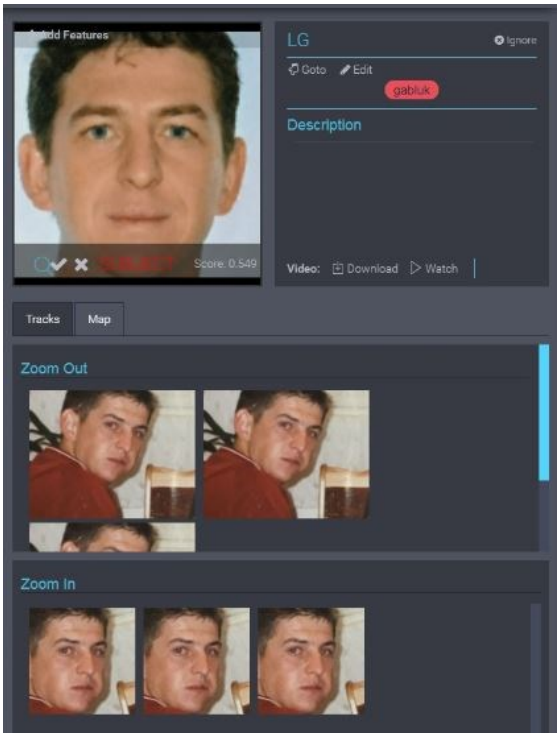
Očekávaný výsledkem je takový, že snímek na obrázku 32 bude systémem detekován jako první kandidát na osobu s označením „LG“ a score shody se bude blížit hodnotě „1“.

Výsledky testu algoritmu Neo Face Watch jsou zobrazeny na obrázku 33, přičemž došlo k správné identifikaci osoby na obrázku. Score bylo programem stanoveno na 0,642. Druhý kandidát v pořadí měl score 0,401, třetí kandidát hodnotu 0,4.



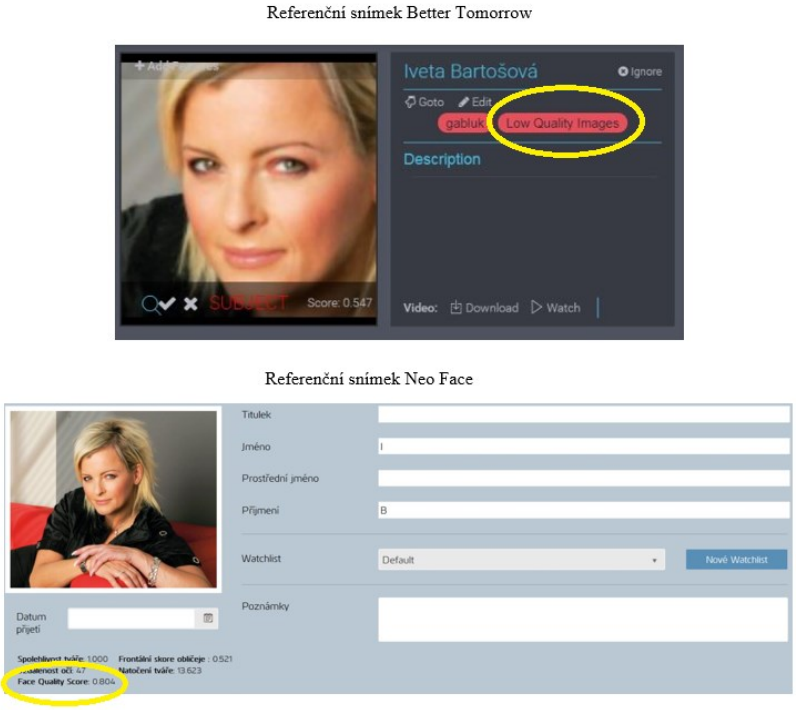
Obrázek 33 – Výsledky testu – Neo Face Watch

Better Tomorrow rovněž správně identifikoval osobu z obrázku 32 a score stanovil na 0,549. Bohužel ve výsledku nabízí jen jednoho kandidáta, tudíž není možné zjistit, jaké score měla druhá osoba v pořadí.



Obrázek 34 – Výsledky testu – Better Tomorrow

Následující testovací sada byla zaměřena na ženu – bělošku. Pro testování byla zvolena zpěvačka Iveta Bartošová. Fotografie byly staženy z volně dostupných zdrojů na internetu. Referenční snímky, které byly vloženy do Watch Listu v obou programech, jsou zobrazeny na obrázku 35. V Better Tomorrow bylo zadáno jméno a příjmení „Iveta Bartošová“, u Neo Face Watch se jedná o osobu „IB“. Rozlišení vstupních snímků testované osoby je 450 x 380 pixelů. Zajímavostí je, že Better Tomorrow označil referenční snímek nízkou kvalitou (viz obrázek 35 - žlutý kroužek), zatímco u Neo Face Watch bylo Face Quality Score vyčísleno hodnotou 0,804 bodů, přičemž maximum je 1 (viz obrázek 34 – žlutý kroužek).



Obrázek 35 – Referenční snímky v programech

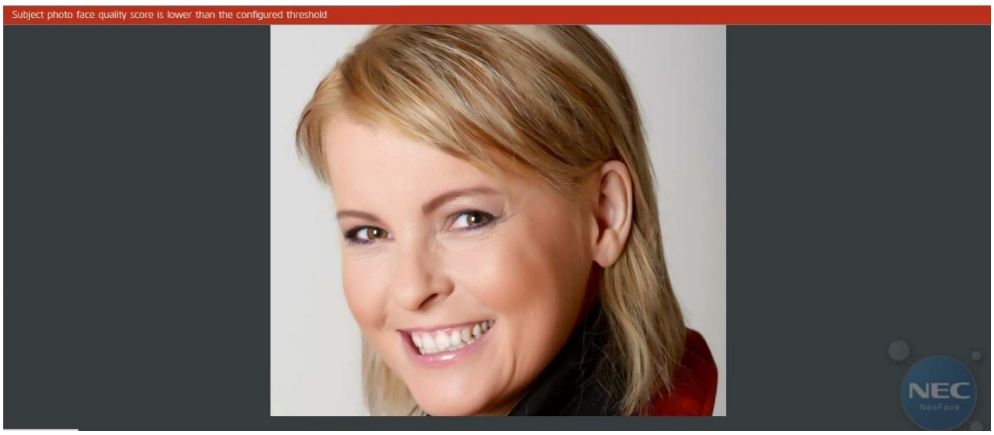
Jako první byl testován snímek s rozlišením 1113 x 800 pixelů, na němž je fotografie ženy, která má lehce natočenou tvář. Vložený snímek je na obrázku 36.

Obrázek 36 – Vstupní foto (38)

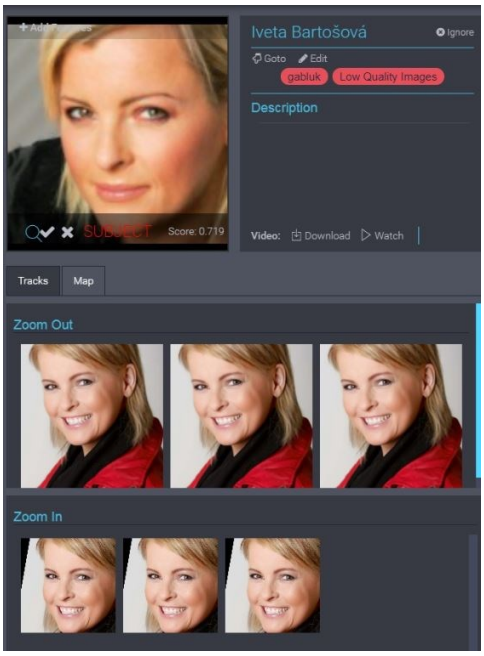
Po vložení vstupní fotografie měl být výsledek takový, že algoritmus Neo Face Watch měl určit jako hledanou osobu „IB“ a Better Tomorrow vyhledat osobu „Iveta Bartošová“. Opět bylo očekáváno, že kandidát bude na prvním místě a score bude blížící se hodnotě „1“.

Výsledky obou programů jsou odlišné, zatímco Neo Face Watch ukončil identifikaci s tím, že „Vzdálenost očí na fotografii je nižší, než nastavená prahová hodnota“ viz obrázek 37.

Jak je patrno na obrázku 38, Better Tomorrow správně identifikoval hledanou osobu jako „Iveta Bartošová“ se score 0, 719.

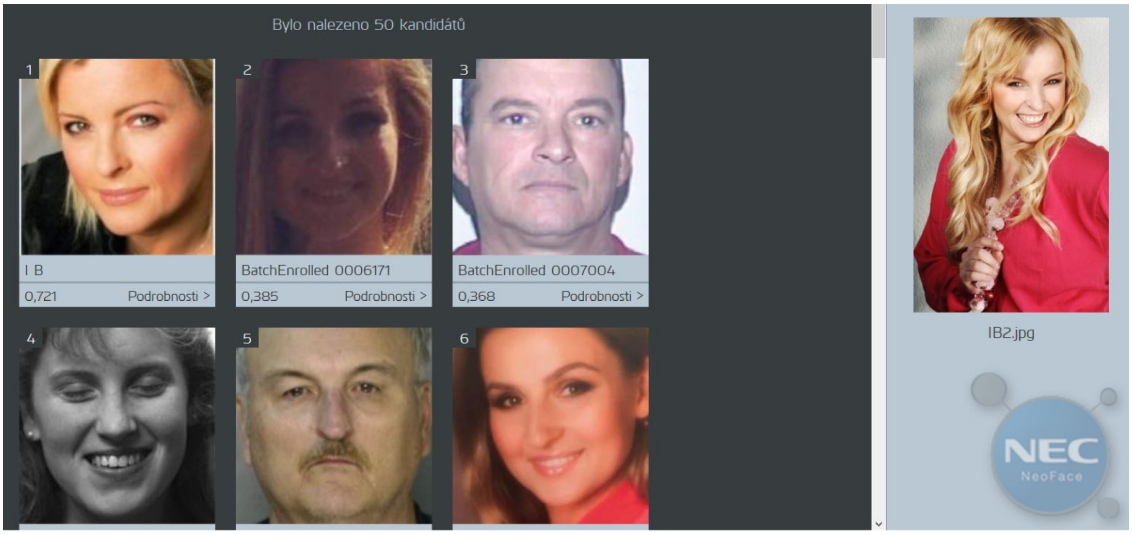


Obrázek 37 – Výsledek Neo Face Watch – Nelze detekovat obličej

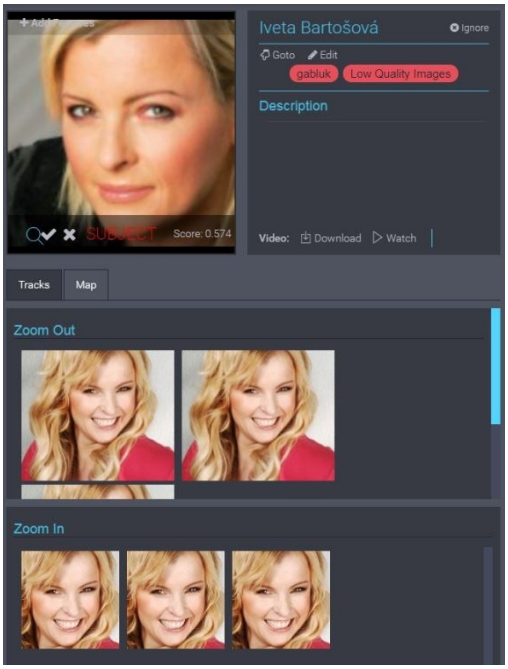


Obrázek 38 – Výsledek Better Tomorrow – správná identifikace

V dalším testu měl snímek rozlišení 604 x 401 pixelů a je na něm přímí pohled na usmívající se ženu. Oba testované programy správně identifikovaly hledanou osobu jako „IB“ u Neo Face Watch i „Iveta Bartošová“ u Better Tomorrow. Rozdílné výsledky jsou však ve score, kdy Neo Face Watch určil score na 0,721 bodu a Better Tomorrow na 0,574. U dalších kandidátů programu Neo Face Watch bylo určeno score druhého kandidáta (ženy) na 0,385. Třetí kandidát se score 0,368 byl muž. Better Tomorrow vyhodnotil jednoho kandidáta „Iveta Bartošová“ a jiné kandidáty již nenabídl.

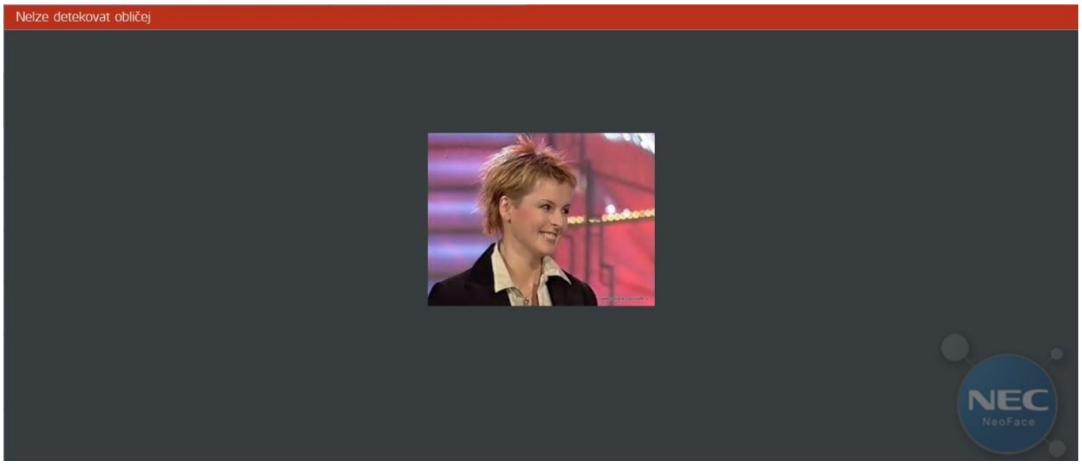


Obrázek 39 – Výsledky identifikace Neo Face Watch

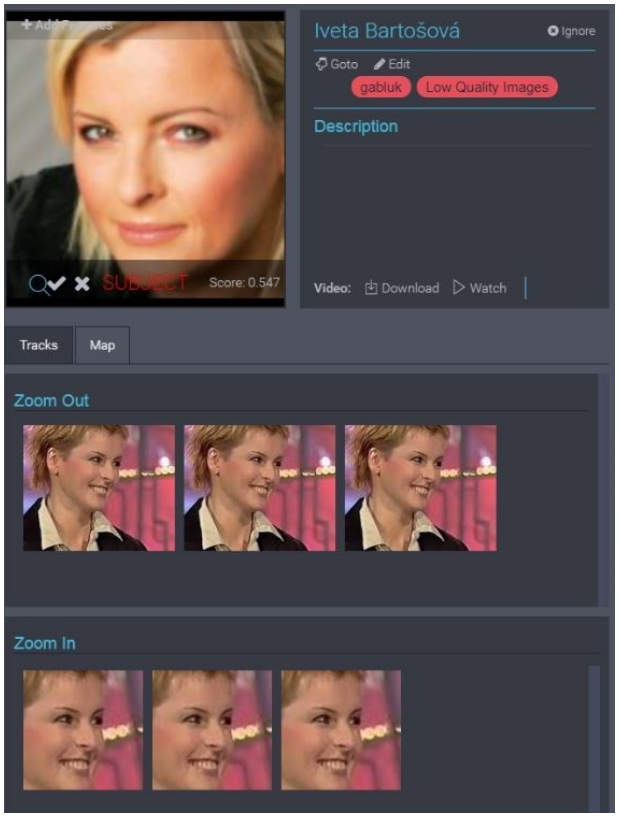


Obrázek 40 – Výsledky testu – Better Tomorrow

K třetímu testu byl použit snímek s rozlišením 257 x 196 pixelů a je na něm zachycena žena s pootočenou hlavou ještě více, než bylo u prvního testu ženy. Testované algoritmy vyhodnotili fotografie různě, Neo Face Watch nedetekoval obličej a Better Tomorrow dosáhl score 0,547. Výsledky jsou zobrazeny na obrázcích 41 a 42.



Obrázek 41 – Výsledek testu – Neo Face Watch

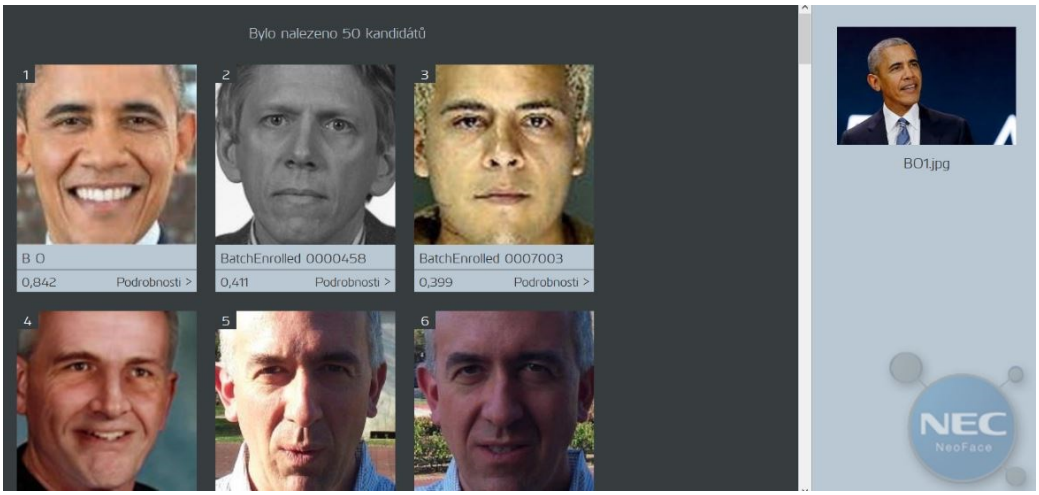


Obrázek 42 – Výsledek testu – Better Tomorrow

Pro další testovací sadu byl vybrán muž černošského původu ve věku přibližně 50 – 55 let (nelze přesně určit dobu vzniku fotografie), jedná se o bývalého prezidenta Spojených států amerických Baracka Obamu. Fotografie byly staženy z volně dostupných internetových zdrojů. Do Watch Listu obou testovaných programů byly vloženy a pojmenovány referenční fotografie s rozlišením 299 x 169 pixelů. U Neo Face Watch byl snímek nazván jako „BO“ a u Better Tomorrow jako „BO ref“. Face Quality score byla u Neo Face Watch 0,919, zatímco Better Tomorrow vyhodnotil referenční snímek jako „Low Quality Image“.

První testovací snímek měl rozlišení 277 x 182 pixelů. Po vložení fotografie k identifikaci měl být výsledek takový, že algoritmus Neo Face Watch měl určit jako hledanou osobu „BO“ a Better Tomorrow vyhledat osobu „BO ref“. Score vyhledané osoby se mělo blížit k hodnotě k „1“.

Oba algoritmy správně označily hledanou osobu, ale rozdíl byl v score, kdy Neo Face Watch dosáhl hodnoty 0,842 a Better Tomorrow hodnoty 0,661. Další kandidáti u Neo Face Watch dosáhli poloviční míry shody jako správně identifikovaný „BO“. Better Tomorrow nabídl standardně jen jednoho a to správně identifikovaného kandidáta. Dosažené výsledky jsou na obrázku 43 a obrázku 44.



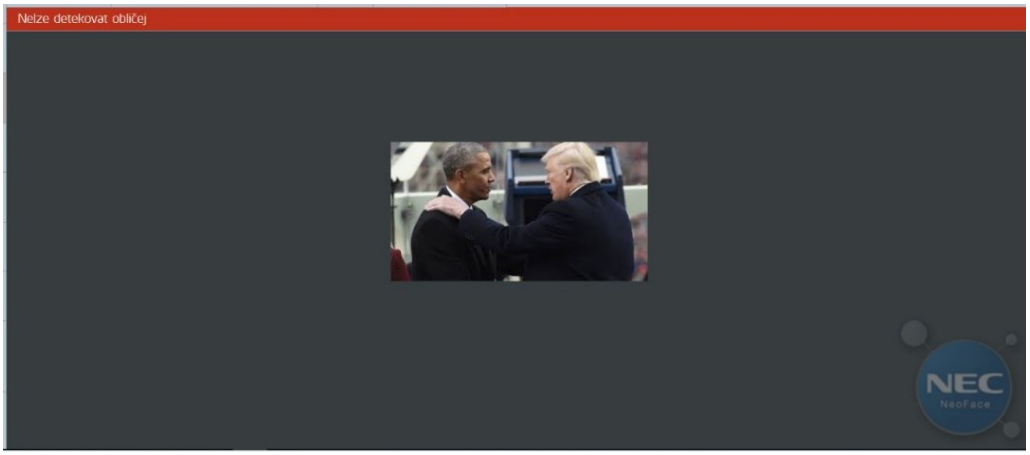
Obrázek 43 – První test – Neo Face Watch

Obrázek 44 – První test – Better Tomorrow

Následný test byl zaměřen na detekci osoby, která je otočena bokem a je jí vidět pouze půl obličeje. Snímek měl rozlišení 305 x 165 pixelů a je z venkovního prostředí.

Obrázek 45 – Barack Obama a Donald Trump (39)

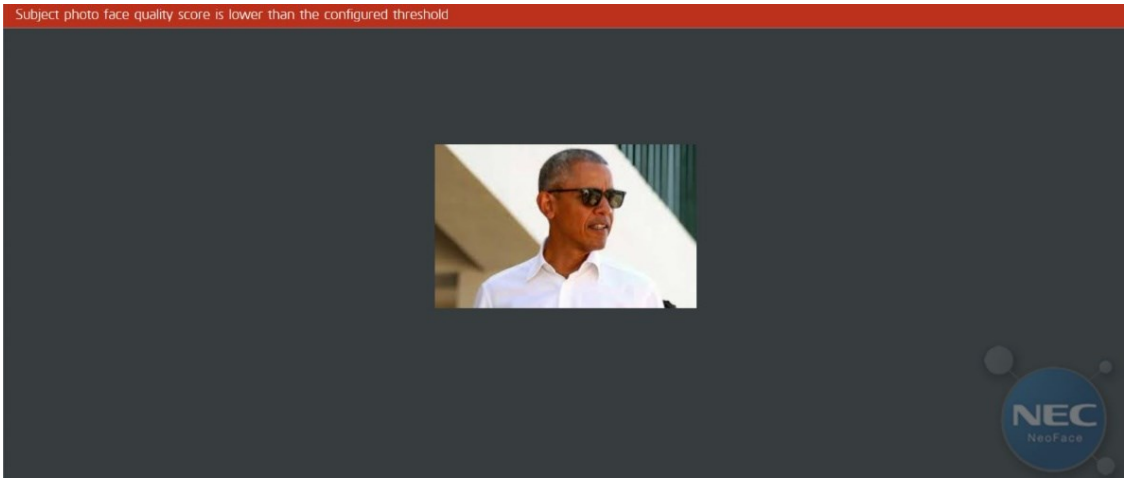
Programy vloženou fotografii vyhodnotily rozdílně. Neo Face Watch nedokázal na fotografii detekovat obličej (viz obrázek 46) a Better Tomorrow správně identifikoval osobu jako „BO ref“ se score 0,485, což je vidět na obrázku 47. Pozoruhodné je, že Better Tomorrow detekoval a identifikoval obličej pouze Baracka Obamy, přičemž u druhého muže (Donald Trump) k detekci obličeje nedošlo. Na první pohled by se mohlo zdát, že jsou obě osoby vzhledem k fotografovi, ve stejné poloze. Při bližším prozkoumání snímku na obrázku 45 si je možné všimnout, že přeci jenom obličej Donalda Trumpa je o trochu méně natočen k fotografovi, než obličej Baracka Obamy.



Obrázek 46 – Výsledek porovnání – Neo Face Watch

Obrázek 47 – Výsledek testu – Better Tomorrow

Poslední test z této sady byl zaměřen na muže ve slunečních brýlích, když byla do programů vložena fotografie s rozlišením 284 x 177 pixelů z venkovního prostředí. Výsledky jsou opět rozdílné, zatím co Neo Face Watch vyhodnotil fotografii jako „Vzdálenost očí na fotografii je nižší, než nastavená prahová hodnota“ (obrázek 48), Better Tomorrow dokázal správně identifikovat „BO ref“ se score 0, 513 viz obrázek 49.



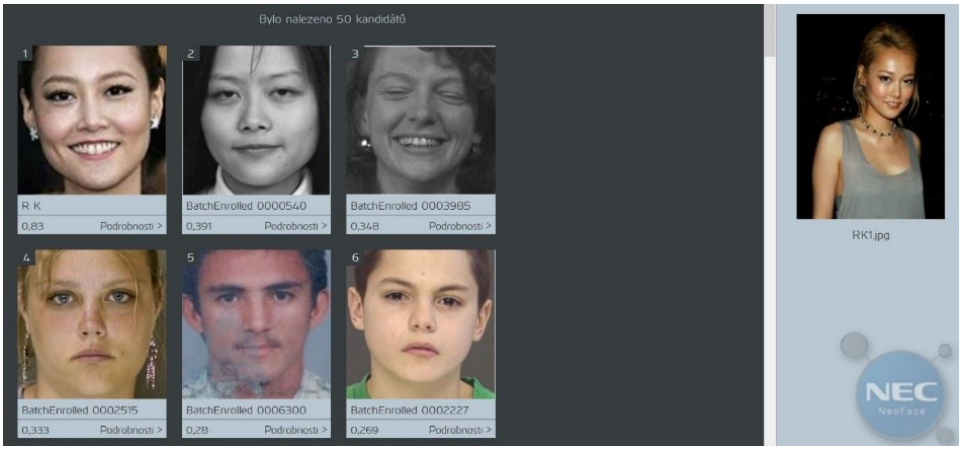
Obrázek 48 – Vyhodnocení fotografie – Neo Face Watch

Obrázek 49 – Správná identifikace – Better Tomorrow

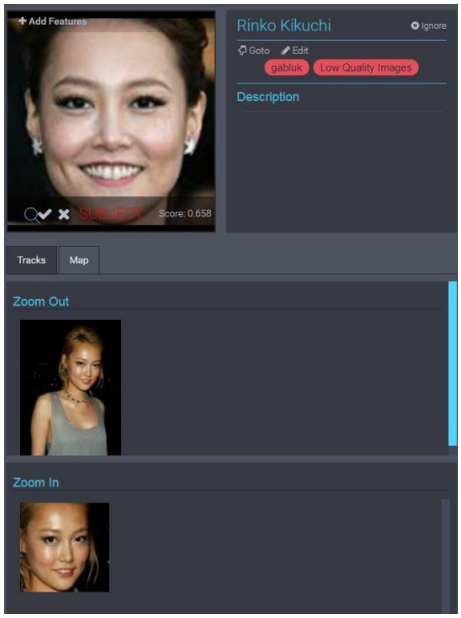
Poslední testovací sada byla zaměřena na ženu s asijskými kořeny původu. Jednalo se o japonskou horečku Rinko Kikuchi ve věku přibližně 30 let. Fotografie byly staženy z volně dostupných internetových zdrojů. Do Watch Listu obou testovaných programů byly vloženy a pojmenovány referenční fotografie s rozlišením 273 x 183 pixelů. U Neo Face Watch byl snímek nazván jako „RF“ a u Better Tomorrow jako „Rinko Kikuchi“. Face Quality score byla u Neo Face Watch 0,905 a Better Tomorrow vyhodnotil referenční snímek jako „Low Quality Image“.

První testovací snímek měl rozlišení 264 x 191 pixelů a je na něm hledaná žena, za kterou je tmavé pozadí. Po vložení fotografie k identifikaci měl být výsledek takový, že algoritmus Neo Face Watch měl určit jako hledanou osobu „RK“ a Better Tomorrow vyhledat osobu „Rinko Kikuchi“. Score vyhledané osoby se mělo blížit k hodnotě k „1“.

Oba softwarové nástroje identifikovaly fotografii správně a přiřadily jméno dle očekávaných výsledků. Rozdíl byl opět ve score, kdy Neo Face Watch ohodnotilo shodu na 0,83 (obrázek 50) a Better Tomorrow na 0,658 (obrázek 51).

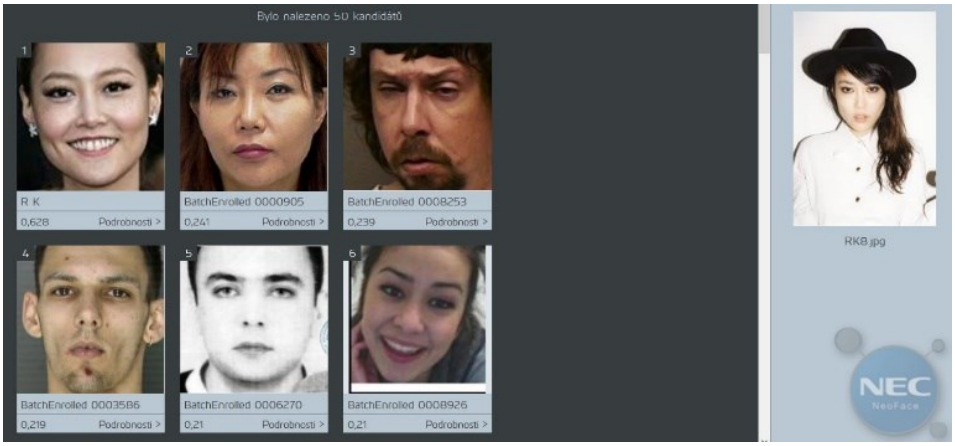


Obrázek 50 – Výsledek testu – Neo Face Watch

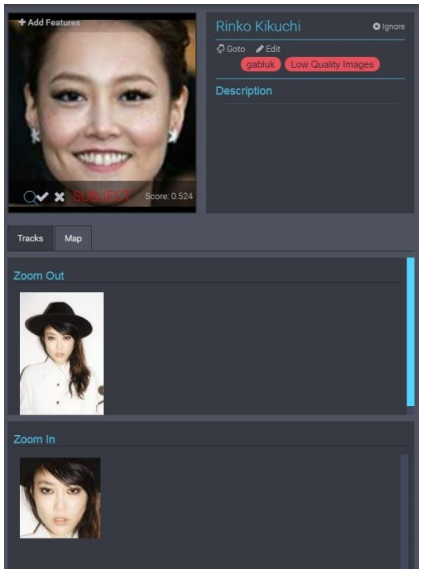


Obrázek 51 – Výsledek porovnání – Better Tomorrow

Druhý testovací snímek měl rozlišení 275 x 183 pixelů, na němž je Rinko Kikuchi v klobouku. Výsledky identifikace měly být stejné jako v prvním testu.



Obrázek 52 – Výsledek testu - Neo Face Watch



Obrázek 53 – Výsledek testu - Better Tomorrow

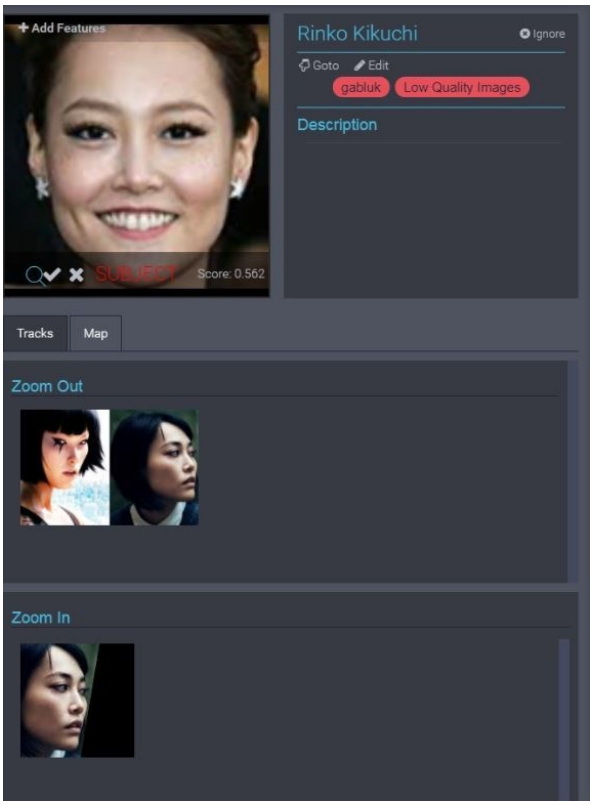
Dle očekávání byly oba výsledky správné, jak je možné vidět na obrázku 52 a 53. Hodnotící score pro Neo Face Watch je 0,628 a Better Tomorrow určilo shodu 0,524.

Třetím testem bylo určení osoby na fotografii, která je na obrázku 54. Snímek měl rozlišení 253 x 199 pixelů. Bohužel u tohoto snímku nedokázal ani jeden software správně určit Rinko Kikuchi. Better Tomorrow určil score na 0,340, což je pod stanovenou hranici „Trasholds“ a algoritmus Neo Face Watch dokončil hledání s výsledkem „Vzdálenost očí na fotografii je nižší, než nastavená prahová hodnota“.

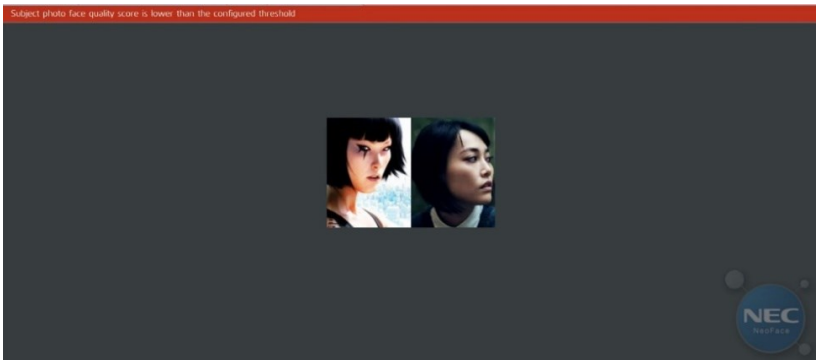
Obrázek 54 – Neúspěšný test

Posledním testem byla fotografie, ve které jsou vloženy dvě různé fotografie stejné osoby (Rinko Kikuchi). Úkolem algoritmů bylo správně detekovat a identifikovat osobu na obou fotografiích. Fotografie měla rozlišení 278 x 181 pixelů.

Ani jeden ze software nedokázal správně detekovat a identifikovat výše uvedený příklad. Better Tomorrow si pro detekci a identifikace „vybral“ pravý snímek a správně označil hledanou osobu se score 0,562. Pro produkt Neo Face Watch skončilo vyhledávání již při detekci obličeje. Výstupy z testovaných software jsou na obrázcích 55 a 56.



Obrázek 55 – Výsledek testu - Better Tomorrow



Obrázek 56 – Neo Face Watch – neúspěšná detekce obličeje

5.2 Celkové zhodnocení testovaných software

Představené ukázky detekce a identifikace osob u produktů Better Tomorrow a Neo Face Watch představují jen část testovaných dat a jedná se o základní testování 1:M. Je nezbytné podotknout, že vstupní snímky byly záměrně pořizovány ve snížené kvalitě nebo v situacích, kdy jsou hledané osoby v různých pozicích na hranici deklarovaných možností algoritmu. Celkově bylo otestováno několik stovek vstupních fotografií podobných, jako jsou uvedeny na obrázku 57.

Obrázek 57 – Ukázka vstupních fotografií k porovnání (40)

U software Neo Face Watch bylo 38 % testovaných snímků správně identifikováno dle předem stanoveného scénáře. Algoritmus Better Tomorrow dosáhl úspěšnosti 53 %. V potaz nebylo bráno score nižší, než 0,45. Tato hodnota byla stanovena výrobci jako hraniční pro správnou identifikaci. Samotnou otázku je určení score neboli shody. Jak je zřejmé v kapitole 5, výsledky shody vloženého snímku s referenčním snímkem se u obou výrobců v průběhu celého testování liší. Například na obrázku 50 je správná identifikace hledané osoby se shodou 0,83 (Neo Face Watch), zatímco algoritmus Better Tomorrow vyhodnotil

stejný snímek s přesností 0,658 (obrázek 51). I když v průběhu celého testování dosahoval produkt Better Tomorrow nižší shody oproti Neo Face Watch, dokázal správně přiřadit identitu u více osob. Z výše uvedeného plyne, že míra shody (score) nemůže být brána jako směrodatný parametr pro určení, který testovaný algoritmus je spolehlivější.

V průběhu testování bylo zjištěno, že pokud algoritmus dokáže na snímku správně detekovat obličej osoby, tak následná identifikace oproti referenčnímu snímku je na velmi vysoké úrovni. Software Neo Face Watch při identifikaci vždy navrhoval několik kandidátů, které se nejvíce shodují s osobou na vloženém snímku. Jelikož hledané osoby byly testerovi známé, věděl uživatel, jaké kandidáty má očekávat na prvních pozicích, a tudíž dokázal vyhodnotit relevantnost očekávaného výsledku. Hledaná osoba byla, v drtivé většině případů, navržena mezi prvními pěti kandidáty a nejčastěji se jednalo o kandidáta na prvním místě, tedy nejvyšší pravděpodobnost, že se jedná o stejnou osobu jako na referenčním snímku. U algoritmu Better Tomorrow nebyla možnost vidět další kandidáty s nižší mírou shody a testerovi byl představen jen jeden kandidát, který však byl v 99 % správný. Oba výrobci ve svých markentingových materiálech deklarují míru správné identifikace vyšší, než 99 % a špatně identifikovanou osobu v počtu méně, než jedna 1% za den. Z výsledků testování je tedy možné konstatovat, že výrobci deklarované hodnoty jsou dosažitelné za předpokladu, že budou dodrženy požadavky na kvalitu snímku a viditelnost hlavních markantů obličeje.

6. MOŽNOSTI VYUŽITÍ FACE RECOGNITION V BEZPEČNOSTNÍ OBLASTI

Jak již bylo uvedeno v minulé kapitole, výsledky byly dosaženy na základě jednoho snímku, který byl vložen do software. V bezpečnostní oblasti se k monitorování prostorů používají kamerové systémy. Současné kamery snímají scénu ve vysokém rozlišení (HD či Full HD) a zvýšil se i počet snímků za sekundu (standardně 15 až 30 snímků), což jsou důležité parametry pro další zpracování získaných dat. Je nespornou výhodou, že v případě instalace kamerového systému a současně software pro identifikaci osob dochází k získávání mnohem kvalitnějších vstupních fotografií, než pokud je k porovnání používána jediná fotografie. I v případech, kdy je využíván komplexní systém (kamerový systém a software pro FR) nemusí být získán kvalitní snímek. Vliv na výsledky bude mít skutečnost, zda jsou snímky pořizovány ve vnitřním nebo venkovním prostředí. Snímek z kamery s vysokým rozlišením, z venkovního prostředí, za snížené viditelnosti a zhoršených klimatických podmínek (déšť, sněžení nebo mlha) nemusí nutně znamenat záruku zvýšení pravděpodobnosti správné identifikace osoby. Dalším aspektem, který bude mít vliv na kvalitu snímku detekovaných osob je skutečnost, zda budou snímky získané ze spolupracující či nespolupracující scény. Snímky získané z bezpečnostního koridoru, do kterého osoby vstupují jednotlivě, budou určitě kvalitnější, než záběry z rušné ulice, kde je několik desítek osob.

V praxi jsou využívány přístupové systémy, které k ověření identity používají dvou faktorové autentizace. Jedním identifikátorem je vstupní karta, druhým autentizačním prvek je právě obličej vstupující osoby. Systém je používán například u turniketů, které mají integrovanou čtečku identifikačních karet a kameru. Po přiložení oprávněné karty je ještě nutné, aby se osoba, která kartu přiložila, rovněž shodovala s fotografií osoby, která je s kartou spárována. Jedná se o využívání identifikace 1:1. Tyto turnikety jsou nejčastěji instalovány již v prostorách objektu, kde jsou relativně stabilní klimatické i světelné podmínky a kvalita vstupních snímků pro správnou identifikaci by měla být na vysoké úrovni. Následná identifikace tudíž bude vyhodnocena s vysokou mírou shody.

V některých oblastech komerční bezpečnosti je již FR využíván k identifikaci osob na úrovni perimetru a to z toho pohledu, zda se nesnaží neoprávněná osoba proniknout do zájmového objektu spolu s ostatními zaměstnanci. V případě zjištění takové skutečnosti vzniká dostatečný reakční čas pro operátory na tuto skutečnost adekvátně zareagovat a zabránit tak potencionálnímu riziku zneužití informací nebo škodě na majetku společnosti. Nejčastěji se

software pro FR využívá u společností, kde není možné efektivně kontrolovat totožnost každého ze vstupujících zaměstnanců.

V bankovním sektoru se již pomalu ustupuje od notifikace platebních příkazů pomocí textových zpráv a jednou z možností potvrzování plateb je i využití identifikace majitele bankovního účtu nebo platební karty pomocí FR. Jeden z možných scénářů je takový, že potvrzení platby se provede pomocí bezpečné aplikace přes mobilní telefon. Je však otázkou do jaké míry bude uživatel schopný pořídit pomocí mobilního telefonu kvalitní vstupní snímek, který bude sloužit pro verifikaci v databázi fotografií v bance. Samostatnou otázkou je bezpečnost přenášených a spravovaných dat na úrovni mobilního telefonu, mobilní sítě a datového úložiště banky.

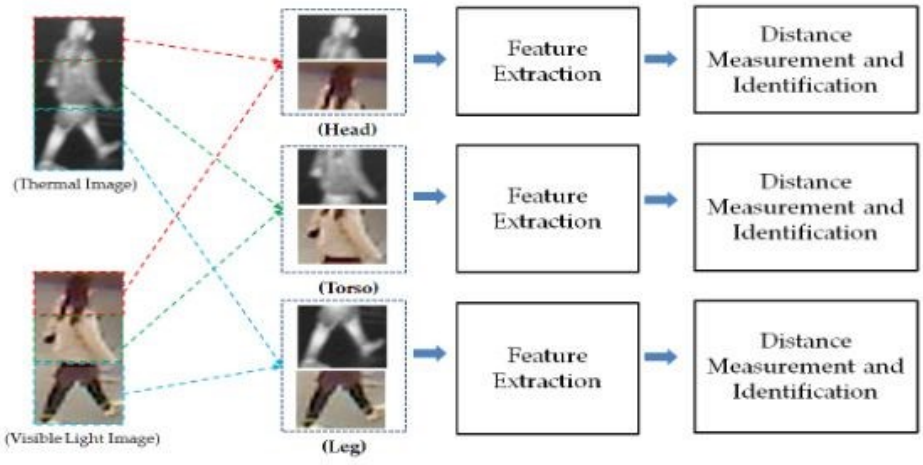
Oblast identifikace osob má však široké využití i u policejních orgánů, zpravodajských služeb nebo orgánů státní správy. Policie České republiky má zákonnou možnost ke své činnosti monitorovat veřejné prostranství, které rovněž aktivně využívá a v každém policejním vozidle je integrována nejméně dvojice kamer, které pořizují nepřetržitě záznam. V praxi se využívá i malých kamerových jednotek umístněných přímo na výstroji jednotlivých policistů. Dle mého názoru je jen otázkou několika málo let a do těchto kamerových jednotek (nebo vozidel) budou instalovány speciální software pro identifikaci osob s následným porovnáním v registru obyvatelstva nebo osob vstupujících do Schengenského prostoru. Policisté tak bude mít komplexní informace o osobě, se kterou jednají a mohou adekvátně reagovat na případného pachatele trestné činnosti nebo pohřešovanou osobu. Informace o osobě by mohla být policistovi sdělená pomocí zvukové notifikace anebo přenesena do zobrazovacího zařízení (brýlí) díky rozšířené realitě. I zda však bude nutné vyřešit problematiku bezpečnosti dat a dále aktualizaci databázi osob. Otázkou je zda se bude jednat o on-line vyhledávání v registrech obyvatelstva nebo bude do kamerové jednotky stažena jen off-line databáze, které se bude aktualizovat jen v určitý stanovený čas nebo po připojení do informačních systémů Policie České republiky.

S problematikou identifikace osob rovněž souvisí i se zabezpečením osobních údajů. Ochrana osobních údajů je v právním systému členských zemí Evropské unie pevně zakotvena a je nutné respektovat právo na soukromí. Vývojové společnosti řeší ochranu osobních dat softwarovým vymaskováním obličeje osob, které se nacházejí na monitorované scéně. Pokud vznikne potřeba určitou osobu v záznamu vyhledat, je možné softwarově odmaskovat určenou osobu a provést její identifikaci. Ostatní osoby na scéně zůstávají stále zamaskované.

Celospolečenské vnímání monitorování osob a shromažďování osobních informací je velmi citlivé téma. Většina obyvatel si nepřeje, aby jejich fotografie či biometrické údaje byly uloženy v databázích různých společností a je proto nutné, dbát na dodržování zákonem stanovených podmínek týkajících se osobních údajů. I když je třeba připomenout, že fotografie nebo jiné citlivé údaje jsou velmi snadno dostupné na sociálních sítích, kde je lidé vkládají sami…

V budoucnu lze očekávat další zvýšení spolehlivosti algoritmů, které detekují a identifikují osoby. Počítačový výkon, který je nutný pro zpracování dat se bude s největší pravděpodobností i nadále zvyšovat a bude tedy možné zavádět nové algoritmy, které pracují na principu konvolučních neuronových sítí. Již v současné době se vývojové a softwarové společnosti zabývají možnosti identifikace osob na základě pohybu osob - Body Recognition.

Vědci z dongguksé univerzity v Jižní Koreji představili ve své práci z roku 2017 možnost detekce a identifikace osob na základě jejich pohybu. Vstupní data k zpracování jsou získávána pomocí duální kamery, která byla složená ze standardně používané kamery a termální kamery. Následně probíhá zpracování získaného obrazu a identifikace s využitím algoritmu pracujícího na principu konvolučních neuronových sítí a PCA algoritmu. Na obrázku 58 je vidět, jakým způsobem algoritmus klasifikuje jednotlivé části lidského těla.



Obrázek 58 – Klasifikace lidského těla (41)

Testování bylo zaměřené na genderové rozdělení osob a proběhlo na více než čtyři sta osobách, které se pohybovaly po snímané scéně, aniž by byly dopředu obeznámeny

s testováním. Při pokusu se podařilo dosáhnout nejnižší chybovosti na úrovni 1,465 %, ale standardně se chybovost pohybovala v rozmezí 5 až 6 %. (41)

Uvedené výsledky nedosahují takové přesnosti jako detekce a identifikace osob na základě FR. Zajímavé by mohlo být využití termální kamery, k lepší detekci obličejů v případech, kdy je obličej zahalen, nebo jsou použity kamuflážní prostředky.

ZÁVĚR

Cílem diplomové práce nebylo jen testování spolehlivost software pro detekci a identifikaci osob, ale i objasnění celé problematiky tak, aby bylo možné v budoucnu učinit správné rozhodnutí o případné instalaci software pro detekci a identifikaci osob. Diplomová práce se zmíněnou problematikou zabývá nejen z pohledu samotné činnosti se software, ale v práci jsou i technické pasáže, protože je nutné dodržet některé specifické požadavky zejména na kvalitu vstupních snímků, instalační výšku samotné kamery nebo dodržení požadavků na software a hardware jednotlivých součástí systému.

V teoretické části diplomové práce jsou v první kapitole popsány jednotlivé části kamerového systému. Jedná se o průřez nejdůležitějšími komponenty, které jsou součástí kamerových systémů, včetně možnosti ukládání záznamu a exportu snímků. V druhé kapitole je stručně popsán proces zpracování vstupních podkladů, které jsou určeny pro detekci a identifikaci osob. Dále jsou ve druhé kapitole samostatně popsány jednotlivé algoritmy pro detekci osob (obličejů), a jsou představeny některé používané algoritmy pro správnou identifikaci osob. Poslední podkapitola je věnována databázím a požadavkům na vstupní a referenční snímky.

V praktické části je nejdříve vyjmenováno několik desítek výrobců software určeného pro detekci a identifikaci osob, následuje celek pojednávající o mezinárodní autoritě zabývající se testováním software pro Face Recognition a jsou zde představeny některé testy a jejich výsledky. Ve čtvrté kapitole je krátce představen software pro detekci a identifikaci osob, který je integrován přímo v kamerovém systému společnosti Panasonic, a jsou zde ukázány testy některých funkcionalit. Na výsledcích testování je patrné, že software nedokáže správně identifikovat osobu, která má nasazeny sluneční brýle nebo má přes obličej šátek. Stěžejní pátá část je věnována testováním software pro Face Recognition jako samostatný systém třetích stran. Testování bylo zaměřeno na ověření správné identifikace předem známé osoby vůči databázi několika tisíc fotografií (1:M). Cílem bylo zjistit, jak software dokážou vyhodnotit i snímky horší kvality nebo snímky z „běžného života“. Jednotlivé výsledky obou porovnávaných software jsou dokumentovány na přiložených fotografiích. V závěru páté části je vedena diskuze nad získanými výsledky a je konstatováno, že pokud algoritmus dokáže ve snímku najít obličej, je následná identifikace oproti databázi osob velmi spolehlivá. Závěrečná kapitola pojednává o možnosti využití Face Recognition v oblasti bezpečnostního průmyslu a je zde krátce popsána další možnost detekce osob, tak zvaný Body Recognition.

SEZNAM POUŽITÉ LITERATURY

1. Mihulka, Stanislav. 100+1 zahraničních zajímavostí. *Technologie přírody: Jaké je vlastně rozlišení lidského oka?* 2017, 11.

2. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby 2017.* [Online] 03. Prosinec 2018. [Citace: 30. Leden 2019.] https://www.bis.cz.

3. Válová, Irena. Česká justice. [Online] 16. Únor 2018. [Citace: 30. Leden 2019.] http://www.ceska-justice.cz.

4. Lukáš, Luděk. *Bezpečnostní technologie, systémy a management II.* Zlín : VeR-BuM, 2012. ISBN 978-80-87500-19-4.

5. Loveček, Tomáš a Nagy, Peter. *Bezpečnostné systémy:kamerové bezpečnostné systémy.* Žilina : Žilinská univerzita, 2008. ISBN 978-80-8070-893-1.

6. *moje Tajemno: Ohnisková vzdálenost.* [Online] 28. Červenec 2015. [Citace: 12. Leden 2019.] https://moje.tajemno.net/ohniskova-vzdalenost/.

7. *Blackem světem: Jak na foťák I.* [Online] 28. Prosinec 2014. [Citace: 23. Listopad 2018.] https://www.blackemsvetem.cz/jak-na-zrcadlovku-i/.

8. Pihan, Roman. *Digimanie.* [Online] 30. Leden 2008. [Citace: 31. Leden 2019.] https://www.digimanie.cz.

9. Adámek, Milan. *4. přednáška z předmětu Kamerové systémy.* Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2018.

10. TSS Group. [Online] 2019. [Citace: 12. Duben 2019.] https://www.tssgroup.cz/documents/8.0-h4a-d1/sdilene/datasheety%20-%20datasheety%20-%20datasheets/avigilon%20h4a-d%20en%20datasheet.pdf.

11. Bartošák, Kamil. Diplomová práce. *Součinnost analogovýh systémů s hybridními CCTV a jejich využití v průmyslu komerční bezpečnosti.* Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2007.

12. Křeček, Stanislav. *Příručka zabezpečovací techniky.* Praha : Cricetus, 2006. ISBN 80-902938-2-4.

13. Horký, Stanislav a Krsek, Libor. *Úvod do multimédií.* Praha : Oeconomica, 2009. ISBN 978-80-245-1608-0.

14. Long, Ben a Schenk, Sonja. *Velká kniha digitálního videa.* Brno : Computer Press, 2005. ISBN 80-251-0580-6.

15. technologie, Stasanet Bezpečnostní. Stasanet.cz. *IP vs. analog kamery a základní pojmy.* [Online] [Citace: 07. Únor 2019.] https://www.stasanet.cz/IP-vs-analog-kamery-a-zakladni-pojmy/.

16. Lukáš, Luděk. *Bezpečnostní technologie, systémy a management I.* Zlín : VeR-BuM, 2011. ISBN 978-80-87500-05-7.

17. Cepek, Alois. Diplomová práce. *Modernizace kamerového systému Univerzity Tomáše Bati ve Zlíně.* Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2018.

18. Security magazín. *Panoramatické kamery AXIS pro monitorování velkých otevřených ploch - letišť , nádraží nebo náměstí.* [Online] 29. Březen 2016. [Citace: 10. Duben 2019.] https://www.securitymagazin.cz/security/panoramaticke-kamery-axis-pro-monitorovani-velkych-otevrenych-ploch-letist-nadrazi-nebo-namesti-1404049819.html.

19. Variant plus s.r.o. Variant plus. *Strukturovaný kabelážní systém - příručka.* [Online] [Citace: 10. Únor 2019.] https://www.variant.cz/soubory-ve-skladu/Karty/Spol_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf.

20. Trulove, James. *Sítě LAN: hardware, instalace a zapojení.* Praha : Grada, 2009. 978-80-247-2098-2.

21. Kašpar, Martin. CCTV Calculator. *CCTV Calculator: Úložiště záznamu kamer.* [Online] 2019. [Citace: 12. Duben 2019.] https://www.cctvcalculator.net/cs/vypocty/uloziste-zaznamu-kamer/.

22. Netcam.cz. *Encykopledie síťového videa: Netcam.cz.* [Online] [Citace: 10. Únor 2019.] https://netcam.cz/encyklopedie-ip-zabezpeceni/co-je-to-videoserver.php.

23. Höll, Karel. Diplomová práce. *Aplikace metod detekce a rozpoznání obličeje.* Brno : Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2013.

24. Dvořák, Pavel. Diplomová práce. *Popis objektů v obraze.* Brno : Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011.

25. Rak, Roman, Matyáš, Václav a Říha, Zdeněk. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích.* Praha : Grada, 2008. 978-80-247-2365-5.

26. Acar, Nev. Towards Data Science. [Online] 21. Srpen 2018. [Citace: 12. Únor 2019.] https://towardsdatascience.com/eigenfaces-recovering-humans-from-ghosts-17606c328184.

27. Núdziková, Pavlína, a další. Učební text. *Elektromobilita - Identifikace člověka.* Ostrava : Vysoká škola báňská – Technická univerzita Ostrava, 2014.

28. Burián, Pavel. Bakalářská práce. *Rozpoznávání lidské tváře.* Brno : Vysoké učení technické v Brně, Fakulta informačních technologí, 2010.

29. Svozil, Lukáš. Bakalářská práce. *Aspekty biometrické identifikace osob s využitím rozpoznávání tváře.* Zlín : Univerzita Tomáše Bati ve Zlíne, Fakulta aplikované informatiky, 2009.

30. Li, Stan,Z. a Jain, Anil. *Handbook of Face Recognition.* London : Springler-Verlag, 2011. ISBN 978-0-85729-932-1.

31. Gong, Shaogang, McKenna, J. Stephen a Alexandra, Psarrou. *Dynamic Vision: From Images to Face Recognition.* místo neznámé : Imperial College Press, 2005. ISBN 978-1860941818.

32. Drahanský, Martin. Ábíčko.cz. *Tajemství biometrie 1: Otisky prstů.* [Online] 29. Listopad 2017. [Citace: 30. Leden 2019.] https://www.abicko.cz/clanek/precti-si-technika/22381/tajemstvi-biometrie-1-otisky-prstu.html.

33. Španko, Adrián. Diplomová práce. *Metódy rozpoznávania objektov v obraze.* Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2017.

34. Grother, Patrick a Ngan, Mei. National Institute of Standards and Technology. *NIST IR 8009.* [Online] 26. Květen 2014. [Citace: 29. Leden 2019.] www.nist.com.

35. Grother, Patrick a Ngan, Mai. National Institute of Standards and Technology. *NIST IR 8052.* [Online] Duben 2015. [Citace: 29. Leden 2019.] www.nist.com.

36. Grother, Patrick, Ngan, Mei a Hanaoka, Kayee. National Institute of Standards and Technology. *NIST IR 8238.* [Online] Listopad 2018. [Citace: Leden. 29 2019.] www.nist.com.

37. Panasonic. *New Face PRO.* [Online] 2019. [Citace: 18. Leden 2019.] https://www.security.us.panasonic.com/technologies/facepro.

38. Horník, Petr. Novinky.cz. [Online] 2. Listopad 2012. [Citace: 9. Říjen 2018.] https://www.novinky.cz/zena/styl/282280-iveta-bartosova-zacinam-druhou-pulku-zivota.html.

39. Epstein, Jeniffer. The Spoksmen - Review. [Online] 27. Únor 2017. [Citace: 17. Září 2018.] http://www.spokesman.com/stories/2017/feb/28/trump-blames-obama-for-protests-i-think-hes-behind/.

40. Pxhere. [Online] [Citace: 31. březen 2019.] http:/pxhere.com.

41. Nguyen, Dat Tien, a další. Person Recognition System Based on a Combinationof Body Images from Visible Light andThermal Cameras. *PublMed.gov*. [Online] US National Library of Medicine National Institutes of Health, 16. Květen 2017. [Citace: 15. Duben 2019.] https://www.ncbi.nlm.nih.gov/pubmed/28300783.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

1:1	One - to - one
1:M	One - to - many
2D	Dvourozměrný prostor
3D	Trojrozměrný prostor
AVI	Audio Video Interleave
CCD	Charge Coupled Devices
CCTV	Uzavřený televizní okruh
CIF	Common Intermediate Format
CMOS	Complementary Metal -Oxide-Semiconductor
CPU	Central Processing Unit
CRT	Carthode Ray Tube
DNR	Digital Noise Reduction
DPS	Digital Pixes System
DRAM	Dynamic Random Access Memory
DVR	Digital Video Recorder
F	Clonové číslo ve vztahu k světelnosti
f	Clonové číslo ve vztahu ke cloně
Face ID	Systém rozpoznávání obličeji od společnosti Apple Inc.
FMR	False Match Rate
FNMR	False Non Match Rate
FTP	Foiled Twisted Pair
GB	Giga Byte
Gbps	Gigabit za sekundu
GHz	Giga Hertz
HD	Hight Definition

HDD	Hard Disk Drive
IK krytí	Odolnost proti mechanickému poškození
IP	Intrenet Protokol
IP krytí	Odolnost elektrického zařízení proti vniknutí cizího tělesa a vniknutí kapalin
IR	Infra Red
ISTP	Individual Shielded Twisted Pair
JPEG	Joint Photographic Experts Group
LCD	Liquad Crystal Display
LED	Light Emitting Diode
M:M	Many - to - many
Mbps	Megabit za sekundu
MHz	Mega Hertz
MP4	Multimediální soubor
Mpx	Mega Pixel
NIST	National Institute of Standards and Technology
NTSC	National Television System Committe
NVR	Network Video Recorder
PAL	Phase Alternation by Line
PCI	Peripheral Component Interconnect.
PNG	Portable Network Graphics
PoE	Power over Ethernet
RAID	Redundant Array of Independent Disks
RJ – 45	Zakončení ethernetového konektoru
SD karta	Secure Digital kart
SIF	Standard Interchange Format
STP	Shielded Twisted Pair

USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VCR	Videocassete Recorder
VMS	Video Management System
VPN	Virtual Privat Network
WDR	Wide Dynamic Range
WMV	Windows Media Video

SEZNAM OBRÁZKŮ