

3D čtečky obličeje pro identifikaci osob

A 3D Face Reader for Identification of Individuals

Bc. Stanislav Kovář

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Stanislav Kovář**
Osobní číslo: **A12313**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **3D čtečky obličeje pro identifikaci osob**
Téma anglicky: **A 3D Face Reader for the Identification of Individuals**

Zásady pro vypracování:

1. Vypracujte literární rešerši zaměřenou na biometrickou identifikaci osob.
2. V rámci literární rešerše se zaměřte na možnosti využití obličeje pro identifikaci osob.
3. Provedte základní měření identifikace osob pomocí 3D čtečky obličeje, při měření se zaměřte na spolehlivost použité metody.
4. Provedte měření obličeje pomocí 3D čtečky za různých podmínek, zejména při snížené světelné viditelnosti, při fyzické zátěži člověka.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.
2. BLAŽEK, Vladimír a Radek TRNKA. Lidský obličej: Vnímání tváře z pohledu kognitivních, behaviorálních a sociálních věd. Vyd. 1. Praha: Karolinum, 2009. ISBN 978-80-246-1556-1.
3. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Vyd. 1. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.
4. LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.
5. RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Vyd. 1. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.
6. MARIEB, Elaine Nicpon a Jon MALLATT. Anatomie lidského těla. Vyd. 1. Brno: CP Books, 2005, xvi, 863 s. ISBN 8025100669.
7. JANEČEK, Tomáš. Biometrika[online] [cit. 2014-01-21]. Dostupné z <http://www.nula.wz.cz/biometrika/>.

Vedoucí diplomové práce:

doc. Mgr. Milan Adámek, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

7. února 2014

Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce je zaměřena na biometrické systémy. V teoretické části práce jsou objasněny pojmy související s biometrickými systémy, zabývající se řešením spolehlivosti biometrických systémů a jsou uvedeny příklady některých běžně používaných biometrických zařízení. Praktická část je věnována biometrickému systému Broadway. V závěru práce uvede hodnocení biometrického systému Broadway.

Klíčová slova: biometrie, 3D čtečka obličeje, identifikace, verifikace, registrace, Broadway
3D

ABSTRACT

The thesis is focused on biometric systems. In the theoretical part are explained notions related with biometric systems, following up with solving of reliability of biometric systems and there are mentioned examples of some casually used biometric devices. The practical part is devoted to a biometric system Broadway. In the conclusion he adduces evaluation of the biometrics system Broadway.

Keywords: biometrics, 3D face reader, identification, verification, registration, Broadway
3D

Touto cestou bych rád poděkoval vedoucímu své diplomové práce panu doc. Mgr. Milanu Adámkovi a také paní Ing. Haně Talandové, za odborné rady, vedení a připomínky, které mi pomohly při vypracování této práce.

Prohlašuji, že

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

Prohlašuji,

- že jsem na 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

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 ZÁKLADNÍ POJMY	11
2 SPOLEHLIVOST BIOMETRICKÝCH SYSTÉMŮ	12
2.1 FALSE ACCEPTANCE RATE (FAR).....	13
2.2 FALSE REJECTION RATE (FRR)	14
2.3 FAILURE TO ENROLL (FTE).....	15
2.4 FAILURE TO ACQUIRE (FTA).....	16
2.5 FALSE MATCH RATE (FMR) A FALSE NON-MATCH RATE (FNMR)	16
2.6 EQUAL ERROR RATE (ERR)	17
2.7 RECEIVER OPERATING CHARACTERISTICS (ROC)	18
3 TYPY BIOMETRICKÝCH ČTEČEK	20
3.1 OTISK PRSTU.....	21
3.1.1 Optoelektronické snímače	21
3.1.2 Kapacitní snímače	22
3.1.3 Teplotní snímače	22
3.1.4 Radiofrekvenční snímače	22
3.1.5 Elektroluminiscenční snímače.....	23
3.1.6 Multispektrální snímače	23
3.2 BIOMETRIE KREVNIHO ŘEČIŠTĚ.....	23
3.2.1 Vlastnosti.....	26
3.3 LIDSKÉ OKO.....	26
3.3.1 Duhovka	27
3.3.2 Sítnice.....	29
3.4 BIOMETRIE OBLIČEJE	30
3.4.1 2D čtečky obličeje	31
3.4.2 3D čtečky obličeje	33
3.4.3 Termo čtečky obličeje	36
II PRAKTICKÁ ČÁST	38
4 BROADWAY 3D	39
4.1 WEBOVÝ PROHLÍZEČ	43
4.2 TURNSTILE ENROLLMENT APPLICATION	47
4.2.1 Registrace uživatele.....	54
4.2.2 Identifikace uživatele	55
4.2.3 Verifikace uživatele.....	55
4.2.4 Turnstile mode	56
5 TESTOVÁNÍ BROADWAY 3D	59

5.1	REGISTRACE.....	61
5.2	IDENTIFIKACE.....	63
5.3	VERIFIKACE.....	66
ZÁVĚR		73
ZÁVĚR V ANGLIČTINĚ.....		74
SEZNAM POUŽITÉ LITERATURY.....		75
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		76
SEZNAM OBRÁZKŮ		77
SEZNAM TABULEK.....		78
SEZNAM PŘÍLOH.....		79

ÚVOD

Prudký rozvoj technologie v oblasti biometrických systémů můžeme pozorovat až v posledních letech. Nicméně jejich počátek lze datovat již tisíce let před naším letopočtem. Biometrické charakteristiky jsou unikátní pro každého člověka, proto slouží jako významný prvek při identifikaci dané osoby. Obličej představuje ideální možnost pro určení totožnosti osob, neboť je to jedna z mála částí těla, kterou člověk vystavuje na veřejnosti. Lidé od nepaměti identifikovali jiné osoby podle jejich tváře, očí, nosu, úst a jiných charakteristických prvků. V podstatě lze lidské tělo považovat za biometrický systém, kde oči slouží ke snímání osob a získané informace posílají do mozku. Mozek signály zpracuje a porovná s informacemi uloženými v paměti, které souvisejí s danou osobou. A na základě porovnání údajů následně vyhodnotí, zda je osoba opravdu tou, za kterou se vydává. Tento proces probíhá v hlavě každého člověka prakticky denně, aniž by si to uvědomoval.

Na stejném principu pracují i biometrické systémy, které však mají mnohem větší rozlišovací schopnost než lidské oko a jsou schopny jednoznačně rozlišit části lidského těla. S vývojem technologií začínají biometrické systémy pracovat i s jinými charakteristikami, jako např. otisk prstu, krevní řečiště, sken sítnice a duhovky, apod. Jednotlivé orgány lidského těla jsou nahrazeny konkrétními technickými zařízeními, která vykonávají svou činnost mnohem přesněji. Velké množství místa v paměťových zařízeních uchová větší množství biometrických dat, než kolik by dokázal lidský mozek trvale pojmout. V současné době dokáží biometrické systémy též určit totožnost člověka i bez jeho spolupráce. Uživatelé nejsou tedy systémem nijak omezováni, jako tomu bylo v minulosti.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

Biometrie

Biometrii lze definovat jako vědu, ve které se na základě typických vlastností člověka (otisk prstu, duhovka, sítnice, atd.) identifikuje nebo autorizuje konkrétní osoba. Biometrie se rozděluje na fyziologickou a behaviorální (biometrii chování). Fyziologická biometrie vychází z výše uvedených jedinečných lidských vlastností, kterými každá osoba disponuje od svého narození. Naopak u biometrie chování se zkoumají charakteristické rysy konkrétní osoby, např. styl písma, dynamika podpisu, stisk kláves, apod.

Verifikace

Jedná se o porovnání uživatele žádajícího o přístup s uživateli uloženými v databázi. Uživatel prokáže svou identitu pomocí identifikačního média (token, čip) nebo hesla a následně poskytne své biometrické údaje. Protože uživatelé používají identifikační média, databáze nemusí prohledávat všechny uložené biometrické prvky, ale pouze údaje vztahující se ke konkrétnímu uživateli. Tím se zamezuje možnosti vstupu kradenou kartou nebo heslem. Jde tedy o porovnání 1:1, protože jeden biometrický údaj se porovnává pouze s jedním biometrickým údajem.

Identifikace

Na rozdíl od verifikace, se u identifikace uživatel neproказuje identifikačním médiem ani heslem, ale pouze biometrickými údaji. Tyto údaje se po sejmutí porovnávají se všemi biometrickými údaji uloženými v databázi. Identifikace je tedy porovnání 1:N.

Matching

Matching nebo-li srovnání, je stupeň shody mezi posuzovanými biometrickými vzorky. Výsledek srovnání se potom nazývá score. To udává, zda je vzorek shodný či nikoli. Při srovnávání biometrických vzorků nikdy nedochází ke stoprocentní shodě, proto musí být stanovena určitá hranice, po kterou je údaj vyhodnocen jako vyhovující.

Biometrický vzorek

Jedná se o data, která byla získána biometrickým zařízením a reprezentují charakteristické biometrické vlastnosti člověka.

2 SPOLEHLIVOST BIOMETRICKÝCH SYSTÉMŮ

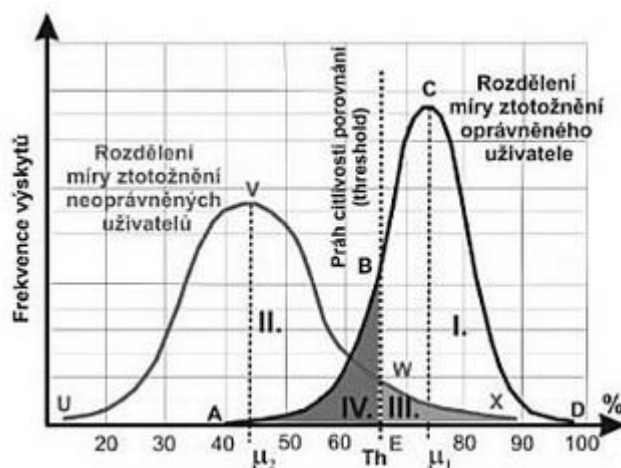
Informace pro vypracování této kapitoly byly získány ze zdrojů [1] a [5], není-li uvedeno jinak.

V současné době existuje mnoho výrobců biometrických systémů uvádějících na trh své produkty. Zákazník si tedy podle svých kritérií může vybrat systém, který bude nejlépe vyhovovat jeho účelu. Mezi taková kritéria patří bezesporu cena systému, která bude mít vždy svou důležitou roli, dále uživatelská přívětivost, kapacitní možnosti (počet možných realizací verifikace a identifikace uživatelů za určitý časový interval), odolnost, životnost apod. Ovšem nejdůležitější vlastností celého biometrického systému je spolehlivost, resp. správné rozeznání oprávněného a neoprávněného uživatele. Systém, který nedokáže správně rozpoznat nebo ověřit autorizovaného uživatele, nelze z bezpečnostního hlediska považovat za důvěryhodný (spolehlivý). Spolehlivost se odvíjí od kvality zařízení, resp. technologie použité pro snímání biometrických vzorků a jeho uchování v databázi. Ovlivňuje jí také způsob snímání vzorků uživatele. Při kontaktním snímání může na snímací ploše zůstat vzorek předešlého uživatele, mastnota, prach, což usnadňuje vznik problémů s následným přijetím a odmítnutím. V případě otisku biometrického vzorku může navíc dojít ke zneužití pro podvodné účely.

Při porovnání dvou biometrických prvků nikdy nedochází ke stoprocentní shodě, proto se musí stanovit hranice, pro kterou jsou vzorky systémem vyhodnoceny jako správné či nikoli. Výsledky score se liší i v závislosti na použité biometrické aplikaci a na technickém řešení. Vyjádření pravděpodobnosti přijetí či odmítnutí se realizuje grafickým zobrazením v histogramu. Vychází se ze dvou křivek, první (A, B, C, D) prezentuje četnost úspěšného přijetí uživatele při identifikaci, resp. verifikaci, druhá křivka (U, V, W, X) vyjadřuje četnost pokusů o proniknutí neoprávněné osoby. Do grafu se zanese příčka BE (kolmá na osu x) značící práh citlivosti a spolu s křivkami rozdělí plochu grafu na čtyři oblasti (v grafu označeny římskými čísly I. - IV.). Pro vzniklé oblasti platí:

- 1) Oblast I. (vytvořena body E, B, C, D, E) odpovídá tzv. korektnímu přijetí autorizovaného uživatele. Uživatel byl rozpoznán a byl mu umožněn přístup.
- 2) Oblast II. (dána body U, V, W, E, U) reprezentuje tzv. korektní odmítnutí neautorizovaného uživatele. Systém odolal pokusu o vniknutí neoprávněnou osobou.

- 3) Oblast III. (určena body E, W, X, E) představuje tzv. nekorektní přijetí neautorizované osoby. Systém nelze považovat za bezpečný, jestliže umožňuje rozpoznat neoprávněného uživatele.
- 4) Oblast IV. (vytvořená z bodů A, B, E, A) značí tzv. nekorektní odmítnutí autorizovaného uživatele. Uživatel nebyl systémem rozpoznán, tudíž systém nelze považovat za spolehlivý.



Obrázek 1: Scóre porovnání [1]

Pro vyjádření pravděpodobnosti chybného přijetí či odmítnutí, se v praxi zavedly termíny False Acceptance Rate (FAR) a False Rejection Rate (FRR).

2.1 False Acceptance Rate (FAR)

Neboli pravděpodobností chybného přijetí se rozumí bezpečnostní kritérium biometrického systému. Udává pravděpodobnost, že budou dva odlišné biometrické vzorky (vzorek právě získaný a vzorek uložený v databázi) posouzeny biometrickým systémem jako shodné a tím povolen přístup neoprávněné osobě. Taková situace je z hlediska bezpečnosti nežádoucí a vyžaduje oprávnění k provedení eliminace rizika chybného přijetí systému.

Pro výpočet pravděpodobnosti chybného přijetí v případě identifikace lze použít následující vzorec:

$$FAR = \frac{N_{FA}}{N_{IA}} \cdot 100 [\%],$$

kde N_{FA} představuje počet chybných přijetí a N_{IA} počet pokusů neautorizovaných uživatelů o identifikaci.

V případě výpočtu FAR pro verifikaci uživatelů vypadá vzorec obdobně:

$$FAR = \frac{N_{FA}}{N_{IA}} \cdot 100 [\%],$$

kde N_{IVA} vyjadřuje počet pokusů neautorizovaných uživatelů o verifikaci.

Hodnotu pravděpodobnosti chybného přijetí lze získat i z histogramu (Obrázek 1) uvedeného v kapitole Spolehlivost biometrických zařízení. Kdy do čitatele je dosazena hodnota oblasti III. a do jmenovatele plocha definována body U, V, X, U. Výsledný vzorec tedy bude vypadat následovně:

$$FAR = \frac{P_{III}}{P_{U,V,X,U}} \cdot 100 [\%].$$

2.2 False Rejection Rate (FRR)

FRR vyjadřuje pravděpodobnost chybného odmítnutí autorizovaného uživatele biometrickým systémem. Na rozdíl od případu FAR, FRR nepředstavuje bezpečnostní ohrožení, pouze tak říkajíc znepríjemňuje uživateli život. Pokud nastane situace, že nedojde ke shodě získaného biometrického vzorku a šablony uložené v databázi, musí uživatel znovu prokázat svou identitu a vyčkat na vyhodnocení systémem. Takové situace mohou nastat, jestliže není prováděná pravidelná údržba zařízení, nebo pokud došlo k poškození uloženého vzorku.

Pravděpodobnost chybného odmítnutí autorizovaného uživatele je definována, stejně jako v případě FAR, jak pro identifikaci, tak pro verifikaci a to následovně:

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

kde N_{FR} vyjadřuje počet chybných odmítnutí systémem a N_{EIA} počet pokusů autorizovaných uživatelů o identifikaci.

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

kde N_{EVA} prezentuje počet pokusů autorizovaných osob o verifikaci.

Vyjádření vztahu FRR z grafického zobrazení (Obrázek 1) v kapitole Spolehlivost biometrických zařízení, je dáno jako poměr oblasti IV. a plochy ohraničené body A, B, C, D, A. Vzorec tedy vypadá, takto:

$$FRR = \frac{P_{IV}}{P_{A,B,C,D,A}} \cdot 100 [\%].$$

2.3 Failure to Enroll (FTE)

Při stanovení FAR a FRR je vhodné mít k dispozici dílčí informace (důvody proč došlo k chybám), podle kterých lze přesněji stanovit výslednou spolehlivost biometrického systému. Jedním z příkladů je FTE neboli pravděpodobnost neúspěšného sejmutí biometrického vzorku. V některých případech se uživatel není schopen se zaregistrovat do systému, což může být způsobeno fyziologickými anomáliemi. Příkladem může být absence článků prstů či celých prstů, omezená kontrola orgánů očí (šilhavost), apod. FTE tedy udává poměr uživatelů, u nichž není možné získat biometrický vzorek. Nejedná se o stálou veličinu a lze jí stanovit pro konkrétního uživatele i konkrétní fyziologickou vlastnost. FTE pro jednu osobu (biometrickou vlastnost) lze vypočítat podle následujícího vztahu:

$$FTE = \frac{N_{UA}}{N_{TA}} \cdot 100 [\%],$$

kde N_{UA} vyjadřuje počet neúspěšných pokusů jednoho uživatele a N_{TA} celkový počet pokusů.

Pravděpodobnost neúspěšného sejmutí vzorku více uživatelů se získá podle vzorce:

$$FTE = \frac{1}{n} \cdot \sum_{i=1}^n FER(i),$$

kde n značí počet uživatelů a $FER(i)$ pravděpodobnost neúspěšného sejmutí vzorku jedné osoby.

Výsledky jsou úměrné počtu provedených pokusů, čím více pokusů bude, tím spolehlivější informace budou získány.

2.4 Failure to Acquire (FTA)

Koeficient selhání přístupu definuje situaci, kdy je uživatel schopen se zaregistrovat se do systému, ovšem při následné identifikaci nebo verifikaci není systémem přijat. To může nastat z důvodu nedostatečného množství charakteristických znaků biometrického vzorku. Chyba může být částečná (malé zranění, nesprávná údržba biometrického zařízení, vliv okolí, atd.) nebo trvalá (operace). Trvalá chyba vyžaduje nasnímání nového referenčního vzorku, který se uloží do databáze. Výsledná hodnota FTA je ovlivněna stanovenou prahovou hodnotou vstupního signálu nebo obrazu a vypočítá se dle vzorce:

$$FTA = \frac{N_{US}}{N_{TS}} \cdot 100 [\%],$$

kde N_{US} vyjadřuje počet neúspěšných snímání a N_{TS} celkový počet snímání biometrických vzorků.

2.5 False Match Rate (FMR) a False Non-Match Rate (FNMR)

FMR vyjadřuje pravděpodobnost, že určitý biometrický vzorek bude chybně systémem vyhodnocen při identifikaci či verifikaci jako správný. Naopak FNMR udává pravděpodobnost vzniku situace, při níž bude vzorek autorizované osoby chybně vyhodnocen jako nesprávný. Výpočet FMR je dán vzorcem:

$$FMR = \frac{N_{ILIS}}{N_{TM}} \cdot 100 [\%],$$

kde N_{ILIS} představuje počet nesprávně označených identických biometrických vzorků a N_{TS} celkový počet srovnání.

FNMR se zjišťuje obdobně, jen do čitatele se tentokrát umístí hodnota počtu nepravděpodobně označených odlišných vzorků:

$$FNMR = \frac{N_{ILDS}}{N_{TM}} \cdot 100 [\%].$$

FMR a FNMR jakožto dílčí výpočty (informace) mají pevnou vazbu na FAR a FRR a při zjišťování pravděpodobnosti chybného přijetí nebo odmítnutí se s nimi pracuje. Při znalosti FMR a FTA lze pro potřeby verifikace určit hodnotu pravděpodobnosti FAR, podle vztahu:

$$FAR = FMR \cdot (1 - FTA).$$

Stejně jako pravděpodobnost chybného přijetí, tak i pravděpodobnost chybného odmítnutí pro případ verifikace uživatelů se znalostí hodnot FNMR a FTA lze vypočíst podle vzorce:

$$FRR = FTA + FNMR \cdot (1 - FTA).$$

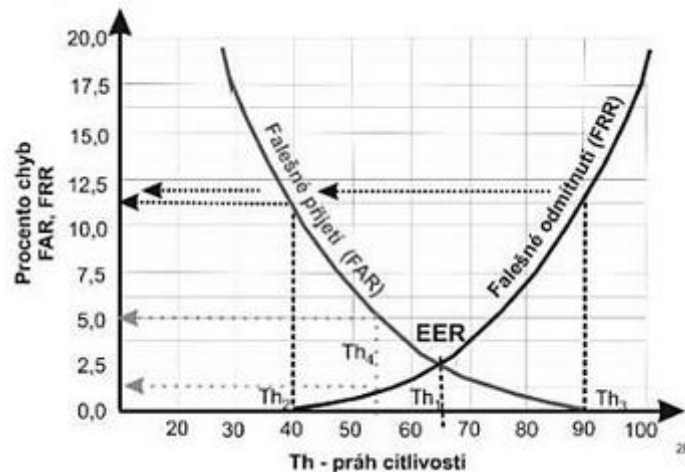
2.6 Equal Error Rate (ERR)

Křížový koeficient (ERR) udává ideální rozložení pravděpodobnosti chyb FAR a FRR (Obrázek 2) a zároveň musí pro vzniklý bod platit následující rovnost:

$$FRR \cdot ERR = FAR \cdot ERR \Rightarrow FRR = FAR.$$

V ideálním případě by byly hodnoty pravděpodobnosti chybného přijetí a odmítnutí nulové, tzn. systém by byl dokonalý. Nedocházelo by k žádným chybným přijetím neautorizovaných osob či odmítnutím autorizovaných uživatelů. V praxi ovšem ideální systém neexistuje, proto je důležité vyhledat rovnovážný stav mezi bezpečností a použitelností biometrického systému. Obrázek 2 ukazuje, jak bude vypadat průběh FAR, resp. FRR při různém nastavení prahové hodnoty citlivosti. Jestliže bude FAR rovno nule, systém lze považovat za velice bezpečný, ale hodnota FRR bude přibližně na 12%, tedy 12% oprávněných uživatelů bude systémem chybně vyhodnoceno jako neoprávněná osoba (Obrázek 2). Naopak pokud bude FRR nastaveno na hodnotu 0, lze systém považovat za spolehlivý, nebude docházet k chybným odmítnutím, ale systém nebude bezpečný. Obrázek 2 v takovém případě udává pravděpodobnost chybných přijetí blízká se hodnotě 11%, což představuje bezpečnostní problém. Ve skutečnosti je průběh křivek FAR a FRR více dynamický, než je uvedeno na Obrázku 2, dané zobrazení je použito pro snadnější pochopení problematiky.

Znalost průběhu křivek FAR a FRR v závislosti na hodnotě prahu je nezbytná pro přesné stanovení spolehlivosti a bezpečnosti systému. V mnohých případech výrobci garantují hodnoty pravděpodobnosti chybného přijetí a odmítnutí blízké nule (např. FAR=0,01%, FRR=0,02%), což může být zkreslené. Pro výrobce je stanovení nízké hodnoty výhodné, ale uživatel nemá bez znalosti průběhu FAR a FRR možnost si je ověřit.



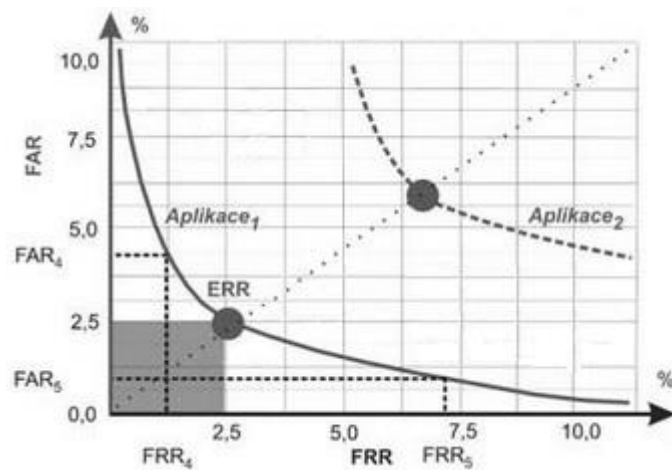
Obrázek 2: Závislost FAR a FRR [1]

Nastavení FRR a FAR se liší podle požadavků zákazníka. Pokud je pro zákazníka prioritou bezpečnost, stanoví pro svůj systém kritérium, aby se pravděpodobnost chybného přijetí blížila nule nebo jí byla rovna. Musí ovšem počítat se situací, kdy budou autorizovaní uživatelé systémem odmítání. Naopak jestliže je pro zákazníka prioritou spolehlivost stanoví hodnotu FRR blízkou nebo rovnu nule. V takovém případě, nebude systém bezpečný a zákazník musí počítat s možností vniknutí nepovolaných osob.

2.7 Receiver Operating Characteristics (ROC)

Prahová operační charakteristika souvisí s předcházející podkapitolou. ROC vyjadřuje vzájemný vztah mezi pravděpodobností chybného přijetí a odmítnutí, kdy protnutím křivek chyb vznikne bod ERR. Jinak řečeno prahová operační charakteristika slouží k posouzení kvality příslušného biometrického zařízení.

ROC se určuje podle podmínek, pro jaké má být biometrická aplikace využita. Jak již bylo uvedeno v předcházející podkapitole, kritéria uživatelů se liší. Kritérium bezpečnosti vyžaduje nízkou hodnotu FAR, naopak kritérium spolehlivosti zase spoléhají na nízké FRR. Ale existují i situace (např. bankomaty, počítače, mobilní telefony), kdy je potřeba, aby byly obě hodnoty co nejnižší. V takových případech musí křivka ROC procházet pomyslným čtvercem umístěným v levém dolním rohu na Obrázku 3.



Obrázek 3: Receiver operating characteristics [1]

3 TYPY BIOMETRICKÝCH ČTEČEK

Informace k úvodní části této kapitoly byly čerpány ze zdroje [2], není-li uvedeno jinak.

Jak již bylo napsáno v první kapitole, existuje velké množství možností, jak identifikovat, resp. verifikovat osobu. Proto trh disponuje širokou škálou různých typů biometrických čteček a záleží jen na zákaznících, kterou variantu zvolí. Každá metoda má své klady i zápory, které musí být před realizací důkladně zhodnoceny, ne každý typ čteček se hodí všude. Zpravidla se volí jako součást přístupových systémů zajišťujících především zvýšení bezpečnosti a komfortu uživatelů. Velký rozmach zaznamenaly biometrické systémy v oblasti počítačové techniky prostřednictvím čteček otisků prstů, které usnadňovaly uživateli přístup do systému, bez nutnosti pamatování si hesla. S touto možností poprvé přišla v roce 2001 společnost IBM v notebookech řady ThinkPad. V dnešní době už jsou čtečky otisků prstů běžně podporované téměř ve všech notebookech. Jedná se ovšem o výjimečný případ nasazení čteček otisku prstu. V přístupových systémech dochází k jejich nahrazení efektivnějšími biometrickými čtečkami, např. 3D čtečkami obličeje.

Základní princip je u všech typů biometrických systémů stejný, liší se jen způsoby snímání fyziologických vlastností člověka. Aby byl systém schopen rozpoznat nebo ověřit uživatele, musí mít v databázi uložený referenční (biometrický) vzorek příslušné biometrické charakteristiky. Výsledný biometrický vzorek se zpravidla získává zprůměrováním více vzorků, aby se eliminovaly možné chyby při identifikaci a verifikaci. K tomuto výslednému referenčnímu vzorku se přiřadí identifikátor, který vzorek jednoznačně propojí s konkrétní osobou, čehož se využívá u ověřování uživatelů. Vzorek se uloží do databáze, která se může nacházet:

- V biometrickém čtecím zařízení – což umožňuje rychlou reakci při vyvolání požadavku na zpřístupnění vzorku a odpadá nutnost zabezpečení spojení k jiným externím úložným zařízením, jak je tomu u dalších variant. Nevýhodou zůstává fakt, že všechny uložené vzorky jsou závislé na funkčnosti čtecího zařízení, tzn. při poruše se poškodí i databáze biometrických vzorků a je potřeba znovu projít procesem ukládání.
- Ve vzdálené centrální databázi – biometrické vzorky se nacházejí v databázi mimo biometrické čtecí zařízení, ale jsou vzájemně propojeny. Při poškození čtecího

zařízení tedy nedojde ke ztrátě vzorků. Avšak na rozdíl o předešlé metody je nezbytné zabezpečit spojení k vzdálenému uložení, protože výpadek spojení mezi biometrickým čtecím zařízením a centrální databází by znamenalo vyřazení systému z činnosti.

- V přenosných tokenech – uživatel si přenáší biometrický vzorek prostřednictvím tokenů (čipové karty, apod.). Odpadá potřeba tvorby databáze (centrální i lokální) a tedy i s ní spjaté problémy. Nevýhoda spočívá v ceně a realizaci, jelikož je velmi technologicky náročné integrovat biometrické čtecí zařízení a token v rámci jednoho funkčního celku. Navíc hrozí nebezpečí ztráty nebo krádeže tokenu, čímž by útočník získal možnost neomezeného pohybu v rámci daného bezpečnostního systému.
- Kombinace metod – eliminace nevýhod předcházejících metod, čímž lze dosáhnout vyšší efektivity a bezpečnosti biometrického systému.

Po vysvětlení základních informací, nezbytných pro pochopení biometrických systémů, je možné přejít k podstatě této kapitoly. Cílem kapitoly je popsat jednotlivé typy fyziologických biometrických čteček.

3.1 Otisk prstu

Snímání otisků prstu je jednou z nejstarších a nejjednodušších metod identifikace konkrétních osob. Základem metody je snímání papilárních linií na vnitřní straně rukou a nohou. Metoda snímání otisků prstů se začala poprvé používat koncem 19. století, kdy byly definovány charakteristické body na prstech. Na prst byla nanesena vrstva inkoustu a následně natištěna na papír tak, aby vynikly jednotlivé linie prstu. V dnešní době se takové postupy nevyužívají, celý proces je totiž zmodernizován. K dispozici je na trhu velké množství snímačů otisků prstů, pracujících na různém principu.

3.1.1 Optoelektronické snímače

Celý princip činnosti snímání otisku prstu optoelektronickým biometrickým snímačem je založen na rozdílném odrazu světla. Nebo-li, jde o rozptyl světla mezi rozhraním snímací plochy hranolu a přiloženým prstem. Pro přesnější snímání prstu je pod povrchem dotykové plochy (tam kam přikládáme prst) přidána vrstva fosforu, čímž dojde k osvětlení

celé plochy prstu. Světlo odražené od povrchu prstu, pak prochází luminoformní vrstvou do maticového CCD detektoru, kde se vytvoří obraz snímaného prstu, který je následně digitalizován. Nakonec dojde ke zpracování algoritmem pro rozpoznávání obrazu.

Při snímání je třeba udržovat dotykovou plochu čistou, při dotyku prstu s plochou na ploše zůstávají otisky, což může zkomplikovat další snímání. K tomu dochází především v případech, kdy jsou voleny levnější snímače nebo nedochází k pravidelné údržbě biometrické čtečky. Jinak jsou ovšem optoelektronické biometrické snímače jednou z nejkvalitnějších technologií využívajících se v oblasti biometrických zařízení.

3.1.2 Kapacitní snímače

Tyto snímače mají velmi jednoduchý princip funkčnosti. Činnost kapacitního snímače je založena na rozdílu kapacity mezi deskou snímače a povrchem snímaného prstu. Prst se přikládá na citlivou plochu, která obsahuje velké množství mikroelektrod. Tyto mikroelektrody následně kapacitně převedou otisk snímaného prstu na digitální obraz, jenž se dále zpracovává.

V porovnání s optoelektronickými snímači jsou kapacitní biometrické snímače velmi malé, při srovnatelné kvalitě snímání otisků prstů. Nevýhodou je nízká odolnost vůči statické elektřině, což má vliv na nižší životnost snímače. Z pravidla je nutná výměna snímače po 3 letech činnosti.

3.1.3 Teplotní snímače

Základem teplotních biometrických snímačů je pyrodetektor, jenž umožňuje měřit rozdíl tepelné energie prstu v okamžiku, kdy se dotkne povrchu snímací plochy. Výsledný otisk prstu se získá složením jednotlivých částí otisků ve formě digitálního pásu. Nevýhodou tohoto snímání je nutnost, přejíždět prstem po snímací ploše vícekrát, což může způsobit, že je vždy snímána jiná část prstu a tím pádem se jednotlivé části prstu mohou překrývat a vznikne úplně nový a neznámý otisk.

3.1.4 Radiofrekvenční snímače

U radiofrekvenčních biometrických snímačů se využívá generátoru střídavého signálu, který je přiveden na snímač a na plochu otisku snímaného prstu. Mezi těmito plochami vzniká elektrické pole, které se v případě snímání otisku prstu, změní tak, aby kopírovalo

tvar papilárních linií snímaného prstu. Po přiložení prstu dochází ke zvlnění elektrického pole a na senzory potom dopadá signál s rozdílnou velikostí. Snímání výběžků odpovídá vyšší úrovni signálu, zatímco prohlubně jsou charakterizovány signálem o nižší úrovni. Tyto snímače pořizují několik snímků, které jsou optimalizovány do výsledné podoby a následně vyhodnoceny.

3.1.5 Elektroluminiscenční snímače

Základem elektroluminiscenčních biometrických snímačů je snímací plocha tvořená několika vrstvami, přičemž nejdůležitější je v tomto případě světlo vyzařující vrstva. Po přiložení prstu na snímací plochu, tato vrstva eliminuje světlo v místech, kde na ní tlačí papilární linie snímaného prstu. Obraz otisku prstu je zpracován pomocí fotodiod a zobrazen v digitální formě. Velkou výhodou elektroluminiscenčních snímačů je výborné rozlišení snímání. Nevýhodou malá odolnost vůči mechanickým poškozením a velká náchylnost na znečištění.

3.1.6 Multispektrální snímače

Multispektrální biometrické snímače se nemusí omezovat pouze snímáním povrchu prstu, ale jsou schopny snímat a zpracovávat vlastnosti celého snímaného prstu, tedy i jeho vnitřní strukturu. Hlavními částmi senzoru multispektrálního snímače jsou zdroj světla a zobrazovací systém. Světlo umožňuje ozařovat snímaný prst světlem o různých vlnových délkách. Tím získáme více identifikačních údajů o prstu.

Oproti jiným biometrickým snímačům otisku prstu jsou multispektrální snímače odolné vůči extrémním vnějším podmínkám (voda, externí zdroje světla, atd.). V případě znečištěných prstů nebo nedostatečného přiložení prstu na snímanou plochu jsou snímače s multispektrální technologií schopny tyto nedostatky odstranit a zabránit odmítnutí oprávněného uživatele na rozdíl od jiných snímačů. Multispektrální snímače využívají principy spektrální analýzy a zabraňují tím možnosti falešných přístupů.

3.2 Biometrie krevního řečiště

Informace pro vypracování této kapitoly byly získány ze zdroje [4], není-li uvedeno jinak.

Dalším způsobem identifikace a verifikace uživatele je metoda pomocí krevního řečiště. Jde o jednu z nejmodernějších metod v oblasti biometrických systémů. Vyznačuje se svou bezpečností, jelikož není možné zfalšovat síť cév uvnitř ruky. Tvar krevního řečiště se člověku v průběhu života nemění a je unikátní pro každého jedince. Ani u identických dvojčat není síť cév stejná. Viditelnost žilní sítě ovlivňuje celá řada faktorů, např. věk, aktivita, množství podkožního tuku, pigmentace kůže, atd. U této biometrické metody lze skenovat dlaň, hřbet ruky nebo jen jeden prst. Snímání se provádí bezkontaktně, tzn. nelze ze snímací plochy získat žádné skryté dodatečné informace.

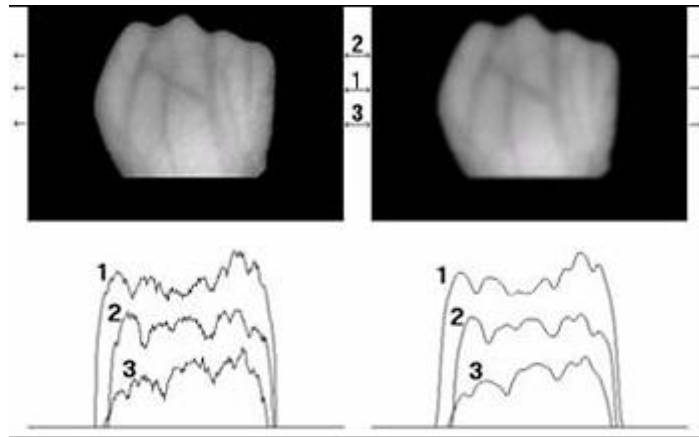
Biometrické systémy pracující na principu snímání krevního řečiště využívají speciální (CCD) kameru a zdroj infračerveného záření, resp. spektrum blízké se IR záření. Kamera zaznamenává černobílý obraz tvaru žil viditelných pod IR zářením. V žilách se nachází odkysličený hemoglobin, který absorbuje světlo a tím dochází k zvýraznění struktury žil od zbylé části ruky. IR záření proniká pouze 3mm pod kůži, tedy jen do míst kde se nachází síť cévního řečiště. Snímaný obraz je dále převeden do digitální formy, přičemž se ukládají pouze důležité prvky (vlastnosti) obrazu krevního řečiště. Konkrétně se jedná o tloušťku žil, body a úhly jednotlivých větvení žil. Po získání obrazu krevního řečiště se přechází na další fáze rozpoznání struktury cévního řečiště, jde o:

- **členění obrazu** – cílem je rozdělit výsledný obraz na části, tedy v tomto případě na část ruky a část pozadí. Na Obrázek 4 je uvedeno, jak členění obrazu vypadá. První část je zaměřena na zobrazení ruky a cévního řečiště, v druhé části je snímek ruky nahrazen bílou barvou, aby bylo zvýrazněno pozadí, poslední část je v podstatě výstup prvních dvou.



Obrázek 4: Segmentace [4]

- **vyhlazení obrazu a redukce šumu** – tento krok slouží k úpravě obrazu žilní sítě ruky a odstranění nedostatků obrazu plynoucí z tvaru povrchu ruky. Užívá se různých obrazových filtrů dle potřeby, např. nelineární rozptýlení nebo Gaussovské rozmazání, apod.



Obrázek 5: Ukázka vyhlazení obrazu [4]

- **lokální prahování** – jde v podstatě o vyjmutí struktury krevního řečiště z obrazu. Výsledkem tohoto kroku tedy bude tvar řečiště na bílém pozadí, tzn. bude jasně viditelná jeho struktura připravená k porovnání. Vychází se z histogramu, kdy je stanovena mezní hodnota (práh) a následně se vyhledávají všechny hodnoty jasu nižší, resp. vyšší než je hodnota prahu. Hodnota prahu se určí jako průměrná hodnota všech okolních pixelů. Nižší hodnoty jasu odpovídají pozadí obrazu a vyšší hodnoty popředí obrazu. V praxi existuje několik metod jak oddělit krevní řečiště od zbytku obrazu, patří sem členění: prahováním, pomocí hran, pomocí oblastí a porovnáním.



Obrázek 6: Lokální prahování [4]

- **postprocessing** – po dokončení všech předešlých úprav je k dispozici obrázek s jasně vyjádřenou strukturou žil, který lze považovat za výchozí šablonu. Šablona se uloží do databáze systému a slouží jako podklad pro provádění následných verifikací uživatelů.



Obrázek 7: Postprocessing [4]

3.2.1 Vlastnosti

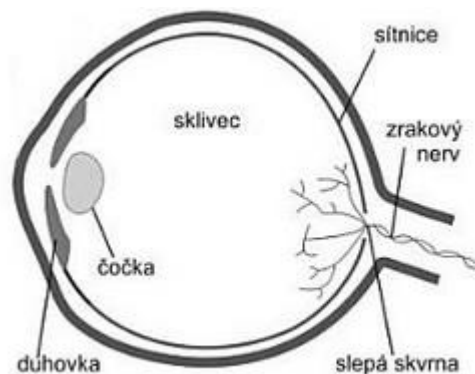
- Správné provedení verifikace neohroží případné šperky (prsteny), onemocnění kůže na rukou, apod.
- Výhoda spočívá v nemožnosti oklamání těchto biometrických systémů různými duplikáty, jako tomu bylo u čteček otisků prstů.
- Nízké riziko pravděpodobnosti chybných odmítnutí (10^{-1} %) či přijetí (10^{-4} %).
- Zpracování biometrickými systémy je velmi rychlé, snímání je provedeno do 0,5 sekund.
- Stálost struktury žil dovoluje použít jednoduché algoritmy.
- Síť cév zajišťuje stabilní a dostatečně velký biometrický rys.

3.3 Lidské oko

Informace pro zpracování této podkapitoly byly čerpány ze zdroje [1] a [10], není-li uvedeno jinak.

Lidské oko patří k mnoha orgánům, které jsou vhodné pro využití biometrickými systémy. Oko je dokonalý a velice složitý systém, jehož jednotlivé části musí spolupracovat v rámci celku. Pro potřeby biometrických systémů se využívají pouze dvě části lidského oka, konkrétně duhovka a sítnice. Samotný fakt, že se obě části nacházejí uvnitř orgánu (duhovka v popředí a sítnice v pozadí), vylučuje možnost duplikace. Lidské oko je párový orgán, jehož výjimečnost spočívá ve skutečnosti, že ani oči daného člověka nejsou stejné. Proto není možné biometrické systémy pracující na principu skenování duhovky resp.

sítnice, nijak oklamat. Samotný fakt, že obě části se nacházejí uvnitř orgánu (duhovka v popředí a sítnice v pozadí) oka, vylučuje možnost duplikace.



Obrázek 8: Schéma lidského oka [1]

- Sklivec – průhledná, rosolovitá hmota, která se nachází uvnitř oka.
- Čočka – průhledná bikonvexní spojka uvnitř oka, kde ve spolupráci s rohovkou upravuje lom světla tak, aby směřoval na sítnici.
- Zrakový nerv – velké množství nervových vláken vedoucí do ústředního nervového systému.
- Slepá skvrna – místo v sítnici, kde nerozvětvený zrakový nerv ústí do oční bulvy.
- Duhovka a sítnice budou detailněji rozebrány v dalších částech této podkapitoly.

3.3.1 Duhovka

První z metod, kterou biometrické systémy využívají pro rozpoznání resp. ověření uživatele, je duhovka. Jak již bylo uvedeno, duhovka je část oka, která obsahuje nejvíc rozlišovacích znaků ze všech metod (až 250 detailů). Na rozdíl od sítnice je po celý život člověka neměnná, ve většině případů ji neovlivní ani nemoci (zákaly, apod.), tudíž ji není možné nijak duplikovat. Struktura duhovky je velmi složitá a je tvořena množstvím charakteristických znaků (orientace, prstence, koróny, rýhy, skvrny, apod.). Právě tyto charakteristické znaky jsou podstatné pro činnost systému, protože jsou zcela náhodné u každého jedince. Biometrické systémy na bázi skenování duhovky lze považovat za jedny z nejpřesnějších. Jako důkaz lze uvést ověřené tvrzení, že pravděpodobnost nalezení dvou stejných duhovek je zhruba 1050x menší, než pravděpodobnost nalezení dvou identických otisků prstu.

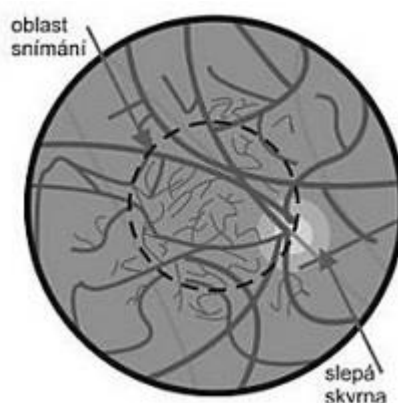
Duhovka se vyznačuje nehomogenní strukturou, což má za následek vznik malého (anulus iridis minor) a velkého (anulus iridis major) prstence na přední straně oka. Duhovka je složena z 6 částí (vrstev) z nichž nejdůležitější jsou vrstvy svalová a pigmentová. Svalová vrstva, která obsahuje svěrač a rozšiřovač zornice, slouží k regulaci světla přiváděného do oka. Pigmentová vrstva určuje zbarvení duhovky na základě množství uloženého pigmentu. Princip činnosti těchto biometrických systémů je v podstatě stejný jako v předchozích případech. Základem je zdroj IR záření a standardní CCD kamera, která snímá duhovku oka osvětlenou infračerveným světlem. K dispozici je polopropustné zrcátko, které umožňuje kontrolovat pohyb oka, dokud není alespoň částečně stabilizován a následně se provede snímání. Charakteristické znaky duhovky jsou během snímání převáděny do digitální podoby a uchovávány v databázi systému, kde při prvním snímání slouží jako šablony konkrétní osoby. Proces verifikace či identifikace uživatelů lze provádět různými metodami. První metodou je porovnání dvou duhovek, jako klasických obrázků, tzn. získaný snímek se porovnává s šablonou a následně se vyhodnocuje shoda. V případě identifikace je tato metoda náročná, protože jeden snímek duhovky se musí postupně porovnávat se všemi snímky v databázi. Druhá metoda spočívá v pokrytí celého snímku duhovky sítí křivek. Z hodnot jasů jednotlivých bodů všech křivek se vytvoří (např. pomocí Gaborovy vlnkové transformace) kód duhovky o velikosti 256 – 1024B. Další variantou je transformace, tedy přenesení charakteristických znaků do soustavy polárních souřadnic. Při porovnávání biometrických vzorků se užívá vzájemné souvztažnosti kódů duhovky nebo výpočtů pro zjištění Hammingovy vzdálenosti mezi dvěma kódy. Celý proces probíhá bezkontaktně, přičemž vzdálenost duhovky od čtečky je garantována v rozmezí 10 cm až jednotek metrů, podle výrobce zařízení.

Problémy mohou nastat, jestliže uživatel trpí opakovanými záněty duhovek, či prodělal operaci duhovky, v takovém případě je nutné provést nové snímání duhovky za účelem získání nové šablony. Oční onemocnění mohou způsobit změnu průhlednosti očních médií nebo změnu charakteristických znaků duhovky. Další problémy mohou způsobovat oční vady jako např. šilhavost nebo nystagmus, kdy dochází k nekontrolovatelnému pohybu oční bulvy, což komplikuje skenování duhovky. Brýle a kontaktní čočky u kvalitnějších zařízení nepředstavují problém a systém si s nimi lehce poradí.

3.3.2 Sítnice

Biometrické systémy snímající sítnici lidského oka jsou velice efektivní a využívají se především v institucích s vysokými bezpečnostními požadavky. Sítnice obsahuje fotoreceptory, což jsou v podstatě buňky citlivé na světlo. Ty převádí energii dopadajícího světla na nervové signály, které posílají nervovými soustavami do mozku. Fotoreceptory se z hlediska barevných podnětů dělí na tyčinky a čípky. Čípky (asi 6,5 milionů) jsou určeny pro barevné vidění během dne, tyčinky (cca 120 milionů) naopak umožňují černobílé vidění v noci. Centrem sítnice je makula, též nazývaná jako žlutá skvrna, která obsahuje největší množství receptorů, proto je zde obraz nejostřejší. V blízkosti žluté skvrny se nachází slepá skvrna, která je protikladem makuly. Jde o místo, kde dochází k propojení zrakového nervu a oční bulvy, tzn. nerv není rozvětven na jednotlivá vlákna a neobsahuje žádné fotoreceptory.

Princip snímání sítnice spočívá v získání obrazu struktury nervové soustavy z oblasti choroidu na pozadí oka v okolí slepé skvrny (viz. Obrázek 9). Využívá koherentního zdroje infračerveného záření o nízké intenzitě (nervový systém rychle vstřebá IR záření) a optoelektický systém (jen jedna LED dioda, čím se sníží riziko z poškození oka ozářením). Výsledný obraz se převede do digitální podoby pro další zpracování či uložení. Při verifikaci musí uživatel sledovat konkrétní bod ve vymezeném prostoru, dokud nedojde k zaostření a stabilizaci oka. Tento způsob ověřování může být pro některé uživatele, trpící různými vadami zraku (šilhavost, apod.) nevhodný.



Obrázek 9: Snímání sítnice [1]

Sítnice poskytuje biometrické vzorky s velkým množstvím charakteristických znaků pro identifikaci/verifikaci, které se liší u každého člověka a dokonce i u jednovaječných dvojčat.

Duplikace není možná z důvodu umístění sítnice a nutnosti snímání pouze živého orgánu. Na rozdíl od duhovky se sítnice v průběhu let mění a její nervová struktura je ovlivněna různými nemocemi (zelený zákal, apod.). Proto se databáze s uloženými vzorky musí mnoha případů v určitých časových intervalech obměňovat, aby byli uživatelé vždy správně identifikováni či verifikováni. Další nevýhodou je vysoká cena těchto biometrických zařízení, což znesnadňuje masivnější rozšíření.

3.4 Biometrie obličeje

Informace pro zpracování této podkapitoly byly čerpány ze zdroje [6], není-li uvedeno jinak.

Rozpoznání osob podle obličeje lze v jistém smyslu považovat za nejstarší metodu. Obličej je část lidského těla reprezentující člověka, tudíž je vhodná pro potřeby identifikace či verifikace. Už od svých počátků lidé poznávali jiné osoby podle obličeje, protože se jednalo o nejsnazší a nejpřirozenější způsob. Tato metoda postupně zavedla i do oblasti bezpečnosti, např. při vstupu do objektu předložil uživatel vrátnému identifikační doklad a ten následně podle přiložené fotografie obličeje porovnával, zda se jedná o oprávněnou osobu. Tento způsob verifikace je vyžíván dodnes, protože se jedná o nejjednodušší a mnohdy i jediné možné řešení. Avšak s pokrokem technologií se rozvinula i biometrie obličeje a rozhodovací subjekt byl nahrazen technologickým systémem. Zařízení pro rozpoznání obličeje umožnilo rychlejší, přesnější a z dlouhodobého hlediska levnější (odpadl plat vrátného) řešení.

Obličej se skládá ze tří základních charakteristických vnějších struktur (oči, nos, ústa), které pomáhají utvářet celkový obraz obličeje. Tyto části jsou pro jednotlivé etnické skupiny proměnné (variabilní), což snižuje pravděpodobnost výskytu dvou různých osob s identickými všemi charakteristikami. Pro jednoznačnou identifikaci konkrétní osoby je nutná znalost celkového tvaru obličeje, na kterém jsou další morfologické znaky umístěny. Dalšími znaky určujícími podobu obličeje jsou brada a tvář, které mají svůj význam především u 3D čteček obličeje. Tvar brady se nachází v dolní části obličeje a určuje spodní část celkového tvaru obličeje. Bradu tvoří kosterní podklad, podkožní vazivo a bradový sval, jež určují profilový tvar obličeje. Ve vertikálním směru bradu od rtů (dolního rtu) odděluje bradorettní rýha, zatímco v horizontálním směru přechází plynule v tvář. Tvář je další část, která výrazná především při profilovém pozorování a je utvářena tvarem

lícni a spánkové kostí a jejich vzájemným propojením jářmovými (lícními) oblouky. Dále její tvar ovlivňují měkké části obličeje, tedy tvářový sval a podkožní vazivo.

V praxi v podstatě existují dva přístupy snímání jednotlivých uživatelů, a to se spoluprací uživatele a bez spolupráce uživatele. V prvním případě stejně jako u jiných biometrických systémů vyžaduje zařízení jistou účast uživatele, tzn. uživatel musí před čtečkou zastavit a dívat se určeným směrem, případně odložit části oděvu znemožňující jednoznačnou identifikaci (čepice, brýle, atd.). V druhém případě uživatel nemusí s biometrickým zařízením nijak spolupracovat a je identifikovaný během chůze, resp. během přechodu kolem čtečky. Při detekci uživatele mohou působit problémy i okolní vlivy, např. osvětlení, nepřívětivé pozadí, více přítomných osob na snímku, apod. Základní vlastností obličeje je jeho variabilita, kdy vyjma výše uvedených příkladů, podobu obličeje na první pohled nejvíce ovlivňuje vizáž, mimika a stárnutí. Biometrické systémy proto musí být navrženy tak, aby byly schopny správně identifikovat uživatele i při těchto změnách.

Biometrické systémy pro identifikaci obličeje se dělí na základě snímaných charakteristik:

- identifikace podle 2D snímku,
- identifikace podle 3D snímku,
- identifikace podle termosnímku.

3.4.1 2D čtečky obličeje

Identifikace resp. verifikace obličeje podle 2D snímků je jednou z nejrozšířenějších metod. Přesto tuto metodu nelze považovat za zcela spolehlivou, protože je velmi snadné 2D snímky získat a následně systém obelstít. Při detekci se nejprve lokalizuje konkrétní obličej na snímku, protože může nastat situace, kdy se na snímku vyskytuje více osob. Nasnímané obličeje se odlišují v barvě, pozici, orientaci, mimice, apod. V praxi se detekce provádí dvěma způsoby: podle expertních znalostí a strojového učení.

Detekce podle expertních znalostí

Metoda detekce na základě expertních znalostí spoléhá na fakt, že všechny lidské obličeje mají společné některé fyziologické charakteristiky (pozice očí, nosu a úst, barva kůže, barva očí, atd.). Při detekci se nejprve kompenzuje osvětlení, následně se určuje barva kůže (spolehlivost závislá na počtu etnických skupin uložených v databázi), vymezení

charakteristických rysů obličeje (oči, nos, ústa, tvar obličeje) a nakonec se vypočítají hranice obličeje na základě velikosti obličeje a orientaci gradientů. Podstatou této metody je převod barevných prostorů charakteristik z barevného modelu RGB (červená, zelená, modrá) do YCbCr, což určuje způsob, jakým jsou RGB informace kódovány.

Detekce dle strojového učení

Podstatou metody je rozdělení získaného 2D snímku na jednotlivé části, jež jsou postupně předkládány klasifikačnímu algoritmu, který vyhodnocuje, zda obsahují lidský obličej či nikoliv. Úseky v nichž byl algoritmem zjištěn výskyt obličeje, systém označí pro další vyhodnocování. Příkladem klasifikačního algoritmu je AdaBoost, jehož síla spočívá v kombinaci velkého množství jednoduchých slabých klasifikátorů (např. Haarovy příznaky) do jednoho silného celku.

Obličej detekovaný některou z předcházejících metod se musí před procesem porovnání nejprve upravit (normalizovat). Cílem této operace je eliminace nesprávného vyhodnocení při porovnání vlivem nekvalitní předlohy. Příklady normalizace:

- měřítko – všechny oblasti, v nichž se nachází obličej, jsou převedeny do jednotných rozměrů.
- nahrazení pozadí – barevně různorodé pozadí se nahradí konkrétní jednotnou barvou (zpravidla černou).
- zarovnání vnitřních struktur – na snímku obličeje se označí charakteristické body (oči, nos, ústa), která se patřičným způsobem transformují do podoby odpovídající stanovené šablonové pozici.
- jasová kompenzace – vyrovnání jasů ve snímku do rovnoměrného rozložení, nejčastěji se převádí snímek do plného rozsahu jasu.

Podle biometrického zařízení lze využít i další typy normalizací, které detekují konkrétní charakteristiky (oči, nos, ústa) nebo eliminují vliv vlasů, vousů, brýlí, apod. Druhů normalizací existuje celá řada, avšak v praxi se využívají jen ty, které mají pro stanovený rozpoznávací proces význam.

Spolehlivost procesu rozpoznání osob podle obličeje závisí na kvalitě operací normalizace snímků, na jejichž základě se rozpoznání provádí. Samotný rozpoznávací proces lze v podstatě členit do dvou kategorií, a to:

- 1) **rozpoznání na základě podobnosti obrazových dat** – využívají se postupy vyhledávající podobnosti mezi snímanými daty a daty uloženými v databázi. Tato metoda používá proces normalizace, čímž se usnadní vzájemné porovnání obrazu obličeje. Protože porovnání šablony s daty, získanými přímo z biometrické čtečky nemusí mít dostatečně uspokojivé výsledky. Základem metody je jednorozměrný vektor o délce n (Feature Vector), který vzniká převzorkováním vstupního snímku obličeje na stanovenou pevnou velikost o $w \times h$ bodech a složením řádků za sebe do výsledného vektoru. Ve vzniklém n -dimenzionálním prostoru R reprezentuje každý bod určitý obličej. Cílem je oddělit body představující jednu konkrétní osobu od všech ostatních bodů definujících ostatní uživatele. Do této kategorie patří statické metody (Principal Component Analysis), lineární metody (Linear Discriminant Analysis), metody přímého porovnání (bod po bodu) nebo metody používající strojové učení (neuronové sítě, Support Vector Machines).
- 2) **rozpoznání na základě topologické vlastnosti obličeje** – metoda vyžaduje nejprve získat informace o obličej, tedy určit polohu očí, nosu, obličej, tvar hlavy, případně výraz (mimika) nebo výskyt doplňků (brýle, klobouk), apod. Ze získaných údajů se následně provádí výpočty podobnosti snímků. Na rozdíl od první kategorie není v tomto případě většinou nutné provádět normalizaci obličeje, protože algoritmy této kategorie procesy normalizace v určité míře obsahují. Za příklady lze uvést metody Active Appearance Model, Active Shape Model a Elastic Bunch Graph Matching. Metody AAM a ASM využívají tzv. aktivní šablony, kdy uživatel pro různé obličeje vytvoří významné body (koutek oka, ušní lalůček), které dále slouží jako šablony při procesu porovnávání.

3.4.2 3D čtečky obličeje

Biometrické systémy pro rozpoznání osob podle 3D snímků představují nejbezpečnější a nejefektivnější metodu identifikace. Zařízení vytvářející 3D snímky obličeje odstraňují nedostatky 2D snímků, kde při transformaci obličeje do roviny dochází ke ztrátě některých podstatných informací. V současné době není znám žádný způsob, jak by mohl útočník 3D čtečky obelstít na rozdíl od čteček 2D obličeje (fotografie). Ovšem na rozdíl od 2D čteček jsou 3D finančně nákladnější a především náročnější na zpracování obrazu, kvůli většímu množství informací. Hlavní rozdíl mezi 2D a 3D snímáním obličeje spočívá ve snímacím

zařízení, které u 3D snímání pracuje na bázi 2,5D skenerů. Ten v podstatě vytváří klasický 2D obraz, jenž v každém bodě uchovává informaci o hloubce obrazu a tím umožňuje prezentovat prostorová data. V takovém případě se ale nejedná o 3D obraz, jelikož není možné prezentovat body mající stejné souřadnice, ale rozdílnou hloubku. K vytvoření 3D obrazu se při snímání obličeje využívá zdroje světla (IR, viditelného), s jehož pomocí se provádí snímání pod určitým úhlem a vytváří se 2,5D obraz. Aby se zajistil vznik uceleného obrazu, je nezbytné snímání opakovat pod různými úhly a z různých míst, čímž se zamezí vzniku děr v obraze. Všechny získané 2,5D snímky jsou ve finální fázi seskládány do výsledného 3D obrazu. Avšak tvorba 3D obrazu prostřednictvím více míst se považuje za nepraktickou, nákladnou (nutnost více snímacích zařízení), proto si systém při rozpoznání obličeje musí vystačit pouze s informacemi získanými z jednoho místa. Získané informace o obličeji systém může vizualizovat několika způsoby, nejčastěji třemi základními. Zaprvé jako shluk bodů (mrak bodů), vyjadřující souřadnice jednotlivých míst obličeje, bez jakýchkoliv vzájemných vazeb. Z toho důvodu není, i přes svou jednoduchost, uživatelsky přívětivý. Druhý způsob tzv. polygonální síť, vytváří na povrch 3D modelu obličeje síť polygonů, obvykle trojúhelníkového tvaru. Poslední způsob reprezentace obličeje se nazývá hloubková mapa, což je v podstatě 2,5D sken, kde intenzita bodů se rovná vzdálenosti v prostoru. Všechny uvedené způsoby vizualizují informace získané skenováním obličeje ve formě 3D modelu, který je připraven k další části procesu, tedy rozpoznání.

Princip porovnání získaného 3D modelu obličeje s šablonou uloženou v databázi je podobný způsobu porovnání 2D modelu. V podstatě existují čtyři metody, jak porovnávat 2D resp. 3D modely.

- 1) 2D šablona, 2D snímek – klasická metoda porovnávání pro 2D modely.
- 2) 3D šablona, 2D snímek – při porovnání se nalezne 3D šablona, která se vhodně převede do 2D modelu, tak aby bylo možné oba modely porovnat. Výhoda metody spočívá v možnosti využívání pouze jednoho 3D zařízení, a to pro získání referenční šablony. Ostatní čtecí zařízení mohou být na bázi 2D, čímž se sníží náklady a také bezpečnost systému.
- 3) 2D šablona, 3D snímek – proces porovnávání je v podstatě stejný, opět je nutná konverze mezi 2D a 3D do jednotného finálního modelu. Výhody a nevýhody jsou

inverzní k předešlé metodě, kvůli potřebě více 3D čtecích zařízení rapidně vzrůstají náklady a zároveň bezpečnost.

- 4) 3D šablona, 3D snímek – metoda pracuje s více informacemi, což má vliv na přesnější výsledky porovnávání. Odpadá potřeba převádění mezi rovinným a prostorovým modelem. Výhody a nevýhody jsou identické, jako v předchozím případě.

Jak bylo uvedeno výše, při procesu porovnání je nezbytné snímáním získaný obraz (snímek) zpracovat do vhodné podoby. Tento proces je podobný jako u zpracování 2D snímků, s jediným rozdílem v množství zpracovávaných dat. Při porovnání dvou snímků je třeba uvědomit si fakt, že nikdy nebudou dva snímky naprosto identické, z toho důvodu se musí získaný snímek upravit (konkrétně normalizovat). Je nutno určit klíčové body, jimiž jsou např. špička nosu, koutky očí, apod., které umožňují model převést do podoby, v níž je dosažena co nejvyšší souvztažnost mezi stanovenými body. Tento postup lze realizovat několika metodami, z nichž se může uvést např.:

- detekce nosu – jakožto jeden z charakteristických znaků lidského obličeje, představuje ideální volbu pro zarovnání modelu. Polohu nosu v 3D modelu vyjadřuje hodnota z , definující nejméně vzdálený bod. Zbylé hodnoty souřadnic určují x a y rotaci hlavy kolem svých os. Další možností je přepokládat pozici nosu v ose y , kdy se v rovině yz určí maximální a průměrná hodnota plochy a následně se zjistí hodnota maxima, což umožní získat hodnotu x .
- hrubé zarovnání – podstatou metody je práce s trojicí bodů se vzájemnými vazbami (tvoří trojúhelník). Body v obličeji by měly být dobře detekovatelné a pokud možno neměnné (gestikulace, apod.). Nejprve se definuje neměnná pozice trojice bodů (označí se např. A), poté druhá trojice (např. B), pro kterou se pomocí transformace hledá B' takové, aby byla celková odchylka mezi A_i a B'_i , kde i nabývá hodnot od 1 do 3, ideálně co nejnižší.

V poslední fázi procesu rozpoznání se vyhledávají analogie určitých prvků obličeje mezi získaným 3D snímkem a v databázi systému uloženou šablonou. Stejně jako u všech předcházejících fázích ani zde neexistuje univerzální metoda, jak jednoznačně identifikovat osobu. Tyto metody se liší buď podle požadavků zákazníka (bezpečnost, rychlost), nebo

použitého biometrického zařízení. Jako příklad lze uvést některé ze základních metod používaných pro vyhledávání podobnosti:

- 1) **analogie 3D modelu** – algoritmus vyhledá všechna jemná zarovnání obou snímků, na jejichž základě stanoví míru rozdílnosti tvarů a určí výslednou hodnotu podobnosti snímků. Ze získaného snímku obličeje se vybere množina bodů (kontrolní body) ve zvolených místech, kde nedochází vlivem gestikulace či stárnutím nedochází k výrazným změnám, a zároveň pokrývají co největší plochu. Transformací získaného snímku se musí dosáhnout minimální vzdálenosti kontrolních bodů od povrchu uložené šablony.
- 2) **analogie podle tvaru a vzhledu** – 3D model uložený v databázi se pomocí transformace a následných vhodných úprav (osvětlení snímku, syntéza vzhledu, apod.) převede do podoby odpovídající získanému snímku. S využitím metody podobnosti 3D modelu se určí n různých testovaných snímků, na které se aplikuje syntéza vzhledu.
- 3) **analogie hloubkových map** – jde o nejjednodušší metodu, jak vyhledat podobnosti ve 3D modelech. V podstatě metoda pracuje s 2D snímkem, resp. jeho hloubkovou mapou, která se získá už v procesu normalizace. V praxi se ovšem využívá především filtrovaná forma hloubkové mapy (Sobelův operátor).

3.4.3 Termo čtečky obličeje

Princip termo čteček obličeje je obdobný jako u 2D a 3D čteček, liší se jen v použitém snímacím zařízení, tedy i výstupu z něj, a spektru světla. Na rozdíl od 2D a 3D čteček, termo čtečky využívají pro svou činnost výhradně IR záření dlouhé vlnové délky (LWIR). Rozmezí vlnové délky u LWIR se pohybuje mezi 8 až 15 μm (někdy se uvádí 7-14 μm). Oproti běžnému viditelnému světlu LWIR během snímání obličeje neoslňuje uživatele, čímž se zvýší kvalita vstupních dat. Klasická kamera, jakožto snímací zařízení je nahrazena speciální kamerou, která je schopna snímat IR záření a nazývá se termokamera. Termokamera převádí pro lidské oko neviditelné infračervené záření na elektrický signál, který putuje do zobrazovacího zařízení, kde se zpracuje do podoby viditelné pro uživatele. Před použitím termokamery je třeba správně nastavit tyto parametry:

- emisivita povrchu – číslo v intervalu od 0 do 1, které je dáno jako poměr energie vyzářené konkrétním objektem při určité teplotě k energii vyzářené černým tělesem při stejné teplotě. V tomto případě povrch představuje kůže, pro kterou je hodnota emisivity asi 0,98.
- konstantní vzdálenost – tím se rozumí správné nastavení kamery, aby byl zaostřen požadovaný objekt (obličej).
- relativní vlhkost okolí
- teplota okolí

Masivnímu rozšíření termokamer v biometrických systémech brání jejich cena, proto se využívají jen na místech, kde se klade velký důraz na bezpečnost a spolehlivost bez ohledu na cenu (letišť). Výstupem termokamery jsou termovizní snímky (termomapy) obličejů, které se zpracovávají podobně jako klasické 2D snímky. Nejprve se určí pozice charakteristických prvků (oči, nos, ústa, atd.), následuje zarovnání a nakonec se vyhledávají podobnosti snímků. (viz. 3.4.1 2D čtečky obličejů). Použitím termočteček obličejů se odstraní některé nevýhody 2D čteček, bohužel vyvstávají i nové problémy. Hlavní výhodou, stejně jako u 3D čteček, spočívá v bezpečnosti zařízení, není možné oklamat termočtečku běžnou fotografií. Vytvoření padělku znesnadňuje proměnlivá teplota v různých místech obličejů. Další výhodou je vznik kvalitního snímku za jakýchkoliv okolních podmínek (slunce, šero, noc, apod.). Avšak výhody mohou za určitých podmínek představovat významné nevýhody. Protože zařízení vyhodnocuje LWIR závislé na aktuálním teplotním rozložení člověka, může při porovnání získaného snímku a šablony nastat u identického uživatele neshoda, způsobená právě změnou teploty. Změny způsobuje např. vykonávaná aktivita, nemoc, teplota okolí, případně emoce člověka. Z tohoto důvodu se termokamery v některých případech využívají v kombinaci s běžnými zařízeními.

II. PRAKTICKÁ ČÁST

4 BROADWAY 3D

Informace pro zpracování této kapitoly byly čerpány ze zdrojů [7], [8], [9], není-li uvedeno jinak.

Biometrické zařízení Broadway 3D představuje možnost ochrany objektů, které vyžadují vysoký stupeň zabezpečení. Broadway se řídí stejnými pravidly, jako všechna biometrická zařízení. Při registraci jsou zařízením získány biometrické vzorky obličeje (šablona) uživatele, které jsou následně využity při identifikaci či verifikaci. Proces registrace na rozdíl od procesů identifikace a verifikace, vyžaduje přítomnost obsluhy (např. správce). Broadway zcela autonomně vyhodnotí, zda se jedná o oprávněného uživatele či nikoli. Výsledná informace je zobrazena na připojené zobrazovací jednotce nebo signalizována pomocí diod v horní části rozpoznávacího zařízení.

Broadway 3D se vyznačuje vysokou mírou spolehlivosti, především odstraňuje nedostatky lidského faktoru. Bezpečnostní pracovník může chybovat v případě kontrolování velkého množství lidí, kdežto Broadway dokáže zpracovat až 60 osob za minutu. Nelze jej obelstít ani s využitím masky či částečným zakrytím obličeje (pokrývky hlavy, sluneční brýle, apod.). U verifikace, v případě ztráty nebo krádeže identifikátoru, nehrozí nebezpečí neoprávněného vniknutí. Broadway 3D může sloužit i jako docházkový systém, protože nehrozí možnost padělání nebo zneužití údajů o docházce.

Snímání obličeje a následné ukládání do databáze, na rozdíl od jiných biometrických systémů, nepřináší rizika zneužití citlivých údajů. Neboť informace o obličeji jsou veřejně přístupné (sociální sítě, identifikační průkazy, atd.) oproti otiskům prstů, apod.

Čtečka obličeje Broadway 3D je první zařízení na světě, které je schopno vizuálně identifikovat osobu stejně snadno jako se lidé identifikují navzájem. Přičemž identifikace trvá jen zlomek vteřiny. Pohled na zařízení při chůzi či dokonce běhu stačí k tomu, aby Broadway rozpoznala identitu jednoho uživatele z desítek tisíc předem registrovaných jedinců. Rozpoznání tváře, oproti snímání jiných biometrických znaků, nevyžaduje přímý fyzický kontakt nebo přesné umístění v přední části identifikačního zařízení. 3D Broadway identifikuje osoby bez ohledu na jejich věk či výšku. 3D čtečka obličeje Broadway je vybavena 3D kamerovým systémem, který zaznamenává a ukládá unikátní trojrozměrný tvar obličeje. Na rozdíl od lidského oka má přístroj schopnost rozlišit nepatrné rozdíly geometrie s přesností až na zlomky milimetru, což mu umožňuje rozeznat i identická

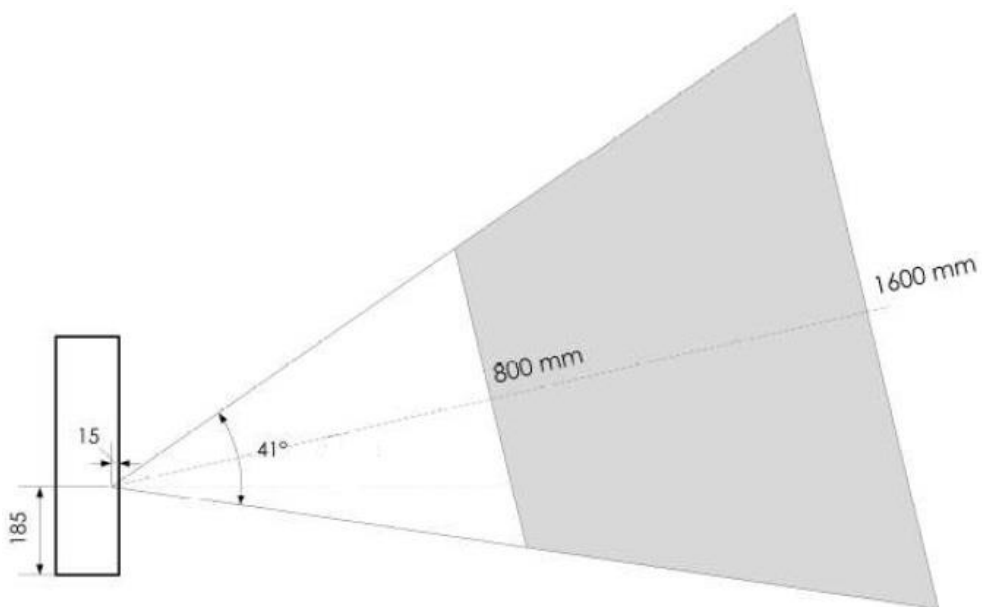
dvojčata. Technologie 3D skenování umožňuje rychlé a přesné pořízení povrchu snímaného objektu pomocí tzv. metody strukturovaného světla. Světlo je promítáno přes vzor (v tomto případě se jedná o mřížku) na povrch objektu v paralaxe, což je úhel mezi dvěma přímkami vedoucí z různých míst v prostoru vzhledem k pozorovanému bodu (místo kde se přímky protínají). Jinak řečeno kamera snímá povrch objektu z jiného místa než osvětlení, tím dochází k měření dvou parametrů (úhlu a vzdálenosti). Výhoda 3D rozpoznání obličeje spočívá ve schopnosti měřit jak úhel, tak vzdálenost, na rozdíl od 2D rozpoznání, které měří pouze vzdálenosti ve struktuře obličeje. Mřížka vytvoří na povrchu snímaného objektu síť souřadnic, jež slouží pro přesný výpočet každého bodu. Textura kamery je synchronizována s 3D senzorem, jenž má široké zorné pole. Senzor současně zachycuje tvar a strukturu povrchu objektu. Právě kamera je nejsilnější stránkou celého zařízení. Jedná se o kameru nové generace, která pořizuje snímky v širokém úhlu až 41°, tzn. je schopna zachytit obličej osob dosahující poloviny výšky dospělého člověka (dětí, vozíčkáři, apod.). Snímková frekvence kamery je 15 snímků za sekundu a to i ve stroboskopickém režimu, např. když uživatel kolem čtečky proběhne. Rekonstrukční algoritmy a příslušný hardware umožňují přesné rozpoznání objektů. Hardware je součástí balení, poskytované společností Artec Group při nákupu biometrické čtečky Broadway 3D BR.

Technické specifikace 3D čtečky obličeje:

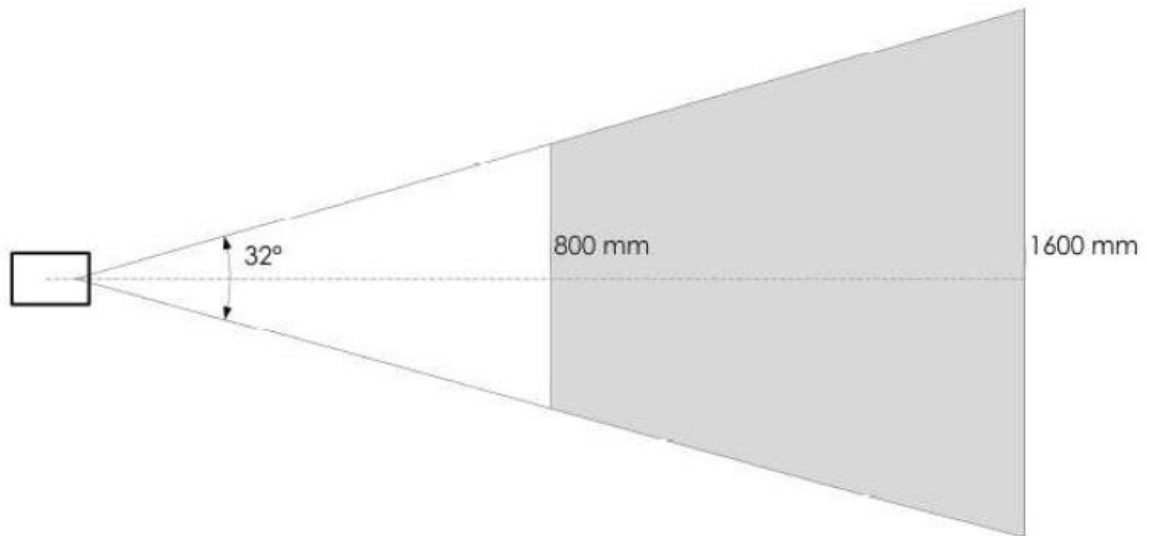
- vysoké rozlišení (až 200 milionů bodů),
- snímková frekvence v reálném čase (15 fps),
- vysoká přesnost (až 0,1 mm),
- velký rozsah výškového pokrytí (140 – 210 cm)
- zorné pole (32°/41°- h/v),
- dosah: 0,6 – 1,8 m,
- krátká doba expozice (0,2 ms),
- rozhraní: USB,
- administrativní rozhraní: Ethernet,
- možnost zachycení pohybujících se objektů (do 5 km/h),

- čas zápisu: 2 s,
- čas rozpoznání: 1 s,
- provoz ve slunečním světle i ve tmě,
- světelný zdroj: žárovka (ne laser),
- napájení: 100 – 240 VAC,
- provozní teplota: 15 – 30°C,
- provozní vlhkost: 15% - 80% (nekondenzující),
- False Rejection Rate (FFR): 1x1 000,
- False Acceptance Rate (FAR): 1x1 000 000,
- Failure to Enroll (FTE): 0,
- malá velikost biometrické šablony (3,4 kb).

Na obrázcích 10 a 11 je znázorněn rozsah horizontálního, resp. vertikálního zorného pole.

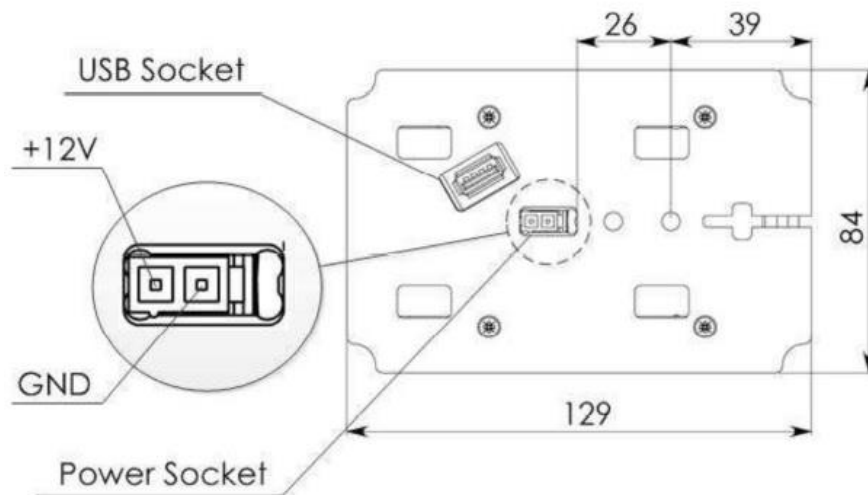


Obrázek 10: Vertikální zorné pole [9]



Obrázek 11: Horizontální zorné pole [9]

V následujícím obrázku je uvedeno schéma připojení kabeláže (USB a napájení) k biometrické čtečce obličeje Broadway 3D. USB kabel se připojuje k počítačové jednotce. Může se jednat o počítač s nainstalovanými programy výrobce nebo počítač s doplňujícím softwarem, např. k získání 3D modelů.

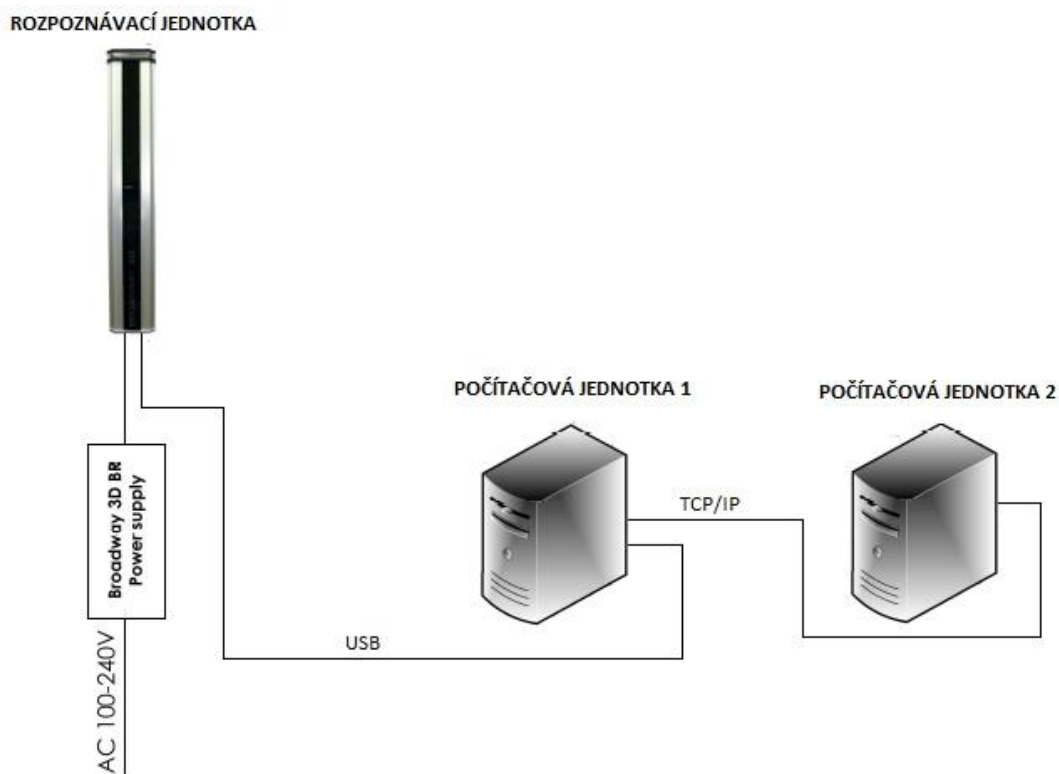


Obrázek 12: Popis připojení kabeláže [9]

Datové připojení je realizováno prostřednictvím ethernetového rozhraní, kdy využívá komunikačního protokolu TCP/IP.

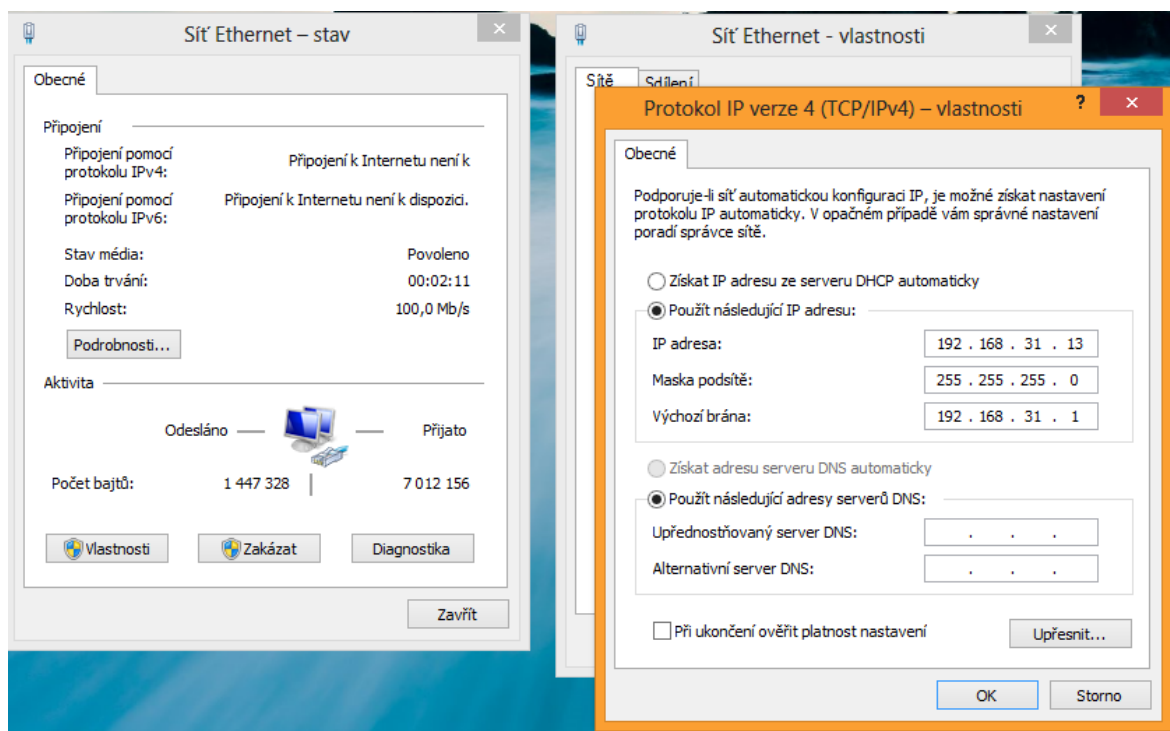
4.1 Webový prohlížeč

Primární možnost konfigurace biometrické čtečky je prostřednictvím webového prohlížeče. Obrázek 13 znázorňuje schéma zapojení zařízení Broadway s počítačovými jednotkami. Počítačová jednotka 1 obsahující databázi biometrických vzorků je propojena s počítačovou jednotkou 2 přes ethernetový kabel, kdežto spojení mezi počítačovou jednotkou 1 a rozpoznávací jednotkou realizuje univerzální sériová sběrnice.



Obrázek 13: Schéma zapojení [9]

Komunikace mezi počítačovými jednotkami, propojenými ethernetovým kabelem, je realizována protokolem TCP/IP. Na straně počítačové jednotky 2 se v Ovládacích panelech, resp. nastavení Sítě a Internetu, upraví vlastnosti protokolu TCP/IPv4, viz. Obrázek 14.



Obrázek 14: Nastavení TCP/IPv4

IP adresa 192.168.31.13 s maskou podsítě 255.255.255.0 představuje adresu počítačové jednotky 2. Jako adresa brány, tedy uzlu spojujícím biometrické zařízení a počítač 2, byla definována 192.168.31.1.

Za pomoci jakéhokoliv webového prohlížeče (Firefox, Chrome, Internet Explorer, atd.) se provádí základní nastavení zařízení Broadway. Pro vstup do konfiguračního módu je nezbytné zadat adresu biometrického zařízení do adresního řádku prohlížeče, v tomto případě 192.168.31.12, čímž se zobrazí informační stránka společnosti Artec Group. V dalším kroku bude uživatel vyzván k zadání přihlašovacích údajů, které jsou dodávány se zařízením. Konfigurační mód je určen pro správce a osoby odpovědné za činnost biometrického zařízení, proto by k němu neměl mít běžný uživatel přístup. Po přihlášení se na stránce zobrazí tři záložky, týkající se základních informací, práce s databází osob a konfigurace. První ze záložek informuje správce o verzi biometrického zařízení, době provozu, stavu zařízení od posledního přihlášení, apod. Druhá karta Person View (obrázek 15) umožňuje správci pracovat s uživateli. Správce tedy může do databáze přidávat nové uživatele a naopak je i odebírat. Při přidávání osob do databáze je nutné uvést křesní jméno a příjmení, dále je možné uvést prostřední jméno, datum narození či pohlaví uživatele, pro případ verifikace i číslo identifikační karty. Tyto údaje usnadňují vyhledávání uživatelů v rozsáhlých databázích. Každý nově přidaný uživatel dostane tzv. PID, což značí

identifikační číslo konkrétní osoby. Přidání uživatele do databáze nestačí, jestliže nebyl uživateli sejmuto biometrický vzorek obličeje. K tomu slouží tlačítko Enroll, které pošle požadavek na snímání obličeje do zařízení Broadway 3D a následně je vzorek přiřazen do databáze k danému uživateli. Snímání se provádí ve vzdálenosti 1 až 1,2 metrů od biometrického zařízení. Z důvodů zachování dostatečné kvality při identifikaci či verifikaci se biometrické vzorky obnovují nejméně jednou za tři roky. Obnova šablony biometrických údajů se realizuje dvěma způsoby. První je pomocí tlačítka Reenroll, kdy se uživatel nechá znovu nasnímat, přičemž PID a další údaje zůstávají zachovány. Druhou možností je smazání starých údajů a vytvoření nových, u této varianty se ztrácí původní hodnota PID.

Artec Group
3D Scanning Technologies

Broadway 3D®
Web Configuration Module

Logged in: root [logout]

Info Person View Configuration

Controls
Persons per page: 10
Persons without 3D:

Search
search
Search results:
Add person:

Database management console
All Persons
Page: 1
From 1 to 10 of 6 persons, in 1 pages

PID	Last Name	First Name	Middle Name	3D	CID	Action
1	Valer	Tomas		Ok	Ok	Reenroll
2	Pecsek	Jaroslav		Ok	Ok	Reenroll
3	Dara			Ok	Ok	Reenroll
4	Talandová	Hanka		Ok	Ok	Reenroll
5	Kovář	Stanik		Ok	Ok	Reenroll
6	Baroň	Roman		Ok	Ok	Reenroll

© Artec Group, 2007-2010

Obrázek 15: Person View

Poslední ze záložek je Configuration, která slouží k nastavení biometrického zařízení podle potřeb zákazníka, správce, apod. Záložka Configuration sama o sobě nabízí několik dalších podzáložek podle potřeb správce. První z nich se nazývá General a zabývá se konfigurací biometrického zařízení. Umožňuje měnit prahové hodnoty zařízení při identifikaci nebo verifikaci, nastavit přístup k databázi zařízení nebo její zabezpečení (viz. Obrázek 16).

Artec Group
3D Scanning Technologies

Broadway 3D®
Web Configuration Module

Logged in: root

Info Person View **Configuration**

Section

- General
- Networking
- Camera Setup
- Theme Management
- Miscellaneous

General Device Configuration

Autonomous Mode

Verification
Threshold (0.XXX, Range: 0.411 - 0.764)

Identification
Threshold (0.XXX, Range: 0.411 - 0.764)

Database Host

Local
 Remote
IP Address (XXX, Range: 0 - 255)

Database Settings

User (Range: 0 - 9, a - z, A - Z)
Password (Range: 0 - 9, a - z, A - Z)
Database Name

© Artec Group, 2007-2010

Obrázek 16: Obecná konfigurace zařízení Broadway

Záložka Networking správci umožní změnu IP adresy zařízení, masky nebo výchozí brány. Tato karta je po zpřístupnění zařízení vyplněná, viz. jeden z prvních kroků, kde se v počítačové jednotce 2 nastavoval přístup k zařízení Broadway 3D.

Artec Group
3D Scanning Technologies

Broadway 3D®
Web Configuration Module

Logged in: root

Info Person View **Configuration**

Section

- General
- Networking
- Camera Setup
- Theme Management
- Miscellaneous

Network Configuration

Device IP Settings

Automatic (DHCP)
 Manual

IP Address (XXX, Range: 0 - 255)
Network Mask (XXX, Range: 0 - 255)
Gateway IP Address (XXX, Range: 0 - 255)

Event Listeners

IP Address (XXX, Range: 0 - 255)

192.168.31.12/index.php?m=1&s=1 © Artec Group, 2007-2010

Obrázek 17: Konfigurace síťového připojení

V záložce Camera Configuration se seřizují parametry kamery podle aktuálních (daných) potřeb. Je nutné kameru uzpůsobit podmínkám, ve kterých bude zařízení Broadway pracovat. Toto nakonfigurování je náročné a značně komplikované, pokud bereme v úvahu možnost grafického zobrazování v reálném čase při měnění hodnot jednotlivých

parametrů. Z toho důvodu je vhodnější využívat některý z grafických softwarů, např. Turnstile Enrollment Application.

Section

- General
- Networking
- Camera Setup
- Theme Management
- Miscellaneous

Camera Configuration

3D Camera Preview Settings

Auto Gain	<input checked="" type="checkbox"/>	
Auto Shutter Speed	<input type="checkbox"/>	
Initial Gain	<input type="text" value="1.67"/>	(XXX, Range: 0.1 - 23.8)
Initial Exposure	<input type="text" value="10"/>	(XX.X, Range: 0.1 - 66.1)
Gamma	<input type="text" value="1"/>	(XX.X, Range: 0.1 - 5.0)
Contrast	<input type="text" value="1"/>	(XXX, Range: 1 - 100)
Brightness	<input type="text" value="0"/>	(XXX, Range: -180 - 180)

High Quality Texture Camera Settings

Auto Gain	<input type="checkbox"/>	
Auto Shutter Speed	<input type="checkbox"/>	
Initial Gain	<input type="text" value="2"/>	(XX.X, Range: 0.1 - 23.8)
Initial Exposure	<input type="text" value="50"/>	(XX.X, Range: 0.1 - 66.1)
Gamma	<input type="text" value="1.4"/>	(XX.X, Range: 0.1 - 5.0)
Contrast	<input type="text" value="1"/>	(XXX, Range: 1 - 100)
Brightness	<input type="text" value="0"/>	(XXX, Range: -180 - 180)
Saturation	<input type="text" value="1.0"/>	(XX.X, Range: 0 - 10)
Hue	<input type="text" value="0"/>	(XXX, Range: -180 - 180)
Color Preset	<input type="text" value="Fluorescent"/>	
Gain R	<input type="text" value="2.2"/>	(X.XX, Range: 1.0 - 3.89)
Gain G	<input type="text" value="1.0"/>	(X.XX, Range: 1.0 - 3.89)
Gain B	<input type="text" value="1.5"/>	(X.XX, Range: 1.0 - 3.89)

Advanced

Disable high quality texture camera

Obrázek 18: Konfigurace kamery biometrického zařízení

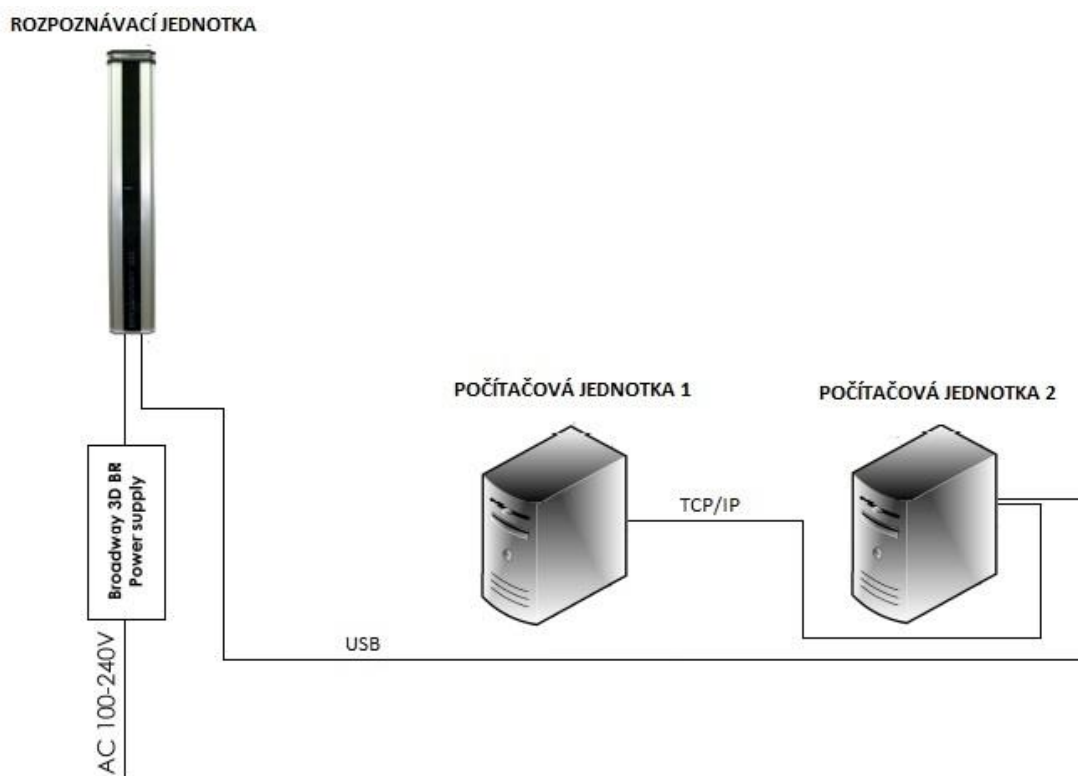
Další záložky správci neumožní žádné technické nastavení zařízení, ale pouze tematické nastavení nebo možnost restartu biometrického zařízení.

Na závěr této podkapitoly je uvedeno malé shrnutí webového prohlížeče sloužící ke konfiguraci Broadway 3D. Oproti konfiguračním softwarům má velkou výhodu, že není potřebná instalace zařízení, apod. S tím souvisí i menší využití procesoru počítačové jednotky a hlavně se ušetří místo na disku. Naopak neumožňuje grafické zobrazení a nemusí být pro některé uživatele dostatečně přívětivý. Zařízení není určeno pro začátečníky, neboť je nutná určitá úroveň znalostí správce.

4.2 Turnstile Enrollment Application

Freewarový software Turnstile Enrollment Application, nebo-li zkráceně TEA, představuje další nástroj pro práci s biometrickým zařízením Broadway 3D. Aplikace TEA byla vyvinuta pro správu biometrické databáze. Na rozdíl od předchozího způsobu konfigurace je TEA uživatelsky přívětivější a nabízí mnohem více možností. TEA představuje snadnější alternativu za SDK, které také umožňuje ze čtečky získat biometrické údaje. V případě SDK jsou ovšem vyžadovány rozsáhlejší znalosti programování. Pro uvedení do provozu je nutné mít v počítačové jednotce 2 nainstalovaný databázový systém MySQL

Server nejméně verze 5.0. Schéma zapojení je obdobné jako u webového prohlížeče s výjimkou propojení počítačových jednotek a rozpoznávacího zařízení. Broadway 3D se připojí přímo k počítačové jednotce 2 přes USB. Propojení a nastavení počítačových jednotek prostřednictvím TCP/IPv4 zůstává stejné. Počítačová jednotka 1 uchovává databázi biometrických vzorků a komunikuje s aplikací TEA nainstalovanou v počítačové jednotce 2.



Obrázek 19: Schéma zapojení s využitím aplikace TEA [9]

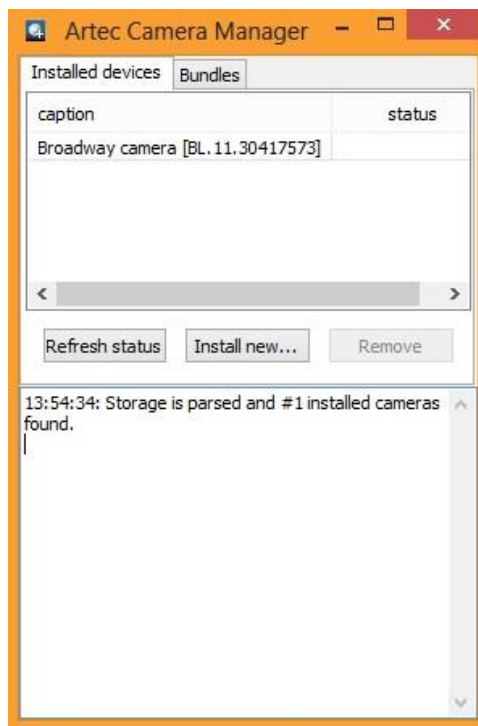
TEA může sloužit jako doplňkový software k webovému prohlížeči za předpokladu, že je správně nastavená databáze biometrických údajů. Při instalaci je správce vyzván k vytvoření administrátorského hesla a určení vlastností připojení k databázovému serveru MySQL, kam se budou data z aplikace TEA ukládat (Obrázek 20). Do pole host se uvede IP adresa biometrického zařízení, v poli port zůstane hodnota 0, do polí login a password se uvedou příslušné údaje. V tomto případě se uvedou údaje z obrázku s pořadovým číslem 20, kdy heslo bude bss. Nastavení vlastností lze doplnit i dodatečně v grafickém rozhraní. Další možností je vytvoření nové databáze nezávislé na databázi vytvořené při práci s webovým prohlížečem. V takovém případě se bude nastavení vlastností připojení lišit od Obrázku 20.



Obrázek 20: Nastavení připojení

Jestliže se tento krok nevyplní, zůstane nastavení v defaultní podobě, což znamená, že správce musí vytvořit novou databázi. Pokud se připojení MySQL provede správně, bude správce vyzván k výběru databáze podle požadavků. Na výběr jsou možnosti použití již vytvořené databáze (v tomto případě se jmenuje `bss_db`) nebo vytvoření zcela nové databáze.

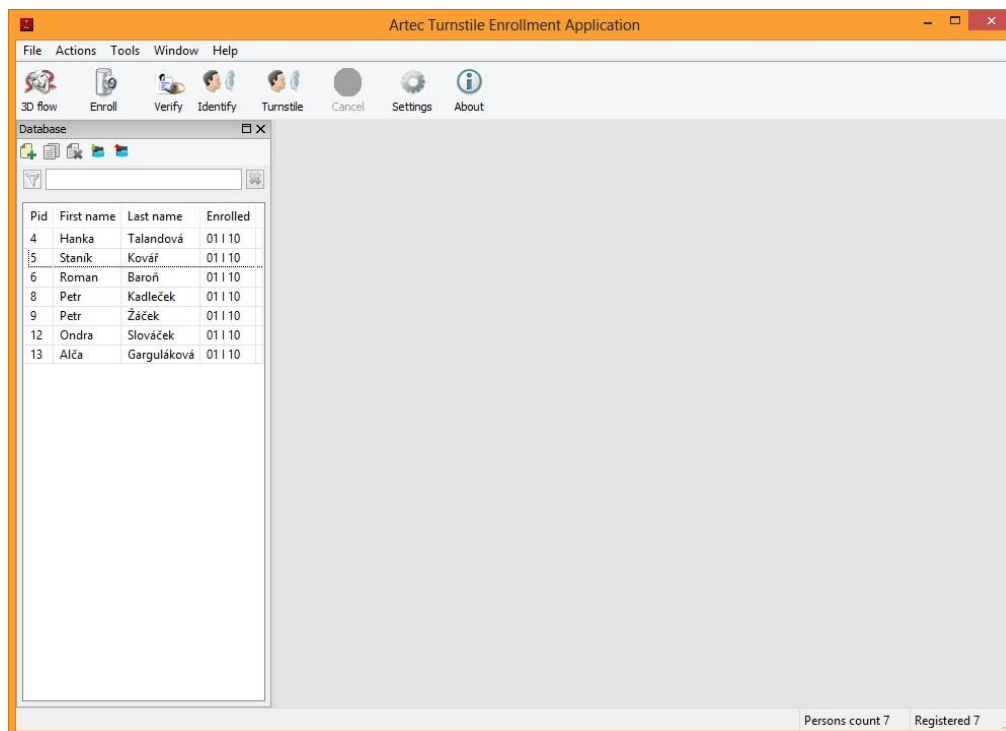
Jakmile bude instalace dokončena, bude správce programem vyzván ke spuštění aplikace Artec Camera Manager. Každé zařízení Broadway 3D je dodáváno spolu s konfiguračním souborem s příponou `.add`, který je vyžadován kvůli správnému fungování aplikace TEA a biometrického zařízení. S pomocí Artec Camera Manager lze spravovat kamery nainstalované v počítači. Hlavní okno programu je zobrazeno na Obrázku 21.



Obrázek 21: Hlavní okno Artec Camera Manager

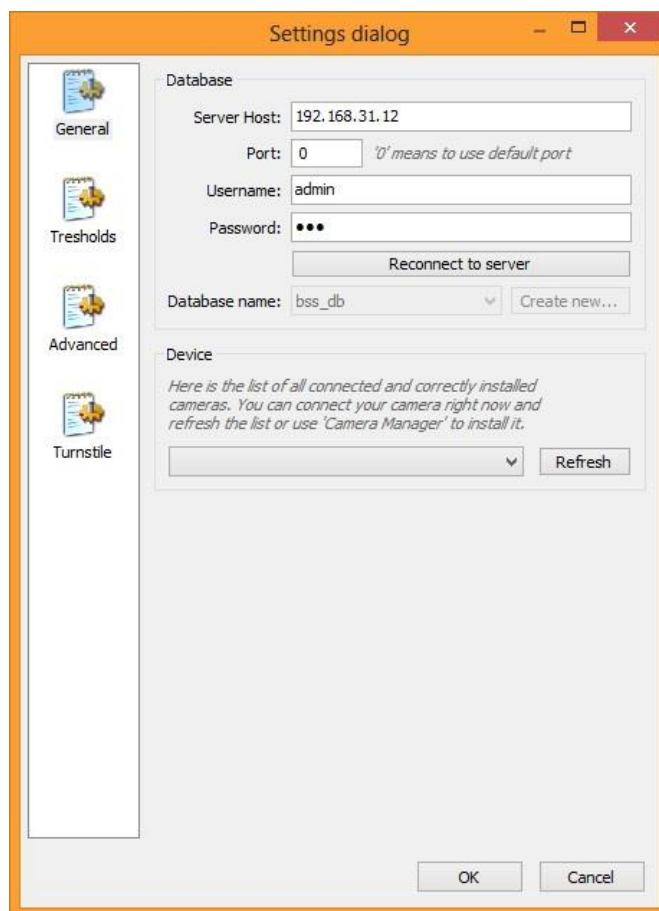
Záložka Installed devices obsahuje seznam kamer, které jsou již v systému nainstalovány. Jestliže je kamera připojena k počítači, indikujeme informaci v této kartě. Pokud není k dispozici žádná kamera, nainstaluje se nová za pomoci konfiguračního souboru, který je zmiňován výše. Je-li instalace úspěšná, objeví se v seznamu nový řádek vztahující se k instalované kameře.

Po nainstalování kamery je možné spustit aplikaci TEA, která správce (uživatel) před zobrazením hlavního menu vyzve k zadání administrátorského (uživatelského) hesla, jež se zadávalo při instalaci. Podle pozice, ze které byl zvolen přístup do aplikace, se liší i možností oprávnění. Autor diplomové práce využíval pro svou činnost administrátorského přístupu. Hlavní menu (Obrázek 22) umožňuje vybírat z konkrétních činností aplikace hned několika způsoby. Jedná se o klasické hlavní menu programu, dále se jedná o panel pro rychlé spuštění vybraných činností nebo využitím klávesových zkratk.



Obrázek 22: Hlavní menu aplikace TEA

Pokud byly během instalace nastaveny vlastnosti připojení a zvolena správná databáze v hlavním okně aplikace, bude na levé straně zobrazena již vytvořená databáze registrovaných uživatelů i s jejich biometrickými vzorky tak, jak je vidět na předcházejícím obrázku. V případě, že konfigurace nebyla při instalaci aplikace provedena, lze ji dodatečně provést v nastavení. A právě menu nastavení představuje výrazný rozdíl mezi konfigurací prostřednictvím webového prohlížeče a aplikací TEA. Po spuštění nastavení vyskočí okno, ve kterém se primárně zobrazuje záložka General (Obrázek 23), kde se provádí konfigurace vlastností připojení k databázovému serveru MySQL. Do nastavení se zadají stejné údaje, které byly uvedeny už dříve v bodu instalace. Po vyplnění všech políček je nutné restartovat připojení, aby mohlo dojít ke správnému nastavení. V posledním kroku se už jen vybere konkrétní databáze.



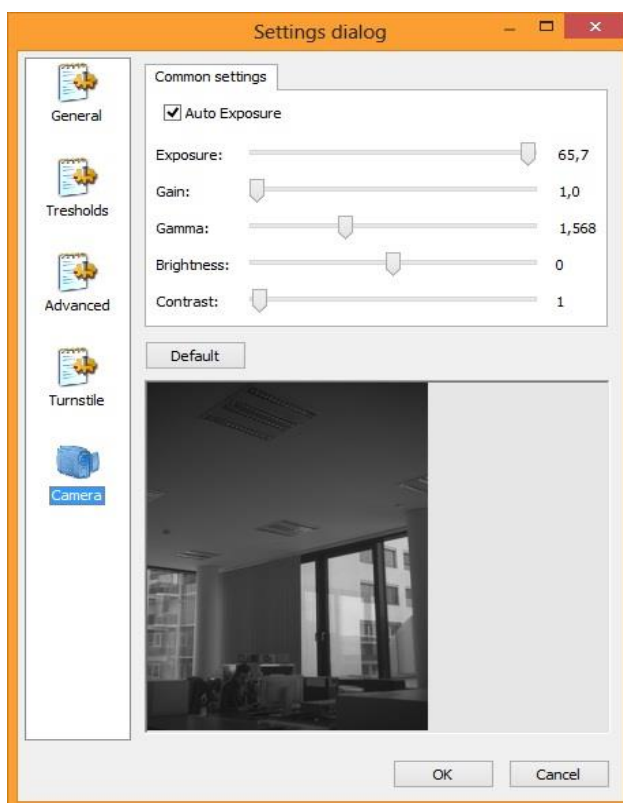
Obrázek 23: Záložka General

Záložka Tresholds nabízí možnosti v oblasti snímání při registraci, identifikaci či verifikaci. Podle požadavků se stanoví časový limit potřebný na snímání lidského obličeje a požadavky na kvalitu. Pro potřeby identifikace či verifikace se určí prahová hodnota, tedy nejnižší možná hodnota, která vyvolá reakci biometrického systému. Obecně platí, že čím menší prahová hodnota bude, tím větší je pravděpodobnost nesprávné identifikace či verifikace osoby. A naopak při vysoké prahové hodnotě, nemusí být konkrétní uživatel identifikován. V tomto případě záleží na kvalitě modelu, vzniklého během snímání obličeje, který je ovlivněn okolím. V průměru se během snímání zjistilo, že uživatel má při různých světelných podmínkách při identifikaci shodu v rozmezí 50 až 65%, u vyšších prahových hodnot, docházelo často k neúspěšným identifikacím.

Další záložky slouží pro běžné nastavení aplikace, např. změna hesla, nastavení jazyku, nastavení karet při verifikaci, vzhled aplikace, apod.

Poslední záložka Camera (Obrázek 24) umožňuje nastavit parametry kamery, které mají být použity při snímání textury. V režimu čekání jsou získané snímky průběžně

analyzovány pro vyhledávání 3D obličeje osoby. Pokud je nalezena tvář, bude zahájen proces identifikace. Kvalita snímků získaných v režimu čekání má vliv na výsledky při hledání 3D modelu tváře. Proto se doporučuje provést nastavení tak, aby se nevyskytovaly podexponované nebo přexponované oblasti.



Obrázek 24: Nastavení kamery

Expozice – udává, jak velké množství světla dopadá na senzor kamery. Aplikace TEA umožňuje vybrat ze dvou možností. První z nich je automatická expozice, která je určena především pro začátečníky, pokročilí uživatelé ocení možnost ručního nastavení hodnoty expozice.

Gain – označení pro citlivost, která u vyšších hodnot přidává do obrazu šum. V automatickém režimu je nastavena nejnižší hodnota.

Gama korekce – zajišťuje opravu převodních charakteristik obrazovek. V závislosti na charakteru snímané scény lze měnit gradaci obrazu.

Jas – atribut vizuálního vnímání, který představuje relativní vyjádření intenzity energetického výstupu viditelného světelného zdroje. Ve výchozím nastavení je hodnota jasu rovna nule.

Kontrast – formuluje rozdíly mezi světlými a tmavými oblastmi obrazu, tedy rozlišuje světlé a tmavé barvy.

Při úpravách kamery může správce sledovat změny nastavení, ve zmenšeném okně umístěném pod nástroji nastavení. Tento způsob je určen především pro osoby s malými zkušenostmi v oblasti videotechniky.

4.2.1 Registrace uživatele

Pokud je aplikace TEA nastavena podle požadovaných podmínek a je k dispozici databáze uživatelů, lze se přesunout k jednotlivým funkcím. První z nich je registrace uživatelů. Proces biometrické registrace je nezbytný pro získání osobních biometrických údajů uživatele. Postup se skládá ze dvou fází: získávání biometrických údajů a zadávání osobních údajů. Lze také znovu „zapsat“ uživatele, tj. registrovat nové biometrické údaje o uživateli v databázi bez opětovného zadávání osobních údajů. Při registraci je uživatel vyzván, aby předstoupil před Broadway 3D. Při procesu snímání obličeje by uživatel měl dodržovat stanovenou vzdálenost 90 do 120 centimetrů od biometrického zařízení. Pod modelem, který se během snímání vytváří na zobrazovacím zařízení, je uvedena vzdálenost od obličeje. Po dokončení snímání si správce může prohlédnout výsledný model a následně zhodnotit, zda je model vhodný pro použití jako referenční vzorek (šablona) nebo se musí skenování obličeje provést ještě jednou. Kvalita modelu vytvořeného během registrace může být hodnocena na základě hodnoty kvality registrace. Tento parametr může nabývat hodnot mezi 0 a 1000. Rozsah hodnot kvality registrace jsou uvedeny v tabulce č. 1.

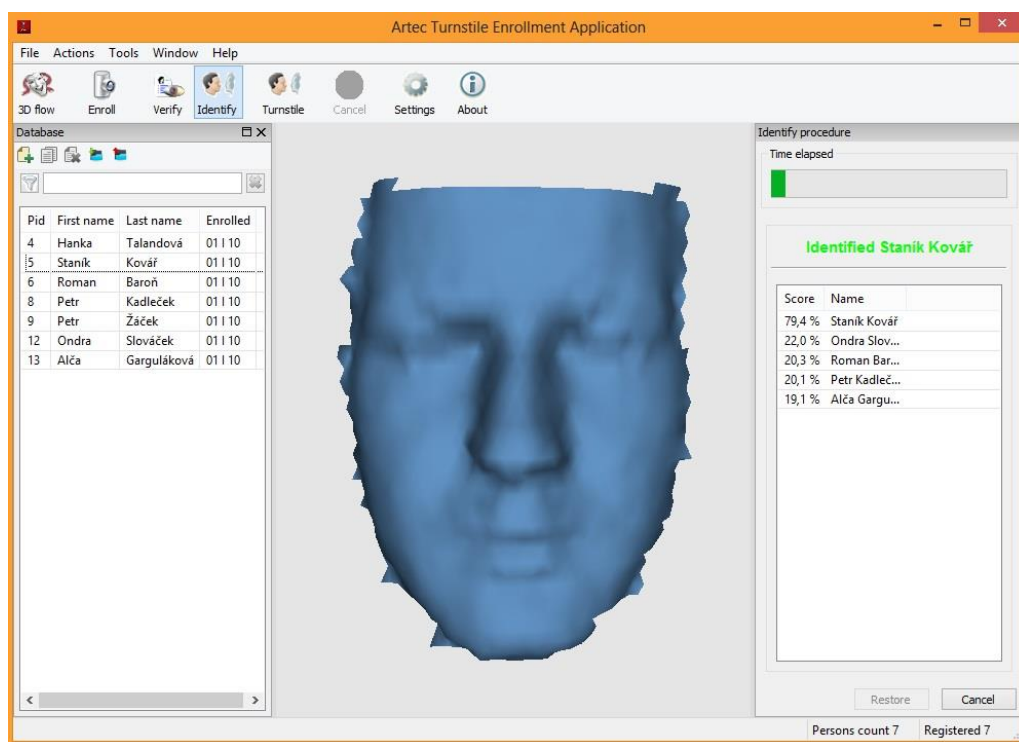
Rozsah hodnot	Kvalita	Barva kvality registrace
0 - 800	špatná	červená
800 - 850	uspokojivá	žlutá
850 - 900	dobrá	světle zelená
900 - 1000	excelentní	zelená

Tabulka 1: Rozsah hodnot kvality registrace

Je-li kvalita získaných dat špatná nebo pouze uspokojivá, měl by se proces registrace opakovat. Každé nově přidané osobě se přiřadí osobní identifikátor, pro snadnější prohledávání rozsáhlých databází. Protože se údaje ukládají do databází, musí se při registraci vyplnit několik osobních údajů, např. jméno, příjmení, datum narození, pohlaví, atd. Všechny tyto informace stejně jako ID uživatele, slouží pro rychlé vyhledávání.

4.2.2 Identifikace uživatele

Proces identifikace uživatele stanoví stupeň shody biometrického vzorku získaného během procesu skenování obličeje a uživatelské šablony uložené v databázi aplikace TEA. Uživatel stejně jako v případě registrace předstoupí ve stanovené vzdálenosti před rozpoznávací jednotku. Biometrické zařízení následně provede sken obličeje a porovnává jej s databází šablon. Rychlost tohoto procesu je závislá na výkonu počítačové jednotky, u výkonnostně slabších počítačů může identifikace trvat i několik minut. Dalším výrazným faktorem, který ovlivňuje rychlost vyhodnocování je kvalita šablony a aktuálního skenu. Mohou nastat situace, kdy vzorek v databázi je velice kvalitní a aktuální skenování nedokáže kvalitu snímku napodobit (mimika, vzdálenost od čtečky, špatná údržba, atd.). Při porovnávání nikdy nedochází ke stoprocentní shodě, vždy se vyskytnou alespoň několika procentní anomálie. Při praktickém měření dosahovala anomálie mezi vzorky i přes 20%.

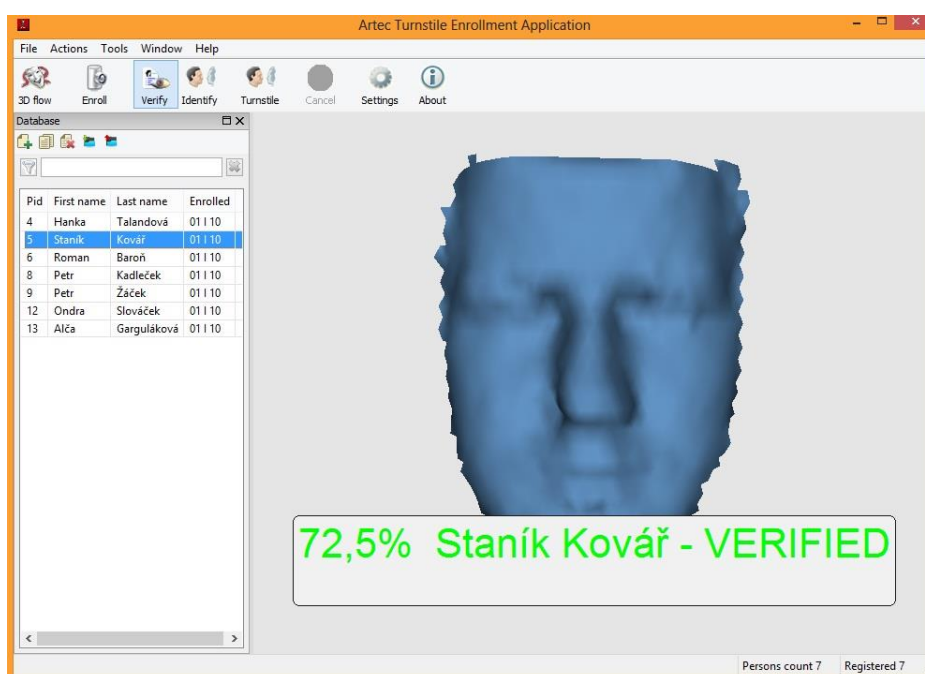


Obrázek 25: Proces identifikace

4.2.3 Verifikace uživatele

Proces verifikace je vlastně identifikace v porovnávání 1:1, tzn. Broadway neprohledává celou databází, ale srovnává údaje konkrétního uživatele. Aplikace TEA umožňuje

provádět verifikaci i bez identifikátoru. Nejedná se o klasickou formu verifikace a pro praktické použití jen těžko realizovatelné. Především se vyžaduje interakce obsluhy, která musí označit jiným způsobem ověřenou osobu a spustit proces verifikace. Systém následně provede srovnání biometrických vzorků a pod 3D modelem zobrazí procentuální shodu (Obrázek 26). V závislosti na nastavených prahových hodnotách systém rozhodne, zda může být uživatel vpuštěn (např. do objektu, jestliže je Broadway propojen s přístupem) či nikoliv. Pokud je biometrické zařízení propojeno s čtečkou karet, lze realizovat proces verifikace po vložení karty do čtečky. Tím se určí konkrétní osoba a verifikace probíhá autonomně, bez přítomnosti obsluhy. Při registraci uživatele, lze nastavit číslo karty, které primárně odpovídá PID v databázi uživatelů.



Obrázek 26: Proces verifikace

4.2.4 Turnstile mode

Nebo-li turniketový (přístupový) režim. Jde o simulovanou podobu grafického zobrazení, jež je vyobrazeno při reálném provozu biometrické čtečky. V tomto režimu lze realizovat všechny tři výše uvedené scénáře: identifikace, verifikace a registrace. Prostřednictvím externích karet, tzv. master card, se přepíná mezi jednotlivými scénáři. Defaultně je aplikací TEA nastavena identifikace uživatele. Tento režim vyžaduje pro svůj provoz rozlišení zobrazovací jednotky 1024×768 , tedy s poměrem stran 4:3. Jednotlivé procesy mají stejný průběh jako v případě webového prohlížeče, tzn. zobrazují se pouze výsledky

vyhodnocení (např. přístup povolen nebo odmítnut) nikoliv údaje o shodě, či jiné informační údaje. Aplikace obsahuje algoritmus, který vyhledá na scéně obličej uživatele a následně provede porovnání s databází. Tento nástroj je vhodný pro měření či testování biometrického zařízení, protože správce na videu z kamery může kontrolovat, zda aplikace označila správnou část těla. Kromě Turnstile mode aplikace TEA nabízí ještě další možnost zjednodušené demonstrace provozu zařízení, jestliže je Broadway použit jako kontrolní bod. Tento režim se nazývá Quick Turstile mode a představuje jednodušší variantu režimu Turnstile, neboť nejsou potřeba žádné master karty, ale přepínání mezi scénáři se provádí v grafickém prostředí aplikace TEA.



Obrázek 27: Turnstile mode

Na závěr podkapitoly následuje malé shrnutí aplikace TEA. Aplikace určena především pro práci s databází uživatelů a jejich biometrickými vzorky. Docení ji hlavně správci přístupových systémů, kteří chtějí získat detailnější informace o uživateli. TEA představuje uživatelsky přívětivější možnost správy databáze a také širší možnosti v nastavení zařízení Broadway 3D. Výjimkou je nastavení kamery, které u aplikace TEA nabízí pouze základní možnosti. Naopak možnost sledování změn nastavení kamery v reálném čase je výhodou především pro začátečníky. Zahrnuje všechny možnosti, které nabízela konfigurace webovým prohlížečem. Největší nevýhodou u aplikace TEA představuje nutnost výkonné počítačové jednotky a grafické karty, což u konfigurace pomocí webového prohlížeče není nutné. S výkonem počítače souvisí čas potřebný pro provedení vybraných operací, které TEA nabízí. U počítačů s nedostatečným výkonem a grafickou kartou se zvyšuje čas potřebný pro registraci uživatelů. Ve výchozím zapojení

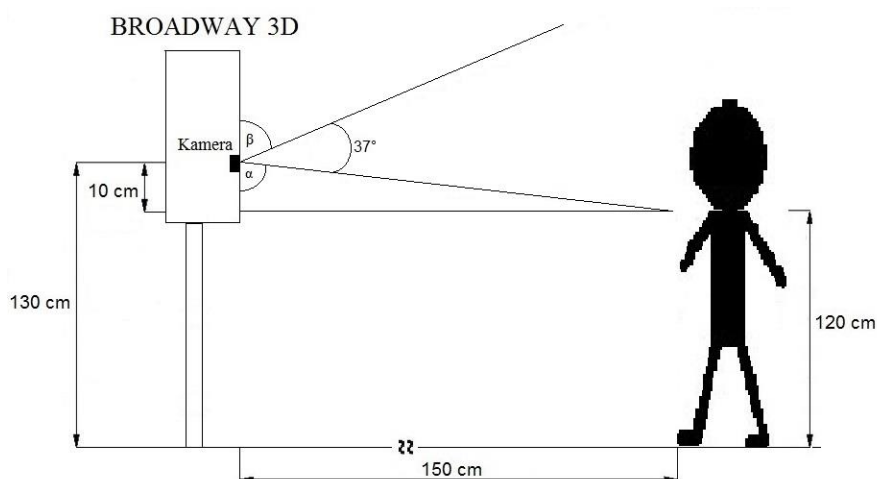
obstarává veškerý výkon počítačová jednotka 1, která obsahuje pouze uloženou databázi a základní (převážně vizualizační) programy. Počítač je tedy optimalizovaný na konkrétní činnost. Aplikace TEA se tedy vyplatí užívat pouze pro případy testování, studentské účely nebo úplné začátečníky v oblasti. Neposkytuje žádné informace o markantech obličeje. Na rozdíl od výrobcem dodávaného SDK nevyžaduje žádné speciální znalosti. Je snadno ovladatelná a instalovatelná.

5 TESTOVÁNÍ BROADWAY 3D

Tato kapitola bude zaměřena na praktické testování biometrické čtečky Broadway 3D. Zhodnotí se přesnost čtečky při procesech identifikace, verifikace na základě kvality 3D modelu při registraci uživatelů. Veškeré testovací situace vycházejí z teoretických znalostí čtečky a biometrie obličeje.

Všechny informace o osobách jsou zveřejněny na základě jejich souhlasu.

Biometrická čtečka Broadway 3D je postavena na stativu ve výšce cca 125 cm, kvůli stabilitě a širokému výškovému rozsahu při snímání osob (spolehlivě pracuje s osobami malého i velkého vzrůstu). Společnost Artic Group garantuje u biometrické čtečky snímací úhel pro horizontální směr v rozmezí 41° až 43°. Tedy takový rozsah, aby Broadway spolehlivě identifikovalo i osoby na vozíčku, případně děti. Aby byla tato podmínka splněna, musí se čtečka umístit do vhodné výšky, protože rozsah úhlu v horizontálním směru není symetrický. Jestliže se kamera biometrické čtečky nachází cca 130 cm vysoko, bylo měřením určeno, že výška člověka musí být minimálně v rozmezí 135 až 140 cm (v závislosti na velikosti hlavy). Brada se musí nacházet nejméně ve výšce 120 cm. U dětí či osob na vozíčku se zkracuje maximální vzdálenost pro identifikaci ze 180 cm na 150 cm. Při testování bylo zjištěno, že u vyšších vzdáleností nebyla čtečka schopna uživatele rozpoznat.



Obrázek 28: Schéma pro výpočet úhlů α a β

Podle základních vzorců pro výpočet pravoúhlého trojúhelníku se vypočítá hodnota úhlu α .

$$\operatorname{tg} \alpha = \frac{a}{b} = \frac{150}{10} = 15 \Rightarrow \alpha = 86^\circ$$

Kamera zachytí snímáný objekt při úhlu zhruba 86° od země. Úhel se bude lišit (cca o 1 až 2 stupně) v závislosti na vzdálenosti od čtečky. Hodnoty uvedené v obrázku výše byly zjištěny na základě praktických podmínek pro měření. Údaj 10 cm se určí jako rozdíl výšky kamery od země (130 cm) a minimální výšky člověka při identifikaci, resp. vzdálenost brady od země. Aplikace TEA snížila možnosti Broadway 3D na tolik, že zařízení uživatele vůbec nevidovalo ani při výšce 150 cm. Obdobným způsobem se určila i hodnota β . Nejprve se zjistila nejmenší vzdálenost, ve které byla čtečka schopna uživatele identifikovat, při stanovené výšce 220 cm. Určil se rozdíl mezi výškami 220 cm a 130 cm a výsledná hodnota se uvede do následujícího vzorce. Vzdálenost uživatele od kamery byla 140 cm.

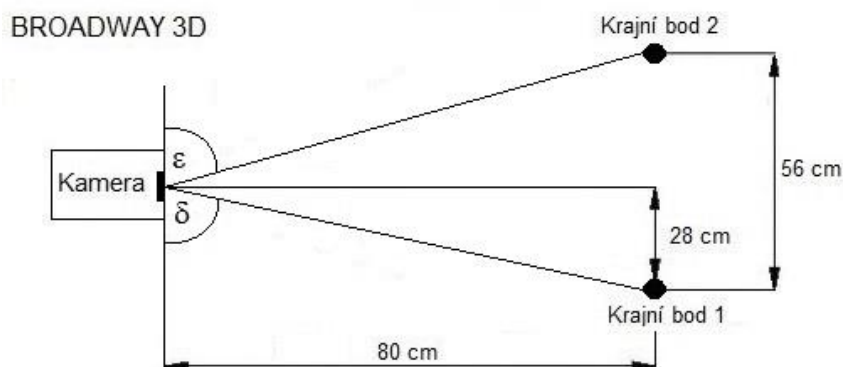
$$\operatorname{tg} \beta = \frac{a}{b} = \frac{140}{90} = 1,56 \Rightarrow \beta = 57^\circ$$

Z vypočítaných hodnot úhlů α a β , lze snadno určit úhel pro snímání osob, takto:

$$\chi = 180^\circ - (\alpha + \beta) = 180^\circ - 143^\circ = 37^\circ$$

Z výsledku vyplývá, že skutečný snímací úhel je 37° . Nesplňuje ovšem výrobcem stanovený vertikální úhel v rozmezí 41° až 43° . Je nutné vzít v úvahu i toleranci způsobenou nepřesnostmi při měření. Výsledná hodnota se ve skutečnosti může lišit o jeden až dva stupně.

Při výpočtu horizontálního snímacího úhlu se postupovalo obdobně. Určily se krajní body, ve kterých je zařízení ještě schopno identifikovat uživatele, při vzdálenosti 80 cm od kamery čtečky. Vzdálenost mezi krajními body je 56 cm. Předpokladem pro výpočet úhlu δ je osová souměrnost obou bodů od potenciálního středu kamery.



Obrázek 29: Schéma pro výpočet úhlu δ a ε

Úhel δ se vypočítá stejně jako v předešlých případech.

$$\operatorname{tg} \delta = \frac{a}{b} = \frac{80}{28} = 2,86 \Rightarrow \alpha = 70^\circ$$

Za předpokladu osově souměrnosti bude úhel ε roven úhlu δ . Úhel η se vypočítá následovně:

$$\eta = 180^\circ - (\delta + \varepsilon) = 180^\circ - 140^\circ = 40^\circ$$

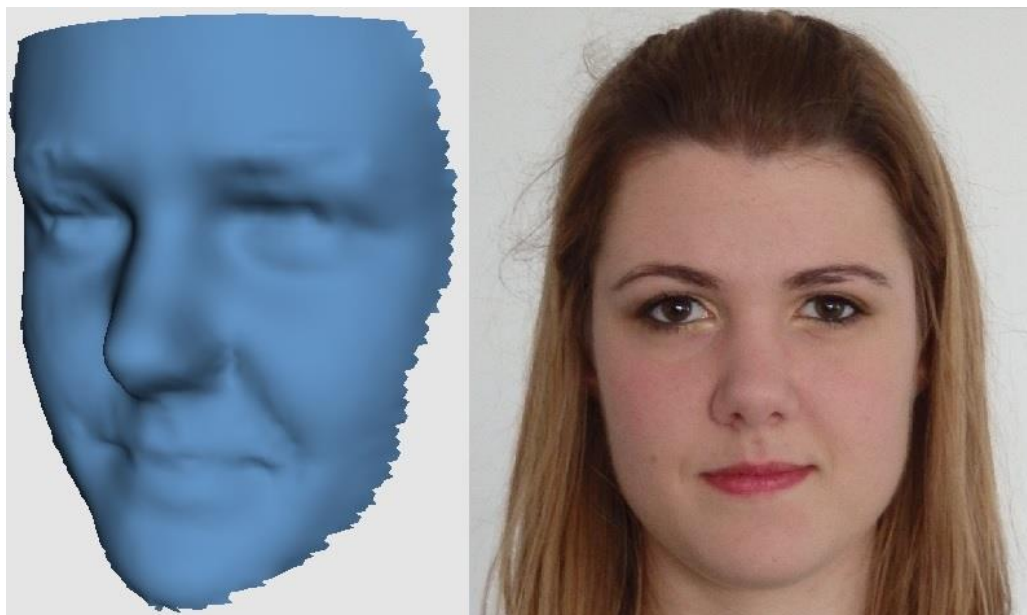
Výsledný snímací úhel bude tedy větší, než výrobcem garantovaný úhel. U výpočtu je třeba počítat s tolerancí jednoho až dva stupně, způsobenou nepřesnostmi u měření.

Zohlednit se také musí podmínky osvětlení v místnosti, které jsou v každé situaci rozdílné. Vzhledem k přítomnosti IR přísvitů u kamery, rozdílné podmínky nepředstavovaly problém. Naopak procesy registrace i následné identifikace a verifikace byly provedeny spolehlivě i za snížených světelných podmínek. Prakticky se vyzkoušelo i snímání obličeje s využitím externího osvětlení. Biometrická čtečka si i v těchto situacích poradila, aniž by se došlo k výrazným změnám při jednotlivých procesech. Během testování se zjistilo, že největší vliv má silný světelný zdroj umístěný za zády uživatele. Při denním světle zvýšil takto umístěný zdroj světla spolehlivost zařízení o více než 5%. Oproti tomu při snížených světelných podmínkách působil zdroj světla potíže a snižoval schopnosti biometrické čtečky. Zdroj byl ve vzdálenosti 3,46m od kamery biometrické čtečky, na kterou dopadalo osvětlení 698.73 luxů. Jako zdroj světla byla použita ruční svítilna o světelném toku 200 lumenů.

Při testování se pracuje s aplikací Turnstile Enrollment Application, která sice snižuje provozní možnosti biometrické čtečky, ale je vhodná pro dané účely.

5.1 Registrace

V procesu registrace uživatelů se využilo optimálního výchozího zapojení, při němž se pracuje s webovým prohlížečem. Tato metoda byla zvolena především kvůli rychlosti a kvalitě registrace osob. Kvalita šablony se kontroluje prostřednictvím aplikace Turnstile Enrollment Application, viz. tabulka 1 (Kapitola 4.2), přičemž by kvalita snímku měla přesahovat hodnotu 900. Praktické testování ukázalo, že průměrná hodnota kvality šablony se pohybuje kolem 912. Čím vyšší bude hodnota kvality, tím lepší výsledky budou v procesech verifikace a identifikace.



Obrázek 30: Ukázka 3D modelu a předlohy

Z ukázky si lze udělat představu o kvalitě modelu vzhledem k jeho předloze. Více obrázků k porovnání je k dispozici v příloze. Následující obrázek obsahuje informace o osobě, včetně informace o kvalitě šablony. Hodnota je doplněna barvou podle rozsahu kvality.

The image is a screenshot of a software window titled "Person's Info". The window is divided into two main sections: "Info" and "Photo".
The "Info" section contains several input fields and a dropdown menu:
- First name: "Alča" (highlighted in blue)
- Middle name: empty field
- Last name: "Garguláková"
- Birth date: "14. 4. 2014" (with a calendar icon)
- Sex: "female" (dropdown menu)
- Card number: "13"
- Facility code: "255"
- Card format: "Wiegand26" (dropdown menu)
- Below these fields is a "Generate" button.
- Enroll date: "01 leden 2010"
- Enroll cam.: "XX.00.00000000"
- Enroll dist.: empty field
- Enroll qual.: "901" (highlighted in green)
The "Photo" section shows a dark, low-quality image of a person's face. Below the photo are two radio buttons:
- "From database" (selected)
- "Loaded"
A "Load..." button is located to the right of the "Loaded" radio button.
At the bottom of the window are two buttons: "Apply & Close" and "Cancel".

Obrázek 31: Informace o uživateli

Registrace byla výrazně obtížnější u dívek, které mají dlouhé vlasy. Vlasy v mnohých případech spadávají do tváře a snižují viditelnou plochu obličeje, což se projeví na výsledné kvalitě šablony. Proto bylo mnohdy nutné proces registrace opakovat, aby se

dosáhlo přijatelné kvality. I přesto se kvalita šablony pohybovala na hranici uspokojivé až dobré, tedy kolem hodnoty 850. V případě ‚dobré‘ kvality šablony mohou nastat problémy při opakovaných identifikacích a verifikacích. Ovšem uživatelé s nízkou kvalitou šablony, u kterých byl proces ověřování testován např. po měsíci, měli mnohokrát problémy a dosahovali velice nízkých výsledků (záleží na stanovené hranici – Threshold). Dalším problémem při registraci osob byly dioptrické brýle, které výrazně snižovaly kvalitu vzniklého modelu. Proto se musela provádět registrace bez brýlí.

Výrobce zařízení doporučuje provádět registraci ve vzdálenosti 80 až 120 cm, ovšem reálný rozsah při zachování dostatečné kvality šablony může být řádově o jednotky cm vyšší. Během procesu registrace je uživatel v případě špatné aktuální polohy upozorňován na změnu pozice (posun směrem ke kameře, či od ní). U aplikace TEA byly problémy se sníženými možnostmi biometrické čtečky vlivem neoptimálního zapojení a techniky. Proto byl čas na registraci výrazně prodloužen (více než 5 minut) a vzdálenost byla zkrácena maximálně do 120 cm od kamery. Taková situace je v praxi nežádoucí.

5.2 Identifikace

Proces identifikace byl realizován jak ve výchozím zapojení, tak prostřednictvím aplikace TEA. TEA umožňuje zobrazit procentuální shodu biometrického vzorku s šablonou, proto byla výhodnější. Navíc zobrazuje i procentuální shodu jiných biometrických vzorků s aktuálním snímkem. Identifikace bude rozdělena podle pohlaví kvůli rozdílným charakteristikám u mužů a žen. Toto rozdělení bylo zvoleno především kvůli procesům verifikace uvedené v následující podkapitole.

Při procesech identifikování a ověřování uživatelé očekávají, že nebudou omezováni (zastavením před čtečkou, díváním do kamery, apod.). Broadway 3D ve výchozím zapojení takové požadavky splní. Testováním bylo určeno, že uživatel může sklonit hlavu směrem dolů o cca. 80°, aniž by byly problémy s rozpoznáním, tzn. že při kontrole mohou lidé číst, používat telefon, atd. V horizontálním směru lze natáčet hlavu v rozmezí 90°, tzn. 45° na každou stranu od středu (kamery).

Identifikace a verifikace není oproti registraci tak limitovaná vzdáleností. Limit samozřejmě čtečka má, ale s výrazně vyšším rozsahem než tomu bylo u registrace. Ve výchozím zapojení se vzdálenost při identifikaci pohybovala v rozmezí 50 až 180 cm od

kamery čtečky. Verifikaci nebylo možné realizovat, kvůli absenci čtečky karet. U aplikace TEA, jak již bylo několikrát zmíněno, nebylo možné využít plný potenciál Broadway 3D ani v tomto ohledu. Vzdálenost se pohybovala jen v registračním rozsahu a u vzdáleností vyšších, resp. nižších biometrické zařízení nebylo často schopno identifikaci provést.

Vzdálenost [cm]	Průměrná hodnota
120,0	69,5
110,0	71,2
100,0	72,9
90,0	74,0
80,0	75,9

Tabulka 2: Závislost identifikace na vzdálenosti

V tabulkách jsou uvedeny průměrné hodnoty jednotlivých uživatelů, kterých dosahovali při různých prahových hodnotách. Tabulka 3 představuje výsledky identifikace a tabulka 4 výsledky FRR, tedy chybné odmítnutí autorizovaných uživatelů biometrickou čtečkou Broadway 3D. Výsledky False Rejection Rate byly určeny na základě jednotlivých identifikací konkrétních uživatelů. Obě tabulky znázorňují pouze výsledky pánů.

Výsledky identifikace - pánové:

Identifikace		Pan T.	Pan P.	Pan K.	Pan O.	Pan Š.	Pan G.	Pan M.	Pan R.
prahová hodnota	průměrná hodnota								
60%	71,8	64,8	62,3	66,1	79,5	79,2	67,2	77,2	78,0
70%	74,7	73,2	78,3	73,1		78,9	65,2	76,0	76,4
80%	78,4	74,1	82,4			81,0	77,4	74,9	80,4
90%	75,5	72,0	85,0			74,8	57,6	79,7	

Tabulka 3: Identifikace - pánové

Výsledky False Rejection Rate u identifikace - pánové:

FRR - identifikace		Pan T.	Pan P.	Pan K.	Pan O.	Pan Š.	Pan G.	Pan M.	Pan R.
prahová hodnota	průměrná hodnota								
60%	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
70%	13,9	0,0	33,3	0,0		0,0	50,0	0,0	0,0
80%	28,7	60,0	0,0			28,6	33,3	50,0	0,0
90%	93,3	100,0	100,0			100,0	100,0	80,0	

Tabulka 4: FRR - identifikace - pánové

Z výsledků je patrné, že u prahových hodnot 60 a 70%, probíhá identifikace bez problémů. Pánové Š. a M. dosahovali při 60% prahové hodnoty vyšších výsledků než ostatní uživatelé a to i přes skutečnost, že kvalita jejich šablony byla nižší než pánů T. a R. Pan R. měl excelentní kvalitu šablony, což se projevilo i na výsledcích. Jako jediní byli čtečkou téměř pravidelně identifikováni i při prahové hodnotě 80% pouze pánové P. a R. U pana O. byla provedena jen jedna série testů a to pro prahovou hodnotu 60%, během které byl spolehlivě zařízením identifikován. Biometrická čtečka vykazovala problémy při identifikaci pan G., který nosí dioptrické brýle. Bez brýlí nedocházelo k tak častým odmítnutím. Pan P. dosahoval při prahové hodnotě 80% a 90% vyšších výsledků z důvodu registrace nového biometrického vzorku. S předešlou šablonou nedosahoval uspokojivých výsledků. U ostatních uživatelů se identifikace při prahové hodnotě vyšší než 70% povedla jen výjimečně. Chybné odmítnutí oprávněného uživatele při treshold nižší než 70% byla způsobena převážně nízkou kvalitou a hlavně dlouhým časovým intervalem mezi procesy registrace a identifikace (cca. měsíc).

Následující dvě tabulky představují stejnou situaci, ale u dam. Na začátku je třeba zdůraznit, že kvalita biometrických šablon u dam byla výrazně nižší než u pánů.

Výsledky identifikace - dámy:

Identifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.
prahová hodnota	průměrná hodnota					
60%	69,8	65,8	65,9	67,1	66,4	83,7
70%	73,7	70,5	70,7	69,6	71,3	83,2
80%	73,6		61,4	71,7	80,5	80,7
90%	79,6				69,3	89,8

Tabulka 5: Identifikace - dámy

Výsledky False Rejection Rate u identifikace - dámy:

FRR - identifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.
prahová hodnota	průměrná hodnota					
60%	0,0	0,0	0,0	0,0	0,0	0,0
70%	8,4	16,7	16,7	16,7	0,0	0,0
80%	45,8		100,0	83,3	0,0	0,0
90%	66,7				100,0	33,3

Tabulka 6: FRR - identifikace - dámy

Nižší kvalita šablony je zjevná z výsledků tabulek. U dam se i přes opakované pokusy registrace nepodařilo vytvořit dostatečně kvalitní šablony. Hodnota kvality se pohybovala na hranici 900. S výjimkou slečny P., která dosahovala nejlepší výsledků ze všech testovaných subjektů. Jako jediná žena byla pravidelně identifikována biometrickou čtečkou i při prahové hodnotě 80%. Provádění testování s prahovou hodnotou 90% nemělo smysl, vzhledem k neuspokojivým výsledkům u hodnoty 80%.

Z testování čtečky Broadway 3D vyplývá, že čtečka snadno identifikuje uživatele při hodnotě threshold 60%. Hodnotu 70% lze považovat za spolehlivou především u kvalitních biometrických šablon. Vzhledem ke skutečnosti, že v praxi se nerozlišuje mezi pohlavími, je nezbytné klást důraz na registraci žen, aby nedocházelo v provozu k chybným odmítnutím autorizovaných osob. Broadway identifikuje i více uživatelů pohybujících se na snímané scéně.

Identifikace ve výchozím zapojení, kdy počítačová jednotka 2 slouží pouze pro práci s databází, neposkytovala žádné detailní informace o shodě. Čtečka pouze vyhodnotí uživatele jako oprávněného či nikoliv. Výsledky identifikace budou vyhodnoceny až v podkapitole Verifikace, protože v tomto případě není možnost verifikace (absence čtečky karet) a výsledky souvisí s testováním verifikace.

5.3 Verifikace

Testování kvality verifikace bylo možné provést pouze prostřednictvím aplikace TEA, protože zařízení Broadway je primárně určeno pro identifikaci. TEA poskytuje informace o výsledcích verifikace, které jsou zaznamenány v této podkapitole. Celou podkapitolu Verifikace lze rozdělit do dvou částí. První částí je ekvivalent předcházející kapitoly, kde se účastníci testování rozdělí dle pohlaví. Určí se průměrná hodnota verifikace pro jednotlivé uživatele a následně celou skupinu. Verifikace se bude provádět pro rozdílné prahové hodnoty. V druhé části budou uvedeny výsledky z testování použitých grimas či pokrývek hlavy, apod. Tato část už nebude obsahovat měnící se prahové hodnoty, ale bude nastavena jedna výchozí hodnota. Konkrétně bude Threshold roven 70%. Obě části budou navíc doplněny o výsledky False Rejection Rate (kapitola 2.2). Čas potřebný na verifikaci byl nastaven na 10 sekund.

Výsledky verifikace - dámy:

Verifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.
prahová hodnota	průměrná hodnota					
60%	65,7	54,6	64,7	64,5	67,3	77,5
70%	72,6	70,1	73,0	69,1	71,5	79,2
80%	74,9	65,2		71,7	74,0	81,7
90%	84,8				81,9	87,7

Tabulka 7: Verifikace - dámy

Výsledky False Rejection Rate u verifikace - dámy:

FRR - verifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.
prahová hodnota	průměrná hodnota					
60%	0,0	0,0	0,0	0,0	0,0	0,0
70%	14,3	28,6	0,0	42,9	0,0	0,0
80%	65,0	100,0		100,0	60,0	0,0
90%	92,9				100,0	85,7

Tabulka 8: FRR - verifikace - dámy

V případě verifikace uživatelé dosahovali výrazně nižších výsledků než v případě identifikace. Během testování nebyl zjištěn žádný případ, kdy byl subjekt vyhodnocen systémem jako někdo jiný (FAR). Verifikace stejně jako identifikace byla bezproblémová u prahových hodnot 60% a 70%. Vyšší treshold měl význam pouze u slečny P., která byla výjimečně identifikována i při hodnotě 90%.

Výsledky verifikace - pánové:

Verifikace		Pan T.	Pan P.	Pan M.	Pan O.	Pan R.
prahová hodnota	průměrná hodnota					
60%	69,9	66,7	63,6	77,7	75,0	66,2
70%	70,6	71,5	63,7	74,8	71,4	71,7
80%	74,6	72,2	67,3	79,1	74,0	80,3
90%	75,7	73,1				78,3

Tabulka 9: Verifikace - pánové

Výsledky False Rejection Rate u verifikace - pánové:

FRR - Verifikace		Pan T.	Pan P.	Pan M.	Pan O.	Pan R.
prahová hodnota	průměrná hodnota					
60%	0,0	0,0	0,0	0,0	0,0	0,0
70%	20,0	0,0	100,0	0,0	0,0	0,0
80%	73,3	66,7	100,0	83,3	100,0	16,7
90%	91,7	83,3				100,0

Tabulka 10: FRR - verifikace - pánové

Pánové dosahovali o něco slabších výsledků než dámy, s čímž souvisí i průměrný počet chybných odmítnutí. Nastavení treshold na hodnotu 80% a vyšší nemá smysl. Avšak je třeba zdůraznit, že za horšími výsledky stojí mimo jiné neoptimalizovaný počítač s instalovanou aplikací TEA.

Další část testování bude zaměřená na hodnocení kvality verifikace při zakrytí hlavy běžnými pomůckami (brýle, čepice, atd.) či použití grimas (úsměv, atd.). Hodnotily se též výsledky po fyzické zátěži, či pohybu uživatele směrem ke, resp. kolem čtečky. Testování bude opět rozděleno dle pohlaví. Prahová hodnota verifikace byla nastavena na 70% a čas na 10s.

Výsledky verifikace při zakrytí tváře nebo grimase - dámy:

Verifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.	Slečna T.
	průměrná hodnota						
úsměv	43,9	19,8			42,2	73,5	40,0
zavřené oči	68,4	68,4					
sluneční brýle	68,9	62,9	65,4	73,6	60,9	77,9	72,5
dioptrické brýle	67,2		66,1	64,6	63,1	73,3	68,7
zívání	24,1	20,7					27,4
červená paruka	71,1		67,2	69,6	69,3	78,2	
blond paruka	68,7		69,4		63,2	73,5	
pohyb ke čtečce	57,6		35,5	70,8	62,0		62,1

Tabulka 11: Verifikace při zakrytí obličeje - dámy

Výsledky False Rejection Rate u verifikace při zakrytí tváře nebo grimase - dámy:

FRR - Verifikace		Slečna A.	Slečna H.	Slečna V.	Slečna D.	Slečna P.	Slečna T.
	průměrná hodnota						
úsmev	100,0	100,0			100,0	100,0	100,0
zavřené oči	0,0	0,0					
sluneční brýle	26,2	0,0	57,1	0,0	83,3	0,0	16,7
dioptrické brýle	55,6		57,1	87,5	100,0	0,0	33,3
zívání	100,0	100,0					100,0
červená paruka	26,2		71,4	16,7	16,7	0,0	
blond paruka	44,4		50,0		83,3	0,0	
pohyb ke čtečce	42,9		100,0	0,0	71,4		0,0

Tabulka 12: FRR - verifikace při zakrytí obličeje - dámy

Pohyb ke čtečce vyžadoval snížení treshold ze 70% na 60%, aby se dosáhlo alespoň nějakých úspěchů.

Výsledky verifikace při zakrytí tváře nebo grimase - pánové:

Verifikace		Pan T.	Pan P.	Pan K.	Pan O.	Pan Š.	Pan M.	Pan R.
	průměrná hodnota							
úsmev	42,5	45,0	46,0	56,3	15,2	40,2	51,5	43,2
zavřené oči	72,2	74,2	75,1	64,6	74,7			
mrkání	66,0	72,4	64,7	65,3	61,7			
sluneční brýle	66,8	56,0		61,4		73,3	73,1	70,3
dioptrické brýle	66,5					65,4	65,3	67,0
zívání	33,8	35,5		32,0				
čepice	63,1				63,1			73,4
červená paruka	69,6			64,3		73,8	72,8	67,6
blond paruka	62,6			54,4				70,7
fyzická zátěž	72,4				70,1	72,4	72,1	74,8

Tabulka 13: Verifikace při zakrytí obličeje - pánové.

Výsledky False Rejection Rate u verifikace při zakrytí tváře nebo grimase - pánové:

FRR - Verifikace		Pan T.	Pan P.	Pan K.	Pan O.	Pan Š.	Pan M.	Pan R.
	průměrná hodnota							
úsmev	97,1	100,0	100,0	80,0	100,0	100,0	100,0	100,0
zavřené oči	5,0	0,0	20,0	0,0	0,0			
mrkání	10,0	20,0		0,0				
sluneční brýle	35,2	100,0	80,0	0,0	50,0	0,0	0,0	16,7
dioptrické brýle	79,4					71,4	66,7	100,0
zívání	100,0	100,0		100,0				
čepice	0,0				0,0			0,0
červená paruka	20,8			83,3		0,0	0,0	0,0
blond paruka	50,0			100,0				0,0
fyzická zátěž	0,0				0,0	0,0	0,0	0,0

Tabulka 14: FRR - verifikace při zakrytí obličeje - pánové

Během testování bylo zjištěno, že Broadway při verifikaci i identifikaci reaguje především na změnu svalů kolem úst. Jedná se především o následující svaly:

- Svaly zavírající ústa člověka:
 - spánkový sval,
 - zevní sval žvýkací,
 - vnitřní křídlový sval – pomocný sval.
- Svaly otevírající ústa člověka:
 - zevní křídlový sval.
- Svaly mimické:
 - kruhový sval ústní – svírá, resp. špulí rty,
 - smíchový sval.

Tyto informace byly získány na základě změn těchto svalů při úsměvu, či zívání. Naopak zakrytí očí dioptrickými nebo slunečními brýlemi proběhlo více méně bez problémů. U dioptrických brýlí byly problémy při verifikaci výrazně větší než u slunečních brýlí s reflexní povrchovou vrstvou. Reflexní vrstva na slunečních brýlích způsobila na vzniklém modelu v místech očí bílé čtverečky, odpovídající obsahu brýlí. Pokrývky hlavy (čepice) nepředstavovaly pro biometrickou čtečku žádný problém a uživatelé byli spolehlivě verifikováni. Dámy, které použily při verifikaci paruky, byly systémem chybně

verifikovány především v případě blond paruky. Tato paruka v podstatě prodlužovala původní délku původních vlasů, což působilo čtečce potíže. Změnou barvy vlasů se Broadway nezabývá. Zajímavější je skutečnost, že u pánů byly problémy menší. Přestože testované subjekty měly převážně krátké vlasy a tudíž byla tvář viditelnější (žádné zakrývání obličeje padajícími vlasy, apod.), nepůsobily paruky simulující dlouhé vlasy nesnáze. Jinak řečeno, kvalita šablony byla natolik dobrá, že byla verifikace ve většině případů úspěšná i přes sníženou plochu snímaného obličeje. Tím lze dokázat, že nejdůležitější markanty jsou v oblasti úst. Průměrná pravděpodobnost chybného odmítnutí autorizované osoby vzrostla o necelých 6% u blond paruky a naopak o 5,4% klesla u červené kudrnaté paruky. Červená paruka je vyrobena do stylu afro, tudíž nespadá směrem k ramenům, jako blond paruka.

Kromě mimických, resp. ústních svalů představoval pro Broadway 3D problém též sval čelní. Ten se stará o zdvih obočí, čímž vznikají vrásky. Toto měření vykazovalo nerovnoměrné výsledky a v tabulce není uvedeno kvůli malému množství testovaných subjektů. Průměrná pravděpodobnost chyby při verifikaci autorizovaných osob byla stanovena na hodnotu 83,3%, tedy velice vysoká. Vzhledem ke skutečnosti, že vrásky se vytváří v průběhu let, je vhodné obnovovat biometrickou šablonu nejméně jednou za dva až tři roky.

Na závěr testování se vyzkoušelo, zda bude mít na verifikaci vliv fyzická zátěž člověka. Vybraní uživatelé se podrobili fyzické činnosti a následně proběhl proces verifikace. Dle očekávání neměla žádný vliv, tzn. autorizovaný uživatel bude vyhodnocen jako oprávněný, i po výraznější fyzické činnosti. Dámy vyzkoušely vliv make-upu při verifikaci. Ten ovšem stejně jako fyzická zátěž neměl vliv na správné porovnání uživatelů.

V poslední části podkapitoly Identifikace bylo poukázáno na souvislosti s touto kapitolou. Jak již bylo řečeno, ve výchozím zapojení není kvůli absenci čtečky karet možné realizovat proces verifikace. Proto se kvalita zařízení Broadway 3D určovala pomocí identifikace. K dispozici byly všechny pomůcky popsány v této kapitole. Absence aplikace TEA umožní provádět identifikaci v rozsahu 50 až 180 cm od čtečky. Navíc dosahuje výrazně lepších výsledků při ověřování osob pohybujících se kolem čtečky. Přehled výsledků obsahuje následující tabulka.

	přímý pohled	chůze
sluneční brýle	ano	ano
dioptrické brýle	ano	ne
červená paruka	ano	ano
blond paruka	ano	ano
úsměv	ne	ne

Tabulka 15: Výsledky identifikace

Identifikace uživatele stojícího přímo proti biometrické čtečce se slunečními brýlemi proběhla v pořádku. Nicméně ověření uživatele během chůze bylo problematictější. Uživatel se musel podívat přímo do kamery, aby byl zařízením identifikován. Nesnáze nastaly s dioptrickými brýlemi, kdy ověření přímým pohledem proběhlo až po uplynutí delšího časového intervalu. Během chůze zařízení mnohokrát uživatele s dioptrickými brýlemi ani nevidovalo. S identifikací osoby s parukami si čtečka poradila hravě, jen u blond paruky byly ze začátku potíže (první ověření trvalo delší dobu). Ověření úsměvu proběhlo se stejnými výsledky jako u verifikace. Problémem zůstává výrobcem garantovaná správná identifikace či verifikace za chůze. Podle technických manuálů je biometrická čtečka schopna rozpoznat uživatele při rychlosti chůze do 5 km/h. V praxi se stávalo, že zařízení procházejícího uživatele ani nezaznamenalo, pokud nesnížil rychlost chůze alespoň na polovinu nebo méně.

ZÁVĚR

Biometrické systémy zaujaly významné postavení v oblasti bezpečnosti. Důvodem je jejich spolehlivost, rychlost, bezpečnost a jednoznačnost při identifikaci a verifikaci osob. Nasazení biometrických čteček k rozpoznání obličeje člověka zvyšuje komfort a snižuje čas potřebný na rozpoznání. V budoucnu lze předpokládat další vývoj biometrických systémů a s tím spojené využití v přístupových systémech.

Cílem práce bylo testování biometrické čtečky pro identifikaci osob Broadway 3D. Při testování se vycházelo z teoretických znalostí v oblasti biometrie. Teoretická část práce se zaměřuje na interpretaci základních pojmů v dané oblasti, dále na spolehlivost biometrických systémů v jednotlivých situacích. Poslední část se věnuje některým typům fyziologických biometrických čteček, popisu jejich činností a informací vztahující se ke konkrétnímu biometrickému prvku (prst, oko, obličej, atd.).

Praktická část je zaměřena na představení biometrické čtečky Broadway 3D, včetně jejich technických parametrů. Zahrnuje možnosti konfigurace biometrického zařízení a řízení, prostřednictvím aplikačního softwaru Turnstile Enrollment Application, popis funkčních možností aplikace a dalších důležitých informací, potřebných pro konečné testování. Závěr práce obsahuje detailní popis testování procesů registrace, identifikace a verifikace. Porovnání skutečných dovedností biometrické čtečky s výrobcem garantovanými dovednostmi. Prezentování výsledků z jednotlivých procesů včetně jejich hodnocení.

Biometrická čtečka Broadway 3D je výborná volba pro přístupové systémy v objektech s velkou frekvencí osob. Avšak není úplně spolehlivá ve všech výrobcem garantovaných situacích. Zvláště problematická je identifikace za chůze. Zařízení se dodává s SDK, které ovšem vyžaduje rozsáhlé znalosti programovacího jazyku C++. Dalším problémem jsou chybějící knihovny a popis v manuálu, který byl určený jen pro získání dat ze zařízení, nikoliv však pro zprovoznění SDK. Naštěstí existuje alternativní aplikace TEA, která alespoň částečně zvládne nahradit SDK. Závěrem je třeba dodat, že biometrickou čtečku Broadway 3D lze považovat za kvalitní zařízení, kde klady převyšují zápory.

ZÁVĚR V ANGLIČTINĚ

Biometric systems have become an important part of the security. The reason is their reliability, speed, security and the clarity in the identification and verification of the people. The deployment of biometric readers for recognition of human faces increases comfort and reduces the time needed for recognition. In the future, we can expect additional development of biometric systems, coupled with the use in access control systems.

The object of this thesis was testing of biometric reader Broadway 3D, which is used for identification of the people Broadway 3D. The testing procedure was based on the theoretical knowledge in the domain of biometrics. The theoretical part is focused to the interpretation of the basic concepts in that domain and also in explanation of the reliability of biometric systems in specific situations. The last part writes about types of physiological biometric readers, description of their operation and information related to a specific of a biometric element (finger, eye, face, etc.).

The practical part is focused to presenting biometric readers Broadway 3D, including their technical parameters. It also includes configuration options of biometric devices and its controls through application software Turnstile Enrollment Application and also description of application's functional possibilities and the other important information needed for final testing. The conclusion contains a detailed description of the testing processes of registration, identification and verification. Comparison of real biometric reader's skills with a skills guaranteed by a manufacturer. Presentation of results from individual processes and their evaluation.

Biometric reader Broadway 3D is an excellent choice for access systems in buildings with a high frequency of people. However, it is not completely reliable in all situations guaranteed by the manufacturer. Especially it is problematic identification for walking people. The device comes with the SDK, which requires large knowledge of the programming in language C++. Another problem with SDK is the absence of library and description in the manual, which was only intended to get data from the device, but not for launching SDK. Fortunately there is an alternative application TEA, which is at least partly able to replace the SDK. Finally, we can state that the biometric reader Broadway 3D could be considered as a quality device where positives outweigh the negatives.

SEZNAM POUŽITÉ LITERATURY

- [1] RAK, Roman. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.
- [2] JANEČEK, Tomáš. Biometrika[online] [cit. 2014-01-21]. Dostupné z <http://www.nula.wz.cz/biometrika/>.
- [3] Biometrie otisku prstu. *Biometrie* [online]. © 2011-2014 [cit. 2014-01-20]. Dostupné z: <http://www.biometricke-ctecy.cz/biometriky/otisk-prstu/>.
- [4] *BIOMETRIE - Technologie žil hřbetu / dlaně ruky* [online]. 2006 [cit. 2014-01-21]. Dostupné z: <http://www.biometricke-systemy.cz/>.
- [5] ADAMEC, Lukáš. *Testování biometrického systému založeného na dynamice podpisu* [online]. Brno, 2011 [cit. 2014-01-26]. Dostupné z: is.muni.cz/th/208425/fi_m/xadamec1_DiplomaThesis.pdf. Diplomová práce. Masarykova univerzita.
- [6] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.
- [7] *Biometrie* [online]. © 2011-2014 [cit. 2014-04-13]. Dostupné z: <http://www.biometricke-ctecy.cz/>
- [8] ARTEC GROUP, Inc. *Turnstile Enrollment Application: User Manual*. Luxembourg, 2011.
- [9] ARTEC GROUP, Inc. *Broadway 3D: Uživatelský manuál*. Brno, [2011].
- [10] MARIEB, Elaine N. *Anatomie lidského těla*. 1. vyd. Brno: CP Books, 2005, 863 s. ISBN 80-251-0066-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

- FAR False Acceptance Rate – pravděpodobnost chybného přijetí neautorizované osoby.
- FRR False Rejection Rate – pravděpodobnost chybného odmítnutí autorizované osoby.
- FTE Failure to Enroll – pravděpodobnost neúspěšného sejmutí biometrického vzorku.
- FTA Failure to Acquire – koeficient selhání přístupu.
- ERR Equal Error Rate – ideální rozložení pravděpodobnosti chyb FAR a FRR.
- ROC Receiver Operating Characteristics – vzájemný vztah mezi FAR a FRR.
- FMR False Match Rate – pravděpodobnost, že určitý biometrický vzorek bude chybně systémem vyhodnocen.
- FNMR False Non-Match Rate – pravděpodobnost vzniku situace, při níž bude vzorek autorizované osoby chybně vyhodnocený jako nesprávný.
- TEA Turnstile Enrollment Application

SEZNAM OBRÁZKŮ

Obrázek 1: Scóre porovnání [1].....	13
Obrázek 2: Závislost FAR a FRR [1]	18
Obrázek 3: Receiver operating characteristics [1]	19
Obrázek 4: Segmentace [4].....	24
Obrázek 5: Ukázka vyhlazení obrazu [4].....	25
Obrázek 6: Lokální prahování [4].....	25
Obrázek 7: Postprocessing [4]	26
Obrázek 8: Schéma lidského oka [1]	27
Obrázek 9: Snímání sítnice [1]	29
Obrázek 10: Vertikální zorné pole [9]	41
Obrázek 11: Horizontální zorné pole [9]	42
Obrázek 12: Popis připojení kabeláže [9].....	42
Obrázek 13: Schéma zapojení [9].....	43
Obrázek 14: Nastavení TCP/IPv4.....	44
Obrázek 15: Person View	45
Obrázek 16: Obecná konfigurace zařízení Broadway.....	46
Obrázek 17: Konfigurace síťového připojení	46
Obrázek 18: Konfigurace kamery biometrického zařízení	47
Obrázek 19: Schéma zapojení s využitím aplikace TEA [9]	48
Obrázek 20: Nastavení připojení	49
Obrázek 21: Hlavní okno Artec Camera Manager.....	50
Obrázek 22: Hlavní menu aplikace TEA	51
Obrázek 23: Záložka General	52
Obrázek 24: Nastavení kamery	53
Obrázek 25: Proces identifikace	55
Obrázek 26: Proces verifikace	56
Obrázek 27: Turnstile mode	57
Obrázek 28: Schéma pro výpočet úhlů α a β	59
Obrázek 29: Schéma pro výpočet úhlu δ a ϵ	60
Obrázek 30: Ukázka 3D modelu a předlohy.....	62
Obrázek 31: Informace o uživateli.....	62

SEZNAM TABULEK

Tabulka 1: Rozsah hodnot kvality registrace	54
Tabulka 2: Závislost identifikace na vzdálenosti	64
Tabulka 3: Identifikace - pánové	64
Tabulka 4: FRR - identifikace - pánové	64
Tabulka 5: Identifikace - dámy	65
Tabulka 6: FRR - identifikace - dámy	65
Tabulka 7: Verifikace - dámy	67
Tabulka 8: FRR - verifikace - dámy	67
Tabulka 9: Verifikace - pánové	67
Tabulka 10: FRR - verifikace - pánové	68
Tabulka 11: Verifikace při zakrytí obličeje - dámy	68
Tabulka 12: FRR - verifikace při zakrytí obličeje - dámy	69
Tabulka 13: Verifikace při zakrytí obličeje - pánové	69
Tabulka 14: FRR - verifikace při zakrytí obličeje - pánové	70
Tabulka 15: Výsledky identifikace	72

SEZNAM PŘÍLOH

Příloha P I: Ukázky modelů a jejich předloh

PŘÍLOHA P I: UKÁZKY MODELŮ A JEJICH PŘEDLOH

