VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

BIOMETRICKÁ BRÁNA VYUŽÍVAJÍCÍ KAMER PRO IDENTIFIKACI OSOB

BIOMETRIC GATEWAY USING CAMERA TO IDENTIFY PEOPLE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. VILÉM JELEN**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. TOMÁŠ GOLDMANN**
SUPERVISOR

BRNO 2019

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav inteligentních systémů (UITS) Akademický rok 2018/2019

Zadání diplomové práce

Student: **Jelen Vilém, Bc.**
Program: Informační technologie Obor: Počítačová grafika a multimédia
Název: **Biometrická brána využívající kamer pro identifikaci osob**
Biometric Gateway Using Camera to Identify People
Kategorie: Bezpečnost

Zadání:

1. Nastudujte základní informace o biometrických systémech. Prostudujte současnou nabídku biometrických bran, analyzujte jejich vlastnosti a vyberte 2-3 relevantní pro tuto práci.
2. Seznamte se s biometrickými systémy využívající kamery pro identifikaci osob. Sumarizujte informace o duhovce z pohledu biometrie. Dále pak popište Daugmanův algoritmus, který se používá pro převod snímku duhovky na binární kód.
3. Navrhněte biometrickou bránu, která se bude skládat ze 3 kamer pro snímání obličeje a duhovky lidského oka. Pro snímání duhovky předpokládejte využití vysokorychlostní kamery. Návrh rozmístění kamer proveď na základě experimentů.
4. Zkonstruujte zařízení a implementujte řídící software. Software implementujte pro MS Windows. Předpokládejte, že se data budou získávat současně ze všech kamer ve stejný okamžik. Aplikace při výskytu hlavy v požadované oblasti bude provádět snímání a identifikaci. Pro realizaci identifikačního algoritmu použijte běžně dostupné klasifikační algoritmy.
5. Proveďte experimenty zaměřené na úspěšnost identifikace osob s využitím biometrické brány.

Literatura:

- DAVIES, E. R. Computer vision: theory, algorithms, practicalities. 5th edition. Cambridge, CA: Elsevier, 2017. ISBN 978-0-12-809284-2.
- WAYMAN, James. Biometric systems: technology, design, and performance evaluation. London: Springer, 2005. ISBN 978-1852335960.

Při obhajobě semestrální části projektu je požadováno:

- Body č. 1 a 2

Podrobné závazné pokyny pro vypracování práce viz http://www.fit.vutbr.cz/info/szz/

Vedoucí práce: **Goldmann Tomáš, Ing.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1. listopadu 2018
Datum odevzdání: 22. května 2019
Datum schválení: 1. listopadu 2018

Abstrakt

Biometrické brány se používají pro rychlou a přesnou identifikaci osob. Z biometrických charakteristik jsou běžně používány duhovka, obličej a otisky prstů. Jejich kombinací lze dosáhnout lepších výsledků identifikace. Cílem této práce je vytvoření takové biometrické brány společně s řídící aplikací. Využita je kombinace duhovky obou očí a obličeje, který je snímán kamerami ze tří úhlů pro zvýšení přesnosti. K detekci a extrakci příznaků obličeje jsou použity neuronové sítě. Rozpoznání duhovky je realizováno pomocí Daugmanova algoritmu.

Abstract

Biometric gateways are used to quickly and accurately identify people. Of the biometric characteristics, iris, face and fingerprints are commonly used. By combining them, better identification results can be achieved. The aim of this thesis is to create such a biometric gateway together with the control application. A combination of iris of both eyes and face is used, which is captured by cameras from three angles to increase accuracy. Neural networks are used to detect and extract face features. Iris recognition is realized using Daugman's algorithm.

Klíčová slova

Rozpoznávání duhovky, rozpoznávání obličeje, identifikace osoby, identifikace, biometrická brána, biometrie, duhovka, obličej, rozpoznávání, Daugmanův algoritmus, OpenCV, Dlib

Keywords

iris recognition, face recognition, person identification, identification, biometric gateway, biometrics, iris, face, recognition, Daugman's algorithm, OpenCV, Dlib

Citace

JELEN, Vilém. *Biometrická brána využívající kamer pro identifikaci osob*. Brno, 2019. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Tomáš Goldmann

Biometrická brána využívající kamer pro identifikaci osob

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Goldmanna. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Vilém Jelen
29. května 2019

Poděkování

Děkuji vedoucímu práce za jeho odbornou pomoc, rodině a přátelům za zázemí a podporu při studiu. Děkuji také všem, kteří mi pomohli během tvorby této práce.

Obsah

Kapitola 1

Úvod

V současnosti stále stoupá potřeba pro rychlou, bezpečnou a pohodlnou identifikaci a verifikaci osob. Důvodů je mnoho, například v oblasti letecké dopravy je tato potřeba evidentní. Cestující nechtějí čekat dlouho ve frontách a obecně se raději vyhnou komplikacím a nepohodlí. Pro hraniční kontrolu naopak stoupá potřeba pro systémy kontroly, které jsou bezpečnější a odolnější proti podvrhům. Důvodem je zde riziko terorismu a čím dál kvalitnější techniky podvodů. Řešením těchto potřeb jsou biometrické systémy. Uživatelé mohou od nich očekávat rychlejší a pohodlnější kontroly. Personál zajišťující bezpečnost využije jejich větší odolnost vůči podvrhům a u nejnovějších generací biometrických bran mnohem kvalitnější ohodnocení rizika, které kontrolovaná osoba představuje. Z těchto důvodů se stále více států a organizací snaží modernizovat, vyvíjet a nasazovat biometrické systémy. Zejména v podobě biometrických bran, které jsou například na letišti Václava Havla v Praze od roku 2011.

Z biometrických charakteristik jsou pro účely biometrických bran nejpoužívanější tři a to rozpoznávání podle obličeje, duhovky a otisků prstů. Tato práce se zaměřuje na použití kombinace charakteristik obličeje a duhovky. Vyhnutí se použití otisků prstů je výhodné pro pohodlnost a v některých případech i rychlost identifikace, také není třeba řešit případné poškození prstů nebo přítomnost různých kožních onemocnění. Výhodou použití duhovky je také její větší unikátnost a odolnost proti podvrhu oproti otiskům prstů. Nevýhodou je ztížení nebo zamezení identifikace v případě nekooperujícího uživatele.

Cílem je biometrická brána identifikující osoby pomocí tří kamer ze tří různých úhlů a snímače duhovky obou očí. Umístění kamer je vhodně navrhnuto na základě experimentů. Identifikace probíhá na základě kombinované charakteristiky osoby odvozené z nasnímaného obrazu obličeje a duhovky. Využití tohoto systému je zejména jako bezpečnostní brány pro umožnění vstupu do hlídané oblasti nebo jako součást odbavovacího procesu například na letišti.

Pro vytvoření biometrické brány je nutné se nejprve seznámit s biometrií, o té pojednává kapitola 2, v první části jsou popsány základní biometrické vlastnosti a charakteristiky. V druhé je detailněji popsáno rozpoznávání podle duhovky, anatomie lidského oka a Daugmanův algoritmus, který slouží k převodu snímku duhovky do binárního kódu. Kapitola pokračuje popisem rozpoznávání podle obličeje. Závěrem kapitoly je popsáno vyhodnocování biometrických vlastností, kde je vysvětlen rozdíl mezi verifikací a identifikací. A jsou popsány chyby, které vznikají při porovnávání biometrických dat.

Další kapitola je zaměřena na lepší pochopení biometrických bran. Na její úvod jsou popsány okolnosti, které motivují jejich další rozvoj. V další části je uveden průběh vývoje biometrických bran. Následující sekce popisuje jejich architekturu. Dále je vysvětleno

hodnocení výkonu bran, používané metriky a důležité vlastnosti bran. Pokračuje popisem problémů existujících systémů. Závěrem jsou uvedeny biometrické brány používané v současnosti.

V pořadí čtvrtá kapitola se zabývá návrhem biometrické brány, její konstrukcí, rozmístěním kamer a návrhem algoritmů identifikace tváře a duhovky. Následuje kapitola popisující detaily implementace aplikace, která řídí sestavenou biometrickou bránu. Nejprve jsou zmíněny použité nástroje, dále použité funkce a metody pro algoritmus biometrické brány. V další části jsou popsány algoritmy snímání osob, a to ve dvou různých režimech, při registraci nového uživatele a při identifikaci osoby. V posledních dvou částech kapitoly jsou blíže vysvětleny postupy identifikace obličeje a identifikace duhovky. Na tuto kapitolu navazuje další, která obsahuje popis provedených experimentů na dvaceti osobách ověřujících úspěšnost identifikace osob vytvořenou biometrickou bránou. Závěrem jsou zmíněny případná vylepšení a práce je vyhodnocena.

Kapitola 2

Biometrie

Biometrií je myšleno v biomedicínské oblasti měření nebo statistická analýza fyzických a povahových vlastností osob. V oboru informačních technologií se jedná o automatické rozpoznávání osob podle jejich charakteristických rysů. Základním předpokladem je, že každého člověka lze přesně rozeznat podle jeho vlastností, tedy na základě toho, kým je. Mezi používané fyzické vlastnosti patří například obličej, duhovka a otisk prstu. Povahovými vlastnostmi jsou například chůze nebo hlas. Používání biometrie v současnosti roste a je o něj stále větší zájem. Důvodů je více, podstatnými jsou lepší bezpečnost než jen s pomocí hesla a efektivnější ověření identity. Příkladem je rozsáhlé rozšíření senzorů otisku prstu na mobilních telefonech. Kromě tohoto použití je biometrie nasazena při zajištění bezpečnosti na hranicích v podobě biometrických bran, v bankovnictví, na letištích pro odbavení cestujících, využití bezpečnostními složkami a na dalších místech.

Tato kapitola slouží k seznámení se základními biometrickými vlastnostmi a charakteristikami. Zaměřena je zejména na rozpoznávání podle duhovky a obličeje, jelikož se jedná o biometrické charakteristiky využité v této práci pro identifikaci osob pomocí biometrické brány. Důvodem výběru je jejich snadné snímání a zároveň vyšší přesnost identifikace. V části popisující rozpoznávání duhovky je popsán Daugmanův algoritmus, který slouží k převodu snímku duhovky do binárního kódu. Zmíněny jsou i základní informace o anatomii lidského oka. V části zabývající se rozpoznáváním obličeje jsou popsány jeho vlastnosti a postup identifikace. Kapitolu uzavírá vyhodnocování biometrických vlastností, kde je vysvětlen rozdíl mezi verifikací a identifikací. A jsou popsány chyby vznikající při porovnání biometrických dat.

2.1 Biometrické vlastnosti a charakteristiky

V různých aplikacích jsou používány následující biometrické charakteristiky. Každá má své výhody a nevýhody, a proto výběr biometrické vlastnosti pro konkrétní účel závisí na několika faktorech, kromě úspěšnosti rozpoznávání. Jain a kolektiv [18] určili sedm faktorů, které rozhodují o užitečnosti fyzické nebo povahové vlastnosti pro biometrickou aplikaci:

1. **Univerzalita**: Každý uživatel aplikace by měl mít danou vlastnost.
2. **Unikátnost**: Daná vlastnost by měla být dostatečně rozdílná mezi jedinci v populaci.
3. **Trvalost**: Biometrická vlastnost jednotlivce by měla být dostatečně neměnná po určitou dobu s ohledem na použitý porovnávací algoritmus. Vlastnost, která se během času významně mění není užitečná.

4. **Měřitelnost**: Mělo by být možné získat a digitalizovat biometrickou vlastnost použitím vhodných nástrojů, které nezpůsobují zbytečné nepříjemnosti danému jednotlivci. Dále, ze získaných surových dat by mělo být možné extrahovat reprezentativní množinu vlastností.

5. **Výkon**: Přesnost rozpoznávání a zdroje potřebné k dosažení této přesnosti by měly splňovat omezení dané aplikace.

6. **Přijatelnost**: Jednotlivci kteří budou používat danou aplikaci by měli být ochotní darovat jejich biometrická data danému systému.

7. **Jednoduchost podvodu**: Jak náročné je obcházení daného systému pomocí imitace biometrické vlastnosti (např. falešné prsty nebo napodobování chování).

Nelze očekávat, že biometrická vlastnost bude efektivně splňovat všechny požadavky ve všech aplikacích, jinými slovy neexistuje ideální biometrická vlastnost, ale několik jich je použitelných. Relevance dané vlastnosti závisí na povaze a požadavcích aplikace a vlastnostech dané biometrické charakteristiky. Níže jsou uvedeny běžně používané biometrické charakteristiky podle [19]:

1. **Obličej** - Rozpoznání obličeje je bezdotyková metoda, přičemž rysy obličeje jsou pravděpodobně lidmi nejčastěji používanou vlastností osoby pro vzájemné rozpoznání. Aplikace rozpoznávání obličeje mohou být statické nebo dynamické s rušným okolím. Populární přístupy k identifikaci obličeje jsou založené na rozmístění a tvaru rysů obličeje (např. očí, obočí, nosu, rtů nebo brady) a jejich vzájemném vztahu nebo může být založeno na globální analýze snímku obličeje, který jej reprezentuje jako váženou kombinaci počtu kanonických obličejů. Mezi problémy současných řešení identifikace podle obličeje patří nepřesnost porovnávání snímků pořízených pod jiným úhlem, za jiných světelných podmínek nebo v jinou dobu. Kvůli tomu je otázkou, zda pro velmi přesné rozpoznání osoby bez dalších informací stačí pouze obličej. Dobře fungující systém rozpoznávání obličeje by měl být schopný automaticky detekovat, zda je na pořízeném snímku obličej, přesně určit pozici obličeje na snímku a obecně rozpoznat daný obličej (v různých pózách a za rozdílných podmínek okolí).

2. **Otisk prstu** - Otisky jsou využívány k identifikaci osob po mnoho desetiletí. Přesnost identifikace pomocí otisků je velmi vysoká [36]. Otisk je vzor vyvýšenin a prohlubní na povrchu prstu, jeho tvorba probíhá během prvních sedmi měsíců vývoje plodu. Empiricky bylo dokázáno, že otisky identických dvojčat jsou rozdílné a také že každý prst člověka má jiný otisk [24]. Dnes je cena skenerů otisků nízká, a i proto jsou tyto snímače často používané například v mobilních telefonech. Více otisků jednoho člověka umožňují identifikaci ve velkém měřítku, zahrnující miliony identit. Jedním problémem takové identifikace na základě otisků je jejich obrovská výpočetní náročnost, zejména při použití režimu identifikace. Nevýhodou otisků je jejich možná nepoužitelnost v automatické identifikaci pro malou část populace, důvodem mohou být genetické faktory, stárnutí, vliv prostředí nebo zaměstnání (např. manuálně pracující lidé mohou mít na prstech množství říznutí a oděrek).

3. **Geometrie ruky** - Systémy rozpoznávající podle geometrie ruky používají několika měření lidské ruky, včetně jejího tvaru, velikosti dlaně, délky a šířky prstů [18]. Tato technika je velmi jednoduchá, relativně snadno použitelná a levná. Faktory prostředí

jako například suché ovzduší nebo ojedinělé anomálie jako suchá kůže nezatěžují negativně přesnost identifikace pomocí geometrie ruky. Nevýhodou je nízká rozdílnost geometrie ruky mezi jedinci populace, proto tato metrika není použitelná pro rozpoznání jedince ve velké populaci. Dalším problémem mohou být změny geometrie v průběhu dětství. V některých případech mohou šperky (např. prsteny) nebo omezení v obratnosti (např. artritida) ztížit snímání správných informací o geometrii ruky. Systémy snímaní ruky jsou velké, a proto je nelze implementovat například v laptopech. Také jsou však dostupné autentifikační systémy využívající pouze měření několika prstů namísto celé ruky. Tyto zařízení jsou menší než ty měřící celou ruku, ale stále jsou větší než například senzor snímání otisků prstů.

4. **Otisk dlaně** - Povrch lidské dlaně se skládá z podobných vyvýšenin a prohlubní jako povrch prstů. Protože je povrch dlaně větší než povrch prstu, lze jako důsledek očekávat větší rozlišitelnost otisků dlaně než otisků prstů [40]. Kvůli potřebě sejmutí větší plochy jsou skenery otisků dlaně větší a dražší než skenery otisků prstů. Lidské dlaně navíc také mají další rozlišitelné prvky, jako hlavní linie a rýhy, které lze sejmout i pomocí levnějšího skeneru s nižším rozlišením. Při použití skeneru s vyšším rozlišením lze kombinovat všechny vlastnosti ruky jako například geometrie, tvar rýh, hlavní linie a vrásky do velmi přesného biometrického systému.

5. **Duhovka** - Kruhovitá část oka ohraničená zornicí a bělmem (*sclera*) je nazývána duhovkou. Textura duhovky je vytvářena během vývoje plodu a stabilizuje se během prvních dvou let života. Avšak samotná pigmentace pokračuje ve změnách déle. Komplexní textura duhovky nese velmi rozdílnou informaci pro každou osobu a je tak užitečná při rozpoznávání [6]. U aktuálně používaných systémů rozpoznávání podle duhovky je přesnost a rychlost slibná a umožňuje tak použití těchto systémů ve velké škále (na velké části populace). Každá duhovka je jiná, a to platí i pro duhovky identických dvojčat. Dokonce lze detekovat kontaktní čočky s falešnou duhovkou (více v [5]). Rozšiřování a smršťování zornice oka lze také použít pro měření živosti. Přestože počáteční rozpoznávací systémy podle duhovky vyžadovaly značnou účast uživatele a byly drahé, jsou novější systémy více uživatelsky přívětivé a cenově efektivnější [27]. Rozpoznávání duhovky má velmi nízkou FAR (*False Accept Rate*, viz. sekce 2.4.2) při porovnání s dalšími biometrickými vlastnostmi, ale FRR (*False Reject Rate*, viz. sekce 2.4.2) těchto systémů bývá spíše vyšší [15].

6. **Stisk klávesy** - Existuje hypotéza, že každá člověk píše vlastním charakteristickým způsobem na klávesnici. Od této biometrické charakteristiky nelze očekávat unikátnost mezi jednotlivci, ale může poskytnout dostatečně odlišnou informaci, která připouští verifikaci identity [26]. Dynamika stisku klávesy je biometrická vlastnost závislá na povaze, lze očekávat větší rozdíly ve stylu psaní osoby kvůli emočním změnám, pozici uživatele vzhledem ke klávesnici, typu použité klávesnice apod. Stisky kláves mohou být sledovány nenápadně během toho, jak uživatel zadává své údaje. Tato charakteristika umožňuje průběžnou verifikaci identity jedince během jeho sezení v systému, potom co se přihlásí pomocí silnější charakteristiky jako je otisk prstu nebo duhovka.

7. **Podpis** - Způsob jakým se člověk podepisuje je znám jako charakteristika daného jedince. Přestože k podpisu je třeba kontaktu s psacím nástrojem a úsilí od uživatele, jsou podpisy používány ve státních, právních a komerčních transakcích k ověření

identity. Podpis je biometrická charakteristika závislá na chování jedince, proto se s časem mění a je ovlivněn fyzickým a psychickým stavem podepisující osoby. U některých osob se jejich podpis značně mění, dokonce po sobě jdoucí podpisy mohou být značně rozdílné. Hlavní nevýhodou podpisu je schopnost profesionálních padělatelů oklamat systém ověřování podpisů.

8. **Hlas** - Hlas je kombinací fyzické a povahové biometrické charakteristiky. Fyzické vlastnosti hlasu jsou závislé na tvaru a velikosti hlasivek, úst, nosních dutin, rtů a dalších, které se účastní syntézy zvuku. Tyto fyzické charakteristiky lidské řeči jsou u jedince neměnné, ale povahový nebo psychický aspekt řeči se mění s časem, důvodem je například věk, zdravotní stav (např. chřipka), emocionální stav a další. Hlas také není příliš rozlišitelný a nemusí být vhodný pro identifikaci ve velkém měřítku. Systém rozpoznání hlasu závislý na textu je založený na projevu předem určené fráze. Naopak systém textově nezávislý dokáže rozpoznat mluvčího nezávisle na tom co říká. Textově nezávislý systém má komplikovanější návrh, ale je odolnější proti podvodům. Nevýhodou rozpoznávání hlasu je citlivost na velké množství okolností například na šum v pozadí. Rozpoznávání mluvčího je vhodné použít v aplikacích spojených s telefonováním, avšak kvůli přenosu je zde problém degradace zvukového signálu.

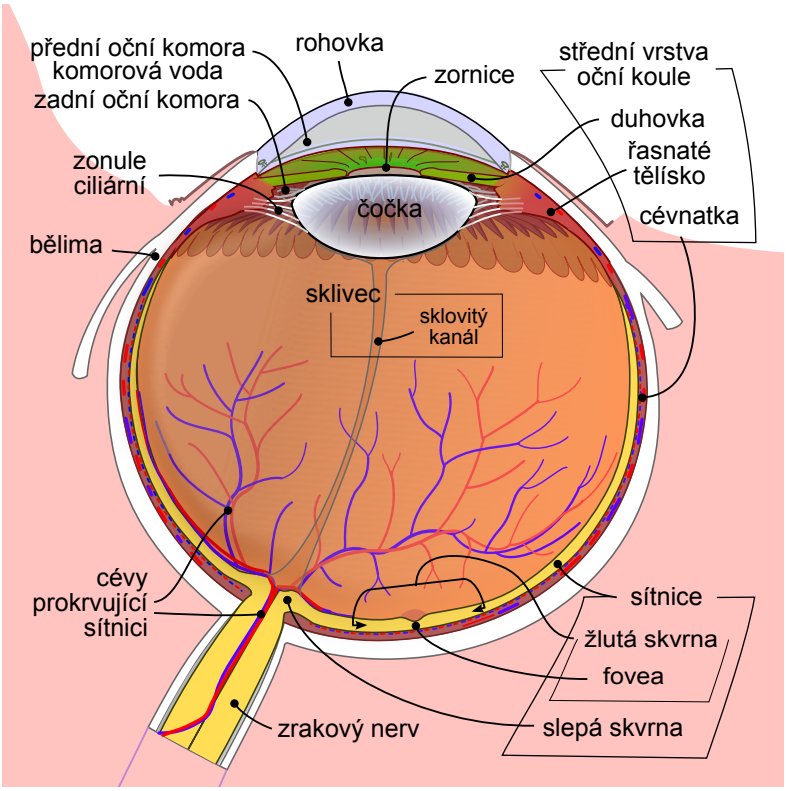
9. **Krok** - Krokem se myslí způsob chůze. Jedná se o jednu z mála biometrických vlastností, kterou lze použít pro rozpoznání osoby na dálku. Proto je tato vlastnost velmi vhodná v situacích se sledováním, kdy lze takto získat identitu osoby tajně. Většina algoritmů rozpoznávání kroku se snaží nejprve získat siluetu osoby, za účelem odvození prostorově-časových atributů pohybu dané osoby. Z tohoto důvodu je výběr dobrého modelu reprezentace lidského těla základem pro efektivní funkci systému rozpoznávání kroku. Užitečnou vlastností systémů rozpoznání kroku je možnost sledování pohybu jedince po delší dobu. Na druhou stranu je krok jedince ovlivněn několika faktory, mezi které patří výběr obuvi, povahou oděvu, případným postižením nebo zraněním nohou a dalšími.

2.2 Rozpoznávání podle duhovky

V této části je detailněji popsána duhovka a rozpoznávání podle duhovky, ke kterému je mimo jiné používán Daugmanův algoritmus. Výhodou duhovky je její složitost, proto je vhodnou biometrickou charakteristikou použitelnou na velkou skupinu uživatelů. Její nevýhodou je možná obava uživatelů z poranění oka a také náročnější získání snímků duhovky v případě nespolupracujícího uživatele.

2.2.1 Anatomie lidského oka

Díky unikátnosti lidského oka jej lze použít jako biometrickou charakteristiku. Kromě duhovky je biometricky užitečnou částí oka i sítnice, ležící uvnitř oka, tudíž ji nelze pozorovat pouze pohledem. Průmyslová řešení rozpoznávání podle sítnice oka jsou dosud velmi omezená a v současnosti je proto vhodnější se při konstrukci biometrické brány zaměřit na duhovku. Vzorkování duhovky je unikátní dokonce i u jednovaječných dvojčat. Avšak barva a struktura duhovky jsou geneticky závislé.



Obrázek 2.1: Anatomie lidského oka. Převzato z [35].

Na obrázku 2.1 je diagram anatomie oka, které se mimo jiné skládá z následujících částí (podle [8][35]):

- **Rohovka** je průhledná vazivová tkáň, která je umístěna v přední části oka. Společně s čočkou umožňuje lom světla do oka. Je více vyklenuta než bělima, odchylka od tohoto zakřivení způsobuje *astigmatismus*.
- **Přední oční komora** obsahuje komorovou vodu, která je stále obnovována.
- **Duhovka** je kruhovitě uspořádaná svalovina, která rozšiřuje nebo stahuje zornici. Její barva je určena množstvím a hloubkou uložení pigmentových buněk, například modré oči jich mají nejméně. Pigmentová vrstva slouží jako clona, tedy omezuje průchod světla.
- **Zornice** je otvor uprostřed duhovky, skrze ni dopadá světlo dovnitř oka.
- **Čočka** má schopnost se vyklenout a tím zaostřit pomocí změny indexu lomu, čočka je zavěšena na řasnatém tělísku. Jedná se o průhlednou dvojvypuklou spojku.
- **Bělima** je tuhá a bílá blána, která pokrývá 4/5 oční bulvy, v přední části přechází v rohovku.
- **Sklivec** je průhledná rosolovitá hmota, vyplňuje vnitřek oka. Udržuje stálý tvar oka.
- **Sítnice** zachycuje obraz který se na ní zobrazuje pomocí buněk citlivých na světlo. Jsou na ní umístěné nervové a smyslové buňky. Tyčinky jsou světločivé buňky, rozlišují

pouze odstíny šedi, poskytují menší zrakovou ostrost, ale jsou citlivější na světlo a umožňují tak vidění za šera. Čípky jsou světločivé buňky umožňující barevné vidění. Místo s největší ostrostí je nazýváno žlutá skvrna, je zde nejvyšší hustota čípků.

- **Zrakový nerv** ústí skrze slepou skvrnu na sítnici do centrálního nervového systému.

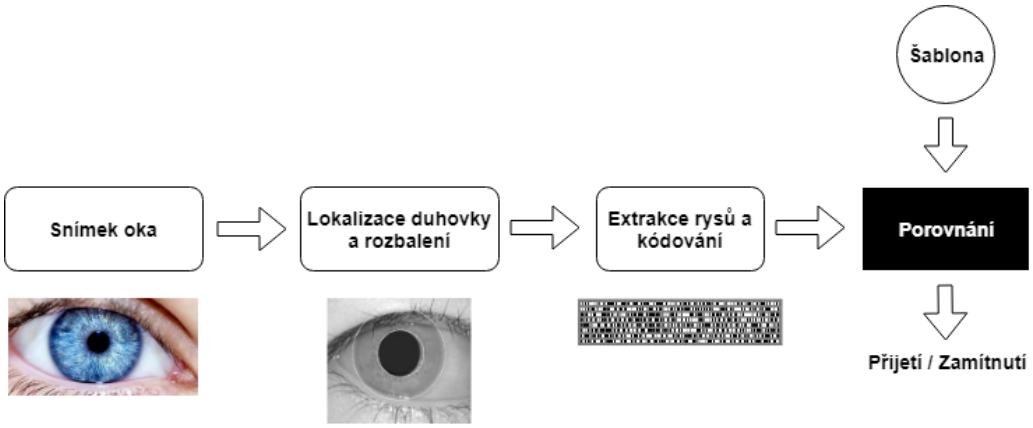
Struktura duhovky je poměrně složitá. U duhovky bylo popsáno přibližně 250 rysů, které obsahuje, podstatné pro identifikaci jsou následující tři [8]. Radiální rýhy – jemné paprskovité vroubky, tažené od čočky k límečku, který se nachází přibližně v polovině prstence duhovky. Krypty – jsou to nejtenčí místa duhovky, nacházejí se její přední části a utvářejí její typickou kresbu. Pigmentové skvrny – povrchové shluky pigmentu.

Pro snímání duhovky je vhodné použití infračerveného (IR) světla. Důvodem je větší absorpce viditelného světla melaninem, který je obsažen v pigmentu duhovky. IR je také příjemnější pro uživatele, protože neoslňuje. Rozpoznávání duhovky lze v základu provádět čtyřmi algoritmy [8]:

- Daugmanův algoritmus (nebo též Gaborova demodulace) - všechny vzory na duhovce jsou jednotlivě demodulovány, tím je získána fázová informace k extrakci rysů [6].
- *Wavelet features* (Vlnkové rysy) - extrahování rysů do vektoru pomocí vlnkové transformace [23].
- Analýza nezávislých komponent - koeficienty nezávislých komponent slouží jako vektor rysů. [38]
- Variace lokálních klíčů - podstatné informace jsou reprezentovány sadou intenzit signálů, vlnkovou transformací jsou extrahovány rysy.

2.2.2 Daugmanův algoritmus

Algoritmus začíná lokalizací duhovky na snímku. Ten musí být kvalitní, aby bylo možné duhovku namapovat do fázových diagramů, nesoucích informace o pozici, orientaci a počtu identifikačních rysů. Po extrakci rysů se provádí porovnání se vzory v databázi. Postup Daugmanova algoritmu je na obrázku 2.2.



Obrázek 2.2: Postup identifikace Daugmanovým algoritmem.

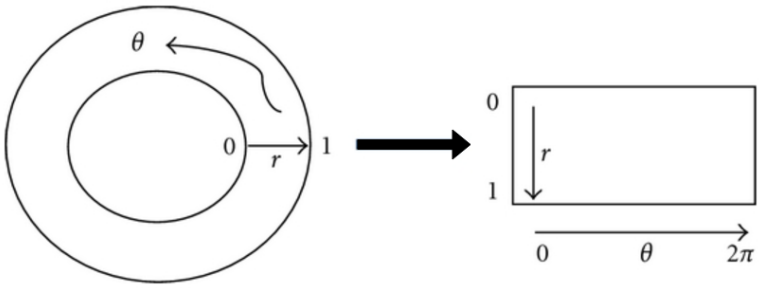
Lokalizace duhovky probíhá podle následujícího operátoru [8]:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \tag{2.1}$$

kde $G_\sigma(r)$ je Gaussova funkce vyhlazení podle σ, $I(x,y)$ je vstupní snímek, ve kterém operátor hledá maximum v rozostřené parciální derivaci obrazu podle poloměru r a středových souřadnic (x_0, y_0). Jedná se tedy o kruhový detektor, který vrací maximum v případě, že kandidátská kružnice sdílí poloměr a střed zornice.

V dalším kroku se obdobným způsobem lokalizuje horní a dolní víčko oka. V operátoru hledání duhovky se vymění detekce kontury z kruhové na obloukovou a parametry se upraví tak, aby odpovídaly hranicím víčka.

Dále jsou podle Daugmanova modelu hrubého zarovnání mapovány všechny body duhovky do polárních souřadnic (r, θ), kde $r \in < 0, 1 >$ a $\theta \in < 0, 2n >$. Reprezentace pomocí těchto souřadnic je neměnná vůči velikosti a translaci, tím je dosaženo kompenzace dilatace zornice a odstranění inkonzistencí v její velikosti [8]. Rotační nekonzistence je řešena ve fázi porovnávání dvou šablon duhovky, pomocí posunu ve směru θ. Mapování do polárních souřadnic je znázorněno na obrázku 2.3.



Obrázek 2.3: Mapování do souřadného systému v Daugmanově algoritmu. V případě, že střed duhovky a zornice je stejný. Upraveno z [8].

Pokračuje se kódováním duhovky v polárním souřadném systému pomocí Gaborova filtrování, které je definováno [8]:

$$G(r,\theta) = e^{j\omega(\theta-\theta_0)} e^{-\frac{(r-r_0)^2}{\alpha^2}} e^{-\frac{j(\theta-\theta_0)^2}{\beta^2}} \tag{2.2}$$

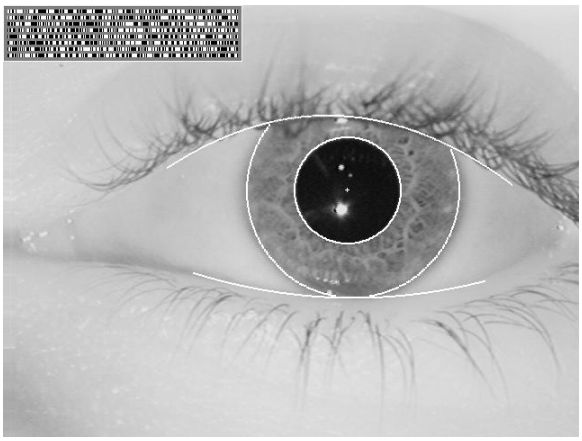
kde (r, θ) je pozice v obrazu, (α, β) je efektivní výška a délka, ω je frekvence filtru. Demodulace a fázová kvantizace je počítána následovně [8]:

$$g_{\{Re,Im\}} = \operatorname{sgn}_{\{Re,Im\}} \iint_{\rho\phi} I(\rho,\phi) e^{j\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{j(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi \tag{2.3}$$

kde $g_{\{Re,Im\}}$ je bit v komplexní rovině, který má hodnotu reálné a imaginární části 1 nebo 0, podle znaménka (sgn) integrálu. $I(\rho, \phi)$ je hrubý obrázek duhovky v polárních souřadnicích, α, β jsou parametry velikosti vlnky, ω je frekvence vlnky a (r_0, θ_0) reprezentují polární souřadnice jednotlivých částí duhovky, pro které je počítáno $g_{\{Re,Im\}}$.

Celkem se kód duhovky skládá z 2048 bitů (tedy 256 bytů). Vstupní obrázek má rozlišení 64×256 bytů, kód duhovky 8×32 bytů a Gaborův filtr 64×256 bytů. Na obrázku 2.4 je

ukázka kódu duhovky, která byla nasnímána monochromaticky přibližně ze vzdálenosti 35 cm [6].



Obrázek 2.4: Příklad kódu duhovky. Bílé linie zvýrazňují výsledky lokalizace duhovky, zornice a víček. Vlevo nahoře je výsledek demodulace. Převzato z [6].

Porovnání dvou kódů duhovky se provádí výpočtem Hammingovy vzdálenosti. Ta je mezi kódy A a B definována:

$$HD = \frac{1}{N} \sum_{j=1}^{N} A_j \otimes B_j \tag{2.4}$$

kde N je počet bitů kódu duhovky a $\otimes$ je operátor XOR. Pro dva vzorky stejné duhovky je jejich Hammingova vzdálenost rovna nebo blízká nule. Pro eliminaci vlivu rotace jsou vždy jednomu ze vzorů bity posunuty doleva nebo doprava a je vypočtena Hammingova vzdálenost, jako výsledek porovnání je pak brána nejnižší nalezená Hammingova vzdálenost [8][6].

2.2.3 Extrakce příznaků vlnkovou transformací

Algoritmus publikován ve článku *Efficient Iris Recognition through Improvement of Feature Vector and Classifier* [23]. S cílem zvýšit efektivitu a přesnost algoritmu rozpoznávání duhovky pomocí využití vlkové transformace. Experimenty autorů ukázaly, že má podobnou přesnost jako Daugmanův algoritmus [23]. Předzpracování snímků je obdobné jako v Daugmanově algoritmu. Nejprve je nalezena duhovka, pak je snímek převeden do polárních souřadnic. Následuje již samotná extrakce rysů duhovky. K tomu je použita 2-D vlnková transformace. V posledním kroku probíhá identifikace nebo verifikace. Pro klasifikaci vektorů s rysy duhovky použili autoři metodu LVQ (*Learning Vector Quantization*) [23].

Jako bázovou funkci při extrakci rysů je použita Haarova vlnka. Na snímek duhovky o rozměrech 450×60 pixelů, který je výsledkem předzpracování je čtyřikrát aplikována vlnková transformace, výsledkem je několik obrázků s rozměry 28×3 pixelů. Vektor rysů je vytvořen kombinací 84 rysů a výsledný vektor má 87 dimenzí. Každá dimenze má desetinnou hodnotu od -1 do 1. Pro redukci velikosti a výpočetní náročnosti je každá hodnota přepočítána na binární, jednoduchou konverzí kladných hodnot na 1 a záporných na 0. Výsledná reprezentace snímku duhovky má tedy jen 87 bitů [23].

2.3 Rozpoznávání podle obličeje

Nejpoužívanější přirozený způsob identifikace, kterým intuitivně osoby rozpoznáváme. Přirozeně pro nás funguje s relativně vysokou spolehlivostí, ale vytvořit spolehlivý biometrický systém rozpoznávání obličeje není jednoduché. Jelikož obličej má velkou vnitro-třídní variabilitu (například při gestikulaci) a také vyšší mezitřídní variabilitu (například u dvojčat) [8]. K rozpoznávání tváře existují tři hlavní přístupy: z 2D snímku, z 3D snímku a z termosnímku. Pro kvalitnější a spolehlivější identifikaci je vhodné použít 3D obličeje, který navíc zvyšuje biometrickou entropii. Avšak nelze popřít výhody 2D obličeje, a to jeho snadná akvizice a ve většině případů menší náklady na identifikaci, jak cenové, tak výpočetní. Lidský obličej vyniká mezi používanými biometrickými vlastnostmi svou velkou vnitro-třídní variabilitou, která je způsobena zejména těmito vlivy [8]:

- **Variabilita osvětlení:** snímky obličeje se mění v závislosti na osvětlení scény. Vliv různého osvětlení lze minimalizovat využitím vhodných technik, příkladem je systém FaceNet (popsán v sekci 2.3.2).
- **Mimika:** tímto vlivem se může výsledný snímek tváře silně měnit. Nejvíce se mění oblasti kolem čela, obočí, očí a úst.
- **Vlasy a vousy:** vzhled obličeje může být ovlivněn účesem a nebo vousy.
- **Brýle a další doplňky:** další způsob jak změnit vzhled tváře je nošení brýlí a různých doplňků (například čepice nebo šátku).
- **Stárnutí:** vliv stárnutí není dosud příliš prozkoumán. Pokud biometrický systém pracuje s databází aktuálních snímků, lze jej zanedbat.

Ze tří hlavních metod je nejrozšířenější rozpoznávání tváře z 2D snímku, zejména proto, že lze tyto snímky snadno získat. Rozpoznání obličeje většinou probíhá v těchto čtyřech krocích [8]:

1. Detekce tváře na snímku.
2. Normalizace detekovaného obličeje (osvětlení, velikosti, pozice, ...).
3. Extrakce příznaků = transformace získaných dat do zvolené datové reprezentace tváře.
4. Porovnání extrahovaných příznaků s databází uložených šablon (příznaků tváří).

2.3.1 Detekce tváře

Lokalizace obličeje ve snímku. Detektor by měl být robustní a schopný tak rozpoznat obličeje za různého osvětlení, v různých pozicích, rozměrech, orientací, s různými výrazy. Obvykle se tento problém řeší dvěma způsoby [8]:

- **Využití expertních znalostí:** detektor využívá znalostí o charakteristikách typických pro lidský obličej (pozice a barva očí, pozice nosu a úst, barva kůže, ...).
- **Využití strojového učení:** detektor využívá algoritmů strojového učení, které jsou trénovány na databázích velkého množství snímků, které mají vyznačenou oblast obličeje. Používanými metodami jsou například neuronové sítě nebo kaskády klasifikátorů. Výstupem učení je model, který umí rozpoznat lidskou tvář.

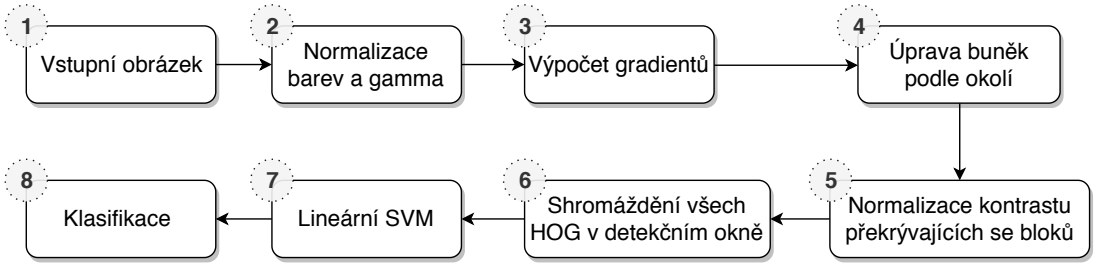
V současnosti jsou více využívány metody strojového učení, které bývají výpočetně náročnější, ale jsou schopny obličej lépe detekovat než metody využívající expertních znalostí. V některých případech může kombinace obou přístupů podávat lepší výsledky. Postup při detekci pomocí expertních znalostí je následující dle [8]:

1. Kompenzace osvětlení scény.
2. Detekce tónu kůže.
3. Detekce rysů obličeje (oči, ústa a nos).
4. Výpočet hranic obličeje.

Detekce na základě strojového učení probíhá odlišně. Důležitou částí je klasifikační algoritmus, který dokáže označit část obrázku za obličej.

Histogramy orientovaných gradientů

Detektor původně navržený k detekci lidské siluety, publikován v roce 2005 [4]. Jádrem algoritmu je využití tzv. histogramů orientovaných gradientů (*Histograms of Oriented Gradients*), dále jen HOG. Tento přístup k detekci se dá aplikovat na různé objekty, a tedy i na lidský obličej. V této práci je HOG jednou ze dvou implementovaných možností detekce obličeje. Ke klasifikaci je v původním článku používán jednoduchý lineární SVM (*Support Vector Machine*). Základní myšlenkou algoritmu je možnost dobré charakterizace vzhledu a tvaru objektu podle lokálního rozmístění gradientů (směru změn intenzity) nebo směrů hran ve snímku [4]. Na obrázku 2.5 je schéma detekce objektu pomocí algoritmu HOG.



Obrázek 2.5: Schéma detekce objektu pomocí algoritmu HOG.

Myšlenka je uvedena v praxi rozdělením obrázku na menší části (buňky). Pro všechny pixely v buňce je vypočítán 1-D histogram směrů gradientů nebo natočení hran. Reprezentace objektu je potom tvořena kombinací těchto histogramů. Nejdříve jsou vypočítány středové gradienty bez vyhlazování ($\sigma = 0$), které jsou orientované horizontálně nebo vertikálně. Na základě experimentů provedených autory [4] jsou pro jejich výpočet nejvhodnější následující 1-D masky ve směrech x a y [4]:

$$D_x = \begin{bmatrix} -1 & 0 & 1 \end{bmatrix} \qquad D_y = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} \tag{2.5}$$

V dalším kroku je vypočítána orientace gradientu (vektoru) se složkami g_x a g_y, které jsou získány aplikací masky D na snímek I [7]:

$$\theta = \arctan(\frac{g_y}{g_x}), \quad g_x = ID_x, \quad g_y = ID_y \tag{2.6}$$

Velikost gradientu je pak [7]:

$$g = \sqrt{g_x^2 + g_y^2} \tag{2.7}$$

Použití větší masky nebo vyhlazování (např. $\sigma = 2$) výrazně snižuje rychlost algoritmu. Při použití barevného vstupu jsou vypočítány gradienty pro jednotlivé barvy (definované barevným prostorem RGB nebo LAB[1])) odděleně a nejvhodnější z nich je vybrán jako vektor gradientu daného pixelu. Pokud je vstupem obraz v odstínech šedi, pak experimenty s detekcí siluety osob ukázaly zhoršení výsledků o 1,5% při 10^{-4} FPPW (*False Positives Per Window*). Lepší detekce lze také dosáhnout při použití rozložení úhlů histogramů se znaménkem od od 0° do 180° (než při použití celého rozsahu od 0° do 360° bez znaménka) Při použití znaménka jej lze ignorovat, což vede ke zlepšení například u detekce osob.

Pro zvýšení odolnosti detektoru vůči různému osvětlení je užitečná normalizace kontrastu buněk. Normalizace probíhá na větších blocích, které vznikají spojením několika buněk. Pro HOG byly testovány tyto metody normalizace [4]:

$$\text{L2-norm:} \quad f = \frac{v}{\sqrt{\|v\|_2^2 + \epsilon^2}} \tag{2.8}$$

$$\text{L1-norm:} \quad f = \frac{v}{\|v\|_1 + \epsilon} \tag{2.9}$$

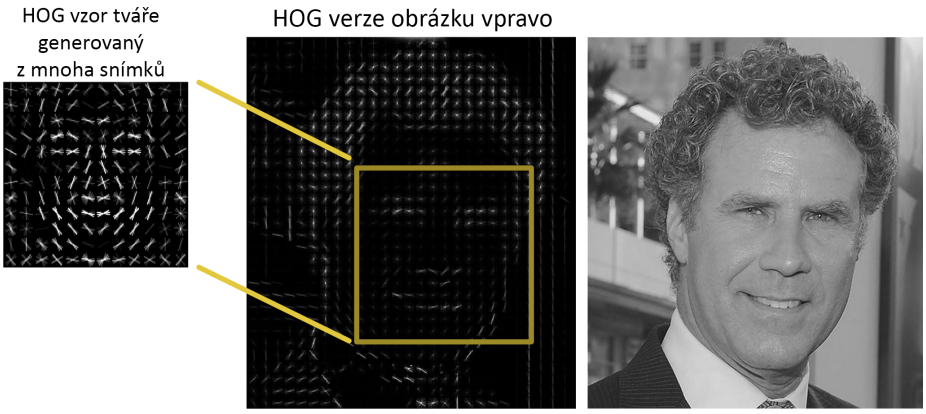
$$\text{L1-sqrt:} \quad f = \sqrt{\frac{v}{\|v\|_1 + \epsilon}} \tag{2.10}$$

kde v je vektor obsahující histogramy daného bloku, $||v||_k$ je jeho k-norm pro $k = 1, 2$ a ϵ je malá konstanta. Dále byla uvedena i čtvrtá metoda normalizace L2-hys, která spočívá v normalizaci pomocí L2-norm, oříznutí hodnot v na 0,2 a opakování normalizace. Dle zjištění autorů jsou L2-hys, L2-norm a L1-sqrt přibližně stejně výkonné, přičemž nejhorší výsledky podávala metoda L1-norm [4].

Vhodná velikost bloku při detekci osob je 3×3 buněk. Výkon detektoru a kvalitu normalizace lze zlepšit pomocí částečného překrývání bloků. Bloky jsou dvojího typu: R-HOG (kruhový) a C-HOG (čtvercový) [4]. Kruhové bloky se podobají přístupu popisu vlastností v SIFT (*Scale Invariant Feature Transform*). Vlastnosti detektoru lze měnit parametry jsou ς, η, β. Kde $\varsigma \times \varsigma$ je mřížka rozdělující obraz do buněk o velikosti $\eta \times \eta$ pixelů, které obsahují β směrů vektorů. Při detekci lidské siluety je nejúčinnější velikost bloků 3×3 buněk o velikosti 6×6pixelů [4].

V C-HOG bloku jsou buňky uspořádány dvěma způsoby. Uprostřed bloku je jedna buňka nebo je centrální buňka rozdělena podle úhlů krajních buněk. Oba typy bloků měly v experimentech podobný výkon, proto byly ve finální implementaci použity strukturálně jednodušší R-HOG bloky [4]. Při detekci metodou HOG je detekční okno postupně posunováno po obrazu a pro každou pozici jsou vypočítány buňky a bloky uvnitř a následně provedena klasifikace lineárním SVM. Na obrázku 2.6 je ukázka nalezení tváře ve snímku podle natrénovaného HOG vzoru tváře.

[1]Barva pixelu je definována světelností (L-*lightness*), osou A (od zelené k červené barvě) a osou B (od modré ke žluté barvě).



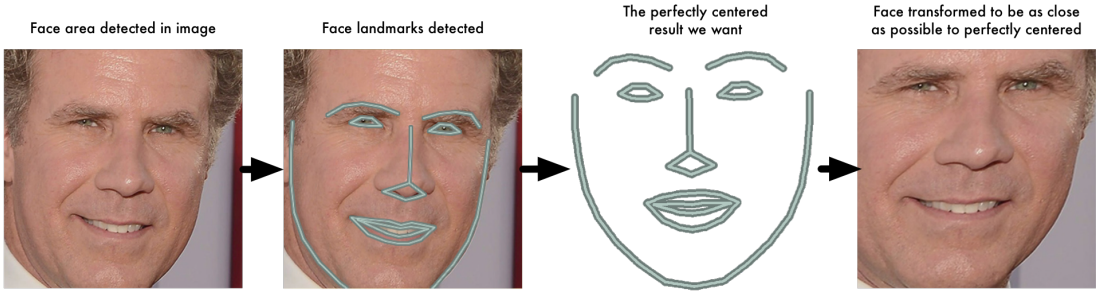
Obrázek 2.6: Příklad nalezení tváře pomocí HOG vzoru, vytvořeného z mnoha tváří. Upraveno z [11].

2.3.2 Extrakce příznaků tváře

Po detekování obličeje je vhodné před samotnou extrakcí příznaků provést normalizaci detekované tváře. Cílem je zvýšit přesnost porovnání získaných příznaků obličeje. Běžně jsou prováděny tyto druhy normalizace dle [8]:

- Extrakce obličeje z pozadí – pozadí kolem obličeje je nahrazeno černou barvou.
- Změna měřítka – všechny detekované tváře jsou upraveny na stejnou velikost.
- Zarovnání význačných bodů – jsou detekovány pozice očí, nosu, úst a obrázek je transformován podle požadavků algoritmu extrahujícího příznaky. Ukázka takové transformace je na obrázku 2.7. Zobrazený postup využívá algoritmu ze článku *One Millisecond Face Alignment with an Ensemble of Regression Trees* [20].
- Kompenzace jasu – obvykle je jas ve snímku převeden do plného jasového rozsahu.
- Další druhy normalizace – například lze minimalizovat vliv mimiky nebo vlasů a vousů.

Jako příklad extrakce příznaků tváře a její rozpoznávání následuje popis modelu FaceNet.



Obrázek 2.7: Ukázka úpravy natočení tváře ve snímku pomocí detekce významných bodů v obličeji. Převzato z [11].

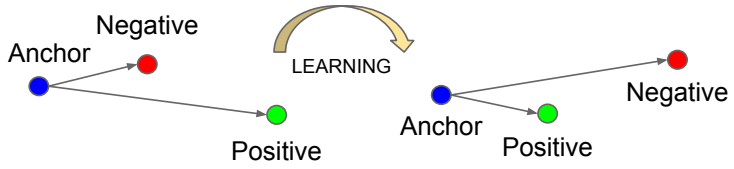
FaceNet: jednotný *embedding* pro rozpoznávání a shlukování

V roce 2015 tým ze společnosti Google uvedl nový způsob řešení rozpoznávání obličeje pod jménem FaceNet, který se přímo učí, jak mapovat snímek obličeje do kompaktního Euklidovského prostoru, v němž vzdálenosti přímo odpovídají podobnosti dvou obličejů [31]. Jakmile je takový prostor vytvořen, úkoly jako například rozpoznávání obličeje, verifikace a shlukování mohou být jednoduše implementovány běžnými technikami s FaceNet *embeddings* jako vektory příznaků (*feature vectors*). Tento systém má tři hlavní oblasti nasazení: verifikace tváře (je to stejná osoba), rozpoznání tváře (kdo je daná osoba) a shlukování (nalezení podobných osob mezi danými tvářemi).

Metoda autorů používá hlubokou konvoluční síť, trénovanou pro optimalizaci samotného *face embedding*, spíše než jako mezivrstvu, která často algoritmus zbytečně brzdí. Jak tomu bylo u předešlých přístupů používajících *deep learning*. Pro trénování jsou použity trojice zhruba zarovnaných tváří, které jsou generovány s použitím nového způsobu online dolování trojic. Hlavní výhodou FaceNet přístupu je daleko větší efektivita reprezentace tváře, s použitím pouze 128 bytů na obličej [31].

Na široce používané databázi *Labeled Faces in the Wild* (LFW) pro testování přesnosti rozpoznávání obličeje, dosahuje tento systém přesnosti 99,63 % [31]. Novinkou tohoto přístupu je také koncept harmonických *embeddings* a harmonického *triplet loss*, které popisují různé verze *face embeddings* (vytvořené různými sítěmi), které jsou kompatibilní mezi sebou a lze je tak přímo porovnat. Navržená síť je trénována tak, aby vzdálenosti L2 v daném *embedding* prostoru umocněné na druhou, přímo odpovídaly podobnosti obličejů: tváře stejné osoby mají malé vzdálenosti a rozlišitelné osoby mají velké vzdálenosti [31]. Jakmile je vytvořen takový *embedding*, potom již je řešení výše zmíněných problémů přímočaré. Verifikace obličeje je řešitelná nastavením vhodného prahu pro maximální vzdálenost mezi dvěma *face embeddings*. Rozpoznání obličeje se stane problémem k-NN klasifikace[2]. A shlukování lze dosáhnout použitím již dostupných technik, jako například algoritmu *k-means*.

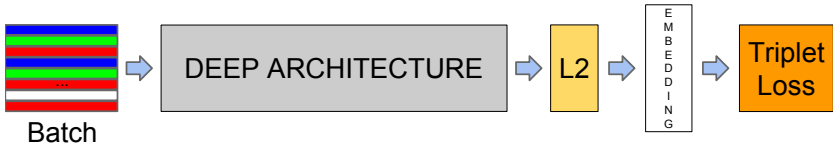
Na rozdíl od předešlých přístupů FaceNet přímo trénuje svůj výstup k tomu, aby jím byl kompaktní 128 dimenzionální *embedding*. Používá k tomu chybovou funkci (*loss function*) založenou na trojicích, které jsou složeny ze dvou obrázků stejné osoby a obrázku jiné osoby. Cílem chybové funkce je oddělit pozitivní pár od negativního snímku určitou vzdáleností. Obrázky jsou oříznuté oblasti snímku s tváří, bez 2D nebo 3D zarovnání do roviny, pouze je upravena jejich velikost a posun. Pro dosažení dobrých výsledků je klíčové vybrat správné trojice, autoři proto vyvinuli nový způsob jejich výběru, který je popsán níže. Na obrázku 2.8 je ukázána funkce *triplet loss*.



Obrázek 2.8: *Triplet loss* funkce minimalizuje vzdálenost mezi kotvou a pozitivem, přičemž obě mají stejnou identitu. A maximalizuje vzdálenost mezi kotvou a negativem, který má jinou identitu. Převzato z [31].

[2] Algoritmus *k-nearest neighbors* (k-nejbližších sousedů) slouží pro rozpoznávání vzorů.

Přístup FaceNet je metodou čistě založenou na datech, která se učí reprezentovat obličej přímo z pixelů tváře. Pro dosažení odpovídající invariance vzhledem k pozici, osvětlení a dalších podmínek, je využita velká databáze označených obličejů. Ve článku autoři zkoumají použitelnost dvou architektur hlubokých neuronových sítí, obě jsou konvolučními sítěmi. První architektura je postavena na modelu *Zeiler&Fergus*, který se skládá z několika prokládaných konvolučních vrstev, nelineárních aktivací, normalizací lokální odezvy a *max pooling* vrstev [39]. K této architektuře je navíc přidáno několik $1 \times 1 \times d$ konvolučních vrstev. Druhá architektura sítě FaceNet je založena na modelu *Inception* [33].



Obrázek 2.9: Architektura modelu FaceNet. Tato síť se skládá z dávkové vstupní vrstvy, hluboké konvoluční neuronové sítě, za kterou následuje L_2 normalizace, jejíž výstupem je *face embedding*. Během trénování sítě je tato fáze následována *triplet loss* funkcí. Převzato z [31].

Na obrázku 2.9 je architektura modelu FaceNet, detaily hluboké konvoluční sítě (*deep architecture*) jsou popsány níže. Nejdůležitější částí tohoto přístupu je učení celého systému, od začátku do konce. Přičemž poslední částí modelu je *triplet loss* funkce, která přímo reflektuje cíle, kterých je třeba dosáhnout pro rozpoznávání tváří [31]. Konkrétně, cílem je *embedding* $f(x)$, ze snímku x do prostorů s příznaky $\mathbb{R}^d$, takového, že vzdálenost umocněná na druhou mezi všemi tvářemi, nezávisle na podmínkách snímání, je pro stejné identity malá, ale pro různé identity je velká. Výhodou optimalizace vzdálenosti pro trojice identit (*triplet loss*) je lepší schopnost pokrýt vnitro třídní variabilitu u obličeje [31]. Než jaké lze dosáhnout při použití optimalizace pro dvojice (páry pozitiv a negativ), kdy tato funkce podporuje projekci všech obličejů jedné identity do jednoho bodu v *embedding* prostoru. Přičemž použití trojic se snaží zachovat určitou volnost mezi páry tváří jedné identity vzhledem ke všem ostatním. Toto umožňuje větší rozmanitost pro obličeje jedné identity a zároveň dostatečnou rozlišitelnost od ostatních identit.

Embedding je reprezentován funkcí $f(x) \in \mathbb{R}^d$. Která přepočítává obrázek x do d-dimenzionálního Euklidovského prostoru. Navíc je tento *embedding* omezen do daného prostoru takto: $\|f(x)\|_2 = 1$. V *triplet loss* funkci je třeba zajistit, že obrázek x_i^a určité osoby (kotva) je blízko všem ostatním obrázkům x_i^p stejné osoby (pozitiv), než k obrázku x_i^n všech jiných osob (negativ). Jak je zobrazeno na obrázku 2.8. Tedy je hledán vztah:

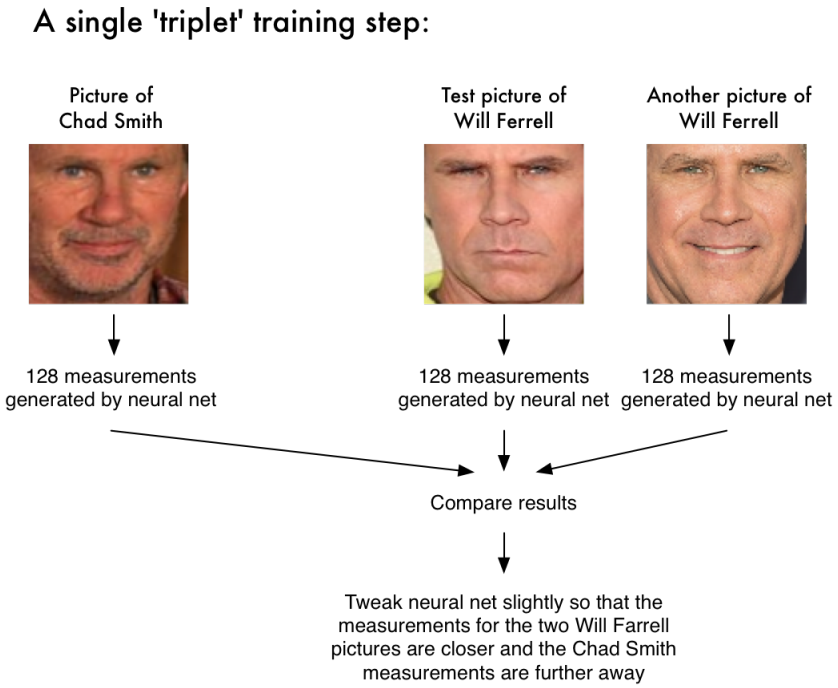
$$\|f(x_i^a) - f(x_i^p)\|_2^2 + \alpha < \|f(x_i^a) - f(x_i^n)\|_2^2, \qquad \forall (f(x_i^a), f(x_i^p), f(x_i^n)) \in \mathcal{T} \tag{2.11}$$

kde α je minimální vzdálenost mezi pozitivními a negativními páry. $\mathcal{T}$ je množina všech možných trojic v trénovací množině s kardinalitou N. Pak je při optimalizaci hledána minimální vzdálenost:

$$L = \sum_i^N \left[\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha \right]_+ \tag{2.12}$$

Generování všech dostupných trojic by vytvořilo mnoho trojic, které jsou lehce splnitelné (nalezení splnitelných vzdáleností podle podmínek v rovnici 2.11). Takové trojice však nepřispívají ke trénování sítě a jen zpomalují konvergenci. Proto je klíčový výběr těžko splnitelných trojic (*hard triplets*), které pomáhají zlepšování modelu. Na obrázku 2.10 je ukázka

vybrané trojice, která je hůře splnitelná. V následujícím odstavci je popsán výběr takových trojic.



Obrázek 2.10: Příklad trojice vybrané pro trénování modelu FaceNet a jednoho trénovacího kroku. Z každého snímku je generováno 128 ohodnocení tváře, ty jsou porovnány a podle výsledků je upravena neuronová síť tak, aby obrázky stejné osoby měly vzdálenost ohodnocení menší a obrázky rozdílných osob větší. Převzato z [11].

K dosažení rychlé konvergence je nutné vybírat trojice, které porušují podmínku v rovnici 2.11. Pro dané x_i^a je vybírán těžký positiv x_i^p (*hard positive*) a těžký negativ x_i^n (*hard negative*), tak aby:

$$\text{argmax}_{x_i^p} \|f(x_i^a) - f(x_i^p)\|_2^2, \qquad \text{argmin}_{x_i^n} \|f(x_i^a) - f(x_i^n)\|_2^2. \tag{2.13}$$

Není možné počítat argmin a argmax přes celou trénovací množinu [31]. Navíc by to mohlo vést ke špatným výsledkům, jelikož špatně označené tváře nebo tváře s horšími snímky by dominovaly těžká pozitiva a negativa. Tento problém lze řešit dvěma způsoby:

- *Offline* generování trojic. Každých několik kroků s použitím posledního uloženého bodu sítě a provádění výpočtu argmin a argmax na podmnožině trénovacích dat.
- *Online* generování trojic. Výběrem těžkých pozitiv a negativ z malých dávek trénovacích dat.

V systému FaceNet je používáno *online* generování trojic, přesněji jsou používány dávky trénovacích dat v řádu několika tisíců snímků, argmin a argmax jsou počítány jen v rámci dávky. Aby byly ve výsledku dosažena smysluplná reprezentace vzdálenosti mezi kotvou a pozitivem, je nutné zajistit, aby v každé dávce byl určitý minimální počet jedné identity. V rámci experimentů autoři vybírali přibližně 40 tváří od každé identity pro každou trénovací dávku. Výběr nejtěžších negativ může vést k nevhodnému lokálnímu minimu, přesněji

může být výsledkem zhroucení modelu ($f(x) = 0$). Tomu to případu se lze vyhnou vybráním x_i^n takto:

$$\|f(x_i^a) - f(x_i^p)\|_2^2 < \|f(x_i^a) - f(x_i^n)\|_2^2 \tag{2.14}$$

Taková negativa jsou označována jako polo-těžká.

Trénování konvolučních sítí FaceNet bylo prováděno pomocí *Stochastic Gradient Descent* s standardním *backpropagation* algoritmem a *AdaGrad* [31]. V rámci experimentů byly prozkoumány dvě rozdílné architektury, které se liší v parametrech a počtu FLOPS (*floating point operations per second*). Prvním modelem je 22 vrstvý Zeiler&Fergus s 140 milióny parametrů, který vyžaduje přibližně 1,6 miliard FLOPS na jeden snímek [31][39]. Druhá architektura je postavena na Inception modelech ve stylu GoogLeNet [31][33]. Tyto modely mají přibližně 20krát méně parametrů (cca 7 miliónů) a až 5 krát méně FLOPS (500 miliónů až 1,6 miliard). Některé modely jsou dramaticky zmenšeny a lze je tak spouštět na mobilních telefonech. V praxi záleží výběr nejlepšího modelu na požadavcích a zdrojích dané aplikace, například výkon datacentra versus mobilního zařízení.

Ohodnocení systému FaceNet probíhalo na 4 databázích, zajímavé jsou výsledky na populární LFW (*Labeled Faces in Wild*). U které probíhalo ohodnocení ve dvou režimech. V prvním byly použity snímky tváří označené z LFW, bez úprav poskytnutého zarovnání. Ve druhém případě byl použit proprietární detektor tváří, pro správné zarovnání obličejů ve snímcích LFW. Pokud selhal, bylo použito původní. V prvním případě dosáhl FaceNet přesnosti 98,87 %, ve druhém (při použití lepšího zarovnání obličeje) byla úspěšnost 99,63 % [31].

2.4 Vyhodnocování biometrických vlastností

V biometrii se rozlišují tři typy klasifikace: verifikace, identifikace a rozpoznávání. Při každé z těchto klasifikací dochází k různým chybám a je třeba mít dostupné způsoby jejich měření a vyhodnocování přesnosti biometrických systémů. Důležitým pojmem při hodnocení je biometrická entropie, která značí množství informace v konkrétní biometrické vlastnosti. V praxi jsou lépe využitelné vlastnosti s větší biometrickou entropií, ale vlastnosti, které ji mají příliš již ne, v obou případech nízké nebo vysoké entropie dochází totiž k většímu výskytu chyb [8]. Chyby se v biometrických systémech mohou vyskytovat ve všech jejich fázích činnosti. Tedy při snímání (sběru dat), zpracovávání nasbíraných dat, jejich ukládání, porovnávání a při učinění rozhodnutí. V této části je níže nejprve popsán rozdíl mezi verifikací a identifikací. Dále jsou popsány některé chyby biometrických systémů.

2.4.1 Verifikace versus identifikace

V závislosti na aplikaci může biometrický systém pracovat v režimu verifikace nebo identifikace. V módu verifikace systém provádí validaci identity člověka porovnáním snímaných biometrických dat s daty uloženými v databázi systému. Uživatel tohoto systému chce být rozpoznán na základě jeho identity, běžně používaným identifikátorem je PIN, uživatelské jméno nebo například čipová karta. K rozpoznání systém provede jedna ku jedné porovnání a určí, zda jde skutečně o daného uživatele. Typicky je verifikace používána pro pozitivní rozpoznávání, při kterém je cílem zamezit použití stejné identity více osobami.

V režimu identifikace systém rozpoznává jednotlivce pomocí hledání shody v databázi údajů všech uživatelů. Je tedy prováděno porovnání jedna ku mnoha, které prokáže identitu osoby (nebo také neprokáže, pokud cíl nemá svá data uložena v databázi) bez toho, aniž by si daná osoba nárokovala totožnost na základě nějakého identifikátoru. Proto je identifikace

kritická zejména při aplikacích využívající negativního rozpoznávání, při kterém systém prokáže zda osoba je osobou, kterou odmítá (implicitně nebo explicitně), že je. Cílem negativního rozpoznávání je zabránit jednotlivci v používání několika identit. Identifikaci lze využít i při pozitivním rozpoznávání pro větší komfort uživatele (není třeba si nárokovat totožnost). Přičemž tradiční metody rozpoznávání osob jako například hesla, klíče nebo PIN, mohou fungovat k pozitivnímu rozpoznávání, negativní rozpoznávání lze provádět pouze s využitím biometrických dat [19].

2.4.2 Chyby při porovnání biometrických dat

Při identifikaci vznikají u biometrických systémů chyby v důsledku rozhodování na základě skóre porovnání a nastaveného prahu. Obecně se biometrický systém skládá z částí: zachycení dat, zpracování signálu, uložení dat, porovnání a rozhodnutí. V části porovnání probíhá srovnání šablony z databáze se šablonou získanou zpracováním signálu. Výstupem porovnání je skóre, podle kterého se dále rozhoduje. Skóre porovnání bývá označeno s, jeho výsledek závisí na prahu $T \in < 0, 1 >$. Přičemž platí, že pokud je $s < T$, pak je tvrzení o identitě odmítnuto. V případě $s \geq T$, pak systém přijme tvrzení o identitě. Výsledkem je jeden z následujících stavů [8]:

- A přijato jako A, tedy *správné přijetí (True Accept*)
- A odmítnuto jako B, tedy *správné odmítnutí (True Reject)*
- A přijato jako B, tedy *chybné přijetí (False Accept)*
- A odmítnuto jako A, tedy *chybné odmítnutí (False Reject)*

Pro hodnocení biometrických systémů jsou významné metriky chybových stavů. Chybový stav nastane v případech, kdy jsou dva vzory rozdílných osob klasifikovány jako stejné (False Accept) nebo kdy jsou dva vzory stejné osoby klasifikovány jako různé (False Reject). Z těchto stavů jsou odvozeny následující chybové metriky.

Míra chybného přijetí

Míra chybného přijetí - FAR (*False Accept Rate*) je pravděpodobnost, kdy biometrický systém chybně klasifikuje dva různé vzory jako shodné. Tedy jde o podíl chybně potvrzených s celkovým počtem porovnání různých [8]:

$$\textbf{FAR} = \frac{\text{Počet chybně přijatých různých vzorů}}{\text{Celkový počet porovnání různých vzorů}}$$

Míra chybného odmítnutí

Míra chybného odmítnutí - FRR (*False Reject Rate*) je pravděpodobnost, kdy biometrický systém chybně klasifikuje dva vzory téže osoby jako různé. Tedy jde o podíl chybně odmítnutých s celkovým počtem porovnání stejných [8]:

$$\textbf{FRR} = \frac{\text{Počet chybně odmítnutých vzorů osoby A}}{\text{Celkový počet porovnání vzorů osoby A}}$$

Míra chybné shody

Míra chybné shody - FMR (*False Match Rate*) je podíl chybně přijatých osob s celkovým počtem, ale rozdílně od FAR nejsou do celkového počtu započítány pokusy neúspěšné ještě před srovnáním (tedy FTA nebo FTE - viz níže). FMR je definováno:

$$\mathbf{FMR}(T) = \int_{T}^{1} p(s|H_1)ds \tag{2.15}$$

kde T je práh rozhodování, H_1 je výrok „různé“ (porovnávané vzory jsou rozdílné), p je hustota pravděpodobnosti, že výrok v závorce je pravdivý, s je skóre porovnání [8].

Míra chybné neshody

Míra chybné neshody - FNMR (*False Non-Match Rate*) je podíl chybně odmítnutých osob s celkovým počtem, ale rozdílně od FRR nejsou do celkového počtu započítány pokusy neúspěšné ještě před srovnáním (FTA a FTE - viz níže). FNMR je definováno:

$$\mathbf{FNMR}(T) = \int_{0}^{T} p(s|H_0)ds \tag{2.16}$$

kde T je práh rozhodování, H_0 je výrok „shodné“ (porovnávané vzory jsou od stejné osoby), p je hustota pravděpodobnosti, že výrok v závorce je pravdivý, s je skóre porovnání [8].

Míra neschopnosti nasnímat

Míra neschopnosti nasnímat - FTA (*Failure To Acquire*) je podíl chybných snímků v automatickém módu daného senzoru ku celkovému počtu snímků v tomto režimu. Především je tato míra vhodná pro hodnocení kvality senzorů, vyšší hodnota znamená menší vhodnost senzoru pro daný úkol [8].

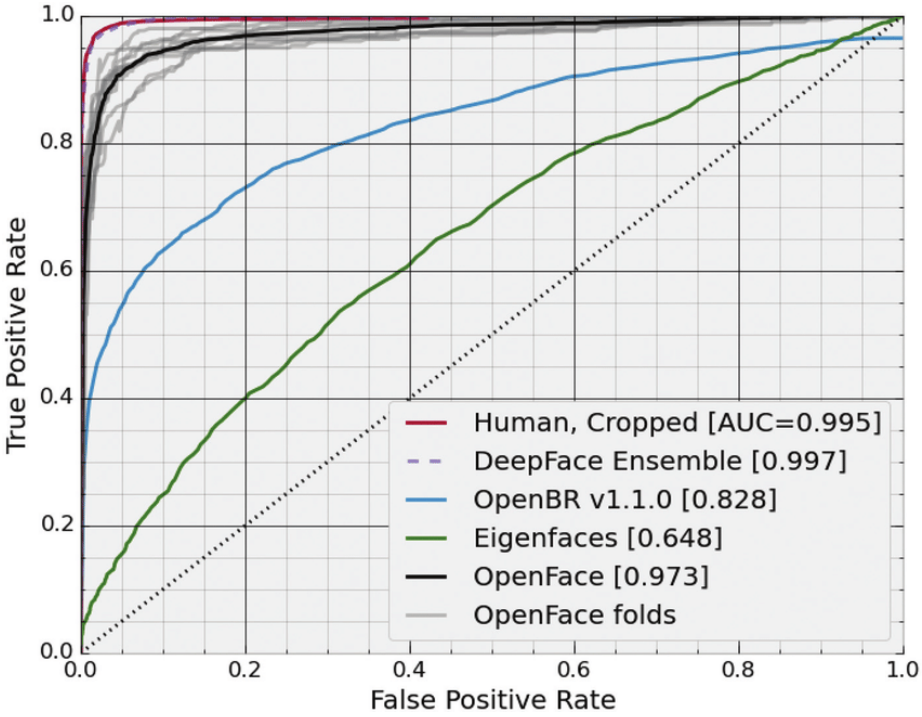
Míra neschopnosti zaregistrovat

Míra neschopnosti zaregistrovat - FTE (*Failure to Enroll*) je podíl uživatelů, které se systém nedokáže naučit rozpoznat k celkovému počtu pokusů o nasnímání uživatelů. Tato míra je užitečná u systémů s kontrolou kvality biometrické charakteristiky. FTE lze také chápat jako ohodnocení schopnosti algoritmu pracovat s nekvalitními charakteristikami [8].

Míra neschopnosti porovnat

Míra neschopnosti porovnat - FTM (*Failure To Match*) je podíl biometrických charakteristik, které nelze porovnat se šablonou a nebo jinak zpracovat (pro registrované uživatele) [8]. Ukazuje schopnost systému rozhodnout výsledek porovnání.

Se změnou hodnoty prahu T (práh určující rozhodnutí o přijetí nebo odmítnutí) se mění hodnota chybových metrik FMR a FNMR. Mění se obě hodnoty zaráz opačnými směry. Proto je třeba výkonnost systému udávat jinou metrikou. Používá se k tomu tzv. ROC křivka (*Receiver Operating Curve*). Někdy je používán ekvivalent ROC křivky v podobě DET křivky (*Detection Error Trade-off*). Který se liší pouze v reprezentaci zanášených hodnot do grafu. Křivka ROC ukazuje detekční schopnost funkce FMR vzhledem k FNMR (nebo FAR/FRR). Na obrázku 2.11 je ukázán příklad ROC křivky.



Obrázek 2.11: ROC křivka, v grafu jsou porovnány algoritmy rozpoznávání obličeje. Testování probíhalo na databázi LFW. Převzato z [34].

Kapitola 3

Biometrické brány

Častým použitím biometrických bran je jejich nasazení na letištích pro automatizované odbavení cestujících, pro toto využití jsou používány pojmy *Automated Border Control* (dále jen ABC) nebo eGate. Tyto systémy nasazené například v Německu a České Republice ověřují uživatele podle obličeje [32]. Španělský systém používá kombinaci otisků a obličeje, která podává srovnatelné výsledky s Britským systémem IRIS rozpoznávajícím pouze duhovku [2].

Vysoce zranitelnou částí těchto systémů je lidský faktor. Mezi důvody chyb zaměstnanců patří nedostatečný trénink, nízká motivace a spokojenost z práce, únava, spatné podmínky na pracovišti a obecné omezení pracovního výkonu a vnímání u lidí. Ke zvládnutí těchto problémů jsou vyvíjeny nové strategie modernizace hraničních kontrol. Za klíčové je považována automatizace a vylepšení procesu ověření totožnosti a odbavení cestujících.

V následujícím textu níže je nejprve popsán vývoj biometrických bran a jejich architektura. V další části je popsán systém ohodnocení výkonu biometrických bran. Následuje část popisující problémy existujících bran. Na tuto část navazuje popis ABC systémů používaných v současnosti. V poslední části jsou vybrány podstatné vlastnosti biometrické brány pro tuto práci.

3.1 Vývoj biometrických bran

Prvotním použitím biometrie jako technologie pro automatické ověření osob na základě jejich vlastností, bylo v omezení přístupu, například do budov nebo jiných chráněných oblastí. Řízení přístupu pomocí otisků nebo snímku duhovky se stalo jednou z nejpoužívanějších aplikací biometrie v praxi. Přičemž stále v těchto systémech existují určité problémy, v mnoha organizacích se staly podstatnou částí jejich zabezpečení. Pro tyto systémy bylo vyvinuto několik standardů a pokynů pro jejich správné nasazení a také k ohodnocení jejich výkonů [25].

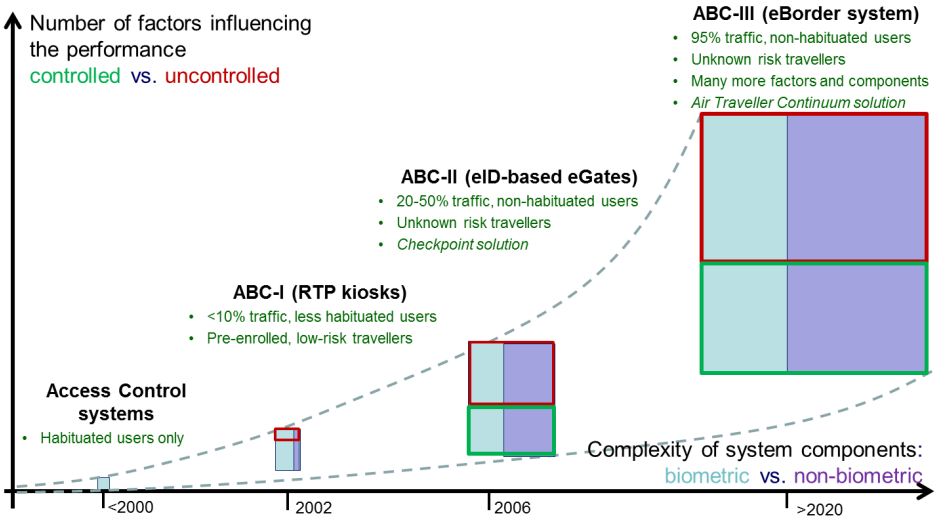
Díky úspěchu biometrických systémů řízení přístupu, bylo přirozenější jejich rozšíření pro použití při kontrolách na hranicích. Kolem roku 2000 několik států začalo podporovat programy pro prověřené nebo registrované cestovatele, které umožňovaly překročení hranic pro předem prověřené osoby pouze s kontrolou jejich biometrických údajů [13]. Dosaženo toho bylo pomocí opětovného použití některých systémů využívaných již při řízení přístupu. Přestože jsou však oba systémy podobné, biometrické brány pro hraniční kontrolu mají několik podstatných rozdílů oproti branám používaným pro řízení přístupu (dle [13]):

1. Uživatelé většinou nejsou na systém zvyklí.

2. Otevřená množina uživatelů.
3. Uživatelé s neznámým bezpečnostním rizikem.
4. Větší počet podpůrných technologií (komplexnější).
5. Více automatizovaný provoz a školení personálu.
6. Náročnější podmínky pro infrastrukturu.
7. Méně ovlivnitelné prostředí, méně pod kontrolou.

Také je vhodné podotknout, že tyto systémy jsou většinou nasazeny ve veřejných prostorech a jejich operátoři patří k různým skupinám (správa letiště, ochranka veřejné dopravy, celní kontrola), které mají různé a někdy i konfliktní záměry použití biometrických bran.

Na rozdíl od prvotních generací eGate a podobných systémů, jejichž použití bylo dobrovolné a pouze doporučené, jsou dnešní biometrické brány považovány za nutnou součást moderní hraniční kontroly. V současnosti je snahou postupně zpracovávat většinu kontrol cestujících pomocí automatických bran. Tedy brána musí pracovat bez výpadků 24/7, čímž je nutné ji neustále monitorovat a zajišťovat správný chod. V některých případech, je tato podpora zajištěna pracovníky, kteří mají zároveň další kritické povinnosti a tím je narušována bezpečnost.



Obrázek 3.1: Diagram průběhu vývoje biometrických bran. Ilustruje podpůrné technologie každé generace a okolnosti které ovlivňují výkon ABC v různých generacích. Převzato z [13].

Evoluce biometrických systémů je zobrazena na obrázku 3.1. Následníkem biometrických systémů řízení přístupu (*access control systems*), jsou systémy nasazené pro ověřené cestující RTP (*Registered Traveler Program*), které jsou označovány za 1. generaci biometrických bran. Za druhou generaci jsou považovány eGate nainstalovány na letištích, které prověřují cestující na základě jejich ePasu a dalších dokumentů s biometrickými údaji (na obrázku 3.1: ABC-II). Budoucí systémy budou zpracovávat všechny pasažéry, na základě informací o nich posbíraných během jejich cestování (ABC-III na obrázku 3.1).

Příkladem biometrických bran první generace jsou odbavovací zařízení NEXUS, založené na verifikaci duhovky, použité na hranici mezi Kanadou a USA [3]. Nebo již zmíněné

přístroje IRIS, které byly v roce 2012 v Anglii vyřazeny z provozu [9]. Zařízení druhé jsou například systémy eGate použité v České Republice a jinde v Evropě [32]. Analýzu a definice těchto systémů provádí organizace Frontex [9]. Třetí generace je konceptem dalšího vývoje biometrických bran, v mnoha zemích je podporován vývoj a budoucí nasazení těchto systémů, které slibují bezpečnější a rychlejší odbavení cestujících [13].

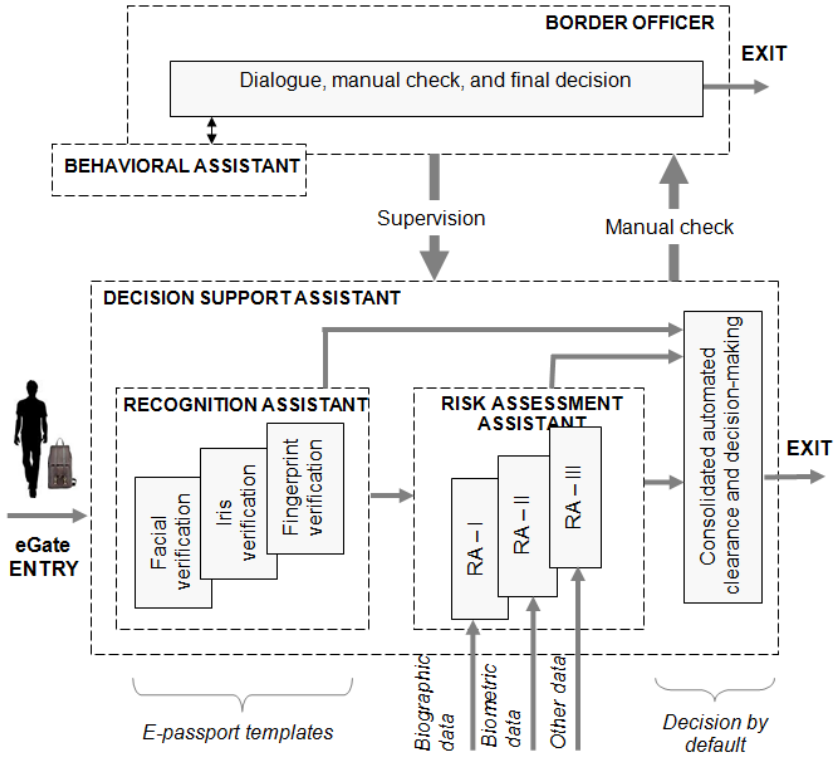
Formálně lze definovat bránu třetí generace systém, který má následující vlastnosti [13]:

1. Využívá zcela infrastruktury letiště a procesů souvisejících s ním.
2. Je to rozsáhlý (*large-scale*) systém.
3. Provádí ověřování cestujících.
4. Jedná se o poloautomatický systém, který pracuje pod dohledem pracovníka.
5. Jedná se o systém rozlišující rizika (profilování), který analyzuje dostupné informace o každém cestujícím a přiděluje mu rizikový faktor.
6. Automaticky komunikuje přes síť s dalšími ABC stroji a součástmi *eBorder*.
7. Lze jej používat v provozním režimu, ale i v tréninkovém režimu, který slouží pro rychlé a automatizované školení obsluhy.

3.2 Architektura ABC zařízení

Na obrázku 3.3 je zobrazena koncepce ABC zařízení, které lze vnímat jako asistenta podpory rozhodování. Jeho součástí je asistent rozpoznávání (*Recognition Assistant*), jehož úkolem je verifikovat identitu pomocí biometrických metod specifikovaných elektronickým pasem. Další částí je asistent ohodnocení rizika (*Risk Assessment Assistant*), který provádí funkci ohodnocení rizika, jejíž vstupem jsou veškeré dostupné informace o cestujícím. Zprávy poskytované těmito asistenty jsou zpracovávány na základě principů konsolidovaného schvalování a rozhodování [13]. Výstupem je doporučení, které je ve výchozím nastavení konečné. Toto nastavení odpovídá poloautomatickému principu kontroly. Pokud byl cestující přesměrován na ruční kontrolu, řídící pracovník používá techniku rozhovoru, který lze podporovat pomocí behaviorálního asistenta (*Behavioral Assistant*) [37].

Obrázek 3.2: Systém EasyGO nasazený na letišti Václava Havla v Praze. Převzato z [32].



Obrázek 3.3: Architektura ABC systému. Převzato z [13].

3.3 Hodnocení výkonnosti biometrické brány

Existuje několik různých přístupů hodnocení výkonnosti biometrické brány. Jejich výkon je měřen různými metrikami, například *Operational Reject Rate* [28] nebo *Throughput Rate* [10]. Tyto techniky hodnocení pokrývají základní scénáře nasazení ABC zařízení. V některých scénářích lze výkonnost měřit pomocí vhodných technik modelování a simulace. Běžně je k hodnocení výkonnosti potřebné jednoduché metriky kombinovat, tento přístup obecně poskytuje lepší výsledky. Zároveň je nutné do hodnocení zahrnout fakt, že operační výkon ABC systému je značně menší než výkon konkrétní komponenty biometrického rozpoznávání nebo softwaru [28]. Pro sledování efektu poklesu výkonu je nutné použít kombinované metriky.

Výkon ABC zařízení je ovlivněn technickými i netechnickými faktory. Technické lze efektivně řídit. Například lze vylepšit výkon použitých rozpoznávacích algoritmů, rozhraní mezi strojem a člověkem lze navrhnout pro lepší schopnost adaptace uživateli, je možné vylepšit ergonomii brány, modernizovat logistiku letiště a lépe vyškolit zaměstnance.

Netechnické faktory zahrnují sociální, psychické, etnické, kulturní, náboženské a zeměpisné faktory. Běžně je těžké nebo přímo nemožné je ovlivnit, přičemž mohou značně ovlivnit výkonnost systému.

Ve článku *Automated border control: Problem formalization* autoři definují hodnocení výkonu biometrické brány během různých fází životního cyklu následovně (dle [13]):

1. Fáze návrhu: *Theoretical* nebo algoritmický limit výkonu, jedná se o výkon algoritmu rozpoznávání biometrické charakteristiky, který je naměřen testováním na databázi biometrických vzorků.

2. Fáze tvorby prototypu: *Predicted* nebo výkon udávaný výrobcem. Jedná se o výkon biometrického algoritmu integrovaného do biometrické brány.

3. Fáze používání: *Operational* nebo reálný výkon brány nasazené v praxi, který určuje poměr cestujících, které brána nedokáže ověřit s těmi ostatními. Většinou je vyjádřena frází: „Jeden z N cestujících je přesměrován na ruční kontrolu“.

Kombinované hodnocení výkonu během celého životního cyklu zahrnuje dvě metriky: FRR (*False Reject Rate*) pro měření teoretického a předpokládaného výkonu a ORR (*Operational Reject Rate*) pro měření provozního výkonu [28].

Důležité vlastnosti biometrické brány

Pro uživatele je velmi důležitou vlastností doba, kterou trvá identifikace pomocí biometrické brány. Například u EasyGO systémů se jedná přibližně o 15 až 18 sekund [32]. Další podstatnou vlastností je parametr ORR, který určuje kolik uživatelů je nutné odbavit ručně, jelikož je automatický systém nebyl schopný identifikovat. Oba tyto parametry jsou pro bránu v této práci podstatné, jelikož cílem je vytvořit rychlý a spolehlivý systém pro identifikaci.

3.4 Problémy existujících systémů

Zkoumáním problémů s nasazenými biometrickými bránami, včetně problémů, které vedly k ukončení programu UK IRIS [1] a těch které způsobují odchylky ve výkonech evropských eGate systémů, lze vyvodit následující závěry.

Podstatné procento selhání zjištěných v těchto systémech nesouvisí s výkonem rozpoznávání biometrických vlastností. Například systémy eGate posílají přibližně každého osmého cestujícího na ruční kontrolu, s mírou odmítnutých měnící se drasticky mezi různými státy. Tento jev indikuje přítomnost dalších faktorů, které ovlivňují výkonnost biometrické brány [28], kromě kvality rozpoznávání biometrických dat. Některé z těchto faktorů lze ovládat, jako například rozhraní mezi přístrojem a člověkem, ergonomie, logistika letiště a trénink zaměstnanců. Jiné faktory ovládat nelze, například únavu cestujících nebo jejich obeznámenost se systémem.

Mimo to je biometrická brána jen jednou z mnoha komponent v komplexním procesu překročení hranice. Díky tomu, lze chyby biometrického rozpoznávání způsobené jeho nedostatky, vyvážit pomocí ne-biometrických prostředků. Tedy je podstatné obecně znát proces odbavení pomocí biometrických technologií a jakou roli v něm hrají biometrické komponenty.

Iris Recognition Immigration System byl program odbavení cestujících pomocí biometrických bran v Anglii [1]. Cílem bylo poskytnout rychlejší a automatické odbavení pro předem zapsané a časté cestující, kteří nesou nízké bezpečnostní riziko, pomocí biometrie duhovky. Systém porovnával aktuální snímky duhovky se snímky uloženými v databázi. V roce 2013 byl zrušen a nahrazen branami používajícími elektronické pasy [1] Klíčové faktory, které vedly k jeho zavření jsou popsány ve článku *Ten Reasons Why IRIS Needed 20:20 Foresight: Some Lessons for Introducing Biometric Border Control Systems* [30].

V současnosti je nejvíce rostoucím projektem odbavení pomocí biometrických bran systém eGate, provozovaný v Evropě. Výsledkem jejich analýzy jsou následující zjištění. Zatímco německá policie je obecně spokojena s výsledky EasyPASS systémů, je množství

odmítnutých cestujících, označováno jako *Operational Reject Rate* (ORR), které je definováno jako celkový poměr lidí odeslaných na ruční kontrolu, stále příliš vysoké. Na základě aktuálních statistik je v budoucnu cíleno na dosažení výsledků ORR < 10 %. Tento cíl se dělí na dvě části, biometrickou (< 5 %) a část ORR kterou ovlivňují kontroly dokumentů a další faktory (< 5 %). Obecně je cílem optimalizace uživatelského protokolu úplné vyhnutí se odmítnutí systémem z důvodu chování cestujícího.

Statistiky z článku [2] poskytují další detaily ohledně rozdílných výsledků biometrických bran pro různé skupiny uživatelů. Nejlepší FRR obličeje byla dosažena u Portugalců (FRR = 1,36 %) a nejhorší u občanů Dánska (FRR = 18,18 %). Průměrně byl během měření odmítnut z důvodu chyby verifikace obličeje každý desátý cestovatel (FRR = 9,30 %, pro 18884 testovaných uživatelů).

3.5 Biometrické brány používané v současnosti

V tabulce 3.1 je shrnutí kombinovaného měření výkonnosti pro některé brány nasazené v Evropě. První tři sloupce obsahují název brány a zemi nasazení, rok měření a odkaz na zdroj informací. Další sloupce obsahují naměřené hodnoty výkonnosti ve fázích používání, tvorby prototypu a návrhu (teoretický výkon) v kontextu $1{:}N$ (1 osoba z N je chybně nerozpoznána). Pro zjednodušení data v posledním sloupci odpovídají následujícím FRR hodnotám algoritmů rozpoznávání: FRR duhovky = 0,1%, FRR otisků prstů = 0,1%, FRR obličeje = 1%, FRR kombinace otisků prstů a obličeje = 0. ,1% [14].

Zařízení	**Praktický výkon**	**Odhadovaný výkon**	**Teoretický výkon**
IRIS (UK)	1:10	1:50 (2 %)	1:1000
EasyPASS (DE)	1:8	1:20 (5 %)	1:100
ABC System (ES)	1:10	1:25 (4 %)	1:1000

Tabulka 3.1: Porovnání výkonu ABC zařízení použitých ve Spojeném království (duhovka), Německu (obličej) a Španělsku (obličej a otisk prstu) [2]. Význam poměru určujícího výkon je: 1 osoba z N je chybně nerozpoznána.

Nejlepší praktické výsledky u současných biometrických bran pracují s výsledky přibližně ORR = 1:10, tedy 1 z 10 cestujících je přesměrován na ruční kontrolu. Všechny v praxi používané biometrické brány mají dobré zdroje pro vylepšení výkonu. Například zařízení použité v Anglii, rozpoznávající duhovku, používalo jen 1/100 svých zdrojů. Brány identifikující podle obličeje, které jsou nasazeny v Německu a Španělsku, používají 1/10 potencionálních zdrojů [13]. Instituce jako NIST a ISO podstoupily značné úsilí pro zlepšení návrhu a výkonu algoritmů rozpoznávání biometrických vlastností. Avšak z dostupných výsledků lze vidět, že samotné zlepšení výkonu rozpoznávacích algoritmů nemusí zlepšit výkonu celého systému. Například Španělský systém používající kombinaci dat obličeje a otisků prstů, podává jen o trochu lepší výsledky než systémy s jedinou biometrickou vlastností [2]. U nekontrolovatelných faktorů je zde postupně úsilí o snížení jejich vlivu, ale pro zlepšení situace je nutné ji lépe prozkoumat. Tyto faktory většinou nejsou technického původu, jedná se například o chování cestujících [13]. V České Republice jsou používány brány rozpoznávající obličej cestujících, na obrázku 3.2 lze vidět jejich umístění na letišti Václava Havla v Praze.

Kapitola 4

Návrh biometrické brány

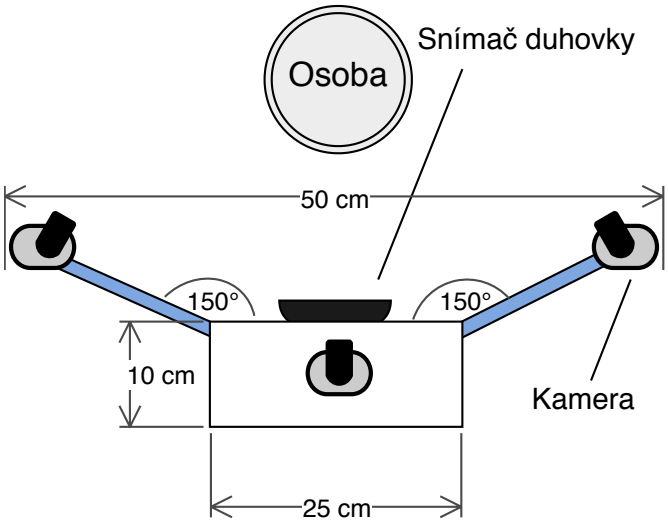
Cílem je navrhnout biometrickou bránu využívající tří kamer pro snímání obličeje ze tří úhlů a snímače duhovky obou očí. Obsluhu brány zajišťuje aplikace, která pracuje ve dvou hlavních režimech. Prvním je registrace nového uživatele brány do databáze, druhým režimem je identifikace osoby nacházející se v záběru brány. Aplikace pracuje jako konzolový program s výstupem v okně na obrazovce a zároveň s výstupem do terminálu. Při identifikaci je třeba, aby se uživatel posadil před biometrickou bránu a podíval se do snímače duhovky. Aby byl snímek duhovky v dobré kvalitě, bude uživatel indikovat svou připravenost pro snímání duhovky stiskem klávesy. Snímání obličeje probíhá následně a již plně automaticky. Registrace bude poloautomatická, aplikace bude spuštěna v režimu registrace a osoba kontrolující bránu bude řídit snímání nového uživatele. Vstupem při režimu registrace jsou údaje o novém uživateli. Po dokončení snímání nového uživatele je systém trénován na jeho rozpoznání. V režimu identifikace je v okně zobrazen výstup z kamery a výsledky identifikace v podobě označení obličeje ve snímku, zobrazení jména uživatele s procentuální podobností nebo vzdáleností od jeho šablony v databázi. Tyto údaje budou výstupem každé kamery a také výstupem identifikace duhovky levého i pravého oka. Výsledné rozhodnutí identifikace závisí na nastavení důležitosti jednotlivých biometrických charakteristik a požadovaného počtu správně identifikovaných (například 4 z 5 možných).

V této kapitole jsou stručně popsány návrhy konstrukce brány a rozmístění kamer, uložení nového uživatele do databáze, algoritmu identifikace tváře ze tří úhlů, algoritmu identifikace duhovky a pravidel pro určení identity na základě výstupu těchto algoritmů.

4.1 Konstrukce biometrické brány

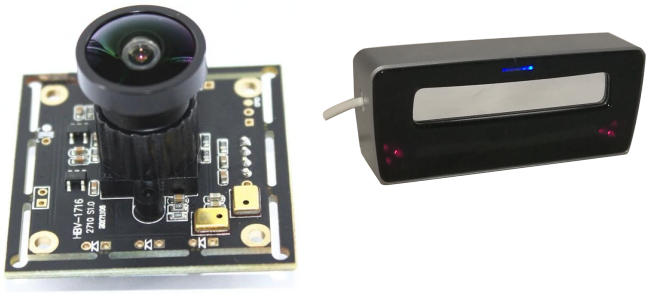
Pro návrh biometrické brány je vhodné vybrat způsob konstrukce, který umožňuje snadno měnit pozice a úhly kamer, aby šlo jednoduše testovat rozmístění kamer a vybrat vhodné nastavení brány. V případě hotové a otestované konstrukce, kterou není třeba příliš měnit, je vhodné použít k její stavbě například 3D tiskárnu.

Na obrázku 4.1 je ukázán návrh konstrukce brány. Na obrázku je vidět navržené rozmístění kamer snímajících obličej. Umístění jedné kamery frontálně a dvou na každou stranu obličeje je vhodné zejména díky dosažení větší variability snímků obličeje. Tato konstrukce byla navržena na základě experimentů při stavbě brány a výsledné rozmístění, společně s úhly natočení postranních kamer poskytují vhodné snímky, u kterých použitý algoritmus rozpoznávání tváře dokáže dostatečně rozeznat úhel snímaného obličeje při identifikaci. Detaily experimentů s identifikací tváře jsou popsány níže v kapitole 6.



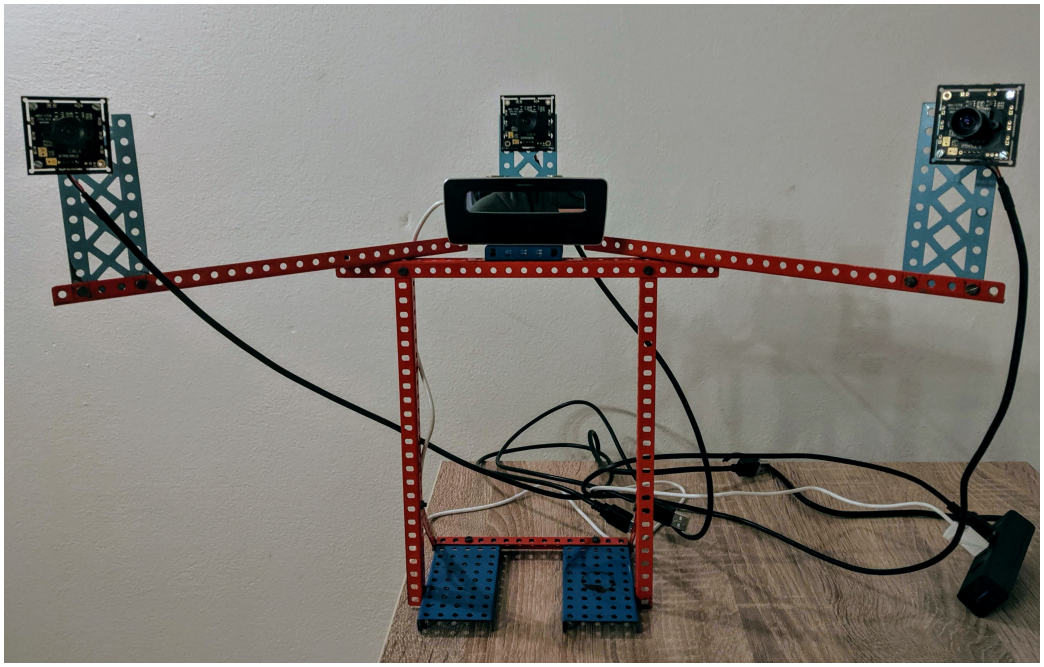
Obrázek 4.1: Návrh biometrické brány pro identifikaci osob podle obličeje a duhovky.

Pro snímání obličeje byly vybrány kamery HBV-1716 s rozlišením 1980 × 1080 pixelů (na obrázku 4.2 vlevo). Dle specifikace poskytuje kamera video s tímto rozlišením při 30 snímcích za sekundu, dále má úhel zorného pole 110°, ideální vzdálenost snímaného objektu 5 až 130 cm a připojení přes rozhraní USB. Tato kamera plně vyhovuje požadavkům aplikace, navíc jsou její výhodou malé rozměry. Pro snímání duhovky bylo vybráno zařízení IR2800D od firmy INJES (na obrázku 4.2 vpravo). Snímání duhovky probíhá ve vzdálenosti 16 až 20 cm, rozlišení snímků je 640 × 480 pixelů. Kamera má snímače pro obě oči, uživatel se při snímání řídí pohledem do vestavěného zrcátka. Dle specifikace má hodnoty FAR $<$ 0,000001 % a FRR $<$ 1 %. Tato kamera je dostačující pro splnění požadavků zadání, není však vysokorychlostní, avšak při navrženém algoritmu identifikace není toto omezení překážkou.



Obrázek 4.2: Vlevo kamera HBV-1716 pro snímání obličeje. Vpravo snímač duhovky obou očí INJES IR2800D.

Při návrhu a stavbě brány byla použita stavebnice Merkur společně s výtisky ze 3D tiskárny pro uchycení postranních kamer. Takto sestavená brána, společně s kamerami uvedenými výše lze připojit k počítači s operačními systémy Windows, Linux či Mac OS. Kromě operačního systému jsou požadovány 4 samostatné USB porty. Na obrázku 4.3 je výsledná biometrická brána.



Obrázek 4.3: Biometrická brána postavená pomocí stavebnice Merkur.

4.2 Snímání biometrických vlastností

Vybranými biometrickými vlastnostmi jsou duhovka a obličej. Důvodů pro toho rozhodnutí je několik, obě vlastnosti lze snímat bezdotykově, tedy relativně pohodlně a rychle. Tím bude dosažen jeden z cílů používání biometrických bran, kterým je usnadnění identifikace osob. Zároveň je vhodné tyto vlastnosti kombinovat, výsledkem kombinace by měla být větší přesnost zařízení (jak bylo popsáno v předešlé kapitole o biometrických branách). Použití těchto vlastností je také vhodné ke snížení nákladů na stavbu brány, jelikož pro snímaní tváře stačí použití běžných kamer, snímače duhovky jsou již nákladnější (než například otisků prstů). Ale použitím otisků by byly ztraceny některé výhody duhovky, dalším je například i větší unikátnost duhovky oproti otiskům prstů. V této části je nejprve popsán návrh rozpoznávání obličeje a poté návrh rozpoznávání duhovky. Blokové diagramy jejich algoritmů jsou v následující kapitole o jejich implementaci. Také je uveden význam pravidel pro určení identity a základní návrh práce řídící aplikace.

4.2.1 Rozpoznávání obličeje

K detekci obličeje jsou vybrány dva algoritmy, mezi kterými lze v programu přepínat, dle potřeby a zdrojů uživatele. Prvním je HOG, který je méně náročný a zároveň méně přesný. Druhým je detektor CNN. Oba jsou implementovány v knihovně Dlib[1], detaily detektorů jsou popsány v sekci 2.3.1. Detektor CNN podporuje akceleraci pomocí grafického procesoru s využitím knihovny CUDA, díky tomu může být rychlejší než HOG a zároveň přesnější.

Po nalezení obličeje ve snímku jsou extrahovány jeho příznaky, k tomu je vybrán opět algoritmus z knihovny Dlib, založený na ResNet neuronových sítích. Princip výpočtu je podobný systému FaceNet, který je uveden v sekci 2.3.2. Výstupem extrakce příznaků je 128

[1] http://dlib.net/

dimenzionální *embedding*. Který je dostatečně odolný vůči varianci v osvětlení a pozici tváře. Tyto příznaky jsou pak porovnány se vzdáleností od uložených šablon. K tomu je použit klasifikační algoritmus, pro klasifikaci takového 128 dimenzionálního vektoru je například vhodný algoritmus k-nejbližších sousedů.

4.2.2 Rozpoznávání duhovky

Pro rozpoznávání duhovky lze pro zjednodušení přepokládat, že vstupem jsou snímky duhovky. Proto není třeba do algoritmu identifikace zahrnout i detektor. Pro extrakci příznaků duhovky je vybrán Daugmanův algoritmus (popsán v sekci 2.2.2). Využita bude knihovní implementace Daugmanova algoritmu v jazyce Python, detaily její implementace jsou v následující kapitole. Po sejmutí snímků duhovky jsou oba obrázky převedeny na binární kód a uloženy do databáze šablon se jménem a označením oka dané osoby (identity). Při identifikaci je pak stejným způsobem nasnímána duhovka, její snímek je převeden na binární kód a ten je porovnán s databází šablon, hledá se, zda existuje šablona s požadovanou minimální Hammingovou vzdáleností. Výstupem rozpoznávání je výsledek identifikace pro každé oko, s odhadovanou identitou a vzdáleností od snímaného oka.

4.2.3 Pravidla pro určení identity

Protože brána má celkem 5 kamer a z každé je počítán výstup identifikace, je třeba navrhnout pravidla určení identity snímané osoby. To znamená určit jakou váhu bude mít výsledek jednotlivých rozpoznávání a kolik rozpoznávání se musí na výsledné identitě shodnou, aby bylo provedeno rozhodnutí, že se skutečně jedná o danou osobu. Váhy jednotlivých biometrických charakteristik a nastavení počtu shodujících se identit pro úspěšnou identifikaci je vhodné provádět společně s experimenty ověřujícími úspěšnost identifikace jednotlivých částí. Proto budou detaily pravidel popsány později v kapitolách implementace a experimenty.

4.2.4 Aplikace

Výsledná aplikace bude pracovat ve dvou hlavních režimech, a to registrace nového uživatele a identifikace osoby bránou. Z výstupu aplikace by mělo být zřejmé jaký je výsledek identifikace, zda se jedná o neznámou osobu nebo byla nalezena odpovídající identita a s jakou pravděpodobností. Případně s jakou vzdáleností od uložených biometrických charakteristik dané osoby. Aplikace bude implementována pro spouštění a ovládání přes příkazovou řádku, s výstupem na obrazovku v podobě přenosu z přední kamery biometrické brány a popisnými údaji s výsledky identifikace.

Kapitola 5

Implementace

V této kapitole jsou popsány detaily implementace návrhu biometrické brány a aplikace pro identifikaci osob podle obličeje a duhovky. Pro implementaci byl jako vhodný vybrán jazyk Python, jelikož jeho prostředí poskytuje vhodné možnosti a nástroje pro zpracování obrazu a obsluhu kamer. Program byl implementován pro operační systém Windows, avšak díky použitým nástrojům jej lze používat i na systému Linux nebo Mac OS. V první části této kapitoly jsou popsány použité nástroje. Dále následuje stručný popis použitých metod a funkcí z knihoven. Pokračuje popis nejprve registrace nového uživatele, pak samotné identifikace osoby. V posledních částech je blíže popsána implementace rozpoznávání tváře a rozpoznávání duhovky.

5.1 Použité knihovny a nástroje

Program byl vyvíjen a testován pod operačním systémem Windows pro 64 bitovou architekturu. Použitým jazykem a interpretem je Python ve verzi 3.7.0 64-bit. Další použité nástroje jsou OpenCV 4.1.0 (*Open Source Computer Vision Library*), NumPy 1.16.1, Nvidia CUDA 10, Dlib 19.16 [21], balíček `face-recognition` verze 1.2.3 (autorem je Adam Geigey), `imutils` 0.5.2 (autorem Adrian Rosebrock) a `scikit-learn` 0.20.3.

OpenCV

Open Source Computer Vision je knihovna s otevřeným kódem zaměřená na počítačové vidění a strojové učení. OpenCV bylo vyvinuto k poskytnutí obecné infrastruktury pro aplikaci v počítačovém vidění a k rychlejšímu rozšíření strojového vidění v praxi. Je vydáváno s licencí BSD.

Tato knihovna obsahuje více jak 2500 optimalizovaných algoritmů, mezi které patří obsáhlá skupina klasických i současných technik zpracování obrazu a strojového učení [29]. Například lze tyto algoritmy použít pro detekci a rozpoznání tváře, identifikaci objektů, sledování pohybu kamery, sledování pohyblivých předmětů, tvorba 3D modelů objektů ze scény, inteligentní spojování snímků, hledání podobných obrázků, sledování pohybu očí, rozpoznání scény a její zapojení do rozšířené reality a mnoho dalších způsobů použití. Počet stažení OpenCV přesahuje 18 miliónů a komunita uživatelů této knihovny překračuje 47 tisíc lidí, velkou částí těchto uživatelů jsou firmy, výzkumné skupiny a vládní orgány [29]. OpenCV je prakticky nasazeno například pro tvorbu Google Street View, v Izraeli k detekci narušitelů z videopřenosu bezpečnostních kamer, pro monitoring důlních zařízení v Číně, v Evropě k detekci topících se lidí v bazénu nebo v Japonsku k rychlé detekci tváří.

Tato knihovna má rozhraní pro jazyky Python, C++, Java a MATLAB [29]. Napsána je nativně v jazyce C++. Podporuje operační systémy Windows, Linux, Android a Mac OS. Primárním zaměřením je zpracování obrazu a počítačové vidění v reálném čase.

V implementovaném programu je knihovna OpenCV využita pro práci s kamerami, pořizování, načítání a ukládání snímků. Dále pro vykreslení a zobrazení výstupu identifikace. Některé její funkce, například pro otevření proudu dat z kamery nebo úpravu obrázků, jsou použity v rámci balíčku `imutils`, který zaobaluje několik funkcí OpenCV a umožňuje tak s nimi pohodlnější práci.

NumPy

NumPy je knihovna zaměřená na vědecké výpočty v jazyce Python. Do kterého přidává podporu pro velké N-dimenzionální pole a matice, společně s množstvím matematických funkcí pro operace nad těmito datovými typy. NumPy je využito i v knihovně OpenCV, příkladem je reprezentace obrázků pomocí NumPy polí. Kromě jiného tato knihovna také obsahuje funkce pro lineární algebru, Fourierovu transformaci a práci s náhodnými čísly.

Nvidia CUDA

CUDA je platforma pro paralelní výpočty a programování vyvíjená společností Nvidia. Díky paralelizaci umožňuje lépe využít výkon grafického procesoru. Využití technologie CUDA je rozsáhlé, například při simulaci klimatu, počasí nebo oceánu, strojovém učení, zpracování obrazu v medicíně nebo v superpočítačích [17]. Součástí této platformy je také soubor knihoven cuDNN pro hluboké neuronové sítě. V tomto projektu je CUDA využita pro akceleraci rychlosti rozpoznání tváře.

Dlib

Dlib je soubor moderních nástrojů pro strojové učení a zpracování obrazu. Tato *open source* knihovna je napsána v jazyce C++ a kromě množství algoritmů pro strojové učení, má velmi kvalitní dokumentaci s ukázkovými programy. Na knihovně Dlib je postaven balíček `face-recognition` pro jazyk Python, který tato práce používá. Z knihovny Dlib jsou v implementaci identifikace použity modely detekce a rozpoznávání tváře. Jako detektor je v základním nastavení používán CNN model, který je výpočetně náročnější, ale přesnější než starší HOG model. Pro porovnání a experimenty lze mezi používanými modely detekce přepínat. K rozpoznávání tváří je z knihovny Dlib použit ResNet model s 29 konvolučními vrstvami [21]. Jedná se v podstatě o upravenou síť ResNet-34 ze článku *Deep Residual Learning for Image Recognition* [16].

Face Recognition

Face Recognition je balíček pro jazyk Python, který je zaměřen na rozpoznávání obličeje, autorem je Adam Geigey. Postaven je na knihovně Dlib, uvedené v sekci výše. Proto jeho algoritmy a modely pro detekci a rozpoznání tváře jsou modely knihovny Dlib, obaleny o pomocné funkce. Balíček obsahuje funkce pro detekci obličeje, hledání a manipulaci s významnými body obličeje (nos, ústa, oči) a rozpoznávání tváří. Lze jej používat samostatně jako nástroj pro příkazovou řádku nebo jako modul pro jazyk Python.

5.2 Použité metody a funkce pro algoritmus biometrické brány

V implementaci programu pro identifikaci osob pomocí biometrické brány je využíváno několika knihoven a jejich metod. Tato část obsahuje stručný popis použitých metod a funkcí. V poznámce pod čarou jsou odkazy na dostupné dokumentace těchto knihoven, kde lze nalézt doplňující informace. Z knihovny OpenCV[1] jsou používány následující metody:

- `imread` - Načte obrázek ze souboru a vrátí jej jako NumPy pole. Pokud nelze obrázek načíst vrátí prázdnou matici. Volitelným parametrem `flags` lze nastavit režim čtení, ve výchozím nastavení vrací hodnoty barev v pořadí BGR. Při načítání snímků duhovky je použit režim `IMREAD_GRAYSCALE`.
- `cvtColor` - Převod obrázku z jednoho barevného prostoru do druhého. Používány převody `BGR2RGB` a `BGR2GRAY` (z prostoru BGR do odstínů šedi).
- `imshow` - Zobrazí obrázek v pojmenovaném okně. Obrázek je zobrazen v plné velikosti, při použití parametru `WINDOW_AUTOSIZE`, jinak je jeho velikost upravena podle okna.
- `resize` - Zmenší nebo zvětší obrázek podle zadaných parametrů. Lze volit mezi několika druhy interpolace: při zmenšování je vhodná `INTER_AREA`, naopak při zvětšení je lepší `INTER_CUBIC` nebo `INTER_LINEAR` (rychlejší, ale hůře vypadá).
- `waitKey` - Sleduje stisknuté klávesy a vrací jejich kód. Funguje pouze v přítomnosti alespoň jednoho okna vytvořeného funkcí `imshow`.
- `VideoCapture` - Třída pro načítání snímků z videozáznamu nebo snímání kamerami. Vstupem je číslo kamery a volitelně lze nastavit preferované API (*Application Programming Interface*) pro snímání. Metoda `read` vrací následující dekódovaný snímek.

Z balíčku `face-recognition`[2], který obsahuje modely z knihovny Dlib, jsou používány tyto metody:

- `face_locations` - Detekuje obličeje ve snímku a pro daný obrázek vrací pole se souřadnicemi obdélníků ohraničujících (*bounding box*) lidské tváře. Lze volit mezi HOG a CNN detektory (viz. sekce 2.3.1). CNN je přesnější a lze jej akcelerovat pomocí grafické karty.
- `face_encodings` - Pro daný obrázek vrací pro každý obličej 128 byte *embedding*, vypočítaný z extrahovaných příznaků obličeje (viz. 2.3.2). Tento *embedding* je biometrickou šablonou dané tváře.

Balíček `sklearn`[3] poskytuje metody pro strojové učení, používán je modul `neighbors` a jeho třída `KNeighborsClassifier` pro klasifikaci algoritmem k-NN (nejbližších sousedů) s metodami:

- `KNeighborsClassifier` - Klasifikátor implementující algoritmus k-NN. Parametry lze zvolit (kromě jiných) počet sousedů, rozdělení vah a typ algoritmu (v implementovaném programu je používán `ball_tree`).
- `fit` - Vytvoří klasifikační model podle množiny trénovacích dat X a cílových hodnot y.

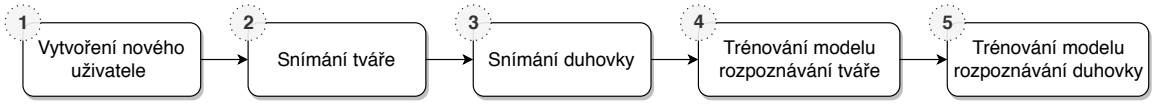
[1] https://docs.opencv.org/4.1.0/
[2] https://face-recognition.readthedocs.io/en/latest/face_recognition.html
[3] https://scikit-learn.org/stable/modules/classes.html#module-sklearn.neighbors

- `predict` - Klasifikuje vstupní hodnotu a vrací odhad nejbližšího souseda (třídu do které by měla hodnota patřit).

Při identifikaci duhovky není použita knihovna, ale jsou převzaty metody implementující Daugmanův algoritmus v jazyce Python. Autorem balíčku `iris-recognition`[4] je Thuy Ng, použity jsou zejména metody:

- `extractFeature` - Pro vstupní snímek duhovky extrahuje její příznaky a převede pomocí Daugmanova algoritmu do binární reprezentace. Vrací šablonu a masku dané šablony.
- `calHammingDist` - Pro dvojici šablon a jejich masek vypočítá Hammingovu vzdálenost. Výstupem je vzdálenost mezi biometrickými šablonami duhovky.

5.3 Snímání osob biometrickou bránou



Obrázek 5.1: Schéma algoritmu snímání při registraci nového uživatele.

Na obrázku 5.1 je postup registrace nového uživatele do systému biometrické brány. Implementován je ve funkci `enroll`. Program v tomto režimu se spouští příkazem `python gate.py -e JMENO`. Vstupem funkce je jméno nového uživatele a cesta k databázi biometrických šablon. Nejprve je ověřeno, zda je uživatelské jméno volné. Pak jsou vytvořeny složky pro uložení snímků obličeje a duhovky.

Ve druhé části je prováděno snímání obličeje ze tří různých úhlů, třemi kamerami současně. K tomu slouží funkce `capture3`, která inicializuje a spustí snímání kamerami funkcí `WebcamVideoStream`. Pokud je zapnutý parametr `capVideo`, pak je zároveň inicializováno natáčení a ukládání videozáznamu, pomocí třídy `VideoWriter`. V průběhu snímání jsou na obrazovce zobrazeny výstupy všech kamer (funkce `imshow`) a stiskem klávesy „C“ jsou uloženy (funkce `imwrite` automaticky pojmenované snímky z každé kamery do databáze. Stiskem klávesy „Q“ je snímání obličeje ukončeno.

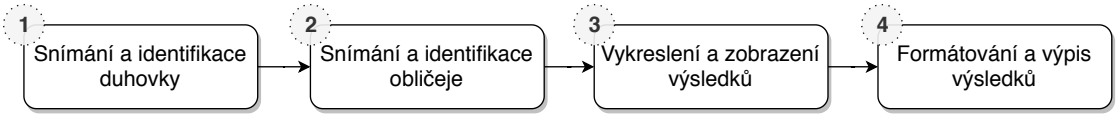
Dalším krokem je snímání duhovky obou očí, pomocí funkce `captureIris`. Tato funkce pracuje obdobně jako `capture3`. Funkcí `WebcamVideoStream` jsou inicializovány snímače duhovky. Klávesou „C“ je ovládáno snímání a ukládání obrázků. Klávesou „Q“ je proces snímání duhovky ukončen.

Ve čtvrtém a pátém kroku volitelně probíhá trénování modelu rozpoznávání tváře a modelu rozpoznávání duhovky. Funkce `trainKNN` provádí trénování k-NN klasifikačního modelu pro rozpoznávání obličeje. Vstupem je cesta k databázi uživatelů a cesta pro uložení modelu. Parametry lze volit počet sousedů (výchozím nastavením je automatická volba) a datovou strukturu pro k-NN (výchozí je *ball tree*). Funkce prochází všechny snímky tváře v databázi a na každém provede následující sekvenci úkonů: načte snímek, převede do barevného prostoru RGB, snímky s větším rozlišením zmenší (rychlejší zpracování). Dále detekuje ve snímku tváře (funkce `face_locations`), pokud na snímku není nalezen obličej nebo jich je nalezeno více, je snímek přeskočen. Pokud je nalezena tvář, jsou extrahovány

[4] https://github.com/AntiAegis/Iris-Recognition

její příznaky funkcí `face_encodings` a uloženy do pole `X`, zároveň je do pole `y` uložena třída odpovídající danému snímku. Každá osoba má celkem tři třídy pro svůj obličej, které odpovídají úhlu pohledu z levé, přední a pravé kamery. Po zpracování všech snímků je inicializován `KNeighborsClassifier` a metodou `fit(X,y)` je vytvořen model klasifikace obličejů, který je uložen do databáze.

Trénování modelu pro klasifikaci duhovky probíhá obdobně, ale bez využití k-NN klasifikátoru. Začíná procházením všech snímků duhovky v databázi. Z každého snímku je funkcí `extractFeature` vypočítána šablona a maska dané duhovky, které jsou uloženy společně s odpovídajícím jménem třídy. Každý uživatel má dvě třídy šablon duhovky, pro každé oko jednu. Po zpracování všech snímků je výsledná datová struktura uložena do databáze.



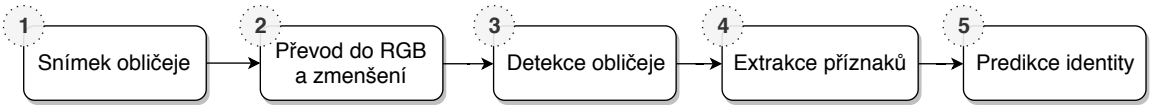
Obrázek 5.2: Schéma algoritmu identifikace.

Na obrázku 5.2 je algoritmus identifikace osoby, který je implementován ve funkci `identify`. Nejprve je získán snímek duhovky a je provedena jeho identifikace, pomocí funkce `captureIrisIdentify`. Vstupem jsou čísla kamer snímacích duhovku a natrénovaný model rozpoznávání duhovky. Tato funkce nejprve inicializuje kamery pomocí `WebcamVideoStream` a poté na obrazovce zobrazí jejich záběry. Stisknutím klávesy „C“ jsou pořízeny snímky duhovky a jsou poslány do funkce `identifyIris`, která z nich extrahuje příznaky Daugmanovým algoritmem a hledá v databázi biometrických šablon nejbližší šablonu duhovky. Výsledek je předán zpět do funkce `identify`.

Dalším krokem je snímání a identifikace obličeje ze snímků ze tří kamer zároveň. Toto provádí funkce `faceRecStream3`. Identifikaci lze provádět i v případě připojení pouze jedné kamery, pak je spuštěna funkce `faceRecStream` a identifikace duhovky je přeskočena. Při identifikaci podle snímků ze tří kamer jsou nejprve opět kamery inicializovány a v cyklu běží algoritmus rozpoznávání obličeje ve funkci `processFrameKNN`, dokud není ukončen stiskem klávesy „Q“. Mezi zobrazovaným výstupem jednotlivých kamer lze přepínat stiskem klávesy „A“ pro levou, „S“ pro přední a „D“ pro pravou kameru.

Vykreslení výsledků je spouštěno ve funkci `processFrameKNN` a prováděno je ve funkci `drawUI`. Která podle nastavených parametrů, jako je barva, font, velikost vykresluje informace na snímek, který je poté zobrazen. Vykreslen je *bounding box*, jméno rozpoznané osoby, procento podobnosti se šablonou, výsledek identifikace duhovky a aktuální výsledky z ostatních kamer. Lze zapnout počítání a zobrazování aktuálních FPS (*Frames per Second*, počet snímků za sekundu). Po ukončení identifikace jsou finální výsledky vypsány na standardní výstup.

5.3.1 Rozpoznání osoby podle obličeje



Obrázek 5.3: Schéma algoritmu rozpoznávání tváře.

Na obrázku 5.3 je schéma algoritmu rozpoznávání tváře. Tento algoritmus je implementován ve funkci `processFrameKNN`, která vezme vstupní snímek obličeje a provede na něm všechny kroky rozpoznávání, vrací zpět výsledky predikce identity a snímek s vykreslenými výsledky rozpoznání. Tato funkce obaluje funkce `predictKNN` a `drawUI`. V první z nich je prováděn odhad identity na snímku tváře. Nejprve je snímek převeden do barevného prostoru RGB z BGR a zmenšen podle nastavení aplikace, pro rychlejší zpracování. Nastavení zmenšení či zvětšení je vhodné upravit podle velikosti snímku, výchozí je zmenšení na 0,35násobek původní velikosti (parametr `frameScale`). Dále je pro zvýšení rychlosti zpracováván každý druhý snímek, v nastavení lze parametrem `processAll` zapnout možnost zpracování všech snímků.

Dalším krokem je detekce obličeje ve snímku. K tomu slouží funkce `face_locations`, u které lze parametrem `faceDetector` vybrat použitý algoritmus detekce. Na výběr je HOG (viz. 2.3.1) a CNN detektor. Oba jsou implementovány v knihovně Dlib, jedná se vždy o detektor MMOD (*Max Margin Object Detector*), který extrahuje příznaky pomocí HOG nebo konvoluční neuronové sítě [22]. HOG je méně náročný, ale méně přesný. CNN je přesnější a náročnější, ale v případě použití akcelerace pomocí technologie CUDA, může být i rychlejší než HOG (záleží na grafickém procesoru). Při experimentech prováděných na grafickém procesoru Nvidia GTX 1050Ti a procesoru Intel i7-7700HQ 2,8GHz, byla rychlost CNN detektoru cca 16 FPS (HOG pracoval rychlostí přibližně 11 FPS, velikost snímku 1280×720 pixelů, `frameScale` 0,35, zpracovávání všech snímků).

Pro extrakci příznaků je použita funkce `face_encodings`, která pro známé lokace tváří ve snímku vrací jejich ohodnocení v podobě 128 byte vektoru, tzv. *embedding*. Tato funkce používá model z knihovny Dlib, jedná se o ResNet síť s 29 konvolučními vrstvami. Postavenou podle článku *Deep Residual Learning for Image Recognition* [16]. Před výpočtem ohodnocení tváře je upraveno její natočení, pomocí detekce významných bodů tváře (viz. 2.3.2).

V posledním kroku je získaný *embedding* porovnán pomocí k-NN klasifikace a je odhadnuta jeho třída, neboli identita osoby, které patří. K tomu slouží funkce `kneighbors`, která vrací vzdálenosti k daným datům. A funkce `predict_proba`, která vrací pravděpodobnosti jednotlivých predikcí. Samotná predikce je vracena metodou `predict`, která vrátí jméno rozpoznané osoby. Pokud je nalezená vzdálenost mezi šablonami větší než zadaný práh `faceDistanceThreshold` (výchozí je 0,58), pak nebyla osoba rozpoznána.

Získané výsledky lze vykreslit na obrazovku pomocí funkce `drawUI`. Ta používá funkci `calcPercentDist` pro přepočet vzdálenosti mezi šablonami na procentuální podobnost. Její výpočet není lineární a je třeba přepočet měnit podle vztahu velikosti prahu a vzdálenosti. Samotná knihovna `face-recognition` nemá procentuální podobnost mezi tvářemi implementovánu. Pokud je vzdálenost větší než práh, je vrácena lineární hodnota L_p [12]:

$$L_p = \frac{1 - vzdalenost}{2(1 - prah)} \tag{5.1}$$

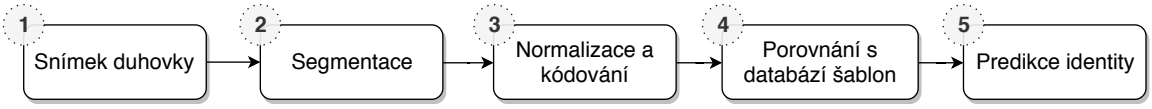
V opačném případě (vzdálenost menší než práh, osoba rozpoznána), je podobnost vypočítána [12]:

$$L_p = a + (1 - a) \cdot (2a - 1)^{\frac{1}{5}}, \qquad a = 1 - \frac{vzdalenost}{2 \cdot prah} \tag{5.2}$$

Na obrázku 5.4 je výsledek rozpoznání tváře, vykreslení výsledků a přepočítané vzdálenosti na procentuální podobnost.

Obrázek 5.4: Ukázka vstupu a výstupu identifikace obličeje. Pro trénování modelu byly použity 3 snímky. Hodnota prahu *faceDistanceThreshold* byla 0,58.

5.3.2 Rozpoznání osoby podle duhovky



Obrázek 5.5: Schéma algoritmu rozpoznávání duhovky.

Na obrázku 5.5 je schéma algoritmu rozpoznávání duhovky. Na snímek duhovky je aplikována funkce `extractFeature`. Která implementuje Daugmanův algoritmus (viz. 2.2.2). Nejprve je provedena segmentace metodou `segment`. V první části je nalezena hranice duhovky funkcemi `searchInnerBound` a `searchOuterBound`. Poté jsou nalezeny umístění očních víček funkcemi `findTopEyeLid` a `findBottomEyelid`. Dále je oblast duhovky normalizována funkcí `normalize`, proveden je převod do polárních souřadnic. Posledním krokem je kódování funkcí `encode`, která vrací biometrickou šablonu duhovky v binárním kódu a binární masku duhovky. Konvoluce je prováděna funkcí `gaborconvolve`.

Získaná šablona duhovky je porovnána s databází a podle nastaveného prahu je vrácena nejbližší nalezená šablona, která splňuje podmínku prahu (výchozí hodnota prahu je 0,34). Hammingova vzdálenost mezi šablonami je počítána funkcí `calHammingDist`.

Kapitola 6

Experimenty a analýza výsledků

Pro vyhodnocení úspěšnosti bylo vytvořenou bránou nasnímáno 20 osob, konkrétně jejich obličeje ze tří úhlů a duhovky obou očí. Experimentováno bylo s různým nastavením aplikace, prahu pro duhovku, obličej, a dalších. Základním experimentem u osoby bylo vyhodnocení, zda došlo k identifikační shodě v každém úhlu při identifikaci biometrickou bránou. Stejný experiment byl proveden i pro otestování identifikace duhovky. Následují pokročilejší experimenty, které vyhodnocují počet správných a chybných rozpoznání pro identity známé a neznámé. Pro tyto experimenty byly nasnímané data rozdělena na skupinu 10 známých a 10 neznámých osob, tyto skupiny byly prostřídány a bylo tak dosaženo celkem 240 testů pro experiment ověřující identifikaci osob. Ve kterém bylo použito 6 snímků tváře na osobu. Pro obdobný experiment ověřující úspěšnost identifikace duhovky bylo použito dvou snímků duhovky na osobu a tedy provedeno 80 testů. Posledním experimentem je ověření úspěšnosti kompozice rozpoznávání obličeje a duhovky, kdy je přidáno pravidlo pro požadovaný počet správných predikcí, v tomto experimentu bylo provedeno 80 testů.

6.1 Snímání osob

Pro provedení experimentů ověření úspěšnosti identifikace bylo nasnímáno celkem 20 osob. U každé osoby bylo vytvořeno přibližně 10 snímků obličeje pro každý ze tří úhlů (počet snímků každé osoby se liší, vyhodnocení úspěšnosti bylo provedeno pro jednotné počty snímků). Snímky obličeje jsou v rozlišení 1920×1080 pixelů, pořízené třemi kamerami HBV-1716 současně. S využitím zařízení INJES IR2800D byla u všech osob nasnímána duhovka obou očí. Rozlišení snímků duhovky je 640×480 pixelů. Snímání probíhalo v několika prostředích za různých světelných podmínek. Každé focení snímků probíhalo se stejným nastavením programu i použitých kamer a při stejném nastavení úhlů natočení kamer na konstrukci brány. Postup snímání je následující:

1. Osoba se rovně posadí před biometrickou bránu.
2. Je upravena vertikální poloha brány, aby byl v záběru celý obličej osoby.
3. Snímání snímků obličeje ze tří úhlů ve stejný čas.
4. Osoba změní polohu a dívá se zblízka do zrcátka snímače duhovky.
5. Snímání duhovky obou očí.

Obrázek 6.1: Osoba během snímání obličeje pomocí biometrické brány.

Výsledná databáze obsahuje snímky dvaceti mužů a žen různého věku (přibližně od 18 do 80 let). Pro každý úhel obličeje jedné osoby je v databázi 8 až 15 snímků. Pro každé oko jedné osoby je v databázi 4 až 8 snímků duhovky.

6.2 Identifikace obličeje na základě snímků ze tří úhlů

V této části je popsán průběh a výsledky experimentů s identifikací obličeje. Před prováděním experimentů byla nejprve upravena vytvořená databáze s 20 osobami. A to vyřazením snímků s rozmazanými záběry a rozdělením databáze na trénovací a testovací množiny. Také byly počty snímků každé osoby sjednoceny, aby nevyváženost databáze neovlivnila výsledky experimentů.

Experiment 1: ověření identity uživatele

Pro každou osobu byl ověřen výsledek identifikace. Celkem bylo prověřeno 20 osob, přičemž každá identita je složena ze 3 biometrických šablon. Ty odpovídají jednotlivým úhlům snímání obličeje. Každá osoba byla nasnímána celkem šestkrát ze tří různých úhlů. Výsledná biometrická šablona je tak složena z třech příznakových šablon. Jako testovací snímky byly použity další 2 snímky obličeje z každého úhlu.

Pro 120 testovacích snímků bylo 119 identifikováno správně. Protože byly snímky velmi podobné trénovacím snímkům je procentuální shoda průměrně 98 %. Chybná identifikace daného snímku nenastane ve všech případech, závisí totiž na nastavení parametrů identifikace. Snímek je při jiném nastavení zmenšení (než 0,35krát) identifikován správně. Níže je v tabulce 6.1 zobrazen přehled výsledků tohoto experimentu.

	Min.	**Max.**	**Průměr**
Vzdálenost	0,059	0,472	0,188
Shoda [%]	89,6	99,2	98,6

Tabulka 6.1: Výsledky základního experimentu ověření identifikace tváře. Pro celkem 120 testovacích snímků bylo 119 identifikováno správně.

Experiment 2: ověření úspěšnosti identifikace tváře

Databáze nasnímaných osob je pro tento experiment rozdělena na dvě části: na 10 osobách je natrénována identifikace, na zbylých 10 je pouze testována. Experiment probíhal ve dvou kolech, kdy se ve druhé části vymění množiny trénovacích a testovacích identit. Celkem bylo provedeno 240 ověření identity, přičemž u 120 je správným výsledkem nalezení odpovídající identity a u 120 potvrzení, že osoba není známa.

Výsledky experimentu jsou v tabulce 6.2, kde jsou po sloupcích počty výsledků: TP (*True Positive*): Správné rozpoznání známé identity. FN (*False Negative*): Chybné rozpoznání známé identity. FP: Chybné rozpoznání neznámé identity. TN: Správné rozpoznání neznámé identity. Použito bylo nastavení programu: *faceDistanceThreshold* = 0,57 (práh maximální vzdálenosti tváře), *faceDetector* = CNN, *frameScale* = 0,35 (0,35x zmenšení vstupního snímku).

		Skutečná identita	
		True (známá)	False (neznámá)
Predikce	*Positive*	118	12
	Negative	2	108

Tabulka 6.2: Výsledky druhého experimentu identifikace tváře. Celkem bylo provedeno 240 testů, z toho 120 byly známé identity a 120 testy neznámé identity.

V tabulce 6.3 jsou hodnoty FPR (*False Positive Rate*), TPR (*True Positive Rate*) a ACC (přesnost identifikace) pro různé hodnoty prahu určujícího rozpoznání tváře (*faceDistanceThreshold*).

Práh	**0,62**	**0,61**	**0,60**	**0,59**	**0,58**	**0,57**
FPR	0,56	0,43	0,36	0,29	0,20	0,10
TPR	0,98	0,98	0,98	0,98	0,98	0,98
ACC	0,71	0,78	0,81	0,85	0,89	0,94

Tabulka 6.3: Výsledky FPR (*False Positive Rate*), TPR (*True Positive Rate*) a ACC (přesnost identifikace) pro druhý experiment s různými hodnotami prahu *faceDistanceThreshold*, který určuje, zda byla nalezena shoda identit.

Výsledky tohoto experimentu ukazují poměrně dobré hodnoty FPR a přesnosti identifikace tváře ze tří úhlů. Ze dvou výskytů *False Negative* byla jedna identita rozpoznána správně, ale byl rozpoznán špatný úhel tváře. Autor knihovny, pomocí které je implementováno rozpoznávání tváře, doporučuje jako práh hodnotu 0,6. Experimenty ukázaly, že při použití navržené biometrické brány a malých rozdílů mezi trénovacími snímky a testovacími, je vhodné použít jako hodnotu prahu 0,57. Malé rozdíly (nízká vzdálenost) jsou způsobeny také podobnými podmínkami při snímání a identifikaci, díky kterým je výhodnější použít nižšího prahu rozpoznávání.

6.3 Identifikace osoby podle duhovky

V této části je popsán průběh a výsledky experimentů s identifikací duhovky. Pro každou ze 20 snímaných osob byly pro trénování použity 3 snímky duhovky každého oka. A jeden snímek každého oka pro testování. Celkem tedy 8 snímků duhovky na osobu.

Experiment 1: ověření identity uživatele

Pro každou osobu byl ověřen výsledek identifikace duhovky. Celkem bylo prověřeno 20 osob, přičemž každá identita je složena ze 2 identit. Ty odpovídají pravému a levému oku.Každá identita byla trénována na 3 snímcích duhovky každého oka. Pro testování byl použit jeden snímek duhovky každého oka. Z celkem 40 testovacích snímků bylo 23 správně identifikováno, což odpovídá přesnosti 58%. Experiment byl proveden při nastavení: *irisDistanceThreshold* = 0,38 a identifikace výběrem nejbližší šablony z databáze k danému snímku. Vysoký počet *false negative* (chybných rozpoznání známé identity) je pravděpodobně způsoben nízkými detaily v pořízených snímcích duhovky. Jelikož bylo v tomto experimentu úspěšně rozpoznáno jedno oko u většiny osob, lze velmi dobrých výsledků dosáhnout změnou podmínky správné identifikace. Pokud je za správnou identifikaci považováno: správná identifikace alespoň jednoho oka u dané osoby. Pak je správně rozpoznáno 18 ze 20 osob, což odpovídá přesnosti 90%.

Experiment 2: ověření úspěšnosti identifikace duhovky

Pro tento experiment je databáze rozdělena na dvě části: na 10 osobách je natrénována identifikace, na zbylých 10 je pouze testována. Experiment probíhal ve dvou kolech, kdy se ve druhé části vymění množiny trénovacích a testovacích identit. Celkem bylo provedeno 80 ověření identity, přičemž u 40 je správným výsledkem nalezení odpovídající identity a u 40 potvrzení, že duhovka není známa.

Výsledky experimentu jsou v tabulce 6.4. Použito bylo nastavení programu: *irisDistanceThreshold* = 0,33 (práh maximální Hammingovy vzdálenosti mezi kódy duhovek) a výběr nejbližší šablony jako výsledku identifikace.

		Skutečná identita	
		True (známá)	False (neznámá)
Predikce	*Positive*	23	7
	Negative	17	33

Tabulka 6.4: Výsledky druhého experimentu identifikace duhovky.Celkem bylo provedeno 80 testů, z toho 40 byly známé identity a 40 testy neznámé identity. Hodnoty v tabulce odpovídají TPR = 0,58, FPR = 0,18, ACC = 70 %.

V tabulce 6.5 jsou hodnoty FPR (*False Positive Rate*), TPR (*True Positive Rate*) a ACC (přesnost identifikace) pro různé hodnoty prahu určujícího rozpoznání duhovky (*irisDistanceThreshold*).

Práh	**0,32**	**0,33**	**0,34**	**0,35**	**0,36**	**0,37**
FPR	0,08	0,18	0,20	0,28	0,35	0,43
TPR	0,48	0,58	0,58	0,58	0,58	0,58
ACC	0,70	0,70	0,69	0,65	0,61	0,58

Tabulka 6.5: Hodnoty pro druhý experiment s rozpoznáním duhovky s různými hodnotami prahu maximální Hammingovy vzdálenosti.

Nižší přesnost rozpoznávání je pravděpodobně způsobena snímky duhovky, které nejsou dostatečně detailní. Z výsledků experimentů vyšla nejlépe hodnota prahu 0.33.

6.4 Identifikace podle obličeje a duhovky

Tento experiment spočívá v přidání pravidel identifikace a ověření celkového výsledku při použití kombinace pěti různých zdrojů biometrických charakteristik. Jelikož je použita kombinace biometrických charakteristik obličeje a duhovky, jedná se o experimenty s multimodálním systémem. Počítáno je s výsledky druhých experimentů s identifikací tváře a duhovky při základním nastavení parametrů programu. Pro nastavení větší priority výsledků rozpoznání tváře před výsledky rozpoznání duhovky, stačí pouze sčítat správně predikovaná jména osob, jelikož je výsledků tváře více. V tomto experimentu je za správnou predikci označena taková, při které byly správně identifikovány alespoň 4 z 5 biometrických charakteristik. Bylo použito následující nastavení: *faceDistanceThreshold* 0,57, detektor CNN, *frameScale* 0,35, rozlišení snímků tváře 1920 × 1080 pixelů a duhovky 640 × 480 pixelů, *irisDistanceThreshold* 0,33 a výběr nejbližší šablony. Pro toto nastavení a požadavku shodných 4 z 5 výsledků byly osoby správně identifikovány v celkem 69 z 80 testů. Což odpovídá přesnosti 86,25 %. Testy byly provedeny pro nasnímaných 20 osob, přičemž v polovině testů se zkoumala schopnost správně označit osobu za neznámou a ve druhé schopnost rozeznání správné identity.

Kapitola 7

Závěr

K dosažení cíle práce byly nastudovány potřebné detaily o biometrických systémech a jejich vlastnostech. Klíčové bylo zjištění vlastností jednotlivých biometrických charakteristik a způsobů hodnocení výkonnosti biometrických systémů. Větší pozornost byla věnována rozpoznávání podle duhovky a podle obličeje, jelikož se jedná o biometrické vlastnosti, které mají v rámci této práce být řešené. Proto první část práce popisuje anatomii lidského oka a algoritmy, které se používají pro extrakci biometrických příznaků ze snímku duhovky, zejména byl popsán Daugmanův algoritmus. Jelikož řešená biometrická brána snímá i obličej osoby, byly v další teoretické části popsány základy rozpoznávání obličeje a vybrané používané algoritmy. Kapitola je uzavřena hodnocením biometrických systémů a popisem chyb vznikajících při porovnání biometrických dat.

Ve třetí kapitole zabývající se biometrickými bránami, byl popsán jejich vývoj, architektura, hodnocení výkonu a byly vybrány dvě vlastnosti podstatné pro biometrické brány. Dále byly popsány zjištěné problémy existujících systémů a několik biometrických bran v používaných v současnosti. Návrh biometrické brány a řídících algoritmů byl popsán ve čtvrté kapitole. Kde byla na základě třetího bodu zadání navrhnuta konstrukce biometrické brány, která se skládá ze tří kamer snímajících obličej a snímače duhovky lidského oka. Kamery byly rozmístěny tak, aby jedna z nich frontálně snímala obličej a zbylé dvě snímaly obličej z levé a pravé strany.

Brána byla zkonstruována pomocí stavebnice Merkur a dílu vytištěných na 3D tiskárně. K jejímu řízení byl implementován software v jazyce Python pro operační systém MS Windows. Data jsou získávány současně ze všech kamer snímajících obličej, kamery snímající duhovku jsou odděleny a identifikace tak probíhá nejprve pro duhovku a následně pro obličej. Důvodem je nižší náročnost programu a nižší požadovaný počet USB konektorů. Nebyla tak využita vysokorychlostní kamera, jelikož použitá je dostačující a větší počet snímků za vteřinu by byl nebyl využit, výhodou je také nižší cena. Bránu tak lze provozovat i na běžném přenosném počítači, který má USB konektorů méně. Implementace řídící aplikace je popsána v páté kapitole.

Pro zhodnocení práce byly provedeny experimenty ověřující úspěšnost identifikace osob s využitím zkonstruované biometrické brány. Pro ověření úspěšnosti bylo nasnímáno celkem dvacet osob, pro každou až 15 snímků obličeje ze tří různých úhlů a až 8 snímků duhovky. Na základě těchto dat, která byla rozdělena na trénovací a testovací snímky bylo provedeno celkem 240 testů pro ověření identifikace tváře. Kde bylo dosaženo přesnosti až 94 %. A celkem 80 testů identifikace duhovky, kde byla naměřena přesnost až 70 %. Tomu odpovídají i výsledky experimentu s kombinací obou charakteristik, kdy byla zjištěna přesnost 86 %. Výsledky experimentů ukazují, že implementovaný algoritmus rozpoznávání tváře ze tří úhlů je

poměrně robustní a při vhodném nastavení podává dobré výsledky. K tomu pomáhá kromě využití více úhlů záběru i podobnost podmínek při kterých jsou osoby registrovány a rozpoznávány bránou. Výsledky identifikace duhovky nejsou v porovnání s výsledky rozpoznání tváře vysoké, důvodem může být horší kvalita snímků duhovky, během snímání osob pro experimenty bylo obtížné pořídit velmi kvalitní snímky duhovky. Avšak pokud je uvažována nižší kvalita snímků duhovky, pak lze výsledky považovat za uspokojivé. Experimenty s multimodálním systémem ukázaly, že celková přesnost je závislá na přesnosti jednotlivých komponent.

Literatura

[1] Best, J.: £9m cost of eye scanning 'would have been better spent on immigration staff'. Online, 2012, [cit. 06.01.2019].
URL https://www.theguardian.com/government-computing-network/2012/apr/11/iris-ukba-egates-eborders-report

[2] Cantarero, D. C.; Herrero, D. A. P.; Méndez, F. M.: A Multi-modal Biometric Fusion Implementation for ABC Systems. In *2013 European Intelligence and Security Informatics Conference*, Aug 2013, s. 277–280, doi:10.1109/EISIC.2013.71.

[3] CBSA: NEXUS. Online, 2019, [cit. 07.01.2019].
URL http://www.cbsa-asfc.gc.ca/prog/nexus/menu-eng.html

[4] Dalal, N.; Triggs, B.: Histograms of oriented gradients for human detection. In *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, ročník 1, IEEE, 2005, s. 886–893.

[5] Daugman, J.: Recognising persons by their iris patterns. In *Advances in biometric person authentication*, Springer, 2004, s. 5–25.

[6] Daugman, J.: How iris recognition works. In *The essential guide to image processing*, Elsevier, 2009, s. 715–739.

[7] Davies, E. R.: *Computer vision*. Cambridge, CA: Elsevier, páté vydání, 2018, ISBN 978-0-12-809284-2.

[8] Drahanský, M.; Orság, F.: *Biometrie*. [Brno: M. Drahanský], první vydání, 2011, ISBN 978-80-254-8979-6.

[9] Frontex: BIOPASS Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports. *Research Gate*, 2007.

[10] Frontex: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems. Online, 2012, [cit. 06.01.2019].
URL https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf

[11] Geitgey, A.: Machine Learning is Fun! Part 4. Online, 2016, [cit. 21. 5. 2019].
URL https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78

[12] Geitgey, A.: Calculating Accuracy as a Percentage. Online, 2019, [cit. 21. 5. 2019].
URL https://github.com/ageitgey/face_recognition/wiki/Calculating-Accuracy-as-a-Percentage

[13] Gorodnichy, D.; Yanushkevich, S.; Shmerko, V.: Automated border control: Problem formalization. In *2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)*, Dec 2014, ISSN 2325-4300, s. 118–125, doi:10.1109/CIBIM.2014.7015452.

[14] Grother, P. J.; Quinn, G. W.; Matey, J. R.; aj.: IREX III-Performance of iris identification algorithms. Technická zpráva, No. NIST Interagency/Internal Report (NISTIR)-7836., 2012.

[15] Group, I. B.: Independent testing of iris recognition technology: Final report. Online, 2005, [cit. 27.11.2018].
URL https://www.hsdl.org/?abstract&did=464567

[16] He, K.; Zhang, X.; Ren, S.; aj.: Deep Residual Learning for Image Recognition. *CoRR*, ročník abs/1512.03385, 2015, [cit. 19. 5. 2019], 1512.03385.
URL http://arxiv.org/abs/1512.03385

[17] Heller, M.: What is CUDA? Parallel programming for GPUs. Online, 2018, [cit. 20.05.2019].
URL https://www.infoworld.com/article/3299703/what-is-cuda-parallel-programming-for-gpus.html

[18] Jain, A.; Bolle, R. M.; Pankanti, S.: *Biometrics*. US: Springer, první vydání, 2006, ISBN 978-0-387-28539-9.

[19] Jain, A. K.; Flynn, P.; Ross, A. A.: *Handbook of biometrics*. New York: Springer, první vydání, 2008, ISBN 978-0-387-71040-2.

[20] Kazemi, V.; Sullivan, J.: One millisecond face alignment with an ensemble of regression trees. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, s. 1867–1874.

[21] King, D. E.: Dlib-ml: A Machine Learning Toolkit. *Journal of Machine Learning Research*, ročník 10, 2009: s. 1755–1758.

[22] King, D. E.: Max-Margin Object Detection. *CoRR*, ročník abs/1502.00046, 2015, [cit. 17. 5. 2019], 1502.00046.
URL http://arxiv.org/abs/1502.00046

[23] Lim, S.; Lee, K.; Byeon, O.; aj.: Efficient iris recognition through improvement of feature vector and classifier. *ETRI journal*, ročník 23, č. 2, 2001: s. 61–70.

[24] Maltoni, D.; Maio, D.; Jain, A. K.; aj.: *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[25] Mansfield, A.; Wayman, J.: Best practice standards for testing and reporting on biometric device performance. *National Physical Laboratory of UK*, 2002: s. 1–32.

[26] Monrose, F.; Rubin, A.: Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security*, ACM, 1997, s. 48–56.

[27] Negin, M.; Chmielewski, T. A.; Salganicoff, M.; aj.: An iris biometric system for public and personal use. *Computer*, ročník 33, č. 2, 2000: s. 70–75.

[28] Nuppeney, M.: Automated Border Control–state of play and latest developments. In *NIST International Biometric Performance Conference. April*, 2014, s. 1–3.

[29] OpenCV: About OpenCV. Online, 2019, [cit. 7. 5. 2019].
URL https://opencv.org/about/

[30] Palmer, A.; Hurrey, C.: Ten Reasons Why IRIS Needed 20:20 Foresight: Some Lessons for Introducing Biometric Border Control Systems. 08 2012, doi:10.1109/EISIC.2012.31.

[31] Schroff, F.; Kalenichenko, D.; Philbin, J.: FaceNet: A Unified Embedding for Face Recognition and Clustering. *CoRR*, ročník abs/1503.03832, 2015, [cit. 18. 5. 2019], 1503.03832.
URL http://arxiv.org/abs/1503.03832

[32] Solutions, V. I.: EasyGO Self-Service Border Crossing System. Online, 2018, [cit. 26.12.2018].
URL http://www.vitkovice.cz/documents/10181/90066/easyGo/fc06885e-060b-4ce2-9044-1dcf447229d8

[33] Szegedy, C.; Liu, W.; Jia, Y.; aj.: Going Deeper with Convolutions. *CoRR*, ročník abs/1409.4842, 2014, [cit. 15. 5. 2019], 1409.4842.
URL http://arxiv.org/abs/1409.4842

[34] Wang, J.; Amos, B.; Das, A.; aj.: Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework. *ACM Transactions on Multimedia Computing, Communications, and Applications*, ročník 14, 06 2018: s. 1–24, doi:10.1145/3209659.

[35] Wikipedia: Lidské oko. Online, 2019, [cit. 15. 1. 2019].
URL https://cs.wikipedia.org/wiki/Lidsk%C3%A9_oko

[36] Wilson, C.; Hicklin, A.; Bone, M.; aj.: Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. *NIST Technical Report NISTIR*, ročník 7123, 2004.

[37] Yanushkevich, S. N.; Boulanov, O.; Stoica, A.; aj.: Support of interviewing techniques in physical access control systems. In *International Workshop on Computational Forensics*, Springer, 2008, s. 147–158.

[38] Yong Wang; Jiu-Qiang Han: Iris recognition using independent component analysis. In *2005 International Conference on Machine Learning and Cybernetics*, ročník 7, Aug 2005, ISSN 2160-133X, s. 4487–4492 Vol. 7, doi:10.1109/ICMLC.2005.1527729.

[39] Zeiler, M. D.; Fergus, R.: Visualizing and Understanding Convolutional Networks. *CoRR*, ročník abs/1311.2901, 2013, [cit. 22. 5. 2019], 1311.2901.
URL http://arxiv.org/abs/1311.2901

[40] Zhang, D. D.; Kong, W.; You, J.; aj.: Online palmprint identification. *IEEE Transactions on pattern analysis and machine intelligence*, 2003.

Příloha A

Obsah přiloženého paměťového média

src Zdrojové kódy programu a vytvořená databáze snímků.

- **dataset** Vytvořená databáze snímků použitá v experimentech.
- **testset** Podmnožina snímků, které byly použity pro testování.
- **readme** Seznam potřebných knihoven a návod k ovládání aplikace.

report Tento text ve formátu PDF.

- **src** Zdrojové texty v LaTeXu a použité obrázky.

tools Instalační soubory používaných knihoven a nástrojů.