VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

MULTIKAMEROVÁ BIOMETRICKÁ BRÁNA PRO IDENTIFIKACI OSOB

MULTICAMERAS BIOMETRIC GATEWAY TO IDENTIFY PEOPLE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **DOMINIK KOSÍK**
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 bakalářské práce

Student: **Kosík Dominik**
Program: Informační technologie
Název: **Multikamerová biometrická brána pro identifikaci osob**
Multicameras Biometric Gateway to Identify People
Kategorie: Bezpečnost

Zadání:

1. Nastudujte základní informace o biometrických systémech. Sumarizujte informace o biometrických branách.
2. Seznamte se s biometrickými systémy využívající kamery pro identifikaci osob.
3. Navrhněte biometrickou bránu, která se bude skládat z RGB kamer a termokamery. Data z RGB kamer budou sloužit pro vytvoření 3D modelu obličeje, zatímco data z termokamery budou pouze rozšiřovat datovou množinu.
4. Navržené řešení implementujte na vhodné platformě. Pro rekonstrukci 3D modelu obličeje použijte FlowSDK od firmy 3DFlow. Pro extrakci příznaku pro identifikaci můžete použít dostupný software.
5. Proveďte experimenty zaměřené na úspěšnost identifikace osoby.

Literatura:

- T. Horprasert, Y. Yacoob and L. S. Davis, "Computing 3-D head orientation from a monocular image sequence," *Proceedings of the Second International Conference on Automatic Face and Gesture Recognition*, Killington, VT, USA, 1996, pp. 242-247.
- PETROVSKA-DELACRÉTAZ, Dijana; CHOLLET, Gérard; DORIZZI, Bernadette. *Guide to biometric reference systems and performance evaluation*. Berlin: Springer, 2009.

Pro udělení zápočtu za první semestr je požadováno:

- Body 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: 15. května 2019
Datum schválení: 1. listopadu 2018

Abstrakt

Tato práce řeší vytvoření biometrické brány pro identifikaci osob. Identifikace probíhá za pomocí 5 barevných kamer a IR kamery. IR kamera zajišťuje detekci osoby a následně se ze snímku barevných kamer vytváří 3D model obličeje osoby. Na základě tohoto modelu se provádí identifikace. Jelikož při vytváření samotného 3D modelu docházelo k nepřesnostem, což má vliv na rozpoznání osoby, není výsledná identifikace dostatečně přesná. Z toho důvodu je zapotřebí upravit algoritmy zpracovávající 3D model, a tak dosáhnout dostatečné přesnosti.

Abstract

This thesis is about creating biometric gate to identify people. The Identification is achieved with 5 RGB cameras and one thermal camera. Thermal camera is used for detection of person. Then, from images acquired from RGB cameras, is created 3D model of photographed person. This model is then used for the identification. However due to inaccuracies in created model, identification isn't precise enough. Because of that, it's necessary to modify used algorithms processing 3D model, so better precision is achieved.

Klíčová slova

Identifikace, Verifikace, Rozpoznávání, Biometrické systémy, Biometrické brány, 2D obličej, 3D obličej, 3D model, RGB snímky, Snímek z termokamery, 3DFlow, FlowEngine, .obj, Řezy 3D modelu, extrakce příznaků

Keywords

Identification, Verification, Recognition, Biometric systems, Biometric gateways, 2D face, 3D face, 3D model, RGB iamge Thermal image, 3DFlow, FlowEngine, .obj, 3D model slice, Feature extraction

Citace

KOSÍK, Dominik. *Multikamerová biometrická brána pro identifikaci osob.* Brno, 2019. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Tomáš Goldmann

Multikamerová biometrická brána pro identifikaci osob

Prohlášení

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

.....
Dominik Kosík
12. května 2019

Poděkování

Rád bych poděkoval vedoucímu mé práce panu Ing. Tomáši Goldmannovi za pomoc při vytváření návrhu a implementaci biometrické brány.

Obsah

1 Úvod **3**

2 Biometrické přístupové systémy **4**
2.1 Co jsou biometrická data 4
2.2 Biometrické systémy 4
2.2.1 Chyby při rozpoznávání 6
2.2.2 Identifikace osob na základě obrazu 7
2.3 Vestavěné systémy 13
2.3.1 Komunikační rozhraní mezi prvky systému 14
2.4 Digitální fotoaparáty a kamery 16
2.5 Biometrické brány 17

3 Návrh biometrické brány a proces vytváření 3D modelu **18**
3.1 Hardwarová část systému 18
3.2 Návrh softwaru pro biometrickou bránu 18
3.2.1 Vytvoření 3D modelu obličeje 18
3.2.2 Extrakce příznaků z 3D modelu v *.obj* formátu 22
3.2.3 Zpracování dat z IR kamery 24

4 Implementace návrhu biometrické brány **25**
4.1 Implementace pořízení RGB fotografií 25
4.2 Implementace vytváření 3D modelu 25
4.2.1 Vytvoření klíčových bodu a odhad umístění kamer 26
4.2.2 Výpočet okolních bodů k získání hloubky modelu 26
4.2.3 Převedení modelu ze shluku vertexů na polygony 27
4.2.4 Finální úprava povrchu modelu - textura 27
4.2.5 Zpracování souboru s 3D informacemi 27
4.2.6 Extrakce vertexů z *Wavefront object file* 27
4.2.7 Získání bodu určující špičku nosu 28
4.2.8 Získání řezu obličeje procházejícím nosem modelu 28
4.2.9 Úprava návrhu řezů 3D modelem 30
4.3 Využití termokamery v biometrické bráně 31
4.3.1 Pořízení snímku z IR kamery 31
4.3.2 Zpracování získaného snímků 31
4.4 Identifikace osob 32
4.4.1 Získání dat o osobě 32
4.4.2 Zpracování příznaků 32
4.4.3 Možnosti zpřesnění identifikace osob 33

5 Experimenty na systému biometrické brány **35**
5.0.1 Porovnání dvou modelů osob 35
5.0.2 Odchylka modelů stejné osoby 37
5.0.3 Identifikace několika osob 37
5.1 Výsledky testování a experimentů 38
5.1.1 Chyby při rekonstrukci modelu 38
5.1.2 Chyba rozpoznání modelu 39

6 Závěr **40**

Literatura **41**

Kapitola 1

Úvod

Na mnoha místech je nutné před povolením vstupu nebo provedením určitého úkonu ověřit o koho se jedná. Ať už jde o kontrolu na letišti před nástupem do letadla nebo odemčení mobilního telefonu otiskem prstu. Bezpečnostní prvky se tedy stávají velkou součástí běžného života. K ověření této skutečnosti je potřeba určitý mechanismus prokázání, zda se opravdu jedná o danou osobu a né o někoho, kdo se za ní pouze vydává, případně, že se nejedná o hledanou osobu.

V dnešní době plní systémy na rozpoznávání osob důležitou roli v bezpečnosti mnoha veřejných míst. Nicméně žádný z těchto systémů není neomylný, a je tedy neustálá snaha zvyšovat přesnost, rychlost nebo jiné vlastnosti identifikace. Zlepšení těchto aspektů vede k lepšímu přijetí biometrických systémů veřejností a to díky menšímu počtu falešných poplachů a času stráveného čekáním.

V současné době se úspěšnost a rychlost těchto systémů čím dál více zvyšuje společně s pokrokem v ostatních oborech jako například větší rozlišení kamer, vyšší výpočetní výkon procesorů nebo lepší technologie zpracování obrazu. Na základě tohoto rozvoje lze vytvářet komplexnější postupy zpracovávání informací a lze dosáhnout téměř dokonalé identifikace osob, či věcí při standardních podmínkách.

Přínosem této práce by měl být pokrok v oblasti identifikace osob bez nutnosti použití specializovaného anebo drahého vybavení. Tedy zvýšit míru spolehlivosti rozpoznávání osob bez vysokých nákladů.

Samotný cíl projektu je tedy vytvořit biometrickou bránu, která za pomocí několika barevných kamer vytvoří 3D model obličeje společně s jednou termokamerou pro zvýšení přesnosti systému. Tyto informace se následně uloží do databáze, kde budou využity jako referenční model pro identifikaci dané osoby. Takže výsledný systém umožňuje rozpoznat osobu, o kterou se s největší pravděpodobností jedná.

Následující kapitola popisuje funkci biometrických systémů a informace o biometrických branách. Dále obsahuje popis zpracování 2D a 3D obrazu obličeje pro identifikaci osob. V Kapitole 3 je návrh celého systému (hardware i software). Implementace návrhu biometrické brány s jejím popisem je ve 4. kapitole a zhodnocení práce se nachází v poslední kapitole Závěr.

Kapitola 2

Biometrické přístupové systémy

Biometrické systémy a obecně biometrie se zabývá rozpoznáváním osob na základě určitých údajů získaných od rozpoznávané osoby. Tyto systémy jsou důležité z pohledu ochrany přístupu do určitých míst nebo k určitým údajům. Údaje od rozpoznávaných osob, které jsou použité pro identifikaci nebo verifikaci, se nazývají biometrická data.

2.1 Co jsou biometrická data

Jakékoliv měřitelné fyzické vlastnosti nebo způsob chování člověka lze použít jako biometrický údaj pro rozpoznávání, pokud bude splňovat následující vlastnosti:

- Univerzálnost: každý člověk by měl mít tyto údaje.
- Unikátnost: žádné dvě osoby by údaje neměly mít stejné.
- Trvalost: měřené údaje by měly být neměnné v čase.
- Sběratelnost: údaje lze snadno získat.

Nicméně při praktickém využití jsou na tyto údaje kladeny ještě další nároky:

- Výkon: udává přesnost rozpoznávání, které lze dosáhnout; nutné prostředky pro dosažení této přesnosti a faktory, které mohou ovlivnit přesnost rozpoznávaní.
- Přijatelnost: určuje, do jaké míry jsou lidé ochotní poskytovat biometrický údaj.
- Oklamatelnost: jak jednoduše lze systém podvést za pomocí podvodných technik.

[15]

2.2 Biometrické systémy

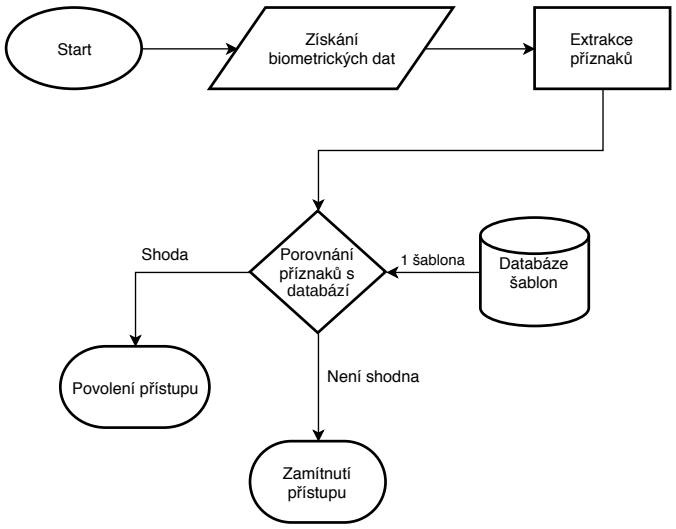
Biometrické systémy jsou v podstatě systémy na rozpoznávání vzorů. Jejich funkce je založena na základě získávání biometrických dat od osob, extrakci příznaků z dat a porovnání vůči množině šablon uložených v databázi systému. S ohledem na účel použití je výsledkem verifikace nebo identifikace. [16]

Verifikace a identifikace

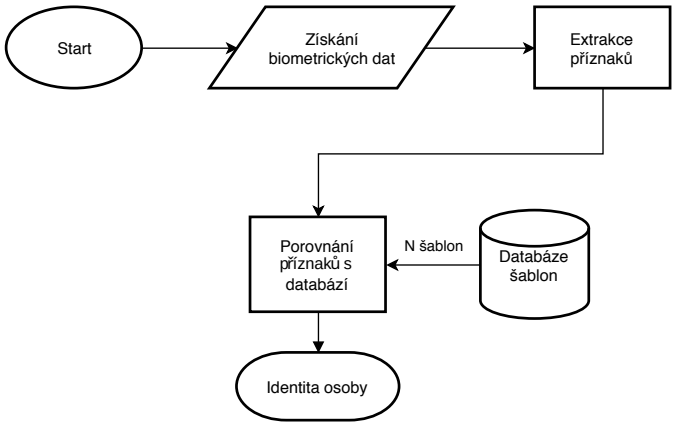
Při vytváření jakéhokoliv systému na rozpoznávání je nutné si nejprve určit samotný cíl tohoto systému. V praxi jsou pojmy verifikace a identifikace často zaměňovány, přestože mají každý svůj specifický význam a případy užití.

Při verifikaci systém za pomocí biometrických dat ověřuje, zda se opravdu jedná o danou osobu. Naměřená data jsou porovnána s uloženými daty v databázi pro danou osobu a určí, zda ověřovaná osoba je opravdu ta, za kterou se vydává. Tyto systémy se používají k zamezení použití stejné identity více lidmi. Vývojový diagram pro postup verifikace lze vidět na obrázku 2.1.

Naproti tomu při identifikaci se systém snaží z naměřených údajů zjistit o koho se jedná. Ze získaných dat se extrahují příznaky a ty se porovnávají vůči všem šablonám v databázi. Na základě těchto prování systém určí o jakou osobu se jedná, pokud byla nalezena shoda. Postup identifikace lze vidět na obrázku 2.2.



Obrázek 2.1: Vývojový diagram biometrického systému pro verifikaci osoby.



Obrázek 2.2: Vývojový diagram biometrického systému pro identifikaci osoby.

Porovnání běžně používaných biometrických charakteristik

V biometrických systémech se využívá velké množství různých biometrických charakteristik. Každá z těchto charakteristik má svoje silné i slabé stránky a výběr závisí na místě uplatnění. Jinak řečeno, žádná biometrika není perfektní. Výběr specifické charakteristiky k určitému uplatnění závisí na způsobu použití a požadovaných vlastnostech biometrické charakteristiky. Níže je porovnání jednotlivých charakteristik. [16]

V této práci se budou využívat pouze biometriky obličeje a snímky obličeje za pomocí termokamery (*Face* a *Facial thermogram* v tabulce níže).

Použití těchto biometrik je výhodné z pohledu snadnosti jejich získání a obecně lidé nemají problém se nechat vyfotografovat za účelem identifikace. Problémy mohou nastat u snímků obličeje, jelikož mnoho lidí má podobný obličej, což znamená nižší rozlišitelnost a je tedy zapotřebí robustnější algoritmus pro rozpoznávání. Další nevýhodou může být jednoduché falšování snímků obličeje, ale při spojení s termokamerou lze tyto případy jednoduše odhalit.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tabulka porovnávající jednotlivé běžně používané biometriky na základě jejich vlastností z pohledu autorů [16]. H, M a L znamená High (hodně), Medium(středně) a Low(málo). Převzato z [16] strana 11.

2.2.1 Chyby při rozpoznávání

Ať už se používá sebelepší systém pro rozpoznávání osob nebo jiných objektů, žádný systém nebude dokonalý. Chyby které mohou nastat jsou falešně pozitivní (anglicky false positive)

nebo falešně negativní (false negative). Například při falešně pozitivní chybě se jedná o to, že přístup byl umožněn neoprávněné osobě. Oproti tomu u falešně negativní chybě byl oprávněné osobě přístup zamítnut.

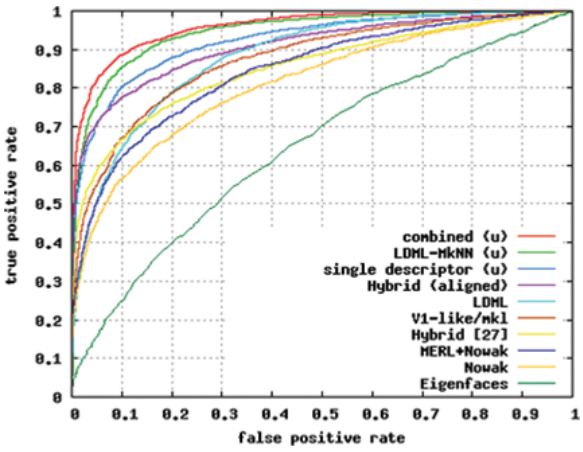
Každé využití biometrických systémů má svoji váhu pro dovolení přístupu neoprávněné osoby a zamítnutí oprávněné osoby. Falešně pozitivní identifikace má daleko větší dopad na společnost pokud se stane při přístupu do jaderné elektrárny, než při napadení osobního bankovního účtu. Na druhou stranu banka může ztrácet klienty, pokud budou chybně nepřipuštěni ke svému kontu na základě falešně negativní chyby. [23]

Křivky ROC a DET

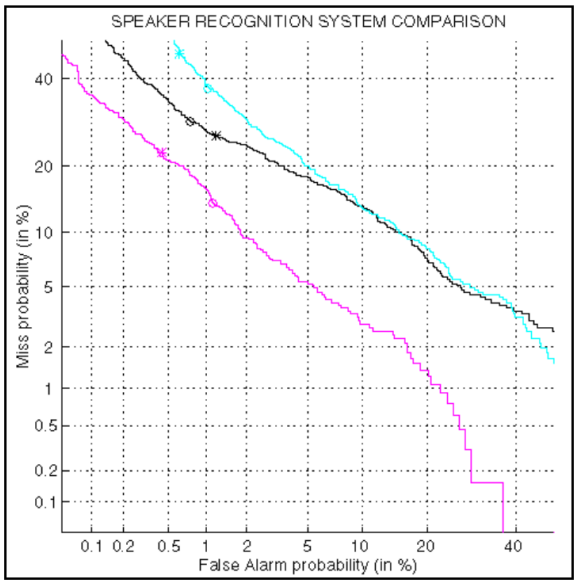
Při vytváření biometrických systémů je nutné mít způsob porovnání jejich úspěšností. Jedním ze způsobů, jak toho dosáhnout, je porovnat systémy pomocí křivky ROC (Receiver Operating Characteristic) nebo křivky DET (Detection Error Tradeoff).

Křivka ROC porovnává systémy podle toho, kdy systém dává pozitivní výsledek. Tedy pravděpodobnost detekce (pravdivě pozitivní) a falešný alarm (falešně pozitivní). Příklad této křivky lze vidět na obrázku 2.3a.

Oproti tomu křivka DET určuje poměr mezi propásnutými detekcemi (falešně negativní) a falešnými alarmy (falešně pozitivní). U DET křivky je na osy vynesena chyba systému ve stejném měřítku pro obě osy. Na základě této křivky lze zvolit systém a poměr chyb v závislosti na oblasti aplikace biometrického systému. [20]
Ukázka DET křivky je na obrázku 2.3b.



(a) Příklad ROC křivky porovnávající různé algoritmy na rozpoznávání obličeje [31].



(b) Příklad DET křivky porovnávající 3 různé systémy pro rozpoznávání mluvčího [20].

Obrázek 2.3: Příklad ROC a DET křivek.

2.2.2 Identifikace osob na základě obrazu

Rozeznávání lidí od sebe na základě obličeje je jedna ze základních schopností člověka, kterou využíváme denně. Tuto schopnost se snažíme zreprodukovat k dosažení vysoké přes-

nosti identifikace lidí za účelem zvýšení míry zabezpečení. Nicméně, ačkoliv se může zdát, že obličeje lidí jsou od sebe dostatečně odlišné, z pohledu počítačového zpracovaní obrazu tomu tak není.

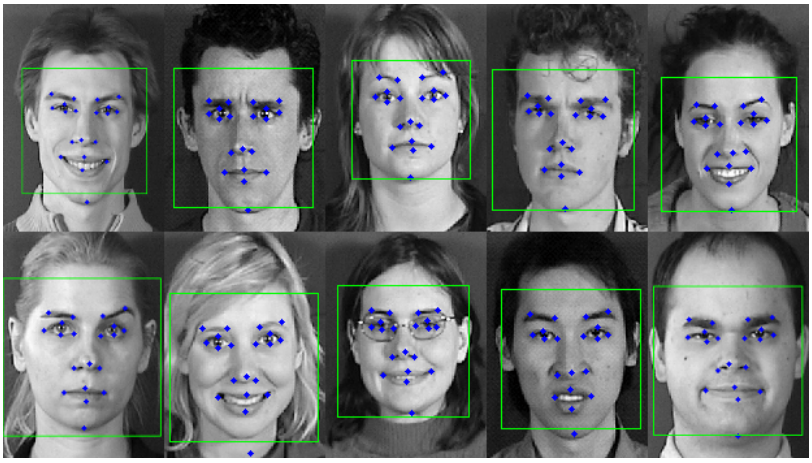
K rozpoznávání obličeje bylo navrženo několik řešení na základě 2D nebo 3D obrazu. Všeobecně jsou technologie na rozeznávání obličeje rozděleny na dva kroky. Prvním krokem je vytvoření unikátních šablon pro osoby, které budeme chtít rozpoznávat. Tyto šablony jsou vytvořeny na základě příznaků získaných z předefinované množiny obrazů obličejů. Druhý krok je samotná identifikace nebo verifikace, kdy z pořízených obrazů jsou získány příznaky k popisu obličeje, které jsou porovnány s uloženými šablonami. [23]

Rozpoznávání osob na základě 2D snímků obličeje

Rozpoznávání osoby z 2D snímku je běžný způsob verifikace na mnoha místech. Pro získání biometriky, jako je lidský obličej, není potřeba použít speciální vybavení ani prostory. Nicméně způsob získání takovýchto informací může mít vliv na přesnost celého systému.

Jelikož rozpoznávání na základě obličeje vyžaduje určité obecné znalosti o lidské tváři, mohou být tyto systémy rozděleny do dvou skupin na základě využití těchto znalostí. Techniky využívané v první skupině jsou založeny na klasické metodologii rozpoznávání, kde se nejdříve extrahují nízkoúrovňové příznaky před jejich analýzou. Vlastnosti obličeje, které se zde používají jsou například barva kůže nebo geometrie tváře. Tento způsob rozpoznávání je nazýván *feature-based* (založen na příznacích). Druhá skupina využívá pokroku v teorii rozpoznávání vzorů a považuje rozpoznávání obličeje jako obecný problém pro rozpoznávání. Tato skupina se označuje jako *image-based* (založen na obrazu) a využívá algoritmy k identifikaci nebo verifikaci z obrazu jako dvou dimenzionálního pole, bez předešlé extrakce příznaků nebo analýzy. [12]

Rozpoznávání založené na příznacích:
Při identifikaci osob na základě příznaků je nejprve nutné stanovit o jaké příznaky se bude konkrétně jednat a zda-li jsou vhodné s ohledem na způsoby pořízení snímků obličeje. Například při rozeznávání na základě barvy bude mít vliv na výslednou přesnost světlo při získání obrazu.



Obrázek 2.4: Zobrazené klíčové body obličeje, na základě kterých se může provádět rozpoznávání [22].

Jedním z používaných způsobů rozpoznávání je na základě geometrie obličeje, tedy vzdálenosti mezi jednotlivými části tváře. Toto uspořádání lze popsat pomocí vektorů popisujících umístění a velikost hlavních částí obličeje: oči, obočí, nos a ústa. Tyto informace mohou být doplněny o celkový tvar obličeje. Použití těchto příznaků zaručuje nízkou závislost na světle a výrazu tváře. Nevýhoda tohoto přístupu spočívá v normalizaci. Pro přesné výsledky musí být zaručena stejná pozice, měřítko a otočení tváře na snímku. [3]

Způsob, kterým lze systém na rozpoznávání naučit příznaky osob, může být využití lineárních klasifikátorů jako například *Perceptron* nebo *Support vector machines*.

Popis perceptronu převzat z prezentace [19].
Perceptron je jednoduchý lineární klasifikátor pro binární rozhodnutí založený na aktivační funkci $f(a)$, kde a je vstup do klasifikátoru:

$$f(a) = \begin{cases} +1, a \geqslant 0 \\ -1, a < 0 \end{cases} \tag{2.1}$$

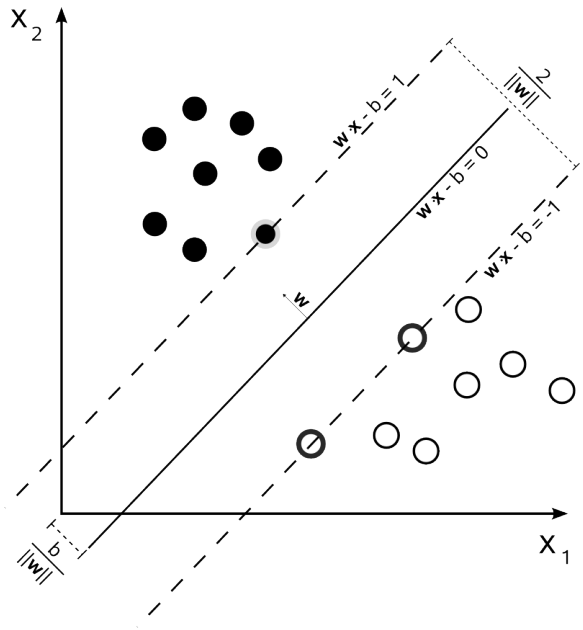
Při předpokladu, že w_0 je nultý koeficient vektoru $\mathbf{w}$ a obsahuje jednotlivé váhy k vektoru vstupních hodnot $\mathbf{x}$, kde x_0 je vždy 1. Lze perceptron vyjádřit jako:

$$y(\mathbf{x}) = f(\mathbf{w}^T\mathbf{x}) \tag{2.2}$$

Při učení se cyklicky procházejí jednotlivé trénovací vzory a při špatně klasifikovaném vzoru se změní vektor $\mathbf{w}$, kde $\mathbf{x}$ je vektor vstupních hodnot a $\mathbf{t}$ je vektor očekávaných hodnot:

$$\mathbf{w}^{\tau+1} = \mathbf{w}^{\tau} + \mathbf{x}_n\mathbf{t}_n \tag{2.3}$$

Support vector machines (SVM) je algoritmus na strojové učení s učitelem. SVM zobrazí všechny body do n-dimenzionálního prostoru (n je počet příznaků), kde souřadnice v prostoru odpovídají hodnotě příznaků. Poté SVM vytvoří nadrovinu, která rozděluje jednotlivé třídy na základě podpůrných vektorů. Podpůrné vektory jsou body, co leží na okraji hraniční oblasti kolem nadroviny. Učení SVM spočívá v hledání této nadroviny, kde vzdálenost od podpůrných vektorů je co největší. Tento způsob dokáže klasifikovat jednotlivé třídy pouze pokud jsou lineárně odlišitelné. Nicméně SVM lze mapovat do nového více dimenzionálního prostoru za pomocí jádrových funkcí, kde jednotlivé třídy mohou být lineárně separovatelné.



Obrázek 2.5: Optimální nadrovina s hraničním pásmem SWM rozdělující dvě třídy. Body na okraji pásma jsou podpůrné vektory. [6]

Rozpoznávání založené na obrazu:
Rozpoznávání na základě celého obrazu namísto extrahovaných příznaků je novější přístup při identifikaci. Jelikož tyto metody provádí extrakci příznaků z obrazu i samotné rozhodování, tak jsou méně náchylné například na osvětlení nebo výraz tváře.

Jednou z čím dál více používanou technologií jsou neuronové sítě, specificky hluboké učení. Standardní neuronová síť se skládá z mnoha jednoduchých propojených jednotek zvaných neurony. Vstupní neurony jsou aktivovány na základě vnímaní prostředí. Ostatní neurony jsou aktivovány váženými propoji z dříve aktivovaných neuronů. Učení znamená hledání vah, kdy chování neuronové sítě odpovídá předpokládanému chování (v našem případě správná identifikace osoby). [29]

Jako příklad algoritmu, který se používá pro rozpoznávání na základě celého obrazu mohou být často používané hluboké konvoluční neuronové sítě. Tato popularita může být připsána pokroku v oblasti výpočetního výkonu nutného k učení samotných sítí a popularizací velkými firmy jako například Google nebo Facebook [7].

Hluboké učení nebo hluboké konvoluční sítě je v dnešní době pouze nadnesený název. Ve své podstatě jde o upravené normální neuronové sítě, které jsou uzpůsobeny k rozpoznávání obrazu a zvuku. Popis principu těchto neuronových sítí je převzat od [30], který byl zkrácen, jelikož zde jde jen o krátký náhled na jejich fungování.

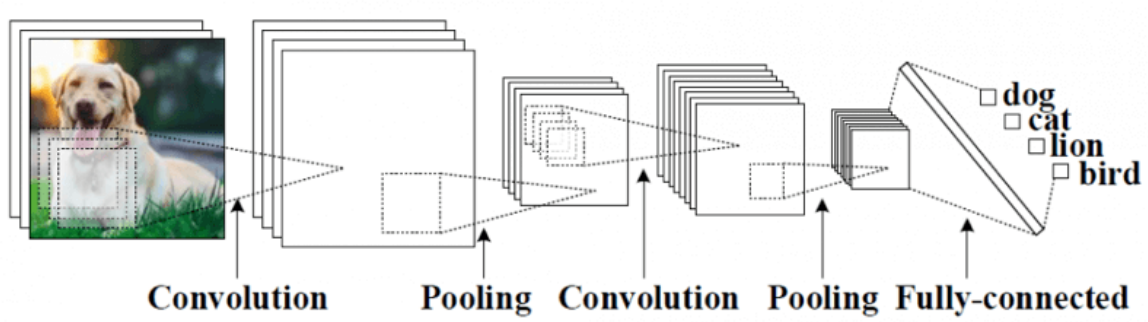
Rozdíl od klasických neuronových sítí je v tom, že namísto vstupu dat v podobě vstupního vektoru používají tenzory. Tenzor je matematický objektu zobecněného vektoru, který může nabývat libovolného počtu dimenzí.

Poté tyto sítě mají na vstupu například celý obraz jako 3-dimenzionální pole (výška × šířka × RGB barvy) a provádí nad tímto obrazem konvoluci menším výřezem původního tenzoru. Tímto způsobem neuronová sít může extrahovat z obrazu příznaky, podle kterých

v dalších vrstvách pracuje. Kdy co zachovat je určeno samotnou natrénovanou neuronovou sítí. Vrstvy, které provádějí tuto změnu se jmenují konvoluční vrstvy a využívají bloky, co se označují jako filtry nebo kernely.

Další druh vrstvy je označován jako max-pooling, downsampling anebo subsampling. V této vrstvě se snižuje velikost jednotlivých matic taktéž za pomocí filtru anebo kernelů.

V posledním kroku se poté jedná o normální plně propojenou neuronovou síť, ze které můžeme číst výsledky.



Obrázek 2.6: Ukázka konvoluční neuronové sítě na klasifikaci obrazu. V průběhu zpracování se střídají konvoluční a pooling vrstvy, provádějící extrakci příznaků a snižování velikosti zpracovávaných dat. V poslední vrstvě je plně propojená neuronová síť provádějící samotnou klasifikaci [4].

Snímky z termokamery

Jedním ze způsobů jak zpřesnit rozpoznávání obličeje je využití termokamery. Snímek z ní zachycuje rozložení tepla na obličeji za pomocí infračervených paprsků, a tedy zde není problém s osvětlením (stíny, odrazy, nízká světelnost). Taktéž z tohoto snímku lze většinou jednoduše separovat obličej od pozadí díky rozdílné teplotě. [33]

Další možnost využití termokamery nebo LWIR (Longwave Infrared) kamery je obecná detekce přítomnosti osoby, která se může použít pro rozpoznání podvrhů, kdy namísto skutečné osoby před kamerou je pouze jeho fotografie.

Informace ze snímků lze zpracovat podobnými metodami, jako se používají na zpracování snímků viditelného spektra. Nicméně se musí dát pozor, že určité povrchy odrážejí LWIR paprsky jinak než barevné světlo. Tento jev je vidět například při focení osob s brýlemi nebo vousy.

Rozpoznávání osob na základě 3D snímků obličeje

Další možností, kdy je možné provést rozpoznávání lidského obličeje je vytvořit 3D model dané osoby. V tomto případě nejspíše nepůjde využít postup založený na obrazu, ale určitě půjde využít rozpoznávání založené na příznacích. 3D model osoby obsahuje mnohem více informací o obličeji, a tak je možné získat různorodější údaje o něm. Příkladem může být geometrie obličeje, stejně jako u 2D snímku, ale v 3D modelu lze získat například i zakřivení tváře a hloubku jednotlivých částí.

Jeden ze způsobů, jak lze těchto výhod využít je pořídit několik 2D snímků obličeje a z nich poté vytvořit 3D model obličeje pro extrakci příznaků.

Složení 3D modelů a počítačové grafiky

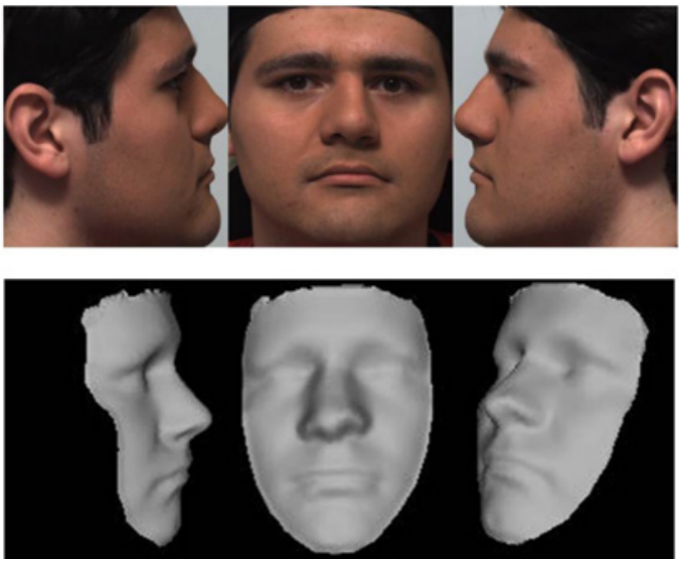
Před tvorbou a zpracováním 3D modelů za účelem jejich rozpoznávání, je nejprve nutné popsat z čeho se takové modely skládají. Na rozdíl od 2D grafiky 3D objekty existují, až na výjimky, pouze ve vektorovém formátu. Tedy tvořené souřadnicemi jednotlivých bodů, matematickým popisem křivek a samotných ploch.

Nejčastějším popisem 3D objektů je za pomocí polygonů, kde grafické karty a vykreslovací software jsou uzpůsobeny k jejich rychlému vykreslení. Tedy n-rozměrnými plochami, které jsou zadány body v prostoru: vertexy. Tyto vertexy tvoří polygonovou síť tvořící celý objekt. Na tyto plochy může poté být nanesena textura, barvy a mohou mít normálové vektory z důvodu výpočtu osvětlení objektu. Jediná záporná stránka tohoto popisu objektu je, že polygony jsou plochy, a tedy nelze nimi dokonale popsat zaoblené povrchy.

Získávání 3D modelu obličeje

Při rozpoznávání za použití pouze 2D snímku obličeje je mnoho faktorů, které mohou způsobit chyby. Mezi takové vlivy může patřit jiné osvětlení, natočení anebo mimika tváře. Tyto faktory je možné do jisté míry eliminovat za pomocí použití 3D modelu obličeje k rozpoznávání. Nicméně toto řešení má vlastní problémy jako je například získání modelu obličeje. Pro vytvoření modelu existují 3 hlavní přístupy.

První přístup spočívá v použití dvou nebo více kalibrovaných kamer. Tyto kamery pořídí snímek obličeje osoby, ze kterých lze vypočítat hloubku pro každý bod, jak lze vidět na obrázku 2.7. Druhý přístup využívá projekci strukturovaného vzoru světla. Na základě zakřivení tohoto vzoru lze vypočítat hloubku. Třetí přístup využívá laserové snímače. Tento způsob je sice přesný, ale cenově nákladný a pomalý. Komerční řešení existují pro všechny tři přístupy, ale většinou se využívá více kamer/snímačů k vytvoření 3D modelu obličeje. [23]



Obrázek 2.7: Příklad rekonstrukce 3D obličeje ze 3 snímků: čelní snímek a dvou profilových snímků [34].

Rekonstrukce 3D modelu pomocí *FlowEngine*

FlowEngine je nástroj pro vytváření 3D modelů od italské firmy 3Dflow[1]. Tento software umožňuje za pomocí fotografií a fotogrammetrie vytvořit 3D modely včetně textur. Fotogrammetrie se zabývá rekonstrukcí objektů, měření vzdáleností a určování polohy předmětů z fotografií. Samotný *FlowEngine* je pouze SDK napsané v C++ pro platformy Microsoft Windows a GNU/Linux umožnující provádět rekonstrukci 3D modelů, jako je například lidský obličej. Firma 3Dflow má také ve svém portfoliu software 3DF Zephyr, který vyžívá *FlowEngine*, obsahuje uživatelské rozhraní a umožňuje export do běžných 3D formátů.

Při používání samotného SDK je možnost řídit celý proces výroby 3D modelu buď za pomocí XML souboru s nastavením anebo přímo v programu využívající knihovnu. Tímto způsobem lze přizpůsobit celou tvorbu k požadovaným podmínkám a dosáhnout větší kvality rekonstruovaného modelu.

2.3 Vestavěné systémy

Vestavěné systémy jsou kombinace softwaru a hardwaru, které jsou většinou vytvořené pro jediný specifický účel. Tento účel mohou být průmyslové stroje, medicínské zařízení, výdejové automaty, ale i kamery a domácí elektronika. [26]

Samotný systém není stavěný pro koncové uživatele jako osobní počítače. Uživatel může systém obsluhovat, ale nemůže změnit jeho funkcionalitu přidáním nebo změnou softwaru. Vestavěné systémy jsou tedy vytvořeny pro jednu specifickou úlohu a dokáží vykonávat pouze tuto funkci. [10]

Biometrické brány jsou ve většině případech vestavěné systémy určené pro provádění identifikace nebo verifikace, kde jiná činnost od nich není vyžadována a jsou sestrojeny pouze k tomuto účelu.

Výpočetní jednotky a komunikační rozhraní

K vytvoření vestavěného systému je zapotřebí mít výpočetní jednotku, která se stará o běh celého systému a ovládání externích prvků za pomocí komunikačních rozhraní (USB, SPI, univerzální piny apod.). Pro tento účel se využívá MCU(*microcontroller*). Tyto MCU mají určitou vnitřní architekturu procesoru RISC (reduced instruction set computer) nebo CISC (complex instruction set computer). Typický zástupce CISC architektury je architektura x86 a pro RISC architektura ARM.

Mezi systémy využívající architekturu x86 a ARM je rozdíl v jejich instrukční sadě. Procesory založené na architektuře x86 mají velké množství instrukcí (některé i poměrně složité), které je procesor schopen vykonat v jednom taktu. Nicméně tato vlastnost je za cenu vyšších výrobních nákladů a větší energetické náročnosti oproti jednodušším procesorům architektury ARM. [2]

Z tohoto důvodu se často ve vestavěných systémech používají procesory právě architektury ARM. Jeden z jednoduchých počítačů využívající architekturu ARM jen například Raspberry Pi.

[1] `https://www.3dflow.net/`

Raspberry Pi

Jelikož vestavěné systémy ve většině případů vyžadují mít jednotku, která se stará o zpracování informací, je Raspberry Pi často dobrá volba a to díky jeho vhodným parametrům s ohledem na různé konektory, velikosti zařízení a nízkého požadovaného napájení.

Samotné Raspberry Pi se momentálně vyrábí v několika variantách, v závislosti na ceně modelu, požadavků a velikosti. Poslední model obsahuje připojení na Ethernet, bezdrátovou Wi-Fi technologii, HDMI port pro zapojení monitoru a dva USB porty. Kromě toho obsahuje 40 pinů pro obecné užití, což je téměř nutnost pro připojení různých digitálních zařízení (například rozhraní SPI). Celé toto zařízení je na malé desce tištěných spojů, a lze ho tedy jednoduše integrovat do celého návrhu vestavěného systému.

Raspberry Pi lze také využít pro různorodá čidla, kde systém může například zpracovávat obraz z kamer a odeslat data na server jen v případě pohybu objektů v záběru.

2.3.1 Komunikační rozhraní mezi prvky systému

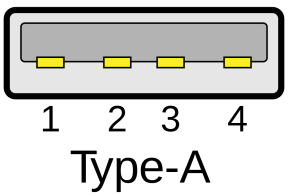
Jak již bylo řečeno, celá biometrická brána je většinou tvořena několika fyzickými částmi. Tyto části je nutné určitým způsobem propojit, aby mohly mezi sebou komunikovat. Velká část zařízení již dokáže využívat standardní univerzální sériové rozhraní (USB), které lze jednoduše připojit k výpočetnímu serveru. Nicméně určitá zařízení jsou určena pro vestavěné systémy a mají pouze jednodušší komunikační rozhraní. Jedno z takových rozhraní může být i SPI (sériové periferní rozhraní).

Univerzální sériové rozhraní

Původní motivace vytvořit univerzální sériové rozhraní pramenila z několika základních úvah. Snadno použitelné rozhraní pro koncové uživatele, kde toto rozhraní má nahradit sériové/paralelní porty a specifické porty ke klávesnicím/myším/joysticku apod. Vytvořit tedy rozhraní, které umožňuje obousměrnou komunikaci, není příliš drahé a umožňuje nízkou až středně rychlou komunikaci. Poté by toto rozhraní mohlo zamezit rozrůstání specifických rozhraní pro různá zařízení. [14]

V dnešní době již existuje několik generací rozhraní USB, kdy poslední generace (USB typu C) se liší výrazně od předchozích. Standardní USB typu A má čtyři piny, kde je napětí +5 V, vodič pro data +, vodič pro data - a zem. USB má také kromě standardní verze i zmenšené verze a to, MiniUSB a MicroUSB, kde je jeden pin navíc pro určení hosta a zařízení (strana hosta je připojena na zem, kde strana zařízení není vůbec připojena).

Podrobný popis způsobu komunikace a napájení za pomocí rozhraní USB, rozdíly mezi generacemi a ostatní informace jsou definovány ve standardu IEC 62680 [13].

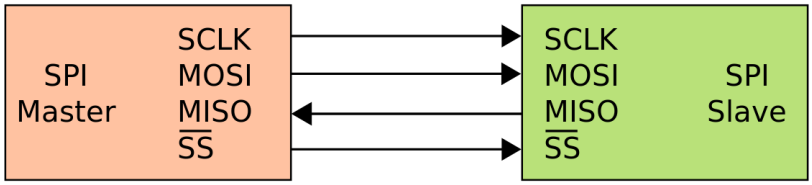


Obrázek 2.8: USB typu-A s očíslovanými piny. Zleva doprava se jedná o +5 V, vodič pro data -, vodič pro data + a zem [8].

Sériové periferní rozhraní

Další možnost připojení zařízení k biometrické bráně může být za pomocí sériového periferního rozhraní (SPI) vytvořené firmou Motorola [21]. Pro SPI neexistuje formální standard a z toho důvodu existuje mnoho protokolů komunikace [27].

SPI komunikace umožňuje duplexní synchronní komunikaci v master/slave režimu. Samotné rozhraní má čtyři piny pro komunikaci. MOSI (Master Out Slave In) pro odesílání dat z masteru na slave. MISO (Master In Slave Out) k opačné činnosti, tedy odesílání dat ze slave směrem k masteru. SS (Slave Select) pin sloužící k domluvě, které zařízení je master a které slave. Poslední pin je SCLK (Serial Clock), který funguje jako výstup pro master k odesílání hodinového signálu. [21]



Obrázek 2.9: Jedno zařízení master připojeno k jednomu zařízení slave za pomocí SPI rozhraní. SCLK je pro hodinový signál, MOSI je výstup dat z master, MISO je vstup dat do slave a pin SS slouží k domluvě master/slave [5].

Síťové rozhraní

Jako poslední rozhraní, které budeme využívat v této práci je síťové rozhraní. Přestože je komunikace po síti výrazně pomalejší než přímým připojením, někdy se jedná o výhodné řešení z důvodu absence fyzických kabelů mezi prvky. Z důvodu rozsáhlosti standardu síťového rozhraní a definovaného chování na síti, zde bude uvedena pouze část, která bude později využita v samotné implementaci biometrické brány. Tedy bude se jednat o přenosový protokol TCP (RFC 793 [25]) a komunikaci přes rozhraní Wi-Fi (IEEE 802.11 [1]). Následující popis v této podkapitole vychází z výše zmiňovaných standardů.

Protokol TCP je spolu s UDP jeden ze základních protokolů pro přenos informací po internetu/lokální síti. Na rozdíl od protokolu UDP, protokol TCP byl vytvořen pro spolehlivý přenos mezi koncovými body v síti využívající pakety. Tento protokol je schopný nepřetržitého přenosu dat v obou směrech mezi jejich uživateli přes síť internetu anebo intranetu. Jak již bylo zmíněno, tento protokol je stavěn tak, aby byl spolehlivý a všechna ztracené data během přenosu jsou znova odeslána tak, aby uživatel vždy dostal veškerá data. Tato funkce je zaručena tím, že před samotnou komunikací proběhne vytvoření spojení mezi koncovými body. Při přenosu se udržují určité informace o spojení, které zajišťují spolehlivost komunikace (například sekvenční čísla paketů).

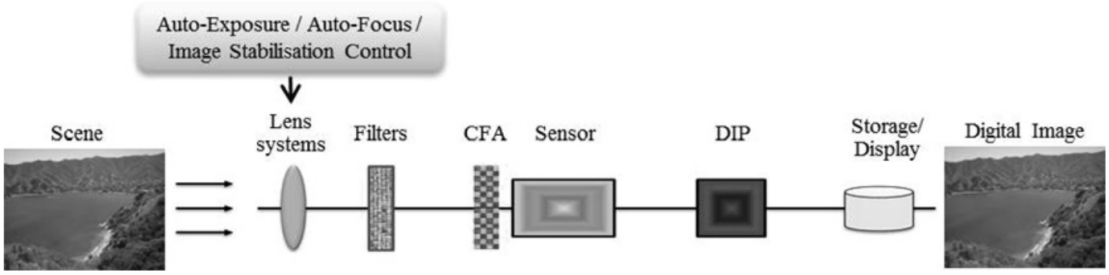
Po vybraní komunikačního protokolu už zbývá jen samotné médium. Při použití připojení za pomocí kabelu (optika nebo kroucená dvojlinka) ztrácí využití síťového rozhraní, místo přímého připojení, smysl. Z toho důvodu je využito pro přenos bezdrátové radiokomunikace technologií Wi-Fi. Tato technologie umožňuje se připojit k přístupovým bodům (access points), skrz které se mohou zařízení připojit do vnitřní sítě anebo k internetu.

2.4 Digitální fotoaparáty a kamery

Jedním z biometrických údajů, který je téměř vždy použit u biometrických bran na identifikaci či verifikaci, je snímek obličeje. Tento snímek je pořízen buď digitálním fotoaparátem nebo kamerou.

Princip digitálního fotoaparátu

Moderní fotoaparát se skládá ze systému optických čoček, filtrů, obrazového snímače a procesoru na digitalizaci obrazu (DIP). Za pomocí soustavy čoček se přivádí světlo ze scény do fotoaparátu. Zde se také provádí i ostření, minimalizace chromatické aberace a stabilizace obrazu. Po průchodu čočkami světlo prochází filtry, které propouští pouze viditelné záření a odstraňují aliasing. V jádru fotoaparátu se nachází obrazový snímač. Tento snímač se skládá z matice fotodiod, které generují analogový signál na základě intenzity světla a ten je poté digitalizován. Tyto snímače nejsou citlivé na barvu a vytváří pouze monochromatický obraz. Z tohoto důvodu se využívají barevné filtry před snímačem (CFA) a poté se barevný snímek vytvoří za pomocí Bayerovy masky. [18]



Obrázek 2.10: Princip zachycení a zpracování fotografie za pomocí digitálního fotoaparátu. Obrázek převzat z článku [28].

V dnešní době se používají dvě technologie pro snímání světla. Tyto technologie jsou starší CCD (*charged coupled device*) a novější CMOS (*complimentary metal oxide semiconductor*).

Technologie CCD byla vytvořena v roce 1970 a využívá tisíce až miliony fotocitlivých buněk, které vytvářejí náboj v závislosti na množství světla, které na ně dopadne. Každá z těchto buněk je tvořena vrstvou polovodiče typu P, vrstvou polovodiče typu N, vrstvou oxidu křemíku zakončená elektrodou. Při dopadu světla se v polovodiči uvolňují elektrony, které lze poté odvést a zaznamenat. [32]

Podobně jak je tomu u CCD, tak také CMOS senzory jsou tvořeny maticí fotocitlivých buněk, ale způsob principu je jiný. Každá buňka obsahuje fotodiodu, kondenzátor a až tři tranzistory. Před snímáním se nabijí kondenzátory na určitou známou hodnotu, kde poté je kondenzátor postupně vybíjen za pomocí fotodiody, kdy rychlost vybíjení je přímo závislá na dopadajícím světle. Poté je zbývající náboj v kondenzátoru přečten a digitalizován. [32]

Princip termokamery

Kromě lidmi viditelného barevného světla, které většina objektů odráží, také všechny objekty vyzařují určité množství infračerveného (IR) záření na základě jejich teploty (čím vyšší teplota objektu, tím více IR vyzařuje). Toto záření je rozděleno do několika pásem:

IR krátké vlnové délky (1 μm až 3 μm), IR střední vlnové délky (3 μm až 5 μm) a IR dlouhé vlnové délky (8 μm až 14 μm) [11].

K snímání tohoto záření se převážně využívají dva druhy senzorů: detektor fotonů a detektor tepla.

Detektory fotonů převádí elektromagnetické záření přímo na volné nosiče náboje v polovodičích, které mohou být poté převedeny na digitální snímek. Tyto senzory dokáží rozlišit i malé změny v prostředí, kde jsou vysoké rozdíly teplot a mají vysokou frekvenci snímků. Nicméně velká nevýhoda těchto senzorů je, že k správné činnosti musí mít teplotu nižší než 77 K ke snížení okolního šumu. [9]

Oproti tomu detektory tepla jsou přístupnější, jelikož nemusí být chlazeny pro správné fungování. Tyto detektory převádí elektromagnetické záření na tepelnou energii, která vede ke zvýšení teploty na detektoru. K převedení této teploty se používá bolometr, který při změně teploty mění svůj odpor. Tato změna je následně převedena na elektrický signál a digitální obraz. [9]

2.5 Biometrické brány

Biometrické brány se používají k automatizaci kontroly oprávnění přístupu do budovy nebo prostoru. Ověřování v tomto systému se skládá z několika kroků. První část je načtení biometrických údajů z nosiče. Poté se ověřuje věrohodnost předložených dokumentů, a zda-li ověřovaná osoba má či nemá povolení k průchodu bránou. Nakonec se porovnávají biometrické údaje načtené z nosiče s údaji pořízenými biometrickou bránou k verifikaci dané osoby.

Tedy jako celek se jedná o vestavěný systém využívající komunikační rozhraní ke spolupráci s externími zařízeními (například kamery v případě této práce) k identifikaci nebo verifikaci osob.

Logická a fyzická struktura biometrické brány

Tato podkapitola je převzata a zkrácena z [17] podkapitol 2.1.1 a 2.1.2.

Biometrická brána může být logicky reprezentována jako systém skládající se z několika navzájem propojených podsystémů za pomocí komunikačních rozhraní. První z nich se stará o ověřování pravosti dokladu, načtení údajů ze strojově čitelné oblasti a načtení údajů z čipu v dokladu. Další podsystém je hlavní částí celého systému, jelikož se stará o verifikaci identity ověřované osoby na základě biometrických příznaků. Poslední dvě části jsou propojení se zabezpečovacím systémem a rozhraním pro externí zařízení.

Odbavení biometrickou bránou může být jedno-krokové nebo dvou-krokové, podle toho, kde se předkládají doklady a kde probíhá verifikace biometrickými systémy. Při jedno-krokové kontrole probíhá předložení dokumentu i verifikace uvnitř brány. Při dvou-krokové kontrole se nejprve započne verifikace před bránou a dokončí se uvnitř brány.

Většinou je biometrická brána složena z následujících fyzických částí, které odpovídají výše uvedeným podsystémům: jedna nebo dvě fyzické zábrany (podle počtu kroků při verifikaci), čtečka na čtení textu a čipu z biometrických pasů, monitory pro zobrazení průběhu/instrukcí verifikace, zařízení pro získání biometrických údajů a HW/SW systému, který je použit i na komunikaci s externími systémy.

Kapitola 3

Návrh biometrické brány a proces vytváření 3D modelu

Celý systém biometrické brány se skládá z hardwarové a softwarové části. Hardwarová část systému se skládá z 5 RGB kamer pro zachycení snímků osoby a jedné termokamery. Softwarová část se poté stará o vytvoření modelu z pořízených snímků, extrakci příznaků a využití dat z termokamery. Přesnější popis se nachází v odpovídajících sekcích.

3.1 Hardwarová část systému

Fyzicky se biometrická brána skládá z 5 RGB kamer a IR kamery. Kamery pro zachycení barevných snímků jsou uspořádány do kruhu. Toto uspořádání bylo vybráno pro výsledný systém, jelikož kvalita později vytvořeného 3D modelu závisí z kolika úhlů/fotek lze každý výsledný vertex vidět.

Vzdálenosti pro RGB kamery se pohybuji kolem 30 cm podle focené osoby. Vzdálenost termokamery je přibližně 50 cm. Tyto vzdálenosti jsou vybrány tak, aby focená osoba byla v celém snímku.

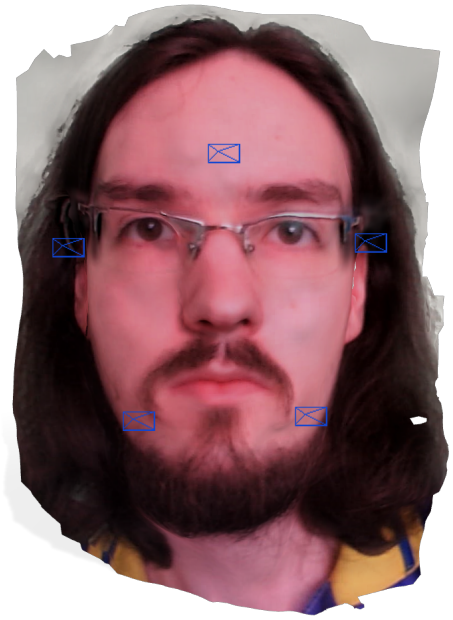
Jelikož LWIR kamera musí být připojena za pomocí SPI rozhraní, tak bylo v návrhu využito Raspberry Pi B+ pro komunikaci s termokamerou. Výsledný pořízený snímek je poté zaslán pomocí Wi-Fi a TCP protokolu na cílový počítač provádějící vytvoření 3D modelu a identifikaci.

3.2 Návrh softwaru pro biometrickou bránu

Software pro biometrickou bránu se především stará o dvě úlohy. První část se stará o vytvoření 3D modelu z pořízených fotografií. Druhá část spočívá v extrakci příznaků z vytvořeného modelu.

3.2.1 Vytvoření 3D modelu obličeje

K vytvoření 3D modelu ze snímků pořízených za pomocí RGB kamer je využita SDK knihovna *FlowEngine* od firmy 3Dflow. Jelikož tato SDK knihovna není primárně určena pro vytvoření 3D modelu z malého počtu snímků, tak je nutné mít poměrně vysokou kvalitu snímků a správně nastavenou rekonstrukci obličeje.



Obrázek 3.1: Obrázek zobrazující umístění kamer při focení osoby.

Kvůli poměrně velké složitosti algoritmů, které jsou zapotřebí ke spočítání vertexů z fotografií, je samotná rekonstrukce 3D modelu v *FlowEngine* rozdělena do několika následujících kroků:

- Vytvoření klíčových bodů na základě pořízených snímků.
- Dopočítání ostatních bodů kolem klíčových.
- Převedení bodů na polygony.
- Vypočítání textury na výsledný model.

Vytvoření klíčových bodů modelu

V první fázi se snímky použité pro rekonstrukci modelu navzájem porovnávají, kde se hledají shodné body a vzájemné umístění fotografii. Důležitá nastavení v této fázi jsou určení kolik shodných bodů se na modelu hledá a jak přísné podmínky musejí splňovat. Výsledné body jsou zobrazené na obrázku 3.2a.

Spočítání ostatních bodů

Po vytvoření klíčových bodů je nutné spočítat ostatní body kolem klíčových. U těchto bodů se dá říct, že tvoří hloubku modelu, protože tvoří jeho obrys. A tedy většina nastavení při vytváření těchto bodů se týká hloubky výsledného modelu. Zobrazené body jsou na obrázku 3.2b.

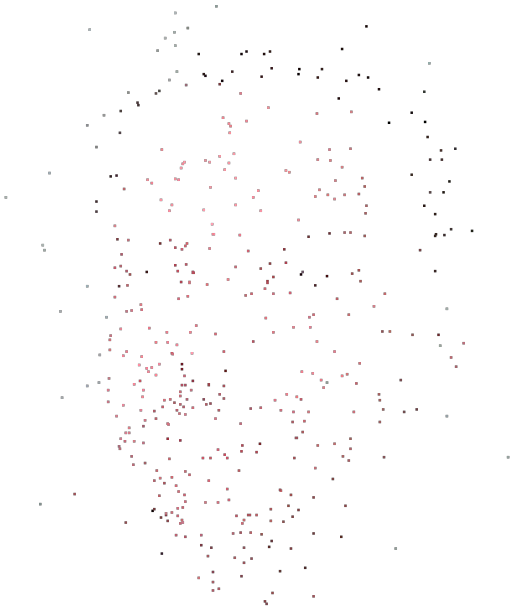
Vytvoření povrchu modelu

Při tomto kroku se vytvořené body (vertexy) spojují v polygony, a tím vytváří konsistentní povrch modelu. Za pomocí nastavení v tomto kroku lze docílit vhodného chování pro vy-

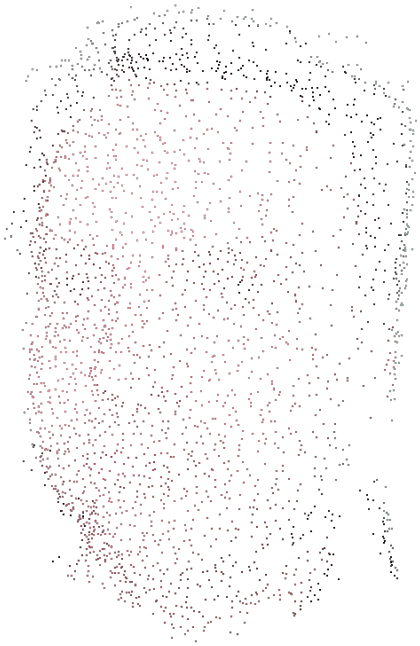
tváření modelu obličeje: vyhlazení povrchu modelu a vyplnění chybějících míst v něm. Vytvořený model z polygonů je na obrázku 3.2c.

Pokrytí texturou

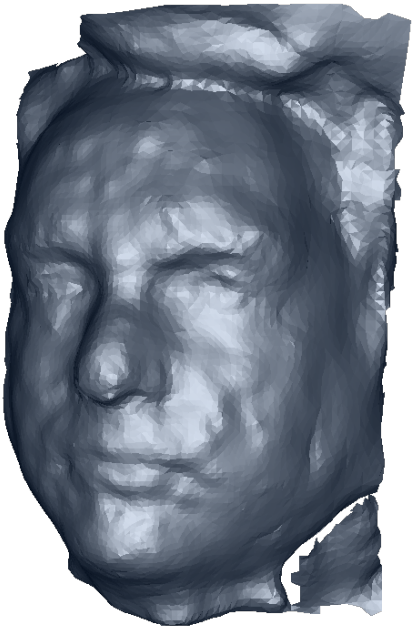
V posledním kroku se vytváří textura na vytvořený 3D model. Ačkoliv model i bez textury připomíná focenou osobu, neobsahuje samostatnou texturu, ale jen každý vertex má určitou barvu. Nicméně v této fázi se z použitých fotek extrahuje textura, která se poté mapuje na samotný model. Finální model s texturou je na obrázku 3.2d.



(a) Vytvořené klíčové body na modelu obličeje.



(b) Dopočítané ostatní body k vytvoření hloubky modelu a jeho obrysu.



(c) Vytvořené polygony z vertexů vytvořených v minulé fázi.

(d) Finální model pokrytý texturou z fotografií.

Obrázek 3.2: Čtyři obrázky popisující postupnou tvorbu modelu za pomocí SDK knihovny *FlowEngine* of firmy 3DFlow.

3.2.2 Extrakce příznaků z 3D modelu v *.obj* formátu

Před provedením samotné identifikace nebo verifikace je pro většinu metod nutné nejprve extrahovat příznaky. Tyto příznaky se vybírají s ohledem na jejich kvality jako rozlišitelnost, neměnnost apod. V návrhu pro biometrickou bránu je využito horizontálního a vertikálního řezu procházejícího přes špičku nosu modelu jako příznaky pro následnou identifikace osob.

Formát *.obj* pro uložení 3D modelu

Jeden z používaných formátů pro nekódované ukládání 3D modelů za pomocí ASCII formátu je *.obj*, nebo-li *Wavefront object file*. Tento formát byl vytvořen firmou Wavefront Technologies pro jejich aplikaci The Advanced Visualizer.

Samotný soubor definuje geometrii a ostatní vlastnosti objektu původně pro jejich software. Nicméně dnes se obecně používá jako vstup a výstup napříč mnoha aplikacemi umožnující práci s 3D modely.

Popis formátu je zkrácen s ohledem na jeho použití v této práci z [24], kde se nachází cely podrobný popis. Formát umožňuje uložit objekty tvořené z polygonů (body, přímky, stěny) i volné objekty (křivky a plochy). V této práci nás budou zajímat pouze 3D modely tvořené vertexy. Tedy jejich umístění v prostoru, mapování textury, jejich normály a popis jak tvoří samotné polygony.

Vybraná syntaxe zápisu v *.obj* formátu s ohledem na tuto práci:

- Umístění vertexů

  $v \quad x \quad y \quad z \quad w$

  kde x, y, z je umístění v prostoru a w je váha při použití racionálních křivek.

- Umístění textury

  $vt \quad u \quad v \quad w$

  kde pro 3D pozici je nutné zadat všechny 3 parametry u, v, w pro umístění horizontálně, vertikálně a hloubky textury.

- Normálový vektor

  $vn \quad i \quad j \quad k$

  kde i, j, k jsou souřadnice pro normálu vertexu.

- Skupina vertexů

  $f \quad v/vt/vn \quad v/vt/vn \quad v/vt/vn$

  každá skupina vertexů je v našem případe tvořena 3 vertexy (model je tvořen z trojúhelníků). Jejich umístěním, texturou a normálovým vektorem.

Extrakce vertexů z modelu

K získání řezů pro identifikace je nejprve nutné ze souboru, obsahující 3D obličej osoby, extrahovat potřebná data. Naštěstí model, získaný ze snímků obličeje, je uložen ve formátu *.obj*, který není speciálně kódován. Z tohoto souboru lze jednoduše extrahovat pouze sou-

řadnice vertexů a ignorovat ostatní, pro nás nepodstatné informace, jako barvy vertexů, mapování textur nebo jejich propojení do polygonů.

Získání horizontálního a vertikálního řezu z obličeje

V návrhu biometrické brány byly zvoleny dva řezy obličeje na základě, kterých se poté bude rozhodovat o výsledné identifikaci osoby. Tyto řezy prochází přes špičku nosu, jelikož je tvořena body, které jsou znatelně vystouplé oproti ostatním. Po nalezení umístění nosu, je nutné si zvolit šířku řezu. Malá šířka nemusí obsahovat dostatečné množství informací k identifikaci, ale zase příliš velká může způsobovat problémy při konečné úpravě řezu.

Po získání bodů, které jsou v řezu, je nutné je ještě upravit. První úprava těchto bodů se týká omezení dimenzí, tedy převedení vertexů z 3D prostoru pouze do 2D. Jelikož výsledek má být řez, tak je nutné pouze zachovat hloubku a délku řezu. Další úprava se týká normalizace počtu bodů a vzdálenosti mezi nimi, jelikož z podstaty 3D modelu detailnější části obsahují více vertexů. Tato úprava může být provedena vybráním konstantního intervalu na kterou se bude mapovat celá šířka/výška modelu. Poté podle počtu bodů se rovnoměrně pokryje vybraný interval body, což zajistí jednu z výsledných souřadnic bodu. Druhá souřadnice, v tomto případě hloubka, může být určena podle hloubky vertexů.

Výsledné body, převedené pouze do dvou rozměrů a do jisté míry normalizované, mohou být poté uloženy pro referenční model k pozdější identifikaci. Nebo pokud se jedná už o získání příznaků od osoby, kterou se snažíme identifikovat, můžeme je porovnat s uloženými referenčními modely.

Obrázek 3.3: Obrázek zobrazující umístění dvou řezů modelu obličeje, které budou tvořit příznaky pro následnou identifikaci.

3.2.3 Zpracování dat z IR kamery

Pro návrh byla použita FLIR Lepton 2.0 kamera. Tato verze kamery neumožňuje přímé čtení teploty povrchu, ale při testování vrací hodnotu kolem 7800 pro pixel bez tepla z obličeje a hodnotu kolem 8100 pro obličej. Tyto hodnoty byly experimentálně zjištěny za pomocí focení lidského obličeje a objektů při pokojové teplotě.

Samotná data jsou tedy matice o velikosti 60 x 80 bodů s hodnotami v přibližném rozmezí od 7800 až 8100. Termokamera, která je součástí biometrické brány, tedy bude sloužit pro určením zda je opravdu focena osoba anebo pouze replika 3D obličeje. Tato kontrola by měla jít docílit prostým součtem všech hodnot a nastavením určitého prahu pro potvrzení, že před kamerou je skutečný člověk.

Kapitola 4

Implementace návrhu biometrické brány

Implementace biometrické brány je z velké části napsána v jazyce C++. Jako cílový systém provádějící výpočty je operační systém Microsoft Windows 10. Z tohoto důvodu některé zdrojové kódy lze přeložit pouze pod touto platformou bez dodatečných úprav (zejména síťová komunikace s Raspberry Pi, linkovaní SDK knihoven *FlowEngine* a operace se soubory).

4.1 Implementace pořízení RGB fotografií

Jako první krok v identifikaci biometrickou bránou je pořízení snímků osoby, kterou chceme identifikovat nebo zavést do systému. K tomuto účelu je využito pěti RGB kamer. K implementaci byly využity malé kamery HBV-1716, které lze jednoduše zabudovat do biometrické brány a mají dostatečně vysoké rozlišení potřebné k vytvoření kvalitního 3D modelu. Tyto kamery jsou staticky umístěny před obličejem focené osoby tak, aby každý z klíčových bodů, které jsou potřeba při extrakci příznaků, byl viděn ze 3 kamer. Vzdálenost kamer je upravena podle konkrétní osoby tak, aby obličej tvořil většinu plochy snímku.

Při pozdější tvorbě 3D modelu dané osoby je využita maska na snímky. Tato maska zlepšuje kvalitu výsledného 3D modelu, díky oříznutí okolí kolem obličeje. Z tohoto důvodu je nutné, aby obličej na snímku byl vždy na středu fotografie.

Samotná implementace pořízení fotek je napsána v jazyce C++ za pomocí knihovny OpenCV[1] verze 4. Tento program zachytí snímek ze všech pěti kamer naráz a uloží je ve formátu *Portable Network Graphics* pro pozdější využití k vytvoření 3D modelu obličeje.

4.2 Implementace vytváření 3D modelu

Když máme pořízené fotografie, získané z pěti barevných kamer, můžeme přistoupit k dalšímu kroku a to vytvoření 3D modelu focené osoby. Celý proces je zprostředkován aplikací v C++ využívající SDK knihovnou *FlowEngine* od firmy 3DFlow[2]. Momentální implementace umožňuje přeložení pouze na operačním systému MS Windows a 64-bitové architektuře z důvodu nutnosti mít k SDK knihovně i předkompilované knihovny (firma dodává i knihovny pro GNU/Linux systémy).

[1] `https://opencv.org`
[2] `https://www.3dflow.net`

V prvním kroku je nutné nastavit samotný *FlowEngine*. To znamená načíst konfigurační soubor, který později bude řídit proces vytváření samotného modelu. Poté je nutné nastavit cesty adresářů pro výstup, dočasné soubory, logy a zdrojové fotky.

Po tomto nastavení se může přejít k načtením obrázků ze předem určené složky. V této složce se také nacházejí soubory popisující masky jednotlivých obrázků. Ty se načítají spolu se snímky a přiřazují se k nim. V tomto kroku se také mohou zadat údaje pro kalibraci kamer (snímků z nich pořízených). Samotná kalibrace byla provedena v programu 3DF Zephyr od stejné firmy co poskytuje používané SDK knihovny, jelikož jsou použity i v tomto výše zmíněném programu. Pro fotografie, u kterých bychom neměli jejich kalibraci, je také možné použít automatickou kalibraci, kterou si umí software sám vytvořit.

Následující čtyři kroky popisují a starají se samotné vytváření výsledného 3D modelu focené osoby. Což konkrétně znamená vytváření klíčových bodu a odhadnutí umístění kamer, dopočítání okolních bodů kolem klíčových k vytvoření hloubky modelu, vytvoření polygonů z doposud vytvořených klíčových bodů a jejich vyhlazení a nakonec namapování textury z původních fotografií na výsledný model.

Jelikož v ostrém nasazení nebudeme mít ideální podmínky pro pořizování fotografií obsahuje nástroj pro tvorbu modelu prostředky pro zlepšení výsledné kvality. Jedním z těchto prostředků je využití už výše zmíněné masky pro snímky a tím výrazně omezit pravděpodobnost, že systém bude chtít vytvořit 3D model něčeho, co je v pozadí a né samotného obličeje. Druhý prostředek pro pomoc vytváření modelu je částečně součástí průběhu tvorby obličeje. Hned po prvním kroku generování modelu se vytvoří obdélník, který určuje hranice aktuálního modelu a díky tomu systém ignoruje body, které jsou později mimo obličej.

4.2.1 Vytvoření klíčových bodu a odhad umístění kamer

V první fázi samotného vytváření modelu jde o to zpracovat všechny vstupní fotografie a snažit se odhadnout jak navzájem tvoří výslednou scénu. Toto je docíleno porovnáváním každého snímku s každým snímkem a určení shodný bodů na snímcích. Proces zjištění pozice kamer lze knihovně ulehčit tím, že řekneme jak jdou snímky po sobě (kolem objektu, v mřížce, lineárně apod.). Počet těchto bodů a kolik okolních bodů z jiného snímku se musí shodovat je nastavené v konfiguračním souboru pro celý proces generování 3D modelu.

V momentálním řešení bylo empiricky zjištěno, že nejlépe funguje v této fázi vytvořit 600 klíčových bodů při tvorbě obličeje. Taktéž v nastavení této fázi byly vypnuty urychlující algoritmy, jelikož cenou za rychlost je snížení kvality modelu. Tuto kvalitu už nelze moc snižovat z důvodu, že se snažíme vytvořit model pouze z pěti fotografií a nesmíme mít příliš zkreslený výsledný model pro přesnou identifikaci osoby.

4.2.2 Výpočet okolních bodů k získání hloubky modelu

V druhé fázi vytváření obličeje ze snímků se musí spočítat umístění poměrně velkého množství bodů kolem už vytvořených klíčových. Tyto body dodávají výslednému modelu jakousi hloubku a pokrývají téměř celý povrch obličeje, a tedy lze z nich už poznat danou osobu.

Tento krok tedy využívá předešlé klíčové body a umístění kamer, aby mohl spočítat již zmíněné ostatní body. Z pohledu nastavení se zejména jedná o počet použitých snímku k vytvoření hloubkové mapy a různé vyhlazování výsledného modelu (redukce šumu, dopočítávání a uzavírání prázdných míst). Jako v předešlém kroku, tak i při nastavování tohoto kroku byl kladen důraz na vytvoření přesného modelu před rychlostí zpracování.

4.2.3 Převedení modelu ze shluku vertexů na polygony

V této části tvorby modelu se vlastně vytváří samotný model. Z pouhého shluku vertexů, které byly vytvořeny ve dvou předchozích fázích se vytváří polygony. Výstupní polygony z *FlowEngine* jsou tvořeny trojúhelníky, tedy vždy třemi vertexy. Poté ke každému polygonu je dodán normálový vektor, který se později (né v našem případě) může využít třeba pro výpočet osvětlení modelu. Tento krok je důležitý z pohledu celkové tvorby 3D modelu pro všeobecné použití, nicméně pro naše potřeby, kromě vyhlazování hran, je téměř zbytečný, protože příznaky se stejně extrahují z vertexů těchto polygonů.

Při nastavení této fáze lze určit od základních věcí, jako minimální a maximální počty vertexů v celém modelu až po použití komplexnějších algoritmů, které se starají o vytváření a upravování výsledného povrchu modelu. Mezi důležité nastavení pro správnou rekonstrukci lidského obličeje patří dopočítávání mezer v objektu a vyhlazování povrchu, jelikož obličej neobsahuje ostré hrany.

4.2.4 Finální úprava povrchu modelu - textura

Poslední krok vytvoření modelu je pokrýt ho texturou. Pro normální účely se i normálně méně kvalitní 3D modely dají vzhledově opticky převést do vysoké kvality díky ostré textuře, kde model pak působí více propracovaný. Bohužel pro potřeby tohoto projektu je úplně irelevantní a zbytečně se zabírá čas vytvářením textury modelu, neboť se stejně při jeho zpracování nevyužije.

Nicméně při případné nutnosti zvýšit přesnost celého systému, je možnost využít i tuto informaci. Systémy pro rozpoznávání obličeje fungují efektivně i z pouhého 2D snímku obličeje, a tedy mít namapovaný snímek na 3D model, kde je jednoduší najít umístění výrazných částí obličeje může výrazně zvýšit přesnost samotného rozpoznávání.

4.2.5 Zpracování souboru s 3D informacemi

Jako výstup z *FlowEngine* SDK je buď soubor ve formátu *3DFlow SDK* (.3dk), který lze použít k načtení do 3DF Zephyr od stejné firmy zprostředkující uživatelské rozhraní nad celou tvorbou 3D modelu. Nicméně tento výstup nás nezajímá, jelikož jeho kódování není veřejné. Pro naše potřeby jde po provedení posledního kroku tvorby výroby 3D modelu, tedy pokrytí texturou, získat model obličeje v *.obj* formátu. Tento formát má veřejně definovanou strukturu a je často používán mnoha nástroji, co pracují s 3D modely.

Pro účel extrakce jednotlivých bodů z *Wavefront object file* formátu (.obj) je vytvořen program v jazyce C++, který načte soubor obsahující 3D model a získá z něj požadované informace. Tyto informace jsou poté dále zpracovány k získání příznaků k identifikaci.

4.2.6 Extrakce vertexů z *Wavefront object file*

Získání samotných bodů objektu je jednoduchá část zpracování modelu. Formát *.obj* je kódován v ASCII, a tedy lze jednoduše načíst. Ve vytvořeném souboru z SDK knihovny se nacházejí čtyři údaje. Umístění jednotlivých vertexů v prostoru, pozice pro mapování textury, vektor normály pro vertexy a popis jednotlivých polygonů (trojúhelníků v našem případě). Pro účely extrakce příznaků použijeme pouze pozice vertexů (řádky začínající znakem v, kde následují souřadnice x, y a z). K zpřesnění identifikace by bylo možné použít i mapování textury na vertexy spolu s vytvořenými texturami, jak bylo popsáno v podkapitole 4.2.4.

4.2.7 Získání bodu určující špičku nosu

K provedení identifikace nebo verifikace je nutné mít příznaky, které mají pro jejich funkci dobré vlastnosti. Tyto příznaky by měly být ideálně pro stejnou osobu úplně totožné nehledě na podmínkách. Bohužel ve většině případů jsou přímo získané údaje o osobě velice proměnlivé. Tak tomu je i do jisté míry u vytvořeného 3D modelu obličeje. Z toho důvodu použijeme špičku nosu jako statický bod, ze kterého můžeme vycházet, jelikož lze jednoduše z modelu určit.

Díky tomu, že je špička nosu nejvíce vystouplá část modelu, můžeme použít tuto skutečnost k jejímu nalezení. Při tomto předpokladu stačí z načtených bodů určit nejvíce vystouplých bodů a provést z nich prostý průměr. Další možné řešení je zjistit celkovou hloubku modelu a vzít všechny body co spadají do 1 % nejvíce vystouplých bodu v daném směru.

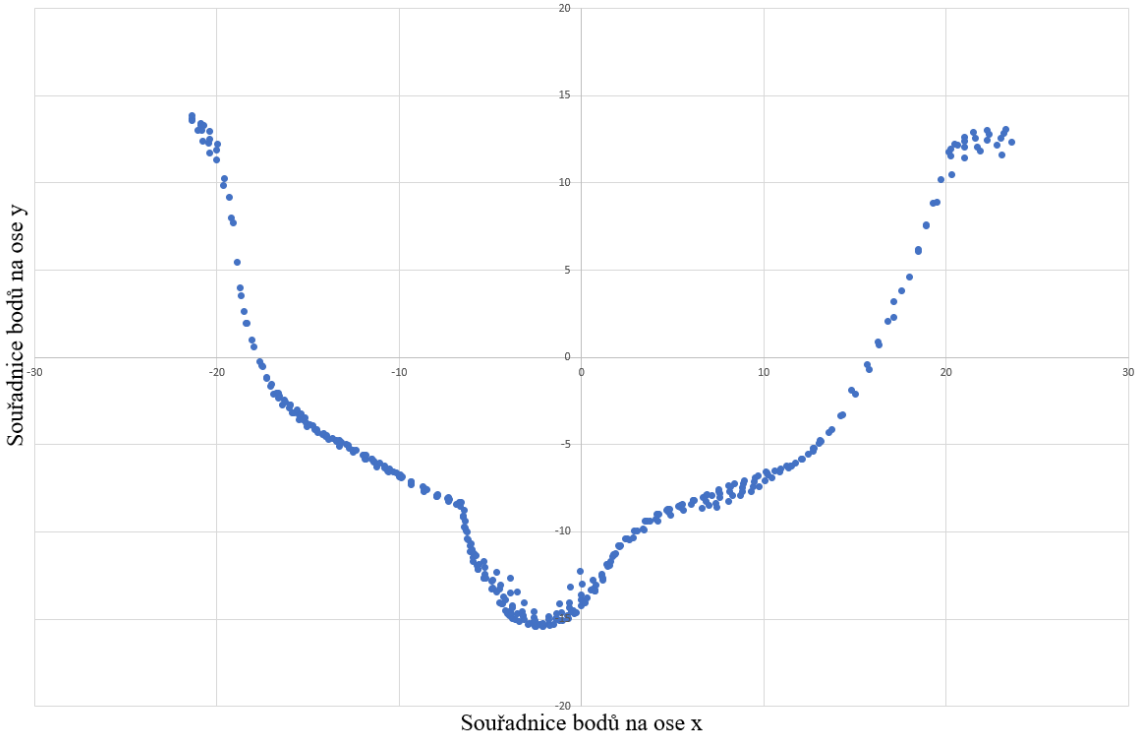
4.2.8 Získání řezu obličeje procházejícím nosem modelu

Po získání pozice špičky nosu můžeme provést řez modelem s tím, že bude vždy u stejné osoby procházet stejným místem a tak zajistit konzistenci mezi různými 3D modely stejné osoby. Díky této vlastnosti budeme blíže k získání příznaků, které lze použít při samotné identifikaci.

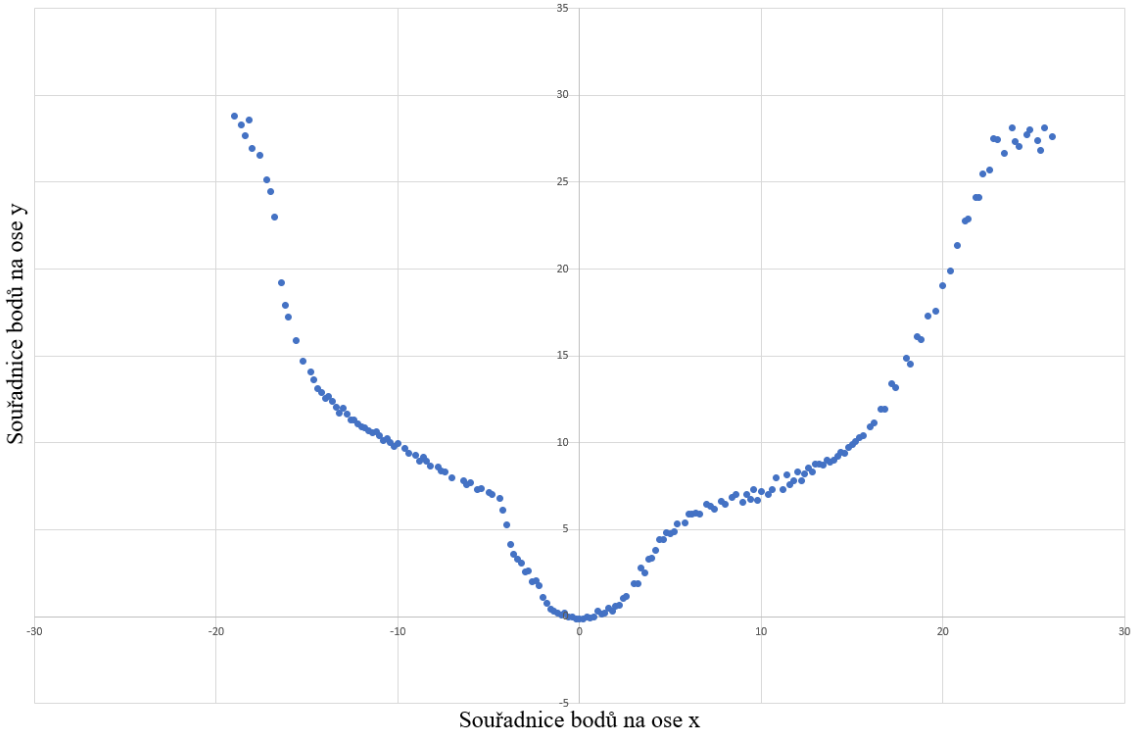
K získání samotného řezu si musíme nejprve určit šířku řezu. Tato velikost musí být dostatečně veliká, aby bylo možné rozlišit kontury obličeje, kde bude procházet řez, ale nesmí už být zkreslen zakřivením obličeje. Po určení samotné šířky už nyní zbývá jen vybrat z načtených vertexů modelu ty, co zapadají do řezu. Tedy ty, co jsou vzdáleny +- šířku řezu od souřadnic vrcholu nosu v jedné z os (v našem případě kolem osy z pro horizontální řez a osy x pro vertikální řez).

Po získání horizontálního a vertikálního řezu je nutné provést ještě normalizaci k usnadnění porovnávání mezi řezy různých modelů. První normalizace, kterou lze provést je posun celého řezu v souřadném systému. Jelikož získaný model nemusí mít střed vždy v opravdovém středu, a tedy se může různě lišit, je dobré celý řez posunout v ose y (hloubka modelu) tak, aby špička nosu byla v této ose v bodě 0 a zbytek bodů tedy v kladné části. Druhý posun, který můžeme provést je v ose řezu. Tím, že vrchol nosu v řezu bude na souřadnicí (0, 0), tak nemusíme starat o zarovnání různých řezů modelu a tím je ulehčena práce při následné identifikaci.

Další normalizace, k ulehčení porovnávání řezů, je převzorkovat celý řez. Momentální řez je sice tvořen jednotlivými body, ale jejich hustota se může lišit v závislosti složitosti polygonů v daném místě modelu. Tahle nerovnoměrnost může způsobovat problémy při jejich následném porovnávání. Z toho důvodu jsou vytvořeny nové body s konstantní vzdáleností, kdy se těmto bodům přiřazuje hloubka s ohledem na extrahované vertexy.



(a) Nenormalizovaný horizontální řez modelu obličeje procházející přes špičku nosu.



(b) Normalizovaný horizontální řez modelu obličeje procházející přes špičku nosu.

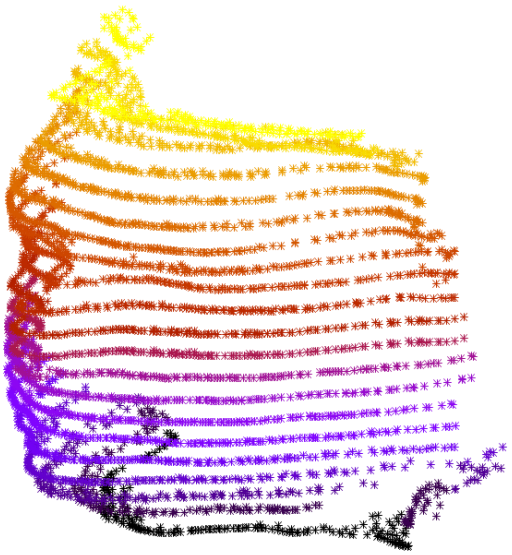
Obrázek 4.1: Ukázka normalizovaného a nenormalizovaného horizontálního řezu.

4.2.9 Úprava návrhu řezů 3D modelem

Při předběžném testování identifikace osoby za pomocí horizontálního a vertikálního řezu bylo zjištěno, že tyto dva řezy nejsou dostatečně specifické k jednoznačnému určení osoby. Při porovnání těchto řezů po zarovnání na špičku nosu byly rozdíly pouze na okrajích snímku, které jsou nejspíše způsobeny nepřesnostmi při vytváření 3D modelu z fotografií. Z tohoto důvodu byl přehodnocen přístup k extrakci příznaků z modelu. Namísto získání horizontálního a vertikálního řezu procházejícím přes špičku nosu je momentálně získáváno 21 horizontálních řezů. Při větším počtu řezů je pokryta větší plocha obličeje (v tomto případě celý obličej), a tedy výsledné porovnání je přesnější z důvodu redukce místních nepřesností modelu.

Počet těchto řezů byl zvolen tak, aby každý řez obsahoval dostatek informací, a tedy nesl určitou hodnotu o modelu. Nicméně tato velikost nesmí být ani příliš veliká z důvodu ztráty hloubky u určitých řezů (například řez procházející přes oči modelu) a ani příliš malá, neboť by řez neobsahoval dostatek potřebných informací. Pro zaručení přiřazení řezů stejných částí u každého modelu je prostřední řez vždy původní řez procházející přes špičku nosu. Poté jsou ostatní řezy a jejich velikosti určeny tak, aby vyplnily horní část obličeje a spodní část obličeje. Tedy rovnoměrně přes celý model. Normalizace jednotlivých řezů zůstává téměř stejná, až na normalizaci počtu a vzdálenosti bodů.

Při řezech co jsou na okraji modelu (nahoře nebo dole) se může stát, že model nebude zabírat celou šířku, a tedy při převzorkování neexistuje odpovídající bod v modelu. Tyto body jsou tedy zahozeny, protože ani v modelu neexistují. Další změna v ohledu převzorkování jsou určité oblasti (oči, nos, ústa), kde není jednoznačné jakou hloubku pro daný bod vybrat. V tomto případě se vybírá nejhlubší bod (ale je možné brát průměr nebo nejvyšší bod).



Obrázek 4.2: Vizuální zobrazení 21 řezů popisující celý model 3D obličeje.

4.3 Využití termokamery v biometrické bráně

Poslední část biometrické brány je kamera pořizující snímky infračerveného záření. Jedna z výhod tohoto záření je, že nevyžaduje přítomnost barevného světa. Nicméně při využití této kamery tuto vlastnost přímo nepoužíváme, ale díky datům pořízených z termokamery můžeme zvýšit bezpečnost biometrického systému proti neoprávněnému přístupu za pomocí umělého 3D modelu jiného člověka.

4.3.1 Pořízení snímku z IR kamery

V momentální implementaci je použita malá IR kamera Lepton 2.0 od firmy FLIR. Tato kamera umožňuje zachytit dlouhé vlny infračerveného záření s rozlišením 80 na 60 bodů. Kvůli snadnějšímu připojení k biometrické bráně je kamera umístěna na desce tištěných spojů s vyvedenými kontakty SPI rozhraní.

Nicméně v momentální sestavě nelze termokameru připojit přímo k výpočetnímu serveru, který se stará o vytváření 3D modelu a extrakci příznaků, z důvodu chybějícího komunikačního rozhraní SPI na straně serveru. Kvůli tomu je tato kamera připojena k Raspberry Pi B3+, který obsahuje distribuci Linuxu založenou na distribuci Debian: Raspbian. Díky tomu je možné za pomocí skriptu v Pythonu pořídit snímek z termokamery. Tento skript na straně Raspberry neustále naslouchá a při získání povelu od serveru vytvoří snímek z IR kamery. Snímek je poté částečně zakódován pro účel přenosu a za pomocí technologie Wi-Fi a TCP protokolu odeslán na server, který o pořízení snímku požádal.

4.3.2 Zpracování získaného snímků

Hlavní server biometrické brány může po získání snímku zahájit jeho zpracování. Přestože je získaný snímek poměrně malý, pro naše účely úplně postačuje. Data získaná z tohoto modelu IR kamery je tedy dvou-dimenzionální matice celých čísel o rozměrech 80 na 60. Bohužel hodnoty z modelu momentálně použitého v biometrické bráně nelze přímo převést na stupně vyjadřující teplotu. Nicméně po testech termokamery lze zhruba určit hodnoty vyjadřující teplá a studená místa. Tedy pro teplotu lidského obličeje jsou výstupní hodnoty okolo čísla 8100 a při pořízení snímku chladnějších předmětů (například omítnutá stěna) se hodnoty pohybuji okolo 7800.

Obrázek 4.3: Snímek pořízený z termokamery Lepton 2.0, kde barevné rozmezí je mapováno na interval hodnot 7800 (černá) až 8100 (bíla/žlutá).

Za tohoto předpokladu provedeme kontrolu, zda focený obličej je opravdu "živý"a né umělý model. Pokud tedy máme získané data z termokamery, tak stačí buď udělat průměrnou hodnotu z jednotlivých hodnot a určit práh k potvrzení nebo pouze sečíst všechny hodnoty a opět určit práh. Tento způsob kontroly by měl být pro biometrickou bránu dostatečně spolehlivý, ale v případě potřeby lze provést drobné úpravy jako ignorovat rohy snímků, kde s největší pravděpodobností už nebude obličej.

Jediným problémem s tímto přístupem mohou být lidé s brýlemi nebo vousy, jelikož ani jedna z těchto věcí dobře neodráží LWIR záření, a tedy výsledná průměrná hodnota bude výrazně nižší.

4.4 Identifikace osob

Jako poslední krok celého systému biometrické brány je provést samotnou identifikaci. Za tímto účelem se provedou postupně všechny kroky doposud zmíněné v implementaci.

4.4.1 Získání dat o osobě

Poté co se osoba postaví/posadí před biometrickou bránu se může spustit program starající se o průběh celého procesu pořizování fotografií osoby, tvorby modelu, extrakce příznaků a identifikace.

První část, která se provede, je odeslání požadavku na Raspberry Pi, aby došlo k vytvoření snímku z připojené termokamery. Tento snímek je následně odeslán zpět a zpracován. Výsledkem tohoto kroku je, zda-li se má začít proces vytváření modelu osoby či nikoliv.

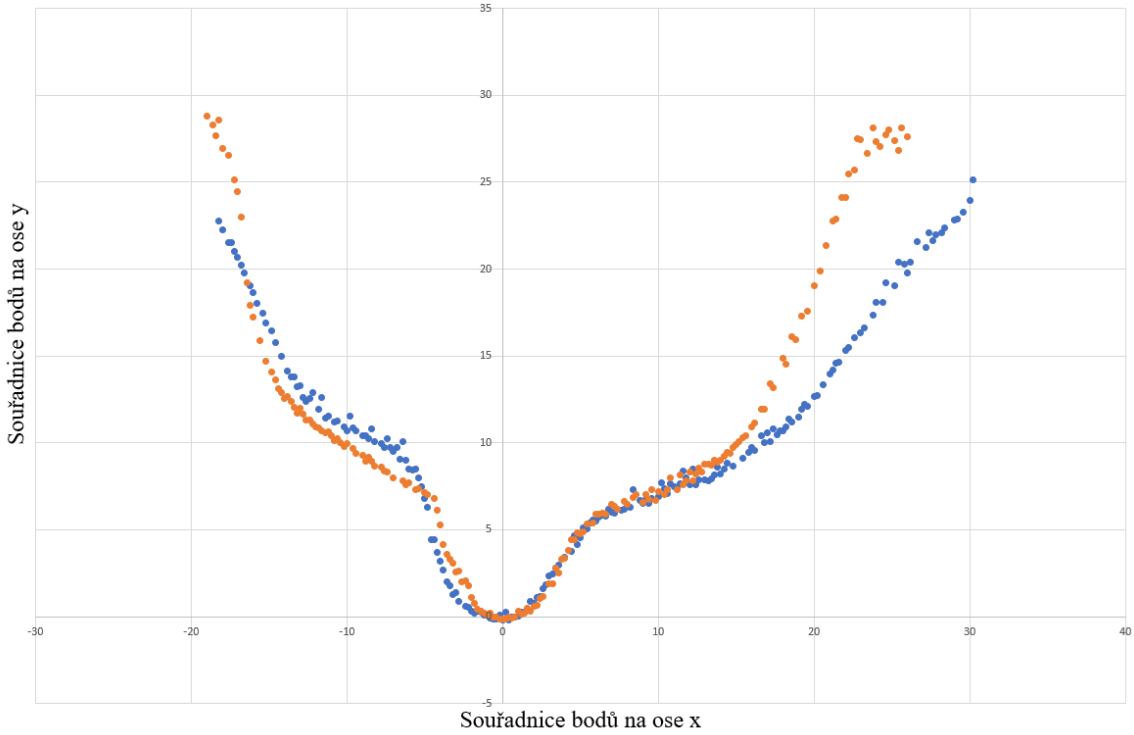
Pokud tato část proběhne úspěšně pořídí se naráz pět snímků z pěti, tentokrát z barevných kamer, k vytvoření 3D modelu obličeje osoby, kterou chceme identifikovat. Tyto snímky se poté předají programu starajícího se o samotnou rekonstrukci.

Po získání modelu můžeme přistoupit k poslednímu kroku zabývajícím se získáváním dat o osobě. A to extrakci příznaků z vytvořeného modelu obličeje. Výstupem tohoto kroku jsou pozičně normalizované horizontální řezy obličejem, kde prostřední řez je vždy na středu (tedy procházející přes nos).

4.4.2 Zpracování příznaků

Samotná identifikace je založena na porovnávání příznaků získaných z aktuálně vytvořeného 3D modelu obličeje a referenčních příznacích uložených v systému biometrické brány. Pokud nemáme žádné uložené příznaky o dané osobě, je možné využít stejný postup získání dat jako je popsán v podkapitole 4.4.1 a namísto pokračování v identifikaci osoby je uložit.

Pokud tedy již máme referenční modely uložené a chceme provést samotnou identifikaci musíme porovnat získané příznaky s veškerými uloženými referenčními příznaky. V momentálním řešení je pouze prováděno jednoduché porovnání založené na kvadratické odchylce jednotlivých bodů (pokud získaný model i referenční model tento bod obsahuje) v jednotlivých řezech. Výsledná chyba je poté vydělena počtem porovnaných bodů, jelikož při převzorkování nemusí být vytvořen každý bod (důvod tohoto jevu je vysvětlen na konci podkapitoly 4.2.9).



Obrázek 4.4: Porovnání řezů modelů dvou odlišných osob. Zobrazený je jen jeden řez (procházející přes špičku nosu) z 21 vytvořených řezů.

Finální určení o koho se jedná je provedeno na základě průměrné chyby při porovnání, tedy čím menší průměrná chyba, tím větší pravděpodobnost, že se opravdu jedná o danou osobu. V případě, že biometrickou bránu může použít osoba, která není zavedena v databázi, tak lze nastavit určitá hranice průměrné chyby určující, že se nejedna o žádnou osobu ze systému.

4.4.3 Možnosti zpřesnění identifikace osob

Jak již bylo uvedeno v předchozí kapitole, momentální postup při závěrečné identifikaci je jen jednoduchá metoda porovnání dvou modelu. Tento způsob ovšem lze vylepšit.

Jedním z problémů může být samotné vytváření 3D modelu obličeje. Použitý nástroj není přímo uzpůsobení na přímou tvorbu obličeje, ale na vytváření různorodých objektu, kde se ještě počítá s vytvořením celého 3D modelu (v našem případě celé hlavy a né pouze tváře). Takže i přes snahu uzpůsobit nastavení průběhu identifikace pro lidský obličej vznikají kolem tváře určité artefakty, které mohou na okrajích zkreslovat model. Z toho důvodu by byla možnost při porovnávání jednotlivých řezů využít určitého váhování chyby. Takže místům na okrajích modelu, tedy v horních a spodních řezech plus na okrajích každého řezu, bude přiřazena menší váha. Tato váha bude způsobovat, že výsledná chyba porovnání modelu bude klást větší důraz na podobnost ve středu modelu než na okrajích.

Další chyba, která může vznikat při vytváření modelu je mírné zkreslení měřítka nebo natočení obličeje. Řešení v tomto případě může být poměrně jednoduché, přestože výpočetně náročné. Při porovnávání vůči referenčnímu modelu je možné trochu upravit měřítko jednotlivých os anebo natočení řezu za pomocí matic a snažit se najít měřítko a natočení,

co bude nejvíce odpovídat referenčnímu modelu. Jediným problémem při testování této úpravy je možnost zvýšení podobnosti se špatnou osobou, kde skutečná osoba může mít například užší obličej, který se díky tomuto změní.

Jiná možnost zpřesnění identifikace osob se netýká zpřesnění modelu anebo úpravy extrahovaných příznaků, ale celkové změny v postupu získávání příznaků. Namísto provádění řezu obličeje se budou jednotlivé modely porovnávat na základě geometrie obličeje. Po nalezení špičky nosu se tento bod použije jako referenční bod pro celý model. Poté je na řadě těžší část, a to nalezení ostatních klíčových bodů na obličeji (koutky úst, očí, obočí apod.). Po získání všech těchto bodů lze zjistit eukleidovskou vzdálenost bodů a využít tyto hodnoty pro identifikaci osob.

Poslední vylepšení se týká využití termokamery. V momentálním řešení je použita jednoduchá termokamera s poměrně malým rozlišením. Nicméně za předpokladu využití novějšího modelu můžeme získat větší rozlišení snímku i přesnou teplotu v kelvinech. S touto vyšší přesností lze provést i rozpoznání osoby přímo ze snímku termokamery a využít tak tento výsledek k přesnějšímu rozhodnutí o koho se jedná.

Kapitola 5

Experimenty na systému biometrické brány

Pro vyzkoušení úspěšnosti biometrické brány byly vybrány určité experimenty k jejímu otestování. První prováděný experiment bude jednoduché porovnávání jedna ku jedné, z čeho se poté skládá i finální způsob práce biometrické brány. Další experiment je zaměřený na podobnost různých 3D modelů stejné osoby a jejich odchylky.

5.0.1 Porovnání dvou modelů osob

Ke správnému fungování biometrické brány je nutnost mít dobrou úspěšnost v porovnávání. Při vlastní činnosti biometrické brány je porovnáván model obličeje vyfocené osoby postupně se všemi referenčními modely. Tedy jde vždy o porovnání pouze dvou modelů a určení výsledné chyby, podle které se vybere nejpodobnější referenční model a tedy i identita.

Nicméně k pochopení, co funguje pro rozhodování a co nefunguje, je dobré se nejprve podívat a vizuálně porovnat testované modely.

Vizuální porovnání dvou modelů

Porovnávání v této podkapitole bude ze dvou uvedených modelů, které jsou zobrazeny na obrázku 5.1.

Obrázek 5.1: Modely dvou osob, mezi kterými bude prováděna identifikace.

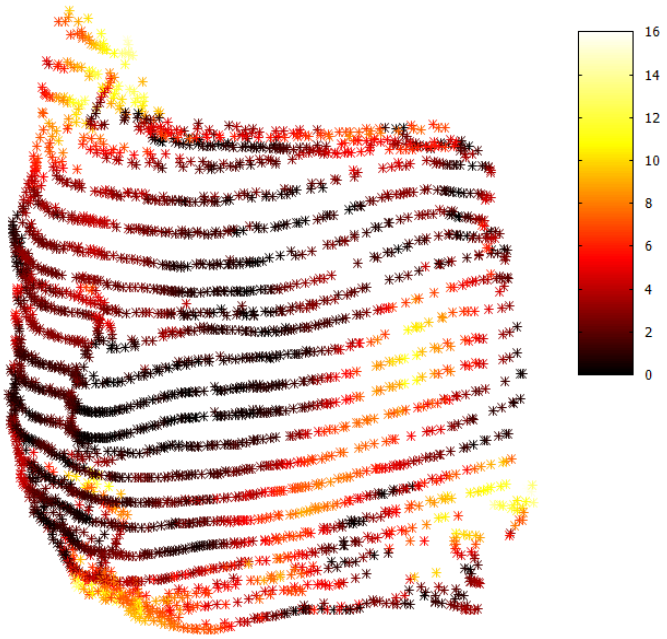
Jak je vidět na obrázku 5.1, tak tyto dva modely jsou odlišné v šířce obličeje, která by měla jít jednoduše rozeznat. Ostatní části jsou docela podobné, ale v případě jiných modelů mohou být patrné i další rozdíly (hlavně rozdíly mezi tváří muže a ženy). Dalšími velkými rozdíly mohou být speciální případy jako dlouhé vlasy, vousy, brýle apod. V této práci nejsou tyto speciální případy řešeny, a tedy budou mít velký vliv na výslednou identifikaci biometrické brány.

Porovnání modelů z pohledu biometrické brány

Pro porovnání dvou modelů v systému biometrické brány je jeden model určen jako referenční a poté je získaný model k referenčnímu porovnáván. Při tomto porovnání se pro každý shodný bod, který obsahují oba modely, spočítá kvadratický rozdíl. Při normální identifikaci se poté spočítá průměrná chyba, jelikož každé porovnání nemusí mít stejný počet bodů a vybere se jako výsledný model ten s nejnižší chybou vůči referenčnímu modelu.

Nicméně při porovnávání jen dvou modelů to nelze určit. Proto je zvolen jiný způsob zobrazení porovnání dvou modelů. Pro zobrazení se vybere testovaný model (tedy focené osoby) a každému bodu se přiřadí hodnota odpovídající chybě bodu od referenčního. Takto vykreslený model lze vidět na obrázku 5.2, kde jsou porovnány modely z obrázku 5.1.

Na těchto vykreslených bodech lze vidět, že oba modely jsou poměrně shodné okolo nosu, ale v určitých částech obličeje se liší. Vysoká chyba v bodech, které leží na okraji modelu, je způsobena nepřesností vytvořeného modelu z *FlowEngine*, jelikož tento nástroj není speciálně stavěn na rekonstrukci obličeje ze snímků kamery.



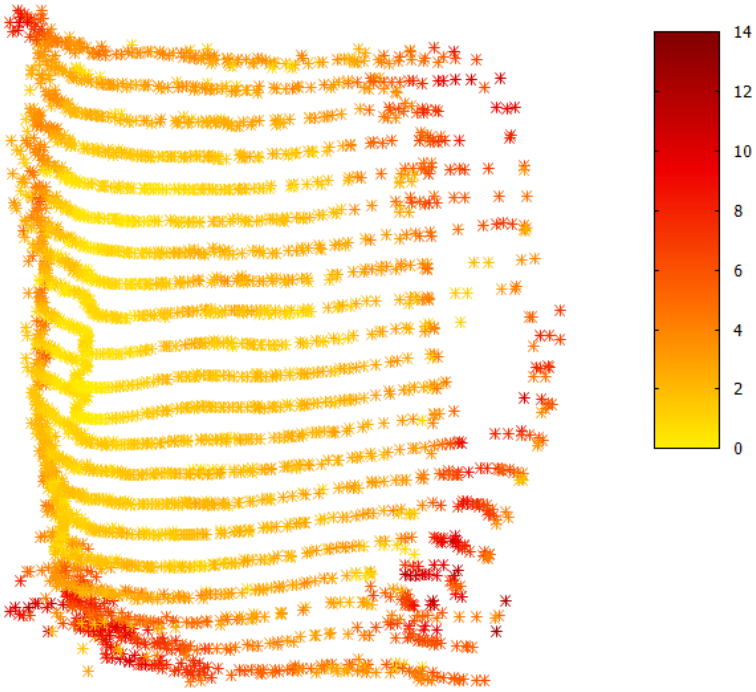
Obrázek 5.2: Model znázorňující rozdíl dvou modelů obličeje. Pozice bodů je určena podle původního modelu. Barva jednotlivých bodů odpovídá kvadratickému rozdílu dvou porovnávaných modelů. Černá barva je vysoká shoda, červená až bílá barva označuje větší rozdíl modelů.

5.0.2 Odchylka modelů stejné osoby

Další důležitý experiment k otestování brány je porovnat několik modelů stejné osoby, jelikož každý model vytvořený bránou má určitou odchylku. Tato odchylka by měla být dostatečně malá, aby systém focenou osobu poznal pokaždé stejně.

K ověření tohoto systému byly pořízeny 4 modely obličeje stejné osoby. Snímky pro tyto modely nebyly pořízeny v perfektních podmínkách, a tedy by měly více odpovídat reálnému použití. K zobrazení byla použita směrodatná odchylka, kde každý výsledný bod musel být obsažen alespoň ve 3 ze 4 modelů. Výsledné zobrazení bodů je na obrázku 5.3.

Z obrázku je patrné, že kolem středu obličeje, kde každý bod lze vidět z 4 nebo všech 5 kamer je odchylka téměř nulová (kolem špičky nosu). Nicméně, jak začíná ubývat počet snímků, ze kterých lze vidět bod, tak narůstá odchylka modelu. Bohužel jak bylo vidět na obrázku z předchozí podkapitoly (obrázek 5.2), tak hlavní místa, kde se jednotlivé osoby liší jsou právě místa, kde odchylka narůstá.



Obrázek 5.3: Zobrazení směrodatné odchylky různých modelů stejné osoby spočítané ze 4 modelů obličeje. Žlutá barva zobrazuje minimální odchylku v daném bodě a červená barva maximální.

5.0.3 Identifikace několika osob

Poslední prováděný experiment na biometrické bráně je její výsledná funkčnost, tedy identifikace osob. K tomuto experimentu byly použity čtyři osoby. Od každé osoby bylo vytvořeno pět 3D modelů obličeje, které byly následně využity pro otestování identifikace. Jako tyto modely byly vybrány pouze ty, kde úspěšně proběhla rekonstrukce celého obličeje.

U každé osoby byl první model určen jako referenční vzor pro biometrickou bránu. Zbylé čtyři modely od každé osoby se použily pro otestovaní identifikace, tedy celkem bylo provedeno 16 identifikací. Každá identifikace byla prováděna porovnáním kvadratické chyby

modelu vůči referenčním modelům. Referenční model s nejmenší kvadratickou chybou byl určen jako identita osoby.

Při tomto způsobu identifikace dopadlo 9 porovnání pozitivně a 7 negativně s výslednou úspěšností sytému 56,25 %. U 7 z 16 identifikací byla výsledná chyba porovnání modelu méně než 10 % od druhé nejpravděpodobnější osoby.

5.1 Výsledky testování a experimentů

Přestože systém biometrické brány ve výsledku tvoří ucelený celek, tak je lépe popsat testování a prováděné experimenty s jednotlivými částmi systému kvůli lepšímu pochopení příčiny nepřesností.

Jediná část, která dává smysl uvést jako celek je rychlost celé identifikace. Z pohledu normálního systému pro rozpoznávání není většinou nutné uvádět rychlost anebo nároky na výpočty, protože většinou jde o dopředu natrénovaný systém, kde není problém nechat učení i několik týdnů. Nicméně v tomto případě systém neobsahuje žádný algoritmus, který je nutný trénovat, ale samotná rekonstrukce zabírá velké množství výpočetního výkonu.

V momentální sestavě celý systém běží na MS Windows s poměrně drahým hardwarem. S 6 jádrovým procesorem běžící na taktovací frekvenci 4,9 GHz a dedikovanou grafickou kartou GTX 1060 od firmy Nvidia trvá celková identifikace do 30 s. Se slabším hardwarem je možné, že se celkový čas zpomalí až na čas okolo jedné minuty, ale focená osoba musí stát před biometrickým systémem jen prvních pár vteřin k pořízení snímků z kamer. Nicméně rychlost generovaní 3D modelu lze také zrychlit za mírnou cenu kvality.

Další možností je, kdy bychom měli několik biometrických bran, využití Raspberry Pi jako hlavní jednotku systému. Ten by pořídil snímky osob a odeslal je na vzdálený výpočetní server, který by provedl samotnou rekonstrukci a identifikaci. Následné výsledky by zaslal zpátky biometrické bráně, která provede úkony v závislosti na výsledku rozpoznávání.

Ohledně úspěšnosti systému, jak již bylo možné částečně pochopit z podkapitoly 4.4.3, zabývající se možnosti vylepšení výsledné identifikace, většina problému se týká procesu vytvoření 3D modelu obličeje. Ostatní části jsou úspěšné (zjištění osoby za pomocí termokamery) anebo závislé na kvalitě vytvořeného modelu.

5.1.1 Chyby při rekonstrukci modelu

Při pořizování snímků fotografií v ideálních podmínkách, tedy dostatečné a rozptýlené osvětlení, bílé pozadí bez předmětů a ideální nastavení vzdáleností kamer, se vytvoření modelu podařilo téměř ve všech případech. Nicméně v podmínkách, které více odpovídají využití biometrické brány, rekonstrukce často selhala a jakákoliv chyba v této části ve většina případů způsobila zkreslený model, tedy model se buď nevytvořil vůbec nebo se vytvořila pouze část obličeje. V obou případech se ve výsledku jedná o to, že nelze provést extrakci příznaků a následnou identifikaci.

Tato chyba hlavně nastává, protože systém *FlowEngine* je stavěn na obecnou rekonstrukci celého modelu a né jen přední části. Pokud je tedy na několika snímcích z kamer za focenou osobou nějaký předmět, systém předpokládá, že patří k focenému obličeji a vytvoří tento předmět i ve výsledném modelu. Takto vytvořený model je ale nepoužitelný pro následnou identifikaci.

5.1.2 Chyba rozpoznání modelu

Pokud dojde k správnému vytvoření modelu obličeje, výsledek identifikace dost záleží na tom, jak vypadají osoby, mezi kterými se snažíme rozpoznávat. Pokud mají osoby dostatečně rozdílnou stavbu obličeje, tak je systém úspěšný. Nicméně z důvodu využití horizontálních řezů a poměrně velké odchylky v okrajích modelu při rekonstrukci obličeje má systém problém rozeznat mezi lidmi s podobnou velikostí obličeje, kde profil tvořený řezem je téměř nerozeznatelný.

Kapitola 6

Závěr

Cílem této práce bylo vytvořit biometrickou bránu a její systém, který by na základě zachycení několika snímků z kamery vytvořil model dané osoby a provedl její identifikaci.

Tento cíl práce byl splněn i přes nečekané problémy, které při začátku i někdy v průběhu práce na systému nebyly zřejmé.

Návrh biometrické brány byl vytvořen z pěti barevných kamer, kde se za pomocí dostupných nástrojů vytvořil 3D model focené osoby. Samotná termokamera plnila roli kontroly před začátkem celého procesu. Výsledný návrh byl implementován na platformách Microsoft Windows, kde se nachází hlavní část implementace biometrické brány, a na zařízení Raspberry Pi k pořízení snímků z termokamery. Tedy samotná rekonstrukce obličeje probíhala na již zmíněném operačním systému MS Windows. Zde je i po rekonstrukci 3D modelu prováděna samotná extrakce příznaků, jejich normalizace a poté konečná identifikace focené osoby.

Výsledná úspěšnost biometrického systému je pod původní míru očekávání z několika důvodu, které byly zjištěny až v průběhu práce na tomto systému. Hlavní příčina tohoto nečekaného výsledku jsou nepřesnosti při vytváření samotného 3D modelu. Použitý systém je skvělý pro tvorbu modelů, nicméně není specializovaný na přesnou tvorbu obličeje. Toto spolu s né úplně vhodně zvolenými příznaky přispělo k poměrně nízké míře úspěšnosti na rozdíl od jiných systémů k identifikaci osob.

Nicméně samotná práce byla pro mě velkým přínosem v ohledu oblasti vestavěných systému a využívání externích zařízení ke shromažďování dat, kde jsem se naučil pracovat s různými typy zařízení.

Část na které bych rád pokračoval se týká změny získávání příznaků ze samotného modelu. S těmito přesnějšími údaji o modelu by se výrazně vylepšily výsledky identifikace osob za pomocí systému biometrické brány. Momentálně použitý způsob není zcela vhodný a jiné zamýšlené způsoby získávání informací z modelu obličeje byly příliš rozsáhlé pro současnou implementaci.

Mezi dlouhodobější cíle patří, najít nebo vytvořit jiný nástroj k získaný 3D modelu. Tento nástroj by měl být speciálně zaměřen na vytvoření 3D modelu lidského obličeje a díky tomu vylepšit celkovou kvalitu získaného modelu.

Literatura

[1] IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, Dec 2016: s. 1–3534.

[2] Arm Holdings: Cortex-A Series Programmer's Guide.
URL `http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.den0013d/index.html`

[3] Brunelli, R.; Poggio, T.: Face recognition: features versus templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, ročník 15, č. 10, Oct 1993: s. 1042–1052, ISSN 0162-8828, doi:10.1109/34.254061.

[4] Carlsson, G.: The structure of a Convolutional Neural Network. [Online], [cit. 1. 5. 2019].
URL
`https://www.ayasdi.com/blog/artificial-intelligence/using-topological-data-analysis-understand-behavior-convolutional-neural-networks/`

[5] Cburnett: A single master and a single slave on a Serial Peripheral Interface (SPI) bus. [Online], [cit. 1. 5. 2019].
URL `https://commons.wikimedia.org/wiki/File:SPI_single_slave.svg`

[6] Cyc: Svm max sep hyperplane with margin. [Online], [cit. 21. 1. 2019].
URL `https://commons.wikimedia.org/w/index.php?curid=3566688`

[7] Fogg, A.: A History of Deep Learning. [Online], [cit. 29. 4. 2019].
URL `https://www.import.io/post/history-of-deep-learning/`

[8] Fred the Oyster: USB Type-A receptacle, with numbered pins. [Online], [cit. 1. 5. 2019].
URL `https://commons.wikimedia.org/wiki/File:USB_Type-A_receptacle.svg`

[9] Gade, R.; Moeslund, T. B.: Thermal cameras and applications: a survey. *Machine Vision and Applications*, ročník 25, Jan 2014, ISSN 1432-1769, doi:10.1007/s00138-013-0570-5.
URL `https://doi.org/10.1007/s00138-013-0570-5`

[10] Heath, S.: *Embedded Systems Design*. Newton, MA, USA: Butterworth-Heinemann, druhé vydání, 2002, ISBN 0750655461.

[11] HGH Infrared Systems: What are the wavelength boundaries of infrared radiation? [Online], [cit. 5. 5. 2019].
URL https://www.hgh-infrared.com/FAQ/Infrared-Testing/What-are-the-wavelength-boundaries-of-infrared-radiation

[12] Hjelmås, E.; Kee Low, B.: Face Detection: A Survey. *Computer Vision and Image Understanding*, ročník 83, 09 2001: s. 236–274, doi:10.1006/cviu.2001.0921.

[13] Universal Serial Bus interfaces for data and power. Standard, International Electrotechnical Commission.

[14] Universal serial bus interfaces for data and power - Part 2-1: Universal Serial Bus Specification, Revision 2.0. Standard, International Electrotechnical Commission, 09 2015.

[15] Jain, A.; Bolle, R.; Pankanti, S.: *Biometrics: Personal Identification in Networked Society*. The Springer International Series in Engineering and Computer Science, Springer US, 2006, ISBN 9780306470448.

[16] Jain, A. K.; Ross, A.; Prabhakar, S.: An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, ročník 14, č. 1, Jan 2004: s. 4–20, ISSN 1051-8215, doi:10.1109/TCSVT.2003.818349.

[17] Labati, R. D.; Genovese, A.; Muñoz, E.; aj.: Biometric Recognition in Automated Border Control: A Survey. *ACM Comput. Surv.*, ročník 49, č. 2, Červen 2016: s. 24:1–24:39, ISSN 0360-0300, doi:10.1145/2933241.
URL http://doi.acm.org/10.1145/2933241

[18] Lanh, T. V.; Chong, K.; Emmanuel, S.; aj.: A Survey on Digital Camera Image Forensic Methods. In *2007 IEEE International Conference on Multimedia and Expo*, July 2007, ISSN 1945-7871, s. 16–19, doi:10.1109/ICME.2007.4284575.

[19] Lukáš, B.: Lineární klasifikátory, 05 2017.
URL https://www.fit.vutbr.cz/study/courses/IKR/public/prednasky/04_lin_klasifikatory/lin_klasifikatory.pdf

[20] Martin, A.; Doddington, G.; Kamm, T.; aj.: The DET curve in assessment of detection task performance. 1997, s. 1895–1898.

[21] Motorola, Inc.: SPI Block Guide V03.06. [Online], [cit. 29. 4. 2019].
URL https://web.archive.org/web/20150413003534/http://www.ee.nmt.edu/~teare/ee308l/datasheets/S12SPIV3.pdf

[22] Pantic, M.; Booth, J.; Martinez, B.; aj.: Detection of static geometric facial features. [Online], [cit. 20. 1. 2019].
URL https://ibug.doc.ic.ac.uk/research/detection-static-geometric-facial-features

[23] Petrovska-Delacrtaz, D.; Chollet, G.; Dorizzi, B.: *Guide to Biometric Reference Systems and Performance Evaluation*. Springer Publishing Company, Incorporated, první vydání, 2009, ISBN 1848002912, 9781848002913.

[24] Reddy, M.: Appendix B1. Object Files. [Online], [cit. 24. 4. 2019].
URL http://www.martinreddy.net/gfx/3d/OBJ.spec

[25] TRANSMISSION CONTROL PROTOCOL. Standard, DARPA INTERNET PROGRAM, 09 1981.

[26] Rouse, M.: embedded system. [Online], [cit. 7. 5. 2019].
URL
https://internetofthingsagenda.techtarget.com/definition/embedded-system

[27] SafeSPI: Overview of SafeSPI. [Online], [cit. 7. 5. 2019].
URL https://safespi.org/overview/

[28] Sandoval Orozco, A.; Hernandez-Castro, J.; García Villalba, L.; aj.: Smartphone image acquisition forensics using sensor fingerprint. *IET Computer Vision*, ročník 9, 06 2015, doi:10.1049/iet-cvi.2014.0243.

[29] Schmidhuber, J.: Deep Learning in Neural Networks. *Neural Netw.*, ročník 61, č. C, Leden 2015: s. 85–117, ISSN 0893-6080, doi:10.1016/j.neunet.2014.09.003.
URL http://dx.doi.org/10.1016/j.neunet.2014.09.003

[30] Skymind Inc.: A Beginner's Guide to Convolutional Neural Networks (CNNs). [Online], [cit. 29. 4. 2019].
URL https://skymind.ai/wiki/convolutional-network

[31] Sundaram, M.; Mani, A.: *Face Recognition: Demystification of Multifarious Aspect in Evaluation Metrics*. 07 2016, ISBN 978-953-51-2421-4, doi:10.5772/62825.

[32] Taylor, S.: CCD and CMOS Imaging Array Technologies: Technology Review. 5 1998.
URL https://www.microsoft.com/en-us/research/publication/ccd-and-cmos-imaging-array-technologies-technology-review

[33] Yoshitomi, Y.; Miyaura, T.; Tomita, S.; aj.: Face identification using thermal image processing. In *Proceedings 6th IEEE International Workshop on Robot and Human Communication. RO-MAN'97 SENDAI*, Sep. 1997, s. 374–379, doi:10.1109/ROMAN.1997.647015.

[34] Zeng, D.; Zhao, Q.; Long, S.; aj.: Examplar Coherent 3D Face Reconstruction from Forensic Mugshot Database. *Image Vision Comput.*, ročník 58, č. C, Únor 2017: s. 193–203, ISSN 0262-8856, doi:10.1016/j.imavis.2016.03.001.
URL https://doi.org/10.1016/j.imavis.2016.03.001