

# Spolehlivost skeneru oční duhovky pro biometrickou identifikaci osob

Martin Lužný

---

Bakalářská práce  
2015



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2014/2015

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin Lužný**  
Osobní číslo: **A11036**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Spolehlivost skeneru oční duhovky pro biometrickou identifikaci osob**

Téma anglicky: **The Reliability of Iris Scanners for the Biometric Identification of Individuals**

Zásady pro vypracování:

1. Vypracujte literární rešerši zaměřenou na biometrickou identifikaci osob.
2. V rámci literární rešerše se zaměřte i na možnosti využití oční duhovky pro biometrickou identifikaci osob.
3. Proveďte základní měření identifikace osob pomocí skeneru oční duhovky.
4. Ověřte spolehlivost skeneru oční duhovky. Ověření spolehlivosti proveďte za různých podmínek, zejména při snížené světelné viditelnosti, při fyzické zátěži člověka.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BITTO, Ondřej. Šifrování a biometrika ? aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.
2. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Vyd. 1. Brno: M. Drahanský, 2011, 294 s. ISBN 978-80-254-8979-6.
3. RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Vyd. 1. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.
4. MARIEB, Elaine Nicpon a Jon MALLATT. Anatomie lidského těla. Vyd. 1. Brno: CP Books, 2005, xvi, 863 s. ISBN 8025100669.
5. JANEČEK, Tomáš. Biometrikaonline! [cit. 2014-01-21]. Dostupné z <http://www.nula.wz.cz/biometrika/>.

Vedoucí bakalářské práce:

**doc. Mgr. Milan Adámek, Ph.D.**  
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

**6. února 2015**

Termín odevzdání bakalářské práce:

**3. června 2015**

Ve Zlíně dne 6. února 2015



L.S.

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*

Ing. Jan Valouch, Ph.D.  
*ředitel ústavu*

### **Prohlašuji, že**

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

### **Prohlašuji,**

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

Ve Zlíně 1. 6. 2015

  
.....  
podpis diplomanta

## **ABSTRAKT**

Bakalářská práce je zaměřena na biometrickou identifikaci osob pomocí biometrických systémů, se kterými se můžeme setkat v bezpečnostním oboru. Hlavním tématem práce je identifikace osob pomocí oční duhovky a zejména ověření spolehlivosti skeneru oční duhovky. Tato práce se skládá ze dvou částí, teoretické a praktické. V teoretické části jsou objasněny základní pojmy, jako jsou identita, verifikace, identifikace a autentizace. Dále jsou popsány jednotlivé biometrické systémy, které se vyskytují v průmyslu komerční bezpečnosti. V praktické části je provedeno měření na skeneru oční duhovky a ověření spolehlivosti skeneru za různých podmínek, a to zejména při snížené světelné viditelnosti, při fyzické zátěži člověka a při používání brýlí a kontaktních čoček.

**Klíčová slova:** biometrický systém, identifikace, verifikace, autentizace, spolehlivost skeneru

## **ABSTRACT**

The thesis is focused on the biometric identification of individuals using the biometric systems which are destined for the security field. The main theme is the identification of individuals using iris and in particular the verification of the reliability of the iris scanner. This work consists of two parts, theoretical and practical. The theoretical part explains the basic concepts such as the verification of identity, identification and authentication. It describes individual biometric systems, which occur in commercial security industry. The practical part presents the results of the measurement performed on the iris scanner. It deals with different conditions such as reduced visibility, increased physical activity, wearing glasses or contact lenses.

**Keywords:** biometric system, identification, verification, authentication, reliability of scanner

Rád bych poděkoval svému vedoucímu panu doc. Mgr. Milanovi Adámkovi, Ph.D. za vedení a rady při zpracovávání této bakalářské práce. Dále bych moc rád poděkoval Ing. Haně Talandové za spolupráci a cenné rady při měření na skeneru oční duhovky. Také děkuji všem studentům doktorského studia za poskytnutí biometrických údajů. V neposlední řadě děkuji rodině za podporu a trpělivost v době studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 BIOMETRIE</b> .....	<b>11</b>
1.1 VYMEZENÍ POJMŮ.....	12
1.1.1 Identita.....	12
1.1.2 Verifikace .....	12
1.1.3 Identifikace.....	12
1.1.4 Autentizace.....	13
1.2 MĚŘENÍ VÝKONNOSTI BIOMETRICKÝCH ZAŘÍZENÍ.....	13
1.2.1 FRR .....	14
1.2.2 FAR .....	14
1.2.3 Vztah FRR a FAR .....	14
<b>2 JEDNOTLIVÉ BIOMETRICKÉ SYSTÉMY</b> .....	<b>16</b>
2.1 OTISK PRSTU .....	16
2.1.1 Základní klasifikační vzory.....	16
2.1.2 Snímání otisku prstu.....	17
2.2 GEOMETRIE RUKY .....	18
2.2.1 Výhody a nevýhody použití technologie geometrie ruky .....	19
2.3 TVAR KREVNÍHO ŘEČIŠTĚ .....	20
2.4 TVAR LŮŽKA NEHTU.....	20
2.5 PÍSMO A PODPIS .....	21
2.6 DYNAMIKA STISKU KLÁVES.....	21
2.7 DNA .....	22
2.8 GEOMETRIE TVÁŘE.....	22
2.8.1 Použité algoritmy .....	23
2.9 OVĚŘOVÁNÍ HLASU .....	24
2.9.1 Výhody a nevýhody .....	24
2.10 DYNAMIKA CHŮZE .....	24
2.11 SÍTNICE OKA.....	25
2.11.1 Výhody a nevýhody .....	26
<b>3 IDENTIFIKACE PODLE OČNÍ DUHOVKY</b> .....	<b>27</b>
3.1 HISTORIE METODY.....	27
3.2 STRUKTURA LIDSKÉHO OKA .....	27
3.3 STRUKTURA OČNÍ DUHOVKY .....	28
3.4 PRINCIP IDENTIFIKACE PODLE OČNÍ DUHOVKY .....	30
3.5 VÝHODY A NEVÝHODY POUŽITÍ OČNÍ DUHOVKY PRO BIOMETRICKOU IDENTIFIKACI.....	31
<b>II PRAKTICKÁ ČÁST</b> .....	<b>32</b>
<b>4 SKENER OČNÍ DUHOVKY</b> .....	<b>33</b>

4.1	TECHNICKÉ PARAMETRY SKENERU ICAM7000.....	34
4.2	POTŘEBNÉ VYBAVENÍ K FUNKČNÍMU PROVOZU.....	34
4.3	POPIS OVLÁDACÍCH PRVKŮ SKENERU ICAM7000 .....	35
4.4	UŽIVATELSKÉ ROZHRANÍ .....	35
4.5	PROPOJENÍ SKENERU S PC .....	36
4.5.1	Instalace softwaru.....	36
4.5.2	Uživatelské prostředí.....	41
4.6	NAMĚŘENÁ DATA POMOCÍ SKENERU OČNÍ DUHOVKY .....	42
4.6.1	Měření za denního světla .....	43
4.6.2	Měření při snížené viditelnosti.....	45
4.6.3	Měření při úplném zatmění .....	47
4.6.4	Měření při umělém osvětlení .....	49
4.6.5	Měření pod různým úhlem pohledu .....	51
4.6.6	Měření při fyzické zátěži člověka .....	53
4.7	DISKUZE VÝSLEDKŮ .....	54
	<b>ZÁVĚR .....</b>	<b>55</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>56</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>59</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>60</b>
	<b>SEZNAM TABULEK.....</b>	<b>62</b>



## ÚVOD

Lidé už od pradávna, aniž by si to uvědomovali, používají denně biometrické rozpoznávání osob podle fyziologických rysů např. dle obličeje, hlasu apod. Tyto rysy lze označit za biometrické vlastnosti člověka. Nejenom lidé, ale i zvířata se rozeznávají na základě různých vlastností např. pach apod.

Nejstarší důkazy o použití biometrie se datují kolem 14. století našeho letopočtu na území Číny. Jednalo se o otisky prstů nalezené na keramice. Nicméně se vědci dohadují, zda tuto stopu autor keramiky zanechal záměrně kvůli důkazu o autorství, anebo vznikla pouze jeho nedbalostí.

První potvrzující materiály o použití biometrie spadají do 19. století našeho letopočtu. Z dochovaných materiálů se jednalo o otisky prstů používaných především v oblasti kriminalistiky k identifikaci osob.

V dnešním světě se biometrické systémy dostávají do popředí při zabezpečování objektů a majetku proti nežádoucím vlivům ze strany kriminálních živlů. V současnosti a také především v budoucnu bude tato technologie napomáhat chránit nejen objekty, ale i osoby, které si tuto technologii zvolí jako klíčovou při zabezpečování majetku a důležitých informací.

Snahou této práce je seznámit širokou veřejnost s technologiemi a systémy, které se využívají v bezpečnostní praxi. V práci jsou popsány jednotlivé biometrické systémy, jejich výhody a nevýhody. Hlavní zaměření je soustředěno na využití oční duhovky pro biometrickou identifikaci osob. V praktické části je ověřena spolehlivost skeneru oční duhovky za různých podmínek, a to zejména při snížené světelné viditelnosti, při fyzické zátěži člověka a při používání brýlí a kontaktních čoček.

## **I. TEORETICKÁ ČÁST**

## 1 BIOMETRIE

Výraz biometrie je složen ze dvou slov „bios“ a „metron“ pocházející z řečtiny. První slovo znamená život a druhé slovo vyjadřuje měřítko. Můžeme biometrii tedy nazvat jako vědu, zabývající se měřením charakteristik živých organismů [1].

Biometrie pak slouží k automatizovanému rozpoznávání lidských rysů na základě jejich jedinečnosti. Tyto charakteristické rysy se rozdělují na anatomické a behaviorální [1].

### **Anatomické (fyziologické) vlastnosti**

Tyto vlastnosti se také nazývají *fyzické statické*, protože jsou vždy přítomny a nejsou ovlivnitelné stavem člověka. Vyznačují se tím, že jeden pevný rys je jedna biometrická vlastnost. Mezi anatomické vlastnosti patří:

- otisk prstu
- dlaň
- oční duhovka a sítnice
- tvar ucha
- geometrie ruky
- obličej
- DNA [4].

### **Behaviorální vlastnosti**

Tyto vlastnosti se také nazývají jako dynamické a vyplývají z nějaké akce, kterou dotyčná osoba vykonává. Tato biometrická vlastnost se na základě některých onemocnění a úrazů může měnit. Některé vlastnosti se dají naučit a tím pádem může docházet k prolomení těchto biometrických systémů pachatelem. Mezi tyto vlastnosti patří:

- chůze
- mimika obličeje
- pohyb rtů
- dynamika stisku kláves
- hlas / řeč [1].

## 1.1 Vymezení pojmů

Lidé, aniž by si to uvědomovali, rozpoznávají osoby automaticky na základě jejich charakteristických znaků. Je to založeno na jednoznačné identitě člověka.

### 1.1.1 Identita

Identita vyjadřuje podstatné znaky každého jedince. Rozlišujeme fyzickou a elektronickou identitu. Fyzická identita definuje náš vzhled a chování. Je dokázáno, že na světě neexistuje stejná fyzická identita mezi osobami. Naopak u elektronické identity může existovat identit, kolik chceme. Jedná se např. o různé identifikační karty, účty na internetových portálech apod. [1].

### 1.1.2 Verifikace

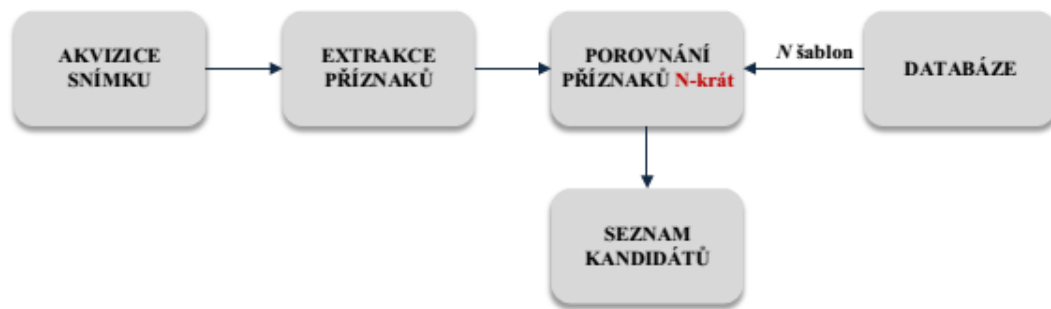
Při ověřování identity (verifikaci) osoba uvede svoji totožnost a tu následně potvrzuje svým heslem. S verifikací se setkáváme vždy při vstupu do portálů, kde musíme uvést svoje přihlašovací jméno a potvrdit ho heslem. Svoji identitu při vstupu do objektu můžeme potvrdit např. identifikační kartou a poté čtecí zařízení nám sejme biometrická data, která se porovnají s referenční šablonou uloženou v systému [2,5].



Obrázek 1. Schéma verifikace [6]

### 1.1.3 Identifikace

Při identifikaci osoba zadá systému svoji biometrickou vlastnost, ale nepoví svoji totožnost. Systém pak porovná vzorky ze vstupu s celou databází uložených vzorků. Tento způsob je časově zdoluhavý, zejména v rozsáhlejších databázích, které obsahují velké množství registrovaných osob [1].



Obrázek 2. Schéma identifikace [6]

#### 1.1.4 Autentizace

Pojem autentizace můžeme také nazvat jako ověřování totožnosti uživatele před povolením vstupu. Autentizace se provádí pomocí tří forem a to:

- **Autentizace heslem** - Vychází ze znalosti a zadání přístupového hesla uživatelem, který žádá o přístup do chráněného objektu.
- **Autentizace předmětem** - Založeno na předložení identifikačního předmětu neboli tokenu, který umožní uživateli přístup do chráněného objektu.
- **Biometrická autentizace** - Založeno na prokázání biometrických vlastností člověka [5].

## 1.2 Měření výkonnosti biometrických zařízení

Při realizování biometrického systému a následného uvedení do praxe vzniká u uživatele myšlenka, která zní: Jak je biometrické zařízení spolehlivé a výkonné? Pro tyto otázky existují charakteristiky, pomocí kterých můžeme porovnat jednotlivé biometrické systémy. Mezi hlavní kritérium pro výběr vhodného systému může být rychlost zpracování naměřených dat, kapacita (tj. počet identifikací a verifikací v určitém časovém úseku), cena zařízení, uživatelská přijatelnost, odolnost a spolehlivost zařízení pracovat v provozním režimu [3].

V praxi se avšak setkáváme s nežádoucími jevy, které se mohou objevit v každém systému. Především se jedná o pravděpodobnost chybného odmítnutí a pravděpodobnost chybného přijetí [3].

### 1.2.1 FRR

Zkratka FRR neboli pravděpodobnost chybného odmítnutí vychází z anglického názvu **False Reject Rate**. Jedná se tedy o pravděpodobnost, kdy biometrický systém nerozpozná oprávněného uživatele, který má uložený záznam v databázi vzorků. Poté dojde k jeho odmítnutí nebo je znovu vyzván, aby přistoupil k druhému měření [4].

FRR můžeme vypočítat podle následujícího vzorce: [3]

$$FRR = \frac{\text{Počet chybných odmítnutí}}{\text{Počet pokusů oprávněných osob o identifikaci/verifikaci}}$$

### 1.2.2 FAR

Zkratka FAR neboli pravděpodobnost chybného přijetí vychází z anglického názvu **False Accept Rate**. Pojednává o tom, kdy biometrický systém nesmí akceptovat neoprávněné osoby (útočníky). Osoby, které se snaží o neoprávněný přístup do chráněného objektu, jsou biometrickým systémem odmítnuty a následně vyhodnoceny jako osoby neoprávněné.

FAR můžeme vypočítat podle následujícího vzorce: [3]

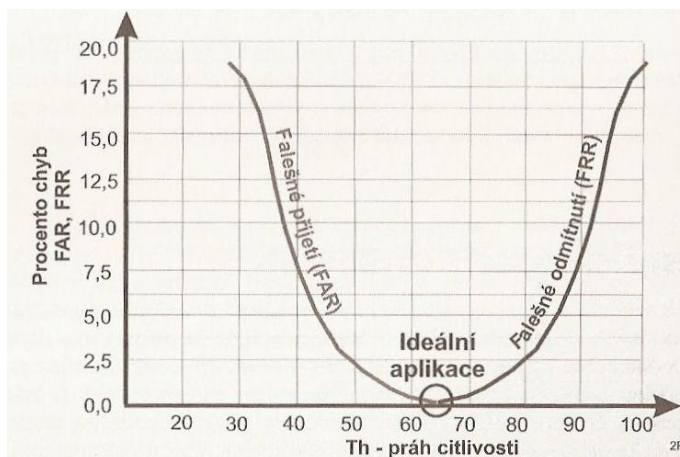
$$FAR = \frac{\text{Počet chybných přijetí}}{\text{Počet pokusů neoprávněných osob o identifikaci/verifikaci}}$$

### 1.2.3 Vztah FRR a FAR

Biometrické zařízení, které by vykazovalo nulovou chybovost a nespolehlivost, bychom mohli nazvat ideálním biometrickým systémem. Ovšem v praxi neexistuje takové ideální zařízení, které by odpovídalo těmto podmínkám. Ovlivňování výsledné činnosti zařízení způsobuje především citlivost na veškeré vlivy, které působí na toto zařízení [3,7].

Pro ideální zařízení platí vztah:

$$FAR = FRR = 0$$

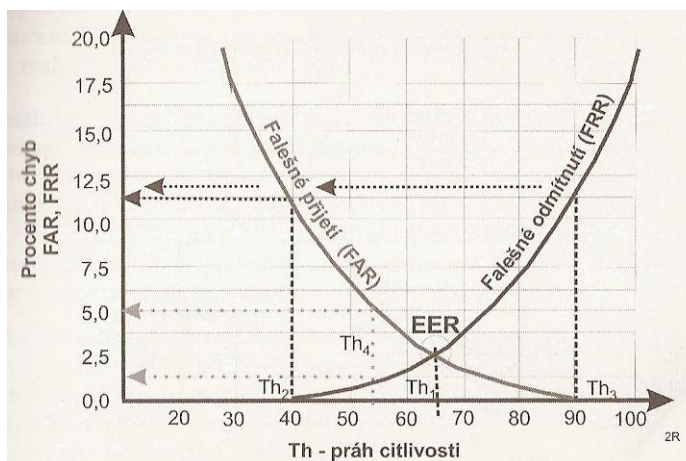


Obrázek 3. Ideální biometrická aplikace [3]

Z grafu je patrné, že pokud nastavíme práh citlivosti tak, aby FRR se rovnalo nule, můžeme tím hovořit o komfortu. Ve skutečnosti to znamená, že registrovaní uživatelé budou přijati, aniž by byly zaznamenány nějaké chyby. Tím ovšem roste počet nežádoucích přijetí od neregistrovaných uživatelů [7].

Pokud nastavíme práh citlivosti tak, aby FAR se rovnalo nule, můžeme hovořit o bezpečnosti. Tím dojde k tomu, že hodnota komfortu klesne a registrovaní uživatelé nebudou tak často přijímáni, jak tomu bylo v předchozím případě. Mezi výhody patří to, že nežádoucí uživatel tento systém nebude narušovat [7].

Naopak pokud zvolíme střední cestu mezi komfortem a bezpečností, tak bychom měli práh citlivosti nastavit v průsečíku FAR a FRR. Bod, ve kterém se tyto křivky protínají, se značí jako EER. Zkratka vychází opět z anglického názvu **Equal Error Rate** a v překladu znamená *míra vyrovnání chyb*, která slouží pro orientační porovnání dvou aplikací [7].



Obrázek 4. Reálná biometrická aplikace [3]

## 2 JEDNOTLIVÉ BIOMETRICKÉ SYSTÉMY

V této kapitole jsou popsány jednotlivé biometrické systémy, které slouží k identifikaci osob. V bezpečnostním oboru existuje mnoho metod ke zjišťování totožnosti jedinců a právě tato kapitola je zaměřená na nejznámější a nejčastěji využívané biometrické systémy, s kterými se můžeme setkat v bezpečnostní praxi.

### 2.1 Otisk prstu

Tato identifikace pomocí otisku prstu je jednou z nejrozšířenějších a nejznámějších biometrických metod, se kterou se můžeme setkat každý den. Každý jedinec má na vnitřní straně rukou i nohou vyvýšené reliéfy kůže, které se odborně nazývají papilární linie. Tyto papilární linie má každý člověk odlišné a na základě jejich průběhu lze rozlišovat jednotlivé osoby mezi sebou. Hlavní předností papilárních linií je jednoduché získání srovnávacího vzorku a další výhodou je to, že vzorek lze získat z 10 prstů [8].

Obraz otisku prstu je vytvořen ze struktury papilárních linií, které se tvoří již v prenatálním období při vývoji každého konkrétního jedince. Papilární linie jsou vysoké v rozmezí 0,1 - 0,4 mm a jejich šířka dosahuje hodnoty v rozmezí 0,2 - 0,5 mm [1].

#### 2.1.1 Základní klasifikační vzory

Vzory, podle kterých rozeznáváme otisky prstů, se dělí do tří základních kategorií, a to na oblouky, víry a smyčky, které je možno vidět na obrázku níže. Smyčky tvoří 65% ze všech otisků prstů, víry obsahují kolem 30% a zbývajících 5% připadá na oblouky [5].

Papilární linie tvaru oblouku neobsahují žádné delty (tj. rozbíhání do třech směrů), zatímco vzor ve tvaru smyčky musí obsahovat mezi deltou a středem aspoň jednu probíhající linii. Pokud papilární linie tvoří oválné nebo spirálovité obrazce s jádrem v ohnisku, jedná se o tzv. vír, kde vzor obsahuje přinejmenším dvě delty a alespoň jednu samostatně probíhající linii [2].



Obrázek 5. Základní klasifikační vzory [9]



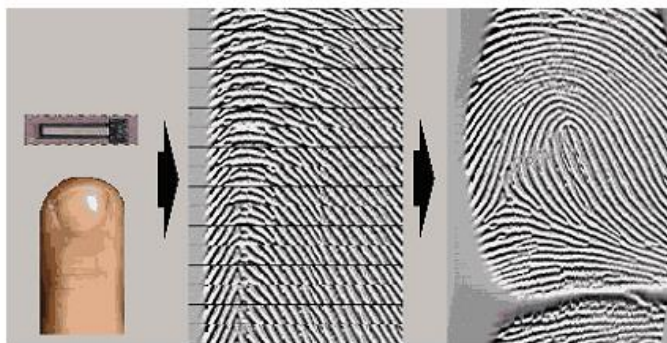
Při identifikaci osoby pomocí otisku prstů se soustředíme hlavně na nalezení a porovnání význačných znaků, které se odborně nazývají markanty. Jsou tvořeny právě papírnými liniemi. Existují různé druhy těchto markantů mezi, které patří např. **body** (velmi malé rýhy), **ostrůvky** (je to rýha, která je o málo větší než body ležící v prostoru mezi rozdvojenou rýhou) a **můstky** (malé rýhy spojující dvě sousední rýhy). Některé markanty se vyskytují častěji než jiné a na otisku prstu se nachází přibližně 75 až 175 markantů [2].

### 2.1.2 Snímání otisku prstu

Existuje mnoho metod a technologií, pomocí kterých je možné zachytit otisk prstů dotyčné osoby. V této podkapitole je vypsán stručný souhrn jednotlivých metod a technologií s kterými se můžeme setkat v bezpečnostním oboru.

#### Metody zachycení otisku prstů

- *Získání pomocí inkoustu a papíru* - Používá se ve forenzní sféře policií.
- *Statické snímání* - Uživatel přitiskne prst na snímač bez žádného pohybu.
- *Snímání šablonováním* - Uživatel přejíždí prstem po snímači [8].



Obrázek 6. Snímání šablonováním [8]

#### Technologie snímačů otisků prstů

- *Optické snímače na základě odrazu* - Uživatel přitiskne prst nad skleněnou podsvětlenou vrstvou, světlo se odráží od prstu a prochází do CCD snímače a ten zachytí vizuální obraz otisku prstu.
- *Transmisní optické snímače* - Snímání je založeno na světelných paprscích, které prochází prstem ruky a z vrchní části je prosvěcován všesměrovým zdrojem světla.

- *Tlakové snímače otisku prstu* - Snímač je složen ze tří vrstev, přičemž mezi elektrovodivé vrstvy je uložen nevodivý gel. Po přiložení prstu na plochu snímače dojde ke stisku nevodivého gelu v místě dotyku papilárních linií a tím se elektrovodivé vrstvy dotknou.
- *Teplotní snímače otisku prstu* - Princip je založen na tepelném záření. Papilární linie vyzařují vyšší teplotu než prohlubně mezi nimi. Po přiložení prstu na pyroelektrickou buňku snímající tepelné záření dochází k přečtení otisku.
- *Ultrazvukové snímače* - Princip spočívá v tom, že měří odraženou zvukovou vlnu jako např. u sonaru [1,8].

## 2.2 Geometrie ruky

Tato biometrická metoda se používá do provozů, kde není možné použít otisk prstů nebo jinou biometriku. Většinou se používá do oblastí s omezeným přístupem osob, kde je problém špinavých rukou z výroby a proto se nemůže použít otisk prstů [9].

Každá osoba má odlišný tvar ruky a tento tvar se u dospělé osoby během života nemění. Právě díky této odlišnosti ruky mezi osobami je tato metoda často využívána mezi biometrickými systémy.

Pro ověření identity pomocí ruky se používají následující charakteristiky:

- délka prstů
- šířka prstů
- výška prstů
- zakřivení a lokální anomálie [1].

V dnešní bezpečnostní sféře se používají 3D skenery, které snímají typické geometrické znaky ruky v desítkách bodů za jednu sekundu. Dotyčná osoba při vstupu do objektu položí ruku na horizontální desku skeneru, která obsahuje distanční kolíčky. Tyto kolíčky zajišťují požadovanou polohu ruky na podložce. K nasvícení ruky dochází pomocí infračervených LED diod. Pomocí zrcadel dochází k odrazu obrazu do digitální kamery. Použitá podložka se vyznačuje velkou optickou odrazivostí, která umožňuje zvýšení kontrastu mezi rukou a podložkou [9].

Ke snímání obrazu dochází pomocí skeneru, který snímá černobílou siluetu dlaně a prstů. Snímání geometrie ruky je prováděno ze shora kolmo dolů na snímací podložku a z boku pomocí postranního zrcadla [9].



*Obrázek 7. Rozmístění prstů mezi  
distančními kolíky [8]*

### 2.2.1 Výhody a nevýhody použití technologie geometrie ruky

Hlavní předností této technologie je její rychlost a odolnost proti měnícím se detailům, tj. drobná poranění, pot nebo špina rukou. Takle metoda je převážně používána pro verifikaci osob, protože se nevyznačuje vysokou přesností. Mezi hlavní nevýhody metody geometrie ruky jsou velká poranění, která mohou způsobit zkreslení a následné odmítnutí při vstupu do objektu. Jedná se především o amputování nějakého prstu či článku na ruce a také při deformaci kloubů vlivem nemoci. Další problém může nastat při montáži zařízení do oblastí, kde zařízení může být vystaveno přímému slunečnímu svitu. Proto se do zařízení přidává světelná clona, která zabrání oslepení skeneru slunečním světlem [2,9].



*Obrázek 8. Zařízení  
pro rozpoznávání geo-  
metrie ruky [10]*

### 2.3 Tvar krevního řečiště

Metoda k rozpoznávání osob podle tvaru krevního řečiště není zas tak známá, jako předchozí metody, které jsou uvedeny výše. V tomto textu je stručně popsáno, jak lze určit identitu pomocí uspořádání žil ruky. Každý jedinec má neměnný a unikátní tvar krevního řečiště ruky a díky těmto vlastnostem lze použít tuto metodu v bezpečnostní sféře k omezení vstupu do hlídaných objektů.

Technologie je založena na principu získávání obrazu žil ruky. Dochází k nasvícení krevního řečiště pomocí infračerveného světla, jelikož cévní strom není možné vidět pouhým okem a tím zvýrazní rozložení žil v ruce jedince. Odkysličené krevní barvivo hemoglobin absorbuje infračervené světlo, zatímco povrch kůže jej odráží a tím dochází k tomu, že cévní řečiště se projeví tmavší barvou než kůže. Dále dochází k vyfotografování obrazu pomocí CCD kamery a poté se porovná získaný obraz s referenční šablonou uloženou v databázi [1,11].

Mezi výhody tohoto systému patří především jeho vysoká spolehlivost a nenáchylnost na falšování identity. Nevýhodou tohoto systému je jeho nepřesné zpracování a vliv na případný šum [11].



Obrázek 9. Žíly hřbetu ruky [3]

### 2.4 Tvar lůžka nehtu

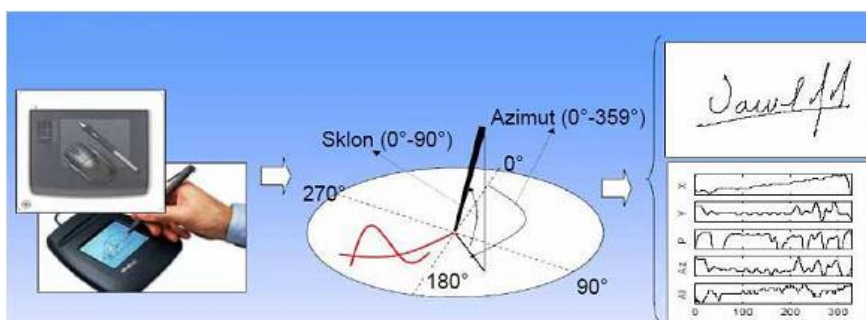
Při pohledu na svůj nehet můžeme vidět, že povrch nehtu není úplně rovný. Je to způsobeno tím, že nehet při svém růstu kopíruje tvar lůžka, které je umístěno pod ním. Další zajímavostí je to, že každý prst má jiný tvar lůžka, např. palec je jinak tvarovaný než ukazováček. Právě podle tvaru lůžka lze rozlišit dva jedince mezi sebou. Jelikož pod nehtem se nachází přírodní polymer, který má schopnost měnit orientaci polarizovaného svět-

la, lze udělat rozbor změny paprsku po odraze a tím získat tvar požadovaného lůžka nehtu [2].

## 2.5 Písmo a podpis

V dnešním světě je tato metoda nejvíce používaná, protože podpis je brán jako potvrzení, že dotyčná osoba souhlasí s daným dokumentem. Při biometrickém zpracování lze rozlišit statický a dynamický podpis.

Statická podoba podpisu zaznamenává jenom konečný výsledek celého procesu psaní. Tuto formu podpisu lze snáze zfalšovat. Naopak dynamická podoba podpisu popisuje změnu přítlaku pera v závislosti na konkrétním bodu na ploše. Takle forma vyžaduje speciální zařízení a je bezpečnější oproti statické, protože není možné napodobit celý proces psaní [11].



Obrázek 10. Identifikace podle podpisu [13]

## 2.6 Dynamika stisku kláves

Dynamika stisku kláves je metoda identifikace, která měří dobu trvání stlačených kláves a času mezi jednotlivými stisky kláves. Kvůli nízké přesnosti není tato technologie vhodná k identifikaci, a proto se využívá k verifikaci. Nevýhodou je náchylnost proti neoprávněným osobám při vstupu do chráněného objektu.

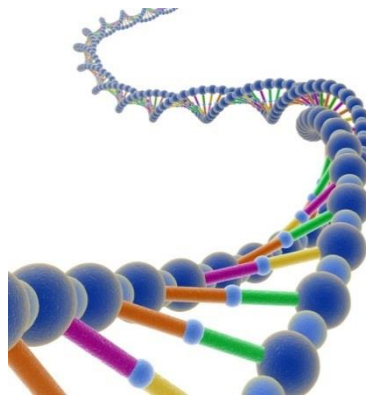
Jednou za čas je zapotřebí opakovat registrace z důvodu toho, že uživatel se postupem času naučí psát rychleji s využitím všech prstů a tím by docházelo k odmítnutí přístupu [9].



*Obrázek 11. Stisk kláves [11]*

## 2.7 DNA

Identifikace podle DNA je založena na tom, že každá osoba má svůj jedinečný DNA-otisk až na výjimku jednovaječných dvojčat, které mají DNA-otisk stejný. DNA lze získat mnoha způsoby např. ze slin nebo krve. Výhodou této metody je, že nemůže být chirurgicky změněna jak třeba u otisku prstu a je velmi přesná. Bohužel mezi veřejností tahle metoda není moc oblíbená, protože získávání vzorků nemusí být pro každého jedince vždy příjemnou záležitostí a pohodlností, jak tomu bylo v předchozích metodách, které jsou popsány v textu výše [5].



*Obrázek 12. DNA [19]*

## 2.8 Geometrie tváře

Rozpoznávání druhých osob podle obličeje provádíme každý den, aniž si to uvědomujeme. Každý jedinec si přirozeně v paměti vytváří obraz druhého a na základě toho poznáváme jeho identitu.

Biometrický systém pracující na rozpoznávání osob vychází z toho, že tvář každého z nás je odlišná a je možno toho využít v bezpečnostním průmyslu k zamezení vstupu do chráněných prostorů. Výjimku mohou avšak tvořit jednovaječná dvojčata, u kterých je podobnost tváře velmi vysoká, ale v jistých rysech se od sebe liší. Naši tvář využíváme i k zajištění identity na různých dokladech a průkazech apod.

### 2.8.1 Použité algoritmy

Biometrické systémy pro rozpoznávání podle obličeje se dělí podle použitých algoritmů:

- porovnávání křivek
- porovnávání šablon
- porovnávání pozic význačných bodů
- užití termálního snímku [11].

Algoritmy pro porovnávání obličeje podle křivek nejsou moc spolehlivé. Pro zpracování obličeje se využívá postup pro 2D snímky, kde se hledají shodné křivky a hrany obličeje. Tyto křivky a hrany obličeje se porovnávají v databázi. Nevýhodou porovnání obličeje podle křivek je, že je lze přelstít např. pomocí masek apod. [11].

Algoritmy pro porovnávání obličeje podle šablon potřebují velké množství vstupních informací. Pořizuje se více snímků osoby většinou přední a boční pohled tváře a dochází k vytvoření sady šablon a ty mají za úkol vystihnout typické rysy obličeje. Získané šablony se testují na shodnost s daty, které jsou uloženy v databázi. Mezi nevýhody patří velké množství vzorů v databázi [11].

Algoritmus pro porovnávání obličeje podle význačných bodů. Na obličeji se vyznačí význačné body a poté se změří jejich vzdálenost mezi nimi. Význačnými body mohou být oči, uši, nos a také brada a tváře. Měřením vzdáleností mezi těmito body dochází k vytvoření 3D grafu vzoru. Měření je prováděno z různých úhlů, aby nedocházelo ke zkreslení snímku a tím se dosáhlo přesnějšího měření [11].

Využití termálního snímku obličeje spadá mezi nejmodernější metody. Snímání obličeje je provedeno termokamerou a pořízený snímek je pro každého člověka unikátní. Nevýhodou tohoto termálního snímku je, že termální snímek není stabilní a je závislý na okolní teplotě.



Obrázek 13. Termální snímek [9]

## 2.9 Ověřování hlasu

Identifikace podle hlasu je založena na odlišnostech řečového orgánu identifikovaných osob. Biometrický otisk je vytvořen pomocí tvaru a rezonance ústní dutiny, hlasivek, jazyka a zubů. U této biometriky rozlišujeme dva pojmy a to ověřování a rozpoznávání hlasu. U ověřování hlasu je dotyčnou osobou vyslovená fráze, která se porovná v databázi, s již vytvořeným registračním vzorem a určí případnou shodu nebo ne. V druhém případě se jedná o rozpoznávání hlasu, kde dotyčný člověk vysloví slovo a systém prohledá databázi a rozhodne, které slovo nejvíce odpovídá existující výslovnosti [2].

Při registraci si vytvoří každá osoba svůj tzv. otisk hlasu. Čím delší bude vytvořen otisk hlasu, tím také vzroste i vyšší stupeň zabezpečení, než by tomu bylo u krátkých otisků [2].

### 2.9.1 Výhody a nevýhody

Mezi výhody tohoto bezpečnostního systému můžeme zařadit nízkou hardwarovou náročnost a její rychlost. Pro ověřování hlasu se používá standardně mikrofon a na větší vzdálenost lze využít i telefonu. K nevýhodám řadíme závislost na stavu člověka, protože jakákoliv nemoc hlasivek nebo problémy s rýmou a kašlem mohou způsobit, že systém špatně vyhodnotí ověřovaný hlas a zamezí přístup uživatele např. do hlídaného objektu [2].

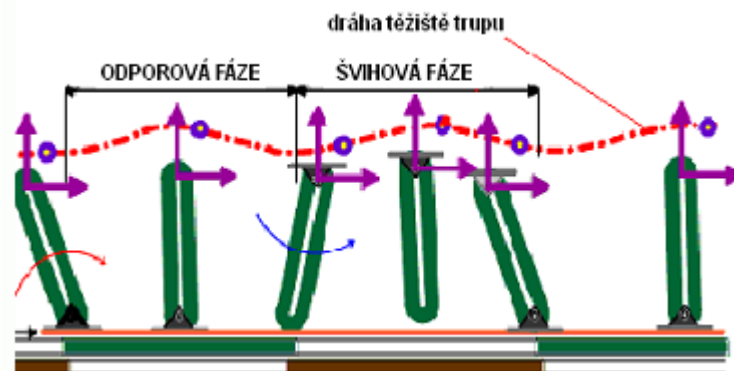
## 2.10 Dynamika chůze

Identifikovat osoby lze i na základě jejich pohybu, protože lidský pohyb je určitým způsobem unikátní. Jedná se především o pohyb po dvou dolních končetinách, který se



odborně nazývá bipedální lokomoce. Výhodou této metody zjišťující dynamiku pohybů je, že dokáže identifikovat pachatele i přes různé převleky a maskování obličeje. Využití této technologie je široké např. na letišti, na nádraží apod. K nevýhodám patří různé faktory a to zejména zdravotní problémy, požití alkoholu nebo drog. Všechny tyto negativní faktory dokáží ovlivnit chůzi dotyčné osoby [8].

Celý bezpečnostní systém pracuje tak, že porovnává křivky drah, které kopírují určité body na lidském těle. Lidské tělo se při svém pohybu nedokáže udržet ve vzpřímené poloze a dochází k tomu, že tělo se různě pohybuje, naklání a vychyluje různými směry [8,9].



Obrázek 14. Pohyb těžiště lidského těla [8]

## 2.11 Sítnice oka

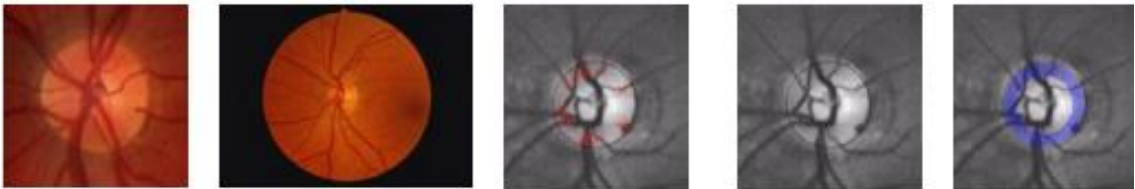
Metoda k identifikování osob podle oční sítnice, patří mezi ty nejpřesnější a nejspolehlivější metody. Každý člověk má jinou sítnici a na základě tohoto tvrzení lze využít biometrického systému, který porovnává obraz sítnice u dotyčných osob.

Využití těchto systémů je široké, ale především se využívá v oblastech, kde je potřeba zajistit nejvyšší stupeň zabezpečení objektu. Sítnice je světlo-citlivý povrch oka, který se nachází na zadní straně bulvy a obsahuje velké množství nervových buněk. Snímání je prováděno pomocí infračerveného paprsku produkujícího nízkou intenzitu záření, které prochází přes zornici až na samostatnou sítnici oka. Sítnice se jeví jako průhledná (obrázek 14) a zvýrazněné cévy sítnice vytvářejí obraz použitelný k identifikaci osob [8,9].

### 2.11.1 Výhody a nevýhody

Mezi výhody biometrického systému, který pracuje na rozpoznávání osob pomocí oční sítnice, je její rychlost a přesnost. Proto je využívána pro nejvyšší stupeň zabezpečení.

K nevýhodám patří vysoká pořizovací cena a také menší oblíbenost mezi uživateli. Je to z toho důvodu, že při pořizování obrazu sítnice je nutné vydržet cca 10 vteřin bez pohybu, což pro někoho nemusí být zrovna příjemné. Dalším problémem pro některé může být svícení do oka. Také se mezi uživateli šíří mýtus o tom, že při snímání může nastat poškození sítnice. Tohle tvrzení je ovšem nepravdivé, protože se jedná o zcela bezpečnou metodu. Další nepříjemnost může nastat pro osoby nosící brýle, které se musí před snímáním sítnice sundat z očí [9].



Obrázek 15. Znázornění cév za oční sítnicí [8]

### 3 IDENTIFIKACE PODLE OČNÍ DUHOVKY

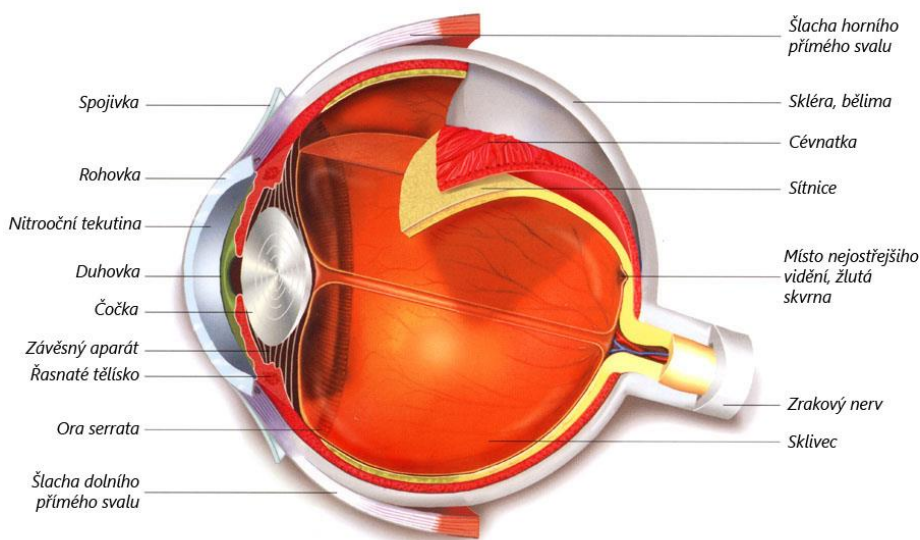
Tato kapitola je zaměřena podrobně na využití oční duhovky pro biometrickou identifikaci osob. Je zaměřena na počátky vzniku rozpoznávání osob podle oční duhovky. Dále je zde popsána struktura lidského oka, rysy oční duhovky, principy pořízení a zpracování snímků z lidského zraku. V neposlední řadě jednotlivé metody zabývající se lidským okem především oční duhovkou.

#### 3.1 Historie metody

První zmínky o využití oční duhovky pro biometrii spadají do roku 1880, kde policista Albert Bertillon se snažil realizovat ideu identifikace podle oční duhovky. V roce 1987 lékaři Aran Safir a Leonard Flom zabývající se oční medicínou (oftalmologie) si nechali patentovat ideu principu zjišťování totožnosti podle oční duhovky. Na základě jejich zkoumání v roce 1994 John Daugman vytvořil algoritmus k porovnání charakteristik lidského oka. Tento algoritmus tvoří základ pro biometrické systémy pracující s obrazem oční duhovky [14].

#### 3.2 Struktura lidského oka

Lidský zrak patří mezi nejdůležitější smysly, díky kterým získáváme informace z vnějšího prostředí. Orgánem lidského zraku je oko. Oko je kulovitého tvaru, který má za následek vnímání obrazu. Oko je velmi složitý smyslový orgán tvořen mnoha částmi, které jsou popsány na obrázku níže [15].



Obrázek 16. Anatomie lidského oka [16]

### Popis jednotlivých částí oka:

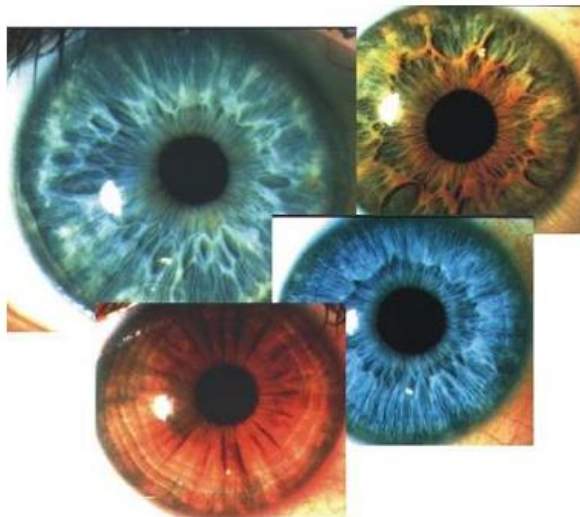
- *Oční rohovka* - Je umístěna v přední části oka. Je to čirá tkáň bez cév, která láme dopadající světlo.
- *Přední komora* - Je to prostor mezi rohovkou a duhovkou, který je vyplněný nitrooční tekutinou.
- *Duhovka* - Je svalovina, která je kruhovitě uspořádána do tvaru připomínající mezikruží. Uprostřed duhovky je otvor, nazývaný pupila (zornice), který reguluje množství dopadajícího světla.
- *Čočka* - Je zavěšená na řasnatém tělísku a má schopnost měnit svůj tvar a sílu indexu lomu. Čočka má schopnost akomodace neboli zaostření na různě vzdálené předměty. Stářím se tato vlastnost snižuje, a proto člověk potřebuje brýle.
- *Oční bělmo* - Stará se o stabilitu oční koule pokrývající celé oko a v přední části přechází v rohovku.
- *Sklivec* - Vyplňuje 2/3 vnitřní části oka. Sklivec má rosolovitou, čirou konzistenci.
- *Sítnice* - Obsahuje tzv. fotoreceptory. Tyto buňky přijímají světelné a barevné podněty, které nám umožňují vidět.
- *Zrakový nerv* - Nese obrovský počet nervových vláken ústících do mozku.
- *Cévnatka* - Je tvořena střední vrstvou stěny oční koule. Obsahuje převážně cévy a je to nejvíce prokrvená tkáň tělesa. Má na starosti výživu vnější sítnice [1,17].

### **3.3 Struktura oční duhovky**

Každý z nás má jedinečnou oční duhovku, která se formuje od 3 měsíce těhotenství. Jedná se o pigmentovanou membránu obklopující čočku oka a její struktura se časem nemění. Tato biometrická metoda pracující na rozpoznávání podle oční duhovky patří mezi ty nejpřesnější a nespolehlivější techniky, jak tomu bylo u oční sítnice, která je popsána v předchozí kapitole. Díky své spolehlivosti jsou i menší šance odmítnutí.

Oční duhovky jsou u jednovaječných dvojčat rozdílné a jedinečné. Dokonce i lidská osoba má obě duhovky odlišné a jedinečné a z tohoto tvrzení vyplývá, že oční duhovka patří mezi k jedinečné rozlišovací charakteristice člověka [18].

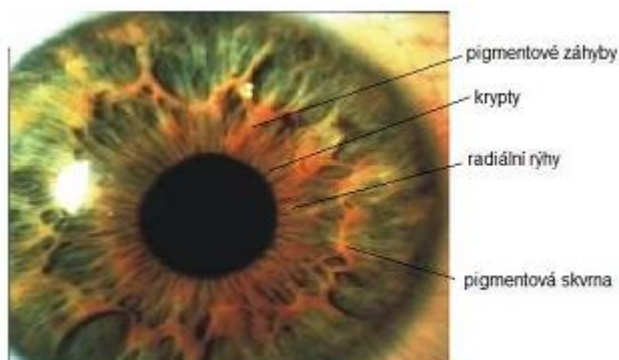
Oční duhovky mají různou barevnost, která je způsobená barvivem nazývaným *melanin*. Na obrázku jsou vidět různé barevné formy duhovek.



Obrázek 17. Různá barevnost oční duhovky [9]

#### Vnější charakteristiky duhovky:

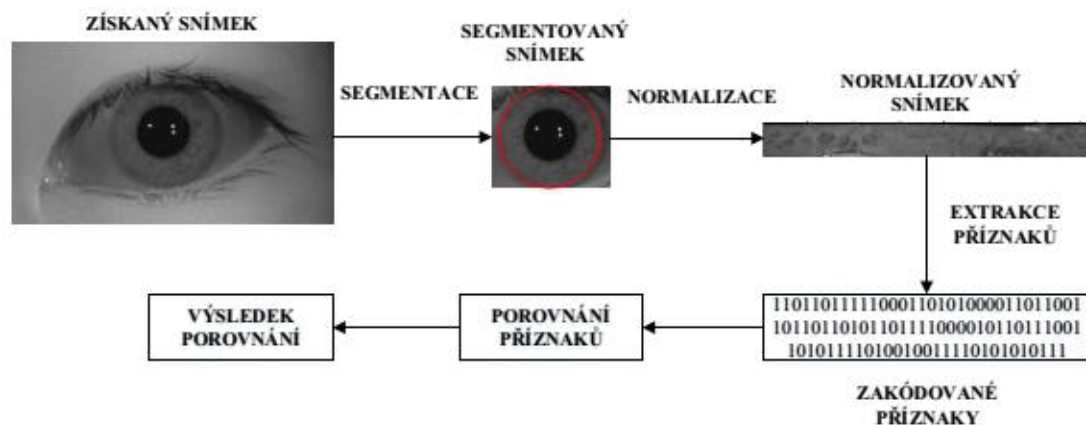
- *Pigmentové skvrny* - Náhodný hlouček pigmentových buněk u povrchu duhovky, výskyt v řasnaté oblasti.
- *Krypty* - Tmavá místa, kde je duhovka docela tenká, výskyt na rozhraní mezi řasnatou a zornicovou oblastí.
- *Pigmentové záhyby* - Vystupující spodní vrstva duhovky v okolí zornice.
- *Radiální rýhy* - Výskyt poblíž zornice a paprskovitě vyběhající směrem k okraji duhovky.



Obrázek 18. Rysy oční duhovky [9]

### 3.4 Princip identifikace podle oční duhovky

Postup zpracování snímku oční duhovky je rozdělen do 4 kroků a to do segmentace, normalizace, extrakce příznaků a porovnání příznaků. Na základě různých postupů vzniklo několik metod k identifikaci osob podle oční duhovky, níže je popsán nejznámější postup analýzy oční duhovky [11].



Obrázek 19. Obecné schéma biometrie oční duhovky [6]

#### Získání snímku

Při získávání snímku ze snímače může dojít k různým negativním faktorům, které mohou mít za následek zhoršení zpracovaného snímku. Mezi vlivy patří např. šum, rozmazání apod. Při odstranění těchto vlivů se zvýší především přesnost biometrického systému. Snímač převede všechny získané barevné obrázky do šedavého spektra a tím dojde k odstranění některých odchylek v barevných tónech. Tyto odchylky mohou vznikat v důsledku použitých CCD snímačů. Poté je nutné normalizovat barevnou škálu pořízeného snímku k lepšímu zvýraznění hran [11].

#### Segmentace

Dalším krokem je segmentace, která má za následek určit polohu duhovky a zornice (pupila). Tahle část analýzy oční duhovky patří mezi ty pomalejší z celého systému. Je to způsobeno tím, že je nutné určit polohu duhovky a zornice a zajistit všechny hrany, které se nachází v získaném snímku. Pro zjišťování hran z obrázku existují různé algoritmy např. Sobelův a Canneho detektor hran, které jsou založené na objevování gradientu v sousedních pixelech [11].

### Normalizace

Základem normalizace jsou souřadnice bodů snímané duhovky a jejího středu. Postup funguje tak, že duhovka tvaru mezikružní je převedena do obdélníkového tvaru. Výsledný snímek je obdélník, na kterém najdeme souřadnice poloměrů a úhlů. Na kratší straně obdélníku tj. svislá osa, jsou poloměry kružnice a na delší straně tj. vodorovná osa, jsou pak úhlové souřadnice. Jedná se o převod kartézských souřadnic na souřadnice polární [6].

### Extrakce příznaků

Dalším krokem je extrakce příznaků, kde jsou vstupní data extrahována a zakódována do významných znaků. Výsledkem pak vznikne dvoubitová informace, která obsahuje souřadnice části duhovky.

### Porovnání příznaků

Tento krok je poslední v metodě biometrie duhovky, kde dochází k porovnání příznaků se šablonou uloženou v databázi a výsledek je nazýván **míra shody**. Míra shody nám ukazuje jaká je podobnost mezi kódem šablony a kódem duhovky. Pokud se příznaky shodují se šablonou uloženou v databázi, systém přístup schválí a v opačném případě přístup odmítne. Porovnání se provádí pomocí Hammingovy vzdálenosti mezi dvěma body [6].

## **3.5 Výhody a nevýhody použití oční duhovky pro biometrickou identifikaci**

### Mezi výhody patří:

- Duhovka je během života stabilní.
- Pořizování snímků pro uživatele není nepříjemné.
- Duhovka je dobře chráněna proti vnějším vlivům, protože se jedná o vnitřní orgán.
- Malá velikost šablony v databázi.

### Mezi nevýhody patří:

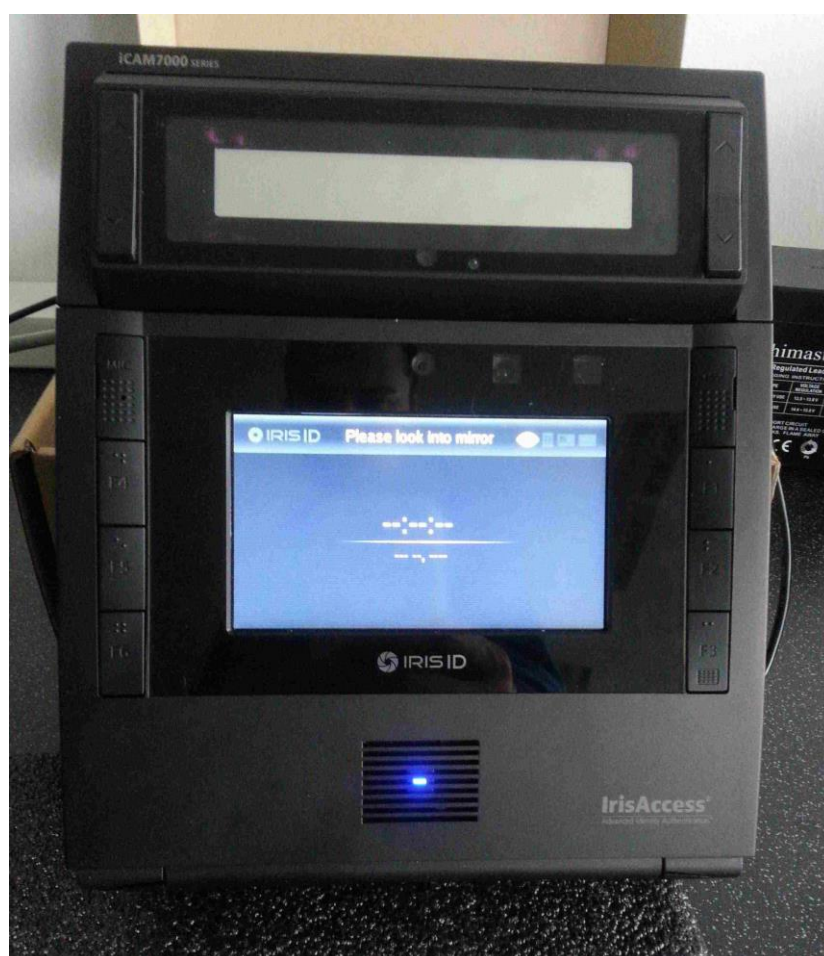
- Duhovka se vlivem různých nemocí může změnit, např. při operaci šedého zákalu.
- Velké pořizovací náklady [1].

## **II. PRAKTICKÁ ČÁST**



## 4 SKENER OČNÍ DUHOVKY

Pro vypracování praktické části bylo provedeno měření na skeneru oční duhovky od firmy Iris ID Systems ze série IrisAccess® 7000, konkrétně iCAM7000. Tento skener využívá plně automatické snímání oční duhovky a umožňuje i zachycení snímku obličeje kolem očí. Je vybaven hlasovým a vizuálním rozhraním, což vede k rychlejšímu a přesnějšímu zápisu duhovky a následné identifikaci/verifikaci. Ke správné identifikaci osob mu postačuje 60 - 70% viditelnosti oční duhovky.



Obrázek 20. iCAM7000

Společnost Iris ID System se posledních 15 let zabývá vývojem technologií k rozpoznávání oční duhovky. IrisAccess nadále vede na trhu jako nejvyspělejší a nejrozšířenější platforma pro rozpoznávání duhovky na světě.

## 4.1 Technické parametry skeneru iCAM7000

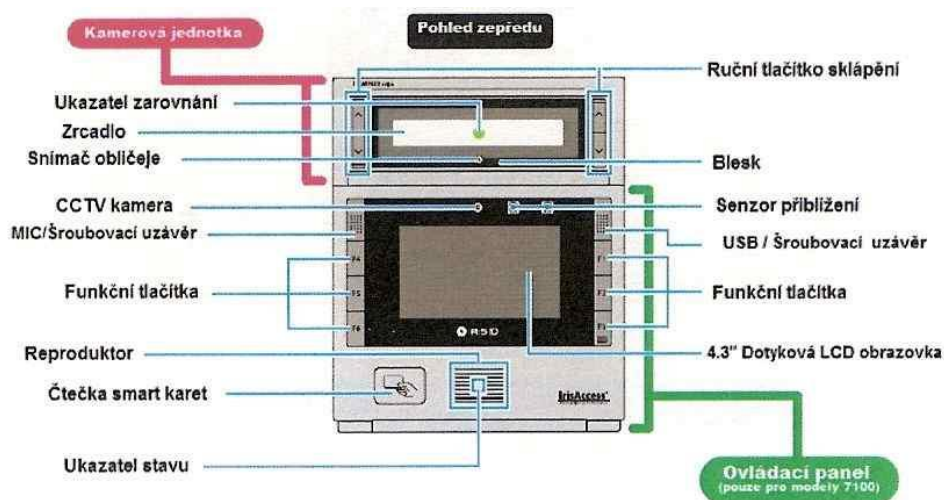
Tabulka 1. Technické specifikace skeneru [20]

Rozměry	178mm x 211mm x 64mm
Hmotnost	1,6 kg
Příkon (spotřeba)	12 - 24 VDC, 2A @ 12VDC / 24 W
Parametry LED	Více barev - červená, zelená, modrá
Parametry pracovního rozsahu (duhovka)	Dvoubarevný - oranžová, zelená
Hlasová indikace	Standardně Angličtina, zbytek po stažení
Rozsah snímání duhovky	31 cm - 35 cm
Uživatelský vstup	Funkční klávesy - 6 uživatelsky definovaných
Dotyková LCD obrazovka	4,3 " (480 x 272 pixelů / iCAM7100)
Blesk	Vysoce výkonný blesk pro snímání obličeje
Kamera pro snímání obličeje	Face camera CMOS - 5Mpx
2 Relé (dveře, ostatní)	Ovládání všech elektricky uzamykatelných mechanismů + pomocné relé pro uživatelsky definované operace.
Připojení externího paměťového zařízení	USB port
Provozní teplota	0 °C - 45 °C
Skladová teplota	-20 °C - 95 °C
Vlhkost	Až 90 % (nekondenzující)
Rotační úhel kamery	+35° /-25°
Komunikace	Ethernet (LAN, WAN), RS422, RS232
Vstupy / výstupy	Proximity Card Reader (Wiegand In), Embedded Smart Card Reader (Optional), Wiegand In, Wiegand Out, Dry Contact Relay x 2, Programmable GPIO x 4
Zařízení dodávaná s iCAM7000	Manuál - Příručka HW

## 4.2 Potřebné vybavení k funkčnímu provozu

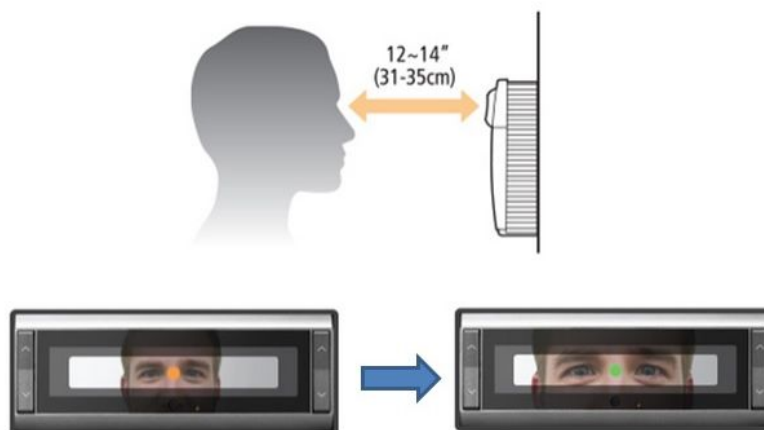
- Zdroj napájení
  - 12 - 24 VDC +/- 10% / Minimum 24W (12 VDC @ 2A) (měřeno v jednotkách iCAM)
  - Stabilní zdroj napájení
- Síť
  - Ethernetová kabeláž -> CAT5e Ethernet kabeláž
- Software

### 4.3 Popis ovládacích prvků skeneru iCAM7000



Obrázek 21. Ovládací prvky skeneru [20]

### 4.4 Uživatelské rozhraní



Obrázek 22. Potřebná vzdálenost k zachycení snímku [20]

Zařízení iCAM se aktivuje, pokud se uživatel přiblíží, nebo předloží identifikační kartu. Skener je schopný zachytit obraz ve vzdálenosti 31 - 35 cm a má možnost automatického nebo vlastního nastavení výšky pomocí ovládacích tlačítek.

Zařízení iCAM je vybaveno indikační tečkou v místě horní části nosu, která napomáhá k zarovnání očí do správné polohy. Ve chvíli, kdy se uživatel nachází ve správné

vzdálenosti, se oranžová tečka změní na zelenou. Celý proces snímání je ještě doplněn o zvukové výzvy k snadnějšímu pořízení snímku.

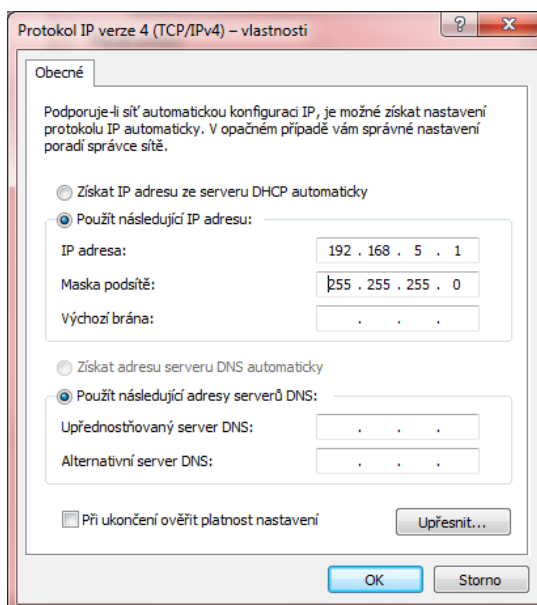
## 4.5 Propojení skeneru s PC

V první řadě je potřeba nainstalovat potřebný software, který je určený pro komunikaci mezi počítačem a skenerem. Pomocí nainstalovaného softwaru se provádí řada operací, a to zejména identifikace a vytvoření referenčního záznamu nových uživatelů.

V dalším kroku bylo potřeba připojit ke skeneru napájecí adaptér s minimálním příkonem 24W a propojit skener s počítačem pomocí ethernetového kabelu.

Poté je potřeba nastavit v počítači IP adresu (obrázek 23), aby došlo ke správné komunikaci mezi zařízeními, a to provedeme následovně:

- Otevřeme *Ovládací panely* → *Síť a Internet* → *Síťová připojení* a u místní sítě změníme *Protokol IP verze 4 (TCP/IPv4)* na parametry, jak je možné vidět na obr. 23 a tím je zajištěno spojení mezi zařízeními.

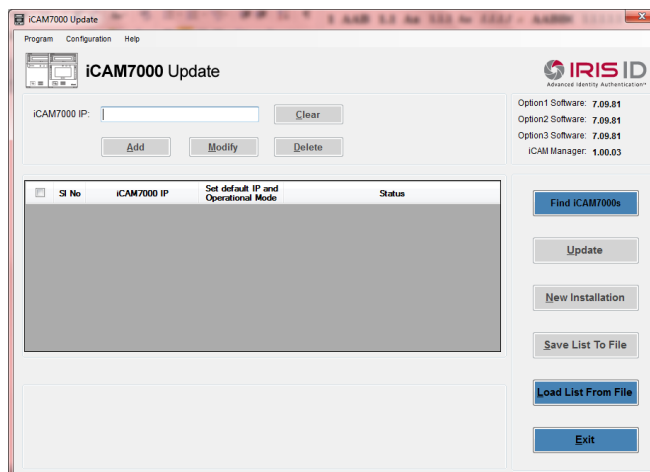


Obrázek 23. Vlastnosti IPv4 protokolu

### 4.5.1 Instalace softwaru

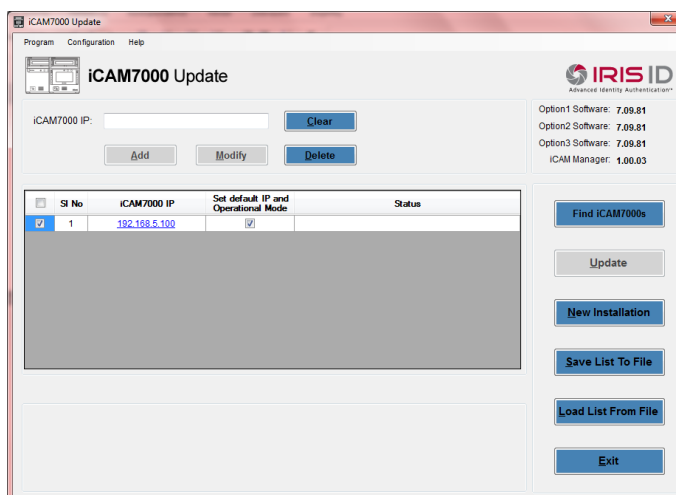
Po vložení CD do mechaniky nainstalujeme software iCAM Manager SDK, který byl součástí balení. Po zdařilé instalaci se nám v počítači objeví tři nově nainstalované aplikace, které si popíšeme v dalších krocích.

- Otevřeme aplikaci **iCAM7000Update**.



Obrázek 24. Rozhraní aplikace

- Klikneme na záložku *Find iCAM7000s* a tím dojde k vyhledání zařízení.

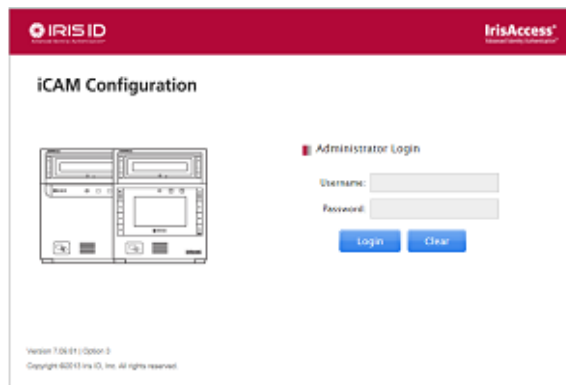


Obrázek 25. Vyhledané zařízení

- Klikneme na záložku *New Installation*, a tím dojde k nainstalování skeneru do počítače.
- Otevřeme internetový prohlížeč, kde vepíšeme IP adresu skeneru - 192.168.5.100 a posléze se objeví okno, jak je možné vidět na obrázku 26. Do tohoto okna napíšeme přihlašovací údaje:

Username: **iCAM7000**

Password: **iris7000**

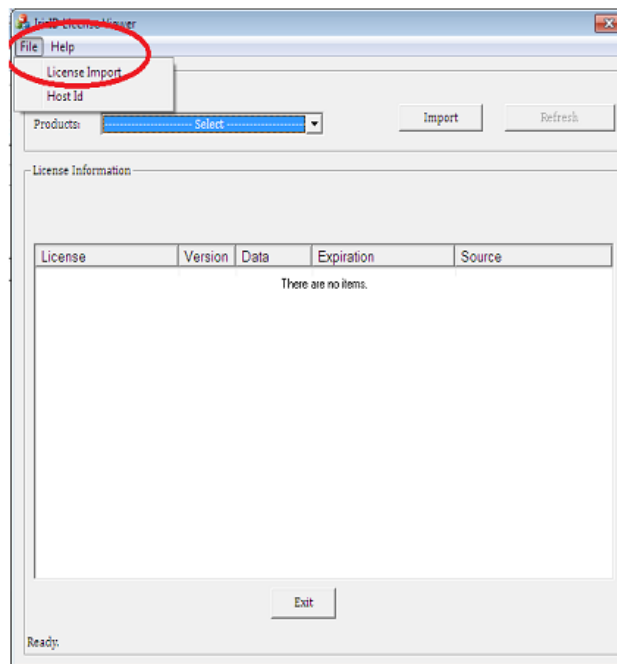


Obrázek 26. Přihlašovací okno

- Při vyplnění přihlašovacích údajů se objeví okno, kde nastavíme správný provozní režim "ICAM Manager" a v posledním políčku nastavíme *Security ID* na výchozí hodnotu (11111111111111) a stiskneme tlačítko *Apply*.

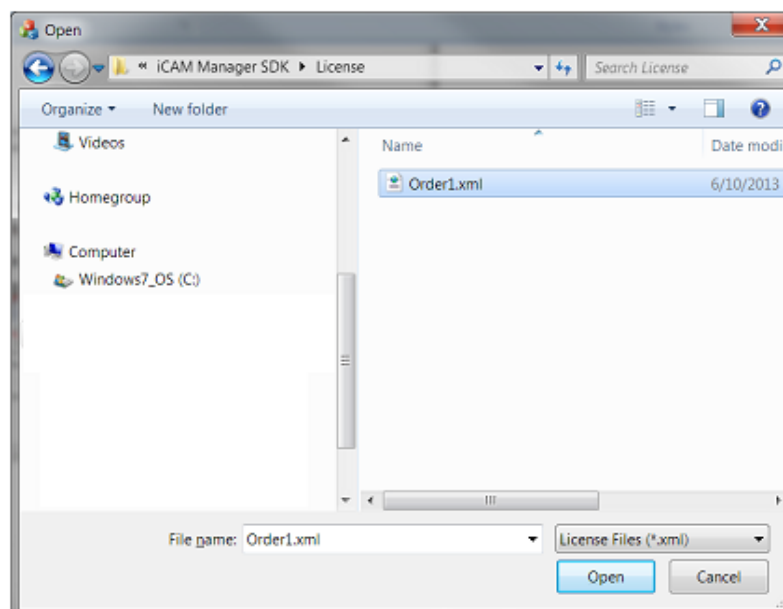
Obrázek 27. Nastavení provozního režimu

- Spustíme aplikaci **iCAM License Viewer** a klikneme na *File* → *License Import*.



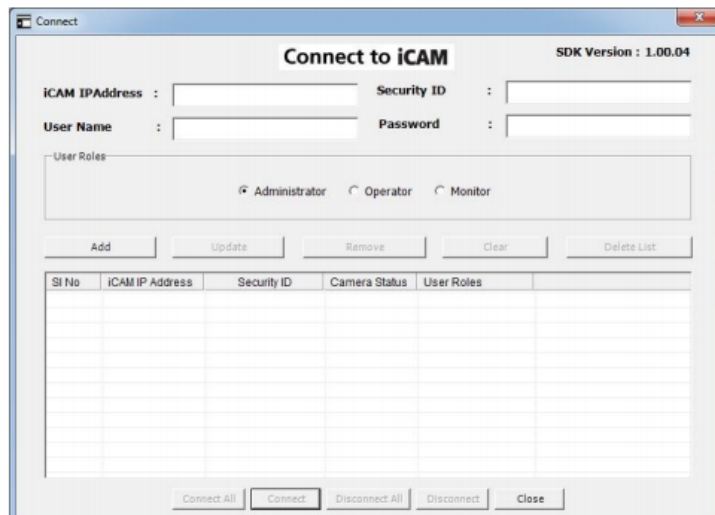
Obrázek 28. License Import

- Otevře se okno, kde vybereme příslušnou licenci, jak je vidět na obrázku níže a potvrdíme tlačítkem *otevřít*.



Obrázek 29. Vložení licence

- Tím je vložena licence do programu.
- Otevřeme aplikaci **iCAM Manager SDK Sample**.



Obrázek 30. iCAM Manager SDK Sample

- Kde zadáme *iCAM IP Address*, *Security ID*, *User Name*, *Password*, *User Roles*:

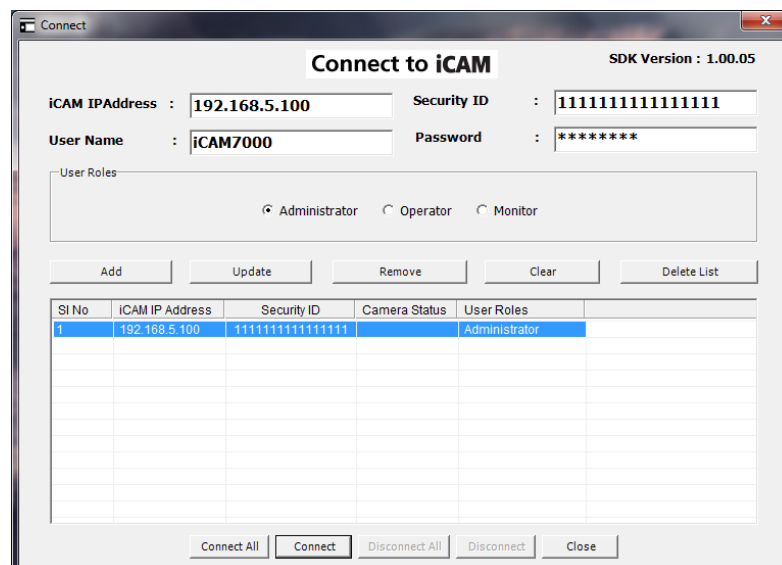
iCAM IP Address = 192.168.5.100

Security ID = 1111111111111111

User Name = iCAM7000

Password = iris7000

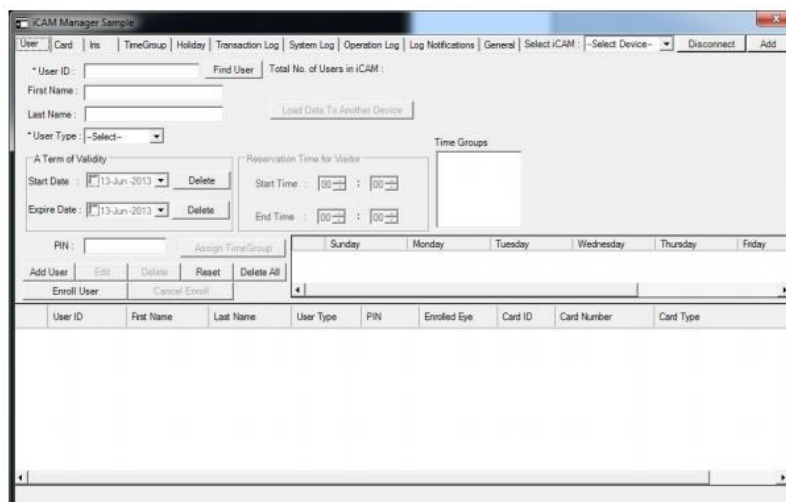
- Klikneme na *Add* a tím bude přidáno zařízení do seznamu.



Obrázek 31. Připojení ke skeneru

- Klikneme na *Connect* a pokud jsou hodnoty správné, zobrazí se hlavní obrazovka.





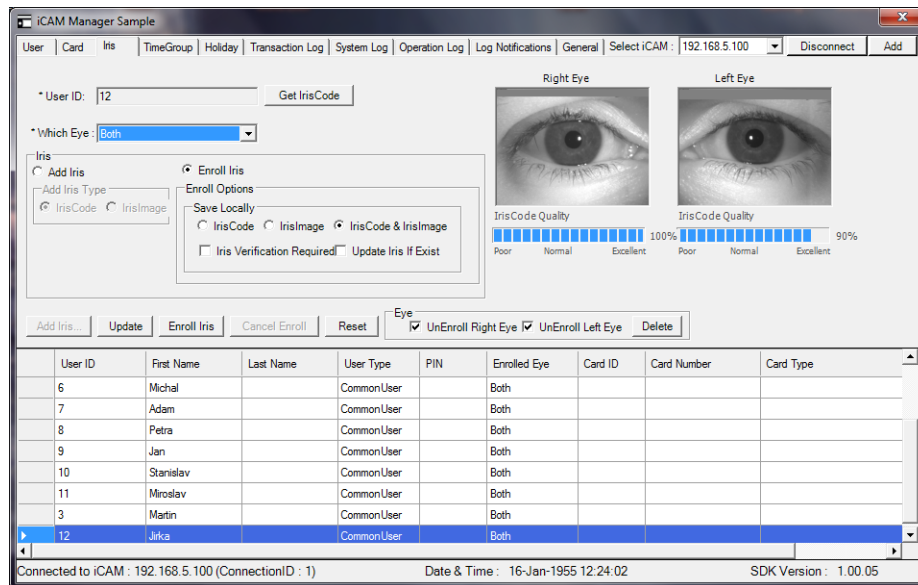
Obrázek 32. Hlavní obrazovka iCAM Manageru

Tímto jsme docílili správného nastavení a konfigurace zařízení s počítačem a nyní je skener připraven ke správnému fungování.

#### 4.5.2 Uživatelské prostředí

Po spuštění programu *iCAM Manager SDK Sample* se zobrazí hlavní okno, kde vytvoříme referenční záznam s novými uživateli. Do jednotlivých polí (User ID, First Name, Last Name, User Type) napíšeme informace o uživateli a pomocí tlačítka *Add User* přidáme dotyčnou osobu do databáze uživatelů. Pomocí tlačítka *Enroll User* se zvolí, jaké oko bude zaznamenáno (pravé, levé nebo obě), a poté se provede snímek oční duhovky pomocí skeneru. Tím se vytvoří snímek oční duhovky a uloží se do databáze k patřičné osobě. Při novém přístupu ke skeneru už nedochází k vytvoření nového snímku oční duhovky, ale přistupuje se už dříve k uloženému záznamu, který je uchován v databázi pod dotyčnou osobou. Na základě naskenování oční duhovky systém buď povolí, nebo zamítne přístup uživateli.

Snímek pořízený skenerem a následné vyobrazení očních duhovek v programu *iCAM Manager SDK Sample* je možné vidět na obrázku (Obrázek 33.).



Obrázek 33. Snímek očí v iCAM Manageru

#### 4.6 Naměřená data pomocí skeneru oční duhovky

Úkolem bylo ověřit spolehlivost skeneru oční duhovky a to za různých podmínek:

- Při snížené světelné viditelnosti - Měření bylo provedeno za denního světla, při snížené viditelnosti, při umělém osvětlení a při úplném zatmění.
- Pod různým úhlem pohledu - Měření bylo provedeno pod úhlem 45° a to tak, že dotyčná osoba se dívala pěti různými směry od zrcadla skeneru (nahoru, dolů, doprava, doleva a šikmo od pravého rohu zrcadla skeneru).
- Při fyzické zátěži člověka - Měření bylo provedeno při různé fyzické zátěži lidského organismu.

Všechna měření na skeneru byla měřena i pomocí časomíry, pro zjištění časového intervalu od přístupu uživatele k zařízení, až po samostatné vyhodnocení skenerem. Jednotlivé časy jsou uvedeny v příčinných tabulkách níže.

Měření bylo zaměřeno také na vliv kontaktních čoček a dioptrických brýlí na spolehlivost skeneru.

Dále byla testována možnost obejít biometrického systému za pomocí fotografie očí ve skutečné velikosti. Test měl ukázat vliv fotografie na identifikaci osoby, která je v systému zaregistrována.

Jednotlivá měření jsou rozdělena na uživatele s dioptrickými brýlemi, bez dioptrických brýlí a na uživatele s kontaktními čočkami.

#### 4.6.1 Měření za denního světla

Tabulka 2. Za denního světla bez dioptrických brýlí

Měření za denního světla bez dioptrických brýlí				
	Obě oči		Jedno oko	
	Čas [s]	Umožněn přístup	Čas [s]	Umožněn přístup
Uživatel 1	4,45	ANO	3,10	ANO
	5,41	ANO	2,90	ANO
	3,74	ANO	2,50	ANO
	6,39	ANO	2,30	ANO
	7,00	ANO	3,50	ANO
Uživatel 7	1,42	ANO	3,87	ANO
	1,21	ANO	1,95	ANO
	1,78	ANO	2,10	ANO
	1,30	ANO	3,21	ANO
	1,88	ANO	3,65	ANO
Uživatel 8	1,14	ANO	1,23	ANO
	1,32	ANO	1,54	ANO
	0,95	ANO	2,19	ANO
	1,43	ANO	2,87	ANO
	0,71	ANO	1,88	ANO
Uživatel 9	2,10	ANO	1,79	ANO
	1,54	ANO	2,29	ANO
	1,30	ANO	1,51	ANO
	2,10	ANO	1,65	ANO
	1,52	ANO	2,04	ANO
Uživatel 10	1,58	ANO	2,13	ANO
	1,29	ANO	1,52	ANO
	1,23	ANO	1,30	ANO
	1,42	ANO	1,87	ANO
	1,14	ANO	2,41	ANO
Uživatel 11	2,78	ANO	2,14	ANO
	2,54	ANO	2,25	ANO
	2,07	ANO	2,41	ANO
	2,45	ANO	2,32	ANO
	1,50	ANO	2,66	ANO

Tabulka 3. Za denního světla s dioptrickými brýlemi

Měření za denního světla s dioptrickými brýlemi				
	Obě oči		Jedno oko	
	Čas [s]	Umožněn přístup	Čas [s]	Umožněn přístup
Uživatel 4	2,25	ANO	1,58	ANO
	2,55	ANO	3,04	ANO
	3,23	ANO	2,65	ANO
	3,38	ANO	2,78	ANO
	4,49	ANO	1,65	ANO
Uživatel 5	1,61	ANO	4,78	NE
	1,80	ANO	6,32	NE
	1,94	ANO	4,45	NE
	1,79	ANO	5,78	NE
	2,05	ANO	4,63	ANO
Uživatel 6	4,03	ANO	9,95	NE
	2,46	ANO	4,58	NE
	1,88	ANO	3,18	ANO
	1,85	ANO	5,46	NE
	1,70	ANO	6,62	ANO

Tabulka 4. Za denního světla s kontaktními čočkami

Měření za denního světla s kontaktními čočkami				
	Obě oči		Jedno oko	
	Čas [s]	Umožněn přístup	Čas [s]	Umožněn přístup
Uživatel 2	1,58	ANO	3,40	ANO
	3,03	ANO	2,90	ANO
	3,68	ANO	2,50	ANO
	2,20	ANO	4,21	ANO
	2,40	ANO	3,98	ANO

Tabulka 5. Za denního světla bez kontaktních čoček

Měření za denního světla bez kontaktních čoček				
	Obě oči		Jedno oko	
	Čas [s]	Umožněn přístup	Čas [s]	Umožněn přístup
Uživatel 2	1,52	ANO	4,23	ANO
	3,91	ANO	2,48	ANO
	3,07	ANO	3,03	ANO
	2,75	ANO	3,54	ANO
	2,86	ANO	4,20	ANO

Měření za denního světla bylo provedeno pro obě oči a při zakrytí jednoho oka. Zakrytí jednoho oka nemělo žádný vliv na povolení přístupu uživatelem, protože počáteční registrace byla provedena pro obě oči.

Je možno vidět, že u uživatelů bez dioptrických brýlí (uživatel: 1,7,8,9,10,11) proběhlo měření se 100% povolením přístupu. Zatímco u uživatelů s dioptrickými brýlemi vykazoval skener u uživatele 5 při zavření jednoho oka 20% spolehlivosti, a u uživatele 6 při zavření jednoho oka 40% spolehlivosti, což může být způsobeno špatným načtením snímku oka při počáteční registraci.

Jak je možné vidět u uživatele 2, kontaktní čočky nemají žádný vliv na umožnění přístupu dotyčné osoby.

#### 4.6.2 Měření při snížené viditelnosti

Zatemnění bylo provedeno pomocí žaluzií, a tím bylo docíleno snížení intenzity osvětlení.

Tabulka 6. Při snížené viditelnosti s dioptrickými brýlemi

<b>Měření při snížené viditelnosti s dioptrickými brýlemi</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 4</b>	2,44	ANO
	1,58	ANO
	1,99	ANO
	1,57	ANO
	1,42	ANO
<b>Uživatel 5</b>	1,76	ANO
	1,58	ANO
	1,45	ANO
	1,52	ANO
	2,27	ANO
<b>Uživatel 6</b>	2,75	ANO
	4,02	ANO
	1,48	ANO
	1,67	ANO
	2,95	ANO

Tabulka 7. Při snížené viditelnosti bez dioptrických brýlí

<b>Měření při snížené viditelnosti bez dioptrických brýlí</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 1</b>	2,70	ANO
	2,30	ANO
	2,00	ANO
	1,80	ANO
	0,50	ANO
<b>Uživatel 7</b>	3,12	ANO
	1,48	ANO
	1,57	ANO
	1,86	ANO
	1,48	ANO
<b>Uživatel 8</b>	2,38	ANO
	1,76	ANO
	1,17	ANO
	1,26	ANO
	1,36	ANO
<b>Uživatel 9</b>	2,09	ANO
	1,73	ANO
	1,72	ANO
	1,98	ANO
	1,57	ANO
<b>Uživatel 10</b>	2,00	ANO
	1,42	ANO
	1,11	ANO
	1,42	ANO
	1,29	ANO
<b>Uživatel 11</b>	2,57	ANO
	2,11	ANO
	2,35	ANO
	1,70	ANO
	2,43	ANO

Tabulka 8. Při snížené viditelnosti s kontaktními čočkami

<b>Měření při snížené viditelnosti s kontaktními čočkami</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 2</b>	2,25	ANO
	2,10	ANO
	2,60	ANO
	3,00	ANO
	1,90	ANO

Tabulka 9. Při snížené viditelnosti bez kontaktních čoček

Měření při snížené viditelnosti bez kontaktních čoček		
	Čas [s]	Umožněn přístup
Uživatel 2	2,65	ANO
	2,14	ANO
	3,87	ANO
	4,00	NE
	3,07	ANO

Měření kromě uživatele 2 s kontaktními čočkami vykazovalo 100% spolehlivost skeneru k povolení přístupu registrovaných osob. Při měření uživatele 2 bez kontaktních čoček vykazovala spolehlivost 80%.

#### 4.6.3 Měření při úplném zatmění

Měření bylo provedeno za úplné tmy.

Tabulka 10. Při úplném zatmění s dioptrickými brýlemi

Měření při úplném zatmění s dioptrickými brýlemi		
	Čas [s]	Umožněn přístup
Uživatel 4	3,93	NE
	2,28	ANO
	2,26	ANO
	1,18	ANO
	1,95	ANO
Uživatel 5	1,58	NE
	1,55	NE
	2,57	NE
	1,60	NE
	2,81	ANO
Uživatel 6	5,63	ANO
	1,50	ANO
	1,54	ANO
	7,80	ANO
	2,01	ANO

Tabulka 11. Při úplném zatmění bez dioptrických brýlí

Měření při úplném zatmění bez dioptrických brýlí		
	Čas [s]	Umožněn přístup
Uživatel 1	5,72	ANO
	10,81	ANO
	4,02	ANO
	0,78	NE
	1,05	NE
Uživatel 7	11,19	ANO
	5,90	ANO
	6,63	NE
	2,83	ANO
	1,15	ANO
Uživatel 8	1,05	ANO
	6,57	ANO
	1,17	NE
	0,70	NE
	1,05	ANO
Uživatel 9	2,01	ANO
	1,39	ANO
	1,24	ANO
	1,40	ANO
	1,42	ANO
Uživatel 10	4,23	ANO
	1,70	ANO
	1,42	ANO
	0,98	ANO
	0,86	NE
Uživatel 11	12,70	ANO
	5,87	ANO
	1,55	ANO
	19,48	ANO
	8,09	ANO

Tabulka 12. Při úplném zatmění s kontaktními čočkami

Měření při úplném zatmění s kontaktními čočkami		
	Čas [s]	Umožněn přístup
Uživatel 2	2,40	NE
	6,10	NE
	5,10	ANO
	4,70	ANO
	3,20	ANO



Tabulka 13. Při úplném zatmění bez kontaktních čoček

Měření při úplném zatmění bez kontaktních čoček		
	Čas [s]	Umožněn přístup
Uživatel 2	3,54	ANO
	3,22	NE
	5,36	ANO
	4,20	ANO
	2,55	ANO

Úplné zatmění mělo nepatrný vliv na skener, přestože je skener vybaven vlastním bleskem a infračerveným světlem. Měření u uživatele 4 skener vykazoval 80% úspěšnosti, uživatel 5 - 20% úspěšnosti, uživatel 1 - 60% úspěšnosti, uživatel 7 - 80% úspěšnosti, uživatel 8 - 60% úspěšnosti, uživatel 10 - 80% úspěšnosti, uživatel 2 s kontaktními čočkami - 60% úspěšnosti a bez kontaktních čoček 80% úspěšnosti povolení přístupu do systému.

#### 4.6.4 Měření při umělém osvětlení

Měření bylo provedeno za pomoci osvětlení místnosti zářivkami umístěnými na stropě.

Tabulka 14. Při umělém osvětlení s dioptrickými brýlemi

Měření při umělém osvětlení s dioptrickými brýlemi		
	Čas [s]	Umožněn přístup
Uživatel 4	1,77	ANO
	1,32	ANO
	1,35	ANO
	1,45	ANO
	1,29	NE
Uživatel 5	2,20	ANO
	1,94	NE
	1,95	ANO
	1,54	ANO
	1,30	ANO
Uživatel 6	2,84	ANO
	1,73	NE
	2,50	ANO
	2,42	NE
	3,90	ANO

Tabulka 15. Při umělém osvětlení bez dioptrických brýlí

<b>Měření při umělém osvětlení bez dioptrických brýlí</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 1</b>	3,80	ANO
	1,40	ANO
	1,30	ANO
	1,90	ANO
	1,00	ANO
<b>Uživatel 7</b>	1,63	ANO
	1,38	ANO
	1,90	ANO
	1,36	ANO
	1,27	ANO
<b>Uživatel 8</b>	2,63	ANO
	1,70	ANO
	1,15	ANO
	1,23	ANO
	1,04	ANO
<b>Uživatel 9</b>	2,25	ANO
	1,15	ANO
	1,41	ANO
	1,17	ANO
	1,23	ANO
<b>Uživatel 10</b>	1,89	ANO
	1,17	ANO
	1,05	ANO
	0,91	ANO
	1,46	ANO
<b>Uživatel 11</b>	1,88	ANO
	1,33	ANO
	1,76	ANO
	1,67	ANO
	1,71	ANO

Tabulka 16. Při umělém osvětlení s kontaktními čočkami

<b>Měření při umělém osvětlení s kontaktními čočkami</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 2</b>	2,70	ANO
	2,90	ANO
	2,30	ANO
	2,40	ANO
	2,47	ANO

Tabulka 17. Při umělém osvětlení bez kontaktních čoček

Měření při umělém osvětlení bez kontaktních čoček		
	Čas [s]	Umožněn přístup
Uživatel 2	3,45	ANO
	3,04	ANO
	2,87	ANO
	2,66	ANO
	3,14	ANO

Při umělém osvětlení vykazoval skener u uživatele 4 - 80%, uživatel 5 - 80%, uživatel 6 - 60% a u ostatních 100% úspěšnosti při povolení přístupu.

#### 4.6.5 Měření pod různým úhlem pohledu

Měření bylo provedeno pod úhlem 45° a to tak, že dotyčná osoba se dívala pěti různými směry od zrcadla skeneru (nahoru, dolů, doprava, doleva a šikmo od pravého rohu zrcadla skeneru).

Tabulka 18. Při pozorovacím úhlu s dioptrickými brýlemi

Měření při pozorovacím úhlu s dioptrickými brýlemi		
	Čas [s]	Umožněn přístup
Uživatel 4	2,14	ANO
	2,26	ANO
	1,64	ANO
	2,73	ANO
	1,82	ANO
Uživatel 5	7,63	ANO
	1,79	ANO
	1,51	ANO
	2,08	ANO
	1,54	ANO
Uživatel 6	2,00	ANO
	2,45	NE
	2,60	ANO
	2,19	ANO
	3,65	ANO

Tabulka 19. Při pozorovacím úhlu bez dioptrických brýlí

<b>Měření při pozorovacím úhlu bez dioptrických brýlí</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 1</b>	5,48	ANO
	3,87	ANO
	4,22	NE
	6,88	ANO
	4,64	ANO
<b>Uživatel 7</b>	1,69	ANO
	5,73	NE
	2,10	NE
	8,33	NE
	1,86	NE
<b>Uživatel 8</b>	2,04	ANO
	1,95	NE
	2,04	ANO
	1,82	ANO
	1,67	NE
<b>Uživatel 9</b>	3,65	ANO
	3,19	NE
	8,19	ANO
	1,86	ANO
	3,80	NE
<b>Uživatel 10</b>	4,74	NE
	1,27	NE
	10,87	NE
	2,32	NE
	6,35	NE
<b>Uživatel 11</b>	3,90	ANO
	4,95	ANO
	5,60	NE
	3,94	ANO
	5,07	NE

Tabulka 20. Při pozorovacím úhlu s kontaktními čočkami

<b>Měření při pozorovacím úhlu s kontaktními čočkami</b>		
	<b>Čas [s]</b>	<b>Umožněn přístup</b>
<b>Uživatel 2</b>	5,20	ANO
	10,60	ANO
	3,20	ANO
	11,90	NE
	3,80	ANO

Tabulka 21. Při pozorovacím úhlu bez kontaktních čoček

Měření při pozorovacím úhlu bez kontaktních čoček		
	Čas [s]	Umožněn přístup
Uživatel 2	4,51	ANO
	6,73	NE
	5,36	NE
	5,53	ANO
	4,12	ANO

Měření při pohledu mimo zrcadlo skeneru mělo větší vliv na povolení přístupu. Úhel pohledu byl změřen úhloměrem a následné vyznačení bodů kam se uživatelé mají dívat.

Měření u uživatele 1 vykazoval skener - 80% úspěšnost, uživatel 7 - 20% úspěšnost, uživatel 8 - 60% úspěšnost, uživatel 9 - 60% úspěšnost, uživatel 10 - 0% úspěšnost, uživatel 11 - 60% úspěšnost, uživatel 6 - 80% úspěšnost, uživatel 2 s kontaktními čočkami - 80% a bez kontaktních čoček - 60% úspěšnosti povolení přístupu.

#### 4.6.6 Měření při fyzické zátěži člověka

Tabulka 22. Při fyzické zátěži člověka

Měření při fyzické zátěži		
	Čas [s]	Umožněn přístup
Uživatel 3	3,46	ANO
	2,84	ANO
	2,32	ANO
	1,29	ANO
	0,74	ANO
Uživatel 10	2,80	ANO
	2,20	ANO
	1,40	ANO
	2,23	ANO
	3,22	ANO
Uživatel 11	1,74	ANO
	1,54	ANO
	1,91	ANO
	1,86	ANO
	3,99	ANO

Měření bylo provedeno na třech dobrovolnících, kteří se podrobili fyzické zátěži a následnému naskenování. U dvou dotyčných osob neměla fyzická zátěž žádný vliv na povolení přístupu osoby skenerem.

Byla zjištěna zajímavost, že uživatel 11, který vykonával 5 minutový běh do schodů, se nechal okamžitě po běhu naskenovat a zjistilo se, že skeneru trvalo přibližně 30 sekund, než dotyčnou osobu rozpoznal.

#### 4.7 Diskuze výsledků

Měření za denního světla vykazovalo největší úspěšnost povolení přístupu registrovaných osob. Test, který byl proveden pro obě oči, vykazoval 100% úspěšnost, zatímco test při zavření jednoho oka vykazoval menší úspěšnost. Mohlo to být způsobeno horší kvalitou snímku při počáteční registraci. Také dioptrické brýle s vyšším počtem dioptrií mohou mít vliv na procento úspěšnosti, což se ukázalo u uživatele 5, který měl v testu zavřené jedno oko. Kontaktní čočky neměly žádný vliv na umožnění přístupu dotyčné osoby.

Měření při snížené viditelnosti bylo provedeno pro obě oči, kde procento úspěšnosti bylo 100% až na uživatele 2, který neměl nasazené kontaktní čočky. U něho skener vykazoval 80% úspěšnosti. Z tohoto lze říci, že snížená viditelnost nemá vliv na funkčnost skeneru, protože skener je opatřen infračerveným světlem.

U měření za úplné tmy se spolehlivost skeneru nepatrně snížila, než tomu bylo v předešlých případech. Z toho vyplývá, že úspěšnost skeneru je o 20% - 30% nižší.

Při umělém osvětlení se ukázalo, že u sedmi uživatelů vykazoval skener 100% úspěšnost povolení přístupu, u dvou uživatelů 80% a u jednoho uživatele 60% úspěšnost povolení přístupu do systému. Z toho lze vyvodit, že měření za denního světla a umělého osvětlení dosahuje podobných výsledků.

Největší vliv na spolehlivost skeneru mělo měření při různých směrech pohledu mimo střed zrcadla skeneru. Zjistilo se, že procento úspěšnosti měření dosahovalo podstatně nižších hodnot než v předešlých případech.

Měření, při kterém byli uživatelé vystaveni fyzické zátěži organismu, se prokázalo, že čím je zátěž vyšší, tím se prodlužuje doba rozpoznání dotyčné osoby.

## ZÁVĚR

Cílem této bakalářské práce bylo seznámení s jednotlivými biometrickými systémy pro zvýšení bezpečnosti osob a majetku. Hlavním tématem bylo ověření spolehlivosti skeneru oční duhovky za různých podmínek. Zejména za snížených světelných podmínek, při fyzické zátěži člověka a při používání brýlí a kontaktních čoček.

Tato práce se ve své teoretické části zabývá biometrickou identifikací osob. V první části jsou vymezeny jednotlivé pojmy, se kterými se můžeme setkat v oblasti biometrie. Další část se zabývá jednotlivými biometrickými systémy, které jsou používány v současné době v bezpečnostním průmyslu.

Praktická část je zaměřena na ověření spolehlivosti skeneru oční duhovky za různých podmínek. Měření bylo provedeno na skeneru iCAM7000. Základem úspěšného měření bylo nejdříve správné nastavení skeneru a propojení s počítačem. Dalším důležitým faktorem pro měření bylo zapojení většího počtu osob, které se zúčastnili tohoto měření. Na tomto základě bylo možné provést více měření a tím lépe zjistit a porovnat spolehlivost skeneru oční duhovky. Měření bylo provedeno za různých světelných podmínek, a to zejména při umělém osvětlení, při částečném zatemnění, při denním světle a při úplné tmě. Při úplném a částečném zatemnění místnosti se skenerem bylo zjištěno, že naměřené údaje vykazovaly nižší hodnoty spolehlivosti. V dalším měření se zjišťovalo, jaký vliv bude mít fyzická zátěž. Na základě provedeného měření jsme došli k závěru, že fyzická zátěž lidského organismu nemá téměř žádný vliv na povolení přístupu uživatele. Ani kontaktní čočky nemají vliv na funkčnost zařízení. Naopak při pokusu s fotografií očí systém odmítl vstup uživatele. Při snímání je duhovka osvětlena a tím je snímáný pohyb duhovky při reakci na světlo. Zjistilo se, že skener reaguje pouze na živou tkáň.

Závěrem lze říci, že díky jedinečnosti oční duhovky bude tento biometrický systém v budoucnosti patřit k nejvyužívanějším a k nejspolehlivějším metodám při identifikaci osob. Jedná se o přístup do chráněných objektů, ochranu osob nebo např. o ochranu osobních údajů v běžném každodenním životě.

**SEZNAM POUŽITÉ LITERATURY**

- [1] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. [Brno: M. Dražanský], 2011, 294 s. ISBN 978-80-254-8979-6.
- [2] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.
- [3] RAK, Roman. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.
- [4] VALOVIČ, Róbert. 2014. *Spolehlivost 3D čtečky obličeje* [online]. Zlín [cit. 2015-03-09]. Dostupné z: [https://digilib.k.utb.cz/bitstream/handle/10563/30240/valovi%C4%8D\\_2014\\_dp.pdf?sequence=1&isAllowed=y](https://digilib.k.utb.cz/bitstream/handle/10563/30240/valovi%C4%8D_2014_dp.pdf?sequence=1&isAllowed=y). Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Doc. Mgr. Milan Adámek, Ph.D.
- [5] ONDRŮŠEK, Roman. 2006. *Identifikační biometrické prostředky* [online]. Zlín [cit. 2015-03-01]. Dostupné z: [https://digilib.k.utb.cz/bitstream/handle/10563/743/ondr%C5%AF%C5%A1ek\\_2006\\_bp.pdf?sequence=1](https://digilib.k.utb.cz/bitstream/handle/10563/743/ondr%C5%AF%C5%A1ek_2006_bp.pdf?sequence=1). Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Mgr. Milan Kvasnička, CSc.
- [6] TOBIÁŠOVÁ, Nela. 2014. *Biometrie s využitím snímků duhovky* [online]. Brno [cit. 2015-03-21]. Dostupné z: [https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/31568/nela\\_tobiasova\\_DP.pdf?sequence=2&isAllowed=y](https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/31568/nela_tobiasova_DP.pdf?sequence=2&isAllowed=y). Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Doc. Ing. Radim Kolář, Ph.D.
- [7] BRÁNÍK, Daniel. 2014. *Využití skeneru žilního řečiště v průmyslu komerční bezpečnosti* [online]. Zlín [cit. 2015-03-21]. Dostupné z: [https://digilib.k.utb.cz/bitstream/handle/10563/30239/br%C3%A1n%C3%ADk\\_2014\\_dp.pdf?sequence=1&isAllowed=y](https://digilib.k.utb.cz/bitstream/handle/10563/30239/br%C3%A1n%C3%ADk_2014_dp.pdf?sequence=1&isAllowed=y). Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Hana Talandová.
- [8] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava, 2006 [cit. 2015-04-23]. Dostupné z: [https://www.fbi.vsb.cz/export/sites/fbi/040/.content/systems/resource/PDF/biometricke\\_metody.pdf](https://www.fbi.vsb.cz/export/sites/fbi/040/.content/systems/resource/PDF/biometricke_metody.pdf)



- [9] TALANDOVÁ, Hana. 2010. *Studie využití biometrických systémů v průmyslu komerční bezpečnosti* [online]. Zlín [cit. 2015-04-04]. Dostupné z: [https://digilib.k.utb.cz/bitstream/handle/10563/13364/talandov%C3%A1\\_2010\\_bp.pdf?sequence=1&isAllowed=y](https://digilib.k.utb.cz/bitstream/handle/10563/13364/talandov%C3%A1_2010_bp.pdf?sequence=1&isAllowed=y). Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Petr Navrátil, Ph.D.
- [10] *BSA Security Integrators* [online]. [cit. 2015-04-21]. Dostupné z: <http://www.bsasi.com/schlage-handkeyii-biometric-reader>
- [11] AUERBACH, Alois. 2013. *Biometrická analýza oční duhovky* [online]. Plzeň [cit. 2015-04-22]. Dostupné z: [https://otik.uk.zcu.cz/bitstream/handle/11025/7587/DP\\_Auerbach.pdf?sequence=1](https://otik.uk.zcu.cz/bitstream/handle/11025/7587/DP_Auerbach.pdf?sequence=1). Diplomová práce. Západočeská univerzita v Plzni.
- [12] *iSlovácko: Internetový portál týdeníku* [online]. [cit. 2015-05-22]. Dostupné z: <http://www.islovacko.cz/Zpravy/973-sampionka-v-psani-na-klavesnici-vyrazi-na-mistrovstvi-sveta>
- [13] KOHOUTOVÁ, Hana. 2009. *Aplikace biometrie v ICT* [online]. Praha [cit. 2015-04-22]. Dostupné z: [https://is.bivs.cz/th/6213/bivs\\_b/HKohoutova\\_Biometrie.pdf](https://is.bivs.cz/th/6213/bivs_b/HKohoutova_Biometrie.pdf). Bakalářská práce. Bankovní institut vysoká škola Praha. Vedoucí práce Ing. Vladimír Beneš.
- [14] HORNÍČEK, Vladimír. 2008. *Identifikace osob pomocí oční duhovky* [online]. Brno [cit. 2015-04-29]. Dostupné z: [https://dspace.vutbr.cz/bitstream/handle/11012/14950/Vladim%C3%ADr%20Hornicek%2089119\\_BP\\_Identifikace%20osob%20pomoc%C3%AD%20o%C4%8Dn%C3%AD%20duhovky.pdf?sequence=1&isAllowed=y](https://dspace.vutbr.cz/bitstream/handle/11012/14950/Vladim%C3%ADr%20Hornicek%2089119_BP_Identifikace%20osob%20pomoc%C3%AD%20o%C4%8Dn%C3%AD%20duhovky.pdf?sequence=1&isAllowed=y). Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Tomáš Frýza, Ph.D.
- [15] *Lidské smysly* [online]. [cit. 2015-05-01]. Dostupné z: <http://www.lidske-smysly.wbs.cz/Zrak.html>
- [16] *Ordinace odborného očního lékaře* [online]. [cit. 2015-04-04]. Dostupné z: <http://www.stavaocniambulance.cz/ocni-onemocneni>
- [17] *Vidění* [online]. [cit. 2015-04-04]. Dostupné z: <http://www.videni.cz/oko/32-anatomie-oka>
- [18] *Biometrika* [online]. [cit. 2015-04-05]. Dostupné z: <http://www.nula.wz.cz/biometrika/duhovka.html>
- [19] *Discovery: Zone* [online]. [cit. 2015-05-22]. Dostupné z: <http://www.discovery-zone.com/the-twentieth-centurys-greatest-scientific-discovery/>

---

[20] *Iris ID* [online]. [cit. 2015-05-24]. Dostupné z:  
<http://www.irisid.com/productssolutions/hardwareproducts/icam7-series/>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

°C	Stupeň celsia
A	Ampér
CD	Compact disc
cm	Centimetr
DNA	Deoxyribonucleic Acid
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
HW	Hardware
IP	Internet Protocol
kg	Kilogram
LAN	Local Area Network
mm	Milimetr
Mpx	Megapixel
PC	Personal Computer
s	Sekunda
TCP	Transmission Control Protocol
USB	Universal Serial Bus
V	Volt
W	Watt
WAN	Wide Area Network

**SEZNAM OBRÁZKŮ**

<i>Obrázek 1. Schéma verifikace [6]</i> .....	12
<i>Obrázek 2. Schéma identifikace [6]</i> .....	13
<i>Obrázek 3. Ideální biometrická aplikace [3]</i> .....	15
<i>Obrázek 4. Reálná biometrická aplikace [3]</i> .....	15
<i>Obrázek 5. Základní klasifikační vzory [9]</i> .....	16
<i>Obrázek 6. Snímání šablonováním [8]</i> .....	17
<i>Obrázek 7. Rozmístění prstů mezi distančními kolíky [8]</i> .....	19
<i>Obrázek 8. Zařízení pro rozpoznávání geometrie ruky [10]</i> .....	19
<i>Obrázek 9. Žíly hřbetu ruky [3]</i> .....	20
<i>Obrázek 10. Identifikace podle podpisu [13]</i> .....	21
<i>Obrázek 11. Stisk kláves [11]</i> .....	22
<i>Obrázek 12. DNA [19]</i> .....	22
<i>Obrázek 13. Termální snímek [9]</i> .....	24
<i>Obrázek 14. Pohyb těžiště lidského těla [8]</i> .....	25
<i>Obrázek 15. Znárodnění cév za oční sítnici [8]</i> .....	26
<i>Obrázek 16. Anatomie lidského oka [16]</i> .....	27
<i>Obrázek 17. Různá barevnost oční duhovky [9]</i> .....	29
<i>Obrázek 18. Rysy oční duhovky [9]</i> .....	29
<i>Obrázek 19. Obecné schéma biometrie oční duhovky [6]</i> .....	30
<i>Obrázek 20. iCAM7000</i> .....	33
<i>Obrázek 21. Ovládací prvky skeneru [20]</i> .....	35
<i>Obrázek 22. Potřebná vzdálenost k zachycení snímku [20]</i> .....	35
<i>Obrázek 23. Vlastnosti IPv4 protokolu</i> .....	36
<i>Obrázek 24. Rozhraní aplikace</i> .....	37
<i>Obrázek 25. Vyhledané zařízení</i> .....	37
<i>Obrázek 26. Přihlašovací okno</i> .....	38
<i>Obrázek 27. Nastavení provozního režimu</i> .....	38
<i>Obrázek 28. License Import</i> .....	39
<i>Obrázek 29. Vložení licence</i> .....	39
<i>Obrázek 30. iCAM Manager SDK Sample</i> .....	40
<i>Obrázek 31. Připojení ke skeneru</i> .....	40
<i>Obrázek 32. Hlavní obrazovka iCAM Manageru</i> .....	41

---

*Obrázek 33. Snímek očí v iCAM Manageru ..... 42*

**SEZNAM TABULEK**

<i>Tabulka 1. Technické specifikace skeneru [20]</i> .....	34
<i>Tabulka 2. Za denního světla bez dioptrických brýlí</i> .....	43
<i>Tabulka 3. Za denního světla s dioptrickými brýlemi</i> .....	44
<i>Tabulka 4. Za denního světla s kontaktními čočkami</i> .....	44
<i>Tabulka 5. Za denního světla bez kontaktních čoček</i> .....	44
<i>Tabulka 6. Při snížené viditelnosti s dioptrickými brýlemi</i> .....	45
<i>Tabulka 7. Při snížené viditelnosti bez dioptrických brýlí</i> .....	46
<i>Tabulka 8. Při snížené viditelnosti s kontaktními čočkami</i> .....	46
<i>Tabulka 9. Při snížené viditelnosti bez kontaktních čoček</i> .....	47
<i>Tabulka 10. Při úplném zatmění s dioptrickými brýlemi</i> .....	47
<i>Tabulka 11. Při úplném zatmění bez dioptrických brýlí</i> .....	48
<i>Tabulka 12. Při úplném zatmění s kontaktními čočkami</i> .....	48
<i>Tabulka 13. Při úplném zatmění bez kontaktních čoček</i> .....	49
<i>Tabulka 14. Při umělém osvětlení s dioptrickými brýlemi</i> .....	49
<i>Tabulka 15. Při umělém osvětlení bez dioptrických brýlí</i> .....	50
<i>Tabulka 16. Při umělém osvětlení s kontaktními čočkami</i> .....	50
<i>Tabulka 17. Při umělém osvětlení bez kontaktních čoček</i> .....	51
<i>Tabulka 18. Při pozorovacím úhlu s dioptrickými brýlemi</i> .....	51
<i>Tabulka 19. Při pozorovacím úhlu bez dioptrických brýlí</i> .....	52
<i>Tabulka 20. Při pozorovacím úhlu s kontaktními čočkami</i> .....	52
<i>Tabulka 21. Při pozorovacím úhlu bez kontaktních čoček</i> .....	53
<i>Tabulka 22. Při fyzické zátěži člověka</i> .....	53