FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Autentizace uživatelů pomocí oční duhovky
Student:	Pavla Louthánová
Vedoucí:	Ing. Josef Kokeš
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2021/2022

Pokyny pro vypracování

1) Seznamte se s dostupnými technologiemi pro autentizaci uživatelů pomocí biometrie.
2) Zaměřte se rozpoznávání oční duhovky. Popište současný stav vědění, metody, techniky, postupy.
3) Navrhněte systém umožňující rozpoznávání uživatelů pomocí oční duhovky. Soustřeďte se na minimalizaci ceny a použití běžně dostupných komponent.
4) Naprogramujte základní funkce pro realizaci rozpoznávání podle duhovky jako knihovnu a demonstrační program k ní.
5) Analyzujte bezpečnostní aspekty svého řešení: Spolehlivost rozpoznání vzhledem k měnícím se parametrům, zneužitelnost uložené informace, odolnost vůči útočníkům.
6) Diskutujte své výsledky.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 18. ledna 2021 v Praze.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Autentizace uživatelů pomocí oční duhovky

Pavla Louthánová

Katedra počítačových systémů
Vedoucí práce: Ing. Josef Kokeš

6. května 2021

Poděkování

Tímto bych ráda poděkovala vedoucímu své práce, Ing. Josefu Kokešovi, za jeho vedení, cenné rady a veškerý čas, který mi při zpracování této práce věnoval.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 6. května 2021 . . . . . .

Odkaz na tuto práci

Louthánová, Pavla. *Autentizace uživatelů pomocí oční duhovky.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2021.

Abstrakt

Práce se zabývá rozpoznáváním uživatelů pomocí oční duhovky. Náplní rešeršní části práce je seznámení s biometrickými metodami a systémy pro autentizaci uživatelů. Následně se práce zaměřuje na rozpoznávání oční duhovky. V praktické části práce je s přihlédnutím na minimalizaci ceny a použití běžně dostupných komponent navrhnut systém umožňující snímání oční duhovky a vytvoření vlastní databáze snímků. Dále jsou implementovány jednotlivé fáze rozpoznávání, datové úložiště a demonstrační program. Na závěr je diskutována časová náročnost, spolehlivost a bezpečnost implementace.

Klíčová slova biometrie, rozpoznávání duhovky, biometrická identifikace, biometrická verifikace, Python, MongoDB, Raspberry Pi

Abstract

The work deals with the recognition of users using their irises. The research part of the thesis acquaintances the reader with biometric methods and systems for user authentication. Subsequently, the work focuses on the recognition of the iris. In the practical part of the work, taking into account the minimization of the price and the use of commonly available components, a system for scanning the iris and to create its own database of images is designed. Furthermore, the individual phases of recognition, data storage and demonstration program are implemented. Finally, the time required, reliability and security of implementation are discussed.

Keywords biometrics, iris recognition, biometric identification, biometric verification, Python, MongoDB, Raspberry Pi

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Lidé jsou schopni rozpoznávat jiné osoby podle obličeje, hlasu, způsobu chůze, typu písma či podpisu. Biometrie je technika, která umožňuje ověřit identitu jednotlivce pomocí jedné nebo více jeho jedinečných osobnostních charakteristik. Její výhodou je zvýšení úrovně zabezpečení pomocí identifikačních dat, která na rozdíl od hesel a karet nelze ztratit či zapomenout, protože přímo souvisejí s tělem nebo chováním jednotlivce.

Biometrické systémy byly před veřejností dlouho skrývány. Jednalo se totiž především o zařízení chránící tajemství. Příkladem byla kosmická střediska, vojenské jaderné laboratoře nebo řídící operační centrály. Teprve s expanzí výpočetní techniky došlo k jejich rozšíření i do civilní sféry.

Duhovka je barevnou částí oka, kterou lze pozorovat pouhým pohledem. Barva a textura duhovky jsou u každého jedince zcela jedinečné. Poskytují velké množství informací, které lze využít k biometrickým účelům.

Cílem teoretické části bakalářské práce je seznámit se s biometrickými metodami a následně se podrobněji zaměřit na biometrické rozpoznávání osob podle oční duhovky.

Cílem praktické části je navrhnout snímací systém s přihlédnutím na cenu a dostupnost komponent, implementovat základní funkce pro realizaci rozpoznávání osob podle oční duhovky, vytvořit demonstrační program a analyzovat bezpečnostní aspekty svého řešení.

Kapitola 1

Biometrie

Tato kapitola je rozdělena do dvou částí. V první části jsou popsány nejpoužívanější biometrické metody. Popis rozpoznávání oční duhovky je vynechán, jelikož je obsahem následující kapitoly. V druhé části je popsán základní princip obecného biometrického systému, hodnocení spolehlivosti a přehled potenciálně zranitelných míst.

1.1 Biometrické metody

Pojem biometrie pochází z řečtiny a je složen ze slov bios a metron. První slovo znamená život, druhé měřítko. Termín biometrie má v různých oborech odlišný význam. V biomedicínské oblasti biometrie označuje měření a statistickou analýzu biologických dat. V oboru informačních technologií je biometrie definována jako automatizované rozpoznávání jedinců na základě jejich charakteristických rysů. [1]

Biometrické metody jsou založené na automatizovaném měření a porovnávání biometrických charakteristik člověka. Biometrické charakteristiky, též nazývané biometriky, jsou měřitelné vlastnosti člověka, které jsou pro každého jedinečné. Lze je rozdělit do dvou kategorií – na anatomicko-fyziologické a behaviorální. [1]

Anatomicko-fyziologické biometrické charakteristiky jsou založené na vrozených rysech jedince. Jedná se o části lidského těla. Do této kategorie patří například otisk prstu, obličej, oční duhovka, oční sítnice, geometrie ruky, obraz krevního řečiště a DNA. Tyto biometrické vlastnosti jsou unikátní a časově stálé. [2]

Behaviorální biometrické charakteristiky odrážejí specifické rysy lidského chování. Do této kategorie lze zařadit například hlas, podpis, chůzi a dynamiku stisku kláves. Tyto vlastnosti jsou sice jedinečné, avšak mohou být vlivem různých faktorů časově nestálé. Jsou poměrně jednoduše ovlivnitelné, každé nasnímání dané biometrické vlastnosti může vést k naprosto odlišné

sadě biometrických vzorků. Používají se proto v praxi méně často než metody anatomicko-fyziologické. [2]

Ne všechny anatomicko-fyziologické nebo behaviorální vlastnosti člověka lze považovat za biometriky. Pro funkčnost biometrického systému a jeho praktické nasazení je důležité, aby vybraná biometrická vlastnost splňovala v co možná největší míře určitá kritéria. Dle [3, 4] mezi základní kritéria patří:

- Jedinečnost: Vlastnost musí být dostatečně unikátní, aby bylo možné od sebe odlišit dva jedince s vysokou spolehlivostí a přesností.
- Univerzálnost: Vlastnost musí být měřitelná u co možná největší množiny osob.
- Stálost: Charakteristiky, na kterých je založená daná vlastnost, musí být neměnné v čase.
- Měřitelnost: Biometrická vlastnost musí být měřitelná.
- Přijatelnost: Vlastnost musí být snadno a pohodlně měřitelná. Snímání, zpracování, uchovávání a vyhodnocování biometrických údajů by mělo být přijatelné pro vysoké procento lidí.

Tabulka 1.1 porovnává základní biometrické metody na základě výše uvedených vlastností. Každá metoda je ohodnocena mírou splnění dané vlastnosti, symbol (+) označuje míru vysokou, (0) reprezentuje míru střední a (−) značí míru nízkou.

Tabulka 1.1: Základní biometrické metody a jejich charakteristiky [5]

Biometrická metoda	Jedinečnost	Univerzálnost	Stálost	Měřitelnost	Přijatelnost
Obličej	−	+	0	+	+
Otisk prstu	+	0	+	0	0
Geometrie ruky	0	0	0	+	0
Krevní řečiště ruky	0	0	0	0	0
Oční duhovka	+	+	+	0	−
Oční sítnice	+	+	0	−	−
Podpis	−	0	−	+	+
Hlas	−	0	−	0	+

1.1.1 Rozpoznávání podle otisku prstu

Otisk prstu je tvořen kresbou papilárních linií vytvářející určitou grafickou podobu. Jedná se o zvrásnění kůže, která jsou formována během embryonálního vývoje. Tento vzor zůstává po celý život jedince relativně neměnný. S přibývajícím věkem se sice mění rozměry prstů, ale struktura linií zůstává stejná. Papilární linie jsou obnovovány dorůstáním kůže, nemohou tak být jednoduše

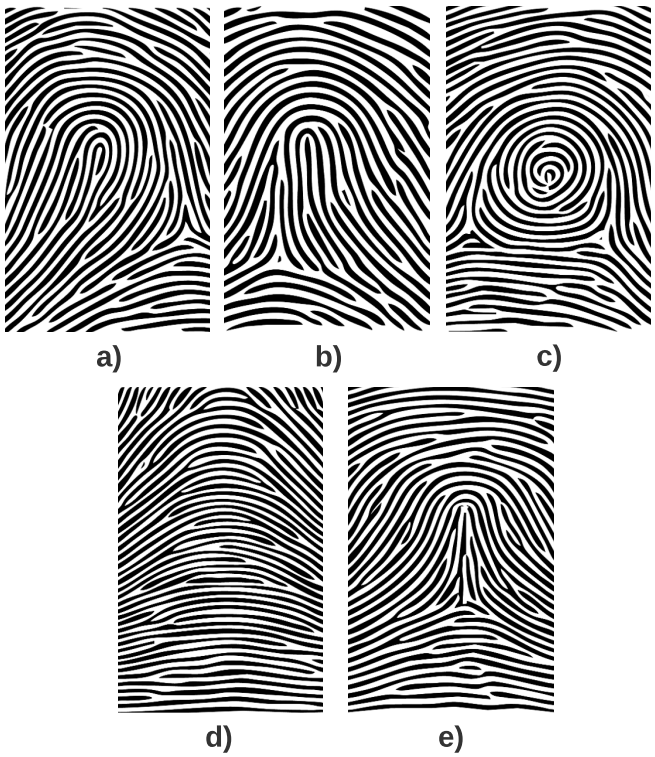
pozměněny či odstraněny. Pokud ovšem dojde k poškození epidermální vrstvy kůže, pak již na tomto místě k obnově papilárních linií nedojde. [6]

Vzor tvořený papilárními liniemi jednoznačně určuje fyzickou identitu člověka, lze tak na jeho základě rozlišovat jedince mezi sebou. Identifikace osob vyžaduje porovnání otisku prstu s velkým množstvím otisků uložených v databázi. Tento proces je velice výpočetně náročný. K rychlejšímu porovnávání slouží klasifikace otisků prstů podle jejich typické kresby, která je nazývána třídou otisku prstu. Otisky prstů jsou rozděleny do příslušných tříd. Porovnávání je pak provedeno pouze v podmnožině databáze, která odpovídá příslušné třídě. Mezi základní třídy patří oblouk, smyčka a vír, z nichž jsou odvozeny další třídy, jako je klenutý oblouk, pravá smyčka, levá smyčka, případně dvojitá smyčka. [1]

Otisky prstů jsou mezi sebou rozlišovány na základě speciálních útvarů, tzv. markantů, které tvoří papilární linie. K základním markantům patří ukončení, vidlička, očko, hák, křížení, boční kontakt, bod, interval, smyčka, most. Daktyloskopické metody využívané v kriminalistice používají velké množství těchto markantů. Naproti tomu přístupové systémy používají pouze ukončení papilární linie a vidličku. [2]

V biometrických systémech se pro nasnímání otisků používají různé druhy kontaktních a bezkontaktních snímačů. Jedná se například o technologii optickou, kdy je prst přiložen na osvětlenou skleněnou plochu senzoru a nasnímán kamerou. V případě technologie kapacitní je senzor tvořen maticí malých vodivých plošek. Při snímání otisku se pak využívá rozdílu kapacity mezi deskou snímače a povrchem prstu. Podstatou ultrazvukové technologie je rotující ultrazvukový vysílač a přijímač, který odrazem ultrazvukových vln snímá otisk prstu. [1]

Prvním krokem při zpracování zaznamenaného otisku prstu je potlačení nežádoucích částí obrazu, tzv. šumu, a zvýraznění papilárních linií. Obraz otisku je rozdělen na malé části, ve kterých je u každé papilární linie určen její směr. Tento filtr je následně aplikován na každý bod obrazu. Tím jsou zvýrazněny všechny obrazové body, které se nacházejí ve směru papilární linie ve stejné oblasti a naopak potlačeny body, které jsou orientovány jiným směrem. Tímto je odstraněn nežádoucí šum. Následuje binarizace obrazu, kdy je původních 256 odstínů šedé barvy převedeno do dvou binárních hodnot, nesoucích význam černé a bílé barvy. Papilární linie jsou reprezentovány černou barvou, pozadí kresby papilárních linií bílou. Posledním krokem předzpracování obrazu je skeletizace, ztenčení papilárních linií na tloušťku jednoho obrazového bodu. Dalším krokem je detekce a extrakce markantů. Detekují se dva základní typy – ukončení papilární linie a vidlička. Ostatní typy markantů jsou kombinací těchto dvou základních typů. Ke každému markantu se ukládají údaje o pozici (souřadnice x a y), typu (ukončení nebo vidlička) a orientaci (směr papilární linie). Výsledek extrakce markantů je porovnán s uloženou šablonou z databáze. [1]



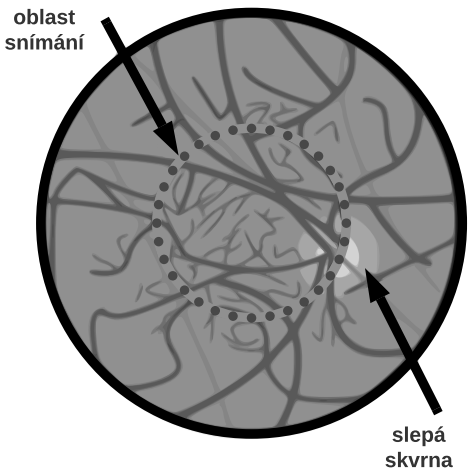
Obrázek 1.1: Třídy otisků prstů: a) levá smyčka, b) pravá smyčka, c) vír, d) oblouk, e) klenutý oblouk [7]

1.1.2 Rozpoznávání podle oční sítnice

Sítnice není pozorovatelná pouhým pohledem, nachází se v zadní části oka. Obsahuje buňky citlivé na světlo, tzv. tyčinky a čípky. Tyčinky detekují intenzitu světla a umožňují tak černobílé vidění. Čípky detekují barvy a zprostředkovávají barevné vidění. Na sítnici jsou pozorovatelné dva významné body – žlutá a slepá skvrna. Slepá skvrna je místem, kde do oka ústí zrakový nerv a neobsahuje žádné světločivé buňky. Žlutá skvrna je místem nejostřejšího vidění, obsahuje největší množství čípků. Sítnice je vyživována pomocí cévnatky, což je vrstva mezi sítnicí a bělimou, která obsahuje cévy a pigment absorbující nadbytek světla. [8]

Pro snímání sítnice se používá speciální kamera. Sítnice je osvětlena paprskem infračerveného světla, který je částečně odražen zpět a zaznamenán kamerou. Při osvětlení se sítnice jeví jako téměř průhledná. Pro rozpoznávání osob se využívá odrazu vzoru cév v cévnatce, která se nachází za sítnicí. Pro usnadnění snímání slouží fixační bod, který uživatel v průběhu snímání

sleduje. Výsledkem je kruhový snímek vzoru cév, ze kterého se dále zpracovává pouze prstencová oblast (obrázek 1.2). Šablona sítnice je reprezentována jako pole čísel, která reprezentují kontrast rovnoměrně rozmístěných bodů na nasnímaném kruhu. Při snímání může mít uživatel mírně pootočenou hlavu, proto je použit rotační algoritmus, který posunuje data a hledá nejlepší shodu nasnímaného vzorku s uloženým referenčním záznamem. [2]



Obrázek 1.2: Obraz sítnice [2]

1.1.3 Rozpoznávání podle geometrie ruky

K rozlišení jedinců mezi sebou se využívá kombinace rozměrů délky, šířky, tloušťky a tvaru prstů. Od dospělosti se identifikační charakteristiky nemění. Případné změny mohou nastat změnou tloušťky prstů a dlaně, nebo mohou být způsobeny některými onemocněními či úrazy. [1]

Uživatel položí ruku na plochu skeneru, která je opatřena speciálními fixačními kolíky tak, aby při každém snímání byla poloha ruky pokud možno stejná. Následně je kamerou nasnímán černobílý obraz siluety ruky. Jeden obraz je snímán ze shora kolmo na rovinu snímací desky. Druhý obraz je snímán zboku pomocí postranního zrcadla. Skener snímá pouze siluetu dlaně s prsty, ignoruje délku nehtů, neboť se v čase velmi rychle mění a ovlivňuje tak měřené charakteristiky. Plocha skeneru je tvořena podložkou z leštěného materiálu, který odráží dopadající světlo. Tím je zvýšen kontrast mezi rukou a podložkou, což značně usnadňuje separaci ruky od pozadí. V případě použití přídavného zrcadla pro nasnímání boční siluety ruky je reflexní podložka umístěna i na boční snímací stěnu. Naměřené rozměry ruky jsou konvertovány

do biometrické šablony. Referenční šablona vznikne jako aritmetický průměr trojího snímání, což eliminuje drobné nepřesnosti umístění ruky. Při verifikaci se porovnávají vzdálenosti předem určených bodů, jejichž počet a umístění záleží na konkrétním biometrickém zařízení. [2]

Tato biometrická metoda neposkytuje příliš mnoho informací, proto je používána výhradně v komerčně-bezpečnostní sféře v režimu verifikace a nelze ji používat pro identifikační účely [2]. Mohlo by totiž snadno dojít k záměně identity s jinou osobou. Více informací o verifikaci a identifikaci lze nalézt v části 1.2.2.

1.1.4 Rozpoznávání podle krevního řečiště ruky

Lidská ruka je protkána sítí cév. Jejich rozmístění je specifické pro každého jedince. Pro biometrické účely lze využít krevní řečiště na hřbetu ruky, na dlani ruky nebo v prstech rukou.

Ruka je osvětlena infračerveným zdrojem světla, které je pohlcováno hemoglobinem v cévách a dochází tak k jejich zvýraznění. K nasnímání je použita monochromatická CCD kamera, která je citlivá na blízké infračervené záření. Existují dvě metody snímání. Buď je kamera spolu se světelným zdrojem umístěna na stejné straně ruky, pak se jedná o tzv. reflexivní metodu, nebo je ruka prosvícena, v tomto případě je ruka vložena mezi zdroj světla a kameru a jedná se o tzv. transmisivní metodu. [1]

Po nasnímání obrazu krevního řečiště ruky je obraz zpracován. Nejprve je oblast nasnímané ruky segmentací oddělena od pozadí. Poté je třeba oddělit cévy od pozadí, odstranit šum a neostré hrany. Výsledkem je binární obraz sítě cév ze kterého je vygenerována biometrická šablona. [2]

1.1.5 Rozpoznávání podle obličeje

Rozpoznávání osoby na základě obličeje je pro člověka přirozeným způsobem identifikace, kterého využívá běžně v každodenním životě při styku s jinými osobami. Lidský obličej je jedinečný, avšak jeho rozpoznávání může být ovlivněno celou řadou faktorů. Jedná se například o mimiku, změnu účesu, úpravu vousů, make-up, brýle, pokrývky hlavy, změnu osvětlení, úhel snímání nebo stárnutí. Existuje velké množství metod a algoritmů pro rozpoznávání založené na podobě lidské tváře.

Metoda založená na rozpoznávání obličeje z 2D snímků je nejrozšířenější. Snímání probíhá kamerou ve viditelném světle. Prvním krokem je detekce a lokalizace obličeje v rámci obrazu. Nalezený obličej je následně normalizován, čímž dojde ke kompenzaci různého osvětlení, natočení hlavy, pozici hlavy a velikosti hlavy. V dalším kroku jsou extrahovány rysy pomocí filtrace či statistické analýzy. Nakonec je vyhodnocena podobnost se šablonou nebo sadou šablon. [1]

Metoda založená na rozpoznávání obličeje z 3D snímku používá speciální snímací zařízení. Na rozdíl od 2D je pro každý bod obrazu uložená informace o jeho hloubce. Získaný 3D obraz je třeba normalizovat. Normalizace probíhá přes detekci klíčových bodů, jimiž jsou koutky očí a špička nosu. Po jejich správné detekci lze model transformovat do výchozí polohy, ve které se předpokládá vysoká míra korelace mezi dvěma modely stejného obličeje. Nakonec jsou aktuální data porovnána s referenční šablonou uloženou v databázi. [1]

Další možností je rozpoznávání obličeje na základě termosnímku. Snímky jsou pořizovány v infračerveném světle pomocí speciálního zařízení, termokamery. Výstupem jsou pak obrázky termomap obličeje, které jsou založené na rozložení tepla v obličeji a jeho vyzařování do okolí. Rozdíly teplot jsou vyjádřeny pomocí barev, které dle teploty utvářejí obrazce. V termomapách se hledají pozice očí, nosu, úst a tvar obličeje. Dalším krokem je překryv obou termoobličejů a jejich zarovnání. V poslední části se hledá podobnost mezi snímky. Rozpoznávání pak probíhá na základě porovnávání těchto tvarů obrazců. Tato technologie je nezávislá na vnějším osvětlení, při kterém je tvář snímána. Teplota obličeje se může měnit působením různých vlivů, rozložení teplotních ploch však zůstává obdobné. [2]

1.1.6 Rozpoznávání podle hlasu

Lidský hlas je tvořen v hrtanu, kde vydechovaný vzduch naráží do napnutých hlasivek a rozechvívá je. Díky vibraci hlasivek a střídavému rozevírání a zavírání hlasové štěrbiny je v hrtanu tvořen zvuk. Jeho modifikací na podkladě rezonance v dutině hrtanu, úst, nosu, vedlejších nosních dutin a za použití artikulačních svalů tváří, jazyka, dásní, zubů a rtů, dochází k tvorbě hlásek lidské řeči. [9]

Hlas je nasnímán mikrofonem, zpracován a následně rozpoznáván. Systémy pro rozpoznávání hlasu mohou být rozděleny podle typu textu, který uživatel při snímání vyslovuje, na systémy textově závislé, s textovou výzvou a textově nezávislé. Textově závislé systémy využívají stejnou část textu pro registraci i pro následné rozpoznávání. V případě systémů s textovou výzvou není sekvence slov, které mají být vysloveny, uživateli předem známá. Systém požádá uživatele o vyslovení náhodně vybrané sekvence slov, poté provede rozpoznávání obsahu řeči, aby si ověřil, že uživatel opravdu řekl očekávanou sekvenci slov. Pokud je rozpoznání řeči úspěšné, proběhne identifikace mluvčího podle hlasu. U textově nezávislých systémů nejsou kladena žádná omezení na text, který je uživatelem vyřčen, není tedy předem známo, co uživatel vysloví. [2]

1.1.7 Rozpoznávání podle podpisu

Obecně lze rozdělit systémy rozpoznávající osoby podle podpisu na on-line systémy a off-line systémy. Pro rozpoznávání podpisu je využíváno statických nebo dynamických vlastností podpisu.

Off-line systémy využívají statických vlastností podpisu a je uchováván pouze výsledek psaní. Podpis je napsán na papír a následně naskenován nebo nasnímán kamerou. Po nasnímání je podpis předzpracován. Binarizací je obraz podpisu převeden z odstínů šedi do binární podoby. Vyhlazováním je z obrazu odstraněn šum, normalizací je obraz převeden do určitého definovaného měřítka. Nakonec je podpis skeletizován na šířku jednoho obrazového bodu, čímž vznikne základní kostra podpisu. Srovnání získaného vzorku s referenčním vzorkem pak probíhá na základě porovnání tvaru podpisu. Mezi statické charakteristiky podpisu patří například začátky a konce jednotlivých částí podpisu, křížení, uzavřené oblasti, tah směrem vzhůru, křivky a smyčky. [2]

On-line systémy získávají data v reálném čase pomocí tabletu či pera. Tyto systémy využívají statických i dynamických vlastností podpisu. Kromě obrazové podoby podpisu je zaznamenán také tlak pera, průběh a rychlost psaní. [2]

1.2 Biometrické systémy

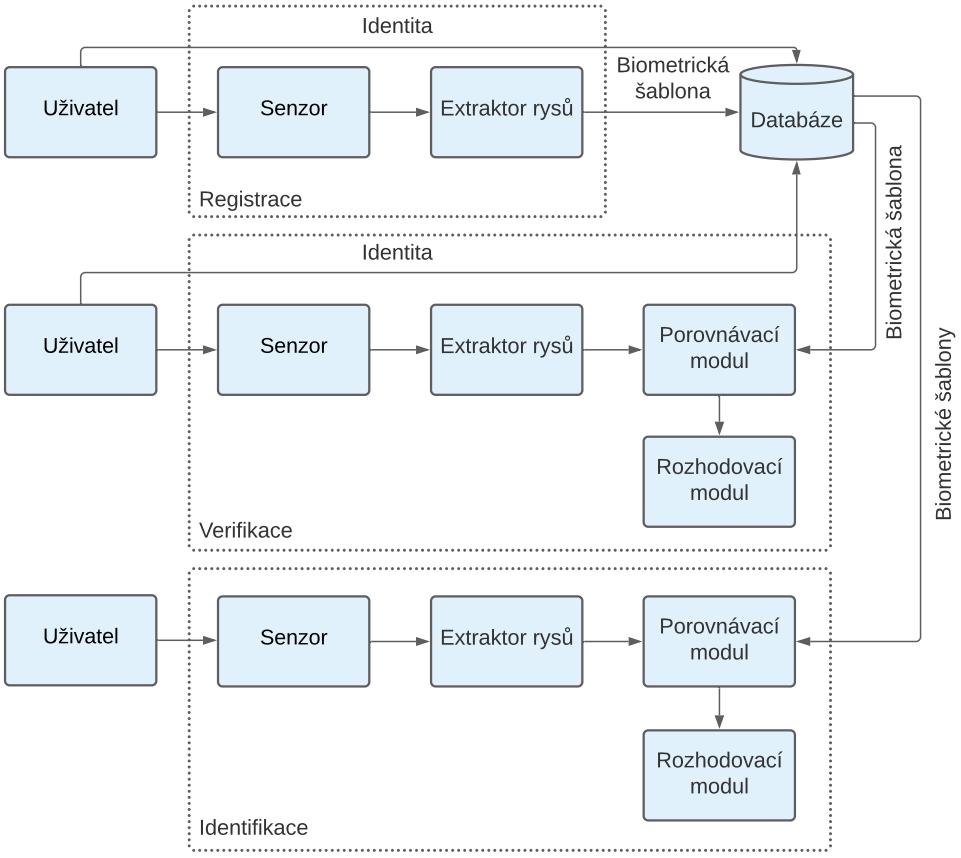
Biometrické systémy umožňují automatizované rozpoznávání osob na základě jejich charakteristických rysů. Rozpoznávání osob je založeno na jednoznačné identitě jedince. Je důležité rozlišovat mezi identitou fyzickou a elektronickou. Fyzická identita je definována vzhledem a chováním člověka, které jsou pro každého naprosto unikátní. Avšak elektronických identit může mít jedinec více. Jedná se například o on-line účty a identifikační karty. [1]

Autentizace je proces ověření identity. Identitu je možné prokázat třemi základními způsoby, tzv. autentizačními faktory. Prvním z nich je znalost. Metoda je postavená na znalosti tajné informace, která je známá pouze oprávněné osobě. Jedná se například o znalost hesla nebo PINu. Druhým faktorem je vlastnictví. Uživatel vlastní nějaký technický prostředek. Může jím být čipová karta nebo klíč. Posledním faktorem je biometrie. Jedná se o identifikaci na základě biometrických charakteristik člověka. Příkladem může být otisk prstu nebo oční duhovka. Každý z uvedených autentizačních faktorů má své výhody a nevýhody. Za účelem dosažení vyšší úrovně bezpečnosti se v praxi faktory často vzájemně kombinují, jedná se o tzv. vícefaktorovou autentizaci.

1.2.1 Komponenty biometrického systému

Mezi postupy biometrického zpracování jednotlivých biometrických charakteristik existují společné rysy, které lze zobecnit. Na obrázku 1.3 je znázorněno schéma obecného biometrického systému, který je složen z následujících základních částí:

- Biometrický senzor: Slouží k získání biometrického vzorku.
- Extraktor markantů: Zde je vzorek nasnímané biometrické vlastnosti zpracován. Jsou extrahovány biometrické markanty na jejichž základě je vytvořena biometrická šablona.
- Porovnávací modul: Porovnává právě získanou šablonu s jednou šablonou či více šablonami z databáze. Výsledkem je skóre porovnání.
- Rozhodovací modul: Zde dochází k rozhodnutí na základě získaného skóre porovnání a nastaveného prahu. Výsledkem je rozhodnutí o tom, zda je identita přijata či odmítnuta nebo nalezena či nenalezena.
- Databáze: Obsahuje biometrické referenční šablony a informace o elektronické identitě.



Obrázek 1.3: Schéma obecného biometrického systému [10]

1.2.2 Zpracování biometrických dat

Činnost biometrického systému lze rozdělit do dvou fází zpracování. První fází je registrace, též označována jako zavedení. Druhou fází je rozpoznávání, které lze provádět v režimu verifikace nebo identifikace.

Dříve než bude uživatel používat biometrický systém k rozpoznávání, musí databáze obsahovat jeho referenční biometrickou šablonu. Při registraci uživatele je nejprve pomocí biometrického senzoru sejmut jeho biometrický vzorek dané vlastnosti. Kvalita pořízeného vzorku je velmi důležitá, protože podstatně ovlivňuje úspěšnost pozdějšího rozpoznávání. Spolu s prezentací biometrické vlastnosti uživatel předkládá informaci o své identitě. Vzorek je po sejmutí zpracován, dochází k extrakci biometrických markantů, které daného uživatele jednoznačně identifikují. Následně je vytvořena referenční šablona a uložena společně s identifikací uživatele do databáze. K vytvoření referenční šablony je často požadováno opakované měření biometrické vlastnosti uživatele, aby se dosáhlo co největší kvality referenční šablony.

Poté, co je uživatel zaregistrován, může systém používat k rozpoznávání (verifikaci či identifikaci). Během fáze rozpoznávání je pomocí senzoru sejmut biometrický vzorek, který je dále zpracován obdobným způsobem jako je tomu u registrace. Získaná biometrická šablona ovšem není uložena do databáze, ale je porovnána s příslušnou referenční šablonou nebo více referenčními šablonami z databáze. Na základě výsledného skóre, porovnaného s prahovou hodnotou, dojde k rozhodnutí o úspěchu či neúspěchu rozpoznání daného uživatele.

Při verifikaci uživatel předkládá systému kromě své biometrické vlastnosti také svou elektronickou identitu, na jejímž základě je v databázi vyhledána příslušná biometrická šablona. Pokud záznam v databázi neexistuje, je přístup uživatele zamítnut. Pokud je ovšem záznam úspěšně nalezen, dojde k porovnání šablon. Verifikace je označována jako porovnání 1:1, porovnává se totiž jedna právě vytvořená šablona s jednou referenční šablonou z databáze. V případě shody dojde k potvrzení identity, v opačném případě je identita nepotvrzena. Cílem verifikace je tedy ověřit fyzickou identitu osoby.

Při identifikaci uživatel předkládá systému svou biometrickou vlastnost, ale na rozdíl od verifikace systému nesděluje svou elektronickou identitu. Identifikace je označována jako porovnání 1:N, protože je porovnána jedna aktuálně získaná šablona se všemi uloženými šablonami z databáze. Výstupem je buď nalezená identita a nebo je identita nenalezena. Cílem identifikace je tedy rozpoznat jedince, nalézt jeho elektronickou identitu.

1.2.3 Spolehlivost biometrických systémů

Cílem verifikace a identifikace je jednoznačné a bezchybné ověření nebo nalezení identity. Je prakticky nemožné, aby uživatel při rozpoznávání poskytl systému naprosto stejný biometrický vzorek jako během procesu registrace.

V důsledku toho se pak mohou lišit i porovnávané šablony. Proto je nutné povolit určitou variabilitu mezi srovnávanými vzorky.

Výsledek biometrického porovnání je závislý na nastaveném prahu. Jeho hodnota udává, zda má být skóre porovnání interpretováno jako shoda nebo neshoda. Po porovnání výsledného skóre s prahem vyhodnotí biometrický systém závěr, který může skončit správným nebo chybným rozhodnutím. Toto rozhodnutí může být ovlivněno tzv. vnitrotřídní či mezitřídní variabilitou.

Vnitrotřídní variabilita označuje rozdíly, které nastanou u jednoho konkrétního jedince během různých snímání. Při snímání může být jedinec ovlivněn svým psychickým a fyzickým stavem. Každá biometrická vlastnost se tak může při jednotlivých snímáních projevit s drobnou odlišností. Tato variabilita je nežádoucí, měla být u dané biometriky co nejnižší, aby nebyl jedinec zaměněn z někým jiným. Ideálním stavem je nulová vnitrotřídní variabilita. Jedná se například o změnu výrazu obličeje nebo stárnutí jedince při rozpoznávání obličeje. [1]

Mezitřídní variabilita označuje rozdílnost jedinců mezi sebou. Tato míra by měla být u dané biometriky co nejvyšší, aby bylo možné jednoznačně odlišit jednoho jedince od druhého. Problém s nízkou mezitřídní variabilitou často nastává například u jednovaječných dvojčat při rozpoznávání obličeje. [1]

V důsledku vysoké vnitrotřídní variability nebo nízké mezitřídní variability se biometrický systém může při rozhodovaní o správnosti identity dopouštět chyb. Chyba prvního typu, též označována jako chybné odmítnutí oprávněného uživatele, nastává pokud jsou dvě šablony od stejného jedince rozpoznány jako odlišné. Chyba druhého typu, též nazývána chybné přijetí neoprávněného uživatele, nastává pokud jsou dvě šablony od dvou odlišných jedinců rozpoznány jako shodné. Z uvedených chybových stavů jsou odvozeny chybové míry, které se používají při hodnocení spolehlivosti a bezpečnosti biometrických systémů. [1]

Veličina FRR udává, s jakou pravděpodobností biometrický systém chybně rozpozná dva biometrické vzorky od stejné osoby jako odlišné. Ve výsledku je uživatel v případě verifikace odmítnut, v případě identifikace není vůbec nenalezen. Musí se tak znovu pokusit o prokázání své identity. Pravděpodobnost chybného odmítnutí je definována jako:

$$FRR = \frac{N_{FR}}{N_{EIA}} \quad \text{nebo} \quad FRR = \frac{N_{FR}}{N_{EVA}} \tag{1.1}$$

kde N_{FR} značí počet chybných odmítnutí, N_{EIA} je počet pokusů oprávněných osob o identifikaci a N_{EVA} je počet pokusů oprávněných osob o verifikaci. [2]

Veličina FAR udává, s jakou pravděpodobností biometrický systém chybně rozpozná dva odlišné biometrické vzorky jako shodné. Pravděpodobnost chybného přijetí je definována jako:

$$FAR = \frac{N_{FA}}{N_{IIA}} \quad \text{nebo} \quad FAR = \frac{N_{FA}}{N_{IVA}} \tag{1.2}$$

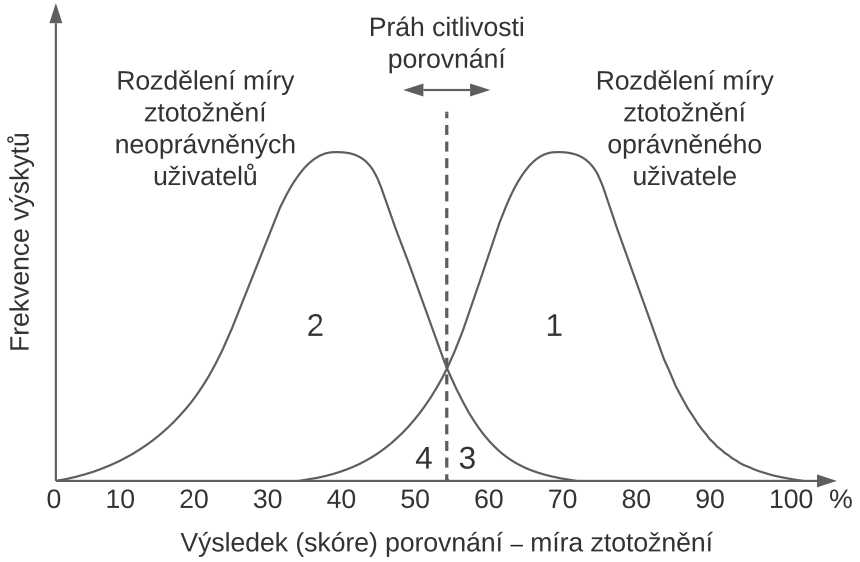
kde N_{FA} je počet chybných přijetí, N_{IIA} je počet pokusů neoprávněných osob o identifikaci a N_{IVA} značí počet pokusů neoprávněných osob o verifikaci. [2]

Hodnota EER, tzv. míra vyrovnání chyb, odpovídá situaci, kdy dochází k rovnosti hodnot FAR a FRR. Při natavení prahu na hodnotu EER bude chybně přijat i chybně odmítnut stejný počet osob. [1]

Na obrázku 1.4 je zobrazen histogram rozdělení míry ztotožnění oprávněných a neoprávněných uživatelů. Každá z křivek rozdělení odpovídá jedné skupině osob. Jedna křivka znázorňuje rozdělení míry ztotožnění oprávněného uživatele, který se opakovaně podrobil procesu verifikace nebo identifikace. Druhá křivka znázorňuje rozdělení míry ztotožnění neoprávněných uživatelů, jejichž cílem je proniknout do systému. Dle [2] nastavený práh citlivosti společně s oběma křivkami rozděluje plochu do čtyř oblastí:

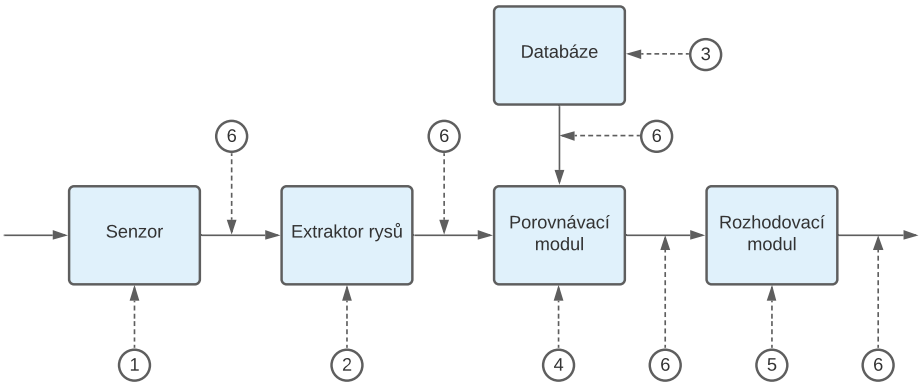
- Oblast číslo 1: Správné přijetí oprávněného uživatele.
- Oblast číslo 2: Správné odmítnutí neoprávněného uživatele.
- Oblast číslo 3: Chybné přijetí neoprávněného uživatele.
- Oblast číslo 4: Chybné odmítnutí oprávněného uživatele.

Oprávněný uživatel, který má výsledné skóre porovnání vyšší než je nastavený práh, je aplikací akceptován, v opačném případě je odmítnut. Neoprávnění uživatelé, kteří mají výsledné skóre porovnání vyšší než je nastavený práh, jsou aplikací akceptováni a v případě nižší hodnoty odmítáni.



Obrázek 1.4: Histogram rozdělení míry ztotožnění oprávněných a neoprávněných uživatelů [2]

1.2.4 Bezpečnost biometrických systémů



Obrázek 1.5: Slabá místa biometrického systému [11]

Každá z komponent biometrického systému může být potenciálním zranitelným místem. Na obrázku 1.5 jsou vyznačena slabá místa obecného biometrického systému. Čísla v obrázku odpovídají očíslování v následujícím souhrnu typických způsobů napadení biometrického systému dle [1, 11]:

1. Senzor: Snímači může být předložena falešná biometrická vlastnost. Tento typ útoku může být proveden při rozpoznávání nebo již ve fázi registrace. Dalším možným útokem může být předložení biometrické vlastnosti oprávněné osoby, avšak neoprávněným způsobem. Jinými slovy, legitimní uživatel může být donucen umožnit přístup do systému útočníkovi.

2. Extraktor rysů: Může být vygenerována předem určená množina rysů, která je následně použita pro vygenerování šablony.

3. Databáze: Může dojít k neoprávněnému čtení šablon, modifikaci jednoho nebo více záznamů, záměně šablon, změně vazeb mezi identifikátorem a příslušnou biometrickou šablonou. K záměně šablony, která má být uložena do databáze, může dojít již ve fázi registrace.

4. Porovnávací modul: Porovnávací modul může být ovlivněn, může dojít k vygenerování předem definovaného skóre porovnání, pomocí něhož může útočník proniknout do systému. Dalším možným útokem může být úprava vstupních dat s ohledem na výsledné skóre porovnání. Pokud se mírnou úpravou dat skóre zvýší, modifikace je zachována, jinak je úprava zahozena. Tento postup je opakován až do dosažení požadovaného výsledného skóre.

5. Rozhodovací modul: Finální rozhodnutí vygenerované v závislosti na zvolené prahové hodnotě a vypočteném skóre porovnání může být změněno.

6. Kanály propojující různé části biometrického systému: Komunikace mezi jednotlivými komponentami biometrického systému může být napadena. Může dojít k odchycení přenášených biometrických dat, jejich záměně nebo opětovnému zaslání již dříve použitých biometrických údajů. Dále může dojít k manipulaci s výsledným skóre porovnání a finálním rozhodnutí.

1.2.5 Testování živosti

Testování živosti je pro bezpečnost biometrického systému důležité. V případě některých biometrik není obtížné biometrická data získat. Biometrický systém by měl před samotným zpracováním biometrického vzorku ověřit, zda předložená biometrická charakteristika opravdu pochází od skutečné osoby, která je autentizována.

Při rozpoznávání duhovky může být snímači předložena útočníkem například fotografie duhovky nebo speciální kontaktní čočka. Existuje několik možností pro ověření živosti duhovky. Jedním ze způsobů je zkoumání poměru mezi průměrem zornice a duhovky. Zornice mění při změně intenzity světla svůj průměr. Je tedy možné záměrně měnit úroveň osvětlení a sledovat reakci zornice. Dalším způsobem může být detekce odrazů od světelných zdrojů. V tomto případě je kamera obklopena několika zdroji světla, které mohou být náhodně zapínány a vypínány. Detekce živosti pak probíhá analyzováním změn odrazu světla v oku. Žádný z těchto testů ovšem nemůže zabránit úspěšné autentizaci oprávněného uživatele, který byl donucen umožnit přístup někomu jinému. Řešením pak může být například zaregistrování obou očí uživatele, přičemž jedno z očí slouží pro autentizaci uživatele, druhé oko pro detekci tohoto typu útoku. [2]

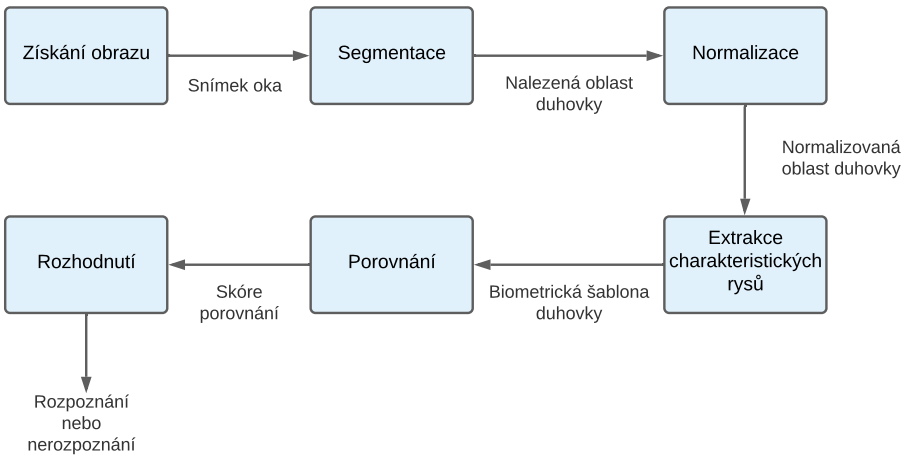
Kapitola 2

Rozpoznávání oční duhovky

V této kapitole jsou popsány nejčastěji používané metody a postupy při rozpoznávání oční duhovky.

2.1 Proces rozpoznávání

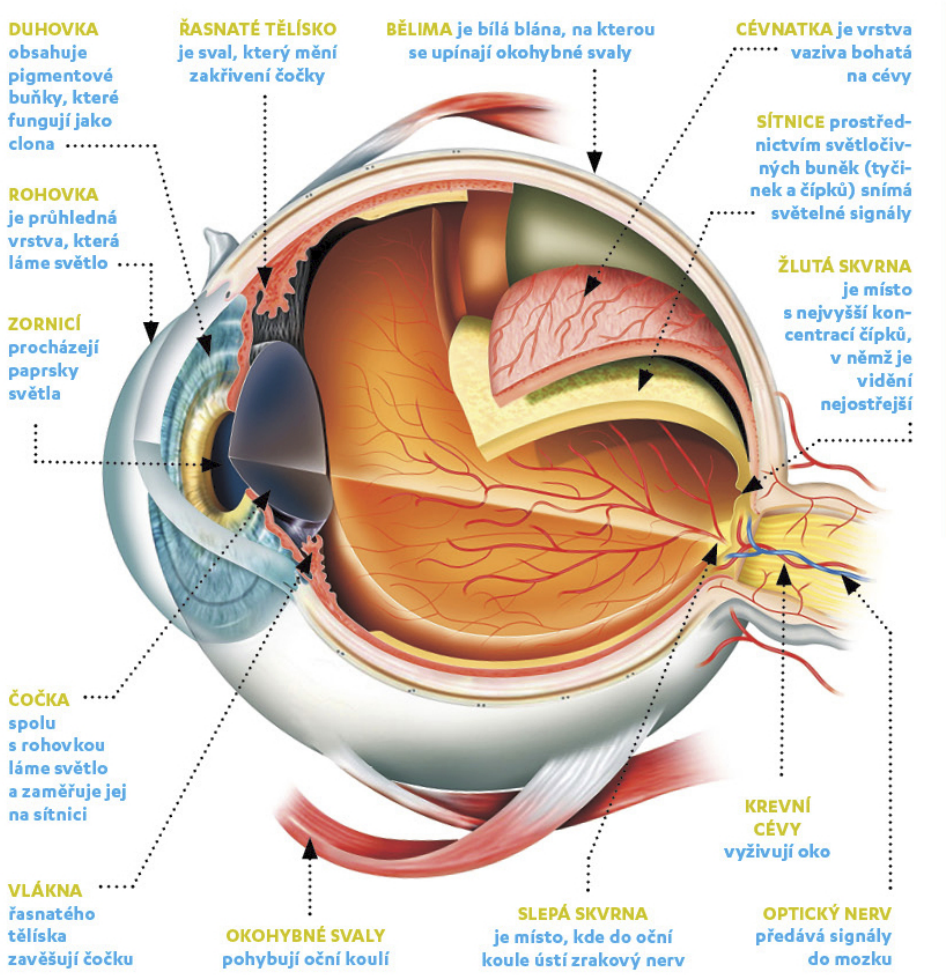
Cílem rozpoznávání oční duhovky je jednoznačné určení identity člověka na základě charakteristické textury duhovky. Proces rozpoznávání (obrázek 2.1) obvykle sestává z následujících základních kroků: získání obrazu, segmentace duhovky, normalizace duhovky, extrakce příznaků, porovnání a následné rozhodnutí.



Obrázek 2.1: Proces rozpoznávání oční duhovky [12]

2.2 Anatomie oka

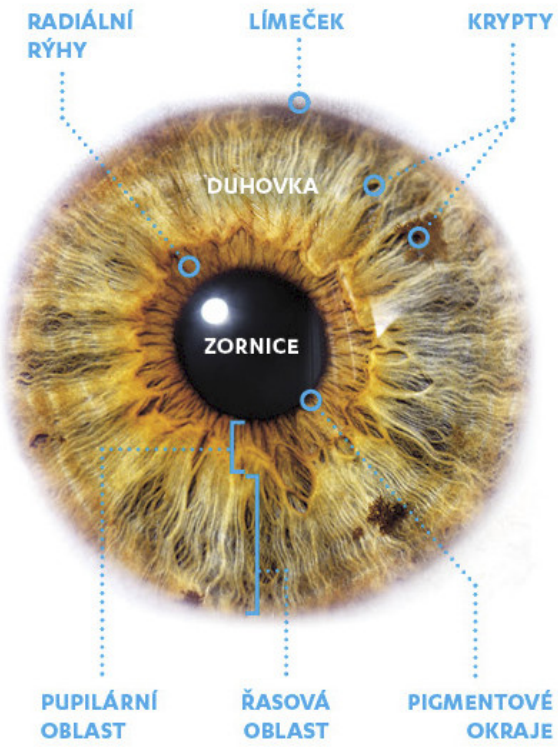
Oko je velmi složitým smyslovým orgánem. Umožňuje vnímat světlo a barvy, zprostředkovává získávání velkého množství informací o okolním prostředí a usnadňuje orientaci v prostoru. Zrakové ústrojí je tvořeno oční koulí a přídatnými očními orgány. Oční koule je uložena v očnici a je složena z několika částí a vrstev. Obalem oční koule je bělima, pevná vazivová blána bílé barvy. Upíná se na ní šest okohybných svalů zajišťujících pohyblivost oka. V přední části přechází bělima v rohovku, průhlednou kopulovitě zakřivenou vrstvu, která kryje duhovku a zornici. [8, 9]



Obrázek 2.2: Anatomie oka [13]

Duhovka má tvar mezikruží se středovým černým otvorem zvaným zornice. Obsahuje dva hladké svaly, svěrač a rozvěrač, které mění průměr zornice a regulují tak množství světla, které proniká do oční koule. Svěrač zornice je tvořen cirkulárně orientovanými svalovými vlákny. Umožňuje zúžení zornice, a tím omezení množství světla, které vniká do oka. Rozvěrač zornice je tvořen radiálně uspořádanými svalovými vlákny a zajišťuje rozšíření zornice při nedostatku světla. Automatická reakce zornice na různou intenzitu světla se nazývá zornicový reflex. [8]

Duhovka má na svém povrchu velké množství rysů jako jsou například krypty, radiální rýhy či pigmentové skvrny, které tvoří její typickou kresbu a dělají duhovku jedinečnou. Přední plochu duhovky dělí kruhovitý vlnitý lem na dva různě velké prstence, vnitřní pupilární a vnější ciliární, též nazývanou řasovou. Pupilární část je užší a obsahuje jemnější krypty. Ciliární část je naopak širší a obsahuje krypty hrubší. Struktura duhovky je popsána na obrázku 2.3. Barva duhovky podmiňuje barvu očí. Závisí na množství pigmentu nazývaného melanin. Hnědá barva je výsledkem velkého množství pigmentu, naproti tomu u modrých očí pigment chybí. [14]



Obrázek 2.3: Struktura duhovky [13]

2.3 Získání obrazu

Prvním krokem procesu rozpoznávání oční duhovky je pořízení snímku oka kamerou. Snímání se obvykle provádí v blízkém infračerveném spektru vlnové délky mezi 700–900 nm. Další možností je snímání duhovky ve viditelném spektru. Použití infračerveného osvětlení přináší oproti snímání ve viditelném světle řadu výhod, které usnadňují proces rozpoznávání. Infračervené osvětlení je příjemnější pro uživatele, neboť neoslňuje. Další jeho výhodou je, že eliminuje v oku zrcadlové odrazy od jiných světelných zdrojů z prostředí. Odhaluje více texturních informací obsažených v duhovce, protože melanin infračervené světlo převážně odráží zatímco viditelné světlo melanin v duhovce obvykle absorbuje. [15]

2.4 Segmentace

Cílem segmentace je nalezení oblasti duhovky v pořízeném snímku oka. Oblast duhovky lze aproximovat dvěma kružnicemi, jednou větší, představující hranici mezi duhovkou a bělimou, druhou menší, představující hranici mezi duhovkou a zornicí.

Úspěšnost segmentace závisí na kvalitě pořízeného snímku. Pořízený obraz duhovky může obsahovat odrazy světla, řasy, oční víčka, zornici, bělimu a další nežádoucí části, které komplikují segmentaci. Tyto části je třeba detekovat a z výsledné oblasti duhovky vynechat. Tento krok je důležitý pro následné rozpoznávání. Oblasti, které jsou falešně označeny jako součást duhovky, mohou ovlivnit přesnost a výsledek porovnávání.

2.4.1 Houghova transformace

Houghova transformace je algoritmus, který lze použít k určení parametrů jednoduchých geometrických objektů v obraze, jako jsou čáry a kružnice, které lze popsat rovnicí. Kruhová Houghova transformace může být použita k nalezení poloměru a středových souřadnic zornice a duhovky.

Nejprve jsou pomocí hranového detektoru v obrázku nalezeny hrany, tedy místa, kde dochází k velké změně kontrastu pixelů. Vznikne tak tzv. mapa hran, která je vstupním bodem pro použití Houghovy transformace. Každý nalezený hranový bod je projektován do prostoru parametrů. Projekce probíhá přičtením pevně dané konstanty na všechna místa prostoru parametrů, kterými prochází pomyslná kružnice se středem ve zvoleném hranovém bodě a s daným poloměrem. Za předpokladu známého poloměru se v bodě středu hledaného kruhu v prostoru parametrů vyskytne maximum. Pro neznámý poloměr je postup obdobný, provede se projekce pro hodnoty poloměru ve zvoleném rozsahu a následně je nalezena maximální hodnota přes celý prostor parametrů. [15]

2.4.2 Integro-diferenciální operátor

Integro-diferenciální operátor je technika segmentace oční duhovky navržená Johnem Daugmanem [16]. Operátor slouží k nalezení vnitřního a vnějšího okraje duhovky. Předpokládá, že zornice a duhovka jsou kruhové útvary a chová se jako kruhový hranový detektor. Využívá toho, že na hranici duhovky s bělimou a hranici duhovky se zornicí dochází k velké změně jasu. Integro-diferenciální operátor je definován jako:

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

kde $I(x, y)$ je intenzita pixelu na souřadnicích (x, y) v analyzované obrazové matici. Symbol $*$ značí konvoluci a $G_\sigma(r)$ je vyhlazovací funkce, kterou může být například Gaussův filtr. Hodnota σ určuje míru vyhlazení obrazu. Proces vyhlazení pomáhá zmírnit šum a eliminovat slabé hrany, které jsou v obraze nežádoucí, a naopak zachovat požadované silnější hrany. Operátor prochází obrazovou oblast a hledá maximální hodnotu z parciální derivace normalizované kontury integrálu vstupního obrazu s ohledem na poloměr r a středové souřadnice (x_0, y_0). Výstupem jsou parametry kružnice, které nejlépe vyhovují vnitřní a vnější hranici duhovky.

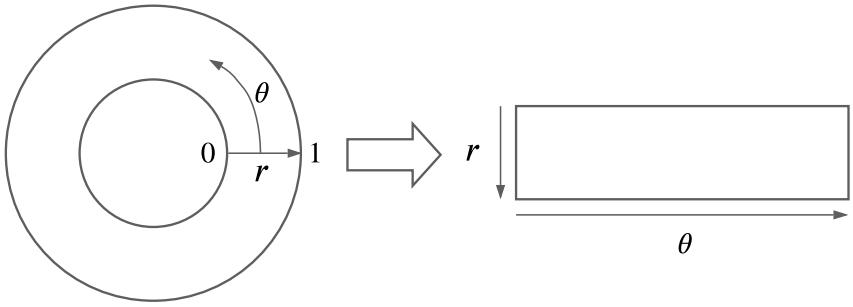
Úpravou parametrů je možné realizovat také detekci horního a dolního očního víčka. Část vzorce, která je použita k detekci kontury je zaměněna z kruhové na obloukovou. [15]

2.5 Normalizace

Po úspěšné segmentaci obvykle následuje další fáze, kterou je normalizace. Tento krok je v zásadě volitelný, avšak značně zjednodušuje následující části procesu rozpoznávání. Tvar a velikost nalezené oblasti duhovky může ovlivnit řada faktorů. Jedním z nich je zužování a rozšiřování zornice v reakci na různou intenzitu okolního osvětlení. V případě zúžení zornice se plocha duhovky zvětší, naopak při rozšíření zornice se plocha duhovky zmenší. Velikost duhovky může být také ovlivněna vzdáleností oka od kamery. Dalším faktorem je, že oblast zornice není vždy soustředná s oblastí duhovky a je obvykle mírně posunuta směrem k nosu. Cílem normalizace je transformace oblasti duhovky ve tvaru mezikruží do obdélníkového tvaru s pevnými rozměry.

2.5.1 Daugmanův model hrubého zarovnání

Každý bod (x, y) v oblasti duhovky je převeden z kartézských souřadnic na polární souřadnice (r, θ), kde r je z intervalu $[0, 1]$ a θ je úhel z intervalu $[0, 2\pi]$. Proces je znázorněn na obrázku 2.4. [1]



Obrázek 2.4: Daugmanův model hrubého zarovnání [1]

Přemapování oblasti duhovky z (x, y) kartézských souřadnic na normalizovanou polární reprezentaci je definováno jako:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \tag{2.2}$$

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta)$$
$$y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta)$$

kde $I(x, y)$ je obraz duhovky, (x, y) jsou kartézské souřadnice v původním obrazu a (r, θ) jsou odpovídající polární souřadnice, (x_p, y_p) a (x_l, y_l) jsou souřadnice hranic zornice a duhovky při úhlu θ. [16]

Tento postup kompenzuje výše uvedené faktory ovlivňující tvar a velikost duhovky. Nekompenzuje však rotační nekonzistenci, ta je řešena až při porovnávání šablon duhovek.

2.6 Extrakce příznaků

Cílem procesu extrakce příznaků je získání charakteristických rysů ze vzoru duhovky a vytvoření její kompaktní reprezentace vhodné pro porovnávání s jinými duhovkami.

2.6.1 2D Gaborův filtr

V procesu demodulace fáze, použité pro kódování vzoru duhovky, jsou části duhovky promítnuty na plochu 2D Gaborových filtrů, čímž jsou vytvořeny komplexní koeficienty, jejichž reálná a imaginární část specifikuje souřadnice fázoru v komplexní rovině. Úhel každého fázoru je pak kvantován do jednoho ze čtyř kvadrantů (obrázek 2.5). Tím jsou získány dva bity fázové informace. Tento proces je opakován pro všechny části duhovky, pro různé velikosti filtrů, frekvence a orientace. Výstupem je kód duhovky. [16]

Na obraz duhovky, získaný v procesu normalizace, jsou aplikovány 2D Gaborovy filtry definované jako:

$$G(\rho,\phi) = e^{-i\omega(\theta_0-\phi)} e^{\frac{-(r_0-\rho)^2}{\alpha^2}} e^{\frac{-(\theta_0-\phi)^2}{\beta^2}} \tag{2.3}$$

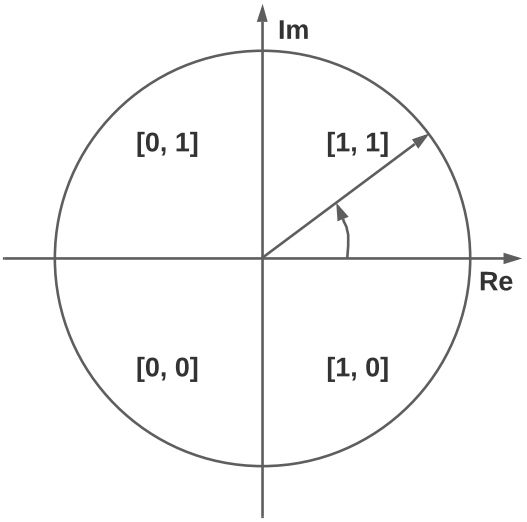
kde (ρ,ϕ) udává pozici v obrazu, (α,β) značí výšku a šířku filtru a ω je frekvence filtru. [16]

Komplexní Gaborova odpověď je následně kvantována do dvou bitů pomocí následujících nerovností:

$$h_{Re} = \begin{cases} 1 & \text{pokud} \quad Re \int_\rho \int_\phi I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{\frac{-(r_0-\rho)^2}{\alpha^2}} e^{\frac{-(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi \geq 0 \\ 0 & \text{pokud} \quad Re \int_\rho \int_\phi I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{\frac{-(r_0-\rho)^2}{\alpha^2}} e^{\frac{-(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi < 0 \end{cases} \tag{2.4}$$

$$h_{Im} = \begin{cases} 1 & \text{pokud} \quad Im \int_\rho \int_\phi I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{\frac{-(r_0-\rho)^2}{\alpha^2}} e^{\frac{-(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi \geq 0 \\ 0 & \text{pokud} \quad Im \int_\rho \int_\phi I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{\frac{-(r_0-\rho)^2}{\alpha^2}} e^{\frac{-(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi < 0 \end{cases} \tag{2.5}$$

kde r_0 a θ_0 reprezentují polární souřadnice ω, α, β jsou parametry Gaborových filtrů, $I(\rho,\phi)$ je normalizovaný obrázek duhovky, h_{Re} je reálná část komplexně ohodnoceného bitu a h_{Im} je imaginární část komplexně ohodnoceného bitu, který může nabývat 0 nebo 1 v závislosti na znaménku integrálu. [17]



Obrázek 2.5: Fázová kvantizace [16]

2.6.2 Lokální binární vzor

Metoda lokálního binárního vzoru (LBP) slouží k popisu textury obrazu na základě příznaku, který daný obraz charakterizuje. Tento příznak je reprezentován histogramem. Vzorec pro výpočet LBP je definován jako:

$$LBP_{P,R}(x_c, y_c) = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \tag{2.6}$$

kde P je počet sousedních bodů centrálního pixelu na souřadnicích (x_c, y_c), R označuje poloměr kružnice, na které se body nacházejí, g_c reprezentuje hodnotu jasu středového pixelu a g_p značí hodnotu jasu každého sousedního pixelu. Funkce $s(x)$, kde x je rozdíl hodnot g_p a g_c je definována následovně:

$$s(x) = \begin{cases} 1 & \text{pro} \quad x \geq 0 \\ 0 & \text{pro} \quad x = 0 \end{cases} \tag{2.7}$$

Vstupem do metody je obraz ve stupních šedi, který je postupně procházen pixel po pixelu. Hodnota každého bodu z okolí je porovnána s hodnotou centrálního bodu. Pokud je hodnota větší nebo rovna než hodnota centrální, výsledkem porovnání je 1, v opačném případě 0. Tímto je získán binární kód. Následuje váhování každého členu binárního kódu binomickou vahou 2^p. Výsledné hodnoty každého členu jsou sečteny a je tak získán LBP kód daného centrálního bodu. Stejným způsobem je určena hodnota LBP každého pixelu v obraze, vyjma okrajových pixelů, které nemají dostatek těchto sousedních bodu. Ze všech LBP hodnot je nakonec vytvořen histogram. [15]

2.7 Porovnání

Aby bylo možné určit, zda dva biometrické vzorky duhovky pochází ze stejného oka, je potřeba vzájemně porovnat jejich biometrické šablony. Na základě výsledného skóre porovnání a nastaveném prahu pak proběhne rozhodnutí.

2.7.1 Hammingova vzdálenost

Porovnání dvou kódů duhovek lze provést výpočtem Hammingovy vzdálenosti (HD) dané následujícím vzorcem:

$$HD = \frac{1}{N} \sum_{i=1}^{N} codeA_i \oplus codeB_i \tag{2.8}$$

kde *codeA* a *codeB* jsou kódy duhovek, N je velikost kódu duhovky v bitech a $\oplus$ je bitový exkluzivní součet (XOR). Hammingova vzdálenost je spočtena jako suma exkluzivních součtů mezi jednotlivými bity kódů duhovek. [1]

V případě, že je duhovka zastíněna víčkem, jsou použity binární masky definující platné oblasti duhovky. Porovnání dvou kódů duhovek pak lze provést výpočtem Hammingovy vzdálenosti dané následujícím vzorcem:

$$HD = \frac{||(codeA \oplus codeB) \cap maskA \cap maskB||}{||maskA \cap maskB||} \tag{2.9}$$

kde $\oplus$ je bitový exkluzivní součet (XOR), $\cap$ je bitový součin (AND), $||$ je norm operátor určující počet jedničkových bitů v daném vektoru, $codeA$ a $codeB$ jsou porovnávané kódy duhovek, $maskA$ a $maskB$ jsou jejich příslušné binární masky. [16]

Hammingova vzdálenost udává počet bitů, ve kterých se šablony duhovek liší, vydělené počtem platných bitů. Operátor XOR v čitateli detekuje neshodu mezi odpovídajícími páry bitů kódů duhovek. Aby se zamezilo tomu, že jsou kódy zastřené víčky, jsou použity příslušné bitové masky definující platné oblasti pro porovnávání. Jmenovatel tedy odpovídá celkovému počtu platných bitů.

Při snímání oka může dojít k natočení hlavy a tím i k natočení duhovky. Aby se předešlo nežádoucímu vlivu rotace duhovky na výsledek porovnání, je použit vzájemný bitový posun kódů duhovek. Šablona jedné z duhovek je posouvána ve zvoleném rozsahu doprava a doleva o daný počet bitů. Pro každý z těchto posunů je zvlášť vypočítána Hammingova vzdálenost, přičemž nejmenší dosažená vzdálenost je pak brána jako výsledná hodnota porovnání. V případě použití masek definujících platné oblasti je posouvána spolu s biometrickou šablonou i příslušná binární maska. Příklad porovnání kódů duhovek s použitím posunů je uveden na obrázku 2.6. [1]

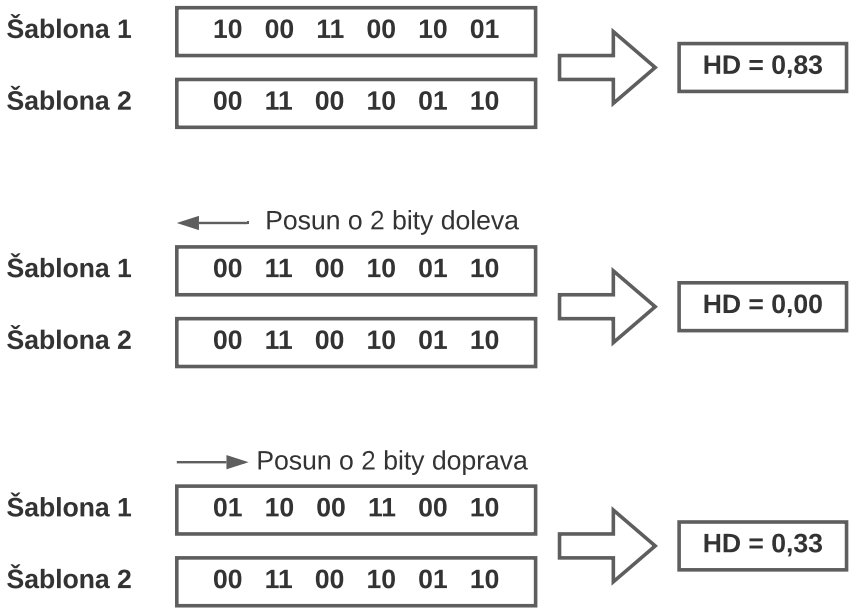
Každý bit kódu duhovky může být se stejnou pravděpodobností roven 0 nebo 1. Dvě duhovky pocházející z rozdílných očí jsou proto nekorelované, očekávaná Hammingova vzdálenost je tak blízká $0,5$. Pokud jsou oba kódy získány ze stejné duhovky, pak je díky vysoké korelaci obou kódů Hammingova vzdálenost mezi nimi blízká nule. [2]

2.7.2 Euklidovská vzdálenost

Dalším způsobem, jak porovnat dvě šablony duhovek, je použití Euklidovské vzdálenosti. Vzdálenost D_E mezi dvěma šablonami x a y v N-rozměrném prostoru lze definovat jako

$$D_E(x, y) = \sqrt{\sum_{i=1}^{N}(x_i - y_i)^2} \tag{2.10}$$

kde x_i je i-tý prvek biometrické šablony a y_i je i-tý prvek referenční biometrické šablony. [21]



Obrázek 2.6: Použití posunů při porovnávání kódů duhovek [1]

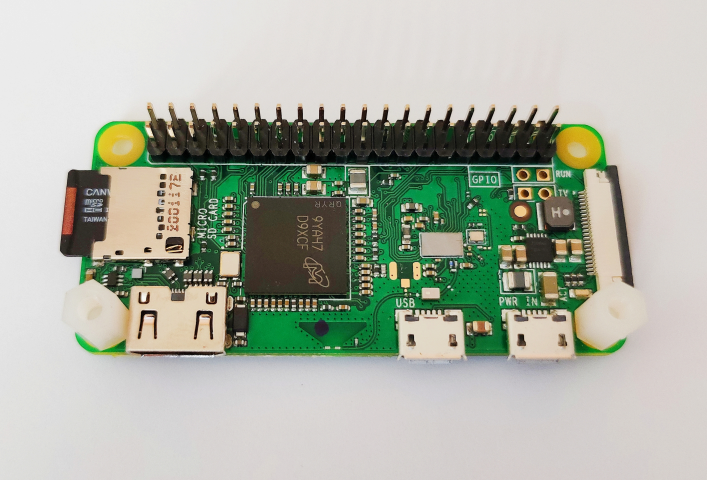
Kapitola 3

Zařízení pro snímání oční duhovky

V této kapitole je popsáno zvolené snímací zařízení, orientační pořizovací ceny komponent a demonstrační databáze snímků.

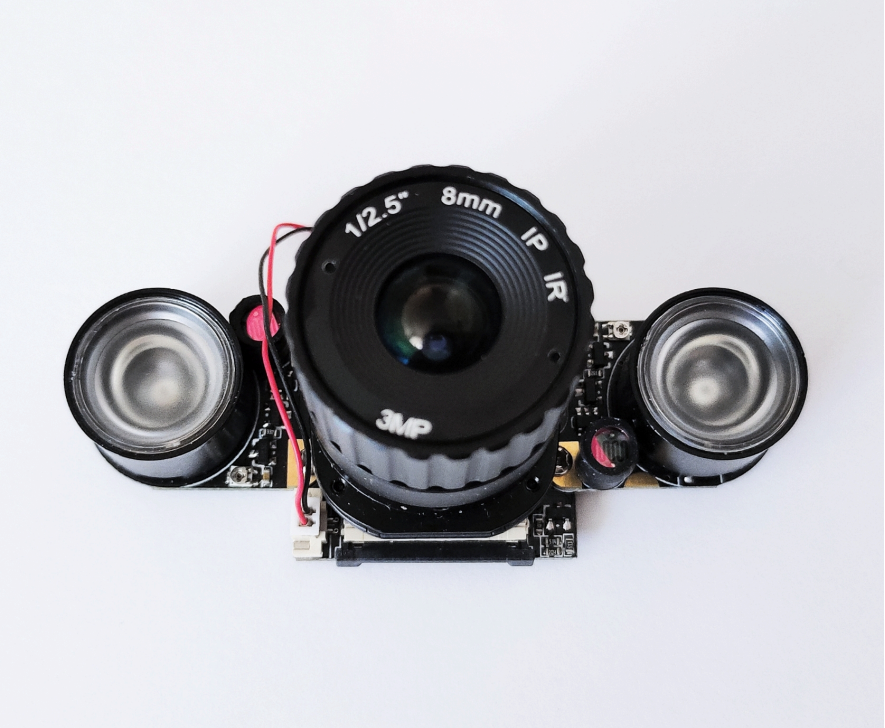
3.1 Snímací zařízení

S přihlédnutím na cenu a dostupnost komponent bylo pro realizaci snímacího zařízení vybráno Raspberry Pi Zero. Jedná se v současnosti o jedno z nejlevnějších, nejmenších a nejúspornějších Raspberry Pi. Konkrétně byl vybrán model WH, kde písmeno W označuje variantu Raspberry Pi Zero s vestavěnou WiFi a Bluetooth anténou, písmeno H značí osazený GPIO header. Zařízení je napájeno pomocí microUSB konektoru.



Obrázek 3.1: Raspberry Pi Zero WH

Osoby s tmavě pigmentovanými duhovkami mají při pořizování snímků v přirozeném světle velmi nízký kontrastní rozdíl mezi zornicí a duhovkou, což velmi ztěžuje průběh segmentace. Problém lze vyřešit použitím infračerveného osvětlení, které více odhaluje texturní informace obsažené v duhovce a zbytečně nepříjemně neoslňuje uživatele. Proto byla vybrána kamera Waveshare IR-CUT (B) určená pro Raspberry Pi. Tato kamera podporuje funkci nočního vidění a připojení infračervených nebo obyčejných LED. Obsahuje vestavěný vyjímatelný filtr IR-CUT, který eliminuje zkreslení barev při denním světle. Kamera je připojena k Raspberry Pi 15-pinovým plochým kabelem.



Obrázek 3.2: Kamera Waveshare IR-CUT (B)

Vybraná kamera nedisponuje automatickým zaostřováním, je nutné zaostřit obraz manuálně a stanovit předem danou vzdálenost oka od snímače. Tato vzdálenost byla naměřena v rozmezí 10–20 cm. Definovaná vzdálenost zaručuje ostrost snímku.

Na pravou a levou stranu kamery byl přimontován přísvit v podobě dvou Waveshare Infrared LED (B) určených pro kamery Waveshare Raspberry Pi. Každá z LED má integrovaný fotorezistor, který detekuje okolní světlo, a nastavitelný rezistor, kterým lze nastavit práh okolního světla při přepínání infračervené LED. Tyto LED vyzařují infračervené záření o vlnové délce 850 nm.

3.2 Orientační pořizovací ceny

Tabulka 3.1 obsahuje aktuální orientační pořizovací ceny jednotlivých komponent, které byly vybrány pro realizaci snímacího zařízení.

Tabulka 3.1: Orientační pořizovací ceny

Komponenta	Orientační cena [Kč]
Raspberry Pi Zero WH	500
Kamera Waveshare IR-CUT (B)	800
Waveshare Infrared LED (B)	100
Raspberry Pi Zero kamera kabel	100

3.3 Databáze snímků duhovek

Pro demonstrační účely byla vytvořena databáze snímků duhovek. Pomocí výše popsaného snímacího zařízení bylo nafoceno celkem 7 osob. Databáze obsahuje 5 snímků pravého oka a 5 snímků levého oka každé osoby. Snímky jsou označeny třemi informacemi oddělenými podtržítky. První část označuje osobu, druhá část značí, zda se jedná o oko pravé nebo levé, třetí část rozlišuje snímky stejného oka od sebe.

Kapitola 4

Implementace

V první části této kapitoly je popsána implementace jednotlivých kroků rozpoznávání oční duhovky. V druhé části kapitoly je popsána implementace datového úložiště pro potřeby demonstrační aplikace. Kompletní zdrojové kódy jsou k dispozici na přiloženém DVD.

4.1 Implementace rozpoznávání duhovky

Implementace je napsána v jazyce Python, konkrétně verze 3.8.5. Pro práci s obrazem bylo využito knihoven OpenCV a scikit-image, pro práci s poli byla použita knihovna NumPy. Pro implementaci uživatelského rozhraní demonstrační aplikace bylo zvoleno PyQt5.

4.1.1 Předzpracování

Cílem předzpracování pořízeného snímku je vylepšení jeho stávajících parametrů. Je vhodné upravit obraz tak, aby následná segmentace a další části rozpoznávání byly co nejpřesnější, nejspolehlivější a nejrychlejší.

Po nasnímání je nejprve barevný obraz oka převeden do odstínů šedi. Pro snadnější zpracování snímku je výhodné pracovat pouze s jednou hodnotou intenzity pro každý bod obrazu namísto původních tří. Tímto krokem jsou také eliminovány drobné odchylky v barevných tónech, které mohou být způsobené například změnou okolního osvětlení a snímač tak není schopen při každém snímání zaznamenat naprosto stejný barevný odstín.

4.1.2 Segmentace

Cílem segmentace je nalezení oblasti duhovky v obraze. Pro zjednodušení se předpokládá, že zornice a duhovka jsou kruhové útvary. Jsou hledány jejich poloměry a souřadnice středů. Střed zornice bývá často nesoustředný se středem duhovky, parametry obou kružnic je proto nutné odhadnout nezávisle na

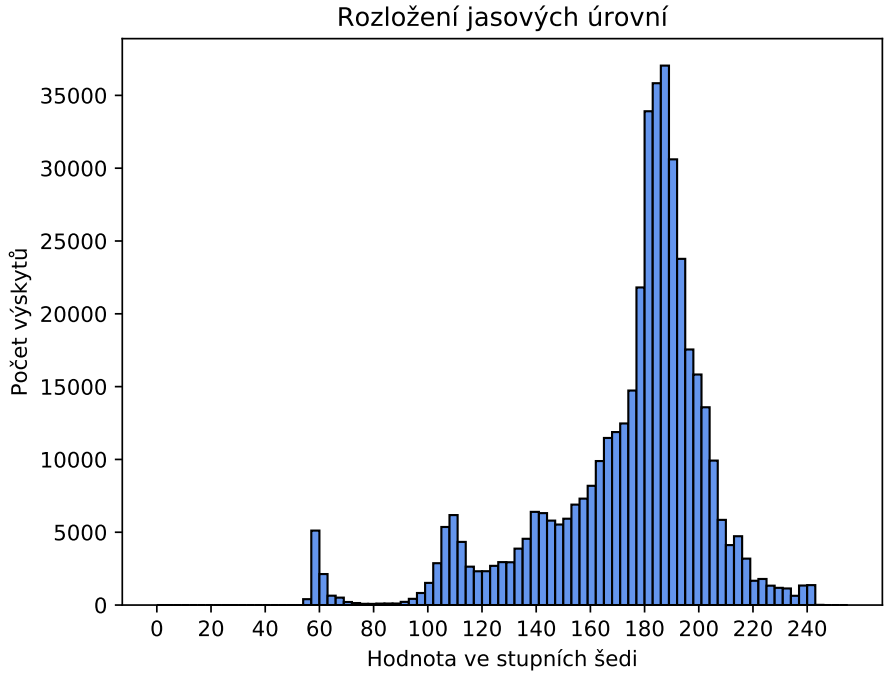
sobě. Mezi zornicí a duhovkou dochází k většímu jasovému rozdílu pixelů než mezi duhovkou a bělimou. Jako první je tedy hledána vnitřní hranice duhovky, protože lze v obraze snadněji nalézt.

K nalezení oblasti zornice je použita metoda prahování. Tato metoda na základě jasu pixelů a nastaveného prahu převádí obraz ve stupních šedi na černobílý. Prahování je funkce upravující obraz podle předpisu:

$$b(x,y) = \begin{cases} 1 & \text{pokud} \quad I(x,y) \leq T \\ 0 & \text{pokud} \quad I(x,y) > T \end{cases} \tag{4.1}$$

kde $b(x,y)$ je nová hodnota obrazového bodu na souřadnicích (x,y), $I(x,y)$ je intenzita bodu na souřadnicích (x,y) v původním obraze a T je prahová hodnota.

Pro úspěšnou segmentaci je klíčové stanovit správnou hodnotu prahu. Ta může být nalezena analýzou histogramu obrazu. Lze využít toho, že zornice je jednou z nejtmavších oblastí snímku. Z histogramu na obrázku 4.1 lze pak odhadnout úrovně jasu patřící oblasti zornice. Práh byl na základě analýzy všech snímků duhovek odhadnut a nastaven na hodnotu 80, která odděluje hodnoty jasu zornice (hodnoty nižší než práh) od hodnot jasu zbylých částí obrazu (hodnoty vyšší než práh).



Obrázek 4.1: Histogram pořízeného snímku oka v odstínech šedi

Podobné jasové hodnoty jako u zornice lze pozorovat u řas, které mohou zasahovat do oblasti zornice a duhovky. Zornice je však dominantní oblastí, řasy lze považovat za šum, který je třeba eliminovat. K tomu je použit mediánový filtr. Ten vezme definované body obrazu z aktuálního okolí bodu a vybere z nich medián, který se stane novou hodnotou zpracovávaného obrazového bodu. Pro úspěšnost filtrace šumu je důležité správně nastavit velikost filtru vzhledem k velikosti obrazu. Při použití příliš malého filtru dochází k nedostatečné eliminaci šumu, naopak u příliš velkého filtru dochází k odfiltrování některých důležitých částí obrazu.

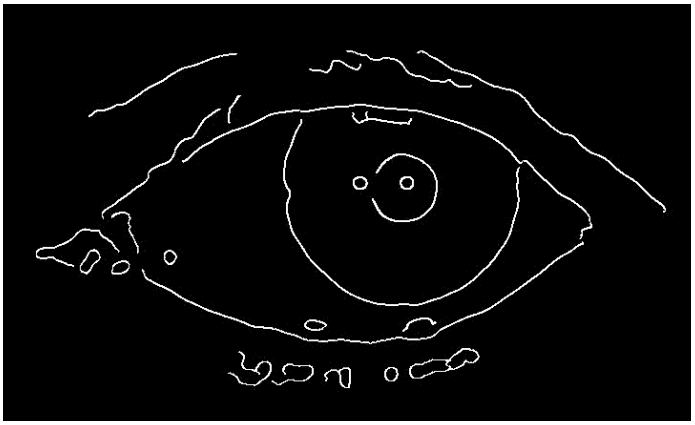
Dalším nežádoucím jevem můžou být odlesky v oblasti zornice. Ty jsou eliminovány morfologickým filtrováním obrazu. Konkrétně jsou použity operace dilatace a eroze, jejichž kombinací lze získat další užitečné morfologické transformace. Nejprve je na binární obraz aplikována dilatace, následně eroze. Jedná se o tzv. morfologické uzavření, kdy jsou spojeny objekty, které se nachází blízko u sebe a zaplněny malé díry.

Následně je vytvořena mapa hran. Hrany jsou oblasti v obraze, ve kterých dochází k prudkým změnám jasu. K jejich nalezení je použit Cannyho hranový detektor, který se při implementaci osvědčil jako nejlepší volba.

V závěrečném kroku detekce vnitřního okraje duhovky je aplikována kruhová Houghova transformace, která je popsána v části 2.4.1. Výstupem jsou souřadnice středu kružnice zornice a její poloměr.

Obrázek 4.2: Detekce vnitřního okraje duhovky: a) prahování, b) mediánový filtr, c) dilatace, d) eroze, e) Cannyho hranový detektor

Poté následuje detekce vnějšího okraje duhovky. Pomocí Cannyho hranového detektoru je opět nalezena mapa hran. Poté je aplikována kruhová Houghova transformace. Se znalostí parametrů zornice získaných v předchozím kroku lze při hledání hranice mezi duhovkou a bělimou prohledávanou oblast omezit. Kružnice představující vnější hranici duhovky musí splňovat určitá kritéria. Její střed se musí nacházet uvnitř oblasti zornice, její poloměr musí být větší než je poloměr nalezené kružnice obklopující zornici a tato kružnice nesmí procházet oblastí zornice. Takto je vybrána nejlépe vyhovující kružnice. Výstupem jsou souřadnice středu duhovky a její poloměr.



Obrázek 4.3: Detekce vnějšího okraje duhovky: Cannyho hranový detektor

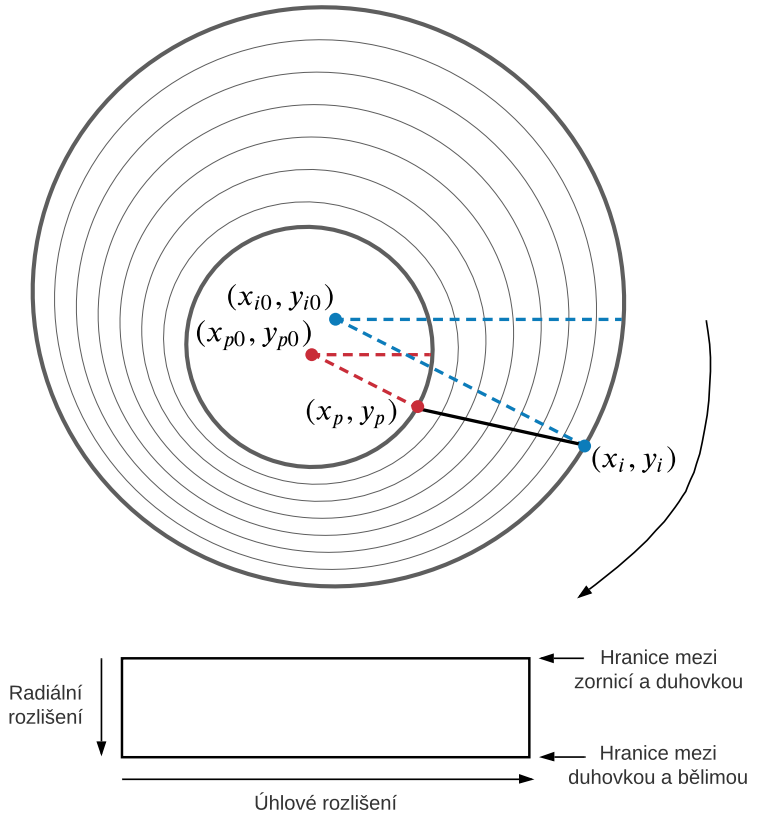
4.1.3 Normalizace

Velikost duhovky se může během různých snímání lišit. Tyto změny bývají způsobené odlišnou vzdáleností oka od kamery nebo reakcí na intenzitu okolního osvětlení, rozšířením či zúžením zornice. Dále je třeba brát v úvahu, že zornice a duhovka nejsou vždy soustředné. Tyto deformace můžou ovlivnit samotné rozpoznávání a je třeba je eliminovat. Duhovka je proto podobně jako v Daugmanově modelu hrubého zarovnání, popsaného v podkapitole 2.5.1, převedena na obdélníkový obraz pevné velikosti, kde svislá osa reprezentuje radiální rozlišení a vodorovná představuje úhlové rozlišení.

Na obrázku 4.4 je ilustrován implementovaný proces normalizace duhovky. Vstupem do této metody jsou souřadnice středů duhovky a zornice a jejich poloměry nalezené ve fázi segmentace. Před samotným rozbalováním textury duhovky je nejprve zvoleno vhodné radiální a úhlové rozlišení výsledné normalizované oblasti. Následně jsou pro zvolený úhel nalezeny příslušné souřadnice nacházející se na vnitřní a vnější hranici duhovky. Ty lze vypočítat pomocí následujících rovnic:

$$\begin{aligned} x_p &= x_{p0} + r_p \cdot cos(\theta) \\ y_p &= y_{p0} + r_p \cdot sin(\theta) \\ x_i &= x_{i0} + r_i \cdot cos(\theta) \\ y_i &= y_{i0} + r_i \cdot sin(\theta) \end{aligned} \tag{4.2}$$

kde souřadnice (x_{p0}, y_{p0}) označují střed zornice, (x_{i0}, y_{i0}) značí střed duhovky, (x_p, y_p) představují bod na hranici mezi zornicí a duhovkou, (x_i, y_i) jsou souřadnice bodu nacházejícího se na hranici mezi duhovkou a bělimou.



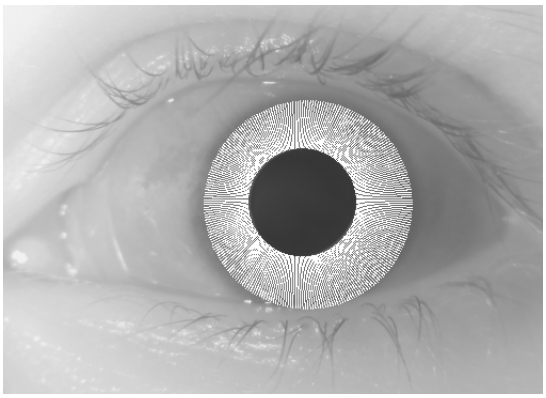
Obrázek 4.4: Proces normalizace duhovky

V radiálním směru je textura normalizována od vnitřní hranice duhovky k vnější hranici. V úhlovém směru je textura rozbalována po směru hodinových ručiček. Pomocí nalezených bodů na vnější a vnitřní hranici duhovky pro daný úhel je vypočítán radiální krok. Implementace bere v úvahu, že vzdálenost mezi těmito body může být pro každý z úhlů odlišná. Velikost radiálního kroku se tedy dynamicky upravuje s ohledem na aktuální vzdálenost mezi body. Tento přístup se ukázal jako lepší řešení než rozbalování s pevným radiálním krokem, které může mít za následek ztrátu informací. Velikost výsledné normalizované duhovky je pak vždy 128×768 obrazových bodů.

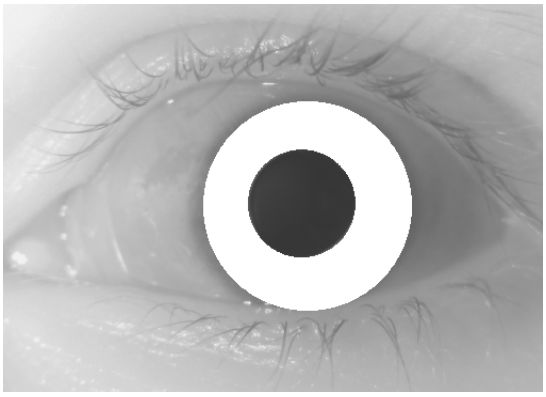
Aby byla normalizace úspěšná, je důležité zvolit dostatečně malé radiální a úhlové kroky. Volba těchto parametrů ovlivňuje výsledek normalizace a pozdějšího extrahování charakteristických rysů. Na obrázku 4.5 jsou vidět vynechané body obrazu, které nejsou obsažené v normalizovaném obraze duhovky. Obrázek 4.6 znázorňuje správnou volbu velikosti kroků, díky které jsou normalizovány všechny potřebné obrazové body duhovky.

Před dalším zpracováním je vhodné zvýšit kontrast normalizovaného obrazu duhovky za účelem zvýraznění jejích charakteristických rysů. Na snímek

je aplikována metoda ekvalizace histogramu. Tato metoda mění rozložení intenzit v obraze tak, aby se docílilo obrazu, který bude mít přibližně rovnoměrné rozložení jasových hodnot v histogramu.

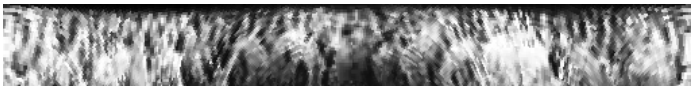


Obrázek 4.5: Nesprávně zvolený krok pro normalizaci duhovky



Obrázek 4.6: Správně zvolený krok pro normalizaci duhovky

Obrázek 4.7: Normalizovaná duhovka



Obrázek 4.8: Normalizovaná duhovka se zvýšeným kontrastem

4.1.4 Extrakce charakteristických rysů

Extrakce příznaků je realizována pomocí 2D Gaborova filtru a fázového demodulátoru popsaného v části 2.6.1. Nejprve je provedena konvoluce normalizovaného obrazu duhovky s Gaborovým filtrem. Výstupem jsou dvě matice představující reálnou a imaginární část komplexní odpovědi filtru. Pro zvýšení přesnosti při porovnávání a úsporu místa jsou navíc obě matice rozděleny na několik bloků. Pro každý blok je nalezen jeho průměr. Poté je použit fázový demodulátor, který mapuje získané hodnoty do binárního kódu. Toto mapování závisí na znaménku reálné a imaginární části. Mapovány mohou být čtyři kombinace bitů (tabulka 4.1). První bit vyjadřuje znaménko reálné části, druhý bit zastupuje znaménko imaginární části. Výsledkem jsou dvojice bitů, které představují vždy jednu komplexní hodnotu. Tím je vytvořena biometrická šablona.

Tabulka 4.1: Kombinace bitů

Znaménko reálné části	Znaménko imaginární části	Výsledná dvojice bitů
−	−	00
−	+ nebo 0	01
+ nebo 0	−	10
+ nebo 0	+ nebo 0	11

4.1.5 Porovnání

Pro porovnávání kódů duhovek byla zvolena Hammingova vzdálenost. Implementace disponuje dvěma možnými způsoby porovnání kódů duhovek. Prvním z nich je porovnávání v aplikaci, kdy jsou získána data z databáze a následně porovnána s daty aktuálně zpracovávanými. Tento způsob však nechrání uložená data. Druhým způsobem je porovnání kódů v databázi. O tom pojednává následující část práce.

Při snímání oka může dojít k natočení hlavy a tím i k natočení textury duhovky. Ve snaze docílit co nejpřesnějších výsledků je při porovnání šablona duhovky posouvána doprava a doleva a je hledána nejnižší Hammingova vzdálenost, která je poté výstupem porovnání.

Rozhodnutí pak probíhá porovnáním výsledného skóre s nastaveným prahem. Na základě analýzy provedené v části vyhodnocení byla zvolena prahová hodnota $0,32$.

4.2 Implementace datového úložiště

V této části je popsáno datové úložiště pro potřeby aplikace na rozpoznávání uživatelů na základě oční duhovky. Pro implementaci datového úložiště byla zvolena databáze MongoDB. Pro zajištění komunikace aplikace s datovým úložištěm byl použit ovladač PyMongo.

4.2.1 Datové úložiště

Aby bylo možné provádět verifikaci a identifikaci uživatelů, je třeba mít uložené všechny biometrické šablony na jednom místě. Pokud by tato data byla uložena přímo v aplikaci nebo v lokálním úložišti uživatele, pak by součástí instalace aplikace musela být i všechna data. Proto je vhodnější vytvořit databázi pro ukládání těchto dat. Tento databázový systém může běžet buď lokálně spolu s aplikací v systému uživatele, nebo může běžet na vzdáleném serveru. Implementovaná aplikace pak představuje klienta, který se k této databázi připojuje. Výhodou je i to, že se k jedné databázi může připojit několik klientů najednou. Pokud je zvolen databázový systém, který umožňuje horizontální škálování, pak lze využít distribuce dat na více uzlů systému. Díky tomu se pak k jedné databázi může připojit v podstatě neomezený počet klientů. To může být výhodné například v případě využití více přístupových zařízení v rámci jedné organizace.

Pro implementaci datového úložiště lze použít klasické relační databáze, nebo lze sáhnout po nějaké alternativě ze světa NoSQL databází. Oblast nerelačních databází se v poslední době velmi vyvíjí, tyto technologie jsou neustále zdokonalovány a pokrývají čím dál více potřeb uživatelů. Proto jsou v této práci pro implementaci datového úložiště použity právě NoSQL databáze.

Cílem těchto databází je nabídnout řešení pro nové typy aplikací, pro které klasické relační databáze nejsou úplně vhodné. K dispozici jsou 4 základní typy NoSQL databází. Konkrétně se jedná o sloupcové, dokumentové, grafové databáze a databáze typu klíč-hodnota. Pro řešení implementované aplikace nejsou vhodné grafové databáze, jelikož data uložených očních duhovek nemají grafovou strukturu. Taktéž jsou nevyhovující databáze typu klíč-hodnota, protože nabízejí pouze efektivní hledání hodnot podle klíče. Pokud by bylo třeba provádět dotazy nad kódy duhovek, pak by tyto databázové systémy byly nepoužitelné. Sloupcové a dokumentové databáze jsou pro implementované řešení vyhovující. Dokumentové databáze mají navíc tu výhodu, že není třeba definovat schéma ukládaných záznamů. Pokud by bylo nutné v budoucnu schéma změnit, není třeba složitě měnit definici dat, jako tomu je v případě klasických relačních databází.

Z těchto důvodů byla pro implementaci datového úložiště zvolena multiplatformní NoSQL dokumentová databáze MongoDB. Tento databázový systém běží pod veřejnou licencí na straně serveru (SSPL) [20]. MongoDB ukládá záznamy jako dokumenty, které jsou ve formátu BSON, tedy v binární repre-

zentaci JSON dokumentů. Samotné dokumenty se skládají z datových položek typu klíč-hodnota, kde klíč představuje datový typ `string` a hodnota může představovat kterýkoliv z datových typů BSON formátu [18]. Hodnota tedy může obsahovat i další dokument či pole dokumentů.

Pro uložení dokumentů je třeba vytvořit v systému MongoDB databázi a v ní kolekci, která slouží k uložení jednotlivých dokumentů. Pro účely implementované aplikace byla vytvořena databáze `iris` a v ní kolekce s názvem `iriscodes`. Jednotlivé dokumenty pak vypadají následovně:

```
{
  "_id": ObjectId("606355befe304234c4a8adbc"),
  "username": "novakjan",
  "iriscode": <iriscodeArray>
}
```

Datová položka `_id` představuje primární klíč dokumentu, který musí být unikátní v rámci kolekce. Tento klíč nelze měnit a může být jakéhokoliv datového typu s výjimkou pole. Každý dokument musí obsahovat tuto položku a musí být na prvním místě. Pokud není na první pozici v dokumentu, pak je automaticky přesunuta na začátek dokumentu. Pokud ji vkládaný dokument nemá, pak jí databázový systém MongoDB vytvoří automaticky a její hodnota je datového typu `ObjectID`. Tento datový typ představuje unikátní hodnotu, která má délku 12 bajtů a skládá se z časové známky (Unixový čas) o délce 4 bajty, náhodné hodnoty o délce 5 bajtů a hodnoty čítače o délce 3 bajtů, kdy tento čítač je inicializován náhodně. Další datová položka `username` představuje jméno uživatele a její hodnota obsahuje `String`. V poslední položce `iriscode` je uloženo pole s jednotlivými bity iriskódu. Prvky tohoto pole jsou typu `Boolean`. [19]

4.2.2 Validace dokumentů

Databázový systém MongoDB umožňuje nedefinovat schéma pro dokumenty. Díky této vlastnosti je možné kdykoliv schéma dokumentů rozšířit. Pokud by například v budoucnu bylo potřeba ukládat další informace o jednotlivých uživatelích, lze velmi snadno přidat do dokumentů další datové položky. Zároveň je dobré zajistit, aby dokumenty vždy měly zmíněné položky `username` a `iriscode`. K tomu je využit koncept JSON Schema [19], který umožňuje detailně popsat strukturu dokumentů. Implementace využívá následující JSON Schema:

```
{
  "bsonType": "object",
  "required": [ "username", "iriscode" ],
  "properties": {
    "username": {
      "bsonType": "string",
      "minLength": 5,
      "maxLength": 20,
      "pattern": "^[0-9A-Za-z_]*$",
      "description": "must be a string and is required"
    },
    "iriscode": {
      "bsonType": [ "array" ],
      "minItems": 2048,
      "maxItems": 2048,
      "description": "must be an array and is required",
      "items": {
        "bsonType": "bool"
      }
    }
  }
}
```

Aby byl dokument validní vůči tomuto schématu, musí nutně obsahovat datové položky `username` a `iriscode`. Uživatelské jméno musí být řetězec a musí obsahovat alespoň 5 znaků, ale zároveň nesmí být delší než 20 znaků. Pomocí klíčového slova `pattern` lze definovat regulární výraz, který musí uživatelské jméno splňovat. Implementace tohoto schématu tedy navíc vyžaduje, aby uživatelské jméno obsahovalo pouze symboly z anglické abecedy, čísla a podtržítko. Datová položka `iriscode` musí být pole s přesně 2048 položkami `true` nebo `false`.

```
db.createCollection( "iriscodes", {
  "validator": {
    "$jsonSchema": <JSONSchema>
  },
  "validationAction": "error",
  "validationLevel": "moderate"
} )
```

Pomocí výše uvedeného příkazu byla v `mongo` konzoli vytvořena kolekce `iriscodes` s popsanými validačními pravidly. Hodnota `<JSONSchema>` představuje výše zmíněné JSON Schema. Pro validaci schématu jsou využity dvě další možnosti, které určují chování databázového systému. Datová položka

`validationAction` zajistí, aby při operacích zápisu nebylo možné vytvořit nevalidní dokument. Pokud se o to kdokoliv pokusí, vrátí systém MongoDB chybovou hlášku s kódem 121.

Může ale nastat situace, kdy toto chování systému není úplně žádoucí. Pokud jsou v databázi dokumenty, které vyhovují tomuto schématu, avšak v budoucnu bude schéma změněno a bude vyžadovat další povinnou položku, současné dokumenty nebudou validní vůči novému schématu, jelikož novou položku neobsahují. To systému MongoDB nevadí, avšak kvůli hodnotě `error` u položky `validationAction` nebude moci provádět některé potřebné změny. Pokud by například bylo třeba u původních dokumentů změnit pouze iriskód, pak to systém neumožní. Tento problém řeší hodnota `moderate` u datové položky `validationLevel`. Toto nastavení umožní provést nevalidní úpravu pouze v případě, že původní dokument v kolekci také nebyl validní.

4.2.3 Dotazy

Tato sekce obsahuje dotazy, které byly použity v implementaci pro manipulaci s daty. V první řadě je potřeba vložit dokument do databáze. K tomu slouží následující dotaz.

```
db.iriscodes.insertOne(
  {
    "username": <name>,
    "iriscode": <iriscode>
  }
)
```

Je nutné zmínit, že všechny operace pro zápis jsou atomické na úrovni dokumentu. Místo hodnot `<name>` a `<iriscode>` se používají skutečné hodnoty uživatelského jména a iriskódu.

```
db.iriscodes.find(
  {
    "username": <user>
  },
  {
    "_id": 1,
    "username": 1
  }
)
```

Dále je využíván výše uvedený dotaz pro vyhledání záznamu. V metodě `find()` lze uvést kritéria selekce (první parametr) a projekce (druhý parametr). V předchozím dotazu je tedy vybrán uživatel s uživatelským jménem `<user>` a ve výsledku jsou uvedeny pouze datové položky `_id` a `username`.

```
db.iriscodes.deleteOne(
  {
    "username": <user>
  }
)
```

Výše uvedený dotaz slouží k odstranění konkrétního uživatele a jeho referenční biometrické šablony z databáze.

Pro odstranění všech zaregistrovaných uživatelů a jejich biometrických šablon je použit následující dotaz.

```
db.iriscodes.deleteMany({})
```

4.2.4 Indexy

Při vyhodnocování dotazu pro vyhledávání dokumentů, musí databázový systém MongoDB projít všechny dokumenty v kolekci sekvenčně a vybrat ty, co splňují kritéria selekce. To v případě velkého množství záznamů může být velmi neefektivní. Proto je vhodné vytvořit index nad klíčem `username`. To lze velmi snadno pomocí následujícího příkazu.

```
db.iriscodes.createIndex(
  {
    "username": 1
  }
)
```

Vytvořené indexy používají strukturu B-stromů, které umožňují snadno a rychle procházet dokumenty a vybrat ty, které splňují kritéria selekce.

4.2.5 Verifikace

Kromě jednoduchých dotazů pro čtení a zápis umožňuje MongoDB provádět a vyhodnocovat složitější agregované dotazy. K dispozici jsou tři základní možnosti provádění agragací nad dokumenty. Jedná se o koncepty Aggregation Pipeline, Single Purpose Aggregation Operations a MapReduce. Pro implementaci verifikace a identifikace byl zvolen koncept Aggregation Pipeline, který je postaven na konceptu Data Pipeline. Dokumenty jsou postupně zpracovány pomocí jednotlivých operací a jsou transformovány na agregovaný výsledek. Výstup jedné operace slouží jako vstup pro další operaci. Dotaz pro verifikaci je implementován následovně:

```
db.collection.aggregate([
  { "$match": { "username": <user> } },
  { "$project": { "XORarray": <XORarray> } },
  { "$project":{
      "hammingDistance": {
        "$size": {
          "$filter": {
            "input": "$XORarray", "as": "bool", "cond": {
              "$eq": [ "$$bool", true ]
            }
          }
        }
      }
    }},
  { "$project":{
      "result":{
        "$cond": {
          "if": {
            "$lte": [ "$hammingDistance", <threshold> ]
          },
          "then": true,
          "else": false
        }
      }
    }
  }
])
```

V první části agregačního dotazu pro verifikaci uživatele je použit agregační operátor `$match`. Pomocí tohoto operátoru lze provést selekci záznamů na základě uživatelského jména. Jelikož se verifikace týká pouze jednoho uživatele, je možné vyfiltrovat pouze tento jeden záznam pro daného uživatele. Výstupem této operace je dokument, který obsahuje pouze zadané uživatelské jméno v proměnné `<user>`. Následuje agregační operace `$project`, pomocí které lze provést projekci. Pomocí této operace je sestaveno pole, které obsahuje výsledky všech operací $A_i \oplus B_i$, kde A_i je i-tý bit iriskódu daného uživatele v databázi a B_i je i-tý bit v porovnávaném poli. Výsledkem této operace je dokument, ve kterém má daný uživatel položku `XORarray` obsahující vypočtené pole. Z tohoto pole lze vypočítat počet odlišných bitů porovnávaných polí, jelikož operace XOR vrací hodnotu 1 v případě odlišných bitů a 0 v případě bitů shodných. Proto druhá projekce počítá počet prvků v poli, které obsahují hodnotu `true`. Tato projekce uloží počet odlišných bitů do datové položky `hammingDistance`. Poslední agregační operátor představuje opět projekci, která pouze zkontroluje, zda je počet odlišných bitů přípustný pomocí

hodnoty v proměnné `<threshold>`. Výsledkem této projekce je dokument, ve kterém má daný uživatel datovou položku `result`, která obsahuje hodnotu `true` v případě, že byla verifikace uživatele úspěšná, `false` v případě, že byla neúspěšná. Výsledek tohoto dotazu je ve formátu `{_id:<userId>, result: <boolean> }`.

V předchozím dotazu nebyla popsána struktura proměnné `XORarray`. V této proměnné je uloženo pole, jehož prvky jsou předzpracovány pro operaci XOR. Jelikož operaci XOR MongoDB nenabízí, byla implementována pomocí agregačních operátorů `$and`, `$or` a `$not`. Z matematické logiky totiž platí:

$$(A \oplus B) \Leftrightarrow ((A \wedge \neg B) \vee (\neg A \wedge B)).$$

Pro všechny prvky v porovnávaném poli je tedy vytvořen tento prvek pole `XORarray`. Zde i značí i-tý bit pole a `iriscodeArray` představuje zadané pole s iriskódem. Pomocí agregačního operátoru `$arrayElemAt` lze přistoupit k danému prvku pole, které je uloženo v databázi.

```
{
  "$or": [ {
    "$and": [ {
      "$not": [ {
        "$arrayElemAt":["$iriscode",i]
      } ]
    },
    iriscodeArray[i]
    ]
  },
  {
    "$and": [ {
      "$arrayElemAt":["$iriscode",i]
    },
    {
      "$not":[ iriscodeArray[i] ]
    } ]
  } ]
}
```

Porovnávání zadaného pole s polem v databázi probíhá pouze na úrovni databáze. Tímto dotazem uniká z databáze pouze jedna informace. Touto informací je, zda je počet odlišných bitů iriskódů větší nebo menší (či rovno) než stanovená hranice, tudíž hodnota `true` nebo `false`.

4.2.6 Identifikace

Pro implementaci dotazu pro identifikaci byl také zvolen koncept Aggregation Pipeline. Na rozdíl od verifikace je nutné provést porovnání iriskódu u všech uživatelů v databázi. Zde už však nestačí pouze hodnota `true` nebo `false` značící shodu nebo neshodu při porovnávání. Je třeba znát také uživatele, jejichž Hammingova vzdálenost je nižší než nastavený práh. Dotaz vypadá následovně:

```
db.collection.aggregate([
  { "$project": {
      "username": "$username",
      "XORarray": <XORArray>
  }},
  { "$project":{
      "username": "$username",
      "hammingDistance": {
        "$size": {
          "$filter": {
            "input": "$XORarray", "as": "bool", "cond": {
              "$eq": [ "$$bool", true ]
            }
          }
        }
      }
  }},
  { "$project":{
      "username": "$username",
      "result":{
        "$cond": {
          "if": {
            "$lte": [ "$hammingDistance", <threshold> ]
          },
          "then": true,
          "else": false
        }
      }
  }},
  { "$match": { "result": true } },
  { "$project":{ "username": "$username" } }
])
```

Dotaz začíná velmi podobně jako v případě verifikace. Zde však není provedena selekce uživatelů, jelikož výpočet je proveden pro všechny uživatele v databázi. První dvě projekce jsou téměř shodné s prvními projekcemi v dotazu pro verifikaci. Zde je ale navíc ponechána u každého uživatele datová položka `username`. Výsledkem těchto dvou projekcí je tedy seznam všech uživatelů, kteří obsahují datové položky `_id`, `username` a `hammingDistance` obsahující počet odlišných bitů s porovnávaným iriskódem. Další agregační operátor představuje opět projekci, která zkontroluje, zda je počet odlišných bitů přípustný pomocí hodnoty v proměnné `<threshold>`. Výsledkem této projekce jsou dokumenty, ve kterých mají uživatelé datovou položku `result`, která obsahuje hodnotu `true` v případě, že byla identifikace uživatele úspěšná, v opačném případě hodnotu `false`. Poslední projekce je použita pouze pro úpravu struktury záznamu. Ani v tomto případě se žádný z uložených iriskódů nedostane ven z databáze. Dotaz pouze poskytne uživatelská jména všech uživatelů, kteří v porovnání uspěli.

4.2.7 Zabezpečení

Aby bylo možné používat databázi MongoDB, musí být spuštěn daemon proces `mongod`, který zpracovává požadavky klientů, spravuje přístup k datům a prování potřebné operace na pozadí. Proces `mongod` je v základním nastavení spuštěn na TCP portu 27017. Tento port lze případně změnit pomocí přepínače `--port <port>`.

Pomocí přepínače `--auth` při spouštění serveru lze povolit autorizaci k řízení přístupu uživatele k databázovým prostředkům a operacím. V případě, že je zapnuta autorizace, pak je vyžadováno, aby se každý klient nejprve autentizoval, než bude rozhodnuto o jeho přístupu. Uživatel musí zadat své uživatelské jméno a heslo, k tomu je použit následující dotaz.

```
db.auth( {
  "user": <username>,
  "pwd": <password>,
  "mechanism": "SCRAM-SHA-256"
} )
```

Místo hodnot `<username>` a `<password>` je zadáno příslušné uživatelské jméno a heslo. Hodnota `SCRAM-SHA-256` značí použitý mechanismus ověřování. Pokud je autentizace úspěšná, příkaz vrátí hodnotu 1, v opačném případě 0.

V databázi byly pro demonstrační účely vytvořeny dva typy účtů, které slouží k přihlášení do aplikace, zároveň k autentizaci klienta a přidělení příslušných oprávnění. Prvním typem je běžný uživatelský účet. Takový uživatel je oprávněn pouze k vykonávání procesu identifikace či verifikace. Dalším typem je administrátorský účet. Tento uživatel může navíc provádět registraci nových uživatelů do databáze a mazání uživatelů z databáze. Uživatelský účet je vytvořen následujícím příkazem.

```
db.createUser( {
  "user": <username>,
  "pwd": <password>,
  "roles": [ { role: <role>, db: "iris" } ],
  "mechanisms": [ "SCRAM-SHA-256" ]
 } )
```

Hodnota `<username>` označuje uživatelské jméno, `<password>` příslušné heslo. Hodnota `<role>` definuje oprávnění uživatele pro danou databázi. Administrátorský účet má nastavenou roli `readWrite`, která uživateli umožňuje číst a upravovat data, běžný uživatel má roli `read`, která dovoluje pouze čtení dat. Hodnota `SCRAM-SHA-256` zde opět značí použitý mechanismus ověřování.

Komunikace mezi klientem a serverem je šifrována pomocí protokolu TLS. Pro povolení TLS pro všechna síťová připojení slouží přepínač `--tlsMode <mode>`, kde `<mode>` je nastaven na hodnotu `requireTLS`. Server tak používá pouze šifrovaná TLS připojení.

Kapitola 5

Demonstrační program

V této kapitole jsou popsány funkce demonstračního programu. Aplikace podporuje práci v režimu registrace, verifikace a identifikace. Demonstrační program je k dispozici na přiloženém DVD.

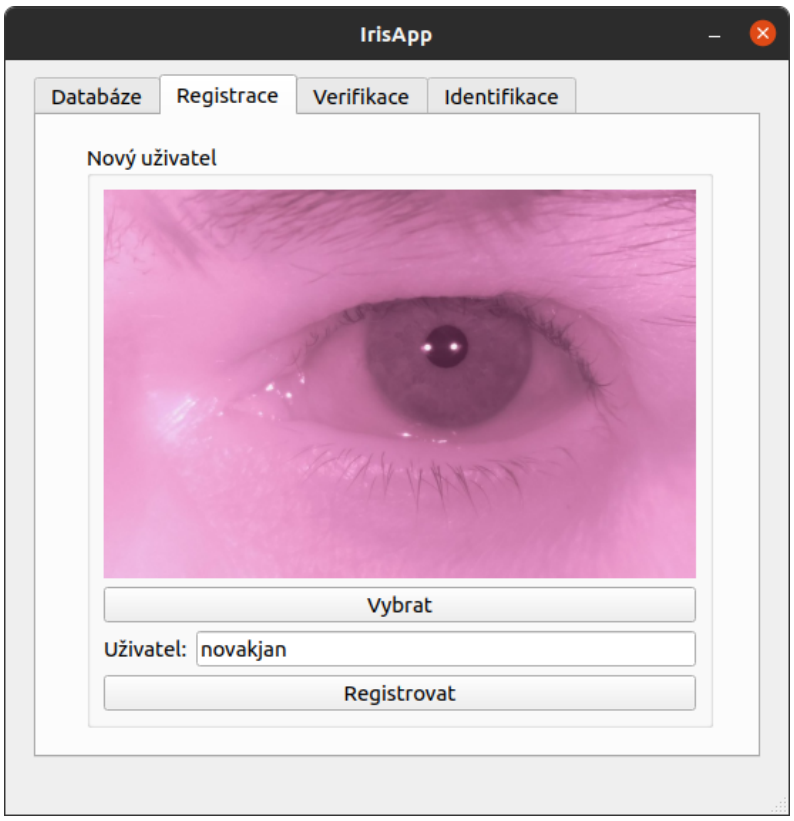
5.1 Přihlášení

Po spuštění aplikace je nejprve vyžadováno přihlášení uživatele pomocí příslušného uživatelského účtu popsaného v části 4.2.7. V případě úspěšného přihlášení jsou uživateli přidělena příslušná oprávnění, v opačném případě je přístup zamítnut. Tyto účty přiděluje uživatelům administrátor databáze, proto zde není možnost vytvoření nového účtu nebo jeho smazání.

Obrázek 5.1: Demonstrační program – přihlášení do aplikace

5.2 Registrace

Aplikace využívá demonstračních snímků popsaných v části 3.3. Při registraci uživatel předkládá svou fyzickou i elektronickou identitu. Pokud zadané uživatelské jméno již v databázi existuje, je registrace odmítnuta. V opačném případě je předložený snímek duhovky zpracován. Je vytvořena příslušná biometrická šablona, která je následně porovnána se všemi šablonami v databázi. Pokud je pro nastavenou prahovou hodnotu nalezena shoda s nějakou z referenčních šablon, je registrace odmítnuta. Jinak je výsledná biometrická šablona spolu s identifikací uživatele uložena do databáze.

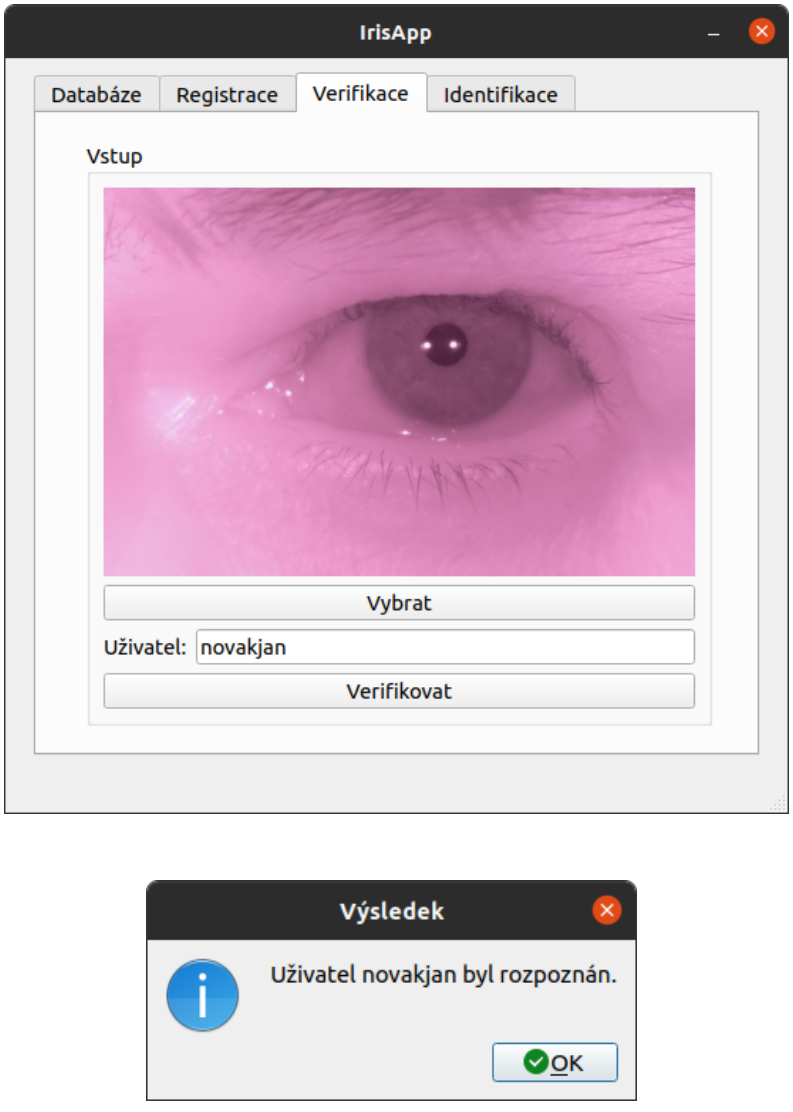


Obrázek 5.2: Demonstrační program – registrace uživatele

Pro demonstrační účely a usnadnění testování funkčnosti rozpoznávání umožňuje aplikace i registraci všech demonstračních snímků najednou, případně smazání jednoho nebo všech uživatelů z databáze.

5.3 Verifikace

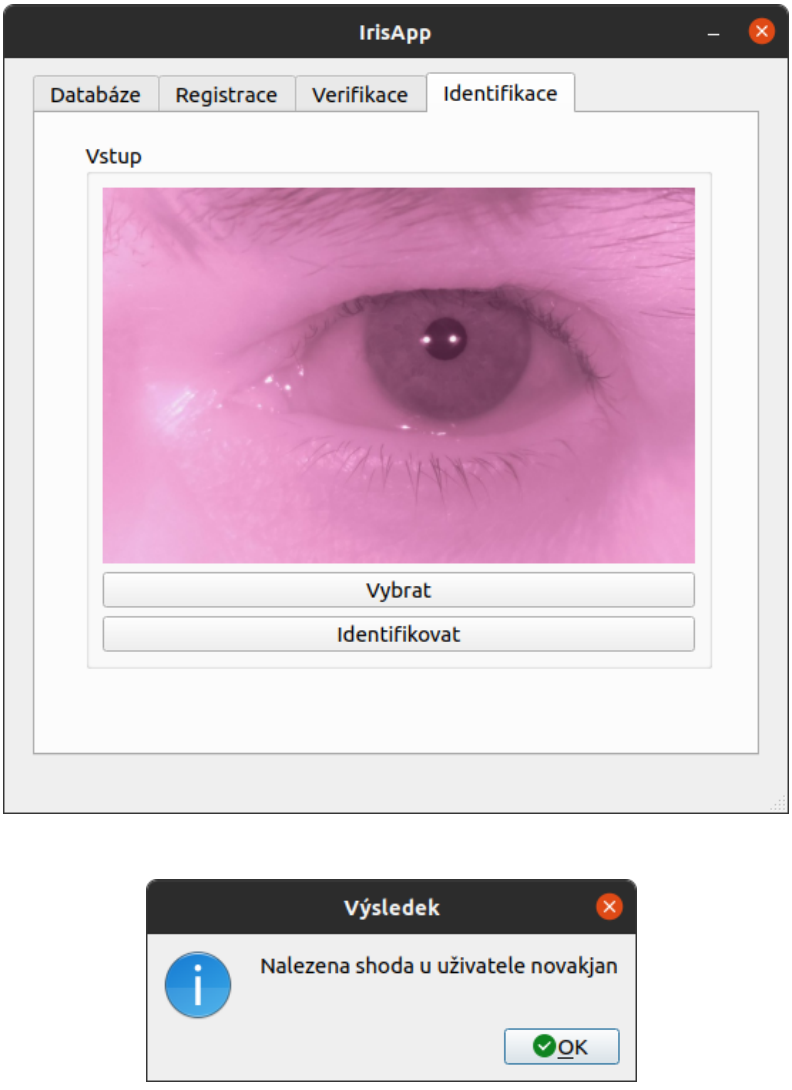
V režimu verifikace uživatel předkládá spolu se svou duhovkou navíc svou elektronickou identitu. Pokud zadané uživatelské jméno v databázi neexistuje, pak je verifikace uživatele ukončena. V opačném případě je duhovka zpracována a je vytvořena biometrická šablona. Dle uživatelského jména je v databázi vyhledána příslušná referenční šablona, která je porovnána s právě získanou šablonou. Nakonec je zobrazeno rozhodnutí o přijetí identity nebo jejím odmítnutí.



Obrázek 5.3: Demonstrační program – verifikace uživatele

5.4 Identifikace

V režimu identifikace uživatel předkládá systému svou duhovku, která je zpracována. Výsledná biometrická šablona je porovnána se všemi referenčními šablonami uloženými v databázi. V případě nalezení shody je na výstupu zobrazeno příslušné uživatelské jméno. Pokud je pro nastavenou prahovou hodnotu nalezeno osob více, pak je vypsán seznam všech těchto osob. V opačném případě je identita nenalezena.



Obrázek 5.4: Demonstrační program – identifikace uživatele

Kapitola 6

Vyhodnocení

V této kapitole je prezentována časová náročnost implementace, spolehlivost a bezpečnost systému. Pro testování byla použita kompletní databáze nafocených snímků. Naměřená data jsou k dispozici na přiloženém DVD.

6.1 Časová náročnost

V této části je testována rychlost implementace. Testování proběhlo na počítači s procesorem Intel Core i7-9850H 2.60GHz a s operačním systémem Ubuntu 20.04.2 LTS. Měření bylo provedeno pro všechny snímky z databáze, výsledkem je vždy průměrný čas všech těchto měření.

V tabulce 6.1 jsou uvedeny naměřené průměrné časy jednotlivých fází rozpoznávání. Nejvíce časově náročný je proces segmentace duhovky, konkrétně část nalezení vnějšího okraje duhovky. To je způsobeno použitím Houghovy transformace a následným výběrem nejlépe vyhovující kružnice.

Tabulka 6.1: Průměrné časy jednotlivých kroků rozpoznávání

Operace	Čas běhu [s]
Segmentace – celkem	5,362
Segmentace – vnitřní okraj duhovky	0,796
Segmentace – vnější okraj duhovky	4,356
Normalizace – celkem	0,067
Extrakce rysů – celkem	1,389

Průměrné časy registrace, verifikace a identifikace jsou uvedeny v tabulce 6.2. Do měření času byl zahrnut celý proces rozpoznávání, to znamená i samotné vytvoření biometrické šablony z předloženého snímku a následně její porovnání v databázi. Do času registrace nebyl započítán čas ověřování, zda se již daná fyzická identita nenachází v databázi, jelikož se jedná o totéž jako v případě identifikace.

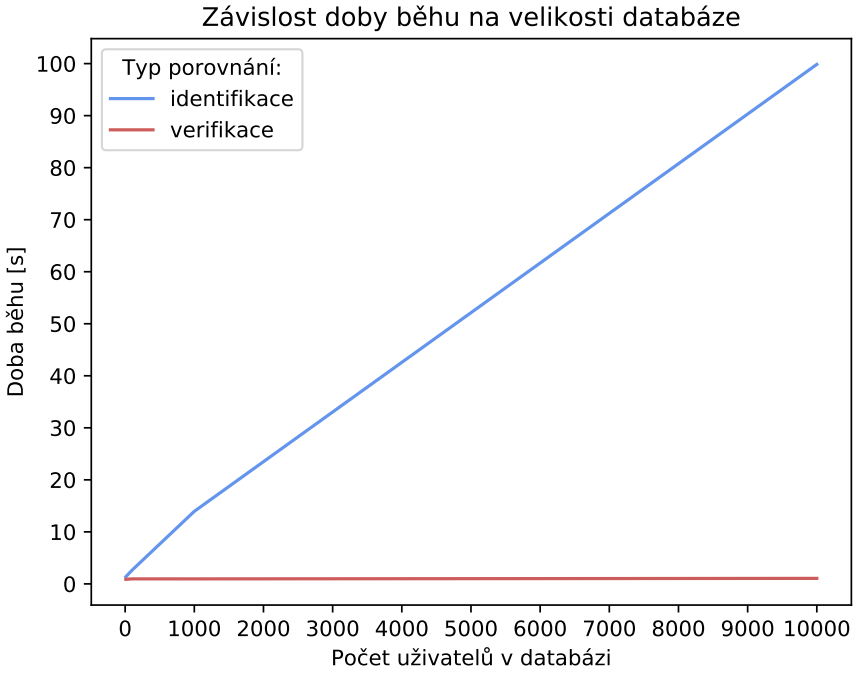
Tabulka 6.2: Průměrné časy registrace, verifikace a identifikace

Operace	Čas běhu [s]
Registrace	6,821
Verifikace	7,332
Identifikace	8,588

Dále byly změřeny časy porovnávání šablon v databázi při verifikaci a při identifikaci. Databáze byla naplněna náhodnými daty. Do měření času není započítána část rozpoznávání.

Tabulka 6.3: Průměrné časy porovnání v závislosti na velikosti databáze

Počet uživatelů v databázi	Čas verifikace [s]	Čas identifikace [s]
10	0,881	1,377
100	0,966	2,633
1000	0,963	13,945
10000	1,061	99,851



Obrázek 6.1: Závislost doby běhu na velikosti databáze

Z tabulky 6.3 a obrázku 6.1 vyplývá, že rychlost identifikace je na rozdíl od verifikace velmi závislá na velikosti databáze, to znamená na celkovém počtu uložených šablon. Při verifikaci je za pomoci předložené elektronické identity vyhledána příslušná referenční biometrická šablona, se kterou je aktuálně získaná šablona porovnána. Dochází tedy pouze k jednomu porovnání. Při identifikaci se však prochází celá databáze a dochází k porovnání aktuální šablony se všemi referenčními šablonami v databázi.

6.2 Vliv hodnoty prahu na spolehlivost a bezpečnost systému

Nastavená prahová hodnota má velký vliv na výsledek porovnání a tím i na spolehlivost a bezpečnost biometrického systému. Čím níže je práh nastaven, tím je systém bezpečnější. Jinými slovy, je menší pravděpodobnost, že dojde k chybnému přijetí neoprávněné osoby. Na druhou stranu může docházet k chybnému odmítnutí oprávněné osoby, což může značně snížit uživatelskou přívětivost systému. Čím výše je práh nastaven, tím uživatelská přívětivost roste, jelikož nejsou oprávnění uživatelé chybně odmítáni. Bezpečnost systému naopak klesá, velmi se zvyšuje riziko chybného přijetí neoprávněné osoby.

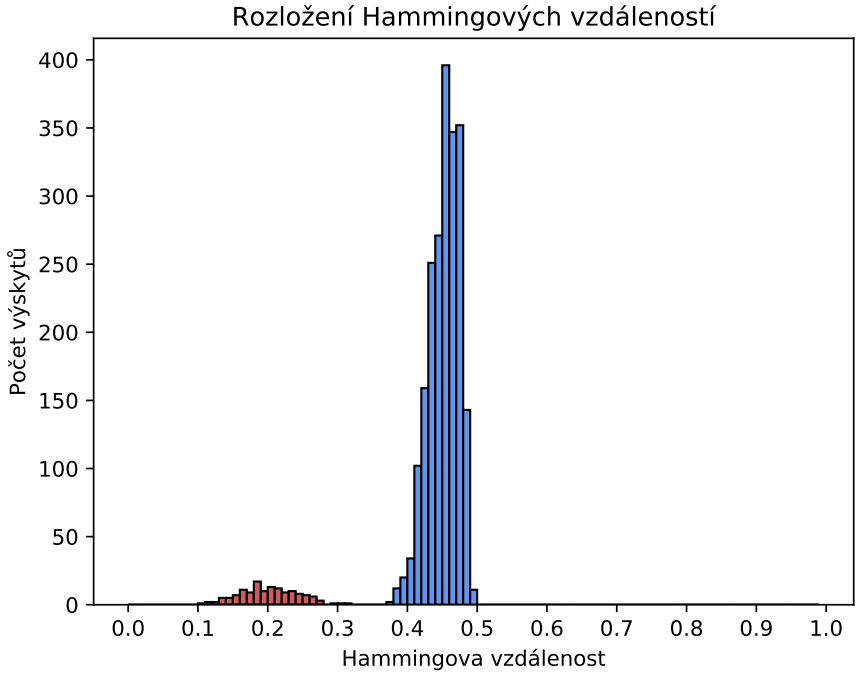
Chybné odmítnutí je tedy v případě verifikačních aplikací nežádoucí z hlediska uživatelské přívětivosti a spolehlivosti systému. Z pohledu identifikačních aplikacích se jedná o závažný nedostatek. Osoba u které má dojít k potvrzení identity totiž nemusí být rozpoznána. Chybné přijetí je z hlediska verifikačních aplikací považováno za bezpečnostní incident. V případě identifikačních aplikací může být osoba, u které má dojít k potvrzení identity, chybně ztotožněna s jinou osobou.

Tabulka 6.4 obsahuje počty chybných přijetí a chybných odmítnutí v závislosti na nastavené prahové hodnotě. Pro každý uvedený práh, byly mezi sebou porovnány všechny snímky a následně byla vyhodnocena chybovost systému. V rozmezí hodnot od 0,32 do 0,37 v tomto případě nedochází k žádné z výše uvedených chyb. K eliminaci chyb je vhodné umístit prahovou hodnotu do tohoto rozmezí. Aby bylo dosaženo vyšší bezpečnosti systému, byla prahová hodnota demonstrační aplikace nastavena co nejníže, konkrétně na hodnotu 0,32. Hodnoty nižší než 0,10 a vyšší než 0,50 nejsou již v tabulce uvedeny, jelikož počty chybných přijetí a odmítnutí jsou stejné jako v případě těchto krajních hodnot.

Tabulka 6.4: Vliv prahové hodnoty na spolehlivost a bezpečnost systému

Prahová hodnota	Počet chybných přijetí	Počet chybných odmítnutí
0,10	0	140
0,11	0	139
0,12	0	137
0,13	0	135
0,14	0	130
0,15	0	125
0,16	0	118
0,17	0	107
0,18	0	98
0,19	0	81
0,20	0	71
0,21	0	58
0,22	0	46
0,23	0	37
0,24	0	27
0,25	0	18
0,26	0	12
0,27	0	6
0,28	0	3
0,29	0	3
0,30	0	2
0,31	0	1
0,32	0	0
0,33	0	0
0,34	0	0
0,35	0	0
0,36	0	0
0,37	0	0
0,38	2	0
0,39	14	0
0,40	34	0
0,41	68	0
0,42	170	0
0,43	329	0
0,44	580	0
0,45	851	0
0,46	1247	0
0,47	1594	0
0,48	1946	0
0,49	2089	0
0,50	2100	0

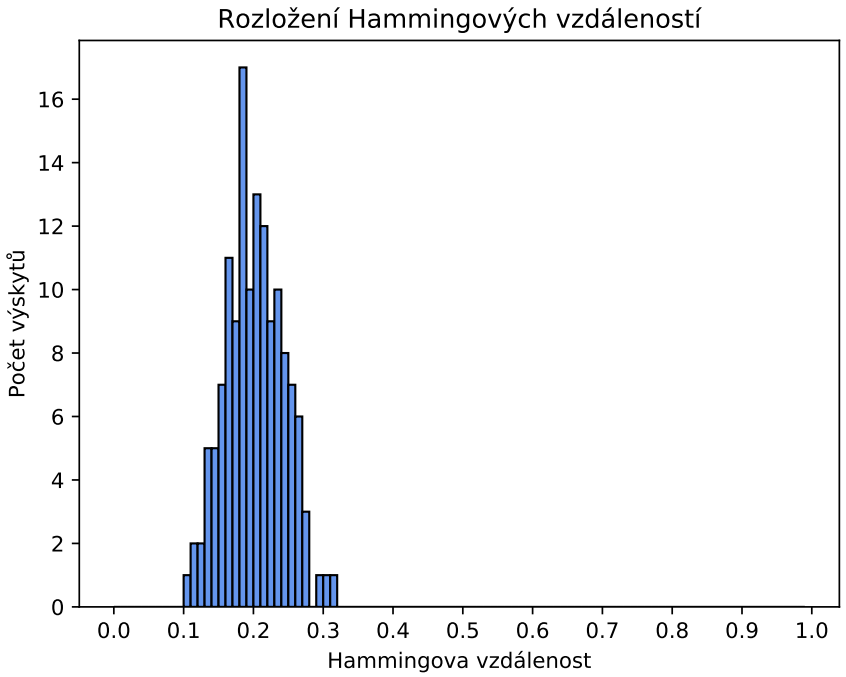
Na obrázku 6.2 je vyobrazen histogram rozdělení ztotožnění oprávněných a neoprávněných uživatelů. Červená oblast v levé části obrázku znázorňuje rozdělení míry ztotožnění oprávněného uživatele, modrá oblast v pravé části zobrazuje rozdělení míry ztotožnění neoprávněných uživatelů.



Obrázek 6.2: Rozložení Hammingových vzdáleností oprávněných a neoprávněných uživatelů

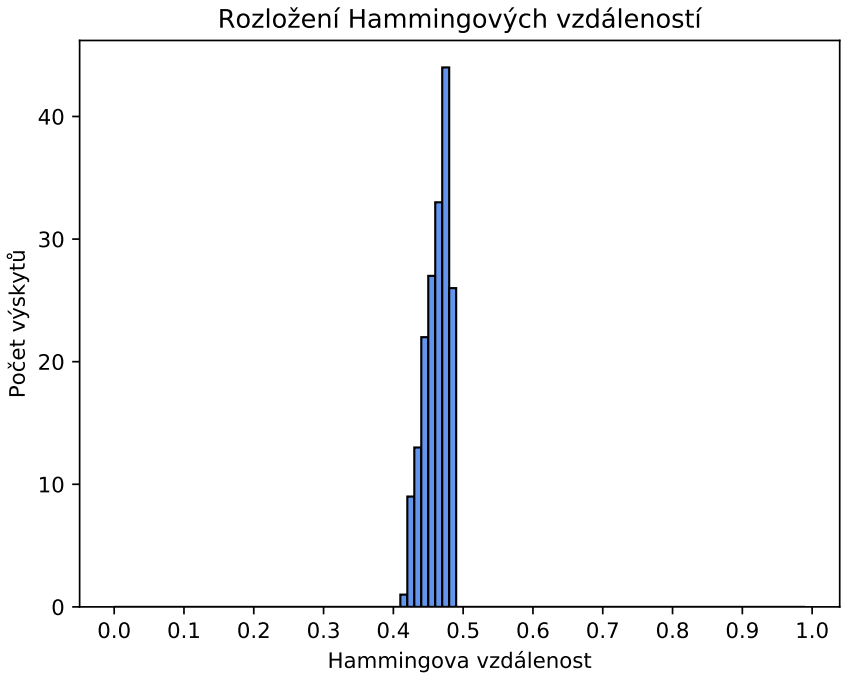
6.3 Výsledky porovnání

Histogram na obrázku 6.3 zobrazuje distribuci Hammingových vzdáleností získaných pomocí 140 porovnání mezi duhovkami pocházejícími ze stejného oka. Naměřená střední hodnota Hammingovy vzdálenosti je 0,2 se směrodatnou odchylkou 0,04. Minimální naměřená hodnota vzdálenosti je 0,109 a maximální hodnota je 0,318.



Obrázek 6.3: Rozložení Hammingových vzdáleností mezi různými snímky stejných duhovek

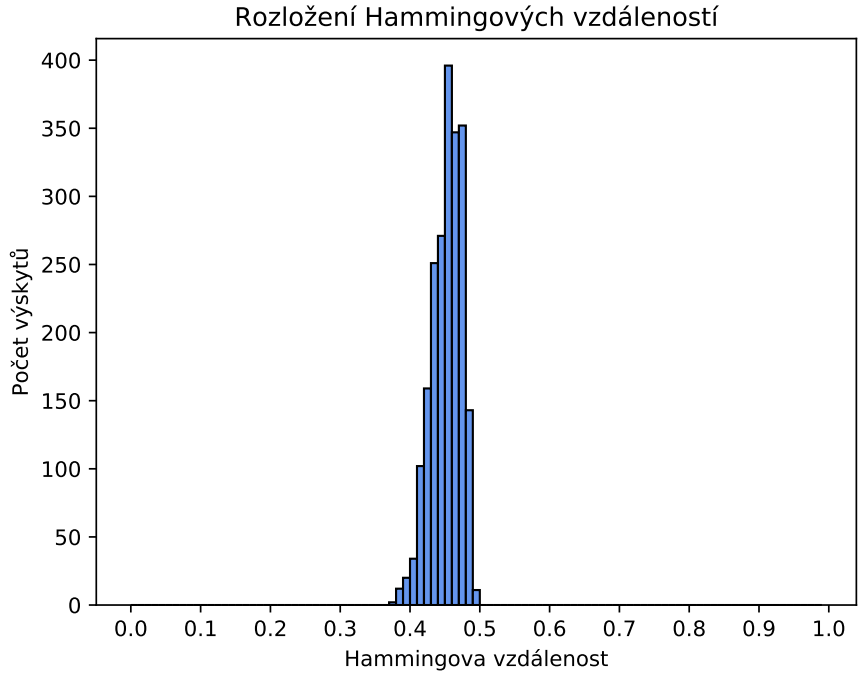
Na obrázku 6.4 je zobrazeno rozložení Hammingových vzdáleností mezi pravými a levými duhovkami pocházejících od stejné osoby. Celkem bylo provedeno 175 porovnání mezi různými páry duhovek. Byla naměřena střední hodnota 0,46 se směrodatnou odchylkou 0,017. Nejnižší hodnotou je 0,41, nejvyšší 0,48.



Obrázek 6.4: Rozložení Hammingových vzdáleností mezi pravými a levými duhovkami

Z výše uvedeného histogramu vyplývá, že ačkoliv obě duhovky vždy pocházejí od stejného jedince, jsou jejich vzory odlišné. Proto pokud uživatel nemá v systému zaregistrovány duhovky obě, není možné se prokazovat druhou duhovkou, která není v systému zaregistrována.

Histogram na obrázku 6.5 zobrazuje distribuci Hammingových vzdáleností všech možných srovnání mezi duhovkami pocházejícími od odlišných osob. Celkem bylo provedeno 2100 porovnání. Srovnání pravého oka s levým konkrétní osoby bylo vynecháno. Byla naměřena střední hodnota 0,45 se směrodatnou odchylkou 0,02. Minimální zaznamenaná hodnota Hammingovy vzdálenosti byla 0,37 a maximální 0,49.



Obrázek 6.5: Rozložení Hammingových vzdáleností mezi různými duhovkami

6.4 Útok na snímací zařízení

Pro realizaci útoku byly z databáze nafocených duhovek vybrány náhodně tři snímky, každý pocházející od jiné osoby. Tyto snímky byly vytištěny na černobílé laserové tiskárně a předloženy před snímací zařízení. Kvůli špatné kvalitě tisku nebyl systém schopen správně lokalizovat vnější hranici duhovky a útok tedy nebyl zdařilý. Následně byly vybrané snímky duhovek předloženy před kameru prostřednictvím obrazovky mobilního telefonu v barevné podobě a poté v šedotónové variantě. V obrazovce telefonu se odráží světlo z infračervených LED připojených ke kameře. Obě LED byly tedy před samotným snímáním zakryty. Každá z následujících tabulek shrnuje výsledky útoku pro konkrétní osobu. Rozhodovací práh systému byl nastaven na hodnotu 0,32. Ve

sloupci s názvem původní snímek je pro srovnání uvedena Hammingova vzdálenost mezi originálním snímkem a všemi dalšími nafocenými snímky oka dané osoby. Nula značí, že byl snímek porovnán sám se sebou a vzdálenost mezi nimi je tedy nulová. Další dva sloupce shrnují výsledky porovnání podvrženého snímku se snímky z databáze.

Tabulka 6.5: Hodnoty Hammingovy vzdálenosti – osoba 1

	původní snímek	útok – barevný	útok – odstíny šedi
snímek 1	0,206	0,277	0,331
snímek 2	0,211	0,311	0,399
snímek 3	0,214	0,299	0,352
snímek 4	0	0,265	0,286
snímek 5	0,182	0,304	0,315

Tabulka 6.6: Hodnoty Hammingovy vzdálenosti – osoba 2

	původní snímek	útok – barevný	útok – odstíny šedi
snímek 1	0,192	0,239	0,276
snímek 2	0,187	0,257	0,302
snímek 3	0,150	0,255	0,280
snímek 4	0	0,294	0,272
snímek 5	0,179	0,287	0,310

Tabulka 6.7: Hodnoty Hammingovy vzdálenosti – osoba 3

	původní snímek	útok – barevný	útok – odstíny šedi
snímek 1	0,133	0,362	0,268
snímek 2	0	0,315	0,237
snímek 3	0,140	0,316	0,256
snímek 4	0,132	0,341	0,265
snímek 5	0,135	0,356	0,252

Z celkových třiceti pokusů byl útok pouze šestkrát neúspěšný. Třikrát v případě předložení barevného snímku a třikrát při předložení snímku v odstínech šedi. Na základě naměřených dat tedy nelze rozhodnout, která z variant je pro útok vhodnější. Pro praktické nasazení biometrického systému je z hlediska bezpečnosti důležité, aby systém prováděl před zpracováním snímku test živosti. Pokud test není implementován, pak není systém bezpečný a lze jej snadno obejít předložením falešné biometrické vlastnosti.

6.5 Registrace

Registraci duhovek uživatelů by měla s uživateli provádět pouze pověřená osoba, neměli by tuto činnost provádět sami. Tím lze částečně předejít k předložení falešné biometrické vlastnosti nebo registraci pod falešnou elektronickou identitou. K tomuto účelu zde slouží administrátorský účet.

Před zaregistrováním uživatele je třeba prověřit, zda již není uživatel v databázi zaregistrován. Nejprve je zkontrolováno, zda se předložená elektronická identita již nenachází v databázi. Pokud ano, je registrace zamítnuta, pokud ne, tak dochází k dalšímu prověření, které proběhne na základě předložené fyzické identity. Získaná šablona je porovnána se všemi šablonami v databázi stejně jako je tomu při identifikaci uživatele. Pokud je nalezena shoda s některou již uloženou šablonou, k registraci nedojde. Pokud naopak, uživatel není nalezen, je do databáze přidán.

6.6 Komunikace aplikace s databází

Komunikace mezi klientem a serverem může být napadena. Může dojít k odchycení přenášených dat, která mohou být následně zneužita. Dále může dojít k záměně dat nebo opětovnému zaslání již dříve použitých dat. Komunikace mezi aplikací a databází je v této implementaci šifrována pomocí TLS protokolu.

6.7 Uložená data

Při zcizení biometrické šablony hrozí možnost jejího zneužití. Z šablony může být sestavena přibližná původní informace, která může být použita k obejití biometrického systému. Protože jsou šablony porovnávány pomocí Hammingovy vzdálenosti s použitím posunů šablony, není tak možné je jednoduše zašifrovat a v takové formě porovnávat. V této implementaci probíhá porovnávání biometrických šablon duhovek v databázi. V režimu verifikace databáze vrací pouze odpověď `true` v případě, že byla identita potvrzena nebo hodnotu `false` v případě, že identita potvrzena nebyla. V režimu identifikace databáze v případě úspěchu vrací uživatelská jména, která byla na základě nastaveného prahu rozpoznána jako osoba jenž předložila svůj biometrický vzorek. Referenční biometrické šablony tak nikdy neopouští databázi.

Závěr

Práce se zabývá biometrií se zaměřením na rozpoznávání osob podle oční duhovky. Byly nastudovány a popsány nejčastěji používané biometrické metody. Dále byl představen obecný princip biometrických systémů, hodnocení jejich spolehlivosti a souhrn základních potenciálně zranitelných míst. Byly popsány nejznámější postupy používané při rozpoznávání osob podle oční duhovky. Bylo navrhnuto levné a dostupné snímací zařízení, s pomocí kterého byly nafoceny demonstrační snímky. Dále byl implementován a následně popsán proces rozpoznávání oční duhovky. Bylo implementováno datové úložiště pro ukládání biometrických šablon a vytvořena demonstrační aplikace, která umožňuje registraci, verifikaci a identifikaci uživatele. V poslední části byla implementace otestována a vyhodnocena její spolehlivost, bezpečnost a časová náročnost.

Hodnocení implementace bylo provedeno na vlastní databázi nafocených snímků duhovek. Na základě zjištěných výsledků porovnání bylo dokázáno, že i s levným a dostupným zařízením lze realizovat systém na rozpoznávání uživatelů podle oční duhovky. Výsledky analýzy vlivu hodnoty prahu na spolehlivost a bezpečnost systému ukázaly, že implementace je pro zvolený práh a snímky malé skupiny osob spolehlivá.

Před snímací zařízení byly předloženy prostřednictvím obrazovky mobilního telefonu vybrané snímky duhovek v barevné a šedotónové variantě. Následně zrealizovaný útok na systém proběhl téměř ve všech pokusech úspěšně. Systém lze tedy poměrně lehce obejít předložením falešné biometrické vlastnosti. Program by bylo vhodné, pro zajištění vyšší úrovně bezpečnosti, rozšířit o implementaci testování živosti duhovky.

Literatura

[1] DRAHANSKÝ, Martin a ORSÁG, Filip. *Biometrie*. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

[2] RAK, Roman, MATYÁŠ, Václav a ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

[3] JAIN, Anil K., ROSS, Arun A. a NANDAKUMAR, Karthik. *Introduction to Biometrics* [online]. Boston: Springer, 2011. [cit. 2021-03-25]. ISBN 978-0-387-77326-1. Dostupné z: DOI: 10.1007/978-0-387-77326-1

[4] BOLLE, Ruud M., CONNELL, Jonathan H., PANKANTI, Sharath, RATHA, Nalini K. a SENIOR, Andrew W. *Guide to Biometrics* [online]. New York: Springer, 2004. [cit. 2021-04-01]. ISBN 978-1-4757-4036-3. Dostupné z: DOI: 10.1007/978-1-4757-4036-3

[5] JAIN, Anil K., ROSS, Arun a PRABHAKAR, Salil. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology* [online]. 2004, **14**(1), 4–20. [cit. 2021-03-27]. ISSN 1051-8215. Dostupné z: DOI: 10.1109/TCSVT.2003.818349

[6] ČIHÁK, Radomír. *Anatomie 3*. 3. upravené a doplněné vydání. Praha: Grada, 2016. ISBN 978-80-247-5636-3.

[7] WYZYKOWSKI, André Brasil Vieira, SEGUNDO, Mauricio Pamplona a LEMES, Rubisley de Paula. *Level Three Synthetic Fingerprint Generation* [online]. 2020. [cit. 2021-04-13]. Dostupné z: https://arxiv.org/pdf/2002.03809.pdf

[8] SYNEK, Svatopluk a SKORKOVSKÁ, Šárka. *Fyziologie oka a vidění*. 2. doplněné a přepracované vydání. Praha: Grada, 2014. ISBN 978-80-247-3992-2.

[9] MERKUNOVÁ, Alena a OREL, Miroslav. *Anatomie a fyziologie člověka pro humanitní obory*. Praha: Grada, 2008. ISBN 978-80-247-1521-6.

[10] LI, Stan Z. a JAIN, Anil K. *Encyclopedia of Biometrics* [online]. 2nd edition. Boston: Springer, 2015. [cit. 2021-03-26]. ISBN 978-1-4899-7487-7. Dostupné z: DOI: 10.1007/978-1-4899-7488-4

[11] CAMPISI, Patrizio. *Security and Privacy in Biometrics* [online]. London: Springer, 2013. [cit. 2021-03-30]. ISBN 978-1-4471-5229-3. Dostupné z: DOI: 10.1007/978-1-4471-5230-9

[12] NAIT-ALI, Amine a FOURNIER, Regis. *Signal and Image Processing for Biometrics* [online]. New York: Wiley-ISTE, 2012. [cit. 2021-04-12]. ISBN 978-1-118-58819-2. Dostupné z: https://ebookcentral.proquest.com/lib/techlib-ebooks/detail.action?docID=1120464

[13] Anatomie oka. In: *Ábíčko.cz* [online]. 2018. [cit. 2021-04-13]. Dostupné z: https://www.abicko.cz/galerie/precti-si-technika/45641/tajemstvi-biometrie-3-duhovka-a-sitnice

[14] HORNOVÁ, Jara. *Oční propedeutika*. Praha: Grada, 2011. ISBN 978-80-247-4087-4.

[15] BOWYER, Kevin W. a BURGE, Mark J. *Handbook of Iris Recognition* [online]. 2nd edition. London: Springer, 2016. [cit. 2021-04-12]. ISBN 978-1-4471-6784-6. Dostupné z: DOI: 10.1007/978-1-4471-6784-6

[16] DAUGMAN, John. How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology* [online]. 2004, **14**(1), 21–30. [cit. 2021-03-25]. ISSN 1051-8215. Dostupné z: DOI: 10.1109/TCSVT.2003.818350

[17] DAUGMAN, John. Demodulation by complex-valued wavelets for stochastic pattern recognition. *Int'l Journal of Wavelets and Multi-resolution Information Processing* [online]. 2003, **1**(1), 1–17. [cit. 2021-04-13]. Dostupné z: https://www.cl.cam.ac.uk/ jgd1000/complex.pdf

[18] *BSON (Binary JSON): Specification* [online]. [cit. 2021-04-19]. Dostupné z: http://bsonspec.org/spec.html

[19] *The MongoDB 4.4 Manual* [online]. MongoDB. 2008. [cit. 2021-04-19]. Dostupné z: https://docs.mongodb.com/manual/

[20] *Server Side Public License FAQ* [online]. MongoDB. 2021. [cit. 2021-04-21]. Dostupné z: https://www.mongodb.com/licensing/server-side-public-license/faq

[21] SANCHEZ-AVILA, C. a SANCHEZ-REILLO, R. Two different approaches for iris recognition using Gabor filters and multiscale zero-crossing representation. *Pattern Recognition* [online]. 2005, **38**(2), 231–240. [cit. 2021-04-13]. ISSN 0031-3203. Dostupné z: DOI: 10.1016/j.patcog.2004.07.004

Příloha A

Seznam použitých zkratek

2D Two-Dimensional

3D Three-Dimensional

BSON Binary JSON

CCD Charge-Coupled Device

DB Database

DVD Digital Versatile Disc

EER Equal Error Rate

FAR False Acceptance Rate

FRR False Rejection Rate

GPIO General-Purpose Input/Output

HD Hamming Distance

JSON JavaScript Object Notation

LBP Local Binary Pattern

LED Light Emiting Diode

NIR Near Infra Red

SCRAM Salted Challenge Response Authentication Mechanism

SHA Secure Hash Algorithm

SSPL Server Side Public License

TCP Transmission Control Protocol

TLS Transport Layer Security

USB Universal Serial Bus

Příloha B

Obsah přiloženého DVD

- `data` ..... naměřená data
- `database` ..... adresář obsahující JSON schéma
- `irisapp` ..... adresář se spustitelnou formou implementace
- `readme.pdf` ..... popis obsahu DVD a uživatelská příručka
- `src` ..... adresář se zdrojovými kódy
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... adresář s textem bakalářské práce
  - `BP_Louthanova_Pavla_2021.pdf` ..... text práce ve formátu PDF